Catalyst 6500 シリーズ スイッチ ソフトウェア コンフィギュレーション ガイド

Software Release 8.5

Text Part Number: OL-7193-01-J

CONTENTS

はじめに

ここでは、『*Catalyst 6500 シリーズ スイッチ ソフトウェア コンフィギュレーション ガイド*』の対象読者、マニュアルの構成、および手順や情報を記述するための表記法について説明します。

対象読者

このマニュアルは、Catalyst 6500 シリーズ スイッチの設定および保守を担当する、経験豊富なネットワーク管理者を対象としています。

マニュアルの構成

（注） このマニュアルには、従来『*Catalyst 6000 Family Multilayer Switch Feature Card (12.x) and Policy Feature Card Configuration Guide*』に記載されていた情報が含まれています。

このマニュアルの構成は、次のとおりです。

章	タイトル	説明
第 1 章	製品の概要	Catalyst 6500 シリーズ スイッチの概要について説明します。
第 2 章	CLI	CLI（コマンドライン インターフェイス）について説明します。
第 3 章	スイッチの IP アドレスおよび デフォルト ゲートウェイの設定	スイッチを基本的なレベルで設定する方法について説明します。
第 4 章	イーサネット、ファスト イーサネット、ギガビット イーサネット、および 10 ギガビット イーサネット スイッチングの設定	イーサネット、ファスト イーサネット、およびギガビット イーサネット スイッチングを設定する手順について説明します。
第 5 章	イーサネット VLAN トランクの設定	ファスト イーサネット ポートおよびギガビット イーサネット ポート上で、ISL（スイッチ間リンク）および IEEE 802.1Q VLAN（仮想 LAN）トランクを設定する手順について説明します。
第 6 章	EtherChannel の設定	Fast EtherChannel および Gigabit EtherChannel ポート バンドルの設定手順について説明します。
第 7 章	IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングの設定	802.1Q トンネリングを設定する手順について説明します。
第 8 章	スパニングツリーの設定	Spanning-Tree Protocol（STP; スパニングツリー プロトコル）プロトコルの設定手順およびスパニングツリーの仕組みについて説明します。
第 9 章	スパニングツリー PortFast、UplinkFast、BackboneFast、およびループ ガードの設定	スパニングツリーの PortFast、UplinkFast、および BackboneFast 機能を設定する手順について説明します。
第 10 章	VTP の設定	スイッチ上で VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）を設定する手順について説明します。
第 11 章	VLAN の設定	スイッチ上で VLAN を設定する手順について説明します。
第 12 章	VLAN 間ルーティングの設定	Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）上で VLAN 間ルーティングを設定する手順について説明します。
第 13 章	CEF for PFC2 および CEF for PFC3A の設定	CEF for PFC2 を設定する手順について説明します。
第 14 章	MLS の設定	Multilayer Switching（MLS; マルチレイヤ スイッチング）を設定する手順について説明します。
第 15 章	アクセス制御の設定	Access Control List（ACL; アクセス制御リスト）を設定する手順について説明します。
第 16 章	NDE の設定	NetFlow Data Export（NDE; NetFlow データ エクスポート）を設定する手順について説明します。
第 17 章	GVRP の設定	スイッチ上で GARP VLAN Registration Protocol（GVRP）を設定する手順について説明します。

章	タイトル	説明
第 18 章	VMPS によるダイナミック ポート VLAN メンバーシップの設定	VLAN Management Policy Server（VMPS; VLAN マネージメント ポリシー サーバ）を使用してスイッチ上にダイナミック ポート VLAN メンバーシップを設定する手順を説明します。
第 19 章	ステータスおよび接続の確認	モジュールおよびスイッチ ポートの情報を表示する方法、ping、Telnet、および IP traceroute を使用して接続を確認する方法について説明します。
第 20 章	GOLD の設定	オンライン診断を設定する手順について説明します。
第 21 章	スイッチの管理	システム名を設定し、ログイン バナーを作成する手順、スイッチ上でその他の管理作業を実行する手順について説明します。
第 22 章	冗長機能の設定	Catalyst 6500 シリーズ スイッチに冗長スーパバイザ エンジンおよび MSFC を搭載して設定する手順について説明します。
第 23 章	NSF/SSO MSFC 冗長機能の設定	この章では、Cisco Nonstop Forwarding（NSF）/Stateful Switchover（SSO）を使用して MSFC 冗長性を設定する手順について説明します。
第 24 章	スイッチの起動設定の変更	BOOT 環境変数、コンフィギュレーション レジスタをはじめ、スイッチの起動設定を変更する手順について説明します。
第 25 章	フラッシュ ファイル システムの使用	フラッシュ ファイル システムに関連するさまざまな手順について説明します。
第 26 章	システム ソフトウェア イメージの操作	システム ソフトウェア イメージのダウンロードおよびアップロード手順について説明します。
第 27 章	コンフィギュレーション ファイルの操作	スイッチ コンフィギュレーション ファイルの作成、ダウンロード、およびアップロード手順について説明します。
第 28 章	システム メッセージ ロギングの設定	システム メッセージ ロギング（Syslog）機能を設定する手順について説明します。
第 29 章	DNS の設定	Domain Name System（DNS; ドメイン ネーム システム）を設定する手順について説明します。
第 30 章	CDP の設定	Cisco Discovery Protocol（CDP）を設定する手順について説明します。
第 31 章	UDLD の設定	Unidirectional Link Detection（UDLD; 単一方向リンク検出）プロトコルを設定する手順について説明します。
第 32 章	DHCP スヌーピングおよび IP ソースガードの設定	DHCP スヌーピングおよび IP 送信元ガードを設定する手順について説明します。
第 33 章	NTP の設定	Network Time Protocol（NTP）を設定する手順について説明します。
第 34 章	ブロードキャスト抑制の設定	ハードウェアおよびソフトウェアのブロードキャスト抑制を設定する手順について説明します。
第 35 章	レイヤ 3 プロトコル フィルタリングの設定	イーサネット ポート、ファスト イーサネット ポート、およびギガビット イーサネット ポート上でプロトコル フィルタリングを設定する手順について説明します。
第 36 章	IP 許可リストの設定	IP 許可リストを設定する手順について説明します。
第 37 章	ポート セキュリティの設定	セキュア ポート フィルタリングを設定する手順について説明します。
第 38 章	AAA によるスイッチ アクセスの設定	Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）を設定して、CLI へのアクセスをモニタし、制御する手順について説明します。
第 39 章	802.1X 認証の設定	802.1X 認証を設定する手順について説明します。
第 40 章	MAC 認証バイパスの設定	MAC 認証バイパスを設定する手順について説明します。
第 41 章	Web ベース プロキシ認証の設定	Web ベース プロキシ認証を設定する手順について説明します。

章	タイトル	説明
第 42 章	NAC の設定	Network Admission Control（NAC）を設定する手順について説明します。
第 43 章	ユニキャスト フラッディング ブロックの設定	ユニキャスト フラッディング ブロックを設定する手順について説明します。
第 44 章	SNMP の設定	SNMP（簡易ネットワーク管理プロトコル）を設定する手順について説明します。
第 45 章	RMON の設定	Remote Monitoring（RMON）機能を設定する手順について説明します。
第 46 章	SPAN および RSPAN の設定	Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）および Remote SPAN（RSPAN）を設定する手順について説明します。
第 47 章	スイッチ TopN レポートの使用方法	スイッチ TopN レポートを作成する手順について説明します。
第 48 章	マルチキャスト サービスの設定	Internet Group Management Protocol（IGMP）スヌーピング、GARP Multicast Registration Protocol（GMRP）、および Router Group Management Protocol（RGMP）を設定する手順について説明します。
第 49 章	QoS の設定	Quality of Service（QoS; サービス品質）を設定する手順について説明します。
第 50 章	自動 QoS の使用	自動 QoS 設定機能を使用する手順について説明します。
第 51 章	ASLB の設定	Accelerated Server Load Balancing（ASLB; Accelerated Server ロード バランシング）を設定する手順について説明します。
第 52 章	スイッチ ファブリック モジュールの設定	スイッチ ファブリック モジュールを設定する手順について説明します。
第 53 章	VoIP ネットワークの設定	VoIP ネットワークを設定する手順について説明します。
付録 A	略語	このマニュアルで使用している略語の一覧です。

関連資料

Catalyst 6500 シリーズ スイッチの関連資料は、次のとおりです。

- 『*Catalyst 6500 Series Switch Module Installation Guide*』
- 『*Catalyst 6500 Series Switch Installation Guide*』
- 『*Catalyst 6500 Series Switch Command Reference*』
- 『*ATM Software Configuration and Command Reference ― Catalyst 5000 Family and Catalyst 6000 Family Switches*』
- 『*Catalyst 6500 Series Switch System Message Guide*』
- 『*Release Notes for Catalyst 6500 Series Switch Software Release 7.x*』
- Cisco IOS のコンフィギュレーション ガイドおよびコマンド リファレンス ― MSFC、MSM、および Asynchronous Transfer Mode（ATM; 非同期転送モード）モジュール上で稼働する Cisco IOS ソフトウェアの設定に関して記載されています。
- MIB（管理情報ベース）については、次の URL を参照してください。
  http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

表記法

（注） このマニュアル全体を通じて、*スーパバイザ エンジン*という用語は、特に明記されていないかぎり Supervisor Engine 1、Supervisor Engine 2、および Supervisor Engine 720 を意味します。*MSFC* という用語は、特に明記されていないかぎり MSFC、MSFC2、および MSFC3 を意味します。

このマニュアルでは、次の表記法を使用しています。

表記	説明
太字	コマンド、コマンド オプション、およびキーワードは**太字**で示しています。
イタリック体	ユーザが値を指定する引数は、*イタリック体*で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{ x | y | z }	必ずどれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
ストリング	引用符を付けない一組の文字。ストリングの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてストリングとみなされます。
`screen` フォント	システムが表示する端末セッションおよび情報は、`screen` フォントで示しています。
太字の **`screen`** フォント	ユーザが入力しなければならない情報は、**太字**の **`screen`** フォントで示しています。
*イタリック体*の *`screen`* フォント	ユーザが値を指定する引数は、*イタリック体*の *`screen`* フォントで示しています。
⟶	このポインタは、例の中の重要な行を強調しています。
^	^ 記号は、Ctrl キーを表します。たとえば、画面に表示される ^D というキーの組み合わせは、Ctrl キーを押しながら D キーを押すことを意味します。
< >	パスワードのように出力されない文字は、かぎカッコ（< >）で囲んで示しています。

（注）は、次のように表しています。

（注） 「*注釈*」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

注意は、次のように表しています。

注意 「*要注意*」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

マニュアルの入手方法

シスコ製品のマニュアルおよびその他の資料は、Cisco.com で入手することができます。また、テクニカル サポートおよびその他のテクニカル リソースは、さまざまな方法で入手することができます。ここでは、シスコ製品に関する技術情報を入手する方法について説明します。

Cisco.com

シスコの最新のマニュアルは、次の URL からアクセスしてください。

http://www.cisco.com/techsupport

シスコの Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com

http://www.cisco.com/jp

シスコの Web サイトの各国語版へは、次の URL からアクセスしてください。

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

シスコ製品のマニュアルおよびその他の資料は、製品に付属の Product Documentation DVD パッケージでご利用いただけます。Product Documentation DVD は定期的に更新されるので、印刷資料よりも新しい情報が得られます。

Product Documentation DVD は、ポータブル メディアに収容された、技術的な製品マニュアルの総合的なライブラリです。この DVD を使用すると、シスコ製品の各種バージョンのハードウェアのインストレーション、ソフトウェアのインストール、設定、およびコマンドに関するガイドにアクセスし、HTML で技術マニュアルを表示できます。DVD を使用することで、インターネットに接続しなくてもシスコの Web サイトと同じマニュアルを参照できます。製品によっては、マニュアルの PDF バージョンも用意されています。

Product Documentation DVD は単独または購読契約で入手できます。Cisco.com（Cisco Direct Customers）に登録されている場合、Cisco Marketplace から Cisco Documentation DVD（Customer Order Number DOC-DOCDVD=）を発注できます。次の URL にアクセスしてください。

http://www.cisco.com/go/marketplace/

マニュアルの発注方法

Cisco.com に登録されている場合、2005 年 6 月 30 日から、次の URL にある Cisco Marketplace の Product Documentation Store でシスコ製品のマニュアルを発注できます。

http://www.cisco.com/go/marketplace/

Cisco.com に登録されていない場合、製品を購入された代理店へお問い合わせください。

シスコ製品のセキュリティ

シスコでは、無償の Security Vulnerability Policy ポータルを次の URL で提供しています。

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

このサイトから、以下のタスクを実行できます。

- シスコ製品における脆弱性を報告する。
- シスコ製品のセキュリティ問題に対する支援を受ける。
- シスコからのセキュリティ情報を入手するために登録を行う。

シスコ製品に関するセキュリティ勧告および注意のリストが以下の URL で確認できます。

http://www.cisco.com/go/psirt

勧告および注意事項が変更された際に、リアルタイムで確認したい場合は、以下の URL から Product Security Incident Response Team Really Simple Syndication（PSIRT RSS）にアクセスできます。

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

シスコ製品のセキュリティ問題の報告

シスコでは、安全な製品を提供することを目指しています。製品のリリース前に社内でテストを実施し、すべての脆弱性を迅速に修正するように努めております。お客様がシスコ製品の脆弱性を発見したと思われる場合は、次の PSIRT にご連絡ください。

- 緊急度の高い問題 — security-alert@cisco.com

  緊急度の高い問題とは、システムが激しい攻撃を受けている状態、または急を要する深刻なセキュリティの脆弱性を報告する必要がある状態を指します。それ以外の状態はすべて、緊急度の低い問題とみなされます。
- 緊急度の低い問題 — psirt@cisco.com

緊急度の高い問題の場合、次の電話番号で PSIRT に問い合わせることができます。

- 1 877 228-7302
- 1 408 525-6532

ヒント お客様が第三者に知られたくない情報をシスコに送信する場合、Pretty Good Privacy（PGP）または PGP と互換性のある製品を使用して情報を暗号化することを推奨します。PSIRT は、PGP バージョン 2.*x* ～ 8.*x* と互換性のある暗号化情報を取り扱うことができます。

無効な暗号鍵または失効した暗号鍵は使用しないでください。PSIRT と通信する際に使用する有効な公開鍵は、次の URL にある Security Vulnerability Policy ページの Contact Summary の項にリンクされたものです。

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

このページのリンクには、現在使用中の PGP 鍵の ID が含まれます。

テクニカル サポート

Cisco Technical Support では、評価の高い 24 時間体制のテクニカル サポートを提供しています。Cisco.com の Cisco Technical Support & Documentation Web サイトでは、広範囲にわたるオンラインでのサポート リソースを提供しています。さらに、シスコシステムズとサービス契約を結んでいる場合は、Technical Assistance Center（TAC）のエンジニアによる電話サポートも提供されます。シスコシステムズとサービス契約を結んでいない場合は、リセラーにお問い合わせください。

Cisco Technical Support & Documentation Web サイト

Cisco Technical Support & Documentation Web サイトでは、オンラインで資料やツールを利用して、トラブルシューティングやシスコ製品およびテクノロジーに関する技術上の問題の解決に役立てることができます。この Web サイトは 24 時間ご利用いただけます。次の URL にアクセスしてください。

http://www.cisco.com/techsupport

Cisco Technical Support & Documentation Web サイト上のツールにアクセスする際は、いずれも Cisco.com のログイン ID およびパスワードが必要です。サービス契約が有効で、ログイン ID またはパスワードを取得していない場合は、次の URL で登録手続きを行ってください。

http://tools.cisco.com/RPF/register/register.do

（注） テクニカル サポートにお問い合わせいただく前に、Cisco Product Identification（CPI）ツールを使用して、製品のシリアル番号をご確認ください。CPI ツールへは、Documentation & Tools の下にある **Tools & Resources** リンクをクリックして、Cisco Technical Support & Documentation Web サイトからアクセスできます。Alphabetical Index ドロップダウン リストから **Cisco Product Identification Tool** を選択するか、Alerts & RMAs の下にある **Cisco Product Identification Tool** リンクをクリックしてください。CPI ツールは、製品 ID またはモデル名、ツリー表示、または特定の製品に対する **show** コマンド出力のコピー＆ペーストによる 3 つの検索オプションを提供します。検索結果には、シリアル番号のラベルの場所がハイライトされた製品の説明図が表示されます。テクニカル サポートにお問い合わせいただく前に、製品のシリアル番号のラベルを確認し、メモなどに控えておいてください。

Japan TAC Web サイト

Japan TAC Web サイトでは、利用頻度の高い TAC Web サイト（http://www.cisco.com/tac）のドキュメントを日本語で提供しています。Japan TAC Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/jp/go/tac

サポート契約を結んでいない方は、「ゲスト」としてご登録いただくだけで、Japan TAC Web サイトのドキュメントにアクセスできます。

Japan TAC Web サイトにアクセスするには、Cisco.com のログイン ID とパスワードが必要です。ログイン ID とパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://www.cisco.com/jp/register/

Service Request ツールの使用

オンラインの TAC Service Request ツールを使えば、S3 および S4 の問題について最も迅速にテクニカル サポートを受けられます（ネットワークの障害が軽微である場合、あるいは製品情報が必要な場合）。状況をご説明いただくと、TAC Service Request ツールが推奨される解決方法を提供します。これらの推奨リソースを使用しても問題が解決しない場合は、シスコの技術者が対応します。TAC Service Request ツールは次の URL からアクセスできます。

http://www.cisco.com/techsupport/servicerequest

問題が S1 または S2 であるか、インターネットにアクセスできない場合は、電話で TAC にご連絡ください（運用中のネットワークがダウンした場合、あるいは重大な障害が発生した場合）。S1 および S2 の問題にはシスコの技術者がただちに対応し、業務を円滑に運営できるよう支援します。

電話でテクニカル サポートを受ける際は、次の番号のいずれかをご使用ください。

アジア太平洋：+61 2 8446 7411（オーストラリア：1 800 805 227）
EMEA：+32 2 704 55 55
米国：1 800 553-2447

TAC の連絡先一覧については、次の URL にアクセスしてください。

http://www.cisco.com/techsupport/contacts

問題の重大度の定義

すべての問題を標準形式で報告するために、問題の重大度を定義しました。

重大度 1（S1）— ネットワークがダウンし、業務に致命的な損害が発生する場合。24 時間体制であらゆる手段を使用して問題の解決にあたります。

重大度 2（S2）— ネットワークのパフォーマンスが著しく低下、またはシスコ製品のパフォーマンス低下により業務に重大な影響がある場合。通常の業務時間内にフルタイムで問題の解決にあたります。

重大度 3（S3）— ネットワークのパフォーマンスが低下しているが、ほとんどの業務運用が機能している場合。通常の業務時間内にサービスの復旧を行います。

重大度 4（S4）— シスコ製品の機能、インストレーション、基本的なコンフィギュレーションについて、情報または支援が必要で、業務への影響がほとんどまたはまったくない場合。

その他の資料および情報の入手方法

シスコの製品、テクノロジー、およびネットワーク ソリューションに関する情報について、さまざまな資料をオンラインおよび印刷物で入手することができます。

- Cisco Marketplace では、さまざまなシスコの書籍、参考資料、マニュアル、およびロゴ入り商品を提供しています。Cisco Marketplace には、次の URL からアクセスしてください。

  http://www.cisco.com/go/marketplace/

- Cisco Press では、ネットワーク、トレーニング、認定関連の出版物を幅広く発行しています。初心者から上級者まで、さまざまな読者向けの出版物があります。Cisco Press の最新の出版情報などについては、次の URL からアクセスしてください。

  http://www.ciscopress.com

- 『*Packet*』は、シスコシステムズが発行するテクニカル ユーザ向けの季刊誌で、インターネットやネットワークへの投資を最大限に活用するのに役立ちます。『*Packet*』には、ネットワーク分野の最新動向、テクノロジーの進展、およびシスコの製品やソリューションに関する記事をはじめ、ネットワークの配置やトラブルシューティングのヒント、設定例、お客様の事例研究、認定やトレーニングに関する情報、および多数の詳細なオンライン リソースへのリンクが盛り込まれています。『*Packet*』には、次の URL からアクセスしてください。

  http://www.cisco.com/packet

- 『*iQ Magazine*』は、シスコのテクノロジーを使って収益の増加、ビジネス効率の向上、およびサービスの拡大を図る方法について学ぶことを目的とした、シスコシステムズが発行する成長企業向けの季刊誌です。この季刊誌は、実際の事例研究や事業戦略を用いて、これら企業が直面するさまざまな課題や、問題解決の糸口となるテクノロジーを明確化し、テクノロジーの投資に関して読者が正しい決断を行う手助けをします。『*iQ Magazine*』には、次の URL からアクセスしてください。

  http://www.cisco.com/go/iqmagazine

  または次の URL でデジタル版をご覧いただけます。

  http://ciscoiq.texterity.com/ciscoiq/sample/

- 『*Internet Protocol Journal*』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコシステムズが発行する季刊誌です。『*Internet Protocol Journal*』には、次の URL からアクセスしてください。

  http://www.cisco.com/ipj

- シスコシステムズが提供するネットワーク製品およびカスタマー サポート サービスについては、次の URL からアクセスしてください。

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection は、ネットワーキング専門家がネットワーキング製品やネットワーキング技術に関する質問、提案、情報をシスコの専門家および他のネットワーキング専門家と共有するためのインタラクティブな Web サイトです。ディスカッションに参加するには、次の URL にアクセスしてください。

  http://www.cisco.com/discuss/networking

- シスコシステムズは最高水準のネットワーク関連のトレーニングを実施しています。トレーニングの最新情報については、次の URL からアクセスしてください。

  http://www.cisco.com/en/US/learning/index.html

CHAPTER 1

製品の概要

Catalyst 6500 シリーズ スイッチは、次の構成をサポートします。

- Supervisor Engine 32、およびオンボード コンポーネントである Policy Feature Card 3B（PFC3B; ポリシー フィーチャ カード 3B）または PFC3BXL、および Multilayer Switch Feature Card 2A（MSFC2A; マルチレイヤ スイッチ フィーチャ カード 2A）
- Supervisor Engine 720、およびオンボード コンポーネントである PFC3A、PFC3B、または PFC3BXL、MSFC3、および 720 Gbps 統合スイッチ ファブリック
- Supervisor Engine 2、PFC2、および MSFC2
- Supervisor Engine 2 および PFC2
- Supervisor Engine 1、PFC、および MSFC または MSFC2
- Supervisor Engine 1 および PFC
- Supervisor Engine 1

Catalyst 6500 シリーズ スイッチでサポートされるシャーシ、モジュール、ソフトウェア機能、プロトコル、および MIB（管理情報ベース）の詳細については、『*Release Notes for Catalyst 6500 Series Switch Software Release 8.x*』を参照してください。

(注) このマニュアル全体を通じて、*スーパバイザ エンジン*という用語は、特に明記されていないかぎり Supervisor Engine 1、Supervisor Engine 2、Supervisor Engine 720、および Supervisor Engine 32 を意味します。*MSFC* という用語は、特に明記されていないかぎり MSFC、MSFC2、MSFC2A、および MSFC3 を意味します。*PFC3* という用語は、特に明記されていないかぎり、PFC3A、PFC3B、または PFC3BXL を意味します。

(注) このマニュアルには、従来『*Catalyst 6000 Family Multilayer Switch Feature Card (12.x) and Policy Feature Card Configuration Guide*』に記載されていた情報が含まれています。

(注) このマニュアルで使用する Cisco IOS コマンドの詳細については、『*Catalyst 6500 Series Switch MSFC IOS Command Reference*』を参照してください。次の URL からアクセスできます。

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/index.htm

CHAPTER 2

CLI

この章では、Catalyst 6500 シリーズ スイッチ モジュールを設定するために使用する CLI（コマンド ライン インターフェイス）について説明します。スイッチ コマンドおよび ROM モニタ コマンドについては、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

(注) Asynchronous Transfer Mode（ATM; 非同期転送モード）Cisco IOS の CLI およびコマンドについては、『*ATM Software Configuration Guide and Command Reference ― Catalyst 5000 Family and 6000 Family Switches*』を参照してください。

この章で説明する内容は、次のとおりです。

Catalyst CLI

ここでは、Catalyst CLI について説明します。

ROM モニタの CLI

ROM モニタは、プラットフォームの電源投入時、リセット時、または重大な例外が発生したときに実行される ROM ベースのプログラムです。ROM モニタ モードが開始されるのは、スイッチが有効なシステム イメージを見つけることができなかった場合、NVRAM 内の設定が壊れていた場合、またはコンフィギュレーション レジスタが ROM モニタ モードを開始するように設定されていた場合です。ROM モニタ モードで、フラッシュ メモリ、ネットワーク サーバ ファイル、またはブートフラッシュからシステム イメージを手動でロードできます。

スイッチを再起動し、起動から 60 秒以内に **Break** キーを押すと、ROM モニタ モードを開始できます。

(注)　コンフィギュレーション レジスタの設定値で Break キーがオフに設定されているかどうかに関係なく、システムの再起動から 60 秒間は、Break キーが常に有効です。

端末サーバから ROM モニタにアクセスするには、Telnet プロンプトに戻って、端末エミュレーション プログラムに対して **send break** コマンドを入力し、ROM モニタ モードを開始します。

ROM モニタ モードが開始されると、プロンプトが rommon> になります。**?** コマンドを使用して、使用できる ROM モニタ コマンドを表示します。

スイッチ CLI

スイッチの CLI は、UNIX の C シェルに類似した基本的なコマンドライン インタープリタです。

ここでは、スイッチ CLI を使用する手順について説明します。

スイッチ CLI へのアクセス

CLI には、スーパバイザ エンジンのコンソール ポートまたは Telnet セッションを介してアクセスします。

ここでは、スイッチ CLI にアクセスする手順について説明します。

コンソール ポートから CLI にアクセスする場合

コンソール ポートからスイッチの CLI にアクセスするには、EIA/TIA-232（RS-232）ケーブルを使用して、コンソール端末をコンソール ポートに接続する必要があります。

（注） スーパバイザ エンジンのコンソール ポートに接続する詳しい手順については、各スイッチのハードウェアのマニュアルを参照してください。

コンソール ポートからスイッチにアクセスする手順は、次のとおりです。

	作業	コマンド
ステップ 1	端末からスイッチ コンソール プロンプトへの接続を開始し、**Return** キーを押します。	–
ステップ 2	プロンプトで、システム パスワードを入力します。Console> プロンプトが表示されます。これは CLI にユーザ モードでアクセスしたことを表します。	–
ステップ 3	必要な場合、イネーブル モードを開始します（スイッチの設定を変更するには、イネーブル モードを開始する必要があります）。	**enable**
ステップ 4	必要なコマンドを入力して、作業を行います。	–
ステップ 5	作業が終わったら、セッションを終了します。	**exit**

コンソール ポートからスイッチにアクセスすると、次のように表示されます。

```
Cisco Systems Console
Enter password:
Console>
```

Telnet で CLI にアクセスする場合

スイッチとの Telnet セッションを開始するには、まず最初にスイッチの IP アドレスを設定する必要があります。IP アドレスの設定手順については、「帯域内（sc0 および sc1）インターフェイス IP アドレスの割り当て」（p.3-8）を参照してください。同時に最高 8 つの Telnet セッションを利用できます。Telnet セッションがアイドル状態のまま所定の時間が経過すると、そのセッションは自動的に切断されます。

Telnet を使用してリモート ホストからスイッチ CLI にアクセスする手順は、次のとおりです。

	作業	コマンド
ステップ 1	リモート ホストから **telnet** コマンド、およびアクセスするスイッチの名前または IP アドレスを入力します。	**telnet** {*hostname* | *ip_addr*}
ステップ 2	プロンプトに CLI のパスワードを入力します。パスワードを設定していない場合は、**Return** キーを押します。	–
ステップ 3	必要なコマンドを入力して、作業を行います。	–
ステップ 4	作業が終わったら、Telnet セッションを終了します。	**exit**

次に、スイッチとの Telnet セッションをオープンする例を示します。

```
unix_host% telnet Catalyst_1
Trying 172.16.10.10...
Connected to Catalyst_1.
Escape character is '^]'.


Cisco Systems Console



Enter password:
Catalyst_1>
```

スイッチから MSFC にアクセスする場合

ここでは、直接接続されたコンソール ポートまたは Telnet セッションから Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）にアクセスする方法について説明します。

- コンソール ポートから MSFC にアクセスする場合（p.2-4）
- Telnet セッションから MSFC にアクセスする場合（p.2-5）

「MSFC CLI」（p.2-9）を参照してください。

コンソール ポートから MSFC にアクセスする場合

switch console コマンドを使用して、スーパバイザ エンジンのコンソール ポートに直接接続されたスイッチ CLI から MSFC にアクセスします。MSFC CLI を終了してスイッチの CLI に戻るには、Router> プロンプトに対して **Ctrl-C** を 3 回入力します。

スイッチ CLI から MSFC にアクセスする手順は、次のとおりです。

作業	コマンド
スイッチ CLI から MSFC にアクセスします。	**switch console** [*mod*][1]

1. *mod* 引数は、MSFC のモジュール番号を指定します。モジュール番号 15 は、MSFC がスロット 1 のスーパバイザ エンジンに搭載されていることを示します。モジュール番号 16 は、MSFC がスロット 2 のスーパバイザ エンジンに搭載されていることを示します。Supervisor Engine 720 の場合、*mod* 引数は MSFC3 のモジュール番号を指定します。モジュール番号 15 は、MSFC3 がスロット 5（6 または 9 スロットのスイッチ）またはスロット 7（13 スロットのスイッチ）にある Supervisor Engine 720 に搭載されていることを示します。モジュール番号 16 は、MSFC3 がスロット 6（6 または 9 スロットのスイッチ）またはスロット 8（13 スロットのスイッチ）にある Supervisor Engine 720 に搭載されていることを示します。

（注） モジュール番号を指定しない場合、コンソールはアクティブ スーパバイザ エンジン上の MSFC に切り替わります。

（注） スタンバイ MSFC の Cisco IOS CLI にアクセスするには、そのスタンバイ スーパバイザ エンジンのコンソール ポートに接続します。

次に、スイッチ CLI からアクティブ スーパバイザ エンジンのアクティブ MSFC にアクセスし、MSFC CLI を終了してスイッチ CLI に戻る例を示します。

```
Console> (enable) switch console 15
Trying Router-15...
Connected to Router-15.
Type ^C^C^C to switch back...
Router> ^C^C^C
Console> (enable)
```

Telnet セッションから MSFC にアクセスする場合

session *mod* コマンドを入力して、スイッチ CLI から Telnet セッションによって MSFC にアクセスします。MSFC CLI を終了してスイッチ CLI に戻るには、Router> プロンプトで **^]** または **exit** コマンドを入力します。

（注） *mod* 引数は、MSFC のモジュール番号を指定します。モジュール番号 15 は、MSFC がスロット 1 のスーパバイザ エンジンに搭載されていることを示します。モジュール番号 16 は、MSFC がスロット 2 のスーパバイザ エンジンに搭載されていることを示します。Supervisor Engine 720 の場合、*mod* 引数は MSFC3 のモジュール番号を指定します。モジュール番号 15 は、MSFC3 がスロット 5（6 または 9 スロットのスイッチ）またはスロット 7（13 スロットのスイッチ）にある Supervisor Engine 720 に搭載されていることを示します。モジュール番号 16 は、MSFC3 がスロット 6（6 または 9 スロットのスイッチ）またはスロット 8（13 スロットのスイッチ）にある Supervisor Engine 720 に搭載されていることを示します。

次に、スイッチ CLI から MSFC にアクセスし、MSFC CLI を終了してスイッチ CLI に戻る例を示します。

```
Console> (enable) session 15
Trying Router-15...
Connected to Router-15.
Escape character is '^]'.
Router> exit
Console> (enable)
```

CLI の操作

ここでは、スイッチ CLI の操作手順について説明します。

- スイッチ CLI コマンドのモード（p.2-5）
- コマンドラインでのモジュール、ポート、および VLAN の指定（p.2-6）
- MAC アドレス、IP アドレス、および IP エイリアスの指定（p.2-7）
- コマンドラインの編集（p.2-7）
- ヒストリ置換（p.2-8）
- コマンド ヘルプの利用方法（p.2-8）

スイッチ CLI コマンドのモード

スイッチ CLI は、2 つの操作モード、ユーザ モードとイネーブル モードをサポートします。どちらのモードもパスワードで保護されます。ユーザ モード コマンドは、日常的なシステム モニタリング作業に使用します。イネーブル モード コマンドは、システムを設定し、基本的なトラブルシューティングを実行する場合に使用します。

ログイン後、システムは自動的にユーザ モードになり、ユーザ モード コマンドだけが使用できます。イネーブル モードにアクセスするには、**enable** コマンドと、その後ろにイネーブル モード パスワードを入力します。イネーブル モードを終了してユーザ モードに戻るには、プロンプトに **disable** コマンドを入力します。

次に、イネーブル モードにアクセスする例を示します。

```
Console> enable
Enter Password: <password>
Console> (enable)
```

コマンドラインでのモジュール、ポート、および VLAN の指定

スイッチ コマンドに大文字と小文字の区別はありません。また、コマンドおよびパラメータは、現在使用可能な他のコマンドおよびパラメータと明確に区別できる文字数まで、省略することが可能です。

Catalyst 6500 シリーズ スイッチは、マルチモジュール システムです。CLI から入力したコマンドは、システム全体に適用することも、特定のモジュール、ポート、または VLAN（仮想 LAN）に適用することもできます。

モジュール、ポート、および VLAN には、1 から始まる番号が順番に与えられます。スーパバイザ エンジンはモジュール 1 で、スロット 1 に搭載します。スイッチに冗長スーパバイザ エンジンが搭載されている場合は、スロット 1 とスロット 2 にスーパバイザ エンジンを搭載します。Supervisor Engine 720 は、6 または 9 スロットのスイッチの場合はモジュール 5 で、スロット 5 に搭載します。また、13 スロットのスイッチの場合はモジュール 7 で、スロット 7 に搭載します。冗長 Supervisor Engine 720 を使用する場合、6 または 9 スロットのスイッチではスロット 5 と 6、13 スロットのスイッチではスロット 7 と 8 に Supervisor Engine 720 を搭載します。

特定のモジュールを指定するには、モジュール番号を使用します。

ポート 1 は常に左端のポートです。特定モジュールの特定ポートを指定するには、*mod/port* というコマンド構文を使用します。たとえば、**3/1** はモジュール 3 のポート 1 を表します。**set trunk** および **set port channel** などの一部のコマンドでは、ポートのリストを指定できます。

複数のポートを指定するには、カンマで区切って（スペースを入れずに）個々のポートを指定するか、2 つのポート番号をハイフン（-）でつないでポート範囲を指定します。ハイフンの方がカンマより優先されます。

表 2-1 に、ポートおよびポート範囲の指定例を示します。

表 2-1　ポートおよびポート範囲の指定

例	機能
`2/1`	モジュール 2 のポート 1 を指定します。
`3/4-8`	モジュール 3 のポート 4、5、6、7、8 を指定します。
`5/2,5/4,6/10`	モジュール 5 のポート 2 およびポート 4 を指定し、さらにモジュール 6 のポート 10 を指定します。
`3/1-2,4/8`	モジュール 3 のポート 1 およびポート 2 を指定し、さらにモジュール 4 のポート 8 を指定します。

VLAN は、各 VLAN に 1 つずつ対応付けられた番号である VLAN ID によって識別します。VLAN のリストを指定するには、カンマで区切って（スペースを入れずに）個々の VLAN を指定するか、2 つの VLAN 番号をハイフン（-）でつないで VLAN 範囲を指定します。

表 2-2 に、VLAN および VLAN 範囲の指定例を示します。

表 2-2　VLAN および VLAN 範囲の指定

例	機能
10	VLAN 10 を指定します。
5,10,15	VLAN 5、10、15 を指定します。
10-50,500	VLAN 10 ～ 50（両端を含む）および VLAN 500 を指定します。

MAC アドレス、IP アドレス、および IP エイリアスの指定

一部のコマンドでは、MAC（メディア アクセス制御）アドレス、IP アドレス、または IP エイリアスを標準形式で指定する必要があります。MAC アドレスの形式は、次のように、6 つの 16 進数字をハイフンで区切って指定します。

```
00-00-0c-24-d2-fe
```

IP アドレスの形式は 32 ビットであり、次のように、ネットワーク セクション、オプションのサブネット セクション、およびホスト セクションを表す 4 つのオクテットをピリオドで区切って指定します（ドット付き 10 進表記）。

```
126.2.54.1
```

スイッチ上で IP エイリアスを設定している場合は、ドット付き 10 進表記の IP アドレスの代わりに IP エイリアスを使用できます。IP エイリアスは、IP アドレスまたは IP エイリアスを定義するコマンドを除き、IP アドレスを使用するほとんどのコマンドに使用できます。IP エイリアスの使用方法については、「スイッチ上での IP エイリアスの定義」（p.21-8）を参照してください。

スイッチ上で Domain Name System（DNS; ドメイン ネーム システム）を設定している場合、IP アドレスの代わりに DNS ホスト名を使用できます。DNS の設定手順については、第 29 章「DNS の設定」を参照してください。

コマンドラインの編集

最後に入力した 20 個のコマンドは、ヒストリ バッファに保存されます。これらのコマンドをスクロールし、プロンプトからコマンドを入力したり編集したりすることができます。表 2-3 に、スイッチ コマンドを入力および編集するときに使用するキーボード ショートカットを示します。

表 2-3　コマンドライン編集用キーボード ショートカット

キーストローク	機能
Ctrl-A	コマンドラインの先頭文字に移動します。
Ctrl-B または左矢印キー	カーソルを 1 文字分だけ後退させます。
Ctrl-C	エスケープしてプロンプトおよび作業を打ち切ります。
Ctrl-D	カーソル位置の文字を削除します。
Ctrl-E	現在のコマンドラインの末尾に移動します。
Ctrl-F または右矢印キー[1]	カーソルを 1 文字分だけ進めます。
Ctrl-K	カーソル位置からコマンドラインの末尾までを削除します。
Ctrl-L、Ctrl-R	現在のコマンドラインを改行して繰り返します。
Ctrl-N または下矢印キー [1]	ヒストリ バッファ内の次のコマンドラインを入力します。
Ctrl-P または上矢印キー [1]	ヒストリ バッファ内の 1 つ前のコマンドラインを入力します。

表 2-3　コマンドライン編集用キーボード ショートカット（続き）

キーストローク	機能
Ctrl-U、Ctrl-X	カーソル位置からコマンドラインの先頭までを削除します。
Ctrl-W	最後に入力した単語を削除します。
Esc B	単語 1 つ分だけカーソルを後退させます。
Esc D	カーソルから単語の末尾までを削除します。
Esc F	単語 1 つ分だけカーソルを進めます。
Delete キーまたは Backspace キー	コマンド入力時の誤りを消去し、このキーに続けてコマンドを再入力します。

1. 矢印キーは、VT100 などの ANSI 互換端末に限って有効です。

ヒストリ置換

ヒストリ バッファには、端末セッションで最後に入力した 20 個のコマンドが保存されます。ヒストリ置換により、特殊な省略形式のコマンドを使用して、再入力せずにこれらのコマンドにアクセスできます。表 2-4 に、ヒストリ置換コマンドを示します。

表 2-4　ヒストリ置換コマンド

コマンド	機能
最近入力したコマンドを反復する場合	
!!	最後に入力したコマンドを反復
!-nn	最後から *nn* 番めのコマンドを反復
!n	コマンド *n* を反復
!aaa	文字列 *aaa* から始まるコマンドを反復
!?aaa	文字列 *aaa* を含むコマンドを反復
最後に入力したコマンドを変更して反復する場合	
^aaa^bbb	最後に入力したコマンドの文字列 *aaa* を文字列 *bbb* に置換
前に入力したコマンドの末尾に文字列を追加して反復する場合	
!!aaa	最後に入力したコマンドの末尾に文字列 *aaa* を追加
!n aaa	コマンド *n* の末尾に文字列 *aaa* を追加
!aaa bbb	文字列 *aaa* から始まるコマンドの末尾に文字列 *bbb* を追加
!?aaa bbb	文字列 *aaa* が含まれるコマンドの末尾に文字列 *bbb* を追加

コマンド ヘルプの利用方法

ユーザ モードまたはイネーブル モードで、**help** または **?** と入力すると、そのモードで使用できるコマンドが表示されます。特定のコマンドの後ろに **help** または **?** を入力すると、コマンドの使用方法などの補足説明が表示されます。コマンドの入力時に引数の数を間違えた場合、または無効な引数を指定した場合には、コマンドの使い方、ヘルプ メニュー、および該当する場合にはパラメータ範囲が表示されます。また、**help** または **?** をコマンド カテゴリに追加すると、そのカテゴリのコマンド リストが表示されます。

MSFC CLI

ここでは、MSFC CLI について説明します。

(注)　「スイッチから MSFC にアクセスする場合」（p.2-4）で説明した方法に加えて、MSFC に Telnet で直接アクセスするように Cisco IOS ソフトウェアを設定できます。次の URL にある『*Cisco IOS Security Configuration Guide*』の「Configuring Authentication」を参照してください。
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/scprt1/scdathen.htm

Cisco IOS コマンド モード

Cisco IOS のユーザ インターフェイスには、さまざまなモードがあります。現在のモードによって、使用できるコマンドが決まります。現在のモードで使用できるコマンドのリストを表示するには、システム プロンプトで疑問符（?）を入力します。詳細については、「Cisco IOS コマンドおよび構文のリスト表示」（p.2-10）を参照してください。

スイッチ上でセッションを開始するときは、ユーザ モード（別名ユーザ EXEC モード）で始めます。EXEC モードでは、限られた一部のコマンドしか使用できません。すべてのコマンドを使用できるようにするには、イネーブル EXEC モードを開始しなければなりません。イネーブル EXEC モードにアクセスするには、通常、パスワードの入力が必要です。イネーブル EXEC モードでは、任意の EXEC コマンドを入力できるほか、グローバル コンフィギュレーション モードにアクセスできます。EXEC コマンドのほとんどは、**show** コマンド（現在のコンフィギュレーション ステータスを表示）、**clear** コマンド（カウンタまたはインターフェイスを消去）などのように、一回かぎりのコマンドです。スイッチを再起動しても EXEC コマンドが保存されることはありません。

コンフィギュレーション モードでは、実行コンフィギュレーションの変更を行うことができます。設定をあとで保存した場合、スイッチの再起動後もコマンドが保存されています。最初にグローバル コンフィギュレーション モードを開始する必要があります。グローバル コンフィギュレーション モードから、インターフェイス コンフィギュレーション モード、サブインターフェイス コンフィギュレーション モード、および各種プロトコル固有のモードを開始できます。

ROM モニタ モードは、スイッチが正常に起動できない場合に使用する個別のモードです。たとえば、スイッチの起動時に有効なシステム イメージが見つからない場合、またはスイッチのコンフィギュレーション ファイルが壊れている場合に、スイッチで ROM モニタ モードが開始される場合があります。詳細については、「ROM モニタの CLI」（p.2-2）を参照してください。

表 2-5 に、使用頻度の高い Cisco IOS モードを示します。

表 2-5　使用頻度の高い Cisco IOS コマンド モード

モード	用途の説明	アクセス方法	プロンプト
ユーザ EXEC	リモート装置への接続、端末の一時的な設定変更、基本的なテストの実行、およびシステム情報の表示。	ログインします。	`Router>`
イネーブル EXEC	動作パラメータの設定。イネーブル コマンド セットには、ユーザ EXEC モードのコマンドのほかに **configure** コマンドが含まれます。このコマンドを使用して、別のコマンド モードにアクセスします。	ユーザ EXEC モードで、**enable** コマンドおよびイネーブル パスワードを入力します。	`Router#`
グローバル コンフィギュレーション	システム全体に影響を及ぼす機能の設定。	イネーブル EXEC モードで、**configure terminal** コマンドを入力します。	`Router(config)#`
インターフェイス コンフィギュレーション	インターフェイス別に使用できるさまざまな機能があります。インターフェイス コマンドは、ギガビット イーサネットまたはファスト イーサネット インターフェイスの動作をイネーブルにし、変更します。	グローバル コンフィギュレーション モードで、**interface** *type location* コマンドを入力します。	`Router(config-if)#`
コンソール コンフィギュレーション	直接接続されたコンソールまたは Telnet 接続による仮想端末から、このコンフィギュレーション モードを使用してコンソール インターフェイスを設定します。	グローバル コンフィギュレーション モードで、**line console 0** コマンドを入力します。	`Router(config-line)#`

ユーザが入力したコマンドは、Cisco IOS コマンド インタープリタ（別名 EXEC）によって解析および実行されます。コマンドを入力する際、他のコマンドと区別がつく文字数だけを入力することにより、コマンドおよびキーワードを省略できます。たとえば、**show** コマンドは **sh**、**configure terminal** コマンドは **config t** と省略できます。

exit と入力すると、スイッチは 1 レベル前に戻ります。コンフィギュレーション モードを完全に終了してイネーブル EXEC モードに戻るには、**Ctrl-Z** キーを押します。

Cisco IOS コマンドおよび構文のリスト表示

どのコマンド モードでも、疑問符（?）を入力することにより、使用できるコマンドのリストを表示できます。

```
Router> ?
```

特定の文字シーケンスで始まるコマンドのリストを表示するには、それらの文字を入力し、その後ろに疑問符（?）を入力します。スペースは入れないでください。この形式のヘルプは、ユーザに代わって 1 つの単語を完成させるので、ワード ヘルプといいます。

```
Router# co?
configure
```

キーワードまたは引数のリストを表示するには、キーワードまたは引数の代わりに疑問符を入力します。疑問符の前にスペースを 1 つ入れてください。この形式のヘルプは、すでに入力したコマンド、キーワード、および引数に基づいて、使用できるキーワードまたは引数を表示するので、コマンド構文ヘルプといいます。

```
Router# configure ?
   memory                Configure from NV memory
   network               Configure from a TFTP network host
   overwrite-network     Overwrite NV memory from TFTP network host
   terminal              Configure from the terminal
```

前に入力したコマンドを再表示するには、上矢印キーまたは **Ctrl-P** キーを押します。上矢印キーを続けて押すことにより、直前に入力した 20 個のコマンドを表示できます。

ヒント　コマンドの入力について問題が生じた場合は、システム　プロンプトを確認するとともに、疑問符（?）を入力して使用できるコマンドのリストを表示してください。コマンド モードが間違っているか、間違った構文を使用している可能性があります。

どのモードでも、**Ctrl-Z** キーを押すとイネーブル EXEC モードに戻ることができます。1 つ前のモードに戻るには、**exit** を入力します。

Cisco IOS CLI

ここでは、ルーティングを設定する前に理解しておくべき、Cisco IOS での基本的な設定作業について説明します。

Cisco IOS コンフィギュレーション モードへのアクセス

Cisco IOS コンフィギュレーション モードにアクセスする手順は次のとおりです。

（注）　**switch console** コマンドを使用して、スーパバイザ エンジンのコンソール ポートに直接接続されたスイッチ CLI から MSFC にアクセスします。Telnet セッションから MSFC にアクセスする方法については、「Telnet セッションから MSFC にアクセスする場合」（p.2-5）を参照してください。

	作業	コマンド
ステップ 1	スイッチ CLI を使用している場合は、MSFC CLI を開始します。	Console> **switch console** [*mod*]
ステップ 2	EXEC プロンプトで、イネーブル モードを開始します。	Router> **enable**
ステップ 3	イネーブル EXEC プロンプトで、グローバル コンフィギュレーション モードを開始します。	Router# **configure terminal**

	作業	コマンド
ステップ 4	各種コマンドを入力して、ルーティングを設定します	（このマニュアルで後述する該当の設定手順を参照してください）
ステップ 5	コンフィギュレーション モードを終了します。	Router(config)# **Ctrl-Z**

Cisco IOS コンフィギュレーションの表示および保存

変更を行ったあと、設定を表示および保存する手順は次のとおりです。

	作業	コマンド
ステップ 1	イネーブル EXEC プロンプトで、現在の実行コンフィギュレーションを表示します。	Router# **show running-config**
ステップ 2	NVRAM に保存されている設定を表示します。	Router# **show startup-config**
ステップ 3	現在の設定を NVRAM に保存します。	Router# **copy running-config startup-config**

MSFC インターフェイスをアップにする方法

状況によっては、MSFC インターフェイスが管理上のシャットダウン状態になることがあります。インターフェイスのステータスを確認するには、**show interface** コマンドを使用します。

（注） 冗長スーパバイザ エンジンのセットアップ時に、1 つの MSFC 上のインターフェイスがシャットダウンすると、冗長 MSFC 上の対応する VLAN インターフェイスはパケット転送を停止します。したがって、冗長 MSFC 上の対応するインターフェイスを手動でシャットダウンする必要があります。

管理上のシャットダウン状態になっている MSFC インターフェイスをアップにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	アップにするインターフェイスを指定します。	Router(config)# **interface** *interface_type interface_num*
ステップ 2	インターフェイスをアップにします。	Router(config-if)# **no shutdown**
ステップ 3	コンフィギュレーション モードを終了します。	Router(config-if)# **Ctrl-Z**

CHAPTER 3

スイッチの IP アドレスおよびデフォルト ゲートウェイの設定

この章では、Catalyst 6500 シリーズ スイッチ上で IP アドレス、サブネット マスク、およびデフォルト ゲートウェイを設定する手順について説明します。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

この章で説明する内容は、次のとおりです。

スイッチ管理インターフェイスの機能概要

Catalyst 6500 シリーズ スイッチには、帯域内（sc0 および sc1）インターフェイスおよび帯域外管理 Serial Line Internet Protocol（SLIP; シリアル ライン インターネット プロトコル）（sl0）インターフェイスという、3 種類の設定可能な IP 管理インターフェイスがあります。

帯域内（sc0 および sc1）管理インターフェイスは、スイッチング ファブリックに接続しているので、スパニングツリー、Cisco Discovery Protocol（CDP）、VLAN（仮想 LAN）メンバーシップなど、標準のスイッチ ポート機能をすべてサポートします。帯域外管理インターフェイス（sl0）は、スイッチング ファブリックに接続していないので、これらの機能をサポートしません。

sc0 および sc1 インターフェイスの IP アドレス、サブネット マスク、ブロードキャスト アドレス、および VLAN メンバーシップを設定する場合には、Telnet または SNMP（簡易ネットワーク管理プロトコル）を使用してスイッチにアクセスします。SLIP（sl0）インターフェイスを設定する場合には、ワークステーションからコンソール ポートを介してスイッチにポイントツーポイント接続を確立することができます。

スイッチ自体が生成したすべての IP トラフィック（スイッチからホストに対して開始した Telnet セッションなど）は、そのスイッチの IP ルーティング テーブルのエントリに応じて転送されます。インターサブネットワーク通信を行うには、sc0 または sc1 インターフェイス用に少なくとも 1 つのデフォルト ゲートウェイを設定する必要があります。スイッチ IP ルーティング テーブルは、スイッチ自体が生成したトラフィックを転送するときだけに使用され、スイッチに接続されている装置から送信されたトラフィックの転送には使用されません。

自動 IP コンフィギュレーションの機能概要

ここでは、スイッチに IP コンフィギュレーションを自動的に取得させる方法について説明します。

（注）　ここでの説明は sc0 インターフェイスだけに当てはまります。自動 IP コンフィギュレーション機能は、sc1 や sl0 インターフェイスには適用されません。

自動 IP コンフィギュレーションの概要

スイッチは次のいずれかのプロトコルを使用することにより、対応する IP コンフィギュレーションを自動的に取得できます。

- Bootstrap Protocol（BOOTP）
- Dynamic Host Configuration Protocol（DHCP）
- Reverse Address Resolution Protocol（RARP）

BOOTP、DHCP、および RARP 要求が発行されるのは、スイッチの起動時に sc0 インターフェイス IP アドレスが 0.0.0.0 に設定されている場合に限られます。これは新しいスイッチ、または **clear config all** コマンドによってコンフィギュレーション ファイルが消去されているスイッチのデフォルト アドレスです。BOOTP、DHCP、および RARP 要求のブロードキャスト送信ができるのは、sc0 インターフェイスからだけです。

（注）　CONFIG_FILE 環境変数が設定されている場合、スイッチはすべてのコンフィギュレーション ファイルを処理したあとで、BOOTP、DHCP、および RARP 要求をブロードキャストするかどうかを決定します。CONFIG_FILE 環境変数の詳細については、第 24 章「スイッチの起動設定の変更」を参照してください。

DHCP の概要

DHCP サーバから IP アドレスを取得するには、次の 3 通りの方法があります。

- 手動割り当て — ネットワーク管理者がスイッチの MAC（メディア アクセス制御）アドレスと DHCP サーバの IP アドレスを対応付けます。
- 自動割り当て — スイッチが初めて DHCP サーバにアクセスしたときに、IP アドレスを取得します。アドレスはそのスイッチに永続的に割り当てられます。
- 動的割り当て — スイッチは一定期間だけ「リースされた」IP アドレスを取得します。その期間が終了すると、IP アドレスが取り消され、スイッチがアドレスを放棄します。スイッチは別の IP アドレスを要求しなければなりません。

スイッチは sc0 インターフェイスの IP アドレスのほかに、サブネット マスク、ブロードキャスト アドレス、およびデフォルト ゲートウェイ アドレスを取得できます。ユーザが設定した値がある場合は、DHCP によって学習した値は使用されません。

すべてのスイッチ ポートがオンラインになると、スイッチから DHCPDISCOVER メッセージが 1 ～ 10 秒間ブロードキャストされます。スイッチは DHCPDISCOVER メッセージで必ず、無期限のリース期間を要求します。

DHCP サーバまたは BOOTP サーバから要求に対する応答があると、スイッチは適切な処置を実行します。DHCP サーバから DHCPOFFER メッセージを受け取った場合、スイッチはメッセージ内のサポートされるすべてのオプションを処理します。表 3-1 に、サポートされる DHCP オプションを示します。DHCPOFFER メッセージに他のオプションが指定されていても、スイッチは無視します。

表 3-1　サポートされる DHCP オプション

コード	オプション
1	サブネット マスク
2	タイム オフセット
3	ルータ
6	ドメイン ネーム サーバ
12	ホスト名
15	ドメイン名
28	ブロードキャスト アドレス
33	スタティック ルート
42	NTP サーバ
51	IP アドレス リース期間
52	オプション オーバーロード
61	クライアント ID
66	Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバ名

BOOTP サーバから BOOTP 応答を受け取った場合、スイッチは BOOTP 応答で指定されたアドレスに、帯域内（sc0）インターフェイスの IP アドレスを設定します。

応答として DHCPOFFER メッセージまたは BOOTP 応答がなかった場合、スイッチは指数バックオフ アルゴリズム（要求送信間隔を指数に従って延長）を使用して、要求を再びブロードキャストします。10 分経過しても応答がない場合（かつ BOOTP 要求および RARP 要求も同様に失敗した場合）、sc0 インターフェイスの IP アドレスは 0.0.0.0 に設定されたままになります。

DHCP または BOOTP で取得した IP アドレスを使用して、スイッチをリセットした場合、または電源切断後に再投入した場合、DHCP または BOOTP から学習した情報が維持されます。起動時に、スイッチは IP アドレスのリースを更新しようとします。応答がなければ、スイッチはその時点での IP アドレスを維持します。

BOOTP および RARP の概要

BOOTP および RARP の場合、スイッチの MAC アドレスを BOOTP サーバまたは RARP サーバ上の IP アドレスにマッピングします。スイッチは起動時に、サーバから対応する IP アドレスを自動的に取得します。

すべてのスイッチ ポートがオンラインになると、スイッチは 10 個の BOOTP 要求および RARP 要求をブロードキャストします。応答を受信すると、スイッチは帯域内（sc0）インターフェイスの IP アドレスを応答で指定されたアドレスに設定します。

応答がない場合（かつ DHCP 要求も同様に失敗した場合）、sc0 インターフェイスの IP アドレスは 0.0.0.0 に設定されたままになります。

BOOTP または RARP で取得した IP アドレスを使用して、スイッチをリセットした場合、または電源切断後に再投入した場合、BOOTP または RARP から学習した情報が維持されます。

IP アドレスおよびデフォルト ゲートウェイの設定準備

スイッチの IP アドレスおよびデフォルト ゲートウェイを設定する前に、次の情報を調べておいてください。

- スイッチの IP アドレス（sc0 および sc1 インターフェイスのみ）
- サブネット マスク / サブネット ビット数（sc0 および sc1 インターフェイスのみ）
- （任意）ブロードキャスト アドレス（sc0 および sc1 インターフェイスのみ）
- VLAN メンバーシップ（sc0 および sc1 インターフェイスのみ）
- SLIP および SLIP 宛先アドレス（sl0 インターフェイスのみ）
- インターフェイス接続タイプ
  - 帯域内（sc0 および sc1）インターフェイス ― スイッチの帯域内管理インターフェイスに IP アドレス、サブネット マスク、および VLAN を割り当てる場合、このインターフェイスを設定します。
  - SLIP（sl0）インターフェイス ― 端末とスイッチ間でポイントツーポイント SLIP 接続を設定する場合、このインターフェイスを設定します。

MSFC の初回の起動方法

Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）ブートフラッシュには、2 つの MSFC イメージが用意されています。ブート ローダ イメージとシステム イメージです。ブート ローダ イメージは、ネットワーク インターフェイス コードおよびエンドホスト プロトコル コードを含む、機能の限られたシステム イメージです。システム イメージは、マルチプロトコル ルーティングを完全にサポートする、Cisco IOS の主要なソフトウェア イメージです。

出荷時の設定では、MSFC は最初にブート ローダ イメージを起動し、次にブートフラッシュからシステム イメージを起動するように設定されています。ただし、スーパバイザ エンジンでフラッシュ PC カードが使用できる場合には、新しいシステム イメージ（アップグレード）を、MSFC のブートフラッシュではなく、スーパバイザ エンジンのフラッシュ PC カードですべて保存することを推奨します。ブート ローダ イメージは、MSFC のブートフラッシュで保存する*必要*があります。

注意　ブート ローダ イメージは*消去しないでください*。このイメージは、最初に起動するイメージとして常に使用されるので、MSFC ブートフラッシュ上で最初に検出されるイメージとして残しておく必要があります。

（注）　スーパバイザ エンジンのフラッシュ PC カードに保存されたシステム イメージを使用するには、BOOTLDR 環境変数を設定する必要があります。イネーブル モードで、**boot bootldr bootflash:***boot_loader_image* コマンドを入力します。

スーパバイザのフラッシュ PC カード上にシステム イメージを保存するには、MSFC の設定に次のコマンドを追加して、フラッシュ PC カード上の該当するイメージから MSFC を起動するように、MSFC の設定を変更する必要があります。

```
boot sup-slot0:system_image
```

上記の例で、*system_image* は、スーパバイザのフラッシュ PC カード上の目的とするイメージ名です。

（注）　スーパバイザ エンジンのフラッシュ PC カードに保存されているシステム イメージを起動するには、少なくとも 1 つの VLAN インターフェイスが設定され、アクティブになっている必要があります。

この推奨手順に従った場合、ブートフラッシュ上に新しいシステム イメージを保存する必要はありません。必要に応じて、次のコマンドを入力することにより、スーパバイザ エンジンのフラッシュ PC カード上のイメージからブートフラッシュ上のシステム イメージをアップデートできます。

```
delete bootflash:old_system_image
squeeze bootflash:
copy sup-slot0:new_system_image bootflash:
```

デフォルト IP アドレスおよびデフォルト ゲートウェイの設定

表 3-2 に、デフォルト IP アドレスおよびデフォルト ゲートウェイの設定を示します。

表 3-2　スイッチの IP アドレスおよびデフォルト ゲートウェイのデフォルト設定

機能	デフォルト値
帯域内（sc0）インターフェイス	• IP アドレス、サブネット マスク、およびブロードキャスト アドレスを 0.0.0.0 に設定 • VLAN 1 に割り当て
帯域内（sc1）インターフェイス	• IP アドレス、サブネット マスク、およびブロードキャスト アドレスを 0.0.0.0 に設定 • VLAN 2 に割り当て
デフォルト ゲートウェイ アドレス	メトリック 0 で 0.0.0.0 に設定
SLIP[1]（sl0）インターフェイス	• IP アドレスおよび SLIP 宛先アドレスを 0.0.0.0 に設定 • コンソール ポートの SLIP は非アクティブ（**detach** に設定）

1. SLIP = Serial Line Internet Protocol

sc0 および sc1 帯域内インターフェイスによってサポートされる機能

表 3-3 に、sc0 および sc1 帯域内インターフェイスによってサポートされる機能を示します。

表 3-3　sc0 および sc1 帯域内インターフェイスによってサポートされる機能

sc0 インターフェイス	sc1 インターフェイス
イメージのダウンロード	イメージのダウンロード
ping	ping
Telnet	Telnet
SNMP	SNMP
デフォルト ゲートウェイのサポート	デフォルト ゲートウェイのサポート
BOOTP	
DHCP	
RARP	

帯域内（sc0 および sc1）インターフェイス IP アドレスの割り当て

Telnet を使用してスイッチに接続する場合、または SNMP を使用してスイッチを管理する場合には、あらかじめ帯域内（sc0 または sc1）論理インターフェイスのいずれかに IP アドレスを割り当てる必要があります。

ヒント　sc1 または sc0 インターフェイスをデフォルト アドレスの 0.0.0.0 に戻す（*クリアする*）には、**set interface** {**sc0** | **sc1**} **0.0.0.0** コマンドを使用します。

ヒント　sc0 および sc1 の両方の帯域内インターフェイスが設定されている場合、スイッチは 2 つの異なる VLAN から同時に直接アクセスが可能です。

サブネット マスク（*netmask*）は、サブネット ビット数を使用して、またはドット付き 10 進表記のサブネット マスクを使用して指定できます。

帯域内（sc0 または sc1）管理インターフェイスの IP アドレスおよび VLAN メンバーシップを設定するには、イネーブル モードで次の作業を行います（この例では sc0 インターフェイスを設定します）。

	作業	コマンド
ステップ 1	帯域内（sc0 または sc1）インターフェイスに、IP アドレス、サブネット マスク（またはサブネット ビット数）、および（任意で）ブロードキャスト アドレスを割り当てます。	**set interface** {**sc0**	**sc1**} [*ip_addr* [*netmask* [*broadcast*]]] または **set interface** {**sc0**	**sc1**} [*ip_addr*/*netmask* [*broadcast*]]
ステップ 2	適切な VLAN に帯域内インターフェイスを割り当てます（IP アドレスが所属するネットワークと VLAN が対応付けられていることを確認します）。	**set interface** {**sc0**	**sc1**} [*vlan*]
ステップ 3	必要に応じて、インターフェイスをアクティブにします。	**set interface** {**sc0**	**sc1**} **up**
ステップ 4	インターフェイスの設定を確認します。	**show interface**

次に、帯域内 sc0 インターフェイスに IP アドレスを割り当て、サブネット ビット数および VLAN の割り当てを指定する例を示します。

```
Console> (enable) set interface sc0 172.20.52.124/29
Interface sc0 IP address and netmask set.
Console> (enable) set interface sc0 5
Interface sc0 vlan set.
Console> (enable)
```

次に、VLAN の割り当てを指定し、IP アドレスを割り当て、ドット付き 10 進表記でサブネット マスクを指定し、設定を確認する例を示します。この例では sc0 インターフェイスを設定します（sc1 および sl0 インターフェイスは設定されていません）。

```
Console> (enable) set interface sc0 5 172.20.52.124/255.255.255.248
Interface sc0 vlan set, IP address and netmask set.
Console> (enable) show interface
sl0: flags=51<UP,POINTOPOINT,RUNNING>
        slip 0.0.0.0 dest 0.0.0.0
sc0: flags=63<UP,BROADCAST,RUNNING>
        vlan 5 inet 172.20.52.124 netmask 255.255.255.248 broadcast 172.20.52.17
sc1: flags=62<DOWN,BROADCAST,RUNNING>
        vlan 0 inet 0.0.0.0 netmask 0.0.0.0 broadcast 0.0.0.0
Console> (enable)
```

デフォルト ゲートウェイの設定

スーパバイザ エンジンは、ほかの IP サブネット宛の IP パケットをデフォルト ゲートウェイ（通常はスイッチ IP アドレスと同じネットワークまたはサブネットのルータ インターフェイス）に送信します。スイッチは、接続装置からのトラフィックの転送には IP ルーティング テーブルを使用しません。スイッチ自体が生成した IP トラフィック（Telnet、TFTP、および ping など）の転送だけに使用します。

（注） デフォルト ゲートウェイのほかに、スタティック IP ルートを設定する場合もあります。スタティック ルートの設定については、「スイッチ上でのスタティック ルートの設定」（p.21-9）を参照してください。

デフォルト IP ゲートウェイは、3 つまで定義できます。ゲートウェイをプライマリ ゲートウェイにするには、**primary** キーワードを使用します。プライマリのデフォルト ゲートウェイを指定しなかった場合、最初に設定したゲートウェイがプライマリ ゲートウェイになります。また、複数のゲートウェイをプライマリとして指定した場合には、最後に設定したゲートウェイがプライマリのデフォルト ゲートウェイになります。

スイッチはネットワークからのすべての IP トラフィックをプライマリ デフォルト ゲートウェイに送信します。プライマリ ゲートウェイに接続できなくなった場合、スイッチは設定された順にバックアップ ゲートウェイを使用します。スイッチは定期的に ping メッセージを送信して、各デフォルト ゲートウェイがアクティブかどうかを判別します。プライマリ ゲートウェイに再び接続できるようになると、プライマリ ゲートウェイへのトラフィック送信が再開されます。

（注） システムは、ルートとゲートウェイを該当する sc0 または sc1 帯域内インターフェイスに自動的に対応付けます。

1 つまたは複数のデフォルト ゲートウェイを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチのデフォルト IP ゲートウェイ アドレスを設定します。	**set ip route default** *gateway* [*metric*] [**primary**]
ステップ 2	（任意）スイッチ用に追加のデフォルト ゲートウェイを設定します。	**set ip route default** *gateway* [*metric*] [**primary**]
ステップ 3	デフォルト ゲートウェイが IP ルーティング テーブルに正しく組み込まれていることを確認します。	**show ip route**

デフォルト ゲートウェイ エントリを削除するには、イネーブル モードで次のいずれかの作業を行います。

作業	コマンド
特定のデフォルト ゲートウェイ エントリを消去します。	**clear ip route default** *gateway*
すべてのデフォルト　ゲートウェイおよびスタティック ルートを消去します。	**clear ip route all**

次に、スイッチ上で 3 つのデフォルト ゲートウェイを設定し、デフォルト ゲートウェイの設定を確認する方法を示します。

```
Console> (enable) set ip route default 10.1.1.10
Route added.
Console> (enable) set ip route default 10.1.1.20
Route added.
Console> (enable) set ip route default 10.1.1.1 primary
Route added.
Console> (enable) show ip route
Fragmentation   Redirect   Unreachable
-------------   --------   -----------
enabled         enabled    enabled

The primary gateway: 10.1.1.1
Destination      Gateway          RouteMask    Flags   Use       Interface
---------------  ---------------  ----------   -----   --------  ---------
default          10.1.1.1         0x0          UG      6           sc0
default          10.1.1.20        0x0          G       0           sc0
default          10.1.1.10        0x0          G       0           sc0
10.0.0.0         10.1.1.100       0xff000000   U       75          sc0
default          default          0xff000000   UH      0           sl0
Console> (enable)
```

コンソール ポートでの SLIP（sl0）インターフェイスの設定

スイッチと IP ホスト間のポイントツーポイント SLIP 接続には、SLIP（sl0）インターフェイスを使用します。

注意　SLIP 接続には、コンソール ポートを使用する*必要*があります。SLIP 接続がイネーブルになり、コンソール ポート上で SLIP 接続が行われると、コンソール ポートから EIA/TIA-232 端末に接続することはできません。コンソール ポートからスイッチの CLI に接続している場合に、**slip attach** コマンドを入力すると、コンソール ポート接続が切断されます。その場合、Telnet を使用してスイッチにアクセスし、イネーブル モードを開始して、**slip detach** コマンドを入力すると、コンソール ポート接続を復元できます。

コンソール ポート上で SLIP をイネーブルにして接続するには、次の作業を行います。

	作業	コマンド
ステップ 1	リモート ホストからスイッチに Telnet でアクセスします。	**telnet** {*host_name* | *ip_addr*}
ステップ 2	スイッチ上でイネーブル モードを開始します。	**enable**
ステップ 3	コンソール ポートの SLIP アドレス、および接続ホストの宛先アドレスを設定します。	**set interface sl0** *slip_addr dest_addr*
ステップ 4	SLIP インターフェイスの設定を確認します。	**show interface**
ステップ 5	コンソール ポートに対して SLIP をイネーブルにします。	**slip attach**

コンソール ポート上で SLIP をディセーブルにするには、次の作業を行います。

	作業	コマンド
ステップ 1	リモート ホストからスイッチに Telnet でアクセスします。	**telnet** {*host_name* | *ip_addr*}
ステップ 2	スイッチ上でイネーブル モードを開始します。	**enable**
ステップ 3	コンソール ポートに対して SLIP をディセーブルにします。	**slip detach**

コンソール ポート上で SLIP を設定し、その設定を確認する例を示します。

```
sparc20% telnet 172.20.52.38
Trying 172.20.52.38 ...
Connected to 172.20.52.38.
Escape character is '^]'.

Cisco Systems, Inc. Console

Enter password:
Console> enable

Enter password:
Console> (enable) set interface sl0 10.1.1.1 10.1.1.2
Interface sl0 slip and destination address set.
Console> (enable) show interface
sl0: flags=51<UP,POINTOPOINT,RUNNING>
        slip 10.1.1.1 dest 10.1.1.2
sc0: flags=63<UP,BROADCAST,RUNNING>
        vlan 522 inet 172.20.52.38 netmask 255.255.255.240 broadcast 172.20.52.7
Console> (enable) slip attach
Console Port now running SLIP.

Console> (enable) slip detach
SLIP detached on Console port.
Console> (enable)
```

BOOTP、DHCP、または RARP を使用して IP アドレスを取得する場合

（注） スイッチで BOOTP、DHCP、または RARP を使用して IP コンフィギュレーションを取得する手順の詳細については、「自動 IP コンフィギュレーションの機能概要」（p.3-3）を参照してください。

BOOTP、DHCP、または RARP を使用してスイッチの IP アドレスを取得するには、次の作業を行います。

	作業	コマンド
ステップ 1	ネットワーク上に DHCP サーバ、BOOTP サーバ、または RARP サーバがあることを確認します。	–
ステップ 2	モジュール 1（スーパバイザ エンジン）について MAC アドレス範囲内で最後のアドレスを取得します。このアドレスは、MAC-Address(es) の見出しの下に表示されます（DHCP を使用する場合、手動割り当て方式を使用するときに限り、この作業が必要です）。	**show module**
ステップ 3	DHCP、BOOTP、または RARP のサーバ コンフィギュレーションの各スイッチにエントリを追加し、スイッチの MAC アドレスをスイッチの IP コンフィギュレーション情報に対応付けます（DHCP を使用する場合、手動または自動割り当て方式を使用するときに限り、この作業が必要です）。	–
ステップ 4	sc0 インターフェイスの IP アドレスを 0.0.0.0 に設定します。	**set interface sc0 0.0.0.0**
ステップ 5	スイッチをリセットします。DHCP　要求および RARP 要求は、スイッチの起動時に限りブロードキャストされます。	**reset system**
ステップ 6	スイッチの再起動後、sc0 インターフェイスの IP アドレス、サブネット マスク、およびブロードキャスト アドレスが正しく設定されているかどうかを確認します。	**show interface**
ステップ 7	DHCP の場合、ほかのオプション（デフォルト ゲートウェイ アドレスなど）が正しく設定されているかどうかを確認します。	**show ip route**

次に、スイッチが DHCP 要求をブロードキャストし、DHCP オファーを受信し、DHCP オファーの内容に基づいて IP アドレスおよびそのほかの IP パラメータを設定する例を示します。

```
Console> (enable)
Sending RARP request with address 00:90:0c:5a:8f:ff
Sending DHCP packet with address: 00:90:0c:5a:8f:ff
dhcpoffer
Sending DHCP packet with address: 00:90:0c:5a:8f:ff
Timezone set to '', offset from UTC is 7 hours 58 minutes
Timezone set to '', offset from UTC is 7 hours 58 minutes
172.16.30.32 added to DNS server table as primary server.
172.16.31.32 added to DNS server table as backup server.
172.16.32.32 added to DNS server table as backup server.
NTP server 172.16.25.253 added
NTP server 172.16.25.252 added
%MGMT-5-DHCP_S:Assigned IP address 172.20.25.244 from DHCP Server 172.20.25.254
Console> (enable) show interface
sl0: flags=51<UP,POINTOPOINT,RUNNING>
        slip 0.0.0.0 dest 0.0.0.0
sc0: flags=63<UP,BROADCAST,RUNNING>
        vlan 1 inet 172.20.25.244 netmask 255.255.255.0 broadcast 172.20.25.255
dhcp server: 172.20.25.254
Console>
```

DHCP で割り当てられた IP アドレスの更新および解除

DHCP を使用して IP アドレスを割り当てる場合、次のどちらかの DHCP 関連作業を行うことができます。

- DHCP で割り当てられた IP アドレスのリースを更新します。
- DHCP で割り当てられた IP アドレスのリースを解除します。

DHCP で割り当てられた、帯域内（sc0）管理インターフェイスの IP アドレスを更新または解除するには、イネーブル モードで次のいずれかの作業を行います。

作業	コマンド
DHCP で割り当てられた IP アドレスのリースを更新します。	**set interface sc0 dhcp renew**
DHCP で割り当てられた IP アドレスのリースを解除します。	**set interface sc0 dhcp release**

次に、DHCP で割り当てられた IP アドレスのリースを更新する例を示します。

```
Console> (enable) set interface sc0 dhcp renew
Renewing IP address...
Console> (enable) Sending DHCP packet with address: 00:90:0c:5a:8f:ff
（テキスト出力は省略）
```

次に、DHCP で割り当てられた IP アドレスのリースを解除する例を示します。

```
Console> (enable) set interface sc0 dhcp release
Releasing IP address...
Console> (enable) Sending DHCP packet with address: 00:90:0c:5a:8f:ff
Done

Console> (enable)
```

CHAPTER 4

イーサネット、ファスト イーサネット、ギガビット イーサネット、および 10 ギガビット イーサネット スイッチングの設定

この章では、CLI（コマンドライン インターフェイス）を使用して Catalyst 6500 シリーズ スイッチ上でイーサネット、ファスト イーサネット、ギガビット イーサネット、および 10 ギガビット イーサネット スイッチングを設定する手順について説明します。この章で説明する設定手順は、イーサネット、ファスト イーサネット、ギガビット イーサネット、および 10 ギガビット イーサネット スイッチング モジュールのほかに、スーパバイザ エンジン上のアップリンク ポートにも当てはまります。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

この章で説明する内容は、次のとおりです。

イーサネットの機能概要

Catalyst 6500 シリーズ スイッチは、イーサネット セグメント間での同時並列接続をサポートします。イーサネット セグメント間のスイッチの接続が維持されるのは、パケットの送信中だけです。次のパケットでは、別のセグメント間で新しい接続を行うことができます。

Catalyst 6500 シリーズ スイッチは、装置（サーバなど）ごとに専用の 10、100、1000、または 10000 Mbps セグメントを割り当てることにより、広帯域幅装置および大量ユーザに起因する輻輳問題を解消します。スイッチのイーサネット ポートごとに、別々のイーサネット セグメントとなるので、適切に設定されたスイッチング環境のサーバは、帯域へのフルアクセスが可能です。

イーサネット ネットワークでは、コリジョンが障害の主な原因であるため、効果的な解決方法は全二重通信です。Catalyst 6500 シリーズ スイッチの 10 Mbps ポートまたは 100 Mbps ポートでは、全二重モードがオプションとして提供されています（ギガビット イーサネットおよび 10 ギガビット イーサネット ポートは常に全二重で動作します）。一般的に、イーサネットは半二重モードで動作しますが、これは各ステーションが送信または受信のどちらか一方しかできないことを意味します。全二重モードでは、2 つのステーション間で同時に送受信を行うことができます。同時に両方向にパケットを送れる場合、有効イーサネット帯域幅は 2 倍になり、10 Mbps ポートで 20 Mbps に、ファスト イーサネット ポートで 200 Mbps になります。Catalyst 6500 シリーズ スイッチのギガビット イーサネットおよび 10 ギガビット イーサネット ポートは、全二重（それぞれ有効帯域幅は 2 Gbps と 20 Gbps）のみです。

ここでは、イーサネットについて説明します。

セグメント間のフレーム スイッチング

Catalyst 6500 シリーズ スイッチ上の各イーサネット ポートは、1 台のワークステーションまたはサーバに接続することも、ハブを介してそこからネットワークに接続する複数のワークステーションまたはサーバに接続することもできます。

一般的なイーサネット ハブのポートはすべて、ハブ内の共通バックプレーンに接続され、ハブに接続されたすべての装置間でネットワーク帯域が共有されます。2 つのステーション間で、相当量の帯域を使用するセッションを確立した場合には、そのハブに接続されたほかのすべてのステーションで、ネットワーク パフォーマンスが低下します。

このようなパフォーマンスの低下を軽減するために、スイッチは各ポートをそれぞれ独立したセグメントとして扱います。別のポート上のステーションで通信が必要になった場合、スイッチはワイヤ スピードで、あるポートから別のポートへフレームを転送するので、各セッションに確実にフル帯域を与えることができます。

ポート間のフレーム スイッチングを効率的に行うために、スイッチはアドレス テーブルを維持します。フレームがスイッチに入ると、スイッチによって、送信側ステーションの MAC（メディア アクセス制御）アドレスとフレームを受信したポートが対応付けられます。

アドレス テーブルの作成

Catalyst 6500 シリーズ スイッチは、受信したフレームの送信元アドレスを使用してアドレス テーブルを作成します。アドレス テーブルに宛先アドレスが登録されていないフレームをスイッチが受信した場合、そのフレームを受信したポート以外の同一 VLAN（仮想 LAN）のすべてのポートに、フレームがフラッディングされます。宛先ステーションから応答があると、スイッチが適切な送信元アドレスおよびポート ID をアドレス テーブルに追加します。スイッチは以後、1 つのポートだけに後続フレームを転送します。すべてのポートにフラッディングすることはありません。

アドレス テーブルには、エントリのフラッディングを伴わずに少なくとも 32,000 のアドレス エントリを保存できます。スイッチは設定可能なエージング タイマーによって定められたエージング メカニズムを使用するので、アドレスが指定された秒数だけ非アクティブ状態になると、アドレス テーブルから削除されます。

ポート ネゴシエーションの概要

（注） **set port negotiation** コマンドをサポートしているのは、ギガビット イーサネット ポートだけです。WS-X6316-GE-TX モジュールおよび WS-X6516-GE-TX モジュールはこのコマンドをサポートしていません。ポートがこのコマンドをサポートしていない場合、[Feature not supported on Port N/N] というメッセージが表示されます。N/N はモジュールとポート番号を示しています。

（注） このリリースでは、1000BASE-TX（銅線）ギガビット イーサネット ポートにポート ネゴシエーションを設定することはできません。ネゴシエーションがディセーブルに設定されているポートに 1000BASE-TX GBIC を搭載すると、ディセーブルの設定は無視され、そのポートはネゴシエーション イネーブル モードで動作します。

（注） ポート　ネゴシエーションには、ネゴシエーションを行うポートの速度は関係しません。**set port speed** コマンドを使用してポート ネゴシエーションをディセーブルに設定することはできません。

ポート ネゴシエーションでは、フロー制御パラメータ、リモート障害情報、およびデュプレックス情報が交換されます。ポート ネゴシエーションの設定は、**set port negotiation** コマンドを使用して行います。ポート ネゴシエーションは、デフォルトではイネーブルに設定されています。

（注） 16 ポート 10/100/1000BASE-T イーサネット モジュールでポート ネゴシエーションをイネーブルにした場合、システムはフロー制御のみについて自動ネゴシエーションを実行します。

リンクの両端のポートは、同じ設定でなければなりません。リンクの両端でポートの設定が一致していないと（一方のポートでポート ネゴシエーションがイネーブルで、他方のポートでディセーブルに設定されている場合など）、リンクが確立されません。

表 4-1 に、使用できる 4 種類のポート ネゴシエーション設定および各設定に対応するリンク ステータスを示します。

表 4-1　ポート ネゴシエーションの設定およびリンク ステータス

ポート ネゴシエーション ステート		リンク ステータス	
近端[1]	遠端[2]	近端	遠端
オフ	オフ	アクティブ	アクティブ
オン	オン	アクティブ	アクティブ
オフ	オン	アクティブ	ダウン
オン	オフ	ダウン	アクティブ

1. 近端とは、ローカル ポートです。
2. 遠端とは、リンクの他端にあるポートです。

イーサネット、ファスト イーサネット、ギガビット イーサネット、および 10 ギガビット イーサネットのデフォルト設定

表 4-2 に、イーサネット、ファスト イーサネット、ギガビット イーサネット、および 10 ギガビット イーサネットのデフォルト設定を示します。

表 4-2　イーサネットのデフォルト設定

機能	デフォルト値
ポート イネーブル ステート	すべてのポートがイネーブル
ポート名	なし
デュプレックス モード	• 10 Mbps イーサネット ポートでは半二重 • 10/100 Mbps ファスト イーサネット ポートでは速度とデュプレックスを自動ネゴシエーション • 100 Mbps ファスト イーサネット ポートではデュプレックスを自動ネゴシエーション • 1000 Mbps ギガビット イーサネット ポートでは全二重 • 10000 Mbps ギガビット イーサネット ポートでは全二重
フロー制御（10 ギガビット イーサネット）	フロー制御は受信（Rx）で on、（Tx）送信で off
フロー制御（ギガビット イーサネット）	フロー制御は Rx で off、Tx で desired
フロー制御（そのほかのイーサネット）	フロー制御は Rx で off、Tx はサポートされていない
Spanning-Tree Protocol（STP; スパニング ツリー プロトコル）	VLAN 1 でイネーブル
ネイティブ VLAN	VLAN 1
ポート VLAN コスト	• 10 Mbps イーサネット ポートでは 100 • 10/100 Mbps ファスト イーサネット ポートでは 19 • 100 Mbps ファスト イーサネット ポートでは 19 • 1000 Mbps ギガビット イーサネット ポートでは 4 • 10000 Mbps ギガビット イーサネット ポートでは 1
EtherChannel	すべてのイーサネット ポート上でディセーブル
ジャンボ フレーム	すべてのイーサネット ポート上でディセーブル

ポート コンフィギュレーションの設定

ここでは、Catalyst 6500 シリーズ スイッチ上でイーサネット、ファスト イーサネット、ギガビット イーサネット、および 10 ギガビット イーサネット スイッチングを設定する手順について説明します。

Supervisor Engine 720 のポート設定

Supervisor Engine 720 のポート 1 には Small Form-factor Pluggable（SFP）コネクタがあり、固有の設定オプションはありません。

Supervisor Engine 720 のポート 2 には、RJ-45 コネクタと SFP コネクタ（デフォルト）があります。RJ-45 コネクタを使用するには、設定を変更する必要があります。

Supervisor Engine 720 上のポート 2 を設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
Supervisor Engine 720 上のポート 2 を設定します。	**set port media-type** *mod/port* {**rj45** | **sfp**}

次に、RJ-45 コネクタを使用できるように Supervisor Engine 720 上のポート 2 を設定する例を示します。

```
Console> (enable) set port media-type 5/2 rj45
Port 5/2 media type set to RJ-45.
Console> (enable)
```

ポート名の設定

イーサネット、ファスト イーサネット、ギガビット イーサネット、および 10 ギガビット イーサネット スイッチング モジュール上のポート名を設定し、スイッチ管理を容易にすることができます。

ポート名を設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポート名を設定します。	**set port name** *mod/port* [*name_string*]
ステップ 2	ポート名の設定を確認します。	**show port** [*mod*[*/port*]]

次に、ポート 1/1 および 1/2 に名前を設定し、それらのポート名が正しく設定されているかどうかを確認する例を示します。

```
Console> (enable) set port name 1/1 Router Connection
Port 1/1 name set.
Console> (enable) set port name 1/2 Server Link
Port 1/2 name set.
Console> (enable) show port 1
Port  Name               Status     Vlan         Duplex Speed Type
----- ------------------ ---------- ----------   ------ ----- ------------
 1/1  Router Connection  connected  trunk          full  1000 1000BaseSX
 1/2  Server Link        connected  trunk          full  1000 1000BaseSX
.
.
.
Last-Time-Cleared
--------------------------
Wed Jun 16 1999, 16:25:57
Console> (enable)
```

ポート速度の設定

10/100 Mbps イーサネット スイッチング モジュール上でポート速度を設定できます。近接ポートとの間で、ポート速度とデュプレックス モードの自動ネゴシエーションが行われるようにするには、**auto** キーワードを使用します。

（注） 10/100 Mbps イーサネット ポート上でポート速度を **auto** に設定すると、速度とデュプレックスの両方について、自動ネゴシエーションが行われます。

10/100/1000 Mbps の速度をサポートするポート上では、**auto-10-100** キーワードを使用します。**auto-10-100** キーワードを使用することで、そのポートを、速度が **auto** に設定されている 10/100 Mbps のポートと同様に動作させることができます。速度とデュプレックスはネゴシエートされます（1000 Mbps の速度はネゴシエートされません）。

イーサネット ポートのポート速度を設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	イーサネット ポートのポート速度を設定します。	**set port speed** *mod/port* {**10** | **100** | **1000** | **auto** | **auto-10-100**}
ステップ 2	ポートの速度が正しく設定されていることを確認します。	**show port** [*mod*[*/port*]]

次に、ポート 2/2 のポート速度を 100 Mbps に設定する例を示します。

```
Console> (enable) set port speed 2/2 100
Port 2/2 speed set to 100 Mbps.
Console> (enable)
```

次に、ポート 2/1 と近接ポートとの間で速度およびデュプレックスの自動ネゴシエーションが行われるようにする例を示します。

```
Console> (enable) set port speed 2/1 auto
Port 2/1 speed set to auto-sensing mode.
Console> (enable)
```

ポートのデュプレックス モードの設定

イーサネットおよびファスト イーサネット ポートのデュプレックス モードを全二重または半二重に設定できます。

（注） ギガビット イーサネットおよび 10 ギガビット イーサネットは全二重通信専用です。ギガビット イーサネットおよび 10 ギガビット イーサネット ポートのデュプレックス モードを変更することはできません。

（注） 10/100 Mbps イーサネット ポート上でポート速度を **auto** に設定すると、速度とデュプレックスの両方において、自動ネゴシエーションが行われます。自動ネゴシエーション ポートのデュプレックス モードは変更できません。

ポートのデュプレックス モードを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポートのデュプレックス モードを設定します。	**set port duplex** *mod/port* {**full** | **half**}
ステップ 2	ポートのデュプレックス モードが正しく設定されていることを確認します。	**show port** [*mod*[*/port*]]

次に、ポート 2/1 のデュプレックス モードを半二重に設定する例を示します。

```
Console> (enable) set port duplex 2/1 half
Port 2/1 set to half-duplex.
Console> (enable)
```

自動 MDI/MDIX のイネーブル化 / ディセーブル化

自動 Media-Dependent Interface（MDI; メディア依存型インターフェイス）/Media-Dependent Interface crossover（MDIX; メディア依存型インターフェイス クロスオーバー）が有効な場合は、ストレート ケーブルまたはクロス ケーブルを使用できます。モジュールはケーブル タイプを自動的に検出し、それに合わせて調整します。自動 MDI/MDIX は速度が auto/1000 Mbps に設定されている場合に機能しますが、速度が 10 Mbps または 100 Mbps に設定されている場合は機能しません。つまり、**set port speed** *mod/port* **auto** または **set port speed** *mod/port* **1000** コマンドを使用して速度が auto/1000 に設定されている場合には、ストレート ケーブルまたはクロス ケーブルによるリンクが起動します。**auto** モードでは、速度が 10 Mbps または 100 Mbps で自動ネゴシエートされている場合でも、リンクは起動します。ただし、**set port speed** *mod/port* **10** コマンドまたは **set port speed** *mod/port* **100** コマンドを入力した場合、正しいケーブルが使用されていなければ、リンクは起動しません。

次のモジュールでは、自動 MDI/MDIX が常にイネーブルです。

- WS-X6548-RJ-45、WS-X6548-RJ-21、WS-X6148-GE-TX、WS-X6548-GE-TX

  10、100、および 1000 Mbps モードの場合、自動 MDI/MDIX は自動ネゴシエートされた速度および固定速度で機能します。
- WS-X6516-GE-TX

  自動 MDI/MDIX は速度が auto/1000 Mbps に設定されている場合に機能しますが、速度が 10 Mbps または 100 Mbps に設定されている場合は機能しません。
- WS-X6316-GE-TX

Release 8.2(1) 以降のソフトウェア リリースでは、次のモジュールでも自動 MDIX がイネーブルです。

- WS-X6748-GE-TX、Supervisor Engine 720 ポート 2（RJ-45）

  自動 MDI/MDIX は速度が auto/1000 に設定されている場合に機能しますが、速度が 10 Mbps または 100 Mbps に設定されている場合は機能しません。
- WS-X6148X2-RJ-45、WS-X6148X2-45AF

  自動 MDI/MDIX は速度が auto に設定されている場合に機能しますが、速度が 10 Mbps または 100 Mbps に設定されている場合は機能しません。

（注） 自動 MDI/MDIX は、そのほかの 10/100 Mbps イーサネット モジュールまたは GBIC（ギガビット インターフェイス コンバータ）、SFP、および XENPAK ポートではサポートされません。

Release 8.3(1) 以降のソフトウェア リリースには、**set port auto-mdix** *mod/port* {**enable** | **disable**} コマンドが導入されています。このコマンドを使用すると、自動 MDI/MDIX 機能がデフォルトでイネーブルであるすべてのモジュール上で、この機能をディセーブルにすることができます。自動 MDI/MDIX 設定を表示するには、**show port auto-mdix** [*mod*[/*port*]] コマンドを使用します。

IEEE 802.3X フロー制御の設定

Catalyst 6500 シリーズ スイッチ上のギガビット イーサネットおよび 10 ギガビット イーサネット ポートは、ポートへのパケット転送を一定時間禁止するために、フロー制御を使用します。そのほかのイーサネット ポートは、フロー制御を使用してフロー制御要求に応答します。

ギガビット イーサネットまたは 10 ギガビット イーサネット ポートの受信バッファがいっぱいになると、ポートは「休止（pause）」パケットを送信し、一定時間、そのポートへの後続パケットの送信を遅らせるようにリモート ポートに指示します。すべてのイーサネット ポート（10000 Mbps、1000 Mbps、100 Mbps、および 10 Mbps）は、他の装置から「休止」パケットを受信し、これに対応できます。

ポートにフロー制御を設定するには、**set port flow control** コマンドを入力します。表 4-3 に、**set port flowcontrol** コマンドのキーワードとその機能を示します。

表 4-3　イーサネット フロー制御キーワードの機能

キーワード	機能
receive on[1]	ポートは、近接ポートが指示したフロー制御を使用します。
receive desired	ポートは、近接ポートがフロー制御を使用しているときはフロー制御を使用し、近接ポートが使用していないときは使用しません。
receive off	ポートは、近接ポートがフロー制御を要求するかどうかに関係なく、フロー制御を使用しません。
send on[2]	ポートは、近接ポートにフロー制御フレームを送信します。
send desired[2]	ポートは、近接ポートからフロー制御の使用を要求された場合に、近接ポートにフロー制御フレームを送信します。
send off[2]	ポートは、近接ポートにフロー制御フレームを送信しません。

1. 10 ギガビット イーサネット ポート上では、受信側のフロー制御は常に on です。off に設定することはできません。
2. ギガビット イーサネットおよび 10 ギガビット イーサネット ポートに限りサポートされます。

フロー制御を設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	フロー制御パラメータを設定します。	**set port flowcontrol** *mod/port* {**receive** | **send**} {**off** | **on** | **desired**}
ステップ 2	フロー制御の設定を確認します。	**show port flowcontrol**

次に、送受信のフロー制御をオンにし、フロー制御の設定を確認する例を示します。

```
Console> (enable) set port flowcontrol 3/1 send on
Port 3/1 will send flowcontrol to far end.
Console> (enable) set port flowcontrol 3/1 receive on
Port 3/1 will require far end to send flow control
Console> (enable) show port flowcontrol
Port  Send-Flowcontrol  Receive-Flowcntl  RxPause  TxPause
      Admin   Oper      Admin   Oper
----- ----------------  ----------------  -------  -------
 3/1  on      disagree  on      disagree  0        0
 3/2  off     off       off     off       0        0
 3/3  desired on        desired off       10       10
Console> (enable)
```

ポート ネゴシエーションのイネーブル化およびディセーブル化

ポート ネゴシエーションをイネーブルに設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポート ネゴシエーションをイネーブルにします。	**set port negotiation** *mod*/*port* **enable**
ステップ 2	ポート ネゴシエーションの設定を確認します。	**show port negotiation** [*mod*/*port*]

次に、ポート ネゴシエーションをイネーブルにし、設定を確認する例を示します。

```
Console> (enable) set port negotiation 2/1 enable
Port 2/1 negotiation enabled
Console> (enable) show port negotiation 2/1
Port   Link Negotiation
-----  ----------------
 2/1   enabled
Console> (enable)
```

ポート ネゴシエーションをディセーブルに設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポート ネゴシエーションをディセーブルにします。	**set port negotiation** *mod*/*port* **disable**
ステップ 2	ポート ネゴシエーションの設定を確認します。	**show port negotiation** [*mod*/*port*]

次に、ポート ネゴシエーションをディセーブルにし、設定を確認する例を示します。

```
Console> (enable) set port negotiation 2/1 disable
Port 2/1 negotiation disabled
Console> (enable) show port negotiation 2/1
Port   Link Negotiation
-----  ----------------
 2/1   disabled
Console> (enable)
```

デフォルトのポート イネーブル ステートの変更

(注) デフォルトのポート イネーブル ステートを変更すると、イーサネットだけでなく、すべてのポート タイプに適用されます。

clear config all コマンドを入力したり、設定情報が消失したりすると、すべてのポートが VLAN 1 にまとめられます。これにより、セキュリティ上の問題やネットワークが不安定になる問題が生じることがあります。**set default portstatus** コマンドを入力すると、ポートがすべてディセーブル ステートになり、設定が消失している間のトラフィック フローがブロックされます。その場合は、手動で設定をイネーブル ステートに戻すことができます。

デフォルトのポート ステータス設定はシャーシに保存されています。この設定は、スーパバイザ エンジンではなく、シャーシに対応付けられています。**clear config all** コマンドは、この設定を使用して、デフォルト設定に戻るときにポートをイネーブルにするかディセーブルにするかを決定します。**clear config all** コマンドは、シャーシ上のデフォルトのポート ステータス設定を変更しません。**show config** コマンドの出力には、その時点でのデフォルト ポート ステータス設定が表示されます。

ポート イネーブル ステートを変更するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポート イネーブル ステートを変更します。	**set default portstatus {enable | disable}**
ステップ 2	ポート イネーブル ステートを表示します。	**show default**

次に、デフォルトのポート イネーブル ステートをイネーブルからディセーブルに変更する例を示します。

```
Console> (enable) set default portstatus disable
Default port status set to disable.
Console> (enable)
```

次に、ポートのイネーブル ステートを表示する例を示します。

```
Console> (enable) show default
portstatus: disable
Console> (enable)
```

ポート デバウンス タイマーの設定

イーサネット、ファスト イーサネット、ギガビット イーサネット、および 10 ギガビット イーサネットの各ポートに対してポート単位でポート デバウンス タイマーを設定できます。ポート デバウンス タイマーが設定されると、スイッチはメイン プロセッサへのリンク変更の通知を遅延します。このリンク変更により、ネットワークの再設定によるトラフィック損失を軽減することができます。

注意

ポート デバウンス タイマーをイネーブルにすると、リンクのアップおよびダウンの検出が遅れ、デバウンス期間の間、データ トラフィックの損失が発生します。この状況により、レイヤ 2 およびレイヤ 3 の各種プロトコルのコンバージェンスおよび再コンバージェンスに影響が及ぶことがあります。

表 4-4 に、デバウンス タイマーをイネーブルにする前とあとで、スイッチがメイン プロセッサにリンク変更を通知するまでに発生する遅延時間を表示します。

表 4-4　ポート デバウンス タイマーの遅延時間

ポート タイプ	デバウンス タイマーをディセーブル化	デバウンス タイマーをイネーブル化
10BASE-FL ポート	300 ミリ秒	3100 ミリ秒
10/100BASE-TX ポート	300 ミリ秒	3100 ミリ秒
100BASE-FX ポート	300 ミリ秒	3100 ミリ秒
10/100/1000BASE-TX ポート	300 ミリ秒	3100 ミリ秒
1000BASE-TX ポート	300 ミリ秒	3100 ミリ秒
ファイバ ギガビット イーサネット ポート	10 ミリ秒	100 ミリ秒
10 ギガビット イーサネット ポート	10 ミリ秒	100 ミリ秒

ポート デバウンス タイマーを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポート デバウンス タイマーをイネーブルにします。	**set port debounce** *mod num/port num* {**enable** | **disable**}
ステップ 2	ポート デバウンス タイマーが正しく設定されていることを確認します。	**show port debounce** [*mod* | *mod_num/port_num*]

次に、ポート 2/1 上でデバウンス タイマーをイネーブルにする例を示します。

```
Console> (enable) set port debounce 2/1 enable
Debounce is enabled on port 2/1
Warning: Enabling port debounce causes Link Up/Down detections to be delayed.
It results in loss of data traffic during debouncing period, which might
affect the convergence/reconvergence of various Layer 2 and Layer 3 protocols.
Use with caution.
Console> (enable)
```

次に、ポート単位でのデバウンス タイマーの設定を表示する例を示します。

```
Console> (enable) show port debounce
Port   Debounce link timer
-----  ---------------
 2/1   enable
 2/2   disable
Console> (enable)
```

ポート デバウンス タイマーの設定変更

(注) ポート デバウンス タイマーの設定変更は、ファイバ ギガビット イーサネット ポート上でのみ可能です。

ポート デバウンス タイマーの値は、100 の倍数で最大 5000 ミリ秒まで増やすことができます。タイマー値を調整する前に、ポート デバウンス タイマーをイネーブルにする必要はありません。ディセーブル ステートのデフォルト値よりも大きいタイマー値を指定した場合、デバウンス タイマーはイネーブルになります。

ポート デバウンス タイマーの設定を変更するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポート デバウンス タイマーの設定を変更します。	**set port debounce** *mod num/port num* **delay** *time*
ステップ 2	ポート デバウンス タイマーの設定が変更されていることを確認します。	**show port debounce** [*mod* | *mod_num/port_num*]

次に、ポート 2/1 上でデバウンス タイマーの設定を変更する例を示します。

```
Console> (enable) set port debounce 2/1 delay 500
Debounce time for port 2/1 set to 500 ms.
Warning:Enabling port debounce causes Link Up/Down detections to be delayed.
It results in loss of data traffic during debouncing period, which might
affect the convergence/reconvergence of various Layer 2 and Layer 3 protocols.
Use with caution.
Console> (enable)
```

次に、ポート 2/1 上でポート単位でのデバウンス タイマーの設定を表示する例を示します。

```
Console> (enable) show port debounce 2/1
Port   Debounce link timer
-----  ------------------
 2/1   enabled (500 ms)
Console> (enable)
```

ポートの errdisable ステートにおけるタイムアウト設定

ポートが NVRAM（不揮発性 RAM）ではイネーブルに設定されていても、実行時に何らかのプロセスによってディセーブルにされた場合、そのポートは errdisable ステートになります。たとえば、UniDirectional Link Detection（UDLD; 単一方向リンク検出）が単一方向リンクを検出すると、ポートは実行時にシャットダウンされます。ただし、そのポートの NVRAM 設定はイネーブルに設定されている（ユーザがポートをディセーブルにしていない）ので、ポートのステータスは errdisable として表示されます。

ポートが errdisable ステートになると、指定時間が経過したあと、そのポートは再びイネーブルになります。タイムアウト機能が強化され、errdisable タイムアウトの設定によってポートがイネーブルになるのを手動で防ぐことができます。このようにするには、**set port errdisable-timeout** *mod/port* **disable** コマンドを使用して、タイムアウトをディセーブルにします。

グローバル タイマーはすべてのポートに対して維持されます。プロセスは、*t* 秒が経過するたびに（*t* はユーザが設定したタイムアウト時間）errdisable ステートになっているポートがないかどうかチェックします。errdisable ステートになっているポートのうち、errdisable タイムアウトが設定されている（イネーブル）ポートだけが SCP メッセージによってイネーブルに戻ります。

デフォルトでは、グローバル タイマーがタイムアウトになると、errdisable ステートになっているポートはすべてイネーブルに戻ります。

ポートが errdisable ステートになる理由には、次のものがあります（これらは、**set errdisable-timeout enable** コマンドの設定オプションとして表示されます）。

- ARP inspection（ARP 検査）
- Broadcast suppression（ブロードキャスト抑制）
- BPDU port-guard（BPDU ポート ガード）
- CAM monitor（CAM モニタ）
- Channel misconfiguration（チャネルの設定ミス）
- Crossbar failure（クロスバー障害）
- Duplex mismatch（デュプレックス モードが不一致）
- Layer 2 protocol tunnel misconfiguration（レイヤ 2 プロトコル トンネルの設定ミス）
- Layer 2 protocol tunnel threshold exceeded（レイヤ 2 プロトコル トンネル スレッシュホールド超過）
- Layer 2 protocol tunnel CDP threshold exceeded（レイヤ 2 プロトコル トンネル CDP スレッシュホールド超過）
- Layer 2 protocol tunnel STP threshold exceeded（レイヤ 2 プロトコル トンネル STP スレッシュホールド超過）

- Layer 2 protocol tunnel VTP threshold exceeded（レイヤ 2 プロトコル トンネル VTP スレッシュホールド超過）
- リンク エラー RX スレッシュホールド 超過
- リンク エラー TX スレッシュホールド 超過
- UDLD
- Other（上記以外の原因）
- All（上記の原因のすべてに errdisable タイムアウトを適用）

上記のそれぞれの原因について、errdisable タイムアウトをイネーブルまたはディセーブルに設定できます。[other] を指定した場合、上記以外の原因で errdisable ステートになったすべてのポートが、errdisable タイムアウト後にイネーブルになります。[all] を指定した場合は、原因が何であるかにかかわらず、errdisable ステートになったすべてのポートが、errdisable タイムアウト後にイネーブルになります。

errdisable 機能は、デフォルトではディセーブルです。ポートがイネーブルに設定されるデフォルトの間隔は 300 秒です。この間隔は、30 ～ 86,400 秒（30 秒～ 24 時間）の範囲で設定できます。

errdisable ステートのポートのタイムアウト時間をイネーブルにして設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
ポートが errdisable ステートになったあとにタイムアウトになってもイネーブルに戻らないようにします。	**set port errdisable-timeout** *mod/port* **disable**
BPDU ガードが原因による errdisable タイムアウトをイネーブルにします。	**set errdisable-timeout enable bpdu-guard**
あらゆる原因による errdisable タイムアウトをイネーブルにします。	**set errdisable-timeout enable all**
errdisable タイムアウト間隔を設定します。	**set errdisable-timeout interval** *interval*
errdisable タイムアウト設定を表示します。	**show errdisable-timeout**

次に、ポート 3/3 が errdisable ステートになったあとにタイムアウトになってもイネーブルに戻らないようにする例を示します。

```
Console> (enable) set port errdisable-timeout 3/3 disable
Successfully disabled errdisable-timeout for port 3/3.
Console> (enable)
```

次に、BPDU ガードが原因による errdisable タイムアウトをイネーブルにする例を示します。

```
Console> (enable) set errdisable-timeout enable bpdu-guard
Successfully enabled errdisable-timeout for bpdu-guard.
Console> (enable)
```

次に、あらゆる原因による errdisable タイムアウトをイネーブルにする例を示します。

```
Console> (enable) set errdisable-timeout enable all
Successfully enabled errdisable-timeout for all.
Console> (enable)
```

次に、errdisable タイムアウト間隔を 450 秒に設定する例を示します。

```
Console> (enable) set errdisable-timeout interval 450
Successfully set errdisable timeout to 450 seconds.
Console> (enable)
```

次に、errdisable タイムアウトの設定を表示する例を示します。

```
Console> (enable) show errdisable-timeout
ErrDisable Reason                       Timeout Status
--------------------------------------- --------------
arp-inspection                          enable
bcast-suppression                       enable
bpdu-guard                              enable
cam-monitor                             enable
channel-misconfig                       enable
crossbar-fallback                       enable
duplex-mismatch                         enable
gl2pt-ingress-loop                      enable
gl2pt-threshold-exceed                  enable
gl2pt-cdp-threshold-exceed              enable
gl2pt-stp-threshold-exceed              enable
gl2pt-vtp-threshold-exceed              enable
link-rxcrc                              enable
link-txcrc                              enable
udld                                    enable
other                                   enable

Interval: 450 seconds

Port  ErrDisable Reason    Port ErrDisableTimeout  Action on Timeout
----  -------------------  ----------------------  -----------------
Console> (enable)
```

自動モジュール シャットダウンの設定

自動モジュール シャットダウンをイネーブルにすると、ネットワーク接続の問題を管理できます。頻繁にリセットするモジュールでは、トラフィックのロード バランシングが中断する可能性があります。自動モジュール シャットダウンをイネーブルにすることで、ハードウェアまたはソフトウェア障害が原因で頻繁にリセットされるモジュールをディセーブルにして、完全にシャットダウンする前にモジュール自身がリセットする回数を制限できます。

また **set module disable** または **set module power down** コマンドを使用して手動でモジュールをシャットダウンできます。

モジュールのシャットダウン後、モジュールを手動で再度イネーブルにする必要があります。

デフォルトで、自動モジュール シャットダウンはディセーブルです。自動モジュール シャットダウンをイネーブルにする場合、モジュール自身がリセットできる回数はデフォルトで 2 分間に 3 回です。

自動シャットダウンが発生する前にこれらの 2 つのパラメータを設定する必要があります。

- 頻度 ― 自動モジュール シャットダウンのスレッシュホールド値を指定できます。リセット回数がこのオプションに割り当てられた値に達すると、イーサネット モジュールが自動シャットダウンを実行できます。
- 期間 ― リセット回数が発生すべき期間を指定できます。期間は、次のいずれかの条件で測定されます。
  - ― スイッチが最初に起動する時
  - ― スーパバイザ エンジンがスイッチオーバーを実行する時
  - ― イーサネット モジュールの電源投入時
  - ― モジュールの自動シャット カウンタが消去される時

定義した期間内にリセットの発生回数が頻度スレッシュホールドに達した場合、イーサネット モジュールが自動的にシャットダウンされて次のようなサンプルの Syslog メッセージが表示されます。

```
%SYS-5-MOD_AUTOSHUT:Module 2 shutdown automatically, reset 4 times in last 5 minutes
due to inband failure
```

頻度スレッシュホールドに達して定義した期間外でリセットが発生した場合、モジュールは自動的にシャットダウンせずに次のようなサンプルの Syslog メッセージが表示されます。

```
%%SYS-4-MOD_AUTOSHUT_SLOW:Module 1 reset frequency exceeded threshold but over 46
mins.Hence NOT powering down module
```

イーサネット モジュールの実行変数ステートは、スタンバイ スーパバイザ エンジンとは同期しません。スタンバイ スーパバイザ エンジン上の **show autoshut** コマンドの出力は、リセット回数やリセットの理由を追跡しません。**autoshut** コマンドでモジュールの電源を切断する場合、出力は同じままです。

リセット回数を追跡するために自動モジュール シャットダウンをイネーブルにする必要はありません。自動モジュール シャットダウンをイネーブルにしなくともリセットは追跡されます。

ランタイム カウンタは、次のような条件でのみ消去されます。

- **clear autoshut** コマンドを入力した時
- スイッチがリセットされた時
- モジュールの電源投入時
- スーパバイザ エンジンのスイッチオーバー時

（注） 自動モジュール シャットダウンは、イーサネット モジュールでのみサポートされます。

自動モジュール シャットダウンをイネーブルにして設定するには、イネーブル モードで次のいずれかの作業を行います。

作業	コマンド
モジュールで自動モジュール シャットダウンをイネーブルにします。	**set module autoshut enable** *mod num*
モジュールで自動モジュール シャットダウンをディセーブルにします。	**set module autoshut disable** *mod num*
モジュール自身がリセットできる回数のスレッシュホールドを設定します。	**set autoshut frequency** *num*
頻度が有効な期間を分単位で設定します。	**set autoshut period** *minutes*
特定のモジュールのランタイム カウンタを消去します。	**clear autoshut counters** *mod num*
自動シャットダウンの頻度をデフォルト設定にリセットします。	**clear autoshut frequency**
自動シャットダウンの期間をデフォルト設定にリセットします。	**clear autoshut period**
自動モジュール シャットダウン設定と現在のステータス情報を表示します。	**show autoshut**

次に、モジュールで自動モジュール シャットダウンをイネーブルにする例を示します。

```
Console> (enable) set module autoshut enable 2
```

次に、モジュールで自動モジュール シャットダウンをディセーブルにする例を示します。

```
Console> (enable) set module autoshut disable 2
```

次に、モジュール自身がリセットできる回数のスレッシュホールドを設定する例を示します。

```
Console> (enable) set autoshut frequency 4
```

次に、頻度が有効な期間を分単位で設定する例を示します。

```
Console> (enable) set autoshut period 3
```

次に、特定のモジュールのランタイム カウンタを消去する例を示します。

```
Console> (enable) clear autoshut counters 3
Automatic shutdown counters cleared for module 3
Console> (enable)
```

次に、自動モジュール シャットダウンの頻度をデフォルト設定にリセットする例を示します。

```
Console> (enable) clear autoshut frequency
```

次に、自動モジュール シャットダウンの期間をデフォルト設定にリセットする例を示します。

```
Console> (enable) clear autoshut period
```

次に、自動モジュール シャットダウン設定と現在のステータス情報を表示する例を示します。

```
Console> (enable) show autoshut
AutoShut Frequency:     3 times
AutoShut Period:        5 minutes

Mod Autoshut Current  Number Reason for last Time of last reset
num status   status   resets reset
--- -------- -------- ------ ---------------- -------------------------
1   NA       ok       -      -                -
2   enabled  shutdown 4       inband failure  Mon Jul 14 2003, 22:55:45
3   disabled ok       0      None             -
4   enabled  ok       1      scp failure      Mon Jul 14 2003, 21:03:17
Console> (enable)
```

ポート エラー検出の設定

（注）　EtherChannel のすべてのポートで、ポート エラー検出設定が同じである必要があります。

ポート上でポート エラー検出をイネーブルまたはディセーブルにするには、イネーブル モードで次の作業を行います（inerrors、RXCRC、および TXCRC のデフォルト ポート設定はディセーブルです）。

	作業	コマンド
ステップ 1	ポート上でポート エラー検出をイネーブルまたはディセーブルにします。	**set port errordetection** *mod/port* {**inerrors** | **rxcrc** | **txcrc**} {**disable** | **enable**}
ステップ 2	ポートの設定を確認します。	**show port errordetection** [*mod* | *mod/port*]

次に、ポート 3/1 上で RXCRC ポート エラー検出をイネーブルにする例を示します。

```
Console> (enable) set port errordetection 3/1 rxcrc enable
Port(s)  3/1 set to errordetection rxcrc enable.
Console> (enable) show port errordetection 3/1
Port    Rxcrc     Txcrc
-----   --------  --------
 3/1    enabled   disabled
Console> (enable)
```

冗長フレックス リンクの設定

冗長フレックス リンクでは、ユーザが STP をディセーブル化しても、リンクレベルの冗長性を実現し、STP に代わる解決策を提供します。冗長フレックス リンクは、高速スイッチオーバー冗長性によるリンク バックアップ機能を提供します。フレックス リンクの冗長性により、2 つのポートを指定して、冗長リンク機能を形成できます。一方のポートをアクティブ ポートとして、もう一方のポートをバックアップまたは*ピア* ポートとして設定します。アクティブ ポートはフォワーディング ステートでも、バックアップ ポートがブロッキング ステートのため、トラフィックは通過できません。

フレックス リンクのアクティブ ポートに障害がある場合、MAC アドレスはフラッシュされ、フラッディングされます。フレックス リンクのバックアップ ポートは、MAC アドレスを学習して、再び接続できるようにします。フェールオーバー コンバージェンス時間は、VLAN 数および MAC アドレス数により異なります。フレックスリンク ポート上では STP をイネーブルにできませんが、スイッチの他のポート上では STP を稼働できます。

ヒント　2 つのアップリンク ポートを介してレイヤ 2 コンセントレータ スイッチと接続する、共通 VLAN を持つ複数のレイヤ 2 アクセス スイッチの構成において、冗長フレックス リンクを使用することを推奨します。

ここでは、Catalyst 6500 シリーズ スイッチ上で冗長フレックス リンクを設定する手順について説明します。

- 冗長フレックス リンクの設定に関する注意事項および制限事項（p.4-19）
- フレックス リンクのアクティブ ポートおよびバックアップ ポートの指定（p.4-19）

- フレックス リンクのポート設定の表示（p.4-20）
- フレックス リンクのポート設定の消去（p.4-20）

冗長フレックス リンクの設定に関する注意事項および制限事項

ここでは、冗長フレックス リンクを設定する際の注意事項と制限事項を説明します。

- フレックス リンク ペアの最大数（1 つのアクティブ ポートと 1 つのバックアップ ポート）は、スイッチごとに 16 です。
- フレックスリンク ポートを、EtherChannel の一部にすることはできません。
- STP ― フレックスリンク ポートは、STP 動作に加入しません。フレックスリンク ポートは、STP BPDU を生成せず、受信したすべての BPDU を廃棄します。
- Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）― SPAN はフレックスリンク ポートと連動します。
- VTP ― VTP プルーニングは STP と連動する必要があるので、フレックスリンク ポートでは機能しません。
- Internet Group Management Protocol（IGMP）― IGMP はフレックスリンク ポートと連動します。
- Dynamic Trunking Protocol（DTP; ダイナミック トランキング プロトコル）― DTP はフレックス リンク ポート上で稼働できます。
- 冗長フレックス リンクは、単純なアクセス トポロジー（1 つのリーフ ノードから 2 つのアップリンク）用です。配線クローゼットからアクセス ネットワークへのパスにループがないことを確認する必要があります。STP とは異なり、フレックスリンク ポートはループを検出するように設計されていません。
- エッジでフレックスリンク冗長を実行しながら、コア ネットワークで STP を配置するのが好ましい設定です。
- フレックス　リンクは、直接接続されたリンクで障害が起こった場合にのみ高速で収束されます。ネットワーク内のその他の障害は、フレックスリンクの高速コンバージェンスにより改善されません。

フレックス リンクのアクティブ ポートおよびバックアップ ポートの指定

フレックス リンクのアクティブ ポートおよびバックアップ（ピア）ポートを指定するには、イネーブル モードで次の作業を実行します。

作業	コマンド
フレックス リンクのアクティブ ポートおよびバックアップ（ピア）ポートを指定します。	**set port flexlink** *mod/port* **peer** *mod/port*

次に、ポート 3/48 をフレックスリンクのアクティブ ポートに、ポート 3/47 をフレックスリンクのバックアップ（ピア）ポートに指定する例を示します。

```
Console> (enable) set port flexlink 3/48 peer 3/47
Flexlink is successfully set on the port 3/48 and 3/47
Console> (enable)
```

フレックス リンクのポート設定の表示

フレックスリンクのポート設定についての情報を表示するには、ユーザ モードで次の作業を実行します。

作業	コマンド
フレックスリンクのポート設定についての情報を表示します。	**show port flexlink** [*mod* | *mod/port*]

次に、スイッチ上で設定されたすべてのフレックスリンク ポートについての情報を表示する例を示します。

```
Console> (enable) show port flexlink
Port   State       Peer port  State
-----  ----------  ---------  ----------
 3/47  linkdown    3/48       active
 3/48  active      3/47       linkdown
Console> (enable)
```

フレックス リンクのポート設定の消去

フレックス リンクのポート設定を消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
フレックス リンクのポート設定を消去します。	**clear port flexlink** *mod/port* [**peer** *mod/port*]

次に、フレックスリンクのアクティブ ポートとしてポート 3/48 を、フレックスリンクのバックアップ（ピア）ポートとしてポート 3/47 を消去する例を示します。

```
Console> (enable) clear port flexlink 3/48 peer 3/47
Port 3/48 and 3/47 flexlink pair cleared
Console> (enable)
```

ジャンボ フレームの設定

ここでは、ジャンボ フレームを設定する手順について説明します。

- スーパバイザ エンジン上でのジャンボ フレームの設定（p.4-20）
- MSFC2 上でのジャンボ フレームの設定（p.4-22）

スーパバイザ エンジン上でのジャンボ フレームの設定

あるポートに対してジャンボ フレーム機能をイネーブルに設定すると、そのポートで大きい（つまりジャンボ）フレームをスイッチングできるようになります。この機能はサーバ間の転送パフォーマンスを最適化するのに役立ちます。デフォルトの Maximum Transmission Unit（MTU; 最大伝送ユニット）フレーム サイズは、すべてのイーサネット ポートで 1548 バイトです。ポート上でジャンボ フレーム機能をイネーブルに設定すると、MTU サイズは 9216 バイトに増えます。

ポート単位でジャンボ フレーム機能をイネーブルに設定する際は、次の注意事項に従ってください。

（注）　WS-X6148 および WS-X6548 GE-TX モジュールはジャンボ フレームをサポートしていません。

- ジャンボ フレーム機能は、次のポート上でサポートされます。
  - すべてのイーサネット ポート
  - トランク ポート
  - EtherChannel
  - sc0 インターフェイス（ジャンボ フレームは sc0 インターフェイスを通過します。これはユーザが設定できないデフォルト設定なので、CLI による設定は不要です）。
- 次のスイッチング モジュールでは、最大 8092 バイトの入力フレーム サイズをサポートしています。
  - 100 Mbps で動作する WS-6516-GE-TX。10 Mbps および 1000 Mbps では、ジャンボ フレームのデフォルト値である 9216 バイトをサポートしています。
  - WS-X6148-RJ-45、WS-X6148-RJ-45V、WS-X6148-RJ21、および WS-X6148-RJ21V
  - WS-X6248-RJ-45、WS-X6248A-RJ-45、WS-X6248-TEL、および WS-X6248A-TEL
  - WS-X6348-RJ-45、WS-X6348-RJ45V、WS-X6348-RJ-21、および WX-X6348-RJ21V

  ジャンボ フレームのサポートを設定すると、これらのモジュールは 8092 バイトを超える入力フレームを廃棄します。
- WS-X6548-RJ-21、および WS-X6548-RJ-45 モジュールは、Physical Sublayer（PHY; 物理サブレイヤ）レベルで異なるハードウェアを使用して、ジャンボ フレームの最大デフォルト値である 9216 バイトをサポートしています。
- ジャンボ フレームは、すべての OSM（オプティカル サービス モジュール）上でサポートされています。
- ジャンボ フレームは、Asynchronous Transfer Mode（ATM; 非同期転送モード）モジュール（WS-X6101-OC12-SMF/MMF）上ではサポートされていません。
- Multilayer Switch Feature Card 2（MSFC2; マルチレイヤ スイッチ フィーチャ カード 2）は、Cisco IOS Release 12.1(2)E 以降のリリースによりジャンボ フレームのルーティングをサポートしています。
- MSFC および Multilayer Switch Module（MSM）は、ジャンボ フレームのルーティングをサポートしていません。これらのルータにジャンボ フレームが送信されると、ルータのパフォーマンスが著しく低下します。

（注） **show port jumbo** コマンドを入力すると、1 つまたは複数のポートに関して [Jumbo frames inconsistent state] メッセージが表示されることがあります。その場合には、**set port jumbo** コマンドを入力してポートを再度イネーブルに設定してください。

イーサネット ポート上でジャンボ フレームをイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ジャンボ フレームをイネーブルに設定します。	**set port jumbo** *mod*/*port* **enable**
ステップ 2	ポートの設定を確認します。	**show port jumbo**

次に、ポート上でジャンボ フレーム機能をイネーブルにし、設定を確認する例を示します。

```
Console> (enable) set port jumbo 2/1 enable
Jumbo frames enabled on port 2/1
Console> (enable) show port jumbo
Jumbo frames MTU size is 9216 bytes
Jumbo frames enabled on port(s) 2/1
```

イーサネット ポート上でジャンボ フレーム機能をディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ジャンボ フレームをディセーブルに設定します。	**set port jumbo** *mod*/*port* **disable**
ステップ 2	ポートの設定を確認します。	**show port jumbo**

次に、ポート上でジャンボ フレームをディセーブルにする例を示します。

```
Console> (enable) set port jumbo 2/1 disable
Jumbo frames disabled on port 2/1
Console> (enable)
```

MSFC2 上でのジャンボ フレームの設定

MSFC2 では、ジャンボ フレームのルーティングに対応できるように、VLAN インターフェイス上の MTU サイズを設定できます。

ジャンボ フレーム機能では、スイッチのデフォルトより大きい MTU サイズが 1 つだけサポートされています。デフォルトより大きい MTU サイズで VLAN インターフェイスを設定すると、デフォルトより大きい MTU サイズに設定されているほかのすべての VLAN インターフェイスが、新しく設定されたサイズに自動的に変更されます。デフォルトから変更していない VLAN インターフェイスについては、影響はありません。

MTU 値を設定するには、次の作業を行います。

	作業	コマンド
ステップ 1	VLAN インターフェイス コンフィギュレーション モードにアクセスします。	Router(config)# **interface vlan** *vlan_ID*
ステップ 2	MTU サイズを設定します。有効な値は、64 ～ 17952 バイトです[1]。	Router(config-if)# **mtu** *mtu_size*
ステップ 3	設定を確認します。	Router# **show interface vlan 111**

1. MTU サイズは、9216（スーパバイザ エンジンでサポートされるサイズ）以下に設定してください。

次に、VLAN インターフェイス上の MTU サイズを設定し、設定を確認する例を示します。

```
Router(config)# interface vlan 111
Router(config-if)# mtu 9216
Router(config-if)# end
Router# show interface vlan 111
.
.
.
MTU 9216 bytes, BW 1000000 Kbit, DLY 10 usec,
.
.
.
Router#
```

接続の確認

接続を確認するには、**ping** コマンドおよび **traceroute** コマンドを使用します。

ポートからの接続を確認するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	テスト対象ポートの先にあるリモート ホストに対して、ping を実行します。	**ping** [**-s**] *host* [*packet_size*] [*packet_count*]
ステップ 2	スイッチからテスト対象ポートの先にあるリモート ホストまでのパケット ルートを、ホップ単位で追跡します。	**traceroute** *host*
ステップ 3	ホストが応答しない場合には、スイッチに設定されている IP アドレスおよびデフォルト ゲートウェイを確認します。	**show interface** **show ip route**

次に、リモート ホストに ping を実行し、**traceroute** を使用してネットワーク上のパケット パスをホップ単位で追跡する例を示します。

```
Console> (enable) ping somehost
somehost is alive
Console> (enable) traceroute somehost
traceroute to somehost.company.com (10.1.2.3), 30 hops max, 40 byte packets
 1 engineering-1.company.com (173.31.192.206) 2 ms 1 ms 1 ms
 2 engineering-2.company.com (173.31.196.204) 2 ms 3 ms 2 ms
 3 gateway_a.company.com (173.16.1.201) 6 ms 3 ms 3 ms
 4 somehost.company.com (10.1.2.3) 3 ms * 2 ms
Console> (enable)
```

CHAPTER 5

イーサネット VLAN トランクの設定

この章では、Catalyst 6500 シリーズ スイッチ上でイーサネット VLAN（仮想 LAN）トランクを設定する手順について説明します。

(注) VLAN の詳しい設定手順については、第 11 章「VLAN の設定」を参照してください。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

この章で説明する内容は、次のとおりです。

VLAN トランクの機能概要

ここでは、Catalyst 6500 シリーズ スイッチ上での VLAN トランクの機能について説明します。

トランクの概要

トランクとは、1 つまたは複数のイーサネット スイッチ ポートと他のネットワーキング装置（スイッチ、ルータなど）の間に設定するポイントツーポイント リンクです。トランクを使用して複数の VLAN トラフィックを転送することにより、ネットワーク全体にわたって VLAN を拡張することができます。

すべてのイーサネット ポート上で、次の 2 種類のトランキング カプセル化方式を使用できます。

- ISL（スイッチ間リンク）― ISL は、シスコ独自のトランキング カプセル化方式です。
- IEEE 802.1Q ― 802.1Q は、業界標準のトランキング カプセル化方式です。

トランクを設定できるのは、1 つのイーサネット ポートまたは EtherChannel バンドルに対してです。EtherChannel の詳細については、第 6 章「EtherChannel の設定」を参照してください。

イーサネットのトランク ポートは、5 種類のトランキング モードをサポートしています（表 5-1 を参照）。さらに、トランクでの ISL カプセル化の使用、802.1Q カプセル化の使用、またはカプセル化タイプの自動ネゴシエーションを指定することもできます。

自動ネゴシエーションでトランキングを行うには、各ポートが同じ VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）ドメインに存在する必要があります。ただし、異なるドメインにあっても、**on** または **nonegotiate** モードを使用して、ポートを強制的にトランクにすることができます。VTP ドメインの詳細については、第 10 章「VTP の設定」を参照してください。

トランク ネゴシエーションは、Dynamic Trunking Protocol（DTP; ダイナミック トランキング プロトコル）によって管理されます。DTP は、ISL および 802.1Q の両方のトランクで自動ネゴシエーションをサポートしています。

トランキング モードおよびカプセル化タイプ

（注） ISL カプセル化をサポートしないモジュールの完全なリストについては、次の URL にある『*Catalyst 6500 Series Release Notes*』を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/index.htm

表 5-1 に、**set trunk** コマンドで設定できるトランキング モードと、ファスト イーサネット、ギガビット イーサネット、および 10 ギガビット イーサネット ポート上におけるその機能を示します。

表 5-1　イーサネット トランキング モード

モード	機能
on	ポートに永続的なトランキング モードを設定し、リンクをトランク リンクに変換するためのネゴシエーションを行います。近接ポートが変更に同意しなくても、ポートはトランク ポートになります。
off	ポートに永続的な非トランキング モードを設定し、リンクを非トランク リンクに変換するためのネゴシエーションを行います。近接ポートが変更に同意しなくても、ポートは非トランク ポートになります。
desirable	リンクからトランク リンクへの変換をポートに積極的に試行させます。近接ポートが **on**、**desirable**、または **auto** モードに設定されていれば、ポートはトランク ポートになります。
auto	ポートにリンクからトランク リンクへの変換を試行させます。近接ポートが **on** または **desirable** モードに設定されていれば、ポートはトランク ポートになります。これはすべてのイーサネット ポートのデフォルトのモードです。
nonegotiate	ポートを永続的なトランキング モードにしますが、ポートが DTP フレームを生成しないようにします。トランク リンクを確立するには、近接ポートを手動でトランク ポートとして設定する必要があります。

表 5-2 に、**set trunk** コマンドで設定できるカプセル化タイプ、およびイーサネット ポート上での機能を示します。**show port capabilities** コマンドを入力すると、個々のポートでサポートされているカプセル化タイプを判別することができます。

表 5-2　イーサネット トランク カプセル化タイプ

カプセル化	機能
isl	トランク リンクに ISL カプセル化を指定します。
dot1q	トランク リンクに 802.1Q カプセル化を指定します。
negotiate	ポートが近接ポートとネゴシエーションを行い、近接ポートの設定および機能に応じて、ISL（優先）または 802.1Q トランクになることを指定します。

トランク リンクを確立できるかどうか、および確立したリンクに設定されるトランク タイプは、2 つの接続ポートのトランキング モード、トランク カプセル化タイプ、およびハードウェア機能によって決まります。表 5-3 に、可能なトランク設定およびその結果を示します。

表 5-3　ファスト イーサネット、ギガビット イーサネット、および 10 ギガビット イーサネットのトランク設定の結果

近接ポートのトランク モードおよびカプセル化	ローカル ポートのトランク モードおよびカプセル化								
	off **isl または dot1q**	**on** **isl**	**desirable** **isl**	**auto** **isl**	**on** **dot1q**	**desirable** **dot1q**	**auto** **dot1q**	**desirable** **negotiate**	**auto** **negotiate**
off **isl または dot1q**	ローカル：非トランク 近接：非トランク	ローカル：ISL トランク 近接：非トランク	ローカル：非トランク 近接：非トランク	ローカル：非トランク 近接：非トランク	ローカル：1Q トランク 近接：非トランク	ローカル：非トランク 近接：非トランク	ローカル：非トランク 近接：非トランク	ローカル：非トランク 近接：非トランク	ローカル：非トランク 近接：非トランク
on **isl**	ローカル：非トランク 近接：ISL トランク	ローカル：ISL トランク 近接：ISL トランク	ローカル：ISL トランク 近接：ISL トランク	ローカル：ISL トランク 近接：ISL トランク	ローカル：1Q トランク[1] 近接：ISL トランク[1]	ローカル：非トランク 近接：ISL トランク	ローカル：非トランク 近接：ISL トランク	ローカル：ISL トランク 近接：ISL トランク	ローカル：ISL トランク 近接：ISL トランク
desirable **isl**	ローカル：非トランク 近接：非トランク	ローカル：ISL トランク 近接：ISL トランク	ローカル：ISL トランク 近接：ISL トランク	ローカル：ISL トランク 近接：ISL トランク	ローカル：1Q トランク 近接：非トランク	ローカル：非トランク 近接：非トランク	ローカル：非トランク 近接：非トランク	ローカル：ISL トランク 近接：ISL トランク	ローカル：ISL トランク 近接：ISL トランク
auto **isl**	ローカル：非トランク 近接：非トランク	ローカル：ISL トランク 近接：ISL トランク	ローカル：ISL トランク 近接：ISL トランク	ローカル：非トランク 近接：非トランク	ローカル：1Q トランク 近接：非トランク	ローカル：非トランク 近接：非トランク	ローカル：非トランク 近接：非トランク	ローカル：ISL トランク 近接：ISL トランク	ローカル：非トランク 近接：非トランク
on **dot1q**	ローカル：非トランク 近接：1Q トランク	ローカル：ISL トランク[1] 近接：1Q トランク[1]	ローカル：非トランク 近接：1Q トランク	ローカル：非トランク 近接：1Q トランク	ローカル：1Q トランク 近接：1Q トランク	ローカル：1Q トランク 近接：1Q トランク	ローカル：1Q トランク 近接：1Q トランク	ローカル：1Q トランク 近接：1Q トランク	ローカル：1Q トランク 近接：1Q トランク
desirable **dot1q**	ローカル：非トランク 近接：非トランク	ローカル：ISL トランク 近接：非トランク	ローカル：非トランク 近接：非トランク	ローカル：非トランク 近接：非トランク	ローカル：1Q トランク 近接：1Q トランク	ローカル：1Q トランク 近接：1Q トランク	ローカル：1Q トランク 近接：1Q トランク	ローカル：1Q トランク 近接：1Q トランク	ローカル：1Q トランク 近接：1Q トランク
auto **dot1q**	ローカル：非トランク 近接：非トランク	ローカル：ISL トランク 近接：非トランク	ローカル：非トランク 近接：非トランク	ローカル：非トランク 近接：非トランク	ローカル：1Q トランク 近接：1Q トランク	ローカル：1Q トランク 近接：1Q トランク	ローカル：非トランク 近接：非トランク	ローカル：1Q トランク 近接：1Q トランク	ローカル：非トランク 近接：非トランク
desirable **negotiate**	ローカル：非トランク 近接：非トランク	ローカル：ISL トランク 近接：ISL トランク	ローカル：ISL トランク 近接：ISL トランク	ローカル：ISL トランク 近接：ISL トランク	ローカル：1Q トランク 近接：1Q トランク	ローカル：1Q トランク 近接：1Q トランク	ローカル：1Q トランク 近接：1Q トランク	ローカル：ISL トランク 近接：ISL トランク	ローカル：ISL トランク 近接：ISL トランク
auto **negotiate**	ローカル：非トランク 近接：非トランク	ローカル：ISL トランク 近接：ISL トランク	ローカル：ISL トランク 近接：ISL トランク	ローカル：非トランク 近接：非トランク	ローカル：1Q トランク 近接：1Q トランク	ローカル：1Q トランク 近接：1Q トランク	ローカル：非トランク 近接：非トランク	ローカル：ISL トランク 近接：ISL トランク	ローカル：非トランク 近接：非トランク

1. この設定はスパニングツリー ループの原因になるので推奨できません。

（注） DTP はポイントツーポイント プロトコルです。ただし、インターネットワーキング装置によっては、DTP フレームが正しく転送されないことがあります。この問題を回避するために、スイッチ以外の装置に接続するポートで、これらのポートのリンクにトランクを使用しない場合には、トランク モードを必ず **off** に設定してください。シスコ製ルータへのリンク上のトランクを手動でイネーブルにする場合は、**nonegotiate** キーワードを入力してください。これにより、ポートはトランクを設定しても DTP フレームを生成しません。

802.1Q トランク設定時の注意事項および制限事項

802.1Q トランクを使用し、かつネットワークのトランク設定にいくつかの制限を設ける場合、以下の注意事項および制限事項を考慮してください。

- 802.1Q トランクを介してシスコ製スイッチを接続している場合は、802.1Q トランクのネイティブ VLAN が、トランク リンクの両端で同じであることを確認してください。トランクの一端のネイティブ VLAN と反対側のネイティブ VLAN が異なると、スパニングツリー ループの原因になります。
- ネットワーク上のすべてのネイティブ VLAN についてスパニングツリーをディセーブルにせずに、802.1Q トランクの VLAN 上のスパニングツリーをディセーブルにすると、スパニングツリー ループが発生することがあります。802.1Q トランクのネイティブ VLAN 上のスパニングツリーは、イネーブルのままにしてください。それができない場合は、ネットワークのすべての VLAN のスパニングツリーをディセーブルにしてください。スパニングツリーをディセーブルにする場合には、前もってネットワークで物理ループが発生しないことを確認してください。
- 802.1Q トランクを使用して 2 台のシスコ製スイッチを接続している場合は、スイッチはトランク上で許容されている VLAN ごとにスパニングツリー Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）を交換します。トランクのネイティブ VLAN 上の BPDU は、タグなしで予約 IEEE 802.1D スパニングツリー マルチキャスト MAC（メディア アクセス制御）アドレス（01-80-C2-00-00-00）に送信されます。トランクの残りの VLAN 上の BPDU は、タグ付きで予約 Cisco Shared Spanning Tree（SSTP）マルチキャスト MAC アドレス（01-00-0c-cc-cc-cd）に送信されます。
- 他社製の 802.1Q スイッチは、すべての VLAN のスパニングツリー トポロジーを定義するスパニングツリーの 1 つのインスタンス（Mono Spanning Tree [MST]）しか維持しません。802.1Q トランクを介して他社製のスイッチにシスコ製スイッチを接続すると、他社製のスイッチの MST とシスコ製スイッチのネイティブ VLAN スパニングツリーが統合されて、Common Spanning Tree（CST）という 1 つのスパニングツリー トポロジーを形成します。

  他社製のスイッチにシスコ製スイッチを接続した場合、CST は常に VLAN 1 上にあります。シスコ製スイッチは、CST の VLAN 1 上でタグのない IEEE BPDU（01-80-C2-00-00-00）を送信します。ネイティブ VLAN 上では、シスコ製スイッチはタグのない Cisco BPDU（01-00-0C-CC-CC-CC）を送信します。この Cisco BPDU は他社製スイッチが転送しても処理対象になりません（ネイティブ VLAN 上では、IEEE BPDU は転送されません）。
- シスコ製スイッチは、トランクのネイティブ VLAN 以外の VLAN 上で SSTP マルチキャスト MAC アドレスに BPDU を送信するので、他社製のスイッチはこれらのフレームを BPDU とは認識せず、対応する VLAN のすべてのポートにフラッディングします。他社製の 802.1Q に接続されたほかのシスコ製スイッチは、このフラッディングされた BPDU を受信します。これにより、シスコ製スイッチは、他社製の 802.1Q スイッチ ネットワークの間で、VLAN ごとにスパニングツリー トポロジーを維持できます。シスコ製スイッチを分離する他社製の 802.1Q ネットワークは、802.1Q トランクを介して他社製の 802.1Q ネットワークに接続しているすべてのスイッチ間の単一のブロードキャスト セグメントとして処理されます。
- ネイティブ VLAN は、他社製の 802.1Q ネットワークにシスコ製スイッチを接続する すべての 802.1Q トランク上で必ず同じになるようにしてください。
- 他社製の 802.1Q ネットワークに複数のシスコ製スイッチを接続する場合は、すべての接続において 802.1Q トランクを使用する*必要があります*。ISL トランクまたはアクセス ポートを使用して、シスコ製スイッチを他社製の 802.1Q ネットワークに接続することは*できません*。接続した場合、ISL トランクまたはアクセス ポートは、スパニングツリーの port inconsistent ステートとスイッチにより判断され、そのポートではトラフィックを伝送できなくなります。

トランクのデフォルト設定

表 5-4 に、イーサネット トランクのデフォルト設定を示します。

表 5-4　イーサネット トランクのデフォルト設定

機能	デフォルト設定
トランク モード	**auto**
トランク カプセル化	**negotiate**
VLAN 許容範囲	VLAN 1 ～ 1005、1025 ～ 4094[1]

1. Release 8.3(1) 以降のソフトウェア リリースでは、ユーザ VLAN および内部 VLAN のみが存在し、予約 VLAN は存在しません。VLAN を必要とする機能のために、VLAN マネージャが VLAN を永久的に確保しておくことはありません。VLAN は必要に応じて動的に割り当てられます。ユーザ（および内部）VLAN は VLAN 範囲全体（1 ～ 4094）を使用できます。

トランク リンクの設定

ここでは、イーサネット ポート上のトランク リンクの設定手順、およびトランク上での VLAN 許容範囲の定義方法について説明します。

ISL トランクの設定

ISL トランクを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ISL トランクを設定します。	**set trunk** *mod/port* [**on** | **off** | **desirable** | **auto** | **nonegotiate**] **isl**
ステップ 2	トランキングの設定を確認します。	**show trunk** [*mod/port*]

次に、ポートをトランクとして設定し、トランク設定を確認する例を示します。この例では、近接ポートが **auto** モードに設定されていると想定します。

```
Console> (enable) set trunk 1/1 on
Port(s) 1/1 trunk mode set to on.
Console> (enable) 06/16/1998,22:16:39:DTP-5:Port 1/1 has become isl trunk
06/16/1998,22:16:40:PAGP-5:Port 1/1 left bridge port 1/1.
06/16/1998,22:16:40:PAGP-5:Port 1/1 joined bridge port 1/1.
Console> (enable) show trunk
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 1/1      on           isl            trunking      1
Port      Vlans allowed on trunk
--------  ---------------------------------------------------------------------
 1/1      1-1005, 1025-4094

Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------------------
 1/1      1,521-524
Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------------------
 1/1
Console> (enable)
```

次に、ポートを **desirable** モードに設定し、トランク設定を確認する例を示します。この例では、近接ポートが **auto** モードに設定されていると想定します。

```
Console> (enable) set trunk 1/2 desirable
Port(s) 1/2 trunk mode set to desirable.
Console> (enable) 06/16/1998,22:20:16:DTP-5:Port 1/2 has become isl trunk
06/16/1998,22:20:16:PAGP-5:Port 1/2 left bridge port 1/2.
06/16/1998,22:20:16:PAGP-5:Port 1/2 joined bridge port 1/2.
Console> (enable) show trunk 1/2
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 1/2      desirable    isl            trunking      1
Port      Vlans allowed on trunk
--------  ---------------------------------------------------------------------
 1/2      1-1005, 1025-4094
Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------------------
 1/2      1,521-524
Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------------------
 1/2
Console> (enable)
```

802.1Q トランクの設定

802.1Q トランクを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	802.1Q トランクを設定します。	**set trunk** *mod/port* [**on** | **off** | **desirable** | **auto** | **nonegotiate**] **dot1q**
ステップ 2	トランキングの設定を確認します。	**show trunk** [*mod/port*]

次に、802.1Q トランクを設定し、トランク設定を確認する例を示します。

```
Console> (enable) set trunk 2/9 desirable dot1q
Port(s) 2/9 trunk mode set to desirable.
Port(s) 2/9 trunk type set to dot1q.
Console> (enable) 07/02/1998,18:22:25:DTP-5:Port 2/9 has become dot1q trunk

Console> (enable) show trunk
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 2/9      desirable    dot1q          trunking      1

Port      Vlans allowed on trunk
--------  ---------------------------------------------------------------------
 2/9      1-1005, 1025-4094

Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------------------
 2/9      1,5,10-32,101-120,150,200,250,300,400,500,600,700,800,900,1000

Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------------------
 2/9      5,10-32,101-120,150,200,250,300,400,500,600,700,800,900,1000
Console> (enable)
```

ISL/802.1Q ネゴシエーション トランク ポートの設定

トランク ポートがトランク カプセル化タイプ（ISL または 802.1Q）のネゴシエーションを行うように設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポートにトランク カプセル化タイプのネゴシエーションを設定します。	**set trunk** *mod/port* [**on** | **off** | **desirable** | **auto** | **nonegotiate**] **negotiate**
ステップ 2	トランキングの設定を確認します。	**show trunk** [*mod/port*]

次に、ポートにカプセル化タイプのネゴシエーションを設定し、トランク設定を確認する例を示します。この例では、近接ポートは **auto** モードで、カプセル化は **isl** または **negotiate** が設定されています。

```
Console> (enable) set trunk 4/11 desirable negotiate
Port(s) 4/11 trunk mode set to desirable.
Port(s) 4/11 trunk type set to negotiate.
Console> (enable) show trunk 4/11
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 4/11     desirable    n-isl          trunking      1

Port      Vlans allowed on trunk
--------  ---------------------------------------------------------------------
 4/11     1-1005,1025-4094

Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------------------
 4/11     1,5,10-32,55,101-120,998-1000

Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------------------
 4/11     1,5,10-32,55,101-120,998-1000
Console> (enable)
```

トランク上での許容 VLAN の定義

トランク ポートを設定すると、すべての VLAN がそのトランクの許容 VLAN リストに追加されます。許容リストから VLAN を削除することにより、特定の VLAN のトラフィックがトランク上で伝送されないようにすることができます。

(注)　ポートを最初にトランクとして設定する時点では、**set trunk** コマンドの入力により、常にトランクの許容 VLAN リストにすべての VLAN が追加されます。VLAN 範囲を指定しても、その VLAN 範囲は無視されます。許容 VLAN リストを変更するには、**clear trunk** コマンドと **set trunk** コマンドを組み合わせて、許容 VLAN を指定します。

Release 8.3(1) より前のソフトウェア リリースで、トランク ポート用の許容 VLAN リストを定義するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	トランクの許容 VLAN リストから VLAN を削除します。	**clear trunk** *mod/port vlans*
ステップ 2	（任意）トランクの許容 VLAN リストに、特定の VLAN を追加します。	**set trunk** *mod/port vlans*
ステップ 3	トランクの許容 VLAN リストを確認します。	**show trunk** [*mod/port*]

次に、トランク ポート 1/1 の許容 VLAN リストで VLAN 1 ～ 100、VLAN 500 ～ 1005、および VLAN 2500 が許可されるように定義し、トランクに設定した許容 VLAN リストを確認する例を示します。

```
Console> (enable) clear trunk 1/1 101-499
Removing Vlan(s) 101-499 from allowed list.
Port 1/1 allowed vlans modified to 1-100,500-1005.
Console> (enable) set trunk 1/1 2500
Adding vlans 2500 to allowed list.
Port(s) 1/1 allowed vlans modified to 1-100,500-1005,2500.
Console> (enable) show trunk 1/1
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 1/1      desirable    isl            trunking      1
Port      Vlans allowed on trunk
--------  ---------------------------------------------------------------------
 1/1      1-100, 500-1005,2500
Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------------------
 1/1      1,521-524
Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------------------
 1/1      1,521-524
Console> (enable)
```

Release 8.3(1) 以降のソフトウェア リリースで、トランクを設定し、このトランク上で VLAN を許可しない場合は、次のように **none** キーワードを入力します。

```
Console> (enable) set trunk 7/1 on none dot1q
Removing Vlan(s) 1-4094 from allowed list.
Port 7/1 allowed vlans modified to none.
Port(s) 7/1 trunk mode set to on.
Port(s) 7/1 trunk type set to dot1q.
Console> (enable)
```

トランク ポートのディセーブル化

ポートのトランキングをオフにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポートのトランキングをオフにします。	**set trunk** *mod/port* **off**
ステップ 2	トランキングの設定を確認します。	**show trunk** [*mod/port*]

ポートをそのポート タイプに応じたデフォルトのトランク タイプおよびモードに戻すには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポートを、そのポート タイプに応じたデフォルトのトランク タイプおよびモードに戻します。	**clear trunk** *mod/port*
ステップ 2	トランキングの設定を確認します。	**show trunk** [*mod/port*]

トランク上での VLAN 1 のディセーブル化

Catalyst 6500 シリーズ スイッチでは、制御プロトコルがネットワーク トポロジー全体でパケットを送受信できるように、VLAN 1 はデフォルトでイネーブルに設定されています。ただし、大規模で複雑なネットワークのトランク リンク上で VLAN 1 がイネーブルになっていると、ブロードキャスト ストームによる影響が大きくなります。スパニングツリーはネットワーク全体に適用されるので、すべてのトランク リンクで VLAN 1 がイネーブルになっていると、スパニングツリー ループが発生する可能性が大きくなります。このような状況を防ぐため、トランク インターフェイス上で VLAN 1 をディセーブルにすることができます。

トランク インターフェイス上で VLAN 1 をディセーブルにすると、そのトランク インターフェイスではユーザ トラフィックは送受信されなくなりますが、スーパバイザ エンジンが引き続き Cisco Discovery Protocol（CDP）、VTP、Port Aggregation Protocol（PAgP）、および DTP などの制御プロトコルからのパケットを送受信します。

VLAN 1 をディセーブルにしたトランク ポートが非トランク ポートになると、そのポートはネイティブ VLAN に追加されます。ネイティブ VLAN が VLAN 1 である場合は、ポートはイネーブルになり、VLAN 1 に追加されます。

トランク インターフェイス上で VLAN 1 をディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	トランク インターフェイス上で VLAN 1 をディセーブルにします。	**clear trunk** *mod/port* [*vlan-range*]
ステップ 2	トランクの許容 VLAN リストを確認します。	**show trunk** [*mod/port*]

次に、トランク リンク上で VLAN 1 をディセーブルにし、設定を確認する例を示します。

```
Console> (enable) clear trunk 8/1 1
Removing Vlan(s) 1 from allowed list.
Port  8/1 allowed vlans modified to 2-1005.
Console> (enable) show trunk 8/1
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 8/1      on           isl            trunking      1

Port      Vlans allowed on trunk
--------  --------------------------------------------------------------------
 8/1      2-1005, 1025-4094

Port      Vlans allowed and active in management domain
--------  --------------------------------------------------------------------
 8/1      2-6,10,20,50,100,152,200,300,400,500,521,524,570,776,801-802,850,917,9
99,1003,1005

Port      Vlans in spanning tree forwarding state and not pruned
--------  --------------------------------------------------------------------
 8/1      2-6,10,20,50,100,152,200,300,400,500,521,524,570,776,802,850,917,999,1
003,1005
Console> (enable) show config
```

ネイティブ VLAN トラフィックの 802.1Q タギングのイネーブル化

set dot1q-all-tagged enable コマンドは、スイッチがネイティブ VLAN（デフォルト VLAN）内のトラフィックも含めて 802.1Q トランクからのすべてのフレーム（802.1Q タグ付き）を転送し、802.1Q トランクには 802.1Q タグ付きフレームだけを流し、タグなしトラフィック（ネイティブ VLAN 内のタグなしトラフィックも含む）は廃棄するように設定するグローバル コマンドです。802.1Q トランクによる 802.1Q トンネリングのサポートが必要な任意のスイッチに、このコマンドを入力できます。

802.1Q トランク上ですべての 802.1Q タグ付きフレームを転送するようにスイッチを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチがすべての 802.1Q タグ付きフレームを転送できるようにします。	**set dot1q-all-tagged** [**enable** | **disable**]
ステップ 2	設定を確認します。	**show dot1q-all-tagged**

次に、すべての 802.1Q トラフィックをスイッチが転送できるようにし、その設定を確認する例を示します。

```
Console> (enable) set dot1q-all-tagged enable
Dot1q-all-tagged feature enabled globally.
Console> (enable) show dot1q-all-tagged
Dot1q-all-tagged feature globally enabled.
Console> (enable)
```

特定ポート上での 802.1Q タギングのディセーブル化

set port dot1q-all-tagged *mod/port* **enable** | **disable** コマンドを使用すると、特定ポート上での 802.1Q タギングをディセーブルにできます。802.1Q タグ付きトラフィックをサポートしないデバイスに接続するポート上での 802.1Q タギングを選択的にディセーブルにするには、**set port dot1q-all-tagged disable** コマンドを使用します。EtherChannel ポート上での 802.1Q タギングをイネーブルまたはディセーブルにすると、その設定はチャネル内のすべてのポートに適用されます。

（注） グローバル **set dot1q-all-tagged enable** コマンドを使用しなかった場合は、デフォルトのグループにはタグ付けされず、ポート単位の設定も無効です。

グローバル **set dot1q-all-tagged enable** コマンドを使用した場合は、ポート単位の設定によってフレームがタギングされるかどうかが制御されます。

（注） MSFC 上のポートや WS-X6101 OC-12 ATM（非同期転送モード）モジュール上のポートでは、**set port dot1q-all-tagged** *mod/port* **enable** | **disable** コマンドはサポートされていません。

特定ポート上での 802.1Q タグ付きフレームの転送をディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	特定ポート上またはすべてのポート上での 802.1Q タグ付きフレームの転送をイネーブルまたはディセーブルにします。	**set port dot1q-all-tagged** *mod/port* **enable** | **disable**
ステップ 2	設定を確認します。	**show port dot1q-all-tagged**

次に、ポート 3/2 上での 802.1Q タグ付きフレームの転送をディセーブルにし、その設定を確認する例を示します。

```
Console> (enable) set port dot1q-all-tagged 3/2 disable
Packets on native vlan will not be tagged on port  3/2.
Console> (enable) show port dot1q-all-tagged

Dot1q-all-tagged feature globally enabled.
Port    Dot1q-all-tagged mode
----    --------------------
 2/1    enable
 2/2    enable
 3/1    enable
 3/2    disable
 3/3    enable
 3/4    enable
 3/5    enable
（テキスト出力は省略）
```

カスタム 802.1Q Ethertype フィールドの指定

（注） カスタム 802.1Q Ethertype フィールドは、次のモジュール上でのみサポートされています。Supervisor Engine 2 のアップリンク ポート、Supervisor Engine 720 のアップリンク ポート、Supervisor Engine 32 のアップリンク ポート、WS-X6516-GBIC、WS-X6516A-GBIC、WS-X6516-GE-TX、WS-X6148-GE-TX、WS-X6148V-GE-TX、WS-X6548-GE-TX、WS-X6548V-GE-TX、WS-X6748-GE-TX、WS-X6724-SFP、WS-X6704-10GE、および WS-X6501-10GEX4 です。

（注） カスタム 802.1Q Ethertype フィールドは EtherChannel 上ではサポートされていません。カスタム 802.1Q Ethertype フィールドでポートを設定した場合、そのポートはチャネルに加入できません。チャネルがすでに設定されている場合、すべてのチャネル ポート上で 802.1Q Ethertype を変更できません。

（注） WS-X6516A-GBIC、WS-X6516-GBIC、および WS-X6548-GE-TX モジュール上で、ポート グループ 1 ～ 8 または 9 ～ 16 内のうち 1 つのポートをカスタム 802.1Q Ethertype で設定すると、グループ内のすべてのポートがそのカスタム 802.1Q Ethertype で設定されます。WS-X6516-GE-TX モジュール上で、ポート グループ 1 ～ 4、5 ～ 8、9 ～ 12、または 13 ～ 16 内のうち 1 つのポートをカスタム 802.1Q Ethertype で設定すると、グループ内のすべてのポートがそのカスタム 802.1Q Ethertype で設定されます。

（注） カスタム 802.1Q Ethertype フィールドは、トランク ポート、802.1Q アクセス ポート、および 802.1Q/802.1p マルチ VLAN アクセス ポート上で使用することができます。その場合、カスタム Ethertype 値をリンクの両端と同一に設定する必要があります。

カスタム Ethertype フィールドを指定することで、標準の 0x8100 Ethertype を使用しないシスコ製および他社製のスイッチをネットワークにサポートさせ、802.1Q タグ付きフレームを識別させることができます。カスタム Ethertype フィールドを指定した場合、802.1Q タグ付きフレームを識別し、特定の VLAN にフレームを切り替えることができます。Ethertype の直後に続く 2 バイトが、標準の 802.1Q タグとして解釈されます。Ethertype フィールドの 2 バイトの値は 16 進数で指定します。**デフォルト**値は 8100 です。

802.1Q タグでカスタム 802.1Q Ethertype 値を指定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポートにカスタム Ethertype フィールドを指定します。	**set port dot1q-ethertype** *mod/port* {*value* | **default**}
ステップ 2	設定を確認します。	**show port dot1q-ethertype** [*mod* | *mod/port*]

次に、ポート 2/1 上で 802.1Q Ethertype に 0x1234 を設定し、その設定を確認する例を示します。

```
Console> (enable) set port dot1q-ethertype 2/1 1234
All the group ports 2/1-2 associated with port 2/1 will be modified.
Do you want to continue (y/n) [n]?y
Dot1q Ethertype value set to 0x1234 on ports 2/1-2.
Console> (enable)

Console> (enable) show port dot1q-ethertype 2/1
Port    Dot1q ethertype value
----    ---------------------
 2/1    1234
Console> (enable)
```

カスタム 802.1Q Ethertype フィールドから標準の Ethertype への復帰

カスタム 802.1Q Ethertype フィールドから標準の Ehtertype フィールド（0x8100）に戻すのに必要なのは、**set port dot1q-ethertype** *mod/port* {*value* | **default**} コマンドだけです。

カスタム Ethertype フィールドからデフォルト値（0x8100）に戻すには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポートの Ethertype フィールドを標準の値（0x8100）に戻します。	**set port dot1q-ethertype** *mod/port* **default**
ステップ 2	設定を確認します。	**show port dot1q-ethertype** [*mod* | *mod/port*]

次に、ポート 2/1 上で 802.1Q Ethertype フィールドを標準の Ethertype フィールド（0x8100）に戻し、その設定を確認する例を示します。

```
Console> (enable) set port dot1q-ethertype 2/1 default
All the group ports 2/1-2 associated with port 2/1 will be modified.
Do you want to continue (y/n) [n]?y
Dot1q Ethertype value set to 0x8100 on ports 2/1-2.
Console> (enable)

Console> (enable) show port dot1q-ethertype 2/1
Port    Dot1q ethertype value
----    ---------------------
 2/1    8100
Console> (enable)
```

VLAN トランクの設定例

ここでは、VLAN トランクの設定例を紹介します。

ISL トランクの設定例

ここでは、2 台のスイッチ間に ISL トランクを設定し、トランクの許容 VLAN を VLAN 1 および VLAN 520 ～ 530 に制限する設定例を示します。

この例では、スイッチ 1 上のポート 1/1 は、ほかのスイッチ上のファスト イーサネット ポートに接続しています。どちらのポートもデフォルトの状態で、トランク モードは **auto** です（詳細については、「トランクのデフォルト設定」[p.5-6] を参照）。

2 台のスイッチ間に ISL トランクを設定し、トランクの許容 VLAN を VLAN 1 および VLAN 520 ～ 530 に制限する手順は、次のとおりです。

ステップ 1　**set trunk** コマンドを入力して、スイッチ 1 上のポート 1/1 を ISL トランク ポートとして設定します。近接ポート（スイッチ 2 上のポート 1/2）との自動ネゴシエーションが行われるように、**desirable** キーワードを指定します。ここでは、ISL がハードウェア タイプに基づいてカプセル化されていることを前提としています。

```
Switch1> (enable) set trunk 1/1 desirable
Port(s) 1/1 trunk mode set to desirable.
Switch1> (enable) 06/18/1998,12:20:23:DTP-5:Port 1/1 has become isl trunk
06/18/1998,12:20:23:PAGP-5:Port 1/1 left bridge port 1/1.
06/18/1998,12:20:23:PAGP-5:Port 1/1 joined bridge port 1/1.
Switch1> (enable)
```

ステップ 2　**show trunk** コマンドを入力して、設定を確認します。画面出力の Status フィールドで、ポート 1/1 が trunking になっています。

```
Switch1> (enable) show trunk 1/1
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 1/1      desirable    isl            trunking      1
Port      Vlans allowed on trunk
--------  ---------------------------------------------------------------------
 1/1      1-1005, 1025-4094
Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------------------
 1/1      1,521-524
Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------------------
 1/1
Switch1> (enable)
```

ステップ 3　トランクの許容 VLAN リストを定義するために、**clear trunk** コマンドを使用して、このトランク リンク上でトラフィックを伝送しない VLAN を削除します。

```
Switch1> (enable) clear trunk 1/1 2-519
Removing Vlan(s) 2-519 from allowed list.
Port 1/1 allowed vlans modified to 1,520-1005.
Switch1> (enable) clear trunk 1/1 531-1005
Removing Vlan(s) 531-1005 from allowed list.
Port 1/1 allowed vlans modified to 1,520-530.
Switch1> (enable) show trunk 1/1
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 1/1      desirable    isl            trunking      1
Port      Vlans allowed on trunk
--------  --------------------------------------------------------------------
 1/1      1,520-530
Port      Vlans allowed and active in management domain
--------  --------------------------------------------------------------------
 1/1      1,521-524
Port      Vlans in spanning tree forwarding state and not pruned
--------  --------------------------------------------------------------------
 1/1      1,521-524
Switch1> (enable)
```

ステップ 4　**ping** コマンドを入力して、トランクの接続を確認します。

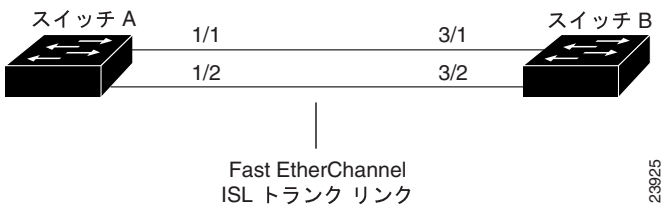
```
Switch1> (enable) ping switch2
switch2 is alive
Switch1> (enable)
```

EtherChannel リンクによる ISL トランクの例

次に、2 台のスイッチ間に EtherChannel リンクによる、ISL トランクを設定する例を示します。

図 5-1 に、2 つの 100BASE-TX ファスト イーサネット ポートで接続されている 2 台のスイッチを示します。

図 5-1　Fast EtherChannel リンクによる ISL トランク



2 ポートの EtherChannel バンドルを形成するためにスイッチを設定し、ISL トランク リンクとして EtherChannel バンドルを設定する手順は、次のとおりです。

ステップ 1　**show port channel** および **show trunk** コマンドを入力して、スイッチのチャネル ステータスおよびトランク ステータスを確認します。

```
Switch_A> (enable) show port channel
No ports channelling
Switch_A> (enable) show trunk
No ports trunking.
Switch_A> (enable)

Switch_B> (enable) show port channel
No ports channelling
Switch_B> (enable) show trunk
No ports trunking.
Switch_B> (enable)
```

ステップ 2　**set port channel** コマンドを入力して、近接スイッチと EtherChannel バンドルをネゴシエーションするように、スイッチ A のポートを設定します。次の例では、スイッチ B の近接ポートは EtherChannel **auto** モードであると想定しています。EtherChannel バンドルの編成については、システム ログ メッセージで確認できます。

```
Switch_A> (enable) set port channel 1/1-2 desirable
Port(s) 1/1-2 channel mode set to desirable.
Switch_A> (enable) %PAGP-5-PORTFROMSTP:Port 1/1 left bridge port 1/1
%PAGP-5-PORTFROMSTP:Port 1/2 left bridge port 1/2
%PAGP-5-PORTFROMSTP:Port 1/2 left bridge port 1/2
%PAGP-5-PORTTOSTP:Port 1/1 joined bridge port 1/1-2
%PAGP-5-PORTTOSTP:Port 1/2 joined bridge port 1/1-2

Switch_B> (enable) %PAGP-5-PORTFROMSTP:Port 3/1 left bridge port 3/1
%PAGP-5-PORTFROMSTP:Port 3/2 left bridge port 3/2
%PAGP-5-PORTFROMSTP:Port 3/2 left bridge port 3/2
%PAGP-5-PORTTOSTP:Port 3/1 joined bridge port 3/1-2
%PAGP-5-PORTTOSTP:Port 3/2 joined bridge port 3/1-2
```

ステップ 3　EtherChannel バンドルのネゴシエーションのあと、**show port channel** コマンドを入力して、設定を確認します。

```
Switch_A> (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 1/1  connected  desirable channel     WS-C5000    009979082(Sw  3/1
 1/2  connected  desirable channel     WS-C5000    009979082(Sw  3/2
----- ---------- --------- ----------- ------------------------- ----------
Switch_A> (enable)

Switch_B> (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 3/1  connected  auto      channel     WS-C5500    069003103(Sw  1/1
 3/2  connected  auto      channel     WS-C5500    069003103(Sw  1/2
----- ---------- --------- ----------- ------------------------- ----------
Switch_B> (enable)
```

ステップ 4　**set trunk** コマンドを入力して、ISL トランクのネゴシエーションを行うように EtherChannel バンドル内のポートの 1 つを設定します。

設定は、そのバンドル内のすべてのポートに適用されます。次の例では、スイッチ B の近接ポートは **isl** または **negotiate** カプセル化を使用するように設定され、**auto** トランク モードになっていると想定しています。ISL トランクの編成は、システム ログ メッセージで確認できます。

```
Switch_A> (enable) set trunk 1/1 desirable isl
Port(s) 1/1-2 trunk mode set to desirable.
Port(s) 1/1-2 trunk type set to isl.
Switch_A> (enable) %DTP-5-TRUNKPORTON:Port 1/1 has become isl trunk
%DTP-5-TRUNKPORTON:Port 1/2 has become isl trunk
%PAGP-5-PORTFROMSTP:Port 1/1 left bridge port 1/1-2
%PAGP-5-PORTFROMSTP:Port 1/2 left bridge port 1/1-2
%PAGP-5-PORTTOSTP:Port 1/1 joined bridge port 1/1-2
%PAGP-5-PORTTOSTP:Port 1/2 joined bridge port 1/1-2

Switch_B> (enable) %DTP-5-TRUNKPORTON:Port 3/1 has become isl trunk
%DTP-5-TRUNKPORTON:Port 3/2 has become isl trunk
%PAGP-5-PORTFROMSTP:Port 3/1 left bridge port 3/1-2
%PAGP-5-PORTFROMSTP:Port 3/2 left bridge port 3/1-2
%PAGP-5-PORTTOSTP:Port 3/1 joined bridge port 3/1-2
%PAGP-5-PORTTOSTP:Port 3/2 joined bridge port 3/1-2
```

ステップ 5　ISL トランク リンクのネゴシエーションのあと、**show trunk** コマンドを使用して、設定を確認します。

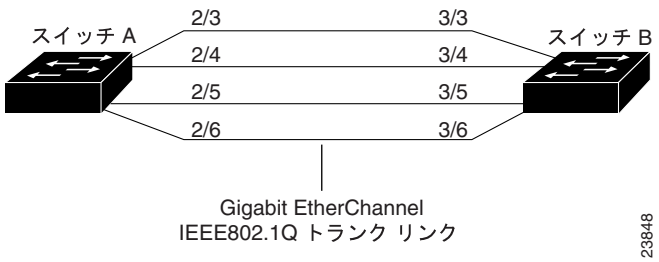
```
Switch_A> (enable) show trunk
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 1/1      desirable    isl            trunking      1
 1/2      desirable    isl            trunking      1

Port      Vlans allowed on trunk
--------  ---------------------------------------------------------------------
 1/1      1-1005, 1025-4094
 1/2      1-1005, 1025-4094

Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------------------
 1/1      1-5,10,20,50,152,200,300,400,500,521-524,570,850,917,999
 1/2      1-5,10,20,50,152,200,300,400,500,521-524,570,850,917,999

Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------------------
 1/1      1-5,10,20,50,152,200,300,400,500,521-524,570,850,917,999
 1/2      1-5,10,20,50,152,200,300,400,500,521-524,570,850,917,999
Switch_A> (enable)

Switch_B> (enable) show trunk
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 3/1      auto         isl            trunking      1
 3/2      auto         isl            trunking      1

Port      Vlans allowed on trunk
--------  ---------------------------------------------------------------------
 3/1      1-1005, 1025-4094
 3/2      1-1005, 1025-4094

Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------------------
 3/1      1-5,10,20,50,152,200,300,400,500,521-524,570,850,917,999
 3/2      1-5,10,20,50,152,200,300,400,500,521-524,570,850,917,999
Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------------------
 3/1      1-5,10,20,50,152,200,300,400,500,521-524,570,801,850,917,999
 3/2      1-5,10,20,50,152,200,300,400,500,521-524,570,801,850,917,999
Switch_B> (enable)
```

EtherChannel リンクによる 802.1Q トランクの例

次に、2 台のスイッチ間に EtherChannel リンクによる 802.1Q トランクを設定する例を示します。

図 5-2 に、4 つの 1000BASE-SX ギガビット イーサネット ポートで接続されている 2 台のスイッチを示します。

図 5-2　EtherChannel リンクによる 802.1Q トランク



4 ポートの EtherChannel バンドルを形成するためにスイッチを設定し、802.1Q トランク リンクとして EtherChannel バンドルを設定する手順は、次のとおりです。

ステップ 1　**set vlan** コマンドを入力して、スイッチ A とスイッチ B の両方のすべてのポートが同じ VLAN に割り当てられていることを確認します。この VLAN は、トランクの 802.1Q ネイティブ VLAN として使用されます。次の例では、すべてのポートが VLAN 1 のメンバーとして設定されます。

```
Switch_A> (enable) set vlan 1 2/3-6
VLAN  Mod/Ports
---- ------------------------
1     2/1-6

Switch_A> (enable)

Switch_B> (enable) set vlan 1 3/3-6
VLAN  Mod/Ports
---- ------------------------
1     3/1-6

Switch_B> (enable)
```

ステップ 2　**show port channel** および **show trunk** コマンドを入力して、スイッチのチャネル ステータスおよびトランク ステータスを確認します。

```
Switch_A> (enable) show port channel
No ports channelling
Switch_A> (enable) show trunk
No ports trunking.
Switch_A> (enable)

Switch_B> (enable) show port channel
No ports channelling
Switch_B> (enable) show trunk
No ports trunking.
Switch_B> (enable)
```

ステップ 3　**set port channel** コマンドを入力して、近接スイッチと EtherChannel バンドルをネゴシエーションするように、スイッチ A のポートを設定します。次の例では、スイッチ B の近接ポートは EtherChannel **auto** モードであると想定しています。EtherChannel バンドルの編成については、システム ログ メッセージで確認できます。

```
Switch_A> (enable) set port channel 2/3-6 desirable
Port(s) 2/3-6 channel mode set to desirable.
Switch_A> (enable) %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
%PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
%PAGP-5-PORTFROMSTP:Port 2/5 left bridge port 2/5
%PAGP-5-PORTFROMSTP:Port 2/6 left bridge port 2/6
%PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
%PAGP-5-PORTFROMSTP:Port 2/5 left bridge port 2/5
%PAGP-5-PORTFROMSTP:Port 2/6 left bridge port 2/6
%PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
%PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/3-6
%PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/3-6
%PAGP-5-PORTTOSTP:Port 2/5 joined bridge port 2/3-6
%PAGP-5-PORTTOSTP:Port 2/6 joined bridge port 2/3-6

Switch_B> (enable) %PAGP-5-PORTFROMSTP:Port 3/3 left bridge port 3/3
%PAGP-5-PORTFROMSTP:Port 3/4 left bridge port 3/4
%PAGP-5-PORTFROMSTP:Port 3/5 left bridge port 3/5
%PAGP-5-PORTFROMSTP:Port 3/6 left bridge port 3/6
%PAGP-5-PORTFROMSTP:Port 3/4 left bridge port 3/4
%PAGP-5-PORTFROMSTP:Port 3/5 left bridge port 3/5
%PAGP-5-PORTFROMSTP:Port 3/6 left bridge port 3/6
%PAGP-5-PORTFROMSTP:Port 3/3 left bridge port 3/3
%PAGP-5-PORTTOSTP:Port 3/3 joined bridge port 3/3-6
%PAGP-5-PORTTOSTP:Port 3/4 joined bridge port 3/3-6
%PAGP-5-PORTTOSTP:Port 3/5 joined bridge port 3/3-6
%PAGP-5-PORTTOSTP:Port 3/6 joined bridge port 3/3-6
```

ステップ 4　EtherChannel バンドルのネゴシエーションのあと、**show port channel** コマンドを入力して、設定を確認します。

```
Switch_A> (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/3  connected  desirable channel     WS-C4003    JAB023806(Sw  2/3
 2/4  connected  desirable channel     WS-C4003    JAB023806(Sw  2/4
 2/5  connected  desirable channel     WS-C4003    JAB023806(Sw  2/5
 2/6  connected  desirable channel     WS-C4003    JAB023806(Sw  2/6
----- ---------- --------- ----------- ------------------------- ----------
Switch_A> (enable)

Switch_B> (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 3/3  connected  auto      channel     WS-C4003    JAB023806(Sw  2/3
 3/4  connected  auto      channel     WS-C4003    JAB023806(Sw  2/4
 3/5  connected  auto      channel     WS-C4003    JAB023806(Sw  2/5
 3/6  connected  auto      channel     WS-C4003    JAB023806(Sw  2/6
----- ---------- --------- ----------- ------------------------- ----------
Switch_B> (enable)
```

ステップ 5　**set trunk** コマンドを入力して、802.1Q トランクのネゴシエーションを行うように EtherChannel バンドル内のポートの 1 つを設定します。設定は、そのバンドル内のすべてのポートに適用されます。次の例では、スイッチ B の近接ポートは **dot1q** または **negotiate** カプセル化を使用するように設定され、**auto** トランク モードであると想定しています。802.1Q トランクの編成については、システム ログ メッセージで確認できます。

```
Switch_A> (enable) set trunk 2/3 desirable dot1q
Port(s) 2/3-6 trunk mode set to desirable.
Port(s) 2/3-6 trunk type set to dot1q.
Switch_A> (enable) %DTP-5-TRUNKPORTON:Port 2/3 has become dot1q trunk
%DTP-5-TRUNKPORTON:Port 2/4 has become dot1q trunk
%PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3-6
%DTP-5-TRUNKPORTON:Port 2/5 has become dot1q trunk
%PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/3-6
%PAGP-5-PORTFROMSTP:Port 2/5 left bridge port 2/3-6
%DTP-5-TRUNKPORTON:Port 2/6 has become dot1q trunk
%PAGP-5-PORTFROMSTP:Port 2/6 left bridge port 2/3-6
%PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
%PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/3-6
%PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/3-6
%PAGP-5-PORTTOSTP:Port 2/5 joined bridge port 2/3-6
%PAGP-5-PORTTOSTP:Port 2/6 joined bridge port 2/3-6
Switch_B> (enable) %DTP-5-TRUNKPORTON:Port 3/3 has become dot1q trunk
%DTP-5-TRUNKPORTON:Port 3/4 has become dot1q trunk
%PAGP-5-PORTFROMSTP:Port 3/3 left bridge port 3/3-6
%PAGP-5-PORTFROMSTP:Port 3/4 left bridge port 3/3-6
%PAGP-5-PORTFROMSTP:Port 3/5 left bridge port 3/3-6
%PAGP-5-PORTFROMSTP:Port 3/6 left bridge port 3/3-6
%DTP-5-TRUNKPORTON:Port 3/5 has become dot1q trunk
%DTP-5-TRUNKPORTON:Port 3/6 has become dot1q trunk
%PAGP-5-PORTFROMSTP:Port 3/5 left bridge port 3/3-6
%PAGP-5-PORTFROMSTP:Port 3/6 left bridge port 3/3-6
%PAGP-5-PORTTOSTP:Port 3/3 joined bridge port 3/3-6
%PAGP-5-PORTTOSTP:Port 3/4 joined bridge port 3/3-6
%PAGP-5-PORTTOSTP:Port 3/5 joined bridge port 3/3-6
%PAGP-5-PORTTOSTP:Port 3/6 joined bridge port 3/3-6
```

ステップ 6　802.1Q トランク リンクのネゴシエーションのあと、**show trunk** コマンドを入力して、設定を確認します。

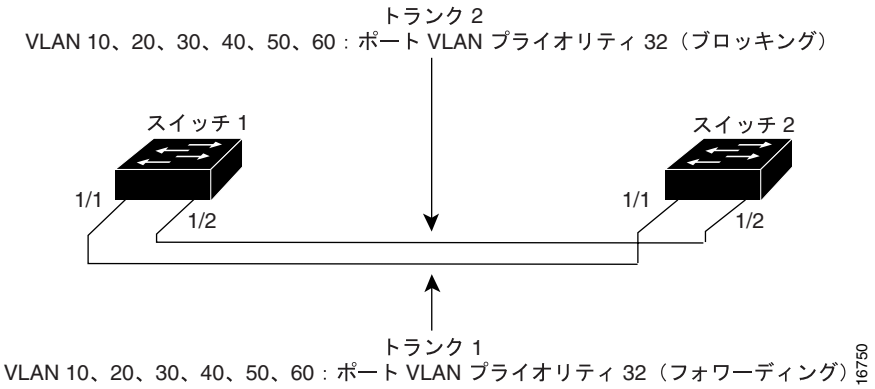
```
Switch_A> (enable) show trunk
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 2/3      desirable    dot1q          trunking      1
 2/4      desirable    dot1q          trunking      1
 2/5      desirable    dot1q          trunking      1
 2/6      desirable    dot1q          trunking      1

Port      Vlans allowed on trunk
--------  ---------------------------------------------------------------------
 2/3      1-1005, 1025-4094
 2/4      1-1005, 1025-4094
 2/5      1-1005, 1025-4094
 2/6      1-1005, 1025-4094

Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------------------
 2/3      1-5,10,20,50,152,200,300,400,500,521-524,570,850,917,999
 2/4      1-5,10,20,50,152,200,300,400,500,521-524,570,850,917,999
 2/5      1-5,10,20,50,152,200,300,400,500,521-524,570,850,917,999
 2/6      1-5,10,20,50,152,200,300,400,500,521-524,570,850,917,999

Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------------------
 2/3
 2/4
 2/5
 2/6
Switch_A> (enable)

Switch_B> (enable) show trunk
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 3/3      auto         dot1q          trunking      1
 3/4      auto         dot1q          trunking      1
 3/5      auto         dot1q          trunking      1
 3/6      auto         dot1q          trunking      1

Port      Vlans allowed on trunk
--------  ---------------------------------------------------------------------
 3/3      1-1005, 1025-4094
 3/4      1-1005, 1025-4094
 3/5      1-1005, 1025-4094
 3/6      1-1005, 1025-4094

Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------------------
 3/3      1-5,10,20,50,152,200,300,400,500,521-524,570,850,917,999
 3/4      1-5,10,20,50,152,200,300,400,500,521-524,570,850,917,999
 3/5      1-5,10,20,50,152,200,300,400,500,521-524,570,850,917,999
 3/6      1-5,10,20,50,152,200,300,400,500,521-524,570,850,917,999

Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------------------
 3/3      1-5,10,20,50,152,200,300,400,500,521-524,570,850,917,999
 3/4      1-5,10,20,50,152,200,300,400,500,521-524,570,850,917,999
 3/5      1-5,10,20,50,152,200,300,400,500,521-524,570,850,917,999
 3/6      1-5,10,20,50,152,200,300,400,500,521-524,570,850,917,999
Switch_B> (enable)
```

並列トランクによる VLAN トラフィック負荷分散の例

スパニングツリーのポート VLAN プライオリティを使用して、並列トランク ポート間で VLAN トラフィックの負荷分散を実行し、一部の VLAN のトラフィックはあるトランクへ、別の VLAN のトラフィックは別のトランクへ伝送することができます。この設定では、（一方のトランクをブロッキング モードにすることなく）トラフィックを両方のトランクで同時に転送できるので、フォールトトレラントな設定を維持しながら、個々のトランク上の総トラフィックを少なくすることができます。

図 5-3 に、スーパバイザ エンジン上のファスト イーサネット アップリンク ポートを使用した、2 台のスイッチ間の並列トランクの設定を示します。

図 5-3　VLAN トラフィック負荷分散設定前の並列トランク設定



デフォルトの設定では、両方のトランクのポート VLAN プライオリティは同じです（値は 32）。STP は転送ループを阻止するために、スイッチ 1 の各 VLAN について、ポート 1/2（トランク 2）をブロックします。トランク 2 は、トランク 1 で障害が発生するまでは、トラフィックの転送に使用されません。

複数の VLAN から発生したトラフィックの負荷が並列トランク上で分散されるようにスイッチを設定するには、次の手順を実行します。

ステップ 1　**set vtp** コマンドを入力して、スイッチ 1 およびスイッチ 2 の両方で VTP ドメインを設定し、スイッチ 1 で設定した VLAN 情報をスイッチ 2 が学習するようにします。スイッチ 1 が、VTP サーバであることを確認してください。スイッチ 2 は、VTP クライアントまたは VTP サーバとして設定できます。

```
Switch_1> (enable) set vtp domain BigCorp mode server
VTP domain BigCorp modified
Switch_1> (enable)

Switch_2> (enable) set vtp domain BigCorp mode server
VTP domain BigCorp modified
Switch_2> (enable)
```

ステップ 2　**set vlan** コマンドを入力して、スイッチ 1 上に VLAN を作成します。この例では、VLAN 10、20、30、40、50、および 60 を設定します。

```
Switch_1> (enable) set vlan 10
Vlan 10 configuration successful
Switch_1> (enable) set vlan 20
Vlan 20 configuration successful
Switch_1> (enable) set vlan 30
Vlan 30 configuration successful
Switch_1> (enable) set vlan 40
Vlan 40 configuration successful
Switch_1> (enable) set vlan 50
Vlan 50 configuration successful
Switch_1> (enable) set vlan 60
Vlan 60 configuration successful
Switch_1> (enable)
```

ステップ 3　**show vtp domain** および **show vlan** コマンドを入力して、スイッチ 1 上の VTP および VLAN 設定を確認します。

```
Switch_1> (enable) show vtp domain
Domain Name                    Domain Index VTP Version Local Mode  Password
------------------------------ ------------ ----------- ----------- ----------
BigCorp                        1            2           server      -

Vlan-count Max-vlan-storage Config Revision Notifications
---------- ---------------- --------------- -------------
11         1023             13              disabled

Last Updater    V2 Mode  Pruning  PruneEligible on Vlans
--------------- -------- -------- -------------------------
172.20.52.10    disabled enabled  2-1000
Switch_1> (enable) show vlan
VLAN Name                             Status    Mod/Ports, Vlans
---- -------------------------------- --------- ----------------------------
1    default                          active    1/1-2
                                                2/1-12
                                                5/1-2
10   VLAN0010                         active
20   VLAN0020                         active
30   VLAN0030                         active
40   VLAN0040                         active
50   VLAN0050                         active
60   VLAN0060                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
.
.
.

Switch_1> (enable)
```

ステップ 4　**set trunk** コマンドを入力して、スイッチ 1 上に ISL トランク ポートとしてスーパバイザ エンジン アップリンクを設定します。スイッチ 1 ポート上に **desirable** モードを指定し、スイッチ 2 上のポートがネゴシエーションによってトランク リンクになるようにします（スイッチ 2 のアップリンクは、デフォルトの **auto** モードです）。

```
Switch_1> (enable) set trunk 1/1 desirable
Port(s) 1/1 trunk mode set to desirable.
Switch_1> (enable) 04/21/1998,03:05:05:DISL-5:Port 1/1 has become isl trunk

Switch_1> (enable) set trunk 1/2 desirable
Port(s) 1/2 trunk mode set to desirable.
Switch_1> (enable) 04/21/1998,03:05:13:DISL-5:Port 1/2 has become isl trunk
```

ステップ 5　**show trunk** コマンドを入力して、トランク リンクがアップになっていることを確認します。

```
Switch_1> (enable) show trunk 1
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 1/1      desirable    isl            trunking      1
 1/2      desirable    isl            trunking      1

Port      Vlans allowed on trunk
--------  ---------------------------------------------------------------------
 1/1      1-1005, 1025-4094
 1/2      1-1005, 1025-4094

Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------------------
 1/1      1,10,20,30,40,50,60
 1/2      1,10,20,30,40,50,60

Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------------------
 1/1
 1/2
Switch_1> (enable)
```

ステップ 6　トランク リンクがアップになると、VTP により、スイッチ 2 上に VTP および VLAN 設定が伝達されることに注意してください。スイッチ 2 で **show vlan** コマンドを入力し、スイッチ 2 が VLAN 設定を学習していることを確認します。

```
Switch_2> (enable) show vlan
VLAN Name                             Status    Mod/Ports, Vlans
---- -------------------------------- --------- ----------------------------
1    default                          active
10   VLAN0010                         active
20   VLAN0020                         active
30   VLAN0030                         active
40   VLAN0040                         active
50   VLAN0050                         active
60   VLAN0060                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
.
.
.
Switch_2> (enable)
```

ステップ 7　スパニングツリーのコンバージェンス処理には 1 ～ 2 分かかります。ネットワークが安定したら、**show spantree** コマンドを入力して、スイッチ 1 上の各トランク ポートのスパニングツリー ステートを確認します。

トランク 1 はすべての VLAN でフォワーディング ステートです。トランク 2 はすべての VLAN でブロッキング ステートです。スイッチ 2 では、両方のトランクがすべての VLAN でフォワーディング ステートですが、スイッチ 1 上のポート 1/2 がブロッキング ステートのため、トラフィックはトランク 2 を通過しません。

```
Switch_1> (enable) show spantree 1/1
Port      Vlan  Port-State     Cost   Priority  Fast-Start  Group-method
--------- ----  -------------  -----  --------  ----------  ------------
 1/1      1     forwarding        19        32   disabled
 1/1      10    forwarding        19        32   disabled
 1/1      20    forwarding        19        32   disabled
 1/1      30    forwarding        19        32   disabled
 1/1      40    forwarding        19        32   disabled
 1/1      50    forwarding        19        32   disabled
 1/1      60    forwarding        19        32   disabled
 1/1      1003  not-connected     19        32   disabled
 1/1      1005  not-connected     19         4   disabled
Switch_1> (enable) show spantree 1/2
Port      Vlan  Port-State     Cost   Priority  Fast-Start  Group-method
--------- ----  -------------  -----  --------  ----------  ------------
 1/2      1     blocking          19        32   disabled
 1/2      10    blocking          19        32   disabled
 1/2      20    blocking          19        32   disabled
 1/2      30    blocking          19        32   disabled
 1/2      40    blocking          19        32   disabled
 1/2      50    blocking          19        32   disabled
 1/2      60    blocking          19        32   disabled
 1/2      1003  not-connected     19        32   disabled
 1/2      1005  not-connected     19         4   disabled
Switch_1> (enable)
```

ステップ 8　設定した VLAN を 2 つのグループに分けます。1 つのトランク リンクで VLAN の半数のトラフィックを伝送し、残りの半分をもう 1 つのトランク リンクで伝送することができます。また、特定の VLAN のトラフィックが多い場合は、その VLAN のトラフィックを 1 つのトランク リンクに転送し、残りの VLAN のトラフィックをもう 1 つのトランク リンクに転送することもできます。

（注）　次の手順では、VLAN 10、20、および 30（グループ 1）のトラフィックをトランク 1 に転送し、VLAN 40、50、および 60（グループ 2）をトランク 2 に転送します。

ステップ 9　スイッチ 1 上で、**set spantree portvlanpri** コマンドを入力し、トランク 1（ポート 1/1）上のグループ 1 の VLAN について、ポート VLAN プライオリティをデフォルトの 32 より小さい整数値に変更します。

```
Switch_1> (enable) set spantree portvlanpri 1/1 1 10
Port 1/1 vlans 1-9,11-1004 using portpri 32.
Port 1/1 vlans 10 using portpri 1.
Port 1/1 vlans 1005 using portpri 4.
Switch_1> (enable) set spantree portvlanpri 1/1 1 20
Port 1/1 vlans 1-9,11-19,21-1004 using portpri 32.
Port 1/1 vlans 10,20 using portpri 1.
Port 1/1 vlans 1005 using portpri 4.
Switch_1> (enable) set spantree portvlanpri 1/1 1 30
Port 1/1 vlans 1-9,11-19,21-29,31-1004 using portpri 32.
Port 1/1 vlans 10,20,30 using portpri 1.
Port 1/1 vlans 1005 using portpri 4.
Switch_1> (enable)
```

ステップ 10 スイッチ 1 上で、**set spantree portvlanpri** コマンドを入力し、トランク 2（ポート 1/2）上のグループ 2 の VLAN について、ポート VLAN プライオリティをデフォルトの 32 より小さい整数値に変更します。

```
Switch_1> (enable) set spantree portvlanpri 1/2 1 40
Port 1/2 vlans 1-39,41-1004 using portpri 32.
Port 1/2 vlans 40 using portpri 1.
Port 1/2 vlans 1005 using portpri 4.
Switch_1> (enable) set spantree portvlanpri 1/2 1 50
Port 1/2 vlans 1-39,41-49,51-1004 using portpri 32.
Port 1/2 vlans 40,50 using portpri 1.
Port 1/2 vlans 1005 using portpri 4.
Switch_1> (enable) set spantree portvlanpri 1/2 1 60
Port 1/2 vlans 1-39,41-49,51-59,61-1004 using portpri 32.
Port 1/2 vlans 40,50,60 using portpri 1.
Port 1/2 vlans 1005 using portpri 4.
Switch_1> (enable)
```

ステップ 11 スイッチ 2 上で、**set spantree portvlanpri** コマンドを入力し、トランク 1（ポート 1/1）上のグループ 1 の VLAN について、ポート VLAN プライオリティをスイッチ 1 の VLAN に設定した値と同じ値に変更します。

注意　リンクの両端で、各 VLAN のポート VLAN プライオリティを同じ値に設定する必要があります。

```
Switch_2> (enable) set spantree portvlanpri 1/1 1 10
Port 1/1 vlans 1-9,11-1004 using portpri 32.
Port 1/1 vlans 10 using portpri 1.
Port 1/1 vlans 1005 using portpri 4.
Switch_2> (enable) set spantree portvlanpri 1/1 1 20
Port 1/1 vlans 1-9,11-19,21-1004 using portpri 32.
Port 1/1 vlans 10,20 using portpri 1.
Port 1/1 vlans 1005 using portpri 4.
Switch_2> (enable) set spantree portvlanpri 1/1 1 30
Port 1/1 vlans 1-9,11-19,21-29,31-1004 using portpri 32.
Port 1/1 vlans 10,20,30 using portpri 1.
Port 1/1 vlans 1005 using portpri 4.
Switch_2> (enable)
```

ステップ 12 スイッチ 2 上で、**set spantree portvlanpri** コマンドを入力し、トランク 2（ポート 1/2）上のグループ 2 の VLAN について、ポート VLAN プライオリティをスイッチ 1 の VLAN に設定した値と同じ値に変更します。

```
Switch_2> (enable) set spantree portvlanpri 1/2 1 40
Port 1/2 vlans 1-39,41-1004 using portpri 32.
Port 1/2 vlans 40 using portpri 1.
Port 1/2 vlans 1005 using portpri 4.
Switch_2> (enable) set spantree portvlanpri 1/2 1 50
Port 1/2 vlans 1-39,41-49,51-1004 using portpri 32.
Port 1/2 vlans 40,50 using portpri 1.
Port 1/2 vlans 1005 using portpri 4.
Switch_2> (enable) set spantree portvlanpri 1/2 1 60
Port 1/2 vlans 1-39,41-49,51-59,61-1004 using portpri 32.
Port 1/2 vlans 40,50,60 using portpri 1.
Port 1/2 vlans 1005 using portpri 4.
Switch_2> (enable)
```

（注） リンクの両端でポート VLAN プライオリティを設定すると、スパニングツリーのコンバージェンス後に新しい設定が使用されます。

ステップ 13 **show spantree** コマンドを入力して、スイッチ 1 上のスパニングツリー ポートのステートを確認します。グループ 1 の VLAN は、トランク 1 上ではフォワーディング、トランク 2 上ではブロッキングになります。グループ 2 の VLAN は、トランク 1 上ではブロッキング、トランク 2 上ではフォワーディングになります。

```
Switch_1> (enable) show spantree 1/1
Port      Vlan  Port-State     Cost   Priority  Fast-Start  Group-method
--------- ----  -------------  -----  --------  ----------  ------------
 1/1      1     forwarding        19        32   disabled
 1/1      10    forwarding        19         1   disabled
 1/1      20    forwarding        19         1   disabled
 1/1      30    forwarding        19         1   disabled
 1/1      40    blocking          19        32   disabled
 1/1      50    blocking          19        32   disabled
 1/1      60    blocking          19        32   disabled
 1/1      1003  not-connected     19        32   disabled
 1/1      1005  not-connected     19         4   disabled
Switch_1> (enable) show spantree 1/2
Port      Vlan  Port-State     Cost   Priority  Fast-Start  Group-method
--------- ----  -------------  -----  --------  ----------  ------------
 1/2      1     blocking          19        32   disabled
 1/2      10    blocking          19        32   disabled
 1/2      20    blocking          19        32   disabled
 1/2      30    blocking          19        32   disabled
 1/2      40    forwarding        19         1   disabled
 1/2      50    forwarding        19         1   disabled
 1/2      60    forwarding        19         1   disabled
 1/2      1003  not-connected     19        32   disabled
 1/2      1005  not-connected     19         4   disabled
Switch_1> (enable)
```

図 5-4 に、VLAN トラフィックの負荷分散を設定したあとのネットワークを示します。

図 5-4　VLAN トラフィック負荷分散設定後の並列トランク設定

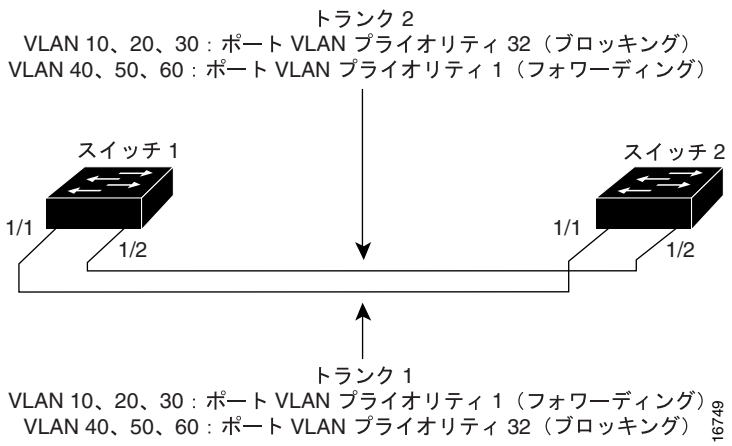


図 5-4 の設定では、ネットワークの正常稼働時には、両方のトランクが使用されます。また、一方のトランク リンクで障害が発生すると、他方のトランク リンクが代替転送パスとなり、障害リンクで送られていたトラフィックを引き受けます。

図 5-4 のトランク 1 でネットワーク障害が発生すると、次の例に示すように、STP の再コンバージェンスにより、すべての VLAN から発生したトラフィックがトランク 2 を使用して転送されます。

```
Switch_1> (enable) 04/21/1998,03:15:40:DISL-5:Port 1/1 has become non-trunk

Switch_1> (enable) show spantree 1/1
Port      Vlan  Port-State     Cost   Priority  Fast-Start  Group-method
--------- ----  -------------  -----  --------  ----------  ------------
 1/1      1     not-connected     19        32   disabled
Switch_1> (enable) show spantree 1/2
Port      Vlan  Port-State     Cost   Priority  Fast-Start  Group-method
--------- ----  -------------  -----  --------  ----------  ------------
 1/2      1     learning          19        32   disabled
 1/2      10    learning          19        32   disabled
 1/2      20    learning          19        32   disabled
 1/2      30    learning          19        32   disabled
 1/2      40    forwarding        19         1   disabled
 1/2      50    forwarding        19         1   disabled
 1/2      60    forwarding        19         1   disabled
 1/2      1003  not-connected     19        32   disabled
 1/2      1005  not-connected     19         4   disabled
Switch_1> (enable) show spantree 1/2
Port      Vlan  Port-State     Cost   Priority  Fast-Start  Group-method
--------- ----  -------------  -----  --------  ----------  ------------
 1/2      1     forwarding        19        32   disabled
 1/2      10    forwarding        19        32   disabled
 1/2      20    forwarding        19        32   disabled
 1/2      30    forwarding        19        32   disabled
 1/2      40    forwarding        19         1   disabled
 1/2      50    forwarding        19         1   disabled
 1/2      60    forwarding        19         1   disabled
 1/2      1003  not-connected     19        32   disabled
 1/2      1005  not-connected     19         4   disabled
Switch_1> (enable)
```

CHAPTER 6

EtherChannel の設定

この章では、CLI（コマンドライン インターフェイス）を使用して Catalyst 6500 シリーズ スイッチ上で EtherChannel を設定する手順について説明します。この章で説明する設定手順は、イーサネット、ファスト イーサネット、ギガビット イーサネット、および 10 ギガビット イーサネット スイッチング モジュールの他に、スーパバイザ エンジン上のアップリンク ポートにも当てはまります。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

この章で説明する内容は、次のとおりです。

(注) Release 8.4(1) 以降のソフトウェア リリースでは、EtherChannel 内のポートの 1 つが設定可能なエラー スレッシュホールドを超えた場合に、EtherChannel 内の別のポートにトラフィックを自動的にフェールオーバーするよう EtherChannel エラー処理を設定できます。詳細については、「EtherChannel/ リンク エラー処理の設定」（p.19-24）を参照してください。

(注) ここで示すコマンドは、Catalyst 6500 シリーズ スイッチのすべてのイーサネット ポート上で使用できます。

EtherChannel の機能概要

EtherChannel は、互換性のある設定がされた最大 8 ポートの帯域幅を集約して 1 本の論理リンクにします。Catalyst 6500 シリーズ スイッチは、最大 128 の EtherChannel をサポートしています。スタンバイ スーパバイザ エンジン上も含めて、すべてのモジュール上のすべてのイーサネット ポートが EtherChannel をサポートしています。これらのポートは、隣接するポートまたは同じモジュール上のポートでなくてもかまいません。各 EtherChannel のポート速度は、すべて同じでなければなりません。

（注） Release 6.3(1) 以降のソフトウェア リリースでは、スパニングツリー機能によるポート ID 処理のため、サポートされる EtherChannel の最大数は、6 スロットまたは 9 スロット シャーシの場合は 126、13 スロット シャーシの場合は 63 です。

（注） Catalyst 6500 シリーズ スイッチに接続するネットワーク装置によって、1 つの EtherChannel にバンドルできるポート数が制限される場合があります。

EtherChannel 内のリンクで障害が発生すると、障害リンク上でそれまで伝送されていたトラフィックが EtherChannel 内の他のリンクに切り替えられます。チャネルの 1 つのリンクに着信したブロードキャストおよびマルチキャスト パケットは、EtherChannel の他のリンクに戻されることはありません。

EtherChannel は、トランクとして設定できます。チャネルの形成後に、チャネル内のいずれかのポートをトランクとして設定すると、チャネル内のすべてのポートにその設定が適用されます。同じ設定のトランク ポートは、1 つの EtherChannel として設定できます。

EtherChannel フレーム配布の機能概要

EtherChannel は、フレーム内のアドレスから構成されるバイナリ パターンの一部分を、チャネルの 1 つのリンクを選択する数値に変換することによって、チャネルの各リンクにフレームを配布します。

EtherChannel フレームは、シスコ独自のハッシュ アルゴリズムに基づいて配布されます。このアルゴリズムは確定型であり、アドレスとセッション情報が同じであれば、常に同じチャネル ポートにハッシュされます。したがって、パケット配信が無秩序になることはありません。

アドレスは、**set port channel all distribution** コマンドの **ip**、**mac**、**session**、および **ip-vlan-session** オプションによって決定されたポリシーに基づき、送信元、宛先、2 つの IP アドレスのコンビネーション、2 つの MAC（メディア アクセス制御）アドレスのコンビネーション、または 2 つの TCP または UDP ポート番号にすることができます。詳細については、「EtherChannel ロードバランシングの設定」（p.6-12）を参照してください。

（注） **set port channel all distribution session** コマンドを使用できるのは、Supervisor Engine 2、Supervisor Engine 720、および Supervisor Engine 32 に限られます。**set port channel all distribution ip-vlan-session** コマンドを使用できるのは、Supervisor Engine 720 と Supervisor Engine 32 に限られます。

すべてのスーパバイザ エンジン上で EtherChannel フレーム配布を設定できるわけではありません。ご使用のスイッチで EtherChannel によるフレーム配布が設定可能かどうかを調べるには、スーパバイザ エンジン上で **show module** コマンドを入力します。このコマンドで [Sub-Type] が [L2 Switching Engine I WS-F6020] と表示された場合、その Catalyst 6500 シリーズ スイッチでは EtherChannel フレーム配布を設定できません。スイッチは送信元と宛先の MAC アドレスを使用します。

それ以外のスイッチング エンジンでは、EtherChannel フレーム配布を設定できます。デフォルトでは、送信元と宛先の IP アドレスを使用します。

PAgP および LACP

Port Aggregation Protocol（PAgP）と Link Aggregation Control Protocol（LACP）は、2 つの異なるプロトコルですが、いずれも、隣接スイッチとのダイナミック ネゴシエーションによって、同じ特性を持つポートを 1 つのチャネルにまとめることができます。PAgP はシスコ独自のプロトコルであり、このプロトコルを使用できるのはシスコ製スイッチおよびシスコのライセンスに基づいてベンダーが販売しているスイッチだけです。LACP は IEEE 802.3ad で定義されているプロトコルであり、シスコ製スイッチは LACP を使用して 802.3ad 仕様適合装置とのイーサネット チャネリングを管理します。

（注） PAgP および LACP の EtherChannel ポートでは、MAC アドレス通知の設定は無視されます。

PAgP の使用については、「PAgP の機能概要」（p.6-7）を参照してください。LACP の使用については、「LACP の機能概要」（p.6-14）を参照してください。

EtherChannel 設定時の注意事項

EtherChannel を正しく設定しないと、ネットワーク ループや他の問題を回避するために、EtherChannel ポートが自動的にディセーブルになることがあります。

(注)　特に明記されていないかぎり、この注意事項は PAgP と LACP の両方に当てはまります。

ここでは、EtherChannel 設定時の注意事項について説明します。

ポート設定時の注意事項

ここでは、ポート設定時の注意事項について説明します。

- EtherChannel ごとに互換性のある設定がされたポートを最大 8 つまで割り当てることができます。これらのポートは隣接していなくてもかまいません。また、同一モジュール上になくてもかまいません。

(注)　異なるモジュールのポートで EtherChannel を設定する場合は、**set port channel** *port_list admin_group* コマンドを使用して、これらのポートを同じ管理グループに入れる必要があります。

- EtherChannel のすべてのポートに、同じプロトコルを使用する必要があります。1 つのモジュール上で 2 種類のプロトコルを使用することはできません。
- PAgP と LACP 間に互換性はありません。したがって、チャネルの両端で同じプロトコルを使用する必要があります。

(注)　**on** モードでは、スイッチの一方に PAgP、反対側に LACP を手動で設定できます。

- プロトコルはいつでも変更できますが、変更すると、既存のすべての EtherChannel が新しいプロトコルのデフォルトのチャネル モードにリセットされます。
- EtherChannel　内のすべてのポートを、同じ速度および同じデュプレックス　モード（全二重は LACP モードのみ）で動作するように設定してください。
- EtherChannel 内のすべてのポートをイネーブルにしてください。EtherChannel 内のポートがディセーブルになっていると、リンク障害とみなされ、そのポートのトラフィックが EtherChannel 内の残りのポートのいずれかに転送されます。
- 1 つのポートが同時に複数のチャネルに属すことはできません。
- ポート パス コスト（**set spantree portcost** コマンドで設定）が異なる複数のポートは、他の条件が矛盾なく設定されているかぎり、EtherChannel を形成できます。異なるポート パス コストを設定すること自体は、EtherChannel の形成に影響はありません。
- PAgP と LACP はそれぞれ個別にチャネルを管理します。チャネルのすべてのポートがディセーブルになると、PAgP がそのチャネルを内部チャネル リストから削除するので、**show** コマンドを実行してもチャネルは表示されません。LACP の場合、チャネルのすべてのポートがディセー

ブルになっても、チャネルを削除しないので、**show** コマンドを実行すると、すべての所属ポートが停止していても、チャネルは引き続き表示されます。チャネルが LACP を使用してトラフィックを活発に送受信しているかどうかを調べるには、**show port** コマンドを入力して、リンクがアップかそれともダウンかを調べます。

- LACP は半二重リンクをサポートしていません。ポートがアクティブまたはパッシブ モードで、半二重になると、ポートは停止します（さらに Syslog メッセージが生成されます）。このようなポートは、**show port** コマンドでは [connected]、**show spantree** コマンドでは [not connected] として表示されます。この矛盾は、ポートが物理的に接続されていても、スパニングツリーに加入していないために生じます。ポートをスパニングツリーに加入させるには、デュプレックスを全二重に設定するか、またはチャネル モードをそのポートではオフに設定します。

  Release 7.3(1) 以降のソフトウェア リリースでは、半二重リンクでの LACP 動作が変わり、対象となるポートが停止することはありません。ポートは停止せず、（存在する場合）LACP Protocol Data Unit（PDU; プロトコル データ ユニット）送信が抑制されます。ポートがチャネルの一部である場合、そのポートはチャネルから切り離されますが、引き続き非チャネル ポートとして機能します。この場合、Syslog メッセージが生成されます。リンクの設定が全二重に戻れば、標準の LACP 動作は自動的にイネーブルに戻ります。

VLAN およびトランク設定時の注意事項

ここでは、VLAN（仮想 LAN）およびトランク関連設定時の注意事項について説明します。

- EtherChannel 内のすべてのポートを同一 VLAN に割り当てるか、トランク ポートとして設定してください。
- EtherChannel をトランクとして設定する場合は、その EtherChannel のすべてのポートに同じトランク モードを設定してください。EtherChannel 内のポートをそれぞれ異なるトランク モードに設定すると、予想外の結果が生じる可能性があります。
- EtherChannel は、1 つのトランキング EtherChannel のすべてのポートで同じ許容範囲の VLAN をサポートしています。VLAN の許容範囲がポート リストで共通していない場合、**set port channel** コマンドで **auto** または **desirable** モードを設定しても、それらのポートは EtherChannel を形成しません。
- EtherChannel 内のポートは、ダイナミック VLAN ポートとして設定しないでください。設定した場合、スイッチのパフォーマンスに悪影響が出る可能性があります。
- 異なる VLAN コストが設定されているポートでチャネルを形成することはできません。

他の機能との相互作用に関する注意事項

ここでは、EtherChannel と他の機能との相互作用に関する注意事項について説明します。

- GARP VLAN Registration Protocol（GVRP）、GARP Multicast Registration Protocol（GMRP）、および Quality of Service（QoS; サービス品質）の設定が異なるポートでは、EtherChannel は形成されません。
- ポート　セキュリティをイネーブルにしている場合、EtherChannel　は形成されません。また、EtherChannel 内のポートに対してポート セキュリティをイネーブルにすることはできません。
- いずれかのポートが Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）宛先ポートである場合、EtherChannel は形成されません。
- プロトコル フィルタリングの設定がポート間で異なっている場合、EtherChannel は形成されません。
- Cisco Discovery Protocol（CDP）は、ポートがチャネルに追加されたあとでも、物理ポート上で動作します。
- VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）および Dual Ring Protocol（DRiP）は、チャネル上で動作します。

- スタンバイ スーパバイザ エンジンへの高速スイッチオーバー時に、チャネルを形成しているすべてのポートでチャネリングの設定およびステートが消去され、リンクが一時的に切断されるので、相手ポートがリセットされます。すべてのポートが非チャネリング ステートにリセットされます。
- dot1q ポート タイプの異なるポートでチャネルを形成することはできません。
- ジャンボ フレームの設定が異なるポートでチャネルを形成することはできません。
- ダイナミック設定が異なるポートでチャネルを形成することはできません。
- スタンバイ スーパバイザ エンジンへのハイアベイラビリティ切り替え時には、チャネルを形成しているすべてのポートが動作可能な状態のままです。ポートがリセットされるのは、スイッチ オーバー時にイベントの欠落が生じた場合だけです。

（注） Release 6.3(1) 以降のソフトウェア リリースでは、PAgP が設定された EtherChannel は、1 ポートしかなくても維持されます（これは LACP が設定された EtherChannel には当てはまりません）。Releases 6.3(1) より前のソフトウェア リリースでは、スパニングツリーから 1 ポート チャネルを削除して個別のポートとしてスパニングツリーに追加するとトラフィックが中断されていました。

（注） Rerease 6.3(1) 以降のソフトウェア リリースでは、スパニングツリー機能によるポート ID 処理のため、EtherChannel の最大数は、6 スロットまたは 9 スロット シャーシの場合は 126、13 スロット シャーシの場合は 63 です。

PAgP の機能概要

（注）　PAgP を使用して EtherChannel を設定する場合は、以下の情報を参考にしてください。LACP を使用する場合は、「LACP の機能概要」（p.6-14）を参照してください。

ここでは、PAgP について説明します。

PAgP モード

PAgP を使用すると、イーサネット ポート間でパケットを交換することによって、EtherChannel を自動的に作成できます。PAgP パケットが交換されるのは、**auto** モードおよび **desirable** モードのポート間に限られます。**on** または **off** モードとして設定されたポートは、PAgP パケットを交換しません。このプロトコルは、ポート グループの能力を動的に学習し、他のポートに通知します。PAgP は、正確に一致している EtherChannel リンクを識別すると、これらのポートを 1 つの EtherChannel としてまとめます。作成された EtherChannel は、単一ブリッジ ポートとしてスパニングツリーに追加されます。

EtherChannel には、ユーザ設定可能なモードが 4 種類あり、**on**、**off**、**auto**、および **desirable** です。このうち PAgP のモードは、**auto** と **desirable** だけです。**auto** および **desirable** のモードは、**silent** および **non-silent** のキーワードを使用して変更できます。デフォルトの設定では、ポートは **auto silent** モードです。

表 6-1 に、PAgP で使用できる EtherChannel モードを示します。

表 6-1　PAgP で使用できる EtherChannel モード

モード	説明
on	PAgP を使用せず、ポートを強制的にチャネル化するモード。**on** モードの場合、使用可能な EtherChannel が存在するのは、**on** モードのポート グループが他の **on** モードのポート グループに接続されている場合だけです。
off	ポートのチャネリングを防止するモード。
auto	ポートをパッシブ ネゴシエーション ステートにする PAgP モード。ポートは受信した PAgP パケットには応答しますが、PAgP パケット ネゴシエーションは開始しません（デフォルト）。
desirable	ポートをアクティブ ネゴシエーション ステートにする PAgP モード。ポートは PAgP パケットを送信して、他のポートとのネゴシエーションを開始します。
silent	**auto** または **desirable** モードとともに使用するキーワード。もう一方の装置からのトラフィックがまったくない場合に、Spanning-Tree Protocol（STP; スパニングツリー プロトコル）に対してリンク障害として報告されるのを防ぐために使用します（デフォルト）。
non-silent	**auto** または **desirable** モードとともに使用するキーワード。もう一方の装置からのトラフィックがある場合に使用します。

auto および **desirable** モードでは、ポートは接続ポートとネゴシエーションを行うことにより、ポート速度、トランキング ステート、VLAN 番号などの条件に基づいて、EtherChannel を形成できるかどうかを判別できます。

次のように、ポート間で PAgP モードが違っていても、相互に通信可能なモードであるかぎり、EtherChannel を形成できます。

- **desirable** モードのポートは、**desirable** または **auto** モードの別のポートと EtherChannel を形成できます。
- **auto** モードのポートは、**desirable** モードの別のポートと EtherChannel を形成できます。
- **auto** モードのポートは、**auto** モードの別のポートとは EtherChannel を形成できません。どちらのポートもネゴシエーションを開始しないためです。

EtherChannel フレーム配布を設定できる場合、MAC アドレス、IP アドレス、およびレイヤ 4 ポート番号を使用できます。送信元アドレス、宛先アドレスのいずれか一方、または送信元 / 宛先の両方のアドレスとレイヤ 4 ポート番号を指定できます。選択したモードは、スイッチ上で設定されているすべての EtherChannel に適用されます。設定の中で最も多様性のあるオプションを使用してください。たとえば、チャネル上のトラフィックが 1 つの MAC アドレスだけを宛先とする場合、送信元アドレス、IP アドレス、またはレイヤ 4 ポート番号を使用してフレーム配布を行えば、MAC アドレスを使用する場合よりも効率的なフレーム配布が可能になります。

PAgP 管理グループ

EtherChannel を設定すると、1 ～ 1024 の整数で表される管理グループが作成され、EtherChannel はその管理グループに属すことになります。管理グループの作成時に、管理グループ番号を手動で割り当てることも、次に利用可能な管理グループ番号を自動的に割り当てることもできます。管理グループ番号を指定せずにチャネルを形成すると、新しい管理グループには自動的に番号が割り当てられます。1 つの管理グループには、最大 8 ポートを所属させることができます。

PAgP EtherChannel ID

それぞれの EtherChannel には、一意の EtherChannel ID が自動的に割り当てられます。EtherChannel ID を表示するには、**show channel group** *admin_group* コマンドを使用します。

PAgP を使用した EtherChannel の設定

ここでは、PAgP を使用して EtherChannel を設定する手順について説明します。

(注)　EtherChannel を設定する前に、「EtherChannel 設定時の注意事項」（p.6-4）を参照してください。

EtherChannel プロトコルの指定

(注)　デフォルトのプロトコルは PAgP です。

(注)　1 つのモジュールで指定できるプロトコルは、PAgP または LACP のどちらか 1 つだけです。

EtherChannel プロトコルを指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
EtherChannel プロトコルを指定します。	**set channelprotocol** [**pagp** | **lacp**] *mod*

次に、モジュール 3 に PAgP プロトコルを指定する例を示します。

```
Console> (enable) set channelprotocol pagp 3
Channeling protocol set to PAGP for module(s) 3.
Console> (enable)
```

EtherChannel の設定

イーサネット ポートのグループ上で EtherChannel を設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
目的とするポート上で EtherChannel を設定します。	**set port channel** *mod/ports...*[*admin_group*] **set port channel** *mod/ports...* **mode** {**on** | **off** | **desirable** | **auto**} [**silent** | **non-silent**]

次に、新しい管理グループで 7 ポートの EtherChannel を設定する例を示します。

```
Console> (enable) set port channel 2/2-8 mode desirable
Ports 2/2-8 left admin_group 1.
Ports 2/2-8 joined admin_group 2.
Console> (enable)
```

EtherChannel ポート モードの設定

ポートの EtherChannel モードを設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
ポートの EtherChannel モードを設定します。	**set port channel** *mod/ports...*[*admin_group*] **set port channel** *mod/port* **mode** {**on** | **off** | **desirable** | **auto**} [**silent** | **non-silent**]

次に、ポート 2/1 を **auto** モードに設定する例を示します。

```
Console> (enable) set port channel 2/1 mode auto
Ports 2/1 channel mode set to auto.
Console> (enable)
```

EtherChannel ポート パス コストの設定

（注） この作業には、LACP と PAgP の両方を設定するグローバル コマンドを使用します。

チャネルのパス コストは、そのチャネルに属する各ポートのポート コストを調整することによって実現されます。コストを指定しなかった場合は、チャネルを形成しているポートの現在のポート コストに基づいて更新されます。1 チャネルまたはすべてのチャネルを指定します。

EtherChannel ポート パス コストを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	管理グループ番号を使用して、EtherChannel ID を表示します。	**show channel group** *admin_group* または **show lacp-channel group** *admin_key*
ステップ 2	EtherChannel ID を使用して、EtherChannel ポート パス コストを設定します。	**set spantree channelcost** {*channel_id* | **all**} *cost*

（注） ***set spantree channelcost*** コマンドを実行しても、コンフィギュレーション ファイルには表示されません。このコマンドにより、チャネル内の各ポートについて、[set spantree portcost] のエントリが作成されます。***set spantree portcost*** コマンドの使用方法の詳細については、第 8 章「スパニングツリーの設定」の「PVST+ ポート コストの設定」を参照してください。

次に、チャネル ID 768 に EtherChannel ポート パス コストを設定する例を示します。

```
Console> (enable) show channel group 20
Admin Port  Status     Channel   Channel
group                  Mode      id
----- ----- ---------- --------- --------
  20    1/1 notconnect on             768
  20    1/2 connected  on             768

Admin Port  Device-ID                       Port-ID                   Platform
group
----- ----- ------------------------------ ------------------------- ----------
  20    1/1
  20    1/2  066510644(cat26-lnf(NET25))     2/1                      WS-C6009
Console> (enable)

Console> (enable) set spantree channelcost 768 12
Port(s) 1/1,1/2 port path cost are updated to 31.
Channel 768 cost is set to 12.
Warning:channel cost may not be applicable if channel is broken.
Console> (enable)
```

EtherChannel VLAN コストの設定

(注)　この作業には、LACP と PAgP の両方を設定するグローバル コマンドを使用します。

EtherChannel VLAN コスト機能は、トランキングによって設定された複数のチャネルで VLAN トラフィックのロードバランシングを行います。

set spantree channelvlancost コマンドを使用して、チャネル内のすべての VLAN に対して初期スパニングツリー コストを設定します。***set spantree channelvlancost*** コマンドは、チャネル内の一部の VLAN に対して代替コストを設定します（チャネルでトランキングしていることが前提です）。このコマンドにより、チャネルごとに最大 2 つの異なるスパニングツリー コストを割り当てることができます。たとえば、チャネル内の一部の VLAN は [vlancost] を、残りの VLAN は [cost] を持つことができます。

set spantree channelvlancost コマンドは、チャネル内の各ポートのコンフィギュレーション ファイルに [set spantree portvlancost] エントリを作成します。***set spantree channelvlancost*** コマンドを実行した場合、チャネル内の少なくとも 1 つのポートに対して **set spantree portvlancost** コマンドを実行して、各ポートに対応付ける VLAN を指定する必要があります。次に、各コマンドを入力した場合の結果を示します。

```
Console> (enable) set spantree channelvlancost 856 10
Port(s) 3/47-48 vlan cost are updated to 16.
Channel 856 vlancost is set to 10.
```

コンフィギュレーション ファイルには、次のコマンドが追加されます。

- **set spantree portvlancost 3/47 cost 16**
- **set spantree portvlancost 3/48 cost 16**

作成された上記コマンドに目的の VLAN を追加するには、次のコマンドを入力します。

```
Console> (enable) set spantree portvlancost 3/47 cost 16 1-1005
Port 3/47 VLANs 1025-4094 have path cost 19.
Port 3/47 VLANs 1-1005 have path cost 16.
Port 3/48 VLANs 1-1005 have path cost 16.
```

EtherChannel VLAN コストを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	管理グループ番号を使用して、EtherChannel ID を表示します。	**show channel group** *admin_group* または **show lacp-channel group** *admin_key*
ステップ 2	EtherChannel ID を使用して、EtherChannel VLAN コストを設定します。	**set spantree channelvlancost** *channel_id cost*
ステップ 3	各ポートに目的とする VLAN のポート コストを設定します。	**set spantree portvlancost** {*mod/port*} [**cost** *cost*] [*vlan_list*]

次に、チャネル ID 856 に EtherChannel VLAN コストを設定する例を示します。

```
Console> (enable) show channel group 22
Admin Port  Status     Channel   Channel
group                  Mode      id
----- ----- ---------- --------- --------
  22    1/1 notconnect on              856
  22    1/2 connected  on              856

Admin Port  Device-ID                        Port-ID                   Platform
group
----- ----- ------------------------------ ------------------------- ----------
  22    1/1
  22    1/2  066510644(cat26-lnf(NET25))     2/1                      WS-C6009
Console> (enable)

Console> (enable) set spantree channelvlancost 856 10
Port(s) 3/47-48 vlan cost are updated to 16.
Channel 856 vlancost is set to 10.
Console> (enable) set spantree portvlancost 3/47 cost 16 1-1005
Port 3/47 VLANs 1025-4094 have path cost 19.
Port 3/47 VLANs 1-1005 have path cost 16.
Port 3/48 VLANs 1-1005 have path cost 16.
Console> (enable)
```

EtherChannel ロードバランシングの設定

ロードバランシング ポリシー（フレーム配布）は、MAC アドレス（レイヤ 2）、IP アドレス（レイヤ 3）、またはポート番号（レイヤ 4）に基づいて設定できます。これらのポリシーはそれぞれ、**mac**、**ip**、および **session** キーワードによってアクティブになります。ロードバランシングは、送信元アドレス（**source** キーワード）単独、宛先アドレス（**destination** キーワード）単独、または送信元と宛先両方のアドレス（**both** キーワード）に基づいて行うことができます。

パケットが選択されたカテゴリに属していない場合は、その次に下位のカテゴリとみなされます。ハードウェアが選択されたフレーム配布方式をサポートしていない場合は、[Feature not supported] というエラー メッセージが表示されます。

EtherChannel ロードバランシングを設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
EtherChannel ロードバランシングを設定します。	**set port channel all distribution {ip | mac | session | ip-vlan-session} [source | destination | both]**

(注)　**set port channel all distribution session** コマンド オプションを使用できるのは、Supervisor Engine 2、Supervisor Engine 720、および Supervisor Engine 32 に限られます。

(注)　**set port channel all distribution ip-vlan-session** コマンドを使用できるのは、Supervisor Engine 720 と Supervisor Engine 32 に限られます。このコマンドは、IP アドレス、VLAN、およびレイヤ 4 トラフィックを使用してフレーム配布方式を指定する際に使用します。

次に、EtherChannel が MAC 送信元アドレスを使用するように設定する例を示します。

```
Console> (enable) set port channel all distribution mac source
Channel distribution is set to mac source.
Console> (enable)
```

EtherChannel トラフィック利用率の表示

EtherChannel ポート上でのトラフィック利用率を表示するには、次の作業を行います。

作業	コマンド
トラフィック利用率を表示します。	**show channel traffic**

次に、EtherChannel ポート上でのトラフィック利用率を表示する例を示します。

```
Console> (enable) show channel traffic
ChanId Port  Rx-Ucst Tx-Ucst Rx-Mcst Tx-Mcst Rx-Bcst Tx-Bcst
------ ----- ------- ------- ------- ------- ------- -------
   808  2/16   0.00%   0.00%  50.00%  75.75%   0.00%   0.00%
   808  2/17   0.00%   0.00%  50.00%  25.25%   0.00%   0.00%
   816  2/31   0.00%   0.00%  25.25%  50.50%   0.00%   0.00%
   816  2/32   0.00%   0.00%  75.75%  50.50%   0.00%   0.00%
Console> (enable)
```

特定のアドレスまたはレイヤ 4 ポート番号の発信ポートの表示

EtherChannel で特定のアドレスまたはレイヤ 4 ポート番号に使用されている発信ポートを表示するには、次の作業を行います。

作業	コマンド
特定のアドレスまたはレイヤ 4 ポート番号の発信ポートを表示します。	**show channel hash** *channel_id src_ip_addr vlan src_port* [*dest_ip_addr vlan dest_port*] **show channel hash** *channel_id dest_ip_addr vlan dest_port*

次に、特定の送信元および宛先 IP アドレスについて、発信ポートを表示する例を示します。

```
Console> (enable) show channel hash 808 172.20.32.10 172.20.32.66
Selected channel port:2/17
Console> (enable)
```

EtherChannel のディセーブル化

EtherChannel をディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
EtherChannel をディセーブルにします。	**set port channel** *mod/port* **mode off**

次に、EtherChannel をディセーブルにする例を示します。

```
Console> (enable) set port channel 2/2-8 mode off
Ports 2/2-8 channel mode set to off.
Console> (enable)
```

LACP の機能概要

（注） LACP を使用して EtherChannel を設定する場合は、以下の情報を参考にしてください。PAgP を使用する場合は、「PAgP の機能概要」（p.6-7）を参照してください。

ここでは、次の項目について説明します。

LACP モード

手動でチャネリングをオンにするには、ポート チャネル モードを **on** に設定します。チャネリングをオフにするには、ポート チャネル モードを **off** に設定します。

LACP でチャネリングを処理する場合は、**active** および **passive** というチャネル モードを使用します。LACP を使用して自動 EtherChannel 設定を開始するには、リンクの少なくとも一端を **active** モードに設定してチャネリングを開始する必要があります。**passive** モードのポートは、開始に応答するだけで、LACP パケットの送信を開始することはありません。

表 6-2 に、LACP で使用できる EtherChannel モードを示します。

表 6-2　LACP で使用できる EtherChannel モード

モード	説明
on	LACP を使用せず、ポートを強制的にチャネル化するモード。**on** モードの場合、使用可能な EtherChannel が存在するのは、**on** モードのポート グループが他の **on** モードのポート グループに接続されている場合だけです。
off	ポートのチャネリングを防止するモード。
passive	ポートをパッシブ ネゴシエーション ステートにする LACP モード。ポートは受信した LACP パケットには応答しますが、LACP パケット ネゴシエーションは開始しません（デフォルト）。
active	ポートをアクティブ ネゴシエーション ステートにする LACP モード。ポートは LACP パケットを送信して、他のポートとのネゴシエーションを開始します。

LACP パラメータ

LACP の設定に使用するパラメータは、次のとおりです。

- システム プライオリティ

  LACP が稼働している各スイッチに、システム プライオリティを割り当てる必要があります。このプライオリティは自動的に指定することも、CLI から指定することもできます（「システム プライオリティの指定」[p.6-17] を参照）。システム プライオリティは、スイッチ MAC アドレスと組み合わせて使用することによって、システム ID が形成されます。また、他のシステムとのネゴシエーション時にも使用されます。

- ポート プライオリティ

  スイッチの各ポートに、ポート プライオリティを割り当てる必要があります。このプライオリティは自動的に指定することも、CLI から指定することもできます（「ポート プライオリティの指定」[p.6-17] を参照）。ポート プライオリティは、ポート番号と組み合わせて使用することによって、ポート ID が形成されます。ポート プライオリティは、ハードウェアの制約ですべての互換ポートを集約することができない場合に、スタンバイ モードにするポートを決定するために使用されます。

- 管理キー

  スイッチの各ポートに、管理キー値を割り当てる必要があります。この値は自動的に指定することも、CLI から指定することもできます（「管理キー値の指定」[p.6-18] を参照）。他のポートに集約されるポートの能力は、管理キーを使用して定義します。ポートが他のポートと集約できるかどうかは、次の要因によって決定付けられます。

  — ポートの物理特性（データ転送速度、デュプレックス能力、ポイントツーポイントまたは共用メディアなど）

  — ユーザが設定したコンフィギュレーション制約

イネーブルの場合、LACP は常に、ハードウェアの最大許容数（8 ポート）まで、チャネルに最大数の互換ポートを設定しようとします。LACP が互換性のあるすべてのポートを集約することができない場合（リモート システムの方がハードウェアの制約が大きい場合など）、チャネルにアクティブとして組み込むことのできなかったポートはすべてホット スタンバイ ステートになり、いずれかのチャネル ポートで障害が発生した場合に限り使用されます。

同じ管理キーを割り当てたポートを使用して、さまざまなチャネルを設定できます。たとえば、8 ポートに同じ管理キーを割り当てた場合、そのうちの 4 ポートを LACP **active** モードを使用するチャネルに設定し、残りの 4 ポートを **on** モードを使用して手動設定したチャネルに含めることができます。管理キーは、その管理キーを割り当てたスイッチのコンテキストの中に限り有効になります。管理キー値にグローバルな有効性はありません。

LACP を使用した EtherChannel の設定

ここでは、LACP を使用して EtherChannel を設定する手順について説明します。

（注） EtherChannel を設定する前に、「EtherChannel 設定時の注意事項」（p.6-4）を参照してください。

EtherChannel プロトコルの指定

（注） デフォルトのプロトコルは PAgP です。

（注） 1 つのモジュールで指定できるプロトコルは、PAgP または LACP のどちらか 1 つだけです。

EtherChannel プロトコルを指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
EtherChannel プロトコルを指定します。	**set channelprotocol** [**pagp** | **lacp**] *mod*

次に、モジュール 2 およびモジュール 3 に LACP プロトコルを指定する例を示します。

```
Console> (enable) set channelprotocol lacp 2,3
Mod 2 is set to LACP protocol.
Mod 3 is set to LACP protocol.
Console> (enable)
```

show channelprotocol コマンドを使用すると、すべてのモジュールのプロトコルが表示されます。

システム プライオリティの指定

(注)　このコマンドはグローバル オプションですが、適用されるのは、LACP がイネーブルのモジュールだけです。PAgP が稼働しているモジュールでは無視されます。

システム プライオリティ値は、1 ～ 65535 の範囲でなければなりません。数字が大きいほど、プライオリティは下がります。デフォルトのプライオリティは 32768 です。

システム プライオリティを指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
システム プライオリティを指定します。	**set lacp-channel system-priority** *value*

次に、システム プライオリティを 20000 として指定する例を示します。

```
Console> (enable) set lacp-channel system-priority 20000
LACP system priority is set to 20000
Console> (enable)
```

show lacp-channel sys-id コマンドを使用すると、LACP システム ID およびシステム プライオリティが表示されます。

ポート プライオリティの指定

ポート プライオリティ値は、1 ～ 255 の範囲でなければなりません。数字が大きいほど、プライオリティは下がります。デフォルトのプライオリティは 128 です。

ポート プライオリティを指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
ポート プライオリティを指定します。	**set port lacp-channel** *mod/ports* **port-priority** *value*

次に、ポート 1/1 ～ 1/4 およびポート 2/6 ～ 2/8 のポート プライオリティを 10 に設定する例を示します。

```
Console> (enable) set port lacp-channel 1/1-4,2/6-8 port-priority 10
Port(s) 1/1-4,2/6-8 port-priority set to 10.
Console> (enable)
```

show lacp-channel group *admin_key* **info** コマンドを使用すると、ポート プライオリティが表示されます。

管理キー値の指定

(注)　NVRAM（不揮発性　RAM）に保存されているシステムまたはモジュールの設定情報が消去されると、管理キーに新しい値が自動的に割り当てられます。モジュールの場合、第 1 ポート、第 5 ポート、第 9 ポートなどから始まる 4 つの連続ポートからなるグループごとに、固有の管理キーが割り当てられます。ポートにはモジュール全体で固有の管理キーを与える必要があります。NVRAM が消去されると、ポートのチャネル モードは [passive] に設定されます。

一連のポートに管理キー値を指定することもできます。また、パラメータ *admin_key* を指定しなかった場合は、システムが自動的に値を選択します。いずれの場合も、admin_key 値の範囲は 1 ～ 1024 です。

選択した管理キー値がシステムですでに使用されている場合は、先に割り当てられていた管理キー値に関連するすべてのポートが自動的に割り当てられた別の値に移され、コマンドで指定したモジュールおよびポートに指定したとおりの管理キー値が割り当てられます。

管理キー値を割り当てることのできるポートの最大数は 8 です。

デフォルトのモードは、管理キーが割り当てられているすべてのポートで passive ですが、チャネルに特定のモードがすでに割り当てられている場合は（「チャネル モードの変更」[p.6-19] を参照）、管理キーを割り当ててもそのチャネルには適用されず、前に指定したチャネル モードが維持されます。

管理キー値を指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
管理キー値を指定します。	**set port lacp-channel** *mod/ports* [*admin_key*]

次に、ポート 4/1 ～ 4/4 に同じ管理キーを割り当て、その値をシステムに自動選択させる例を示します。

```
Console> (enable) set port lacp-channel 4/1-4
Port(s) 4/1-4 are assigned to admin key 96.
Console> (enable)
```

次に、ポート 4/4 ～ 4/6 に管理キー 96 を割り当てる（96 と指定）例を示します。この例では、システムによって別のポート グループに、同じ管理キーがすでに割り当てられています（前の例を参照）。

```
Console> (enable) set port lacp-channel 4/4-6 96
Port(s) 4/1-3 are moved to admin key 97.
Port(s) 4/4-6 are assigned to admin key 96.
Console> (enable)
```

次に、9 個以上のポートに同じ管理キー値を割り当てた場合のシステム応答の例を示します（要求は拒否され、どのポートにも管理キー 123 は割り当てられません）。

```
Console> (enable) set port lacp-port channel 2/1-2,4/1-8 123
No more than 8 ports can be assigned to an admin key.
Console> (enable)
```

show lacp-channel group コマンドを使用すると、ポートの管理キー値が表示されます。

チャネル モードの変更

同じ管理キーがすでに割り当てられている一連のポートについて、チャネル モードを変更できます（「管理キー値の指定」[p.6-18] を参照）。

チャネル モードを変更するには、イネーブル モードで次の作業を行います。

作業	コマンド
チャネル モードを変更します。	**set port lacp-channel** *mod/ports* **mode** [**on** | **off** | **active** | **passive**]

次に、ポート 4/1 および 4/6 のチャネル モードを変更し、**on** に設定する例を示します。ポート 4/1 および 4/6 の管理キーは変わりません。

```
Console> (enable) set port lacp-channel 4/1,4/6 mode on
Port(s) 4/1,4/6 channel mode set to on.
Console> (enable)
```

show lacp-channel group *admin_key* コマンドを使用すると、ポートのチャネル モードが表示されます。

チャネル パス コストの指定

チャネル パス コストは、LACP と PAgP の両方を設定するグローバル コマンドを使用することで指定できます。詳細については、「EtherChannel ポート パス コストの設定」（p.6-10）を参照してください。

チャネル VLAN コストの指定

チャネル VLAN コストは、LACP と PAgP の両方を設定するグローバル コマンドを使用することで指定できます。詳細については、「EtherChannel VLAN コストの設定」（p.6-11）を参照してください。

チャネル ロードバランシングの設定

チャネル ロードバランシングは、LACP と PAgP の両方を設定するグローバル コマンドを使用することで指定できます。詳細については、「EtherChannel ロードバランシングの設定」（p.6-12）を参照してください。

LACP 統計情報の消去

LACP 統計情報を消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
LACP 統計情報を消去します。	**clear lacp-channel statistics**

次に、LACP 統計情報を消去する例を示します。

```
Console> (enable) clear lacp-channel statistics
LACP channel counters are cleared.
Console> (enable)
```

EtherChannel トラフィック利用率の表示

EtherChannel ポート上でのトラフィック利用率を表示するには、次の作業を行います。

作業	コマンド
EtherChannel ポート上でのトラフィック利用率を表示します。	**show lacp-channel traffic**

次に、EtherChannel ポート上でのトラフィック利用率を表示する例を示します。

```
Console> (enable) show lacp-channel traffic
ChanId Port  Rx-Ucst Tx-Ucst Rx-Mcst Tx-Mcst Rx-Bcst Tx-Bcst
------ ----- ------- ------- ------- ------- ------- -------
   808  2/16   0.00%   0.00%  50.00%  75.75%   0.00%   0.00%
   808  2/17   0.00%   0.00%  50.00%  25.25%   0.00%   0.00%
   816  2/31   0.00%   0.00%  25.25%  50.50%   0.00%   0.00%
   816  2/32   0.00%   0.00%  75.75%  50.50%   0.00%   0.00%
Console> (enable)
```

特定のアドレスまたはレイヤ 4 ポート番号の発信ポートの表示

EtherChannel で指定されたアドレスまたはレイヤ 4 ポート番号に使用されている発信ポートを表示するには、次の作業を行います。

作業	コマンド
特定のアドレスまたはレイヤ 4 ポート番号の発信ポートを表示します。	**show lacp-channel hash** *channel_id src_ip_addr* [*dest_ip_addr*] | *dest_ip_address* | *src_mac_addr* [*dest_mac_addr*] | *dest_mac_addr* | *src_port dest_port* | *dest_port*

次に、特定の送信元および宛先 IP アドレスについて、発信ポートを表示する例を示します。

```
Console> (enable) show lacp-channel hash 808 172.20.32.10 172.20.32.66
Selected channel port:2/17
Console> (enable)
```

EtherChannel のディセーブル化

EtherChannel をディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
EtherChannel をディセーブルにします。	**set port lacp-channel** *mod/port* **mode off**

次に、EtherChannel をディセーブルにする例を示します。

```
Console> (enable) set port lacp-channel 2/2-8 mode off
Port(s) 2/2-8 channel mode set to off.
Console> (enable)
```

EtherChannel のスパニングツリー情報の表示

チャネル化されているすべてのポートについて、チャネル ID および切り捨てられたポート リストを表示できます。チャネル化されてないポートは、ポート番号で特定されます。

EtherChannel のスパニングツリー情報を表示するには、次の作業を行います。

作業	コマンド
EtherChannel のスパニングツリー情報を表示します。	**show spantree** *mod/port*

EtherChannel のスパニングツリー情報を表示する例を示します。

```
Console> show spantree 4/6
Port                     Vlan Port-State    Cost  Priority Portfast   Channel_id
------------------------ ---- ------------- ----- -------- ---------- ----------
 4/6                     1    not-connected     4       32 disabled   0
Console>

Console> show spantree 4/7
Port                     Vlan Port-State    Cost  Priority Portfast   Channel_id
------------------------ ---- ------------- ----- -------- ---------- ----------
4/7-8                    1    blocking          3       32 disabled   770
Console>
```

EtherChannel カウンタの消去と復元

show channel traffic コマンドによって、チャネル トラフィックの利用率を表示できます。チャネル トラフィックの利用率は、各チャネル ポートを通過するトラフィックの割合を示すものです。カウンタはパケット タイプ別に保持されています。Release 8.3(1) より前のソフトウェア リリースでは、チャネル ハードウェア カウンタ ベースが消去できない MIB（管理情報ベース）オブジェクトであったため、ベースを消去できませんでした。チャネル カウンタ ベースをリセットするには、**clear counters all** コマンドを入力します。Release8.3(1) 以降のソフトウェア リリースでは、プロトコル単位およびチャネル単位でチャネル ベース カウンタを消去し、復元できます。チャネルベース カウンタをチャネル単位で消去または復元するには、チャネル ID を入力します。チャネル ID を検索するには、PAgP チャネルの場合は **show port channel** コマンド、LACP チャネルの場合は **show port lacp-channel** コマンドを入力します。

EtherChannel カウンタの消去

EtherChannel カウンタを消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
すべての PAgP チャネル カウンタを消去します。	**clear counter channel all**
特定の PAgP チャネル カウンタを消去します。	**clear counter channel** *channel_id*
すべての LACP チャネル カウンタを消去します。	**clear counter lacp-channel all**
特定の LACP チャネル カウンタを消去します。	**clear counter lacp-channel** *channel_id*

次に、EtherChannel カウンタを消去するさまざまな手法の例を示します。

```
Console> (enable) show channel traffic
ChanId Port  Rx-Ucst Tx-Ucst Rx-Mcst Tx-Mcst Rx-Bcst Tx-Bcst
------ ----- ------- ------- ------- ------- ------- -------
   769  1/1    0.00%   0.00%   9.09%  90.90%   0.00%   0.00%
   769  2/1    0.00%   0.00%  90.91%   9.10%   0.00%   0.00%
------ ----- ------- ------- ------- ------- ------- -------
   841  7/17   0.00%   0.00% 100.00% 100.00%   0.00%   0.00%
   841  7/18   0.00%   0.00%   0.00%   0.00%   0.00%   0.00%
Console> (enable) clear counter channel all
This command will reset MAC and port counters reported by the CLI for all ports.
Counters reported by SNMP will not be affected.
Do you want to continue (y/n) [n]? y
MAC and Port counters cleared.
Console> (enable) show channel traffic
ChanId Port  Rx-Ucst Tx-Ucst Rx-Mcst Tx-Mcst Rx-Bcst Tx-Bcst
------ ----- ------- ------- ------- ------- ------- -------
   769  1/1    0.00%   0.00%   0.00% 100.00%   0.00%   0.00%
   769  2/1    0.00%   0.00% 100.00%   0.00%   0.00%   0.00%
------ ----- ------- ------- ------- ------- ------- -------
   841  7/17   0.00%   0.00% 100.00% 100.00%   0.00%   0.00%
   841  7/18   0.00%   0.00%   0.00%   0.00%   0.00%   0.00%
Console> (enable) show channel traffic 769
ChanId Port  Rx-Ucst Tx-Ucst Rx-Mcst Tx-Mcst Rx-Bcst Tx-Bcst
------ ----- ------- ------- ------- ------- ------- -------
   769  1/1    0.00%   0.00%   9.52%  90.47%   0.00%   0.00%
   769  2/1    0.00%   0.00%  90.48%   9.53%   0.00%   0.00%
Console> (enable) clear counter channel 769
This command will reset MAC and port counters reported by the CLI for PAGP channel 769
Counters reported by SNMP will not be affected.
Do you want to continue (y/n) [n]? y
MAC and Port counters cleared.
Console> (enable) show channel traffic 769
ChanId Port  Rx-Ucst Tx-Ucst Rx-Mcst Tx-Mcst Rx-Bcst Tx-Bcst
------ ----- ------- ------- ------- ------- ------- -------
   769  1/1    0.00%   0.00%   0.00% 100.00%   0.00%   0.00%
   769  2/1    0.00%   0.00% 100.00%   0.00%   0.00%   0.00%
Console> (enable)
```

EtherChannel カウンタの復元

EtherChannel カウンタを復元するには、イネーブル モードで次の作業を行います。

作業	コマンド
すべての PAgP チャネル カウンタを復元します。	**restore counter channel all**
特定の PAgP チャネル カウンタを復元します。	**restore counter channel** *channel_id*
すべての LACP チャネル カウンタを復元します。	**restore counter lacp-channel all**
特定の LACP チャネル カウンタを復元します。	**restore counter lacp-channel** *channel_id*

次に、チャネル 769 のチャネルを復元する例を示します。

```
Console> (enable) restore counter channel 769
This command will restore counter values reported by the CLI
for PAGP channel 769 ports to the hardware counter values.
Do you want to continue (y/n) [n]? y
MAC and Port counters restored.
Console> (enable) show channel traffic 769
ChanId Port  Rx-Ucst Tx-Ucst Rx-Mcst Tx-Mcst Rx-Bcst Tx-Bcst
------ ----- ------- ------- ------- ------- ------- -------
   769  1/1    0.00%   0.00%   7.69%  92.30%   0.00%   0.00%
   769  2/1    0.00%   0.00%  92.31%   7.70%   0.00%   0.00%
Console> (enable)
```

IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングの設定

この章では、Catalyst 6500 シリーズ スイッチ上で IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングを設定する手順について説明します。

この章で説明する内容は、次のとおりです。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

802.1Q トンネリングの機能概要

サービス プロバイダーは、802.1Q トンネリングを使用することにより、複数の VLAN（仮想 LAN）を持つ顧客に 1 つの VLAN で対応し、顧客の VLAN ID を維持して、各顧客 VLAN のトラフィックを分離することができます。

802.1Q トンネリングをサポートするように設定されたポートをトンネル ポートといいます。トンネリングを設定する場合は、トンネリング用に使用する VLAN にトンネル ポートを割り当てます。顧客のトラフィックの分離を維持するためには、顧客ごとに個別の VLAN が 1 つ必要ですが、その 1 つの VLAN で各顧客のすべての VLAN に対応できます。

802.1Q トンネリングでは、タグ付けされたトラフィックが顧客の装置の 802.1Q トランク ポートから送信され、トンネル ポートを通じてスイッチに着信します。顧客の装置上の 802.1Q トランク ポートとトンネル ポートの間のリンクを非対称リンクといいます。一方の端は 802.1Q トランク ポートとして設定され、他方の端はトンネル ポートとして設定されているからです。

トンネル ポートは、802.1Q トランク ポートからタグ付きの顧客トラフィックを受信した場合、そのフレーム ヘッダーから 802.1Q タグを取り除くことはありません。トンネル ポートは、802.1Q タグを付けたまま、1 バイトの Ethertype フィールド（0x8100）と 1 バイトの length フィールドを追加したうえで、そのトンネル ポートに割り当てられた VLAN に顧客のトラフィックを渡します。このように、受信した 802.1Q タグが付いた状態の Ethertype 0x8100 トラフィックをトンネル トラフィックといいます。

トンネル トラフィックを伝送する VLAN は、802.1Q トンネルです。VLAN のトンネル ポートはそのトンネルの入口および出口です。

トンネル ポートは同じネットワーク装置上になくてもかまいません。トンネルは、出口のトンネル ポートに到達する前に、他のネットワーク リンクや他のネットワーク装置を通過することができます。また、1 つのトンネルには、そのトンネル経由の通信を必要とする顧客装置をサポートするのに必要なトンネル ポートをいくつでも設定できます。

出口のトンネル ポートは、1 バイトの Ethertype フィールド（0x8100）と 1 バイトの length フィールドを取り除き、802.1Q タグは付けたまま、顧客装置上の 802.1Q トランク ポートにトラフィックを送ります。顧客装置上の 802.1Q トランク ポートは 802.1Q タグを取り除いてから、該当する顧客 VLAN にトラフィックを送ります。

必ずしもすべてのスイッチが標準の 1 バイト Ethertype フィールド（0x8100）をサポートしているわけではありません。ご使用のスイッチが 1 バイト Ethertype フィールドをサポートしていない場合は、GBIC（ギガビット インターフェイス コンバータ）または 10 ギガビット ポートにスイッチを接続して、指定された Ethertype の IP 管理トラフィックからタグ無し IP トラフィックを分離できます。タグ無し IP トラフィックは自動的にネイティブ VLAN に割り当てられ、指定された Ethertype のトラフィックは指定された VLAN に切り替えられます。

802.1Q トンネリングの設定に関する注意事項

ここでは、ネットワークに 802.1Q トンネリングを設定する際の注意事項について説明します。

- トンネルに入る方向とトンネルから出る方向が非対称なリンクを使用します。
- トンネル ポートは必ず、非対称リンクを構築するように設定します。
- 各トンネルに対して専用の VLAN を 1 つ設定します。
- トンネリング用の VLAN にはトンネル ポートだけを割り当てます。
- トランクには、トンネル VLAN の伝送のための特別な設定は必要ありません。
- トンネル ポートのない装置間のトンネル トラフィックの伝送には、ISL（スイッチ間リンク）トランクを使用することを推奨します。802.1Q ネイティブ VLAN 機能のため、802.1Q トランクを使用する場合は、トンネリングの設定に十分注意する必要があります。設定を誤ると、トンネル トラフィックが非トンネル ポートに転送される可能性があります。
- トンネル トラフィックは 802.1Q タグをスイッチ内で維持するので、レイヤ 2 フレームのヘッダー長には、以下の制約があります。
  - レイヤ 2 フレーム内のレイヤ 3 パケットは、識別不可能です。
  - トンネル トラフィックでは、レイヤ 3 以上のパラメータ（レイヤ 3 送信元および宛先アドレスなど）は識別不可能です。
  - トンネル トラフィックはルーティング不可能です。
  - スイッチは、レイヤ 2 パラメータ（VLAN および送信元 / 宛先 MAC [メディア アクセス制御] アドレス）によってのみ、トンネル トラフィックをフィルタリングできます。
  - スイッチはトンネル トラフィックに対し、MAC レイヤ Quality of Service（QoS; サービス品質）だけ提供します。
  - QoS は、802.1Q の 2 バイトの Tag Control Information フィールド内の受信 Class of Service（CoS; サービス クラス）値を検出できません。
- 非対称リンクでは、リンク上にトランク ポートが 1 つしかないので、Dynamic Trunking Protocol（DTP; ダイナミック トランキング プロトコル）はサポートされていません。非対称リンクに 802.1Q トランク ポートを設定するには、**nonegotiate dot1q** トランキング キーワードを使用します。
- 非対称リンク内の 802.1Q トランク ポートのネイティブ VLAN では、トラフィックが伝送されないようにしてください。ネイティブ VLAN のトラフィックにはタグがないので、正しくトンネリングすることができません。別の方法として、グローバル コマンド **set dot1q-all-tagged enable** を使用して、ネイティブ VLAN の出力トラフィックに 802.1Q タグを付けられます。

（注） グローバル **set dot1q-all-tagged enable** コマンドの詳細については、第 5 章「イーサネット VLAN トランクの設定」を参照してください。

- 非対称リンクでは、トンネル ポートの VLAN が 802.1Q トランクのネイティブ VLAN と一致しない場合、Cisco Discovery Protocol（CDP）によってネイティブ VLAN の不一致が報告されます。802.1Q トンネル機能では、VLAN が一致している必要はありません。設定において一致しない VLAN を使用する場合には、このメッセージを無視してください。
- ジャンボ フレームについては、802.1Q タグと合わせたジャンボ フレームの長さが最大フレーム サイズを超えないかぎり、トンネリングが可能です。

（注） Maximum Transmission Unit（MTU; 最大伝送ユニット）の正確なサイズを設定するために、802.1 トンネル トラフィックを伝送するすべてのポート上でジャンボ フレームをイネーブルにする必要があります。

- 次をサポートするように設定したポートには、802.1Q トンネリングを設定できません。
  - プライベート VLAN
  - Voice over IP（VoIP）（Cisco IP Phone 7960）
- 次のレイヤ 2 プロトコルは、非対称リンクで接続された装置間で動作します。
  - CDP
  - UniDirectional Link Detection（UDLD; 単一方向リンク検出）
  - Port Aggregation Protocol（PAgP）
- VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）は、次の装置間では動作しません。
  - 非対称リンクによって接続された装置
  - トンネルを介して通信する装置

（注）EtherChannel を非対称リンクとして設定するには、EtherChannel 内のすべてのポートに同じトンネリング設定を使用する必要があります。レイヤ 2 フレーム内のレイヤ 3 パケットは識別不可能なので、MAC アドレスに基づくフレーム配布を使用するように EtherChannel を設定してください。

- Generic Attribute Registration Protocol（GARP）VLAN Registration Protocol（GVRP）は、トンネルを介して通信する装置間で動作しますが、非対称リンクで接続された装置間では動作しません。
- 相互接続型ネットワークでは、ISP の 2 つの異なるエッジ スイッチへの冗長パスを使用できません。相互接続型ネットワークでは、ISP の同一エッジ スイッチへの冗長パスを使用できますが、カスタマー ネットワークで Per VLAN Spanning-Tree Plus（PVST+）を使用する必要があり、Multi-Instance Spanning-Tree Protocol（MISTP）用または Multiple Spanning-Tree（MST）用に設定することはできません。ISP インフラストラクチャでは、PVST+、MISTP-PVST+ または MST-PVST+ のいずれかを使用する必要があります。

スイッチ上での 802.1Q トンネリングの設定

ここでは、802.1Q トンネルリングの設定手順について説明します。

（注） グローバル **set dot1q-all-tagged enable** コマンドの詳細については、第 5 章「イーサネット VLAN トランクの設定」を参照してください。

802.1Q トンネル ポートの設定

注意 VLAN でトンネリングを設定するときは、設定しているのが該当するトンネル ポートだけであり、トンネルごとに 1 つの VLAN を使用していることを確認してください。VLAN へのトンネル ポートの割り当てを誤ると、トラフィック転送で問題が生じる可能性があります。

ポートに 802.1Q トンネリングを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポートにトンネリングを設定します。	**set port dot1qtunnel** {**all** | *mod/port* **access** | **disable**}
ステップ 2	設定を確認します。	**show port dot1qtunnel** [*mod*[*/port*]]

次に、ポート 4/1 上にトンネリングを設定し、設定を確認する例を示します。

```
Console> (enable) set port dot1qtunnel 4/1 access
Dot1q tunnel feature set to access mode on port 4/1.
Port 4/1 trunk mode set to off.
Console> (enable) show port dot1qtunnel 4/1
Port   Dot1q tunnel mode
-----  -----------------
 4/1   access
```

802.1Q トンネル ポートの解除

ポートから 802.1Q トンネリング サポートを解除するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポートからトンネリングを解除します。	**set port dot1qtunnel** {*mod/port*} **disable**
ステップ 2	設定を確認します。	**show port dot1qtunnel** [*mod*[*/port*]]

次に、ポート 4/1 上のトンネリングを解除し、設定を確認する例を示します。

```
Console> (enable) set port dot1qtunnel 4/1 disable
Dot1q tunnel feature disabled on port 4/1.
Console> (enable) show port dot1qtunnel 4/1
Port   Dot1q tunnel mode
-----  -----------------
 4/1   disabled
```

802.1Q トンネリングのグローバル サポートのディセーブル化

ポートから 802.1Q トンネリングを解除するために必要なコマンドは、**set port dot1qtunnel all disable** だけです。802.1Q トンネリングを解除する場合、**set dot1q-all-tagged disable** コマンドを入力する必要はありません。

スイッチ上での 802.1Q トンネリングのグローバル サポートをディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチ上でトンネリングのグローバル サポートをディセーブルにします。	**set port dot1qtunnel all disable**
ステップ 2	設定を確認します。	**show port dot1qtunnel**

次に、スイッチ上のトンネリング サポートをディセーブルにし、設定を確認する例を示します。

```
Console> (enable) set port dot1qtunnel all disable
Dot1q tunnel feature disabled on all applicable ports.
Console> (enable) show port dot1qtunnel
Port   Dot1q tunnel mode
-----  -----------------
 2/1   disabled
 2/2   disabled
 3/1   disabled
 3/2   disabled
 3/3   disabled
 3/4   disabled
 3/5   disabled
 3/6   disabled
 3/7   disabled
 3/8   disabled
 3/9   disabled
 3/10  disabled
 3/11  disabled
 3/12  disabled
 3/13  disabled
 3/14  disabled
 3/15  disabled
 3/16  disabled
(テキスト出力は省略)
```

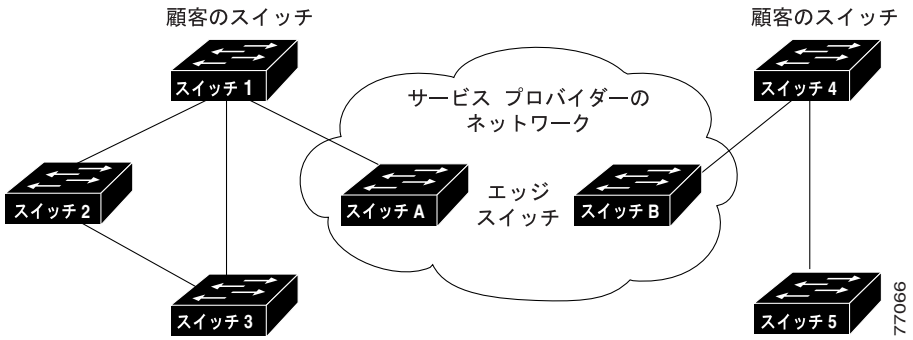
レイヤ 2 プロトコル トンネリングの機能概要

レイヤ 2 プロトコル トンネリングを使用すると、ネットワークを通じて Protocol Data Unit（PDU; プロトコル データ ユニット）（CDP、Spanning-Tree Protocol [STP; スパニングツリー プロトコル]、および VTP）のトンネリングが可能になります。ここで使用する用語の定義をいくつか説明します。

- エッジ スイッチ ― 顧客のスイッチに接続され、サービス プロバイダーのネットワークの境界に配備されているスイッチ（図 7-1 を参照）
- レイヤ 2 プロトコル トンネル ポート ― トンネリング対象の特定のプロトコルのカプセル化やカプセル化解除が可能なエッジ スイッチ上のポート。トンネル ポートは CLI（コマンドライン インターフェイス）コマンドで設定されます。
- トンネリングされた PDU ― CDP、STP、または VTP の PDU

802.1Q トンネリングの現在の実装では、スパニングツリー Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）は、同じエッジ スイッチに属している特別な 802.1Q トンネリング ポートだけにフラッディングされます。この実装は、エッジ スイッチと各サイトの顧客側スイッチの間のループを防ぎます。BPDU は、サービス プロバイダーのネットワーク内のポートのうち、他のサービス プロバイダーのスイッチに接続されているポートにはフラッディングされません。このような BPDU の処理によって、顧客のネットワーク用に異なるスパニングツリー ドメイン（異なるスパニングツリー ルート）が形成されます。たとえば、スイッチ 1（図 7-1 を参照）上の VLAN の STP は、スイッチ 4 および 5 に基づいたコンバージェンス パラメータを考慮することなく、スイッチ 1、2、および 3 上にスパニングツリー トポロジーを構築します。顧客に単一のスパニングツリー ドメインを提供できるようにするため、制御プロトコル PDU（CDP、STP、および VTP）用に BPDU をトンネリングする一般スキームが作成されます。このプロセスをレイヤ 2 プロトコル トンネリングといいます。

図 7-1　レイヤ 2 プロトコル トンネリング ネットワークの設定



レイヤ 2 プロトコル トンネリングは、入口エッジ スイッチで PDU をカプセル化し、それをハードウェアでマルチキャストするソフトウェアによって、PDU トンネリングを実現するスケーラブルな機能です。サービス プロバイダー ネットワーク内のすべてのスイッチは、これらのカプセル化フレームをデータ パケットとして処理し、反対側に転送します。出口のエッジ スイッチは、これらの特殊なカプセル化フレームを待ち受け、カプセル化を解除し、トンネルの外側へ転送します。

カプセル化では、PDU の宛先 MAC アドレスが書き換えられます。入口のエッジ スイッチは、トンネル ポート上で受信された PDU の宛先 MAC アドレスをシスコ独自のマルチキャスト アドレス（01-00-0c-cd-cd-d0）に書き換えます。PDU はそのトンネル ポートのネイティブ VLAN にフラッディングされます。あるポート上でレイヤ 2 プロトコル トンネリングをイネーブルにした場合、イネーブルに設定されたプロトコルの PDU は、送出されません。あるポート上でレイヤ 2 プロトコル トンネリングをディセーブルにした場合、ディセーブルに設定されたプロトコルは、レイヤ 2 プロトコル トンネリングがそのポート上でディセーブルに設定される前と同じように動作します。

レイヤ 2 プロトコル トンネリングの設定に関する注意事項

ここでは、ネットワークにプロトコル トンネリングを設定する際の注意事項について説明します。

- プロトコル トンネリングは、802.1Q トンネリングから独立して機能します。
- パフォーマンス上の理由から、Supervisor Engine 1 が搭載されているシステムにレイヤ 2 プロトコル トンネリングを設定することは推奨できません。
- レイヤ 2 プロトコル トンネリングをイネーブルにできるのは、アクセス ポート、トランク ポート、または 802.1Q トンネリング ポートです。
- レイヤ 2 プロトコル トンネリングをプライベート VLAN と一緒に使用することはできません。
- レイヤ 2 プロトコル トンネリングをダイナミック VLAN と一緒に使用することはできません。
- MST が稼働し、EtherChannel を使用する ISP ネットワークに接続されている場合は、**set spantree link-type** *mod/port* **shared** コマンドを使用して、すべてのチャネリング ポートでリンク タイプを **shared** に設定しなければなりません。このコマンドにより、チャネルの設定の誤りによって EtherChannel が errdisable ステートになるのを防ぐことができます。
- PFC3A の場合、**set rate-limit l2protocol-tunnel** コマンドを入力して、スイッチ上でレイヤ 2 プロトコル トンネル カプセル化 PDU のレート制限をグローバルにイネーブル、ディセーブル、または設定できます。レート制限の設定の詳細については、「スイッチ上でのレイヤ 2 PDU レート制限の設定」（p.8-65）を参照してください。

スイッチ上でのレイヤ 2 プロトコル トンネリングの設定

ここでは、プロトコル トンネリングの設定について説明します。

レイヤ 2 プロトコルの指定

ポートまたはポート範囲上にレイヤ 2 プロトコルを指定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポート上にレイヤ 2 プロトコルを指定します。	**set port l2protocol-tunnel** *mod/port* {**cdp** | **eoam** | **stp** | **vtp**} {**enable** | **disable**}
ステップ 2	設定を確認します。	**show l2protocol-tunnel statistics** [*mod*[*/port*]]

次に、ポート上にレイヤ 2 プロトコルを指定し、設定を確認する例を示します。

（注） 一度に複数のプロトコルを指定することができます。CLI では、各プロトコル タイプをスペースで区切ります。

```
Console> (enable) set port l2protocol-tunnel 3/15 cdp enable
Layer 2 protocol tunneling enabled for CDP on port 3/15.
Port 3/15 trunk mode set to off.

Console> (enable) set port l2protocol-tunnel 3/15 cdp disable
Layer 2 protocol tunneling disabled for CDP on port 3/15.

Console> (enable) set port l2protocol-tunnel 3/15 cdp stp vtp enable
Layer 2 protocol tunneling enabled for CDP STP VTP on port 3/15.
Port 3/15 trunk mode set to off.

Console> (enable) show l2protocol-tunnel statistics 3/15
Tunneling CoS is set to 5.

Port                      CDP Frames Encap     CDP Frames De-encap
------------------------ -------------------- --------------------
 3/15                                   97465                94434

Port                      STP Frames Encap     STP Frames De-encap
------------------------ -------------------- --------------------
 3/15                                   67465                34434

Port                      VTP Frames Encap     VTP Frames De-encap
------------------------ -------------------- --------------------
 3/15                                    1212                 1213
Console> (enable)
```

トランク ポート上のレイヤ 2 プロトコル トンネリングの設定

トランク上でのレイヤ 2 プロトコル トンネリングにより、サービス プロバイダー ネットワーク内でサードパーティ製の機器と Catalyst 6500 シリーズ スイッチを相互運用できます。レイヤ 2 プロトコル トンネリングは、トラフィックがトランク ポートを通過する際に、STP、CDP、および VTP などの制御プロトコル PDU をサービス プロバイダーのネットワークに対してトランスペアレントにします。他社製スイッチとのインターオペラビリティに問題があるため、サードパーティ製のスイッチを使用する場合は、十分な Transparent LAN Service（TLS; 透過型 LAN サービス）を実現したり、802.1Q トンネリングをイネーブルにしたりすることはできません。旧リリースでは、レイヤ 2 プロトコル トンネリングはアクセス ポート上でのみ使用可能でした。

（注） サービス プロバイダーは、レイヤ 2 プロトコル トンネリングがイネーブル化されたトランクに顧客が直接接続できるようにすべきではありません。

「レイヤ 2 プロトコル トンネリングの設定に関する注意事項」（p.7-8）の注意事項に従ってください。また、トランク ポート上に 802.1Q トンネリングを設定できませんが、802 Q トンネリングはトランク ポートを通じてトンネリングすることができます。

（注） 802.1Q トンネリングとレイヤ 2 プロトコル トンネリングの両方を使用した混在ネットワーク環境の場合、サードパーティ製の機器と相互運用するためにパケットを二重にタグ付けする必要があります。

トランク ポートまたはトランク ポート範囲でレイヤ 2 プロトコル トンネリングをイネーブルまたはディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
トランク上でレイヤ 2 プロトコル トンネリングをイネーブルまたはディセーブルにします。	**set l2protocol-tunnel trunk** {**enable** | **disable**}

（注） すでにアクティブなレイヤ 2 プロトコル トンネルが設定されている場合、レイヤ 2 プロトコル トンネリングを設定（イネーブルまたはディセーブル）しないでください。レイヤ 2 プロトコル トンネリングをトランク上に設定する場合は、必ず他のレイヤ 2 プロトコル トンネリング作業を行う前に設定を行ってください。

次に、トランク上でレイヤ 2 プロトコル トンネリングをイネーブルにする例を示します。

```
Console> (enable) set l2protocol-tunnel trunk enable
Layer 2 Protocol Tunnel on trunks is allowed.
Console> (enable)
```

次に、トランク上でレイヤ 2 プロトコル トンネリングをディセーブルにする例を示します。

```
Console> (enable) set l2protocol-tunnel trunk disable
Warning!! Clear any layer 2 protocol tunnel configuration on trunks
before using this command.
Layer 2 Protocol Tunnel on trunks is not allowed.
Console> (enable)
```

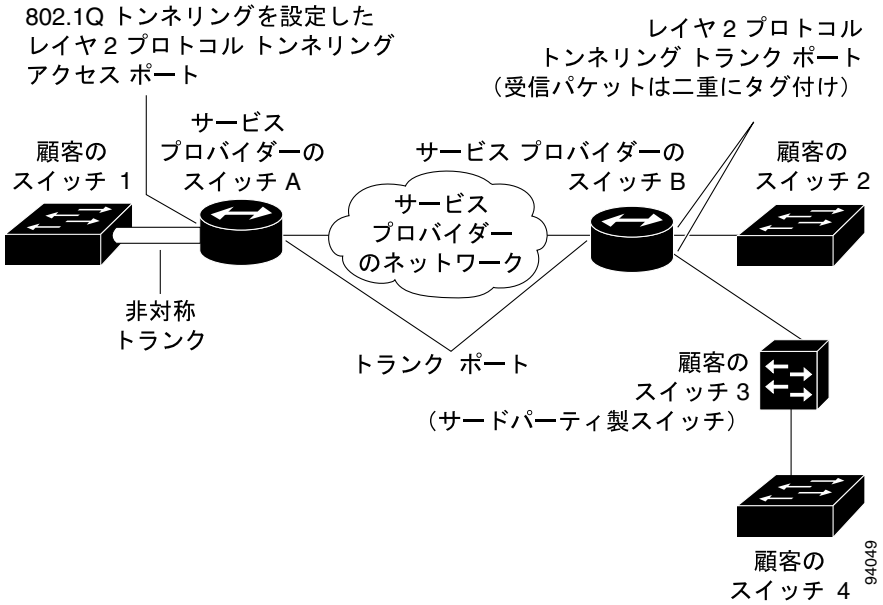
トランク上のレイヤ 2 プロトコル トンネリングの例

図 7-2 の例では、802.1Q トンネリングを設定したレイヤ 2 プロトコル トンネリング ポート（非トランク）、およびレイヤ 2 プロトコル トンネリングを設定した 2 つのトランク ポートを含むサービス プロバイダー ネットワークを示します。

サービス プロバイダー A は、二重タグ付きカプセル化パケットをサービス プロバイダーのネットワークを通じて送信します。パケットは他端で同じ二重タグ付き形式で受信されるものと想定しています。顧客スイッチ 2 と顧客スイッチ 3 が単一タグ付きパケットをサービス プロバイダー B に送信する場合、サービス プロバイダー A の出口で VLAN を特定する方法はありません。しかし、すべてのスイッチが二重タグ付きパケットを送信する場合は、サービス プロバイダー A は出口でそのパケットを正しくトンネリングすることができます。正しい結果を得るには、レイヤ 2 プロトコル トンネリング トランク ポートで受信されるすべてのパケットを二重にタグ付けする必要があります。

もう 1 つの例は、顧客が CDP および VTP パケットをトンネリングする場合です。CDP および VTP パケットは、他のシスコ製スイッチからトンネリングされ、サードパーティ製スイッチから Catalyst 6500 シリーズ スイッチにより受信されます。サービス プロバイダーが複数の顧客をサポートする場合、CDP および VTP パケットをトンネリングする VLAN は VLAN 1 以外にしなければなりません。Catalyst 6500 シリーズ スイッチは VLAN 1 を CDP および VTP パケットの伝送に使用するからです。サードパーティ製のスイッチはレイヤ 2 プロトコル トンネリング トランク ポートに直接接続すべきではないので、サードパーティ製スイッチの 1 つが VLAN 変換または VLAN タギングを行い、パケットが正しい VLAN にトンネリングされるようにする必要があります。

図 7-2　トランク ネットワーク上のレイヤ 2 プロトコル トンネリングの例



レイヤ 2 プロトコル トンネリング ポートに対する廃棄およびシャットダウン スレッシュホールドの指定

シャットダウン スレッシュホールドによって、接続されている顧客のスイッチからのトラフィックがエッジ スイッチの処理能力を超えるのを防ぐためのレート制限のタイプが決まります。レイヤ 2 プロトコル トンネリング ポートと 802.1Q トンネリングを一緒に使用する場合は、常にシャットダウン スレッシュホールドを設定することを推奨します。

シャットダウン スレッシュホールドの最大推奨値は 1000 です。この値は、1 つのエッジ スイッチが入口および出口のトンネリングを実行しながら 1 秒間に（廃棄せずに）処理できる PDU の数に基づいています。エッジ スイッチでは、顧客のスイッチに接続できるレイヤ 2 プロトコル トンネリング ポート数、および各レイヤ 2 プロトコル トンネリング ポートの顧客の VLAN 数も、このシャットダウン スレッシュホールド値によって決まります。推奨最大値を 1000 に決める際には、サービス プロバイダーのネットワークからの出口トンネリングも考慮されました。

レイヤ 2 プロトコル トンネリング ポート（リンク）の数、およびエッジ スイッチが処理できる各レイヤ 2 プロトコル トンネリング ポートの顧客 VLAN 数（各リンクの VLAN）を決定するには、レイヤ 2 プロトコル トンネリング ポートの数に VLAN 数を掛けます。その結果は 1000 以下でなければなりません。次のような設定が可能です。

- レイヤ 2 プロトコル トンネリング ポート 1 個× 1000 VLAN
- レイヤ 2 プロトコル トンネリング ポート 2 個× 500 VLAN
- レイヤ 2 プロトコル トンネリング ポート 5 個× 200 VLAN
- レイヤ 2 プロトコル トンネリング ポート 10 個× 100 VLAN
- レイヤ 2 プロトコル トンネリング ポート 20 個× 50 VLAN
- レイヤ 2 プロトコル トンネリング ポート 100 個× 10 VLAN

（注） シャットダウン スレッシュホールドの数値に達すると、ポートまたはポート範囲は errdisable ステートになり、errdisable タイムアウト時間の経過後に回復します。シャットダウン スレッシュホールドの値は廃棄スレッシュホールド値より大きくなければなりません。廃棄スレッシュホールド値に達したあと、そのポートまたはポート範囲は PDU の廃棄を開始します。

廃棄スレッシュホールドおよびシャットダウン スレッシュホールドのデフォルトは 0 です。値 0 を指定すると、制限は設定されません。

（注） Release8.4(1) 以降のソフトウェア リリースでは、各プロトコルにポート単位で廃棄スレッシュホールドおよびシャットダウン スレッシュホールドを指定できます。スレッシュホールドのみを設定してプロトコルを指定しない場合、パケットはプロトコルに関係なく、累積方式でレートが制限されます。特定のポートの特定のプロトコルにスレッシュホールドを指定すると、パケットは累積方式でレートが制限され、そのあとにプロトコル単位のスレッシュホールドが適用されます。ポート単位のプロトコル廃棄スレッシュホールドおよびシャットダウン スレッシュホールドの範囲は、0 ～ 65535 です。

廃棄およびシャットダウン スレッシュホールドを指定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポート上で廃棄およびシャットダウン スレッシュホールドを指定します。	**set port l2protocol-tunnel** *mod/port* {**drop-threshold** *drop-threshold*} {**shutdown-threshold** *shutdown-threshold*} [**cdp** | **eoam** | **stp** | **vtp**]
ステップ 2	設定を確認します。	**show port l2protocol-tunnel** [*mod*[*/port*]]

次に、ポート上の廃棄スレッシュホールドを 500 に、シャットダウン スレッシュホールドを 1000 に指定する例を示します。

```
Console> (enable) set port l2protocol-tunnel 3/15 drop-threshold 500
shutdown-threshold 1000
Drop Threshold=500, Shutdown Threshold=1000 set on port 3/15.
Console> (enable)
```

次に、ポート上の CDP パケットの廃棄スレッシュホールドを 100 に、シャットダウン スレッシュホールドを 400 に指定する例を示します。

```
Console> (enable) set port l2protocol-tunnel 3/1 drop-threshold 200 shutdown-threshold
400 cdp
Drop Threshold=200, Shutdown Threshold=400 set on port 3/1.
Console> (enable)

Console> (enable) show port l2protocol-tunnel 3/15
Port                      Tunnel Protocol(s) Drop Threshold Shutdown Threshold
------------------------ ------------------ -------------- ------------------
 3/15                     None                          500               1000

Port                 CDP       CDP       STP       STP       VTP       VTP
                     Drop      Shutdown  Drop      Shutdown  Drop      Shutdown
                     Threshold Threshold Threshold Threshold Threshold Threshold
-------------------- --------- --------- --------- --------- --------- ---------
 3/15                        0         0         0         0         0         0
Console> (enable)
Console> (enable) show port l2protocol-tunnel 3/1
Port                      Tunnel Protocol(s) Drop Threshold Shutdown Threshold
------------------------ ------------------ -------------- ------------------
 3/1                      None                           0                   0

Port                 CDP       CDP       STP       STP       VTP       VTP
                     Drop      Shutdown  Drop      Shutdown  Drop      Shutdown
                     Threshold Threshold Threshold Threshold Threshold Threshold
-------------------- --------- --------- --------- --------- --------- ---------
 3/1                       200       400         0         0         0         0
Console> (enable)
```

レイヤ 2 プロトコル トンネリング ポート上での CoS の指定

すべての入口レイヤ 2 プロトコル トンネリング ポート上でグローバルに CoS 値を指定することもできます。CoS 値はすべての入口トンネリング ポートに適用されるので、スイッチによって送出されたカプセル化 PDU の CoS 値はすべて同じになります。有効な値は 0 ～ 7 で、デフォルトの CoS 値は 5 です。

すべての入口レイヤ 2 プロトコル トンネリング ポート上でグローバルに CoS 値を指定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	CoS 値をグローバルに指定します。	**set l2protocol-tunnel cos** *cos-value*
ステップ 2	設定を確認します。	**show l2protocol-tunnel statistics** [*mod*[*/port*]]

次に、CoS 値を 6 に設定する例を示します。

```
Console> (enable) set l2protocol-tunnel cos 6
New CoS value is 6.
Console> (enable)

Console> (enable) show l2protocol-tunnel statistics 4/1
Tunneling CoS is set to 6.
Port  CDP Frames Encap     CDP Frames De-encap
----- -------------------- --------------------
 4/1                 97465                94434
.
.
.
Console> (enable)

Console> (enable) clear l2protocol-tunnel cos
Default Cos set to 5.
Console> (enable)
```

レイヤ 2 プロトコル トンネリング統計情報の消去

1 つのポートまたはすべてのトンネリング ポート上でレイヤ 2 プロトコル トンネリング統計情報を消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
レイヤ 2 トンネル ポートの統計情報を消去します。	**clear l2protocol-tunnel statistics** [*mod/port*]

次に、ポート 7/1 上でレイヤ 2 トンネル ポート統計情報を消去する例を示します。

```
Console> (enable) clear l2protocol-tunnel statistics 7/1
Layer 2 Protocol Tunnel statistics cleared on ports: 7/1.
Console> (enable)
```

CHAPTER 8

スパニングツリーの設定

この章では、IEEE 802.1D ブリッジ Spanning-Tree Protocol（STP; スパニングツリー プロトコル）と、Catalyst 6500 シリーズ スイッチ上でのシスコ独自の STP である Per VLAN Spanning-Tree Plus（PVST+）、および Multi-Instance Spanning-Tree Protocol（MISTP）の使用方法と設定手順を説明します。

(注) スパニングツリー PortFast、UplinkFast、および BackboneFast 機能の設定については、第 9 章「スパニングツリー PortFast、UplinkFast、BackboneFast、およびループ ガードの設定」を参照してください。

この章で説明する内容は、次のとおりです。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

STP の機能概要

ここでは、すべての STP に共通する機能について説明します。シスコ独自の STP である PVST+ および MISTP は、IEEE 802.1D STP に基づいています（詳細については、「PVST+ および MISTP モードの機能」[p.8-13] を参照）。802.1D STP は、不要なループを排除しつつネットワーク内でパスの冗長性を実現するレイヤ 2 管理プロトコルです。STP はすべて、ネットワーク上で最良のループフリー パスを算出するアルゴリズムを使用しています。

STP は分散アルゴリズムを使用します。分散アルゴリズムでは、冗長接続ネットワークのブリッジの 1 つを、スパニングツリー接続したアクティブ トポロジーのルートとして選択します。STP は、アクティブ トポロジー内でのポートの機能に応じて、各ポートに役割を割り当てます。ポートの役割には、次のものがあります。

- ルート ― スパニングツリー トポロジー用に選定された転送ポート
- 指定 ― すべてのスイッチド LAN セグメント用に選定された転送ポート
- 代替 ― スパニングツリーのルート ポートへの代替パスとなるブロック ポート
- バックアップ ― ループバック設定のブロック ポート

このような役割が割り当てられたポートを持つスイッチをルート スイッチまたは指定スイッチと呼びます。詳細については、「ルート スイッチにする方法」（p.8-3）を参照してください。

イーサネット ネットワークでは、任意の 2 つのステーション間に存在するアクティブ パスは 1 つだけです。ステーション間に複数のアクティブ パスがあると、ネットワーク内でループが発生する原因になります。ループが発生すると、一部のスイッチは自身の両側のステーションを認識します。これにより、転送アルゴリズムが正しく機能せず、フレームが重複して転送されます。

スパニングツリー アルゴリズムは、拡張ネットワークのすべてのスイッチにまたがるツリーを定義したあと、特定の冗長データ パスを強制的にスタンバイ（ブロック）ステートにすることにより、パスの冗長性を提供します。ネットワーク上のスイッチは、スパニングツリー パケットを定期的に送受信し、それによってパスを識別します。STP 内の 1 つのネットワーク セグメントが到達不能になるか、またはスパニングツリー コストが変化した場合、スパニングツリー アルゴリズムはスパニングツリー トポロジーを再設定し、スタンバイ パスをアクティブにすることによって、リンクを再度確立します。

スパニングツリーの動作はトランスペアレントなので、エンド ステーションが特定の LAN セグメントに接続されているのか、それとも複数セグメントからなるスイッチド LAN に接続されているのかを、エンド ステーションが検出することはできません。

ここでは、STP について説明します。

トポロジーの作成方法

スパニングツリーを構成する拡張 LAN 上のすべてのスイッチは、データ メッセージを交換することにより、ネットワーク上の他のスイッチに関する情報を収集します。このメッセージは、Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）と呼ばれます。このメッセージ交換により、次の作業が行われます。

- スパニングツリー ネットワーク トポロジーに固有のルート スイッチが選定されます。
- スイッチド LAN セグメントごとに 1 つずつ、指定スイッチが選定されます。
- 冗長スイッチ ポートをバックアップ ステートにすることにより、スイッチド ネットワーク上のループが排除されます。スイッチド ネットワーク内のどの場所からでも、ルート スイッチに到達するために必要でないパスは、すべて STP ブロック モードになります。

アクティブなスイッチド ネットワークのトポロジーは、次の要素によって決まります。

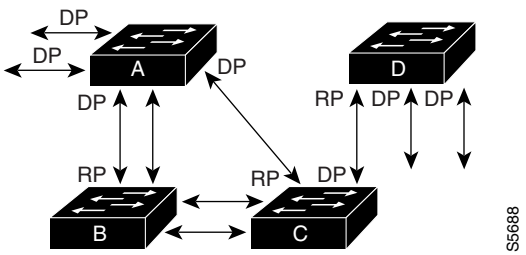
- 各スイッチに対応付けられた、一意のスイッチ ID（スイッチの MAC［メディア アクセス制御］アドレス）
- 各スイッチ ポートに対応付けられたルートに対するパス コスト
- 各スイッチ ポートに対応付けられたポート ID（ポートの MAC アドレス）

スイッチド ネットワークでは、論理上、ルート スイッチがスパニングツリー トポロジーの中心です。STP は BPDU を使用して、スイッチド ネットワーク用のルート スイッチおよびルート ポートを選定し、さらに、各スイッチド セグメントのルート ポートおよび Designated Port（DP; 指定ポート）を選定します。

ルート スイッチにする方法

すべてのスイッチがデフォルトの設定でイネーブルになっている場合は、ネットワーク内で最小 MAC アドレスを持つスイッチがルート スイッチになります。図 8-1 では、スイッチ A が最小 MAC アドレスを持っているのでルート スイッチです。ただし、トラフィック パターン、転送ポートの数、または回線タイプによっては、スイッチ A が最適なルート スイッチとは限りません。最適なスイッチのプライオリティを上げる（プライオリティの数値を下げる）ことにより、そのスイッチを強制的にルート スイッチにすることができます。この操作によって、スパニングツリーはトポロジーを再計算し、選択されたスイッチをルート スイッチにします。

図 8-1　ループフリー トポロジーの設定



RP = ルート ポート
DP = 指定ポート

ポートのプライオリティを変更して、そのポートをルート ポートにすることができます。スパニングツリー トポロジーがデフォルトのパラメータに基づいて算出された場合、スイッチド ネットワーク上の送信元ステーションから宛先ステーションまでのパスが最適とは限りません。また、現在のルート ポートより数字の大きいポートに、より高速のリンクを接続した場合、ルート ポートの変更が必要になる場合があります。最高速のリンクをルート ポートにすることが重要です。

たとえば、スイッチ B のあるポートが光ファイバ リンクで、スイッチ B の別のポート（Unshielded Twisted-Pair［UTP; シールドなしツイストペア］リンク）がルート ポートであるとします。ネットワーク トラフィックは高速の光ファイバ リンクに伝送する方が効率的です。光ファイバ ポートのポート プライオリティ パラメータを UTP ポートより高いプライオリティに変更すると（数値を下げると）、光ファイバ ポートがルート ポートになります。光ファイバ ポートのポート コスト パラメータを UTP ポートより低い値に変更しても同じ結果になります。

BPDU の機能概要

BPDU には、送信側スイッチおよびそのポートについて、MAC アドレス、スイッチのプライオリティ、ポートのプライオリティ、ポート コストなどの設定情報が含まれます。各コンフィギュレーション BPDU に含まれる情報は、次のとおりです。

- 送信側スイッチがルート スイッチとみなしているスイッチの固有の ID
- 送信側ポートからルートへのパスのコスト
- 送信側ポートの ID

スイッチはコンフィギュレーション BPDU を送って通信し、スパニングツリー トポロジーを計算します。BPDU を伝送する MAC フレームは、宛先アドレス フィールドにスイッチ グループ アドレスを送信します。フレームの送信先 LAN に接続されたすべてのスイッチが、その BPDU を受信します。BPDU はスイッチによって直接転送されるわけではありません。受信側のスイッチが、フレームに含まれている情報を使用して BPDU を計算し、トポロジーが変化した時点で BPDU 送信を開始します。

BPDU 交換によって次の作業が行われます。

- 1 台のスイッチがルート スイッチとして選定されます。
- スイッチごとに、ルート スイッチまでの最短距離が計算されます。
- 指定スイッチが選択されます。これは、ルート スイッチに最も近いスイッチであり、このスイッチを経由してフレームがルートへ転送されます。
- 各スイッチのポートが選択されます。スイッチからルート スイッチまでの最適パスを提供するポートです。
- STP に含まれているポートが選択されます。

ポート コストの計算および割り当て

スイッチ ポートのポート コストを計算して割り当てることで、確実に最短距離（つまり最低コスト）でデータをルート スイッチまで送信できます。広帯域幅のポートに対して低いパス コスト値（ポート コスト）を計算して割り当てられます。これには、ショート法（デフォルト）またはロング法を使用します。ショート法は、1 ～ 65535 の値を与える 16 ビット形式を使用します。ロング法は、1 ～ 200,000,000 の範囲の値を与える 32 ビット形式を使用します。デフォルトのコスト モード設定の詳細については、「PVST+ のデフォルト ポート コスト モードの設定」（p.8-31）を参照してください。

（注） ネットワーク内のすべてのスイッチで、同じポート コストの計算方法を使用してください。ロング法の使用を指定しない場合、ポート コストの計算にはショート法が使用されます。計算方法は CLI（コマンドライン インターフェイス）を使用して指定できます。

ショート法を使用したポート コストの計算

IEEE 802.1D 仕様では、帯域幅に基づいて各ポートに 16 ビット（ショート）のデフォルト ポート コスト値を割り当てます。ポート コストは、1 ～ 65535 の範囲で手動で割り当てることもできます。16 ビット値は、ポート コストが特に設定されていないポートにのみ使用します。表 8-1 に、ショート法をポート コスト計算に使用した場合に各タイプのポートに対してスイッチが割り当てるデフォルトのポート コスト値を示します。

表 8-1　ショート法を使用したデフォルトのポート コスト値

ポート速度	デフォルトのコスト値	デフォルトの範囲
10 Mbps	100	1 ～ 65,535
100 Mbps	19	1 ～ 65,535
1 Gbps	4	1 ～ 65,535

ロング法を使用したポート コストの計算

802.1t では、ポートの帯域幅に基づいた公式を使用して各ポートに 32 ビット（ロング）のデフォルト ポート コスト値を割り当てます。ポート コストは、1 ～ 200,000,000 の範囲で手動で割り当てることもできます。デフォルトの 32 ビット ポート コスト取得用の公式では、ポートの帯域幅を 200,000,000 で割ります。表 8-2 に、ロング法をポート コスト計算に使用した場合に、各タイプのポートに対してスイッチが割り当てるデフォルトのポート コスト値、および推奨するコスト値と範囲を示します。

表 8-2　ロング法を使用したデフォルトのポート コスト値

ポート速度	推奨値	推奨範囲	使用可能範囲
≤100 Kbps	200000000	20000000 ～ 200000000	1 ～ 200000000
1 Mbps	20000000	2000000 ～ 200000000	1 ～ 200000000
10 Mbps	2000000	200000 ～ 20000000	1 ～ 200000000
100 Mbps	200000	20000 ～ 2000000	1 ～ 200000000
1 Gbps	20000	2000 ～ 200000	1 ～ 200000000
10 Gbps	2000	200 ～ 20000	1 ～ 200000000

集約リンクのポート コストの計算

集約リンク（ポート バンドル）に対して個々のリンクを追加したり削除したりするため、集約リンクの帯域幅は増減します。帯域幅が変化すると、集約ポートのデフォルトのポート コストを再計算することになります。デフォルトのポート コストが変更されたり、リンクで帯域幅を自動ネゴシエーションすることでポート コストが変更されたりすると、スパニングツリー トポロジーが再計算されます。トポロジーの再計算は、特にリンクの追加や削除が集約リンクの帯域幅にほとんど関係しない場合（たとえば、10 Mbps リンクが 10 Gbps 集約リンクから削除される場合）、望ましいことではありません。トポロジーの自動再計算による制限のため、802.1t では帯域幅の変化によりポートのコストが変化しないようになっています。集約ポートではスタンドアロン ポートと同じポート コスト パラメータを使用します。

スパニングツリー ポート ステート

リンクの確立または切断（障害）に伴い、スイッチド ネットワークのトポロジーが変化する場合があります。スイッチ ポートがトポロジーに含まれていない状態からフォワーディング ステートに直接移行した場合には、一時的にデータ ループが形成されることがあります。ポートは新しいトポロジー情報が LAN 上のスイッチから伝播されるまで待機し、それからフレーム転送を開始しなければなりません。さらに、古いトポロジーで転送されたフレームについて、フレーム存続時間が経過するまで待機する必要があります。

（注）Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）で Cisco IOS Release 12.1.(1)E 以降のリリースを使用する場合、STP Topology Change Notification（TCN; トポロジー変更通知）機能の Address Resolution Protocol（ARP; アドレス解決プロトコル）により、MSFC がスーパバイザ エンジンから TCN を受信したときに、余分なフラッディングが発生しなくなります。この機能によって、MSFC は TCN を受信した VLAN（仮想 LAN）インターフェイスに属するすべての ARP エントリについて、ARP 要求を送信します。ARP 応答が戻ると、Policy Feature Card（PFC; ポリシー フィーチャ カード）はトポロジー変更の結果として消去された MAC エントリを学習します。トポロジーが変化した直後にエントリを学習することで、あとの段階での余分なフラッディングが防止されます。MSFC 上での設定作業は必要ありません。この機能はスーパバイザ エンジン Release 5.4(2) 以降のソフトウェア リリースで動作します。

STP を使用するスイッチ上の各ポートは、次の 5 種類のステートのいずれかになります。

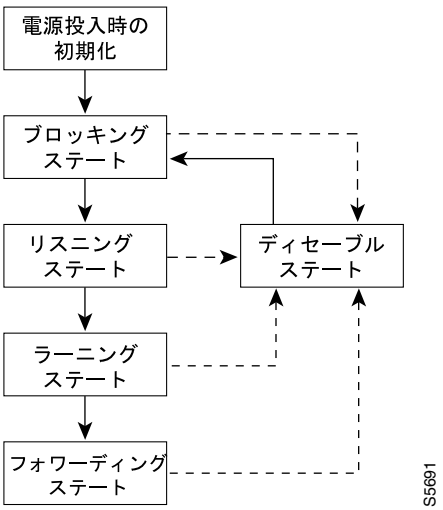
- ブロッキング
- リスニング
- ラーニング
- フォワーディング
- ディセーブル

ポートはこれらのステートを次のように移行します。

- 初期化からブロッキング
- ブロッキングからリスニングまたはディセーブル
- リスニングからラーニングまたはディセーブル
- ラーニングからフォワーディングまたはディセーブル
- フォワーディングからディセーブル

図 8-2 に、ポートがこれらのステートをどのように移行するかを示します。

図 8-2　STP のポート ステート



VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）などの管理ソフトウェアを使用して、各ポート ステートを変更できます。スパニングツリーをイネーブルにすると、ネットワーク上の各スイッチは電源投入時に、必ずブロッキング ステートからリスニングおよびラーニングという移行ステートを通過します。設定が適切であれば、ポートはその後、フォワーディング ステートまたはブロッキング ステートで安定します。

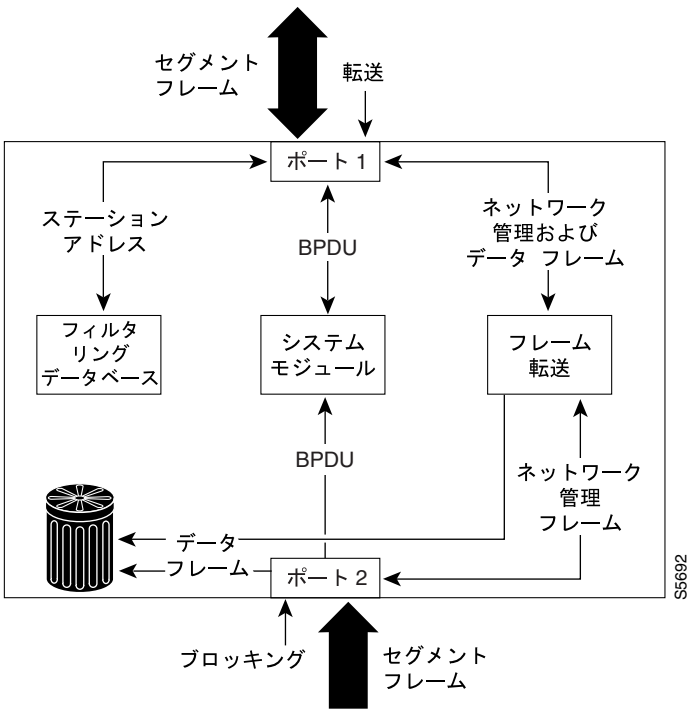
スパニングツリー アルゴリズムによってポートがフォワーディング ステートに移行するプロセスは、次のようになります。

- ポートがリスニング ステートになり、ブロッキング ステートになることを示唆するプロトコル情報を待ち受けます。
- ポートがプロトコル タイマーの満了を待機します。その時点でポートはラーニング ステートになります。
- ラーニング ステートで、ポートは転送データベースに関するステーション ロケーション情報を学習しながら、フレーム転送を引き続きブロックします。
- プロトコル タイマーが満了すると、ポートはフォワーディング ステートに移行し、ラーニングとフォワーディングの両方がイネーブルになります。

ブロッキング ステート

ブロッキング ステートのポートは、フレームの転送に参加しません（図 8-3 を参照）。初期化後、スイッチの各ポートに BPDU が送信されます。スイッチは最初、他のスイッチと BPDU を交換するまでは、スイッチ自身をルートとみなします。この BPDU 交換により、ネットワーク上のどのスイッチが実際のルートであるかが確立されます。ネットワークにスイッチが 1 台しか存在しない場合は、BPDU 交換は行われず、転送遅延タイマーが満了し、ポートはリスニング ステートに移行します。スイッチの初期化後、スイッチは必ずブロッキング ステートになります。

図 8-3　ブロッキング ステートのポート 2



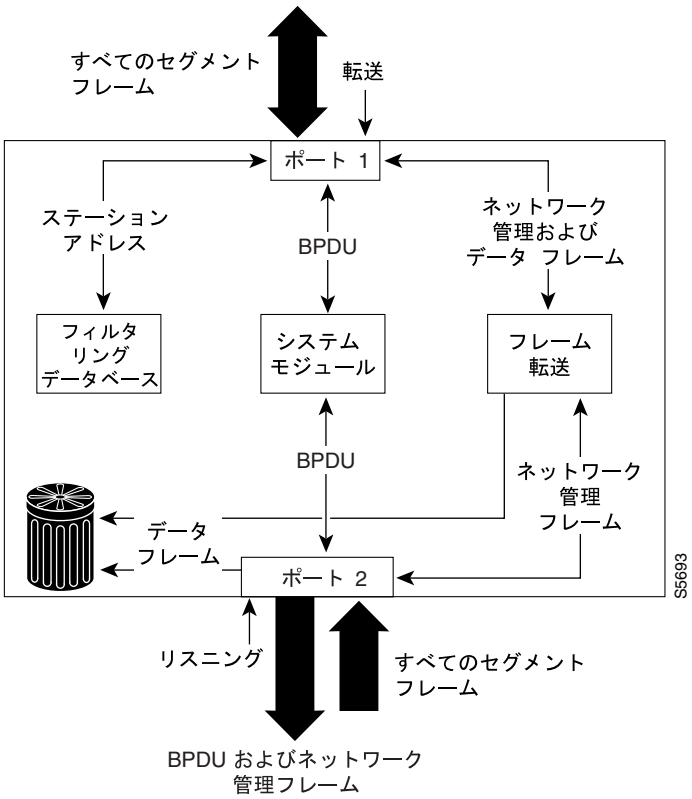
ブロッキング ステートのポートの動作は、次のとおりです。

- 接続セグメントから受信したフレームを廃棄します。
- 転送用に他のポートからスイッチングされたフレームを廃棄します。
- ステーション ロケーションを自分のアドレス データベースに組み込みません（ブロッキング ポートでのラーニングがないため、アドレス データベースのアップデートはありません）。
- BPDU を受信し、それをシステム モジュールに転送します。
- システム モジュールから受信した BPDU を送信しません。
- ネットワーク管理メッセージを受信して応答します。

リスニング ステート

リスニング ステートは、ポートがブロッキング ステートを経て最初に開始する移行ステートです。ポートがリスニング ステートになるのは、スパニングツリーがそのポートをフレーム転送に参加させることを決定した場合です。リスニング ステートでは、ラーニングはディセーブルになります。図 8-4 に、リスニング ステートのポートを示します。

図 8-4　リスニング ステートのポート 2



リスニング ステートのポートの動作は、次のとおりです。

- 接続セグメントから受信したフレームを廃棄します。
- 転送用に他のポートからスイッチングされたフレームを廃棄します。
- ステーション ロケーションを自分のアドレス データベースに組み込みません（この時点ではラーニングがないため、アドレス データベースのアップデートはありません）。
- BPDU を受信し、それをシステム モジュールに転送します。
- システム モジュールから受信した BPDU を処理します。
- ネットワーク管理メッセージを受信して応答します。

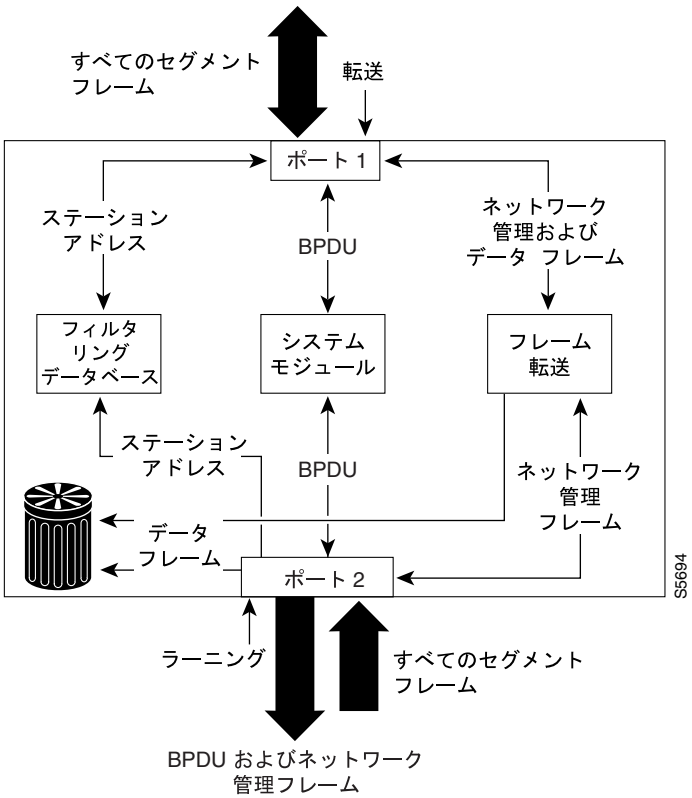
ラーニング ステート

ラーニング ステートのポートは、フレーム転送に参加するための準備をします。ポートは、リスニング ステートからラーニング ステートに移ります。図 8-5 に、ラーニング ステートのポートを示します。

ラーニング ステートのポートの動作は、次のとおりです。

- 接続セグメントから受信したフレームを廃棄します。
- 転送用に他のポートからスイッチングされたフレームを廃棄します。
- ステーション ロケーションを自分のアドレス データベースに組み込みます。
- BPDU を受信し、それをシステム モジュールに転送します。
- システム モジュールから送られた BPDU を受信し、処理して送信します。
- ネットワーク管理メッセージを受信して応答します。

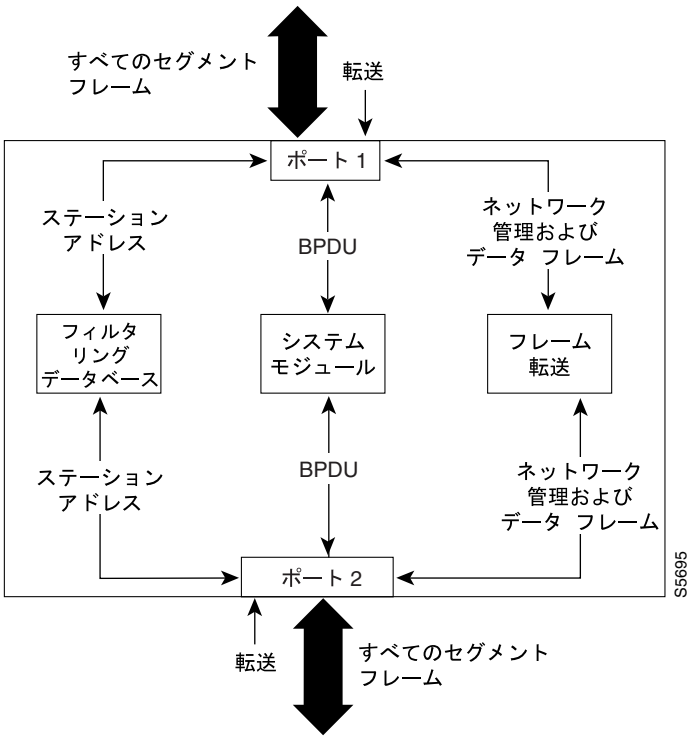
図 8-5　ラーニング ステートのポート 2



フォワーディング ステート

フォワーディング ステートのポートは、フレームを転送します（図 8-6 を参照）。ポートは、ラーニング ステートからフォワーディング ステートに移ります。

図 8-6　フォワーディング ステートのポート 2



フォワーディング ステートのポートの動作は、次のとおりです。

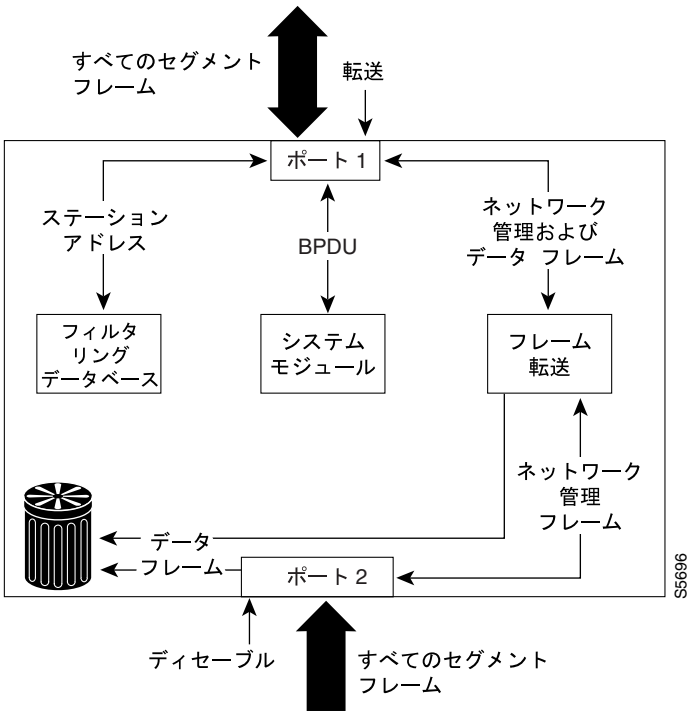
- 接続セグメントから受信したフレームを転送します。
- 転送用に他のポートからスイッチングされたフレームを転送します。
- ステーション ロケーション情報を自分のアドレス データベースに組み込みます。
- BPDU を受信し、それをシステム モジュールに転送します。
- システム モジュールから受信した BPDU を処理します。
- ネットワーク管理メッセージを受信して応答します。

注意　個々のワークステーションに直接接続したポート上でのみ、それらのポートがスパニングツリーの初期化プロセス全体を経由することなく、起動して直接フォワーディング ステートに移行できるように、スパニングツリー PortFast モードを使用してください。不正なトポロジーを防止するため、スイッチ、またはメッセージを転送するその他の装置に接続するポートでは、スパニングツリーをイネーブルに設定してください。PortFast の詳細については、第 9 章「スパニングツリー PortFast、UplinkFast、BackboneFast、およびループ ガードの設定」を参照してください。

ディセーブル ステート

ディセーブル ステートのポートは、フレーム転送にも STP にも参加しません（図 8-7 を参照）。ディセーブル ステートのポートは、事実上、動作不能です。

図 8-7　ディセーブル ステートのポート 2



ディセーブル ポートの動作は、次のとおりです。

- 接続セグメントから受信したフレームを廃棄します。
- 転送用に他のポートからスイッチングされたフレームを廃棄します。
- ステーション ロケーションを自分のアドレス データベースに組み込みません（ラーニングがないため、アドレス データベースのアップデートはありません）。
- BPDU を受信しますが、システム モジュールへは転送しません。
- システム モジュールから送信用 BPDU を受信しません。
- ネットワーク管理メッセージを受信して応答します。

PVST+ および MISTP モードの機能

Catalyst 6500 シリーズ スイッチでは、IEEE 802.1D 規格に準拠する独自の 2 つのスパニングツリー モードと、これら 2 つのモードを組み合わせたモードが提供されます。

- PVST+
- Rapid PVST+
- MISTP
- MISTP-PVST+（組み合わせのモード）

ここでは、各モードについて概要を説明します。各モードの詳細については、下記を参照してください。

- スイッチ上での PVST+ の設定（p.8-27）
- スイッチ上での MISTP-PVST+ または MISTP の設定（p.8-36）

注意　ネットワークで現在 PVST+ を使用しており、特定のスイッチ上で MISTP を使用する場合は、ネットワーク上でのループ発生を防ぐため、最初にそのスイッチ上で MISTP-PVST+ をイネーブルにしてから、MISTP インスタンスを設定してください。

PVST+ モード

PVST+ はスイッチ上の各 VLAN で動作し、各 VLAN にネットワーク上でのループフリー パスを確保します。

PVST+ は、対象となる VLAN に対するレイヤ 2 ロードバランシングを提供しています。これにより、リンクがすべて使用され、かつ特定のリンクがオーバーサブスクライブされないように、ネットワーク上の VLAN を使用してさまざまな論理トポロジーを作成できます。

VLAN 上の PVST+ の各インスタンスには、それぞれ 1 つのルート スイッチがあります。このルート スイッチは、その VLAN に対応するスパニングツリー情報を、ネットワーク上の他のすべてのスイッチに伝送します。このプロセスにより、各スイッチがネットワークに関する共通の知識を持つようになるので、ネットワーク トポロジーが確実に維持されます。

Rapid PVST+

Release 8.1(1) 以降のソフトウェア リリースでは、Rapid PVST+ が Catalyst 6500 シリーズ スイッチ上のすべてのイーサネット、ファスト イーサネット、およびギガビット イーサネット ポートベース VLAN で使用されるデフォルトのスパニングツリー プロトコルになります。Rapid PVST+ は PVST+ と似ていますが、唯一の違いは、Rapid PVST+ では 802.1D ではなく IEEE 802.1w をベースにした Rapid STP を使用している点です。Rapid PVST+ では、PVST+ と同じ設定に最小限の追加設定を行っています。詳細については、「スイッチ上での Rapid PVST+ の設定」（p.8-34）を参照してください。Rapid PVST+ では、トポロジーの変更が行われると、ポート単位でダイナミック CAM（連想メモリ）エントリがただちにフラッシュされます。UplinkFast と BackboneFast がイネーブルに設定されていても、このモードではアクティブではありません。RSTP にその機能が組み込まれているからです。Rapid PVST+ は、ブリッジ、ブリッジ ポート、または LAN の障害のあと、迅速に接続を復旧させます。

非ブリッジング装置（ホスト、ルータなど）に接続するポートは、エッジ ポートです。ハブまたはそのハブによって接続された LAN にブリッジがない場合、ハブに接続するポートもエッジ ポートです。エッジ ポートはリンクがアップすると同時に転送を開始できます。Rapid PVST+ の使用中、ホストおよびルータに接続するポートは、エッジ ポートとして明示的に設定する必要があります。

プロトコルの詳細については、「RSTP」（p.8-19）を参照してください。

MISTP モード

MISTP は、Catalyst 6500 シリーズ スイッチ上で動作するオプションの STP です。MISTP では、複数の VLAN を 1 つのスパニングツリー インスタンス（MISTP インスタンス）にまとめることができます。MISTP は、PVST+ によるレイヤ 2 ロードバランシングの利点と、IEEE 802.1Q による低い CPU 負荷とを組み合わせています。

MISTP インスタンスは、一連のブリッジおよびポート パラメータで定義される仮想論理トポロジーです。MISTP インスタンスに VLAN をマッピングすると、仮想論理トポロジーが物理トポロジーになります。各 MISTP インスタンスには、独自のルート スイッチと、各種の転送リンク（各種のブリッジ パラメータおよびポート パラメータ）があります。

各 MISTP インスタンスには、それぞれ 1 つのルート スイッチがあります。このルート スイッチは、そのインスタンスに対応する情報をネットワーク上の他のすべてのスイッチに伝送します。このプロセスにより、各スイッチがネットワークに関して同じ情報を持つようになるので、ネットワークトポロジーが維持されます。

MISTP は、ネットワーク上のピア エンティティと MISTP BPDU を交換することにより、MISTP インスタンスを作成します。MISTP は、PVST+ のような VLAN 単位ではなく、MISTP インスタンスごとに 1 つの BPDU を使用します。MISTP ネットワークでは BPDU の個数が少ないので、MISTP ネットワークはオーバーヘッドが少ない状態で、高速でコンバージェンスが行われます。MISTP は、PVST+ の BPDU を廃棄します。

1 つの MISTP インスタンスに VLAN を何個でもマッピングできますが、VLAN は 1 つの MISTP インスタンスにしかマッピングできません。MISTP トポロジー内の VLAN（複数可）は、コンバージェンスされている場合は、容易に別の MISTP インスタンスに移動できます（ただし、VLAN の移動と同時にポートが追加されている場合は、コンバージェンス時間が必要です）。

MISTP-PVST+ モード

MISTP-PVST+ は、ネットワーク内で PVST+ を使用しているスイッチとの通信を続けながら、Catalyst 6500 シリーズ スイッチ上で MISTP 機能を利用するための移行用スパニングツリー モードです。MISTP モードを使用するスイッチに接続されている PVST+ モードのスイッチは、相手側のスイッチの BPDU を認識しないので、ネットワークでループを引き起こす可能性があります。MISTP-PVST+ は、両方のモードの BPDU を認識するので、PVST+ と純粋な MISTP とのインターオペラビリティが実現されます。ネットワークを MISTP に変換するには、MISTP-PVST+ を使用してネットワークを PVST+ から MISTP に移行します。

MISTP-PVST+ には PVST+ と同じ制限事項が適用されるので、PVST+ スイッチ以上の VLAN ポートを MISTP-PVST+ スイッチで設定することはできません。

ブリッジ ID の機能概要

ここでは、PVST+ および MISTP で MAC アドレスを一意のブリッジ ID として使用する方法について説明します。

MAC アドレスの割り当て

Catalyst 6500 シリーズ スイッチには、PVST+ または MISTP インスタンスの制御下で動作する、VLAN のブリッジ ID として使用できる 1,024 個の MAC アドレスのプールがあります。**show module** コマンドを使用すると、MAC アドレス範囲を調べることができます。

MAC アドレスは順番に割り当てられます。範囲の先頭 MAC アドレスが VLAN 1 に、範囲の 2 番めの MAC アドレスが VLAN 2 に割り当てられます（以下同様）。範囲の最終 MAC アドレスは、スーパバイザ エンジン帯域内（sc0）管理インターフェイスに割り当てられます。

たとえば、MAC アドレス範囲が 00-e0-1e-9b-2e-00 ～ 00-e0-1e-9b-31-ff の場合、VLAN 1 のブリッジ ID は 00-e0-1e-9b-2e-00、VLAN 2 のブリッジ ID は 00-e0-1e-9b-2e-01、VLAN 3 のブリッジ ID は 00-e0-1e-9b-2e-02 になります（以下同様）。帯域内（sc0）インターフェイスの MAC アドレスは 00-e0-1e-9b-31-ff です。

MAC アドレス リダクション

4,096 の VLAN をサポートする Catalyst 6500 シリーズ スイッチの場合、MAC アドレス リダクションによって、PVST+ で稼働する最大 4,096 の VLAN または 16 の MISTP インスタンスが、スイッチで必要な MAC アドレスの数を増やさずに、一意の ID を持つことができます。MAC アドレス リダクションを使用すると、STP で必要な MAC アドレス数が、VLAN または MISTP インスタンスごとに 1 つから、スイッチごとに 1 つへと減少します。ただし、PVST+ で稼働する VLAN と、MISTP-PVST+ または MISTP で稼働する MISTP インスタンスは、論理ブリッジとみなされ、各ブリッジはネットワークで一意の ID を持つ必要があります。

MAC アドレス リダクションをイネーブルにすると、スパニングツリー BPDU に保存されているブリッジ ID には、*システム ID エクステンション*というフィールドが追加されます。ブリッジ プライオリティと統合することで、システム ID エクステンションは VLAN または MISTP インスタンスの一意の ID として機能します。システム ID エクステンションは、常に VLAN または MISTP インスタンスの番号です。たとえば、VLAN 100 のシステム ID エクステンションは 100 であり、MISTP インスタンス 2 のシステム ID エクステンションは 2 です。

図 8-8 に、MAC アドレス リダクションをイネーブルにしない場合のブリッジ ID を示します。ブリッジ ID は、ブリッジ プライオリティおよび MAC アドレスで構成されています。

図 8-8　MAC アドレス リダクションを行わない場合のブリッジ ID

図 8-9 に、MAC アドレス リダクションをイネーブルにした場合のブリッジ ID を示します。ブリッジ ID は、ブリッジ プライオリティ、システム ID エクステンション、および MAC アドレスで構成されています。ブリッジ プライオリティとシステム ID エクステンションの組み合わせを、*ブリッジ ID プライオリティ*といいます。ブリッジ ID プライオリティは、VLAN または MISTP インスタンスに対する一意の ID です。

図 8-9　MAC アドレス リダクションをイネーブルにした場合のブリッジ ID

show spantree コマンドを実行すると、PVST+ モードの VLAN、または MISTP/MISTP-PVST+ モードの MISTP インスタンスのブリッジ ID プライオリティが表示されます。

次に、MAC アドレス リダクションを PVST+ モードでイネーブルにした場合に、VLAN 1 のブリッジ ID プライオリティを表示する例を示します。この VLAN に対する一意の ID は 32769 です。

```
Console> (enable) show spantree 1
VLAN 1
Spanning tree mode          PVST+
Spanning tree type          ieee
  .
  .
  .
Bridge ID MAC ADDR          00-d0-00-4c-18-00
Bridge ID Priority          32769  (bridge priority: 32768, sys ID ext: 1)
Bridge Max Age 20 sec   Hello Time 2  sec   Forward Delay 15 sec
```

ネットワーク上で Catalyst スイッチを使用し、そのスイッチ上で MAC アドレス リダクションをイネーブルにする場合は、不要なルートが選択されたり、スパニングツリー トポロジーに問題が発生したりしないようにするため、他のすべてのレイヤ 2 接続スイッチ上でも MAC アドレス リダクションをイネーブルにする必要があります。

MAC アドレス リダクションがイネーブルの場合、ルート ブリッジ プライオリティは 4096 の倍数に VLAN ID を加えた値になります。この場合に指定できるスイッチ ブリッジ ID（ルート ブリッジ ID を判別するためにスパニングツリー アルゴリズムで使用される ID、最も小さい値を推奨）は、4096 の倍数のみです。0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、および 61440 です。

同じスパニングツリー ドメイン内の別のブリッジで MAC アドレス リダクション機能が稼働していない場合、このブリッジはブリッジ ID をより細かく選択する機能を利用して、ルート ブリッジの所有権を要求し、獲得することができます。

（注） 64 個の MAC アドレスを持つシスコ製スイッチでは、MAC アドレス リダクション機能がデフォルトでイネーブルです（スイッチでサポートされる MAC アドレスの数については、『*Catalyst 6500 Series Switch Release Notes for Software Release 8.x*』を参照してください）。

MST の機能概要

Multiple Spanning-Tree（MST）機能は、IEEE 802.1s のことで、802.1Q に対する修正規格です。MST は 802.1w Rapid Spanning-Tree（RST）アルゴリズムを複数のスパニングツリーに拡張します。この拡張により、VLAN 環境で高速コンバージェンスとロードバランシングの両方が実現します。Release 8.3(1) では、MST プロトコルは IEEE 802.1 に準拠していて、これより以前のソフトウェア リリースに実装されていた 802.1D STP、802.1w、Rapid Spanning-Tree Protocol（RSTP）、および Cisco PVST+ アーキテクチャと下位互換性があります。Release 8.3(1) の MST プロトコルは、以前のソフトウェア リリースの MST と相互運用します。

MST により、VLAN トランクを介して複数のスパニングツリーを設定できます。VLAN をグループに分け、スパニングツリー インスタンスに対応付けることができます。各インスタンスにはスパニングツリー インスタンスから独立したトポロジーがあり、個別のポート インスタンス コストとポート インスタンス プライオリティを持つことができます。このアーキテクチャにより、データトラフィックに複数の転送パスが与えられ、ロードバランシングが可能になります。1 つのインスタンス（転送パス）で障害が発生しても、他のインスタンス（転送パス）は影響を受けないので、ネットワークの耐障害性が向上します。

大規模なネットワークでは、異なる VLAN スパニングツリー インスタンスをネットワークのさまざまな部分に割り当てておくと、管理が容易になり、冗長パスを最適な形で利用できます。ただし、スパニングツリー インスタンスが存在できるのは、互換性のある VLAN インスタンスが割り当てられているブリッジに限られます。したがって、MST の場合、同じ MST コンフィギュレーション情報を使用して一連のブリッジを設定し、それらが特定のスパニングツリー インスタンス セットに参加することができるようにしなければなりません。同じ MST コンフィギュレーションが与えられて相互接続されたブリッジを MST リージョンといいます。

MST では、Multiple Spanning-Tree Protocol（MSTP）という RSTP の修正版を使用します。MST 機能の特性は、次のとおりです。

- MST は、Internal Spanning-Tree（IST）という形式のスパニングツリーを実行します。IST は Common Spanning-Tree（CST）情報に MST リージョンに関する内部情報を加えます。MST リージョンは、Single Spanning-Tree（SST）リージョンおよび MST リージョンに隣接する単一ブリッジとして認識されます。
- MST を実行しているブリッジは、次のように、シングル スパニングツリー ブリッジとのインターオペラビリティがあります。
  - MST ブリッジは、CST 情報に MST リージョンに関する内部情報を加える形式の STP（IST）を実行します。
  - IST はリージョン内のすべての MST ブリッジを接続し、見かけ上はブリッジで結ばれたドメイン全体を取り囲む CST のサブツリーになります。MST リージョンは、SST ブリッジおよび MST リージョンに隣接する仮想ブリッジとして認識されます。
  - 各 MST リージョンにおける IST の集合、MST リージョンを相互接続する CST、および SST ブリッジによって、Common and Internal Spanning-Tree（CIST）を定義します。CIST は、MST リージョンの内部では IST と同じであり、MST リージョンの外部では CST と同じです。STP、RSTP、および MSTP が一緒になって、CIST のルートとして 1 つのブリッジを選定します。
- MST は各 MST リージョン内部で、追加のスパニングツリーを設定して維持します。これらのスパニングツリーを MST Instance（MSTI）といいます。IST の番号は 0 です。MSTI の番号は 1、2、3 のようになります。各 MSTI は MST リージョンに対してローカルであり、MST リージョンが相互接続されている場合も含めて、他のリージョンの MSTI とは無関係です。MSTI は次のように、MST リージョンの境界で IST と結合し、CST になります。
  - MSTI のスパニングツリー情報が MSTP レコード（M レコード）に組み込まれます。

M レコードは必ず、MST BPDU 内部でカプセル化されます（MST BPDU）。MSTP によって計算された最初のスパニングツリーを M ツリーといいます。M ツリーがアクティブなのは、MST リージョンの内部に限られます。M ツリーは MST リージョンの境界で IST とマージされ、CST を形成します。

- MST は非 CST VLAN 用に PVST+ BPDU を生成することによって、PVST+ とのインターオペラビリティを実現します。
- MST は次のように、MSTP の PVST+ 拡張機能の一部をサポートしています。
  - UplinkFast および BackboneFast は、MST モードでは使用できません。これらは RSTP に含まれます。
  - PortFast はサポートされます。
  - BPDU フィルタリングおよび BPDU ガードは MST モードでサポートされています。
  - ループ ガードおよびルート ガードは MST でサポートされています。MST は、VLAN 1 で BPDU が送信中の場合を除き、VLAN 1 ディセーブル機能を維持します。
  - MST スイッチは、MAC リダクションがイネーブルの場合と同様に動作します。
  - プライベート VLAN（PVLAN）の場合、セカンダリ VLAN はプライマリと同じインスタンスにマッピングされます。

MST を使用する場合は、次の注意事項に従ってください。

- いかなる PVST ブリッジのいかなる VLAN でも、スパニングツリーをディセーブルにしないでください。
- すべての PVST スパニングツリー ルート ブリッジに、CST ルート ブリッジより低い（数字上は大きい）プライオリティを与える必要があります。
- PVST ブリッジを CST のルートとして使用しないでください。
- トランクは、インスタンスにマッピングされたすべての　VLAN　を伝送するか、またはどの VLAN もまったく伝送しないかのどちらかでなければなりません。
- アクセス リンクでスイッチを接続しないでください。アクセス リンクは VLAN を分割する可能性があります。
- メンテナンス ウィンドウで、既存または新規の論理 VLAN ポートを大量に組み込んだ MST コンフィギュレーションを実行する必要があります。増分変化（インスタンスへの新規 VLAN の追加やインスタンスにまたがる VLAN の移動など）のため、MST データベース全体が再初期化されるからです。

ここでは、MST について説明します。

RSTP

RSTP を使用すると、物理トポロジーまたはそのコンフィギュレーション パラメータの変更時に、ネットワークのアクティブ トポロジーを再構成する時間が大幅に短縮されます。RSTP はスパニングツリーで接続されたアクティブ トポロジーのルートとして 1 つのスイッチを選択し、そのスイッチの個々のポートに、ポートがアクティブ トポロジーに含まれているかどうかに応じて、役割を割り当てます。

RSTP を使用すると、スイッチ、スイッチ ポート、または LAN で障害が発生した場合でも、高速な接続が可能になります。新しいルート ポートとブリッジの反対側の DP は、明示的なハンドシェークによって、フォワーディングへ移行します。RSTP により、スイッチの再初期化時にポートが直接フォワーディングに移行できるように、スイッチ ポートを設定できます。

802.1w で規定されている RSTP は、802.1D の STP に代わるものですが、STP との互換性は維持されます。RSTP は、MST が動作する構造を提供します。RSTP は MST 機能を設定するときに設定します。詳細については、「スイッチ上での MST の設定」（p.8-55）を参照してください。

RSTP は、次のように、802.1D ブリッジとの下位互換性があります。

- RSTP はポート単位で、802.1D が設定された BPDU および TCN BPDU を選択して送信します。
- ポートの初期化時に、移行遅延タイマーがスタートし、RSTP BPDU が送信されます。移行遅延タイマーがアクティブな間、ブリッジはそのポート上で受信したすべての BPDU を処理します。RSTP BPDU はポート上では認識されません。バージョン 3 の BPDU だけが認識されます。
- ポートの移行遅延タイマーが満了したあとで、ブリッジが 802.1D BPDU を受信した場合、ブリッジはそれが 802.1D ブリッジに接続されているものとみなして、802.1D BPDU だけを使用するようになります。
- RSTP がポート上で 802.1D BPDU を使用していて、移行遅延タイマーの満了後に RSTP BPDU を受信した場合、RSTP は移行遅延タイマーを再びスタートさせ、そのポート上で RSTP BPDU の使用を開始します。

RSTP ポートの役割

RSTP は、ポートの役割として次の定義を使用します。

- ルート ― スパニングツリー トポロジー用に選定された転送ポート。
- 指定 ― すべてのスイッチド LAN セグメント用に選定された転送ポート。
- 代替 ― 現在のルート ポートによって提供されるルート ブリッジへの代替パス。
- バックアップ ― スパニングツリーのリーフに向かって DP が提供するパスのバックアップ。バックアップ ポートが存在できるのは、2 つのポートがポイントツーポイント リンク、または共用 LAN セグメントとの接続が複数あるブリッジによって、ループバックで接続されている場合だけです。
- ディセーブル ― スパニングツリー動作の中で役割が与えられていないポート。

ポートの役割は、次のように割り当てます。

- ルート ポートまたは DP の役割は、アクティブ トポロジーにポートを含めることです。
- 代替ポートまたはバックアップ ポートの役割は、アクティブ トポロジーからポートを除外することです。

RSTP のポート ステート

ポート ステートは、フォワーディングおよびラーニング プロセスを制御し、廃棄、ラーニング、およびフォワーディングの値を提供します。表 8-3 に、STP ポート ステートと RSTP ポート ステートの比較を示します。

表 8-3　STP と RSTP のポート ステートの比較

動作ステータス	STP のポート ステート	RSTP のポート ステート	アクティブ トポロジーへのポートの組み込み
イネーブル	ブロッキング[1]	廃棄[2]	なし
イネーブル	リスニング	廃棄	なし
イネーブル	ラーニング	ラーニング	あり
イネーブル	フォワーディング	フォワーディング	あり
ディセーブル	ディセーブル	廃棄	なし

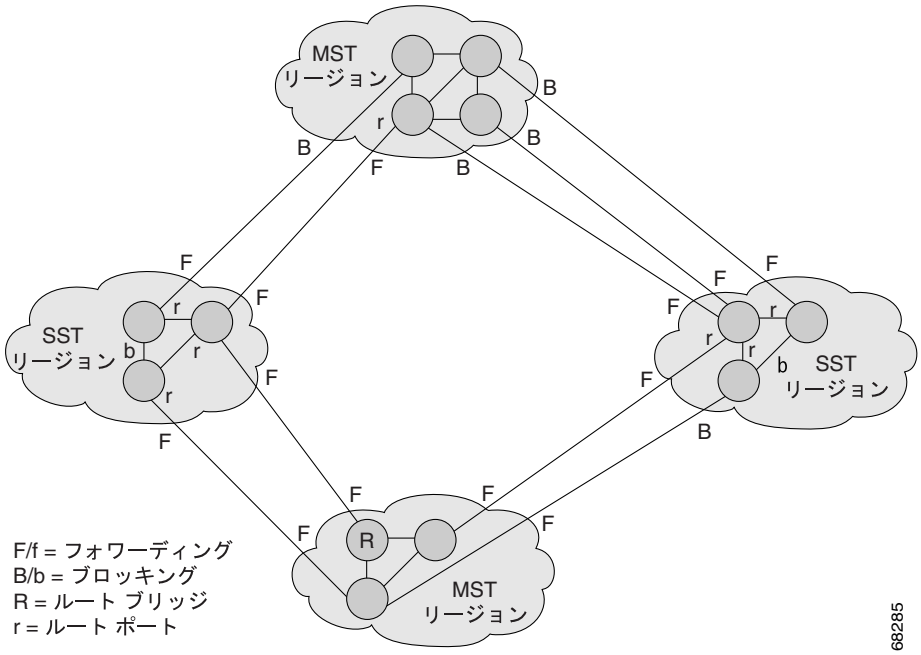
1. IEEE 802.1D のポート ステート指定。
2. IEEE 802.1w のポート ステート指定。廃棄は、MST のブロッキングと同じです。

安定したトポロジーでは、RSTP は各ルート ポートおよび DP がフォワーディングに移行し、すべての代替ポートおよびバックアップ ポートが必ず廃棄ステートになるようにします。

MST と SST のインターオペラビリティ

仮想ブリッジド LAN には、相互接続された SST ブリッジと MST ブリッジのリージョンが含まれることがあります。図 8-10 を参照してください。

図 8-10　SST と MST リージョンが相互接続されているネットワーク



SST リージョンで稼働している STP にとって、MST リージョンは単一 SST または擬似ブリッジとして認識されます。擬似ブリッジは、次のように動作します。

- すべての擬似ブリッジ ポートのすべての BPDU に、ルート ID およびルート パス コストに関して同じ値を設定します。擬似ブリッジは次の点で、単一 SST ブリッジと異なります。
  - 擬似ブリッジ BPDU には異なるブリッジ ID が与えられます。この相違は、ルート ID およびルート コストが同じなので、隣接 SST リージョンの STP 動作には影響を与えません。
  - 擬似ブリッジ ポートから送信された BPDU には、異なるメッセージ エージが与えられていることがあります。メッセージ エージはホップごとに 1 秒ずつ増えるので、メッセージ エージの相違は秒数順に現れます。
- 擬似ブリッジのあるポート（リージョン エッジにあるポート）から別のポートへのデータ トラフィックは、擬似ブリッジ、すなわち MST リージョン内で完全に収まるパスをたどります。
- 異なる VLAN に属するデータ トラフィックは、MST によって設定された MST リージョン内のさまざまなパスをたどります。
- ループは、次のいずれかの方法で防止されます。
  - 境界上のフォワーディング ポートを 1 つだけ許可し、他のすべてのポートをブロックすることによって、該当する擬似ブリッジ ポートをブロックします。
  - SST リージョンのポートをブロックするように、CST パーティションを設定します。
- 擬似ブリッジは単一　SST　ブリッジとは異なります。擬似ブリッジのポートから送信された BPDU には異なるブリッジ ID が与えられるためです。ルート ID およびルート コストは両方のブリッジで同じです。

CST

CST（802.1Q）は、あらゆる VLAN に対応するシングル スパニングツリーです。PVST+ が稼働している Catalyst 6500 シリーズ スイッチでは、VLAN 1 のスパニングツリーが CST に相当します。MST が稼働している Catalyst 6500 シリーズ スイッチでは、IST（インスタンス 0）が CST に相当します。

MSTI

MST は、最大 64 のインスタンスをサポートしています。各スパニングツリー インスタンスは、0 ～ 15 のインスタンス ID で指定します。インスタンス 0 は必須であり、必ず存在します。インスタンス 1 ～ 63 は任意です。

Release 8.3(1) 以降のソフトウェア リリースでは、インスタンス ID の範囲は 0 ～ 4094 です。インスタンス 1 ～ 4094 はオプションです。

MST コンフィギュレーション

MST コンフィギュレーションは次の 3 つの部分からなります。

- 名前 ― MST リージョンを特定する 32 文字のストリング（ヌル埋め込み、ヌルで終了）
- リビジョン番号 ― 現在の MST コンフィギュレーションのリビジョンを特定する、無符号 16 ビット数

（注） MST コンフィギュレーションの一部として必要な場合は、リビジョン番号を設定する必要があります。リビジョン番号は、MST コンフィギュレーションをコミットするたびに、自動的に増えるわけではありません。

- MST コンフィギュレーション テーブル — すべての可能性のある拡張範囲 VLAN を表す 4096 エレメントの配列。エレメント番号 X の値は、VLAN-X がマッピングされたインスタンスを表します。VLAN 0 および VLAN 4095 は使用されず常にインスタンス 0 にマッピングされます。

各バイトを手動で設定する必要があります。SNMP（簡易ネットワーク管理プロトコル）または CLI を使用して設定を実行できます。

MST BPDU には MST コンフィギュレーション ID およびチェックサムが組み込まれます。MST ブリッジが MST BPDU を受け入れるのは、MST BPDU のコンフィギュレーション ID およびチェックサムが、MST ブリッジの MST リージョン コンフィギュレーション ID およびチェックサムと一致した場合だけです。一方の値が異なる場合、その MST BPDU は SST BPDU として扱われます。

コンソールまたは Telnet 接続を介して MST コンフィギュレーションを変更すると、変更をコミットしないままセッションが終了し、編集バッファがロックされます。**set spantree mst config rollback force** コマンドを入力することによって、既存の編集バッファを廃棄し、新しい編集バッファを取得しないかぎり、それ以上のコンフィギュレーションは不可能です。

Release 8.3(1) 以降のソフトウェア リリースでは、MST の VTP モード プライマリ サーバであるスイッチに MST コンフィギュレーションを設定する場合、他のスイッチは MST コンフィギュレーションを受信します。VTP バージョン 3MST 伝播の詳細については、「VTP バージョン 3 の機能概要」（p.10-14）を参照してください。

MST リージョン

同じ MST コンフィギュレーションが与えられて相互接続されたブリッジを MST リージョンといいます。ネットワーク上に存在できる MST リージョンの数に制限はありません。

MST リージョンを形成するために、ブリッジを次のいずれかにすることができます。

- MST リージョンの唯一のメンバーである MST ブリッジ。
- LAN によって相互接続された MST ブリッジ。LAN の指定ブリッジには、MST ブリッジと同じ MST コンフィギュレーションが与えられます。LAN 上のすべてのブリッジが MST BPDU を処理できます。

MST コンフィギュレーションが異なる 2 つの MST リージョンを接続すると、MST リージョンは次の作業を行います。

- ネットワーク上の冗長パス間でのロードバランシング。2 つの MST リージョンが冗長接続されている場合、すべてのトラフィックはネットワークの MST リージョンとの単一接続上を流れます。
- RSTP ハンドシェークによって、リージョン間の高速接続を可能にします。ただし、このハンドシェークは 2 つのブリッジ間の場合ほど高速ではありません。ループを防止するために、リージョン内のすべてのブリッジが他のリージョンとの接続に合意しなければなりません。したがって、一定の遅延が生じます。ネットワークを多数のリージョンに分割することは推奨しません。

Release 8.3(1) 以降のソフトウェア リリースで動作するスイッチは、旧リリースで動作する近接スイッチとは異なるリージョンを形成します。

境界ポート

境界ポートとは、LAN に接続し、その指定ブリッジが SST ブリッジまたは異なる MST コンフィギュレーションのブリッジであるポートです。DP は、STP ブリッジを検出した場合、またはコンフィギュレーションが異なる RST または MST ブリッジから合意メッセージを受信した場合に、境界上にあることを認識します。

境界では、MST ポートの役割は重要ではなく、MST ポート ステートは強制的に IST ポート ステートと同じにされます。ポートに境界フラグが設定されると、MSTP ポートの役割選択メカニズムによって、境界にポートの役割が割り当てられ、さらに IST ポートと同じステートが与えられます。境界上の IST ポートは、バックアップ以外のあらゆる役割を引き受けることができます。

CIST リージョナル ルート

MST リージョンの CIST リージョナル ルートは、ブリッジ ID が最小で、CST ルートに対するパス コストが最も少ないブリッジです。CST のルート ブリッジになった MST ブリッジは、MST リージョンの CIST リージョナル ルートです。CST ルートが MST リージョンの外側にある場合、境界上の MST ブリッジの 1 つが CIST リージョナル ルートとして選択されます。同じリージョンに属する境界上の他のブリッジは、ルートにつながる境界ポートを最終的にブロックします。

リージョン境界の複数のブリッジで、ルートへのパスが同じだった場合は、多少低いブリッジ プライオリティ（多少高いポート プライオリティ番号）を設定することによって、特定のブリッジを CIST リージョナル ルートにすることができます。

リージョン内のルート パス コストおよびメッセージ エージは一定ですが、IST パス コストはホップごとに増え、IST の残りのホップ数は減ります。**show spantree mst** コマンドを入力すると、ブリッジの CIST リージョナル ルート、パス コスト、残りのホップ数に関する情報が表示されます。

エッジ ポート

非ブリッジング装置（ホスト、ルータなど）に接続するポートは、エッジ ポートです。ハブまたはそのハブによって接続された LAN にブリッジがない場合、ハブに接続するポートもエッジ ポートです。エッジ ポートはリンクがアップすると同時に転送を開始できます。

MST の場合、各ホストまたはルータに対応するすべてのポートを設定する必要があります。障害発生後に高速接続を確立するには、中間ブリッジの非エッジ DP をブロックする必要があります。ポートから合意を返すことのできる別のブリッジに接続した場合、ポートはただちに転送を開始します。それ以外の場合、ポートは転送遅延時間が 2 回経過するまで待機して、再び転送を開始する必要があります。MST の使用中、ホストおよびルータに接続するポートは、エッジ ポートとして明示的に設定する必要があります。

（注） エッジ ポートとしてポートを設定するには、そのポートで PortFast をイネーブルにします。**show spantree portfast** *mod/port* コマンドを入力したときに、ポートの指定がエッジだった場合、そのポートも PortFast ポートです。詳細については、第 9 章「スパニングツリー PortFast、UplinkFast、BackboneFast、およびループ ガードの設定」を参照してください。

ポートが BPDU を受信した場合は、誤って設定されないように、PortFast 動作がオフになります。**show spantree mst** *mod/port* コマンドを使用すると、PortFast の設定および動作ステータスを表示できます。

リンク タイプ

高速接続が確立されるのは、ポイントツーポイント リンク上に限られます。ホストまたはルータに対して、ポートを明示的に設定する必要があります。ただし、大部分のネットワークにおけるケーブル接続はこの要件を満たしているので、**set spantree mst link-type** コマンドを入力することによって、すべての全二重リンクをポイントツーポイント リンクとして扱うと、明示的に設定する必要がありません。

メッセージ エージおよびホップ カウント

IST および MSTI は、BPDU に含まれているメッセージ エージおよび最大エージング タイマーの設定値を使用しません。IST および MST は、別個の IP Time to Live（TTL）メカニズムによく似たホップ カウント メカニズムを使用します。最大ホップ カウントを指定して、各 MST ブリッジを設定できます。インスタンスのルート ブリッジは、最大ホップ カウントに等しい残りのホップ カウントとともに BPDU（M レコード）を送信します。BPDU（M レコード）を受信したブリッジは、受信した残りホップ カウントを 1 だけ減らします。これにより、カウントがゼロになった場合、ブリッジは BPDU（M レコード）を廃棄し、そのポートに関して維持されていた情報を期限切れにします。非ルート ブリッジは、少なくなったカウントを残りホップ カウントとして、生成した BPDU（M レコード）で伝播します。

BPDU の RST 部分に含まれているメッセージ エージおよび最大エージング タイマーの設定値は、リージョン内では変わらず、境界に位置するリージョンの DP によって、同じ値が伝播されます。

MST と PVST+ のインターオペラビリティ

ネットワーク全体を範囲として VLAN 1 ～ 100 が設定されている PVST+ スイッチと対話するように、MST スイッチ（すべて同一リージョン内）を設定する場合は、次の注意事項を考慮してください。

- MST リージョン内のすべての VLAN に対応するルートを設定します。境界上の MST スイッチに属するポートは、PVST+ をシミュレートし、すべての VLAN に PVST+ BPDU を送信します。次に、PVST をシミュレートするポートの例を示します。

```
Console> (enable) show spantree mst 3
Spanning tree mode          MST
Instance                    3
VLANs Mapped:               31-40

Designated Root             00-10-7b-bb-2f-00
Designated Root Priority    8195  (root priority:8192, sys ID ext:3)
Designated Root Cost        0          Remaining Hops 20
Designated Root Port        1/0

Bridge ID MAC ADDR          00-10-7b-bb-2f-00
Bridge ID Priority          8195  (bridge priority:8192, sys ID ext:3)

Port                      State         Role Cost     Prio Type
------------------------- ------------- ---- -------- ------------------------
 6/1                      forwarding    BDRY    10000   30 P2P,
Boundary(PVST)
 6/2                      blocking      BDRY    20000   32 P2P,
Boundary(PVST)
```

  PVST+ スイッチ上でループ ガードをイネーブルに設定している場合、MST スイッチの設定が変更されたときに、ポートが loop-inconsistent ステートになる可能性があります。loop-inconsistent ステートを解消するには、PVST+ スイッチ上でループ ガードをいったんディセーブルにしてから、再びイネーブルにする必要があります。

- MST スイッチの PVST+ 側の内側に、一部またはすべての VLAN のルートを配置しないでください。境界上の MST スイッチが DP で、すべてまたは一部の VLAN に対する PVST+ BPDU を受信すると、ルート ガードがポートをブロッキング ステートに設定するからです。低速 CPU で PVST+ を実行するスイッチを、MST 稼働スイッチとして指定しないでください。

PVST+ スイッチを 2 つの異なる MST リージョンに接続すると、PVST+ スイッチからのトポロジー変更が最初の MST リージョンより先へは伝送されません。この場合、トポロジー変更は VLAN が対応付けられているインスタンスで伝播されるだけです。トポロジー変更は最初の MST に対してローカルなままであり、他のリージョンの CAM エントリはフラッシュされません。トポロジー変更が他の MST リージョン全体で認識されるようにするには、VLAN を IST に対応付けるか、またはアクセス リンクを介して PVST+ スイッチを 2 つのリージョンに接続します。

BPDU スキューイングの機能概要

BPDU スキューイングとは、スイッチが BPDU を受信する予想時間と実際にスイッチが BPDU を受信した時間との差です。スキューイングが生じる原因は、次のとおりです。

- スパニングツリー タイマーの経過
- 予期された BPDU をスイッチが受信しなかった場合
- スパニングツリーによるトポロジー変更の検出

スキューにより、BPDU がネットワークに再度フラッディングされ、スパニングツリー トポロジー データベースは最新の状態に維持されます。

ルート スイッチは、設定された Hello タイムごとに BPDU を送信して、その存在をアドバタイズします。非ルート スイッチは、それぞれ設定された時間間隔ごとに BPDU を 1 つ受信して処理します。VLAN はスケジューリングされたとおりに BPDU を受信しないことがあります。設定された時間間隔で VLAN 上で BPDU を受信しなかった場合は、BPDU はスキューされます。

スパニングツリーは、Hello タイム（「Hello タイムの設定」[p.8-52] を参照）を使用してポートからルート スイッチへ接続される時間とその接続が切断される時間を検出します。この機能は、PVST+ と MISTP の両方に適用されます。MISTP では、スキューの検出はインスタンス単位で行われます。

BPDU スキューイングは、ネットワークの非ルート スイッチ上で通常の時間枠内で処理されていない BPDU を検出します。BPDU スキューイングが発生すると、Syslog メッセージが表示されます。Syslog は、PVST+ と MISTP の両方に適用されます。

生成される Syslog メッセージの数は、ネットワークのコンバージェンスとスイッチの CPU 利用率に影響を与えることがあります。報告される Syslog メッセージの数が多いほど、スイッチング プロセスが低速になるので、新しい Syslog メッセージは、すべての VLAN に対する個別のメッセージとしては生成されません。スイッチに対する影響を軽減するため、Syslog メッセージは次のように処理されます。

- 最大エージング タイムの半分で生成されます（「最大エージング タイムの設定」[p.8-53] を参照）。
- 60 秒ごとに 1 つに、レート制限されます。

レイヤ 2 PDU レート制限の機能概要

レート リミッタを使用して近接スイッチから不要な Protocol Data Unit（PDU; プロトコル データ ユニット）または一定の数の PDU を受信しないようにできます。レイヤ 2 PDU レート リミッタは、Catalyst 6500 シリーズ スイッチのハードウェアでサポートされています。このレート リミッタは、Local Target Logic（LTL）インデックスに関してトラフィックを制限します。

最大で 4 つのレート リミッタを設定できます。レート リミッタを設定すると、次の PDU タイプをスイッチ上でグローバルに制限できます。

- スパニングツリー BPDU ― IEEE および Shared Spanning Tree Protocol（SSTP）、Cisco Discovery Protocol（CDP）、Unidirectional Link Detection [UDLD; 単一方向リンク検出]、VTP、および Port Aggregation Protocol（PAgP）
- レイヤ 2 プロトコル トンネルカプセル化 PDU
- 802.1X ポート セキュリティ

次の制限事項は、レート制限をイネーブルにする場合に適用されます。

- ハードウェアベースのレート リミッタは、PFC3A 以上の PFC が搭載された Catalyst 6500 シリーズ スイッチでサポートされています。
- Catalyst 6500 シリーズ スイッチは、truncated モードにはなれません。レート制限をイネーブルにしようとしていて truncated モードの場合、メッセージが表示されます。
- レート　リミッタがイネーブルで、特定のイベントによりシステムが非　truncated　モードから truncated モードに移行した場合、レート制限がディセーブルになりメッセージが表示されます。

スイッチ上での PVST+ の設定

ここでは、イーサネット VLAN 上で PVST+ を設定する手順について説明します。

PVST+ のデフォルト設定

表 8-4 に、PVST+ のデフォルト設定を示します。

表 8-4　PVST+ のデフォルト設定

機能	デフォルト値
VLAN 1	すべてのポートを VLAN 1 に割り当てる
イネーブル ステート	すべての VLAN で PVST+ がイネーブル
MAC アドレス リダクション	ディセーブル
ブリッジ プライオリティ	32768
ブリッジ ID プライオリティ	32769（VLAN 1 のブリッジ プライオリティ + システム ID エクステンション）
ポート プライオリティ	32
ポート コスト	• 10 ギガビット イーサネット：2 • ギガビット イーサネット：4 • ファスト イーサネット：19[1] • FDDI/CDDI：10 • イーサネット：100[2]
デフォルトのスパニングツリー ポート コスト モード	ショート（802.1D）
ポート VLAN プライオリティ	ポート プライオリティと同じ、PVST+ では VLAN 単位で設定可能
ポート VLAN コスト	ポート コストと同じ、PVST+ では VLAN 単位で設定可能
最大エージング タイム	20 秒
Hello タイム	2 秒
転送遅延時間	15 秒

1. 10/100 Mbps ポートが自動ネゴシエーションするか、または 100 Mbps に固定されている場合は、ポート コストは 19 です。
2. 10/100 Mbps ポートが自動ネゴシエーションするか、または 10 Mbps に固定されている場合は、ポート コストは 100 です。

PVST+ ブリッジ ID プライオリティの設定

ブリッジ ID プライオリティは、スイッチが PVST+ モードのときの VLAN のプライオリティです。

スイッチが MAC アドレス リダクションをイネーブルに設定しないで PVST+ モードになっている場合は、ブリッジ プライオリティ値を 0 ～ 65535 の範囲で入力できます。入力したブリッジ プライオリティ値は、その VLAN の VLAN ブリッジ ID プライオリティにもなります。

スイッチが MAC アドレス リダクションをイネーブルにして PVST+ モードになっている場合は、次の 16 種類のブリッジ プライオリティ値のいずれかを入力できます。0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、または 61440 です。

ブリッジ プライオリティはシステム ID エクステンション（VLAN の ID）と組み合わされ、その VLAN のブリッジ ID プライオリティを形成します。

VLAN のスパニングツリー ブリッジ プライオリティを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	VLAN の PVST+ ブリッジ ID プライオリティを設定します。	**set spantree priority** *bridge_ID_priority* [*vlan*]
ステップ 2	ブリッジ ID プライオリティを確認します。	**show spantree** [*vlan*] [**active**]

次に、MAC アドレス リダクションがイネーブルでない場合（デフォルト）に、PVST+ ブリッジ ID を設定する例を示します。

```
Console> (enable) set spantree priority 30000 1
Spantree 1 bridge priority set to 30000.
Console> (enable) show spantree 1
VLAN 1
Spanning tree mode          PVST+
Spanning tree type          ieee
Spanning tree enabled

Designated Root             00-60-70-4c-70-00
Designated Root Priority    16384
Designated Root Cost        19
Designated Root Port        2/3
Root Max Age   14 sec   Hello Time 2 sec   Forward Delay 10 sec

Bridge ID MAC ADDR          00-d0-00-4c-18-00
Bridge ID Priority          30000
Bridge Max Age 20 sec   Hello Time 2 sec   Forward Delay 15 sec

Port                      Vlan Port-State    Cost      Prio Portfast Channel_id
------------------------ ---- ------------- --------- ---- -------- ----------
 1/1                      1    not-connected         4   32 disabled 0
 1/2                      1    not-connected         4   32 disabled 0
 2/1                      1    not-connected       100   32 disabled 0
 2/2                      1    not-connected       100   32 disabled 0
```

次に、MAC アドレス リダクションがイネーブルの場合に、PVST+ ブリッジ ID を設定する例を示します。

```
Console> (enable) set spantree priority 32768 1
Spantree 1 bridge ID priority set to 32769
(bridge priority: 32768 + sys ID extension: 1)
Console> (enable) show spantree 1/1 1
VLAN 1
Spanning tree mode          PVST+
Spanning tree type          ieee
Spanning tree enabled

Designated Root             00-60-70-4c-70-00
Designated Root Priority    16384
Designated Root Cost        19
Designated Root Port        2/3
Root Max Age   14 sec   Hello Time 2 sec   Forward Delay 10 sec

Bridge ID MAC ADDR          00-d0-00-4c-18-00
Bridge ID Priority          32769 (bridge priority: 32768, sys ID ext: 1)
Bridge Max Age 20 sec   Hello Time 2 sec   Forward Delay 15 sec

Port                     Vlan Port-State    Cost      Prio Portfast Channel_id
------------------------ ---- ------------- --------- ---- -------- ----------
 1/1                      1    not-connected         4   32 disabled 0
 1/2                      1    not-connected         4   32 disabled 0
 2/1                      1    not-connected       100   32 disabled 0
 2/2                      1    not-connected       100   32 disabled 0
```

PVST+ ポート コストの設定

スイッチ ポートのポート コストを設定できます。ポート コストが小さいポートほど、フレームを転送するポートとして選択される可能性が高くなります。高速メディア（全二重など）に接続するポートには小さい値を、低速メディアに接続するポートには大きい値を割り当ててください。ポート コストの計算にショート法を使用している場合使用できるコストの値は 1 ～ 65535 で、ロング法を使用している場合は 1 ～ 200000000 です。デフォルトのコストは、メディアによって異なります。ポート コストの計算手順については、「ポート コストの計算および割り当て」（p.8-4）を参照してください。

ポートに PVST+ ポート コストを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチ ポートの PVST+ ポート コストを設定します。	**set spantree portcost** {*mod/port*} *cost*
ステップ 2	ポート コストの設定を確認します。	**show spantree** *mod/port*

（注） **set spantree channelcost** コマンドを実行しても、コンフィギュレーション ファイルには表示されません。このコマンドにより、チャネル内の各ポートについて、[set spantree portcost] のエントリが作成されます。**set spantree channelcost** コマンドの使用方法の詳細については、第 6 章「EtherChannel の設定」の「EtherChannel ポート パス コストの設定」を参照してください。

次に、ポート上に PVST+ ポート コストを設定し、設定を確認する例を示します。

```
Console> (enable) set spantree portcost 2/3 12
Spantree port 2/3 path cost set to 12.
Console> (enable) show spantree 2/3
VLAN 1
   .
   .
   .
Port                     Vlan Port-State    Cost      Prio Portfast Channel_id
------------------------ ---- ------------- --------- ---- -------- ----------
 1/1                     1    not-connected         4   32 disabled 0
 1/2                     1    not-connected         4   32 disabled 0
 2/1                     1    not-connected       100   32 disabled 0
 2/2                     1    not-connected       100   32 disabled 0
 2/3                     1    forwarding           12   32 disabled 0
 2/4                     1    not-connected       100   32 disabled
```

PVST+ ポート プライオリティの設定

PVST+ モードのスイッチ ポートにポート プライオリティを設定できます。プライオリティ値が最小のポートが、すべての VLAN のフレームを転送します。指定できるポート プライオリティ値は、0 ～ 240 の範囲の 16 の倍数です。デフォルトは 32 です。すべてのポートに同じプライオリティ値を指定した場合、ポート番号が最小のポートがフレームを転送します。

ポートに PVST+ ポート プライオリティを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチ ポートに PVST+ ポート プライオリティを設定します。	**set spantree portpri** *mod/port priority*
ステップ 2	ポート プライオリティの設定を確認します。	**show spantree** *mod/port*

次に、ポートの PVST+ ポート プライオリティを設定する例を示します。

```
Console> (enable) set spantree portpri 2/3 48
Bridge port  2/3 port priority set to 48.
Console> (enable) show spantree 2/3
VLAN 1
   .
   .
   .
Port                     Vlan Port-State    Cost      Prio Portfast Channel_id
------------------------ ---- ------------- --------- ---- -------- ----------
 1/1                     1    not-connected         4   32 disabled 0
 1/2                     1    not-connected         4   32 disabled 0
 2/1                     1    not-connected       100   32 disabled 0
 2/2                     1    not-connected       100   32 disabled 0
 2/3                     1    forwarding           19   48 disabled 0
 2/4                     1    not-connected       100   32 disabled 0
```

次に、16 の倍数以外の値（0 ～ 63 の範囲の値）を入力したために最も近い 16 の倍数値が設定されている例を示します。

```
Console> (enable) set spantree portpri 2/3 2
Vlan port priority must be one of these numbers:0, 16, 32, 48, 64, 80,
96, 112, 128, 144,
160, 176, 192, 208, 224, 240
converting 2 to 0 nearest multiple of 16
Bridge port  2/3 port priority set to 0.
```

PVST+ のデフォルト ポート コスト モードの設定

ネットワーク上のいずれかのスイッチが 10 GB 以上のポート速度を使用し、かつネットワークが PVST+ スパニングツリー モードを使用している場合、そのネットワーク上のすべてのスイッチで、パス コストに関して同じデフォルト値を使用する必要があります。**set spantree defaultcostmode** コマンドを使用して、すべてのポートに対応付けられたすべての VLAN に、強制的に同じポート コスト デフォルト値を設定できます。

デフォルトのポート コスト モードとしては、ショートおよびロングの 2 種類があります。

- ショート モードのパラメータは、次のとおりです。
  - portcost
  - portvlancost（トランク ポートのみ）
  - UplinkFast がイネーブルになっている場合、実際のコストは 3000 増えます。
- ロング モードのパラメータは、次のとおりです。
  - portcost
  - portvlancost（トランク ポートのみ）
  - UplinkFast がイネーブルになっている場合、実際のコストは 10,000,000 増えます。
  - EtherChannel は、AVERAGE_COST/NUM_PORT という公式を使用して、バンドルのコストを算出します。

PVST+ モードでは、デフォルトのポート コスト モードはショートに設定されています。ポート速度が 10 GB 以上の場合は、デフォルトのポート コスト モードをロングに設定する必要があります。

PVST+ デフォルト ポート コスト モードを設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
PVST+ デフォルト ポート コスト モードを設定します。	**set spantree defaultcostmode** {**short** | **long**}

次に、PVST+ デフォルト ポート コスト モードを設定する例を示します。

```
Console> (enable) set spantree defaultcostmode long
Portcost and portvlancost set to use long format default values.
Console> (enable)
```

PVST+ ポート VLAN コストの設定

VLAN 単位でポート コストを設定できます。VLAN のポート コストが小さいポートほど、フレームを転送するポートとして選択される可能性が高くなります。高速メディア（全二重など）に接続するポートには小さい値を、低速メディアに接続するポートには大きい値を割り当ててください。ポート コストの計算にショート法を使用している場合使用できるコストの値は 1 ～ 65535 で、ロング法を使用している場合は 1 ～ 200000000 です。デフォルトのコストは、メディアによって異なります。ポート コストの計算手順については、「ポート コストの計算および割り当て」（p.8-4）を参照してください。

ポートに PVST+ ポート VLAN コストを設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
ポート上の VLAN について、PVST+ ポート コストを設定します。	**set spantree portvlancost** {*mod/port*} [**cost** *cost*] [*vlan_list*]

(注)

set spantree channelcost コマンドを実行しても、コンフィギュレーション ファイルには表示されません。このコマンドにより、チャネル内の各ポートについて、[set spantree portcost] のエントリが作成されます。**set spantree channelcost** コマンドの使用方法の詳細については、第 6 章「EtherChannel の設定」の「EtherChannel ポート パス コストの設定」を参照してください。

次に、ポート 2/3 上の VLAN 1 ～ 5 について、PVST+ ポート VLAN コストを設定する例を示します。

```
Console> (enable) set spantree portvlancost 2/3 cost 20000 1-5
Port 2/3 VLANs 6-11,13-1005,1025-4094 have path cost 12.
Port 2/3 VLANs 1-5,12 have path cost 20000.
This parameter applies to trunking ports only.
Console> (enable
```

PVST+ ポート VLAN プライオリティの設定

スイッチが PVST+ モードのとき、VLAN のトランキング ポートにポート プライオリティを設定できます。特定の VLAN に対してプライオリティ値が最小のポートが、その VLAN のフレームを転送します。指定できるポート プライオリティ値は、0 ～ 240 の範囲の 16 の倍数です。デフォルトは 16 です。特定の VLAN に関して、すべてのポートに同じプライオリティ値を指定した場合、ポート番号が最小のポートがその VLAN のフレームを転送します。

ポート VLAN プライオリティ値は、ポート プライオリティ値より小さくする必要があります。

ポートのポート VLAN プライオリティを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポート上の VLAN について、PVST+ ポート プライオリティを設定します。	**set spantree portvlanpri** *mod/port priority* [*vlans*]
ステップ 2	ポート VLAN プライオリティを確認します。	**show config all**

次に、ポート 2/3 上の VLAN 6 について、ポート プライオリティを設定する例を示します。

```
Console> (enable) set spantree portvlanpri 2/3 16 6
Port 2/3 vlans 6 using portpri 16.
Port 2/3 vlans 1-5,7-800,802-1004,1006-4094 using portpri 32.
Port 2/3 vlans 801,1005 using portpri 4.
This parameter applies to trunking ports only.
Console> (enable) show config all
   .
   .
   .
set spantree portcost    2/12,2/15 19
set spantree portcost    2/1-2,2/4-11,2/13-14,2/16-48 100
set spantree portcost    2/3 12
set spantree portpri     2/1-48 32
set spantree portvlanpri 2/1 0
set spantree portvlanpri 2/2 0
   .
   .
   .
set spantree portvlanpri 2/48 0
set spantree portvlancost 2/1 cost 99
set spantree portvlancost 2/2 cost 99
set spantree portvlancost 2/3 cost 20000 1-5,12
```

VLAN 上の PVST+ モードのディセーブル化

スイッチが PVST+ モードのとき、個々の VLAN またはすべての VLAN 上で、スパニングツリーをディセーブルにできます。VLAN でスパニングツリーをディセーブルにすると、スイッチはスパニングツリーに参加せず、その VLAN で受信された BPDU はすべてのポート上にフラッディングされます。

注意　物理的にループフリーであるトポロジーの場合でも、スパニングツリーをディセーブルにしないでください。スパニングツリーは、設定エラーやケーブル接続エラーに対する保護手段として機能します。VLAN 内に物理ループが存在しないことを確認しないまま、スパニングツリーをディセーブルにしないでください。

注意　VLAN　のすべてのスイッチまたはルータでスパニングツリーがディセーブルになっていないかぎり、VLAN のスパニングツリーをディセーブルにしないでください。VLAN 内では、スパニングツリーを、一部のスイッチやルータでディセーブルにし、その他のスイッチやルータではイネーブルのままにしておくことはできません。スイッチおよびルータでスパニングツリーがイネーブルのままになっていると、ネットワークの物理トポロジーに関する情報が不完全なものになります。その結果、予想外の状況が生じる可能性があります。

PVST+ をディセーブルするには、イネーブル モードで次の作業を行います。

作業	コマンド
VLAN 上の PVST+ モードをディセーブルにします。	**set spantree disable** *vlans* [**all**]

次に、VLAN 上で PVST+ をディセーブルにする例を示します。

```
Console> (enable) set spantree disable 4
Spantree 4 disabled.
Console> (enable)
```

スイッチ上での Rapid PVST+ の設定

Rapid PVST+ が Catalyst 6500 シリーズ スイッチ上のすべてのイーサネット、ファスト イーサネット、およびギガビット イーサネット ポートベース VLAN で使用されるデフォルトのスパニングツリー プロトコルになります。Rapid PVST+ を設定するには、スイッチ上に PVST+ も設定する必要があります。PVST+ は、Rapid PVST+ をイネーブルにする前後どちらででも設定できます。

Rapid PVST+ を設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	Rapid PVST+ をイネーブルにします。	**set spantree mode rapid-pvst+**
ステップ 2	ポートのリンクタイプをポイントツーポイント モードに設定します。	**set spantree link-type** *mod/port* **point-to-point**
ステップ 3	ポートのレガシー ブリッジを検出します。	**clear spantree detected-protocols** *mod/port*
ステップ 4	Rapid PVST+ 設定を確認します。	**show spantree** *vlan*

次に、Rapid PVST+ を設定する例を示します。

```
Console> (enable) set spantree mode rapid-pvst+
Spantree mode set to RAPID-PVST+.
Console> (enable) set spantree link-type 3/1 point-to-point
Link type set to point-to-point on port 3/1.
Console> (enable) clear spantree detected-protocols 3/1
Spanning tree protocol detection forced on port 3/1
Console> (enable)
```

次に、VLAN 1 の Rapid PVST+ 設定を確認する例を示します。出力の最初の行にはスパニングツリー モードが表示されています。

```
Console> show spantree 1
Spanning tree mode          RAPID-PVST+
Spanning tree type          ieee
Spanning tree enabled.
.
.
.
Port           State       Role     Cost    Prio   Type
-------------  ----------- -------  -----   ----   -----------------
6/1           forwarding  ROOT     20000    16    Shared, PEER(STP)

Console>
```

次に、ポート 3/6 のリンクタイプ、エッジ ポート、およびガード タイプを確認する例を示します。

```
Console> show spantree 3/6
Port 3/6
Edge Port:      No, (Configured) Default
Port Guard:     Default
Link Type:      P2P(Configured) Auto

Port     VLAN     State       Role    Cost     Prio  Type
------   -----    ----------  ------  -------- ----  -----
3/6       1       listening   DESG    20000    32    P2P
3/6       2       listening   DESG    20000    32    P2P
3/6       3       listening   DESG    20000    32    P2P
3/6       4       listening   DESG    20000    32    P2P
3/6       5       listening   DESG    20000    32    P2P
3/6       6       listening   DESG    20000    32    P2P
3/6       7       listening   DESG    20000    32    P2P
3/6       8       listening   DESG    20000    32    P2P
3/6       9       listening   DESG    20000    32    P2P
3/6       10      listening   DESG    20000    32    P2P
3/6       11      listening   DESG    20000    32    P2P
3/6       12      listening   DESG    20000    32    P2P
3/6       13      listening   DESG    20000    32    P2P
3/6       14      listening   DESG    20000    32    P2P
3/6       15      listening   DESG    20000    32    P2P
3/6       16      listening   DESG    20000    32    P2P
3/6       17      listening   DESG    20000    32    P2P
3/6       18      listening   DESG    20000    32    P2P
3/6       19      listening   DESG    20000    32    P2P

Console>
```

スイッチ上での MISTP-PVST+ または MISTP の設定

Catalyst 6500 シリーズ スイッチにおけるデフォルトのスパニングツリー モードは Rapid PVST+ です。ネットワークで MISTP モードを使用する場合は、接続切断を防ぐため、ここで説明する手順に必ず従ってください。

スパニングツリー モードを変更すると、現在のモードは停止し、実行時に収集された情報を使用して新しいモード用のポート データベースが作成され、新しいスパニングツリー モードによってアクティブ トポロジーの計算が再開されます。ポート ステートに関する情報は消去されます。ただし、前のモードに関するコンフィギュレーション パラメータはすべて保存されます。前のモードに戻ると、同じ設定がそのまま残っています。

(注)　MISTP モードを使用する場合は、使用する Catalyst 6500 シリーズ スイッチ*全部*で MISTP を実行するように設定することを推奨します。

MISTP モードを使用するには、まず MISTP インスタンスをイネーブルにし、次にそのインスタンスに少なくとも 1 つの VLAN をマッピングします。MISTP インスタンスがアクティブになるには、VLAN に少なくとも 1 つのフォワーディング ポートが必要です。

(注)　VTP サーバ モードまたはトランスペアレント モード専用の Catalyst 6500 シリーズ スイッチで、VLAN を MISTP インスタンスにマッピングします。VTP クライアント モードにあるスイッチで、VLAN を MISTP インスタンスにマッピングすることはできません。MISTP 設定に伴う問題を引き起こす VTP 設定エラーを防止するため、第 10 章「VTP の設定」を参照し、VTP バージョン 1、2、および 3 の使用の詳細を確認してください。

スイッチを PVST+ モードから MISTP モードに変更するとき、PVST+ を使用している別のスイッチがネットワークに存在する場合は、MISTP を使用する予定の各スイッチで事前に MISTP-PVST+ モードをイネーブルにしておき、スイッチの設定中に PVST+ BPDU がスイッチ経由で流れるようにしなければなりません。

ネットワーク内のすべてのスイッチが MISTP-PVST+ に設定されている場合は、すべてのスイッチ上で MISTP をイネーブルに設定できます。

ここでは、MISTP-PVST+ または MISTP の使用方法について説明します。

MISTP および MISTP-PVST+ のデフォルト設定

表 8-5 に、MISTP および MISTP-PVST+ のデフォルト設定を示します。

表 8-5　MISTP および MISTP-PVST+ のデフォルト設定

機能	デフォルト値
イネーブル ステート	MISTP インスタンスに VLAN がマッピングされるまでディセーブル
MAC アドレス リダクション	ディセーブル
ブリッジ プライオリティ	32768
ブリッジ ID プライオリティ	32769（MISTP インスタンス 1 のブリッジ プライオリティ + システム ID エクステンション）
ポート プライオリティ	32（グローバル）
ポート コスト	• 10 ギガビット イーサネット：2 • ギガビット イーサネット：4 • ファスト イーサネット：19[1] • FDDI/CDDI：10 • イーサネット：100[2]
デフォルトのポート コスト モード	ショート（802.1D）
ポート VLAN プライオリティ	ポート プライオリティと同じ、PVST+ では VLAN 単位で設定可能
ポート VLAN コスト	ポート コストと同じ、PVST+ では VLAN 単位で設定可能
最大エージング タイム	20 秒
Hello タイム	2 秒
転送遅延時間	15 秒

1. 10/100 Mbps ポートが自動ネゴシエーションするか、または 100 Mbps に固定されている場合は、ポート コストは 19 です。
2. 10/100 Mbps ポートが自動ネゴシエーションするか、または 10 Mbps に固定されている場合は、ポート コストは 100 です。

MISTP-PVST+ または MISTP モードの設定

PVST+ ネットワークで MISTP をイネーブルにする場合、ネットワークをダウンさせないように、注意が必要です。ここでは、ネットワーク上で MISTP または MISTP-PVST+ をイネーブルにする手順について説明します。

注意　スイッチ上で 6,000 を超える VLAN ポートを設定している場合、MISTP モードから PVST+ または MISTP-PVST+ モードに変更すると、ネットワークがダウンする可能性があります。接続切断を防ぐため、スイッチ上の VLAN ポート数を 6,000 以下に減らしてください。

注意　スイッチとの Telnet 接続を使用して作業する場合、MISTP-PVST+ または MISTP モードを初めてイネーブルにするときは、スイッチ コンソールから作業を行う必要があります。データ ポート経由の Telnet 接続は使用しないでください。使用した場合、スイッチとの接続が切断されます。MISTP インスタンスに VLAN をマッピングしたあとは、Telnet でスイッチに接続することができます。

PVST+ から MISTP-PVST+ または MISTP に変更するには、イネーブル モードで次の作業を行います。

作業	コマンド
スパニングツリー モードを設定します。	**set spantree mode** {**mistp** | **pvst+** | **mistp-pvst+**}

次に、スイッチを MISTP-PVST+ モードに設定する例を示します。

```
Console> (enable) set spantree mode mistp-pvst+
PVST+ database cleaned up.
Spantree mode set to MISTP-PVST+.
Warning!! There are no VLANs mapped to any MISTP instance.
Console> (enable)
```

ルート スイッチから実行時に伝播される VLAN/MISTP インスタンスのマッピング情報を表示できます。この情報を表示できるのは、MISTP モードまたは MISTP-PVST+ モードに限られます。PVST+ モードの場合は、オプションのキーワード **config** を使用して、ローカル スイッチ上で設定されているマッピングのリストを表示します。

（注） キーワード **config** を指定した場合、MAC アドレスは表示されません。

スパニングツリー マッピングを表示するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スパニングツリー モードを MISTP に設定します。	**set spantree mode mistp**
ステップ 2	スパニングツリー マッピングを表示します。	**show spantree mapping** [**config**]

次に、MISTP モードでスパニングツリー VLAN インスタンス マッピングを表示する例を示します。

```
MISTP/MISTP-PVST+
Console> (enable) set spantree mode mistp
PVST+ database cleaned up.
Spantree mode set to MISTP.
Console> (enable) show spantree mapping
Inst Root Mac          Vlans
---- ----------------- --------------------------
1    00-50-3e-78-70-00 1
2    00-50-3e-78-70-00 -
3    00-50-3e-78-70-00 -
4    00-50-3e-78-70-00 -
5    00-50-3e-78-70-00 -
6    00-50-3e-78-70-00 -
7    00-50-3e-78-70-00 -
8    00-50-3e-78-70-00 -
9    00-50-3e-78-70-00 -
10   00-50-3e-78-70-00 -
11   00-50-3e-78-70-00 -
12   00-50-3e-78-70-00 -
13   00-50-3e-78-70-00 -
14   00-50-3e-78-70-00 -
15   00-50-3e-78-70-00 -
16   00-50-3e-78-70-00 -
```

MISTP インスタンスの設定

ここでは、MISTP インスタンスの設定手順について説明します。

MISTP ブリッジ ID プライオリティの設定

スイッチが MISTP または MISTP-PVST+ モードのとき、MISTP インスタンスのブリッジ ID プライオリティを設定できます。

ブリッジ プライオリティ値はシステム ID エクステンション（MISTP インスタンスの ID）と組み合わされ、ブリッジ ID プライオリティを形成します。次の 16 種類のブリッジ プライオリティ値のいずれかを設定できます。0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、および 61440 です。

MISTP インスタンスにブリッジ ID プライオリティを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	MISTP インスタンスのブリッジ ID プライオリティを設定します。	**set spantree priority** *bridge_ID_priority* [**mistp-instance** *instance*]
ステップ 2	ブリッジ ID プライオリティを確認します。	**show spantree mistp-instance** *instance* [*mod/port*] **active**

次に、MISTP インスタンスのブリッジ ID プライオリティを設定する例を示します。

```
Console> (enable) set spantree priority 32768 mistp-instance 1
Spantree 1 bridge ID priority set to 32769
(bridge priority: 32768 + sys ID extension: 1)
Console> (enable) show spantree mistp-instance 1
Instance 1
Spanning tree mode          MISTP
Spanning tree type          ieee
Spanning tree instance enabled

Designated Root             00-05-31-40-64-00
Designated Root Priority    32769  (root priority:32768, sys ID ext:1)
Designated Root Cost        20000
Designated Root Port        1/1
VLANs mapped:               1,74
Root Max Age   20 sec   Hello Time 2  sec   Forward Delay 15 sec

Bridge ID MAC ADDR          00-d0-02-27-9c-00
Bridge ID Priority          32769  (bridge priority:32768, sys ID ext:1)
VLANs mapped:               1,74
Bridge Max Age 20 sec   Hello Time 2  sec   Forward Delay 15 sec

Port                      Inst Port-State    Cost      Prio Portfast Channel_id
------------------------- ---- ------------- --------- ---- -------- ----------
 1/1                      1    forwarding        20000   32 disabled 0
 3/1                      1    forwarding       200000   32 disabled 0
 3/25                     1    forwarding       200000   32 disabled 0
 3/26                     1    forwarding       200000   32 disabled 0
 3/27                     1    forwarding       200000   32 disabled 0
 3/28                     1    forwarding       200000   32 disabled 0
 3/29                     1    forwarding       200000   32 disabled 0
```

```
 3/30                    1    forwarding       200000   32 disabled 0
7/1-4                    1    blocking           5000   32 disabled 833
 7/5                     1    forwarding        20000   32 disabled 0
 7/6                     1    forwarding        20000   32 disabled 0
 8/37                    1    blocking         200000   32 disabled 0
 8/38                    1    blocking         200000   32 disabled 0
15/1                     1    forwarding        20000   32 enabled  0
16/1                     1    forwarding        20000   32 enabled  0
Console> (enable)
```

MISTP ポート コストの設定

スイッチ ポートのポート コストを設定できます。ポート コストが小さいポートほど、フレームを転送するポートとして選択される可能性が高くなります。高速メディア（全二重など）に接続するポートには小さい値を、低速メディアに接続するポートには大きい値を割り当ててください。ポート コストの計算にショート法を使用している場合、使用できるコストの値は 1 ～ 65535 で、ロング法を使用している場合は 1 ～ 200000000 です。デフォルトのコストは、メディアによって異なります。ポート コストの計算手順については、「ポート コストの計算および割り当て」（p.8-4）を参照してください。

ポートにポート コストを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチ ポートの MISTP ポート コストを設定します。	**set spantree portcost** *mod/port cost*
ステップ 2	ポート コストの設定を確認します。	**show spantree mistp-instance** *instance* [*mod/port*] **active**

次に、MISTP インスタンス上にポート コストを設定し、設定を確認する例を示します。

```
Console> (enable) set spantree portcost 1/1 20000
Spantree port 1/1 path cost set to 20000.
Console> (enable) show spantree mistp-instance 1 active
Instance 1
Spanning tree mode          MISTP
Spanning tree type          ieee
Spanning tree instance enabled

Designated Root             00-05-31-40-64-00
Designated Root Priority    32769  (root priority:32768, sys ID ext:1)
Designated Root Cost        20000
Designated Root Port        1/1
VLANs mapped:               1,74
Root Max Age   20 sec   Hello Time 2  sec   Forward Delay 15 sec

Bridge ID MAC ADDR          00-d0-02-27-9c-00
Bridge ID Priority          32769  (bridge priority:32768, sys ID ext:1)
VLANs mapped:               1,74
Bridge Max Age 20 sec   Hello Time 2  sec   Forward Delay 15 sec

Port                     Inst Port-State    Cost      Prio Portfast Channel_id
------------------------ ---- ------------- --------- ---- -------- ----------
 1/1                     1    forwarding        20000   32 disabled 0
 3/1                     1    forwarding       200000   32 disabled 0
 3/25                    1    forwarding       200000   32 disabled 0
 3/26                    1    forwarding       200000   32 disabled 0
 3/27                    1    forwarding       200000   32 disabled 0
 3/28                    1    forwarding       200000   32 disabled 0
 3/29                    1    forwarding       200000   32 disabled 0
 3/30                    1    forwarding       200000   32 disabled 0
7/1-4                    1    blocking           5000   32 disabled 833
 7/5                     1    forwarding        20000   32 disabled 0
 7/6                     1    forwarding        20000   32 disabled 0
```

```
 8/37                    1    blocking         200000   32 disabled 0
 8/38                    1    blocking         200000   32 disabled 0
15/1                     1    forwarding        20000   32 enabled  0
16/1                     1    forwarding        20000   32 enabled  0
Console> (enable)
```

MISTP ポート プライオリティの設定

ポートのポート プライオリティを設定できます。プライオリティ値が最小のポートが、すべての VLAN のフレームを転送します。指定できるポート プライオリティ値は、0 ～ 240 の範囲の 16 の倍数です。デフォルトは 32 です。すべてのポートに同じプライオリティ値を指定した場合、ポート番号が最小のポートがフレームを転送します。

ポートにポート プライオリティを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポートに MISTP ポート プライオリティを設定します。	**set spantree portpri** *mod/port*
ステップ 2	ポート プライオリティの設定を確認します。	**show spantree mistp-instance** *instance* [*mod/port*] **active**

次に、ポート プライオリティを設定し、設定を確認する例を示します。

```
Console> (enable) set spantree portpri 1/1 32
Bridge port 1/1 port priority set to 32.
Console> (enable) show spantree mistp-instance 1
Instance 1
Spanning tree mode          MISTP
Spanning tree type          ieee
Spanning tree instance enabled

Designated Root             00-05-31-40-64-00
Designated Root Priority    32769  (root priority:32768, sys ID ext:1)
Designated Root Cost        20000
Designated Root Port        1/1
VLANs mapped:               1,74
Root Max Age   20 sec   Hello Time 2  sec   Forward Delay 15 sec

Bridge ID MAC ADDR          00-d0-02-27-9c-00
Bridge ID Priority          32769  (bridge priority:32768, sys ID ext:1)
VLANs mapped:               1,74
Bridge Max Age 20 sec   Hello Time 2  sec   Forward Delay 15 sec

Port                      Inst Port-State    Cost      Prio Portfast Channel_id
------------------------- ---- ------------- --------- ---- -------- ----------
 1/1                      1    forwarding        20000   32 disabled 0
 3/1                      1    forwarding       200000   32 disabled 0
 3/25                     1    forwarding       200000   32 disabled 0
 3/26                     1    forwarding       200000   32 disabled 0
 3/27                     1    forwarding       200000   32 disabled 0
 3/28                     1    forwarding       200000   32 disabled 0
 3/29                     1    forwarding       200000   32 disabled 0
 3/30                     1    forwarding       200000   32 disabled 0
7/1-4                     1    blocking           5000   32 disabled 833
 7/5                      1    forwarding        20000   32 disabled 0
 7/6                      1    forwarding        20000   32 disabled 0
 8/37                     1    blocking         200000   32 disabled 0
 8/38                     1    blocking         200000   32 disabled 0
15/1                      1    forwarding        20000   32 enabled  0
16/1                      1    forwarding        20000   32 enabled  0
Console> (enable)
```

MISTP ポート インスタンス コストの設定

MISTP または MISTP-PVST+ インスタンスに、ポート インスタンス コストを設定できます。インスタンス コストが小さいポートほど、フレームを転送するポートとして選択される可能性が高くなります。高速メディア（全二重など）に接続するポートには小さい値を、低速メディアに接続するポートには大きい値を割り当ててください。デフォルトのコストは、メディアによって異なります。ポート インスタンス コストに設定できる値の範囲は、1 ～ 268435456 です。

ポートにポート インスタンス コストを設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
ポート上に MISTP ポート インスタンス コストを設定します。	**set spantree portinstancecost** {*mod/port*} [**cost** *cost*] [*instances*]

次に、特定のポート上に MISTP ポート インスタンス コストを設定する例を示します。

```
Console> (enable) set spantree portinstancecost 1/1 cost 110110 2
Port 1/1 instances 1,3-16 have path cost 20000.
Port 1/1 instances 2 have path cost 110110.
This parameter applies to trunking ports only.
Console> (enable)
```

MISTP ポート インスタンス プライオリティの設定

MISTP インスタンスにポート プライオリティを設定できます。特定の MISTP インスタンスに対してプライオリティ値が最小のポートが、そのインスタンスにフレームを転送します。指定できるポート インスタンスの範囲は、0 ～ 63 です。指定できるポート プライオリティ値は、0 ～ 240 の範囲の 16 の倍数です。特定の MISTP インスタンスに関して、すべてのポートに同じプライオリティ値を指定した場合、ポート番号が最小のポートがそのインスタンスにフレームを転送します。

MISTP インスタンス上にポート インスタンス プライオリティを設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
MISTP インスタンス上にポート インスタンス プライオリティを設定します。	**set spantree portinstancepri** {*mod/port*} *priority* [*instances*]

次に、MISTP インスタンス上にポート インスタンス プライオリティを設定し、設定を確認する例を示します。

```
Console> (enable) set spantree portinstancepri 1/1 16 2
Port 1/1 MISTP Instances 2 using portpri 16.
Port 1/1 mistp-instance 1,3-16 using portpri 32.
Console> (enable)
```

MISTP インスタンスのイネーブル化

最大 16 個の MISTP インスタンスをイネーブルに設定できます。各 MISTP インスタンスは、固有のスパニングツリー トポロジーを定義します。MISTP インスタンス 1（デフォルトのインスタンス）は、デフォルトでイネーブルに設定されています。ただし、インスタンスをアクティブにするには、そのインスタンスに VLAN をマッピングする必要があります。1 つの MISTP インスタンス、またはある範囲のインスタンスをイネーブルにしたり、**all** キーワードを使用してすべてのインスタンスを一度にイネーブルにすることもできます。

(注)　MISTP インスタンスにアクティブ ポートを持つ VLAN をマッピングしないかぎり、MISTP インスタンスのステータスは表示されません。

MISTP インスタンスをイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	MISTP インスタンスをイネーブルにします。	**set spantree enable mistp-instance** *instance* [**all**]
ステップ 2	インスタンスがイネーブルになったことを確認します。	**show spantree mistp-instance** [*instance*] [**active**] *mod/port*

(注)　**active** キーワードを入力して、アクティブ ポートだけを表示します。

次に、MISTP インスタンスをイネーブルにする例を示します。

```
Console> (enable) set spantree enable mistp-instance 2
Spantree 2 enabled.

Console> (enable) show spantree mistp-instance 2
Instance 2
Spanning tree mode          MISTP
Spanning tree type          ieee
Spanning tree instance enabled
   .
   .
   .
```

MISTP インスタンスへの VLAN マッピング

スイッチ上で MISTP-PVST+ または MISTP を使用する場合、MISTP-PVST+ または MISTP をアクティブにするには、1 つの MISTP インスタンスに少なくとも 1 つの VLAN をマッピングする必要があります。ここでは、MISTP インスタンスの設定手順について説明します。

- MISTP インスタンスの判別 ― VLAN マッピングの矛盾（p.8-44）
- MISTP インスタンスからの VLAN マッピングの解除（p.8-46）

(注)　VLAN の詳しい使用手順および設定手順については、第 11 章「VLAN の設定」を参照してください。

MISTP インスタンスに VLAN をマッピングする場合、次の注意事項に従ってください。

- MISTP インスタンスにマッピングできるのは、イーサネット VLAN だけです。
- MISTP-PVST+ または MISTP をアクティブにするには、インスタンスで少なくとも 1 つの VLAN にアクティブ ポートがなければなりません。
- 1 つの MISTP インスタンスに対し、必要に応じて複数のイーサネット VLAN をマッピングできます。
- 1 つの VLAN を、複数の MISTP インスタンスにマッピングすることはできません。

（注） VLAN 1025 ～ 4094 を使用するには、MAC アドレス リダクションをイネーブルにする必要があります。拡張範囲 VLAN の詳しい使用方法については、第 11 章「VLAN の設定」の「拡張範囲 VLAN の作成」（p.11-8）を参照してください。

MISTP インスタンスに VLAN をマッピングするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	MISTP インスタンスに VLAN をマッピングします。	**set vlan** *vlan* **mistp-instance** *instance*
ステップ 2	VLAN がマッピングされたことを確認します。	**show spantree mistp-instance** [*instance*] [**active**] *mod/port*

次に、MISTP インスタンス 1 に VLAN をマッピングし、マッピングを確認する例を示します。

```
Console> (enable) set vlan 6 mistp-instance 1
Vlan 6 configuration successful
Console> (enable) show spantree mist-instance 1
Instance 1
Spanning tree mode          MISTP-PVST+
Spanning tree type          ieee
Spanning tree instance enabled

Designated Root             00-d0-00-4c-18-00
Designated Root Priority    49153 (root priority: 49152, sys ID ext: 1)
Designated Root Cost        0
Designated Root Port        none
VLANs mapped:               6
Root Max Age   20 sec   Hello Time 2 sec   Forward Delay 15 sec

Bridge ID MAC ADDR          00-d0-00-4c-18-00
Bridge ID Priority          49153 (bridge priority: 49152, sys ID ext: 1)
VLANs mapped:               6
Bridge Max Age 20 sec   Hello Time 2 sec   Forward Delay 15 sec
Port                      Inst Port-State    Cost      Prio Portfast Channel_id
------------------------ ---- ------------- --------- ---- -------- ----------
 2/12                     1    forwarding     22222222   40 disabled 0
```

MISTP インスタンスの判別 ― VLAN マッピングの矛盾

VLAN は、1 つの MISTP インスタンスだけにマッピングが可能です。1 つの VLAN を複数のインスタンスにマッピングしようとすると、その VLAN のすべてのポートがブロッキング モードになります。VLAN をどの MISTP インスタンスにマッピングしようとしたかを判別するには、**show spantree conflicts** コマンドを使用します。

このコマンドでは、VLAN と対応付けられた MISTP インスタンスのリスト、VLAN マッピング情報を含む BPDU を送信しているルート スイッチの MAC アドレス、および VLAN と MISTP インスタンスのマッピングに関するタイマーが出力されます。1 つのエントリしか出力されない場合、またはすべてのエントリが同じインスタンスに対応付けられている場合には、VLAN はそのインスタンスにマッピングされています。リスト内の複数のエントリが異なる MISTP インスタンスに対応付けられている場合には、VLAN に矛盾があります。

この矛盾を解消するには、ルート スイッチから誤ったマッピングを手動で削除する必要があります。この作業で残ったリスト エントリが、正式なマッピングになります。

VLAN マッピングの矛盾を判別するには、イネーブル モードで次の作業を行います。

作業	コマンド
VLAN マッピングの矛盾を判別します。	**show spantree conflicts** *vlan*

次に、トポロジーの 3 番めのスイッチから見て、2 台の異なるスイッチ上にある MISTP インスタンス 1 および MISTP インスタンス 3 に、VLAN 2 をマッピングしようとしている例を示します。

```
Console> (enable) show spantree conflicts 2
Inst MAC               Delay     Time left
---- ----------------- --------- ---------
1   00-30-a3-4a-0c-00 inactive        20
3   00-30-f1-e5-00-01 inactive        10
```

Delay タイマーは、VLAN がインスタンスに加入するまでの残り時間（秒）を示します。このフィールドは、VLAN がインスタンスにすでにマッピングされている（タイマーが満了した）場合、または VLAN がインスタンス間で矛盾している場合には、*inactive* と表示されます。

Time Left タイマーは、エントリが期限切れとなり、テーブルから削除されるまでの残り時間（秒）を示します。このタイマーは、着信 BPDU によってマッピングが確認されるたびに再開されます。ルート スイッチに対応するエントリは、ルート スイッチ自身については *inactive* と表示されます。

次に、VTP バージョン 3 がイネーブルになっている例を示します。ルート スイッチは、非ルート スイッチに対してプライマリ サーバでもあります。ルート スイッチは矛盾のあるスイッチに対してはプライマリ サーバではありません。そうしたスイッチは分割されているからです。

次に、ルート スイッチからの例を示します。

```
Console> (enable) show spantree conflicts 1
No conflicts for vlan 1.
Inst MAC               Delay     Time left
---- ----------------- --------- ---------
  1  00-05-31-40-64-00  inactive  inactive
Console> (enable)
```

次に、非ルート スイッチからの例を示します。

```
Console> (enable) show spantree conflicts 3
No conflicts for vlan 3.
Inst MAC               Delay     Time left
---- ----------------- --------- ---------
  3  00-05-31-40-64-00  inactive        19
Console> (enable)
```

次に、矛盾のあるスイッチからの例を示します（スイッチは inactive になっていることに注意してください）。

```
Console> (enable) show spantree conflicts 6
Inst MAC               Delay     Time left
---- ----------------- --------- ---------
  6  00-05-31-40-64-00  inactive        18
  5  00-09-7b-62-b0-80  inactive  inactive

Console> (enable)
```

MISTP インスタンスからの VLAN マッピングの解除

特定の VLAN が現在マッピングされている MISTP インスタンスから、その VLAN のマッピングを解除するには、**none** キーワードを使用します。MISTP インスタンスから VLAN マッピングを解除すると、その VLAN（VLAN が存在する場合）のすべてのポートがブロッキング ステートになります。

MISTP インスタンスから特定の VLAN またはすべての VLAN マッピングを解除するには、イネーブル モードで次の作業を行います。

作業	コマンド
MISTP インスタンスから VLAN マッピングを解除します。	**set vlan** *vlan* **mistp-instance none**

次に、MISTP インスタンスから VLAN マッピングを解除する例を示します。

```
Console> (enable) set vlan 6 mistp-instance none
Vlan 6 configuration successful
```

MISTP-PVST+ または MISTP のディセーブル化

スイッチが MISTP モードのとき、スイッチ全体ではなく、特定のインスタンスについてスパニングツリーをディセーブルにします。

MISTP インスタンス上でスパニングツリーをディセーブルにすると、そのインスタンスは引き続きスイッチ上に存在しますが、インスタンスにマッピングされていたすべての VLAN のすべてのポートがフォワーディング ステートになり、インスタンス BPDU はフラッディングされます。

MISTP インスタンスをディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
MISTP インスタンスをディセーブルにします。	**set spantree disable mistp-instance** *instance* [**all**]

次に、MISTP インスタンスをディセーブルにする例を示します。

```
Console> (enable) set spantree disable mistp-instance 2
MI-STP instance 2 disabled.
```

ルート スイッチの設定

ここでは、ルート スイッチを設定する手順について説明します。

プライマリ ルート スイッチの設定

スイッチが PVST+ モードの場合は VLAN 上に、スイッチが MISTP モードの場合は MISTP インスタンス上に、ルート スイッチを設定できます。**set spantree root** コマンドを実行すると、ブリッジ プライオリティ（スイッチに対応付けられる値）がデフォルト（32768）から小さい値に変更され、そのスイッチをルート スイッチにすることができます。

スイッチをプライマリ ルートとして指定すると、そのスイッチが VLAN のルートになるように、デフォルトのブリッジ プライオリティが変更されます。スイッチは VLAN ごとに、現在のルート スイッチのブリッジ プライオリティを確認します。指定された VLAN のブリッジ プライオリティを 8192 に設定することによってスイッチがこの VLAN のルートになる場合は、ブリッジ プライオリティが 8192 に設定されます。指定された VLAN のルート スイッチのブリッジ プライオリティが 8192 より小さい場合、スイッチはその VLAN のブリッジ プライオリティを、最小のブリッジ プライオリティより 1 だけ小さい値に設定します。異なる VLAN ではルート スイッチが異なる可能性があるので、選択したブリッジ VLAN プライオリティによって、このスイッチが指定したすべての VLAN のルートになります。ブリッジ プライオリティを 1 まで下げてもスイッチがルート スイッチにならない場合には、メッセージが表示されます。

注意　**set spantree root** コマンドは、バックボーン スイッチまたは分配スイッチに対してだけ入力し、アクセス スイッチに対しては入力しないでください。

スイッチをプライマリ ルート スイッチとして設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
スイッチをプライマリ ルート スイッチとして設定します。	**set spantree root** [*vlans*] [**dia** *network_diameter*] [**hello** *hello_time*]

次に、VLAN 1 ～ 10 のプライマリ ルート スイッチを設定する例を示します。

```
Console> (enable) set spantree root 1-10 dia 4
VLANs 1-10 bridge priority set to 8192
VLANs 1-10 bridge max aging time set to 14 seconds.
VLANs 1-10 bridge hello time set to 2 seconds.
VLANs 1-10 bridge forward delay set to 9 seconds.
Switch is now the root switch for active VLANs 1-6.
Console> (enable)
```

スイッチをインスタンスのプライマリ ルート スイッチとして設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
スイッチをインスタンスのプライマリ ルート スイッチとして設定します。	**set spantree root mistp-instance** *instance* [**dia** *network_diameter*] [**hello** *hello_time*]

次に、インスタンスのプライマリ ルート スイッチを設定する例を示します。

```
Console> (enable) set spantree root mistp-instance 2-4 dia 4
Instances 2-4 bridge priority set to 8192
VLInstances 2-4 bridge max aging time set to 14 seconds.
Instances 2-4 bridge hello time set to 2 seconds.
Instances 2-4 bridge forward delay set to 9 seconds.
Switch is now the root switch for active Instances 1-6.
Console> (enable)
```

セカンダリ ルート スイッチの設定

スイッチが PVST+ モードの場合は VLAN 上に、スイッチが MISTP モードの場合は MISTP インスタンス上に、セカンダリ ルート スイッチを設定できます。

set spantree root secondary コマンドを実行すると、ブリッジ プライオリティが 16,384 に下がります。その結果、スイッチはプライマリ ルート スイッチの故障時にルート スイッチとなる候補スイッチになります。プライマリ ルート スイッチの故障に備えて、このコマンドを複数のスイッチで実行し、複数のバックアップ スイッチを作成できます。

スイッチをセカンダリ ルート スイッチとして設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
スイッチをセカンダリ ルート スイッチとして設定します。	**set spantree root** [**secondary**] *vlans* [**dia** *network_diameter*] [**hello** *hello_time*]

次に、VLAN 22 および 24 のセカンダリ ルート スイッチを設定する例を示します。

```
Console> (enable) set spantree root secondary 22,24 dia 5 hello 1
VLANs 22,24 bridge priority set to 16384.
VLANs 22,24 bridge max aging time set to 10 seconds.
VLANs 22,24 bridge hello time set to 1 second.
VLANs 22,24 bridge forward delay set to 7 seconds.
Console> (enable)
```

スイッチをインスタンスのセカンダリ ルート スイッチとして設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
スイッチをインスタンスのセカンダリ ルート スイッチとして設定します。	**set spantree root** [**secondary**] **mistp-instance** *instance* [**dia** *network_diameter*] [**hello** *hello_time*]

次に、インスタンスのセカンダリ ルート スイッチを設定する例を示します。

```
Console> (enable) set spantree root secondary mistp-instance 2-4 dia 4
Instances 2-4 bridge priority set to 8192
VLInstances 2-4 bridge max aging time set to 14 seconds.
Instances 2-4 bridge hello time set to 2 seconds.
Instances 2-4 bridge forward delay set to 9 seconds.
Switch is now the root switch for active Instances 1-6.
Console> (enable)
```

コンバージェンス向上のためのルート スイッチの設定

ルート スイッチの Hello タイム、転送遅延タイマー、最大エージング タイマーの各パラメータの値を小さくすると、コンバージェンス時間を減らすことができます。このようなタイマー設定の詳細については、「スイッチ上でのスパニングツリー タイマーの設定」（p.8-52）を参照してください。

（注） タイマーのパラメータ値を減らすことができるのは、ネットワークに 10 Mbps 以上の速度の LAN リンクが装備されている場合だけです。10 Mbps 以上の速度のリンクがあるネットワークでは、ネットワークの直径（ホップ数）は最大値の 7 に達します。WAN 接続では、パラメータを減らすことはできません。

ブリッジド ネットワークでリンク障害が発生すると、ネットワークの再構成はすぐには行われません。Hello タイム、転送遅延タイマー、最大エージング タイマーのデフォルトのパラメータ（IEEE 802.1D による指定）の再設定には、50 秒の遅延が必要になります。この再構成時間はネットワークの直径によって異なります。ネットワークの直径とは、任意の 2 つのエンド ステーション間のブリッジの最大数をいいます。

コンバージェンスをスピードアップするには、802.1D で認められているデフォルト以外のパラメータを使用します。14 秒の再コンバージェンスに対するデフォルト以外のパラメータについては、表 8-6 を参照してください。

表 8-6　デフォルト以外のパラメータ

パラメータ	時間
ネットワークの直径（dia）	2
Hello タイム	2 秒
転送遅延タイマー	4 秒
最大エージング タイマー	6 秒

（注） コンバージェンスを向上させるために、スイッチ ポートを PortFast モードに設定することもできます。PortFast モードでは、ポートがただちにフォワーディング ステートに移行するので、ディセーブル（リンクがダウン）からイネーブル（リンクがアクティブ）への移行しか行われません。PortFast モード以外のポートは、ブロッキングを開始すると、リスニング、ラーニングを経てからフォワーディング ステートになります。PortFast の詳細については、第 9 章「スパニングツリー PortFast、UplinkFast、BackboneFast、およびループ ガードの設定」の「PortFast の機能概要」（p.9-2）を参照してください。

コンバージェンスが向上するようにスパニングツリー パラメータを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	VLAN または MISTP インスタンスに Hello タイムを設定します。	**set spantree hello** *interval* [*vlan*] **mistp-instance** [*instances*]
ステップ 2	設定を確認します。	**show spantree** [*vlan* | **mistp-instance** *instances*]
ステップ 3	VLAN または MISTP インスタンスに転送遅延時間を設定します。	**set spantree fwddelay** *delay* [*vlan*] **mistp-instance** [*instances*]
ステップ 4	設定を確認します。	**show spantree** [*mod/port*] **mistp-instance** [*instances*] [**active**]
ステップ 5	VLAN または MST インスタンスに最大エージング タイムを設定します。	**set spantree maxage** *agingtime* [*vlans*] **mistp-instance** *instances*
ステップ 6	設定を確認します。	**show spantree** [*mod/port*] **mistp-instance** [*instances*] [**active**]

次に、スパニングツリーの Hello タイム、転送遅延タイマー、最大エージング タイマーを 2、4、および 6 秒に設定する例を示します。

```
Console> (enable) set spantree hello 2 100
Spantree 100 hello time set to 7 seconds.
Console> (enable)
Console> (enable) set spantree fwddelay 4 100
Spantree 100 forward delay set to 21 seconds.
Console> (enable)
Console> (enable) set spantree maxage 6 100
Spantree 100 max aging time set to 36 seconds.
Console> (enable)
Console> (enable) set spantree root 1-10 dia 4
VLANs 1-10 bridge priority set to 8192
VLANs 1-10 bridge max aging time set to 14 seconds.
VLANs 1-10 bridge hello time set to 2 seconds.
VLANs 1-10 bridge forward delay set to 9 seconds.
Switch is now the root switch for active VLANs 1-6.
Console> (enable)
```

ルート ガードの使用 — スイッチがルートにならないようにする方法

スイッチがルート スイッチにならないほうがよい場合があります。ルート ガードは、ポートを強制的に DP にし、リンクの反対側のスイッチがどれもルート スイッチにならないようにします。

ポート単位でルート ガードをイネーブルに設定すると、そのポートが属するすべてのアクティブ VLAN に、自動的にルート ガードが適用されます。ルート ガードをディセーブルにすると、指定したポートでルート ガードがディセーブルになります。ポートがルートに対して root-inconsistent ステートになると、そのポートは自動的にリスニング ステートになります。

スイッチがルートにならないようにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポート上でルート ガードをイネーブルにします。	**set spantree guard** {**root** | **none**} *mod/port*
ステップ 2	ルート ガードがイネーブルに設定されたことを確認します。	**show spantree guard** {*mod/port* | *vlan*} {**mistp-instance** *instance* | *mod/port*}

次に、ルート ガードをイネーブルにする例を示します。

```
Console> (enable) set spantree guard root 5/1
Rootguard on port 5/1 is enabled.
Warning!! Enabling rootguard may result in a topolopy change.
Console> (enable)
```

スパニングツリー BPDU 統計情報の表示

スパニングツリー BPDU（送信、受信、処理、廃棄）の総数を表示するには、**show spantree statistics bpdu** コマンドを実行します。このコマンドは、BPDU のレート（秒単位）も表示します。BPDU カウンタは、**clear spantree statistics bpdu** コマンド実行時、またはシステム起動時に消去されます。

スパニングツリー BPDU 統計情報を表示するには、ユーザ モードで次の作業を行います（統計情報の消去はイネーブル モードから行います）。

	作業	コマンド
ステップ 1	スパニングツリー BPDU 統計情報を表示します。	**show spantree statistics bpdu**
ステップ 2	BPDU 統計情報を消去します。	**clear spantree statistics bpdu**

次に、スパニングツリー BPDU 統計情報を表示する例を示します。

```
Console> show spantree statistics bpdu
              Transmitted       Received      Processed        Dropped
           -------------- -------------- -------------- --------------

Total            52943073       52016589       52016422            167

Rate(/sec)            989            971            971              0
```

次に、スパニングツリー BPDU 統計情報を消去する例を示します。

```
Console> (enable) clear spantree statistics bpdu
Spanning tree BPDU statistics cleared on the switch.
Console> (enable)
```

スイッチ上でのスパニングツリー タイマーの設定

スパニングツリー タイマーは、スパニングツリーのパフォーマンスに影響を及ぼします。PVST+ モードでは VLAN に、MISTP モードでは MISTP インスタンスに、スパニングツリー タイマーを設定できます。スイッチが PVST+ モードの場合、VLAN を指定しないと、VLAN 1 が指定されたものとみなされます。スイッチが MISTP モードの場合、MISTP インスタンスを指定しないと、MISTP インスタンス 1 が指定されたものとみなされます。

ここでは、スパニングツリー タイマーを設定する手順について説明します。

注意　これらのコマンドを使用する場合は注意してください。**set spantree root** および **set spantree root secondary** コマンドを使用して、スパニングツリーのパフォーマンス パラメータを変更することを推奨します。

表 8-7 で、スパニングツリーのパフォーマンスに影響を与えるスイッチ変数について説明します。

表 8-7　スパニングツリー タイマー

変数	説明	デフォルト
Hello タイム	スイッチから他のスイッチへ Hello メッセージをブロードキャストする間隔を決定します。	2 秒
最大エージング タイマー	ポートに関して記録された受信プロトコル情報の有効期間を計測し、その有効期間がスイッチによって記録されている最大エージ パラメータの値を超過した時点でその情報を廃棄するようにします。タイムアウト値は、スイッチの最大エージ パラメータです。	20 秒
転送遅延タイマー	ポートがラーニング ステートおよびリスニング ステートで費やした時間をモニタします。タイムアウト値は、スイッチの転送遅延パラメータです。	15 秒

Hello タイムの設定

set spantree hello コマンドを使用して、特定の VLAN、MISTP インスタンス、またはポート単位ベースで、Hello タイムを変更します。指定できる *interval* の範囲は 1 ～ 10 秒です。

VLAN または MISTP インスタンスにスパニングツリー ブリッジ Hello タイムを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	VLAN または MISTP インスタンスに Hello タイムを設定します。	**set spantree hello** *interval* {[*vlan*] | **mistp-instance** [*instances*] | **mst** [*mod*/*port*]}
ステップ 2	設定を確認します。	**show spantree** [*vlan* | **mistp-instance** *instances*]

次に、VLAN 100 のスパニングツリー Hello タイムを 7 秒に設定する例を示します。

```
Console> (enable) set spantree hello 7 100
Spantree 100 hello time set to 7 seconds.
Console> (enable)
```

次に、特定のインスタンスのスパニングツリー Hello タイムを 3 秒に設定する例を示します。

```
Console> (enable) set spantree hello 3 mistp-instance 1
Spantree 1 hello time set to 3 seconds.
Console> (enable)
```

次に、VLAN 4/5 のスパニングツリー Hello タイムを 4 秒に設定する例を示します。

```
Console> (enable) set spantree hello 4 mst 4/1
MST hello time set to 4 on port 4/1.
Console> (enable)
```

転送遅延時間の設定

set spantree fwddelay コマンドを使用して、特定の VLAN に関して、スパニングツリーの転送遅延時間を設定します。指定できる *delay* の範囲は 4 ～ 30 秒です。

VLAN のスパニングツリー転送遅延時間を設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	VLAN または MISTP インスタンスに転送遅延時間を設定します。	**set spantree fwddelay** *delay* [*vlan*] **mistp-instance** [*instances*]
ステップ 2	設定を確認します。	**show spantree** [*mod/port*] **mistp-instance** [*instances*] [**active**]

次に、VLAN 100 のスパニングツリー転送遅延時間を 21 秒に設定する例を示します。

```
Console> (enable) set spantree fwddelay 21 100
Spantree 100 forward delay set to 21 seconds.
Console> (enable)
```

次に、特定のインスタンスのブリッジ転送遅延時間を 16 秒に設定する例を示します。

```
Console> (enable) set spantree fwddelay 16 mistp-instance 1
Instance 1 forward delay set to 16 seconds.
Console> (enable)
```

最大エージング タイムの設定

set spantree maxage コマンドを使用して、特定の VLAN またはインスタンスに関して、スパニングツリーの最大エージング タイムを変更します。指定できる *agingtime* の範囲は 6 ～ 40 秒です。

VLAN またはインスタンスにスパニングツリー最大エージング タイムを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	VLAN または MST インスタンスに最大エージング タイムを設定します。	**set spantree maxage** *agingtime* [*vlans*] **mistp-instance** *instances*
ステップ 2	設定を確認します。	**show spantree** [*mod/port*] **mistp-instance** [*instances*] [**active**]

次に、VLAN 100 のスパニングツリー最大エージング タイムを 36 秒に設定する例を示します。

```
Console> (enable) set spantree maxage 36 100
Spantree 100 max aging time set to 36 seconds.
Console> (enable)
```

次に、特定のインスタンスの最大エージング タイムを 25 秒に設定する例を示します。

```
Console> (enable) set spantree maxage 25 mistp-instance 1
Instance 1 max aging time set to 25 seconds.
Console> (enable)
```

スイッチ上での MST の設定

ここでは、MST の設定手順について説明します。

MST のイネーブル化

スイッチ上で MST をイネーブルにして設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	PSVT+ モードを開始します。	**set spantree mode pvst+** [**mistp** | **pvst+** | **mistp-pvst+** | **mst**]
ステップ 2	STP ポートを表示します。	**show spantree active**
ステップ 3	MST リージョンを設定します。	**set spantree mst config** {[**name** *name*] | [**revision** *number*] [**commit** | **rollback** | **force**]}
ステップ 4	設定を確認します。	**show spantree mst config**
ステップ 5	VLAN を MSTI にマッピングします。	**set spantree mst** *instance* **vlan** *vlan*
ステップ 6	新しいリージョン マッピングをコミットします。	**set spantree mst config commit**
ステップ 7	MST を有効にします。	**set spantree mode mst** [**mistp** | **pvst+** | **mistp-pvst+** | **mst**]
ステップ 8	MST 設定を確認します。	**show spantree mst config**
ステップ 9	MSTI 設定を確認します。	**show spantree mst** *instance*
ステップ 10	MST モジュールおよびポートの設定を確認します。	**show spantree mst** *mod/port*

次に、MST をイネーブルにする例を示します。

```
Console> (enable)
Console> (enable) set spantree mode pvst+
Spantree mode set to PVST+.
Console> (enable) show spantree active
VLAN 1
Spanning tree mode          PVST+
Spanning tree type          ieee
Spanning tree enabled

Designated Root             00-60-70-4c-70-00
Designated Root Priority    16384
Designated Root Cost        19
Designated Root Port        3/48
Root Max Age   14 sec   Hello Time 2  sec   Forward Delay 10 sec

Bridge ID MAC ADDR          00-d0-00-4c-18-00
Bridge ID Priority          32768
Bridge Max Age 20 sec   Hello Time 2  sec   Forward Delay 15 sec

Port                     Vlan Port-State    Cost      Prio Portfast Channel_id
------------------------ ---- ------------- --------- ---- -------- ----------
 3/48                    1    forwarding           19   32 disabled 0
 7/2                     1    forwarding            4   32 enabled  0
Console> (enable) set spantree mst config name cisco revision 1
Edit Buffer modified.
Use 'set spantree mst config commit' to apply the changes
```

```
Console> (enable) show spantree mst config
Current (NVRAM) MST Region Configuration:              1 instance
Configuration Name:                                    Revision: 0
Instance VLANs
-------- ------------------------------------------------------------
   0     1-4094
================================================================================
NEW MST Region Configuration (Not committed yet)       1 instance
Configuration Name: cisco                              Revision: 1
Instance VLANs
-------- ------------------------------------------------------------
   0     1-4094
================================================================================
Edit buffer is locked by: Console (pid 143)
Console> (enable) set spantree mst 1 vlan 2-10
Edit Buffer modified.
Use 'set spantree mst config commit' to apply the changes
Console> (enable) set spantree mst 2 21-30
Usage:set spantree mst <instance> vlan <vlan>
Console> (enable) set spantree mst 2 vlan 21-30
Edit Buffer modified.
Use 'set spantree mst config commit' to apply the changes
Console> (enable) set spantree mst 3 vlan 31-40
Edit Buffer modified.
Use 'set spantree mst config commit' to apply the changes
Console> (enable) set spantree mst 4 vlan 41-50
Edit Buffer modified.
Use 'set spantree mst config commit' to apply the changes
Console> (enable) show spantree mst config
Current (NVRAM) MST Region Configuration:              1 instance
Configuration Name:                                    Revision: 0
Instance VLANs
-------- ------------------------------------------------------------
   0     1-4094
================================================================================
NEW MST Region Configuration (Not committed yet)       5 instances
Configuration Name: cisco                              Revision: 1
Instance VLANs
-------- ------------------------------------------------------------
   0     1,11-20,51-4094
   1     2-10
   2     21-30
   3     31-40
   4     41-50
================================================================================
Edit buffer is locked by: Console (pid 143)
Console> (enable) set spantree mst config commit
Console> (enable) show spantree mst config
Current (NVRAM) MST Region Configuration:              5 instances
Configuration Name: cisco                              Revision: 1
Instance VLANs
-------- ------------------------------------------------------------
   0     1,11-20,51-4094
   1     2-10
   2     21-30
   3     31-40
   4     41-50
================================================================================
Console> (enable) set spantree mode mst
PVST+ database cleaned up.
Spantree mode set to MST.
Console> (enable) show spantree mst 0
Spanning tree mode          MST
Instance                    0
VLANs Mapped:               1,11-20,51-4094

Designated Root             00-60-70-4c-70-00
Designated Root Priority    16384  (root priority: 16384, sys ID ext: 0)
Designated Root Cost        200000
```

```
Designated Root Port        3/48
Root Max Age   14 sec   Forward Delay 10 sec

CIST Regional Root          00-d0-00-4c-18-00
CIST Regional Root Priority 32768
CIST Internal Root Cost     0          Remaining Hops 20

Bridge ID MAC ADDR          00-d0-00-4c-18-00
Bridge ID Priority          32768  (bridge priority: 32768, sys ID ext: 0)
Bridge Max Age 20 sec   Hello Time 2  sec   Forward Delay 15 sec  Max Hops 20

Port                     State         Role Cost      Prio Type
------------------------ ------------- ---- --------- ---- --------------------
 3/48                    forwarding    ROOT    200000   32 Shared, Boundary(STP)
 7/2                     forwarding    DESG     20000   32 P2P, Edge
Console> (enable) show spantree mst 1
Spanning tree mode          MST
Instance                    1
VLANs Mapped:               2-10

Designated Root             00-00-00-00-00-00
Designated Root Priority    0  (root priority: 0, sys ID ext: 0)
Designated Root Cost        0          Remaining Hops 0
Designated Root Port        1/0

Bridge ID MAC ADDR          00-d0-00-4c-18-00
Bridge ID Priority          32769  (bridge priority: 32768, sys ID ext: 1)

Port                     State         Role Cost      Prio Type
------------------------ ------------- ---- --------- ---- --------------------
Console> (enable) show spantree mst 7/2
Edge Port:          Yes, (Configured) Enable
Link Type:          P2P, (Configured) Auto
Port Guard:    Default
Boundary:            No
Hello:                2, (Local bridge hello: 2)

Inst State         Role Cost      Prio VLANs
---- ------------- ---- --------- ---- ----------------------------------
   0 forwarding    DESG     20000   32 1
Console> (enable) show spantree mst config
Current (NVRAM) MST Region Configuration:              5 instances
Configuration Name: cisco                              Revision: 1
Instance VLANs
-------- ------------------------------------------------------------
   0     1,11-20,51-4094
   1     2-10
   2     21-30
   3     31-40
   4     41-50
==============================================================================
Console> (enable)
```

MST ブリッジ ID プライオリティの設定

スイッチが MST モードのとき、MSTI のブリッジ ID プライオリティを設定できます。

ブリッジ プライオリティ値はシステム ID エクステンション（MSTI の ID）と組み合わされ、ブリッジ ID プライオリティを形成します。次の 16 種類のブリッジ プライオリティ値のいずれかを設定できます。0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、および 61440 です。

MSTI にブリッジ ID プライオリティを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	MSTI のブリッジ ID プライオリティを設定します。	**set spantree priority** *bridge_priority* **mst** [*instance*]
ステップ 2	ブリッジ ID プライオリティを確認します。	**show spantree mst** [*instance* | *mod/port*]

次に、MSTI のブリッジ ID プライオリティを設定する例を示します。

```
Console> (enable) set spantree priority 8192 mst 3
set spantree priority 8192 mst 3
MST instance 3 bridge ID priority set to 8195
(bridge priority: 8192 + sys ID extension: 3)
Console> (enable) show spantree mst 3
Spanning tree mode          MST
Instance                    3
VLANs Mapped:               31-40

Designated Root             00-00-00-00-00-00
Designated Root Priority    0  (root priority: 0, sys ID ext: 0)
Designated Root Cost        0          Remaining Hops 0
Designated Root Port        1/0

Bridge ID MAC ADDR          00-d0-00-4c-18-00
Bridge ID Priority          8195  (bridge priority: 8192, sys ID ext: 3)

Port                     State         Role Cost      Prio Type
------------------------ ------------- ---- --------- ---- --------------------
6/1                       forwarding   MSTR     2000   32   P2P, Boundary (PVST)
6/2                       blocking     MSTR     2000   32   P2P, Boundary (PVST)
```

MST ポート コストの設定

スイッチ ポートのポート コストを設定できます。ポート コストが小さいポートほど、フレームを転送するポートとして選択される可能性が高くなります。高速メディア（全二重など）に接続するポートには小さい値を、低速メディアに接続するポートには大きい値を割り当ててください。ポート コストの計算にショート法を使用している場合、使用できるコストの値は 1 ～ 65535 で、ロング法を使用している場合は 1 ～ 200000000 です。デフォルトのコストは、メディアによって異なります。ポート コストの計算手順については、「ポート コストの計算および割り当て」（p.8-4）を参照してください。

ポートにポート コストを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチ ポートの MST ポート コストを設定します。	**set spantree portcost** *mod/port cost* [**mst**]
ステップ 2	ポート コストの設定を確認します。	**show spantree mst** [*instance* | *mod/port*]

次に、MSTI 上にポート コストを設定し、設定を確認する例を示します。

```
Console> (enable) set spantree portcost 6/1 10000 mst
Spantree port 6/1 path cost set to 10000.
Console> (enable)
Console> (enable) show spantree mst 6/1
Edge Port:       No,  (Configured) Default
Link Type:      P2P,  (Configured) Auto
Port Guard:   Default
Boundary:     Yes (PVST)

Inst State         Role Cost      Prio VLANs
---- ------------- ---- --------- ----------------------------------------
   0 forwarding    ROOT     10000   32 1
   1 forwarding    MSTR     10000   32 2-20
   2 forwarding    MSTR     10000   32 21-30
   3 forwarding    MSTR     10000   32 31-40
   4 forwarding    MSTR     10000   32 41-50
Console> (enable)
```

MST ポート プライオリティの設定

ポートのポート プライオリティを設定できます。プライオリティ値が最小のポートが、すべての VLAN のフレームを転送します。指定できるポート プライオリティ値は、0 ～ 240 の範囲の 16 の倍数です。デフォルトは 32 です。すべてのポートに同じプライオリティ値を指定した場合、ポート番号が最小のポートがフレームを転送します。

ポートにポート プライオリティを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポートに MST ポート プライオリティを設定します。	**set spantree portpri** *mod/port priority* [**mst**]
ステップ 2	ポート プライオリティの設定を確認します。	**show spantree mst** [*instance* | *mod/port*]

次に、ポート プライオリティを設定し、設定を確認する例を示します。

```
Console> (enable) set spantree portpri 6/1 30 mst
Bridge port  6/1 port priority set to 30.
Console> (enable)
Console> (enable) show spantree mst 6/1
Edge Port:       No,  (Configured) Default
Link Type:      P2P,  (Configured) Auto
Port Guard:   Default
Boundary:     Yes (PVST)

Inst State         Role Cost      Prio VLANs
---- ------------- ---- --------- ----------------------------------------
   0 forwarding    ROOT     10000   30 1
   1 forwarding    MSTR     10000   30 2-20
   2 forwarding    MSTR     10000   30 21-30
   3 forwarding    MSTR     10000   30 31-40
   4 forwarding    MSTR     10000   30 41-50
Console> (enable)
```

MST ポート インスタンス コストの設定

MSTI にポート インスタンス コストを設定できます。インスタンス コストが小さいポートほど、フレームを転送するポートとして選択される可能性が高くなります。高速メディア（全二重など）に接続するポートには小さい値を、低速メディアに接続するポートには大きい値を割り当ててください。デフォルトのコストは、メディアによって異なります。ポート インスタンス コストに設定できる値の範囲は、1 ～ 268435456 です。

トランク ポート内のインスタンスには、別のポート インスタンス コストを割り当てられます。

ポートにポート インスタンス コストを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポート上での MST ポート インスタンス コストを設定します。	**set spantree portinstancecost** *mod/port* [**cost** *cost*] **mst** [*instances*]
ステップ 2	ポート上での MST インスタンスのパス コストを確認します。	**show spantree portinstancecost** *mod/port* **mst**

次に、特定のポート上で MST ポート インスタンス コストを設定する例を示します。

```
Console> (enable) set spantree portinstancecost 4/1 cost 5000 mst 4
Command successful. Modified port 4/1 configuration:
        Cost       Instances
        ---------- ------------------------------------------------------------
        5000       4
Default 200000     0-3,5-4094
Console> (enable) set spantree portinstancecost 4/1 cost 6000 mst 4000
Command successful. Modified port 4/1 configuration:
        Cost       Instances
        ---------- ------------------------------------------------------------
        5000       4
        6000       4000
Default 200000     0-3,5-3999,4001-4094

Console> (enable) show spantree portinstancecost 4/1
This command is not valid when STP is in MST mode.
Console> (enable) show spantree portinstancecost 4/1 mst
Port 4/1 cost configuration:
        Cost       Instances
        ---------- ------------------------------------------------------------
        5000       4
        6000       4000
Default 200000     0-3,5-3999,4001-4094
Console> (enable)
```

MST ポート インスタンス プライオリティの設定

MSTI にポート プライオリティを設定できます。特定の MSTI に対してプライオリティ値が最小のポートが、そのインスタンスにフレームを転送します。指定できるポート インスタンスの範囲は 0 ～ 240 です。特定の MSTI に関して、すべてのポートに同じプライオリティ値を指定した場合、ポート プライオリティ番号が最小のポートがそのインスタンスにフレームを転送します。

トランク ポート内のインスタンスには、別のポート インスタンス プライオリティを割り当てられます。

MSTI 上でポート インスタンス プライオリティを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	MSTI 上でポート インスタンス プライオリティを設定します。	**set spantree portinstancepri** *mod/port priority* **mst** [*instance*]
ステップ 2	ポート インスタンス プライオリティの設定を確認します。	**show spantree mst** [*instance* | *mod/port*]

次に、MSTI 上でポート インスタンス プライオリティを設定し、設定を確認する例を示します。

```
Console> (enable) set spantree portinstancepri 4/1 16 mst 2
Command successful. Modified port 4/1 configuration:
        Priority   Instances
        ---------- ------------------------------------------------------
        16         2
Default 32         0-1,3-4094
Console> (enable) set spantree portinstancepri 4/1 48 mst 200
Command successful. Modified port 4/1 configuration:
        Priority   Instances
        ---------- ------------------------------------------------------
        16         2
        48         200
Default 32         0-1,3-199,201-4094
Console> (enable) show spantree mst 4/1
Edge Port:          No, (Configured) Default
Link Type:         P2P, (Configured) Auto
Port Guard:   Default
Boundary:           No
Hello:               4, (Local port hello:4)

Inst State         Role Cost      Prio VLANs
---- ------------- ---- --------- ---- ---------------------------------
   0 forwarding    DESG    200000   32 None
   2 forwarding    DESG    200000   16 1
 200 forwarding    DESG    200000   48 2
Console> (enable)
```

MSTI への VLAN マッピングおよびマッピング解除

デフォルトでは、すべての VLAN が IST（インスタンス 0）にマッピングされます。MSTI 1 ～ 15 をアクティブにするには、少なくとも 1 つの VLAN を MSTI にマッピングする必要があります。IST は、VLAN が IST にマッピングされているかどうかに関係なく、必ずアクティブになります。MST には別個のリージョンを与えることによって、VLAN マッピングの矛盾を防止します。MSTI に対する VLAN のマッピングおよびマッピング解除については、次の注意事項に従ってください。

(注)　VLAN の詳しい使用手順および設定手順については、第 11 章「VLAN の設定」を参照してください。

- MSTI にマッピングできるのは、イーサネット VLAN だけです。
- MST をアクティブにするには、インスタンスで少なくとも 1 つの VLAN にアクティブ ポートがなければなりません。
- 1 つの MSTI に対し、必要に応じてイーサネット VLAN をいくつでもマッピングできます。
- 1 つの VLAN を、複数の MSTI にマッピングすることはできません。
- MST は、モジュールおよびすべてのスパニングツリーに設定された Hello タイム、最大エージング タイマー、および転送遅延タイマーをグローバルに使用します。

（注） VLAN 1025 ～ 4094 を使用するには、MAC アドレス リダクションをイネーブルにする必要があります。拡張範囲 VLAN の詳しい使用方法については、第 11 章「VLAN の設定」の「拡張範囲 VLAN の作成」（p.11-8）を参照してください。

MSTI に VLAN をマッピングするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	MSTI に VLAN をマッピングします。	**set spantree mst** *instance* **vlan** *vlan*
ステップ 2	新しいリージョン マッピングを有効にします。	**set spantree mst config commit**
ステップ 3	VLAN がマッピングされたことを確認します。	**show spantree mst** [*instance*] [**active**] *mod/port*

次に、MSTI 1 に VLAN をマッピングし、マッピングを確認する例を示します。

```
Console> (enable) show spantree mst config
Current (NVRAM) MST Region Configuration:             3 instances
Configuration Name:arthur                             Revision:23703
Instance VLANs
-------- ---------------------------------------------------------------
   0     1,31-4094
   2     2-20
   3     21-30
================================================================================
Console> (enable) set spantree mst 1400 vlan 900-999
Edit Buffer modified.
Use 'set spantree mst config commit' to apply the changes
Console> (enable) show spantree mst config
Current (NVRAM) MST Region Configuration:             3 instances
Configuration Name:arthur                             Revision:23703
Instance VLANs
-------- ---------------------------------------------------------------
   0     1,31-4094
   2     2-20
   3     21-30
================================================================================
NEW MST Region Configuration (Not committed yet)       4 instances
Configuration Name:arthur                             Revision:23703
Instance VLANs
-------- ---------------------------------------------------------------
   0     1,31-899,1000-4094
   2     2-20
   3     21-30
1400     900-999
================================================================================
Edit buffer is locked by:Console (pid 143)
Console> (enable) clear spantree mst 1400 vlan 900-998
Edit Buffer modified.
Use 'set spantree mst config commit' to apply the changes
Console> (enable) set spantree mst config commit
Console> (enable) show spantree mst config
Current (NVRAM) MST Region Configuration:             4 instances
Configuration Name:arthur                             Revision:23703
Instance VLANs
-------- ---------------------------------------------------------------
   0     1,31-998,1000-4094
   2     2-20
   3     21-30
1400     999
================================================================================
Console> (enable)
```

スイッチ上での BPDU スキューイングの設定

スパニングツリー BPDU スキューイング機能をサポートするコマンドは、次の機能を実行します。

- BPDU スキューイングをイネーブルまたはディセーブルにします。デフォルトの設定はディセーブルです。
- **show spantree summary** の出力を変更して、スキューの検出がイネーブルになっているかどうか、どの VLAN または PVST+/MISTP インスタンスに対するスキューが検出されたのかを表示します。
- スキューの影響を受けた VLAN、PVST+、または MISTP インスタンスとポートは、次のような情報が含まれる表示を行います。
  - 最後のスキューの期間（絶対時間）
  - 最も長いスキューの期間（絶対時間）
  - 最も長いスキューの日時

スパニングツリーが BPDU スキュー統計情報を収集する方法を変更するには、**set spantree bpdu-skewing** コマンドを使用します。**bpdu-skewing** コマンドは、ディセーブルがデフォルトの設定です。

VLAN について BPDU スキュー統計情報収集を設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	BPDU スキューイングを設定します。	**set spantree bpdu-skewing** [**enable** | **disable**]
ステップ 2	設定を確認します。	**show spantree bpdu-skewing** *vlan* [*mod/port*] **show spantree bpdu-skewing mistp-instance** [*instance*] [*mod/port*]

次に、BPDU スキューイングを設定し、スキュー統計情報を表示する例を示します。

```
Console> (enable) set spantree bpdu-skewing
Usage:set spantree bpdu-skewing <enable|disable>
Console> (enable) set spantree bpdu-skewing enable
Spantree bpdu-skewing enabled on this switch.
Console> (enable)

Console> (enable) show spantree bpdu-skewing 1
Bpdu skewing statistics for vlan 1
Port    Last Skew ms   Worst Skew ms     Worst Skew Time
------  -------------  -------------  -------------------------
8/2              5869         108370  Tue Nov 21 2000, 06:25:59
8/4              4050         113198  Tue Nov 21 2000, 06:26:04
8/6            113363         113363  Tue Nov 21 2000, 06:26:05
8/8              4111         113441  Tue Nov 21 2000, 06:26:05
8/10           113522         113522  Tue Nov 21 2000, 06:26:05
8/12             4111         113600  Tue Nov 21 2000, 06:26:05
8/14           113678         113678  Tue Nov 21 2000, 06:26:05
8/16             4111         113755  Tue Nov 21 2000, 06:26:05
8/18           113833         113833  Tue Nov 21 2000, 06:26:05
8/20             4111         113913  Tue Nov 21 2000, 06:26:05
8/22           113917         113917  Tue Nov 21 2000, 06:26:05
8/24             4110         113922  Tue Nov 21 2000, 06:26:05
8/26           113926         113926  Tue Nov 21 2000, 06:26:05
8/28             4111         113931  Tue Nov 21 2000, 06:26:05
Console> (enable)
```

次に、モジュール 8、ポート 2 の VLAN 1 について、BPDU スキューイングを設定し、スキュー統計情報を表示する例を示します。

```
Console> (enable) show spantree bpdu-skewing 1 8/4
Bpdu skewing statistics for vlan 1
Port    Last Skew ms   Worst Skew ms     Worst Skew Time
------  -------------  -------------  -------------------------
8/4              5869         108370  Tue Nov 21 2000, 06:25:59
```

MISTP が稼働中の場合と同様の出力が表示されます。

show spantree summary コマンドは、BPDU スキュー検出がイネーブルになっているかどうかを示し、スキューで影響を受けた VLAN またはインスタンスの一覧も表示します。次に、**show spantree summary** コマンドの出力例を示します。

```
Console> (enable) show spantree summary
Root switch for vlans: 1
BPDU skewing detection enabled for the bridge
BPDU skewed for vlans: 1
Portfast bpdu-guard disabled for bridge.
Portfast bpdu-filter disabled for bridge.
Uplinkfast disabled for bridge.
Backbonefast disabled for bridge.

Summary of connected spanning tree ports by vlan

VLAN  Blocking Listening Learning Forwarding STP Active
----- -------- --------- -------- ---------- ----------
    1        6         4        2          0         12

      Blocking Listening Learning Forwarding STP Active
----- -------- --------- -------- ---------- ----------
Total      6         4        2          0         12
Console> (enable)
```

スイッチ上でのレイヤ 2 PDU レート制限の設定

（注） この機能がサポートされるのは、PFC3A 以上の PFC が搭載されている場合のみです。

（注） この機能は、truncated モードでは動作しません。

レイヤ 2 PDU レート リミッタを使用して、パケット数を通常のレートに制限し、異常な入力レートを回避することができます。

レイヤ 2 PDU レート制限をサポートするコマンドにより、次のような機能が実行できます。

- スパニングツリー BPDU（IEEE および PVST/SSTP、CDP、Dynamic Trunking Protocol [DTP; ダイナミック トランキング プロトコル]、UDLD、VTP、Link Aggregation Control Protocol [LACP]、および PAgP）のレート制限をスイッチ上でグローバルにイネーブル化、ディセーブル化、または設定すること
- レイヤ 2 プロトコル トンネルカプセル化 PDU のレート制限を、スイッチ上でグローバルにイネーブル、ディセーブル、設定すること
- 802.1x ポート セキュリティ レート リミッタをスイッチ上でグローバルにイネーブル、ディセーブル、設定すること

3 種類すべてのレート リミッタは、互いに独立して動作します。

レイヤ 2 PDU レート制限をイネーブルにするには、**set rate-limit** {**l2pdu** | **l2port-security** | **l2protocol-tunnel**} {**enable** | **disable**} コマンドを入力します。レイヤ 2 PDU レート制限はデフォルトでディセーブルです。

レイヤ 2 PDU レート制限を設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	レイヤ 2 PDU レート制限をイネーブルにします。	**set rate-limit** {**l2pdu** | **l2port-security** | **l2protocol-tunnel**} **enable**
ステップ 2	レート リミッタ値を設定します。	**set rate-limit** {**l2pdu** | **l2port-security** | **l2protocol-tunnel**} **rate** *rate*
ステップ 3	設定を確認します。	**show rate-limit** **show rate-limit config**

次のようなレイヤ 2 プロトコル パケットのレート制限を実行するには、**l2pdu** キーワードを使用します。

- スパニングツリー IEEE ― 宛先 MAC アドレス 01-80-c2-00-00-00
- PVST/SSTP ― 宛先 MAC アドレス 01-00-0C-CC-CC-CD
- CDP/DTP/UDLD/LACP/PAgP/VTP ― 宛先 MAC アドレス 01-00-0C-CC-CC-CC

（注） レイヤ 2 プロトコルのレート制限の仕組みは、次のとおりです。1) 宛先 MAC アドレス（上記）によって、フレームがレイヤ 2 制御フレームとして分類されます。2) これらのフレームに LTL インデックスが割り当てられます。3) LTL インデックスがフォワーディング エンジンに送られて、関連するすべてのフレームの（集約）レート制限が実行されます。

レイヤ 2 802.1x ポート セキュリティ パケットのレート制限には、**l2port-security** キーワードを使用します。

MAC アドレス（01-00-0C-CD-CD-D0）のレイヤ 2 プロトコル トンネルカプセル化パケットのレート制限には、**l2protocol-tunnel** キーワードを使用します。

次に、レイヤ 2 レート制限をイネーブルにし、レート リミッタ値を設定し、設定を確認する例を示します。

```
Console>(enable) set rate-limit l2pdu enable
Layer 2 rate limiter for PDUs enabled on the switch.
Console>(enable)

Console>(enable) set rate-limit l2pdu rate 1000
Layer 2 rate limiter for PDU rate set to 1000.
Console>(enable)

Console>(enable) set rate-limit l2protocol-tunnel disable
Layer 2 rate limiter for l2protocol-tunnel disabled on the switch.
Console>(enable)

Console>(enable) show rate-limit
Configured Rate Limiter Settings:
Rate Limiter Type    Status  Rate (pps)     Burst
-------------------- ------  -------------- -----
VACL LOG             On      2500           1
ARP INSPECTION       On      500            1
L2 PDU               On      1000           1
L2 PROTOCOL TUNNEL   On      1000           1
L2 PORT SECURITY     On      1000           1
MCAST NON RPF        Off     *              *
MCAST DFLT ADJ       Off     *              *
MCAST DIRECT CON     Off     *              *
ACL INGRESS BRIDGE   Off     *              *
ACL EGRESS BRIDGE    Off     *              *
L3 SEC FEATURES      Off     *              *
FIB RECEIVE          Off     *              *
FIB GLEAN            Off     *              *
MCAST PARTIAL SC     Off     *              *
RPF FAIL             Off     *              *
TTL FAIL             Off     *              *
NO ROUTE             Off     *              *
ICMP UNREACHABLE     Off     *              *
ICMP REDRECT         Off     *              *
MTU FAIL             Off     *              *
Console>(enable)
```

次に、レイヤ 2 レート リミッタ管理および操作ステータス情報を表示する例を示します。

```
Console> show rate-limit config

Rate Limiter Type    Admin Status Oper Status
-------------------- ------------ -----------
l2pdu                On           On
l2protocol-tunnel    On           On
l2port-security      On           On
Console>
```

CHAPTER 9

スパニングツリー PortFast、UplinkFast、BackboneFast、およびループ ガードの設定

この章では、Catalyst 6500 シリーズ スイッチ上でスパニングツリー PortFast、UplinkFast、BackboneFast、およびループ ガード機能を設定する方法について説明します。

(注) Spanning-Tree Protocol（STP; スパニングツリー プロトコル）の設定については、第 8 章「スパニングツリーの設定」を参照してください。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

この章で説明する内容は、次のとおりです。

PortFast の機能概要

スパニングツリー PortFast 機能により、スイッチ ポートまたはトランク ポートが直接スパニングツリー フォワーディング ステートになり、リスニング ステートとラーニング ステートが省略されます。

単一ワークステーション、スイッチ、またはサーバに接続されたスイッチ ポートまたはトランク ポート上で PortFast を使用すると、ポートがリスニング ステート、ラーニング ステートを経てフォワーディング ステートに移行するのを待たずに、これらの装置をただちにネットワークに接続することができます。

注意　PortFast は、単一エンド ステーションまたはスイッチ ポートとスイッチ ポートの接続に使用できます。スイッチなど、別のレイヤ 2 装置に接続されたポートで PortFast をイネーブルにすると、ネットワーク ループが生じる可能性があります。

スイッチの起動時、または装置がポートに接続された時点で、ポートはスパニングツリー リスニング ステートになります。転送遅延タイマーが満了すると、ポートはラーニング ステートになります。さらにもう一度、転送遅延タイマーが満了すると、ポートはフォワーディング ステートまたはブロッキング ステートに移行します。

スイッチ ポートまたはトランク ポート上で PortFast をイネーブルにすると、ポートはただちにスパニングツリー フォワーディング ステートに移行します。

PortFast BPDU ガードの機能概要

Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）ガードは、ポートが BPDU を受信した場合に、そのポートを errdisable ステートに移すことによってスパニングツリー ループを防止します。スイッチ上で BPDU ガード機能をイネーブルに設定した場合、インターフェイスが BPDU を受信すると、スパニングツリーはそのインターフェイスをスパニングツリー ブロッキング ステートにする代わりにシャットダウンします。BPDU ガードをグローバルにイネーブルに設定し、ポート単位の設定では BPDU ガードをデフォルトにした場合（「スイッチ上での PortFast BPDU ガードの設定」[p.9-13] を参照）、BPDU ガードがイネーブルになるかディセーブルになるかは PortFast の設定によって決まります。

ポートの設定がデフォルトでない場合、PortFast は BPDU ガードの設定に影響しません。表 9-1 に、BPDU ガードに関するポート設定のすべての可能性を示します。BPDU ガード機能では、管理者がインターフェイスを手動でサービス状態に戻す必要があるので、無効な設定を防止できます。

表 9-1　BPDU ガードのポート設定

ポート単位の設定	グローバル設定	PortFast 動作値	BPDU ガードの動作
デフォルト	イネーブル	イネーブル	イネーブル
デフォルト	イネーブル	ディセーブル	ディセーブル
デフォルト	ディセーブル	X	ディセーブル
ディセーブル	X	X	ディセーブル
イネーブル	X	X	イネーブル

PortFast BPDU フィルタリングの機能概要

BPDU フィルタリングを使用することにより、エンド システムに接続されたポート上で BPDU が送信されないようにすることができます。スイッチ上で BPDU フィルタリングをイネーブルに設定した場合、スパニングツリーは、リスニングとラーニングのステートを経ずにポートをただちにフォワーディング ステートにします。BPDU フィルタリングをグローバルにイネーブルに設定し、ポート単位の設定では BPDU フィルタリングをデフォルトにした場合（「スイッチ上での PortFast BPDU フィルタリングの設定」[p.9-16] を参照）、BPDU フィルタリングがイネーブルになるかディセーブルになるかは PortFast の設定によって決まります。

ポートの設定がデフォルトでない場合、PortFast の設定は BPDU フィルタリングに影響しません。表 9-2 に、BPDU フィルタに関するすべての設定の組み合わせを示します。BPDU フィルタは、エンド ホストが接続されるとすぐに、アクセス ポートがフォワーディング ステートに直接移行できるようにします。

表 9-2　BPDU フィルタのポート設定

ポート単位の設定	グローバル設定	PortFast 動作値	BPDU フィルタの動作
デフォルト	イネーブル	イネーブル	イネーブル[1]
デフォルト	イネーブル	ディセーブル	ディセーブル
デフォルト	ディセーブル	X	ディセーブル
ディセーブル	X	X	ディセーブル
イネーブル	X	X	イネーブル

1. ポートは少なくとも 10 個の BPDU を送信します。このポートが BPDU を受信すると、PortFast の動作値はディセーブル、BPDU フィルタの動作もディセーブルになります。

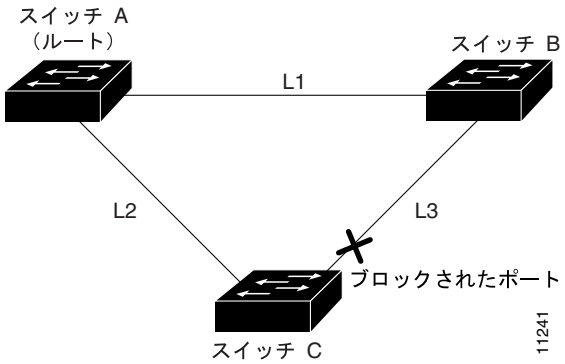
UplinkFast の機能概要

UplinkFast は、スパニングツリー トポロジーの変化後に高速コンバージェンスを行い、アップリンク グループを使用する冗長リンク間でロードバランシングを行います。アップリンク グループは、（VLAN［仮想 LAN］ごとの）ポートの集合であり、どの時点でも、その中の 1 つのポートだけが転送を行います。すなわち、アップリンク グループは、（転送を行う）ルート ポートと、ブロックされたポートの集合で構成されます。ブロックされたポートにはセルフループ ポートは含まれていません。アップリンク グループは、現在転送中のリンクで障害が起きた場合に代替パスを提供します。

(注)　UplinkFast は、配線クローゼット スイッチに使用すると最も効果的です。それ以外の用途には、有効でない場合があります。

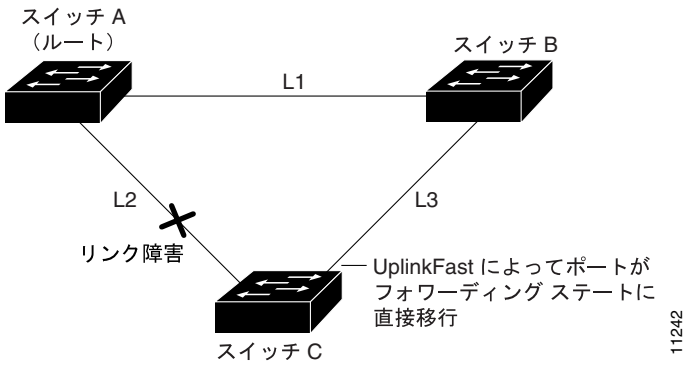
図 9-1 に、リンク障害が発生する前のトポロジーの例を示します。ルート スイッチであるスイッチ A は、リンク L1 を介してスイッチ B に、リンク L2 を介してスイッチ C に直接接続されています。スイッチ B に直接接続されているスイッチ C のポートは、ブロッキング ステートです。

図 9-1　直接リンク障害発生前の UplinkFast の例



スイッチ C が、現在アクティブ リンクである L2 上でリンク障害（直接リンク障害）を検出すると、UplinkFast がスイッチ C 上でブロックされていたポートのブロックを解除し、リスニング ステートおよびラーニング ステートを経ずに、ただちにフォワーディング ステートに移行させます（図 9-2 を参照）。このスイッチオーバーに要する時間は、1 ～ 5 秒ほどです。

図 9-2　直接リンク障害発生後の UplinkFast の例



BackboneFast の機能概要

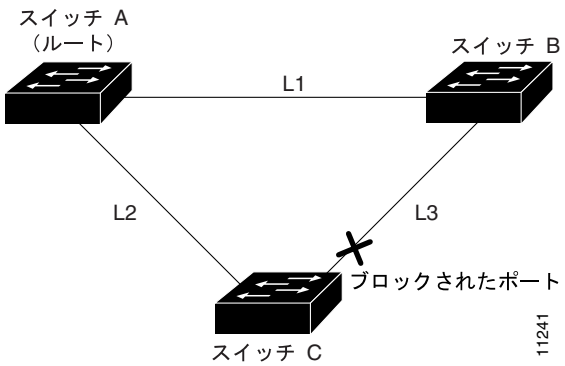
スイッチ上のルート ポートまたはブロックされたポートが、そのポートの指定ブリッジから下位 BPDU を受信すると、BackboneFast が開始されます。下位 BPDU は、1 台のスイッチをルート ブリッジおよび指定ブリッジの両方として識別します。スイッチが下位 BPDU を受信すると、スイッチはそのスイッチが直接接続されていないリンク（間接リンク）で障害が発生した（つまり、指定ブリッジのルート ブリッジへの接続が切断された）ものとみなします。標準的なスパニングツリー ルールに従っている場合、スイッチは設定済みの最大エージング タイム（**set spantree maxage** コマンドの *agingtime* 変数で指定）にわたって下位 BPDU を無視します。

スイッチは、ルート ブリッジへの代替パスの有無を判別します。下位 BPDU がブロック ポートの 1 つに着信すると、スイッチのルート ポートとその他のブロックされたポートがルート ブリッジの代替パスになります（セルフループ ポートはルート ブリッジの代替パスとはみなされません）。下位 BPDU がルート ポートに到達した場合には、すべてのブロックされたポートがルート ブリッジへの代替パスになります。下位 BPDU がルート ポートに到達し、かつブロックされたポートがない場合には、スイッチはルート ブリッジへの接続が切断されたものとみなし、ルートの最大エージング タイムを満了させ、通常のスパニングツリー ルールに従ってルート スイッチになります。

スイッチにルート ブリッジへの代替パスがある場合、スイッチはそれらの代替パスを使用して、ルート ブリッジへのすべての代替パスに対して、Root Link Query Protocol Data Unit（PDU; プロトコル データ ユニット）と呼ばれる新しい種類の PDU を送信します。ルートへの代替パスがまだあることを判別すると、スイッチは、下位 BPDU を受信したポートの最大エージング タイムを満了させます。ルート ブリッジに対するすべての代替パスが、スイッチとルート ブリッジ間の接続が切断されていることを示している場合には、スイッチは、下位 BPDU を受信したポートの最大エージング タイムを満了させます。1 つまたは複数の代替パスからルート ブリッジに引き続き接続できる場合には、スイッチは、下位 BPDU を受信したすべてのポートを Designated Port（DP; 指定ポート）にして、（ブロッキング ステートになっていた場合）ブロッキング ステートから除外して、リスニング ステートおよびラーニング ステートを経て、フォワーディング ステートに移行させます。

図 9-3 に、リンク障害が発生する前のトポロジーの例を示します。ルート スイッチであるスイッチ A は、リンク L1 を介してスイッチ B に、また、リンク L2 を介してスイッチ C に直接接続されています。スイッチ B に直接接続されているスイッチ C のポートは、ブロッキング ステートです。

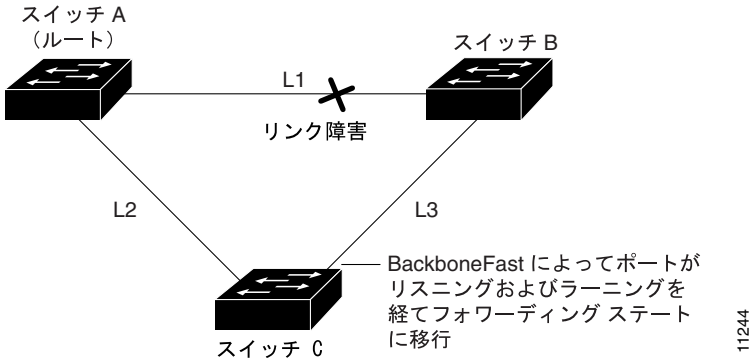
図 9-3　間接リンク障害発生前の BackboneFast の例



リンク L1 で障害が起きた場合、スイッチ C がリンク L1 に直接接続されていないため、スイッチ C はその障害を間接障害として検出します。スイッチ B には、ルート スイッチまでのパスがありません。BackboneFast により、スイッチ C のブロックされたポートは、そのポートに設定されている最大エージング　タイムの満了を待たずに、ただちにリスニング　ステートに移行します。

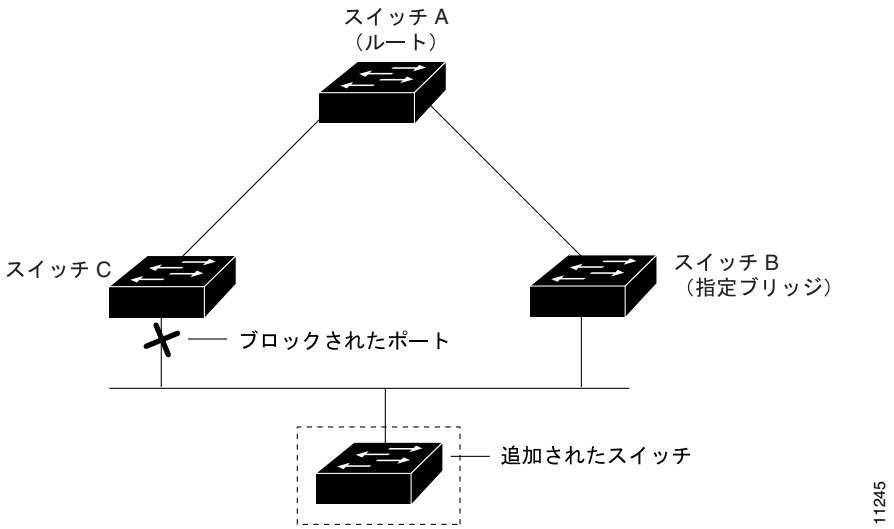
BackboneFast はさらに、スイッチ C のポートをフォワーディング ステートに移行させ、スイッチ B からスイッチ A までのパスを提供します。このスイッチオーバーに要する時間は、約 30 秒です。図 9-4 に、BackboneFast がリンク L1 で発生した障害に応じてどのようにトポロジーを再設定するかを示します。

図 9-4　間接リンク障害発生後の BackboneFast の例



新しいスイッチがメディア共有型トポロジーに組み込まれた場合、BackboneFast は起動されません。図 9-5 に、新しいスイッチが追加されたメディア共有型トポロジーを示します。新しいスイッチは、自分がルート スイッチであることを伝える下位 BPDU の送信を開始します。ただし、他のスイッチはこれらの下位 BPDU を無視します。その結果、新しいスイッチはスイッチ B がルート スイッチであるスイッチ A への指定ブリッジであることを学習します。

図 9-5　メディア共有型トポロジーにおけるスイッチの追加



ループ ガードの機能概要

BPDU がない場合には、単一方向リンク障害によって、ルート ポートまたは代替ポートがルートとして指定される可能性があります。ソフトウェア障害によってはネットワークに一時的なループが引き起こされる場合があります。ループ ガードは、ルート ポートまたは代替ポートが BPDU を受信するかどうかを確認します。ポートが BPDU を受信していない場合、ループ ガードは、再度 BPDU の受信を始めるまで、ポートを inconsistent ステートにします。ループ ガードは障害を切り離して、スパニングツリーを障害リンクや障害ブリッジのない安定したトポロジーに収束させます。

ループ ガードは、ポート単位でイネーブルに設定できます。ループ ガードをイネーブルに設定すると、そのポートが属するすべてのアクティブなインスタンスまたは VLAN に、自動的にループ ガードが適用されます。ループ ガードをディセーブルにすると、指定したポートでループ ガードがディセーブルになります。ループ ガードをディセーブルにすると、すべての loop-inconsistent ポートがリスニング ステートに移行します。

あるチャネルでループ ガードをイネーブルに設定し、最初のリンクが単一方向になる場合は、ループ ガードは、対象となるポートがチャネルから削除されるまでは、チャネル全体をブロックします。図 9-6 に示すのは、3 台のスイッチで構成されるループ ガードです。

図 9-6　ループ ガード搭載の 3 台のスイッチ構成

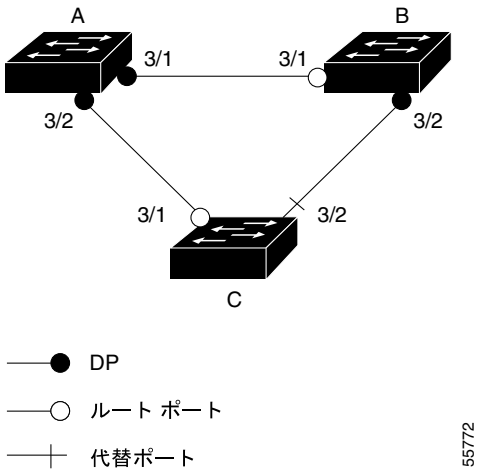


図 9-6 のスイッチ構成は、次のとおりです。

- スイッチ A および B は、分配スイッチです。
- スイッチ C は、アクセス スイッチです。
- ループ ガードは、スイッチ A、B、および C のポート 3/1 と 3/2 でイネーブルに設定されています。

ループ ガードは、ブロックされたポートがあるトポロジーでのみ使用してください。ブロックされたポートがないトポロジーは、ループフリーで、この機能をイネーブルにする必要がありません。ルート スイッチに対してループ ガードをイネーブルにしても効果はありませんが、ルート スイッチが非ルート スイッチになったときに保護機能を実行します。

ループ ガード使用の際は、次の注意事項に従ってください。

- ループ ガードは、PortFast がイネーブルに設定された VLAN ポートまたはダイナミック VLAN ポートではイネーブルに設定できません。
- ループ ガードが設定されたポートでは、PortFast をイネーブルに設定できません。
- ルート ガードがイネーブルの場合は、ループ ガードをイネーブルにできません。

ループ ガードは、他の機能との間で次のような相互作用があります。

- ループ ガードは、UplinkFast や BackboneFast の機能には影響を与えません。
- 共用リンクに接続されたポートでは、ループ ガードをイネーブルに設定しないでください。

（注） アクセス スイッチのルート ポートおよび代替ポートでは、ループ ガードをイネーブルに設定することを推奨します。

- ルート ガードは、常にポートをルート ポートとして指定させます。ループ ガードが有効なのは、ポートがルート ポートまたは代替ポートである場合だけです。あるポートに対してループ ガードとルート ガードを同時にイネーブルに設定することはできません。
- リンクが確立されると、PortFast はポートをただちにフォワーディング ステートに移行します。PortFast がイネーブルに設定されているポートは、ルート ポートや代替ポートにならないので、同じポートにループ ガードと PortFast を設定することはできません。ポートに対してダイナミック VLAN メンバーシップを割り当てるには、そのポートで PortFast がイネーブルに設定されている必要があります。ダイナミック VLAN メンバーシップを備えた、ループ ガードがイネーブルのポートを設定することはできません。
- ネットワークに、タイプに一貫性のないポートまたは port VLAN identifier（PVID; ポート VLAN ID）に一貫性のないポートがある場合は、設定の誤りが修正されるまで、すべての BPDU が廃棄されます。メッセージが期限切れになると、ポートは一貫性のないステートから移行します。ループ ガードは、タイプに一貫性のないポートや PVID に一貫性のないポートに対するメッセージ エージの期限切れを無視します。ポートがループ ガードによってブロック済みの場合は、ポートで受信された設定の間違った BPDU は、ループ ガードを回復させますが、ポートはタイプに一貫性のないステートまたは PVID に一貫性のないステートに移行されます。
- ハイ アベイラビリティ スイッチ構成では、ループ ガードによってポートがブロック ステートに移行されると、冗長スーパバイザ エンジンへ切り替えたあとでも、ポートはブロックされたままです。新たに起動されたスーパバイザ エンジンがそのポートを回復させるのは、そのポート上で BPDU が受信されたあとです。
- ループ ガードはスパニングツリーが認識しているポートを使用します。ループ ガードは、Port Aggregation Protocol（PAgP）が提供する論理ポートを利用できます。ただし、チャネルを形成するため、そのチャネルに属するすべての物理ポートが、互換性のある構成を備えている必要があります。PAgP は、すべての物理ポート上でルート ガードまたはループ ガードを均一に設定してチャネルを形成します。

  ループ ガードは、以下の点について注意が必要です。

  - スパニングツリーは、常にチャネルの最初の稼働ポートを選択して BPDU を送信します。そのリンクが単一方向になった場合、ループ ガードは、チャネル内の他のリンクが正常に機能している場合でも、チャネルをブロックします。
  - ループ ガードによってすでにブロックされているポート群でチャネルを形成する場合、スパニングツリーは、これらのポートに対するステート情報をすべて失い、新しいチャネル ポートが指定された役割でフォワーディング ステートになることがあります。
  - ループ ガードによってチャネルがブロックされ、チャネルが破壊されている場合、スパニングツリーは、ステート情報をすべて失います。チャネルを形成するリンクの 1 つまたは複数が単一方向の場合でも、各物理ポートが指定された役割でフォワーディング ステートになることがあります。

  （注） UniDirectional Link Detection（UDLD; 単一方向リンク検出）をイネーブルに設定して、リンク障害を切り離すことができます。UDLD が障害を検出するまでループが発生する可能性がありますが、ループ ガードはそれを検出できません。

- ループ ガードは、ディセーブルになっているスパニングツリー インスタンスや VLAN に対しては無効です。

スイッチ上での PortFast の設定

ここでは、スイッチ上でスパニング ツリー PortFast 機能を設定する手順について説明します。

アクセス ポート上での PortFast のイネーブル化

注意　PortFast は、単一エンド ステーションまたはスイッチ ポートとスイッチ ポートの接続に使用できます。スイッチなど、別のレイヤ 2 装置に接続されたポートで PortFast をイネーブルにすると、ネットワーク ループが生じる可能性があります。

スイッチ ポート上で PortFast をイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	単一ワークステーション、スイッチ、またはサーバに接続されたスイッチ ポート上で PortFast をイネーブルにします。	**set spantree portfast** *mod_num/port_num* **enable** | **disable**
ステップ 2	スイッチ ポート上の PortFast 設定を確認します。	**show spantree** [*mod_num/port_num*] [*vlan*]

次に、モジュール 4 のポート 1 で PortFast をイネーブルにし、設定を確認する例を示します（PortFast のステータスは、[Fast-Start] カラムに表示されます）。

```
Console> (enable) set spantree portfast 4/1 enable
Warning:Connecting Layer 2 devices to a fast start port can cause
temporary spanning tree loops. Use with caution.

Spantree port  4/1 fast start enabled.
Console> (enable) show spantree 4/1
Port      Vlan  Port-State     Cost   Priority  Fast-Start  Group-method
--------- ----  -------------  -----  --------  ----------  ------------
 4/1      1     blocking          19        20   enabled
 4/1      100   forwarding        10        20   enabled
 4/1      521   blocking          19        20   enabled
 4/1      522   blocking          19        20   enabled
 4/1      523   blocking          19        20   enabled
 4/1      524   blocking          19        20   enabled
 4/1      1003  not-connected     19        20   enabled
 4/1      1005  not-connected     19         4   enabled
Console> (enable)
```

（注）　ポート指定がエッジとして表示された場合、そのポートも PortFast ポートです。「エッジ ポート」（p.8-23）を参照してください。

トランク ポート上でのスパニングツリー PortFast のイネーブル化

注意　PortFast は、単一エンド ステーションまたはスイッチ ポートとスイッチ ポートの接続に使用できます。スイッチなど、別のレイヤ 2 装置に接続されたポートで PortFast をイネーブルにすると、ネットワーク ループが生じる可能性があります。

トランク ポート上で PortFast をイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	単一ワークステーション、スイッチ、またはサーバに接続されたトランク ポート上で PortFast をイネーブルにします。	**set spantree portfast** *mod_num/port_num* **enable trunk** **(注)** **trunk** キーワードを使用しないで **set spantree portfast** コマンドをトランク ポートに対して入力すると、トランク ポートはディセーブル モードのままになります。
ステップ 2	トランク ポート上の PortFast 設定を確認します。	**show spantree portfast** [*mod_num/port_num*]

次に、トランク ポートのモジュール 4 のポート 1 上で PortFast をイネーブルにし、このトランク ポートをフォワーディング ステートにして、設定を確認する例を示します（PortFast のステータスは、[Fast-Start] カラムに表示されます）。

```
Console> (enable) set spantree portfast 4/1 enable trunk
Warning:Connecting Layer 2 devices to a fast start port can cause
temporary spanning tree loops. Use with caution.

Spantree port  4/1 fast start enabled.
Console> (enable) show spantree 4/1
Port                     Vlan Port-State    Cost      Prio Portfast
Channel_id
------------------------ ---- ------------- --------- ---- ------------------
 4/1                     1    blocking              4   32 enabled  0
 4/1                     100  forwarding            4   32 enabled  0
 4/1                     521  blocking              4   32 enabled  0
 4/1                     524  blocking              4   32 enabled  0
 4/1                     1003 not-connected         4   32 enabled  0
 4/1                     1005 not-connected         4   32 enabled  0
Console> (enable) show spantree portfast 4/1
Portfast:enable trunk
Portfast BPDU guard is disabled.
Portfast BPDU filter is disabled.
Console>
```

(注)　2 台のスイッチ間で PortFast がイネーブルの場合、システムはネットワークにループがないことを確認してから、ブロッキング トランクをフォワーディング ステートにします。

PortFast のディセーブル化

スイッチ ポートまたはトランク ポート上で PortFast をディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチ ポート上で PortFast をディセーブルにします。	**set spantree portfast** *mod_num/port_num* **disable**
ステップ 2	PortFast の設定を確認します。	**show spantree** *mod_num/port_num*

次に、モジュール 4 のポート 1 上で PortFast をディセーブルにする例を示します。

```
Console> (enable) set spantree portfast 4/1 disable
Spantree port 4/1 fast start disabled.
Console> (enable)
```

PortFast のリセット

スイッチ ポートまたはトランク ポート上で PortFast をリセットし、デフォルトの設定値に戻すには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチ ポート上の PortFast をリセットし、デフォルトの設定値に戻します。	**set spantree portfast** *mod_num/port_num* **default**
ステップ 2	PortFast の設定を確認します。	**show spantree** *mod_num/port_num*

次に、モジュール 4 のポート 1 上で PortFast をリセットし、デフォルトの設定値に戻す例を示します。

```
Console> (enable) set spantree portfast 4/1 default

Spantree port  4/1 fast start set to default.

Console> (enable) show spantree portfast 4/1
Portfast:default
Portfast BPDU guard is disabled.
Portfast BPDU filter is disabled.
Console> (enable)
```

スイッチ上での PortFast BPDU ガードの設定

ここでは、スイッチ上で PortFast BPDU ガードを設定する手順について説明します。

PortFast BPDU ガードのイネーブル化

PortFast 機能はポート単位で設定しますが、PortFast BPDU ガード オプションは、グローバルでもポート単位でも設定できます。

ポート上で PortFast をディセーブルにすると、PortFast BPDU ガードは非アクティブになります。ポートの設定がデフォルト以外の場合は、ポートの設定によってグローバル設定が変更されます。ポートの設定がデフォルトに設定されている場合は、グローバル設定がチェックされます。ポートの設定がイネーブルの場合は、ポートの設定が使用され、グローバル設定は使用されません。

非トランキング スイッチ ポート上で PortFast BPDU ガードをイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポート単位で BPDU ガードをイネーブルにします。	**set spantree portfast bpdu-guard** *mod/port* [**disable** | **enable** | **default**]
ステップ 2	PortFast BPDU ガードの設定を確認します。	**show spantree summary**

次に、スイッチ上で PortFast BPDU ガードをイネーブルにし、Per VLAN Spanning-Tree Plus（PVST+）モードで設定を確認する例を示します。

（注）　PVST+ の詳細については、第 8 章「スパニングツリーの設定」を参照してください。

```
Console> (enable) set spantree portfast bpdu-guard 6/1 enable
Spantree port  6/1 bpdu guard enabled.
Console> (enable)
Console> (enable) show spantree summary
Root switch for vlans: none.
Portfast bpdu-guard enabled for bridge.
Uplinkfast disabled for bridge.
Backbonefast disabled for bridge.

Vlan  Blocking Listening Learning Forwarding STP Active
----- -------- --------- -------- ---------- ----------
   1         0         0        0          4          4
   2         0         0        0          4          4
   3         0         0        0          4          4
   4         0         0        0          4          4
   5         0         0        0          4          4
   6         0         0        0          4          4
  10         0         0        0          4          4
  20         0         0        0          4          4
  50         0         0        0          4          4
 100         0         0        0          4          4
 152         0         0        0          4          4
 200         0         0        0          5          5
 300         0         0        0          4          4
 400         0         0        0          4          4
 500         0         0        0          4          4
 521         0         0        0          4          4
 524         0         0        0          4          4
 570         0         0        0          4          4
 801         0         0        0          0          0
 802         0         0        0          0          0
 850         0         0        0          4          4
 917         0         0        0          4          4
 999         0         0        0          4          4
1003         0         0        0          0          0
1005         0         0        0          0          0

      Blocking Listening Learning Forwarding STP Active
----- -------- --------- -------- ---------- ----------
Total        0         0        0         85         85
```

PortFast BPDU ガードのディセーブル化

スイッチ上で PortFast BPDU ガードをディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチ上で PortFast BPDU ガードをディセーブルにします。	**set spantree portfast bpdu-guard** *mod/port* [**disable** | **enable** | **default**]
ステップ 2	PortFast BPDU ガードの設定を確認します。	**show spantree summary**

次に、スイッチ上で PortFast BPDU ガードをディセーブルにし、設定を確認する例を示します。

```
Console> (enable) set spantree portfast bpdu-guard disable
Spantree portfast bpdu-guard disabled on this switch.
Console> (enable) show spantree summary
Summary of connected spanning tree ports by vlan

Portfast bpdu-guard disabled for bridge.
Uplinkfast disabled for bridge.
Backbonefast disabled for bridge.

Vlan  Blocking Listening Learning Forwarding STP Active
----- -------- --------- -------- ---------- ----------
   1         0         0        0          4          4
   2         0         0        0          4          4
   3         0         0        0          4          4
   4         0         0        0          4          4
   5         0         0        0          4          4
   6         0         0        0          4          4
  10         0         0        0          4          4
  20         0         0        0          4          4
  50         0         0        0          4          4
 100         0         0        0          4          4
 152         0         0        0          4          4
 200         0         0        0          5          5
 300         0         0        0          4          4
 400         0         0        0          4          4
 500         0         0        0          4          4
 521         0         0        0          4          4
 524         0         0        0          4          4
 570         0         0        0          4          4
 801         0         0        0          0          0
 802         0         0        0          0          0
 850         0         0        0          4          4
 917         0         0        0          4          4
 999         0         0        0          4          4
1003         0         0        0          0          0
1005         0         0        0          0          0

      Blocking Listening Learning Forwarding STP Active
----- -------- --------- -------- ---------- ----------
Total        0         0        0         85         85
Console> (enable)
```

スイッチ上での PortFast BPDU フィルタリングの設定

ここでは、スイッチ上で PortFast BPDU フィルタリングを設定する手順について説明します。

PortFast BPDU フィルタリングのイネーブル化

非トランキング スイッチ ポート上で PortFast BPDU フィルタリングをイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポート上で BPDU フィルタ ステートを設定します。	**set spantree portfast bpdu-filter** *mod/port* [**disable** | **enable** | **default**]
ステップ 2	PortFast BPDU フィルタリングの設定を確認します。	**show spantree summary**

各ポート上の BPDU フィルタリングをデフォルト値に設定します。次に、ポート上で PortFast BPDU フィルタリングをイネーブルにし、PVST+ モードで設定を確認する例を示します。

(注)　PVST+ の詳細については、第 8 章「スパニングツリーの設定」を参照してください。

```
Console> (enable) set spantree portfast bpdu-filter 6/1 enable
Warning:Ports enabled with bpdu filter will not send BPDUs and drop all
received BPDUs. You may cause loops in the bridged network if you misuse
this feature.

Console> (enable) show spantree summary
Root switch for vlans: none.
Portfast bpdu-filter enabled for bridge.
Uplinkfast disabled for bridge.
Backbonefast disabled for bridge.

Vlan  Blocking Listening Learning Forwarding STP Active
----- -------- --------- -------- ---------- ----------
   1         0         0        0          4          4
   2         0         0        0          4          4
   3         0         0        0          4          4
   4         0         0        0          4          4
   5         0         0        0          4          4
   6         0         0        0          4          4
.
.
.
 850         0         0        0          4          4
 917         0         0        0          4          4
 999         0         0        0          4          4
1003         0         0        0          0          0
1005         0         0        0          0          0

      Blocking Listening Learning Forwarding STP Active
----- -------- --------- -------- ---------- ----------
Total        0         0        0         85         85
Console> (enable)
```

PortFast BPDU フィルタリングのディセーブル化

スイッチ上で PortFast BPDU フィルタリングをディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチ上で PortFast BPDU フィルタリングをディセーブルにします。	**set spantree portfast bpdu-filter disable**
ステップ 2	PortFast BPDU フィルタリングの設定を確認します。	**show spantree summary** **show portfast**

次に、スイッチ上で PortFast BPDU フィルタリングをディセーブルにし、設定を確認する例を示します。

```
Console> (enable) set spantree portfast bpdu-filter disable
Spantree portfast bpdu-filter disabled on this switch.
Console> (enable) show spantree summary
Summary of connected spanning tree ports by vlan

Portfast bpdu-filter disabled for bridge.
Uplinkfast disabled for bridge.
Backbonefast disabled for bridge.

Vlan  Blocking Listening Learning Forwarding STP Active
----- -------- --------- -------- ---------- ----------
   1         0         0        0          4          4
   2         0         0        0          4          4
   3         0         0        0          4          4
   4         0         0        0          4          4
   5         0         0        0          4          4
   6         0         0        0          4          4
  10         0         0        0          4          4
.
.
 802         0         0        0          0          0
 850         0         0        0          4          4
 917         0         0        0          4          4
 999         0         0        0          4          4
1003         0         0        0          0          0
1005         0         0        0          0          0

      Blocking Listening Learning Forwarding STP Active
----- -------- --------- -------- ---------- ----------
Total        0         0        0         85         85
Console> (enable)
```

スイッチ上での UplinkFast の設定

PVST+ または Multi-Instance Spanning-Tree Protocol（MISTP）に、UplinkFast を設定できます。使用するコマンドは同じですが、出力はわずかに異なる場合があります。

(注) MISTP の詳細については、第 8 章「スパニングツリーの設定」を参照してください。

ここでは、スイッチ上で UplinkFast 機能を設定する手順について説明します。

- UplinkFast のイネーブル化（p.9-18）
- UplinkFast のディセーブル化（p.9-19）

UplinkFast のイネーブル化

set spantree uplinkfast enable コマンドを実行すると、そのスイッチ上のすべてのポートのパス コストが増加します。その結果、スイッチがルート スイッチになる可能性が低くなります。*station_update_rate* の値は、100 ミリ秒間に送信されるマルチキャスト パケットの数を表します（デフォルトでは 15 パケット /100 ミリ秒です）。

(注) **set spantree uplinkfast** コマンドをイネーブルにすると、このコマンドはスイッチ上のすべての VLAN に影響を及ぼします。個々の VLAN 上で UplinkFast を設定することはできません。

スイッチ上で UplinkFast をイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチ上で UplinkFast をイネーブルにします。	**set spantree uplinkfast enable** [**rate** *station_update_rate*] [**all-protocols off** | **on**]
ステップ 2	UplinkFast がイネーブルに設定されたことを確認します。	**show spantree uplinkfast** [{**mistp-instance** [*instances*]}| *vlans*]

次に、PVST+ モードがイネーブルになっている場合にステーション アップデート レートを 15 パケット /100 ミリ秒にして、UplinkFast をイネーブルにし、さらに、UplinkFast がイネーブルになっていることを確認する例を示します。

```
Console> (enable) set spantree uplinkfast enable
VLANs 1-4094 bridge priority set to 49152.
The port cost and portvlancost of all ports set to above 3000.
Station update rate set to 15 packets/100ms.
uplinkfast all-protocols field set to off.
uplinkfast enabled for bridge.
Console> (enable) show spantree uplinkfast 1 100 521-524
Station update rate set to 15 packets/100ms.
uplinkfast all-protocols field set to off.
VLAN          port list
-----------------------------------------------
1             1/1(fwd),1/2
100           1/2(fwd)
521           1/1(fwd),1/2
522           1/1(fwd),1/2
523           1/1(fwd),1/2
524           1/1(fwd),1/2
Console> (enable)
```

次に、すべての VLAN について UplinkFast の設定を表示する例を示します。

```
Console> show spantree uplinkfast
Station update rate set to 15 packets/100ms.
uplinkfast all-protocols field set to off.
VLAN port list
-------------------------------------------------
1-20   1/1(fwd),1/2-1/5
21-50  1/9(fwd), 1/6-1/8, 1/10-1/12
51-100 2/1(fwd), 2/12
Console>
```

MISTP モードがイネーブルになっている場合に UplinkFast をイネーブルにすると、次の例のような出力が表示されます。

```
Console> (enable) set spantree uplinkfast enable
Instances 1-16 bridge priority set to 49152.
The port cost and portinstancecost of all ports set to above 10000000.
Station update rate set to 15 packets/100ms.
uplinkfast all-protocols field set to off.
uplinkfast enabled for bridge.
Console> (enable)
```

次に、特定のインスタンスについて UplinkFast の設定を表示する例を示します。

```
Console> show spantree uplinkfast mistp-instance 1
Station update rate set to 15 packets/100ms.
uplinkfast all-protocols field set to off.
Inst   port list
-------------------------------------------------
1      4/1(fwd)
Console>
```

UplinkFast のディセーブル化

set spantree uplinkfast disable コマンドは、スイッチ上で UplinkFast をディセーブルにしますが、スイッチ プライオリティとポート コストの値は出荷時のデフォルトにはリセットされません。

（注） **set spantree uplinkfast disable** コマンドを入力すると、スイッチ上のすべての VLAN が影響を受けます。個々の VLAN 上で UplinkFast をディセーブルにすることはできません。

スイッチ上で UplinkFast をディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチ上で UplinkFast をディセーブルにします。	**set spantree uplinkfast disable**
ステップ 2	UplinkFast がディセーブルに設定されたことを確認します。	**show spantree uplinkfast**

次に、PVST+ モードがイネーブルになっている場合、スイッチ上で UplinkFast をディセーブルにし、設定を確認する例を示します。

```
Console> (enable) set spantree uplinkfast disable
Uplinkfast disabled for switch.
Use clear spantree uplinkfast to return stp parameters to default.
Console> (enable) show spantree uplinkfast
Station update rate set to 15 packets/100ms.
uplinkfast all-protocols field set to off.
VLAN          port list
-----------------------------------------------
1             1/1(fwd),1/2
100           1/2(fwd)
521           1/1(fwd),1/2
522           1/1(fwd),1/2
523           1/1(fwd),1/2
524           1/1(fwd),1/2
Console> (enable)
```

スイッチ上での BackboneFast の設定

ここでは、BackboneFast の設定手順について説明します。

BackboneFast のイネーブル化

（注） BackboneFast を使用するには、ネットワーク上のすべてのスイッチで BackboneFast をイネーブルに設定する必要があります。BackboneFast は、トークンリング VLAN ではサポートされていません。この機能は、サードパーティ製のスイッチと組み合わせて使用することができます。

スイッチ上で BackboneFast をイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチ上で BackboneFast をイネーブルにします。	**set spantree backbonefast enable**
ステップ 2	BackboneFast がイネーブルに設定されたことを確認します。	**show spantree backbonefast**

次に、スイッチ上で BackboneFast をイネーブルにし、設定を確認する例を示します。

```
Console> (enable) set spantree backbonefast enable
Backbonefast enabled for all VLANs
Console> (enable) show spantree backbonefast
Backbonefast is enabled.
Console> (enable)
```

BackboneFast 統計情報の表示

BackboneFast 統計情報を表示するには、イネーブル モードで次のコマンドを入力します。

作業	コマンド
BackboneFast 統計情報を表示します。	**show spantree summary**

次に、BackboneFast 統計情報の表示例を示します。

```
Console> (enable) show spantree summary
Summary of connected spanning tree ports by vlan

Uplinkfast disabled for bridge.
Backbonefast enabled for bridge.

Vlan  Blocking Listening Learning Forwarding STP Active
----- -------- --------- -------- ---------- ----------
   1         0         0        0          1          1

      Blocking Listening Learning Forwarding STP Active
----- -------- --------- -------- ---------- ----------
Total        0         0        0          1          1
BackboneFast statistics
-----------------------
Number of inferior BPDUs received (all VLANs)  : 0
Number of RLQ req PDUs received (all VLANs)    : 0
Number of RLQ res PDUs received (all VLANs)    : 0
Number of RLQ req PDUs transmitted (all VLANs) : 0
Number of RLQ res PDUs transmitted (all VLANs) : 0
Console> (enable)
```

BackboneFast のディセーブル化

スイッチ上で BackboneFast をディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチ上で BackboneFast をディセーブルにします。	**set spantree backbonefast disable**
ステップ 2	BackboneFast がディセーブルに設定されたことを確認します。	**show spantree backbonefast**

次に、スイッチ上で BackboneFast をディセーブルにし、設定を確認する例を示します。

```
Console> (enable) set spantree backbonefast disable
Backbonefast enabled for all VLANs
Console> (enable) show spantree backbonefast
Backbonefast is disable.
Console> (enable)
```

スイッチ上でのループ ガードの設定

ここでは、ループ ガードの設定手順について説明します。

ループ ガードのイネーブル化

ポート単位でスパニングツリー ループ ガード機能をイネーブルまたはディセーブルにするには、**set spantree guard** コマンドを使用します。

スイッチ上でループ ガードをイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポート上でループ ガードをイネーブルにします。	**set spantree guard loop** *mod/port*
ステップ 2	ループ ガードがイネーブルに設定されたことを確認します。	**show spantree guard** {*mod/port* | *vlan*} **mistp-instance** *instance*

次に、ループ ガードをイネーブルにする例を示します。

```
Console> (enable) set spantree guard loop 5/1
Rootguard is enabled on port 5/1, enabling loopguard will disable rootguard on this
port.
Do you want to continue (y/n) [n]? y
Loopguard on port 5/1 is enabled.
Console> (enable)
```

ループ ガードのディセーブル化

スイッチ上でループ ガードをディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポート上でループ ガードをディセーブルにします。	**set spantree guard none** *mod/port*
ステップ 2	ループ ガードがディセーブルに設定されたことを確認します。	**show spantree guard** {*mod/port* | *vlan*} **mistp-instance** *instance*

次に、ループ ガードをディセーブルにする例を示します。

```
Console> (enable) set spantree guard none 5/1
Rootguard is disabled on port 5/1, disabling loopguard will disable rootguard on this
port.
Do you want to continue (y/n) [n]? y
Loopguard on port 5/1 is disabled.
Console> (enable)
```

■ スイッチ上でのループ ガードの設定

CHAPTER 10

VTP の設定

この章では、Catalyst 6500 シリーズ スイッチ上で VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）を設定する手順について説明します。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

この章で説明する内容は、次のとおりです。

VTP バージョン 1 およびバージョン 2 の機能概要

VTP は、レイヤ 2 のメッセージング プロトコルであり、ネットワーク全体にわたって VLAN（仮想 LAN）の追加、削除、および名称変更などを管理することにより、VLAN 設定の整合性を維持します。VTP を使用すると、VLAN 名の重複、無効な VLAN タイプの指定、セキュリティ違反などのさまざまな問題によって生じる設定の矛盾が最小限に抑えられます。

VTP を使用すると、ネットワークで VLAN 1 ～ 1005 を管理できます（VTP バージョン 1 および VTP バージョン 2 は、VLAN 1025 ～ 4094 をサポートしていません）。VTP では、1 台のスイッチ上で中央集約的に設定変更を行い、それらの変更を自動的にネットワーク上の他のスイッチに伝達することができます。

(注)　VLAN の詳しい設定手順については、第 11 章「VLAN の設定」を参照してください。

ここでは、VTP の機能について説明します。

VTP ドメインの概要

VTP ドメイン（別名、VLAN 管理ドメイン）は、相互接続された 1 つまたは複数のスイッチで構成され、これらのスイッチは同じ VTP ドメイン名を共有します。スイッチが所属できる VTP ドメインは 1 つだけです。ドメインのグローバル VLAN 設定を変更するには、CLI（コマンドライン インターフェイス）または SNMP（簡易ネットワーク管理プロトコル）を使用します。

デフォルトでは、スイッチは VTP サーバ モードであり、トランク リンクを介してドメインについてのアドバタイズを受信するか、ユーザが管理ドメインを設定しないかぎり、非管理ドメイン ステートのままです。管理ドメイン名を指定するか学習するまで、VTP サーバ上で VLAN の作成や変更はできません。

スイッチがトランク リンクを介して VTP アドバタイズを受信すると、管理ドメイン名および VTP コンフィギュレーション リビジョン番号が継承されます。スイッチは、別の管理ドメイン名または古いコンフィギュレーション リビジョン番号が指定されたアドバタイズについては、一切無視します。

スイッチを VTP トランスペアレントとして設定した場合、VLAN の作成および変更は可能ですが、その変更が作用するのは個々のスイッチに限られます。

VTP サーバ上の VLAN 設定を変更すると、その変更は VTP ドメイン内のすべてのスイッチに伝播されます。VTP アドバタイズは、ISL（スイッチ間リンク）、IEEE 802.1Q、IEEE 802.10、および ATM（非同期転送モード）LAN Emulation（LANE; LAN エミュレーション）を含め、すべてのトランク接続に伝送されます。

VTP は、固有の名前と内部インデックスを対応させ、複数の LAN タイプにわたって VLAN を動的にマッピングします。マッピングにより、ネットワーク管理者の装置管理の負担が軽減されます。

VTP モードの概要

次のいずれかの VTP モードで動作するようにスイッチを設定できます。

- サーバ ― VTP サーバ モードでは、VLAN の作成、変更、および削除ができます。また、VTP ドメイン全体に対して他のコンフィギュレーション パラメータ（VTP バージョン、VTP プルーニングなど）を指定できます。VTP サーバは、同一 VTP ドメイン内の他のスイッチに、自分の VLAN 設定をアドバタイズし、また、トランク リンクを介して受信したアドバタイズに基づいて、自分の VLAN 設定を他のスイッチと同期させます。VTP サーバ モードがデフォルトの設定です。
- クライアント ― VTP クライアントは、VTP サーバと同様に動作しますが、VTP クライアント上で VLAN の作成、変更、または削除を行うことはできません。
- トランスペアレント ― VTP トランスペアレント スイッチは、VTP に参加しません。VTP トランスペアレント スイッチは、自身の VLAN 設定をアドバタイズせず、受信したアドバタイズに基づいて同期させることもありません。ただし、VTP バージョン 2 の場合、トランスペアレント スイッチは自身のトランク ポートから受信した VTP アドバタイズを転送します。
- オフ ― 上記の 3 種類のモードで、スイッチが管理ドメイン ステートを開始するとただちに、VTP アドバタイズを送受信します。VTP オフ モードでは、VTP アドバタイズが転送されないことを除き、スイッチの動作は VTP トランスペアレント モードの場合と同じです。

VTP アドバタイズの概要

VTP ドメインの各スイッチは、予約されたマルチキャスト アドレスに対して、それぞれのトランク ポートからアドバタイズを定期的に送信します。VTP アドバタイズを受信した近接スイッチは、必要に応じてそれぞれの VTP および VLAN 設定をアップデートします。

VTP アドバタイズでは、次のグローバル コンフィギュレーション情報が配布されます。

- VLAN ID（ISL および 802.1Q）
- エミュレート LAN 名（ATM LANE 用）
- 802.10 SAID 値（FDDI）
- VTP ドメイン名
- VTP コンフィギュレーション リビジョン番号
- 各 VLAN の Maximum Transmission Unit（MTU; 最大伝送ユニット）サイズなどの VLAN 設定
- フレーム フォーマット

VTP バージョン 2 の概要

ネットワークで VTP を使用する場合は、VTP バージョン 1、バージョン 2、またはバージョン 3 のいずれを使用するかを決定する必要があります（バージョン 3 の詳細については、「VTP バージョン 3 の機能概要」[p.10-14] を参照してください）。

（注） トークンリング環境で VTP を使用する場合、バージョン 2 が必要です。

VTP バージョン 1 ではサポートされず、VTP バージョン 2 でサポートされる機能は、次のとおりです。

- トークンリングのサポート ― VTP バージョン 2 は、トークンリング LAN スイッチングおよび VLAN（Token Ring Bridge Relay Function［TrBRF; トークンリング ブリッジ リレー機能］および Token Ring Concentrator Relay Function［TrCRF; トークンリング コンセントレータ リレー機能］）をサポートしています。トークンリング VLAN の詳細については、第 11 章「VLAN の設定」を参照してください。

- 認識不可能な Type-Length-Value（TLV）のサポート — VTP サーバまたはクライアントは、TLV が認識不可能であっても、設定の変更を他のトランクに伝播します。認識されなかった TLV は、NVRAM（不揮発性 RAM）に保存されます。
- バージョン依存型トランスペアレント モード — VTP バージョン 1 の場合、VTP トランスペアレント スイッチは、VTP メッセージの中のドメイン名およびバージョンを調べ、バージョンおよびドメイン名が一致する場合に限ってメッセージを転送します。スーパバイザ エンジン ソフトウェアでサポートされるドメインは 1 つだけなので、VTP バージョン 2 では、トランスペアレント モードの場合に、バージョンを確認せずに VTP メッセージを転送します。
- 整合性検査 — VTP バージョン 2 では、CLI または SNMP を介して新しい情報が入力された場合に限り、VLAN 整合性検査（VLAN 名、値など）を行います。VTP メッセージから新しい情報を取得した場合、または NVRAM から情報を読み込んだ場合には、整合性検査を行いません。受信した VTP メッセージのダイジェストが有効であれば、整合性検査を行わずに情報が受け入れられます。

VTP プルーニングの概要

（注） VTP バージョン 3 スイッチ上で VTP プルーニングをイネーブルにしても、プルーニングはそのスイッチ上でイネーブルになるだけです。VTP バージョン 1 や VTP バージョン 2 のように伝播されることはありません。

VTP プルーニングは、ブロードキャスト パケット、マルチキャスト パケット、未知のパケット、およびフラッディング ユニキャスト パケットなど、不要なフラッディング トラフィックを削減することにより、ネットワークの帯域幅を拡張します。VTP プルーニングは、目的のネットワーク装置にアクセスするために使用する必要のあるトランク リンクへのフラッディング トラフィックを制限するので、使用可能な帯域幅が増えます。VTP プルーニングは、ディセーブルがデフォルトの設定です。

管理ドメイン内のすべての装置が VTP プルーニングをサポートすることを確認した上で、VTP プルーニングをイネーブルにしてください。VTP プルーニングは、スーパバイザ エンジン Release 5.1(1) 以降のソフトウェア リリースでサポートされています。

（注） ルータを使用してエミュレート LAN 間でルーティングする場合、ATM LANE モジュールが搭載されたスイッチを含む VTP 管理ドメイン内では、VTP プルーニングをディセーブルにする必要があります（ATM LANE モジュールがトランクであるために、VTP プルーニング メッセージが送信されます）。また、ATM LANE モジュールが搭載されたすべてのスイッチ上で、**clear vtp pruneeligible** コマンドを使用して LANE VLAN のプルーニングをディセーブルにすることもできます。

図 10-1 に、VTP プルーニングを使用できない場合のスイッチド ネットワークを示します。スイッチ 1 のポート 1 およびスイッチ 4 のポート 2 は、Red という VLAN に割り当てられています。スイッチ 1 に接続されたホストから、ブロードキャストが送信されます。スイッチ 1 は、ブロードキャストをフラッディングし、Red VLAN にポートのないスイッチ 3、5、および 6 も含めて、ネットワーク内のすべてのスイッチがそれを受信します。

図 10-1　VTP プルーニングを使用しない場合のフラッディング トラフィック

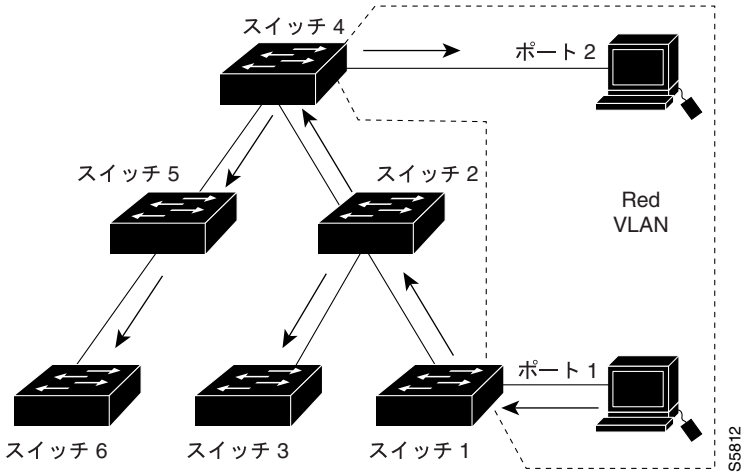
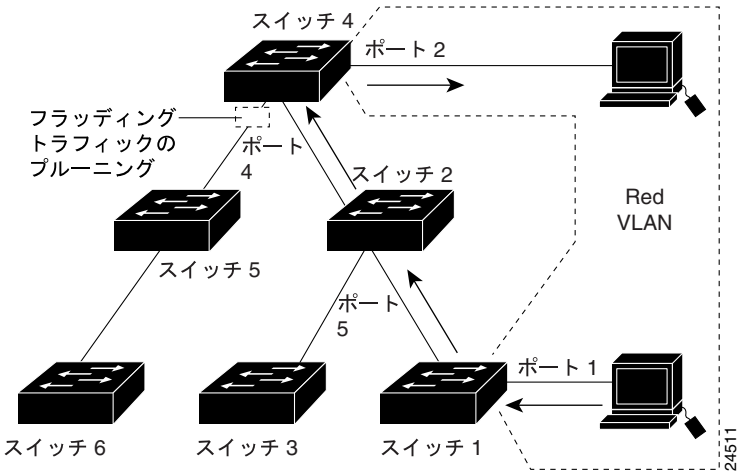


図 10-2 に、上記と同一のスイッチド ネットワークで VTP プルーニングがイネーブルの場合を示します。Red VLAN からのトラフィックが指定されたリンク（スイッチ 2 のポート 5、スイッチ 4 のポート 4）でプルーニングされるので、スイッチ 1 からのブロードキャスト トラフィックは、スイッチ 3、5、および 6 には転送されません。

VTP サーバで VTP プルーニングをイネーブルにすると、管理ドメイン全体にわたってプルーニングがイネーブルになります。VTP プルーニングは、イネーブルにしてから数秒後に有効になります。デフォルトでは、VLAN 2 ～ 1000 がプルーニング適格です。VTP プルーニング不適格の VLAN からのトラフィックはプルーニングされません。VLAN 1 は常にプルーニング不適格であり、VLAN 1 からのトラフィックをプルーニングすることはできません。

VLAN プルーニングを不適格にするには、**clear vtp pruneeligible** コマンドを入力します。VLAN プルーニングを再び適格にするには、**set vtp pruneeligible** コマンドを入力します。VLAN プルーニングの適格性は、ドメインで VTP プルーニングがイネーブルであるか、ディセーブルであるかに関係なく設定できます。プルーニングの適格性が適用されるのは VTP ドメイン全体ではなく、ローカル装置に限定されます。

図 10-2　VTP プルーニングを使用した場合のフラッディング トラフィック



VTP バージョン 1 およびバージョン 2 のデフォルト設定

表 10-1 に、VTP のデフォルト設定を示します。

表 10-1　VTP のデフォルト設定

機能	デフォルト値
VTP ドメイン名	ヌル
VTP モード	サーバ
VTP バージョン 2 のイネーブル ステート	バージョン 1 がイネーブル（バージョン 2 はディセーブル）
VTP パスワード	none
VTP プルーニング	ディセーブル

VTP バージョン 1 およびバージョン 2 設定時の注意事項

ここでは、ネットワークに VTP を実装する際の注意事項について説明します。

- VTP ドメイン内のすべてのスイッチで同じ VTP バージョンを実行する必要があります。
- セキュア　モードの場合、管理ドメイン内の各スイッチでパスワードを設定する必要があります。

注意　セキュア モードで VTP を設定し、ドメイン内の各スイッチに管理ドメイン パスワードを割り当てなかった場合、管理ドメインは正常に動作しません。

- VTP バージョン 2 対応のスイッチ上で VTP バージョン 2 がディセーブルになっている場合（VTP バージョン 2 はディセーブルがデフォルトの設定）、VTP バージョン 2 対応スイッチは、同一 VTP ドメイン内で、VTP バージョン 1 が稼働しているスイッチとして動作可能です。
- 同一 VTP ドメイン内のすべてのスイッチがバージョン 2 に対応する場合以外は、スイッチ上で VTP バージョン 2 をイネーブルにしないでください。スイッチ上で VTP バージョン 2 をイネーブルにすると、ドメイン内のすべてのバージョン 2 対応スイッチが VTP バージョン 2 をイネーブルにします。
- トークンリング環境では、トークンリング VLAN スイッチング機能を正しく動作させるために、VTP バージョン 2 をイネーブルにする必要があります。
- VTP サーバ上で VTP プルーニングをイネーブルまたはディセーブルにすると、管理ドメイン全体で VTP プルーニングがイネーブルまたはディセーブルになります。
- スイッチ上で VLAN プルーニングを適格または不適格にすると、（VTP ドメイン内のすべての装置ではなく）その装置上の VLAN のプルーニング適格性だけが影響を受けます。
- Release 8.1(1) では、すべての VTP バージョンをポート単位で設定できます。「VTP バージョン 3 のポート単位設定」（p.10-15）を参照してください。

VTP バージョン 1 およびバージョン 2 の設定

ここでは、VTP の設定手順について説明します。

VTP サーバの設定

スイッチが VTP サーバ モードの場合、VLAN 設定を変更し、その変更をネットワーク全体に伝播することができます。

VTP サーバとしてスイッチを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	VTP ドメイン名を定義します。	**set vtp domain** *name*
ステップ 2	スイッチを VTP サーバ モードにします。	**set vtp mode server**
ステップ 3	（任意）VTP ドメイン用のパスワードを設定します。	**set vtp passwd** *passwd*
ステップ 4	VTP 設定を確認します。	**show vtp domain**

次に、VTP サーバとしてスイッチを設定し、その設定を確認する例を示します。

```
Console> (enable) set vtp domain Lab_Network
VTP domain Lab_Network modified
Console> (enable) set vtp mode server
Changing VTP mode for all features
VTP domain Lab_Network modified
Console> (enable) show vtp domain
Version      : running VTP2 (VTP3 capable)
Domain Name  : Lab_Network                        Password  : configured (hidden)
Notifications: disabled                           Updater ID: 172.20.52.19

Feature        Mode           Revision
-------------- -------------- -----------
VLAN           Server         0

Pruning             : disabled
VLANs prune eligible: 2-1000
Console> (enable)
```

VTP クライアントの設定

スイッチが VTP クライアント モードの場合、スイッチ上で VLAN 設定を変更することはできません。クライアント スイッチは管理ドメイン内の VTP サーバから VTP アップデート情報を受信し、それに基づいて設定を変更します。

VTP クライアントとしてスイッチを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	VTP ドメイン名を定義します。	**set vtp domain** *name*
ステップ 2	スイッチを VTP クライアント モードにします。	**set vtp mode client**
ステップ 3	VTP 設定を確認します。	**show vtp domain**

次に、VTP クライアントとしてスイッチを設定し、その設定を確認する例を示します。

```
Console> (enable) set vtp domain Lab_Network
VTP domain Lab_Network modified
Console> (enable) set vtp mode client
Changing VTP mode for all features
VTP domain Lab_Network modified
Console> (enable) show vtp domain
Version      : running VTP2 (VTP3 capable)
Domain Name  : Lab_Network                        Password  : configured (hidden)
Notifications: disabled                           Updater ID: 172.20.52.19

Feature        Mode           Revision
-------------- -------------- -----------
VLAN           Client         0

Pruning             : disabled
VLANs prune eligible: 2-1000
Console> (enable)
```

VTP の設定（VTP トランスペアレント モード）

VTP トランスペアレントとしてスイッチを設定すると、スイッチ上で VTP がディセーブルになります。VTP トランスペアレント スイッチは VTP アップデートを送信せず、他のスイッチから受信した VTP アップデートにも反応しません。ただし、VTP バージョン 2 が稼働している VTP トランスペアレント スイッチは、受信した VTP アドバタイズを、対応するすべてのトランク リンクを使用して転送します。

（注） VTP トランスペアレント モードのネットワーク装置は、VTP Join メッセージを送信しません。VTP トランスペアレント モードのネットワーク装置にトランク接続されている Catalyst 6500 シリーズ スイッチに、トランスペアレントモード ネットワーク装置で使用される VLAN、またはプルーニング不適格としてトランク間で伝送する必要がある VLAN を設定します（**clear vtp pruneeligible** コマンドを使用します）。

スイッチ上で VTP をディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	VTP トランスペアレント モードに設定して、スイッチ上で VTP をディセーブルにします。	**set vtp mode transparent**
ステップ 2	VTP 設定を確認します。	**show vtp domain**

次に、スイッチを VTP トランスペアレントとして設定し、その設定を確認する例を示します。

```
Console> (enable) set vtp mode transparent
Changing VTP mode for all features
VTP domain Lab_Net modified
Console> (enable) show vtp domain
Version      : running VTP2 (VTP3 capable)
Domain Name  : Lab_Network                        Password  : configured (hidden)
Notifications: disabled                           Updater ID: 172.20.52.19

Feature        Mode           Revision
-------------- -------------- -----------
VLAN           Transparent    0

Pruning             : disabled
VLANs prune eligible: 2-1000
Console> (enable)
```

オフ モードによる VTP のディセーブル化

オフ モードを使用して VTP をディセーブルにした場合、VTP アドバタイズが転送されないことを除き、スイッチの動作は VTP トランスペアレント モードの場合と同じです。

オフ モードを使用して VTP をディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	オフ モードを使用して VTP をディセーブルにします。	**set vtp mode off**
ステップ 2	VTP 設定を確認します。	**show vtp domain**

次に、オフ モードを使用して VTP をディセーブルにする例を示します。

```
Console> (enable) set vtp mode off
Changing VTP mode for all features
Console> (enable) show vtp domain
Version      :running VTP2 (VTP3 capable)
Domain Name  :Lab_Network                         Password  :configured (hidden)
Notifications:disabled                            Updater ID: 172.20.52.19

Feature        Mode           Revision
-------------- -------------- -----------
VLAN           Off            0

Pruning             :disabled
VLANs prune eligible: 2-1000
Console> (enable)
```

VTP バージョン 2 のイネーブル化

VTP バージョン 2 対応のスイッチ上で、VTP バージョン 2 はディセーブルがデフォルトの設定です。スイッチ上で VTP バージョン 2 をイネーブルにすると、VTP ドメイン内のすべてのバージョン 2 対応スイッチでバージョン 2 がイネーブルになります。

注意　同一 VTP ドメイン内のスイッチに関して、VTP バージョン 1 および 2 の間ではインターオペラビリティはありません。VTP ドメイン内のすべてのスイッチで同じ VTP バージョンを使用する必要があります。VTP ドメイン内のすべてのスイッチが VTP バージョン 2 をサポートしている場合以外は、バージョン 2 をイネーブルにしないでください。

（注）　トークンリング環境では、トークンリング VLAN スイッチング機能を正しく動作させるために、VTP バージョン 2 をイネーブルにする必要があります。

VTP バージョン 2 をイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチ上で VTP バージョン 2 をイネーブルにします。	**set vtp version 2**
ステップ 2	VTP バージョン 2 がイネーブルに設定されたことを確認します。	**show vtp domain**

次に、VTP バージョン 2 をイネーブルにし、設定を確認する例を示します。

```
Console> (enable) set vtp version 2
This command will enable VTP version 2 function in the entire management domain.
All devices in the management domain should be version2-capable before enabling.
Do you want to continue (y/n) [n]? y
VTP domain server modified
Console> (enable) show vtp domain
Version      :running VTP2 (VTP3 capable)
Domain Name  :Lab_Network                        Password  :configured (hidden)
Notifications:disabled                          Updater ID: 172.20.52.19

Feature        Mode           Revision
-------------- -------------- -----------
VLAN           Off            0

Pruning             :disabled
VLANs prune eligible: 2-1000
Console> (enable)
```

VTP バージョン 2 のディセーブル化

VTP バージョン 2 をディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	VTP バージョン 2 をディセーブルにします。	**set vtp version 1**
ステップ 2	VTP バージョン 2 がディセーブルに設定されたことを確認します。	**show vtp domain**

次に、VTP バージョン 2 をディセーブルにする例を示します。

```
Console> (enable) set vtp version 1
This command will enable VTP version 1 function in the entire management domain.
Warning:trbrf & trcrf vlans will not work properly in this version.
Do you want to continue (y/n) [n]? y
VTP domain Lab_Network modified
Console> (enable) show vtp domain
Version      :running VTP1 (VTP3 capable)
Domain Name  :Lab_Network                        Password  :configured (hidden)
Notifications:disabled                          Updater ID: 172.20.52.19

Feature        Mode           Revision
-------------- -------------- -----------
VLAN           Off            0

Pruning             :disabled
VLANs prune eligible: 2-1000
Console> (enable)
```

VTP プルーニングのイネーブル化

VTP プルーニングをイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	管理ドメイン内で VTP プルーニングをイネーブルにします。	**set vtp pruning enable**
ステップ 2	（任意）装置上で特定の VLAN をプルーニング不適格にします（デフォルトでは、VLAN 2 ～ 1000 がプルーニング適格です）。	**clear vtp pruneeligible** *vlan_range*
ステップ 3	（任意）装置上で特定の VLAN をプルーニング適格にします。	**set vtp pruneeligible** *vlan_range*
ステップ 4	VTP プルーニングの設定を確認します。	**show vtp domain**
ステップ 5	所定の VLAN がトランク ポート上でプルーニングされることを確認します。	**show trunk**

次に、管理ドメイン内で VTP プルーニングをイネーブルにし、特定の装置上で、VLAN 2 ～ 99、250 ～ 255、および 501 ～ 1000 をプルーニング適格にする例を示します。

```
Console> (enable) set vtp pruning enable
Cannot modify pruning mode unless in VTP SERVER mode.
Console> (enable) set vtp mode server
Changing VTP mode for all features
VTP domain Lab_Network modified
Console> (enable) set vtp pruning enable
This command will enable the pruning function in the entire management domain.
All devices in the management domain should be pruning-capable before enabling.
Do you want to continue (y/n) [n]? y
VTP domain Lab_Network modified
Console> (enable) clear vtp pruneeligible 100-500
Vlans 1,100-500,1001-1023 will not be pruned on this device.
VTP domain Lab_Network modified.
Console> (enable) set vtp pruneeligible 250-255
Vlans 2-99,250-255,501-1000,1024-4094 eligible for pruning on this device.
VTP domain Lab_Network modified.
Console> (enable) show vtp domain
Version      : running VTP1 (VTP3 capable)
Domain Name  : Lab_Network                     Password  : configured (hidden)
Notifications: disabled                       Updater ID: 172.20.52.19

Feature        Mode           Revision
-------------- -------------- -----------
VLAN           Server         1

Pruning             : enabled
VLANs prune eligible: 2-99,250-255,501-1000
Console> (enable) show trunk
* - indicates vtp domain mismatch
# - indicates dot1q-all-tagged enabled on the port
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
16/1      nonegotiate  isl            trunking      1

Port      Vlans allowed on trunk
--------  ---------------------------------------------------------------------
16/1      1-1005,1025-4094

Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------------------
16/1

Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------------------
16/1
Console> (enable)
```

VTP プルーニングのディセーブル化

VTP プルーニングをディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	管理ドメイン内で VTP プルーニングをディセーブルにします。	**set vtp pruning disable**
ステップ 2	VTP プルーニングがディセーブルに設定されたことを確認します。	**show vtp domain**

次に、管理ドメイン内で VTP プルーニングをディセーブルにする例を示します。

```
Console> (enable) set vtp pruning disable
This command will disable the pruning function in the entire management domain.
Do you want to continue (y/n) [n]? y
VTP domain Lab_Network modified
Console> (enable)
```

VTP 統計情報の表示

送受信された VTP アドバタイズ、VTP エラーなど、VTP 統計情報を表示するには、次の作業を行います。

作業	コマンド
スイッチの VTP 統計情報を表示します。	**show vtp statistics**

次に、スイッチに関する VTP 統計情報を表示する例を示します。

```
Console> (enable) show vtp statistics
VTP statistics:
summary advts received          0
subset  advts received          0
request advts received          0
summary advts transmitted       7843
subset  advts transmitted       4
request advts transmitted       20
No of config revision errors    0
No of config digest errors      0


VTP pruning statistics:

Trunk    Join Transmitted Join Received Summary advts received from GVRP PDU
                                        non-pruning-capable device  Received
-------- ---------------- ------------- ---------------------------- ----------
16/1     75               0             0                            0
Console> (enable)
```

VTP バージョン 3 の機能概要

VTP バージョン 3 は、VLAN を直接処理しない旧 VTP バージョンとは異なります。VTP バージョン 3 は、不明瞭なデータベースのリストを管理ドメインに配信する機能だけを持つプロトコルです。イネーブルにした場合、VTP バージョン 3 により、旧 VTP バージョンよりも次のように機能が強化されます。

- 拡張 VLAN のサポート
- プライベート VLAN の作成およびアドバタイズのサポート
- VLAN インスタンスおよび MST マッピング伝播インスタンスのサポート
- サーバ認証の改良
- 「誤った」データベースが偶発的に VTP ドメイン内に追加されることからの保護
- VTP バージョン 1 および VTP バージョン 2 との相互作用
- ポート単位の設定機能

（注） Release 8.1(1) では、すべての VTP バージョンをポート単位で設定できます。

- VLAN データベース*および*他のデータベースを伝播する機能の提供。VTP バージョン 3 はプロトコル *インスタンス*の集合であり、各インスタンスは特定の機能に対応する 1 つのデータベースを処理します。VTP バージョン 3 は、複数のプロトコル インスタンスを実行することにより、互いに独立して複数のデータベース（機能）の設定を伝播する処理を行います。

（注） Release 8.1(x) および 8.2(x) では、データベース伝播がサポートされるのは VLAN データベースだけです。Release 8.3(1) では、MST データベースの伝播のためにサポートが追加されました。

ここでは、VTP バージョン 3 について説明します。

VTP バージョン 3 認証

VTP バージョン 3 では、VTP パスワードの処理が強化されています。VTP バージョン 3 を使用すれば、*プライマリ サーバ*を設定できます。VTP バージョン 3 サーバは、まずドメインのプライマリ サーバにならなければ、ドメイン内の設定を変更できません。VTP バージョン 3 認証では次の点が強化されています。

- パスワードを設定しないか、VTP バージョン 1 または VTP バージョン 2 と同じ方法で（**hidden** または **secret** キーワードを使用せずに）パスワードを設定した場合、次のようになります。
  - スイッチはプライマリ サーバになり、制限なくドメインを設定することができます。
  - 設定においてパスワードが表示されます。

  この機能強化は、従来の VTP バージョン 1 および VTP バージョン 2 のセキュリティ レベルに相当します。

- パスワードを **hidden** パスワード設定オプションを使用して hidden に設定した場合、次のようになります。
  - 設定においてパスワードはプレーン　テキストでは表示されません。パスワードはシークレットの 16 進数形式で設定に保存されます。
  - スイッチをプライマリ　サーバとして設定しようとすると、パスワード入力を要求されます。パスワードがシークレット パスワードに一致すれば、スイッチはプライマリ サーバとなり、ドメインの設定が可能となります。

パスワード設定の詳細については、「VTP バージョン 3 パスワードの設定」（p.10-28）を参照してください。

VTP バージョン 3 のポート単位設定

（注）　Release 8.1(1) では、すべての VTP バージョンをポート単位で設定できます。

VTP バージョン 3 を使用すれば、プロトコルをポート単位でディセーブルにできます。トランクが、信頼されておらず VTP ドメインと相互作用しないはずのスイッチまたはサーバに接続している場合は、着信 VTP パケットを廃棄することが可能であり、特定のトランクで VTP アドバタイズを防止できます。この設定オプションは、他のプロトコルには影響しません。

ポート単位設定オプションの詳細については、「ポート単位での VTP バージョン 3 のディセーブル化」（p.10-30）を参照してください。

VTP バージョン 3 のドメイン、モード、および分割

ここでは、VTP バージョン 3 でドメイン、モード、および分割を処理する方法を、VTP バージョン 1 および 2 との比較で説明します。

- VTP バージョン 3 サーバは、プライマリまたはセカンダリに設定できます。
- VTP バージョン 3 モード（サーバ、クライアント、およびトランスペアレント）は、VTP インスタンスに固有です。
- VTP バージョン 3 ドメインは分割が可能です。

これらの機能の詳細については、次の項を参照してください。

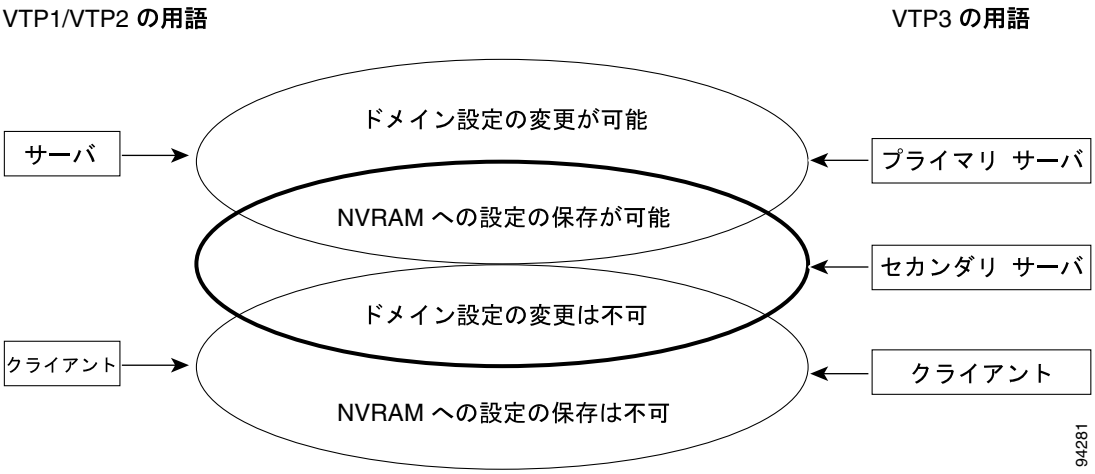
- プライマリ サーバ、セカンダリ サーバ、およびクライアント（p.10-15）
- VTP ドメインの分割（p.10-16）
- 分割 VTP ドメインの再設定（p.10-17）

プライマリ サーバ、セカンダリ サーバ、およびクライアント

VTP の以前の実装では、VTP サーバは VTP ドメイン設定の変更や NVRAM への保存が可能ですが、VTP クライアントはその設定をネットワークから受け取るだけで、保存や変更ができませんでした。

VTP バージョン 3 では、プライマリ サーバは VTP バージョン 1 およびバージョン 2 サーバと同様に機能します。セカンダリ サーバはドメイン設定を保存できますが変更できません。クライアントの概念は VTP バージョン 3 で変更はありません（図 10-3 を参照）。VTP バージョン 3 の主な特徴は、サーバ、クライアント、およびトランスペアレント モードが VTP インスタンスに固有である点です。たとえば、VTP バージョン 3 では、スイッチは 1 つのインスタンスに対してプライマリ サーバとなり、別のインスタンスに対してはクライアントとなることが可能です。

図 10-3　VTP バージョン 3：プライマリ サーバ、セカンダリ サーバ、およびクライアント



VTP ドメインの分割

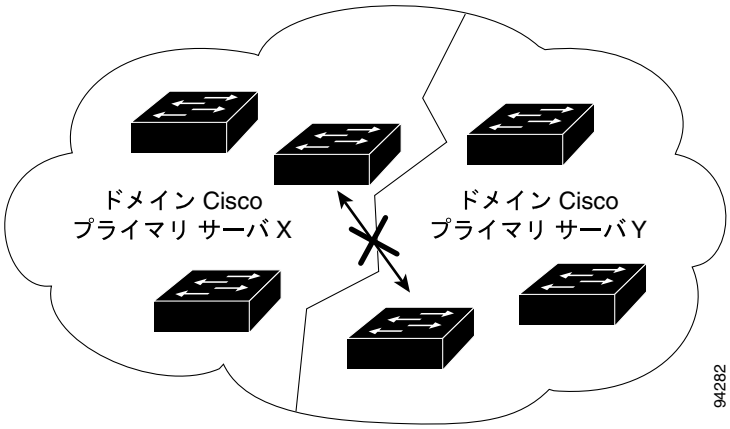
VTP バージョン 3 では、一意のプライマリ サーバに対するドメイン設定権限が次のように制限されます。

- VTP 設定はプライマリ サーバでのみ可能です。
- データベースを生成したプライマリ サーバの ID（識別子）は、VTP アドバタイズに付加されます。
- VTP スイッチはプライマリ サーバの ID を保持し、現在のプライマリ サーバからのみ VTP データベース アップデートを受け入れます。

プライマリ サーバの ID は常に VTP 設定とともに送信されるため、設定を持つスイッチはいずれも対応するプライマリ サーバを認識します。VTP バージョン 1 および VTP バージョン 2 の場合と同様、VTP 設定を持たないスイッチは、受信する最初の設定を受け入れます（「VTP バージョン 3 認証」[p.10-14] で説明したオプションの認証方式に合格した場合）。VTP バージョン 3 スイッチは、設定を生成したプライマリ サーバに*ロック*され、その後このプライマリ サーバからの VTP データベース アップデートのみを待ち受けます。このプロセスは、スイッチが常に同じドメイン内のネイバからの設定を優先的に受け入れる VTP バージョン 1 や VTP バージョン 2 とは著しく異なります。VTP バージョン 3 スイッチは、同じドメインからの設定、*および*同じプライマリ サーバによって生成された設定のみを優先的に受け入れます。

VTP バージョン 3 ドメイン内にはプライマリ サーバを 1 つだけにすることが理想的ですが、複数ある場合は、ドメインは各プライマリ サーバのアップデートに従う複数のグループに分割されます（図 10-4 を参照）。図 10-4 では、Cisco という VTP ドメインが、サーバ X またはサーバ Y をプライマリ サーバとして受け入れるスイッチ間で分割されています。異なるパーティションに属するスイッチは、同一ドメインの一部であってもデータベース情報を交換しません。サーバ X が VTP 設定を変更した場合、ネットワークの左のパーティションのみがそれを受け入れます。

図 10-4　VTP バージョン 3：VTP ドメインの分割



分割の存在理由は、VTP によって自動的に解決できないドメイン設定の不一致にあります。分割は、設定の誤りや、一時的に切断されたドメイン部分に対する個別設定の結果です。VTP バージョン 3 のこの機能は、ドメインを保護し、誤って設定したスイッチを導入したあとに矛盾した設定を受け入れないようにします。新しいスイッチをドメインに追加した場合、手動でそのスイッチを新しいプライマリ サーバに指定しないかぎり、その設定は伝播されません。

VLAN インスタンスのプライマリ サーバを、MST インスタンスのセットのプライマリ サーバとは別のサーバにできます。この場合プライマリ サーバが 2 つになりますが、分割されません。

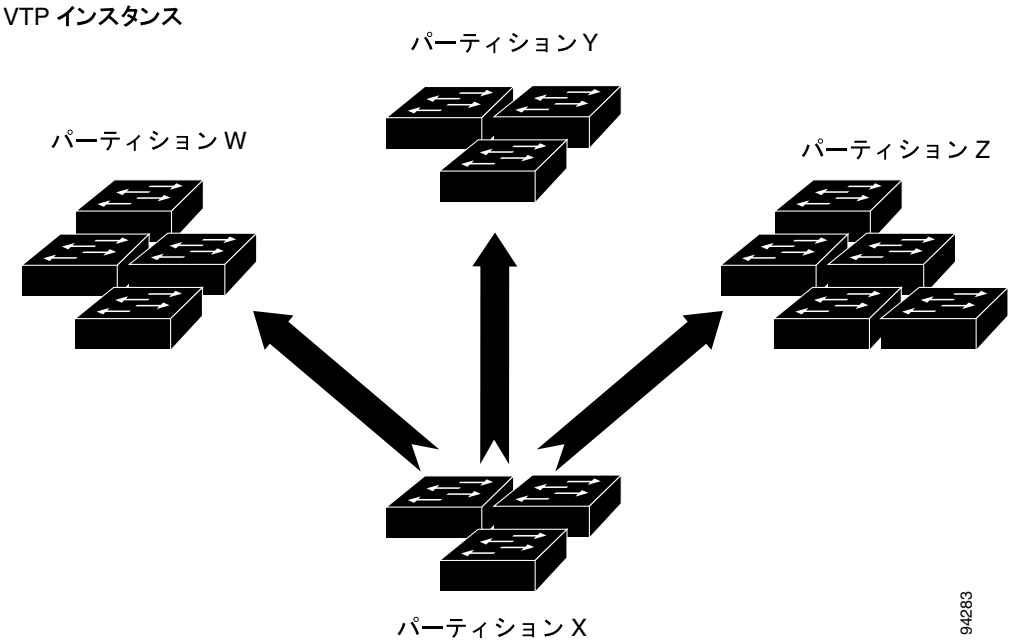
*テイクオーバー*機構を使用した分割 VTP ドメインの再設定について、「分割 VTP ドメインの再設定」（p.10-17）を参照してください。

分割 VTP ドメインの再設定

VTP ドメインの分割はインスタンスに固有です。つまり、あるインスタンスは、別のインスタンスが分割されていなくても分割できます。VTP バージョン 3 では、プロトコル側で最終的な正しい設定を持つプライマリ サーバを判別できないため、パーティションを削除する必要があります。図 10-5 に、1 つの特定の VTP インスタンスについて、4 つのパーティションに分割された VTP ドメインを示します。

図 10-5 では、サーバ X がドメインの正しい設定を持ちます。この分割 VTP ドメインを再設定するには、テイクオーバー メッセージをサーバ X からドメイン全体に発行し、サーバ X をこの特定のインスタンスの新しいプライマリ サーバとしてアドバタイズする必要があります。このドメイン内のすべてのスイッチはプライマリ サーバ X にロックされ、サーバ X によって起動されたインスタンス設定アップデートのみを受け入れます。ドメイン内のすべてのスイッチが、そのインスタンスについて VTP 設定をサーバ X に同期させます。

図 10-5　VTP バージョン 3：分割 VTP ドメインの再設定



テイクオーバーの起動は、次の理由により、重要な操作となります。

- テイクオーバーは、VTP ドメイン内の他のプライマリ サーバに保存されている可能性のある矛盾した設定を消去します。VTP は、（**show vtp conflicts** コマンドを実行すると）矛盾した設定を持つすべてのスイッチをリストし、テイクオーバーの前に確認を要求します（同じ VTP ドメインに属しているにもかかわらず異なるプライマリ サーバを持つ場合、サーバは矛盾した情報を持ちます）。
- テイクオーバーはこのスイッチ（図 10-5 のサーバ X）を、VTP ドメインを管理する唯一のプライマリ サーバとします。

hidden パスワードを設定している場合、テイクオーバーの実行にはパスワードの再入力が必要です。スイッチは正しく認証されなければ、テイクオーバー要求を拒否します。認証がイネーブルでなければ、どのサーバでもテイクオーバーが可能です。

テイクオーバー後は、特定のインスタンスについて VTP ドメイン全体を管理するプライマリ サーバは 1 つだけです。そうでない場合は、次のような理由が考えられます。

- 一部のスイッチが、テイクオーバー メッセージ送信の時点で一時的に切断されて到達不能でした。
- テイクオーバー メッセージが一部のリンク上で失われました（テイクオーバー メッセージは繰り返し送信されるので、この危険は小さくなります）。

いずれの場合も、テイクオーバー メッセージを再発行すれば問題を解消できます。

テイクオーバー設定の詳細については、「VTP バージョン 3 テイクオーバーの設定」（p.10-29）を参照してください。

VTP バージョン 3 のモード

デフォルトの VTP モードは、バージョン 1、サーバ モードです。オフ モードは、VTP ドメイン名をスイッチ上で設定したあとにだけ終了できます。VTP バージョン 1 および VTP バージョン 2 で使用する「ドメイン検出」は、VTP バージョン 3 では使用できません。

VTP バージョン 3 を実行中のスイッチは、次のような共通の特性があります。

- 同じ VTP ドメインからの VTP パケットのみを受け入れます。
- プライマリ サーバを持たない場合、どのインスタンスでも受信した最初の VTP データベースに対応するプライマリ サーバを受け入れます。
- 現在のプライマリ サーバから、より高いリビジョン番号を持つデータベースのみを受け入れます。
- パスワードを設定し、（hidden　を設定しているか否かにかかわらず）正しいパスワードを含む場合、新しいデータベースまたはテイクオーバー メッセージのみを受け入れます。

ここでは、VTP バージョン 3 のモードについて説明します。

- クライアント モード（p.10-19）
- サーバ モード（p.10-19）
- トランスペアレントおよび VTP オフ モード（p.10-20）

モード設定の詳細については、「VTP バージョン 3 のモード変更」（p.10-24）を参照してください。

クライアント モード

VTP バージョン 3 クライアントは、次のように、VTP バージョン 1 および VTP バージョン 2 クライアントと類似しています。

- ネットワークから VTP 設定を受け入れますが、その設定を生成または変更できません。
- 受信した VTP 設定を RAM（NVRAM ではありません）に格納します。起動時には、プライマリ サーバの ID を含めて、VTP によって伝播される設定全体を再取得する必要があります。
- 特定のインスタンスで受信した VTP 設定全体を RAM に格納できない場合、ただちにトランスペアレント モードに移行します。

サーバ モード

プライマリおよびセカンダリ サーバは、2 つのサーバ タイプとして VTP ドメイン内の 1 つの VLAN または VTP インスタンス上に存在できます。

セカンダリ サーバ

スイッチをサーバになるように設定すると、デフォルトではセカンダリ サーバになります。セカンダリ サーバとしては、VTP バージョン 3 スイッチは次の点を除いてクライアントとして動作します。

- セカンダリ サーバは、VTP バージョン 3 を介して受信した情報をただちに NVRAM に保存します。この NVRAM は、実行コンフィギュレーションまたはスタートアップ コンフィギュレーションの一部です。
- 起動時に、NVRAM　内に設定を持つセカンダリ　サーバは設定のアドバタイズを開始します。VTP セカンダリ サーバの主要な目的は、ネットワークに伝播される設定をバックアップすることです。
- クライアントと同様、VTP セカンダリ サーバは VTP 設定を変更できません。
- 設定を NVRAM に保存できない場合、VTP サーバはクライアント モードに戻ります。
- VTP バージョン 3 セカンダリ サーバは、プライマリ サーバになるためにテイクオーバーを発行できます。

プライマリ サーバ

プライマリ サーバは VTP 設定を生成または変更できます。プライマリ サーバ ステートに入るには、スイッチからテイクオーバーを発行する必要があります。テイクオーバーは、ドメイン全体に伝播されます。ドメイン内の他の潜在的プライマリ サーバは、すべてセカンダリ サーバ モードに移行し、その VTP ドメインでプライマリ サーバが 1 つだけになるようにします。

プライマリ サーバが必要なのは、いずれかのインスタンスの VTP 設定を変更する必要がある場合だけです。セカンダリ サーバがリロードを通じて設定の持続性を保証するため、VTP ドメインは、アクティブなプライマリ サーバがなくても動作できます。プライマリ サーバ ステートは、次の理由により終了します。

- スイッチの再起動
- アクティブおよび冗長スーパバイザ エンジン間のハイアベイラビリティ スイッチオーバー
- 別のサーバからのテイクオーバー
- モード設定の変更
- VTP ドメイン設定の変更（バージョン、ドメイン名、またはドメイン パスワードなど）

トランスペアレントおよび VTP オフ モード

VTP バージョン 3 では、トランスペアレント モードはインスタンスに固有です。VTP バージョン 3 のオフ モードは以前の VTP バージョンと同様であり、インスタンスに固有ではありません。いずれのモードでも、VTP が管理する機能をローカルに設定できます。この設定は、（該当する場合）実行コンフィギュレーションにも含まれます。この機能は、VTP が使用するのと同じ NVRAM ブロックにローカル設定を保存します。この機能についての NVRAM 処理は、スイッチがこの機能に対してトランスペアレントであるかどうかにかかわらず、すべて VTP を通じて起こります。VTP トランスペアレント モードでは、スイッチが受信する VTP メッセージはすべてフラッディングされます。VTP オフ モードでは、VTP メッセージはトランクで廃棄されます。

VTP バージョン 3 データベース

VTP バージョン 1 および VTP バージョン 2 は、VLAN 情報に関連付けられています。VTP バージョン 3 は、あらゆる種類の設定（データベース）を VTP ドメイン全体に配信するよう設計されています。

（注） Release 8.1(x) および 8.2(x) では、データベース伝播がサポートされるのは VLAN データベースだけです。Release 8.3(1) では、MST データベースの伝播のためにサポートが追加されました。

ここでは、VTP バージョン 3 データベースについて説明します。

- 有効なデータベース（p.10-21）
- データベース リビジョン番号（p.10-21）
- VTP バージョン 1 および VTP バージョン 2 との相互作用（p.10-22）
- 制限（p.10-22）

有効なデータベース

スイッチがデータベースをアドバタイズするのは、それが有効な場合のみです。データベースの有効性を確認するには、プライマリ サーバになるしかありません。スイッチがプライマリ サーバによって生成されたデータベースを変更した場合（オフまたはトランスペアレント モードで可能）、そのデータベースは無効です。無効なデータベースはローカルに適用されるだけであり、そのスイッチが VTP サーバまたはクライアントである場合、ネットワークで受信したどのデータベースによっても上書きされます。次に、いくつかの有効および無効なデータベースの例を示します。

- VTP バージョン 1 から VTP バージョン 3 に移行するとき、VLAN データベースおよび MST データベースは削除されません。ただし、VTP バージョン 3 のプライマリ サーバではなく、VTP バージョン 1 のサーバによって生成されたため、VLAN データベースは無効とマークされます。
- 有効なデータベースを持つ VTP バージョン 3 サーバがトランスペアレント モードに移行した場合、VLAN データベースおよび MST データベースを設定できますが、データベースを変更するとただちに無効になります。この場合、ネットワークから受信した有効なデータベースにより、トランスペアレントモードの間に行われた変更が上書きされてしまうため、スイッチがサーバ モードに戻り、このデータベースをアドバタイズすることができなくなります。サーバがトランスペアレント モードに移行し、その後データベース設定を変更せずにサーバ モードに戻った場合、そのデータベースは依然として有効です。
- プライマリ サーバ上のデータベース（VLAN 設定など）を変更した場合、そのデータベースは依然として有効であり、ドメインの残りの部分にアドバタイズされます。どのモードでも、ドメイン関連のパラメータ（ドメイン名、VTP バージョン、認証方式［パスワード］など）を設定した場合、すべてのデータベースが無効になります。データベースの無効化に加えて、ドメイン関連パラメータを設定すると、プライマリ サーバはセカンダリ サーバに戻ります。
- ドメイン パラメータを変更すると、そのスイッチは新しいドメインに追加されます。この誤ったデータベースが偶発的に VTP ドメインに追加されることを防止するため、スイッチをプライマリ サーバとして新しいドメインに追加することはできません（有効な設定を消去する可能性があるため）。無効なデータベースを持つため、ドメインに新しく追加されたスイッチは、ただちにネットワーク設定を受け入れます。ネットワーク設定を消去してしまうことはありません。

データベース リビジョン番号

各 VTP インスタンスは、データベース リビジョン番号に関連付けられています。データベース リビジョン番号は、アドバタイズされたチェックサムがカバーするデータベースの値が変更されると、増分します。

装置が、同じドメイン内のインスタンスの同じプライマリ サーバから VTP アドバタイズを受信すると、次のようになります。

- そのアドバタイズ内のデータベース　リビジョン番号が受信側装置のリビジョン番号より小さい場合、そのアドバタイズは無視され、現行リビジョン番号付きのサマリー アドバタイズが、元のアドバタイズが受信されたトランクで伝送されます。
- そのアドバタイズ内のデータベース　リビジョン番号が受信側装置のリビジョン番号と同じである場合、次のようになります。
  - そのアドバタイズのチェックサムが受信側装置に既知である現在の設定のチェックサムと厳密に同じである場合、何も起きません。
  - そのアドバタイズのチェックサムが受信側装置に既知である現在の設定のチェックサムと厳密に同じではない場合、その装置の設定は影響を受けませんが、装置はデータベース管理者に設定エラー状態の発生を示します。
- そのアドバタイズ内のデータベース　リビジョン番号が受信側装置のリビジョン番号よりも大きく、そのアドバタイズのチェックサムおよび設定情報が一致する場合、その受信側スイッチは、古くなったデータベースの正確なサブセットを要求します。

VTP アドバタイズは、装置の各トランク ポート上で再生成されますが、受信したトランク ポート上では再生成されません。

VTP バージョン 1 および VTP バージョン 2 との相互作用

VTP バージョン 3 は、VTP バージョン 1 および VTP バージョン 2 スイッチと以下のように相互作用します。

(注) VTP バージョン 1 および VTP バージョン 2 スイッチを VTP バージョン 3 と正しく連携させるには、それらをクライアントとして設定する必要があります。詳細については、「制限」（p.10-22）を参照してください。

- VTP バージョン 3 スイッチは、VTP バージョン 1 および VTP バージョン 2 スイッチを検出し、VTP バージョン 2 形式のみで、自分のデータベースのスケールダウン バージョンをトランク単位で送信できます。VTP バージョン 1 スイッチは、設定による支援なしで VTP バージョン 2 モードに移行します。
- VTP バージョン 3 スイッチは、あるトランクでレガシー VTP バージョン 1 または VTP バージョン 2 のパケットを初めて受信する場合、そのトランク上で VTP バージョン 2 パケットを送ることはありません。そのため近接するレガシー スイッチは、リンク上で自分の存在をアドバタイズし続ける必要があります。VTP バージョン 3 スイッチがあるトランク上で一定期間レガシー パケットを受信しない場合、そのトランクは VTP バージョン 3 のみのトランクとみなされ、そのトランク上では VLAN データベースまたは MST データベースのスケールダウン バージョンをこれ以降アドバタイズしなくなります。
- あるトランク上で VTP バージョン 2 データベースをアドバタイズする場合でも、VTP バージョン 3 は、そのポートを通じて VTP バージョン 3 アップデートの送信を続けます。これにより、2 種類のネイバがそのトランクで共存できます。
- VTP バージョン 3 スイッチは、予約 VLAN 1002 ～ 1005 を変更できます。ただし、これらの VLAN は、VTP バージョン 2 形式のスケールダウンされたデータベースではデフォルトに設定されます。
- VTP バージョン 3 スイッチは、VTP バージョン 1 または VTP バージョン 2 のネイバから設定を受け入れることはありません。

制限

VTP バージョン 3 の制限は、次のとおりです。

- トランスペアレント モードの VTP バージョン 1 および VTP バージョン 2 リージョンで通信できるのは、2 つの VTP バージョン 3 リージョンだけです。
- VTP バージョン 2 リージョンにサーバがあり、VTP 情報を VTP バージョン 3 リージョンから受信する場合、問題が発生することがあります。VTP バージョン 1 および VTP バージョン 2 リージョンで設定が変更されると、データベースのリビジョンが VTP バージョン 3 リージョンによって生成されるリビジョンより高くなり、VTP バージョン 3 リージョンからのアップデートが無視されることがあります。

  (注) VTP バージョン 1 および VTP バージョン 2 リージョンのスイッチはすべてクライアントに設定し、リビジョン番号をリセットすることを推奨します（リロード実行またはドメイン名変更を繰り返します）。

- 2 つの異なる VTP バージョン 3 リージョンに接続した VTP バージョン 2 リージョンは、矛盾した情報を受信し、その時々の最高のリビジョン番号を持つ VTP バージョン 3 リージョンとデータベースを交換し続けることがあります。この種の設定は推奨できません。
- VTP バージョン 3 スイッチ上で VTP プルーニングをイネーブルにしても、プルーニングはそのスイッチ上でイネーブルになるだけです。VTP バージョン 1 や VTP バージョン 2 のように伝播されることはありません。

VTP バージョン 3 のデフォルト設定

表 10-2 に、VTP バージョン 3 のデフォルト設定を示します。

表 10-2　VTP バージョン 3 のデフォルト設定

機能	デフォルト値
VTP ドメイン名	ヌル
VTP モード	サーバ
VTP バージョン 3 のイネーブル ステート	バージョン 1 がイネーブル
VTP パスワード	none
VTP プルーニング	ディセーブル

VTP バージョン 3 の設定

ここでは、VTP バージョン 3 の設定手順について説明します。

VTP バージョン 3 のイネーブル化

VTP バージョンを指定するには、**set vtp version** *version_number* コマンドを使用します。デフォルトでは、VTP バージョンはバージョン 1 であり、VTP モードはサーバ モードです。VTP バージョンまたは VTP モードを選択する前に、ドメインを指定する必要があります。

VTP バージョン 3 をイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチ上で VTP バージョン 3 をイネーブルにします。	**set vtp version 3**
ステップ 2	VTP バージョン 3 がイネーブルに設定されたことを確認します。	**show vtp domain**

次に、VTP バージョン 3 をイネーブルにし、設定を確認する例を示します。

```
Console> (enable) set vtp version 3
VTP version 3 cannot be enabled on a switch with No Domain.
Console> (enable) set vtp domain ENG
VTP domain ENG modified
Console> (enable) set vtp version 3
VTP version 3 Server/Client for VLANDB requires Reduced Mac Address feature to
be enabled (use "set spantree macreduction enable" command)
Console> (enable) set spantree macreduction enable
MAC address reduction enabled
Console> (enable) set vtp version 3
This command will enable VTP version 3 on this switch.
Do you want to continue (y/n) [n]? y
VTP3 domain ENG modified
Console> (enable) show vtp domain
Version      : running VTP3
Domain Name  : ENG                              Password  : configured
Notifications: disabled                          Switch ID : 00d0.004c.1800

Feature        Mode           Revision    Primary ID     Primary Description
-------------- -------------- ----------- -------------- ----------------------
VLAN           Server         0           0000.0000.0000
MST            Transparent
UNKNOWN        Transparent

Pruning             : disabled
VLANs prune eligible: 2-1000
Console> (enable)
```

VTP バージョン 3 のモード変更

（注） VTP バージョンのモードの詳細については、「VTP バージョン 3 のモード」（p.10-19）を参照してください。

各データベースは VTP プロトコルのインスタンスによって伝播されます。これらのインスタンスは独立しているため、異なるモードで動作可能です。**set vtp mode** コマンドを使用すれば、特定の VTP インスタンスのモードを設定できます。VTP インスタンスは、対応する機能名により特定されます。**set vtp mode** コマンドは拡張されて、このコマンドを適用するデータベースを特定するために指定する *feature* が含められました。**unknown** キーワードにより、解釈できないスイッチ データベースの動作を設定できます（これらのデータベースは、将来、VTP バージョン 3 の拡張で対応する機能です）。**set vtp mode transparent unknown** コマンドを実行すると、機能が unknown のパケットは、そのスイッチを通じてフラッディングされます。**set vtp mode off unknown** コマンドを実行すると、そのパケットは廃棄されます。[unknown] 機能は、オフまたはトランスペアレント モードでのみ設定可能です。デフォルト モードは、すべてのデータベースについてオフです。VLAN データベースおよび MST データベースのモードは、VTP バージョン変更の際、保全されます。

（注） Release 8.1(x) および 8.2(x) では、データベース伝播がサポートされるのは VLAN データベースだけです。したがって、[unknown] データベースはありません。Release 8.3(1) では、MST データベースの伝播のためにサポートが追加されました。

VTP バージョン 3 サーバの設定

スイッチが VTP バージョン 3 サーバ モードの場合、VLAN 設定を変更し、その変更をスイッチ全体に伝播することができます。VTP バージョン 3 サーバとしてスイッチを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	VTP ドメイン名を定義します。	**set vtp domain** *name*
ステップ 2	スイッチを VTP サーバ モードにします。	**set vtp mode server** {**vlan** | **mst** | **unknown**}
ステップ 3	（任意）VTP ドメイン用のパスワードを設定します。	**set vtp passwd** *passwd*
ステップ 4	VTP 設定を確認します。	**show vtp domain**

次に、VTP VLAN サーバとしてスイッチを設定し、その設定を確認する例を示します。

```
Console> (enable) set vtp mode server vlan
Changing VTP mode for vlan feature
VTP3 domain map1 modified
Console> (enable) show vtp domain
Version      : running VTP3
Domain Name  : ENG                             Password  : configured
Notifications: disabled                        Switch ID : 00d0.004c.1800

Feature        Mode           Revision    Primary ID     Primary Description
-------------- -------------- ----------- -------------- ----------------------
VLAN           Server         0           0000.0000.0000
MST            Transparent
UNKNOWN        Transparent

Pruning             : disabled
VLANs prune eligible: 2-1000
Console> (enable)
```

次に、VTP MST サーバとしてスイッチを設定し、その設定を確認する例を示します。

```
Console> (enable) set vtp mode server mst
Changing VTP mode for mst feature
VTP3 domain ENG modified
Console> (enable) show vtp domain
Version      : running VTP3
Domain Name  : ENG                             Password  : configured
Notifications: disabled                        Switch ID : 00d0.004c.1800

Feature        Mode           Revision    Primary ID     Primary Description
-------------- -------------- ----------- -------------- ----------------------
VLAN           Server         0           0000.0000.0000
MST            Server         0           0000.0000.0000
UNKNOWN        Transparent

Pruning             : disabled
VLANs prune eligible: 2-1000
Console> (enable)
```

VTP バージョン 3 クライアントの設定

スイッチが VTP クライアント モードの場合、スイッチ上で VLAN 設定を変更することはできません。クライアント スイッチは管理ドメイン内の VTP サーバから VTP アップデート情報を受信し、それに基づいて設定を変更します。

VTP バージョン 3 クライアントとしてスイッチを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	VTP ドメイン名を定義します。	**set vtp domain** *name*
ステップ 2	スイッチを VTP クライアント モードにします。	**set vtp mode client** [**vlan** | **mst** | **unknown**]
ステップ 3	VTP 設定を確認します。	**show vtp domain**

次に、VTP バージョン 3 VLAN クライアントとしてスイッチを設定し、その設定を確認する例を示します。

```
Console> (enable) set vtp mode client vlan
Changing VTP mode for vlan feature
VTP3 domain ENG modified
Console> (enable) show vtp domain
Version      : running VTP3
Domain Name  : ENG                              Password  : configured
Notifications: disabled                         Switch ID : 00d0.004c.1800

Feature        Mode           Revision    Primary ID     Primary Description
-------------- -------------- ----------- -------------- ----------------------
VLAN           Client         0           0000.0000.0000
MST            Server         0           0000.0000.0000
UNKNOWN        Transparent

Pruning             : disabled
VLANs prune eligible: 2-1000
Console> (enable)
```

VTP バージョン 3 トランスペアレント モードの設定

VTP トランスペアレントとしてスイッチを設定すると、スイッチ上で VTP がディセーブルになります。VTP トランスペアレント スイッチは VTP アップデートを送信せず、他のスイッチから受信した VTP アップデートにも反応しません。

(注) VTP トランスペアレント モードのネットワーク装置は、VTP Join メッセージを送信しません。VTP トランスペアレント モードのネットワーク装置にトランク接続されている Catalyst 6500 シリーズ スイッチに、トランスペアレントモード ネットワーク装置で使用される VLAN、またはプルーニング不適格としてトランク間で伝送する必要がある VLAN を設定します（**clear vtp pruneeligible** コマンドを使用します）。

スイッチ上で VTP をディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	VTP トランスペアレント モードに設定して、スイッチ上で VTP をディセーブルにします。	**set vtp mode transparent** [**vlan** | **mst** | **unknown**]
ステップ 2	VTP 設定を確認します。	**show vtp domain**

次に、スイッチを VTP VLAN トランスペアレントとして設定し、その設定を確認する例を示します。

```
Console> (enable) set vtp mode transparent vlan
Changing VTP mode for vlan feature
VTP3 domain ENG modified
Console> (enable) show vtp domain
Version      : running VTP3
Domain Name  : ENG                              Password  : configured
Notifications: disabled                         Switch ID : 00d0.004c.1800

Feature        Mode           Revision    Primary ID     Primary Description
-------------- -------------- ----------- -------------- ----------------------
VLAN           Transparent
MST            Server         0           0000.0000.0000
UNKNOWN        Transparent

Pruning             : disabled
VLANs prune eligible: 2-1000
Console> (enable)
```

オフ モードによる VTP のディセーブル化

オフ モードを使用して VTP をディセーブルにした場合、VTP アドバタイズが転送されないことを除き、スイッチの動作は VTP トランスペアレント モードの場合と同じです。

オフ モードを使用して VTP をディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	オフ モードを使用して VTP をディセーブルにします。	**set vtp mode off**
ステップ 2	VTP 設定を確認します。	**show vtp domain**

次に、オフ モードを使用して VTP をディセーブルにする例を示します。

```
Console> (enable) set vtp mode off
Changing VTP mode for all features
VTP3 domain server modified
```

（注） Release 8.1(x) および 8.2(x) では VLAN データベースしかないため、**set vtp mode off** コマンドを **vlan** キーワードを指定せずに使用しても、**vlan** キーワードを指定した場合と同じ設定になります。Release 8.3(1) では、MST データベースの伝播のためにサポートが追加されたことに注意してください。

```
Console> (enable) show vtp domain
Version      : running VTP3
Domain Name  : ENG                              Password  : configured
Notifications: disabled                         Switch ID : 00d0.004c.1800

Feature        Mode           Revision    Primary ID     Primary Description
-------------- -------------- ----------- -------------- ----------------------
VLAN           Off
MST            Off
UNKNOWN        Transparent

Pruning             : disabled
VLANs prune eligible: 2-1000
Console> (enable)
```

VTP バージョン 3 パスワードの設定

(注)　パスワードに関する詳細については、「VTP バージョン 3 認証」（p.10-14）を参照してください。

VTP バージョン 3 では、パスワード設定に **hidden** キーワードを追加することで、設定から VTP パスワードを隠すことができます。**hidden** キーワードを使用した場合、設定ではパスワードから生成された 16 進数のシークレット キーが、プレーン テキストのパスワードの代わりに表示されます。パスワードを **hidden** キーワード付きで設定した場合、テイクオーバーの発行にはパスワードの再入力が必要です（テイクオーバー設定の詳細については、「VTP バージョン 3 テイクオーバーの設定」[p.10-29] を参照してください）。

設定では、**set vtp passwd** コマンドは 2 つの異なる形式で表示できます。プレーン テキストのパスワード、または暗号化した 16 進数のシークレット値です。これら 2 つの形式は互いに排他的です。プレーン テキストのパスワードを設定した場合、現在のシークレット パスワードがプレーン テキストに置き換えられます。同様に、シークレット パスワードを設定内にペーストした場合、元のパスワードは削除されます。

VTP パスワードを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	VTP パスワードを設定します。	**set vtp passwd** *passwd* {**hidden** | **secret**}
ステップ 2	VTP パスワードを確認します。	**show config**

次に、VTP パスワードを設定し、その設定を確認する例を示します。

```
Console> (enable) set vtp passwd toto
Generating the secret associated to the password.
VTP3 domain server modified
Console> (enable) show config
.
.
.
set vtp passwd toto
.
.
.
Console> (enable) set vtp passwd toto hidden
Generating the secret associated to the password.
The VTP password will not be shown in the configuration.
VTP3 domain server modified
Console> (enable) show config
.
.
.
set vtp passwd 9fbdf74b43a2815037c1b33aa00445e2 secret
.
.
.
Console> (enable) set vtp passwd toto secret
VTP secret has to be 32 characters in length
Console> (enable)
```

次に、シークレットの 16 進数値を設定からコピーしてコマンドラインにペーストし、設定を確認する例を示します。

```
Console> (enable) set vtp passwd 9fbdf74b43a2815037c1b33aa00445e2 secret
Setting secret.
VTP3 domain server modified
Console> (enable) show config
.
.
.
set vtp passwd 9fbdf74b43a2815037c1b33aa00445e2 secret
.
.
.
```

VTP バージョン 3 テイクオーバーの設定

(注)　テイクオーバーの詳細については、「分割 VTP ドメインの再設定」（p.10-17）を参照してください。

テイクオーバーを設定するには、**set vtp primary** [*feature*] [**force**] コマンドを使用します。テイクオーバーを使用すればセカンダリ サーバはプライマリ サーバになり、そのプライマリ サーバの設定を VTP ドメイン全体に伝播できるため、存在する場合パーティションは消去されます。

(注)　パスワードを **hidden** キーワードを使用して設定した場合、パスワードの再入力を要求されます。

force キーワードを指定しなければ、スイッチはドメイン内で矛盾したサーバを検出しようとします。矛盾したサーバは、ローカル スイッチの設定内のサーバとは異なるプライマリ サーバに従います。ローカル スイッチは、テイクオーバーを進める前に確認を要求します。こうした確認を行うのは、ドメインのテイクオーバーが、あらゆる矛盾したサーバの設定の上書きを伴うからです。

オプションの *feature* 引数を指定しない場合、ローカル スイッチは、それがセカンダリまたはプライマリ サーバとなる各データベースについてテイクオーバー メッセージを送信します。データベースを指定した場合、スイッチは指定した feature に対応するデータベースのみをテイクオーバーします。

テイクオーバーを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	テイクオーバーを設定します。	**set vtp primary** [*feature*] [**force**]
ステップ 2	テイクオーバーを確認します。	**show vtp domain**

次に、hidden パスワードを設定したセカンダリ スイッチからテイクオーバーを設定し、その設定を確認する例を示します。

```
Console> (enable) set vtp primary force
Switch can become primary server for vlan feature only when configured as a server
Switch can become primary server for mst feature only when configured as a server
Console> (enable) set vtp mode server mst
Changing VTP mode for mst feature
VTP3 domain ENG modified
Console> (enable) set vtp mode server vlan
Changing VTP mode for vlan feature
VTP3 domain ENG modified
Console> (enable) set vtp primary force
This switch is becoming primary server for feature vlan.
This switch is becoming primary server for feature mst.
Do you want to continue (y/n) [n]? y
Console> (enable) show vtp domain
Version      : running VTP3
Domain Name  : ENG                              Password  : configured
Notifications: disabled                         Switch ID : 00d0.004c.1800

Feature         Mode            Revision    Primary ID     Primary Description
--------------- --------------- ----------- -------------- ----------------------
VLAN            Primary Server 1            00d0.004c.1800
MST             Primary Server 1            00d0.004c.1800
UNKNOWN         Transparent

Pruning             : disabled
VLANs prune eligible: 2-1000
Console> (enable)
```

ポート単位での VTP バージョン 3 のディセーブル化

（注） ポートごとの VTP バージョン 3 のディセーブル化の詳細については、「VTP バージョン 3 のポート単位設定」（p.10-15）を参照してください。

すべての VTP 相互作用をポート単位でイネーブルまたはディセーブルにするには、**set port vtp** *mod/port* {**enable** | **disable**} コマンドを使用します。この機能は、信頼性のないホストに導くトランクで使用されることがあります。ポートをディセーブルにすると、VTP パケットはそのポートには送信されず、そのポートで受信された VTP パケットはいずれも廃棄されます。デフォルトでは、VTP はイネーブルであり、アドバタイズはすべてのトランクで送受信されます。

ポート単位で VTP をディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	VTP をポート単位でディセーブルにします。	**set port vtp** *mod/port* {**enable** | **disable**}
ステップ 2	変更を確認します。	**show port vtp**

次に、ポート単位で VTP をディセーブルにし、設定を確認する例を示します。

```
Console> (enable) set port vtp 3/1-2 disable
VTP is disabled on ports 3/1-2.
Console> (enable) show port vtp 3
Port      VTP Status
--------  ----------
 3/1      disabled
 3/2      disabled
 3/3      enabled
 3/4      enabled
 .
 .
 .
Console> (enable)
```

VTP バージョン 3 の show コマンド

ドメイン内の他の装置（**devices**）、またはドメイン内で矛盾した（**conflicts**）設定を持つ装置を表示するには、**show vtp** {**conflicts** | **devices** | **domain** | **statistics**} コマンドを使用します。**domain** キーワードを使用すれば、その VTP ドメインに固有の情報を表示できます。**statistics** キーワードを使用すれば、VTP 統計情報を表示できます。トランスペアレントまたはオフ モードのスイッチは VTP ドメインの一部ではなく、要求に応答しません。さらに、有効なデータベースを持たないクライアントまたはサーバは要求に応答しません。

CHAPTER 11

VLAN の設定

この章では、Catalyst 6500 シリーズ スイッチに VLAN（仮想 LAN）を設定する手順について説明します。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

この章で説明する内容は、次のとおりです。

VLAN の機能

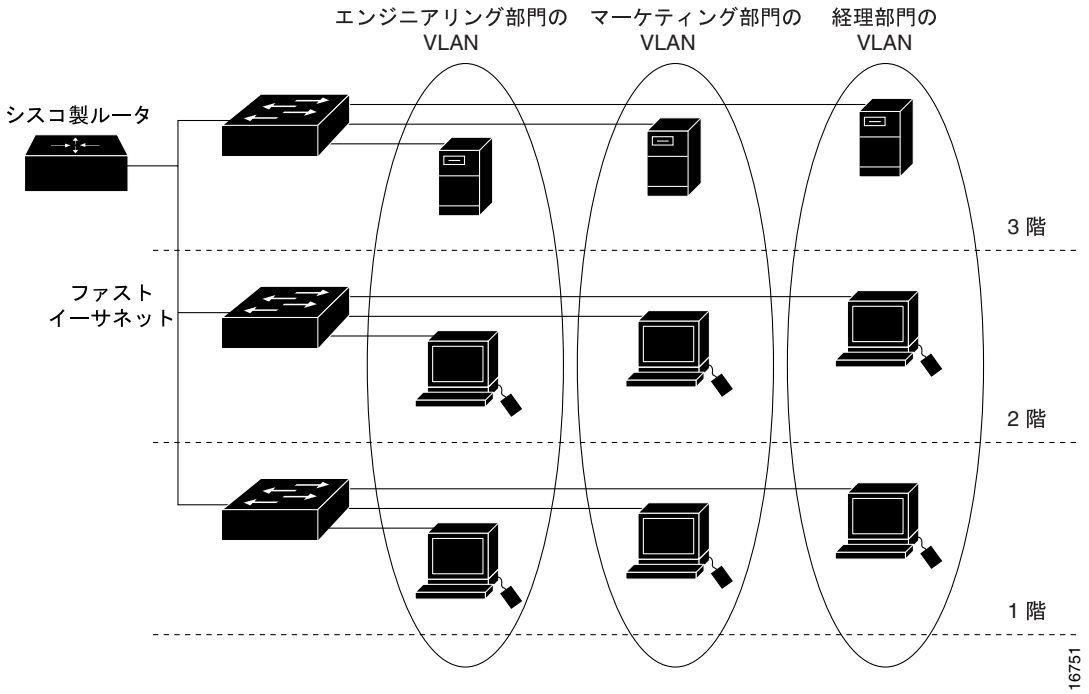
VLAN は、物理的な位置にかかわりなく、共通の要件を持ったエンド ステーションのグループです。VLAN は、物理 LAN と同じ属性をすべて備えていますが、物理的に同じ LAN セグメントに置かれていないエンド ステーションでもグループ化することができます。

VLAN を使用すると、スイッチ上のポートをグループとしてまとめ、ユニキャスト、マルチキャスト、およびブロードキャスト トラフィックのフラッディングを制限することができます。特定の VLAN から送信されたフラッディング トラフィックは、その VLAN に所属する他のポートだけにフラッディングされます。

図 11-1 に、論理的に定義されたネットワークへの VLAN セグメンテーションの例を示します。

ここでは、VLAN について説明します。

図 11-1　論理的に定義されたネットワークとしての VLAN



VLAN は、IP サブネットワークとよく対応付けられます。たとえば、特定の IP サブネットに含まれるすべてのエンド ステーションは同じ VLAN に属します。VLAN 間のトラフィックはルーティングが必要です。スイッチ上のポートの VLAN メンバーシップは、ポート別に手動で割り当てます。この方法でスイッチ ポートを VLAN に割り当てた場合、ポートベース（またはスタティック）VLAN メンバーシップといいます。

スイッチの帯域内（sc0）インターフェイスを任意の VLAN に割り当てることができるので、ルータを経由しなくても、同一 VLAN 上の他のスイッチに直接アクセスできます。帯域内インターフェイスに一度に割り当てることができる IP アドレスは、1 つだけです。IP アドレスを変更し、インターフェイスを別の VLAN に割り当てると、それまでの IP アドレスと VLAN 割り当てが上書きされます。

VLAN の範囲

Catalyst 6500 シリーズ スイッチは、IEEE 802.1Q 規格に従って、4,096 個の VLAN をサポートしています。これらの VLAN は、2 つの範囲で編成されます。各範囲の用途は、少しずつ異なります。VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）などの管理プロトコルを使用すると、ネットワーク上の他のスイッチに伝播される VLAN もあります。伝播されず、個々の該当するスイッチ上で設定が必要な VLAN もあります。

VLAN は次の 2 つの範囲に分けられます。

- 標準範囲 VLAN：1 ～ 1023
- 拡張範囲 VLAN：1024 ～ 4094

（注） VTP バージョン 3 を使用して、VLAN 1006 ～ 4094 を管理できます。これらの VLAN は VTP バージョン 3 により伝播されます。

VLAN パラメータの設定

VLAN 2 ～ 1005 を作成または変更する場合、次のパラメータを設定できます。

（注） イーサネット VLAN 1 および 1025 ～ 4094 については、デフォルト値しか使用できません。

（注） Release 8.3(1) 以降のソフトウェア リリースでは、すべてのユーザ VLAN の名前を付けられます。この機能は、VTP のバージョンまたはモードに関係ありません。

- VLAN 番号
- VLAN 名
- VLAN タイプ：イーサネット、FDDI、FDDINET、Token Ring Bridge Relay Function（TrBRF; トークンリング ブリッジ リレー機能）、または Token Ring Concentrator Relay Function（TrCRF; トークンリング コンセントレータ リレー機能）
- VLAN ステート：アクティブまたは停止
- Multi-Instance Spanning-Tree Protocol（MISTP）インスタンス
- プライベート VLAN タイプ：プライマリ、隔離、コミュニティ、双方向コミュニティ、またはなし
- Security Association Identifier（SAID）
- VLAN の Maximum Transmission Unit（MTU; 最大伝送ユニット）
- FDDI および TrCRF VLAN のリング番号
- TrBRF VLAN のブリッジ識別番号
- TrCRF VLAN の親 VLAN 番号
- TrCRF VLAN の Spanning-Tree Bridge Protocol（STP; スパニングツリー ブリッジ プロトコル）タイプ：IEEE、IBM、または auto
- VLAN メディア間でタイプの変換を行うときに使用する VLAN（VLAN 1 ～ 1005 のみ）。メディア タイプごとに異なる VLAN 番号が必要

- トークンリング VLAN 用ソースルーティング ブリッジ モード：Source-Route Bridge（SRB; ソースルート ブリッジ）または Source-Route Transparent（SRT; ソースルート トランスペアレント）ブリッジ
- TrCRF VLAN のバックアップ
- トークンリング用の最大ホップ VLAN All-Routes Explorer（ARE）フレームおよび Spanning-Tree Explorer（STE）フレーム
- Remote Switched Port Analyzer（RSPAN）

VLAN のデフォルト設定

表 11-1 に、Catalyst 6500 シリーズ スイッチの VLAN デフォルト設定を示します。

表 11-1　VLAN のデフォルト設定

機能	デフォルト値
ネイティブ（デフォルト）VLAN	VLAN 1
ポート VLAN 割り当て	すべてのポートを VLAN 1 に割り当てる トークンリング ポートを VLAN 1003（trcrf-default）に割り当てる
VLAN ステート	アクティブ
MTU サイズ	1,500 バイト トークンリング VLAN の場合 4,472 バイト
SAID 値	100,000 + VLAN 番号（たとえば、VLAN 8 の SAID 値は 100,008、VLAN 4050 の SAID 値は 104,050）
プルーニングの適格性	VLAN 2 ～ 1000 はプルーニング適格、VLAN 1025 ～ 4094 はプルーニング不適格
MAC アドレス リダクション	ディセーブル
スパニングツリー モード	PVST+
デフォルトの FDDI VLAN	VLAN 1002
デフォルトの FDDI NET VLAN	VLAN 1004
デフォルトのトークンリング TrBRF VLAN	VLAN 1005（trbrf-default）およびブリッジ番号 0F
デフォルトのトークンリング TrCRF VLAN	VLAN 1003（trcrf-default）
TrBRF VLAN の STP バージョン	IBM
VLAN ポート プロビジョニング検証	ディセーブル
TrCRF ブリッジ モード	SRB
RSPAN	ディセーブル

スイッチ上での VLAN の設定

ここでは、ユーザ VLAN（1 ～ 4094）の設定手順について説明します。

（注） 標準範囲 VLAN 1 は、設定または変更できません。

標準範囲 VLAN 設定時の注意事項

ここでは、ネットワーク上でユーザ VLAN を作成および変更する場合の注意事項について説明します。

- デフォルトの VLAN タイプはイーサネットです。したがって、VLAN タイプを指定しなかった場合、VLAN はイーサネット VLAN になります。
- VTP を使用してネットワーク上のグローバル VLAN 設定情報を維持する場合には、標準範囲 VLAN を作成する前に、VTP を設定してください。VTP 設定の詳細については、第 10 章「VTP の設定」を参照してください（VTP を使用して拡張範囲 VLAN 1025 ～ 4094 を管理することはできません）。

（注） VTP バージョン 3 を使用して、VLAN 1006 ～ 4094 を管理できます。これらの VLAN は VTP バージョン 3 により伝播されます。

- FlexWAN モジュールおよびルーテッド ポートは、VLAN 1025 で始まる一定数の VLAN を独自に使用するため自動的に割り当てます。これらの装置を使用する場合は、必要数の VLAN を残しておく必要があります。

標準範囲 VLAN の作成

VLAN は一度に 1 つずつ作成することも、1 つのコマンドで一定範囲の VLAN を作成することもできます。一定範囲の VLAN を作成する場合、VLAN 名を指定することはできません。VLAN 名は一意でなければならないためです。

標準範囲 VLAN を作成するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	標準範囲のイーサネット VLAN を作成します。	**set vlan** *vlan* [**name** *name*] [**said** *said*] [**mtu** *mtu*] [**translation** *vlan*]
ステップ 2	VLAN の設定を確認します。	**show vlan** [*vlan*]

次に、スイッチが Per VLAN Spanning-Tree Plus（PVST+）モードのときに標準範囲 VLAN を作成し、設定を確認する例を示します。

```
Console> (enable) set vlan 500-520
Vlan 500 configuration successful
Vlan 501 configuration successful
Vlan 502 configuration successful
Vlan 503 configuration successful
 .
 .
 .
Vlan 520 configuration successful
Console> (enable) show vlan 500-520
VLAN Name                             Status    IfIndex Mod/Ports, Vlans
---- -------------------------------- --------- ------- ------------------------
500                                    active    342
501                                    active    343
502                                    active    344
503                                    active    345
 .
 .
 .
520                                    active    362
VLAN Type  SAID       MTU   Parent RingNo BrdgNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ ------ ---- -------- ------ ------
500  enet  100500     1500  -      -      -      -    -        0      0
501  enet  100501     1500  -      -      -      -    -        0      0
502  enet  100502     1500  -      -      -      -    -        0      0
503  enet  100503     1500  -      -      -      -    -        0      0
 .
 .
 .
520  enet  100520     1500  -      -      -      -    -        0      0
VLAN AREHops STEHops Backup CRF
---- ------- ------- ----------
Console> (enable)
```

標準範囲 VLAN の変更

既存の標準範囲 VLAN について VLAN パラメータを変更するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	既存の標準範囲 VLAN を変更します。	**set vlan** *vlan* [**name** *name*] [**state** {**active** | **suspend**}] [**said** *said*] [**mtu** *mtu*] [**translation** *vlan*]
ステップ 2	VLAN の設定を確認します。	**show vlan** [*vlan*]

スイッチ上での拡張範囲 VLAN の設定

ここでは、拡張範囲 VLAN 1025 ～ 4094 の設定手順について説明します。

拡張範囲 VLAN 設定時の注意事項

ここでは、拡張範囲 VLAN 1024 ～ 4094 作成の際の注意事項について説明します。

- 拡張範囲には、イーサネット タイプの VLAN しか作成できません。
- 拡張範囲 VLAN を使用するには、MAC（メディア アクセス制御）アドレス リダクションをイネーブルにする必要があります。
- 拡張範囲 VLAN の作成および削除は、CLI（コマンドライン インターフェイス）または SNMP（簡易ネットワーク管理プロトコル）を通じてのみ行えます。
- VTP を使用してこれらの VLAN を管理することはできません。これらの VLAN は、各スイッチ上でスタティックに設定する必要があります。

（注） VTP バージョン 3 を使用して、VLAN 1006 ～ 4094 を管理できます。これらの VLAN は VTP バージョン 3 により伝播されます。設定上の理由から、拡張範囲は VLAN 1025 ～ 4094 で構成されます。

- dot1q/isl マッピングを使用する場合は、拡張範囲 VLAN を使用できません。
- 拡張範囲 VLAN には、プライベート VLAN パラメータおよび RSPAN を設定できます。ただし、これ以外の拡張範囲 VLAN パラメータは、いずれもシステム デフォルトだけを使用します。
- スイッチは、内部的な使用のために、拡張範囲から VLAN のブロックを割り当てる場合があります。たとえば、スイッチは、ルーテッド ポートまたは FlexWAN モジュールに VLAN を割り当てる場合があります。VLAN のブロックは、常に VLAN 1006 を起点として割り当てられます。FlexWAN モジュールが必要とする範囲内にユーザが 1 つでも VLAN を作成すると、必要な VLAN がすべて割り当てられなくなります。ユーザの VLAN エリアから、VLAN が割り当てられることはないためです。

注意 FlexWAN モジュールおよびルーテッド ポートは、VLAN 1006 で始まる内部 VLAN の連続的なブロックを自動的に割り当てます。これらの装置を使用する場合は、装置用に必要数の VLAN を残しておく*必要があります*。FlexWAN モジュールに対して十分な VLAN がない場合、一部のポートが機能しない可能性があります。詳細については、『*Catalyst 6500 Series and Cisco 7600 Series Router FlexWAN Module Installation and Configuration Note*』を参照してください。

注意 同一スイッチ上で FlexWAN モジュールをあるスロットから別のスロットに移すと、FlexWAN モジュールはそれまで使用していた VLAN のブロックを削除せずに、新しい VLAN のブロックを割り当てます。FlexWAN モジュールを移動するときは、スイッチを再起動する必要があります。

拡張範囲 VLAN の作成

拡張範囲 VLAN を作成するには、まず MAC アドレス リダクションをイネーブルにして、拡張範囲 VLAN の ID を提供させる必要があります。MAC アドレス リダクションをイネーブルにした場合、拡張範囲 VLAN が存在するかぎり、ディセーブルにすることはできません。

（注） 拡張範囲 VLAN を使用する場合、システムに既存の 802.1Q/ISL（スイッチ間リンク）マッピングがあれば、そのマッピングを削除する必要があります。詳細については、「802.1Q/ISL VLAN マッピングの削除」（p.11-10）を参照してください。

（注） Release 8.1(1) 以降のソフトウェア リリースでは、拡張範囲 VLAN の名前を付けられます。この機能は、VTP のバージョンまたはモードに関係ありません。

MAC アドレス リダクションをイネーブルにし、拡張範囲にイーサネット VLAN を作成するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	MAC アドレス リダクションをイネーブルにします。	***set spantree macreduction*** {***enable*** | ***disable***}
ステップ 2	VLAN を作成します。	**set vlan** *vlan*
ステップ 3	VLAN の設定を確認します。	**show vlan** [*vlan*]

次に、MAC アドレス リダクションをイネーブルにし、拡張範囲のイーサネット VLAN を作成する例を示します。

```
Console> (enable) set spantree macreduction enable
MAC address reduction enabled
Console> (enable) set vlan 2000
Vlan 2000 configuration successful
Console> (enable) show vlan 2000
VLAN Name                             Status    IfIndex Mod/Ports, Vlans
---- -------------------------------- --------- ------- -------------------------
2000 VLAN2000                         active    61

VLAN Type  SAID       MTU   Parent RingNo BrdgNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ ------ ---- -------- ------ ------
2000 enet  102000     1500  -      -      -      -    -        0      0

VLAN Inst DynCreated  RSPAN
---- ---- ---------- --------
2000 -    static     disabled
Console> (enable)
```

次に、アクティブ、停止、および拡張 VLAN の要約を表示する例を示します。

```
Console> (enable) show vlan summary

Vlan status    Count  Vlans
-------------  -----------------------------------------------------
VTP Active       504   1-100,102-500,1000,1002-1005

VTP Suspended      1   101

Extended           1   2000
Console> (enable)
```

VLAN と VLAN のマッピング

（注）　ポート単位または ASIC（特定用途向け IC）単位で VLAN マッピングを設定するには、「ポート単位または ASIC 単位の VLAN マッピングの設定」（p.11-16）を参照してください。

（注）　Release 8.3(1) 以降のソフトウェア リリースでは、ISL トランクによって VLAN 範囲全体（1 ～ 4094）がサポートされるため、グローバル VLAN マッピング機能が不要です。

他社製の装置の VLAN に接続されている 802.1Q トランクから、Catalyst 6500 シリーズ スイッチ上の他の VLAN に接続されている ISL トランクに、VLAN をマッピングできます。

（注）　802.1Q VLAN を ISL VLAN にマッピングする場合、Catalyst 6500 シリーズの旧ソフトウェア リリースからのマッピングを保持できますが、拡張範囲 VLAN は使用できません。

ここでは、VLAN と VLAN をマッピングする手順について説明します。

- 802.1Q VLAN から ISL VLAN へのマッピング（p.11-9）
- 802.1Q/ISL VLAN マッピングの削除（p.11-10）

802.1Q VLAN から ISL VLAN へのマッピング

ネットワーク内の他社製の装置が、802.1Q トランクを通じて Catalyst 6500 シリーズ スイッチに接続されている可能性があります。

ユーザが設定する ISL VLAN の有効範囲は 1 ～ 1000（および 1002 ～ 1005）、1025 ～ 4094 です。IEEE 802.1Q 規格に指定されている VLAN の有効範囲は、0 ～ 4095 です。他社製の装置が 802.1Q トランクを通じてシスコ製スイッチに接続されているネットワーク環境では、1001 以上の 802.1Q VLAN 番号を ISL VLAN 番号にマッピングできます。拡張範囲（1025 ～ 4094）の VLAN を dot1q マッピングに使用する場合は、どの拡張範囲 VLAN もそれ以外の目的で使用することはできません。

1 ～ 1000 の範囲の 802.1Q VLAN は、対応する ISL VLAN に自動的にマッピングされます。シスコ製スイッチで認識し、転送するためには、1001 以上の 802.1Q VLAN 番号を ISL VLAN にマッピングする必要があります。

802.1Q VLAN と ISL VLAN のマッピングには、次の制限事項があります。

- グローバル VLAN マッピング機能およびポート単位 /ASIC 単位の VLAN マッピング機能（「ポート単位または ASIC 単位の VLAN マッピングの設定」[p.11-16] を参照）は相互に排他的であり、同時にイネーブルにできる機能は 1 つのみです。
- スイッチ上に拡張範囲 VLAN がある場合は、新しく 802.1Q VLAN を ISL VLAN にマッピングすることはできません。
- 1 台のスイッチに設定できる 802.1Q VLAN と ISL VLAN のマッピング数は、最大 8 個です。
- 802.1Q VLAN は、イーサネット タイプの ISL VLAN にしかマッピングできません。
- 802.1Q トランクのネイティブ VLAN は、マッピング テーブルに入力しないでください。

- 802.1Q VLAN を ISL VLAN にマッピングすると、マッピング後の ISL VLAN に対応する 802.1Q VLAN 上のトラフィックはブロックされます。たとえば、802.1Q VLAN 2000 を ISL VLAN 200 にマッピングした場合、802.1Q VLAN 200 のトラフィックはブロックされます。
- VLAN マッピングは、各スイッチにローカルに適用されます。ネットワーク内の該当するすべてのスイッチ上で、同じ VLAN マッピングを設定してください。

802.1Q VLAN を ISL VLAN にマッピングするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	802.1Q VLAN を ISL イーサネット VLAN にマッピングします。*dot1q_vlan* の有効範囲は、1001 ～ 4095 です。*isl_vlan* の有効範囲は、1 ～ 1000 です。	**set vlan mapping dot1q** *dot1q_vlan* **isl** *isl_vlan*
ステップ 2	VLAN マッピングを確認します。	**show vlan mapping**

次に、802.1Q VLAN 2000、3000、4000 を ISL VLAN 200、300、400 にマッピングし、設定を確認する例を示します。

```
Console> (enable) set vlan mapping dot1q 2000 isl 200
Vlan mapping successful
Console> (enable) set vlan mapping dot1q 3000 isl 300
Vlan mapping successful
Console> (enable) set vlan mapping dot1q 4000 isl 400
Vlan mapping successful
Console> (enable) show vlan mapping
802.1q vlan     ISL vlan        Effective
----------------------------------------
2000            200             true
3000            300             true
4000            400             true
Console> (enable)
```

802.1Q/ISL VLAN マッピングの削除

802.1Q/ISL VLAN マッピングを削除するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	802.1Q/ISL VLAN マッピングを削除します。	**clear vlan mapping dot1q** {*dot1q_vlan* | **all**}
ステップ 2	VLAN マッピングを確認します。	**show vlan mapping**

次に、802.1Q VLAN 2000 の VLAN マッピングを削除する例を示します。

```
Console> (enable) clear vlan mapping dot1q 2000
Vlan 2000 mapping entry deleted
Console> (enable)
```

次に、すべての 802.1Q/ISL VLAN マッピングを削除する例を示します。

```
Console> (enable) clear vlan mapping dot1q all
All vlan mapping entries deleted
Console> (enable)
```

内部 VLAN の割り当て

VLAN はユーザ VLAN または内部 VLAN のいずれかに分類されます。ユーザ VLAN は、ユーザが作成した 1 ～ 4049 の VLAN になります。内部 VLAN は、ソフトウェア機能が使用する VLAN で、動作するための専用 VLAN が必要です。内部 VLAN は、VLAN マネージャーが必要に応じて割り当てます（VLAN 1006 ～ 4094 を使用）。内部 VLAN の割り当ては VLAN 1006 を起点として、昇順で行われます。ユーザ VLAN と内部 VLAN の競合を回避するために、ユーザ VLAN はできるだけ VLAN 4094 の近くに割り当てる必要があります。

（注） 使用可能な VLAN の数は固定されているので、ユーザ VLAN を割り当てたあとに、十分な数の VLAN が内部 VLAN の割り当て用に残されていることを確認してください。

VLAN へのスイッチ ポートの割り当て

管理ドメイン内で作成された VLAN は、1 つまたは複数のスイッチ ポートが VLAN に割り当てられないかぎり、未使用の状態です。新しい VLAN を作成してから、モジュールとポートを指定することも、また VLAN の作成とモジュールおよびポートの指定を一度に行うこともできます。

（注） スイッチ ポートは必ず、適切なタイプの VLAN に割り当ててください。たとえば、イーサネット タイプの VLAN には、イーサネット、ファスト イーサネット、およびギガビット イーサネット ポートを割り当てます。

1 つまたは複数のスイッチ ポートを VLAN に割り当てるには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	VLAN に 1 つまたは複数のスイッチ ポートを割り当てます。	**set vlan** *vlan mod/port*
ステップ 2	ポートの VLAN メンバーシップを確認します。	**show vlan** [*vlan*] **show port** [*mod*[*/port*]]

次に、VLAN にスイッチ ポートを割り当て、設定を確認する例を示します。

```
Console> (enable) set vlan 560 4/10
VLAN 560 modified.
VLAN 1 modified.
VLAN  Mod/Ports
---- ------------------------
560   4/10

Console> (enable) show vlan 560
VLAN Name                             Status    IfIndex Mod/Ports, Vlans
---- -------------------------------- --------- ------- ------------------------
560  Engineering                      active    348     4/10
VLAN Type  SAID       MTU   Parent RingNo BrdgNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ ------ ---- -------- ------ ------
560  enet  100560     1500  -      -      -      -    -        0      0
VLAN AREHops STEHops Backup CRF
---- ------- ------- ----------
Console> (enable) show port 4/10
Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
4/10                     connected  560        a-half a-100 10/100BaseTX

Port  AuxiliaryVlan AuxVlan-Status
----- ------------- --------------
 4/10  none          none

.
.
.

Last-Time-Cleared
--------------------------
Tue Jun 6 2000, 16:45:18
Console> (enable)
```

VLAN ポート プロビジョニング検証のイネーブル化またはディセーブル化

VLAN ポート プロビジョニング検証がイネーブルの場合は、スイッチ ポートを VLAN に割り当てる際、VLAN 番号に*加えて*、VLAN 名を指定する必要があります。VLAN 名と VLAN 番号の両方を指定する必要があるため、この検証機能は、ポートを不注意で誤った VLAN に配置しないように保証するのに役立ちます。

この機能がイネーブルの場合、**set vlan** *vlan mod/port* コマンドを入力すれば新しい VLAN を作成できますが、VLAN 番号と VLAN 名の両方を指定せずにポートをその VLAN に追加することはできません。この機能は、SNMP、ダイナミック VLAN、802.1x といった他の機能を使用した VLAN へのポート割り当てには影響しません。VLAN ポート プロビジョニング検証機能は、デフォルトではディセーブルです。

VLAN ポート プロビジョニング検証をイネーブルまたはディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	VLAN ポート プロビジョニング検証をイネーブルまたはディセーブルにします。	**set vlan verify-port-provisioning** {**enable** | **disable**}
ステップ 2	VLAN ポート プロビジョニング検証のステータスを確認します。	**show vlan verify-port-provisioning**

次に、VLAN ポート プロビジョニング検証をイネーブルにする例を示します。

```
Console> (enable) set vlan verify-port-provisioning enable
vlan verify-port-provisioning feature enabled
Console> (enable)
```

次に、VLAN ポート プロビジョニング検証のステータスを確認する例を示します。

```
Console> (enable) show vlan verify-port-provisioning
Vlan Verify Port Provisioning feature enabled
Console> (enable)
```

次に、（VLAN ポート プロビジョニング検証をイネーブルにして）VLAN 150 を作成し、ポート 3/16 を追加する例を示します。

```
Console> (enable) set vlan 150 3/16
Vlan 150 configuration successful
VLAN 150 modified.
VLAN 1 modified.
VLAN  Mod/Ports
---- ------------------------
150   3/16
Console> (enable)
```

次に、VLAN ポート プロビジョニング検証をイネーブルにして、ポート 3/17 を VLAN 150 に追加しようとした場合の出力例を示します。

```
Console> (enable) set vlan 150 3/17
Port Provisioning Verification is enabled on the switch.
To move port(s) into the VLAN, use 'set vlan <vlan> <port> <vlan_name>' command.
Console> (enable)
```

次に、VLAN ポート プロビジョニング検証をイネーブルにして、ポート 3/17 を VLAN 150 に追加する例を示します。

```
Console> (enable) set vlan 150 name Eng
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 150 configuration successful
Console> (enable)

Console> (enable) set vlan 150 3/17 Eng
VLAN 150 modified.
VLAN 1 modified.
VLAN  Mod/Ports
---- ----------------------
150   3/16-17
Console> (enable)
```

VLAN の削除

ここでは、VLAN を削除する場合の注意事項について説明します。

- VTP サーバ モードで標準範囲イーサネット VLAN を削除すると、VTP ドメインのすべてのスイッチからその VLAN が削除されます。
- VTP トランスペアレント モードで標準範囲 VLAN を削除すると、現在のスイッチ上に限って VLAN が削除されます。
- 拡張範囲 VLAN は、その VLAN を作成したスイッチ上でしか削除できません。
- デフォルト VLAN は削除できません。
- トークンリング TrBRF VLAN を削除する場合は、最初に子 TrCRF を別の親 TrBRF に割り当てるか、または子 TrCRF を削除する必要があります。

注意　VLAN を削除すると、その VLAN に割り当てられていたすべてのポートが非アクティブになります。これらのポートは、新しい VLAN に割り当てられるまで、元の VLAN に対応付けられています（つまり、非アクティブのままです）。

単一の VLAN を削除することも、一定範囲の VLAN を削除することもできます。スイッチ上の VLAN を削除するには、イネーブル モードで次のコマンドを入力します。

作業	コマンド
VLAN を削除します。	**clear vlan** *vlan*

次に、VLAN を削除する例を示します（この場合、スイッチは VTP サーバです）。

```
Console> (enable) clear vlan 500
This command will deactivate all ports on vlan(s) 500
Do you want to continue(y/n) [n]?y
Vlan 500 deleted
Console> (enable)

This command will deactivate all ports on vlan(s) 10
All ports on normal range vlan(s) 10
will be deactivated in the entire management domain.
Do you want to continue(y/n) [n]?
```

ポート単位または ASIC 単位の VLAN マッピングの設定

ここでは、ポート単位または ASIC 単位で VLAN マッピングを設定する方法について説明します。

VLAN マッピングの概要

Release 8.4(1) 以降のソフトウェア リリースでは、VLAN 範囲を制限しなくても、*任意*の VLAN タイプをその他の VLAN タイプにマッピングできるように、VLAN マッピングが拡張されています。現在、VLAN マッピングはポート単位または ASIC 単位で設定できます。

（注） Release 8.4(1) より前のソフトウェア リリースでは、VLAN マッピングはグローバルに設定されました。詳細については、「VLAN と VLAN のマッピング」（p.11-9）を参照してください。

設定時の注意事項および制限事項

ここでは、VLAN マッピングを設定する際の設定時の注意事項と制限事項を説明します。

- VLAN マッピングを使用した場合、スイッチング モジュールまたはスーパバイザ エンジンに搭載された ASIC タイプに応じて、次のようになります（各モジュール ASIC の仕様については、表 11-2 を参照）。
  - VLAN マッピングがサポートされない
  - ポート単位 VLAN マッピングがサポートされる
  - ASIC 単位 VLAN マッピングがサポートされるが、VLAN マッピングをポート単位でイネーブルまたはディセーブルにすることはできない
  - ASIC 単位 VLAN マッピングがサポートされ、VLAN マッピングをポート単位でイネーブルまたはディセーブルにすることができる。
- モジュールがポート単位 VLAN マッピングをサポートしないで、ASIC 単位 VLAN マッピングのみをサポートしている場合、VLAN マッピングは ASIC 内のすべてのポートに適用されます。ASIC 内の任意のポートのマッピングを変更すると、変更がこの ASIC 内のすべてのポートに適用されます。
- グローバル VLAN マッピング

  グローバル VLAN マッピング機能（「VLAN と VLAN のマッピング」[p.11-9] を参照）およびポート単位 /ASIC 単位 VLAN マッピング機能は相互に排他的であり、同時にイネーブルにできる機能は 1 つのみです。

  任意の VLAN にグローバル VLAN マッピングが設定されている場合に、ポート単位 /ASIC 単位 VLAN マッピングを設定しようとすると、コマンドは拒否され、エラー メッセージが表示されます。逆に、任意の VLAN にポート単位 /ASIC 単位マッピングが設定されている場合に、グローバル VLAN マッピングを設定しようとすると、コマンドは拒否され、エラー メッセージが表示されます。

  グローバル VLAN マッピングは、最大 8 つの VLAN をサポートします。VLAN X が VLAN Y にマッピングされている場合、VLAN Y は内部で廃棄済み VLAN にマッピングされます。ポート単位 /ASIC 単位 VLAN マッピングはこの方法では機能しません。VLAN X が VLAN Y にマッピングされている場合、VLAN Y の特定のポートに内部でスイッチングされるすべてのトラフィックは VLAN X にマッピングされます。

- VLAN マッピングは両方の方向に適用されます。たとえば、ポート P に VLAN x から VLAN y へのマッピングが設定されている場合、VLAN X のポート P で受信されたすべてのトラフィックは VLAN Y にマッピングされ、そこで処理されます。VLAN Y が内部的にタグ付けされたトラフィックのうち、ポート P から送信されたものにはすべて、VLAN X がタグ付けされます。
- EtherChannel

  VLAN マッピングは、PAgP と LACP の両方の EtherChannel でサポートされます。EtherChannel の特定のポートで VLAN マッピングをイネーブルまたはディセーブルにすると、EtherChannel 内のすべてのポートでこの機能がイネーブルまたはディセーブルになります。同様に、EtherChannel の特定のポートに VLAN マッピングを設定すると、EtherChannel 内のすべてのポートにこのマッピングが適用されます。

  EtherChannel 内のすべてのポートで、VLAN マッピングに関するポート ASIC 機能を同じに設定する必要があります。ポート ASIC 機能が異なるポートが存在する EtherChannel に VLAN マッピングを設定しようとしても、コマンドは拒否されます。
- SPAN および RSPAN

  ポート単位 VLAN マッピングがポート上でイネーブルの場合、ポート ASIC は変換元 VLAN を変換先 VLAN に変換します。すべての SPAN（スイッチド ポート アナライザ）設定は、変換先 VLAN で機能します。

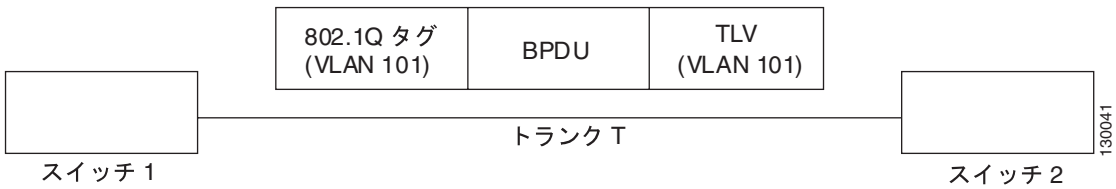
  RSPAN VLAN は変換できません。どの VLAN にも RSPAN VLAN をマッピングしないように設定する必要があります。同様に、変換先 VLAN を RSPAN VLAN として使用することはできません。
- スパニングツリー

  PVST+ が実装されている場合、スパニングツリー Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）には各トランク ポートの「VLAN ID」の TLV がタグ付けされています。この TLV は、ポート VLAN ID の一貫性を判別する際に役立ちます。PVST+ および Rapid-PVST+ では、この VLAN ID はスパニングツリー インスタンス番号（VLAN ID）と同じです。

  Shared Spanning Tree Protocol（SSTP）が有効な場合は、ポート単位 /ASIC 単位 VLAN マッピングがポート上でイネーブルになっている際に注意する必要があります。たとえば、図 11-2 のスイッチ 1 およびスイッチ 2 は、VLAN 101 を伝送するトランク T を使用して接続されています。スイッチ 2 のトランク ポート P では、ポート単位 /ASIC 単位 VLAN マッピングがイネーブルであり、VLAN 101 から VLAN 202 へのマッピングが存在します。図 11-2 に示すように、トランク リンクの BPDU には、VLAN 101 として 802.1Q VLAN および TLV VLAN が設定されています。この BPDU がポート P に到達すると、このマッピングにより 802.1Q VLAN は VLAN 202 に変更されますが、TLV VLAN は VLAN 101 のままです。BPDU がスパニングツリー プロセスに到達すると、スパニングツリーは VLAN 101 BPDU が VLAN 202 に着信したと結論し、一貫性がないと判断して、このポートを矛盾ポートとして報告します。

  この問題を解決するために、スパニングツリーはこの BPDU を VLAN 202 内で処理します。TLV VLAN は変換先 VLAN にマップされ、一貫性があるかチェックされます。この処理が発生した場合、スイッチ 1 のスパニングツリー インスタンス 101 はスイッチ 2 のスパニングツリー 202 とマージされます。このプロセスは、送信側でも実行されます。

図 11-2　VLAN マッピングおよびスパニングツリーの概要



ヒント　スパニングツリー　トポロジーを設計する前に、VLAN　のマージ方法を考慮する必要があります。VLAN マッピングがイネーブル化されたポートから変換元 VLAN を消去し、近接側から変換先 VLAN を消去する必要があります。このようにすると、カスタマー ポートの変換元 VLAN およびプロバイダー ポートの変換先 VLAN がマージされます。

表 11-2　モジュール単位のポート ASIC VLAN マッピング機能

モジュール	サポートされているポート単位 VLAN マッピングの最大数	機能 / 制限
WS-X6548-RJ-45 WS-X6548-RJ-21 WS-X6148X2-RJ-45 WS-X6148X2-45AF WS-X6196-RJ-21[1]	32	ASIC 単位 VLAN のマッピング。マッピングは ISL トランクのポート単位でイネーブルまたはディセーブルにできます。802.1Q トランクでは、常にマッピングが有効です。ディセーブルにすることはできません。マッピングは ISL および 802.1Q トランクに対してサポートされています。
WS-X6K-S2U-MSFC2 WS-X6K-S2-MSFC2 WS-X6K-S2-PFC2 WS-SUP720-3B WS-SUP720-3BXL WS-SUP720 WS-X6516A-GBIC[2] WS-X6516-GE-TX	32	ASIC 単位 VLAN のマッピング。マッピングは ASIC のポート単位でイネーブルまたはディセーブルにできます。任意の VLAN タイプ間の変換がサポートされています。802.1Q トランクでのみサポートされています。[3]
WS-X6748-SFP[4] WS-X6724-SFP WS-X6748-GE-TX	128	ASIC 単位 VLAN のマッピング。マッピングは ASIC のポート単位でイネーブルまたはディセーブルにできます。任意の VLAN タイプ間の変換がサポートされています。マッピングは ISL および 802.1Q トランクに対してサポートされています。
WS-X6148A-GE-TX WS-X6148A-GE-45A WS-X6148-FE-SFP WS-X6148A-RJ-45 WS-X6148A-45AF WS-X6704-10GE[5]	8	ポート単位 VLAN マッピング。任意の VLAN タイプ間の変換がサポートされています。マッピングは ISL および 802.1Q トランクに対してサポートされています。
WS-X6502-10GE	16	ポート単位 VLAN マッピング。任意の VLAN タイプ間の変換がサポートされています。802.1Q トランクでのみサポートされています。
WS-SUP32-GE-3B	16	ポート単位 VLAN マッピング。任意の VLAN タイプ間の変換がサポートされています。マッピングは ISL および 802.1Q トランクに対してサポートされています。

1. WS-X6196-RJ-21 には ASIC 単位 VLAN マッピング機能がありません。VLAN マッピングの単位は 2 つの ASIC のポート 1 ～ 96 です（各 ASIC の 48 個のポートのみではありません）。
2. WS-X6516A-GBIC には ASIC 単位 VLAN マッピング機能がありません。VLAN マッピングの単位は 2 つの ASIC のポート 1 ～ 8 およびポート 9 ～ 16 です（各 ASIC の 4 個のポートのみではありません）。
3. これらのモジュールの ASIC には、次の制限があります。dot1q-all-tagged がディセーブルの場合、ネイティブ VLAN で送信されたパケットには、VLAN 変換が発生しません。
4. WS-X6748-SFP には ASIC 単位 VLAN マッピング機能がありません。VLAN マッピングの単位は 2 つの ASIC のポート 1 ～ 24 および 25 です（各 ASIC の 12 個のポートのみではありません）。
5. WS-X6704-10GE：マッピングは ASIC のポート単位でイネーブルまたはディセーブルにできます。128 のポート単位 VLAN マッピングがサポートされています。

ポート単位 VLAN マッピングのイネーブル化またはディセーブル化

(注) **set port vlan-mapping** コマンドを使用してポート単位で VLAN マッピングを設定する前に、**set port vlan-mapping** *mod/port* **enable** コマンドを入力して、ポート VLAN マッピングをイネーブルにする必要があります。

set port vlan-mapping *mod/port* {**enable** | **disable**} コマンドを入力して、ポート単位で VLAN マッピングをイネーブルまたはディセーブルにします。VLAN 変換が発生するのは、VLAN マッピングがイネーブル化されていて、ポートがトランキングの場合のみです。ASIC 単位の VLAN マッピングのみをサポートする ASIC に関して、ポート単位で VLAN マッピングをイネーブルまたはディセーブルにする機能が有効な場合、このコマンドはポート設定にのみ適用され、ASIC には適用されません。VLAN マッピングをディセーブルにした場合も、マッピングは保護されます。VLAN マッピングはデフォルトでディセーブルです。

ポート単位で VLAN マッピングをイネーブルまたはディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポート単位で VLAN マッピングをイネーブルまたはディセーブルにします。	**set port vlan-mapping** *mod/port* {**enable** | **disable**}
ステップ 2	VLAN マッピング設定を表示します。	**show port vlan-mapping** [*mod* | *mod/port*]

次に、ポート単位で VLAN マッピングをイネーブルにする例を示します。

```
Console>(enable) set port vlan-mapping 7/1 enable
VLAN mapping enabled on port 7/1.
Console>(enable)
```

ポート単位の VLAN マッピングの設定

(注) **set port vlan-mapping** コマンドを使用する前に、**set port vlan-mapping** *mod/port* **enable** コマンドを入力して、ポート VLAN マッピングをイネーブルにする必要があります。

(注) 変換元 VLAN はトランク VLAN（スイッチ外部）、変換先 VLAN はスイッチ内部の VLAN です。

set port vlan-mapping *mod/port source-vlan-id translated-vlan-id* コマンドを入力して、ポート単位で VLAN　マッピングを設定します。このコマンドにより、*source-vlan-id*　のトラフィックは *translated-vlan-id* に変換されます。内部的に *translated-vlan-id* がタグ付けされたすべてのトラフィックは、*source-vlan-id* がタグ付けされたあとに、ポートから送信されます。VLAN 変換が発生するのは、ポートがトランキングの場合のみです。このコマンドは、すべての範囲のポートを対象とします。

ポート単位で VLAN マッピングを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポート VLAN マッピングをイネーブルにします。	**set port vlan-mapping** *mod/port* {**enable** | **disable**}
ステップ 2	ポート単位で VLAN マッピングを設定します。	**set port vlan-mapping** *mod/port source-vlan-id translated-vlan-id*
ステップ 3	VLAN マッピング設定を表示します。	**show port vlan-mapping** [*mod* | *mod/port*]

次に、ポート VLAN マッピングをイネーブルにし、ポート単位で VLAN マッピングを設定する例を示します。この例では、モジュール 7 は 48 ポート 10/100/1000 スイッチング モジュール（WS-X6748-GE-TX）です。このモジュールは、ASIC 単位 VLAN マッピングをサポートします。1 つの ASIC で 12 個のポートをサポートします。

```
Console>(enable) set port vlan-mapping 7/1 enable
VLAN mapping enabled on port 7/1.
Console>(enable) set port vlan-mapping 7/1 2002 3003
VLAN 2002 mapped to VLAN 3003 on ports 7.1. 7/1-12.
Console>(enable) show port vlan-mapping 7/1
Mod/Port Source VLAN Translated VLAN State       Max Allowed (Current) Entries
-------- ----------- --------------- ----------- ----------------------------
7/1      2002        3003            Enabled     128 (1)
Console>(enable)
```

次の例のモジュール 5 は、1 ポート 10GBASE-E シリアル 10 ギガビット イーサネット モジュール（WS-X6502-10GE）です。このモジュールはポート単位 VLAN マッピングをサポートします。

```
Console>(enable) set port vlan-mapping 5/1 2002 3003
VLAN 2002 mapped to VLAN 3003 on port 5/1.
Console>(enable)
```

この例では、モジュール 7 は 48 ポート 10/100/1000 スイッチング モジュール（WS-X6748-GE-TX）です。このモジュールは、ASIC 単位 VLAN マッピングをサポートします。1 つの ASIC で 12 個のポートをサポートします。この例では、ポート 7/1 ～ 4 が EtherChannel に属しています。

```
Console>(enable) set port vlan-mapping 7/1 2002 3003
VLAN 2002 mapped to VLAN 3003 on ports 7/1-12.
Console>(enable)
```

この例では、モジュール 7 およびモジュール 8 は 48 ポート 10/100/1000 スイッチング モジュール（WS-X6748-GE-TX）です。これらのモジュールは、ASIC 単位 VLAN マッピングをサポートします。1 つの ASIC で 12 個のポートをサポートします。この例では、ポート 7/1 ～ 4 および 8/1 ～ 4 が EtherChannel に属しています。

```
Console>(enable) set port vlan-mapping 7/1 2002 3003
VLAN 2002 mapped to VLAN 3003 on ports 7/1-12,8/1-12.
Console>(enable)
```

VLAN マッピングの消去

ポート単位で、すべてのポートで、または特定の変換元 VLAN ID に関して VLAN マッピングを消去するには、**clear port vlan-mapping** コマンドを入力します。一部のモジュールでは、VLAN マッピングは ASIC 単位でサポートされ、ポート単位のマッピングは保存されません。これらのモジュールに **clear port vlan-mapping** *mod/port* コマンドを入力すると、ASIC のすべてのポート上の VLAN マッピングが消去されます。*source_vlan_id* 引数を入力すると、指定されたポートまたは ASIC（ASIC ベース ポートの場合）の VLAN マッピング テーブルから、該当する変換元 VLAN の VLAN マッピングのみが消去されます。

VLAN マッピングを消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
VLAN マッピングを消去します。	**clear port vlan-mapping** *mod/port* **all** **clear port vlan-mapping** *mod/port* [*source-vlan-id*] **clear port vlan-mapping all**

次に、ポート 7/1 から VLAN マッピングを消去する例を示します。

```
Console>(enable) clear port vlan-mapping 7/1 2002
VLAN mapping for VLAN 2002 removed from port 7/1-12.
Console>(enable)
```

VLAN マッピング情報の表示

VLAN マッピング情報を表示するには、**show port vlan-mapping** [*mod* | *mod/port*] コマンドを入力します。

VLAN マッピング情報を表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
VLAN マッピング情報を表示します。	**show port vlan-mapping** [*mod*	*mod/port*]

次に、ポート 7/1 の VLAN マッピング情報を表示する例を示します。

```
Console>(enable) show port vlan-mapping 7/1
Mod/Port Source VLAN Translated VLAN State       Max Allowed (Current) Entries
-------- ----------- --------------- ----------- ------------------------------
7/1      2002        3003            Enabled     128 (1)
Console>(enable)
```

（注） ポートごとにマッピング タイプを表示するには、**show port capabilities** [*mod* | *mod/port*] コマンドを入力します。このコマンドは、ポートごとに許可されている最大マッピング数も表示します。

スイッチ上でのプライベート VLAN の設定

ここでは、プライベート VLAN の機能概要について説明します。

プライベート VLAN の機能概要

プライベート VLAN は、Catalyst 6500 シリーズ スイッチ上の同一プライベート VLAN 内でポート間のレイヤ 2 の隔離を行います。プライベート VLAN に所属するポートは、そのプライベート VLAN 構造を作成する共通のサポート VLAN の集合に対応付けられます。

プライベート VLAN ポートには、次の 3 種類があります。

- 混合 ― 他のすべてのプライベート VLAN ポートと通信し、ルータ、LocalDirector、バックアップ サーバ、および管理ワークステーションとの通信に使用するポートです。

（注） ブロードキャストまたはマルチキャスト パケットが混合ポートに着信すると、そのパケットはプライベート VLAN ドメイン内のすべてのポートに、つまりすべてのコミュニティ ポートおよび隔離ポートに送信されます。

- 隔離 ― 同一プライベート VLAN 内の混合ポート以外のポートから、レイヤ 2 上で完全に隔離されたポートです。
- コミュニティ ― コミュニティ ポート間で通信するだけではなく、自身の混合ポートとも通信します。この種のポートは、同一プライベート VLAN の他のコミュニティに属するポートまたは隔離ポートから、レイヤ 2 で隔離されています。

発信トラフィックをすべての隔離ポートにブロックすることにより、レイヤ 2 上でプライバシが確保されます。すべての隔離ポートは特定の隔離 VLAN に割り当てられており、その VLAN でこのハードウェア機能が実行されます。隔離ポートから受信したトラフィックは、混合ポートだけに転送されます。

プライベート VLAN は、次の 4 つに分類されます。単一プライマリ VLAN、単一隔離 VLAN、および一連のコミュニティ、または双方向コミュニティ VLAN です。

プライベート VLAN を設定するには、まずプライベート VLAN 内の各サポート VLAN を定義する必要があります。

- プライマリ VLAN ― 混合ポートからの着信トラフィックを、他のすべての混合ポート、隔離ポート、コミュニティ ポート、および双方向コミュニティ ポートに送信します。
- 隔離 VLAN ― 隔離ポートが、混合ポートと通信するために使用します。隔離されたポートからのトラフィックは、所属するプライベート VLAN 内のすべての隣接ポートでブロックされ、受信できるのは混合ポートだけになります。
- コミュニティ VLAN ― コミュニティ ポート間の通信を行い、指定の混合ポートを介してプライベート VLAN 外部にトラフィックを送信するためにコミュニティ ポートのグループが使用する単一方向 VLAN。

- 双方向コミュニティ VLAN ― コミュニティ ポート間、コミュニティ ポートと Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）間の通信に、コミュニティ ポートのグループが使用する双方向 VLAN。

（注） Release 6.2(1) 以降のソフトウェア リリースでは、トラフィックが MSFC 混合ポートを通ってプライベート VLAN の境界を越えるとき、双方向コミュニティ VLAN を使用してプライマリ VLAN からセカンダリ VLAN への逆マッピングを実行できます。発信トラフィックと着信トラフィックの両方を同一 VLAN で伝送できるので、VLAN Access Control List（VACL）などの VLAN をベースにした機能をコミュニティ（または顧客）単位で両方向に適用できます。

プライベート VLAN を作成するには、標準 VLAN 範囲の標準 VLAN を複数割り当てます。そのうち 1 つの VLAN をプライマリ VLAN、もう 1 つの VLAN を隔離 VLAN、コミュニティ VLAN、または双方向コミュニティ VLAN として指定します。必要に応じて、それ以外の VLAN をこのプライベート VLAN でそれぞれ隔離 VLAN、コミュニティ VLAN、または双方向コミュニティ VLAN として指定することもできます。VLAN を指定したあとは、それらの VLAN を一括してバインドし、混合ポートに対応付ける必要があります。

プライベート VLAN をサポートする他のスイッチにプライマリ VLAN、隔離 VLAN、コミュニティ VLAN、または双方向コミュニティ VLAN をトランキングすることにより、プライベート VLAN を複数のイーサネット スイッチに拡張できます。

イーサネット スイッチド環境では、個々の VLAN および対応する IP サブネットを、個々のステーションまたはステーションの共通のグループに割り当てることができます。サーバはデフォルト ゲートウェイと通信する能力さえあれば、その VLAN 自身の外部にあるエンド ポイントにアクセスできます。これらのステーションを、その所有権とは無関係に、1 つのプライベート VLAN にまとめることにより、次のような利点があります。

- サーバ ポートを隔離ポートとして指定することにより、レイヤ 2 でのサーバ間通信を防止できます。
- デフォルト ゲートウェイ、バックアップ サーバ、または LocalDirector が接続されたポートを混合ポートとして指定することにより、すべてのステーションがこれらのゲートウェイにアクセス可能になります。
- VLAN の消費が低減します。すべてのステーションが同一のプライベート VLAN に存在するので、ステーションのグループ全体に 1 つの IP サブネットを割り当てるだけで済みます。

MSFC ポートまたは非トランクの混合ポートでは、必要に応じて隔離 VLAN またはコミュニティ VLAN をいくつでも再マッピングすることができます。ただし、非トランクの混合ポートが再マッピングできるのは 1 つのプライマリ VLAN だけであり、MSFC ポートが接続できるのは MSFC ルータだけです。非トランク混合ポートを使用すると、プライベート VLAN への「アクセス ポイント」としてさまざまな装置に接続できます。たとえば、非トランクの混合ポートを LocalDirector の「サーバ ポート」に接続して、多くの隔離 VLAN またはコミュニティ VLAN をそのサーバ VLAN に再マッピングすると、LocalDirector によって隔離 VLAN またはコミュニティ VLAN 内に存在するサーバの負荷を分散させることができます。また、管理ワークステーションからすべてのプライベート VLAN のサーバをモニタしたりバックアップしたりする目的で、非トランクの混合ポートを使用することも可能です。

（注） 双方向コミュニティ VLAN は、MSFC 混合ポート上にしかマッピングできません（非トランクまたはその他のタイプの混合ポート上にはマッピングできません）。

プライベート VLAN 設定時の注意事項

ここでは、プライベート VLAN 設定時の注意事項について説明します。

(注)　ここでは、*コミュニティ VLAN* という用語は、特に明記しないかぎり、単一方向コミュニティ VLAN と双方向コミュニティ VLAN の両方を表す総称として使用しています。

(注)　VLAN ポート プロビジョニング検証がイネーブルの場合は、スイッチ ポートをプライマリおよびセカンダリ VLAN に割り当てる際、VLAN 番号に*加えて*、VLAN 名を指定する必要があります。詳細は、「VLAN ポート プロビジョニング検証のイネーブル化またはディセーブル化」（p.11-13）を参照してください。

- 1 つの VLAN をプライマリ VLAN として指定してください。
- 任意で 1 つの VLAN を隔離 VLAN として指定することができますが、使用できる隔離 VLAN は 1 つだけです。
- 任意でプライベート VLAN コミュニティを使用できますが、コミュニティごとに 1 つずつコミュニティ VLAN を指定する必要があります。
- 隔離 VLAN およびコミュニティ VLAN、またはそのどちらかの VLAN をプライマリ VLAN にバインドし、隔離ポートまたはコミュニティ ポートを割り当ててください。その結果、次のようになります。
  - 隔離 VLAN およびコミュニティ VLAN のスパニングツリー特性は、それぞれのプライマリ VLAN の特性に設定されます。
  - VLAN メンバーシップは、スタティックになります。
  - アクセス ポートは、ホスト ポートになります。
  - BPDU ガード機能がアクティブになります。
- 隔離 VLAN およびコミュニティ VLAN を混合ポート上のプライマリ VLAN にマッピングする VLAN 自動変換を設定してください。非トランク ポートまたは MFSC ポートを混合ポートとして設定します。
- VTP をトランスペアレント モードに設定する必要があります。

  (注)　この制限は VTP バージョン 3 では当てはまりません。

- プライベート VLAN を設定したあとで、VTP モードをクライアントまたはサーバ モードに変更することはできません。VTP はプライベート VLAN タイプおよびマッピングの伝播をサポートしないからです。
- VLAN をプライマリ VLAN、隔離 VLAN、またはコミュニティ VLAN として設定できるのは、現在その VLAN にアクセス ポートがまったく割り当てられていない場合に限られます。VLAN にアクセス ポートが割り当てられていないことを確認するには、**show port** コマンドを使用します。
- プライマリ VLAN に対応付けることができるのは、1 つの隔離 VLAN または複数のコミュニティ、あるいはその両方です。
- 隔離 VLAN またはコミュニティ VLAN に対応付けられるのは、1 つのプライマリ VLAN だけです。
- プライベート VLAN は、VLAN 2 ～ 1000、および 1025 ～ 4096 を使用できます。

- プライマリ VLAN またはセカンダリ VLAN のどちらかを削除すると、その VLAN に対応付けられたポートが非アクティブになります。
- プライベート VLAN を設定するとき、次に説明するハードウェアとソフトウェアの相互作用について考慮してください。
  - プライベート VLAN では、帯域内ポート（sc0）は使用できません。

  （注）　Release 6.3(1) 以降のソフトウェア リリースでは、sc0 ポートはプライベート VLAN ポートとして設定できますが、sc0 ポートを混合ポートとして設定することはできません。

  - プライベート VLAN ポートをトランキングまたはチャネリング モードに設定したり、ダイナミック VLAN メンバーシップを持たせたりすることはできません。ただし例外として、MSFC ポートでは常にトンランキングがアクティブです。
  - 同じ ASIC に属するポートを、1 つのポートがトランキング モード、混合モード、または SPAN 宛先、もう 1 つのポートが表 11-3 に示すモジュール用の隔離ポートまたはコミュニティ ポートになるように設定することはできません。

  このような設定を試みると、警告メッセージが表示され、コマンドが拒否されます。

表 11-3　モジュールとポートの対応（ASIC グループ別）

モジュール番号	説明	ポート（ASIC 別）
WS-X6224-100FX-MT	24 ポート 100BASE-FX マルチモード、MT-RJ	ポート 1 ～ 12 ポート 13 ～ 24
WS-X6324-100FX-SM WS-X6324-100FX-MM	24 ポート 100BASE-FX シングル モードまたはマルチモード、MT-RJ	ポート 1 ～ 12 ポート 13 ～ 24
WS-X6024-10FL-MT	24 ポート 10BASE-FL、MT-RJ	ポート 1 ～ 12 ポート 13 ～ 24
WS-X6248-TEL WS-X6248A-TEL WS-X6348-RJ-21(V) WS-X6148-RJ-21(V) WS-X6148-21AF	48 ポート 10/100BASE-TX、RJ-21	ポート 1 ～ 12 ポート 13 ～ 24 ポート 25 ～ 36 ポート 37 ～ 48
WS-X6348-RJ-45 WS-X6348-RJ-45(V) WS-X6248-RJ-45 WS-X6248A-RJ-45 WS-X6148-RJ-45(V) WS-X6148-45AF	48 ポート 10/100BASE-TX、RJ-45	ポート 1 ～ 12 ポート 13 ～ 24 ポート 25 ～ 36 ポート 37 ～ 48
WS-X6148-GE-TX WS-X6148V-GE-TX WS-X6148-GE-45AF WS-X6548-GE-TX WS-X6548V-GE-TX WS-X6548-GE-45AF	48 ポート 10/100/1000BASE-TX、RJ-45	ポート 1 ～ 8 ポート 9 ～ 16 ポート 17 ～ 24 ポート 25 ～ 32 ポート 33 ～ 40 ポート 41 ～ 48

- 隔離ポートおよびコミュニティ ポートは、設定ミスに起因するスパニングツリー ループを防ぐため、BPDU ガード機能を実行する必要があります。
- プライマリ VLAN および対応する隔離 VLAN とコミュニティ VLAN は、スパニングツリーの設定が同じでなければなりません。この設定は、関連するプライマリ VLAN、隔離 VLAN、およびコミュニティ VLAN の間で一貫したスパニングツリー トポロジーを維持し、接続切断を防ぎます。設定されたプライオリティおよび各種パラメータは、プライマリ VLAN から隔離 VLAN およびコミュニティ VLAN に自動的に伝播されます。
- 次のように MISTP モードで動作するプライベート VLAN を作成できます。
  - MISTP をディセーブルにすると、対応するすべての隔離 VLAN およびコミュニティ VLAN にプライマリ VLAN の設定変更が伝播されます。隔離 VLAN またはコミュニティ VLAN を変更することはできません。
  - MISTP をイネーブルにする場合、MISTP インスタンスを設定できるのはプライマリ VLAN だけです。プライマリ VLAN に適用された変更は、隔離 VLAN およびコミュニティ VLAN に伝播されます。
- ネットワークで MAC アドレス リダクションを使用しているスイッチと使用していないスイッチが混在している場合、STP パラメータは必ずしも伝播されず、スパニングツリー トポロジーが一致しなくなる場合があります。STP の設定を手動でチェックし、プライマリ VLAN、隔離 VLAN、およびコミュニティ VLAN のスパニングツリー トポロジーが一致していることを確認する必要があります。
- Catalyst 6500 シリーズ スイッチ上で MAC アドレス リダクションをイネーブルにする場合は、ネットワーク上のすべてのスイッチ上で MAC アドレス リダクションをイネーブルにして、プライベート VLAN の STP トポロジーを一致させます。そうしない場合は、プライベート VLAN のあるネットワーク上で、MAC アドレス リダクションをイネーブルに設定したスイッチとディセーブルに設定したスイッチが混在していることになり、プライマリ VLAN と対応するすべての隔離 VLAN およびコミュニティ VLAN でルート ブリッジを*共通*にするために、デフォルトのブリッジ プライオリティを使用せざるを得なくなります。システム上で MAC アドレス リダクションをイネーブルにするかどうかにかかわらず、MAC アドレス リダクション機能で使用する範囲には一貫性を持たせてください。MAC アドレス リダクションは個々のレベルにしか対応せず、範囲としては すべての中間値を内部的に使用します。プライベート VLAN および MAC アドレス リダクションのあるルート ブリッジはディセーブルにし、非ルート ブリッジが使用する最高のプライオリティ *レンジ*より高いプライオリティでルート ブリッジを設定する必要があります。
- BPDU ガード モードはシステム全体を対象とし、プライベート VLAN に最初のポートが追加された時点でイネーブルになります。
- 宛先 SPAN ポートをプライベート VLAN ポートとして設定することはできません。また、その逆の設定もできません。
- 送信元 SPAN ポートは、1 つのプライベート VLAN に所属できます。
- VLAN-based SPAN（VSPAN）を使用してプライマリ VLAN、隔離 VLAN、およびコミュニティ VLAN を一括して SPAN の対象にすることもできますし、また 1 つの VLAN だけで SPAN を使用して出力トラフィックまたは入力トラフィックを個別にモニタすることもできます。
- RSPAN VLAN は、プライベート VLAN には使用できません。
- 隔離ポート、コミュニティ ポート、または混合ポート上で EtherChannel をイネーブルにすることはできません。
- プライマリ VLAN、隔離 VLAN、およびコミュニティ VLAN には、それぞれ異なる VACL および Quality of Service（QoS; サービス品質）Access Control List（ACL; アクセス制御リスト）を適用できます。

（注） ACL の設定手順については、「プライベート VLAN 上での ACL の設定」（p.15-42）を参照してください。

- MSFC からのすべての発信トラフィックに適用されるように、双方向コミュニティ VLAN とプライマリ VLAN の両方で出力 ACL を設定する必要があります。

- プライマリ VLAN に Cisco IOS ACL をマッピングすると、対応する隔離 VLAN およびコミュニティ VLAN にその Cisco IOS ACL が自動的にマッピングされます。
- 隔離 VLAN またはコミュニティ VLAN に Cisco IOS ACL をマッピングすることはできません。
- プライベート VLAN インターフェイスで Policy-Based Routing（PBR; ポリシー ベース ルーティング）を使用することはできません。**ip policy route-map** *route_map_name* コマンドを使用してプライベート VLAN インターフェイスにポリシーを適用しようとすると、エラー メッセージが出力されます。
- VLAN にダイナミック Access Control Entry（ACE; アクセス制御エントリ）が設定されている場合、その VLAN をプライベート VLAN にすることはできません。
- 隔離 VLAN またはコミュニティ VLAN のレイヤ 3 スイッチングを停止するには、その VLAN とプライマリ VLAN とのバインディングを破棄します。対応するマッピングを削除するだけでは不十分です。

プライマリ プライベート VLAN の作成

プライマリ プライベート VLAN を作成するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	プライマリ プライベート VLAN を作成します。	**set vlan** *vlan* **pvlan-type primary**
ステップ 2	隔離 VLAN、コミュニティ VLAN、または双方向コミュニティ VLAN を設定します。	**set vlan** *vlan* **pvlan-type** {**isolated** | **community** | **twoway-community**}
ステップ 3	隔離 VLAN、コミュニティ VLAN、または双方向コミュニティ VLAN をプライマリ VLAN にバインドします。	**set pvlan** *primary_vlan* {*isolated_vlan* | *community_vlan* | *twoway_community_vlan*}
ステップ 4	隔離ポート、コミュニティ ポート、または双方向コミュニティ ポートをプライマリ プライベート VLAN に対応付けます。	**set pvlan** *primary_vlan* {*isolated_vlan* | *community_vlan* | *twoway_community_vlan*} [*mod/ports* | **sc0**]
ステップ 5	隔離 VLAN、コミュニティ VLAN、または双方向コミュニティ VLAN を、混合ポートのプライマリ プライベート VLAN にマッピングします。	**set pvlan mapping** *primary_vlan* {*isolated_vlan* | *community_vlan* | *twoway_community_vlan*} *mod/ports*
ステップ 6	プライマリ プライベート VLAN の設定を確認します。	**show pvlan** [*vlan*] **show pvlan mapping**

（注） プライベート VLAN に、隔離ポート、コミュニティ ポート、または双方向コミュニティ ポートをバインドすると同時に、対応付けられた隔離 VLAN、コミュニティ VLAN、または双方向コミュニティ VLAN をバインドするには、**set pvlan** *primary_vlan* {*isolated_vlan* | *community_vlan* | *twoway_community_vlan*} *mod/port* コマンドを入力します。

（注） スイッチがトランクに接続され、そのトランクからプライベート VLAN が削除されていないかぎり、ポートが同じスイッチに存在する必要はありません。

（注） プライベート VLAN で混合ポートに MSFC を使用するとき、MSFC *mod/port* 番号としては、スロット 1 にスーパバイザ エンジンが搭載されている場合は 15/1 を、スロット 2 に搭載されている場合は 16/1 を使用してください。

(注) 隔離ポート、コミュニティ ポート、または双方向コミュニティ ポートのある装置、混合ポートのある装置、およびプライベート VLAN をトランクで伝送する必要のあるすべての*中間*スイッチを含むプライベート VLAN を作成する場合は、必ず **set pvlan** コマンドを使用する必要があります。隔離ポート、コミュニティ ポート、双方向コミュニティ ポート、または混合ポートのないエッジ装置（一般に、プライベート ポートを持たないアクセス装置）では、プライベート VLAN を作成する必要はなく、セキュリティ上の理由でプライベート VLAN をトランクからプルーニングすることができます。

次に、VLAN 7 をプライマリ VLAN として指定する例を示します。

```
Console> (enable) set vlan 7 pvlan-type primary
Vlan 7 configuration successful
Console> (enable)
```

次に、VLAN 901 を隔離 VLAN、VLAN 902 および 903 をコミュニティ VLAN として指定する例を示します。

```
Console> (enable) set vlan 901 pvlan-type isolated
Vlan 901 configuration successful
Console> (enable) set vlan 902 pvlan-type community
Vlan 902 configuration successful
Console> (enable) set vlan 903 pvlan-type community
Vlan 903 configuration successful
Console> (enable)
```

次に、VLAN 901 をプライマリ VLAN 7 にバインドし、ポート 4/3 を隔離ポートとして割り当てる例を示します。

```
Console> (enable) set pvlan 7 901 4/3
Successfully set the following ports to Private Vlan 7,901: 4/3
Console> (enable)
```

次に、VLAN 902 をプライマリ VLAN 7 にバインドし、ポート 4/4 ～ 4/6 をコミュニティ ポートとして割り当てる例を示します。

```
Console> (enable) set pvlan 7 902 4/4-6
Successfully set the following ports to Private Vlan 7,902:4/4-6
Console> (enable)
```

次に、VLAN 903 をプライマリ VLAN 7 にバインドし、ポート 4/7 ～ 4/9 をコミュニティ ポートとして割り当てる例を示します。

```
Console> (enable) set pvlan 7 903
Successfully set association between 7 and 903.
Console> (enable) set pvlan 7 903 4/7-9
Successfully set the following ports to Private Vlan 7,903:4/7-9
Console> (enable)
```

次に、隔離 VLAN またはコミュニティ VLAN を混合ポート 3/1 上のプライマリ VLAN にマッピングする例を示します。

```
Console> (enable) set pvlan mapping 7 901 3/1
Successfully set mapping between 7 and 901 on 3/1
Console> (enable) set pvlan mapping 7 902 3/1
Successfully set mapping between 7 and 902 on 3/1
Console> (enable) set pvlan mapping 7 903 3/1
Successfully set mapping between 7 and 903 on 3/1
```

次に、プライベート VLAN の設定を確認する例を示します。

```
Console> (enable) show vlan 7
VLAN Name                             Status    IfIndex Mod/Ports, Vlans
---- -------------------------------- --------- ------- ------------------------
7    VLAN0007                         active    35      4/4-6
VLAN Type  SAID       MTU   Parent RingNo BrdgNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ ------ ---- -------- ------ ------
7    enet  100010     1500  -      -      -      -    -        0      0
VLAN DynCreated  RSPAN
---- ---------- --------
7    static     disabled
VLAN AREHops STEHops Backup CRF 1q VLAN
---- ------- ------- ---------- -------
Primary Secondary Secondary-Type    Ports
------- --------- ----------------- -----------------
7       901        Isolated          4/3
7       902        Community         4/4-6
7       903        Community         4/7-9

Console> (enable) show vlan 902
VLAN Name                             Status    IfIndex Mod/Ports, Vlans
---- -------------------------------- --------- ------- ------------------------
902  VLAN0007                         active    38      4/4-6
VLAN Type  SAID       MTU   Parent RingNo BrdgNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ ------ ---- -------- ------ ------
7    enet  100010     1500  -      -      -      -    -        0      0
VLAN DynCreated  RSPAN
---- ---------- --------
7    static     disabled
VLAN AREHops STEHops Backup CRF 1q VLAN
---- ------- ------- ---------- -------
Primary Secondary Secondary-Type    Ports
------- --------- ----------------- -----------------
7       902       Isolated          4/4-6

Console> (enable) show pvlan
Primary Secondary Secondary-Type Ports
------- --------- -------------- ------------
7       901       isolated       4/3
7       902       community      4/4-6
7       903       community      4/7-9

Console> (enable) show pvlan mapping
Port  Primary  Secondary
----- -------- ----------
3/1    7        901-903
Console> (enable) show port
Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
(テキスト出力は省略)
 4/3                     notconnect 7,901       half   100 100BaseFX MM
 4/4                     notconnect 7,902       half   100 100BaseFX MM
 4/5                     notconnect 7,902       half   100 100BaseFX MM
 4/6                     notconnect 7,902       half   100 100BaseFX MM
 4/7                     notconnect 7,903       half   100 100BaseFX MM
 4/8                     notconnect 7,903       half   100 100BaseFX MM
 4/9                     notconnect 7,903       half   100 100BaseFX MM
(テキスト出力は省略)
```

プライベート VLAN ポートのポート機能の表示

プライベート VLAN のポート機能を表示するには、**show pvlan capability** *mod/port* コマンドを入力します。

次に , 下記の設定でいくつかのポートについてポート機能を表示する例を示します。

```
Console> (enable) set pvlan 10 20
Console> (enable) set pvlan mapping 10 20 3/1
Console> (enable) set pvlan mapping 10 20 5/2
Console> (enable) set trunk 5/1 desirable isl 1-1005,1025-4094

Console> (enable) show pvlan capability 5/20
Ports 5/13 - 5/24 are in the same ASIC range as port 5/20.

Port 5/20 can be made a private vlan port.

Console> (enable) show pvlan
Primary Secondary Secondary-Type Ports
------- --------- -------------- ------------
10      20        isolated

Console> (enable) show pvlan capability 3/1
Port 3/1 cannot be made a private vlan port due to:
-----------------------------------------------------
Promiscuous ports cannot be made private vlan ports.

Console> (enable) show pvlan capability 5/1
Ports 5/1 - 5/12 are in the same ASIC range as port 5/1.

Port 5/1 cannot be made a private vlan port due to:
-----------------------------------------------------
Trunking ports are not Private Vlan capable.
Conflict with Promiscuous port(s) : 5/2

Console> (enable) show pvlan capability 5/2
Ports 5/1 - 5/12 are in the same ASIC range as port 5/2.

Port 5/2 cannot be made a private vlan port due to:
-----------------------------------------------------
Promiscuous ports cannot be made private vlan ports.
Conflict with Trunking port(s) : 5/1

Console> (enable) show pvlan capability 5/3
Ports 5/1 - 5/12 are in the same ASIC range as port 5/3.

Port 5/3 cannot be made a private vlan port due to:
-----------------------------------------------------
Conflict with Promiscuous port(s) : 5/2
Conflict with Trunking port(s) : 5/1

Console> (enable) show pvlan capability 15/1
Port 15/1 cannot be made a private vlan port due to:
-----------------------------------------------------
Only ethernet ports can be added to private vlans.
```

プライベート VLAN の削除

プライベート VLAN を削除するには、プライマリ VLAN を削除します。プライマリ VLAN を削除すると、そのプライマリ VLAN へのすべてのバインディングが破棄され、プライベート VLAN 上のすべてのポートが非アクティブになり、混合ポート上の関連するマッピングがすべて削除されます。

プライベート VLAN を削除するには、イネーブル モードで次の作業を行います。

作業	コマンド
プライマリ VLAN を削除します。	**clear vlan** *primary_vlan*

次に、プライマリ VLAN 7 を削除する例を示します。

```
Console> (enable) clear vlan 7
This command will de-activate all ports on vlan 7
Do you want to continue(y/n) [n]?y
Vlan 7 deleted
Console> (enable)
```

隔離 VLAN、コミュニティ VLAN または双方向コミュニティ VLAN の削除

隔離 VLAN、コミュニティ VLAN、または双方向コミュニティ VLAN を削除すると、プライマリ VLAN とのバインディングが破棄され、その VLAN に対応付けられていた隔離ポート、コミュニティ ポート、または双方向コミュニティ ポートはすべて非アクティブになり、混合ポート上の関連するマッピングはすべて削除されます。

スイッチ上の VLAN を削除するには、イネーブル モードで次のコマンドを入力します。

作業	コマンド
隔離 VLAN またはコミュニティ VLAN を削除します。	**clear vlan** {*isolated_vlan* | *community_vlan* | *twoway_community_vlan*}

次に、コミュニティ VLAN 902 を削除する例を示します。

```
Console> (enable) clear vlan 902
This command will de-activate all ports on vlan 902
Do you want to continue(y/n) [n]?y
Vlan 902 deleted
Console> (enable)
```

プライベート VLAN マッピングの削除

プライベート VLAN のマッピングを削除すると、隔離ポート、コミュニティ ポート、または双方向コミュニティ ポートと混合ポートとの間の接続が解除されます。混合ポート上のマッピングをすべて削除すると、その混合ポートは非アクティブになります。プライベート VLAN ポートが非アクティブになると、**show port** の出力で、そのポートの VLAN 番号は [pvlan-] と表示されます。

プライベート VLAN ポートが、非アクティブになる原因としては、次のものがあります。

- ポートが属するプライマリ VLAN、隔離 VLAN、コミュニティ VLAN、または双方向コミュニティ VLAN が消去された場合。
- MSFC 以外の混合ポートからのマッピングがすべて削除された場合。
- ポートをプライベート VLAN に設定したときにエラーが発生する場合。

プライベート VLAN からポートのマッピングを削除するには、イネーブル モードで次の作業を行います。

作業	コマンド
プライベート VLAN からポートのマッピングを削除します。	**clear pvlan mapping** primary_vlan {*isolated* | *community* | *twoway-community*} {*mod/ports*}

次に、ポート 3/2 ～ 3/5 上に設定されていた、VLAN 902 から 901 へのマッピングを削除する例を示します。

```
Console> (enable) clear pvlan mapping 901 902 3/2-5
Successfully cleared mapping between 901 and 902 on 3/2-5
Console> (enable)
```

MSFC 上でのプライベート VLAN サポート

ここでは、MSFC 上でのプライベート VLAN のサポートについて説明します。

- プライベート VLAN に関する情報を表示するには、**show pvlan** コマンドを使用します。**show pvlan** コマンドでプライベート VLAN に関する情報が表示されるのは、プライマリ プライベート VLAN がアップになっている場合に限られます。
- スーパバイザ エンジンに対して **set pvlan mapping** または **clear pvlan mapping** コマンドを入力すると、MSFC Syslog メッセージが表示されます。次に例を示します。

```
%PV-6-PV_MSG:Created a private vlan mapping, Primary 100, Secondary 101
%PV-6-PV_MSG:Created a private vlan mapping, Primary 200, Secondary 201
%PV-6-PV_MSG:Purged a private vlan mapping, Primary 100, Secondary 101
```

- プライマリ プライベート VLAN に対してだけレイヤ 3 パラメータを設定するには、**interface vlan** コマンドを使用します。
- MSFC で **interface vlan** コマンドで入力されている VLAN 番号を使用して、スーパバイザ エンジン上で隔離 VLAN またはコミュニティ VLAN を作成することはできません。
- レイヤ 3 のプライベート VLAN インターフェイス上で学習された ARP エントリは、sticky ARP エントリです（プライベート VLAN インターフェイスの ARP エントリを表示して確認することを推奨します）。
- プライベート VLAN インターフェイスの sticky ARP エントリは、セキュリティ上の理由から、期限切れになりません。同じ IP アドレスで新しい装置を接続しても、メッセージが生成され、ARP エントリは作成されません。
- プライベート VLAN インターフェイスの ARP エントリは期限切れにならないので、MAC アドレスを変更した場合はプライベート VLAN インターフェイスの ARP エントリを手動で削除する必要があります。
- プライベート VLAN の ARP エントリは、手動で追加または削除する必要があります。次に例を示します。

```
obelix-rp(config)# no arp 11.1.3.30
IP ARP:Deleting Sticky ARP entry 11.1.3.30

obelix-rp(config)# arp 11.1.3.30 0000.5403.2356 arpa
IP ARP:Overwriting Sticky ARP entry 11.1.3.30, hw:00d0.bb09.266e by
hw:0000.5403.2356
```

- 一部のコマンドにより、プライベート VLAN マッピングが消去および再作成されます。次に例を示します。

```
obelix-rp(config)# xns routing
obelix-rp(config)#
%PV-6-PV_MSG:Purged a private vlan mapping, Primary 100, Secondary 101
%PV-6-PV_MSG:Purged a private vlan mapping, Primary 100, Secondary 102
%PV-6-PV_MSG:Purged a private vlan mapping, Primary 100, Secondary 103
%PV-6-PV_MSG:Created a private vlan mapping, Primary 100, Secondary 101
%PV-6-PV_MSG:Created a private vlan mapping, Primary 100, Secondary 102
%PV-6-PV_MSG:Created a private vlan mapping, Primary 100, Secondary 103
```

スイッチ上での FDDI VLAN の設定

新しい FDDI VLAN を作成するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	新しい FDDI VLAN または FDDI NET タイプの VLAN を作成します。	**set vlan** *vlan* [**name** *name*] **type** {**fddi** | **fddinet**} [**said** *said*] [**mtu** *mtu*]
ステップ 2	VLAN の設定を確認します。	**show vlan** [*vlan*]

既存の FDDI VLAN の VLAN パラメータを変更するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	既存の FDDI VLAN または FDDI NET タイプの VLAN を変更します。	**set vlan** *vlan* [**name** *name*] [**state** {**active** | **suspend**}] [**said** *said*] [**mtu** *mtu*]
ステップ 2	VLAN の設定を確認します。	**show vlan** [*vlan*]

スイッチ上でのトークンリング VLAN の設定

ここでは、VTP バージョン 2 で動作するスイッチ上でサポートされる、2 種類のトークンリング VLAN について説明します。

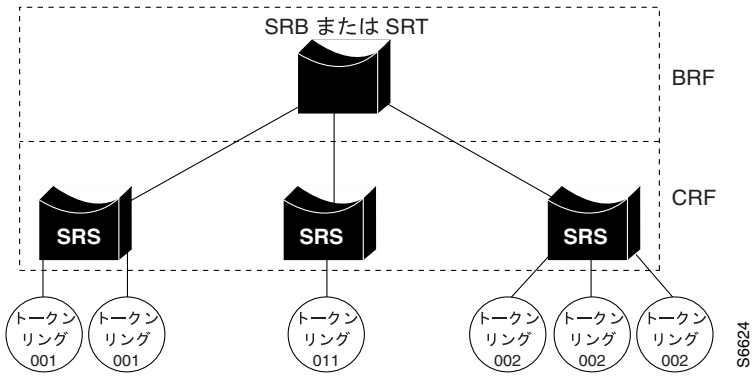
トークンリング VLAN を設定および管理するには、VTP バージョン 2 を使用する必要があります。

（注） Catalyst 6500 シリーズ スイッチでは、ISL カプセル化トークンリング フレームはサポートされていません。

トークンリング TrBRF VLAN の機能概要

TrBRF VLAN は、スイッチド トークンリング ネットワーク環境において、複数の TrCRF VLAN を相互接続します（図 11-3 を参照）。TrBRF は、トランク リンクによって相互接続されたスイッチで構成されるネットワーク全体に拡大することができます。TrCRF と TrBRF 間の接続を*論理ポート*といいます。

図 11-3　相互接続されたトークンリング TrBRF VLAN および TrCRF VLAN



ソース ルーティングでは、スイッチは論理リング間の単一ブリッジとなります。TrBRF は、IBM または IEEE STP を実行する SRB または SRT ブリッジとして動作できます。SRB を使用する場合、重複する MAC アドレスを異なる論理リングで定義できます。

トークンリング ソフトウェアは、TrBRF VLAN ごとに、また、TrCRF VLAN ごとに 1 つずつ STP のインスタンスを実行します。TrCRF VLAN の場合、STP により、論理リングのループが排除されます。TrBRF VLAN の場合、STP はイーサネット VLAN 上での動作と同様、外部ブリッジと対話して、ブリッジ トポロジーからループを排除します。

注意　特定の親 TrBRF STP および TrCRF ブリッジ モードを設定すると、TrBRF の論理ポート（TrBRF と TrCRF 間の接続）がブロック ステートになる可能性があります。詳細については、「VLAN のデフォルト設定」（p.11-4）を参照してください。

ソース ルーティングでは、スイッチは論理リング間の単一ブリッジとなります。TrBRF は、IBM または IEEE STP を実行する SRB または SRT ブリッジとして動作できます。SRB を使用する場合には、複数の異なる論理リングに重複した MAC アドレスを定義できます。

IBM の System Network Architecture（SNA）トラフィックに対応するために、SRT モードと SRB モードを組み合わせて使用することができます。混在モードでは、TrBRF は一部のポート（TrCRF に接続された論理ポート）が SRB モードで動作し、他のポートが SRT モードで動作するものとみなします。

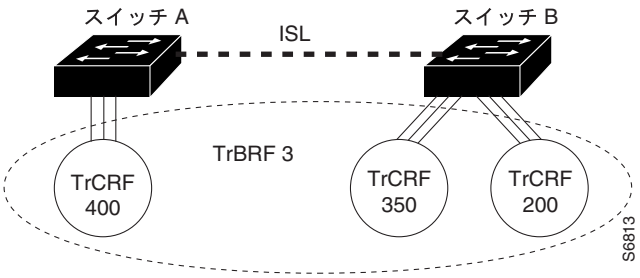
トークンリング TrCRF VLAN の機能概要

TrCRF VLAN では、同じ論理リング番号でポート グループを定義します。ネットワークには、非分散型およびバックアップの 2 種類の TrCRF を設定できます。

通常、TrCRF は非分散型です。これは、各 TrCRF が 1 台のスイッチ上のポートに限定されることを意味します。同一または異なるスイッチ上で、複数の非分散型 TrCRF を 1 つの親 TrBRF に対応させることができます（図 11-4 を参照）。親 TrBRF は、マルチポート ブリッジとして動作し、非分散型 TrCRF 間でトラフィックを転送します。

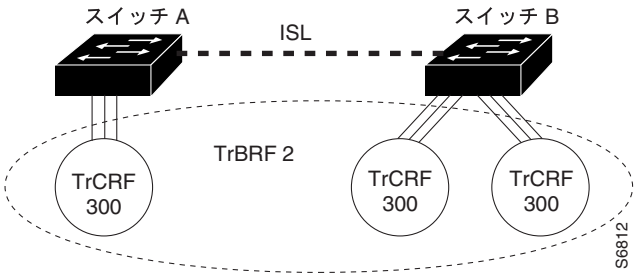
（注）　異なるスイッチ上のリング間でデータを受け渡すには、リングを同一の TrBRF に対応付けて、その TrBRF を SRB として設定します。

図 11-4　非分散型 TrCRF



（注）　デフォルトの設定では、トークンリング ポートはデフォルトの TrCRF（VLAN 1003、trcrf-default）に対応し、これにはデフォルトの TrBRF（VLAN 1005、trbrf-default）が親として存在します。この設定では、分散型 TrCRF が可能であり（図 11-5 を参照）、スイッチが ISL トランクで接続されている場合に、異なるスイッチ上のデフォルトの TrCRF 間でトラフィックを流すことができます。

図 11-5　分散型 TrCRF



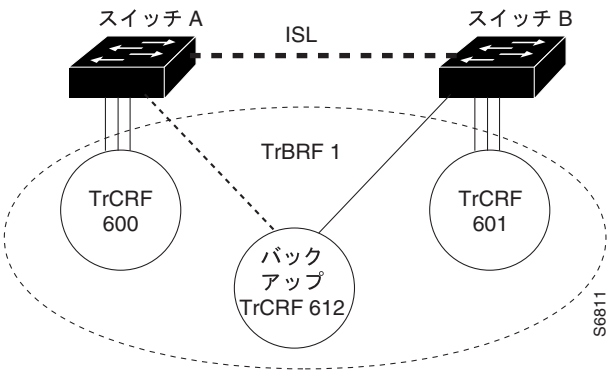
TrCRF 内では、ソースルート スイッチングを使用し、MAC アドレスまたはルート記述子に基づいて転送を行います。VLAN 全体を 1 つのリングとして動作させ、フレームを 1 つの TrCRF 内のポート間でスイッチングすることもできます。

TrCRF ごとに ARE フレームおよび STE フレームの最大ホップ カウントを指定することによって、エクスプローラが通過できる最大ホップ数を制限することができます。ポートで、受け取ったエクスプローラ フレームが指定されたホップ数を超えて経由して来ていることが判別されると、そのフレームは転送されません。TrCRF では、ルート情報フィールドのブリッジ ホップ数に基づいて、エクスプローラが経由したホップ数を判別します。

バックアップ TrCRF を使用すると、スイッチ間の ISL 接続で障害が発生した場合、TrBRF で接続されている複数のスイッチ上の非分散型 TrCRF 間を流れるトラフィック用に、代替ルートを設定することができます。また、TrBRF でバックアップ TrCRF に割り当てることができるポートは、1 台のスイッチで 1 つだけです。

スイッチ間の ISL 接続で問題が起きた場合、影響を受ける各スイッチ上のバックアップ TrCRF ポートがアクティブになり、バックアップ TrCRF を介して非分散型 TrCRF 間のトラフィックが再ルーティングされます。ISL 接続が再び確立されると、バックアップ TrCRF の 1 ポートを除くすべてのポートがディセーブルになります。図 11-6 に、バックアップ TrCRF を示します。

図 11-6　バックアップ TrCRF



トークンリング VLAN 設定時の注意事項

ここでは、トークンリング VLAN 作成または変更時の注意事項について説明します。

- トークンリング VLAN では、デフォルトの TrBRF（VLAN 1005）は、デフォルトの TrCRF（VLAN 1003）の親としてだけ指定できます。ユーザ側で設定した TrCRF の親としてデフォルトの TrBRF を指定することはできません。
- TrBRF を設定してから、TrCRF を設定する必要があります。つまり、TrCRF に指定する親 TrBRF VLAN がすでに存在していなければなりません。
- トークンリング環境では、次のいずれかの条件が存在している場合、TrBRF の論理ポート（TrBRF と TrCRF 間の接続）がブロック ステートになります。
  - TrBRF が IBM STP を実行していて、TrCRF が SRT モード
  - TrBRF が IEEE STP を実行していて、TrCRF が SRB モード

トークンリング TrBRF VLAN の作成または変更

VTP バージョン 2 をイネーブルにしてから、トークンリング VLAN を作成する必要があります。VTP バージョン 2 をイネーブルにする方法については、第 10 章「VTP の設定」を参照してください。

新しい TrBRF を作成する場合、ブリッジ番号を指定しなければなりません。

新しいトークンリング TrBRF VLAN を作成するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	新しいトークンリング TrBRF タイプの VLAN を作成します。	**set vlan** *vlan* [**name** *name*] **type trbrf** [**said** *said*] [**mtu** *mtu*] **bridge** *bridgeber* [**stp** {**ieee** | **ibm**}]
ステップ 2	VLAN の設定を確認します。	**show vlan** [*vlan*]

次に、新しいトークンリング TrBRF VLAN を作成し、設定を確認する例を示します。

```
Console> (enable) set vlan 999 name TrBRF_999 type trbrf bridge a
Vlan 999 configuration successful
Console> (enable) show vlan 999
VLAN Name                             Status    IfIndex Mod/Ports, Vlans
---- -------------------------------- --------- ------- ------------------------
999  TrBRF_999                        active
VLAN Type  SAID       MTU   Parent RingNo BrdgNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ ------ ---- -------- ------ ------
999  trbrf 100999     4472  -      -      0xa    ibm  -        0      0
VLAN AREHops STEHops Backup CRF
---- ------- ------- ----------
Console> (enable)
```

既存のトークンリング TrBRF VLAN 上で VLAN パラメータを変更するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	既存のトークンリング TrBRF タイプの VLAN を変更します。	**set vlan** *vlan* [**name** *name*] [**state** {**active** | **suspend**}] [**said** *said*] [**mtu** *mtu*] [**bridge** *bridgeber*] [**stp** {**ieee** | **ibm**}]
ステップ 2	VLAN の設定を確認します。	**show vlan** [*vlan*]

トークンリング TrCRF VLAN の作成または変更

（注） VTP バージョン 2 を イネーブルにしてから、トークンリング VLAN を作成する必要があります。VTP バージョン 2 をイネーブルにする方法については、第 10 章「VTP の設定」を参照してください。

新しいトークンリング TrCRF VLAN を作成するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	新しいトークンリング TrCRF タイプの VLAN を作成します。	**set vlan** *vlan* [**name** *name*] **type trcrf** [**said** *said*] [**mtu** *mtu*] {**ring** *hex_ringber* | **decring** *decimal_ringber*} **parent** *vlan*
ステップ 2	VLAN の設定を確認します。	**show vlan** [*vlan*]

（注） 新しい TrCRF を作成するときには、（16 進数または 10 進数で）リング番号を指定し、さらに親の TrBRF VLAN を指定しなければなりません。

次に、トークンリング TrCRF VLAN を作成し、設定を確認する例を示します。

```
Console> (enable) set vlan 998 name TrCRF_998 type trcrf decring 10 parent 999
Vlan 998 configuration successful
Console> (enable) show vlan 998
VLAN Name                             Status    IfIndex Mod/Ports, Vlans
---- -------------------------------- --------- ------- -------------------------
998  TrCRF_998                        active    352
VLAN Type  SAID       MTU   Parent RingNo BrdgNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ ------ ---- -------- ------ ------
998  trcrf 100998     4472  999    0xa    -      -    srb      0      0
VLAN AREHops STEHops Backup CRF
---- ------- ------- ----------
998  7       7       off
Console> (enable)
```

既存のトークンリング TrCRF VLAN 上で VLAN パラメータを変更するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	既存のトークンリング TrCRF VLAN を変更します。	**set vlan** *vlan* [**name** *name*] [**state** {**active** | **suspend**}] [**said** *said*] [**mtu** *mtu*] [**ring** *hex_ring*] [**decring** *decimal_ring*] [**bridge** *bridge*] [**parent** *vlan*]
ステップ 2	VLAN の設定を確認します。	**show vlan** [*vlan*]

バックアップ TrCRF を作成するには、TrBRF が経由するスイッチごとに 1 ポートずつ、バックアップ TrCRF に割り当てます。

TrCRF VLAN をバックアップ TrCRF として設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	TrCRF VLAN をバックアップ TrCRF として設定します。	**set vlan** *vlan* **backupcrf on**
ステップ 2	VLAN の設定を確認します。	**show vlan** [*vlan*]

注意　トークンリング Multistation Access Unit（MSAU）にバックアップ TrCRF ポートを接続した場合、別の装置でリング速度とポート モードを設定しないかぎり、バックアップ パスは提供されません。バックアップ TrCRF 用にリング速度とポート モードを設定することを推奨します。

TrCRF における ARE フレームまたは STE フレームの最大ホップ数を指定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	TrCRF における ARE フレームの最大ホップ数を指定します。	**set vlan** *vlan* **aremaxhop** *hopcount*
ステップ 2	TrCRF における STE フレームの最大ホップ数を指定します。	**set vlan** *vlan* **stemaxhop** *hopcount*
ステップ 3	VLAN の設定を確認します。	**show vlan** [*vlan*]

次に、ARE フレームおよび STE フレームを 10 ホップに制限し、設定を確認する例を示します。

```
Console> (enable) set vlan 998 aremaxhop 10 stemaxhop 10
Vlan 998 configuration successful
Console> (enable) show vlan 998
VLAN Name                             Status    IfIndex Mod/Ports, Vlans
---- -------------------------------- --------- ------- -------------------------
998  VLAN0998                         active    357


VLAN Type  SAID       MTU   Parent RingNo BrdgNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ ------ ---- -------- ------ ------
998  trcrf 100998     4472  999    0xff   -      -    srb      0      0


VLAN AREHops STEHops Backup CRF
---- ------- ------- ----------
998  10      10      off
Console> (enable)
```

Firewall Services Module 用の VLAN の設定

Firewall Services Module（WS-SVC-FWM-1-K9）によって保護される VLAN を指定するには、**set vlan** {*vlans*} **firewall-vlan** {*mod*} コマンドを入力します。Firewall Services Module によって保護される VLAN を表示するには、**show vlan firewall-vlan** *mod* コマンドを入力します。

Firewall Services Module で VLAN 範囲を保護するには、次の条件が満たされなければなりません。

1. VLAN にポート メンバーシップが定義され、VLAN がアクティブ ステートになっている。
2. VLAN に、アクティブ ステートになっている MSFC レイヤ 3 インターフェイスがない。
3. VLAN が予約 VLAN でない。

上記の 2 の条件を満たしていない VLAN は、Firewall Services Module で保護しようとする VLAN 範囲から廃棄されます。

2 と 3 の条件を満たしているものの 1 の条件を満たしていない VLAN は、スーパバイザ エンジン データベースに保存されます。これらの VLAN は、1 の条件が満たされるとただちに Firewall Services Module へ送られます。

次に、Firewall Services Module で VLAN 範囲を保護する例を示します。

```
Console> (enable) set vlan 2-55 firewall-vlan 7
Console> (enable)
```

Firewall Services Module の複数 VLAN インターフェイス機能を設定するには、**set firewall multiple-vlan-interfaces** {**enable** | **disable**} コマンドを入力します。複数 VLAN インターフェイス機能をディセーブル化すると、Firewall Services Module は単一 VLAN インターフェイス モードに設定されます。複数 VLAN インターフェイス機能は、デフォルトではディセーブルです。例は次のとおりです。

```
Console> (enable) set firewall multiple-vlan-interfaces  enable
This command will enable multiple-vlan-interfaces feature for all firewall
modules in the chassis.
It can result in traffic bypassing the firewall module.
Do you want to continue (y/n) [n]? y
multiple-vlan-interfaces feature enabled for firewall module 5.
Console> (enable)
```

Release 8.4(1) 以降のソフトウェア リリースでは、**set vlan** {*vlan*} **firewall-vlan** {*mod*} **msfc-fwsm-interface** コマンドを入力して、指定された VLAN を MSFC と Firewall Services Module 間の保護インターフェイスにすることができます。このコマンドを使用できるのは、単一 VLAN インターフェイス モードの場合のみです。複数の VLAN インターフェイスがイネーブル化されている場合は、入力できません。例は次のとおりです。

```
Console> (enable) set vlan 3 firewall-vlan 5 msfc-fwsm-interface
Vlan 3 declared as Secure Vlan interface for module 5
Vlan 3 declared secure for firewall module 5
Console> (enable)
```

(注)

Firewall Services Module の設定の詳細については、次の URL にある Firewall Services Module のマニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod_icn/fwsm/index.htm

CHAPTER 12

VLAN 間ルーティングの設定

この章では、Catalyst 6500 シリーズ スイッチ上で VLAN（仮想 LAN）間ルーティングを行うために Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）を設定する方法について説明します。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

この章で説明する内容は、次のとおりです。

(注) FlexWAN モジュール インターフェイス上でルーティングを設定する手順については、『*FlexWAN Module Port Adapter Installation and Configuration Notes*』を参照してください。

VLAN 間ルーティングの機能概要

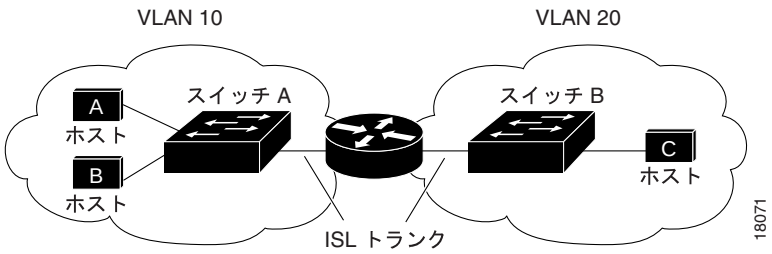
異なる VLAN に所属するネットワーク装置は、VLAN 間でトラフィックを転送するルータがなければ、互いに通信できません。ほとんどのネットワーク環境では、VLAN は個別のネットワークまたはサブネットワークに対応付けられています。

たとえば、IP ネットワークでは、各サブネットワークは個別の VLAN にマッピングされています。Internetwork Packet Exchange（IPX）ネットワークでは、各 VLAN は個別の IPX ネットワーク番号にマッピングされています。

VLAN を設定すると、ブロードキャスト ドメインのサイズが制御され、ローカル トラフィックがローカルのままに保たれるという利点があります。ある VLAN のエンド ステーションが別の VLAN のエンド ステーションと通信しなければならない場合には、VLAN 間通信が必要になります。この通信機能を提供するのが、VLAN 間ルーティングです。適切な宛先 VLAN にトラフィックをルーティングするように、1 台または複数のルータを設定します。

図 12-1 に、VLAN 間の基本的なルーティング トポロジーを示します。スイッチ A は VLAN 10、スイッチ B は VLAN 20 に所属しています。ルータには、各 VLAN とのインターフェイスがあります。

図 12-1　VLAN 間の基本的なルーティング トポロジー



VLAN 10 のホスト A が VLAN 10 のホスト B と通信する場合、ホスト A はホスト B のアドレスを指定したパケットを送信します。スイッチ A は、そのパケットをルータに送信せず、直接ホスト B に転送します。

ホスト A が VLAN 20 のホスト C にパケットを送信するとき、スイッチ A は、VLAN 10 インターフェイスのトラフィックを受信するルータにそのパケットを転送します。ルータはルーティング テーブルを調べ、適正な発信インターフェイスを判別し、パケットを VLAN 20 インターフェイスに転送してスイッチ B に渡します。スイッチ B はパケットを受信すると、ホスト C に転送します。

MSFC 上での VLAN 間ルーティングの設定

(注)　以下に説明する内容は、Cisco IOS ソフトウェアに関する知識があり、Cisco IOS ルーティングを設定した経験があるユーザを対象としています。シスコ ルーティングの設定に不慣れな場合は、Cisco.com で入手できる Cisco IOS マニュアルを参照してください。

ここでは、MSFC 上で VLAN 間ルーティングを設定する手順について説明します。

MSFC ルーティング設定時の注意事項

ここでは、MSFC に VLAN 間ルーティングを設定する場合の注意事項（2 つの主な手順からなる）について説明します。

1. スイッチ上で VLAN を作成および設定し、スイッチ ポートに VLAN メンバーシップを割り当てます。詳細については、第 11 章「VLAN の設定」を参照してください。
2. MSFC 上で VLAN 間ルーティングのための VLAN インターフェイスを作成および設定します。トラフィックをルーティングする相手先 VLAN ごとに、VLAN インターフェイスを設定します。

MSFC 上の VLAN インターフェイスは、仮想インターフェイスです。ただし、設定する手順は物理ルータ インターフェイスの場合と同じです。

MSFC3、MSFC2、MSFC2A、および MSFC は、スーパバイザ エンジンと同じ範囲の VLAN をサポートしています。MSFC3、MSFC2、および MSFC2A は最大 1,000 の VLAN インターフェイスをサポートし、MSFC は最大 256 の VLAN インターフェイスをサポートします。

MSFC 上での IP VLAN 間ルーティングの設定

IP 用に VLAN 間ルーティングを設定するには、次の作業を行います。

	作業	コマンド
ステップ 1	（任意）ルータ上で IP ルーティングをイネーブルにします。[1]	Router(config)# **ip routing**
ステップ 2	（任意）IP ルーティング プロトコルを指定します。[2]	Router(config)# **router** *ip_routing_protocol*
ステップ 3	MSFC 上の VLAN インターフェイスを指定します。	Router(config)# **interface** *vlan-id*
ステップ 4	VLAN に IP アドレスを割り当てます。	Router(config-if)# **ip address** *n.n.n.n mask*
ステップ 5	コンフィギュレーション モードを終了します。	Router(config-if)# **Ctrl-Z**

1. ネットワーク上に複数のルータがある場合は、このステップは必須です。
2. ステップ 1 で IP ルーティングをイネーブルにした場合は、このステップは必須です。このステップには、上記以外のコマンド（ルーティング対象のネットワークを指定する **network** ルータ コンフィギュレーション コマンドなど）が含まれる場合があります。ルーティング プロトコルの詳しい設定手順については、使用するルータ プラットフォームのマニュアルを参照してください。

次に、MSFC 上で IP ルーティングをイネーブルにし、VLAN インターフェイスを作成し、そのインターフェイスに IP アドレスを割り当てる例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip routing
Router(config)# router rip
Router(config-router)# network 10.0.0.0
Router(config-router)# interface vlan 100
Router(config-if)# ip address 10.1.1.1 255.0.0.0
Router(config-if)# ^Z
Router#
```

MSFC 上での IPX VLAN 間ルーティングの設定

（注） Supervisor Engine 720（MSFC3）では、IPX ルーティングはソフトウェアを通じて実行されます。

IPX 用に VLAN 間ルーティングを設定するには、次の作業を行います。

	作業	コマンド
ステップ 1	（任意）ルータ上で IPX ルーティングをイネーブルにします。[1]	Router(config)# **ipx routing**
ステップ 2	（任意）IPX ルーティング プロトコルを指定します。[2]	Router(config)# **ipx router** *ipx_routing_protocol*
ステップ 3	MSFC 上の VLAN インターフェイスを指定します。	Router(config)# **interface** *vlan-id*
ステップ 4	VLAN にネットワーク番号を割り当てます。[3]	Router(config-if)# **ipx network** [*network* | **unnumbered**] **encapsulation** *encapsulation-type*
ステップ 5	コンフィギュレーション モードを終了します。	Router(config-if)# **Ctrl-Z**

1. ネットワーク上に複数のルータがある場合は、このステップは必須です。
2. ステップ 1 で IPX ルーティングをイネーブルにした場合は、このステップは必須です。このステップには、上記以外のコマンド（ルーティング対象のネットワークを指定する **network** ルータ コンフィギュレーション コマンドなど）が含まれる場合があります。ルーティング プロトコルの詳しい設定手順については、使用するルータ プラットフォームのマニュアルを参照してください。
3. このステップにより、VLAN 上で IPX ルーティングがイネーブルになります。VLAN 上で IPX ルーティングをイネーブルにする場合、カプセル化タイプも指定できます。

次に、MSFC 上で IPX ルーティングをイネーブルにし、VLAN インターフェイスを作成し、そのインターフェイスに IPX ネットワーク アドレスを割り当てる例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ipx routing
Router(config)# ipx router rip
Router(config-ipx-router)# network all
Router(config-ipx-router)# interface vlan100
Router(config-if)# ipx network 100 encapsulation snap
Router(config-if)# ^Z
Router#
```

MSFC 上での AppleTalk VLAN 間ルーティングの設定

AppleTalk について VLAN 間ルーティングを設定するには、次の作業を行います。

	作業	コマンド
ステップ 1	（任意）ルータ上で AppleTalk ルーティングをイネーブルにします。[1]	Router(config)# **appletalk routing**
ステップ 2	MSFC 上の VLAN インターフェイスを指定します。	Router(config)# **interface** *vlan-id*
ステップ 3	VLAN にケーブル範囲を割り当てます。	Router(config-if)# **appletalk cable-range** *cable-range*
ステップ 4	VLAN にゾーン名を割り当てます。	Router(config-if)# **appletalk zone** *zone-name*
ステップ 5	コンフィギュレーション モードを終了します。	Router(config-if)# **Ctrl-Z**

1. ネットワーク上に複数のルータがある場合は、このステップは必須です。

次に、MSFC 上で AppleTalk ルーティングをイネーブルにし、VLAN インターフェイスを作成し、そのインターフェイスに AppleTalk ケーブル範囲およびゾーン名を割り当てる例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# appletalk routing
Router(config)# interface vlan100
Router(config-if)# appletalk cable-range 100-100
Router(config-if)# appletalk zone Engineering
Router(config-if)# ^Z
Router#
```

MSFC 機能の設定

ここでは、MSFC 機能について説明します。

- ローカル プロキシ ARP（p.12-5）
- WCCP レイヤ 2 リダイレクション（p.12-6）
- auto state 機能（p.12-6）

ローカル プロキシ ARP

Release 12.1(2)E 以降のリリースでは、ローカル プロキシ Address Resolution Protocol（ARP）機能により、MSFC は通常ルーティングが必要とされないサブネット内部の IP アドレスに関する ARP 要求に応答できます。ローカル プロキシ ARP をイネーブルにすると、MSFC はサブネット内の IP アドレスに対するすべての ARP 要求に応答し、そのサブネット内のホスト間トラフィックをすべて転送します。この機能は、接続先スイッチ上での設定により、意図的にホスト間の直接的なコミュニケーションが禁止されているサブネットについてのみ使用してください。

ローカル プロキシ ARP のデフォルト設定はディセーブルです。インターフェイス上でローカル プロキシ ARP をイネーブルにするには、**ip local-proxy-arp** インターフェイス コンフィギュレーション コマンドを入力します。この機能をディセーブルにするには、**no ip local-proxy-arp** インターフェイス コンフィギュレーション コマンドを入力します。ローカル プロキシ ARP 機能がイネーブルになっているインターフェイス上では、Internet Control Message Protocol（ICMP）リダイレクションはディセーブルになります。

WCCP レイヤ 2 リダイレクション

(注)　Policy Feature Card（PFC; ポリシー フィーチャ カード）を装備した Supervisor Engine 1 では、Release 12.1E(2) 以降のリリースでこの機能がサポートされています。PFC2 を装備した Supervisor Engine 2 では、Release 12.1(3a)E 以降のリリースでこの機能がサポートされています。WCCP レイヤ 2 リダイレクションは、Supervisor Engine 720 または Supervisor Engine 32 ではサポートされていません。

Web Cache Communication Protocol（WCCP）レイヤ 2 リダイレクション機能により、直接接続された Cisco Cache Engine は、レイヤ 2 リダイレクションを使用することができます。これは、Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）によるレイヤ 3 リダイレクションよりも効率的です。WCCP レイヤ 2 リダイレクションをネゴシエーションするように、直接接続された Cisco Cache Engine を設定できます。WCCP レイヤ 2 リダイレクション機能を使用するには、MSFC 上での設定作業は不要です。**show ip wccp web-cache detail** コマンドを使用すると、各キャッシュで使用中のリダイレクション方式を調べることができます。この機能を使用する際は、次の注意事項に従ってください。

- WCCP レイヤ 2 リダイレクションにより、IP フロー マスクが full-flow モードに設定されます。
- Cisco Cache Engine の Release 2.2 以降のソフトウェア リリースでは、WCCP レイヤ 2 リダイレクションを使用するように設定できます。
- レイヤ 2 リダイレクションはスイッチ上で行われ、MSFC からは見えません。MSFC 上で **show ip wccp web-cache detail** コマンドを実行すると、レイヤ 2 リダイレクトされたフローの最初のパケットに関する統計情報が表示されます。それによって、いくつの（パケットではなく）フローがレイヤ 2 リダイレクションを使用しているかがわかります。スーパバイザ エンジン上で **show mls entries** コマンドを実行すると、レイヤ 2 リダイレクトされたフローのその他のパケットが表示されます。

次の URL にある『*Cisco IOS Configuration Fundamentals Configuration Guide*』に記載されているとおりに、Cisco IOS WCCP を設定します。
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/fun_c/fcprt3/fcd305.htm

auto state 機能

次の MSFC auto state ポートベース モードがサポートされています。

- 通常 auto state モード（p.12-6）
- auto state 除外モード（p.12-7）
- auto state 追跡モード（p.12-7）

通常 auto state モード

auto state は、スイッチに対して以下のポート設定の変更が発生すると、MSFC および Multilayer Switch Module（MSM）のレイヤ 3 インターフェイス / サブインターフェイスをシャットダウンまたは起動します。

- VLAN 上または別のルータの sc0 が VLAN のインターフェイス / サブインターフェイス搭載シャーシ内にある場合を除いて、VLAN の最後のポートが停止するとき、その VLAN 上のすべてのレイヤ 3 インターフェイス / サブインターフェイスがシャットダウンします（auto state が実行されます）。
- VLAN の最初のポートが再起動するとき、その VLAN 上のシャットダウンしていたすべてのレイヤ 3 インターフェイスが起動します。

Catalyst 6500 シリーズ スイッチは、MSM や MSFC の設定を認識または制御していません（外部ルータの設定を認識または制御していないのと同じです）。MSM や MSFC が正しく設定されていなければ、auto state は MSM や MSFC 上では動作しません。たとえば、次の MSM トランク コンフィギュレーションについて考えるとします。

```
interface GigabitEthernet0/0/0.200
    encap isl 200
    .
    .
```

この例では、次のいずれかの設定エラーがあると、GigabitEthernet0/0/0.200 インターフェイスは atuto state を実行しません。

- スイッチ上で VLAN 200 が設定されていない。
- 対応するギガビット イーサネット スイッチ ポートでトランキングが設定されていない。
- トランキングは設定されているが、そのトランク上で VLAN 200 が許可されていない。

auto state 除外モード

auto state 除外モードを使用して、auto state から除外するポートを指定できます。通常 auto state モードでは、少なくとも VLAN 上のポートが 1 つでもアップしていればレイヤ 3 インターフェイスはアップしたままになります。VLAN 上のポートにロード バランサやファイアウォール サーバなどのアプライアンスが接続されている場合、これらのポートを auto state 機能から除外するように設定して、これらのポートが非アクティブの場合でも転送 Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）がダウンしないようにできます。

auto state 除外モードは、ポートが属するすべての VLAN に影響し、イーサネット、ファスト イーサネット、およびギガビット イーサネット ポートでのみサポートされます。

（注） auto state 除外モードと auto state トラック モードを同じポートに設定できません。

auto state 追跡モード

MSFC への主要な VLAN またはポート接続を追跡するのに auto state 追跡モードを使用できます。auto state 追跡モードを設定する場合、追跡されている接続が VLAN でアップのままであれば SVI はアップのままになります。追跡モードでは、グローバルに追跡される VLAN グループを定義する必要があります。このグループの VLAN は、追跡するメンバー ポートを定義しているかどうかにかかわらず MSFC auto state によって追跡されます。

auto state が追跡する VLAN とポートを設定する際に、少なくとも VLAN 上のイーサネット ポートの 1 つが Spanning-Tree Protocol（STP; スパニングツリー プロトコル）フォワーディング ステートに移行するまで、追跡される SVI はダウンのままになります。逆に言えば、少なくとも 1 つのイーサネット ポートが STP フォワーディング ステートのままであれば追跡される SVI はアップしたままになります。

auto state 追跡モードは、イーサネット、ファスト イーサネット、およびギガビット イーサネット ポートでのみサポートされます。

（注） auto state 除外モードと auto state トラック モードを同じポートに設定できません。

auto state 除外モードの設定

auto state 除外モードを設定するには、イネーブル モードで次の作業のいずれかを行います。

作業	コマンド
auto state 除外モードを設定します。	**set msfcautostate exclude** *mod/port*
auto state 設定を消去します。	**clear msfcautostate** {**all** | *mod/port*}

次に、MSFC auto state からポートを除外する例を示します。

```
Console> (enable) set msfcautostate exclude 3/1
Port 3/1 configured as excluded port
Console> (enable)
```

次に、auto state 設定を消去する例を示します。

```
Console> (enable) clear msfcautostate 3/1
MSFC autostate config cleared on excluded port 3/1
Console> (enable)
```

auto state 追跡モードの設定

auto state 追跡モードを設定するには、イネーブル モードで次の作業のいずれかを行います。

作業	コマンド
指定した VLAN を追跡するように auto state を設定します。	**set msfcautostate track [disable | enable** *vlan_list*]
指定したポートを追跡するように auto state を設定します。	**set msfcautostate track** *mod/port_list*
auto state 追跡モード設定を消去します。	**clear msfcautostate all |** *mod/port*

次に、VLAN 20、21、22、28 を追跡するように auto state を設定する例を示します。

```
Console> (enable) set msfcautostate track enable 20-22,28
Vlans 20-22,28 added to MSFC autostate track vlan group
Console> (enable)
```

次に、モジュール 3 のポート 1 ～ 5 を追跡するように auto state を設定する例を示します。

```
Console> (enable) set msfcautostate track 3/1-5
Port 3/1-5 configured as tracked port
Console> (enable)
```

auto state 設定の表示

MSM に対するライン プロトコル ステートの現在の判定を表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
MSM に対するライン プロトコル ステートの現在の判定を表示します。	**show msmautostate** *mod*

次に、MSM に対するライン プロトコル ステートの現在の判定を表示する例を示します。

```
Console> show msmautostate
MSM Auto port state: enabled
Console>
```

MSFC に対するライン プロトコル ステートの判定を表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
MSFC に対するライン プロトコル ステートの判定を表示します。	**show msfcautostate**

次に、MSFC に対するライン プロトコル ステートの判定を表示する例を示します。

```
Console> (enable) show msfcautostate
MSFC Auto port state: enabled
Excluded ports:
Tracked ports: 3/1-5
Tracked vlans: 20-22,28
Console> (enable)
```

どの MSM インターフェイスで現在 auto state が実行されているか調べるには、MSM プロンプトからイネーブル モードで次の作業を行います。

作業	コマンド
どの MSM インターフェイスで現在 auto state が実行されているかを調べます。	**show autostate entries**

次に、どの MSM インターフェイスで現在 auto state が実行されているか（auto state によってシャットダウンまたは起動されているか）調べる例を示します。

```
Router# show autostate entries
Port-channel1.5
Port-channel1.6
Port-channel1.4
Router#
```

auto state のディセーブル化

MSM がインストール済みの場合に auto state をディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
MSM がインストール済みの場合に auto state をディセーブルにします。	**set msmautostate disable**

auto state はデフォルトでイネーブルに設定されています。次に、MSM がインストール済みの場合に auto state をディセーブルにする例を示します。

```
Console> (enable) set msmautostate disable
MSM port auto state disabled.
Console> (enable)
```

MSFC のライン プロトコル ステートの判定をディセーブルにするには、イネーブル モードで次の作業を行います。

(注) **msfcautostate** コマンドを切り替える（イネーブルからディセーブルに、および / またはディセーブルからイネーブルにする）場合は、**shutdown** および **no shutdown** コマンドを使用して、MSFC 上の VLAN および WAN インターフェイスをディセーブルにしてから再起動する必要があります。正当な理由がないかぎり、MSFC の auto state 機能をディセーブルにしないでください。

作業	コマンド
MSFC のライン プロトコル ステートの判定をディセーブルにします。	**set msfcautostate disable**

次に、MSFC のライン プロトコル ステートの判定をディセーブルにする例を示します。

```
Console> (enable) set msfcautostate disable

MSM port auto state disabled.
Console> (enable)
```

CHAPTER 13

CEF for PFC2 および CEF for PFC3A の設定

この章では、Catalyst 6500 シリーズ スイッチに Cisco Express Forwarding（CEF）for Policy Feature Card 2（PFC2; ポリシー フィーチャ カード 2）および CEF for PFC3 を設定する手順について説明します。

CEF for PFC2 は、Supervisor Engine 2、PFC2、および Multilayer Switch Feature Card 2（MSFC2; マルチレイヤ スイッチ フィーチャ カード 2）に、IP および Internetwork Packet Exchange（IPX）ユニキャスト レイヤ 3 スイッチング、および IP マルチキャスト レイヤ 3 スイッチング機能を提供します。

CEF for PFC3A は、Supervisor Engine 720、PFC3A、および Multilayer Switch Feature Card 3（MSFC3; マルチレイヤ スイッチ フィーチャ カード 3）に、IP ユニキャスト レイヤ 3 スイッチングおよび IP マルチキャスト レイヤ 3 スイッチング機能を提供します。

(注) Supervisor Engine 720（MSFC3）では、IPX ルーティングはソフトウェアを通じて実行されます。

(注) この章で使用しているスーパバイザ エンジン コマンドの構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

この章で説明する内容は、次のとおりです。

(注) PFC1 および MSFC または MSFC2 を装備した Supervisor Engine 1 は、Multilayer Switching（MLS; マルチレイヤ スイッチング）機能付きのレイヤ 3 スイッチングを行います。詳細については、第 14 章「MLS の設定」を参照してください。

(注) Catalyst 5000 ファミリー スイッチで MLS をサポートするように MSFC2 を設定するには、次の URL にある『*Layer 3 Switching Software Configuration Guide*』を参照してください。
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/rel_5_2/layer3/index.htm.

レイヤ 3 スイッチングの機能概要

ここでは、PFC2 によるレイヤ 3 スイッチングについて説明します。

レイヤ 3 スイッチングの概要

(注) Supervisor Engine 720（MSFC3）では、IPX ルーティングはソフトウェアを通じて実行されます。

レイヤ 3 スイッチングにより、ルータではなくスイッチが、VLAN（仮想 LAN）間で IP/IPX ユニキャスト トラフィックおよび IP マルチキャスト トラフィックを転送できます。レイヤ 3 スイッチングはハードウェアに実装され、MSFC2/MSFC3 ではなくスイッチ上で、ワイヤ速度による VLAN 間転送を行います。レイヤ 3 スイッチングを実行するには、MSFC2/MSFC3 からの最低限のサポートが必要です。レイヤ 3 スイッチングが不可能なトラフィックは、MSFC2/MSFC3 がルーティングします。

(注) レイヤ 3 スイッチングは、MSFC2/MSFC3 上に設定されているルーティング プロトコルをサポートしています。レイヤ 3 スイッチングは、MSFC2/MSFC3 上に設定されているルーティング プロトコルに代わるものではありません。レイヤ 3 スイッチングは、Protocol Independent Multicast（PIM）を使用してマルチキャスト ルートの決定を行います。

Catalyst 6500 シリーズ スイッチ上のレイヤ 3 スイッチングは、フロー統計情報を提供します。この情報を利用してトラフィック特性を識別し、管理、プランニング、およびトラブルシューティングに役立てることができます。レイヤ 3 スイッチングでは、NetFlow Data Export（NDE; NetFlow データ エクスポート）を使用してフロー統計情報をエクスポートします。NDE の詳細については、第 16 章「NDE の設定」を参照してください。

(注) トラフィックがレイヤ 3 スイッチングされるのは、VLAN Access Control List（VACL）機能および Quality of Service（QoS; サービス品質）機能によって処理されたあとです。

レイヤ 3 スイッチド パケットの書き換え

(注)　Supervisor Engine 720（MSFC3）では、IPX ルーティングはソフトウェアを通じて実行されます。

VLAN 上の送信元から別の VLAN 上の宛先へパケットをレイヤ 3 スイッチングするとき、スイッチは MSFC2/MSFC3 から学習した情報に基づいて、出力ポートでパケットの書き換えを行います。この書き換えにより、パケットは MSFC2/MSFC3 によってルーティングされたかのように見えます。

(注)　PFC2 または PFC3A は、IP マルチキャスト パケットを転送するだけでなく、必要に応じて適切な VLAN 上でパケットを複製します。

パケットの書き換えによって変更されるフィールドは、次の 5 つです。

- レイヤ 2（MAC［メディア アクセス制御］）宛先アドレス
- レイヤ 2（MAC）送信元アドレス
- レイヤ 3 IP Time to Live（TTL）または IPX トランスポート コントロール
- レイヤ 3 チェックサム
- レイヤ 2（MAC）チェックサム（別名 FCS［フレーム チェックサム］）

(注)　パケットは、次にホップするサブネットに適したカプセル化を使用して書き換えられます。

送信元 A と宛先 B が異なる VLAN に所属し、送信元 A が MSFC2/MSFC3 にパケットを送信して宛先 B へルーティングさせる場合、スイッチはそのパケットが MSFC2/MSFC3 のレイヤ 2（MAC）アドレスに送信されたことを認識します。

レイヤ 3 スイッチングを実行するため、スイッチはレイヤ 2 フレーム ヘッダーを書き換え、レイヤ 2 宛先アドレスを宛先 B のレイヤ 2 アドレスに変更し、レイヤ 2 送信元アドレスを MSFC2/MSFC3 のレイヤ 2 アドレスに変更します。レイヤ 3 アドレスは変更しません。

IP ユニキャストおよび IP マルチキャスト トラフィックの場合、スイッチはレイヤ 3 TTL 値を 1 だけ減らし、レイヤ 3 パケット チェックサムを再計算します。IPX トラフィックの場合、スイッチはレイヤ 3 トランスポート コントロール値を 1 だけ増やし、レイヤ 3 パケット チェックサムを再計算します。スイッチはレイヤ 2 フレーム チェックサムを再計算し、書き換えたパケットを宛先 B の VLAN に転送します（または、マルチキャスト パケットの場合、必要に応じて複製します）。

ここでは、パケットを書き換える手順について説明します。

- IP ユニキャストの書き換え（p.13-4）
- IPX ユニキャストの書き換え（p.13-4）
- IP マルチキャストの書き換え（p.13-5）

IP ユニキャストの書き換え

受信 IP ユニキャスト パケットのフォーマットは、（概念的には）次のとおりです。

レイヤ 2 フレーム ヘッダー		レイヤ 3 IP ヘッダー				データ	FCS
宛先	送信元	宛先	送信元	TTL	チェックサム		
MSFC2/MSFC3 MAC	*Source A MAC*	*Destination B IP*	*Source A IP*	*n*	*calculation1*		

スイッチが IP ユニキャスト パケットの書き換えを行ったあとのフォーマットは、（概念的には）次のとおりです。

レイヤ 2 フレーム ヘッダー		レイヤ 3 IP ヘッダー				データ	FCS
宛先	送信元	宛先	送信元	TTL	チェックサム		
Destination B MAC	*MSFC2/MSFC3 MAC*	*Destination B IP*	*Source A IP*	*n–1*	*calculation2*		

IPX ユニキャストの書き換え

受信 IPX パケットのフォーマットは、（概念的には）次のとおりです。

レイヤ 2 フレーム ヘッダー		レイヤ 3 IPX ヘッダー			データ	FCS
宛先	送信元	チェックサム / IPX の長さ / トランスポート コントロール	宛先ネットワーク / ノード / ソケット	送信元ネットワーク / ノード / ソケット		
MSFC2 MAC	*Source A MAC*	*n*	*Destination B IPX*	*Source A IPX*		

スイッチが IPX パケットの書き換えを行ったあとのフォーマットは、（概念的には）次のとおりです。

レイヤ 2 フレーム ヘッダー		レイヤ 3 IPX ヘッダー			データ	FCS
宛先	送信元	チェックサム / IPX の長さ / トランスポート コントロール	宛先ネットワーク / ノード / ソケット	送信元ネットワーク / ノード / ソケット		
Destination B MAC	*MSFC2 MAC*	*n+1*	*Destination B IPX*	*Source A IPX*		

IP マルチキャストの書き換え

受信 IP マルチキャスト パケットのフォーマットは、（概念的には）次のとおりです。

レイヤ 2 フレーム ヘッダー		レイヤ 3 IP ヘッダー				データ	FCS
宛先	送信元	宛先	送信元	TTL	チェックサム		
Group G1 MAC[1]	*Source A MAC*	*Group G1 IP*	*Source A IP*	*n*	*calculation1*		

1. 上記の例では、Destination B はグループ G1 のメンバーです。

スイッチが IP マルチキャスト パケットの書き換えを行ったあとのフォーマットは、（概念的には）次のとおりです。

レイヤ 2 フレーム ヘッダー		レイヤ 3 IP ヘッダー				データ	FCS
宛先	送信元	宛先	送信元	TTL	チェックサム		
Group G1 MAC	*MSFC2/MSFC3 MAC*	*Group G1 IP*	*Source A IP*	*n–1*	*calculation2*		

CEF for PFC2/PFC3A の概要

（注）　Supervisor Engine 720（MSFC3）では、IPX ルーティングはソフトウェアを通じて実行されます。

ここでは、CEF for PFC2/PFC3A について説明します。

CEF for PFC2/PFC3A の概要

Supervisor Engine 2、PFC2、および MSFC2 は、CEF for PFC2 によってレイヤ 3 スイッチングを行います。CEF for PFC2 は、Supervisor Engine 2 では永続的にイネーブルになっています。MSFC2 では、CEF for PFC2 のサポートのために Cisco IOS CEF が永続的にイネーブルになっています。

Supervisor Engine 720、PFC3A、および MSFC3 は、CEF for PFC3A によってレイヤ 3 スイッチングを行います。CEF for PFC3A は、Supervisor Engine 720 では永続的にイネーブルになっています。MSFC3 では、CEF for PFC3A のサポートのために Cisco IOS CEF が永続的にイネーブルになっています。

CEF for PFC2/PFC3A は、MSFC2/MSFC3 上の CEF（ユニキャスト トラフィック用）および PIM（マルチキャスト トラフィック用）と連携して、IP、IP マルチキャスト、および IPX トラフィックをサポートします。MSFC2/MSFC3 上の CEF および PIM は、CEF for PFC2/PFC3A サポートのために機能拡張されています。CEF for PFC2/PFC3A はレイヤ 3 スイッチド トラフィックのフロー統計情報を生成します。この情報は CLI（コマンドライン インターフェイス）で表示することも、NDE に使用することもできます。

CEF for PFC2/PFC3A は、完全な Forwarding Information Base（FIB; 転送情報ベース）エントリ（「FIB」[p.13-6] を参照）に一致するすべてのパケットについて、レイヤ 3 スイッチングを行います。CEF for PFC2/PFC3A は、不完全な FIB エントリ（MAC アドレスが解決されていないエントリ）に一致するパケットを、すべて MSFC2/MSFC3 に送信し、MSFC2/MSFC3 が MAC アドレスを解決するまでルーティングさせます。

（注） CEF for PFC2/PFC3A は、レイヤ 2 でアドレス指定されたブリッジ トラフィックを MSFC2/MSFC3 に送信して処理させます。

（注） Access Control List（ACL; アクセス制御リスト）および Policy-Based Routing（PBR）により、CEF for PFC2/PFC3A が転送の決定を行う際、FIB が無視されることがあります（「転送の決定」[p.13-6] を参照）。

転送の決定

CEF for PFC2/PFC3A は、次の事項に基づいてレイヤ 3 スイッチングを行います。

- ポリシー ベース ルーティング決定のための ACL Ternary CAM（TCAM）エントリ
- TCP 代行受信および再帰 ACL 転送の決定のための NetFlow テーブル エントリ（「NetFlow 統計情報の概要」[p.13-11] を参照）
- その他すべての転送決定のための FIB および隣接テーブル エントリ

転送の決定に使用されるエントリに関する情報を表示するには、**show mls entry** コマンドを使用します。CEF for PFC2/PFC3A は、各パケットについて転送決定を行い、各パケットに関する書き換え情報を出力ポートに送信します。パケットがスイッチから送信される際、ポート上で書き換えが行われます。

FIB

FIB は、個別の TCAM に格納されます。隣接テーブルは、DRAM に個別に保存されます。NetFlow テーブルは、DRAM に個別に保存されます。FIB、隣接テーブル、および NetFlow テーブルは、格納スペースをめぐって他の機能と競合することはありません。

FIB は、概念的にはルーティング テーブルと類似しています。FIB は、MSFC2/MSFC3 上のユニキャストおよびマルチキャスト ルーティング テーブルに含まれている転送情報のミラー イメージを維持しています。ネットワーク上でルーティングまたはトポロジーの変化が発生すると、MSFC2/MSFC3 上のユニキャストおよびマルチキャスト ルーティング テーブルが更新され、その変更が FIB に反映されます。FIB は MSFC2/MSFC3 上のルーティング テーブルの情報に基づいて、ネクストホップ アドレス情報を維持します。FIB は 256,000 のエントリをサポートしています。これには、16,000 の IP マルチキャスト エントリ（MSFC3 では 128,000 の IP マルチキャスト エントリ）が含まれます。Reverse Path Forwarding（RPF）チェックがイネーブルの場合、IP エントリ数は 2 倍になります（Supervisor Engine 720 では、IP エントリ数は変わりません）。

FIB 検索機能が使用する基準は、次のとおりです。

- IP ユニキャスト用の宛先 IP アドレス
- IPX ユニキャスト用の宛先 IPX ネットワーク
- RPF チェックによる IP ユニキャスト用の送信元および宛先 IP アドレス
- RPF チェックによる IP マルチキャスト用の送信元および宛先 IP アドレス

(注) FIB は MSFC2/MSFC3 上のユニキャストおよびマルチキャスト ルーティング テーブルをミラーリングしているので、MSFC2/MSFC3 上でユニキャストまたはマルチキャスト ルーティング テーブルを変更するコマンドを実行すると、FIB にも影響が及びます。Supervisor Engine 2 または Supervisor Engine 720 の CLI から転送エントリを削除することはできません。

冗長スーパバイザ エンジンおよび MSFC2/MSFC3 が搭載されたスイッチ内のメイン MSFC2/MSFC3 は、アクティブな Supervisor Engine 2 または Supervisor Engine 720 の FIB をサポートしています。非メイン MSFC2/MSFC3 上のルーティング プロトコルは、メイン MSFC2/MSFC3 上のルーティング プロトコルに情報を送信します。

show mls entry cef コマンドを実行すると、次の情報が表示されます。

- FIB をサポートしている MSFC のモジュール番号
- FIB エントリのタイプ（receive、connected、resolved、drop、wildcard、または default）
- 宛先アドレス（IP アドレスまたは IPX ネットワーク）
- 宛先マスク
- ネクストホップ アドレス（IP アドレスまたは IPX ネットワーク）
- ネクストホップ マスク
- ネクストホップ負荷分散ウエイト

```
Console> (enable) show mls entry cef
Mod FIB-Type  Destination-IP  Destination-Mask NextHop-IP      Weight
--- --------- --------------- ---------------- --------------- ------
 15 receive   0.0.0.0         255.255.255.255
 15 receive   255.255.255.255 255.255.255.255
 15 receive   127.0.0.0       255.255.255.255
 15 receive   127.0.0.52      255.255.255.255
 15 receive   127.255.255.255 255.255.255.255
 15 receive   10.1.1.2        255.255.255.255
 15 receive   10.1.1.0        255.255.255.255
 15 receive   10.1.1.255      255.255.255.255
 15 receive   10.10.1.1       255.255.255.255
 15 receive   10.10.0.0       255.255.255.255
.
.
.
Console> (enable)
```

レイヤ 3 スイッチングの要約を表示するには、**show mls** コマンドを使用します。

```
Console> (enable) show mls
Total packets switched = 35254
Total bytes switched = 2256256
Total routes = 120569
Total number of Netflow entries = 120000

IP statistics flows aging time = 50 seconds
Long-duration flows aging time = 320 seconds
IP statistics flows fast aging time = 0 seconds, packet threshold = 0

IP Current flow mask is Full-Vlan flow
Netflow Data Export version: 7
Netflow Data Export disabled
Netflow Data Export port/host is not configured.
Total packets exported = 0
Destination Ifindex export is enabled
Source Ifindex export is enabled
Rate limiting is turned off, packets are bridged to router
Load balancing hash is based on source and destination IP addresses and universc
Per-prefix Stats for ALL FIB entries is Enabled
Console> (enable)
```

隣接テーブル

CEF for PFC2/PFC3A は、FIB エントリごとに、メイン MSFC2/MSFC3 から提供される隣接ノードに関するレイヤ 2 情報を隣接テーブルに格納します。隣接ノードとは、レイヤ 2 で直接接続されているノードです。CEF for PFC2/PFC3A はトラフィック転送のため、FIB エントリから（隣接エントリをポイントする）ルートを選択し、隣接テーブル エントリに示されている隣接ノードのレイヤ 2 ヘッダーを使用して、レイヤ 3 スイッチング時にパケットを書き換えます。CEF for PFC2 は 256,000 個の隣接テーブル エントリをサポートしています。CEF for PFC3A は 1,000,000 個の隣接テーブル エントリをサポートしています。統計情報を提供するのは、隣接テーブル エントリの半分だけです。

表 13-1 に、隣接タイプを示します。

表 13-1　隣接タイプ

隣接タイプ	説明
connect	完全な書き換え情報を含むエントリ タイプ
punt	MSFC2/MSFC3 にトラフィックを送信するエントリ
no r/w	書き換え情報が不完全な場合に MSFC2/MSFC3 にトラフィックを送信するエントリ
frc drp	ARP スロットリングに起因してパケットを廃棄するために使用するエントリ
drop、null、loopbk	パケットを廃棄するために使用するエントリ

show mls entry cef adjacency コマンドを実行すると、次の情報が表示されます。

- FIB の情報（「FIB」[p.13-6] を参照）
- 隣接タイプ（connect、drop、null、loopbk、frc drp、punt、no r/w）
- ネクストホップ MAC アドレス
- ネクストホップ VLAN
- ネクストホップ カプセル化
- 対応する FIB エントリからこの隣接に送信されたパケット数
- 対応する FIB エントリからこの隣接に送信されたバイト数

```
Console> (enable) show mls entry cef adjacency
Mod:                15
Destination-IP:     140.140.1.5        Destination-Mask:   255.255.255.255
FIB-Type:           resolved

AdjType  NextHop-IP      NextHop-Mac       Vlan Encp Tx-Packets   Tx-Octets
-------- --------------- ----------------- ---- ---- ------------ -------------
connect  140.140.1.5     00-00-d0-00-00-05  140 ARPA            0             0

Mod:                15
Destination-IP:     150.150.1.5        Destination-Mask:   255.255.255.255
FIB-Type:           resolved

AdjType  NextHop-IP      NextHop-Mac       Vlan Encp Tx-Packets   Tx-Octets
-------- --------------- ----------------- ---- ---- ------------ -------------
connect  150.150.1.5     00-00-e0-00-00-05  150 ARPA            0             0

Mod:                15
Destination-IP:     153.153.1.5        Destination-Mask:   255.255.255.255
FIB-Type:           resolved

AdjType  NextHop-IP      NextHop-Mac       Vlan Encp Tx-Packets   Tx-Octets
-------- --------------- ----------------- ---- ---- ------------ -------------
connect  153.153.1.5     00-00-e3-00-00-05  153 ARPA            0             0
.
.
.
Console> (enable)
```

CEF 隣接情報を消去するには、**clear mls entry cef adjacency** コマンドを実行します。

```
Console> (enable) clear mls entry cef adjacency
Adjacency statistics has been cleared.
Console> (enable)
```

マルチキャスト フローの部分的スイッチングおよび完全スイッチング

次の状況では、一部のフローが完全にレイヤ 3 スイッチングされずに、部分的にレイヤ 3 スイッチングされる可能性があります。

- マルチキャスト送信元の RPF インターフェイス上で、MSFC2/MSFC3 が IP マルチキャスト グループのメンバーとして設定されている場合（**ip igmp join-group** コマンドを使用）
- MSFC2/MSFC3 が PIM sparse モードの送信元への第 1 ホップ ルータである場合（この場合、MSFC2/MSFC3 は Rendevous Point [RP; ランデブー ポイント] に PIM-register メッセージを送信しなければなりません）
- フローの出力インターフェイス上にマルチキャスト TTL スレッシュホールドが設定されている場合
- フローの RPF インターフェイスにマルチキャスト ヘルパーが設定されていて、かつマルチキャストからブロードキャストへの変換が必要な場合
- 出力インターフェイス上にマルチキャスト タグ スイッチングが設定されている場合
- インターフェイス上で Network Address Translation（NAT; ネットワーク アドレス変換）が設定されていて、かつ発信インターフェイスのために送信元アドレスの変換が必要な場合

（注） RPF インターフェイスの拡張アクセス リスト拒否条件でレイヤ 3 送信元、レイヤ 3 宛先、または IP プロトコル以外の何か（レイヤ 4 ポート番号など）が指定されていれば、CEF for PFC2/PFC3A はレイヤ 3 スイッチングを提供します。

部分的にスイッチングされるフローでは、そのフローに所属するすべてのマルチキャスト トラフィックが MSFC2/MSFC3 に到達し、レイヤ 3 スイッチングの対象にならないインターフェイスについてはソフトウェア スイッチングが行われます。

（注） すべての（*,G）フローは、常に部分的にレイヤ 3 スイッチングされます。

PFC2/PFC3A は、完全にレイヤ 3 スイッチングされたフロー内のマルチキャスト トラフィックが MSFC2/MSFC3 に到達しないようにし、MSFC2/MSFC3 上の負荷を減らします。**show ip mroute** および **show mls ip multicast** コマンドは、完全にレイヤ 3 スイッチングされるフローを文字列 [RPF-MFD] で識別します。Multicast Fast Drop（MFD）は、MSFC2/MSFC3 側から見た場合、マルチキャスト パケットが PFC2/PFC3A によってスイッチングされたために廃棄されたことを示します。

完全にレイヤ 3 スイッチングされるすべてのフローでは、PFC2/PFC3A はマルチキャスト パケットおよびバイト カウント統計情報を定期的に MSFC2/MSFC3 に送信します。MSFC2/MSFC3 は完全にスイッチングされるフローを確認することができず、マルチキャスト統計情報を記録できないためです。MSFC2/MSFC3 はこの統計情報を使用して、対応するマルチキャスト ルーティング テーブル エントリを更新し、適切な期限タイマーをリセットします。

CEF for PFC2/PFC3A の例

図 13-1 に、単純な IP CEF ネットワーク トポロジーを示します。この例では、ホスト A は販売部門の VLAN（IP サブネット 171.59.1.0）、ホスト B はマーケティング部門の VLAN（IP サブネット 171.59.3.0）、ホスト C はエンジニアリング部門の VLAN（IP サブネット 171.59.2.0）にあります。

ホスト A がホスト C に対して HTTP ファイル転送を開始すると、PFC2/PFC3A は FIB および隣接テーブルの情報を使用して、ホスト A からホスト C にパケットを転送します。

図 13-1　IP CEF トポロジーの例

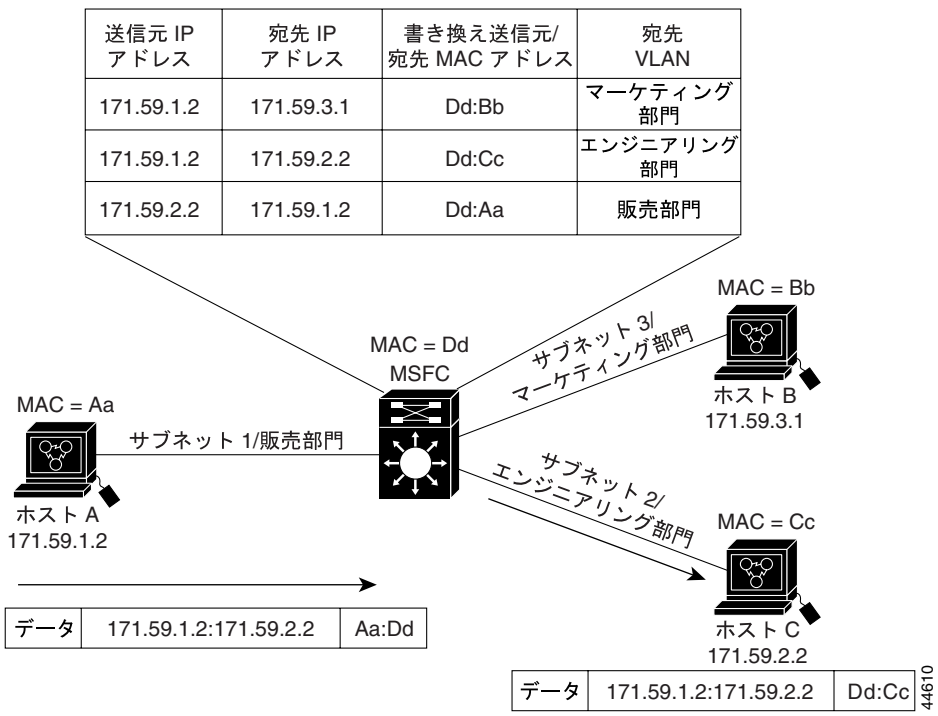
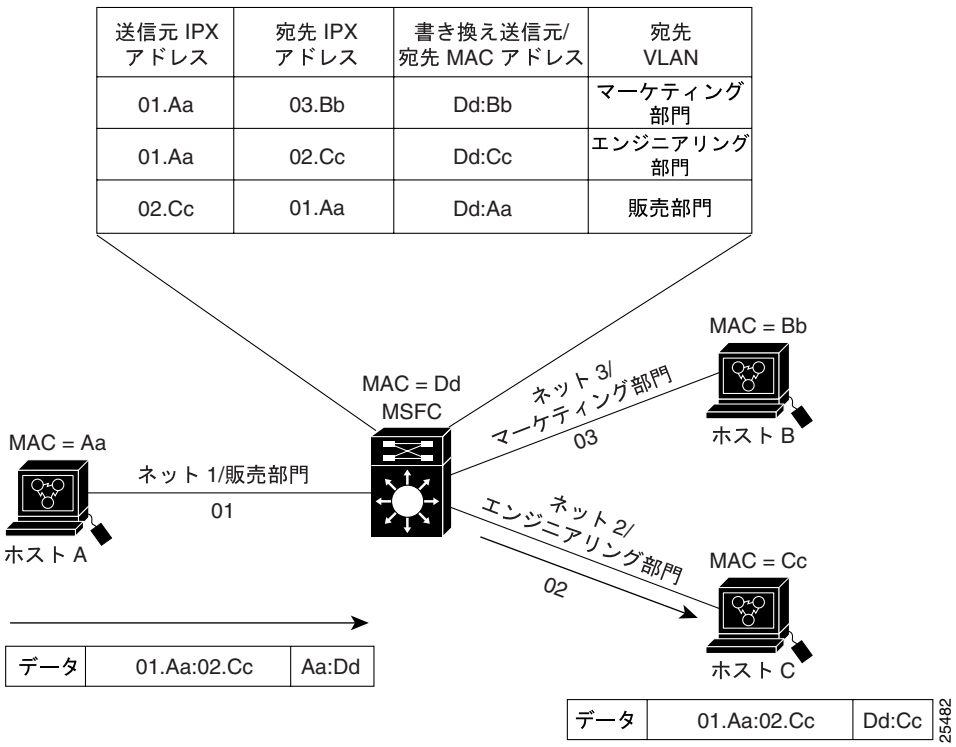


図 13-2 に、単純な IPX CEF ネットワーク トポロジーを示します。この例では、ホスト A は販売部門の VLAN（IPX アドレス 01.Aa）、ホスト B はマーケティング部門の VLAN（IPX アドレス 03.Bb）、ホスト C はエンジニアリング部門の VLAN（IPX アドレス 02.Cc）にあります。

ホスト A がホスト C に対してファイル転送を開始すると、PFC2 は FIB および隣接テーブルの情報を使用して、ホスト A からホスト C にパケットを転送します。

図 13-2　IPX CEF トポロジーの例



NetFlow 統計情報の概要

（注）　Supervisor Engine 720（MSFC3）では、IPX ルーティングはソフトウェアを通じて実行されます。

ここでは、NetFlow 統計情報について説明します。

- NetFlow 統計情報の概要（p.13-11）
- NetFlow テーブル エントリのエージング（p.13-12）
- フロー マスク（p.13-12）

NetFlow 統計情報の概要

CEF for PFC2/PFC3A は、レイヤ 3 スイッチングされるトラフィックに関するフロー統計を生成し、NetFlow テーブルに格納します。NetFlow 統計情報は、**show** コマンドで表示することができ、さらに NDE でも使用できます。

(注) NetFlow テーブルのエントリ数が 32,000 を超えると、統計情報の格納スペースが不足する可能性が高くなります。NetFlow テーブルのエントリ数を減らす方法として、統計情報から特定の IP プロトコルを除外するか、最小粒度のフロー マスクを使用することができます（「NetFlow テーブルからの IP プロトコル エントリの除外」[p.13-30] を参照）。

NetFlow 統計情報は、次のようにユニキャストおよびマルチキャスト フローをサポートします。

- ユニキャスト フローは、次のいずれかです。
  - destination only：特定の IP 宛先に向けられたすべてのトラフィック
  - destination-source：特定の IP 送信元から特定の IP 宛先に向けられたすべてのトラフィック
  - full-flow：特定の IP 送信元から特定の IP 宛先に向けられ、プロトコルおよびトランスポート レイヤ情報が共通するすべてのトラフィック
- マルチキャスト フローは、特定の送信元から特定の宛先マルチキャスト グループのメンバーに向けられ、プロトコルおよびトランスポート レイヤ情報が共通するすべてのトラフィックです。

NetFlow テーブル エントリのエージング

パケット トラフィックがアクティブであるかぎり、フローの状態およびアイデンティティが維持されます。フローのトラフィックがなくなると、エントリは期限切れになります。NetFlow テーブルに保存される NetFlow テーブル エントリのエージング タイムを設定できます。あるエントリが一定期間にわたって使用されない状態が続くと、そのエントリは期限切れになり、そのフローに関する統計情報をフロー コレクタ アプリケーションにエクスポートできるようになります。

フロー マスク

フロー マスクは、NetFlow テーブル エントリの作成方法を決定します。CEF for PFC2 は、すべての統計情報について 1 つのフロー マスク（最も固有性の高いマスク）だけをサポートします。NetFlow for PFC2 がレイヤ 3 スイッチングの実行対象となる MSFC 別に異なるフロー マスクを検出した場合、検出したフロー マスクの中で最も固有性の高いものにフロー マスクを変更します（これは、PFC2/MSFC2 にのみ当てはまります）。

フロー マスクが変化すると、NetFlow テーブル全体が除去されます。CEF for PFC2/PFC3A がキャッシングしたエントリをエクスポートするとき、現在のフロー マスクに基づいてフロー レコードが作成されます。現在のフロー マスクによっては、フロー レコードの一部のフィールドに値が入らない場合があります。サポートされていないフィールドには、ゼロ（0）が充填されます。

統計情報フロー マスクは、次のとおりです。

- destination-ip ― IP 用の最も固有性の低いマスク
- destination-ipx ― IPX 用の唯一のフロー マスク
- source-destination-ip ― IP 用
- source-destination-vlan ― IP マルチキャスト用
- full flow ― 最も固有性の高いフロー マスク
- full vlan ― full flow と送信元 VLAN を合わせたものと同じフィールド

NetFlow テーブルの内容および現在のフロー マスクを表示するには、**show mls statistics entry** コマンドを使用します。キーワード オプションを使用して、特定トラフィックの情報を表示できます（詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照）。

CEF for PFC2/PFC3A のデフォルト設定

表 13-2 に、CEF for PFC2/PFC3A のデフォルト設定を示します。

表 13-2　CEF for PFC2/PFC3A のデフォルト設定

機能	デフォルト値
CEF for PFC2 のイネーブル ステート	イネーブル（ディセーブルにはできません）
MSFC2/MSFC3 上の CEF イネーブル ステート	イネーブル（ディセーブルにはできません）
マルチキャスト サービス（IGMP スヌーピング）	イネーブル
マルチキャスト サービス（GMRP）	ディセーブル
MSFC2/MSFC3 上のマルチキャスト ルーティング	グローバルにディセーブル
MSFC2/MSFC3 上の PIM ルーティング	すべてのインターフェイス上でディセーブル
IP MMLS スレッシュホールド	設定なし ― デフォルト値なし
IP MMLS	マルチキャスト ルーティングおよび Internet Group Management Protocol（IGMP）スヌーピングがイネーブルの場合、イネーブル

CEF for PFC2/PFC3A 設定時の注意事項と制限事項

（注） Supervisor Engine 720（MSFC3）では、IPX ルーティングはソフトウェアを通じて実行されます。

ここでは、CEF for PFC2/PFC3A 設定時の注意事項と制限事項について説明します。

- CEF for PFC2 は、最大 16 の固有 Hot Standby Router Protocol（HSRP）グループ番号をサポートしています。異なる VLAN 上で同じ HSRP グループ番号を使用できます。16 を超える HSRP グループを設定すると、この制限により HSRP グループ番号として VLAN 番号を使用できなくなります。

  （注） 同じ番号の HSRP グループは、同じ仮想 MAC アドレスを使用しますが、これが、MSFC 上でブリッジを設定する場合にエラーを引き起こす可能性があります。

- 16 の固有 HSRP グループ番号という制限のため、CEF for PFC2 では **standby use-bia** HSRP コマンドを使用できません。
- PFC3A は、256 の HSRP グループをサポートしています。
- CEF for PFC2 は、次の入力および出力カプセル化をサポートしています。

  （注） CEF for PFC3A は、イーサネット V2.0（ARPA）のみをサポートしています。

— IP ユニキャストの場合：
イーサネット V2.0（ARPA）
802.3 および 1 バイト制御（SAP1）による 802.2
802.3 および 802.2 と SNAP

— IPX の場合：
イーサネット V2.0（ARPA）
802.3（ロー）
1 バイト制御（SAP1）による 802.2
SNAP

（注） IPX トラフィック用の入力カプセル化が SAP1 の場合、出力カプセル化も SAP1 でないかぎり、CEF for PFC2 はレイヤ 3 スイッチングを行いません。MSFC2 はカプセル化の変更が必要な IPX SAP1 トラフィックをルーティングします。

— IP マルチキャストの場合 — イーサネット V2.0（ARPA）

次の場合には、CEF for PFC2/PFC3A は IP マルチキャスト フローに対するレイヤ 3 スイッチングを行いません。

- 224.0.0.*（* は 0 ～ 255）の範囲の IP マルチキャスト グループ。これらのグループは、ルーティング プロトコルが使用します。CEF for PFC2/PFC3A がサポートする範囲は、225.0.0.* ～ 239.0.0.* および 224.128.0.* ～ 239.128.0.* です。

（注） 224.0.0.* の範囲のグループはルーティング コントロール パケット用に予約されており、VLAN のすべての転送ポートにフラッディングする必要があります。これらのアドレスは、マルチキャスト MAC アドレス範囲 01-00-5E-00-00-*xx*（*xx* は 0 ～ 0xFF）にマッピングされます。

- PIM 自動 RP マルチキャスト グループ（IP マルチキャスト グループ アドレス 224.0.1.39 および 224.0.1.40）。

（注） 冗長 MSFC2/MSFC3 を装備したシステムの場合、PIM インターフェイス コンフィギュレーションは、アクティブ MSFC2/MSFC3 と冗長 MSFC2/MSFC3 の両方で同じでなければなりません。

- インターフェイスまたはグループが PIM sparse モードで動作しているとき、フローの Shortest-Path Tree（SPT）ビットが消去されている場合。
- フラグメント化された IP パケットおよび IP オプション付きのパケット。ただし、フローの中でフラグメント化されていないパケット、または IP オプションを指定されていないパケットは、マルチレイヤ スイッチングの対象になります。
- トンネル インターフェイス上で受信した送信元トラフィック（MBONE トラフィックなど）。
- マルチキャスト タグ スイッチングがイネーブルに設定された RPF インターフェイス。

スイッチ上での CEF for PFC2/PFC3A の設定

ここでは、CEF for PFC2/PFC3A を設定する手順を説明します。

（注）　MSFC2/MSFC3 上でのルーティングの設定手順については、第 12 章「VLAN 間ルーティングの設定」を参照してください。

スーパバイザ エンジン上でのレイヤ 3 スイッチング エントリの表示

CEF for PFC2/PFC3A は、PFC2 および MSFC2 を装備した Supervisor Engine 2、PFC3A および MSFC3 を装備した Supervisor Engine 720 上で永続的にイネーブルです。設定作業は必要ありません。

スーパバイザ エンジン上のレイヤ 3 スイッチング エントリをすべて表示するには、次の作業を行います。

作業	コマンド
レイヤ 3 スイッチング情報を表示します。	**show mls entry** [**pbr-route**] [**cef**] | [**netflow-route**] [**qos**]

次に、レイヤ 3 スイッチング エントリを表示する例を示します。

```
Console> (enable) show mls entry
Mod FIB-Type  Destination-IP  Destination-Mask NextHop-IP      Weight
--- --------- --------------- ---------------- --------------- ------
 15 receive   0.0.0.0         255.255.255.255
 15 receive   255.255.255.255 255.255.255.255
 15 receive   127.0.0.12      255.255.255.255
 16 receive   127.0.0.0       255.255.255.255
 16 receive   127.255.255.255 255.255.255.255
 15 resolved  127.0.0.11      255.255.255.255  127.0.0.11           1
 15 receive   21.2.0.4        255.255.255.255
 16 receive   21.0.0.0        255.255.255.255
 16 receive   21.255.255.255  255.255.255.255
 15 receive   44.0.0.1        255.255.255.255
 16 receive   44.0.0.0        255.255.255.255
 16 receive   44.255.255.255  255.255.255.255
 15 receive   42.0.0.1        255.255.255.255
 16 receive   42.0.0.0        255.255.255.255
 16 receive   42.255.255.255  255.255.255.255
 15 receive   43.0.0.99       255.255.255.255
 15 receive   43.0.0.0        255.255.255.255
 15 receive   43.255.255.255  255.255.255.255
 15 receive   192.20.20.20    255.255.255.255
 16 receive   21.2.0.5        255.255.255.255
 16 receive   42.0.0.20       255.255.255.255
 15 connected 43.0.0.0        255.0.0.0
 15 drop      224.0.0.0       240.0.0.0
 15 wildcard  0.0.0.0         0.0.0.0
```

```
Mod FIB-Type  Dest-IPX-net NextHop-IPX                Weight
--- --------- ------------ -------------------------- ------
 15 connected 21
 15 connected 44
 15 connected 42
 15 resolved  450          42.0050.3EA9.ABFD              1
 15 resolved  480          42.0050.3EA9.ABFD              1
 15 wildcard  0

Destination-IP  Source-IP       Prot  DstPrt SrcPrt Destination-Mac   Vlan EDst
Stat-Pkts  Stat-Bytes  Uptime   Age      TcpDltSeq TcpDltAck
--------------- --------------- ----- ------ ------ ----------------- ---- ----
---------- ------------ -------- -------- --------- ---------
0.0.0.5         0.0.0.5         5     204    104    cc-cc-cc-cc-cc-cc 5    ARPA 0
0           01:03:18 01:00:51 cccccccc  cccccccc
0.0.0.2         0.0.0.2         2     201    101    cc-cc-cc-cc-cc-cc 2    ARPA 0
0           01:03:21 01:00:51 cccccccc  cccccccc
0.0.0.4         0.0.0.4         4     203    X      cc-cc-cc-cc-cc-cc 4    ARPA 0
0           01:03:19 01:00:51 cccccccc  cccccccc
0.0.0.1         0.0.0.1         ICMP  200    100    cc-cc-cc-cc-cc-cc 1    ARPA 0
0           01:03:25 01:00:52 cccccccc  cccccccc
0.0.0.3         0.0.0.3         3     202    102    cc-cc-cc-cc-cc-cc 3    ARPA 0
0           01:03:20 01:00:52 cccccccc  cccccccc
0.0.0.6         0.0.0.6         TCP   205    105    cc-cc-cc-cc-cc-cc 6    ARPA 0
0           01:03:18 01:00:52 cccccccc  cccccccc
Console> (enable)
```

FIB エントリだけを表示するには、**show mls entry cef** コマンドを使用します。TCP 代行受信機能および再帰 ACL のエントリだけを表示するには、**show mls entry netflow-route** コマンドを使用します。PBR エントリだけを表示するには、**show mls entry pbr-route** コマンドを使用します。QoS エントリだけを表示するには、**show mls entry qos** コマンドを使用します。

MSFC2/MSFC3 上での CEF の設定

CEF は、MSFC2/MSFC3 上で永続的にイネーブルに設定されています。CEF for PFC2/PFC3A をサポートするための設定作業は必要ありません。

（注） MSFC2/MSFC3 上で実行する **ip load-sharing per-packet**、**ip cef accounting per-prefix**、および **ip cef accounting non-recursive** の各 Cisco IOS CEF コマンドは、MSFC2/MSFC3 上で CEF にスイッチングされるトラフィックだけに適用されます。これらのコマンドは、スーパバイザ エンジン上で CEF for PFC2/PFC3A によってスイッチングされるトラフィックには影響しません。

CEF 最大ルートの指定

（注） この機能を使用できるのは、Supervisor Engine 720 だけです。

FIB TCAM にプログラミング可能な最大ルート数をプロトコルに対して指定するには、**set mls cef maximum-routes** {**ip** | **ip-multicast**} *routes* コマンドを使用します。構文は次のとおりです。

- ip ― IP MLS を指定します。
- ip-multicast ― IP マルチキャスティング MLS を指定します。
- routes ― FIB TCAM にプログラム可能なルート数を指定します。

FIB TCAM にプログラミングできる最大ルート数を指定する場合は、次の注意事項に従ってください。

- 指定ルート数を超えるルートは、ハードウェアに導入されません。これらのルートを使用するパケットは、MSFC でスイッチングされます。ルート引数は 1,000 エントリ単位です。ルート引数を 0 に設定すると、システムによって決定されるデフォルト値に戻ります。
- プロトコルを設定しない場合は、初期のデフォルト値が各プロトコルに割り当てられます。少なくとも 1 つのプロトコルが設定されている場合は、システムが残りのスペースをその他の未割り当てプロトコルに割り当てようとするため、未割り当てプロトコルのデフォルト値が変更されることがあります。

このコマンドには次のような特長があります。

- 設定変更が有効になるのは、アクティブ スーパバイザ エンジンを再起動したあとのみです。スイッチオーバーが発生しても、変更は有効になりません。
- スタンバイ スーパバイザ エンジンの設定は、アクティブ スーパバイザ エンジンと同期化されます。スタンバイ スーパバイザ エンジンが搭載されている場合は、アクティブ スーパバイザ エンジンの起動設定と新規設定（存在する場合）がスタンバイ スーパバイザ エンジンと同期化します。スタンバイ スーパバイザ エンジンは起動設定を使用して、FIB TCAM を設定します。元の起動設定がアクティブ スーパバイザ エンジンの起動設定と異なる場合は、スタンバイ スーパバイザ エンジンをリセットしなければならないことがあります。この場合は、アクティブ スーパバイザ エンジンのコンソールに情報メッセージ（FIB_MAXROUTES_RESET）が出力されます。
- TCAM を最大限に利用するには、IP ユニキャストの最大ルート数を 16,000 の倍数に設定して、IP マルチキャストの最大ルート数を 8,000 の倍数に設定してください。内部割り当て方式では、ユニキャスト割り当て単位として 16,000 を、マルチキャスト割り当て単位として 8,000 を使用しています。たとえば、IP ユニキャストが 1,000 に設定されている場合、16,000 のエントリが予約されますが、許可されるのは 1,000 のみです。
- 最大ルート数を超過するか、またはプロトコルに割り当てられた TCAM スペースが一杯になると、システム メッセージ（FIB_ALLOC_TCAM_FULL）が表示されます。内部ソフトウェア割り当て方式が原因で、最大ルート数を超過する前に、割り当てられた TCAM スペースが一杯になることがあります。

（注） すべてのプロトコルの最大ルート数の合計が 256,000 を超えることはありません。

（注） すべてのプロトコルのルート数が 0 に設定されている場合は、起動時のデフォルトが使用されます。特定のプロトコルのルート数をゼロ以外の値に設定すると、他のプロトコルのデフォルト値が残りのサイズに変更されます。

（注） MLS プロトコルに最大ルート数が設定されていない場合、システムによって決定されるデフォルト値が表示されます。未割り当てプロトコルに残りのスペースが割り当てられるため、プロトコルのデフォルト値が固定されないことがあります。起動後に最大ルート数の設定が変更された場合に、**show mls cef maximum-routes** コマンドを使用すると、2 種類の情報が表示されます。1 つは現在の（起動）設定で、もう 1 つは再起動後に有効になる新規設定です。

FIB TCAM にプログラミングできるプロトコルの最大ルート数を指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
FIB TCAM にプログラミングできるプロトコルの最大ルート数を指定します。	**set mls cef maximum-routes** {**ip** | **ip-multicast**} *routes*
MLS プロトコルごとに設定された最大ルート数を表示します。	**show mls cef maximum-routes**

次に、IP ユニキャストの最大ルート数を指定する例を示します。

```
Console> (enable) set mls cef maximum-routes ip 220
Configuration change will take effect after next reboot.
Console> (enable) show mls cef maximum-routes
Current:
    IPv4           :192k (default)
    IPv4 multicast : 32k (default)
User configured:(effective after reboot)
    IPv4           :220k
    IPv4 multicast : 16k (adjusted default)
Console> (enable)
```

MSFC2/MSFC3 上での IP マルチキャストの設定

ここでは、MSFC2/MSFC3 を IP マルチキャスト用に設定する手順を説明します。

- IP マルチキャスト ルーティングのグローバルなイネーブル化（p.13-18）
- MSFC2/MSFC3 インターフェイス上での IP PIM のイネーブル化（p.13-19）
- IP MMLS グローバル スレッシュホールドの設定（p.13-19）
- MSFC2/MSFC3 インターフェイス上での IP MMLS のイネーブル化（p.13-20）

（注） ここでは、MSFC2/MSFC3 上で IP マルチキャスト ルーティングをイネーブルにする方法を説明します。IP マルチキャスト設定の詳細については、次の URL にある『*Cisco IOS IP and IP Routing Configuration Guide*』の「IP Multicast」を参照してください。
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_c/ipcprt3/index.htm

IP マルチキャスト ルーティングのグローバルなイネーブル化

MSFC2/MSFC3 上でグローバルに IP マルチキャスト ルーティングをイネーブルにしてから、MSFC2/MSFC3 インターフェイス上で PIM をイネーブルにする必要があります。

MSFC2/MSFC3 上でグローバルに IP マルチキャスト ルーティングをイネーブルにするには、グローバル コンフィギュレーション モードで次の作業を行います。

作業	コマンド
IP マルチキャスト ルーティングをグローバルにイネーブルにします。	Router(config)# **ip multicast-routing**

次に、IP マルチキャスト ルーティングをグローバルにイネーブルにする例を示します。

```
Router(config)# ip multicast-routing
Router(config)#
```

MSFC2/MSFC3 インターフェイス上での IP PIM のイネーブル化

MSFC2/MSFC3 インターフェイス上で IP マルチキャストが機能するためには、これらのインターフェイス上で PIM をイネーブルに設定する必要があります。

MSFC2/MSFC3 インターフェイス上で IP PIM をイネーブルにするには、インターフェイス コンフィギュレーション モードで次の作業を行います。

作業	コマンド
MSFC2/MSFC3 インターフェイス上で IP PIM をイネーブルにします。	Router(config-if)# **ip pim** {**dense-mode** | **sparse-mode** | **sparse-dense-mode**}

次に、MSFC2/MSFC3 インターフェイス上でデフォルト モード（**sparse-dense-mode**）を使用して PIM をイネーブルにする例を示します。

```
Router(config-if)# ip pim
Router(config-if)#
```

次に、MSFC2/MSFC3 インターフェイス上で PIM sparse（疎）モードをイネーブルにする例を示します。

```
Router(config-if)# ip pim sparse-mode
Router(config-if)#
```

IP MMLS グローバル スレッシュホールドの設定

MSFC2/MSFC3 がルーティングするマルチキャスト トラフィックの上限を表すグローバル マルチキャスト レート スレッシュホールド（パケット / 秒）を設定できます。この設定により、Join 要求など、存続期間の短いマルチキャスト フローに対応する MLS エントリの作成が防止されます。

（注） このコマンドは、ルーティング済みのフローに対しては無効です。既存のルートにスレッシュホールドを適用するには、ルートをいったん消去して再度確立します。

IP MMLS スレッシュホールドを設定するには、次の作業を行います。

作業	コマンド
IP MMLS スレッシュホールドを設定します。	Router(config)# [**no**] **mls ip multicast threshold** *ppsec*

次に、IP MMLS スレッシュホールドを 10 パケット / 秒に設定する例を示します。

```
Router(config)# mls ip multicast threshold 10
Router(config)#
```

スレッシュホールドの設定を解除するには、**no** キーワードを使用します。

MSFC2/MSFC3 インターフェイス上での IP MMLS のイネーブル化

MSFC2/MSFC3 インターフェイス上で IP PIM をイネーブルに設定した場合、そのインターフェイス上では IP MMLS がデフォルトでイネーブルになります。ここで説明する作業は、インターフェイス上で IP MMLS をディセーブルにし、再びイネーブルにする場合にだけ実行してください。

(注)　IP MMLS が機能するためには、まず参加しているすべての MSFC2/MSFC3 インターフェイス上で IP PIM をイネーブルにする必要があります。MSFC2/MSFC3 インターフェイス上での IP PIM の設定手順については、「MSFC2/MSFC3 インターフェイス上での IP PIM のイネーブル化」（p.13-19）を参照してください。

MSFC2/MSFC3 インターフェイス上で IP MMLS をイネーブルにするには、次の作業を行います。

作業	コマンド
MSFC2/MSFC3 インターフェイス上で IP MMLS をイネーブルにします。	Router(config-if)# [**no**] **mls ip multicast**

次に、MSFC2/MSFC3 インターフェイス上で IP MMLS をイネーブルにする例を示します。

```
Router(config-if)# mls ip multicast
Router(config-if)#
```

MSFC2/MSFC3 インターフェイス上で IP MMLS をディセーブルにするには、**no** キーワードを使用します。

IP マルチキャスト情報の表示

ここでは、IP マルチキャスト情報の表示方法について説明します。

- MSFC2/MSFC3 上での IP マルチキャスト情報の表示（p.13-20）
- スーパバイザ エンジン上での IP マルチキャスト情報の表示（p.13-24）

MSFC2/MSFC3 上での IP マルチキャスト情報の表示

ここでは、MSFC2/MSFC3 上で IP マルチキャスト情報を表示する方法を説明します。

- IP MMLS インターフェイス情報の表示（p.13-20）
- IP マルチキャスト ルーティング テーブルの表示（p.13-21）
- IP マルチキャスト詳細情報の表示（p.13-22）
- debug コマンドの使用方法（p.13-23）
- SCP に関する debug コマンドの使用方法（p.13-24）

IP MMLS インターフェイス情報の表示

show ip pim interface count コマンドを実行すると、MSFC2/MSFC3 IP PIM インターフェイス上の IP MMLS イネーブル ステート、およびそのインターフェイス上で送受信されたパケット数が表示されます。出力は、ファスト スイッチングおよびプロセス スイッチングされた PIM インターフェイスとこれらのインターフェイスのパケット カウントを示します。IP MMLS がイネーブルなインターフェイスには [H] が表示されます。

show ip interface コマンドを実行すると、MSFC2/MSFC3 インターフェイス上の IP MMLS イネーブル ステートが表示されます。

特定の IP PIM MSFC2/MSFC3 インターフェイスについて IP MMLS 情報を表示するには、次のいずれかの作業を行います。

作業	コマンド
IP MMLS インターフェイス情報を表示します。	Router# **show ip pim interface** [*type number*] **count**
IP MMLS インターフェイスのイネーブル ステートを表示します。	Router# **show ip interface**

次に、IP MMLS インターフェイスの設定情報を表示する例を示します。

```
Router# show ip pim interface count
States: FS - Fast Switched, H - Hardware Switched

Address          Interface          FS  Mpackets In/Out

192.168.10.2       Vlan10             * H 40886/0

192.168.11.2       Vlan11             * H 0/40554

192.168.12.2       Vlan12             * H 0/40554

192.168.23.2       Vlan23             *   0/0

192.168.24.2       Vlan24             *   0/0

Router#
```

IP マルチキャスト ルーティング テーブルの表示

show ip mroute コマンドを実行すると、MSFC2/MSFC3 上の IP マルチキャスト ルーティング テーブルが表示されます。

IP マルチキャスト ルーティング テーブルを表示するには、次の作業を行います。

作業	コマンド
IP マルチキャスト ルーティング テーブルを表示します。	Router# **show ip mroute** [*group*[*source*]] | [**summary**] | [**count**] | [**active** *kbps*]

次に、IP マルチキャスト ルーティング テーブルを表示する例を示します。

```
Router# show ip mroute 239.252.1.1
IP Multicast Routing Table
Flags:D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned
       R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT
       M - MSDP created entry, X - Proxy Join Timer Running
       A - Advertised via MSDP
Outgoing interface flags:H - Hardware switched
Timers:Uptime/Expires
Interface state:Interface, Next-Hop or VCD, State/Mode

(*, 239.252.1.1), 04:04:59/00:02:59, RP 80.0.0.2, flags:SJ
  Incoming interface:Vlan800, RPF nbr 80.0.0.2
  Outgoing interface list:
    Vlan10, Forward/Dense, 01:29:57/00:00:00, H

(22.0.0.10, 239.252.1.1), 00:00:19/00:02:41, flags:JT
  Incoming interface:Vlan800, RPF nbr 80.0.0.2, RPF-MFD
  Outgoing interface list:
    Vlan10, Forward/Dense, 00:00:19/00:00:00, H
```

IP マルチキャスト詳細情報の表示

show mls ip multicast コマンドを実行すると、IP MMLS に関する詳細情報が表示されます。

MSFC2/MSFC3 上の MMLS 詳細情報を表示するには、次のいずれかの作業を行います。

作業	コマンド
IP MMLS グループ情報を表示します。	Router# **show mls ip multicast group** *group-address* [**interface** *type number* | **statistics**]
すべてのインターフェイスについて IP MMLS 詳細情報を表示します。	Router# **show mls ip multicast interface** *type number* [**statistics** | **summary**]
IP MMLS 情報の要約を表示します。	Router# **show mls ip multicast summary**
IP MMLS 統計情報を表示します。	Router# **show mls ip multicast statistics**
IP MMLS 送信元情報を表示します。	Router# **show mls ip multicast source** *ip-address* [**interface** *type number* | **statistics**]

次に、MSFC2/MSFC3 上の IP MMLS 統計情報を表示する例を示します。

```
Router# show mls ip multicast statistics
MLS Multicast configuration and state:
    Router Mac:0050.0f2d.9bfd, Router IP:1.12.123.234
    MLS multicast operating  state:ACTIVE
    Maximum number of allowed outstanding messages:1
    Maximum size reached from feQ:1
    Feature Notification sent:5
    Feature Notification Ack received:4
    Unsolicited Feature Notification received:0
    MSM sent:33
    MSM ACK received:33
    Delete notifications received:1
    Flow Statistics messages received:248

MLS Multicast statistics:
    Flow install Ack:9
    Flow install Nack:0
    Flow update Ack:2
    Flow update Nack:0
    Flow delete Ack:0
    Complete flow install Ack:10
    Complete flow install Nack:0
    Complete flow delete Ack:1
    Input VLAN delete Ack:4
    Output VLAN delete Ack:0
    Group delete sent:0
    Group delete Ack:0
    Global delete sent:7
    Global delete Ack:7

    L2 entry not found error:0
    Generic error :3
    LTL entry not found error:0
    MET entry not found error:0
    L3 entry exists error :0
    Hash collision error :0
    L3 entry not found error:0
    Complete flow exists error :0
```

次に、MSFC2/MSFC3 上の特定の IP MMLS エントリに関する情報を表示する例を示します。

```
Router# show mls ip multicast 224.1.1.1
Multicast hardware switched flows:
(1.1.13.1, 224.1.1.1) Incoming interface: Vlan13, Packets switched: 61590
Hardware switched outgoing interfaces: Vlan20 Vlan9
RFD-MFD installed: Vlan13

(1.1.9.3, 224.1.1.1) Incoming interface: Vlan9, Packets switched: 0
Hardware switched outgoing interfaces: Vlan20
RFD-MFD installed: Vlan9

(1.1.12.1, 224.1.1.1) Incoming interface: Vlan12, Packets switched: 62010
Hardware switched outgoing interfaces: Vlan20 Vlan9
RFD-MFD installed: Vlan12

(1.1.12.3, 224.1.1.1) Incoming interface: Vlan12, Packets switched: 61980
Hardware switched outgoing interfaces: Vlan20 Vlan9
RFD-MFD installed: Vlan12

(1.1.11.1, 224.1.1.1) Incoming interface: Vlan11, Packets switched: 62430
Hardware switched outgoing interfaces: Vlan20 Vlan9
RFD-MFD installed: Vlan11

(1.1.11.3, 224.1.1.1) Incoming interface: Vlan11, Packets switched: 62430
Hardware switched outgoing interfaces: Vlan20 Vlan9
RFD-MFD installed: Vlan11

Total hardware switched installed: 6
Router#
```

次に、MSFC2/MSFC3 上の IP MMLS 情報の要約を表示する例を示します。

```
Router# show mls ip multicast summary
7 MMLS entries using 560 bytes of memory
Number of partial hardware-switched flows:2
Number of complete hardware-switched flows:5
Router#
```

debug コマンドの使用方法

表 13-3 に、IP MMLS 関連のトラブルシューティングのための debug コマンドを示します。

表 13-3　IP MMLS の debug コマンド

コマンド	説明
[no] debug mls ip multicast group *group_id group_mask*	他のすべてのマルチキャスト デバッグ コマンドに適用されるフィルタを設定します。
[no] debug mls ip multicast events	IP MMLS イベントを表示します。
[no] debug mls ip multicast errors	マルチキャスト MLS 関連のエラーに対するデバッグ メッセージをオンにします。
[no] debug mls ip multicast messages	ハードウェア スイッチング エンジンとの間で送受信される IP MMLS メッセージを表示します。
[no] debug mls ip multicast all	すべての IP MMLS メッセージをオンにします。
[no] debug mdss error	すべての Multicast Distributed Switching Services（MDSS）エラー メッセージをオンにします。
[no] debug mdss events	MDSS 関連のイベントをオンにします。
[no] debug mdss all	すべての MDSS メッセージをオンにします。

SCP に関する debug コマンドの使用方法

表 13-4 に、Ethernet Out-of-Band Channel（EOBC）で動作する Serial Control Protocol（SCP）をトラブルシューティングするための、CP 関連の debug コマンドを示します。

表 13-4　SCP の debug コマンド

コマンド	説明
[no] debug scp async	SCP システムを出入りする非同期データのトレースを表示します。
[no] debug scp data	パケット データのトレースを表示します。
[no] debug scp errors	SCP のエラーおよび警告を表示します。
[no] debug scp packets	SCP システムを出入りするパケット データを表示します。
[no] debug scp timeouts	タイムアウトを報告します。
[no] debug scp all	すべての SCP デバッグ メッセージをオンにします。

スーパバイザ エンジン上での IP マルチキャスト情報の表示

ここでは、IP マルチキャスト情報の表示方法について説明します。

- IP マルチキャスト統計情報の表示（p.13-24）
- IP マルチキャスト統計情報の消去（p.13-25）
- IP マルチキャスト エントリの表示（p.13-25）

IP マルチキャスト統計情報の表示

show mls multicast statistics コマンドを実行すると、IP マルチキャスト統計情報が表示されます。

IP マルチキャスト統計情報を表示するには、次の作業を行います。

作業	コマンド
IP マルチキャスト統計情報を表示します。	**show mls multicast statistics** [*ip_addr*]

次に、MSFC2/MSFC3 の IP マルチキャスト統計情報を表示する例を示します。

```
Console (enable) show mls multicast statistics
Router IP          Router Name        Router MAC
-------------------------------------------------------
1.1.9.254          ?                  00-50-0f-06-3c-a0

Transmit:
  Delete Notifications:                    23
  Acknowledgements:                        92
  Flow Statistics:                         56

Receive:
  Open Connection Requests:                1
  Keep Alive Messages:                     72
  Shortcut Messages:                       19
    Shortcut Install TLV:                  8
    Selective Delete TLV:                  4
    Group Delete TLV:                      0
    Update TLV:                            3
    Input VLAN Delete TLV:                 0
    Output VLAN Delete TLV:                0
    Global Delete TLV:                     0
    MFD Install TLV:                       7
    MFD Delete TLV:                        0
```

```
Router IP          Router Name        Router MAC
-----------------------------------------------------
1.1.5.252          ?                  00-10-29-8d-88-01

Transmit:
  Delete Notifications:                    22
  Acknowledgements:                        75
  Flow Statistics:                         22

Receive:
  Open Connection Requests:                1
  Keep Alive Messages:                     68
  Shortcut Messages:                       6
    Shortcut Install TLV:                  4
    Selective Delete TLV:                  2
    Group Delete TLV:                      0
    Update TLV:                            0
    Input VLAN Delete TLV:                 0
    Output VLAN Delete TLV:                0
    Global Delete TLV:                     0
    MFD Install TLV:                       4
    MFD Delete TLV:                        0
Console (enable)
```

IP マルチキャスト統計情報の消去

clear mls multicast statistics コマンドを実行すると、IP マルチキャスト統計情報が消去されます。

IP マルチキャスト統計情報を消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
IP マルチキャスト統計情報を消去します。	**clear mls multicast statistics**

次に、IP マルチキャスト統計情報を消去する例を示します。

```
Console> (enable) clear mls multicast statistics
All statistics for the MLS routers in include list are cleared.
Console> (enable)
```

IP マルチキャスト エントリの表示

show mls multicast entry コマンドを実行すると、PFC2/PFC3A が処理しているマルチキャスト フローに関する各種の情報が表示されます。参加している MSFC2/MSFC3、VLAN、マルチキャスト グループ アドレス、またはマルチキャスト トラフィック送信元を任意に組み合わせて、エントリを表示できます。

IP マルチキャスト エントリに関する情報を表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
IP マルチキャスト エントリに関する情報を表示します。	**show mls multicast entry** [[[*mod*] [**vlan** *vlan_id*] [**group** *ip_addr*] [**source** *ip_addr*]] | [**all**]]

次に、すべての IP マルチキャスト エントリを表示する例を示します。

```
Console> (enable) show mls multicast entry all
Router IP       Dest IP         Source IP       Pkts       Bytes       InVlan
OutVlans
--------------- --------------- --------------- ---------- ----------- -------
--------

1.1.5.252       224.1.1.1       1.1.11.1        15870      2761380     20
1.1.9.254       224.1.1.1       1.1.12.3        473220     82340280    12
1.1.5.252       224.1.1.1       1.1.12.3        15759      2742066     20
1.1.9.254       224.1.1.1       1.1.11.1        473670     82418580    11
1.1.5.252       224.1.1.1       1.1.11.3        15810      2750940     20
1.1.9.254       224.1.1.1       1.1.12.1        473220     82340280    12
1.1.5.252       224.1.1.1       1.1.13.1        15840      2756160     20
1.1.9.254       224.1.1.1       1.1.13.1        472770     82261980    13
1.1.5.252       224.1.1.1       1.1.12.1        15840      2756160     20
1.1.9.254       224.1.1.1       1.1.11.3        473667     82418058    11
Total Entries: 10
Console> (enable)
```

次に、特定の MSFC2/MSFC3 について、IP マルチキャスト エントリを表示する例を示します。

```
Console> (enable) show mls multicast entry 15
Router IP       Dest IP         Source IP       Pkts       Bytes       InVlan
OutVlans
--------------- --------------- --------------- ---------- ----------- -------
--------

1.1.5.252       224.1.1.1       1.1.11.1        15870      2761380     20
1.1.5.252       224.1.1.1       1.1.12.3        15759      2742066     20
1.1.5.252       224.1.1.1       1.1.11.3        15810      2750940     20
1.1.5.252       224.1.1.1       1.1.13.1        15840      2756160     20
1.1.5.252       224.1.1.1       1.1.12.1        15840      2756160     20
Total Entries: 5
Console> (enable)
```

次に、特定のマルチキャスト グループ アドレスについて、IP マルチキャスト エントリを表示する例を示します。

```
Console> (enable) show mls multicast entry group 226.0.1.3 short
Router IP      Dest IP     Source IP    InVlan Pkts   Bytes     OutVlans
-------------- ----------- ------------ ------ ------ --------- ----------
171.69.2.1     226.0.1.3   172.2.3.8    20     171    23512     10,201,22,45
171.69.2.1     226.0.1.3   172.3.4.9    12     25     3120      8,20
Total Entries: 2
Console> (enable)
```

次に、特定の MSFC2/MSFC3 および特定のマルチキャスト送信元アドレスについて、IP マルチキャスト エントリを表示する例を示します。

```
Console> (enable) show mls multicast entry 15 source 1.1.11.1 short
Router IP       Dest IP         Source IP       Pkts       Bytes
 InVlan  OutVlans
--------------- --------------- --------------- ---------- --------------------
  ------ ----------
172.20.49.159   224.1.1.6       1.1.40.4        368        57776
  40     23,25
172.20.49.159   224.1.1.71      1.1.22.2        99         65142
  22     30,37
172.20.49.159   224.1.1.8       1.1.22.2        396        235620
  22     13,19
Console> (enable)
```

スイッチ上での NetFlow 統計情報の設定

（注）　Supervisor Engine 720（MSFC3）では、IPX ルーティングはソフトウェアを通じて実行されます。

ここでは、NetFlow 統計情報を設定する手順について説明します。

インターフェイス単位での NetFlow テーブル エントリの指定

（注）　この機能には PFC3A 以上が必要です。

Release8.4(1) 以降のソフトウェア リリースでは、NetFlow テーブル エントリをインターフェイス単位で作成できます。この機能ではブリッジド フロー統計と同じメカニズムを使用して、フローを作成します。NetFlow エントリはブリッジド フロー統計がイネーブル化された VLAN と、NetFlow エントリ作成がイネーブル化された VLAN の両方に対して作成されます（「VLAN に対するブリッジド フロー統計のイネーブル化およびディセーブル化」[p.16-12] を参照）。

たとえば、VLAN 100 および 200 上でインターフェイス単位のレイヤ 3 エントリ作成をイネーブルにし、同時に、VLAN 150 および 250 上でブリッジド フロー統計をイネーブルにすると、NetFlow エントリおよびブリッジド フロー統計が 4 つのすべての VLAN でイネーブルになります。VLAN 150 および 250 にブリッジド フロー統計のみを指定するには、インターフェイス単位のエントリ機能をディセーブルにする必要があります。

また、VLAN に対してインターフェイス単位の NetFlow エントリ作成をイネーブルにすると、ブリッジド フロー統計が自動的にイネーブルになります。NetFlow テーブル エントリを作成する場合に、この重複を回避する場合は、CLI を使用してインターフェイス単位で NetFlow をディセーブルにすることができます。

この機能のステータスは、**show mls** コマンドの一部として表示されます。エントリ作成がイネーブル化された VLAN は、ブリッジド フロー統計機能がイネーブル化された VLAN の一部として表示されます。

インターフェイス単位の NetFlow テーブル エントリをイネーブルまたはディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
インターフェイス単位の NetFlow テーブル エントリをイネーブルにします。	**set mls netflow-per-interface** [**enable** | **disable**]

次に、インターフェイス単位の NetFlow テーブル エントリをイネーブルにする例を示します。

```
Console> (enable) set mls netflow-per-interface enable
Console> (enable)
```

NetFlow エントリをイネーブルまたはディセーブルにする VLAN を指定できます。VLAN 単位でフロー作成を制御するには、イネーブル モードで次の作業を行います。

作業	コマンド
VLAN 単位の NetFlow テーブル エントリをイネーブルにします。	**set mls netflow-entry-create** [**enable** | **disable**] *vlan-list*

次に、NetFlow テーブル エントリの作成に使用する VLAN を指定する例を示します。

```
Console> (enable) set mls netflow-entry-create enable 150, 250
Console> (enable)
```

NetFlow テーブル エントリのエージング タイム値の指定

各プロトコル（IP および IPX）のエントリ エージング タイムは、プロトコル固有のすべての NetFlow テーブル エントリに適用されます。*agingtime* で指定される期間（秒）にわたって使用されなかったエントリは、期限切れになります。デフォルトは 16 秒です。

通常のエージング タイムには、1 ～ 1092 秒の範囲で 8 秒の倍数を指定できます。8 秒の倍数以外のエージング タイム値を指定すると、最も近い 8 秒の倍数に調整されます。たとえば 65 は 64 に、127 は 128 に調整されます。

IP および IPX の両方についてエントリのエージング タイムを指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
NetFlow テーブル エントリのエージング タイムを指定します。	**set mls agingtime** [*agingtime*]

次に、エントリのエージング タイムを指定する例を示します。

```
Console> (enable) set mls agingtime 16
Multilayer switching agingtime IP and IPX set to 16
Console> (enable)
```

IP エントリのエージング タイムを指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
NetFlow テーブルの IP エントリ エージング タイムを指定します。	**set mls agingtime ip** [*agingtime*]

次に、IP エントリのエージング タイムを指定する例を示します。

```
Console> (enable) set mls agingtime ip 16
Multilayer switching aging time IP set to 16
Console> (enable)
```

IPX エントリのエージング タイムを指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
NetFlow テーブルの IPX エントリ エージング タイムを指定します。	**set mls agingtime ipx** [*agingtime*]

次に、IPX エントリのエージング タイムを指定する例を示します。

```
Console> (enable) set mls agingtime ipx 16
Multilayer switching aging time IPX set to 16
Console> (enable)
```

NetFlow テーブル IP エントリのファスト エージング タイムおよびパケット スレッシュホールド値の指定

(注)　IPX エントリについては、ファスト エージングは使用されません。

NetFlow テーブルの使用率を増加させるには、IP エントリのファスト エージング タイムをイネーブルにします。IP エントリのファスト エージング タイムは、NetFlow テーブル エントリのうち、作成後 *fastagingtime* 秒以内にルーティングされたパケット数が *pkt_threshold* 個に満たないものに適用されます。一般に、Domain Name Server（DNS; ドメイン ネーム サーバ）または Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバとの間のフローに対応する NetFlow テーブル エントリが、削除の対象になります。この種のエントリは、作成後、再び使用されることはありません。これらのエントリを検出して期限切れにすれば、NetFlow テーブルのスペースが節約され、他のデータ トラフィックを格納できるようになります。

デフォルトの *fastagingtime* 値は、0（ファスト エージングなし）です。Supervisor Engine 1 および Supervisor Engine 2 では、*fastagingtime* 値を 8 ～ 128 秒の範囲で、8 秒の倍数で設定できます。Supervisor Engine 720 では、*fastagingtime* 値を 0 ～ 128 秒の範囲で、1 秒単位で設定できます。*fastagingtime* 値をこれ以外の値に設定すると、最も近い値に調整されます。Supervisor Engine 1 および Supervisor Engine 2 では、*pkt_threshold* 値は、0、1、3、7、15、31、63、127 パケットに設定できます。Supervisor Engine 720 では、*pkt_threshold* 値は 1 ～ 127 パケットの範囲で、1 パケット単位で設定できます。

IP エントリのファスト エージング タイムをイネーブルにする場合、最初は 128 秒に設定してください。この設定でも NetFlow テーブルが引き続き一杯になる場合には、設定値を小さくします。それでも NetFlow テーブルが一杯の場合には、通常の IP エントリ エージング タイムを小さくします。

IP エントリのファスト エージング タイムおよびパケット スレッシュホールドを指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
NetFlow テーブル エントリの IP エントリ ファスト エージング タイムおよびパケット スレッシュホールドを指定します。	**set mls agingtime fast** [*fastagingtime*] [*pkt_threshold*]

次に、IP エントリ ファスト エージング タイムを 8 秒、パケット スレッシュホールドを 15 パケットに設定する例を示します。

```
Console> (enable) set mls agingtime fast 8 15
Multilayer switching fast aging time set to 8 seconds for entries with no more than 15
packets switched.
Console> (enable)
```

set mls agingtime long-duration {*longagingtime*} コマンドを実行することにより、アクティブ フローを強制的に期限切れにできます。アクティブ フローのエージング タイムとして設定できる値は、64 ～ 1920 秒の範囲の 64 の倍数です。デフォルトの *longagingtime* は 320 です。

次に、アクティブ フローのエージング タイムを設定する例を示します。

```
Console> (enable) set mls agingtime long-duration 128
Multilayer switching agingtime set to 128 seconds for long duration flows
Console> (enable)
```

最小統計フロー マスクの設定

NetFlow テーブルのフロー マスクの最小粒度を設定できます。実際のフロー マスクは、このコマンドで指定された最低基準になります。各種フロー マスクの機能については、「フロー マスク」（p.13-12）を参照してください。

（注）　**set mls flow** コマンドを入力すると、NetFlow テーブルの既存エントリがすべて削除されます。

NetFlow 最小統計フロー マスクを設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
最小統計フロー マスクを設定します。	**set mls flow** {**destination** | **destination-source** | **null** | **full**}

次に、最小統計フロー マスクを destination-source-ip に設定する例を示します。

```
Console> (enable) set mls flow destination-source
Configured IP flow mask is set to destination-source flow.
Console> (enable)
```

NetFlow テーブルからの IP プロトコル エントリの除外

NetFlow テーブルから特定の IP プロトコルを除外するように設定できます。

NetFlow テーブルから IP プロトコルを除外するには、イネーブル モードで次の作業を行います。

作業	コマンド
NetFlow テーブルから IP プロトコルを除外します。	**set mls exclude protocol** {**tcp** | **upd** | **both**} *port*

パラメータ *port* には、ポート番号または **dns**、**ftp**、**smtp**、**telnet**、**x**（X-Windows）、または **www** といったキーワードを指定できます。

次に、NetFlow テーブルから Telnet トラフィックを除外する例を示します。

```
Console> (enable) set mls exclude protocol tcp telnet
NetFlow table will not create entries for TCP packets with protocol port 23.
Note: MLS exclusion only works in full flow mode.
Console> (enable)
```

NetFlow 統計情報の表示

(注)　転送決定エントリを表示するには、**show mls entry cef** コマンドを使用します（「スーパバイザ エンジン上でのレイヤ 3 スイッチング エントリの表示」[p.13-15] を参照）。

NetFlow テーブル エントリおよび統計情報の要約を表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
すべての NetFlow テーブル エントリおよび統計情報を表示します。	**show mls**

次に、すべての NetFlow テーブル エントリを表示する例を示します（Supervisor Engine 2 からの出力）。

```
Console> (enable) show mls
show mls
=======
Total packets switched = 2
Total bytes switched = 112
Total routes = 48
IP statistics flows aging time = 16 seconds
IP statistics flows fast aging time = 0 seconds, packet threshold = 0
IP Current flow mask is Full flow
Netflow Data Export version:7
Netflow Data Export disabled
Netflow Data Export port/host is not configured.
Total packets exported = 0

IPX statistics flows aging time = 16 seconds
IPX flow mask is Destination flow
IPX max hop is 15

Module 15:Physical MAC-Address 00-50-3e-a9-ab-fc
Vlan Virtual MAC-Address(es)
---- -----------------------
  42 00-00-0c-07-ac-00
Console>
```

次に、すべての NetFlow テーブル エントリを表示する例を示します（Supervisor Engine 720 からの出力）。

```
Console> (enable) show mls
Total packets switched = 35254
Total bytes switched = 2256256
Total routes = 120569
Total number of Netflow entries = 120000

IP statistics flows aging time = 50 seconds
Long-duration flows aging time = 320 seconds
IP statistics flows fast aging time = 0 seconds, packet threshold = 0

IP Current flow mask is Full-Vlan flow
Netflow Data Export version: 7
Netflow Data Export disabled
Netflow Data Export port/host is not configured.
Total packets exported = 0
Destination Ifindex export is enabled
Source Ifindex export is enabled
Rate limiting is turned off, packets are bridged to router
Load balancing hash is based on source and destination IP addresses and universc
Per-prefix Stats for ALL FIB entries is Enabled
Console> (enable)
```

show mls statistics entry コマンドを使用すると、すべての統計情報または特定の NetFlow テーブル エントリの統計情報を表示できます。特定の NetFlow テーブル エントリの統計情報を表示するには、宛先アドレス、送信元アドレス、IP、プロトコル、送信元ポートと宛先ポートを指定します。

src_port または *dst_port* にゼロ（0）を指定した場合、ワイルドカードとして扱われ、すべての NetFlow 統計情報が表示されます（未指定のオプションはワイルドカードとして扱われます）。指定するプロトコルが TCP または UDP 以外の場合には、*src_port* および *dst_prt* を 0 に設定しないと、NetFlow 統計情報は表示されません。

NetFlow テーブル エントリに関する統計情報を表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
NetFlow テーブル エントリに関する統計情報を表示します。NetFlow テーブル エントリを指定しない場合、すべての NetFlow 統計情報が表示されます。	**show mls statistics entry** [**ip** | **ipx** | **uptime**] [**destination** *ip_addr_spec*] [**source** *ip_addr_spec*] [**flow** *protocol src_port dst_port*]

次に、特定の NetFlow テーブル エントリに関する NetFlow 統計情報を表示する例を示します。

```
Console> show mls statistics entry ip destination 172.20.22.14
                                    Last    Used
Destination IP  Source IP       Prot DstPrt SrcPrt Stat-Pkts Stat-Bytes
--------------- --------------- ---- ------ ------ --------- -----------
MSFC 127.0.0.12:
172.20.22.14    172.20.25.10    6    50648  80     3152       347854
Console>
```

show mls statistics entry ip top-talkers コマンドを使用すると、ネットワーク使用率が最大の NetFlow に関する統計情報が表示されます。NetFlow エントリは、各フロー内のパケット数に基づいて、NetFlow テーブルから取得されます。結果は降順で表示され、パケット数が最大のエントリが最上位のトーカーになります。ネットワークの統計情報を表示したり（上位 32 のトーカーを表示）、上位 1 つまたは 2 つのトーカーなど、指定数のフローを表示することができます。

NetFlow テーブル エントリに関する NetFlow の上位トーカーを表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
ネットワーク使用率が最大の NetFlow トーカーを表示します。	**show mls statistics entry ip top-talkers**

次に、ネットワークに関する NetFlow の上位トーカーを表示する例を示します。

```
Console> show mls statistics entry ip top-talkers
Last    Used
Destination IP   Source IP       Prot  DstPrt SrcPrt Vlan  Stat-Pkts  Stat-Bytes
---------------- --------------- ----- ------ ------ ----- ---------  -----------
 12.0.0.5        11.0.0.6        255   N/A    N/A    N/A   387110     17807060
 12.0.0.5        11.0.0.7        255   N/A    N/A    N/A   387109     17807014
 12.0.0.5        11.0.0.4        TCP   8      7      N/A   20         920
 127.0.0.20      127.0.0.19      UDP   67     68     N/A   18         828
 12.0.0.5        11.0.0.2        TCP   6      5      N/A   15         690
 12.0.0.5        11.0.0.5        TCP   8      7      N/A   15         690
 12.0.0.5        11.0.0.3        TCP   6      5      N/A   12         552
Console>
```

次に、ネットワーク使用率が最大の NetFlow の統計情報を指定数だけ表示する例を示します。

```
Console> show mls statistics entry ip top-talkers 2
Last    Used
Destination IP   Source IP       Prot  DstPrt SrcPrt Vlan  Stat-Pkts  Stat-Bytes
---------------- --------------- ----- ------ ------ ----- ---------  -----------
 12.0.0.5        11.0.0.6        255   N/A    N/A    N/A   387110     17807060
 12.0.0.5        11.0.0.7        255   N/A    N/A    N/A   387109     17807014
Console>
```

NetFlow IP および IPX 統計情報の消去

ここでは、NetFlow 統計情報を消去する手順について説明します。

- すべての NetFlow 統計情報の消去（p.13-33）
- NetFlow IP 統計情報の消去（p.13-34）
- NetFlow IPX 統計情報の消去（p.13-34）
- NetFlow 統計の総数情報の消去（p.13-35）

（注）

clear mls コマンドが影響を及ぼすのは、統計情報だけです。**clear mls** コマンドは、転送エントリ、または転送エントリに対応する NetFlow テーブル エントリには影響しません。

すべての NetFlow 統計情報の消去

すべての NetFlow IP および IPX 統計情報を消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
NetFlow 統計情報をすべて消去します。	**clear mls statistics entry all**

次に、NetFlow 統計情報をすべて消去する例を示します。

```
Console> (enable) clear mls statistics entry all
All MLS IP and IPX entries cleared.
Console> (enable)
```

NetFlow IP 統計情報の消去

clear mls statistics entry ip コマンドを実行すると、NetFlow IP 統計情報が消去されます。すべての NetFlow IP 統計情報を消去するには、**all** キーワードを使用します。**destination** キーワードおよび **source** キーワードは、送信元および宛先の IP アドレスを指定します。宛先および送信元の *ip_addr_spec* には、完全な IP アドレス、または *ip_subnet_addr*、*ip_addr/subnet_mask*、*ip_addr/subnet_mask_bits* の形式のサブネット アドレスを指定できます。

flow キーワードでは、追加されたフロー情報を次のように指定します。

- プロトコル ファミリー（*protocol*）― **tcp**、**udp**、**icmp**、またはその他のプロトコル ファミリーに対応する 10 進数を指定します。*protocol* にゼロ（0）を指定すると、ワイルドカードとして扱われます（未指定のオプションはワイルドカードとして扱われます）。
- TCP または UDP の送信元および宛先ポート番号（*src_port* および *dst_port*）― プロトコルとして TCP または UDP を指定する場合、送信元および宛先の TCP または UDP ポート番号を指定します。*src_port* または *dst_port* にゼロ（0）を指定した場合、ワイルドカードとして扱われます（未指定のオプションはワイルドカードとして扱われます）。その他のプロトコルについては、*src_port* および *dst_port* を 0 に設定しないと、エントリは消去されません。

NetFlow テーブルの IP エントリの統計情報を消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
NetFlow テーブルの IP エントリの統計情報を消去します。	**clear mls statistics entry ip** [**destination** *ip_addr_spec*] [**source** *ip_addr_spec*] [**flow** *protocol src_port dst_port*] [**all**]

次に、NetFlow テーブルで宛先 IP アドレス 172.20.26.22 のエントリを消去する例を示します。

```
Console> (enable) clear mls statistics entry ip destination 172.20.26.22
MLS IP entry cleared
Console> (enable)
```

次に、NetFlow テーブルで、宛先 IP アドレス 172.20.22.113、TCP 送信元ポート 1652、TCP 宛先ポート 23 のエントリの統計情報を消去する例を示します。

```
Console> (enable) clear mls statistics entry ip destination 172.20.26.22 source
172.20.22.113 flow tcp 1652 23
MLS IP entry cleared
Console> (enable)
```

NetFlow IPX 統計情報の消去

clear mls statistics entry ipx コマンドを実行すると、NetFlow IPX 統計情報が消去されます。すべての NetFlow IPX 統計情報を消去するには、**all** キーワードを使用します。**destination** および **source** キーワードは、送信元および宛先の IPX アドレスを指定します。

NetFlow テーブルの IPX エントリの統計情報を消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
NetFlow テーブルの IPX エントリの統計情報を消去します。	**clear mls statistics entry ipx** [**destination** *ipx_addr_spec*] [**source** *ipx_addr_spec*] [**all**]

次に、宛先 IPX アドレス 1.0002.00e0.fefc.6000 の IPX MLS エントリに関する統計情報を消去する例を示します。

```
Console> (enable) clear mls statistics entry ipx destination 1.0002.00e0.fefc.6000
MLS IPX entry cleared.
Console> (enable)
```

NetFlow 統計の総数情報の消去

clear mls statistics コマンドを使用して、次の NetFlow 統計情報を消去できます。

- スイッチングされたパケット総数（IP および IPX）
- エクスポートされたパケット総数（NDE へ）

NetFlow 統計の総数情報を消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
NetFlow 統計の総数情報を消去します。	**clear mls statistics**

次に、NetFlow 統計の総数情報を消去する例を示します。

```
Console> (enable) clear mls statistics
All mls statistics cleared.
Console> (enable)
```

NetFlow 統計のデバッグ情報の表示

show mls debug コマンドを実行すると、NetFlow 統計のデバッグ情報が表示されます。必要に応じて、この情報をテクニカル サポートに送信し、解析に利用することができます。

NetFlow 統計のデバッグ情報を表示するには、次の作業を行います。

作業	コマンド
テクニカル サポートに送信できる NetFlow 統計のデバッグ情報を表示します。	**show mls debug**

（注） **show tech-support** コマンドは、スーパバイザ エンジン システム情報を表示します。特定のアプリケーションに関する詳細情報を取得するには、アプリケーション固有のコマンドを使用します。

スイッチ上での MLS IP-directed ブロードキャストの設定

IP-directed ブロードキャストは、主としてティッカー タイプ（株価情報）の装置で使用されますが、ルータ インターフェイス上でこの機能をイネーブルにした場合、悪意ある DoS 攻撃の手段として利用される可能性があります。

IP-directed ブロードキャストは、送信元マシンが直接接続されていないサブネットのブロードキャスト アドレスに送信されるデータグラムです。directed ブロードキャストは、宛先サブネットに到達するまでは、ユニキャスト パケットとしてルーティングされ、宛先サブネットでリンク レイヤ ブロードキャストに変換されます。IP アドレス指定のアーキテクチャにより、IP-directed ブロードキャストを最終的に識別できるのはチェーン内の最後のルータ、つまり宛先サブネットに直接接続されているルータだけです。

Release 7.2(2) より前のスーパバイザ エンジン ソフトウェアでは、MSFC 上で **ip directed-broadcast** コマンドを使用して IP-directed ブロードキャストをイネーブルにすることで、IP-directed ブロードキャスト トラフィックを処理していました。MSFC はプロセス レベルで処理されたため、CPU の使用率は高くなりました。

Release 7.2(2) 以降のソフトウェア リリースでは、ハードウェア（PFC2 を使用）で IP-directed ブロードキャストを処理するように MSFC2 を設定できます。

（注） MSFC2 では、Cisco IOS Release 12.1(11b)E が必要です。

次に、IP-directed ブロードキャストをイネーブルにする例を示します。

```
Router(config-if)# mls ip directed-broadcast ?
  exclude-router  exclude router from recepient list for directed broadcast
  include-router  include router in recepient list for directed broadcast
```

exclude-router オプションを指定すると、IP-directed ブロードキャスト パケットは、ハードウェアで、そのルータを除く VLAN 内のすべてのホストに転送されます。

include-router オプションを指定すると、IP-directed ブロードキャスト パケットは、ハードウェアで、そのルータを含む VLAN 内のすべてのホストに転送されます。このオプションを指定した場合、ルータはその IP-directed ブロードキャスト パケットを二度と転送しません。

このコマンドの **no** 形式は次のとおりです。

```
Router(config-if)# no mls ip directed-broadcast [exclude-router | include-router]
```

no 形式のコマンドを使用すると、インターフェイスの設定がデフォルト モードに戻ります。デフォルト モードでは、IP-directed ブロードキャスト パケットはハードウェアでは転送されません。MSFC2 によってプロセス レベルで処理されます。MSFC2 がパケットを転送するかしないかは、**ip directed-broadcast** コマンドの設定によって決まります。

ip directed-broadcast コマンドと **mls ip directed-broadcast** コマンドが互いに影響し合うことはありません。**ip directed-broadcast** コマンドはソフトウェア転送に、また、**mls ip directed-broadcast** コマンドはハードウェア転送に関与します。

CHAPTER 14

MLS の設定

この章では、Catalyst 6500 シリーズ スイッチに対して Multilayer Switching（MLS; マルチレイヤ スイッチング）を設定する手順について説明します。MLS は、Supervisor Engine1、Policy Feature Card（PFC; ポリシー フィーチャ カード）、および Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）または MSFC2 に対して、IP および Internetwork Packet Exchange（IPX）ユニキャスト レイヤ 3 スイッチング、および IP マルチキャスト レイヤ 3 スイッチング機能を提供します。

(注) この章で使用しているスーパバイザ エンジン コマンドの構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

この章で説明する内容は、次のとおりです。

(注) PFC3A/PFC3B/PFC3BXL と MSFC3 を搭載した Supervisor Engine 720、および PFC3B/PFC3BXL と MSFC2A を搭載した Supervisor Engine 32 は、Cisco Express Forwarding for PFC3（CEF for PFC3）によるレイヤ 3 スイッチングを提供します。詳細については、第 13 章「CEF for PFC2 および CEF for PFC3A の設定」を参照してください。

(注) Supervisor Engine 2、PFC2、および MSFC2 は、Cisco Express Forwarding for PFC2（CEF for PFC2）によるレイヤ 3 スイッチングを提供します。詳細については、第 13 章「CEF for PFC2 および CEF for PFC3A の設定」を参照してください。

レイヤ 3 スイッチングの機能概要

レイヤ 3 スイッチングにより、ルータではなくスイッチが、VLAN（仮想 LAN）間で IP/IPX ユニキャスト トラフィックおよび IP マルチキャスト トラフィックを転送できます。レイヤ 3 スイッチングはハードウェアに実装され、MSFC ではなくスイッチ上で、ワイヤ速度による VLAN 間転送を行います。レイヤ 3 スイッチングを実行するには、MSFC からの最低限のサポートが必要です。レイヤ 3 スイッチングが不可能なトラフィックは、MSFC がルーティングします。

(注)　レイヤ 3 スイッチングは、MSFC 上に設定されているルーティング プロトコルをサポートしています。レイヤ 3 スイッチングは、MSFC 上に設定されているルーティング プロトコルに代わるものではありません。レイヤ 3 スイッチングは IP Protocol Independent Multicast（IP PIM）を使用してマルチキャスト ルートの決定を行います。

Catalyst 6500 シリーズ スイッチ上のレイヤ 3 スイッチングは、トラフィック統計情報を提供します。この情報を利用してトラフィック特性を特定し、管理、プランニング、およびトラブルシューティングに役立てることができます。レイヤ 3 スイッチングは、NetFlow Data Export（NDE;NetFlow データ エクスポート）を使用してフロー統計情報をエクスポートします（NDE の詳細については、第 16 章「NDE の設定」を参照）。

ここでは、Catalyst 6500 シリーズ スイッチ上でのレイヤ 3 スイッチングおよび MLS について説明します。

レイヤ 3 スイッチド パケットの書き換え

VLAN 上の送信元から別の VLAN 上の宛先へパケットをレイヤ 3 スイッチングするとき、スイッチは MSFC から学習した情報に基づいて、出力ポートでパケットの書き換えを行います。この書き換えにより、パケットは MSFC によってルーティングされたかのように見えます。

(注)　スイッチは、IP マルチキャスト パケットを転送するだけでなく、必要に応じて適切な VLAN 上でパケットを複製します。

パケットの書き換えによって変更されるフィールドは、次の 5 つです。

- レイヤ 2（MAC［メディア アクセス制御］）宛先アドレス
- レイヤ 2（MAC）送信元アドレス
- レイヤ 3 IP Time to Live（TTL）または IPX トランスポート コントロール
- レイヤ 3 チェックサム
- レイヤ 2（MAC）チェックサム（別名 FCS［フレーム チェックサム］）

送信元 A と宛先 B が異なる VLAN に所属し、送信元 A が MSFC にパケットを送信して宛先 B へルーティングさせる場合、スイッチはそのパケットが MSFC のレイヤ 2（MAC）アドレスに送信されたことを認識します。

レイヤ 3 スイッチングを実行するため、スイッチはレイヤ 2 フレーム ヘッダーを書き換え、レイヤ 2 宛先アドレスを宛先 B のレイヤ 2 アドレスに変更し、レイヤ 2 送信元アドレスを MSFC のレイヤ 2 アドレスに変更します。レイヤ 3 アドレスは変更しません。

IP ユニキャストおよび IP マルチキャスト トラフィックの場合、スイッチはレイヤ 3 TTL 値を 1 だけ減らし、レイヤ 3 パケット チェックサムを再計算します。IPX トラフィックの場合、スイッチはレイヤ 3 トランスポート コントロール値を 1 だけ増やし、レイヤ 3 パケット チェックサムを再計算します。スイッチはレイヤ 2 フレーム チェックサムを再計算し、書き換えたパケットを宛先 B の VLAN に転送します（または、マルチキャスト パケットの場合、必要に応じて複製します）。

ここでは、パケットを書き換える手順について説明します。

- IP ユニキャストの書き換え（p.14-3）
- IPX ユニキャストの書き換え（p.14-3）
- IP マルチキャストの書き換え（p.14-4）

IP ユニキャストの書き換え

受信 IP ユニキャスト パケットのフォーマットは、（概念的には）次のとおりです。

レイヤ 2 フレーム ヘッダー		レイヤ 3 IP ヘッダー				データ	FCS
宛先	送信元	宛先	送信元	TTL	チェックサム		
MSFC MAC	*Source A MAC*	*Destination B IP*	*Source A IP*	*n*	*calculation1*		

スイッチが IP ユニキャスト パケットの書き換えを行ったあとのフォーマットは、（概念的には）次のとおりです。

レイヤ 2 フレーム ヘッダー		レイヤ 3 IP ヘッダー				データ	FCS
宛先	送信元	宛先	送信元	TTL	チェックサム		
Destination B MAC	*MSFC MAC*	*Destination B IP*	*Source A IP*	*n–1*	*calculation2*		

IPX ユニキャストの書き換え

受信 IPX パケットのフォーマットは、（概念的には）次のとおりです。

レイヤ 2 フレーム ヘッダー		レイヤ 3 IPX ヘッダー			データ	FCS
宛先	送信元	チェックサム / IPX の長さ / トランスポート コントロール	宛先ネットワーク / ノード / ソケット	送信元ネットワーク / ノード / ソケット		
MSFC MAC	*Source A MAC*	*n*	*Destination B IPX*	*Source A IPX*		

スイッチが IPX パケットの書き換えを行ったあとのフォーマットは、（概念的には）次のとおりです。

レイヤ 2 フレーム ヘッダー		レイヤ 3 IPX ヘッダー			データ	FCS
宛先	送信元	チェックサム / IPX の長さ / トランスポート コントロール	宛先ネットワーク / ノード / ソケット	送信元ネットワーク / ノード / ソケット		
Destination B MAC	*MSFC MAC*	*n+1*	*Destination B IPX*	*Source A IPX*		

IP マルチキャストの書き換え

受信 IP マルチキャスト パケットのフォーマットは、（概念的には）次のとおりです。

レイヤ 2 フレーム ヘッダー		レイヤ 3 IP ヘッダー				データ	FCS
宛先	送信元	宛先	送信元	TTL	チェックサム		
Group G1 MAC[1]	*Source A MAC*	*Group G1 IP*	*Source A IP*	*n*	*calculation1*		

1. 上記の例では、Destination B はグループ G1 のメンバーです。

スイッチが IP マルチキャスト パケットの書き換えを行ったあとのフォーマットは、（概念的には）次のとおりです。

レイヤ 2 フレーム ヘッダー		レイヤ 3 IP ヘッダー				データ	FCS
宛先	送信元	宛先	送信元	TTL	チェックサム		
Group G1 MAC	*MSFC MAC*	*Group G1 IP*	*Source A IP*	*n–1*	*calculation2*		

MLS の概要

（注）

Supervisor Engine 1、PFC、および MSFC または MSFC2 は、同じシャーシ内の MSFC/MSFC2 で内部的にしか MLS を実行できません。外部 MLS Route Processor（RP; ルート プロセッサ）を内部 MLS-RP の代わりに使用することはできません。

Supervisor Engine 1、PFC、および MSFC または MSFC2 は、MLS によってレイヤ 3 スイッチングを行います。MLS によるレイヤ 3 スイッチングは、MSFC によって最初のパケットがルーティングされた時点でスイッチ上のフローを識別し、フローの残りのトラフィック転送プロセスをスイッチに移行することによって、MSFC の負荷を軽減します。

ここでは、MLS について説明します。

MLS フローの概要

IP、IPX などのレイヤ 3 プロトコルはコネクションレスです。すなわち、各パケットを他のパケットとは無関係に配信します。ただし、実際のネットワーク トラフィックは多くの場合、ユーザまたはアプリケーション間のエンドツーエンドの対話、またはフローで成り立っています。

MLS は、ユニキャストおよびマルチキャスト フローをサポートしています。

- ユニキャスト フローは、次のいずれかです。
  - 特定の宛先に向けられたすべてのトラフィック
  - 特定の送信元から特定の宛先に向けられたすべてのトラフィック
  - 特定の送信元から特定の宛先に向けられ、プロトコルおよびトランスポート レイヤ情報が共通するすべてのトラフィック

- マルチキャスト フローは、特定の送信元から特定の宛先マルチキャスト グループのメンバーに向けられ、プロトコルおよびトランスポート レイヤ情報が共通するすべてのトラフィックです。

たとえば、クライアントからサーバへの通信、およびサーバからクライアントへの通信は、それぞれ個別のフローです。特定の送信元から特定の宛先に転送される Telnet トラフィックは、同じ送信元および宛先の間で転送される FTP（ファイル転送プロトコル）パケットとは別のフローです。

(注)　PFC はレイヤ 2 マルチキャスト転送テーブルを使用して、レイヤ 2 マルチキャスト トラフィックを転送すべきポート（存在する場合）を識別します。マルチキャスト転送テーブルのエントリは、スイッチ上でイネーブルになっているマルチキャスト制約のある機能（IGMP スヌーピングまたは Generic Attribute Registration Protocol [GARP] Multicast Registration Protocol [GMRP]）によって実装されます。これらのエントリは、宛先マルチキャスト MAC アドレスを、その VLAN への出力スイッチ ポートにマッピングします。

MLS キャッシュの概要

ここでは、MLS キャッシュについて説明します。

MLS キャッシュ

PFC は、レイヤ 3 スイッチド フローのための、MLS キャッシュと呼ばれるレイヤ 3 スイッチング テーブルを維持します。このキャッシュには、パケットのスイッチングと同時に更新されるトラフィック統計情報のエントリも含まれます。PFC が MLS キャッシュ エントリを作成したあと、既存のフローに属することが識別されたパケットは、キャッシュされた情報に基づいて、レイヤ 3 スイッチングされます。MLS キャッシュには、すべてのアクティブ フローに関するフロー情報が維持されます。

ユニキャスト トラフィック

ユニキャスト トラフィックについては、PFC は各ユニキャスト フローで最初にルーティングされたパケットの MLS キャッシュ エントリを作成します。MLS キャッシュ内に現存するユニキャスト フローのどれとも一致しないルーティング済みパケットを受信すると、PFC は新しい MLS エントリを作成します。

マルチキャスト トラフィック

マルチキャスト トラフィックについては、PFC は MSFC から学習した情報を使用して MLS キャッシュを実装します。MSFC は新しいマルチキャスト フローのトラフィックを受信すると、常にマルチキャスト ルーティング テーブルを更新し、新しい情報を PFC に転送します。さらに、マルチキャスト ルーティング テーブルのエントリが期限切れになると、MSFC はそのエントリを削除し、更新された情報を PFC に転送します。

PFC はマルチキャスト フローに関するキャッシュ エントリごとに、宛先 IP マルチキャスト グループへの出力インターフェイスのリストを維持します。PFC はこのリストを使用して、特定のマルチキャスト フローのトラフィックを複製する必要のある VLAN を識別します。

スイッチ上のマルチキャスト MLS キャッシュ エントリに影響する Cisco IOS コマンドは、次のとおりです。

- **clear ip mroute** コマンドを使用して MSFC 上のマルチキャスト ルーティング テーブルを消去すると、PFC 上のマルチキャスト MLS キャッシュ エントリがすべて消去されます。
- **no ip multicast-routing** コマンドを使用して MSFC 上で IP マルチキャスト ルーティングをディセーブルにすると、PFC 上のマルチキャスト MLS キャッシュ エントリがすべて削除されます。

MLS キャッシュのエージング

パケット トラフィックがアクティブであるかぎり、フローの状態およびアイデンティティが維持されます。フローのトラフィックがなくなると、エントリは期限切れになります。MLS キャッシュに保存される MLS エントリのエージング タイムを設定できます。あるエントリが一定期間にわたって使用されない状態が続くと、そのエントリは期限切れになり、そのフローに関する統計情報をフロー コレクタ アプリケーションにエクスポートできるようになります。

MLS キャッシュ サイズ

最大 MLS キャッシュ サイズ（エントリ数）は、128,000 です。MLS キャッシュは、スイッチ上のすべての MLS プロセス（IP MLS、IP MMLS、および IPX MLS）によって共有されます。MLS キャッシュ エントリ数が 32,000 を超えると、フローがレイヤ 3 スイッチングされず、MSFC に転送される可能性が高くなります。

フロー マスクの概要

PFC は、フロー マスクを使用して MLS エントリの作成方法を決定します。

ここでは、フロー マスク モードについて説明します。

- フロー マスク モード ― Release 8.5(1) より前のソフトウェア リリース（p.14-6）
- フロー マスク モード ― Release 8.5(1) 以降のソフトウェア リリース（p.14-7）
- フロー マスク モードおよび show mls entry コマンドの出力（p.14-9）

フロー マスク モード ― Release 8.5(1) より前のソフトウェア リリース

PFC は、その PFC がレイヤ 3 スイッチングするすべての MSFC について、1 つのフロー マスク（最も固有性の高いフロー マスク）だけをサポートします。PFC がレイヤ 3 スイッチングの実行対象にしている MSFC 別に異なるフロー マスクを検出した場合、検出したフロー マスクの中で最も固有性の高いものにフロー マスクを変更します。

PFC フロー マスクが変化すると、MLS キャッシュ全体が削除されます。PFC がキャッシングしたエントリをエクスポートするとき、現在のフロー マスクに基づいてフロー レコードが作成されます。現在のフロー マスクによっては、フロー レコードの一部のフィールドに値が入らない場合があります。サポートされていないフィールドには、ゼロ（0）が充填されます。

MLS フロー マスクは、次のとおりです。

- destination-ip ― 最も固有性の低いフロー マスク。PFC は、レイヤ 3 宛先アドレスごとに 1 つの MLS エントリを維持します。特定のレイヤ 3 宛先アドレスに向けられたフローはすべて、この MLS エントリを使用します。

- destination-ipx ― IPX MLS の唯一のフロー マスク モードが、destination モードです。PFC は、宛先 IPX アドレス（ネットワークおよびノード）ごとに、1 つの IPX MLS エントリを維持します。特定の宛先 IPX アドレスに向けられたフローはすべて、この IPX MLS エントリを使用します。
- source-destination-ip ― PFC は、送信元および宛先 IP アドレスのペアごとに 1 つの MLS エントリを維持します。特定の送信元と宛先の間でやりとりされるフローはすべて、IP プロトコル ポートとは無関係に、この MLS エントリを使用します。
- source-destination-vlan ― IP MMLS 用。PFC は、{source IP, destination group IP, source VLAN} ごとに 1 つの MMLS キャッシュ エントリを維持します。マルチキャスト source-destination-vlan フロー マスクが IP ユニキャスト MLS source-destination-ip フロー マスクと異なる点は、IP MMLS の場合、エントリに送信元 VLAN が含まれている点です。送信元 VLAN は、そのマルチキャスト フローのマルチキャスト Reverse Path Forwarding（RPF）インターフェイスです。
- full flow ― 最も固有性の高いフロー マスク。PFC は、IP フローごとに個別の MLS キャッシュ エントリを作成および維持します。full flow エントリには、送信元 IP アドレス、宛先 IP アドレス、プロトコル、およびプロトコル ポートが含まれます。

フロー マスク モード ― Release 8.5(1) 以降のソフトウェア リリース

Release 8.5(1) 以降のソフトウェア リリースでは、Supervisor Engine 720 上で複数のフロー マスク機能がサポートされます。この機能により、いくつかの NDE 機能が変更されます。

フロー マスクの新しい値は、**null** です。**set mls flow null** コマンドを入力して、フロー マスクをヌル（ヌルは新しいデフォルトのフロー マスクです）に設定します。フロー マスクが **null** に設定され、他の機能でより固有性の高いフロー マスクを使用していない場合、すべてのフローは同じヌル フローに一致します。ヌル フローのカウンタは、フローがヌル フローに一致するたびに加算されます。フロー マスクがヌルで、他の機能でフロー マスクを使用していない場合に、**show mls statistics entry** コマンドを入力すると、コマンド出力で次のようにヌル フローが表示されます（この例では、NDE がディセーブルのため、フローはエクスポートされません）。

```
Console> (enable) show mls statistics entry
Flowmask set to Null. Please set the flowmask to see the flows
                                  Last    Used
Destination IP   Source IP       Prot  DstPrt SrcPrt Vlan  Stat-Pkts  Stat-Bytes

--------------- --------------- ----- ------ ------ ----- ---------  -----------
 -              -               -     -      -      N/A  728915    33530090

Console> (enable)
```

フローの作成をイネーブルにする場合は、**set mls flow** {**destination** | **destination-source** | **null** | **full**} コマンドで **null** 以外のキーワードを指定してフロー マスクを指定します。**null** フロー マスクが設定されている場合に、NDE をイネーブルにすると、NDE はフローをエクスポートしません。例は次のとおりです。

```
Console> (enable) set mls nde enable
Netflow export enabled
Console> (enable) 2005 Sep 18 18:04:43 %MLS-5-FLOWMASK_NULL:IP Flowmask set to
Null:Flows will not be exported
```

逆に、NDE がイネーブルの場合に、フロー マスクを **null** に設定すると、次のメッセージが表示されます。

```
Console> (enable) set mls flow null
2000 Sep 18 18:04:02 %MLS-5-FLOWMASK_NULL:IP Flowmask set to Null:Flows will not be
exported
Console> (enable)
```

Release 8.4(x) から Release 8.5(1) 以降にアップグレードする場合は、次の点に注意してください。

- バイナリ コンフィギュレーション モードの場合
  - Release 8.4(x) では、**set mls flow xxx** コマンドを入力してフロー マスクを「xxx」に設定した場合（xxx はキーワード オプションの*いずれか*）、フロー マスクはアップグレード後も **xxx** のままです。
  - Release 8.4(x) で、フロー マスクを設定しなかった場合、フロー マスクはアップグレード後 **destination** となります。
- テキスト コンフィギュレーション モード
  - Release 8.4(x) で、**set mls flow destination** コマンドを入力してフロー マスクを **destination** に設定した場合、フロー マスクはアップグレード後 **null**（新しいデフォルト）となります。
  - Release 8.4(x) で、フロー マスクを設定しなかった場合、フロー マスクはアップグレード後 **null** となります。
  - Release 8.4(x) で、フロー マスクを **destination** 以外のいずれかのキーワード オプションに設定した場合、フロー マスクはアップグレード後設定したフロー マスクと同じものになります。

スイッチ上では複数のフロー マスクが共存できるため、**show mls statistics entry** コマンドによりフローごとの関連フィールドのみが表示されます。特定のフローを作成するのに使用されるフロー マスクによって、関連フィールドが消去されます。フロー コレクタ ソフトウェアでは、NDE が使用されます。NDE は、すべてのフローは同じフロー マスクにより作成されると想定します。この制限事項のために、NDE は、異なるフロー マスクが必要な特定の機能と同時にイネーブルにできません。明確なケースとして、ハードウェア高速化 Network Address Translation（NAT; ネットワーク アドレス変換）があります。NDE とハードウェア高速化 NAT は、同時に使用できません。

Release 8.5(1) では、一部の MSFC 機能にハードウェア アクセラレーションを導入します。Release 8.4(x) から Release 8.5(1) にアップグレードする場合は、設定済みおよび稼働中の MSFC 機能に関する問題はありません。フロー マスクの競合がなければ、NAT のほかに再帰 Access Control List（ACL; アクセス制御リスト）および Context-Based Access Control（CBAC; コンテキスト ベースのアクセス制御）がハードウェア内で機能できます。NDE または Quality of Service（QoS; サービス品質）マイクロフロー ポリサーなどの他の機能と競合するフロー マスクを必要とする機能でなければ、ハードウェア内で機能します。

また、Release 8.5(1) では、WCCP および TCP 代行受信でもハードウェア アクセラレーションが使用できます。これらの MSFC 機能は、フロー マスクの競合がない限り、NDE と共存できます。ACL マネージャは、異なる機能のフロー マスク要件をマージしようとします。基本的には、すでに割り当てられたフロー マスクとの互換性がない狭義のフロー マスク要件専用に新しいフロー マスクを割り当てます。NDE には狭義のフロー マスク要件がないため、NDE のフロー マスクは狭義にすることができます。

フロー マスクが NDE に設定されている場合（フロー マスクの表示には **show mls** コマンドを使用）に、NAT でハードウェア アクセラレーション機能を使用するには、次の手順を実行します。

ステップ 1　**set mls flow null** コマンドを入力します。

ステップ 2　MSFC は、フロー マスクの要求が必要です。これには、特定の MSFC 機能を再設定する必要があります。

次のいずれかのイベントが発生した場合、NDE は失敗します。

- ハードウェア高速化 NAT がイネーブルである。
- スイッチ上に競合するフロー マスクが設定された複数の機能がある。

逆に、NDE の設定が成功すれば、NAT をハードウェアで機能するように設定できません。また、フロー マスク要件が競合する 2 つの異なる機能は、スイッチ上で設定できません。

Release 8.5(1) は、スイッチ上の各種機能で使用されるフロー マスクを表示する **show mls flowmask** コマンドを導入しました。

次に、MSFC 上で機能がなにも設定されていない場合の各種設定の出力例を示します。

```
Console> show mls flowmask
Netflow Data Export is enabled
NDE Flowmask is configured to use at least Null flowmask
Console>

Console> show mls flowmask
Netflow Data Export is enabled and is using Full flowmask
NDE Flowmask is configured to use at least Full flowmask
Console>

Console> show mls flowmask
Netflow Data Export is disabled
NDE Flowmask is configured to use at least Full flowmask
Console>
```

次に、NAT が MSFC に設定されている場合の出力を示します。

```
Console> show mls flowmask
The MSFC features are using NotVlanFullFlow and VlanFullFlowOnly flow mask on vlan(s)
10-11,50-51,90-91.
Netflow Data Export is disabled
NDE Flowmask is configured to at least the Null flowmask
Console>
```

次に、MSFC 上で再帰 ACL 機能が設定されている場合の各種設定の出力例を示します。

```
Console> show mls flowmask
The MSFC features are using VlanFullFlowOnly flow mask on vlan(s) 13.
Netflow Data Export is disabled
NDE Flowmask is configured to use at least Null flowmask
Console>

Console> show mls flowmask
The MSFC features are using VlanFullFlowOnly flow mask on vlan(s) 13.
Netflow Data Export is enabled and is using Full-Vlan flowmask
NDE Flowmask is configured to use at least Full-Vlan flowmask
Console>
```

フロー マスク モードおよび show mls entry コマンドの出力

destination-ip フロー マスクの場合、送信元 IP、プロトコル、および送信元と宛先ポートの各フィールドに、MLS キャッシュ エントリを使用して最後にレイヤ 3 スイッチングされたパケットの詳細情報が表示されます。

次に、destination-ip モードでの **show mls entry** コマンドの出力例を示します。

```
Console> (enable) show mls entry ip short
Destination-IP  Source-IP       Prot  DstPrt SrcPrt Destination-Mac   Vlan
--------------- --------------- ----- ------ ------ ----------------- ----
 ESrc EDst SPort DPort Stat-Pkts Stat-Byte    Uptime   Age
 ---- ---- ----- ----- --------- ------------ -------- --------
171.69.200.234  -               -     -      -      00-60-70-6c-fc-22 4
 ARPA SNAP 5/8   11/1  3152      347854       09:01:19 09:08:20
171.69.1.133    -               -     -      -      00-60-70-6c-fc-23 2
 SNAP ARPA 5/8   1/1   2345      123456       09:03:32 09:08:12

Total Entries: 2
* indicates TCP flow has ended
Console> (enable)
```

(注) 一部の **show** コマンドには **short** キーワードがあり、これを使用するとテキストが 80 文字で折り返されて出力されます。デフォルトは **long**（テキストの折り返しなし）です。

source-destination-ip フロー マスクの場合、プロトコル、送信元ポート、および宛先ポートの各フィールドに、MLS キャッシュ エントリを使用して最後にレイヤ 3 スイッチングされたパケットの詳細情報が表示されます。

次に、source-destination-ip モードでの **show mls entry** コマンドの出力例を示します。

```
Console> (enable) show mls entry ip short
Destination-IP  Source-IP       Prot  DstPrt SrcPrt Destination-Mac   Vlan
--------------- --------------- ----- ------ ------ ----------------- ----
 ESrc EDst SPort DPort Stat-Pkts Stat-Byte    Uptime   Age
 ---- ---- ----- ----- --------- ------------ -------- --------
171.69.200.234  171.69.192.41   -     -      -      00-60-70-6c-fc-22 4
 ARPA SNAP 5/8   11/1  3152      347854       09:01:19 09:08:20
171.69.1.133    171.69.192.42   -     -      -      00-60-70-6c-fc-23 2
 SNAP ARPA 5/8   1/1   2345      123456       09:03:32 09:08:12

Total Entries: 2
* indicates TCP flow has ended
Console> (enable)
```

full-flow フロー マスクの場合、IP フローごとに個別の MLS エントリが作成されるので、フロー別に詳細情報が表示されます。

次に、full flow モードでの **show mls entry** コマンドの出力例を示します。

```
Console> (enable) show mls entry ip short
Destination-IP  Source-IP       Prot  DstPrt SrcPrt Destination-Mac   Vlan
--------------- --------------- ----- ------ ------ ----------------- ----
 ESrc EDst SPort DPort Stat-Pkts Stat-Byte    Uptime   Age
 ---- ---- ----- ----- --------- ------------ -------- --------
171.69.200.234  171.69.192.41   TCP*  6000   59181  00-60-70-6c-fc-22 4
 ARPA SNAP 5/8   11/1  3152      347854       09:01:19 09:08:20
171.69.1.133    171.69.192.42   UDP   2049   41636  00-60-70-6c-fc-23 2
 SNAP ARPA 5/8   1/1   2345      123456       09:03:32 09:08:12

Total Entries: 2
* indicates TCP flow has ended
Console> (enable)
```

マルチキャスト フローの部分的スイッチングおよび完全スイッチング

次の状況では、一部のフローが完全にレイヤ 3 スイッチングされずに、部分的にレイヤ 3 スイッチングされる可能性があります。

- マルチキャスト送信元の RPF インターフェイスで、MSFC が IP マルチキャスト グループのメンバーとして設定されている場合（**ip igmp join-group** コマンドを使用）
- MSFC が PIM sparse モードの送信元への第 1 ホップ ルータである場合（この場合、MSFC は Rendezvous point（RP; ランデブー ポイント）に PIM-register メッセージを送信しなければなりません）
- フローの出力インターフェイス上にマルチキャスト TTL スレッシュホールドが設定されている場合
- RPF インターフェイスの拡張アクセス リスト拒否条件でレイヤ 3 送信元、レイヤ 3 宛先、または IP プロトコル以外のもの（レイヤ 4 ポート番号など）が指定されている場合
- フローの RPF インターフェイスにマルチキャスト ヘルパーが設定されていて、かつマルチキャストからブロードキャストへの変換が必要な場合
- 出力インターフェイス上にマルチキャスト タグ スイッチングが設定されている場合
- インターフェイス上に NAT が設定されていて、かつ発信インターフェイスのために送信元アドレスの変換が必要な場合

部分的にスイッチングされるフローでは、そのフローに所属するすべてのマルチキャスト トラフィックが MSFC に到達し、レイヤ 3 スイッチングの対象にならないインターフェイスについてはソフトウェア スイッチングが行われます。

PFC は完全にレイヤ 3 スイッチングされたフロー内のマルチキャスト トラフィックが MSFC に到達するのを防ぎ、MSFC の負荷を軽減します。**show ip mroute** および **show mls ip multicast** コマンドは、完全にレイヤ 3 スイッチングされるフローを文字列 [RPF-MFD] で識別します。Multicast Fast Drop（MFD）は、MSFC 側から見た場合、マルチキャスト パケットが PFC によってスイッチングされたために廃棄されたことを示します。

完全にレイヤ 3 スイッチングされるすべてのフローでは、PFC はマルチキャスト パケットおよびバイト カウント統計情報を定期的に MSFC に送信します。MSFC は完全にスイッチングされるフローを確認することができず、マルチキャスト統計情報を記録できないためです。MSFC はこの統計情報を使用して、対応するマルチキャスト ルーティング テーブル エントリを更新し、適切な期限タイマーをリセットします。

MLS の例

図 14-1 に、単純な IP MLS ネットワーク トポロジーを示します。この例では、ホスト A は販売部門の VLAN（IP サブネット 171.59.1.0）、ホスト B はマーケティング部門の VLAN（IP サブネット 171.59.3.0）、ホスト C はエンジニアリング部門の VLAN（IP サブネット 171.59.2.0）にあります。

ホスト A がホスト C に対して HTTP ファイル転送を開始すると、このフローに対応する MLS エントリが作成されます（このエントリは図 14-1 に示されている MLS キャッシュの 2 番めの項目です）。MSFC がホスト A からの最初のパケットをスイッチ経由でホスト C に転送するとき、PFC は MSFC およびホスト C の MAC アドレスを、この MLS エントリに格納します。PFC はこの情報を使用して、ホスト A からホスト C への後続のパケットを書き換えます。

図 14-1　IP MLS トポロジーの例

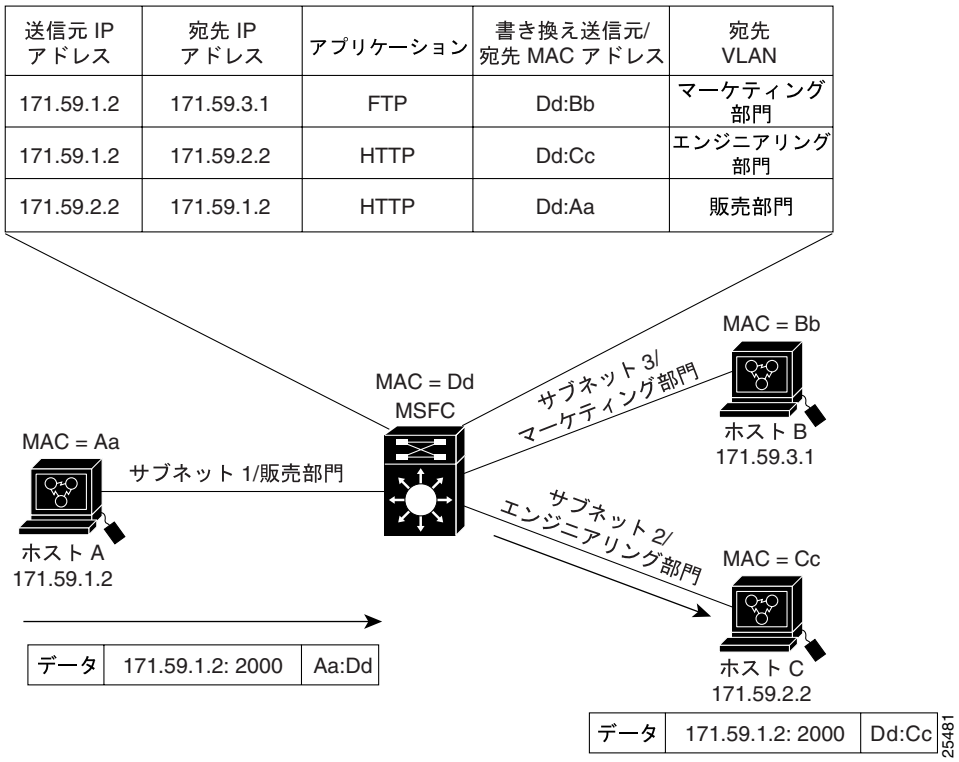
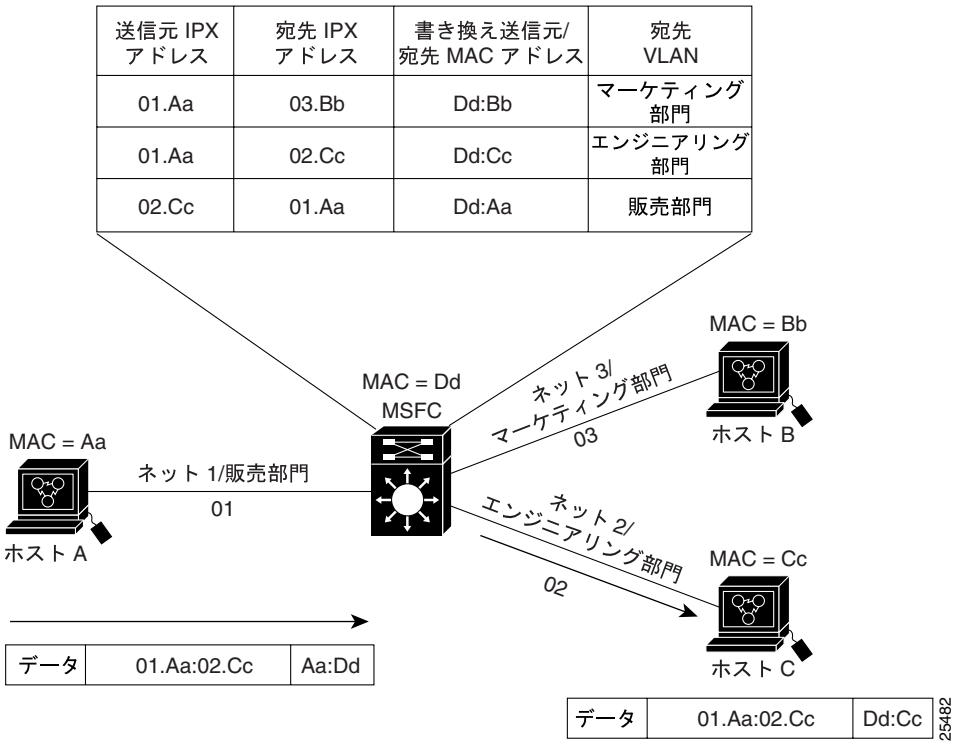


図 14-2 に、単純な IPX MLS ネットワーク トポロジーを示します。この例では、ホスト A は販売部門の VLAN（IPX アドレス 01.Aa）、ホスト B はマーケティング部門の VLAN（IPX アドレス 03.Bb）、ホスト C はエンジニアリング部門の VLAN（IPX アドレス 02.Cc）にあります。

ホスト A がホスト B に対してファイル転送を開始すると、このフローに対応する IPX MLS エントリが作成されます（このエントリは、図 14-1 に示されている表の最初の項目です）。MSFC がホスト A からの最初のパケットをスイッチ経由でホスト B に転送するとき、PFC は MSFC およびホスト B の MAC アドレスを、この IPX MLS エントリに格納します。PFC はこの情報を使用して、ホスト A からホスト B への後続のパケットを書き換えます。

同様に、ホスト A からホスト C へのトラフィック、さらにホスト C からホスト A へのトラフィックについても、MLS キャッシュに個別の IPX MLS エントリが作成されます。トランク リンク上でトラフィックをカプセル化するとき正しい VLAN ID が使用されるようにするため、各 IPX MLS エントリの一部分として宛先 VLAN が格納されます。

図 14-2　IPX MLS トポロジーの例



MLS のデフォルト設定

表 14-1 に、IP MLS のデフォルト設定を示します。

表 14-1　IP MLS のデフォルト設定

機能	デフォルト値
IP MLS のイネーブル ステート	イネーブル
IP MLS エージング タイム	256 秒
IP MLS ファスト エージング タイム	0 秒（ファスト エージングなし）
IP MLS ファスト エージング タイムの パケット スレッシュホールド	0 パケット

表 14-2 に、IP MMLS スイッチのデフォルト設定を示します。

表 14-2　IP MMLS スーパバイザ エンジンのデフォルト設定

機能	デフォルト値
マルチキャスト サービス（IGMP スヌーピングまたは GMRP）	ディセーブル
IP MMLS	イネーブル

表 14-3 に、IP MMLS MSFC のデフォルト設定を示します。

表 14-3　IP MMLS MSFC のデフォルト設定

機能	デフォルト値
マルチキャスト ルーティング	グローバルにディセーブル
IP PIM ルーティング	すべてのインターフェイス上でディセーブル
IP MMLS スレッシュホールド	設定なし ― デフォルト値なし
IP MMLS	マルチキャスト ルーティングがイネーブルで、かつインターフェイス上で IP PIM がイネーブルになっている場合、イネーブル

表 14-4 に、IPX MLS のデフォルト設定を示します。

表 14-4　IPX MLS のデフォルト設定

機能	デフォルト値
IPX MLS のイネーブル ステート	イネーブル
IPX MLS エージング タイム	256 秒

設定時の注意事項および制限事項

ここでは、IP MLS、IP MMLS、および IPX MLS の設定時の注意事項および制限事項について説明します。

IP MLS

ここでは、IP MLS 設定時の注意事項について説明します。

MTU サイズ

IP MLS のデフォルトの Maximum Transmission Unit（MTU; 最大伝送ユニット）は 1500 です。IP MLS がイネーブルに設定されたインターフェイス上の MTU を変更するには、**ip mtu** *mtu* コマンドを使用します。

IP MLS をイネーブルにして IP ルーティング コマンドを使用する場合の制限事項

インターフェイス上で特定の IP プロセスをイネーブルにすると、そのインターフェイス上の IP MLS に影響があります。表 14-5 に、影響のあるコマンドとその動作を示します。

表 14-5　IP ルーティング コマンドの制限事項

コマンド	動作
clear ip route	この MSFC にレイヤ 3 スイッチングを実行しているすべてのスイッチの MLS キャッシュ エントリを消去します。
ip routing	**no** 形式を使用すると、すべての MLS キャッシュ エントリが削除され、この MSFC 上で IP MLS がディセーブルになります。
ip security（このコマンドのすべての形式）	インターフェイス上で IP MLS をディセーブルにします。
ip tcp compression-connections	インターフェイス上で IP MLS をディセーブルにします。
ip tcp header-compression	インターフェイス上で IP MLS をディセーブルにします。

IP MMLS

ここでは、IP MMLS 設定時の注意事項について説明します。

IP MMLS スーパバイザ エンジンの注意事項および制限事項

ここでは、Supervisor Engine 1 に IP MMLS を設定する際の注意事項と制限事項を説明します。

- IP マルチキャスト パケットについては、ARPA 書き換えだけがサポートされています。
- Subnetwork Address Protocol（SNAP）書き換えはサポートされていません。
- IP MMLS を使用するには、スイッチ上でいずれかのマルチキャスト サービス（IGMP スヌーピングまたは GMRP）をイネーブルにする必要があります。
- レイヤ 2 マルチキャスト転送テーブルにエントリがない場合（レイヤ 2 マルチキャスト サービスが 1 つもイネーブルになっていない場合、または転送テーブルがいっぱいの場合など）には、IP マルチキャスト フローはマルチレイヤ スイッチングされません。特定の IP マルチキャスト宛先についてレイヤ 2 エントリを確認するには、**show multicast group** コマンドを使用します。
- レイヤ 2 エントリが消去されると、対応するレイヤ 3 フロー情報が削除されます。
- 同じ VLAN に 1 つまたは複数のインターフェイスを持つ 2 つの MSFC を使用する場合、スイッチは 2 つの予約済み VLAN（VLAN 1012 および 1013）を内部的に使用して、マルチキャスト フローを適切に転送します。
- レイヤ 3 スイッチング ハードウェアを備えた Catalyst 5000 ファミリー スイッチに対しては、MSFC は外部ルータとして動作しません。

IP MMLS MSFC 設定に関する制限事項

次の場合には、IP MMLS は IP マルチキャスト フローに対するマルチレイヤ スイッチングを実行しません。

- 下記の範囲の IP マルチキャスト グループ（* は、0 ～ 255 です）。

  224.0.0.* ～ 239.0.0.*
  224.128.0.* ～ 239.128.0.*

（注） 224.0.0.* の範囲のグループはルーティング コントロール パケット用に予約されており、VLAN のすべての転送ポートにフラッディングする必要があります。これらのアドレスは、マルチキャスト MAC アドレス範囲 01-00-5E-00-00-*xx*（*xx* は 0 ～ 0xFF）にマッピングされます。

- IP PIM 自動 RP マルチキャスト グループ（IP マルチキャスト グループ アドレス 224.0.1.39 および 224.0.1.40）。

（注） 冗長 MSFC を装備したシステムの場合、IP PIM インターフェイス設定は、アクティブ MSFC と冗長 MSFC の両方で同じでなければなりません。

- インターフェイスまたはグループが IP PIM sparse（疎）モードで動作しているとき、マルチキャスト共有ツリーで転送されるフロー（{*,G,*} 転送）。
- インターフェイスまたはグループが IP PIM sparse モードで動作しているとき、フローの Shortest-Path Tree（SPT）ビットがクリアされている場合。
- フラグメント化された IP パケットおよび IP オプション付きのパケット。ただし、フローの中でフラグメント化されていないパケット、または IP オプションを指定されていないパケットは、マルチレイヤ スイッチングの対象になります。
- トンネル インターフェイスで受信した送信元トラフィック（MBONE トラフィックなど）。
- マルチキャスト タグ スイッチングがイネーブルに設定された RPF インターフェイス。

サポートされていない IP MMLS 機能

IP MMLS をイネーブルに設定した場合、インターフェイスに関する IP アカウンティングは正確な値を反映しません。

IPX MLS

ここでは、IPX MLS 設定時の注意事項について説明します。

- IPX MLS と他の機能との相互作用（p.14-17）
- IPX MLS および MTU サイズ（p.14-17）

IPX MLS と他の機能との相互作用

IPX MLS に影響を及ぼす他の Cisco IOS ソフトウェア機能は、次のとおりです。

- IPX アカウンティング ― IPX MLS がイネーブルに設定されたインターフェイス上では、IPX アカウンティングをイネーブルにすることはできません。
- IPX EIGRP ― Enhanced Interior Gateway Routing Protocol（EIGRP）インターフェイス上で MLS をサポートするには、Transport Control（TC; トランスポート コントロール）最大値をデフォルト（16）より大きい値に設定する必要があります。MSFC 上で **ipx maximum-hop** *tc_value* グローバル コンフィギュレーション コマンドを、16 より大きい *tc_value* にして入力します。

IPX MLS および MTU サイズ

IPX では、通信の 2 つのエンド ポイントは MTU をネゴシエートします。MTU サイズはメディア タイプによって制限されます。

MLS の設定

ここでは、MLS を設定する手順について説明します。

MSFC 上でのユニキャスト MLS の設定

ここでは、MSFC 上で MLS を設定する手順について説明します。

MSFC 上でルーティングを設定する手順については、第 12 章「VLAN 間ルーティングの設定」を参照してください。Supervisor Engine 1 上でユニキャスト レイヤ 3 スイッチングを設定する手順については、「Supervisor Engine 1 上での MLS の設定」（p.14-21）を参照してください。

（注） MSFC は、MLS を使用する Catalyst 5000 ファミリー スイッチの MLS-RP として指定できます。MLS の設定手順については、『*Layer 3 Switching Configuration Guide ― Catalyst 5000 Family, 2926G Series, 2926 Series Switches*』を参照してください。

MSFC インターフェイス上でのユニキャスト MLS のディセーブル化およびイネーブル化

IP および IPX に関するユニキャスト MLS はデフォルトでグローバルにイネーブルに設定されていますが、特定のインターフェイス上でディセーブルおよびイネーブルに設定できます。

特定の MSFC インターフェイス上でユニキャスト IP MLS または IPX MLS をディセーブルにするには、次のいずれかの作業を行います。

作業	コマンド
MSFC インターフェイスを指定します。	Router(config)# **interface** *vlan-id*
MSFC インターフェイス上で IP MLS をディセーブルにします。	Router(config-if)# **no mls ip**
MSFC インターフェイス上で IPX MLS をディセーブルにします。	Router(config-if)# **no mls ipx**

次に、MSFC インターフェイス上で IP MLS をディセーブルにする例を示します。

```
Router(config)# interface vlan 100
Router(config-if)# no mls ip
Router(config-if)#
```

次に、MSFC インターフェイス上で IPX MLS をディセーブルにする例を示します。

```
Router(config)# interface vlan 100
Router(config-if)# no mls ipx
Router(config-if)#
```

（注） ユニキャスト MLS はデフォルトでイネーブルに設定されています。イネーブルにする（または再びイネーブルにする）必要があるのは、以前にディセーブルにした場合だけです。

特定の MSFC インターフェイス上でユニキャスト IP MLS または IPX MLS をイネーブルにするには、次の作業を行います。

	作業	コマンド
ステップ 1	MSFC インターフェイスを指定します。	Router(config)# **interface** *vlan-id*
ステップ 2	MSFC インターフェイス上で IP または IPX MLS をイネーブルにします。	Router(config-if)# **mls ip** または Router(config-if)# **mls ipx**

次に、MSFC インターフェイス上で IP MLS をイネーブルにする例を示します。

```
Router(config)# interface vlan 100
Router(config-if)# mls ip
Router(config-if)#
```

次に、MSFC インターフェイス上で IPX MLS をイネーブルにする例を示します。

```
Router(config)# interface vlan 100
Router(config-if)# mls ipx
Router(config-if)#
```

MSFC 上での MLS 情報の表示

show mls status コマンドは、MLS の詳細情報を表示します。MSFC 上の MLS 情報を表示するには、次の作業を行います。

作業	コマンド
MLS のステータスを表示します。	**show mls status**

次に、MSFC 上の MLS ステータスを表示する例を示します。

```
Router# show mls status
MLS global configuration status:
global mls ip:                      enabled
global mls ipx:                     enabled
global mls ip multicast:            disabled
current ip flowmask for unicast:    destination only
current ipx flowmask for unicast:   destination only
Router#
```

MSFC 上での debug コマンドの使用方法

表 14-6 に、MSFC 上で MLS の問題のトラブルシューティングに使用できる MLS 関連の debug コマンドについて説明します。

表 14-6　MLS の debug コマンド

コマンド	説明
[no] debug l3-mgr events	レイヤ 3 マネージャ関連のイベントを表示します。
[no] debug l3-mgr packets	レイヤ 3 マネージャ パケットを表示します。
[no] debug l3-mgr global	IP のグローバル パージ イベントのバグトレースを表示します。
[no] debug l3-mgr all	レイヤ 3 マネージャのデバッグ メッセージをすべてオンにします。

表 14-7 に、MSFC を Catalyst 5000 ファミリー スイッチの外部ルータとして使用する場合に、MLS の問題のトラブルシューティングに使用できる、MLS 関連の debug コマンドについて説明します。

表 14-7　MLS の debug コマンド ― 外部ルータ機能

コマンド	説明
[no] debug mls ip	IP 関連の MLS イベント（ルートの削除、アクセス リストおよびフロー マスクの変更など）をオンにします。
[no] debug mls ipx	IPX 関連の MLS イベント（ルートの削除、アクセス リストおよびフロー マスクの変更など）をオンにします。
[no] debug mls rp	ルート プロセッサ関連のイベントをオンにします。
[no] debug mls locator	MLS 探索パケットを使用して、特定のフローをスイッチングしているスイッチを特定します。
[no] debug mls all	すべての MLS デバッグ イベントをオンにします。

SCP に関する debug コマンドの使用方法

表 14-8 に、Ethernet Out-of-Band Channel（EOBC）で動作する Serial Control Protocol（SCP）をトラブルシューティングするための、SCP 関連の debug コマンドを示します。

表 14-8　SCP の debug コマンド

コマンド	説明
[no] debug scp async	SCP システムを出入りする非同期データのトレースを表示します。
[no] debug scp data	パケット データのトレースを表示します。
[no] debug scp errors	SCP のエラーおよび警告を表示します。
[no] debug scp packets	SCP システムを出入りするパケット データを表示します。
[no] debug scp timeouts	タイムアウトを報告します。
[no] debug scp all	すべての SCP デバッグ メッセージをオンにします。

Supervisor Engine 1 上での MLS の設定

Catalyst 6500 シリーズ スイッチ上では、MLS はデフォルトでイネーブルに設定されています。Supervisor Engine 1 を設定する必要があるのは、次の場合だけです。

- MLS のエージング タイムを変更する場合
- NDE をイネーブルにする場合

ここでは、Supervisor Engine 1 上で MLS を設定する手順について説明します。

スイッチ上で VLAN を設定する手順については、第 11 章「VLAN の設定」を参照してください。MSFC 上で MLS を設定する手順については、「MSFC 上でのユニキャスト MLS の設定」（p.14-18）を参照してください。

（注） MSFC 上で IP または IPX MLS をディセーブルにすると、Supervisor Engine 1 上で IP または IPX MLS が自動的にディセーブルになります。既存のプロトコル固有の MLS キャッシュ エントリはすべて削除されます。MSFC 上で MLS をディセーブルにする方法については、「MSFC インターフェイス上でのユニキャスト MLS のディセーブル化およびイネーブル化」（p.14-18）を参照してください。

（注） NDE がイネーブルに設定されている場合に MLS をディセーブルにすると、既存のキャッシュ エントリに関する統計情報が失われ、エクスポートされなくなります。

MLS エージング タイム値の指定

各プロトコル（IP および IPX）の MLS エージング タイムは、プロトコル固有のすべての MLS キャッシュ エントリに適用されます。*agingtime* で指定される期間（秒）にわたって使用されなかった MLS エントリは、期限切れになります。デフォルトは 256 秒です。

エージング タイムは、8 ～ 2,032 秒の範囲で、8 秒の倍数で設定できます。8 秒の倍数以外のエージング タイム値を指定すると、最も近い 8 秒の倍数に調整されます。たとえば 65 は 64 に、127 は 128 に調整されます。

(注) MLS キャッシュのサイズは、エントリ数 32,000 以下にすることを推奨します。MLS エントリ数が 32,000 を超えると、一部のフローが MSFC に送信されます。MLS キャッシュのサイズを小さくするには、IP の場合、IP MLS ファスト エージングをイネーブルにします（「IP MLS の長期エージング タイム、ファスト エージング タイム、およびパケット スレッシュホールド値の指定」[p.14-23]を参照）。

IP および IPX の両方について MLS エージング タイムを指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
MLS キャッシュ エントリの MLS エージング タイムを指定します。	**set mls agingtime** [*agingtime*]

次に、MLS エージング タイムを指定する例を示します。

```
Console> (enable) set mls agingtime 512
Multilayer switching agingtime IP and IPX set to 512
Console> (enable)
```

IP MLS エージング タイムを指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
MLS キャッシュ エントリの IP MLS エージング タイムを指定します。	**set mls agingtime ip** [*agingtime*]

次に、IP MLS エージング タイムを指定する例を示します。

```
Console> (enable) set mls agingtime ip 512
Multilayer switching aging time IP set to 512
Console> (enable)
```

IPX MLS エージング タイムを指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
MLS キャッシュ エントリの IPX MLS エージング タイムを指定します。	**set mls agingtime ipx** [*agingtime*]

IPX MLS エージング タイムを指定する例を示します。

```
Console> (enable) set mls agingtime ipx 512
Multilayer switching aging time IPX set to 512
Console> (enable)
```

IP MLS の長期エージング タイム、ファスト エージング タイム、およびパケット スレッシュホールド値の指定

（注）　IPX MLS は、ファスト エージングを使用しません。IPX MLS は、destination-source および destination フロー モードでのみ動作します。したがって、MLS テーブルの IPX MLS エントリ数は、full-flow モードの IP MLS エントリ数と比較すると少なくなります。

MLS キャッシュ サイズをエントリ数 32,000 以下にするには、IP MLS ファスト エージング タイムをイネーブルにします。IP MLS ファスト エージング タイムは、MLS エントリのうち、作成後 *fastagingtime* 秒以内にスイッチングされたパケット数が *pkt_threshold* 個に満たないものに適用されます。一般に、Domain Name Server（DNS; ドメイン ネーム サーバ）または Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバとの間のフローに対応するキャッシュ エントリが、削除の対象になります。この種のエントリは、作成後、再び使用されることはありません。これらのエントリを検出して期限切れにすることにより、MLS キャッシュのスペースが節約され、他のデータ トラフィックを格納できるようになります。

デフォルトの *fastagingtime* 値は、0（ファスト エージングなし）です。*fastagingtime* 値は、32、64、96、または 128 秒に設定できます。*fastagingtime* 値をこれ以外の値に設定すると、最も近い値に調整されます。*pkt_threshold* 値は、0、1、3、7、15、31、または 63 パケットに設定できます。

IP MLS ファスト エージング タイムをイネーブルにする場合、最初は 128 秒に設定してください。MLS キャッシュのサイズが引き続きエントリ数 32,000 を超える場合には、キャッシュ サイズが 32,000 より小さくなるまで設定値を減らします。それでもキャッシュ サイズがエントリ数 32,000 より大きくなる場合は、通常の IP MLS エージング タイムを小さくします。

fastagingtime および *pkt_threshold* の一般的な設定値は、32 秒および 0 パケット（エントリの作成後 32 秒以内にパケットがまったくスイッチングされない場合）です。

IP MLS ファスト エージング タイムおよびパケット スレッシュホールドを指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
MLS キャッシュ エントリの IP MLS ファスト エージング タイムおよびパケット スレッシュホールドを指定します。	**set mls agingtime fast** [*fastagingtime*] [*pkt_threshold*]

次に、IP MLS ファスト エージング タイムを 32 秒、パケット スレッシュホールドを 0 パケットに設定する例を示します。

```
Console> (enable) set mls agingtime fast 32 0
Multilayer switching fast aging time set to 32 seconds for entries with no more than 0
packets switched.
Console> (enable)
```

アクティブ フローが期限切れになるように指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
アクティブ フローが期限切れになるように指定します。	**set mls agingtime long-duration** *agingtime*

次に、アクティブ フローを強制的に期限切れにする例を示します。アクティブ フローのエージング タイムとして設定できる値は、64 ～ 1920 秒の範囲の 64 の倍数です。

```
Console> (enable) set mls agingtime long-duration 128
Multilayer switching agingtime set to 128 seconds for long duration flows
Console> (enable)
```

最小 IP MLS フロー マスクの設定

PFC の MLS キャッシュを最小限にするように、フロー マスクの基準を設定できます。実際に使用されるフロー マスクは、このコマンドで指定された最低基準になります。各種フロー マスクの機能については、「フロー マスクの概要」（p.14-6）を参照してください。

たとえば、MSFC 上にアクセス リストを設定しない場合、PFC 上の IP MLS フロー マスクはデフォルトで destination-ip になります。ただし、**set mls flow destination-source** コマンドを使用して最小 IP MLS フロー マスクを設定することにより、PFC に source-destination-ip フロー マスクを強制的に使用させることができます。

注意　**set mls flow destination-source** コマンドを実行すると、MLS キャッシュ内の既存のショートカットがすべて削除され、PFC 上のアクティブ ショートカット数が影響を受けます。このコマンドは、慎重に使用してください。

最小 IP MLS フロー マスクを設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
最小 IP MLS フロー マスクを設定します。	**set mls flow** {**destination** | **destination-source** | **null** | **full**}

次に、最小 IP MLS フロー マスクを destination-source-ip に設定する例を示します。

```
Console> (enable) set mls flow destination-source
Configured IP flow mask is set to destination-source flow.
Console> (enable)
```

スーパバイザ エンジン上の CAM エントリの表示

show cam コマンドを実行すると、特定の MAC アドレスに対応付けられた CAM（連想メモリ）エントリが表示されます。MSFC に所属する MAC アドレスには、[R] が付加されます。

VLAN 番号を指定すると、その VLAN に対応する CAM エントリだけが表示されます。VLAN を指定しない場合は、すべての VLAN に関するエントリが表示されます。

CAM エントリを表示するには、次の作業を行います。

作業	コマンド
MAC アドレス別の CAM エントリを表示します。	**show cam msfc** [*vlan*]

次に、CAM エントリを表示する例を示します。

```
Console> show cam msfc
VLAN  Destination MAC      Destination-Ports or VCs        Xtag  Status
----  ------------------   ------------------------------  ----  ------
194   00-e0-f9-d1-2c-00R   7/1                             2     H
193   00-00-0c-07-ac-c1R   7/1                             2     H
193   00-00-0c-07-ac-5dR   7/1                             2     H
202   00-00-0c-07-ac-caR   7/1                             2     H
204   00-e0-f9-d1-2c-00R   7/1                             2     H
195   00-e0-f9-d1-2c-00R   7/1                             2     H
192   00-00-0c-07-ac-c0R   7/1                             2     H
192   00-e0-f9-d1-2c-00R   7/1                             2     H
204   00-00-0c-07-ac-ccR   7/1                             2     H
202   00-e0-f9-d1-2c-00R   7/1                             2     H
194   00-00-0c-07-ac-5eR   7/1                             2     H
196   00-e0-f9-d1-2c-00R   7/1                             2     H
194   00-00-0c-07-ac-c2R   7/1                             2     H
193   00-e0-f9-d1-2c-00R   7/1                             2     H
Total Matching CAM Entries Displayed = 14
Console>
```

次に、特定の VLAN について CAM エントリを表示する例を示します。

```
Console> show cam msfc 192
VLAN  Destination MAC      Destination-Ports or VCs        Xtag  Status
----  ------------------   ------------------------------  ----  ------
192   00-00-0c-07-ac-c0R   7/1                             2     H
192   00-e0-f9-d1-2c-00R   7/1                             2     H
Console>
```

MLS 情報の表示

show mls コマンドは、プロトコル固有の MLS 情報および MSFC 固有の情報を表示します。

プロトコル固有の MLS 情報および MSFC 固有の情報を表示するには、次の作業を行います。

作業	コマンド
一般的な IP または IPX MLS 情報およびすべての MSFC に関する MSFC 固有の情報を表示します。	**show mls** {**ip** | **ipx**} [*mod*[1]]

1. **mod** キーワードは MSFC のモジュール番号を表し、15（MSFC がスロット 1 の Supervisor Engine 1 上に搭載されている場合）または 16（MSFC がスロット 2 の Supervisor Engine 1 上に搭載されている場合）のどちらかです。

次に、IP MLS 情報および MSFC 固有の情報を表示する例を示します。

```
Console> (enable) show mls ip
Total Active MLS entries = 0
Total packets switched = 0
IP Multilayer switching enabled
IP Multilayer switching aging time = 256 seconds
IP Multilayer switching fast aging time = 0 seconds, packet threshold = 0
IP Flow mask: Full Flow
Configured flow mask is Destination flow
Active IP MLS entries = 0
Netflow Data Export version: 8
Netflow Data Export disabled
Netflow Data Export port/host is not configured
Total packets exported = 0

MSFC ID         Module XTAG MAC               Vlans
--------------- ------ ---- ------------------ --------------------
52.0.03         15     1    01-10-29-8a-0c-00 1,10,123,434,121
                                              222,666,959

Console> (enable)
```

次に、IPX MLS 情報を表示する例を示します。

```
Console> (enable) show mls ipx
IPX Multilayer switching aging time = 256 seconds
IPX flow mask is Destination flow
IPX max hop is 15
Active IPX MLS entries = 356

IPX MSFC ID     Module XTAG MAC               Vlans
--------------- ------ ---- ----------------- ----------------
22.1.0.56       15     1    00-10-07-38-29-18 2,3,4,5,6,
                                              7,8,9,10,11,
                                              12,13,14,15,16,
                                              17,18,19,20,66,
                                              77
                          00-d0-d3-9c-e3-f4 25
                          00-10-07-38-29-18 26,111
                          00-d0-d3-9c-e3-f4 112

22.1.0.58       16     2    00-10-07-38-22-22 2,3,4,5,6,
                                              7,8,9,10,11,
                                              12,13,14,15,16,
                                              17,18,19,20
                          00-d0-d3-33-17-8c 25
                          00-10-07-38-22-22 26,66,77,88,99,
                                              111
                          00-d0-d3-33-17-8c 112

Console> (enable)
```

IP MLS キャッシュ エントリの表示

ここでは、Supervisor Engine 1 上の IP MLS キャッシュ エントリを表示する手順について説明します。

- すべての MLS エントリの表示（p.14-26）
- 特定の宛先 IP アドレスに関する MLS エントリの表示（p.14-27）
- 特定の宛先 IPX アドレスに関する IPX MLS エントリの表示（p.14-28）
- 特定の送信元 IP アドレスに関する MLS エントリの表示（p.14-28）
- 特定の IP フローに関する MLS エントリの表示（p.14-28）
- 特定の MSFC に関する IPX MLS エントリの表示（p.14-29）
- ブリッジド フローの MLS エントリに関する統計情報の表示（p.14-30）

（注） MLS エントリの画面表示に対するフロー マスク モードの影響については、「フロー マスク モードおよび show mls entry コマンドの出力」（p.14-9）を参照してください。

すべての MLS エントリの表示

すべての MLS エントリ（IP および IPX）を表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
MLS エントリをすべて表示します。	**show mls entry** [**short** | **long**]

次に、すべての MLS エントリ（IP および IPX）を表示する例を示します。

```
Console> (enable) show mls entry short
Destination-IP   Source-IP       Prot  DstPrt SrcPrt Destination-Mac  Vlan
--------------- --------------- ----- ------ ------ ----------------- ----
 ESrc EDst SPort DPort Stat-Pkts  Stat-Bytes   Created  LastUsed
 ---- ---- ----- ----- ---------- ------------ -------- --------
171.69.200.234  171.69.192.41   TCP*  6000   59181  00-60-70-6c-fc-22 4
 ARPA SNAP 5/8   11/1  3152       347854       09:01:19 09:08:20
171.69.1.133    171.69.192.42   UDP   2049   41636  00-60-70-6c-fc-23 2
 SNAP ARPA 5/8   1/1   2345       1234567      09:03:32 09:08:12
171.69.1.133    171.69.192.42   UDP   2049   41636  00-60-70-6c-fc-23 2
 SNAP ARPA 5/8   1/1   2345       1234567      09:03:32 09:08:12
171.69.1.133    171.69.192.42   UDP   2049   41636  00-60-70-6c-fc-23 2
 SNAP ARPA 5/8   1/1   2345       1234567      09:03:32 09:08:12
171.69.1.133    171.69.192.42   UDP   2049   41636  00-60-70-6c-fc-23 2
 SNAP ARPA 5/8   1/1   2345       1234567      09:03:32 09:08:12

Total IP entries: 5
* indicates TCP flow has ended.

Destination-IPX           Source-IPX-net Destination-Mac   Vlan Port
 Stat-Pkts Stat-Bytes
------------------------- -------------- ----------------- ---- -----
 --------- -----------
BABE.0000.0000.0001       -              00-a0-c9-0a-89-1d 211  13/37
 30230     1510775
201.00A0.2451.7423        -              00-a0-24-51-74-23 201  14/33
 30256     31795084
501.0000.3100.0501        -              31-00-05-01-00-00 501  9/37
 12121     323232
401.0000.0000.0401        -              00-00-04-01-00-00 401  3/1
 4633      38676

Total IPX entries: 4
Console>
```

特定の宛先 IP アドレスに関する MLS エントリの表示

特定の宛先 IP アドレスについて MLS エントリを表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
特定の宛先 IP アドレスについて MLS エントリを表示します。	**show mls entry ip destination** [*ip_addr*]

次に、特定の宛先 IP アドレスについて MLS エントリを表示する例を示します。

```
Console> (enable) show mls entry ip destination 172.20.22.14/24
Destination-IP   Source-IP       Prot  DstPrt SrcPrt Destination-Mac   Vlan
 EDst ESrc DPort  SPort  Stat-Pkts  Stat-Bytes  Uptime   Age
--------------- --------------- ----- ------ ------ ----------------- ----
 ---- ---- ------ ------ ---------- ----------- -------- --------
MSFC 172.20.25.1 (Module 15):
172.20.22.14    -               -     -      -      00-60-70-6c-fc-22 4
 ARPA ARPA 5/39   5/40   115        5290        00:12:20 00:00:04
MSFC 172.20.27.1 (Module 16):

Total entries:1
Console> (enable)
```

特定の宛先 IPX アドレスに関する IPX MLS エントリの表示

特定の宛先 IPX アドレスについて IPX MLS エントリを表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
特定の宛先 IPX アドレス（net_address.node_address）について IPX MLS エントリを表示します。	**show mls entry ipx destination** *ipx_addr*

次に、特定の宛先 IPX アドレスについて IPX MLS エントリを表示する例を示します。

```
Console> (enable) show mls entry ipx destination 3E.0010.298a.0c00
Destination IPX           Source IPX net Destination Mac   Vlan Port
------------------------- -------------- ----------------- ---- -----
MSFC 22.1.0.56 (Module 15):
3E.0010.298a.0c00                    13 00-00-00-00-00-09 26   4/7

Console> (enable)
```

特定の送信元 IP アドレスに関する MLS エントリの表示

特定の送信元 IP アドレスについて MLS エントリを表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
特定の送信元 IP アドレスについて MLS エントリを表示します。	**show mls entry ip source** [*ip_addr*]

次に、特定の送信元 IP アドレスについて MLS エントリを表示する例を示します。

```
Console> (enable) show mls entry ip source 10.0.2.15
Destination-IP  Source-IP       Prot  DstPrt SrcPrt Destination-Mac   Vlan
 EDst ESrc DPort  SPort  Stat-Pkts  Stat-Bytes  Uptime   Age
--------------- --------------- ----- ------ ------ ----------------- ----
 ---- ---- ------ ------ ---------- ----------- -------- --------
MSFC 172.20.25.1 (Module 15):
172.20.22.14    10.0.2.15       TCP   Telnet 37819  00-e0-4f-15-49-ff 51
 ARPA ARPA 5/39   5/40   115        5290        00:12:20 00:00:04
MSFC 172.20.27.1 (Module 16):
Total entries:1
Console> (enable)
```

特定の IP フローに関する MLS エントリの表示

show mls entry ip flow コマンドを実行すると、特定の IP フローに関する MLS エントリが表示されます。*protocol* 引数には、**tcp**、**udp**、**icmp**、またはその他のプロトコル ファミリーを表す 10 進数を指定できます。プロトコルが TCP または UDP である場合、*src_port* 引数および *dst_port* 引数でプロトコル ポートを指定します。*src_port*、*dst_port*、または *protocol* にゼロ（0）を指定した場合、ワイルドカードとして扱われ、すべてのエントリが表示されます（未指定のオプションはワイルドカードとして扱われます）。指定するプロトコルが TCP または UDP 以外の場合には、*src_port* および *dst_port* を 0 に設定しないと、フローは表示されません。

（フロー マスク モードが full flow の場合）特定の IP フローについて MLS エントリを表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
特定の IP フローについて MLS エントリを表示します（フロー マスク モードが full flow の場合）。	**show mls entry ip flow** [*protocol src_port dst_port*]

次に、特定の IP フローについて MLS エントリを表示する例を示します。

```
Console> (enable) show mls entry ip flow tcp 23 37819
Destination IP  Source IP       Port DstPrt SrcPrt Destination Mac   Vlan Port
--------------- --------------- ---- ------ ------ ----------------- ---- -----
MSFC 51.0.0.3:
10.0.2.15       51.0.0.2        TCP  37819  Telnet 08-00-20-7a-07-75 10   3/1
Console> (enable)
```

特定の MSFC に関する IPX MLS エントリの表示

特定の MSFC について IPX MLS エントリを表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
特定の MSFC について IPX MLS エントリを表示します。	**show mls entry ipx** *mod*[1]

1. **mod** キーワードは MSFC のモジュール番号を表し、15（MSFC がスロット 1 の Supervisor Engine 1 上に搭載されている場合）または 16（MSFC がスロット 2 の Supervisor Engine 1 上に搭載されている場合）のどちらかです。

次に、特定の MSFC について IPX MLS エントリを表示する例を示します。

```
Console> (enable) show mls entry ipx 15
Destination-IPX           Destination-Mac   Vlan EDst ESrc  Port  Stat-Pkts
 Stat-Bytes  Uptime   Age
------------------------- ----------------- ---- ---- ---- ----- ----------
 ----------- -------- --------
MSFC 22.1.0.56 (Module 15):
11.0000.0000.2B10         00-00-00-00-2b-10 11   ARPA ARPA  -     7869
 361974      00:15:52 00:00:00
11.0000.0000.A810         00-00-00-00-a8-10 11   ARPA ARPA  -     3934
 180964      00:15:52 00:00:00
11.0000.0000.3210         00-00-00-00-32-10 11   ARPA ARPA  -     7871
 362066      00:15:52 00:00:00
11.0000.0000.B110         00-00-00-00-b1-10 11   ARPA ARPA  -     3935
 181010      00:15:52 00:00:00
11.0000.0000.1910         00-00-00-00-19-10 11   ARPA ARPA  -     7873
 362158      00:15:52 00:00:00
11.0000.0000.9A10         00-00-00-00-9a-10 11   ARPA ARPA  -     3936
 181056      00:15:52 00:00:00
11.0000.0000.0010         00-00-00-00-00-10 11   ARPA ARPA  3/11  7875
 362250      00:15:52 00:00:00
11.0000.0000.8310         00-00-00-00-83-10 11   ARPA ARPA  -     3937
 181102      00:15:52 00:00:00
10.0000.0000.0109         00-00-00-00-01-09 10   ARPA ARPA  3/10  96364
 4432744     00:15:52 00:00:00
11.0000.0000.4F10         00-00-00-00-4f-10 11   ARPA ARPA  -     7877
 362342      00:15:53 00:00:00
11.0000.0000.CC10         00-00-00-00-cc-10 11   ARPA ARPA  -     3938
 181148      00:15:53 00:00:00
11.0000.0000.5610         00-00-00-00-56-10 11   ARPA ARPA  -     7879
 362434      00:15:53 00:00:00
11.0000.0000.D510         00-00-00-00-d5-10 11   ARPA ARPA  -     3939
 181194      00:15:53 00:00:00
11.0000.0000.7D10         00-00-00-00-7d-10 11   ARPA ARPA  -     3940
 181240      00:15:53 00:00:00
```

```
11.0000.0000.FE10         00-00-00-00-fe-10 11   ARPA ARPA  -     3941
 181286      00:15:53 00:00:00
11.0000.0000.6410         00-00-00-00-64-10 11   ARPA ARPA  -     7883
 362618      00:15:53 00:00:00
11.0000.0000.E710         00-00-00-00-e7-10 11   ARPA ARPA  -     3941
 181286      00:15:53 00:00:00
11.0000.0000.6010         00-00-00-00-60-10 11   ARPA ARPA  -     7885
 362710      00:15:53 00:00:00
11.0000.0000.E310         00-00-00-00-e3-10 11   ARPA ARPA  -     3942
 181332      00:15:53 00:00:00
11.0000.0000.7910         00-00-00-00-79-10 11   ARPA ARPA  -     3943
 181378      00:15:54 00:00:00

Console> (enable)
```

ブリッジド フローの MLS エントリに関する統計情報の表示

ブリッジド フローの MLS エントリに関する統計情報を表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
ブリッジド フローの MLS エントリに関する統計情報を表示します。	**show mls entry**

次に、ブリッジド フローの MLS エントリに関する統計情報を表示する例を示します。

```
Console> (enable) show mls entry
     Destination-IP  Source-IP       Prot  DstPrt SrcPrt Destination-Mac   Vlan EDst
ESrc DPort     SPort     Stat-Pkts  Stat-Bytes  Uptime   Age
     --------------- --------------- ----- ------ ------ ----------------- ---- ----
---- --------- --------- ---------- ---------- -------- --------
     224.0.0.5       21.2.0.22        -     0      0      00-00-00-00-00-00 0    ARPA
ARPA -         5/11      20         1280        00:03:14 00:00:04
     224.0.0.13      1.1.1.2          -     0      0      00-00-00-00-00-00 0    ARPA
ARPA -         5/11      7          210         00:03:02 00:00:02
     255.255.255.255 -                -     0      0      ff-ff-ff-ff-ff-ff 21   ARPA
ARPA -         5/11      28         2996        00:03:10 00:00:02
     10.6.62.195     -                -     0      0      00-00-00-00-00-02 20   ARPA
ARPA -         5/5       291494     13408724    00:03:16 00:00:00

     Destination-IPX           Destination-Mac   Vlan EDst ESrc  Port  Stat-Pkts
Stat-Bytes  Uptime   Age
     ------------------------- ----------------- ---- ---- ---- ----- ----------
---------- -------- --------
Total entries displayed:2
```

MLS キャッシュ エントリの消去

clear mls entry コマンドを使用して、特定の MLS キャッシュ エントリを消去します。**all** キーワードを指定すると、すべての MLS エントリが消去されます。**destination** キーワードおよび **source** キーワードは、送信元および宛先の IP アドレスを指定します。宛先および送信元の *ip_addr_spec* には、完全な IP アドレス、または *ip_subnet_addr*、*ip_addr/subnet_mask*、*ip_addr/subnet_mask_bits* の形式のサブネット アドレスを指定できます。

flow キーワードでは、追加されたフロー情報を次のように指定します。

- プロトコル ファミリー（*protocol*）― **tcp**、**udp**、**icmp**、またはその他のプロトコル ファミリーに対応する 10 進数を指定します。*protocol* にゼロ（0）を指定した場合、ワイルドカードとして扱われ、すべてのプロトコルのエントリが消去されます（未指定のオプションはワイルドカードとして扱われます）。

- TCP または UDP の送信元および宛先ポート番号（*src_port* および *dst_port*）— プロトコルとして TCP または UDP を指定する場合、送信元および宛先の TCP または UDP ポート番号を指定します。*src_port* または *dst_port* にゼロ（0）を指定した場合、ワイルドカードとして扱われ、すべての送信元または宛先ポートのエントリが消去されます（未指定のオプションはワイルドカードとして扱われます）。その他のプロトコルについては、*src_port* および *dst_port* を 0 に設定しないと、エントリは消去されません。

MLS エントリを消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
MLS エントリを消去します。	**clear mls entry ip** [**destination** *ip_addr_spec*] [**source** *ip_addr_spec*] [**flow** *protocol src_port dst_port*] [**all**]

次に、宛先 IP アドレス 172.20.26.22 の MLS エントリを消去する例を示します。

```
Console> (enable) clear mls entry ip destination 172.20.26.22
MLS IP entry cleared
Console> (enable)
```

次に、宛先 IP アドレス 172.20.22.113、TCP 送信元ポート 1652、TCP 宛先ポート 23 の MLS エントリを消去する例を示します。

```
Console> (enable) clear mls entry destination 172.20.26.22 source 172.20.22.113 flow
tcp 1652 23
MLS IP entry cleared
Console> (enable)
```

IPX MLS キャッシュ エントリの消去

clear mls entry ipx コマンドを使用して、特定の IPX MLS キャッシュ エントリを消去します。**destination** および **source** キーワードは、送信元および宛先の IPX アドレスを指定します。**all** キーワードを指定すると、すべての MLS エントリが消去されます。

IP MLS 統計情報の表示

ここでは、IP MLS 統計情報の表示方法について説明します。

- プロトコル別の IP MLS 統計情報の表示（p.14-31）
- MLS キャッシュ エントリに関する統計情報の表示（p.14-32）

プロトコル別の IP MLS 統計情報の表示

show mls statistics protocol コマンドを実行すると、プロトコル別（Telnet、FTP、WWW など）の IP MLS 統計情報が表示されます。**protocol** キーワードが機能するのは、フロー マスク モードが full flow の場合だけです。現在のフロー マスクを調べるには、**show mls** コマンドを使用します。

プロトコル別の IP MLS 統計情報を表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
プロトコル別の IP MLS 統計情報を表示します（IP MLS が full flow モードの場合のみ）。	**show mls statistics protocol**

次に、プロトコル別の IP MLS 統計情報を表示する例を示します。

```
Console> (enable) show mls statistics protocol
Protocol  TotalFlows  TotalPackets    Total Bytes
-------   ----------  --------------  ------------
Telnet    900         630             4298
FTP       688         2190            3105
WWW       389         42679           623686
SMTP      802         4966            92873
X         142         2487            36870
DNS       1580        52              1046
Others    82          1               73
Total     6583        53005           801951
Console> (enable)
```

MLS キャッシュ エントリに関する統計情報の表示

show mls statistics entry コマンドを実行すると、MLS キャッシュ エントリに関する IP MLS 統計情報が表示されます。特定の MLS キャッシュ エントリについて調べるには、宛先 IP アドレス、送信元 IP アドレス、プロトコル、および送信元ポートおよび宛先ポートを指定します。

src_port または *dst_port* にゼロ（0）を指定した場合、ワイルドカードとして扱われ、すべての統計情報が表示されます（未指定のオプションはワイルドカードとして扱われます）。指定するプロトコルが TCP または UDP 以外の場合には、*src_port* および *dst_port* を 0 に設定しないと、統計情報は表示されません。

MLS キャッシュ エントリに関する統計情報を表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
MLS キャッシュ エントリに関する統計情報を表示します。MLS キャッシュ エントリを指定しない場合、すべての統計情報が表示されます。	**show mls statistics entry ip** [**destination** *ip_addr_spec*] [**source** *ip_addr_spec*] [**flow** *protocol src_port dst_port*]

次に、特定の MLS キャッシュ エントリに関する統計情報を表示する例を示します。

```
Console> show mls statistics entry ip destination 172.20.22.14
                                  Last    Used
Destination IP  Source IP       Prot DstPrt SrcPrt Stat-Pkts Stat-Bytes
--------------- --------------- ---- ------ ------ --------- -----------
MSFC 127.0.0.12:
172.20.22.14    172.20.25.10    6    50648  80     3152       347854
Console>
```

MLS 統計情報の消去

clear mls statistics コマンドを使用して、次の統計情報を消去できます。

- スイッチングされたパケット総数（IP および IPX）
- エクスポートされたパケット総数（NDE へ）

IP MLS 統計情報を消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
IP MLS 統計情報を消去します。	**clear mls statistics**

次に、IP MLS 統計情報を消去する例を示します。

```
Console> (enable) clear mls statistics
All mls statistics cleared.
Console> (enable)
```

MLS デバッグ情報の表示

show mls debug コマンドを実行すると、MLS のデバッグ情報が表示されます。必要に応じて、この情報をテクニカル サポートに送信し、解析に利用することができます。

MLS デバッグ情報を表示するには、次の作業を行います。

作業	コマンド
テクニカル サポートに送信できる MLS デバッグ情報を表示します。	**show mls debug**

(注)　**show tech-support** コマンドは、スーパバイザ エンジン システム情報を表示します。特定のアプリケーションに関する詳細情報を取得するには、アプリケーション固有のコマンドを使用します。

IP MMLS の設定

ここでは、IP MMLS を設定する手順について説明します。

- MSFC 上での IP MMLS の設定（p.14-33）
- スーパバイザ エンジン上でのグローバル IP MMLS 情報の表示（p.14-38）

MSFC 上での IP MMLS の設定

ここでは、MSFC に IP MMLS を設定する手順について説明します。

- IP マルチキャスト ルーティングのグローバルなイネーブル化（p.14-34）
- MSFC インターフェイス上での IP PIM のイネーブル化（p.14-34）
- IP MMLS グローバル スレッシュホールドの設定（p.14-34）
- MSFC インターフェイス上での IP MMLS のイネーブル化（p.14-35）
- IP MMLS インターフェイス情報の表示（p.14-35）
- IP マルチキャスト ルーティング テーブルの表示（p.14-36）
- MSFC 上での IP MMLS の詳細情報表示（p.14-36）
- IP MMLS MSFC 上での debug コマンドの使用方法（p.14-38）
- SCP に関する debug コマンドの使用方法（p.14-38）

(注)　MSFC 上でのルーティングの設定手順については、第 12 章「VLAN 間ルーティングの設定」を参照してください。

(注)　MSFC は、MLS を使用する Catalyst 5000 ファミリー スイッチの MLS-RP として指定できます。Catalyst 5000 ファミリー スイッチでの MLS 設定手順については、『*Layer 3 Switching Configuration Guide ― Catalyst 5000 Family, 2926G Series, 2926 Series Switches*』を参照してください。

（注）　ここで説明するのは、MSFC 上で IP マルチキャスト ルーティングをイネーブルにする方法です。IP マルチキャスト設定の詳細については、次の URL にある『*Cisco IOS IP and IP Routing Configuration Guide*』の「IP Multicast」を参照してください。
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_c/ipcprt3/index.htm

IP マルチキャスト ルーティングのグローバルなイネーブル化

MSFC 上で IP マルチキャスト ルーティングをグローバルにイネーブルにしてから、MSFC インターフェイス上で IP MMLS をイネーブルにする必要があります。

MSFC 上で IP マルチキャスト ルーティングをグローバルにイネーブルにするには、グローバル コンフィギュレーション モードで次の作業を行います。

作業	コマンド
IP マルチキャスト ルーティングをグローバルにイネーブルにします。	Router(config)# **ip multicast-routing**

次に、IP マルチキャスト ルーティングをグローバルにイネーブルにする例を示します。

```
Router(config)# ip multicast-routing
Router(config)#
```

MSFC インターフェイス上での IP PIM のイネーブル化

MSFC インターフェイス上で IP MMLS が機能するためには、最初にインターフェイス上で IP PIM をイネーブルに設定しておく必要があります。

インターフェイス上で IP PIM をイネーブルにするには、次の作業を行います。

作業	コマンド
MSFC インターフェイス上で IP PIM をイネーブルにします。	Router(config-if)# **ip pim** {**dense-mode** | **sparse-mode** | **sparse-dense-mode**}

次に、インターフェイス上でデフォルト モード（**sparse-dense-mode**）を使用して IP PIM をイネーブルにする例を示します。

```
Router(config-if)# ip pim
Router(config-if)#
```

次に、インターフェイス上で IP PIM sparse モードをイネーブルにする例を示します。

```
Router(config-if)# ip pim sparse-mode
Router(config-if)#
```

IP MMLS グローバル スレッシュホールドの設定

MSFC がすべての（S,G）マルチキャスト トラフィックをルーティングする上限を表すグローバル マルチキャスト レート スレッシュホールド（パケット / 秒）を設定できます。コマンドを入力することにより、Join 要求など、存続期間の短いマルチキャスト フローに対応する MLS エントリの作成が防止されます。

(注)　このコマンドは、ルーティング済みのフローに対しては無効です。既存のルートにスレッシュホールドを適用するには、ルートをいったん消去して再度確立します。

IP MMLS スレッシュホールドを設定するには、次の作業を行います。

作業	コマンド
IP MMLS スレッシュホールドを設定します。	Router(config)# [**no**] **mls ip multicast threshold** *ppsec*

次に、IP MMLS スレッシュホールドを 10 パケット / 秒に設定する例を示します。

```
Router(config)# mls ip multicast threshold 10
Router(config)#
```

スレッシュホールドの設定を解除するには、**no** キーワードを使用します。

MSFC インターフェイス上での IP MMLS のイネーブル化

MSFC インターフェイス上で IP PIM をイネーブルに設定した場合、そのインターフェイス上では IP MMLS がデフォルトでイネーブルになります。ここで説明する作業は、インターフェイス上で IP MMLS をディセーブルにし、再びイネーブルにする場合にだけ実行してください。

(注)　IP MMLS が機能するためには、まず参加するすべての MSFC インターフェイス上で IP PIM をイネーブルにする必要があります。MSFC インターフェイス上での IP PIM の設定手順については、「MSFC インターフェイス上での IP PIM のイネーブル化」（p.14-34）を参照してください。

MSFC インターフェイス上で IP MMLS をイネーブルにするには、次の作業を行います。

作業	コマンド
MSFC インターフェイス上で IP MMLS をイネーブルにします。	Router(config-if)# [**no**] **mls ip multicast**

次に、MSFC インターフェイス上で IP MMLS をイネーブルにする例を示します。

```
Router(config-if)# mls ip multicast
Router(config-if)#
```

MSFC インターフェイス上で IP MMLS をディセーブルにするには、**no** キーワードを使用します。

IP MMLS インターフェイス情報の表示

show ip pim interface count コマンドを実行すると、MSFC IP PIM インターフェイス上の IP MMLS イネーブル ステート、およびそのインターフェイス上で送受信されたパケット数が表示されます。

show ip interface コマンドを実行すると、MSFC インターフェイス上の IP MMLS イネーブル ステートが表示されます。

特定の IP PIM MSFC インターフェイスについて IP MMLS 情報を表示するには、次のいずれかの作業を行います。

作業	コマンド
IP MMLS インターフェイス情報を表示します。	Router# **show ip pim interface** [*type number*] **count**
IP MMLS インターフェイスのイネーブル ステートを表示します。	Router# **show ip interface**

IP マルチキャスト ルーティング テーブルの表示

show ip mroute コマンドを実行すると、MSFC 上の IP マルチキャスト ルーティング テーブルが表示されます。

IP マルチキャスト ルーティング テーブルを表示するには、次の作業を行います。

作業	コマンド
IP マルチキャスト ルーティング テーブルを表示します。	Router# **show ip mroute** [*group*[*source*]] | [**summary**] | [**count**] | [**active** *kbps*]

次に、239.252.1.1 について IP マルチキャスト ルーティング テーブルを表示する例を示します。

```
Router# show ip mroute 239.252.1.1
IP Multicast Routing Table
Flags:D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned
       R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT
       M - MSDP created entry, X - Proxy Join Timer Running
       A - Advertised via MSDP
Outgoing interface flags:H - Hardware switched
Timers:Uptime/Expires
Interface state:Interface, Next-Hop or VCD, State/Mode

(*, 239.252.1.1), 04:04:59/00:02:59, RP 80.0.0.2, flags:SJ
  Incoming interface:Vlan800, RPF nbr 80.0.0.2
  Outgoing interface list:
    Vlan10, Forward/Dense, 01:29:57/00:00:00, H

(22.0.0.10, 239.252.1.1), 00:00:19/00:02:41, flags:JT
  Incoming interface:Vlan800, RPF nbr 80.0.0.2, RPF-MFD
  Outgoing interface list:
    Vlan10, Forward/Dense, 00:00:19/00:00:00, H
```

MSFC 上での IP MMLS の詳細情報表示

show mls ip multicast コマンドを実行すると、IP MMLS に関する詳細情報が表示されます。

MSFC 上の IP MMLS に関する詳細情報を表示するには、次のいずれかの作業を行います。

作業	コマンド
IP MMLS グループ情報を表示します。	Router# **show mls ip multicast group** *group-address* [**interface** *type number* | **statistics**]
すべてのインターフェイスについて IP MMLS 詳細情報を表示します。	Router# **show mls ip multicast interface** *type number* [**statistics** | **summary**]
IP MMLS 情報の要約を表示します。	Router# **show mls ip multicast summary**
IP MMLS 統計情報を表示します。	Router# **show mls ip multicast statistics**
IP MMLS 送信元情報を表示します。	Router# **show mls ip multicast source** *ip-address* [**interface** *type number* | **statistics**]

次に、MSFC 上の IP MMLS 統計情報を表示する例を示します。

```
Router# show mls ip multicast statistics
MLS Multicast configuration and state:
    Router Mac:0050.0f2d.9bfd, Router IP:1.12.123.234
    MLS multicast operating  state:ACTIVE
    Maximum number of allowed outstanding messages:1
    Maximum size reached from feQ:1
    Feature Notification sent:5
    Feature Notification Ack received:4
    Unsolicited Feature Notification received:0
    MSM sent:33
    MSM ACK received:33
    Delete notifications received:1
    Flow Statistics messages received:248

MLS Multicast statistics:
    Flow install Ack:9
    Flow install Nack:0
    Flow update Ack:2
    Flow update Nack:0
    Flow delete Ack:0
    Complete flow install Ack:10
    Complete flow install Nack:0
    Complete flow delete Ack:1
    Input VLAN delete Ack:4
    Output VLAN delete Ack:0
    Group delete sent:0
    Group delete Ack:0
    Global delete sent:7
    Global delete Ack:7

    L2 entry not found error:0
    Generic error :3
    LTL entry not found error:0
    MET entry not found error:0
    L3 entry exists error :0
    Hash collision error :0
    L3 entry not found error:0
    Complete flow exists error :0
```

次に、MSFC 上の特定の IP MMLS エントリに関する情報を表示する例を示します。

```
Router# show mls ip multicast 224.1.1.1
Multicast hardware switched flows:
(1.1.13.1, 224.1.1.1) Incoming interface: Vlan13, Packets switched: 61590
Hardware switched outgoing interfaces: Vlan20 Vlan9
RFD-MFD installed: Vlan13

(1.1.9.3, 224.1.1.1) Incoming interface: Vlan9, Packets switched: 0
Hardware switched outgoing interfaces: Vlan20
RFD-MFD installed: Vlan9

(1.1.12.1, 224.1.1.1) Incoming interface: Vlan12, Packets switched: 62010
Hardware switched outgoing interfaces: Vlan20 Vlan9
RFD-MFD installed: Vlan12

(1.1.12.3, 224.1.1.1) Incoming interface: Vlan12, Packets switched: 61980
Hardware switched outgoing interfaces: Vlan20 Vlan9
RFD-MFD installed: Vlan12

(1.1.11.1, 224.1.1.1) Incoming interface: Vlan11, Packets switched: 62430
Hardware switched outgoing interfaces: Vlan20 Vlan9
RFD-MFD installed: Vlan11

(1.1.11.3, 224.1.1.1) Incoming interface: Vlan11, Packets switched: 62430
Hardware switched outgoing interfaces: Vlan20 Vlan9
RFD-MFD installed: Vlan11

Total hardware switched installed: 6
Router#
```

次に、MSFC 上の IP MMLS 情報の要約を表示する例を示します。

```
Router# show mls ip multicast summary
7 MMLS entries using 560 bytes of memory
Number of partial hardware-switched flows:2
Number of complete hardware-switched flows:5
Router#
```

IP MMLS MSFC 上での debug コマンドの使用方法

表 14-9 に、IP MMLS 関連のトラブルシューティングのための debug コマンドを示します。

表 14-9　IP MMLS の debug コマンド

コマンド	説明
[no] debug mls ip multicast group *group_id group_mask*	他のすべてのマルチキャスト デバッグ コマンドに適用されるフィルタを設定します。
[no] debug mls ip multicast events	IP MMLS イベントを表示します。
[no] debug mls ip multicast errors	マルチキャスト MLS 関連のエラーに対するデバッグ メッセージをオンにします。
[no] debug mls ip multicast messages	ハードウェア スイッチング エンジンとの間で送受信される IP MMLS メッセージを表示します。
[no] debug mls ip multicast all	すべての IP MMLS メッセージをオンにします。
[no] debug mdss error	MDSS[1] エラー メッセージをオンにします。
[no] debug mdss events	MDSS 関連のイベントをオンにします。
[no] debug mdss all	すべての MDSS メッセージをオンにします。

1. MDSS = Multicast Distributed Switching Services

SCP に関する debug コマンドの使用方法

表 14-10 に、EOBC で動作する SCP をトラブルシューティングするための、SCP 関連の debug コマンドを示します。

表 14-10　SCP の debug コマンド

コマンド	説明
[no] debug scp async	SCP システムを出入りする非同期データのトレースを表示します。
[no] debug scp data	パケット データのトレースを表示します。
[no] debug scp errors	SCP のエラーおよび警告を表示します。
[no] debug scp packets	SCP システムを出入りするパケット データを表示します。
[no] debug scp timeouts	タイムアウトを報告します。
[no] debug scp all	すべての SCP デバッグ メッセージをオンにします。

スーパバイザ エンジン上でのグローバル IP MMLS 情報の表示

ここでは、Supervisor Engine 1 上で IP MMLS を設定する手順について説明します。

(注)　Supervisor Engine 1 上では IP MMLS が永続的にイネーブルになっており、ディセーブルにすることはできません。

(注)　MSFC 上で IP MMLS を設定する手順については、「MSFC 上での IP MMLS の設定」（p.14-33）を参照してください。

IP MMLS 設定情報の表示

show mls multicast コマンドを実行すると、IP MMLS に関するグローバルな設定情報および参加している MSFC のステートが表示されます。

IP MMLS のグローバルな設定情報を表示するには、次の作業を行います。

作業	コマンド
IP MMLS のグローバルな設定情報を表示します。	**show mls multicast**

次に、IP MMLS のグローバルな設定情報を表示する例を示します。

```
Console> (enable) show mls multicast
Admin Status: Enabled
Operational Status: Active
Configured flow mask is {Destination-source-vlan flow}
Active Entries = 10
Router include list :
1.1.9.254 (Active)
1.1.5.252 (Active)
Console> (enable)
```

IP MMLS 統計情報の表示

show mls multicast statistics コマンドを実行すると、マルチキャスト MSFC に関する IP MMLS 統計情報が表示されます。

マルチキャスト MSFC に関する IP MMLS 統計情報を表示するには、次の作業を行います。

作業	コマンド
IP マルチキャスト MSFC 統計情報を表示します。	**show mls multicast statistics** [*ip_addr*]

次に、マルチキャスト MSFC に関する IP MMLS 統計情報を表示する例を示します。

```
Console (enable) show mls multicast statistics
Router IP          Router Name        Router MAC
-------------------------------------------------------
1.1.9.254          ?                  00-50-0f-06-3c-a0

Transmit:
  Delete Notifications:                    23
  Acknowledgements:                        92
  Flow Statistics:                         56

Receive:
  Open Connection Requests:                1
  Keep Alive Messages:                     72
  Shortcut Messages:                       19
    Shortcut Install TLV:                  8
    Selective Delete TLV:                  4
    Group Delete TLV:                      0
    Update TLV:                            3
    Input VLAN Delete TLV:                 0
    Output VLAN Delete TLV:                0
    Global Delete TLV:                     0
    MFD Install TLV:                       7
    MFD Delete TLV:                        0
Router IP          Router Name        Router MAC
-------------------------------------------------------
1.1.5.252          ?                  00-10-29-8d-88-01

Transmit:
  Delete Notifications:                    22
  Acknowledgements:                        75
  Flow Statistics:                         22

Receive:
  Open Connection Requests:                1
  Keep Alive Messages:                     68
  Shortcut Messages:                       6
    Shortcut Install TLV:                  4
    Selective Delete TLV:                  2
    Group Delete TLV:                      0
    Update TLV:                            0
    Input VLAN Delete TLV:                 0
    Output VLAN Delete TLV:                0
    Global Delete TLV:                     0
    MFD Install TLV:                       4
    MFD Delete TLV:                        0
Console (enable)
```

IP MMLS 統計情報の消去

clear mls multicast statistics コマンドを実行すると、参加しているすべての MSFC の IP MMLS 統計情報が消去されます。

IP MMLS 統計情報を消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
IP MMLS 統計情報を消去します。	**clear mls multicast statistics**

次に、IP MMLS 統計情報を消去する例を示します。

```
Console> (enable) clear mls multicast statistics
All statistics for the MLS routers in include list are cleared.
Console> (enable)
```

IP MMLS エントリの表示

show mls multicast entry コマンドを実行すると、PFC が処理しているマルチキャスト フローに関する情報が表示されます。参加している MSFC、VLAN、マルチキャスト グループ アドレス、またはマルチキャスト トラフィック送信元を任意に組み合わせて、エントリを表示できます。

IP MMLS エントリに関する情報を表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
IP MMLS エントリに関する情報を表示します。	**show mls multicast entry** [[[*mod*] [**vlan** *vlan_id*] [**group** *ip_addr*] [**source** *ip_addr*]]	[**all**]]

次に、すべての IP MMLS エントリを表示する例を示します。

```
Console> (enable) show mls multicast entry all
Router IP       Dest IP         Source IP       Pkts       Bytes       InVlan
OutVlans
--------------- --------------- --------------- ---------- ----------- -------
--------

1.1.5.252       224.1.1.1       1.1.11.1        15870      2761380     20
1.1.9.254       224.1.1.1       1.1.12.3        473220     82340280    12
1.1.5.252       224.1.1.1       1.1.12.3        15759      2742066     20
1.1.9.254       224.1.1.1       1.1.11.1        473670     82418580    11
1.1.5.252       224.1.1.1       1.1.11.3        15810      2750940     20
1.1.9.254       224.1.1.1       1.1.12.1        473220     82340280    12
1.1.5.252       224.1.1.1       1.1.13.1        15840      2756160     20
1.1.9.254       224.1.1.1       1.1.13.1        472770     82261980    13
1.1.5.252       224.1.1.1       1.1.12.1        15840      2756160     20
1.1.9.254       224.1.1.1       1.1.11.3        473667     82418058    11
Total Entries: 10
Console> (enable)
```

次に、特定の MSFC について IP MMLS エントリを表示する例を示します。

```
Console> (enable) show mls multicast entry 15
Router IP       Dest IP         Source IP       Pkts       Bytes       InVlan
OutVlans
--------------- --------------- --------------- ---------- ----------- -------
--------

1.1.5.252       224.1.1.1       1.1.11.1        15870      2761380     20
1.1.5.252       224.1.1.1       1.1.12.3        15759      2742066     20
1.1.5.252       224.1.1.1       1.1.11.3        15810      2750940     20
1.1.5.252       224.1.1.1       1.1.13.1        15840      2756160     20
1.1.5.252       224.1.1.1       1.1.12.1        15840      2756160     20
Total Entries: 5
Console> (enable)
```

次に、特定のマルチキャスト グループ アドレスについて IP MMLS エントリを表示する例を示します。

```
Console> (enable) show mls multicast entry group 226.0.1.3 short
Router IP      Dest IP     Source IP    InVlan Pkts   Bytes     OutVlans
-------------- ----------- ------------ ------ ------ --------- ---------
171.69.2.1     226.0.1.3   172.2.3.8    20     171    23512     10,201,22,45
171.69.2.1     226.0.1.3   172.3.4.9    12     25     3120      8,20
Total Entries: 2
Console> (enable)
```

次に、特定の MSFC および特定のマルチキャスト送信元アドレスについて、IP MMLS エントリを表示する例を示します。

```
Console> (enable) show mls multicast entry 15 1.1.5.252 source 1.1.11.1 short
Router IP       Dest IP         Source IP       Pkts       Bytes
 InVlan  OutVlans
--------------- --------------- --------------- ---------- --------------------
  ------ ----------
172.20.49.159   224.1.1.6       1.1.40.4        368        57776
  40     23,25
172.20.49.159   224.1.1.71      1.1.22.2        99         65142
  22     30,37
172.20.49.159   224.1.1.8       1.1.22.2        396        235620
  22     13,19
Console> (enable)
```

CHAPTER 15

アクセス制御の設定

この章では、Catalyst 6500 シリーズ スイッチ上で Access Control List（ACL; アクセス制御リスト）を設定する手順について説明します。ACL の設定は、スーパバイザ エンジンに搭載されているハードウェアのタイプによって異なります。詳細については、「ハードウェアの要件」（p.15-3）を参照してください。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

(注) Policy-Based ACL（PBACL）設定の詳細については、「PBACL の設定」（p.42-21）を参照してください。

この章で説明する内容は、次のとおりです。

(注) 特に明記されていないかぎり、この章で説明する情報および手順は、Policy Feature Card 3B/3BXL（PFC3B/PFC3BXL; ポリシー フィーチャ カード 3B/3BXL）を搭載した Supervisor Engine 32、PFC3A/PFC3B/PFC3BXL を搭載した Supervisor Engine 720、PFC2 を搭載した Supervisor Engine 2、および PFC を搭載した Supervisor Engine 1 に適用されます。

ACL の機能概要

従来、スイッチが動作するのはレイヤ 2 でのみでした。スイッチが VLAN（仮想 LAN）内のトラフィックをスイッチングし、ルータが VLAN 間のトラフィックをルーティングしていました。Catalyst 6500 シリーズ スイッチは、Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）を搭載し、レイヤ 3 スイッチング（Multilayer Switching [MLS; マルチレイヤ スイッチング]）を使用することによって、VLAN 間の高速パケット ルーティングをサポートしています。スイッチがパケットをブリッジングすると、パケットはルータに渡されずに内部的にルーティングされたあと、再びブリッジングされて宛先に送信されます。このプロセスの実行中、スイッチは VLAN 内でブリッジングされるパケットを含み、スイッチングする すべてのパケットをアクセス制御できます。

Cisco IOS ACL が、VLAN 間でルーティングされるトラフィックのアクセス制御を行い、VLAN ACL（VACL）がすべてのパケットのアクセス制御を行います。

パケットの分類には、標準 Cisco IOS ACL および拡張 Cisco IOS ACL を使用します。分類されたパケットには、アクセス制御（セキュリティ）、暗号化、Policy-Based Routing（PBR）など、さまざまな機能が適用されます。標準および拡張 Cisco IOS ACL は、ルータのインターフェイス上だけで設定し、ルーテッド パケットに適用されます。

VACL は、IP および IPX プロトコルのレイヤ 3 アドレスに基づくアクセス制御を行います。サポートされないプロトコルのアクセス制御は、MAC（メディア アクセス制御）アドレス経由で実行されます。VACL は（ブリッジングおよびルーティングされた）すべてのパケットに適用され、任意の VLAN インターフェイス上で設定することができます。VLAN 上で VACL を設定すると、その VLAN に送信されてきた（ルーティングまたはブリッジングされた）すべてのパケットが、VACL チェックの対象になります。パケットは、スイッチ ポートを通じて、またはルーティングされてからルータ ポートを通じて VLAN に送信されます。

（注） Supervisor Engine 720（PFC3A/PFC3B/PFC3BXL）および Supervisor Engine 32（PFC3B/PFC3BXL）では、IPX ルーティングはソフトウェアにより行われ、IPX Cisco IOS ACL および IPX VACL はサポートされません。MAC VACL を使用して IPX パケットを一致させることができます。IPX ARPA フレームを一致させるため、**ipx-arpa** キーワードを入力できます。IPX 非 ARPA フレームおよび Ethertype 0xffff のフレームで一致させるには、0xffff Ethertype を使用します。MAC VACL の設定については、「non-IP version 4/non-IPX VACL（MAC VACL）の作成および ACE の追加」（p.15-53）を参照してください。

ハードウェアの要件

Catalyst 6500 シリーズ スイッチ上で ACL を設定するには、次のハードウェアが必要です。

- Cisco IOS ACL
  - PFC および MSFC または MSFC2 搭載の Supervisor Engine 1
  - PFC2 および MSFC2 搭載の Supervisor Engine 2
  - PFC3A/PFC3B/PFC3BXL および MSFC3 搭載の Supervisor Engine 720
  - PFC3B/PFC3BXL および MSFC2A 搭載の Supervisor Engine 32
- VACL および Quality of Service（QoS; サービス品質）ACL
  - PFC 搭載の Supervisor Engine 1
  - PFC2 搭載の Supervisor Engine 2
  - PFC3A/PFC3B/PFC3BXL 搭載の Supervisor Engine 720
  - PFC3B/PFC3BXL 搭載の Supervisor Engine 32

（注） スイッチ上でサポートされる QoS フィーチャ セットは、スーパバイザ エンジン上に搭載されているスイッチング エンジン ドータ カードによって異なります。詳細については、第 49 章「QoS の設定」を参照してください。

サポートされる ACL

ここでは、Catalyst 6500 シリーズ スイッチがサポートしている ACL について説明します。

QoS ACL

QoS ACL はスイッチ上で設定することができます。第 49 章「QoS の設定」を参照してください。

Cisco IOS ACL

Cisco IOS ACL は、MSFC VLAN インターフェイス上で設定します。ACL は、一連の順序に基づく Access Control Entry（ACE; アクセス制御エントリ）によって、アクセス制御を行います。他の多くの機能もまた、フロー指定のために ACL を使用します。たとえば、(Web Cache Coordination Protocol [WCCP] に基づく）Web キャッシュ リダイレクト機能では、ACL を使用して、Web キャッシュ エンジンにリダイレクトする HTTP フローを指定します。

ほとんどの Cisco IOS 機能は、特定の方向（着信または発信）でインターフェイスに適用されます。ただし、機能によってはグローバルな ACL を使用します。このような機能では、指定した方向のすべてのインターフェイス上に ACL が適用されます。たとえば、TCP 代行受信は、発信方向のすべてのインターフェイス上に適用されるグローバル ACL を使用します。

1 つの Cisco IOS ACL を、特定のインターフェイスの複数の機能と併用できます。また、1 つの機能で複数の ACL を使用することもできます。複数の機能で 1 つの ACL を共有する場合、Cisco IOS ソフトウェアは同じ ACL を何度も検証します。

Cisco IOS ソフトウェアは、特定のインターフェイスおよび方向に設定された各機能について、関連 ACL を検証します。ルータの特定のインターフェイス上にパケットが送信されると、Cisco IOS ソフトウェアは、そのインターフェイス上に設定されているすべての着信機能について、次のような関連 ACL を検証します。

- 着信 ACL（標準、拡張、および再帰、またはそのいずれか）
- 暗号化 ACL（MSFC 上では非サポート）
- ポリシー ルーティング ACL
- 外部から内部へのアドレス変換を指定する Network Address Translation（NAT; ネットワーク アドレス変換）

パケットがルーティングされると、次のホップに転送される前に、Cisco IOS ソフトウェアは出力インターフェイスに設定された発信機能について、次のすべての関連 ACL を検証します。

- 発信 ACL（標準、拡張、および再帰、またはそのいずれか）
- 暗号化 ACL（MSFC 上では非サポート）
- NAT ACL（内部から外部へのアドレス変換）
- WCCP ACL
- TCP 代行受信 ACL

VACL

ここでは、VACL について説明します。

VACL の概要

VACL では、すべてのトラフィックをアクセス制御できます。スイッチ上で VACL を設定し、VLAN が着信または発信するようルーティングされる、または VLAN 内でブリッジングされるすべてのパケットに VACL を適用できます。VACL は、セキュリティ パケット フィルタリングを完全に実行し、トラフィックを特定の物理スイッチ ポートに転送します。Cisco IOS ACL と異なり、VACL には方向（入力または出力）を定義しません。

VACL は、IP および IPX のレイヤ 3 アドレスに基づいて設定します。他のプロトコルはすべて、MAC アドレスおよび MAC VACL を使用する Ethertype によってアクセス制御されます。

注意　IP トラフィックおよび IPX トラフィックは、MAC VACL ではアクセス制御されません。その他のトラフィック タイプ（AppleTalk、DECnet など）はすべて MAC トラフィックとして分類され、MAC VACL によってアクセス制御されます。

（注）　Supervisor Engine 720（PFC3A/PFC3B/PFC3BXL）および Supervisor Engine 32（PFC3B/PFC3BXL）、では、IPX ルーティングはソフトウェアにより行われ、IPX Cisco IOS ACL および IPX VACL はサポートされません。MAC VACL を使用して IPX パケットを一致させることができます。IPX ARPA フレームを一致させるため、**ipx-arpa** キーワードを入力できます。IPX 非 ARPA フレームおよび Ethertype 0xffff のフレームで一致させるには、0xffff Ethertype を使用します。MAC VACL の設定については、「non-IP version 4/non-IPX VACL（MAC VACL）の作成および ACE の追加」（p.15-53）を参照してください。

VACL を適用できるのは、Catalyst 6500 シリーズ スイッチ経由で転送されるパケットだけです。ハブ上のホスト間または Catalyst 6500 シリーズ スイッチに接続している他のスイッチを経由するトラフィックに対して、VACL を適用することはできません。

VACL でサポートされる ACE

VACL には、ACE の順序リストが設定されています。各 VACL に設定できるのは、1 タイプの ACE だけです。各 ACE には、パケットの内容に対応する多数のフィールドがあります。各フィールドに、関連するビットを示す関連ビット マスクを指定します。各 ACE には、条件に一致したパケットをどのように処置するかを指定する 1 つの動作が関連付けられます。この動作は、機能によって異なります。Catalyst 6500 シリーズ スイッチは、ハードウェアで次の 3 タイプの ACE をサポートしています。

- IP ACE
- IPX ACE
- Ethernet ACE

表 15-1 に、各 ACE タイプの関連パラメータを示します。

表 15-1　ACE のタイプおよびパラメータ

ACE タイプ	TCP または UDP[1]	ICMP[1]	その他の IP[1]	IPX	イーサネット[2]
レイヤ 4 パラメータ	送信元ポート				
	送信元ポート演算子				
	宛先ポート				
	宛先ポート演算子	ICMP コード[1]			
	該当なし	ICMP タイプ	該当なし		
レイヤ 3 パラメータ	IP ToS バイト	IP ToS バイト	IP ToS バイト		
	IP 送信元アドレス	IP 送信元アドレス	IP 送信元アドレス	IPX 送信元ネットワーク	
	IP 宛先アドレス	IP 宛先アドレス	IP 宛先アドレス	IPX 宛先ネットワーク	
				IPX 宛先ノード	
	TCP または UDP	ICMP	その他のプロトコル	IPX パケット タイプ	
レイヤ 2 パラメータ					Ethertype
					イーサネット送信元アドレス
					イーサネット宛先アドレス

1. IP ACE
2. IP バージョン 4 または IPX 以外のイーサネット パケット

分割および非分割トラフィックの処理

TCP/UDP または任意のレイヤ 4 プロトコル トラフィックは、分割されると、レイヤ 4 情報（レイヤ 4 送信元 / 宛先ポート）が失われます。この場合、アプリケーションに基づくセキュリティを適用するのは困難です。ただし、分割トラフィックかどうかを識別して、他の TCP/UDP トラフィックと区別することができます。

ACE のレイヤ 4 パラメータは、オフセット 0 のフラグメントを持つ非分割トラフィックおよび分割トラフィックをフィルタリングできます。オフセットが 0 以外の IP フラグメントは、レイヤ 4 ポート情報が失われているので、フィルタリングすることはできません。パケット分割に対応する ACE の例を示します。

次に、1.1.1.1（ポート 68）からのトラフィックが分割されていた場合、最初のフラグメントだけをポート 4/3 に転送する例を示します。ポート 68 からの他のトラフィックはこのエントリの条件とは一致しません。

```
redirect 4/3 tcp host 1.1.1.1 eq 68 host 255.255.255.255
```

次に、1.1.1.1（ポート 68）から発信され、2.2.2.2（ポート 34）を宛先とするトラフィックを許可する例を示します。パケットが分割されている場合、最初のフラグメントはこのエントリの条件と一致するので、許可されます。ただし、オフセットが 0 以外のフラグメントも、デフォルトの分割結果として許可されます。

```
permit tcp host 1.1.1.1 eq 68 host 2.2.2.2 eq 34
```

次に、1.1.1.1（ポート 68）から発信され、2.2.2.2（ポート 34）を宛先とするトラフィックのうち、オフセットが 0 の分割を拒否する例を示します。オフセットが 0 以外のフラグメントは、デフォルトとして許可されます。

```
deny tcp host 1.1.1.1 eq 68 host 2.2.2.2 eq 34
```

Release 6.1(1) より前のソフトウェア リリースでは、フラグメント フィルタリングは完全にトランスペアレントです。**permit tcp .... port eq** *port_number* などの ACE を入力すると、この ACL の先頭に permit tcp any any fragments という ACE がソフトウェアによって暗黙的に付加されます。

Release 6.1(1) 以降のソフトウェア リリースでは、**fragment** オプションが設定されています。**fragment** キーワードを指定しない場合は、旧リリースと同じ結果になります。**fragment** キーワードを指定すると、フラグメントのグローバルな許可ステートメントは自動的には付加されません。このキーワードにより、フラグメントの処理方法を、より詳細に制御できます。

次の例では、サーバ HTTP 接続用として 10.1.1.2 が設定されています。フラグメント ACE を使用しない場合、ACL の先頭に **permit tcp any any fragments** の ACE が自動的に付加されるので、TCP トラフィックのすべてのフラグメントが許可されます。

```
permit tcp any any fragments
```

1. **permit tcp any host 10.1.1.2 eq www**
2. **deny ip any host 10.1.1.2**
3. **permit ip any any**

上の例でエントリ 1 を次のように変更すると、

1. deny tcp any host 10.1.1.2 eq www

permit tcp any any fragments ACE が ACL の先頭に追加されません。エントリが **deny** ステートメントの場合は、次のアクセスリスト エントリが処理されます。

（注） **deny** ステートメントは、非初期フラグメント対非フラグメント化または初期フラグメントとは別の方法で処理されます。

fragment キーワードを指定すると、グローバルな TCP/UDP フラグメント許可ステートメントは付加されません。少なくとも 1 つの ACE に **fragment** キーワードが指定されていると、指定した特定の IP アドレス（またはサブネット）宛てのフローを許可する ACE が自動的に付加されます。

次の ACL の例では、**deny tcp any host 10.1.1.2 fragment** エントリにより、ホスト 10.1.1.2 上のすべての TCP ポートへの分割トラフィックの転送を拒否しています。また、**permit udp any host 10.1.1.2 eq 69** エントリにより、Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバ 10.1.1.2 への接続が許可されています。この場合、**permit for all fragments of udp traffic to host 10.1.1.2** の ACE が自動的に付加されます。この ACE が付加されない場合、フラグメントは **deny ip any host 10.1.1.2** エントリによって拒否されます。

1. **deny tcp any host 10.1.1.2 fragment**
2. **permit tcp any host 10.1.1.2 eq www**
3. **permit udp any host 10.1.1.2 eq 69**
4. **permit udp any gt 1023 10.1.1.2 gt 1023**
5. **deny ip any host 10.1.1.2**
6. **permit ip any any**

ホスト 10.1.1.2 への分割 UDP トラフィックを明示的に停止したい場合には、次の例のように、3 番めのエントリの前に **deny udp any host 10.1.1.2 fragment** を入力します。

[...]

3. **deny udp any host 10.1.1.2 fragment**
4. **permit udp any host 10.1.1.2 eq 69**
5. **permit udp any gt 1023 10.1.1.2 gt 1023**

[...]

VLAN 上での Cisco IOS ACL および VACL の適用

ここでは、ブリッジド パケット、ルーテッド パケット、およびマルチキャスト パケットについて、VLAN に Cisco IOS ACL および VACL を適用する方法について説明します。

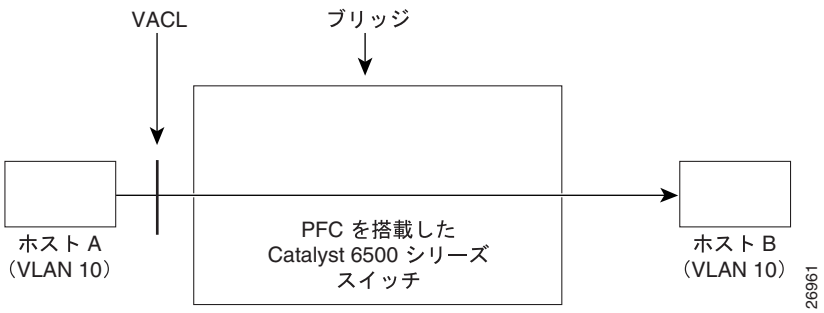
以下、ACL および VACL の適用方法について説明します。

- ブリッジド パケット（p.15-8）
- ルーテッド パケット（p.15-8）
- マルチキャスト パケット（p.15-9）

ブリッジド パケット

図 15-1 は、ブリッジド パケットに ACL がどのように適用されるのかを示しています。ブリッジド パケットの場合は、レイヤ 2 ACL だけが入力 VLAN に適用されます。

図 15-1　ブリッジド パケットへの ACL の適用

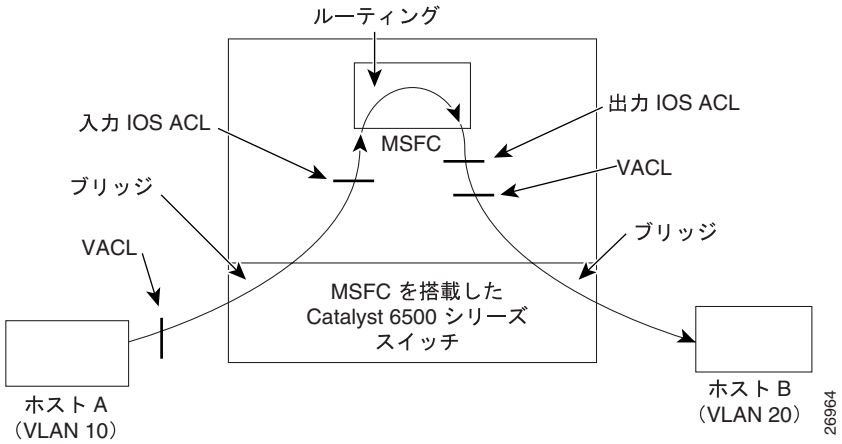


ルーテッド パケット

図 15-2 は、ルーテッド / レイヤ 3 スイッチド パケットに ACL がどのように適用されるのかを示しています。ルーテッド / レイヤ 3 スイッチド パケットの場合、ACL は次の順序で適用されます。

1. 入力 VLAN 用の VACL
2. 入力 Cisco IOS ACL
3. 出力 Cisco IOS ACL
4. 出力 VLAN 用の VACL

図 15-2　ルーテッド パケットへの ACL の適用

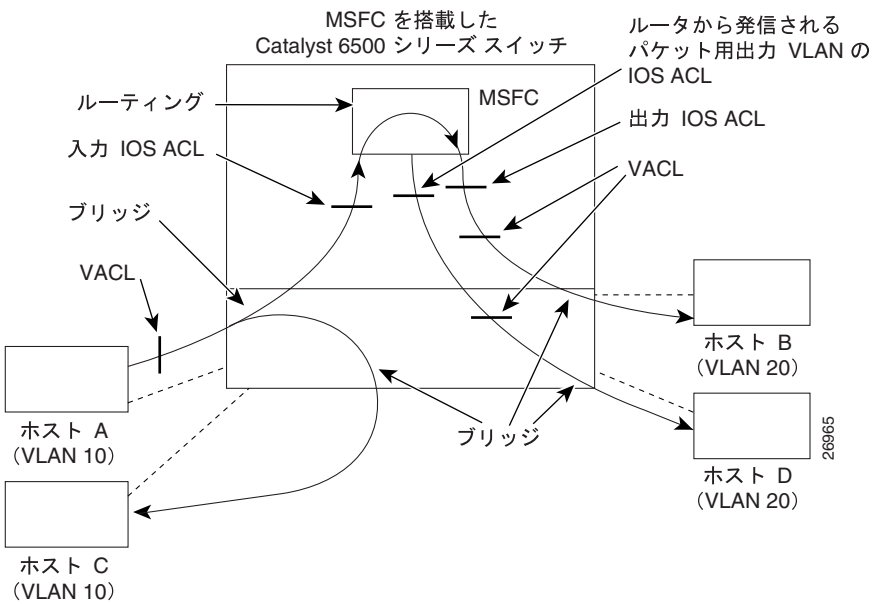


マルチキャスト パケット

図 15-3 は、マルチキャスト拡張を必要とするパケットに対して ACL がどのように適用されるのかを示しています。マルチキャスト拡張を必要とするパケットの場合、ACL は次の順序で適用されます。

1. マルチキャスト拡張を必要とするパケット
   a. 入力 VLAN 用の VACL
   b. 入力 Cisco IOS ACL
2. マルチキャスト拡張後のパケット
   a. 出力 Cisco IOS ACL
   b. 出力 VLAN 用の VACL
3. ルータから発信されたパケット
   a. 出力 VLAN 用の VACL

図 15-3　マルチキャスト パケットへの ACL の適用



ネットワークにおける Cisco IOS ACL の使用方法

（注） Catalyst 6500 シリーズ スイッチのルーテッド VLAN インターフェイス上での Cisco IOS ACL の設定は、他のシスコ製ルータ上での ACL の設定と同じです。Cisco IOS ACL を設定する場合は、「サポートされない機能」（p.15-44）および「VACL 設定時の注意事項」（p.15-45）を参照してください。また、Cisco IOS のコンフィギュレーション ガイドおよびコマンド リファレンスも参照してください。IP の ACL を設定する場合には、『*Network Protocols Configuration Guide*』Part 1 の「Configuring IP Services」を参照してください。

ルータ上にトラフィックを処理する機能（NAT など）を設定すると、その機能に関連付けられている Cisco IOS ACL によって、レイヤ 3 のスイッチングではなくルータにブリッジングされる特定のトラフィックが判別されます。通常、ルータはその機能を適用し、パケットをルーティングします。「PFC でのハードウェアおよびソフトウェアによる Cisco IOS ACL の処理」（p.15-11）で、このプロセスの例外をいくつか紹介しています。

（注） 冗長 MSFC を搭載したシステムでは、両方の MSFC 上で、Cisco IOS ACL および VACL の同じ ACL 設定を適用する必要があります。

注意 PFC の場合：デフォルトでは、パケットがアクセス グループによって拒否されると、MSFC により Internet Control Message Protocol（ICMP）unreachables（到達不能）メッセージが送信されます。アクセス グループによって拒否されたパケットはハードウェアでは廃棄されず、MSFC が ICMP 到達不能メッセージを生成できるように、MSFC にブリッジングされます。アクセス グループによって拒否されたパケットをハードウェアで廃棄するには、**no ip unreachables** インターフェイス コンフィギュレーション コマンドを使用して、ICMP unreachables をディセーブルにする必要があります。**ip unreachables** コマンドは、デフォルトでイネーブルに設定されています。

PFC2 および PFC3A/PFC3B/PFC3BXL の場合：インターフェイス上で IP unreachables または IP redirect がイネーブルに設定されていると、ハードウェア上で拒否が実行されます。ただし、適切な ICMP 到達不能メッセージを生成するため、少数のパケットが MSFC2/MSFC3 に送信されます。

ここでは、PFC、PFC2、および PFC3A/PFC3B/PFC3BXL でのハードウェアおよびソフトウェアによる ACL の処理について説明します。

- PFC でのハードウェアおよびソフトウェアによる Cisco IOS ACL の処理（p.15-11）
- PFC2 および PFC3A/PFC3B/PFC3BXL でのハードウェアおよびソフトウェアによる Cisco IOS ACL の処理（p.15-13）

PFC でのハードウェアおよびソフトウェアによる Cisco IOS ACL の処理

ここでは、PFC でのハードウェアおよびソフトウェアによる Cisco IOS ACL の処理について説明します。

(注)　PFC2 および PFC3A/PFC3B/PFC3BXL での Cisco IOS ACL の情報については、「PFC2 および PFC3A/PFC3B/PFC3BXL でのハードウェアおよびソフトウェアによる Cisco IOS ACL の処理」（p.15-13）を参照してください。

ACL 機能の処理では、ソフトウェアによっていくつかのフローを転送する必要があります。ソフトウェア転送フローの割合は、ハードウェア転送フローに比べると、かなり少ないものです。ACL によりロギングが要求されているフローはソフトウェアに渡されますが、ハードウェアによる非ログフローの転送には影響しません。

(注)　**show ip access-list** コマンドの出力に表示されるマッチ カウントは、ハードウェアでアクセス制御されたパケット数ではありません。

(注)　送信元ホストのノード番号を指定した IPX Cisco IOS ACL を、ハードウェアのスイッチ上で実行することはできません。そのため、MSFC がソフトウェアで ACL を処理することになります。この処理は、システムのパフォーマンスを*著しく*低下させます。

ここでは、各種 ACL とトラフィック フローがハードウェアおよびソフトウェアによってどのように処理されるかについて説明します。

- セキュリティ Cisco IOS ACL（p.15-11）
- 再帰 ACL（p.15-12）
- TCP 代行受信（p.15-12）
- ポリシー ルーティング（p.15-12）
- WCCP（p.15-13）
- NAT（p.15-13）
- ユニキャスト RPF チェック（p.15-13）
- ブリッジ グループ（p.15-13）

セキュリティ Cisco IOS ACL

PFC では、IP および IPX のセキュリティ Cisco IOS ACL は次のように処理されます。

- セキュリティ ACL の [deny]（拒否）ステートメントと一致するフローは、[ip unreachables]（IP 到達不能）をディセーブルに設定しておくと、ハードウェアによって廃棄されます。[permit]（許可）ステートメントと一致するフローは、ハードウェアによりスイッチングされます。
- セキュリティ アクセス制御用の標準 ACL および拡張 ACL（入力および出力）の許可および拒否動作は、ハードウェアによって処理されます。
- 特定のインターフェイス上の ACL アクセス違反の IP アカウントは、そのインターフェイス上で拒否されたすべてのパケットをソフトウェアに転送することによってサポートされます。この動作は他のフローには影響しません。

- ダイナミック（ロックおよび鍵）ACL フローはハードウェアでサポートされますが、アイドル タイムアウトはサポートされません。
- IPX 標準入力 ACL および出力 ACL は、ACL パラメータが IPX 送信元ネットワーク、宛先ネットワーク、および宛先ノードの場合（またはそのいずれかの場合）、ハードウェアによってサポートされます。ACL に他のパラメータが含まれている場合には、ソフトウェアによって処理されます。
- IPX 拡張入力 ACL および出力 ACL は、ACL パラメータが IPX 送信元ネットワーク、宛先ネットワーク、宛先ノード、およびプロトコル タイプの場合（またはそのいずれかの場合）、ハードウェアによってサポートされます。
- ロギングが必要な ACL フローはソフトウェアによって処理されますが、ハードウェアによる非ログ フローの転送には影響しません。

再帰 ACL

ハードウェアにより、最大 512 の同時再帰セッションがサポートされています。再帰 ACL が適用されている際は、フロー マスクが VLAN-full flow に変更されています。

TCP 代行受信

TCP 代行受信は、DoS 攻撃の一種である TCP SYN フラッディング攻撃から TCP サーバを保護するソフトウェアを実装します。TCP 代行受信は、TCP 接続要求を代行受信して検証することにより、SYN フラッディング攻撃を防止できるようにします。代行受信モードの場合、TCP 代行受信ソフトウェアはクライアントからサーバに送られる、拡張アクセス リストと一致する TCP SYN パケットを代行受信します。ソフトウェアは宛先サーバの代わりにクライアントとの接続を確立します。接続が正常に確立されると、クライアントの代わりにサーバとの接続を確立して、2 つの半接続をトランスペアレントにバインドします。このプロセスにより、到達不能なホストからの接続要求がサーバに到達しないようになります。ソフトウェアは接続されている間、代行受信を継続してパケットを転送します。

ポリシー ルーティング

ポリシー ルーティングが必要なフローは、ソフトウェアによって処理されますが、ハードウェアによる非ポリシー ルーティング フローの転送には影響しません。ルート マップに複数の [match]（一致）コマンドが含まれている場合、すべての一致条件を満たしているパケットだけが、ポリシー ルーティングされます。ただし、ルート マップに [match ip address] および [match length] の両方が含まれている場合には、[match ip address] コマンドの ACL に一致するすべてのトラフィックが、[match length] の条件を満たしているかどうかに関係なく、ソフトウェアに転送されます。ルート マップに match length コマンドだけが含まれている場合は、インターフェイスが受信したすべてのパケットがソフトウェアに転送されます。

mls ip pbr グローバル コマンドを使用してハードウェアのポリシー ルーティングをイネーブルにすると、すべてのポリシー ルーティングがハードウェアで実行されます。

注意　**mls ip pbr** コマンドを使用してポリシー ルーティングをイネーブルにした場合、各インターフェイスにポリシー ルーティングが設定されているかどうかに関係なく、ハードウェアのすべてのインターフェイスにポリシー ルーティングが適用されます。

WCCP

WCCP リダイレクトの対象になる HTTP 要求は、ソフトウェアによって処理されます。サーバおよびキャッシュ エンジンからの HTTP 応答は、ハードウェアで処理されます。

NAT

NAT が必要なフローは、ソフトウェアによって処理されますが、ハードウェアによる非 NAT フローの転送には影響しません。

ユニキャスト RPF チェック

ユニキャスト RPF 機能は、PFC 上のハードウェアでサポートされています。ACL ベースの RPF チェックの場合、ユニキャスト RPF ACL によって拒否されたトラフィックは、RPF 検証のために MSFC に転送されます。

注意　ACL ベースのユニキャスト RPF では、ACL によって拒否されたパケットは、CPU に RPF 検証のために送信されます。DoS 攻撃の場合には、このようなパケットは拒否 ACE にほぼ一致するので、CPU に転送されます。トラフィックが多い状況では、これによって CPU の利用率が高くなります。

（注）　ACL ベースの RPF チェックでは、廃棄抑制統計はサポートされていません。

ブリッジ グループ

Cisco IOS ブリッジ グループ ACL は、ソフトウェアによって処理されます。

PFC2 および PFC3A/PFC3B/PFC3BXL でのハードウェアおよびソフトウェアによる Cisco IOS ACL の処理

ここでは、PFC2 および PFC3A/PFC3B/PFC3BXL で構成されたスイッチでのハードウェアおよびソフトウェアによる Cisco IOS ACL の処理について説明します。

ACL 機能の処理では、いくつかのフローをソフトウェアに転送する必要があります。ソフトウェア転送フローの割合は、ハードウェア転送フローに比べると、かなり少ないものです。ACL によりロギングが要求されているフローはソフトウェアに渡されますが、ハードウェアによる非ログ フローの転送には影響しません。

（注）　**show ip access-list** コマンドの出力に表示されるマッチ カウントは、ハードウェアでアクセス制御されたパケット数ではありません。

（注）　送信元ホストのノード番号を指定した IPX Cisco IOS ACL を、ハードウェアのスイッチ上で実行することはできません。そのため、MSFC がソフトウェアで ACL を処理することになります。この処理は、システムのパフォーマンスを*著しく*低下させます。

(注) Supervisor Engine 720（PFC3A/PFC3B/PFC3BXL）および Supervisor Engine 32（PFC3B/PFC3BXL）では、IPX ルーティングはソフトウェアにより行われ、IPX Cisco IOS ACL および IPX VACL はサポートされません。MAC VACL を使用して IPX パケットを一致させることができます。IPX ARPA フレームを一致させるため、**ipx-arpa** キーワードを入力できます。IPX 非 ARPA フレームおよび Ethertype 0xffff のフレームで一致させるには、0xffff Ethertype を使用します。MAC VACL の設定については、「non-IP version 4/non-IPX VACL（MAC VACL）の作成および ACE の追加」（p.15-53）を参照してください。

ここでは、各種 Cisco IOS ACL とトラフィック フローが、PFC2 または PFC3A/PFC3B/PFC3BXL で構成されたスイッチで、ハードウェアおよびソフトウェアによってどのように処理されるかについて説明します。

セキュリティ Cisco IOS ACL

PFC2 または PFC3A/PFC3B/PFC3BXL で構成されたスイッチの IP および IPX のセキュリティ Cisco IOS ACL は次のように処理されます。

- [ip unreachables] または [ip redirect] オプションがイネーブルの場合、ACL の [deny] ステートメントと一致するフローのパケットの大半がハードウェアで廃棄されます。少数のパケットだけは、ルータから適切な ICMP 到達不能メッセージを送信するためにソフトウェアに渡されます。
- セキュリティ アクセス制御用の標準 ACL および拡張 ACL（入力および出力）の許可および拒否動作は、ハードウェアによって処理されます。
- 特定のインターフェイス上の ACL アクセス違反の IP アカウントは、そのインターフェイス上で拒否されたすべてのパケットをソフトウェアに転送することによってサポートされています。この動作は他のフローには影響しません。
- ダイナミック（ロックおよび鍵）ACL フローはハードウェアでサポートされていますが、アイドル タイムアウトはサポートされていません。
- IPX 標準入力 ACL および出力 ACL は、ACL パラメータが IPX 送信元ネットワーク、宛先ネットワーク、および宛先ノードの場合（またはそのいずれかの場合）、ハードウェアによってサポートされます。ACL に他のパラメータが含まれている場合には、ソフトウェアによって処理されます。
- IPX 拡張入力 ACL および出力 ACL は、ACL パラメータが IPX 送信元ネットワーク、宛先ネットワーク、宛先ノード、およびプロトコル タイプの場合（またはそのいずれかの場合）、ハードウェアによってサポートされます。
- ロギングが必要な ACL フローはソフトウェアによって処理されますが、ハードウェアによる非ログ フローの転送には影響しません。

Cisco IOS ACL ロギングのレート制限

Cisco IOS ACL ロギングのレート制限によって、ブリッジド ACE の MSFC CPU に送信されるパケット数が制限されます。ログ オプションが指定された Cisco IOS ACL の結果が拒否または許可の場合、ACE がブリッジングされます。このブリッジ動作の結果、Cisco IOS ACL ロギングは MSFC CPU の過負荷をもたらします。Cisco IOS ACL ロギングのレート制限を設定すると、ブリッジングされた ACE はレート制限付きで MSFC にリダイレクトされます。

Cisco IOS ACL ロギングのレート制限設定時の注意事項

ここでは、Cisco IOS ACL ロギングのレート制限設定時の注意事項について説明します。

- **set acllog ratelimit** *rate* コマンドまたは **clear acllog** コマンドを入力したあとで、MSFC をリセットするか、**log** キーワードが適用された ACE を備えた MSFC インターフェイスに対して shutdown/no shutdown を実行する必要があります。

  set acllog ratelimit *rate* コマンドを入力すると、リセットまたは shutdown/no shutown 動作によってブリッジングされた ACE はレート制限付きで MSFC にリダイレクトされます。

  clear acllog コマンドを入力すると、リセットまたは shutdown/no shutdown 動作によってスイッチは元の動作に戻り、ブリッジ動作は元のままです。

- **set acllog ratelimit** *rate* コマンドを入力して指定する *rate* には、1 ～ 1000 の値を使用できます。*rate* は、リダイレクト ACE と一致し、MSFC に送信される 1 秒当たりのパケット数です。実際の 1 秒当たりのパケット数が指定した *rate* より大きい場合は、指定した *rate* を超えるパケットは廃棄されます。*rate* には、500 パケット / 秒を指定することを推奨します。

Cisco IOS ACL ロギングのレート制限の設定

Cisco IOS ACL ロギングのレート制限を設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ACL ロギングをイネーブルにして、Cisco IOS ACL ロギング レート制限のレートを指定します。	**set acllog ratelimit** *rate*
ステップ 2	ACL ロギング ステータスを表示します。	**show acllog**

次に、ACL ロギングをイネーブルにして、Cisco IOS ACL ロギング レート制限のレートを 500 に指定する例を示します。

```
Console> (enable) set acllog ratelimit 500
If the ACLs-LOG were already applied, the rate limit mechanism will be effective on
system restart, or after shut/no shut the interface.
Console> (enable)

Console> (enable) show acllog
ACL log rate limit enabled, rate = 500 pps.
Console> (enable)
```

次に、ACL ロギングを消去する（ディセーブルにする）例を示します。ACL ロギングを消去すると、ブリッジ動作は元どおりになり、システムの動作は **set acllog ratelimit** コマンドを発行する前と同じになります。

```
Console> (enable) clear acllog
ACL log rate limit is cleared.
If the ACLs-LOG were already applied, the rate limit mechanism will be disabled on
system restart, or after shut/no shut the interface.
Console> (enable)
```

再帰 ACL

ICMP パケットは、ソフトウェアによって処理されます。TCP/UDP フローの場合は、フローが確立されれば、ハードウェアによって処理されます。再帰 ACL が適用されている際は、フロー マスクが VLAN-full flow に変更されています。

TCP 代行受信

（注） TCP 代行受信は、Supervisor Engine 720（PFC3A/PFC3B/PFC3BXL）または Supervisor Engine 32（PFC3B/PFC3BXL）ではサポートされません。

TCP 代行受信は、DoS 攻撃の一種である TCP SYN フラッディング攻撃から TCP サーバを保護するソフトウェアを実装します。TCP 代行受信は、TCP 接続要求を代行受信して検証することにより、SYN フラッディング攻撃を防止できるようにします。代行受信モードの場合、TCP 代行受信ソフトウェアはクライアントからサーバに送られる、拡張アクセス リストと一致する TCP SYN パケットを代行受信します。ソフトウェアは宛先サーバの代わりにクライアントとの接続を確立します。接続が正常に確立されると、クライアントの代わりにサーバとの接続を確立して、2 つの半接続をトランスペアレントにバインドします。このプロセスにより、到達不能なホストからの接続要求がサーバに到達しないようになります。ソフトウェアは接続されている間、代行受信を継続してパケットを転送します。

PFC2 では、TCP 代行受信が次のようにハードウェアによってサポートされています。

1. TCP 代行受信が設定されている場合、TCP 代行受信 ACL 内の permit ステートメントを含む ACE と一致し、かつセキュリティ ACL によって許可されているすべての TCP SYN パケットは、TCP 代行受信機能を適用するソフトウェアに送信されます。このプロセスは、セキュリティ ACL に SYN フラグが指定されていない場合でも発生します。
2. 接続が正常に確立されると、次の処理が適用されます。
   a. TCP 代行受信で使用されている代行受信モードにタイムアウトが指定されている場合は、所定の接続 / フローに属するすべてのトラフィックがソフトウェアで処理されます。
   b. TCP 代行受信がそれ以外のモードを使用している場合、接続が正常に確立されると、ソフトウェアはハードウェア ショートカットをインストールして、残りのフローをハードウェアでスイッチングします。
3. 接続が正常に確立されない場合は、他のトラフィックはそのフローに属することができません。

ポリシー ルーティング

ポリシー ルーティングが必要なフローは、ルート マップに応じて、ハードウェアまたはソフトウェアによって処理されます。ルート マップに match ip address だけが設定され、set コマンドにネクスト ホップが含まれている場合、そのネクスト ホップが到達可能であれば、パケットはハードウェアに転送されます。ルート マップに複数の match コマンドが含まれている場合、すべての一致条件を満たしているパケットだけが、ポリシー ルーティングされます。ただし、ルート マップに match ip address および match length の両方が含まれている場合には、match ip address コマンドの ACL に一致するすべてのトラフィックが、match length の条件を満たしているかどうかに関係なく、ソフトウェアに転送されます。ルート マップに match length コマンドだけが含まれている場合は、インターフェイスが受信したすべてのパケットがソフトウェアに転送されます。

（注） PFC2 または PFC3A/PFC3B/PFC3BXL 上では、**mls ip pbr** コマンドは不要です（サポートされていません）。

WCCP

（注） Release 8.1(x) ～ 8.4(x) では、WCCP は Supervisor Engine 720 または Supervisor Engine 32 でサポートされません。

WCCP リダイレクトの対象になる HTTP 要求は、ソフトウェアによって処理されます。サーバおよびキャッシュ エンジンからの HTTP 応答は、ハードウェアで処理されます。

NAT

NAT が必要なフローは、ソフトウェアによって処理されますが、ハードウェアによる非 NAT フローの転送には影響しません。

ユニキャスト RPF チェック

ユニキャスト RPF は、PFC2 および PFC3A/PFC3B/PFC3BXL 上でハードウェアによってサポートされます。ACL ベースの RPF チェックの場合、ユニキャスト RPF ACL によって拒否されたトラフィックは、RPF 検証のために MSFC2 または MSFC3 に転送されます。

注意 ACL ベースのユニキャスト RPF では、ACL によって拒否されたパケットは、CPU に RPF 検証のために送信されます。DoS 攻撃の場合には、このようなパケットは拒否 ACE にほぼ一致するので、CPU に転送されます。トラフィックが多い状況では、これによって CPU の利用率が高くなります。

（注） ACL ベースの RPF チェックでは、廃棄抑制統計はサポートされていません。

ブリッジ グループ

Cisco IOS ブリッジ グループ ACL は、ソフトウェアによって処理されます。

VACL と Cisco IOS ACL の併用

ブリッジド トラフィックおよびルーテッド トラフィックの両方をアクセス制御するには、VACL だけを使用するか、Cisco IOS ACL と VACL を組み合わせて使用します。Cisco IOS ACL は、入力用および出力用の両方のルーテッド VLAN インターフェイスに定義することができます。VACL は、ブリッジド トラフィックのアクセスを制御するために定義します。

ACL の VACL deny または redirect ステートメントの条件に一致したフローは、Cisco IOS ACL の設定に関係なく、拒否またはリダイレクトされます。Cisco IOS ACL を VACL と組み合わせて使用する場合は、次の事項に注意してください。

- 発信 ACL に設定したロギングを必要とするパケットは、VACL によって拒否された場合、ロギングされません。
- NAT ― VACL は、NAT 変換前のパケットに適用されます。また、変換後のフローをアクセス制御する必要がない場合でも、VACL の設定によっては、変換後のフローがアクセス制御されることがあります。

（注） VACL では、リストの最後に暗黙の拒否ステートメントが付加されます。どの VACL ACE にも一致しないパケットは拒否されます。

ここでは、Cisco IOS ACL の設定、VACL の設定、およびレイヤ 4 演算の注意事項について説明します。

- 同一 VLAN インターフェイス上に Cisco IOS ACL および VACL を設定する場合の注意事項（p.15-18）
- レイヤ 4 演算設定時の注意事項（p.15-25）

同一 VLAN インターフェイス上に Cisco IOS ACL および VACL を設定する場合の注意事項

ここでは、同じ VLAN 上に Cisco IOS ACL *および* VACL の両方を設定する場合の注意事項について説明します。Cisco IOS ACL と VACL を異なる VLAN 上にマッピングする設定では、これらの注意事項は当てはまりません。

Catalyst 6500 シリーズ スイッチのハードウェアは、各方向（入力および出力）についてセキュリティ ACL を 1 度だけ検索します。同じ VLAN 上に Cisco IOS ACL および VACL の両方を適用する場合には、これらをマージする必要があります。Cisco IOS ACL と VACL をマージすると、ACE の数が著しく増加することがあります。

同一 VLAN 上で Cisco IOS ACL と VACL を設定する場合には、Cisco IOS ACL および VACL の両方を、次の注意事項に基づいて設定してください。

（注） **show security acl resource-usage** コマンドを入力すると、使用済みの ACL ストレージの割合が表示されます。

ここでは、Cisco IOS ACL と VACL を設定する場合の注意事項、およびその例を示します。

- 暗黙の拒否ステートメント（p.15-19）
- 動作のグループ化（p.15-19）

暗黙の拒否ステートメント

できるだけ、ACL の最後に付加される暗黙の拒否ステートメント（deny any any）を使用し、許可するトラフィックだけを ACE に定義してください。すべての拒否エントリを定義して、最後に許可ステートメント（**permit ip any any**）を指定しても、同じ結果になります（例 1 [p.15-21] を参照）。

動作のグループ化

ACL に複数の動作（許可、拒否、リダイレクト）を定義する場合には、各動作をタイプ別にグループ化します。例 3（p.15-22）は、各タイプをグループ化しなかった場合の例を示しています。この例では、6 行めの deny ステートメントが、permit ステートメントと同じグループに入っています。この deny ステートメントを削除すると、合成後のエントリ数を 329 から 53 に減らすことができます。

動作数の制限

許可 ACE のみで構成される ACL は、許可と拒否という 2 つの動作を含んでいます（リストの最後の暗黙の拒否のため）。許可とリダイレクトが設定されている ACL では、許可、リダイレクト、拒否という 3 つの動作を含んでいます（リストの最後の暗黙の拒否のため）。

ACL の設定時に 2 種類の動作だけを指定すると、最良のマージ結果が得られます（許可と拒否、リダイレクトと許可、リダイレクトと拒否のマージ）。

（注） Release 7.1(1) 以降のスーパバイザ エンジン ソフトウェア リリースでは、ACL マージのアルゴリズムが改善されているので、ACL の設定時に動作数を制限する必要はありません。

リダイレクトおよび拒否の ACL を定義するには、許可 ACE を使用しません。リダイレクトおよび許可の ACL を定義するには、許可 ACE およびリダイレクト ACE だけを定義し、最後に **permit ip any any** ステートメントを指定します。**permit ip any any** を指定すると、リストの最後に付加される暗黙の拒否（deny ip any）が無効になります（例 4 [p.15-22] を参照）。

レイヤ 4 ポート情報の回避

マージ プロセスが複雑になるので、ACL にはレイヤ 4 情報を入れないでください。full flow（送信元 IP アドレス、宛先 IP アドレス、プロトコル、およびプロトコル ポート）ではなく、IP アドレス（送信元および宛先）だけに基づいてフィルタリングする ACL を定義すると、最良のマージ結果が得られます。

full flow を指定する必要がある場合には、「暗黙の拒否ステートメント」（p.15-19）および「動作のグループ化」（p.15-19）を参照してください。ACL に、IP およびレイヤ 4 情報を含む TCP/UDP/ICMP ACE を指定しなければならない場合には、IP アドレスに基づくトラフィック フィルタリングを優先させ、レイヤ 4 の ACE はリストの最後に指定してください。

Release 7.1(1) より前のスーパバイザ エンジン ソフトウェア リリースの場合のマージ結果の推定

(注)　Release 7.1(1) より前のスーパバイザ エンジン ソフトウェア リリースと、7.1(1) 以降のリリースで、マージ結果を比較する場合は、「Release 7.1(1) 以降のスーパバイザ エンジン ソフトウェア リリースの場合のマージ結果の推定」（p.15-23）を参照してください。

上記の注意事項に基づいて ACL を設定した場合、ACL のマージ結果をおおまかに推測することができます。

たとえば、ACL A、ACL B、および ACL C があるとします。ACL C を、ACL A と ACL B のマージ結果とした場合、ACL A と ACL B のサイズがわかっていれば、ACL C の上限サイズを次の公式によって概算することができます。ただし、ACL A と ACL B にレイヤ 4 ポート情報が含まれていないことが前提です。

ACL C のサイズ =（ACL A のサイズ）×（ACL B のサイズ）×（2）

(注)　Release 7.1(1) より前のソフトウェア リリースでは、この公式を目安として使用できますが、エントリ数は予想範囲を大幅に上回ることがあります。Release 7.1(1) 以降のソフトウェアリリースでは、新しい ACL マージ アルゴリズムを使用するので、この公式で正確な値を知ることができます。レイヤ 4 ポート情報が含まれている場合は、新しいアルゴリズムでも上限サイズはさらに大きくなります。詳細については、「レイヤ 4 演算設定時の注意事項」（p.15-25）を参照してください。

ACL マージ アルゴリズムには、Binary Decision Diagram（BDD）と Order-Dependent Merge（ODM）の 2 種類があります。ODM は、Release 7.1(1) のソフトウェア リリースで採用された拡張アルゴリズムです。BDD アルゴリズムは、Release 7.1(1) より前のソフトウェア リリースで使用されていました。設定の詳細については、「ACL マージ アルゴリズムの指定」（p.15-47）を参照してください。

(注)　Release 8.1(1) 以降のソフトウェア リリースでは、BDD アルゴリズムはどのプラットフォーム（PFC、PFC2、または PFC3A/PFC3B/PFC3BXL）上でもサポートされなくなりました。デフォルトの ACL マージ アルゴリズムは ODM です。Release 8.1(1) 以降のソフトウェア リリースでは、コマンドが次のように変更されています。**set aclmerge algo** および **set aclmerge bdd** コマンドは削除されました。**show aclmerge** {**bdd** | **algo**} コマンドは **show aclmerge algo** になりました。

ここでは、さまざまな Cisco IOS ACL および VACL 設定によるマージ結果の例を示します。それぞれ 1 つずつの VACL および Cisco IOS ACL を同じ VLAN に設定します。

例 1

次に、VACL の設定が推奨事項に従っていない（ACL の最後に暗黙の拒否動作を指定する代わりに、9 行めに拒否動作を定義）ため、マージの結果、ACE 数が増える例を示します。

```
******** VACL  ***********
1  permit udp host 194.72.72.33 194.72.6.160 0.0.0.15
2  permit udp host 147.150.213.94 194.72.6.64 0.0.0.15 eq bootps
3  permit udp 194.73.74.0 0.0.0.255 host 194.72.6.205 eq syslog
4  permit udp host 167.221.23.1 host 194.72.6.198 eq tacacs
5  permit udp 194.72.136.1 0.0.3.128 194.72.6.64 0.0.0.15 eq tftp
6  permit udp host 193.6.65.17 host 194.72.6.205 gt 1023
7  permit tcp any host 194.72.6.52
8  permit tcp any host 194.72.6.52 eq 113
9  deny tcp any host 194.72.6.51 eq ftp
10 permit tcp any host 194.72.6.51 eq ftp-data
11 permit tcp any host 194.72.6.51
12 permit tcp any eq domain host 194.72.6.51
13 permit tcp any host 194.72.6.51 gt 1023
14 permit ip  any host 1.1.1.1
******** Cisco IOS ACL ************
1  deny ip any host 239.255.255.255
2  permit ip any any
******** MERGE **********
has 91 entries entries
```

例 2

例 1 の場合、推奨事項に従って 9 行めを削除し（代わりに、ACL の最後で暗黙の拒否を使用）、9 行めで廃棄するはずだったトラフィックが許可されないように、11 行めおよび 12 行めを変更すると、次のような ACL になり、マージ結果が改善されます。

```
******** VACL **********
1  permit udp host 194.72.72.33 194.72.6.160 0.0.0.15
2  permit udp host 147.150.213.94 194.72.6.64 0.0.0.15 eq bootps
3  permit udp 194.73.74.0 0.0.0.255 host 194.72.6.205 eq syslog
4  permit udp host 167.221.23.1 host 194.72.6.198 eq tacacs
5  permit udp 194.72.136.1 0.0.3.128 194.72.6.64 0.0.0.15 eq tftp
6  permit udp host 193.6.65.17 host 194.72.6.205 gt 1023
7  permit tcp any host 194.72.6.52
8  permit tcp any host 194.72.6.52 eq 113
9  permit tcp any host 194.72.6.51 eq ftp-data
10 permit tcp any host 194.72.6.51 neq ftp
11 permit tcp any eq domain host 194.72.6.51 neq ftp
12 permit tcp any host 194.72.6.51 gt 1023
13 permit ip  any host 1.1.1.1
******** Cisco IOS ACL ************
1  deny ip any host 239.255.255.255
2  permit ip any any
******** MERGE ***********
has 78 entries
```

例 3

次に、VACL の設定が推奨事項に従っていない（すべての動作タイプがひとまとめにされていない）ため、マージの結果、ACE 数が著しく増える例を示します。

```
******** VACL  ***********
1  deny ip 0.0.0.0 255.255.255.0 any
2  deny ip 0.0.0.255 255.255.255.0 any
3  deny ip any 0.0.0.0 255.255.255.0
4  permit ip any host 239.255.255.255
5  permit ip any host 255.255.255.255
6  deny ip any 0.0.0.255 255.255.255.0
7  permit tcp any range 0 65534 any range 0 65534
8  permit udp any range 0 65534 any range 0 65534
9  permit icmp any any
10 permit ip any any
******** Cisco IOS ACL **********
1  deny ip any host 239.255.255.255
2  permit ip any any
******** MERGE **********
has 329 entries
```

例 4

次に、VACL の設定が推奨事項に従っていない（3 種類の動作が指定されている）ため、マージの結果、ACE 数が著しく増える例を示します。

```
******** VACL  ***********
1 redirect 4/25 tcp host 192.168.1.67 host 255.255.255.255
2 redirect 4/25 udp host 192.168.1.67 host 255.255.255.255
3 deny tcp any any lt 30
4 deny udp any any lt 30
5 permit ip any any
*******  Cisco IOS ACL ***********
1  deny ip any host 239.255.255.255
2  permit ip any any
*******  MERGE **********
has 142 entries
```

例 5

次に、例 4 の VACL を変更し、2 種類の動作だけを指定したことによって、マージ結果が大幅に改善される例を示します。

```
******** VACL  ***********
1 redirect 4/25 tcp host 192.168.1.67 host 255.255.255.255
2 redirect 4/25 udp host 192.168.1.67 host 255.255.255.255
3 permit ip any any
*******  Cisco IOS ACL ***********
1  deny ip any host 239.255.255.255
2  permit ip any any
*******  MERGE **********
has 4 entries
```

Release 7.1(1) 以降のスーパバイザ エンジン ソフトウェア リリースの場合のマージ結果の推定

Release 7.1(1) より前のスーパバイザ エンジン ソフトウェア リリースの場合と同様、7.1(1) 以降のリリースでも次の公式が成り立ちます。ACL C のサイズ =（ACL A のサイズ）×（ACL B のサイズ）×（2）。

（注） Release 7.1(1) より前のソフトウェア リリースでは、この公式を目安として使用できますが、エントリ数は予想範囲を大幅に上回ることがあります。Release 7.1(1) 以降のソフトウェアリリースでは、新しい ACL マージ アルゴリズムを使用するので、この公式で正確な値を知ることができます。レイヤ 4 ポート情報が含まれている場合は、新しいアルゴリズムでも上限サイズはさらに大きくなります。詳細については、「レイヤ 4 演算設定時の注意事項」（p.15-25）を参照してください。

ACL マージ アルゴリズムには、BDD と ODM の 2 種類があります。ODM は、Release 7.1(1) で採用された拡張アルゴリズムです。BDD アルゴリズムは、Release 7.1(1) より前のソフトウェア リリースで使用されていました。ソフトウェア設定の詳細については、「ACL マージ アルゴリズムの指定」（p.15-47）を参照してください。

（注） Release 8.1(1) 以降のソフトウェア リリースでは、BDD アルゴリズムはどのプラットフォーム（PFC、PFC2、または PFC3A/PFC3B/PFC3BXL）上でもサポートされなくなりました。デフォルトの ACL マージ アルゴリズムは ODM です。Release 8.1(1) 以降のソフトウェア リリースでは、コマンドが次のように変更されています。**set aclmerge algo** および **set aclmerge bdd** コマンドは削除されました。**show aclmerge** {**bdd** | **algo**} コマンドは **show aclmerge algo** になりました。

例

ここでは、さまざまな Cisco IOS ACL および VACL 設定によるマージ結果の例を示します。それぞれ 1 つずつの VACL および Cisco IOS ACL を同じ VLAN に設定します。

例 1

```
******** VACL  ***********
1  permit udp host 194.72.72.33 194.72.6.160 0.0.0.15
2  permit udp host 147.150.213.94 194.72.6.64 0.0.0.15 eq bootps
3  permit udp 194.73.74.0 0.0.0.255 host 194.72.6.205 eq syslog
4  permit udp host 167.221.23.1 host 194.72.6.198 eq tacacs
5  permit udp 194.72.136.1 0.0.3.128 194.72.6.64 0.0.0.15 eq tftp
6  permit udp host 193.6.65.17 host 194.72.6.205 gt 1023
7  permit tcp any host 194.72.6.52
8  permit tcp any host 194.72.6.52 eq 113
9  deny tcp any host 194.72.6.51 eq ftp
10 permit tcp any host 194.72.6.51 eq ftp-data
11 permit tcp any host 194.72.6.51
12 permit tcp any eq domain host 194.72.6.51
13 permit tcp any host 194.72.6.51 gt 1023
14 permit ip  any host 1.1.1.1
******** Cisco IOS ACL ************
1  deny ip any host 239.255.255.255
2  permit ip any any
*******  MERGE **********
Using the new algorithm - 17 entries
Using the old algorighm - 91 entries
```

例 2

```
******** VACL  **********
1  permit udp host 194.72.72.33 194.72.6.160 0.0.0.15
2  permit udp host 147.150.213.94 194.72.6.64 0.0.0.15 eq bootps
3  permit udp 194.73.74.0 0.0.0.255 host 194.72.6.205 eq syslog
4  permit udp host 167.221.23.1 host 194.72.6.198 eq tacacs
5  permit udp 194.72.136.1 0.0.3.128 194.72.6.64 0.0.0.15 eq tftp
6  permit udp host 193.6.65.17 host 194.72.6.205 gt 1023
7  permit tcp any host 194.72.6.52
8  permit tcp any host 194.72.6.52 eq 113
9  permit tcp any host 194.72.6.51 eq ftp-data
10 permit tcp any host 194.72.6.51 neq ftp
11 permit tcp any eq domain host 194.72.6.51 neq ftp
12 permit tcp any host 194.72.6.51 gt 1023
13 permit ip  any host 1.1.1.1
******** Cisco IOS ACL ************
1  deny ip any host 239.255.255.255
2  permit ip any any
******** MERGE ***********
Using the new algorithm - 16 entries
Using the old algorithm - 78 entries
```

例 3

```
******** VACL  ***********
1  deny ip 0.0.0.0 255.255.255.0 any
2  deny ip 0.0.0.255 255.255.255.0 any
3  deny ip any 0.0.0.0 255.255.255.0
4  permit ip any host 239.255.255.255
5  permit ip any host 255.255.255.255
6  deny ip any 0.0.0.255 255.255.255.0
7  permit tcp any range 0 65534 any range 0 65534
8  permit udp any range 0 65534 any range 0 65534
9  permit icmp any any
10 permit ip any any
******** Cisco IOS ACL **********
1  deny ip any host 239.255.255.255
2  permit ip any any
******** MERGE **********
Using the new algorithm - 12 entries
Using the old algorithm - 303 entries
```

例 4

```
******** VACL  ***********
1 redirect 4/25 tcp host 192.168.1.67 host 255.255.255.255
2 redirect 4/25 udp host 192.168.1.67 host 255.255.255.255
3 deny tcp any any lt 30
4 deny udp any any lt 30
5 permit ip any any
*******  Cisco IOS ACL ***********
1  deny ip any host 239.255.255.255
2  permit ip any any
*******  MERGE **********

Using the new algorithm - 6 entries
Using the old algorithm - 142 entries
```

例 5

```
******** VACL  ***********
1 redirect 4/25 tcp host 192.168.1.67 host 255.255.255.255
2 redirect 4/25 udp host 192.168.1.67 host 255.255.255.255
3 permit ip any any
*******  Cisco IOS ACL ***********
1  deny ip any host 239.255.255.255
2  permit ip any any
*******  MERGE **********

Using the new algorithm - 4 entries
Using the old algorithm - 4 entries
```

レイヤ 4 演算設定時の注意事項

ここでは、レイヤ 4 ポート演算使用時の注意事項について説明します。

- レイヤ 4 演算の使用方法（p.15-25）
- LOU の使用（p.15-26）

レイヤ 4 演算の使用方法

スイッチ ハードウェアには、次のタイプの演算子を指定することができます。

- gt（geater than：より大きい）
- lt（less than：より小さい）
- neq（not equal：等しくない）
- eq（equal：等しい）
- range（inclusive range：包含範囲）

1 つの ACL に指定する演算は、9 つまでにしてください。この数を超えると、新しい演算によって影響される ACE が、複数の ACE に分割されることがあります。

（注） 同じ VLAN インターフェイス上に Cisco IOS ACL および VACL の両方を設定する場合も、レイヤ 4 演算の数は合計で 9 以下にすることを推奨します。

レイヤ 4 演算を定義するときは、次の 2 つの注意事項に従ってください。

1. レイヤ 4 演算は、演算子またはオペランドが異なっていると、異なる演算であるとみなされます。次の ACL には 4 つの異なるレイヤ 4 演算が定義されています（[gt 10] と [gt 11] は 2 つの異なるレイヤ 4 演算です）。

```
... gt 10 permit
... lt 9 deny
... gt 11 deny
... neq 6 redirect
```

（注） [eq] 演算子の使用に制限はありません。[eq] 演算子は Logical Operator Unit（LOU）またはレイヤ 4 演算ビットを使用しないためです。LOU については、「LOU の使用」（p.15-26）を参照してください。

2. レイヤ 4 演算は、同じ演算子とオペランドの組み合わせでも、送信元ポートに適用するか宛先ポートに適用するかによって異なる演算になります。次の ACL では、1 つの ACE には送信元ポート、もう 1 つの ACE には宛先ポートが指定されているので、2 つの異なるレイヤ 4 演算が定義されていることになります。

```
... Src gt 10 ...
... Dst gt 10
```

(注)　ACL のレイヤ 4 ポート演算リソースの使用状況を調べるには、**show security acl resource-usage** コマンドを使用します。

LOU の使用

LOU は、演算子とオペランドの組み合わせを保存するレジスタです。すべての ACL は LOU を使用します。最大 32 の LOU があります。各 LOU には、2 つの異なる演算子 / オペランドの組み合わせを保存できますが、range 演算子だけは例外です。レイヤ 4 演算は、次のように LOU を使用します。

- gt は、1/2 LOU を使用します。
- lt は、1/2 LOU を使用します。
- neq は、1/2 LOU を使用します。
- range は、1 LOU を使用します。
- eq は、LOU を使用しません。

たとえば、次の ACL では、1 つの LOU に 2 つの異なる演算子とオペランドが保存されます。

```
... Src gt 10 ...
... Dst gt 10
```

以下は、より詳細な例です。

```
ACL1
... (dst port) gt 10 permit
... (dst port) lt 9 deny
... (dst port) gt 11 deny
... (dst port) neq 6 redirect
... (src port) neq 6 redirect
... (dst port) gt 10 deny

ACL2
... (dst port) gt 20 deny
... (src port) lt 9 deny
... (src port) range 11 13 permit
... (dst port) neq 6 redirect
```

レイヤ 4 演算数と LOU の使用数は、次のとおりです。

- ACL1 のレイヤ 4 演算：5
- ACL2 のレイヤ 4 演算：4
- LOU：4

LOU は、次のように使用されています。

- LOU 1 に、[gt 10] および [lt 9] が保存されます。
- LOU 2 に、[gt 11] および [neq 6] が保存されます。
- LOU 3 に、[gt 20] が保存されます（半分は空き）。
- LOU 4 に、[range 11 13] が保存されます（range は 1 LOU を使用）。

ネットワークでの VACL の使用

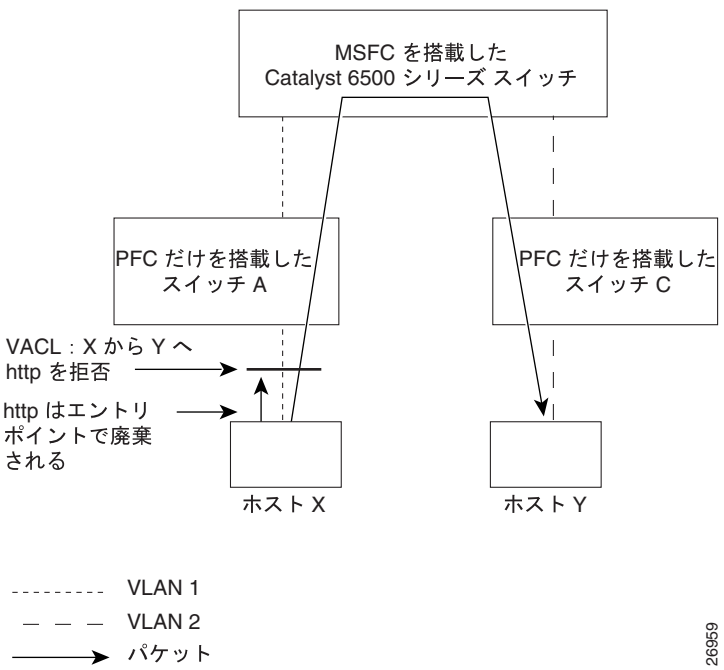
ここでは、VACL の一般的な使用例について説明します。

配線クローゼットの設定

配線クローゼットの設定では、Catalyst 6500 シリーズ スイッチに MSFC（ルータ）が搭載されていないことがあります。この設定では、スイッチにより VACL および QoS ACL がサポートされます。ホスト X およびホスト Y は異なる VLAN 上にあり、配線クローゼットのスイッチ A およびスイッチ C に接続しているとします（図 15-4 を参照）。ホスト X からホスト Y へのトラフィックは、最終的に、MSFC 搭載スイッチによってルーティングされます。ホスト X からホスト Y へのトラフィックは、トラフィックの入口であるスイッチ A でアクセス制御することができます。

ホスト X からホスト Y への HTTP トラフィックをスイッチングしない場合は、スイッチ A に VACL を設定します。この場合、ホスト X からホスト Y への HTTP トラフィックはすべてスイッチ A で廃棄され、MSFC 搭載スイッチにはブリッジングされません。

図 15-4　配線クローゼットの設定



特定のサーバ ポートへのブロードキャスト トラフィックのリダイレクト

一部のアプリケーション トラフィックは、VLAN 内のすべてのホストに到達するブロードキャスト パケットを使用します。VACL により、これらのブロードキャスト パケットを特定のアプリケーション サーバのポートにリダイレクトできます。

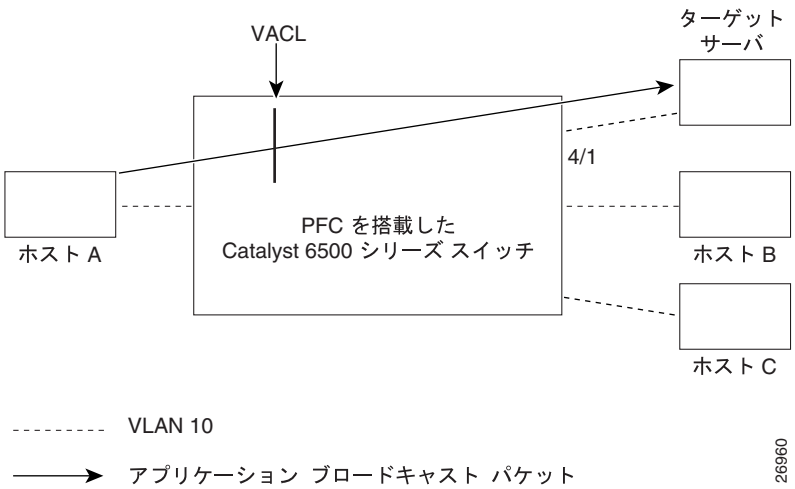
図 15-5 では、ホスト A からアプリケーション ブロードキャスト パケットがターゲットのアプリケーション サーバ ポートにリダイレクトされ、他のポートにパケットは送信されません。

ブロードキャスト トラフィックを特定のサーバ ポートにリダイレクトするには、イネーブル モードで次の作業を行います（対象となるサーバ アプリケーション ポートは、TCP ポート 5000 です）。

	作業	コマンド
ステップ 1	ブロードキャスト パケットをリダイレクトします。	**set security acl ip SERVER redirect 4/1 tcp any host 255.255.255.255 eq 5000**
ステップ 2	他のすべてのトラフィックを許可します。	**set security acl ip SERVER permit ip any any**
ステップ 3	VACL をコミットします。	**commit security acl SERVER**
ステップ 4	VACL を VLAN 10 にマッピングします。	**set security acl map SERVER 10**

（注） トラフィックをポート グループにリダイレクトすることによって、ブロードキャスト トラフィックをマルチキャストの宛先に送信することができます（図 15-5 を参照）。

図 15-5　特定のサーバ ポートへのブロードキャスト トラフィックのリダイレクト



特定のサーバに対する DHCP 応答の制限

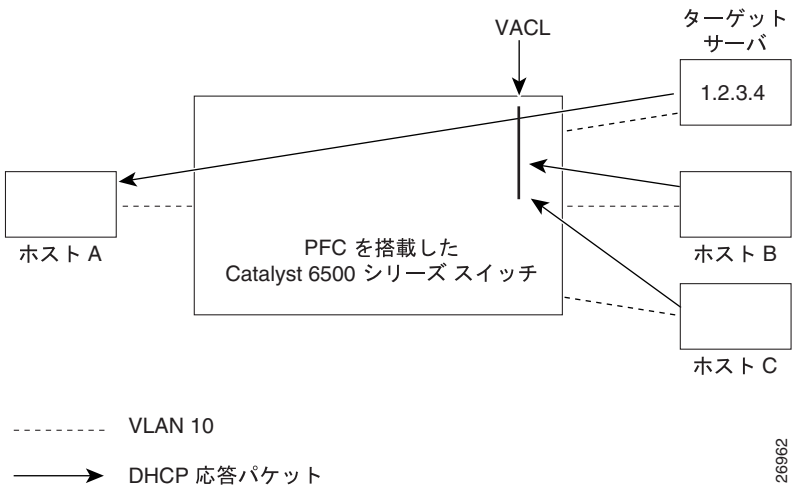
Dynamic Host Configuration Protocol（DHCP）要求がブロードキャストされると、VLAN 内のすべての DHCP サーバに送信されるので、複数の応答が戻されます。VACL によって、*特定の* DHCP サーバからの応答だけを受けるようにし、他の応答を廃棄することができます。

DHCP 応答を特定のサーバに制限するには、イネーブル モードで次の作業を行います（ターゲットの DHCP サーバの IP アドレスは、1.2.3.4 です）。

	作業	コマンド
ステップ 1	ホスト 1.2.3.4 からの DHCP 応答を許可します。	**set security acl ip SERVER permit udp host 1.2.3.4 any eq 68**
ステップ 2	他のホストからの DHCP 応答を拒否します。	**set security acl ip SERVER deny udp any any eq 68**
ステップ 3	他の IP トラフィックを許可します。	**set security acl ip SERVER permit any**
ステップ 4	VACL をコミットします。	**commit security acl SERVER**
ステップ 5	VACL を VLAN 10 にマッピングします。	**set security acl map SERVER 10**

図 15-6 では、DHCP 要求に対して、ターゲット サーバの DHCP 応答だけが戻されています。

図 15-6　特定のサーバの DHCP 応答のリダイレクト



他の VLAN 上のサーバからのアクセス拒否

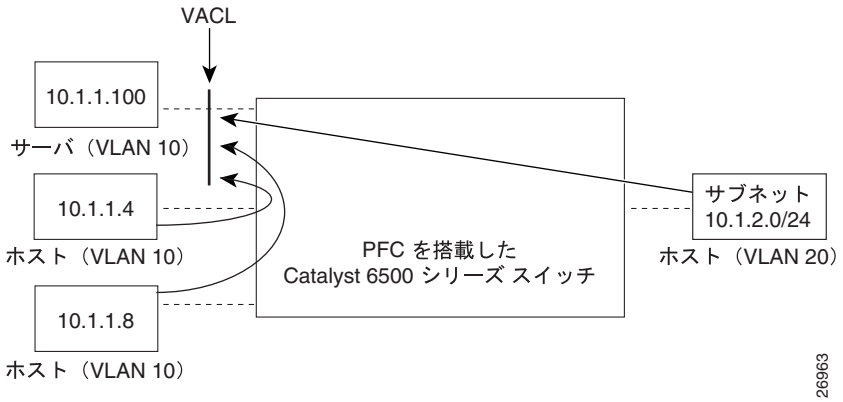
他の VLAN 上のサーバからのアクセスを制限することができます。たとえば、VLAN 10 のサーバ 10.1.1.100 で、次のようなアクセス制限をする必要があるとします（図 15-7 を参照）。

- VLAN 20 のサブネット 10.1.2.0/24 のホストからのアクセスを拒否する
- VLAN 10 のホスト 10.1.1.4 および 10.1.1.8 からのアクセスを拒否する

他の VLAN 上のサーバからのアクセスを拒否するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	サブネット 10.1.2.0/24 のホストからのトラフィックを拒否します。	**set security acl ip SERVER deny ip 10.1.2.0 0.0.0.255 host 10.1.1.100**
ステップ 2	ホスト 10.1.1.4 からのトラフィックを拒否します。	**set security acl ip SERVER deny ip host 10.1.1.4 host 10.1.1.100**
ステップ 3	ホスト 10.1.1.8 からのトラフィックを拒否します。	**set security acl ip SERVER deny ip host 10.1.1.8 host 10.1.1.100**
ステップ 4	他の IP トラフィックを許可します。	**set security acl ip SERVER permit ip any any**
ステップ 5	VACL をコミットします。	**commit security acl SERVER**
ステップ 6	VACL を VLAN 10 にマッピングします。	**set security acl map SERVER 10**

図 15-7　他の VLAN 上のサーバからのアクセス拒否



ARP トラフィックの制限

(注)　この機能を使用できるのは、PFC2 搭載の Supervisor Engine 2、PFC3A/PFC3B/PFC3BXL 搭載の Supervisor Engine 720、および PFC3B/PFC3BXL 搭載の Supervisor Engine 32 だけです。

ARP トラフィックは、デフォルトでは各 VLAN 上で許可されます。**set security acl ip** *acl_name* **deny arp** コマンドを使用して、VLAN 単位で ARP トラフィックを拒否することができます。このコマンドを入力すると、ACL をマッピングした VLAN 上で ARP トラフィックが拒否されます。ARP トラフィックを拒否した VLAN 上で、ARP トラフィックを再び許可するには、**set security acl ip** *acl_name* **permit arp** コマンドを入力します。

ARP トラフィックの検査

(注)　この機能を使用できるのは、PFC2 搭載の Supervisor Engine 2、PFC3A/PFC3B/PFC3BXL 搭載の Supervisor Engine 720、および PFC3B/PFC3BXL 搭載の Supervisor Engine 32 だけです。

ここでは、ARP トラフィック検査機能について説明します。

- 概要（p.15-30）
- 実装（p.15-31）
- ARP トラフィック検査設定時の注意事項（p.15-31）
- ARP トラフィック検査の設定手順（p.15-33）

概要

ARP は認証メカニズムを備えていない簡易プロトコルなので、ARP 要求および応答が正しいかどうかを確認する方法がありません。認証メカニズムがなければ、悪意のあるユーザ / ホストによってレイヤ 2 ネットワークまたはブリッジ ドメインにある同じ VLAN 上の他のホストの ARP テーブルが破壊される可能性があります。

たとえば、ユーザ / ホスト A（悪意のあるユーザ）が、デフォルト ルータの IP アドレスとホスト A の MAC アドレスで、非送信請求 ARP 応答（不必要な ARP パケット）をサブネット上の他のホストに送信することがあります。従来の OS（オペレーティング システム）では、デフォルト ルータのスタティック ARP エントリがホストにすでにある場合でも、ホスト A からの新たにアドバタイズされたバインディングが学習されます。ホスト A が IP 転送をイネーブルにし、「スプーフィングされた」ホストとルータ間ですべてのパケットをやり取りする場合、（たとえば dsniff プログラムを使用した）man-in-the-middle 攻撃を実行できます。このスプーフィングされたホストでは、そのトラフィックのすべてにスニファが行われていることを認識しません。

ARP トラフィック検査によって、セキュリティ ACL（VACL）フレームワーク内に順序依存型の一連のルールを設定して ARP テーブルへの攻撃を防止できます。

実装

VLAN 上の VACL に ARP トラフィック検査の具体的なルールが存在する場合は、すべての ARP パケットは VACL の ACE を介してインデックスによる指定で CPU に送られます。パケットは、ARP トラフィック検査タスクによって指定されたルールへの適合が検査されます。適合パケットは転送されますが、非適合パケットは廃棄されてログが取られます（ロギングがイネーブルの場合）。

ARP トラフィック検査のルールは、次の例に示すように指定された IP アドレスに対して ARP バインディングを指定します。

```
permit arp-inspection host 10.0.0.1 00-00-00-01-00-02
permit arp-inspection host 20.0.0.1 00-00-00-02-00-03
deny arp-inspection host 10.0.0.1 any
deny arp-inspection host 20.0.0.1 any
permit arp-inspection any any
```

上記の一連のルールによって、00-00-00-01-00-02 だけが IP アドレス 10.0.0.1 の MAC アドレスとしてアドバタイズされます。同様に、MAC アドレス 00-00-00-02-00-03 は IP アドレス 20.0.0.1 にバインドされます。10.0.0.1 および 20.0.0.1 のその他の MAC アドレスをアドバタイズする ARP パケットは廃棄されます（3 行めおよび 4 行めの **deny** 動作によって達成）。残りの ARP パケットは通過が許可されます（5 行めの **permit** 動作によって達成）。

ARP トラフィック検査設定時の注意事項

ここでは、ARP トラフィック検査設定時の注意事項について説明します。

- ARP トラフィック検査句を VACL の先頭に表示します。
- VACL に設定できる ARP トラフィック検査句の数の上限は 32 です。
- ARP トラフィック検査句を含んだ ACL の最大文字数は 29 文字です。
- ARP トラフィック検査 ACE は、IP ACE になるように変更できません。その逆も同様です。
- ARP トラフィック検査 ACE は、IP ACE の前に挿入できません。その逆も同様です。
- 同じ VACL で汎用 deny/permit ステートメントを ARP トラフィック検査句と一緒に使用しないでください。汎用 deny/permit ステートメントは、**set security acl ip** *acl_name* {**deny** | **permit**} **arp** コマンドを使用してインストールします。
- MSFC がホストのゲートウェイである場合は、MSFC IP/MAC のバインディングを使用可能にする必要があります。ARP トラフィック検査を実行する場合は、ゲートウェイ IP/MAC バインディングを使用可能にすることを推奨します。
- ARP トラフィック検査は、VACL の既存のロギング機能を使用します。パケットが ARP トラフィック検査ルールを経たあと、結果が [permit] の場合、パケットは宛先 MAC アドレス（またはブロードキャスト アドレス）に転送されます。結果が [deny] の場合は、パケットは廃棄され、VACL ロギング プロセスに送信されます（ロギングがイネーブルの場合）。

VACL ロギングは送信元 MAC アドレスおよび ARP ヘッダーのフィールドを使用して、ロギング フローを定義します。使用するフィールドは、送信元 IP アドレス、送信元 MAC アドレス、および ARP 演算コード（要求、応答）です。

set security acl log maxflow *max_flows* コマンドを入力すると、ログ済みフローの数を制限できます。ただし、**set security acl log ratelimit** *max_rate* コマンドは ARP トラフィック検査ログ済みフローに適用されません。

- RARP パケットはホスト上の ARP エントリの学習に使用されず、ARP を破壊するような害を及ぼすことはありません。PFC2 および PFC3A/PFC3B/PFC3BXL では、ARP および RARP パケットの区別が行われません。CPU への ARP パケットのリダイレクトに使用される ACE も、RARP パケットをリダイレクトします。グローバル レート制限とは、結合 ARP および RARP パケットに対するレート制限のことです。ARP トラフィック検査ルールは RARP パケットには適用されないので、RARP パケットはそのまま転送されます。汎用 ARP deny ステートメントも RARP パケットを拒否します。転送される RARP パケットの数は、**show security acl arp-inspection statistics** コマンドを実行すると表示できます。
- ARP トラフィック検査句を伴う VACL を管理 VLAN（sc0/sc1 インターフェイス）にマッピングすることは、サポートされていません。
- ポートが EtherChannel に組み込まれていたとしても、廃棄およびシャットダウン スレッシュホールドはポートベースのままです。スレッシュホールドは、EtherChannel の形成に必要な*一致*の構成要素ではありません（PAgP は*一致した* EtherChannel リンクを特定すると、そのポートを EtherChannel にまとめます）。
- ハードウェアによる ARP パケットの認識方法が原因で、送信元アドレスが 0.0.0.0、宛先アドレスが 0.0.0.0 の IP パケット、および IP プロトコル ICMP も ARP トラフィック検査タスクにリダイレクトされます。これらのパケットは無効なパケットなので廃棄されます。このようなパケットのカウントは、**show security acl arp-inspection statistics** コマンドの一部として表示されます。
- ARP トラフィック検査タスクによって廃棄されたすべてのパケットについて Syslog メッセージが生成されると、コンソールはメッセージでいっぱいになります。このような状況を避けるため、1 分当たりの許容 Syslog メッセージを 40 に制限します。
- 次に、一般的な設定エラーを回避する例を示します。以下は一般的な ARP トラフィック検査 ACL です。

```
------------------------------
set security acl ip my_arp
------------------------------------------------
arp permit
1. permit arp-inspection host 10.6.62.86 00-b0-c2-3b-db-fd
2. deny arp-inspection host 10.6.62.86 any
3. permit arp-inspection any any
---------------------------
```

この ACL によって、MAC アドレス 00-b0-c2-3b-db-fd だけが IP アドレス 10.6.62.86 の MAC アドレスとしてアドバタイズされます。この ACL は、IP ACL に暗黙の ip deny any any があるので、すべての IP パケットを拒否します。

すべての IP トラフィックを通過させるには、次のように ACL の末尾に明示的な permit ip any any がなければなりません。

```
--------------------
set security acl ip my_arp
------------------------------------------------
arp permit
1. permit arp-inspection host 10.6.62.86 00-b0-c2-3b-db-fd
2. deny arp-inspection host 10.6.62.86 any
3. permit arp-inspection any any
4. permit ip any any
----------------------
```

- 次に、ARP トラフィック検査を使用した一般的な設定例を示します。次の ACL を使用して指定された 2 つの IP アドレスを保護し、指定されたもの以外の MAC アドレスでの ARP トラフィック検査を実行しません。

```
set security acl ip ACL_VLAN951 permit arp-inspection host 132.216.251.129
00-d0-b7-11-13-14
set security acl ip ACL_VLAN951 deny arp-inspection host 132.216.251.129 any log
set security acl ip ACL_VLAN951 permit arp-inspection host 132.216.251.250
00-d0-00-ea-43-fc
set security acl ip ACL_VLAN951 deny arp-inspection host 132.216.251.250 any log
set security acl ip ACL_VLAN951 permit arp-inspection any any
set security acl ip ACL_VLAN951 permit ip any any
```

ARP トラフィック検査の設定手順

ここでは、ARP トラフィック検査の設定手順について説明します。

ARP トラフィック検査の設定

- 特定の IP アドレスと MAC アドレスのバインディングをアドバタイズする ARP パケットの許可または拒否（p.15-33）
- 特定の IP アドレスのバインディングをアドバタイズする ARP の許可または拒否（p.15-34）
- すべての ARP パケットの許可または拒否（p.15-34）
- 特定ネットワーク上の IP アドレスのバインディングをアドバタイズする ARP パケットの許可または拒否（p.15-35）
- MAC アドレスが一致しないパケットの廃棄（p.15-35）
- MAC または IP アドレスが無効なパケットの廃棄（p.15-36）
- ARP トラフィック検査統計情報の表示（p.15-36）
- ARP トラフィック検査統計情報の消去（p.15-37）

ARP トラフィック検査のレート制限の設定

- グローバル ベースのレート制限の設定（p.15-37）
- ポート単位ベースのレート制限の設定（p.15-38）
- ARP トラフィック検査のための errdisable-timeout オプションの設定（p.15-39）

ARP トラフィック検査のロギングの設定

- ARP トラフィック検査のロギングの設定（p.15-39）

特定の IP アドレスと MAC アドレスのバインディングをアドバタイズする ARP パケットの許可または拒否

特定の IP アドレスと MAC アドレスのバインディングをアドバタイズする ARP パケットを許可または拒否するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	特定の IP アドレスと MAC アドレスのバインディングをアドバタイズする ARP パケットを許可または拒否します。	**set security acl ip** *acl_name* {**permit** | **deny**} **arp-inspection host** *ip_address mac_address*
ステップ 2	VACL をコミットします。	**commit security acl** {**acl_name** | **all** | **adjacency**}

次に、IP アドレス 172.20.52.54 と MAC アドレス 00-01-64-61-39-c2 のバインディングをアドバタイズする ARP パケットを許可する例を示します。

```
Console> (enable) set security acl ip ACL1 permit arp-inspection host 172.20.52.54
00-01-64-61-39-c2
Operation successful.
Console> (enable) commit security acl ACL1
Console> (enable) ACL commit in progress.

ACL 'ACL1' successfully committed.
```

特定の IP アドレスのバインディングをアドバタイズする ARP の許可または拒否

指定した IP アドレスのバインディングをアドバタイズする ARP パケットを許可または拒否するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	指定した IP アドレスのバインディングをアドバタイズする ARP パケットを許可または拒否します。	**set security acl ip** *acl_name* {**permit** | **deny**} **arp-inspection host** *ip_address* **any**
ステップ 2	VACL をコミットします。	**commit security acl** {**acl_name** | **all** | **adjacency**}

次に、IP アドレス 172.20.52.19 のバインディングをアドバタイズする ARP パケットを許可する例を示します。

```
Console> (enable) set security acl ip ACL2 permit arp-inspection host 172.20.52.19 any
Operation successful.
Console> (enable) commit security acl ACL2
Console> (enable) ACL commit in progress.

ACL 'ACL2' successfully committed.
```

すべての ARP パケットの許可または拒否

すべての ARP パケットを許可または拒否するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	すべての ARP パケットを許可または拒否します。	**set security acl ip** *acl_name* {**permit** | **deny**} **arp-inspection any any**
ステップ 2	VACL をコミットします。	**commit security acl** {**acl_name** | **all** | **adjacency**}

次に、すべての ARP パケットを許可する例を示します。

```
Console> (enable) set security acl ip ACL3 permit arp-inspection any any
Operation successful.
Console> (enable) commit security acl ACL3
Console> (enable) ACL commit in progress.

ACL 'ACL3' successfully committed.
```

特定ネットワーク上の IP アドレスのバインディングをアドバタイズする ARP パケットの許可または拒否

特定ネットワーク上の IP アドレスのバインディングをアドバタイズする ARP パケットを許可または拒否するには、イネーブル モードで次の作業を行います。

（注） *ip_mask* は逆マスクです。[0] ビットは「一致」を意味し、[1] ビットは「無視」を意味します。たとえば、10.3.5.6 と 0.0.0.255 は 10.3.5/24 に相当します。

	作業	コマンド
ステップ 1	特定ネットワーク上の IP アドレスのバインディングをアドバタイズする ARP パケットを許可または拒否します。	**set security acl ip** *acl_name* {**permit** | **deny**} **arp-inspection** *ip_address ip_mask* **any**
ステップ 2	VACL をコミットします。	**commit security acl** {*acl_name* | **all** | **adjacency**}

次に、サブネット 10.3.5.0/24 上の IP アドレスのバインディングをアドバタイズする ARP パケットを許可する例を示します。

```
Console> (enable) set security acl ip ACL4 permit arp-inspection 10.3.5.6 0.0.0.255
any
Operation successful.
Console> (enable) commit security acl ACL4
Console> (enable) ACL commit in progress.

ACL 'ACL4' successfully committed.
```

MAC アドレスが一致しないパケットの廃棄

（イーサネット ヘッダーの）送信元イーサネット MAC アドレスが ARP ヘッダーの送信元 MAC アドレスと異なるパケットを廃棄するには、イネーブル モードで次の作業を行います。**drop** キーワードを指定しないと、パケットは廃棄されませんが、Syslog メッセージが表示されます。VACL ロギング機能にパケットを送信するには、**log** キーワードを使用します。

ヒント 通常、**match-mac** 句を使用して ARP スプーフィングを防止しても、各 VLAN の特定 ARP 検査 ACL を作成する必要はなくなりません。**match-mac** 句は、より洗練された ARP テーブル攻撃を受けません。大部分の ARP スプーファは、イーサネット ヘッダーの送信元 MAC アドレスを変更して ARP ペイロードのアドレスを一致させます。

	作業	コマンド
ステップ 1	MAC アドレスの一致しないパケットを識別または廃棄します。	**set security acl arp-inspection match-mac** {**enable** [**drop** [**log**]] | **disable**}
ステップ 2	VACL をコミットします。	**commit security acl** {*acl_name* | **all** | **adjacency**}
ステップ 3	設定を表示します。	**show security acl arp-inspection config**

次に、送信元イーサネット MAC アドレスが ARP ヘッダーの送信元 MAC アドレスと異なるパケットを廃棄する例を示します。

```
Console> (enable) set security acl arp-inspection match-mac enable drop
ARP Inspection match-mac feature enabled with drop option.
Console> (enable)

Console> (enable) show security acl arp-inspection config
Match-mac feature is enabled with drop option.
Console> (enable)
```

MAC または IP アドレスが無効なパケットの廃棄

次の MAC アドレスは無効です。

- 00-00-00-00-00-00
- マルチキャスト MAC アドレス（48 番めのビットを設定）
- ff-ff-ff-ff-ff-ff（これは特殊なケースのマルチキャスト MAC アドレスです）

次の IP アドレスは無効です。

- 0.0.0.0
- 255.255.255.255
- クラス D（マルチキャスト）IP アドレス

MAC または IP アドレスが無効なパケットを廃棄するには、イネーブル モードで次の作業を行います（**drop** キーワードを指定しないと、パケットは廃棄されませんが、Syslog メッセージが表示されます）。

	作業	コマンド
ステップ 1	MAC または IP アドレスが無効なパケットを廃棄します。	**set security acl arp-inspection address-validation** {**enable** [**drop** [**log**]] | **disable**}
ステップ 2	VACL をコミットします。	**commit security acl** {*acl_name* | **all** | **adjacency**}
ステップ 3	設定を表示します。	**show security acl arp-inspection config**

次に、MAC または IP アドレスが無効なパケットを廃棄する例を示します。

```
Console> (enable) set security acl arp-inspection address-validation enable drop
ARP Inspection address-validation feature enabled with drop option.
Console> (enable)

Console> (enable) show security acl arp-inspection config
Address-validation feature is enabled with drop option.
Console> (enable)
```

ARP トラフィック検査統計情報の表示

ARP トラフィック検査タスクによって許可および拒否されたパケットの数を表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
ARP トラフィック検査タスクによって許可および拒否されたパケットの数を表示します。	**show security acl arp-inspection statistics** [*acl_name*]

(注)　**show security acl** コマンドを入力すると、特定の ARP トラフィック検査設定情報を表示します。

次に、ARP トラフィック検査タスクによって許可および拒否されたパケットの数を表示する例を示します。

```
Console> (enable) show security acl arp-inspection statistics
ARP Inspection statistics
Packets forwarded = 0
Packets dropped = 0
RARP packets (forwarded) = 0
Packets for which Match-mac failed = 0
Packets for which Address Validation failed = 0
IP packets dropped = 0
Console> (enable)
```

ARP トラフィック検査統計情報の消去

ARP トラフィック検査統計情報を消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
ARP トラフィック検査統計情報を消去します。	**clear security acl arp-inspection statistics** [*acl_name*]

オプションの引数なしでコマンドを入力すると、すべての ACL で ARP トラフィック検査グローバル統計情報カウンタおよび ARP トラフィック検査統計情報カウンタが消去されます。オプションの引数 *acl_name* を指定すると、特定 ACL の ARP トラフィック検査統計情報だけが消去されます。

(注)　**clear security acl** コマンドを入力すると、ARP トラフィック検査の設定値が消去されます。

グローバル ベースのレート制限の設定

グローバルにスーパバイザ エンジン CPU に送信される ARP トラフィック検査パケットの数に対してレート制限を実行できます。デフォルトでは、ARP トラフィック検査のトラフィックは 500 パケット / 秒にレート制限されます。最小値は 1 パケット / 秒、最大値は 1000 パケット / 秒です。Supervisor Engine 720 の場合、ハードウェアにより決められる最小値は 10 パケット / 秒です（1 ～ 9 の値は 10 に設定されます）。レート制限をディセーブルにするには、値を 0 に設定します。

(注)　レート制限は、複数の機能で共有されます。レート制限を共有する機能を表示するには、**show security acl feature ratelimit** コマンドを入力します。

グローバル ベースでスーパバイザ エンジン CPU に送信される ARP トラフィック検査パケットの数に対してレート制限を行うには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	グローバル ベースでスーパバイザ エンジン CPU に送信される ARP トラフィック検査パケットの数に対してレート制限を行います。	**set security acl feature ratelimit** *rate*
ステップ 2	グローバル レート制限値を表示します。	**show security acl feature ratelimit**
ステップ 3	スイッチ プロセッサおよび Route Processor（RP; ルート プロセッサ）で設定された、すべてのレート リミッタ設定を表示します。	**show rate-limit**

次に、CPU に送信される ARP トラフィック検査パケットの数を 1000 にレート制限する例を示します。

```
Console> (enable) set security acl feature ratelimit 1000
Dot1x DHCP and ARP Inspection global rate limit set to 1000 pps.
Console> (enable)

Console> (enable) show security acl feature ratelimit
Rate limit value in packets per second = 1000
Protocols set for rate limiting = Dot1x DHCP, ARP Inspection
Console> (enable)

Console> (enable) show rate-limit
Configured Rate Limiter Settings:

Rate Limiter Type    Status  Rate (pps)     Burst
-------------------- ------  -------------- -----
VACL LOG             On      2500           1
ARP INSPECTION       On      1000           1
FIB RECEIVE          Off     *              *
FIB GLEAN            Off     *              *
L3 SEC FEATURES      Off     *              *

Console> (enable)
```

ポート単位ベースのレート制限の設定

ポート単位でスーパバイザ エンジン CPU に送信される ARP トラフィック検査パケットの数に対してレート制限を実行できます。レートが **drop-threshold** を超える場合、超過パケットは廃棄されます（さらに **shutdown-threshold** 制限に対してカウントされます）。レートが **shutdown-threshold** を超える場合は、*mod/port* によって指定されたポートはシャットダウンされます。デフォルトでは、両方のスレッシュホールド値が 0 です（ポート単位のレート制限は適用されません）。両方のスレッシュホールドの最大値は 1000 パケット / 秒（pps）です。

ポート単位でスーパバイザ エンジン CPU に送信される ARP トラフィック検査パケットの数に対してレート制限を行うには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポート単位でスーパバイザ エンジン CPU に送信される ARP トラフィック検査パケットの数に対してレート制限を行います。	**set port arp-inspection** *mod/port* **drop-threshold** *packets_per_second* **shutdown-threshold** *packets_per_second* **set port arp-inspection** *mod/port* **drop-threshold** *packets_per_second* **set port arp-inspection** *mod/port* **shutdown-threshold** *packets_per_second*

	作業	コマンド
ステップ 2	廃棄およびシャットダウン スレッシュホールドを表示します。	**show port arp-inspection** {[*mod/port*]	[*mod*]}

次に、ポート単位でスーパバイザ エンジン CPU に送信される ARP トラフィック検査パケットの数をレート制限する例を示します。ポート 3/1 に対して廃棄スレッシュホールドを 700、シャットダウン スレッシュホールドを 800 に設定します。

```
Console> (enable) set port arp-inspection 3/1 drop-threshold 700 shutdown-threshold
800
Drop Threshold=700, Shutdown Threshold=800 set on port 3/1.
Console> (enable)

Console> (enable) show port arp-inspection 3/1
Port                      Drop Threshold Shutdown Threshold
------------------------  -------------- ------------------
 3/1                               700                800
Console> (enable)
```

ARP トラフィック検査のための errdisable-timeout オプションの設定

set errdisable-timeout {**enable** | **disable**} **arp-inspection** コマンドを使用して、ARP トラフィック検査のために errdisable-timeout オプションを設定できます。errdisable-timeout オプションの詳細については、「ポートの errdisable ステートにおけるタイムアウト設定」（p.4-13）を参照してください。

ARP トラフィック検査のロギングの設定

ロギング オプションを設定して廃棄される ARP トラフィック検査パケットのログを取るには、イネーブル モードで次の作業を行います。

作業	コマンド
廃棄される ARP トラフィック検査パケットのログを取ります。	**set security acl ip** *acl_name* **deny arp-inspection** {**host** *ip_address* {**any**	*mac_address*}	*ip_address ip_mask* **any**	**any any**} [**log**]

VACL ロギング オプションの詳細については、「VACL ロギングの設定」（p.15-60）を参照してください。ここでは、**set security acl log maxflow** *max_number* コマンドによるログ フローの数の制限についても説明します。

ロギングされた ARP トラフィック検査パケットを表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
ロギングされた ARP トラフィック検査パケットを表示します。	**show security acl log flow arp** [**host** *ip_address* [**vlan** *vlan*]]

オプションの **host** *ip address* を指定すると、指定したホストの IP アドレスのバインディングをアドバタイズする ARP パケットだけが表示されます。オプションの **vlan** *vlan* を指定した場合は、検索が指定した VLAN に限定されます。

ダイナミック ARP 検査

(注) Dynamic ARP Inspection（DAI）を使用できるのは、PFC2 搭載の Supervisor Engine 2、PFC3A/PFC3B/PFC3BXL 搭載の Supervisor Engine 720、および PFC3B/PFC3BXL 搭載の Supervisor Engine 32 のみです。

ここでは、DAI について説明します。

概要

DAI では、バインディングのアドバタイズを適用するのに DHCP スヌーピングで作成されたバインディング情報を使用して、[man-in-the-middle] 攻撃を防ぎます。これらの攻撃では、攻撃者が通信データを代行受信し、それを選択的に変更して通信アソシエーション内の 1 つまたは複数のエントリになりすまします。DAI では、ARP パケットの MAC アドレスおよび IP アドレスが、同一 VLAN 内にある既存の DHCP スヌーピング バインディングと一致することを確認することで、セキュリティ用の特別レイヤを ARP 検査に追加します。DHCP バインディングが存在することを確認する追加のチェックを除いて、ARP 検査の基本的な機能とパケット フローは変わりません（論理フローチャートについては図 15-8 を参照してください）。

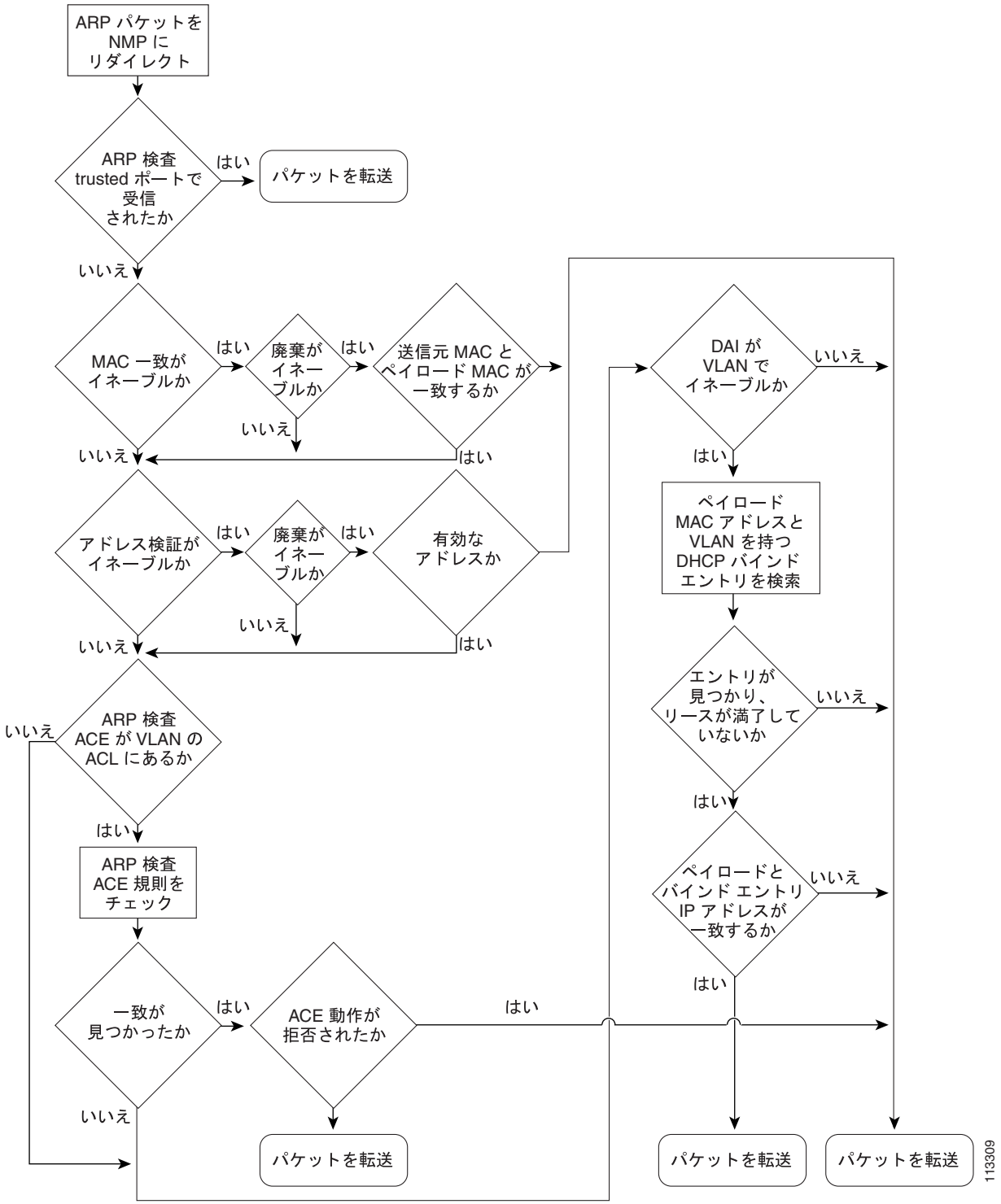
(注) untrusted（信頼性がない）ポートから送信される ARP パケットのみが検査されます。trusted（信頼性のある）ポートから受信した ARP パケットは、検査なしに転送されます（このプロセスは、スタティックおよびダイナミック ARP 検査の両方に適用されます）。デフォルトで、システムは MAFC ポートを ARP 検査 trusted ポートとして設定します。

セキュリティ ACL を作成する場合、静的に設定された ARP 検査規則は DHCP バインディングの DAI チェックよりもプライオリティが高いので、注意が必要です。発生したことに対するチェックができなくなるので、**permit arp-inspection any any** 句をセキュリティ ACL に配置しないでください。

DAI を VLAN 単位でイネーブルまたはディセーブルに設定できます。DAI ポートを untrusted と設定する場合、その DAI ポートを DHCP スヌーピング untrusted ポートとしても設定する必要があります。DAI がイネーブルになっているすべての VLAN で、DHCP スヌーピングをイネーブルにする必要があります。オプションで、DAI で拒否された ARP パケットに対するロギングをイネーブルにできます。

(注) すべての（またはほとんどの）IP アドレスの割り当てが DHCP を使用して実行されている VLAN でイネーブルにした場合に、DAI がもっともよく機能します。

図 15-8　ダイナミック ARP 検査のフロー チャート



注意　管理 VLAN sc0 および sc1 で DAI をイネーブルにできません。

スタティック IP アドレス割り当てが VLAN にある場合、関連ポートを ARP 検査の trusted ポートに設定するか、またはスタティック ARP 検査でこれらの MAC アドレスおよび IP アドレスを許可するように設定する必要があります。

ダイナミック ARP 検査の設定手順

（注） DAI、DHCP スヌーピング、および IP 送信元ガードを使用する場合、ハイ アベイラビリティをイネーブルにすることを推奨します。ハイ アベイラビリティがイネーブルでない場合、スイッチオーバー後にこれらの機能が動作するようにクライアントは IP アドレスを更新する必要があります。DHCP スヌーピングおよび IP 送信元ガードの設定の詳細については、第 32 章「DHCP スヌーピングおよび IP ソース ガードの設定」を参照してください。

DAI を設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	VLAN で DAI をイネーブルにします。	**set security acl arp-inspection dynamic** {**enable** | **disable**} {*vlanlist*}
ステップ 2	ARP パケットの検査をイネーブルまたはディセーブルにします。	**set port arp-inspection** *portlist* **trust** {**enable** | **disable**}
ステップ 3	DAI が拒否したパケットのロギングをイネーブルにします。 **（注）** スタティック ARP 規則拒否のロギングは、引き続き規則（ACE）CPG で制御されます。	**set security acl arp-inspection dynamic log** {**enable** | **disable**}
ステップ 4	DAI および DAI ロギング設定を確認します。	**show security acl arp-inspection config**

次に、VLAN 100 で DAI をイネーブルにする例を示します。

```
Console> (enable) set security acl arp-inspection dynamic enable 100
Dynamic ARP Inspection is enabled for vlan(s) 100.
Console> (enable) set port arp-inspection 2/2 trust enable
Port(s)  2/2 state set to trusted for ARP Inspection.
Console> (enable) set security acl arp-inspection dynamic log enable
Dynamic ARP Inspection logging enabled.
Console> show security acl arp-inspection config
Match-mac feature is disabled.
Address-validation feature is disabled.
Dynamic ARP Inspection is disabled on vlan(s) 1,1006-1013.
Dynamic ARP Inspection is enabled on vlan(s) 100.
Logging for Dynamic ARP Inspection rules is enabled.
Console>
```

プライベート VLAN 上での ACL の設定

プライベート VLAN により、プライマリ VLAN をサブ VLAN（セカンダリ VLAN）に分割し、コミュニティ VLAN または独立 VLAN として設定できます。Release 6.1(1) より前のソフトウェア リリースでは、ACL を設定できるのはプライマリ VLAN 上だけなので、ACL はすべてのセカンダリ VLAN に適用されます。Release 6.1(1) 以降のソフトウェア リリースでは、ACL の適用は次のようになります。

- VACL を、セカンダリ VLAN またはプライマリ VLAN にマッピングできます。
- プライマリ VLAN にマッピングした Cisco IOS ACL が、関連付けられたセカンダリ VLAN にマッピングされます。
- Cisco IOS ACL を、セカンダリ VLAN にマッピングすることはできません。

- ダイナミック ACE を、プライベート VLAN にマッピングすることはできません。
- QoS ACL を、セカンダリ VLAN またはプライマリ VLAN にマッピングできます。

VACL をプライマリ VLAN にマッピングした場合、ルータからホストへのトラフィックがフィルタリングされます。また、セカンダリ VLAN にマッピングした場合は、ホストからルータへのトラフィックがフィルタリングされます。

（注） Release 6.2(1) 以降のソフトウェア リリースでは、MSFC 混合ポートを通ってトラフィックがプライベート VLAN の境界を越えるとき、双方向コミュニティ VLAN を使用してプライマリ VLAN からセカンダリ VLAN への逆マッピングを実行できます。発信と着信の両方のトラフィックは、VLAN ベースの VACL をコミュニティ（または顧客）単位で両方向に適用できる同一の VLAN で伝送できます。

（注） プライベート VLAN の詳細については、「スイッチ上でのプライベート VLAN の設定」（p.11-22）を参照してください。

トラフィック フローのキャプチャ

設定の詳細については、「特定ポート上でのトラフィック フローのキャプチャ」（p.15-58）を参照してください。

サポートされない機能

（注）

Supervisor Engine 720（PFC3A/PFC3B/PFC3BXL）および Supervisor Engine 32（PFC3B/PFC3BXL）では、IPX ルーティングはソフトウェアにより行われ、IPX Cisco IOS ACL および IPX VACL はサポートされません。MAC VACL を使用して IPX パケットを一致させることができます。IPX ARPA フレームを一致させるため、**ipx-arpa** キーワードを入力できます。IPX 非 ARPA フレームおよび Ethertype 0xffff のフレームで一致させるには、0xffff Ethertype を使用します。MAC VACL の設定については、「non-IP version 4/non-IPX VACL（MAC VACL）の作成および ACE の追加」（p.15-53）を参照してください。

ここでは、Catalyst 6500 シリーズ スイッチがサポートしていない、またはサポートが制限されている ACL 関連機能について説明します。

- non-IP version 4/non-IPX Cisco IOS ACL ― 次のタイプの Cisco IOS セキュリティ ACL は、スイッチのハードウェアで実行することはできません。そのため、MSFC が ACL をソフトウェアで処理することになり、システムのパフォーマンスを*著しく*低下させます。
  - ― ブリッジ グループ ACL
  - ― IP アカウンティング
  - ― 着信 / 発信のレート制限
  - ― 送信元ノード番号を指定した標準 IPX
  - ― 送信元ノード番号またはソケット番号を指定した IPX 拡張アクセス リストは、ハードウェアでは実行できません。
  - ― 標準 XNS アクセス リスト
  - ― 拡張 XNS アクセス リスト
  - ― DECnet アクセス リスト
  - ― 拡張 MAC アドレス アクセス リスト
  - ― プロトコル タイプコード アクセス リスト
- ヘッダー長が 5 未満の IP パケットは、アクセス制御されません。
- full flow IPX VACL の非サポート ― IPX VACL は、送信元 / 宛先ネットワーク番号、パケット タイプ、宛先ノード番号だけを指定したフローを対象にしています。IPX フローの指定では、送信元ノード番号およびソケット番号はサポートされません。

VACL の設定

ここでは、VACL の設定方法について説明します。設定の作業を行う前に、「VACL 設定時の注意事項」（p.15-45）を参照してください。

ここでは、VACL 設定時の注意事項と要約について説明します。

VACL 設定時の注意事項

ここでは、VACL 設定時の注意事項について説明します。

注意　ACL の変更はすべて、編集バッファに一時的に保存されます。すべての ACE を NVRAM（不揮発性 RAM）にコミットするには、**commit** コマンドを入力する必要があります。ACE を指定せずにコミットした ACL は、削除されます。ACE をまとめて入力し、**commit** コマンドを使用してすべての変更を NVRAM に保存することを推奨します。

（注）　Cisco IOS ACL と VACL は、NVRAM ではなくフラッシュ メモリから設定できます。詳細については、「VACL および QoS ACL の設定およびフラッシュ メモリへの保存」（p.15-67）を参照してください。

（注）　Supervisor Engine 720（PFC3A/PFC3B/PFC3BXL）および Supervisor Engine 32（PFC3B/PFC3BXL）では、IPX ルーティングはソフトウェアにより行われ、IPX Cisco IOS ACL および IPX VACL はサポートされません。MAC VACL を使用して IPX パケットを一致させることができます。IPX ARPA フレームを一致させるため、**ipx-arpa** キーワードを入力できます。IPX 非 ARPA フレームおよび Ethertype 0xffff のフレームで一致させるには、0xffff Ethertype を使用します。MAC VACL の設定については、「non-IP version 4/non-IPX VACL（MAC VACL）の作成および ACE の追加」（p.15-53）を参照してください。

- 「同一 VLAN インターフェイス上に Cisco IOS ACL および VACL を設定する場合の注意事項」（p.15-18）を参照してください。
- 設定例については、「ネットワークでの VACL の使用」（p.15-27）を参照してください。
- 「サポートされない機能」（p.15-44）を参照してください。
- 「ACL マージ アルゴリズムの指定」（p.15-47）を参照してください。
- VLAN　にマッピングするには、まず　VACL　をコミットする必要があります。デフォルトの VACL はありません。また、VACL/VLAN のデフォルト マッピングもありません。
- ルーテッド VLAN インターフェイス（入力または出力）上のトラフィックを拒否する Cisco IOS ACL が設定されておらず、かつ VACL が設定されていない場合、すべてのトラフィックが許可されます。
- ACL では、ACE の入力順序が重要になります。スイッチに入ってくるパケットは、まず ACL の最初の ACE と照合されます。一致しない場合、パケットはリストの次の ACE と照合されます。どの ACE とも一致しない場合、パケットは拒否（廃棄）されます。

- 編集バッファの内容を変更する前に、必ず **show security acl info** *acl_name* **editbuffer** コマンドを使用して、*現在の* ACE リストを確認してください。
- 冗長 MSFC を搭載したシステムでは、両方の MSFC 上で、Cisco IOS ACL および VACL の同じ ACL 設定を適用する必要があります。
- ACL をコミットしないで削除した場合、システムの ACL の最大数が誤って算出されることがあります。
- **show security acl resource-usage** および **show qos acl resource-usage** コマンドの出力では、ハードウェアに ACL を保存できるスペースがなくなっても、使用率が 100 % にならないことがあります。ACL 管理者が必要に応じてクリーンアップおよびマッピングを実行できるように、予備の ACL スペースが確保されているためです。
- 非常に多数の ACL を設定すると、システムの起動時間が通常より長くなることがあります。
- リダイレクト オプションを使用する場合、次の注意事項に留意してください。
  - リダイレクト パケットを送出できるのは、そのトラフィックが属している VLAN をサポートしているポートだけです。
  - リダイレクト オプションの動作は、パケットを受信してリダイレクト ポートに送信するだけで、ルーティングは実行しません。
  - パケットが多数の VLAN から送信される場合、リダイレクト ポートはこれらの VLAN をフォワーディング ステートにする必要があります。ポートで複数の VLAN をサポートするには、リダイレクト ポートをトランクとして設定しなければならないことがあります。
  - ルーティングされていないトラフィックを受信できるように、キャッシュは混合（promiscuous）モードに設定します。
  - 複数のポートにトラフィックを転送して基本的な VLAN ベースのロードバランシングを実行するには、リダイレクト オプションを使用します。各ポートは、そのポートでフォワーディング ステートになっている VLAN のパケットだけを転送します。

VACL 設定の要約

VACL を作成して、VLAN にマッピングする手順は、次のとおりです。

ステップ 1　**set security acl ip** コマンドを入力して VACL を作成し、ACE を追加します。

ステップ 2　**commit** コマンドを入力して、VACL および関連付けられた ACE を NVRAM にコミットします。

ステップ 3　**set security acl map** コマンドを入力して、VACL を VLAN にマッピングします。

（注） この説明では IP VACL を使用していますが、同じ手順で IPX および non-IP version 4/non-IPX VACL を設定することもできます。

（注） VACL はリストの末尾に暗黙の拒否ステートメントが付加されるので、どの VACL ACE にも一致しないパケットは拒否されます。

CLI からの VACL の設定

ここでは、Catalyst 6500 シリーズ スイッチ上で VACL を作成し、アクティブにする手順について説明します。これらの作業は、実行する順序に従って記載されています。

ここで説明する作業は、次のとおりです。

ACL マージ アルゴリズムの指定

ACL マージ アルゴリズムには、BDD と ODM の 2 種類があります。ODM は、Release 7.1(1) で採用された拡張アルゴリズムです。BDD アルゴリズムは、Release 7.1(1) より前のソフトウェア リリースで使用されていました。ODM を使用した場合、マージ後の ACE は順序に依存します。BDD を使用した場合、マージ後の ACE は順序には関係ありません。

（注） Release 8.1(1) 以降のソフトウェア リリースでは、BDD アルゴリズムはどのプラットフォーム（PFC、PFC2、または PFC3A/PFC3B/PFC3BXL）上でもサポートされなくなりました。デフォルトの ACL マージ アルゴリズムは ODM です。Release 8.1(1) 以降のソフトウェア リリースでは、コマンドが次のように変更されています。**set aclmerge algo** および **set aclmerge bdd** コマンドは削除されました。**show aclmerge** {**bdd** | **algo**} コマンドは **show aclmerge algo** になりました。

（注） ODM アルゴリズムの例については、「Release 7.1(1) 以降のスーパバイザ エンジン ソフトウェア リリースの場合のマージ結果の推定」（p.15-23）を参照してください。

デフォルトのアルゴリズムは ODM です。BDD をディセーブルにした場合、マージ アルゴリズムは ODM だけになります。BDD がイネーブルの場合、BDD アルゴリズムまたは ODM アルゴリズムのどちらか一方を選択できます。ACL マージ アルゴリズムを変更するには、BDD がイネーブルでなければなりません。BDD をイネーブルまたはディセーブルするには、**set aclmerge bdd** コマンドを使用します。BDD をイネーブルまたはディセーブルにした場合、その変更が有効になるのは、システムの再起動後です。

注意　64 MB DRAM が搭載されたスーパバイザ エンジン上で BDD をイネーブルにすると、メモリが不足する可能性があります。これを防ぐためには、メモリを 128 MB にアップグレードするか、BDD をディセーブルにする必要があります。

選択した ACL マージ アルゴリズムは、すべての新規 ACL マージで有効です。設定済みの ACL が変更されることはなく、ACL のマージ時に有効だった ACL マージ アルゴリズムが使用されます。

BDD をイネーブルまたはディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	BDD をイネーブルまたはディセーブルにします。	**set aclmerge bdd** {**enable** | **disable**}
ステップ 2	現在の BDD ステータス、および次回のシステム再起動時に BDD がイネーブルになるのかディセーブルになるのかを表示します。	**show aclmerge** {**bdd** | **algo**}

次に、BDD をディセーブルにする例を示します。

```
Console> (enable) set aclmerge bdd disable
Bdd will be disabled on system restart.
Console> (enable)
```

次に、現在の BDD ステータス、および次回のシステム再起動時に BDD がイネーブルまたはディセーブルのいずれになるのかを表示する例を示します。

```
Console> (enable) show aclmerge bdd
Bdd is not enabled.
On system restart bdd will be disabled.
Console> (enable)
```

ACL マージ アルゴリズムを指定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ACL マージ アルゴリズムを指定します。	**set aclmerge algo** {**bdd** | **odm**}
ステップ 2	現在使用中の ACL マージ アルゴリズムを表示します。	**show aclmerge** {**bdd** | **algo**}

次に、ODM アルゴリズムを指定する例を示します。

```
Console> (enable) set aclmerge algo odm
Acl merge algorithm set to odm.
Console> (enable)
```

次に、現在使用中の ACL マージ アルゴリズムを表示する例を示します。

```
Console> (enable) show aclmerge algo
Current acl merge algorithm is odm.
Console> (enable)
```

IP VACL の作成および ACE の追加

新しい IP VACL を作成して ACE を追加したり、既存の IP VACL に ACE を追加するには、イネーブル モードで次の作業を行います。

作業	コマンド
IP プロトコルを指定する必要がない場合は、この構文を使用します。	**set security acl ip** {*acl_name*} {**permit** | **deny**} {*src_ip_spec*} [**capture**][**before** *editbuffer_index* | **modify** *editbuffer_index*] [**log**[1]]
IP プロトコルを指定する場合は、この構文を使用します。	**set security acl ip** {*acl_name*} {**permit** | **deny** | **redirect** *mod_num/port_num*} {*protocol*} {*src_ip_spec*} {*dest_ip_spec*} [**precedence** *precedence*] [**tos** *tos*] [**capture**] [**before** *editbuffer_index* | **modify** *editbuffer_index*] [**log**[1]]

1. **log** キーワードは、拒否された IP VACL のメッセージを記録するだけです。

次に、IPACL1 に 1 つの ACE を作成し、送信元アドレス 172.20.53.4 からのトラフィックを許可する例を示します。

```
Console> (enable) set security acl ip IPACL1 permit host 172.20.53.4 0.0.0.0
IPACL1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

(注) VACL はリストの末尾に暗黙の拒否ステートメントが付加されるので、他のトラフィックはすべて拒否されます。

次に、IPACL1 に 1 つの ACE を作成して、すべての送信元アドレスからのトラフィックを許可する例を示します。

```
Console> (enable) set security acl ip IPACL1 permit any
IPACL1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

次に、IPACL1 に 1 つの ACE を作成して、送信元アドレス 171.3.8.2 からのトラフィックをブロックする例を示します。

```
Console> (enable) set security acl ip IPACL1 deny host 171.3.8.2
IPACL1 editbuffer modified.  Use 'commit' command to apply changes.
Console> (enable)
```

次に、編集バッファの内容を表示する例を示します。

```
Console> (enable) show security acl info IPACL1 editbuffer
set security acl ip IPACL1
------------------------------------------------------------------
1. permit ip host 172.20.53.4 any
2. permit ip any any
3. deny ip host 171.3.8.2 any
Console> (enable)
```

次に、ACE を NVRAM にコミットする例を示します。

```
Console> (enable) commit security acl all
ACL commit in progress.
ACL IPACL1 is committed to hardware.
Console> (enable)
```

(注) **commit security acl all** コマンドの詳細については、「ACL のコミット」(p.15-54)を参照してください。

変更がコミットされたかどうかを確認するには、**show security acl info IPACL1** コマンドを入力します。この VACL が VLAN にマッピングされていない場合には、**set security acl map** コマンドを使用して VLAN にマッピングします。

次に、IPACL2 に 1 つの ACE を作成して送信元アドレス 172.20.3.2 からのトラフィックをブロックし、この ACE を VACL の ACE 番号 2 の前に挿入する例を示します。任意で、**modify** キーワードを入力して、既存の ACE を新しい ACE に置き換えることができます。NVRAM に保存されている現在の ACE リストを表示するには、**show security acl info** *acl_name* [**editbuffer**] コマンドを使用します（編集バッファの内容を表示する場合、**editbuffer** キーワードを指定します）。

```
Console> (enable) set security acl ip IPACL2 deny host 172.20.3.2 before 2
IPACL2 editbuffer modified. Use ‘commit’ command to apply changes.
Console> (enable)
```

次に、IPACL2 に 1 つの ACE を作成して、送信元アドレスが 1.2.3.4 で宛先アドレスが 255.255.255.255 からの IP トラフィックを、ポート 3/1 にリダイレクトする例を示します。送信元および送信元ワイルドカード 0.0.0.0 の省略形として host を使用できます。また、この ACE は、次の内容も指定しています。

- **precedence** ― IP precedence 値です。優先度は、0（ゼロ）が最も低く、7 が最も高くなります。
- **tos** ― Type of Service（ToS; サービス タイプ）のレベルで、0 ～ 15 を指定します。

(注) ToS 値は IP To S バイトのビット 3 ～ 6 です（RFC 1349 により定義）。precedence 値はビット 0 ～ 2 です（RFC 791 により定義）。

```
Console> (enable) set security acl ip IPACL2 redirect 3/1 ip 1.2.3.4 0.0.0.255 host
255.255.255.255 precedence 1 tos min-delay
IPACL2 editbuffer modified. Use ‘commit’ command to apply changes.
Console> (enable)
```

次に、編集バッファの内容を表示する例を示します。

```
Console> (enable) show security acl info IPACL2 editbuffer
set security acl ip IPACL2
------------------------------------------------------------------
1. deny 172.20.3.2
2. redirect 1.2.3.4
Console> (enable)
```

(注) **show security acl info** コマンドの詳細については、「VACL の内容の表示」（p.15-55）を参照してください。

次に、ACE を NVRAM にコミットする例を示します。

```
Console> (enable) commit security acl all
ACL commit in progress.
ACL IPACL2 is committed to hardware.
Console> (enable)
```

(注) **commit security acl all** コマンドの詳細については、「ACL のコミット」（p.15-54）を参照してください。

変更がコミットされたかどうかを確認するには、**show security acl info IPACL2** コマンドを入力します。この VACL が VLAN にマッピングされていない場合には、**set security acl map** コマンドを使用して VLAN にマッピングします。

IPX VACL の作成および ACE の追加

(注) Supervisor Engine 720（PFC3A/PFC3B/PFC3BXL）および Supervisor Engine 32（PFC3B/PFC3BXL）では、IPX ルーティングはソフトウェアにより行われ、IPX Cisco IOS ACL および IPX VACL はサポートされません。MAC VACL を使用して IPX パケットを一致させることができます。IPX ARPA フレームを一致させるため、**ipx-arpa** キーワードを入力できます。IPX 非 ARPA フレームおよび Ethertype 0xffff のフレームで一致させるには、0xffff Ethertype を使用します。MAC VACL の設定については、「non-IP version 4/non-IPX VACL（MAC VACL）の作成および ACE の追加」（p.15-53）を参照してください。

新しい IPX VACL を作成して ACE を追加したり、既存の IPX VACL に ACE を追加するには、イネーブル モードで次の作業を行います。

作業	コマンド
新しい IPX VACL を作成して ACE を追加するか、既存の IPX VACL に ACE を追加します。	**set security acl ipx** {*acl_name*} {**permit** | **deny** | **redirect** *mod_num/port_num*} {*protocol*} {*src_net*} [*dest_net.*[*dest_node*] [[*dest_net_mask.*]*dest_node_mask*]] [**capture**] [**before** *editbuffer_index* **modify** *editbuffer_index*]

次に、IPXACL1 に 1 つの ACE を作成して、送信元ネットワーク 1234 からのすべてのトラフィックをブロックする例を示します。

```
Console> (enable) set security acl ipx IPXACL1 deny any 1234
IPXACL1 editbuffer modified. Use ‘commit’ command to apply changes.
Console> (enable)
```

次に、IPXACL1 に 1 つの ACE を作成して、宛先アドレスが 1.A.3.4 のすべてのトラフィックをブロックする例を示します。

```
Console> (enable) set security acl ipx IPXACL1 deny any any 1.A.3.4
IPXACL1 editbuffer modified. Use ‘commit’ command to apply changes.
Console> (enable)
```

次に、IPXACL1 に 1 つの ACE を作成して、送信元ネットワーク 3456 からのブロードキャスト トラフィックをポート 4/1 にリダイレクトする例を示します。

```
Console> (enable) set security acl ipx IPXACL1 redirect 4/1 any 3456
IPXACL1 editbuffer modified. Use ‘commit’ command to apply changes.
Console> (enable)
```

次に、編集バッファの内容を表示する例を示します。

```
Console> (enable) show security acl info IPXACL1 editbuffer
set security acl ipx IPXACL1
------------------------------------------------------------------
1. deny any 1234
2. deny any any 1.A.3.4
3. redirect 4/1 any 3456
Console> (enable)
```

(注)　**show security acl info** コマンドの詳細については、「VACL の内容の表示」（p.15-55）を参照してください。

次に、ACE を NVRAM にコミットする例を示します。

```
Console> (enable) commit security acl all
ACL commit in progress.
ACL IPXACL1 is committed to hardware.
Console> (enable)
```

変更がコミットされたかどうかを確認するには、**show security acl info IPXACL1** コマンドを入力します。この VACL が VLAN にマッピングされていない場合には、**set security acl map** コマンドを使用して VLAN にマッピングします。

次に、IPXACL1 に 1 つの ACE を作成して送信元ネットワーク 1 からのすべてのトラフィックを許可し、この ACE を ACE 番号 2 の前に挿入する例を示します。

```
Console> (enable) set security acl ipx IPXACL1 permit any 1 before 2
IPXACL1 editbuffer modified. Use ‘commit’ command to apply changes.
Console> (enable)
```

次に、IPXACL1 に 1 つの ACE を作成して、すべての送信元アドレスからのトラフィックを許可する例を示します。

```
Console> (enable) set security acl ipx IPXACL1 permit any any
IPXACL1 editbuffer modified. Use ‘commit’ command to apply changes.
Console> (enable)
```

次に、編集バッファの内容を表示する例を示します。

```
Console> (enable) show security acl info IPXACL1 editbuffer
set security acl ipx IPXACL1
------------------------------------------------------------------
1. deny any 1234
2. permit any 1
3. deny any any 1.A.3.4
4. redirect 4/1 any 3456
5. permit any any
ACL IPXACL1 Status: Not Committed
Console> (enable)
```

次に、ACE を NVRAM にコミットする例を示します。

```
Console> (enable) commit security acl all
ACL commit in progress.
ACL IPXACL1 is committed to hardware.
Console> (enable)
```

(注)　**commit security acl all** コマンドの詳細については、「ACL のコミット」（p.15-54）を参照してください。

変更がコミットされたかどうかを確認するには、**show security acl info IPXACL1** コマンドを入力します。この VACL が VLAN にマッピングされていない場合には、**set security acl map** コマンドを使用して VLAN にマッピングします。

non-IP version 4/non-IPX VACL（MAC VACL）の作成および ACE の追加

注意　IP トラフィックおよび IPX トラフィックは、MAC VACL ではアクセス制御されません。その他のトラフィック タイプ（AppleTalk、DECnet など）はすべて MAC トラフィックとして分類され、MAC VACL によってアクセス制御されます。

新しい non-IP version 4/non-IPX VACL を作成して ACE を追加したり、既存の non-IP version 4/non-IPX VACL に ACE を追加したりするには、イネーブル モードで次の作業を行います。

作業	コマンド
新しい non-IP version 4/non-IPX VACL を作成して ACE を追加するか、既存の non-IP version 4/non-IPX VACL に ACE を追加します。	**set security acl mac** {*acl_name*} {**permit** | **deny**} {*src_mac_addr_spec*} {*dest_mac_addr_spec*} [*ethertype*] [**capture**] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

次に、MACACL1 に 1 つの ACE を作成して、8-2-3-4-7-A からのすべてのトラフィックをブロックする例を示します。

```
Console> (enable) set security acl mac MACACL1 deny host 8-2-3-4-7-A any
MACACL1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

次に、MACACL1 に 1 つの ACE を作成して、A-B-C-D-1-2 を宛先とするすべてのトラフィックをブロックする例を示します。

```
Console> (enable) set security acl mac MACACL1 deny any host A-B-C-D-1-2
MACACL1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

次に、MACACL1 に 1 つの ACE を作成して、すべての送信元からのトラフィックを許可する例を示します。

```
Console> (enable) set security acl mac MACACL1 permit any any
MACACL1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

次に、編集バッファの内容を表示する例を示します。

```
Console> (enable) show security acl info MACACL1 editbuffer
set security acl mac MACACL1
-----------------------------------------------------------------
1. deny 8-2-3-4-7-A any
2. deny any A-B-C-D-1-2
3. permit any any
Console> (enable)
```

(注)　**show security acl info** コマンドの詳細については、「VACL の内容の表示」（p.15-55）を参照してください。

次に、ACE を NVRAM にコミットする例を示します。

```
Console> (enable) commit security acl all
ACL commit in progress.
ACL MACACL1 is committed to hardware.
Console> (enable)
```

(注)　**commit security acl all** コマンドの詳細については、「ACL のコミット」（p.15-54）を参照してください。

変更がコミットされたかどうかを確認するには、**show security acl info MACACL1** コマンドを入力します。この VACL が VLAN にマッピングされていない場合には、**set security acl map** コマンドを使用して VLAN にマッピングします。

ACL のコミット

すべての ACL または指定した ACL を NVRAM にコミットするには、**commit** コマンドを使用します。ACE が設定されていない ACL は、コミットしても削除されます。

ACL を NVRAM にコミットするには、イネーブル モードで次の作業を行います。

作業	コマンド
ACL を NVRAM にコミットします。	**commit security acl** *acl_name* | **all**

次に、セキュリティ ACL を指定して、NVRAM にコミットする例を示します。

```
Console> (enable) commit security acl IPACL2
ACL commit in progress.
ACL IPACL2 is committed to hardware.
Console> (enable)
```

VACL の VLAN へのマッピング

VACL を VLAN にマッピングするには、**set security acl map** コマンドを使用します。デフォルトの ACL/VLAN マッピングは設定されていないことに注意してください。すべての VACL を VLAN にマッピングする必要があります。

VACL を VLAN にマッピングするには、イネーブル モードで次の作業を行います。

作業	コマンド
VACL を VLAN にマッピングします。	**set security acl map** *acl_name vlans*

次に、IPACL1 を VLAN 10 にマッピングする例を示します。

```
Console> (enable) set security acl map IPACL1 10
ACL IPACL1 mapped to vlan 10
Console> (enable)
```

次に、コミットしていない ACL をマッピングしようとした場合の出力例を示します。

```
Console> (enable) set security acl map IPACL1 10
Commit ACL IPACL1 before mapping.
Console> (enable)
```

VACL の内容の表示

VACL の内容を表示するには、**show security acl info** コマンドを使用します。

VACL の内容を表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
VACL の内容を表示します。	**show security acl info** {*acl_name* | **all**} [**editbuffer** [*editbuffer_index*]]

次に、NVRAM に保存した VACL の内容を表示する例を示します。

```
Console> (enable) show security acl info IPACL1
set security acl ip IPACL1
------------------------------------------------------------------
1. deny A
2. deny ip B any
3. deny c
4. permit any
```

次に、編集バッファ内にある VACL の内容を表示する例を示します。

```
Console> (enable) show security acl info IPACL1 editbuffer
set security acl ip IPACL1
------------------------------------------------------------------
1. deny A
2. deny ip B any
3. deny C
4. deny D
5. permit any
Console> (enable)
```

VACL/VLAN のマッピングの表示

show security acl map コマンドを使用して、特定の ACL または VLAN の VACL/VLAN マッピングを表示することができます。

VACL/VLAN マッピングを表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
VACL/VLAN のマッピングを表示します。	**show security acl map** {*acl_name* | *vlan* | **all**}

次に、特定の VACL のマッピングを表示する例を示します。

```
Console> (enable) show security acl map IPACL1
ACL IPACL1 is mapped to VLANs:
1
Console> (enable)
```

次に、特定の VLAN のマッピングを表示する例を示します。

```
Console> (enable) show security acl map 1
VLAN 1 is mapped to IP ACL IPACL1.
VLAN 1 is mapped to IPX ACL IPXACL1.
VLAN 1 is mapped to MAC ACL MACACL1.
Console> (enable)
```

編集バッファの消去

rollback コマンドを使用して、最後に保存したあとに行った ACL 編集バッファの変更を消去することができます。ACL は、最後の **commit** コマンド実行時の内容に戻ります。

ACL 編集バッファの内容を消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
ACL 編集バッファの内容を消去します。	**rollback security acl** {*acl_name* | **all** | **adjacency**}

次に、特定のセキュリティ ACL について、編集バッファの内容を消去する例を示します。

```
Console> (enable) rollback security acl IPACL1
Editbuffer for 'IPACL1' rolled back to last commit state.
Console> (enable)
```

セキュリティ ACL からの ACE の削除

ACL から特定の ACE またはすべての ACE を削除するには、**clear security acl** コマンドを使用します。このコマンドは、編集バッファから ACE を削除します。

セキュリティ ACL から ACE を削除するには、イネーブル モードで次の作業を行います。

作業	コマンド
セキュリティ ACL から ACE を削除します。	**clear security acl all** **clear security acl** *acl_name* **clear security acl** *acl_name editbuffer_index*

次に、すべての ACL から ACE を削除する例を示します。

```
Console> (enable) clear security acl all
All editbuffers modified. Use 'commit' command to apply changes.
Console> (enable)
```

次に、特定の ACL から特定の ACE を削除する例を示します。

```
Console> (enable) clear security acl IPACL1 2
IPACL1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

セキュリティ ACL マップの消去

VACL/VLAN マッピングを削除するには、**clear security acl map** コマンドを使用します。

セキュリティ ACL マップを消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
セキュリティ ACL マップを消去します。	**clear security acl map all** **clear security acl map** *acl_name* **clear security acl map** *vlan* **clear security acl map** *acl_name vlan*

次に、すべての VACL/VLAN マッピングを消去する例を示します。

```
Console> (enable) clear security acl map all
Map deletion in progress.

Successfully cleared mapping between ACL ip1 and VLAN 10.

Successfully cleared mapping between ACL ipx1 and VLAN 10.

(テキスト出力は省略)
Console> (enable)
```

次に、特定の VLAN 上の特定の VACL のマッピングを消去する例を示します。

```
Console> (enable) clear security acl map IPACL1 50
Map deletion in progress.

Successfully cleared mapping between ACL ipacl1 and VLAN 50.
Console> (enable)
```

VACL 管理情報の表示

VACL 管理情報を表示するには、**show security acl resource-usage** コマンドを使用します。

VACL 管理情報を表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
VACL 管理情報を表示します。	**show security acl resource-usage**

次に、VACL 管理情報を表示する例を示します。

```
Console> (enable) show security acl resource-usage
ACL resource usage:
ACL storage (mask/value): 0.29%/0.10%
ACL to switch interface mapping table: 0.39%
ACL layer 4 port operators: 0.0%
Console (enable)
```

特定ポート上でのトラフィック フローのキャプチャ

set security acl（**ip**、**ipx**、および **mac**）コマンドの **capture** キーワードを入力して、指定したフローと一致するパケットをキャプチャして、キャプチャ ポートから送出することができます。キャプチャ ポートは、**set security acl capture-ports** *mod/ports...* コマンドを使用して指定します。**capture** キーワードを使用すると、指定したフローと一致するパケットが、通常どおりスイッチングされるほか、キャプチャされ、キャプチャ ポートから送出されます。キャプチャ ポートはキャプチャしたすべてのトラフィックを送出するわけではありません。キャプチャ ポートの VLAN に属するトラフィックだけを送出します。

設定時の注意事項

ここでは、キャプチャ ポート設定時の注意事項について説明します。

- キャプチャ ポートは、EtherChannel の一部にすることはできません。
- キャプチャ ポートは、ATM（非同期転送モード）ポートとして使用することはできません。
- キャプチャ ポートは、VLAN のスパニングツリー フォワーディング ステートに設定する必要があります。
- 任意の数のスイッチ ポートをキャプチャ ポートとして指定することができます。キャプチャ ポートは、キャプチャ ポート リストに追加され、その設定が NVRAM に保存されます。
- 許可トラフィックだけがキャプチャされます。ACL により廃棄されたパケットはキャプチャできません。
- キャプチャ ポートは、キャプチャしたすべてのトラフィックを送出するわけではありません。キャプチャ ポートの VLAN に属するトラフィックだけが送出されます。多数の VLAN に宛てられたトラフィックをキャプチャするには、キャプチャ ポートを、必要な VLAN をサポートするトランクとして設定する必要があります。

  ルーテッド トラフィックの場合、キャプチャ ポートがパケットを送信するのは、レイヤ 3 でスイッチングされたあとだけです。したがって、レイヤ 3 でスイッチングされたフローの出力 VLAN がキャプチャ ポートの VLAN と一致する場合に限り、パケットがポートから送出されます。たとえば、VLAN 10 から VLAN 20 へのフローがある場合、（VLAN の 1 つに）これらのフローを許可する VACL を追加し、キャプチャ ポートを指定したと想定します。この場合、トラフィックがキャプチャ ポートから送出されるのは、トラフィックが VLAN 20 に属しているか、またはポートが VLAN 20 をサポートするトランクの場合だけです。キャプチャ ポートが VLAN 10 に存在する場合は、トラフィックは送出されません。キャプチャ ポートがトラフィックを送出するかどうかは、VACL が設定されている VLAN とは無関係です。

  1 つの VLAN から多数の VLAN に宛てられるトラフィックをキャプチャしたい場合には、キャプチャ ポートを、すべての出力 VLAN をサポートするトランクとして設定する必要があります。

  ブリッジド トラフィックの場合、すべてのトラフィックは同じ VLAN 内にとどまるため、キャプチャ ポートはブリッジド トラフィックと同じ VLAN 内に存在します。
- トラフィックをキャプチャするには、1 つの ACL を設定して VLAN グループにマッピングするか、複数の ACL を設定して各 ACL を 1 つの VLAN にマッピングします。必要なトラフィックをキャプチャするには、1 つの ACL ごとに必要なだけ ACE を設定します。

トラフィック フローをキャプチャする手順は、次のとおりです。

（注） この説明では IP VACL を使用していますが、同じ手順で IPX および non-IP version 4/non-IPX VACL を設定することもできます。

ステップ 1　**set security acl ip** コマンドを入力して VACL を作成し、ACE を追加します。**capture** キーワードを指定します。

ステップ 2　**commit** コマンドを入力して、VACL および関連付けられた ACE を NVRAM にコミットします。

ステップ 3　**set security acl map** コマンドを入力して、VACL を VLAN にマッピングします。

ステップ 4　**set security acl capture-ports** *mod/ports...* コマンドを入力して、キャプチャ ポートを指定します。

設定例

次に、my_cap に 1 つの ACE を作成し、許可トラフィックをキャプチャするように指定する例を示します。

```
Console> (enable) set security acl ip my_cap permit ip host 60.1.1.1 host 60.1.1.98
capture
my_cap editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

次に、my_cap ACL を NVRAM にコミットする例を示します。

```
Console> (enable) commit security acl my_cap
ACL commit in progress.

ACL my_cap successfully committed.
Console> (enable)
```

次に、my_cap を VLAN 10 にマッピングする例を示します。

```
Console> (enable) set security acl map my_cap 10
Mapping in progress.

VLAN 10 successfully mapped to ACL my_cap.
The old mapping with ACL captest was replaced with the new one.
Console> (enable)
```

次に、キャプチャ ポートを指定する例を示します。

```
Console> (enable) set security acl capture-ports 1/1-2,2/1-2
Successfully set the following ports to capture ACL traffic:
1/1-2,2/1-2
Console> (enable)
```

次に、キャプチャ ポートとして指定したポートを表示する例を示します。

```
Console> (enable) show security acl capture-ports
ACL Capture Ports: 1/1-2,2/1-2
Console> (enable)
```

次に、キャプチャ ポートを削除する例を示します。

```
Console> (enable) clear security acl capture-ports 1/1,2/1
Successfully cleared the following ports:
1/1,2/1
Console> (enable)
```

次に、ポート 1/1 および 2/1 が削除された例を示します。

```
Console> (enable) show security acl capture-ports
ACL Capture Ports:1/2,2/2
Console> (enable)
```

VACL ロギングの設定

（注） この機能を使用できるのは、PFC2 搭載の Supervisor Engine 2、PFC3A/PFC3B/PFC3BXL 搭載の Supervisor Engine 720、および PFC3B/PFC3BXL 搭載の Supervisor Engine 32 だけです。

拒否 VACL に対して **log** キーワードを使用すると、標準 IP アクセス リストについて、拒否されたパケットのメッセージを記録できます。アクセス リストに一致するパケットによって、コンソールに送信されるパケットに関する情報ロギング メッセージが生成されます。コンソールに記録されるメッセージのレベルは、**set logging level acl** *severity* コマンドによって制御されます。

最初のパケットはアクセス リストをトリガし、それによってただちにロギング メッセージが生成されます。それ以降のパケットは、5 分間隔で収集されてから、表示または記録されます。ロギング メッセージには、過去 5 分間に受信したパケットのフロー パターンと数が含まれています。

デフォルトでは、システム ロギング メッセージがコンソールに送信されます。Syslog サーバにシステム ロギング メッセージを送信するように、スイッチを設定することができます。システム メッセージ ロギングの設定については、第 28 章「システム メッセージ ロギングの設定」を参照してください。

設定時の注意事項

ここでは、VACL ロギング設定時の注意事項について説明します。

- IP VACL からの拒否トラフィックのみを記録します。
- ロギング レベルは 6（情報）または 7（デバッグ）に設定します。

VACL のロギングをイネーブルにする手順は、次のとおりです。

ステップ 1　**set logging level acl** *severity* コマンドを入力して、ロギング レベルを 6（情報）または 7（デバッグ）に設定します。

ステップ 2　（任意）**set security acl log maxflow** *max_number* コマンドを入力して、最大フロー パターン数に基づいて新しいログ テーブルを割り当て、記録されたパケット情報を保存します。正常に実行されると、新しいバッファが古いものと置き換えられ、古いテーブルのフローがすべて消去されます。メモリが不足しているか、最大数が限度を超えている場合は、エラー メッセージが表示され、コマンドは廃棄されます。有効な値は、256 ～ 2048 で、デフォルト値は 500 です。

（注） 最大フロー パターンが max_num の限度を超えている場合は、エラー メッセージが表示され、コマンドは廃棄されます。このようなパケットのメッセージは記録されません。

ステップ 3　（任意）**set security acl log ratelimit** *pps* コマンドを入力して、pps（パケット / 秒）単位でリダイレクト レートを設定します。設定が範囲を超える場合は、コマンドは廃棄され、範囲がコンソールに表示されます。有効な値は 500 ～ 5000 で、デフォルト値は 2500 です。レート制限をディセーブルにするには、値を 0 に設定します。

（注） リダイレクト レートが pps の範囲を超える場合は、コマンドは廃棄され、範囲がコンソールに表示されます。このようなパケットのメッセージは記録されません。

ステップ 4　**set security acl ip** *acl_name* **deny log** コマンドを入力して IP VACL を作成し、ロギングをイネーブルにします。

ステップ 5　**commit security acl** *acl_name* コマンドを入力して、VACL を NVRAM にコミットします。

ステップ 6　**set security acl map** *acl_name vlan* コマンドを入力して、VACL を VLAN にマッピングします。

設定例

次に、ロギング レベルを設定する例を示します。

```
Console> (enable) set logging level acl 6
System logging facility <acl> for this session set to severity 6(information)
```

次に、最大フローに基づく新しいログ テーブルを割り当てる例を示します。

```
Console> (enable) set security acl log maxflow 512
Set VACL Log table to 512 flow patterns.
```

次に、リダイレクト レートを設定する例を示します。

```
Console> (enable) set security acl log ratelimit 1000
Max logging eligible packet rate set to 1000pps.
```

次に、VACL ログの設定を表示する例を示します。

```
Console> (enable) show security acl log config
VACL LOG Configration
------------------------------------------------------------
Max Flow Pattern    : 512
Max Logging Eligible rate (pps) : 1000
```

次に、my_cap に ACE を 1 つ作成し、拒否されたトラフィックを記録するように指定する例を示します。

```
Console> (enable) set security acl ip my_cap deny ip host 21.0.0.1 log
my_cap editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

次に、my_cap ACL を NVRAM にコミットする例を示します。

```
Console> (enable) commit security acl my_cap
ACL commit in progress.

ACL my_cap successfully committed.
Console> (enable)
```

次に、VACL を VLAN にマッピングする例を示します。

```
Console> (enable) set security acl map my_cap 1
Mapping in progress.
ACL my_cap successfully mapped to VLAN 1.
:
:
2000 Jul 19 01:14:06 %ACL-6-VACLLOG:VLAN 1(Port 2/1) denied ip tcp 21.0.0.1(2000) ->
255.255.255.255(3000), 1 packet
2000 Jul 19 01:19:06 %ACL-6-VACLLOG:VLAN 1(Port 2/1) denied ip tcp 21.0.0.1(2000) ->
255.255.255.255(3000), 7 packets
2000 Jul 19 01:25:06 %ACL-6-VACLLOG:VLAN 1(Port 2/2) denied ip tcp 21.0.0.1(2000) ->
255.255.255.255(3000), 1 packets
```

次に、ログ テーブルのフロー情報を表示する例を示します。

```
Console> (enable) show security acl log flow ip any any
Total matched entry number = 1
Entry No. #1, IP Packet
----------------------------------------
Vlan Number            : 1
Mod/Port Number        : 2/1
Source IP address      : 21.0.0.1
Destination IP address : 255.255.255.255
TCP Source port        : 2000
TCP Destination port   : 3000
Received Packet Number : 10
```

次に、ログ テーブルを消去する例を示します。

```
Console> (enable) clear security acl log flow
Log table is cleared.
Console> (enable)
```

すべてのパケット タイプに関する MAC ベース ACL 検索の設定

（注）　この機能を使用できるのは、PFC3B および PFC3BXL だけです。

ここでは、すべてのパケット タイプに関する MAC ベース ACL 検索の設定手順について説明します。

MAC ベース ACL の概要

PFC3A は IP と MAC の 2 つの ACL プロトコル タイプをサポートします。IP ACL は IP バージョン 4 パケットとのみ一致し、MAC ACL は PFC3A で *サポートされない* すべてのパケット タイプと一致します（詳細については、「non-IP version 4/non-IPX VACL（MAC VACL）の作成および ACE の追加」[p.15-53] を参照）。PFC3A でサポートされているパケット タイプは、IP バージョン 4、MPLS、ARP/RARP、および IP バージョン 6 です。ただし、Release 8.4(1) 以前のソフトウェア リリースで作成できるのは、IP バージョン 4 ACL のみです。サポートされないパケット タイプ（IPX パケット タイプなど）は、MAC ACL を使用して一致させます。

（注）　IPX パケット タイプは PFC および PFC2 でサポートされています。

すべてのパケット タイプに関する MAC ベース ACL 検索の使用

PFC3B および PFC3BXL では、MAC ACL を使用して、すべてのパケット タイプに関する ACL 検索を実行できます。この機能は、パケットが IP バージョン 4、IP バージョン 6、IPX、MPLS などのいずれであるかに関係なく、すべてのパケットに関して MAC ベース マッチングを実行する場合に便利です。この機能を利用すると、集約ポリサーと match-all MAC ACL を組み合わせて、VLAN に入るすべてのトラフィックを特定のレートに制限できます。

この機能は入力 VLAN 単位でイネーブルにされ、セキュリティ ACL（VACL）および QoS ACL に影響します。着信 VLAN でこの機能がイネーブルにされている場合、この VLAN に着信するすべてのパケットは、IP バージョン 4 パケットなどの場合であっても、MAC ベース ACL とマッチングされます。

MAC ACL では、IP バージョン 4 Ethertype が追加されるように *ethertype* オプションが拡張されていて、IP バージョン 4 パケットを特に対象とするように ACE を設定できます。

MAC ベース ACL への VLAN および CoS の追加

PFC3B および PFC3BXL では、ポート VLAN 検索をサポートする MAC ACL 検索キーの一部として、Class of Service（CoS; サービス クラス）および VLAN を追加できます。この機能は、VLAN を個別に処理できるトランク ポートで使用すると便利です。この拡張機能は、VACL および QoS MAC ACL に影響します。PFC3B および PFC3BXL では、MAC 検索キーのフレーム タイプ フィールドによって VLAN フィールドが過負荷になります。CoS および VLAN フィールドはマスク可能であるため、両方のフィールドをオプション パラメータとして追加し、古い MAC ACL 設定をサポートできます。

VLAN マッチング

PFC3B および PFC3BXL では、MAC ACL が入力にマッピングされている場合、パケットの入力 VLAN が MAC ACL とのマッチングに使用されます。同様に、MAC ACL が出力にマッピングされている場合、パケットに関連する出力 VLAN が MAC ACL とのマッチングに使用されます。

（注） MAC ACL と VLAN マッチングは、ポートにのみ適用できます。

VLAN マッチングは MAC ベース ACL 検索機能と組み合わせて使用したり、独立して使用することができます。また、検索はポート VLAN 単位で実行できます（VLAN 範囲全体がサポートされます）。

CoS マッチング

入力と出力のいずれの場合も、パケットに対応付けられた入力 CoS が MAC ACL とのマッチングに使用されます。入力 CoS は DBus ヘッダー内の CoS であり、ポートの信頼状態（trust-CoS/DSCP/IPprec/untrusted）、デフォルト CoS、および 802.1Q 対応ポートの CoS/CoS マッピング テーブルを問い合わせたあとに構築されます。

（注） CoS マッチング動作は、パケット転送方法に応じて、出力 ACL（VACL および QoS ACL）ごとに異なる場合があります。標準のハードウェア ショートカット パケットでは、出力 ACL は入力 ACL と同じ CoS に関してマッチングを行います。ただし、ルータやマルチキャスト読み取り / 書き込みエンジンなどの中間転送エンティティを介してパケットが転送される場合、DBus CoS は通常、入力 DBus CoS と異なります。

CoS マッチングは MAC ベース ACL 検索機能と組み合わせて使用したり、または独立して使用することができます。

設定時の注意事項

MAC ベース ACL 検索を設定する場合は、次の注意事項に従ってください。

- この機能をイネーブルにする必要があるのは、レイヤ 2 VLAN のみです（この推奨事項は Metro カスタマーに適用されます）。
- レイヤ 3 VLAN 上でこの機能をイネーブルにする場合は、次の点に注意してください。
  - 一部のレイヤ 3 機能が失われ、次の警告メッセージが表示されます。

```
Warning:IP RACLs, VACLs & some IP features will be ineffective on these vlans.
```

— パケットがハードウェア転送されるか、またはソフトウェア転送されるかに応じて、出力 ACL 検索に矛盾が生じることがあります。この機能をすべての VLAN でイネーブルにして、矛盾を回避することを推奨します（この推奨事項は Enterprise カスタマーに適用されます）。

すべてのパケット タイプに関する MAC ベース ACL 検索の設定

ここに記載されたコマンドは、VACL および QoS MAC ACL の両方に影響します。**set acl mac-packet-classify** *vlans* コマンドを使用すると、送信元 VLAN に着信したすべてのパケット タイプに関して MAC 検索をイネーブルにできます。**clear acl mac-packet-classify** [*vlans*] コマンドを使用すると、指定された VLAN の設定をデフォルトに戻します。デフォルト動作では、MAC ACL に一致するのは MAC パケットのみです。**clear acl mac-packet-classify** [*vlans*] コマンドを使用して VLAN を指定しない場合は、すべての VLAN でこの機能がディセーブルになります。**show acl mac-packet-classify** コマンドを使用すると、MAC パケット分類機能がイネーブルになっている VLAN リストが表示されます。

MAC ACL および拡張 Ethertype への CoS、VLAN、およびパケット タイプの追加

VACL および QoS ACL CLI は、CoS および VLAN に関するマッチングのオプション パラメータを追加するように、拡張されています。これらのコマンドは、次のとおりです。

```
Usage: set security acl mac {acl_name} {permit | deny}
            <src_mac_addr_spec> <dest_mac_addr_spec>
            [<ethertype>] [capture]
            [cos <cos_value>]
            [vlan <vlan>]
            [before <editbuffer_index>|modify <editbuffer_index>]
            (mac_addr_spec = <addr> <mask> or host <addr> or any
     example: 11-22-33-44-00-00 00-00-00-00-ff-ff, host 11-22-33-44-55-66)
            ethertype = names or 0x0, 0x05ff - 0xffff,
            cos_value = 0..7, vlan = 1..4094,

Usage: set qos acl mac {acl_name} {dscp dscp | trust-cos}
            [aggregate <aggregate_name>]
            <src_mac_addr_spec> <dest_mac_addr_spec> [<ethertype>]
            [cos <cos_value>]
            [vlan <vlan>]
            [before <editbuffer_index>|modify <editbuffer_index>]
            (mac_addr_spec = <addr> <mask> or host <addr> or any
     example: 11-22-33-44-00-00 00-00-00-00-ff-ff, host 11-22-33-44-55-66)
            ethertype = names or 0x0, 0x05ff - 0xffff,
            cos_value = 0..7, vlan = 1..4094,
```

CoS および VLAN フィールドはオプションです。このフィールドを指定しない場合は、すべての CoS または VLAN 値と一致します。

（注） VLAN マッチ オプションが指定された ACL は、ポートにのみマッピングできます。

（注） **set acl mac-packet-classify** *vlans* コマンドを使用すると、すべての Cisco IOS ACL が操作不能になります。

IP バージョン 4 オプションを追加するように、Ethertype が拡張されています。これにより、MAC ACL 検索を使用する場合に、IP バージョン 4 パケットを特に対象とすることができます。IP バージョン 4 オプションを選択した場合は、**set acl mac-packet-classify** *vlans* コマンドを使用して、対応する VLAN がイネーブルにされているか確認する必要があります。次のように、IP バージョン 4 オプションが追加されました。

```
Console> (enable) set security acl mac macacl1 permit any any ?
  <0x0, 0x0600 - 0xffff>     Match an EtherType value
  ipv4                       (0x8000)
  ipx-arpa                   (0x8137) Use 0xffff to match on non-arpa IPX
  .......
Console> (enable)
```

次に、MAC ベース ACL 検索 CLI の例を示します。

```
Console> (enable) set acl mac-packet-classify 5
Enabled mac-packet-classify on vlan(s) 5.
Warning:IP RACLs, VACLs & some IP features will be ineffective on these vlans.
Console> (enable) show acl mac-packet-classify
Feature enabled on source vlan(s) 1,5.
Console> (enable) clear acl mac-packet-classify 5
Disabled mac-packet-classify on vlan(s) 5.
Console> (enable)
```

(注) **set** および **clear** コマンドに **all** キーワードを使用すると、すべての VLAN を指定できます。

VACL および QoS ACL の設定およびフラッシュ メモリへの保存

ここでは、VACL および QoS ACL を設定し、NVRAM ではなくフラッシュ メモリに保存する手順について説明します。これまでの作業では、設定情報はすべて NVRAM に保存されます。QoS およびセキュリティ ACL（VACL）を追加すると、NVRAM の空き容量がなくなることがあります。NVRAM の空き容量がなくなると、ACL 設定が制限されるほか、ソフトウェア バージョンのアップグレード時にも支障があります。

（注） ほとんどの場合、VACL および QoS ACL を保存するには 512 KB の NVRAM で十分です。そのため、デフォルトでは、すべての ACL 設定が NVRAM に保存されます。

ここで説明する作業は、次のとおりです。

- VACL および QoS ACL 設定のフラッシュ メモリへの自動的な移動（p.15-67）
- VACL および QoS ACL 設定のフラッシュ メモリへの手動での移動（p.15-68）
- VACL および QoS ACL 設定のフラッシュ メモリからの実行（p.15-70）
- VACL および QoS ACL 設定の NVRAM への再移動（p.15-70）
- 冗長構成の同期化サポート（p.15-70）
- ハイ アベイラビリティの保証（p.15-70）

（注） ここで使用するコマンドの詳細については、第 24 章「スイッチの起動設定の変更」を参照してください。

VACL および QoS ACL 設定のフラッシュ メモリへの自動的な移動

VACL および QoS ACL 設定がフラッシュ メモリに自動的に移動するのは、システム ソフトウェアのアップグレード時に、アップグレードに必要な NVRAM 容量が不足している場合だけです。ソフトウェア アップグレードの実行に必要な NVRAM 容量が不足している場合、NVRAM から QoS ACL および VACL の設定が削除され、ACL 設定が自動的にフラッシュ メモリに移されます。この場合、次の Syslog メッセージが表示されます。

```
1999 Sep 01 17:00:00 %SYS-1-CFG_FLASH:ACL configuration moved to
bootflash:switchapp.cfg
1999 Sep 01 17:00:00 %SYS-1-CFG_ACL_DEALLOC:NVRAM full. Qos/Security ACL configuration
deleted from NVRAM.
```

これで、VACL および QoS ACL 設定がフラッシュ メモリに正常に移動したことが確認できます。この間システムは、同時に次の処理も実行します。

- CONFIG_FILE 変数を bootflash:switchapp.cfg に設定します。
- **set boot config-register auto-config** コマンドの **recurring**、**append**、および **sync** オプションをイネーブルにします。

アップグレード中にエラーが発生すると、次の Syslog メッセージが表示されます。

```
1999 Sep 01 17:00:00 %SYS-1-CFG_FLASH_ERR:Failed to write ACL configuration to
bootflash:switchapp.cfg
1999 Sep 01 17:00:00 %SYS-1-CFG_ACL_DEALLOC:NVRAM full. Qos/Security ACL configuration
deleted from NVRAM.
```

これらのエラー メッセージが表示された場合、VACL および QoS ACL 設定は DRAM だけに保存されています。フラッシュ メモリ内に空き容量を確保して設定をフラッシュ メモリに保存する必要があります（「VACL および QoS ACL 設定の NVRAM への再移動」[p.15-70] を参照）。または、不要な VACL および QoS ACL を削除して、**set config acl nvram** コマンドで ACL 設定を NVRAM に保存することもできます。

VACL および QoS ACL 設定のフラッシュ メモリへの手動での移動

VACL および QoS ACL 設定が、512 KB の NVRAM 容量を超える場合には、次の手順で、VACL および QoS ACL の設定を手動でフラッシュ メモリに移動することができます。

ステップ 1　起動時のスイッチ設定に使用する VACL および QoS ACL auto-config ファイルを指定します。

```
Console> (enable) set boot auto-config bootflash:switchapp.cfg
CONFIG_FILE variable = bootflash:switchapp.cfg
Console> (enable)
```

ステップ 2　スイッチのリセットまたはいったん電源を切ってから再投入する際に、CONFIG_FILE 環境変数の値を保持する（**recurring** キーワード）かまたは消去する（**non-recurring** キーワード）かを指定します。

```
Console> (enable) set boot config-register auto-config recurring
Configuration register is 0x12F
ignore-config: disabled
auto-config: recurring, overwrite, sync disabled
console baud: 9600
boot: image specified by the boot system commands
Console> (enable)
```

ステップ 3　auto-config ファイルにより、NVRAM の設定を上書きするか、または現在の NVRAM の内容に追加するかを指定します。

```
Console> (enable) set boot config-register auto-config append
Configuration register is 0x12F
ignore-config: disabled
auto-config: recurring, append, sync disabled
console baud: 9600
boot: image specified by the boot system commands
Console> (enable)
```

ステップ 4　同期化をイネーブルにするか、ディセーブルにするかを指定します。同期化をイネーブルにすると、auto-config ファイルにより、スタンバイ スーパバイザ エンジンが自動的に同期化されます。

```
Console> (enable) set boot config-register auto-config sync enable
Configuration register is 0x12F
ignore-config: disabled
auto-config: recurring, append, sync enabled
console baud: 9600
boot: image specified by the boot system commands
Console> (enable)
```

ステップ 5　コミットした VACL および QoS ACL 設定の変更を、auto-config ファイルに保存します。

```
Console> (enable) copy acl-config bootflash:switchapp.cfg
Upload ACL configuration to bootflash:switchapp.cfg
2843644 bytes available on device bootflash, proceed (y/n) [n]? y
ACL configuration has been copied successfully.
Console> (enable)
```

ステップ 6　NVRAM から、VACL および QoS ACL の設定を削除します。

```
Console> (enable) clear config acl nvram
ACL configuration has been deleted from NVRAM.
Warning: Use the copy commands to save the ACL configuration to a file and
the 'set boot config-register auto-config' commands to configure the
auto-config feature.
```

（注）　auto-config ファイルには、VACL および QoS ACL のマッピング コマンド（**set qos acl map** および **set security acl map**）も保存されます。VACL および QoS ACL の設定をフラッシュ メモリに保存するとき、マッピング コマンドを使用している場合には、**copy** コマンドを使用して設定をフラッシュ メモリに保存する必要があります。

この時点で VACL および QoS ACL 設定は、NVRAM から削除されています。設定は auto-config ファイルの bootflash:switchapp.cfg に保存されており、システムの起動時に NVRAM 設定に付加されます。

VACL および QoS ACL 設定に変更を加え、変更をコミットした場合には、**copy acl-config bootflash:switchapp.cfg** コマンドを使用して、設定を auto-config ファイルに保存する必要があります。

同期化をイネーブルに設定したので、auto-config ファイルの内容はスタンバイ スーパバイザ エンジンに自動的に反映されます。

VACL および QoS ACL 設定をフラッシュ メモリに書き込めない場合、設定は NVRAM から削除されています。その場合、VACL および QoS ACL 設定が保存されている場所は DRAM のみになります。システムをリセットすると、VACL および QoS ACL 設定はデフォルト設定に戻ります。

（注）　設定をフラッシュ メモリに書き込めない場合には、設定をファイルにコピーし、フラッシュ メモリの空き容量を増やしてから、VACL および QoS ACL 設定を再びフラッシュ メモリに書き込んでください。

システムの起動時に、VACL および QoS ACL 設定の保存場所がフラッシュ メモリに設定されている場合、CONFIG_FILE 変数が設定されていないか、指定したファイルが存在しないと、次の Syslog メッセージが表示されます。

```
1999 Sep 01 17:00:00 %SYS-0-CFG_FLASH_ERR:ACL configuration set to flash but no ACL
configuration file found.
```

VACL および QoS ACL 設定のフラッシュ メモリからの実行

VACL および QoS ACL 設定をフラッシュ メモリに移動したあとは、QoS ACL および VACL のコミット動作は NVRAM に書き込まれません。次のように、設定を手動でフラッシュ ファイルにコピーする必要があります。

- **set boot config-register auto-config append** オプションを使用すると、auto-config ファイルの設定が NVRAM 設定に追加されます。コミットしたあと、VACL および QoS ACL の設定をこのファイルにコピーするだけで済みます。
- **set boot config-register auto-config append** オプションを使用しないと、システムの起動時に、NVRAM の設定が消去されてから、auto-config ファイルが実行されます。この場合、NVRAM に保存した変更は失われます。保存する場合には、（VACL および QoS ACL 設定だけでなく）設定全体を auto-config ファイルにコピーしておく必要があります。

VACL および QoS ACL 設定の NVRAM への再移動

次に、VACL および QoS ACL の設定を NVRAM に戻す例を示します。

```
Console> (enable) set config acl nvram
ACL configuration copied to NVRAM.
Console> (enable)

Console> (enable) clear boot auto-config
CONFIG_FILE variable =
Console> (enable)
```

冗長構成の同期化サポート

set boot コマンドには、auto-config ファイルを自動的に同期化するオプションがあります。

auto-config オプションをイネーブルにして、VACL と QoS ACL の設定がフラッシュ メモリにある場合、アクティブ スーパバイザ エンジン上の auto-config ファイルの変更は常に、スタンバイ スーパバイザ エンジンに同期化されます。たとえば、アクティブ スーパバイザ エンジン上の auto-config ファイルを削除すると、スタンバイ スーパバイザ エンジン上でもそのファイルが削除されます。同様に、新しいスタンバイ スーパバイザ エンジンを搭載すると、アクティブ スーパバイザ エンジンにより、auto-config ファイルが自動的に同期化されます。

ハイ アベイラビリティの保証

スーパバイザ エンジンがスイッチオーバーしても、スタンバイ スーパバイザ エンジンの VACL および QoS ACL 設定は、アクティブ スーパバイザ エンジンの内容、すなわち NVRAM に保存されている VACL および QoS ACL 設定とまったく同じです。唯一の違いは、スタンバイ スーパバイザ エンジンではデータは DRAM に保存されますが、スイッチオーバーの機能的な動作の変更がないことです。

ポート単位の ACL の設定

（注）　この機能を使用できるのは、PFC3A/PFC3B/PFC3BXL 搭載の Supervisor Engine 720 および PFC3B/PFC3BXL 搭載の Supervisor Engine 32 のみです。

ここでは、Port ACL（PACL; ポート ACL）について説明します。

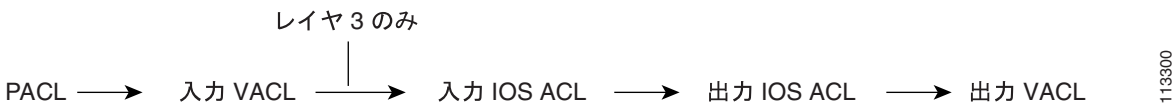
PACL 設定の概要

Release 8.3(1) より前のソフトウェア リリースでは、VACL および Cisco IOS ACL という 2 種類のアクセス リストのみがありました。VACL はレイヤ 2 およびレイヤ 3 転送トラフィックに適用されましたが、Cisco IOS ACL はレイヤ 3 転送パケットにのみ適用されました。いずれのタイプのアクセス リストも VLAN に適用され、パケット ヘッダー情報に基づいてトラフィックをフィルタリングしていました。

Release 8.3(1) には、PACL という追加のアクセス リスト タイプがあります。PACL は、物理ポートにマッピングされるアクセス リストです（通常、VLAN は複数の物理ポートで構成されます）。PACL では、さらに粒度を上げて特定の物理ポート上のトラフィックをフィルタリングします。VACL と同様に、PACL はレイヤ 2 およびレイヤ 3 転送パケットに適用されます。

図 15-9 に、アクセス リストのタイプ間の論理関係を示します。PACL は、まず物理ポートの着信パケットに適用されます。パケットが PACL によって許可されると、関連する入力 VLAN に適用されている VACL によってフィルタリングされます。パケットがレイヤ 3 で転送されて VACL によって許可される場合、同じ VLAN の Cisco IOS ACL でフィルタリングされます。出力方向については、同じ処理が逆方向で行われます。ただし、現在出力 PACL についてはハードウェアのサポートがありません。

図 15-9　アクセス リストのタイプ間の論理関係



PACL には、ポート単位で設定可能な 3 種類の操作モードがあります。

- ポートベース ― PACL が既存の VACL および Cisco IOS ACL を上書きします。このモードでは、Context-Based Access Control（CBAC; コンテキスト ベースのアクセス制御）および NAT などの機能は、物理ポートで機能しません。
- VLAN ベース ― VACL および Cisco IOS ACL が PACL を上書きします。
- マージ ― このモードでは、入力 PACL、VACL、および Cisco IOS ACL が、図 15-9 に示す論理シリアル モデルでマージされます。

ACL がポートにマッピングされていない場合、ポートは内部で VLAN ベース モードに戻ります。

ポートがマージ モードである場合を除き、PACL をトランキング ポートに設定できます。トランキング ポートが独自の ACL を持つ複数の VLAN を設定できるために、このような制限があります。VLAN x 用の VACL を、VLAN y がタグ付けされたパケットに適用する方法は誤りです。PFC3A はポート /VLAN ペアに基づいて検索ができないため、マージ モードで PACL をポートにマッピングできません。

(注)　PACL を作成するための CLI 構文は、VACL のものと同じです。ポートにマッピングされた ACL のインスタンスを PACL といいます。VLAN にマッピングされた ACL のインスタンスを VACL といいます。同じ ACL をポートと VLAN の両方にマッピングできます。VACL と同様に、PACL はすべてのプロトコル タイプでサポートされます。

PACL 設定時の注意事項

ここでは、PACL の設定時の注意事項について説明します。

PACL の VACL および Cisco IOS ACL との相互作用

ここでは、PACL の VACL および Cisco IOS ACL との相互作用における注意事項について説明します。

- ポートがポートベース モードに設定されている場合に、PACL は VACL および Cisco IOS ACL の両方を上書きします。この規則の例外の 1 つとして、パケットが MSFC によってソフトウェアで転送される場合があります。パケットは、PACL モードに関係なく適用された入力 Cisco IOS ACL を取得します。パケットがソフトウェアで転送される例として、次の 2 つがあります。
  - （ロギングや NAT などの機能により）出力ブリッジングされたパケット
  - IP オプションが設定されているパケット

  MSFC は、検出されたパケットに入力および出力 Cisco IOS ACL を再適用します。レイヤ 3 ハードウェアおよびソフトウェア転送パケットに対する PACL 上書きモードは、Cisco IOS ACL とは異なります。
- PACL がキャプチャを許可するように設定されていて VACL が同じパケットを拒否するように設定されている場合、マージ結果は設定誤りとなります。このような場合、PACL が [merge disabled] 状態になります。

EtherChannel および PACL の相互作用

ここでは、EtherChannel および PACL の相互作用における注意事項について説明します。

- 異なる PACL 設定を持つポートは、ポート チャネルを形成できません。ポート チャネルを形成するには、ポートには同じ PACL モード（ポートベース、VLAN ベース、またはマージ）および同じ ACL 名がなければなりません。

- EtherChannel のポートをポートベース ACL から VLAN ベース ACL に変更した場合、そのチャネル内のすべてのポートが VLAN ベース ACL モードに変更されます。
- あるポートの設定変更は、チャネル内のすべてのポートに影響します。あるチャネルに属するポートに ACL をマッピングすると、チャネルに関連付けられた論理ポートを含むチャネル内のすべてのポートにもマッピングされます。すべての物理ポートへのマッピングは、ポートチャネルが破壊されたあとでもハードウェアおよび NVRAM 内に残ります。論理ポートへのマッピングのみが削除されます。
- 新しい PACL が EtherChannel 内のあるポートに適用された場合、チャネル内のすべてのポートが新しい ACL マップを使用するように設定されます。

ダイナミック ACL（マージ モードにのみ適用）

ダイナミック ACL は VLAN ベースで、CBAC および IGMP の 2 つの機能によって使用されます。マージ モードは、ダイナミック ACL と PACL とのマージを*サポートしません*。マージ モードでは、次のような設定はできません。

- 対応する VLAN にダイナミック ACL がマッピングされているポートに PACL を適用しようとすること。
- 構成ポートの 1 つに PACL がインストールされている VLAN にダイナミック ACL を適用しようとすること。ダイナミック ACL は正常にマッピングされますが、矛盾のあるポートが [merge disable] モードになります。ダイナミック ACL が削除されたあとにポートが再びアクティブになります。

トランキング モード（マージ モードにのみ適用）

マージ モードの PACL は、トランキング ポートと互換性がありません。ポートをマージ モードに設定するには、ポートのトランキング モードを **off** に設定する必要があります。逆に言うと、マージ モードのポートはトランキング モードに変更できません。

補助 VLAN（マージ モードにのみ適用）

補助 VLAN がイネーブルのポートにマージ モードを設定できません。逆に言うと、補助 VLAN がイネーブルのポートをマージ モードに変更できません。

プライベート VLAN（マージ モードにのみ適用）

VACL をプライマリまたはセカンダリ プライベート VLAN にマッピングできます。対照的に、Cisco IOS ACL はプライマリ VLAN にしかマッピングできません。プライマリ VLAN にマッピングされる入力 Cisco IOS ACL は、すべての対応するセカンダリ VLAN にマッピングされ、プライマリ VLAN にはマッピングされません。プライマリ VLAN にマッピングされる出力 Cisco IOS ACL は、プライマリ VLAN にマッピングされます。

プライベート VLAN の入力ルックアップは、セカンダリ VLAN でのみ実行されます。マージ モードでは、PACL はセカンダリ VLAN に適用されている入力 VACL および Cisco IOS ACL とマージされます。

ポート VLAN アソシエーション変更（マージ モードにのみ適用）

ポート VLAN アソシエーション変更は、すべての場合に適用されます。ただし、ポートがマージ モードに設定されている場合、ポート VLAN アソシエーションでの変更によりマージ障害が発生する場合があります。そのような場合、ポートは [merge disable] モードになります。

PACL のマッピングを解除したあとに再度マッピングするか、Cisco IOS ACL が自動的に再マージをトリガします。次に、ポート 3/1 が VLAN 1 に関連付けられたあとに VLAN 2 に関連付けられる例を示します。

```
Console> (enable) set port security-acl 3/1 merge
ACL interface is set to merge mode for port(s) 3/1.

Console> (enable) set security acl map ipacl1 3/1
ACL ipacl1 is successfully mapped to port(s) 3/1.

Console> (enable) set security acl map ipacl2 1
ACL ipacl2 is successfully mapped to VLAN 1.

Console> (enable) set security acl map ipacl3 2
ACL ipacl3 is successfully mapped to VLAN 2.

Console> (enable) set vlan 2 3/1
2003 Sep 05 22:34:50 %ACL-3-PACLMERGEFAILED:Failed to merge Security ACLs on Port(s)
3/1 with Vlan 2.
VLAN 2 modified.
VLAN 1 modified.
VLAN  Mod/Ports
---- ----------------------
2     3/1

Console> (enable) show port security-acl 3/1
Port  Interface Type Interface Type Interface Merge Status
      config         runtime        runtime
----- -------------- -------------- ----------------------
 3/1           merge          merge      (VLAN=2) disabled



Config:
Port  ACL name                          Type
----- --------------------------------- ----
 3/1  ipacl1                            IP

Runtime:
Port  ACL name                          Type
----- --------------------------------- ----
No ACL is mapped to port 3/1.


dhcp-snooping:
Port     Trust     Source-Guard    Source-Guarded IP Addresses
----- -----------  ------------    ---------------------------
 3/1   untrusted      disabled

Console> (enable) show security acl map runtime 1
Vlan ACL name                          Type
---- --------------------------------- ----
   1 ipacl2                            IP

Console> (enable) show security acl map runtime 2
Vlan ACL name                          Type
---- --------------------------------- ----
   2 ipacl3                            IP
Console> (enable)
```

OIR の概要

モジュールを取り外したりリセットしたりする場合、モジュールに添付されている PACL も（ハードウェアにプログラミングされている）実行コンフィギュレーションおよび（NVRAM に保存されている）NVRAM コンフィギュレーションから削除されます。コンフィギュレーションは NVRAM に保存されますが、表示されません。モジュールを挿入したりオンラインにした場合、コンフィギュレーションは NVRAM（またはテキスト コンフィギュレーション ファイル）から再び読み込まれて実行コンフィギュレーションに再マッピングされます。

ポートのイネーブルまたはディセーブルは、ポートがマージ モードである場合を除いて、ACL マッピングまたはセキュリティ ACL モードに影響しません。マージ モードでは、VLAN でディセーブルになったり VLAN から消去されたポートは、ポートに関連した VLAN が使用できなくなりポートでパケットの転送や他の VLAN とのマージができなくなるため、[merge disable] ステートになります。

CLI での PACL の設定

ここでは、Catalyst 6500 シリーズ スイッチ上で PACL を作成し、アクティブにする手順について説明します。

PACL モードの指定

デフォルトの PACL モードは VLAN ベースであり、既存の VACL 設定はアクティブのままです。

PACL モードを指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
PACL モードを指定します。	**set port security-acl** *mod/ports..*[**port-based** | **vlan-based** | **merge**]

次に、ポート 3/1 に PACL を指定する例を示します。

```
Console> (enable) set port security-acl 3/1 port-based
Warning: Vlan-based ACL features will be disabled on port(s) 3/1.
ACL interface is set to port-based mode for port(s) 3/1.

Console> (enable) set port security-acl 3/1 merge
ACL interface is set to merge mode for port(s) 3/1.

Console> (enable) set port security-acl 3/1 vlan-based
ACL interface is set to vlan-based mode for port(s) 3/1.
Console> (enable)
```

次に、トランク ポート（ポート 3/1）をマージ モードにしようとした場合の応答の例を示します。

```
Console> (enable) set port security-acl 3/1-4 merge
ACL interface cannot be in merge mode on multi-vlan access port 3/1.
ACL interface is set to merge mode for port(s) 3/2.
ACL interface is set to merge mode for port(s) 3/3.
ACL interface is set to merge mode for port(s) 3/4.
```

PACL 情報の表示

show port security-acl *mod/port* コマンドは、指定したポートの PACL 情報を表示します。Config フィールドでは、NVRAM に保存されているものが表示されます。Runtime フィールドでは、実際にハードウェアにプログラミングされたものが表示されます。また、次のようなマージ操作のステータスも表示されます。

- active ― ポートに PACL が設定されており、VLAN と正常にマージされています。
- inactive ― ポートに設定されている PACL はありません。
- disabled ― ポートに PACL が設定されていますが、(いくつかの理由で)マージに失敗しました。

show port security-acl コマンドも、ポートがマージするように設定されている VLAN を表示します。

PACL 情報を表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
PACL 情報を表示します。	**show port security-acl** *mod/port*

次に、ポート 3/1 の PACL 情報を表示する例を示します。

```
Console> (enable) show port security-acl 3/1
Port  Interface Type Interface Type Interface Merge Status
      config         runtime        runtime
----- -------------- -------------- ----------------------
 3/1      port-based     port-based          not applicable

Config:
Port  ACL name                           Type
----- ---------------------------------- ----
 3/1  ipacl1                             IP

Runtime:
Port  ACL name                           Type
----- ---------------------------------- ----
No ACL is mapped to port 3/1.


dhcp-snooping:
Port     Trust     Source-Guard    Source-Guarded IP Addresses
-----  ----------  ------------    ---------------------------
 3/1   untrusted      disabled

Console> (enable)
```

ポートまたは VLAN への ACL のマッピング

ポートが VLAN ベース モードの場合でも ACL をポートにマッピングできます。このような場合、コンフィギュレーションは NVRAM にコミットされて、あとでポートがポートベース モードまたはマージ モードに変更される際に、ハードウェアに復元されます。この機能は QoS と似ています。

ACL の VLAN へのマッピングでは、次のような操作が実行されます。

1. ACL が VLAN にマッピングされます。
2. マージ モードであるすべての構成ポートとともにマージが自動的にトリガされます。

(1) が失敗した場合、操作が失敗して Syslog メッセージが生成されます。(2) の場合、VACL とのマージに失敗したポートに対して Syslog が生成されます。これらのポートは一時的に VLAN ベース モードになります。ポートがマージに失敗した場合、**show port security-acl** *mod/port* コマンドを通じて表示されるマージのステータスは [merge disabled] になります。[merge disabled] ステータスの例については、「PACL の設定例」(p.15-78) の「例 6」を参照してください。

ポートまたは VLAN に ACL をマッピングするには、イネーブル モードで次の作業を行います。

作業	コマンド
ポートまたは VLAN に ACL をマッピングします。	**set security acl map** *acl_name* [*mod/ports* | *vlans*]

次に、ポート 3/1 に ACL をマッピングする例を示します。

```
Console> (enable) set security acl map ipacl1 3/1
Mapping in progress.
ACL ipacl1 is successfully mapped to port(s) 3/1.

Console> (enable) set port security-acl 3/1 vlan-based
ACL interface is set to vlan-based mode for port(s) 3/1.

Console> (enable) set security acl map ipacl1 3/1
Port 3/1 is set to vlan-based mode, config is saved in Nvram.
Config will be applied when the port is set to port-based/merge mode.
Console> (enable)
```

ACL マッピング情報の表示

show security acl map コマンドは、次のように、ポート マッピングを表示するように拡張されました。

- 設定およびランタイム マッピングを表示するために必須キーワード（**config** および **runtime**）が追加されました。
- 設定された VACL および PACL を表示するために、任意キーワード（**all-vlans** および **all-ports**）が追加されました。

ACL マッピング情報を表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
ACL マッピング情報を表示します。	**show security acl map** [**config** | **runtime**] [*acl_name* | *mod_num*/*port_num* | *vlan* | **all** | **all-vlans** | **all-ports**]

次に、ACL マッピング情報を表示する例を示します。

```
Console> (enable) show security acl map config all
ACL Name                        Type Ports/Vlans
------------------------------- ---- --------------
ipacl1                          IP   11
ipacl2                          IP   3/1

Console> (enable) show security acl map config all-ports
ACL Name                        Type Ports
------------------------------- ---- --------------
ipacl2                          IP   3/1

Console> (enable) show security acl map runtime 3/1
Port  ACL name                         Type
----- ------------------------------- ----
3 / 1 ipacl1                          IP
Console> (enable)
```

EtherChannel の ACL 情報の表示

ポート チャネル上に PACL マッピングを表示するために、**show channel** コマンドが拡張されました。*type* に対して、*security-acl* を指定できます。

EtherChannel の ACL 情報を表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
EtherChannel の ACL 情報を表示します。	**show port channel** [**all** | *mod*[/*port*]] {**info** [*type*]}

次に、EtherChannel の ACL 情報を表示する例を示します。

```
Console> (enable) show port channel 3/40 info security-acl
Port  ACL-Interface Type
----- ------------------
 3/37 port-based
 3/38 port-based

Port  ACL name                         Type
----- -------------------------------- ------
 3/37 ipacl1                           IP
 3/38 ipacl1                           IP
Console> (enable)
```

PACL の設定例

ここでは、PACL の設定例を紹介します。

例 1

次に、ポートが VLAN ベース モードの場合に ACL をポートにマッピングする例を示します。

```
Console> (enable) set port security-acl 3/1 vlan-based
ACL interface is set to vlan-based mode for port(s) 3/1.

Console> (enable) set security acl map ipacl1 3/1
Port 3/1 is set to vlan-based mode, config is saved in Nvram.
Config will be applied when the port is set to port-based/merge.

Console> (enable) show security acl map config 3/1
Port  ACL name                         Type
----- -------------------------------- ----
 3/1  ipacl1                           IP

Console> (enable) show security acl map runtime 3/1
Port  ACL name                         Type
----- -------------------------------- ----
No ACL mapped to port 3/1.

Console> (enable) set port security-acl 3/1 port-based
Warning: Vlan-based ACL features will be disabled on port(s) 3/1.
ACL interface is set to port-based mode for port(s) 3/1.

Console> (enable) show security acl map config 3/1
Port  ACL name                         Type
----- -------------------------------- ----
 3/1  ipacl1                           IP

Console> (enable) show security acl map runtime 3/1
Port  ACL name                         Type
----- -------------------------------- ----
 3/1  ipacl1                           IP
Console> (enable)
```

例 2

次に、ACL マッピング エラーによりセキュリティ ACL モードが変更された場合に障害が発生する例を示します。この例では、ACL が NVRAM にのみマッピングされてハードウェアにはマッピングされません。

```
Console> (enable) set port security-acl 3/1 vlan-based
ACL interface is set to vlan-based mode for port(s) 3/1.

Console> (enable) set security acl map ipacl1 3/1
Port 3/1 is set to vlan-based mode, config is saved in Nvram.
Config will be applied when the port is set to port-based/merge.

Console> (enable) set port security-acl 3/1 port-based
Warning: Vlan-based ACL features will be disabled on port(s) 3/1.
ACL interface is set to port-based mode for port(s) 3/1
2003 Sep 05 22:34:50 %ACL-3-TCAMFULL:Acl engine TCAM table is full
2003 Sep 05 22:34:50 %ACL-3-PACLMAPCOMMITFAIL:Failed to Map Security ACL ipacl1 to
Port 3/1

Console> (enable) show security acl map config 3/1
Port  ACL name                         Type
----- -------------------------------- ----
 3/1  ipacl1                           IP

Console> (enable) show security acl map runtime 3/1
Port  ACL name                         Type
----- -------------------------------- ----
No ACL is mapped to port 3/1.


Console> (enable) show port security-acl 3/1
Port  Interface Type Interface Type Interface Merge Status
      config         runtime        runtime
----- -------------- -------------- ----------------------
 3/1      port-based     port-based         not applicable

Config:
Port  ACL name                         Type
----- -------------------------------- ----
 3/1  ipacl1                           IP

Runtime:
Port  ACL name                         Type
----- -------------------------------- ----
No ACL is mapped to port 3/1.


dhcp-snooping:
Port     Trust     Source-Guard    Source-Guarded IP Addresses
----- -----------  ------------    ---------------------------
 3/1   untrusted      disabled

Console> (enable)
```

例 3

次に、ポートがマージ モードに設定されているものの ACL にマッピングされない例を示します。

```
Console> (enable) set port security-acl 3/1 merge
ACL interface is set to merge mode for port(s) 3/1.

Console> (enable) show port security-acl 3/1
Port  Interface Type Interface Type Interface Merge Status
      config         runtime        runtime
----- -------------- -------------- ----------------------
 3/1           merge          merge      (VLAN 5) inactive

Config:
Port  ACL name                          Type
----- --------------------------------- ----
No ACL is mapped to port 3/1.

Runtime:
Port  ACL name                          Type
----- --------------------------------- ----
No ACL is mapped to port 3/1.


dhcp-snooping:
Port     Trust     Source-Guard    Source-Guarded IP Addresses
-----  -----------  ------------    ---------------------------
 3/1   untrusted      disabled

Console> (enable) set security acl map ipacl1 3/1
ACL ipacl1 is successfully mapped to port(s) 3/1.

Console> (enable) show port security-acl 3/1
Port  Interface Type Interface Type Interface Merge Status
      config         runtime        runtime
----- -------------- -------------- ----------------------
 3/1           merge          merge        (VLAN 5) active

Config:
Port  ACL name                          Type
----- --------------------------------- ----
 3/1  ipacl1                            IP

Runtime:
Port  ACL name                          Type
----- --------------------------------- ----
 3/1  ipacl1                            IP


dhcp-snooping:
Port     Trust     Source-Guard    Source-Guarded IP Addresses
-----  -----------  ------------    ---------------------------
 3/1   untrusted      disabled

Console> (enable)
```

例 4

次に、ACL をポートにマッピングする際に発生する障害の例を示します。この場合、設定は保存されません。

```
Console> (enable) set port security-acl 3/1 merge
ACL interface is set to merge for port(s) 3/1.

Console> (enable) set security acl map ipacl1 3/1
Mapping in progress.
2003 Oct 01 19:44:31 %ACL-3-PACLMAPCOMMITFAIL:Failed to Map Security ACL ipacl1 to
Port 3/15
Failed to attach ACL ipacl1 to port(s) 3/1.

Console> (enable) show security acl map config 3/1
Port  ACL name                         Type
----- -------------------------------- ----
No ACL is mapped to port 3/1.

Console> (enable) show security acl map runtime 3/1
Port  ACL name                         Type
----- -------------------------------- ----
No ACL is mapped to port 3/1.
Console> (enable)
```

例 5

次に、ポートベース モードからマージ モードに変更する際に障害が発生した場合に、モードを変更できない例を示します。

```
Console> (enable) set port security-acl 3/1 port-based
ACL interface is set to port-based for port(s) 3/1.

Console> (enable) set security acl map ipacl1 3/1
ACL ipacl1 is successfully mapped to port 3/1.

Console> (enable) show security acl map config 3/1
Port  ACL name                         Type
----- -------------------------------- ----
 3/1  ipacl1                           IP

Console> (enable) show security acl map runtime 3/1
Port  ACL name                         Type
----- -------------------------------- ----
 3/1  ipacl1                           IP

Console> (enable) set port security-acl 3/1 merge
Failed to set interface to merge mode for port(s) 3/1.
2003 Oct 01 19:53:01 %ACL-3-TCAMFULL:Acl engine TCAM table is full
Console> (enable)
```

例 6

次に、VACL とのマージに失敗したポートに対して Syslog が生成され、これらのポートが一時的に VLAN ベース モードになる例を示します。マージ ステータスは [merge disabled] です。

```
Console> (enable) show port security-acl 3/1
Port  Interface Type Interface Type Interface Merge Status
      config         runtime        runtime
----- -------------- -------------- ----------------------
 3/1           merge          merge        (VLAN=5) active

Config:
Port  ACL name                          Type
----- --------------------------------- ----
 3/1  ipacl1                            IP
 3/1  macacl1                           MAC

Runtime:
Port  ACL name                          Type
----- --------------------------------- ----
 3/1  ipacl1                            IP
 3/1  macacl1                           MAC


dhcp-snooping:
Port     Trust     Source-Guard    Source-Guarded IP Addresses
-----  -----------  ------------    ---------------------------
 3/1   untrusted      disabled

Console> (enable) set security acl map ipacl2 5
ACL ipacl2 is successfully mapped to VLAN 5.
2003 Oct 01 20:01:04 %ACL-3-MERGEFAILED:Failed to merge Security ACLs on ports(s)
3/1-4 with VLAN 5
2003 Oct 01 20:01:04 %ACL-3-PACLSMERGEDFORVLAN:Merge completed for all ports on Vlan 5

Console> (enable) show port security-acl 3/1
Port  Interface Type Interface Type Interface Merge Status
      config         runtime        runtime
----- -------------- -------------- ----------------------
 3/1           merge          merge      (VLAN=5) disabled
Config:
Port  ACL name                          Type
----- --------------------------------- ----
 3/1  ipacl1                            IP
 3/1  macacl1                           MAC

Runtime:
Port  ACL name                          Type
----- --------------------------------- ----
 3/1  ipacl1                            IP
 3/1  macacl1                           MAC


dhcp-snooping:
Port     Trust     Source-Guard    Source-Guarded IP Addresses
-----  -----------  ------------    ---------------------------
 3/1   untrusted      disabled

Console> (enable)
```

例 7

次に、例 6 の続きで、VACL または PACL をマッピングまたはマッピング解除して障害ステートから回復する例を示します。この例では、MAC PACL を切り離すことである種の Ternary CAM（TCAM）リソースを解除して、マージを継続できるようにします。Syslog は、マージが再びイネーブルになると生成されます。

```
Console> (enable) clear security acl map macacl1
Map deletion in progress.
Successfully cleared mapping between ACL macacl1 and port 3/1.
2003 Oct 01 20:01:04 %ACL-3-PACLMERGED:Merged Security ACLs on port(s) 3/1

Console> (enable) show port security-acl 3/1
Port  Interface Type Interface Type Interface Merge Status
      config         runtime        runtime
----- -------------- -------------- ----------------------
 3/1           merge          merge        (VLAN=5) active

Config:
Port  ACL name                         Type
----- -------------------------------- ----
 3/1  ipacl1                           IP

Runtime:
Port  ACL name                         Type
----- -------------------------------- ----
 3/1  ipacl1                           IP


dhcp-snooping:
Port     Trust     Source-Guard    Source-Guarded IP Addresses
-----  ----------  ------------    --------------------------
 3/1   untrusted      disabled

Console> (enable)
```

ACL 統計情報の設定

ここでは、ACL 統計情報を設定する手順について説明します。

ACL 統計情報の概要

set security acl コマンド セットに **statistics** キーワードを指定すると、ACE または ACL（VACL および PACL）に関する統計情報が保存されます。ACL 統計情報はデフォルトでディセーブルです。ACL 単位、VLAN 単位、ACE 単位でイネーブルにできます。

ACL は TCAM でプログラミングされる前に、ACL コンパイラに渡されます。ACL コンパイラは ACL の ACE 数を最適化し、マスクをできるだけ共有することにより、使用される TCAM マスク数を削減します。インターフェイス上に ACL を介して設定された機能 / ポリシーが複数存在する場合は、これらの ACL がマージされ、マージされた ACL が最適化されます。最適化された ACL は、元の ACL と論理的に同等です。

ACL の最適化では、冗長 ACE の削除、ACE のマージ、および ACE の並べ替えが行われます。冗長 ACE を削除して、ACE をマージすると、TCAM エントリ数が削減されます。ACE を並べ替えると、TCAM エントリ数および TCAM マスク数が削減されます。

ACL 統計情報は、最適化された ACL を構成する ACE のカウンタから取得されます。これらの ACE は、マッピング機能によって、元のユーザ定義 ACL に対応する ACE にマッピングされます。

（注） PFC2 および PFC3A では、カウンタはソフトウェア サンプリングに基づいて行われるため、不正確です。PFC3B/PFC3BXL では、ハードウェア カウンタを使用して、正確な統計情報を提供します。PFC2/PFC3A では、カウンタは 300 ms のウィンドウ中に特定の ACE と一致したかどうかを報告しますが、エントリに一致したトラフィック数は示しません。たとえば、1000 パケット / 秒と 10 パケット / 秒の 2 つのフローがある場合、PFC2/PFC3A では両方のフローが同じ結果を戻します。PFC3B/PFC3BXL 以降の PFC には、このような制限がありません。

（注） ACL をアクティブ / スタンバイ TCAM に同時にプログラミングすることはできないため、アクティブ スーパバイザ エンジンとスタンバイ スーパバイザ エンジン間で ACL 統計情報が異なることがあります。ただし、TCAM のプログラミング後に、トラフィックと TCAM との一致が開始すると、ACL 統計情報が同じになります。

CLI からの ACL 統計情報の設定

ここでは、次の手順について説明します。

ACL 単位の ACL 統計情報のイネーブル化

(注)　ARP ACE エントリは ACL マージ後に追加され、常に TCAM リスト内の最初の ACE になるため、ARP エントリ統計情報収集は常にイネーブルです。

ACL 単位でまたはすべての ACL に対して集約 ACL 統計情報をイネーブルにするには、**set security acl statistics** {*acl_name* | **all**} コマンドを入力します。集約統計情報モードでは、指定された ACL 内のすべての ACE に対して統計情報がイネーブルです。このコマンドが有効になるのは、**commit** コマンドを入力して、すべての ACE を NVRAM にコミットした場合のみです。

(注)　**set security acl statistics** {*acl_name* | **all**} コマンドは、ACE 単位コマンドの **set security acl ip/mac** *acl_name* … [**statistics**] を上書きします。

(注)　集約統計情報モードではマージ最適化がディセーブルになり、多数の ACE が使用されることがあります。場合によっては、集約統計情報モードをイネーブルにしたあとで、TCAM に導入済みの ACL が TCAM に収まらなくなることがあります。

集約 ACL 統計情報を ACL 単位でイネーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
集約 ACL 統計情報を ACL 単位でイネーブルにします。	**set security acl statistics** {*acl_name* | **all**}

次に、集約 ACL 統計情報を ACL 単位でイネーブルにする例を示します。

```
Console> (enable) set security acl statistics ACL1
ACL1 editbuffer modified. Use 'commit' command to save changes.
Console> (enable) commit security acl ACL1
ACL commit in progress.

ACL 'ACL1' successfully committed.
Console> (enable)

Console> (enable) show security acl info ACL1
set security acl ip ACL1 statistics
-------------------------------------------------
arp permit
1. permit ip any any
Console> (enable)
```

VLAN 単位の ACL 統計情報のイネーブル化

ACL 統計情報を VLAN 単位でイネーブルにするには、**set security acl map** *acl-name* {*vlan*/*mod_port*} [**statistics enable | disable**] コマンドを入力します。

(注)　VLAN モードでは、ラベル共有がディセーブルです。たとえば、特定の ACL が 10 個の VLAN にマッピングされている場合に、そのうちの 1 つの VLAN で VLAN 単位の統計情報をイネーブルにすると、9 つの VLAN でラベルが共有されます。VLAN 統計情報をイネーブルにした VLAN では別のラベルが使用されますが、これは統計情報がイネーブルであることを意味しません。マッピングした ACL に関して統計情報がイネーブルでない場合（ACE 単位または ACL 単位）、ARP パケットを除いて、統計情報は表示されません。

VLAN 上で VLAN 単位統計情報がイネーブルの場合は、同じ VLAN に設定されたこれ以降のマップでも、VLAN 単位統計情報がイネーブルになります。VLAN 上で VLAN 単位統計情報がディセーブルの場合は、同じ VLAN に設定された以前のマップでも VLAN 単位統計情報がディセーブルになります。

たとえば、**set security acl map ip1 1 statistics enable** コマンドを入力して、そのあとに **set security acl map mac1 1** コマンドを入力した場合、mac1 ACL でも VLAN 単位の統計情報はイネーブルになります。

set security acl map ip1 1 statistics enable コマンドを入力して、そのあとに **set security acl map mac1 1 statistics disable** コマンドを入力した場合は、ip1 ACL でも VLAN 単位統計情報がディセーブルになります。

ACL 統計情報を VLAN 単位でイネーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
ACL 統計情報を VLAN 単位でイネーブルにします。	**set security acl map** *acl-name* {*vlan*/*mod_port*} [**statistics enable	disable**]
設定を表示します。	**show security acl**

次に、ACL 統計情報を VLAN 単位でイネーブルにする例を示します。

```
Console> (enable) set security acl map ACL1 1 statistics enable
Mapping in progress.

ACL ACL1 successfully mapped to VLAN 1.
Console> (enable)

Console> (enable) show security acl info ACL1
set security acl ip ACL1 statistics
---------------------------------------------------
arp permit
1. permit ip any any
Console> (enable)
```

ACE 単位の ACL 統計情報のイネーブル化

ACL 統計情報を ACE 単位でイネーブルにするには、**set security acl ip/mac** *acl_name* … [**statistics**] コマンドを入力します。このオプションを使用すると、ACL 統計情報がイネーブルでない場合にも、設定された ACE に関する統計情報を収集できます。このコマンドが有効になるのは、**commit** コマンドを入力して、すべての ACE を NVRAM にコミットした場合のみです。

ACL 統計情報を ACE 単位でイネーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
ACL 統計情報を ACE 単位でイネーブルにします。	**set security acl ip/mac** *acl_name* … [**statistics**]

次に、ACL 統計情報を ACE 単位でイネーブルにする例を示します。

```
Console> (enable) set security acl ip ACL1 permit ip any any statistics
ACL1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable) commit security acl ACL1
ACL commit in progress.

ACL 'ACL1' successfully committed.
Console> (enable)

Console> (enable) show security acl info ACL1
set security acl ip ACL1 statistics
--------------------------------------------------
arp permit
1. permit ip any any
2. permit ip any any statistics
Console> (enable)
```

ACL 統計情報の消去

ACL 統計情報を消去するには、ここに記載されたコマンドを使用します。

- **clear security acl statistics** *acl_name*

  指定された ACL のすべての ACE に対して、統計情報収集をディセーブルにします。このコマンドが有効なのは、ACL 単位で設定された ACL 統計情報のみです。VLAN 単位または ACE 単位で設定された ACL 統計情報には、このコマンドは無効です。このコマンドが有効になるのは、**commit** コマンドを入力して、すべての ACE を NVRAM にコミットした場合のみです。

  次に例を示します。

  ```
  Console> (enable) clear security acl statistics ACL1
  ACL1 editbuffer modified. Use 'commit' command to save changes.
  Console> (enable) commit security acl ACL1
  ACL commit in progress.

  ACL 'ACL1' successfully committed.
  Console> (enable)
  ```

- **clear security acl counters**

  すべての統計情報カウンタを消去します。

  次に例を示します。

  ```
  Console> (enable) clear security acl counters
  Operation Successful.
  Console> (enable)
  ```

ACL 統計情報の表示

ACL 統計情報を表示するには、ここに記載されたコマンドを使用します。

- **show security acl info** *acl_name* [**statistics** [*ace_index*]]

  指定された ACL の統計情報を表示します。*ace_index* は ACL リスト（コミットされた ACL）のインデックスです。

  次に例を示します。

```
Console> (enable) show security acl info ACL1 statistics
Vlan: 1
set security acl ip ACL1 statistics
------------------------------------------------
arp permit in: 132 out: 132
1. permit ip any any
2. permit ip any any statistics  in: 0 out: 0

Console> (enable)
```

- **show security acl tcam interface** *vlan*

  指定された VLAN に関する TCAM の詳細を表示します。

  次に例を示します。

```
Console> (enable) show security acl tcam interface 1
Input
0. permit arp (matches 45745)
1. deny (l3) tcp any any fragment (matches 0)
2. deny (l3) ip host 21.0.0.130 any (matches 0)
3. deny (l3) udp 1.2.2.0 0.0.0.255 any (matches 0)
4. deny (l3) tcp any any 2001 (matches 0)
5. deny (l3) ip host 21.0.0.128 any (matches 0)
6. deny ip any any (matches 3)


Output
0. permit arp (matches 0)
1. deny (l3) tcp any any fragment (matches 0)
2. deny (l3) ip host 21.0.0.130 any (matches 0)
3. deny (l3) udp 1.2.2.0 0.0.0.255 any (matches 0)
4. deny (l3) tcp any any 2001 (matches 0)
5. deny (l3) ip host 21.0.0.128 any (matches 0)
6. deny (l3) ip any any (matches 0)
Console> (enable)
```

  フィールドの説明は次のとおりです。

  - deny (l3)：レイヤ 3 トラフィックが拒否され、レイヤ 2 トラフィックは許可されます。
  - redirect (l3)：レイヤ 3 トラフィックだけがリダイレクトされます。
  - bridge：このエントリに一致したトラフィックがブリッジされます。
  - Redirect (adj)：隣接情報によってトラフィックが書き替えられます。

- **show security acl** および **show security acl map** *acl_name*

  これらのコマンドに、特定の ACL または VLAN に対してイネーブルにされた統計情報のタイプを表示する新しいフィールドが追加されています。

次に例を示します。

```
Console> (enable) show security acl
Information in the bracket.
   Disable - statistics are not enabled per ACL
   Enable - stats are enabled per ACL
   The number shows the VLANs where per-vlan stattistics are enabled
ACL                              Type VLANS (Statistics)
-------------------------------  ---- ----------------
ip1                              IP   2-9    (2-3 Enable)
ip2                              IP   10     (Disable)
ip3                              IP   11     (Disable)
Console> (enable)
```

フィールドの説明は次のとおりです。

- Disable：ACL で統計情報がディセーブルです。
- Enable：ACL で統計情報がイネーブルです。
- 番号は VLAN 単位の統計情報がイネーブルになっている VLAN を示します（例の [2-3] など）。

CRAM の設定

Compression and Reordering of the ACL Mask（CRAM）機能は、複数の ACL にわたってマスク使用率を最適化します。この最適化によりマスク共有が促進され、TCAM の使用効率が高まり、TCAM 内にさらに多くの ACL をプログラミングできます。

TCAM はハードウェアに ACL を実装する場合に使用されます。8 つの値エントリで 1 つのマスクエントリが共有されます。ACL をプログラミングする場合に、TCAM が一杯であると、エラーが表示され、TCAM ハードウェアに新規 ACL をプログラミングできなくなります。この問題は通常、TCAM マスクの不足が原因で発生します。

CRAM は 2 つのモードで実行できます。手動モードでは、この機能を必要に応じて実行します。自動モードでは、TCAM が一杯となる例外状況が発生した場合に、この機能が実行されます。この機能が実行されると、新規のマスク順序が計算され、ACL ハードウェアがそれに応じてプログラミングされます。

（注） Release 8.4(1) では、CRAM はセキュリティ ACL でのみサポートされています。この機能は QoS ACL で有効ですが、QoS ACL 専用に実行することはできません。

CLI からの CRAM 機能の設定

（注） CRAM 機能を実行すると、ハードウェア プログラミング中に 0.5 秒未満の間、トラフィックが中断（拒否）されます。

ここでは、次の手順について説明します。

CRAM 機能のテスト実行のイネーブル化

ACL マスクの使用の有無を判別するには、**set security acl cram testrun** コマンドを入力します。このコマンドは単なる情報用です。ソフトウェア構造やハードウェア構造は変更されず、トラフィックは中断されません。

CRAM 機能のテスト実行をイネーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
CRAM 機能のテスト実行をイネーブルにします。	**set security acl cram testrun**

次に、CRAM 機能のテスト実行をイネーブルにする例を示します。

```
Console> (enable) set security acl cram testrun
CRAM execution in progress.

CRAM execution complete.
Current ACL storage mask usage 60.0%
ACL storage mask usage if CRAM is run is 41.0%
Console> (enable)
```

CRAM 機能の手動によるイネーブル化

CRAM 機能を手動でイネーブルにするには、**set security acl cram run** コマンドを入力します。

CRAM 機能を手動でイネーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
CRAM 機能を手動でイネーブルにします。	**set security acl cram run**

次に、手動で CRAM 機能をイネーブルにする例を示します。

```
Console> (enable) set security acl cram run
Traffic may be disrupted for some time while programming hardware. Agree (y/n)[n] ? y
CRAM execution in progress.

CRAM execution complete.
Previous ACL storage mask usage 60.0%
Current ACL storage mask usage 41.0%
Console> (enable)
```

CRAM 機能の自動実行のイネーブル化

CRAM 機能の自動実行をイネーブルにするには、**set security acl cram auto** [*nsec*] コマンドを入力します。自動実行がイネーブルの場合、この機能は TCAM が一杯になると自動的に実行されます。デフォルトのタイマー設定は 300 秒です。*nsec* は 60 ～ 3600 秒に指定できます。前回この機能を実行してから TCAM が変更されていない場合は、この機能が自動実行されません。

CRAM 機能の自動実行をイネーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
CRAM 機能の自動実行をイネーブルにします。	**set security acl cram auto** [*nsec*]

次に、CRAM 機能の自動実行をイネーブルにする例を示します。

```
Console> (enable) set security acl cram auto
Cram auto mode enabled. Timer is default =  300 seconds
Console> (enable)

Console> (enable) set security acl cram auto 1000
Cram auto mode enabled. Timer is 1000 seconds
Console> (enable)
```

CRAM 機能のステータス情報の表示

CRAM 機能のステータス情報を表示するには、**show security acl cram** コマンドを入力します。

CRAM 機能のステータス情報を表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
CRAM 機能のステータス情報を表示します。	**show security acl cram**

次に、CRAM 機能のステータス情報を表示する例を示します。

```
Console> (enable) show security acl cram
Cram auto mode is enabled. Timer is 300.
Cram last run on Fri Jun 18 2004, 10:06:29
Security ACL mask usage before: 0.17%
Security ACL mask usage after: 0.12%
Total number of cram executions = 2
Console> (enable)
```

CRAM 機能の自動モードのディセーブル化

CRAM の自動モードをディセーブルにするには、**clear security acl cram auto** コマンドを入力します。

CRAM の自動モードをディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
CRAM の自動モードをディセーブルにします。	**clear security acl cram auto**

次に、CRAM の自動モードをディセーブルにする例を示します。

```
Console> (enable) clear security acl cram auto
Cram auto mode disabled.
Console> (enable)
```

PBF の設定

Policy-Based Forwarding（PBF）機能は、PFC2 および PFC3A/PFC3B/PFC3BXL によってサポートされる VACL リダイレクションの拡張機能です。PBF が特に有効なのは、トランスペアレント ブリッジングに使用され、必要な VLAN 間通信の量が限られているフラットなレイヤ 2 ネットワークや、ブリッジング装置（サーバのロードバランシング装置など）が含まれていたり、ファイアウォールのロードバランシングが実行されていたりするサーバ ファームまたは Demilitarized Zone（DMZ; 非武装地帯）です。

(注) Release 7.5(1) 以降のソフトウェア リリースでは PBF 機能が拡張され、セキュリティ ACL と隣接情報の設定およびコミットのプロセスが簡略化されています。詳細は、「PBF 設定の拡張機能（Releases 7.5(1) 以降のソフトウェア リリース）」（p.15-105）を参照してください。

(注) Release 8.3(1) 以降のソフトウェア リリースではさらに PBF 機能が拡張され、セキュリティ ACL と隣接情報の設定およびコミットのプロセスが簡略化されています。詳細は、「PBF 設定の拡張機能（Releases 8.3(1) 以降のソフトウェア リリース）」（p.15-108）を参照してください。

(注) PBF は、IPX およびマルチキャスト トラフィックをサポートしていません。

(注) PBF は、802.1Q トンネル トラフィックでは機能しません。PBF はレイヤ 3 IP ユニキャスト トラフィックではサポートされていますが、レイヤ 2 トラフィックには適用されません。中間（PBF）スイッチでは、802.1Q トンネル トラフィックはすべてレイヤ 2 トラフィックとみなします。

(注) PBF は、接続したホスト上で設定が必要になる場合があります。ネットワークにルータが存在しない場合は、PBF に参加する各ホストに対して ARP テーブル エントリを静的に追加する必要があります。

ここでは、PBF について説明します。

PBF の機能概要

PBF の設定には、次の作業が必要です。

- PBF のイネーブル化と PFC2 または PFC3A/PFC3B/PFC3BXL 用 MAC アドレスの指定
- PBF のための VACL の設定
- PBF のための接続ホストの設定

PFC2 または PFC3A/PFC3B/PFC3BXL 用 MAC アドレスを指定することで PBF をイネーブルにできます。MAC アドレスは、デフォルト設定のものでもユーザ側で指定する MAC アドレスでもかまいません。パケットを送信する場合は、宛先 MAC アドレスは PFC2 または PFC3A/PFC3B/PFC3BXL MAC アドレスと同じでなければなりません。PFC2 または PFC3A/PFC3B/PFC3BXL は、パケットがレイヤ 3 のパケットであると認識する必要があります。認識しない場合は書き換え処理が行われません。パケットに PFC2 または PFC3A/PFC3B/PFC3BXL MAC アドレスが設定されないで送信された場合、PFC2 または PFC3A/PFC3B/PFC3BXL はこれらのパケットをレイヤ 2 パケットとして処理します。

PBF VACL は **set security acl** コマンドを使用して作成されます。PBF VACL は、PFC2 または PFC3A/PFC3B/PFC3BXL の隣接テーブル エントリとリダイレクト ACE を含みます。PBF に参加している両方の VLAN に対して VACL を設定する必要があります。送信元 VLAN からのパケットが PFC2 または PFC3A/PFC3B/PFC3BXL に着信し、PBF VACL に一致します。隣接テーブルに記入されている情報に基づいてパケット ヘッダーが書き換えられ（宛先 VLAN および送信元と宛先の MAC アドレス）、パケットは宛先 VLAN に転送されます。パケットは、隣接情報に対応付けられた VACL エントリに一致した場合にだけ、VLAN 間で転送されます。

（注） VACL は着信および発信トラフィックに適用されるので、PBF を使用する場合はすべての VACL を慎重に設定する必要があります。VACL が特定されていない場合は、書き換えられたパケットが発信 VACL の deny（拒否）ステートメントと一致し、廃棄される可能性があります。

ネットワークにルータが存在しない場合は、参加しているホスト上でスタティック ARP エントリを指定する必要があります。

PBF のハードウェアおよびソフトウェア要件

PBF のハードウェアおよびソフトウェアの要件は、次のとおりです。

- PBF には、PFC2 搭載の Supervisor Engine 2、PFC3A/PFC3B/PFC3BXL 搭載の Supervisor Engine 720、または PFC3B/PFC3BXL 搭載の Supervisor Engine 32 が必要です。
- PBF は、PBF 用に使用されている Catalyst 6500 シリーズ スイッチで動作する（起動済み）MSFC2、MSFC2A、または MSFC3 ではサポート*されていません。*

  MSFC2、MSFC2A、または MSFC3 が存在して起動した状態で PBF を設定しようとすると、システムはその機能が MSFC2、MSFC2A、または MSFC3 でサポートされていないことを示すメッセージを返します。

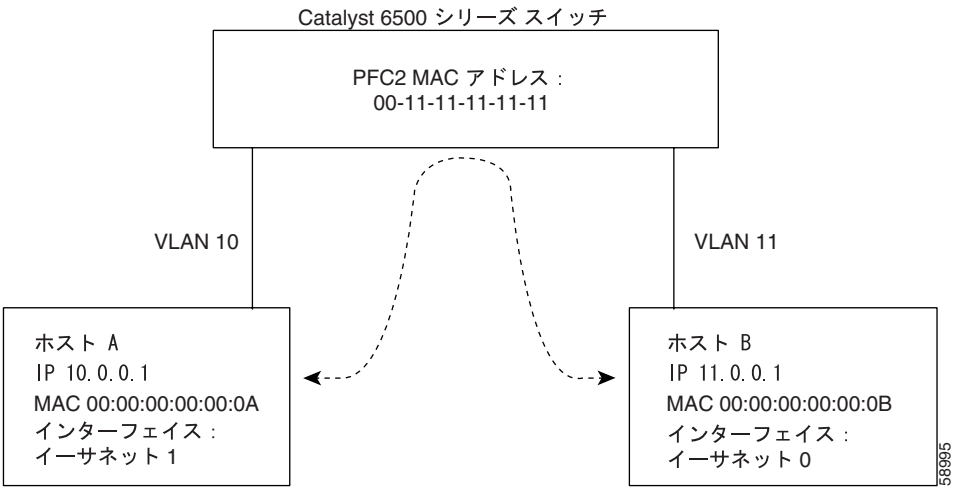
  MSFC2、MSFC2A、または MSFC3 が存在していても起動していない場合は、PBF を設定できます。
- Supervisor Engine 2 の場合、PBF にはスーパバイザ エンジン Release 6.3(1) 以降のソフトウェア リリースが必要です。
- Supervisor Engine 720 の場合、PBF にはスーパバイザ エンジン Release 8.1(1) 以降のソフトウェア リリースが必要です。
- Supervisor Engine 32 の場合、PBF にはスーパバイザ エンジン Release 8.4(1) 以降のソフトウェア リリースが必要です。

CLI からの PBF の設定

(注)　ここでの注意事項および構成例の詳細については、「PBF 設定の拡張機能（Releases 7.5(1) 以降のソフトウェア リリース）」（p.15-105）および「PBF 設定の拡張機能（Releases 8.3(1) 以降のソフトウェア リリース）」（p.15-108）を参照してください。

ここでは、PBF 設定時の注意事項と設定例について説明します。設定例は、図 15-10 の例を参照してください。Catalyst 6500 シリーズ スイッチは、VLAN 10 のホスト A からのトラフィックをすべて VLAN 11 のホスト B にリダイレクトし、ホスト B からのトラフィックをホスト A にリダイレクトします。ここでは PBF の設定手順について説明します。

図 15-10　PBF



PBF のイネーブル化と PFC2 または PFC3A/PFC3B/PFC3BXL 用 MAC アドレスの指定

(注)　MAC アドレスは、デフォルト設定のものでもユーザ側で指定する MAC アドレスでもかまいません。デフォルトの MAC アドレスは、Catalyst 6500 シリーズ スイッチ シャーシの MAC アドレス PROM から取得します。**set pbf mac** コマンドで MAC アドレスを指定する場合は、必ず MAC アドレスは一意のもので、どのインターフェイス上でも未使用であることを確認してください。

MAC アドレス PROM から取得するデフォルトの MAC アドレスを使用することを推奨します。**set pbf mac** コマンドで独自の MAC アドレスを指定する場合、その MAC アドレスが使用中のものと重複すると、パケットが廃棄されることがあります。

PBF のステータスと MAC アドレスを表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
PBF のステータスと MAC アドレスを表示します。	**show pbf**

PBF をイネーブルにするには、イネーブル モードで次のいずれかの作業を行います。

作業	コマンド
デフォルトの MAC アドレスで PBF をイネーブルにします。	**set pbf**
特定の MAC アドレスで PBF をイネーブルにします。	**set pbf** [**mac** *mac_address*]

次に、PBF のステータスと MAC アドレスをチェックし、デフォルトの MAC アドレスで PBF をイネーブルにし、設定を確認する例を示します。

```
Console> (enable) show pbf
Pbf status    Mac address
-----------   ------------------
not set       00-00-00-00-00-00
Console> (enable)
Console> (enable) set pbf
PBF committed successfully.
Operation successful.
Console> (enable)
Console> (enable) show pbf
Pbf status    Mac address
-----------   ------------------
ok            00-01-64-61-39-c2
Console> (enable)
```

次に、特定の MAC アドレスで PBF をイネーブルにする例を示します。

```
Console> (enable) set pbf mac 00-11-11-11-11-11
PBF committed successfully.
Operation successful.
Console> (enable)

Console> (enable) show pbf
Pbf status    Mac address
-----------   ------------------
ok            00-11-11-11-11-11
Console> (enable)
```

PBF をディセーブルにして PBF MAC アドレスを消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
PBF をディセーブルにして PBF MAC アドレスを消去します。	**clear pbf**

次に、PBF MAC アドレスを削除する例を示します。

```
Console> (enable) clear pbf
PBF cleared.
Console> (enable)

Console> (enable) show pbf
Pbf status    Mac address
-----------   ------------------
not set       00-00-00-00-00-00
Console> (enable)
```

VLAN における PBF MAC アドレスの指定

(注)　この PBF 設定手順は、PFC3A/PFC3B/PFC3BXL 搭載の Supervisor Engine 720 上でのみ必要です。

set pbf vlan *vlan* コマンドを実行すると、指定した VLAN 上の PBF レイヤ 2 CAM（連想メモリ）エントリが作成されます。これらのエントリに一致するパケットは、レイヤ 3 パケットとして分類されます。レイヤ 2 エントリが作成されるのは、**set pbf vlan** コマンドを使用する前に **set pbf mac** コマンドを使用して PBF MAC アドレスを設定する場合だけです。

VLAN 上の PBF MAC アドレスを指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
VLAN 上の PBF MAC アドレスを指定します。	**set pbf vlan** *vlan*

次に、VLAN 上の PBF MAC アドレスを指定する例を示します。

```
Console> (enable) set pbf vlan 11-12
Console> (enable) PBF enabled on vlan(s) 11-12.
Operation successful.
Console> (enable) show pbf
Pbf status    Mac address            Vlans
-----------   ------------------     ---------
ok            00-01-64-f8-39-18      11-12
Console> (enable)
```

メッセージ [Operation successful] は、PBF MAC アドレスが NVRAM に保存されたことを示します。

clear pbf コマンドを入力しても、PBF がイネーブルにされた VLAN は消去されません。**clear pbf** コマンドを実行すると、その VLAN に対応付けられたレイヤ 2 テーブル エントリは（MAC アドレスが有効でなくなるため）消去されます。NVRAM から PBF 対応 VLAN を削除するには、**clear pbf vlan** *vlan_list* コマンドを入力して、目的の VLAN を明示的に消去する必要があります。

PBF のための VACL の設定

(注) **set security acl adjacency** コマンドを使用して隣接テーブルの書き換え情報を指定します。この情報により、パケット ヘッダーが書き換えられ（宛先 VLAN および送信元と宛先の MAC アドレス）、宛先 VLAN に転送されます。

送信元 MAC アドレスの指定は任意です。送信元 MAC アドレスを指定しなかった場合は、システムによりデフォルトで PBF MAC アドレスに設定されます。

(注) VLAN には最大 256 の隣接テーブル エントリを設定できます。隣接テーブル エントリの最大数は 1023 です。

(注) PBF を使用してジャンボ フレーム転送をイネーブルにするには、**set security acl adjacency** コマンドで **mtu** キーワードを使用します。

PBF VACL でのエントリの順序は重要です。隣接テーブル エントリは、リダイレクト ACE によりトラフィックのリダイレクトに使用されるので、リダイレクト ACE より先に定義する必要があります。PBF VACL のエントリは、次の順序で作成してください。

1. 隣接テーブル エントリを指定します。
2. 隣接テーブル エントリを使用する PBF VACL のリダイレクト ACE を指定します。
3. 隣接テーブル エントリをコミットします。
4. PBF VACL をコミットします。
5. PBF VACL を 1 つまたは複数の VLAN にマッピングします。

ヒント **commit security acl all** コマンドを使用すると、ステップ 3 およびステップ 4 をまとめることができます。

(注) 複数のリダイレクト ACE で同じ隣接テーブル エントリを使用できます。

PFC2 または PFC3A/PFC3B/PFC3BXL 用の隣接テーブル エントリを指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
PFC2 または PFC3A/PFC3B/PFC3BXL 用の隣接テーブル エントリを指定します。	**set security acl adjacency** *adjacency_name dest_vlan dest_mac* [[*source_mac*] | [*source_mac* **mtu** *mtu_size*] | [**mtu** *mtu_size*]]

次に、隣接テーブル エントリを指定する例を示します。

```
Console> (enable) set security acl adjacency ADJ1 11 00-00-00-00-00-0B
ADJ1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

次に、VLAN 10 の PBF VACL を作成する例を示します（図 15-10 を参照）。

```
Console> (enable) set security acl adjacency ADJ1 11 00-00-00-00-00-0B
ADJ1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable) set security acl ip IPACL1 redirect ADJ1 ip host 10.0.0.1 host
11.0.0.1
IPACL1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable) set security acl ip IPACL1 permit any
IPACL1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable) commit security acl adjacency
Commit operation in progress.

Adjacency successfully committed.
Console> (enable) commit security acl IPACL1
ACL commit in progress.

ACL 'IPACL1' successfully committed.
Console> (enable) set security acl map IPACL1 10
Mapping in progress.

ACL IPACL1 successfully mapped to VLAN 10.
Console> (enable)
```

次に、VLAN 11 の PBF VACL を作成する例を示します（図 15-10 を参照）。

```
Console> (enable) set security acl adjacency ADJ2 10 00-00-00-00-00-0A
ADJ2 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable) set security acl ip IPACL2 redirect ADJ2 ip host 11.0.0.1 host
10.0.0.1
IPACL2 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable) set security acl ip IPACL2 permit any
IPACL2 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable) commit security acl adjacency
Commit operation in progress.

Adjacency successfully committed.
Console> (enable) commit security acl IPACL2
ACL commit in progress.

ACL 'IPACL2' successfully committed.
Console> (enable) set security acl map IPACL2 11
Mapping in progress.

ACL IPACL2 successfully mapped to VLAN 11.
Console> (enable)
```

PBF 情報の表示

ここでは、PBF 関連情報の表示方法について説明します。

隣接テーブル エントリを表示するには、ユーザ モードで次のいずれかの作業を行います。

作業	コマンド
隣接テーブル エントリを表示します。	**show security acl info** [*acl_name* | **adjacency** | **all**] [**editbuffer** [*editbuffer_index*]]
すべての隣接テーブル エントリまたは特定の隣接テーブル エントリに対する PBF 隣接情報を表示します。	**show pbf adjacency** [*adj_name*]
すべての隣接テーブル エントリまたは特定の隣接テーブル エントリに対する PBF 統計情報を表示します。	**show pbf statistics** [*adj_name*]
すべての隣接テーブル エントリまたは特定の隣接テーブル エントリに対する隣接 /VACL マッピングを表示します。	**show pbf map** [*adj_name*]

次に、隣接テーブル エントリを表示する例を示します。

```
Console> show security acl info adjacency
set security acl adjacency ADJ1
------------------------------------------------
1. 11 00-00-00-00-00-0b

set security acl adjacency ADJ2
------------------------------------------------

1. 10 00-00-00-00-00-0a
Console> show pbf adjacency
Index    DstVlan   DstMac             SrcMac             Name
-------------------------------------------------------------------
1        11      00-00-00-00-00-0a  00-00-00-00-00-0b     ADJ1
2        10      00-00-00-00-00-0a  00-00-00-00-00-0b     ADJ2
Console> show pbf statistics
Index    DstVlan   DstMac             SrcMac          HitCount(hex)  Name
-------------------------------------------------------------------------
1        11      00-00-00-00-00-0a  00-00-00-00-00-0b  0x00000000    ADJ1
2        10      00-00-00-00-00-0a  00-00-00-00-00-0b  0x00000000    ADJ2
Console> show pbf map
Adjacency            ACL
-----------------  --------------------
ADJ1               IPACL1

ADJ2               IPACL2
Console> (enable)
```

PBF VACL のエントリの削除

リダイレクト ACE より先に隣接テーブルを消去することはできません。PBF VACL のリダイレクト ACE および隣接テーブル エントリを消去する場合は、次の順序で行ってください。

1. リダイレクト ACE を消去します。
2. PBF VACL をコミットします。
3. 隣接テーブル エントリを消去します。
4. 隣接テーブル エントリをコミットします。

PBF 隣接テーブル エントリを消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
PBF 隣接テーブル エントリを消去します。	**clear security acl adjacency** *adj name*

次に、PBF 隣接テーブル エントリを削除する例を示します。

```
Console> (enable) clear security acl adjacency ADJ1
Adj is in use by a VACL, clear the VACL first then clear adj.
Console> (enable) clear security acl IPACL1
IPACL1 editbuffer modified. Use 'commit' command to save changes.
Console> (enable) commit security acl IPACL1
ACL commit in progress.

ACL 'IPACL1' successfully deleted.
Console> (enable) clear security acl adjacency ADJ1
ADJ1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable) commit security acl adjacency
Console> (enable) Adjacency committed successfully
Commit operation in progress.

Console> (enable)
```

編集バッファ内の隣接テーブル エントリのロール バック

rollback コマンドを使用して、最後のコミット以前に編集バッファ内に作成された隣接テーブル エントリを削除できます。隣接テーブル エントリは、最後のコミットでのステートにロール バックされます。

編集バッファ内の隣接テーブル エントリをロール バックするには、イネーブル モードで次の作業を行います。

作業	コマンド
編集バッファ内の隣接テーブル エントリをロール バックします。	**rollback security acl** {*acl_name* | **all** | **adjacency**}

次に、編集バッファ内の隣接テーブル エントリをロール バックする例を示します。

```
Console> (enable) rollback security acl adjacency
Editbuffer for adjacency info rolled back to last commit state.
Console> (enable)
```

PBF のためのホストの設定

ここでは、次のプラットフォームおよび OS（オペレーティング システム）のホスト設定手順について説明します。

- Linux（p.15-102）
- Sun ワークステーション（p.15-102）
- MS-Windows/NT/2000 ホスト（p.15-103）

（注） ネットワークにルータが存在しない場合は、参加しているホスト上でスタティック ARP エントリを指定する必要があります。ホストの ARP テーブルは、ホスト装置の IP アドレスを PFC2 または PFC3A/PFC3B/PFC3BXL の MAC アドレスにマッピングします。

（注）　次の例の IP アドレスは、図 15-10 で使用される IP アドレスです。これらのアドレスは任意に選択されたものです。ネットワーク構成で使用する IP アドレスが一意のものであることを確認してください。

Linux

次に、Linux OS（オペレーティング システム）が稼働するホストに ARP テーブルを設定する例を示します。

ホスト A を設定する例を示します。

```
arp -s 11.0.0.1 00:11:11:11:11:11 -i eth0
route add 11.0.0.1 eth0
```

ホスト B を設定する例を示します。

```
arp -s 10.0.0.1 00:11:11:11:11:11 -i eth1
route add 10.0.0.1 eth1
```

Sun ワークステーション

PBF を使用して Sun ワークステーションのエンド ホストで 2 つの VLAN 間における転送をイネーブルにする場合は、ホスト設定時に考慮すべき制限事項があるので注意してください。

- PBF の制限事項

  PBF は ARP をサポートしていません。PBF に参加する Sun ワークステーションごとにスタティック ARP エントリを設定する必要があります。各スタティック ARP エントリは、宛先ホストにマッピングされた PBF MAC アドレスを示す必要があります。

  また、Sun ワークステーションにゲートウェイを設定することも必要です。Sun ワークステーションが異なるネットワークと通信する必要がある場合は、PBF を通過するすべてのネットワークに対するホスト ルートを定義する必要があります。また、必要に応じてデフォルトのゲートウェイを定義する必要があります。

  たとえば、VLAN 40 のホスト 10.0.0.1 が VLAN 50 のホスト 11.0.0.1 と通信する必要があり、PBF MAC アドレスが 00-11-11-11-11-11 である場合、スタティック ARP エントリは次のようになります。

  ```
  arp -s 11.0.0.1 00:11:11:11:11:11
  ```

  この場合、00-11-11-11-11-11 は PBF MAC アドレスであり、11.0.0.1 は宛先ホストの IP アドレスです。

- Sun ワークステーションの制限事項

  Sun ワークステーションでは、宛先が別のネットワークの一部である場合（上記の例では 11.x.x.x）、スタティック ARP エントリを設定できません。これはすべての Sun ワークステーションでの ARP の制限事項です。この問題を解決するには、ホスト ルートであるダミー ゲートウェイを定義し、宛先ホストにマッピングされた PBF MAC アドレスを示すスタティック ARP エントリを設定する必要があります。

  上の例を使用して、最初にゲートウェイに対するダミー スタティック ARP エントリを定義する必要があります。ゲートウェイの IP アドレスは、そのネットワーク内のホスト アドレスのいずれかです。

  ```
  (A)Kubera# arp -s 10.0.0.2  00:11:11:11:11:11
  (B)Kubera# route add host  11.0.0.1 10.0.0.2
  ```

  PBF 関連トラフィックのダミー ARP エントリを 1 つと、各宛先ホストのホスト ルートを設定するだけです。

ホスト数が増えた場合は、各宛先ホストについてホスト ルート エントリを設定する必要があります。各宛先ホストのホスト ルート エントリがある /etc/rc2.d に、スタートアップ ファイルを設定できます。このファイルを設定すると、Sun ワークステーションをリセットまたは再起動したあと、すべてのホスト ルートを入力する必要がなくなります。

ファイルのエントリは次の形式を使用します。

```
Route add host <destination Host IP Address> <dummy gateway IP Address>
```

スタートアップ スクリプトの 1 つとしてホスト ルート エントリが記述されているファイルを使用する必要があります。ルート / スーパユーザのフルアクセス権を持つディレクトリにファイルを作成したり、/etc/rc2.d 内のそのファイルを示すソフト リンクを設定したり、あるいは /etc/rc2.d ディレクトリ自体にファイルを作成することもできます。

MS-Windows/NT/2000 ホスト

Windows ベースの PC 上にスタティック ARP エントリを設定する必要があります。Windows ベースの PC では、PBF を使用する VLAN 間のスイッチングのためのダミー ゲートウェイを設定する必要はありません。

次に、Windows ベースのプラットフォームにスタティック ARP エントリを設定する例を示します。

```
C:\> arp -s 11.0.0.1 00-11-11-11-11-11
```

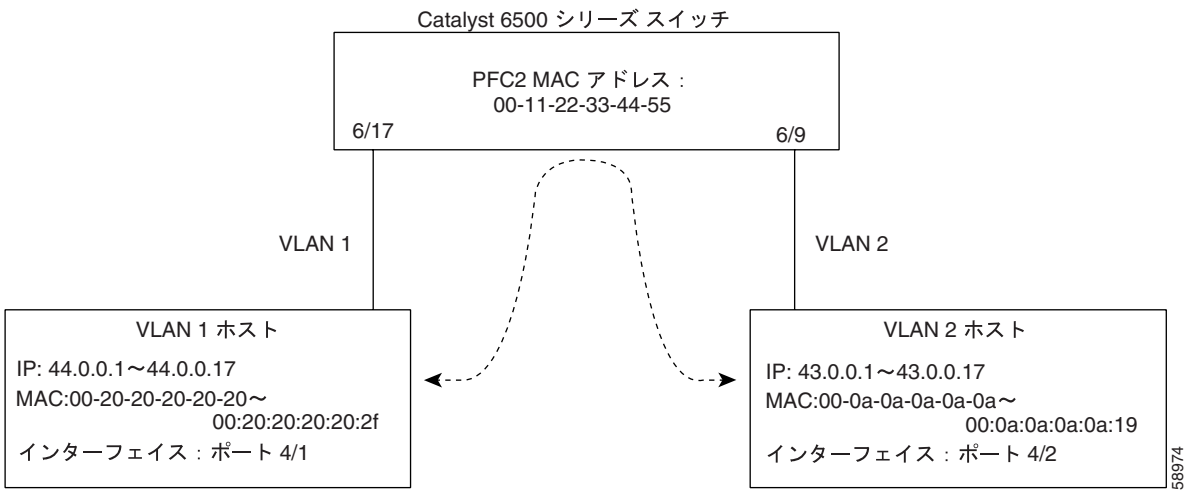
この例では、00-11-11-11-11-11 は PBF MAC アドレスであり、11.0.0.1 は宛先ホストの IP アドレスです。

さらにホストを設定する必要がある場合は、各宛先ホストに対する ARP エントリでバッチ ファイルを作成して、Windows がこのファイルをスタートアップ時に使用するように指定できます。

PBF の設定例

ここでは、VLAN 1 のホストと VLAN 2 のホストとの間の PBF をイネーブルにする設定例を示します（図 15-11 を参照）。

図 15-11　PBF の設定例



次に、VLAN 1 上のホストと VLAN 2 上のホストとの間で PBF をイネーブルにするために作成されたスイッチ コンフィギュレーション ファイルの例を示します。この例では、各 VLAN の最初の 4 つのホストだけが表示されます（44.0.0.1 ～ 44.0.0.4 および 43.0.0.1 ～ 43.0.0.4）。

```
#security ACLs
clear security acl all
#adj set
set security acl adjacency a_1 2 00-0a-0a-0a-0a-0a
set security acl adjacency a_2 2 00-0a-0a-0a-0a-0b
set security acl adjacency a_3 2 00-0a-0a-0a-0a-0c
set security acl adjacency a_4 2 00-0a-0a-0a-0a-0d
set security acl adjacency b_1 1 00-20-20-20-20-20
set security acl adjacency b_2 1 00-20-20-20-20-21
set security acl adjacency b_3 1 00-20-20-20-20-22
set security acl adjacency b_4 1 00-20-20-20-20-23
#ip1
set security acl ip ip1 permit arp
set security acl ip ip1 redirect  a_1  ip host 44.0.0.1 host 43.0.0.1
set security acl ip ip1 redirect  a_2  ip host 44.0.0.2 host 43.0.0.2
set security acl ip ip1 redirect  a_3  ip host 44.0.0.3 host 43.0.0.3
set security acl ip ip1 redirect  a_4  ip host 44.0.0.4 host 43.0.0.4
set security acl ip ip1 permit ip any any
#ip2
set security acl ip ip2 permit arp
set security acl ip ip2 redirect  b_1  ip host 43.0.0.1 host 44.0.0.1
set security acl ip ip2 redirect  b_2  ip host 43.0.0.2 host 44.0.0.2
set security acl ip ip2 redirect  b_3  ip host 43.0.0.3 host 44.0.0.3
set security acl ip ip2 redirect  b_4  ip host 43.0.0.4 host 44.0.0.4
set security acl ip ip2 permit ip any any
#pbf set
set pbf mac 00-11-22-33-44-55
#
commit security acl all
set security acl map ip1 1
set security acl map ip2 2
```

次に、VLAN 1 上のポート 6/17 について、スイッチによって学習された MAC アドレスを表示する例を示します。

```
Console> (enable) show cam dynamic 6/17
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry $ = Dot1x Security Entry

VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs / [Protocol Type]
----  ------------------    -----  -------------------------------------------
1     00-20-20-20-20-23             6/17 [ALL]
1     00-20-20-20-20-22             6/17 [ALL]
1     00-20-20-20-20-21             6/17 [ALL]
1     00-20-20-20-20-20             6/17 [ALL]
1     00-20-20-20-20-27             6/17 [ALL]
1     00-20-20-20-20-26             6/17 [ALL]
1     00-20-20-20-20-25             6/17 [ALL]
1     00-20-20-20-20-24             6/17 [ALL]
1     00-20-20-20-20-2b             6/17 [ALL]
1     00-20-20-20-20-2a             6/17 [ALL]
1     00-20-20-20-20-29             6/17 [ALL]
1     00-20-20-20-20-28             6/17 [ALL]
1     00-20-20-20-20-2f             6/17 [ALL]
1     00-20-20-20-20-2e             6/17 [ALL]
1     00-20-20-20-20-2d             6/17 [ALL]
1     00-20-20-20-20-2c             6/17 [ALL]
Total Matching CAM Entries Displayed for 6/17 = 16 for port 6/9, vlan 2
```

次に、VLAN 2 上のポート 6/9 について、スイッチによって学習された MAC アドレスを表示する例を示します。

```
Console> (enable) show cam dynamic 6/9
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry $ = Dot1x Security Entry

VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs / [Protocol Type]
----  ------------------    -----  ----------------------------------------
2     00-0a-0a-0a-0a-0e             6/9 [ALL]
2     00-0a-0a-0a-0a-0f             6/9 [ALL]
2     00-0a-0a-0a-0a-0c             6/9 [ALL]
2     00-0a-0a-0a-0a-0d             6/9 [ALL]
2     00-0a-0a-0a-0a-0a             6/9 [ALL]
2     00-0a-0a-0a-0a-0b             6/9 [ALL]
2     00-0a-0a-0a-0a-19             6/9 [ALL]
2     00-0a-0a-0a-0a-18             6/9 [ALL]
2     00-0a-0a-0a-0a-17             6/9 [ALL]
2     00-0a-0a-0a-0a-16             6/9 [ALL]
2     00-0a-0a-0a-0a-15             6/9 [ALL]
2     00-0a-0a-0a-0a-14             6/9 [ALL]
2     00-0a-0a-0a-0a-13             6/9 [ALL]
2     00-0a-0a-0a-0a-12             6/9 [ALL]
2     00-0a-0a-0a-0a-11             6/9 [ALL]
2     00-0a-0a-0a-0a-10             6/9 [ALL]
Total Matching CAM Entries Displayed for 6/9 = 16
```

次に、PBF ステータスと PFC2 または PFC3A/PFC3B/PFC3BXL MAC アドレスを表示する例を示します。

```
Console> (enable) show pbf
Pbf status    Mac address
-----------   ------------------
ok            00-11-22-33-44-55
```

次に、PBF 統計情報を表示する例を示します。

```
Console> (enable) show pbf statistics
Index    DstVlan   DstMac             SrcMac          HitCount(hex)  Name
-------------------------------------------------------------------------
1          2      00-0a-0a-0a-0a-0a  00-11-22-33-44-55  0x00026d7c    a_1
2          2      00-0a-0a-0a-0a-0b  00-11-22-33-44-55  0x00026d83    a_2
3          2      00-0a-0a-0a-0a-0c  00-11-22-33-44-55  0x00026d89    a_3
4          2      00-0a-0a-0a-0a-0d  00-11-22-33-44-55  0x00026d90    a_4
5          1      00-20-20-20-20-20  00-11-22-33-44-55  0x000260e3    b_1
6          1      00-20-20-20-20-21  00-11-22-33-44-55  0x000260ea    b_2
7          1      00-20-20-20-20-22  00-11-22-33-44-55  0x000260f1    b_3
8          1      00-20-20-20-20-23  00-11-22-33-44-55  0x000260f8    b_4
```

PBF 設定の拡張機能（Releases 7.5(1) 以降のソフトウェア リリース）

ここでは、Release 7.5(1) 以降のソフトウェア リリースで利用できるコンフィギュレーション コマンドを使用して PBF を設定する手順について説明します。

ここでは、PBF 設定の拡張機能について説明します。

PBF 設定拡張機能の概要

（注）　**set pbf-map** コマンドは Release 8.3(1) で変更されました。詳細については、「PBF 設定の拡張機能（Releases 8.3(1) 以降のソフトウェア リリース）」（p.15-108）を参照してください。

新しい **set pbf-map** コマンドは、入力された情報に基づいてセキュリティ ACL と隣接情報を作成し、ACL を自動的にコミットします。**set pbf-map** コマンドでは、次の 2 つのステップを伴います。

ステップ 1　隣接テーブルの挿入

このステップでは、ACL に追加された各リダイレクト / 隣接 ACE について隣接テーブルにエントリを作成します。

ステップ 2　ACL の作成および変更

このステップでは、リダイレクト / 隣接エントリについて各 ACL に ACE を作成し、ACL の末尾に **permit ip any any** ACE を追加します（この ACE は、ACL にまだ **permit ip any any** ACE がない場合にだけ、追加されます）。

set pbf-map コマンドの構文は、**set pbf-map** *ip_addr_1 mac_1 vlan_1 ip_addr_2 mac_2 vlan_2* です。

簡易構文の例は、**set pbf-map 1.1.1.1 0-0-0-0-0-1 11 2.2.2.2 0-0-0-0-0-2 12** です。

新しい **set pbf-map** コマンドは、次の Release 7.5(1) より前のすべてのコマンドと同じです。

```
set security acl adjacency PBF_MAP_ADJ_0 11 0-0-0-0-0-1
set security acl adjacency PBF_MAP_ADJ_1 12 0-0-0-0-0-2
commit security acl adjacency
set security acl ip PBF_MAP_ACL_11 redirect PBF_MAP_ADJ_1 ip host 1.1.1.1 host 2.2.2.2
set security acl ip PBF_MAP_ACL_12 redirect PBF_MAP_ADJ_0 ip host 2.2.2.2 host 1.1.1.1
```

permit ip any any ACE がない場合は、次の 2 つの **permit ip any any** エントリが追加されます。

```
set security acl ip PBF_MAP_ACL_11 permit ip any any
set security acl ip PBF_MAP_ACL_12 permit ip any any
commit security acl ip PBF_MAP_ACL_11
commit security acl ip PBF_MAP_ACL_12
set security acl map PBF_MAP_ACL_11 11
set security acl map PBF_MAP_ACL_12 12
```

set pbf-map コマンドによって追加された ACL 内の各エントリは、デフォルトの **permit ip any any** ACE の前に挿入されます。

リダイレクト ACE 以外のエントリを隣接テーブルに追加する場合は、**set security acl ip PBF_MAP_ACL_(VLAN_ID)** コマンドを入力します。PBF_MAP_ACL_(VLAN_ID) ACL 名は、次のアルゴリズムに基づきます。つまり、対応するホストの VLAN 番号が PBF_MAP_ACL_ ストリングに追加されます。

PBF_MAP_ACL_(VLAN_ID) ACL に含まれているリダイレクト / 隣接 ACE と隣接情報を削除するには、**clear pbf-map** コマンドを入力します。PBF_MAP_ACL_(VLAN_ID) ACL の一部であるその他すべての ACE タイプを消去するには、**clear security acl** コマンドを入力します。

PBF_MAP_ACL の指定

(注) **set pbf-map** コマンドが使用する ACL 名は、このコマンド用に予約されています。**set security acl** コマンドを入力すると、PBF_MAP_ACL で始まる名前は使用できません。隣接情報に使用される名前も、**set pbf-map** コマンド用に予約されています。**set security acl adjacency** コマンドを入力すると、PBF_MAP_ADJ で始まる名前は使用できません。

PBF_MAP_ACL を指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
PBF_MAP_ACL を指定します。	**set pbf-map** *ip_addr_1 mac_1 vlan_1 ip_addr_2 mac_2 vlan_2*

次に、PBF_MAP_ACL を指定する例を示します。

```
Console> (enable) set pbf-map 1.1.1.1 0-0-0-0-0-1 11 2.2.2.2 0-0-0-0-0-2 22
Commit operation successful.
Commit operation successful.

ACL 'PBF_MAP_ACL_11' successfully committed.
Console> (enable)
ACL PBF_MAP_ACL_11 successfully mapped to VLAN 11.
Console> (enable)
ACL 'PBF_MAP_ACL_22' successfully committed.
Console> (enable)
ACL PBF_MAP_ACL_22 successfully mapped to VLAN 22.
Console> (enable) Operation successful.
Console> (enable)
```

PBF_MAP_ACL 情報の表示

PBF_MAP_ACL 情報を表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
PBF_MAP_ACL 情報を表示します。	**show pbf-map** {*vlan* | **config**}

次に、指定された VLAN の PBF 関連 ACE と、使用された各隣接の統計情報を表示する例を示します。

```
Console> (enable) show pbf-map 11
Index    DstVlan   DstMac             SrcMac          HitCount(hex)  Name
-------------------------------------------------------------------------------
1         22      00-00-00-00-00-02  00-00-00-00-00-00  0x00000000 PBF_MAP_ADJ_1
Console> (enable)
```

次に、PBF マップ設定の例を示します。

```
Console> (enable) show pbf-map config
set pbf_map 1.1.1.1 00-00-00-00-00-01 11 2.2.2.2 00-00-00-00-00-02 22
Console> (enable)
```

PBF_MAP_ACL 設定の消去

PBF_MAP_ACL 設定を消去するには、ユーザ モードで次の作業を行います。

作業	コマンド
PBF_MAP_ACL 設定を消去します。	**clear pbf-map all** | **vlan** *vlan* | *ip_addr_1 mac_1 vlan_1 ip_addr_2 mac_2 vlan_2*

次に、**set pbf-map** コマンドによって作成されたすべての ACL と隣接情報を消去する例を示します。

```
Console> (enable) clear pbf-map all

ACL 'PBF_MAP_ACL_11' successfully deleted.
Console> (enable)
ACL 'PBF_MAP_ACL_22' successfully deleted.
Console> (enable)
```

次に、PBF_MAP_ACL_VLAN_# の名前を持つ ACL とその ACL が使用する隣接テーブルを消去する例を示します。

```
Console> (enable) clear pbf-map vlan 11

ACL 'PBF_MAP_ACL_11' successfully deleted.
Console> (enable) Commit operation successful.
Console> (enable)
```

次に、**permit ip any any** ACE を除いて **set pbf-map** コマンドによって作成された ACE をすべて消去する例を示します。コマンドによって、*vlan_1* および *vlan_2* 上の *ip_addr_1* および *ip_addr_2* であるホスト間のトラフィックをイネーブルにするエントリが削除されます。**clear security acl** コマンドによりエントリが削除済みの場合は、メッセージが表示され、特定のエントリが消去済みであることを示します。実際の削除されたエントリは、2 つの ACE（リダイレクト / 隣接 ACE）と、隣接テーブルの 2 つのエントリです。

```
Console> (enable) clear pbf-map 1.1.1.1 0-0-0-0-0-1 11 2.2.2.2 0-0-0-0-0-2 22

ACL 'PBF_MAP_ACL_11' successfully committed.
Console> (enable)
ACL 'PBF_MAP_ACL_22' successfully committed.
Console> (enable)
```

PBF 設定の拡張機能（Releases 8.3(1) 以降のソフトウェア リリース）

ここでは、Release 8.3(1) 以降のソフトウェア リリースで使用可能な 2 つのコンフィギュレーション コマンド（**set pbf client** および **set pbf gw**）を使用して PBF を設定する例を示します。ここで説明されている PBF 拡張機能は、セキュリティ ACL および隣接情報の設定とコミットのプロセスを簡略化します。拡張された **set pbf-map** コマンドは、入力に基づいてセキュリティ ACL および隣接情報を作成し、それをハードウェアにコミットして、VLAN にマッピングします。ある VLAN から別の VLAN へトラフィックをリダイレクトするために必要な VACL を作成する一部として、ARP パケットがソフトウェアにリダイレクトされてスーパバイザ エンジンがゲートウェイおよびクライアント要求に対する ARP 応答を生成します。

ここでは、PBF 設定の拡張機能について説明します。

- 診断インターフェイスとしての sc1 インターフェイスの使用（p.15-113）

PBF の使用上の注意事項および制限事項

ここでは、PBF を設定する際の使用上の注意事項と制限事項を説明します。

- Supervisor Engine 720 では、**set pbf vlan** *vlan* コマンドを入力して、PBF をイネーブルにしている VLAN を指定する必要があります。詳細については、「VLAN における PBF MAC アドレスの指定」（p.15-97）を参照してください。
- クライアントおよびゲートウェイは別の VLAN 上にあり、どのクライアントまたはゲートウェイにも同じ IP アドレスがないようにしなければなりません。エントリの最大数は 1024 です。
- クライアント名とゲートウェイ名は、12 文字以内でなければなりません。
- すでに VACL が添付されている 2 つの VLAN 間に PBF マップを作成する場合、PBF ACL が前の設定を上書きします。逆も成り立ちます。**set pbf-map** コマンドを入力して PBF ACL を作成し、PBF ACL が VLAN に添付されている場合、同じ VLAN に新しい VACL をマッピングしようとすると、新しい VACL が前の設定を上書きします。

セキュリティ ACL および隣接情報の設定とコミット

新しい **set pbf client** コマンドは、新しいホストに現在のリストを追加します。VLAN 接続を処理するゲートウェイを追加するのに新しい **set pbf gw** コマンドが使用されます。拡張された **set pbf-map** コマンドは、新しい 2 つの ACL（client_name および gateway_name）を作成し、新しく作成されたエントリをハードウェアにコミットし、それを VLAN にマッピングします。

PBF マップを作成するには、次の手順を実行します。

ステップ 1　次のように、各リストにクライアントおよびゲートウェイを追加します。

a. **set pbf client** *client_name ip_addr mac_addr vlan*

b. **set pbf gw** *gateway_name ip_addr ip_mask mac_addr vlan*

ステップ 2　次のように、クライアント リストをゲートウェイ リストにマッピングします。

set pbf-map *client_name gateway_name*

（注）　単一の PBF ゲートウェイにマッピングできる PBF クライアント グループの数は、すでに設定された ACL の数に依存します。サポートされている最大 ACL 数が 250 なので、すでに 20 ACL を定義している場合、229 のクライアント グループをゲートウェイにマッピングできます。

次に例を示します。

```
Console> (enable) set pbf client cl1 21.1.1.1 00-00-00-00-40-01 101
Commit operation successful.
Console> (enable) set pbf gw gw1 21.0.0.128 255.0.0.0 00-a0-c9-81-e1-13 102
Commit operation successful.
Console> (enable) set pbf-map cl1 gw1
.ccl1 editbuffer modified. Use 'commit' command to apply changes.
.ggw1 editbuffer modified. Use 'commit' command to apply changes.
.ccl1 editbuffer modified. Use 'commit' command to apply changes.
.ggw1 editbuffer modified. Use 'commit' command to apply changes.
.ccl1 editbuffer modified. Use 'commit' command to apply changes.
.ggw1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable) ACL commit in progress.
Console> (enable) ACL commit in progress.

ACL '.ccl1' successfully committed.
Console> (enable)
ACL '.ggw1' successfully committed.
Console> (enable) Mapping in progress.
Please configure VLAN 101.

ACL .ccl1 successfully mapped to VLAN 101.
Console> (enable) Mapping in progress.
Please configure VLAN 102.

ACL .ggw1 successfully mapped to VLAN 102.
Console> (enable)
```

新しく拡張されたコマンド セットは、次のコマンドの すべてと同等です。

```
#adj set
set security acl adjacency .c0001cl1 101 00-00-00-00-40-01 21.1.1.1
set security acl adjacency .g0002gw1 102 00-a0-c9-81-e1-13 21.0.0.128 7
#.ccl1
set security acl ip .ccl1 permit arp
set security acl ip .ccl1 permit arp-inspection any any
set security acl ip .ccl1 redirect .g0002gw1 ip host 21.1.1.1 any
set security acl ip .ccl1 permit ip any any
#.ggw1
set security acl ip .ggw1 permit arp
set security acl ip .ggw1 permit arp-inspection any any
set security acl ip .ggw1 redirect .c0001cl1 ip any host 21.1.1.1
set security acl ip .ggw1 permit ip any any
#
commit security acl all
set security acl map .ccl1 101
set security acl map .ggw1 102
```

set pbf-map コマンドによって追加された ACL 内の各エントリは、デフォルトの **permit ip any any** ACE の前に挿入されます。隣接にリダイレクトされる以外のエントリを追加する場合、**set security acl ip client_name** または **gateway_name** コマンドを入力します。ARP 検査エントリは、より個別なものに置き換えることができます。ARP 応答は、ARP 検査 ACE が確認されたあとにのみ生成されます。ARP 応答を取得できるクライアントを制限したい場合、新しい ARP 検査エントリを設定する必要があります。

clear コマンド

clear pbf client コマンドは、最初に PBF マップを削除せずに最後に残っている PBF クライアントを削除するのに使用できません。単一のクライアントまたはすべてのクライアントをリストから削除するには、ユーザ モードで次の作業を行います。

作業	コマンド
単一またはすべてのクライアントを消去できます。	**clear pbf** {**client** | **gw**} *name* [*ip_addr*]

次に、PBF クライアントを消去する例を示します。

```
Console> (enable) clear pbf client cl1
.c0001cl1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable) Commit operation successfull.
Console> (enable)
```

clear pbf gw コマンドは、最初に PBF マップを削除せずに最後に残っている PBF ゲートウェイを削除するのに使用できません。単一ゲートウェイまたはすべてのゲートウェイを消去するには、ユーザ モードで次の作業を行います。

作業	コマンド
単一またはすべてのゲートウェイを消去できます。	**clear pbf** {**client** | **gw**} *name* [*ip_addr*]

次に、PBF ゲートウェイを消去する例を示します。

```
Console> (enable) clear pbf gw gw1
.g0002gw1 editbuffer modified. Use 'commit' command to apply changes.
Commit operation successfull.
Console> (enable)
```

PBF マッピングを消去するには、ユーザ モードで次の作業を行います。

作業	コマンド
PBF マッピングを消去します。	**clear pbf-map** *client_name gw_name*

次に、PBF マッピングを消去する例を示します。

```
Console> (enable) clear pbf-map cl1 gw1
.ccl1 editbuffer modified. Use 'commit' command to save changes.
.ggw1 editbuffer modified. Use 'commit' command to save changes.
Console> (enable) ACL commit in progress.
Console> (enable) ACL commit in progress.

ACL '.ccl1' successfully deleted.
Console> (enable)
ACL '.ggw1' successfully deleted.
Console> (enable)
```

show コマンド

PBF マップをすべて表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
すべての PBF マップを表示します。	**show pbf-map**

次に、すべての PBF エントリを表示する例を示します。

```
Console> (enable) show pbf-map
PBF MAP
Clients             Gatways
-------------------------------------------
cl1                   gw1
Console> (enable)
```

PBF クライアント設定を表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
PBF クライアント設定を表示します。	**show pbf client** [*client_name* | *ip_addr*]

次に、PBF クライアント設定を表示する例を示します。

```
Console> (enable) show pbf client
Client    : cl1
Map       : gw1
VLAN      : 101
Adjacency          ip           mac
-----------------------------------------
.c0001cl1          21.1.1.1     00-00-00-00-40-01


Console> (enable)
```

PBF ゲートウェイ設定を表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
PBF ゲートウェイ設定を表示します。	**show pbf gw** [*gw_name* | *ip_addr*]

次に、PBF ゲートウェイ設定を表示する例を示します。

```
Console> (enable) show pbf gw
Client    : gw1
Map       : cl1
VLAN      : 102
Adjacency          ip           mask           mac
-----------------------------------------------------------------
.g0002gw1          21.0.0.128   255.0.0.0    00-a0-c9-81-e1-13


Console> (enable)
```

診断インターフェイスとしての sc1 インターフェイスの使用

使用しているスイッチと顧客のスイッチやルータとの接続テストを行いやすくするために、一時的に sc1 インターフェイスを PBF クライアント VLAN 内に配置する手順は、次のとおりです。

ステップ 1　**clear pbf arp-inspection** *list_name* コマンドを入力して、テストを行う ARP 検査 ACL ステートメントを PBF クライアント VLAN から削除します。

ARP 検査 ACE がクライアント リストまたはゲートウェイの ACL に設定されている（または設定されていない）ことを確認するには、**show pbf arp-inspection** コマンドを入力します。

ステップ 2　**set interface sc1** コマンドを入力して、sc1 インターフェイスを顧客の VLAN に割り当てて、それを顧客のルータまたはスイッチと同じ IP サブネットの IP アドレスに割り当てます。

ステップ 3　**ping** コマンドを入力して、（インターフェイス sc1 が送信元の）Catalyst 6500 シリーズ スイッチと顧客のルータまたはスイッチとの間で接続性をテストします。sc1 インターフェイスが顧客の MAC アドレスの ARP 要求を送信し、顧客のルータまたはスイッチが応答します。ICMP 応答が送信される前に顧客の装置が ARP 応答を送信した場合、sc1 インターフェイスは MAC アドレスで応答します。

ステップ 4　テストが完了したら、sc1 インターフェイスが顧客の VLAN の一部のままにならないように設定しなおします。

ステップ 5　**set pbf arp-inspection** *list_name* コマンドを入力して ARP 検査 ACL ステートメントを PBF クライアント VLAN に復元します。

CHAPTER 16

NDE の設定

この章では、Catalyst 6500 シリーズ スイッチ上で NetFlow Data Export（NDE; NetFlow データ エクスポート）を設定する手順について説明します。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

この章で説明する内容は、次のとおりです。

NDE の機能概要

ここでは、NDE の機能概要について説明します。

NDE および統合型レイヤ 3 スイッチング管理の概要

Catalyst 6500 シリーズ スイッチは、Supervisor Engine 2、Supervisor Engine 720、および Supervisor Engine 32 に Cisco Express Forwarding（CEF）によるレイヤ 3 スイッチングを提供します。PFC（ポリシー フィーチャ カード）が搭載された Supervisor Engine 1 の場合、レイヤ 3 スイッチングは Multilayer Switching（MLS; マルチレイヤ スイッチング）によって提供されます。NDE を使用して、Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ ガード）経由でレイヤ 3 スイッチングされたすべてのトラフィックをモニタできます。NDE は、すべてのポート トラフィックを調べるためにスイッチに組み込まれた Remote Monitoring（RMON）機能を補足します。

（注） IP マルチキャストまたは Internetwork Packet Exchange（IPX）トラフィックについては、NDE はサポートされていません。

（注） MSFC については、NDE バージョン 7 およびバージョン 8 はサポートされていません。

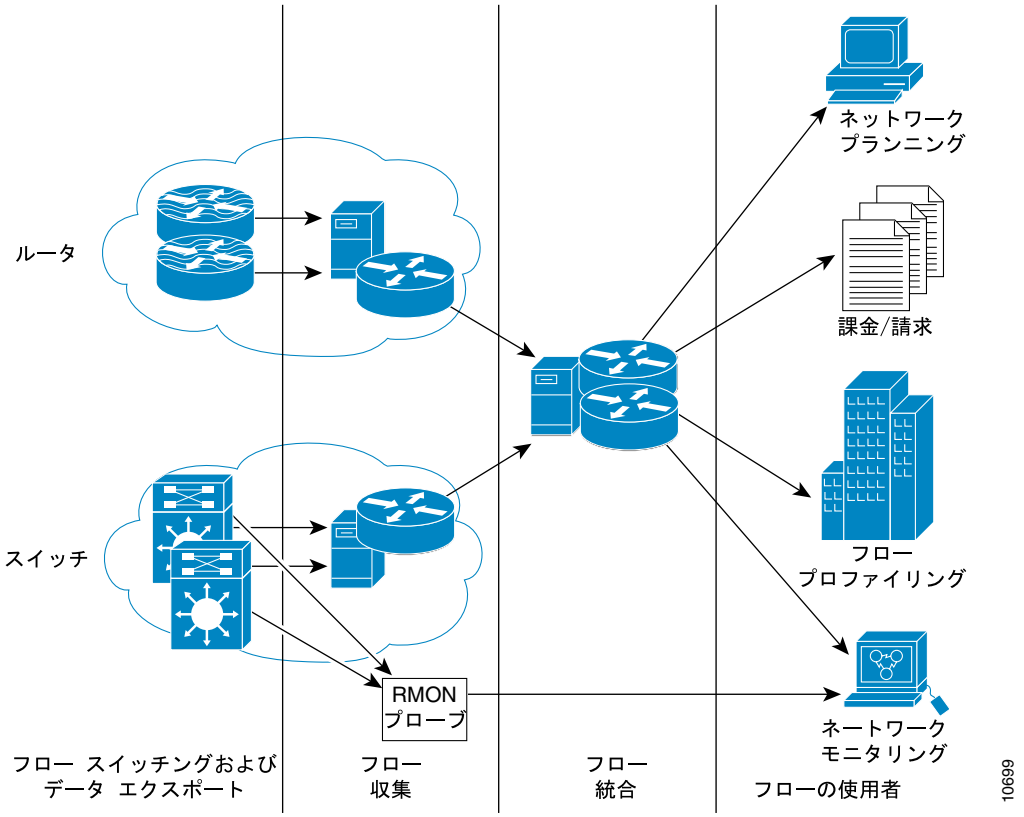
（注） CEF for PFC2 および CEF for PFC3A の設定については、第 13 章「CEF for PFC2 および CEF for PFC3A の設定」を参照してください。MLS の設定については、第 14 章「MLS の設定」を参照してください。

統合型レイヤ 3 スイッチング管理には、フロー統計情報を収集してエクスポートし、その統計情報にデータ リダクションを収集して実行し、トラフィック モニタリング、プランニング、およびアカウンティング用のアプリケーションにそのデータを転送する目的で作られた各種の製品、管理ユーティリティ、およびパートナー アプリケーションが含まれます。フローの収集および分類は、Cisco SwitchProbe、NetFlow FlowCollector などのフロー コレクタが行います。このフロー情報を集約して、TrafficDirector、NetSys、NetFlow Analyzer などのアプリケーションに提供します。

トラフィック統計データの収集

外部のデータ コレクタが、1 台または複数のスイッチまたはシスコ製ルータの統計キャッシュから、フロー エントリを収集します。スイッチまたはルータは、統計キャッシュ内の期限切れになったフローに関するフロー エントリを UDP データグラムにまとめて、フロー コレクタに転送します。このデータグラムは、ヘッダーと一連のフロー エントリで構成されます。図 16-1 を参照してください。

図 16-1　統合型レイヤ 3 スイッチング管理



NDE フィルタの使用方法

デフォルトでは、フィルタを指定しないかぎり、期限切れになったすべてのフローがエクスポートされます。フィルタを指定すると、期限切れになって削除されたフローのうち、指定されたフィルタ基準に合うものだけがエクスポートされます。フィルタ値は NVRAM（不揮発性 RAM）に保存され、NDE をディセーブルにしても消去されません。

フロー マスクが destination-ip モードであり、NDE フィルタに送信元と宛先の両方を対象とするフィルタが含まれている場合には、宛先フィルタだけが有効になります。フロー マスクが destination-ip モードの場合（以下の表示を参照）、宛先アドレス 9.1.2.15 のフローがすべてエクスポートされます。ホスト 10.1.2.15 を指定した送信元フィルタは無視されます。

```
Console> (enable) set mls nde flow destination 9.1.2.15/32 source 10.1.2.15/32
Netflow data export: destination filter set to 9.1.2.15/32
Netflow data export: source filter set to 10.1.2.15/32
Console> (enable)
```

ブリッジド フロー統計情報の使用方法

（注）　ブリッジド フロー統計は、Supervisor Engine 720 または Supervisor Engine 32 ではサポートされません。

VLAN（仮想 LAN）ごとにブリッジド フローの統計レポートが作成されるように設定することができます。ブリッジド フロー統計をイネーブルにすると、ブリッジド フローは NDE を通じてエクスポートされます。

注意　この機能を利用する場合は注意が必要です。NetFlow テーブル内の NetFlow エントリが増えるため、NDE のパフォーマンスが低下することがあります。ブリッジド フロー統計の設定については、「NDE 設定時の注意事項」（p.16-7）を参照してください。

（注）　NetFlow テーブル エントリ作成は VLAN 単位でイネーブルにすることもできます。ただし、ブリッジド フロー統計および VLAN 単位エントリ作成は同じメカニズムを使用して統計情報を収集するため、VLAN エントリが重複することがあります。「インターフェイス単位での NetFlow テーブル エントリの指定」（p.13-27）を参照してください。

NDE バージョン

PFC 上の NDE は次の NDE バージョンをサポートし、レイヤ 3 スイッチングされたトラフィックについて PFC でキャプチャされた統計情報をエクスポートします。

- Supervisor Engine 1 および PFC
  - 7.5 以降のソフトウェア リリースの NDE バージョン 5
  - 6.1 以降のソフトウェア リリースの NDE バージョン 7
- Supervisor Engine 2 および PFC2
  - 7.5 以降のソフトウェア リリースの NDE バージョン 5
  - 6.1 以降のソフトウェア リリースの NDE バージョン 7
- Supervisor Engine 720 および PFC3A/PFC3B/PFC3BXL ― NDE バージョン 5 および 7（Supervisor Engine 720 は当初、Release 8.1(1) でサポートされていました）
- Supervisor Engine 32 および PFC3B/PFC3BXL ― NDE バージョン 5 および 7（Supervisor Engine 32 は当初、Release 8.4(1) でサポートされていました）

現在のフロー マスクによっては、フロー レコードの一部のフィールドに値が入らない場合があります。PFC がキャッシュ エントリをエクスポートする際、サポートされていないフィールドには 0 が入ります。

次の表に、サポートされている NDE フィールドを示します。

- 表 16-1 ― バージョン 5 ヘッダー フォーマット
- 表 16-2 ― バージョン 5 フロー レコード フォーマット
- 表 16-3 ― バージョン 7 ヘッダー フォーマット
- 表 16-4 ― バージョン 7 フロー レコード フォーマット

表 16-1　NDE バージョン 5 ヘッダー フォーマット

バイト	内容	説明
0 ～ 1	version	NetFlow エクスポートのフォーマット バージョン番号
2 ～ 3	count	このパケットでエクスポートされるフローの数（1 ～ 30）
4 ～ 7	SysUptime	ルータ起動以降の現在時間（ミリ秒）
8 ～ 11	unix_secs	0000 UTC 1970 以降の現在秒数
12 ～ 15	unix_nsecs	0000 UTC 1970 以降の残余ナノ秒数
16 ～ 19	flow_sequence	検知された総フローのシーケンス カウンタ
20 ～ 21	engine_type	フロー スイッチング エンジンのタイプ（VS_ENGINE_TYPE_CATALYST_SWITCH）
21 ～ 23	engine_id	0

表 16-2　NDE バージョン 5 フロー レコード フォーマット

			フロー マスク：X = 実装			
バイト	内容	説明	宛先	宛先 送信元	フル	フル VLAN[1]
0 ～ 3	srcaddr	送信元 IP アドレス	**0**	**X**	**X**	**X**
4 ～ 7	dstaddr	宛先 IP アドレス	**X**	**X**	**X**	**X**
8 ～ 11	nexthop	ネクスト ホップ ルータの IP アドレス	**X**	**X**	**X**	**X**
12 ～ 13	input	入力インターフェイスの SNMP ifIndex	**0**	**X**	**X**	**X**
14 ～ 15	output	出力インターフェイスの SNMP ifIndex	**X**	**X**	**X**	**X**
16 ～ 19	dPkts	フロー内のパケット	**X**	**X**	**X**	**X**
20 ～ 23	dOctets	フロー内のオクテット（バイト）	**X**	**X**	**X**	**X**
24 ～ 27	first	フロー開始時の SysUptime（ミリ秒）	**X**	**X**	**X**	**X**
28 ～ 31	last	フローの最終パケット受信時の SysUptime（ミリ秒）	**X**	**X**	**X**	**X**
32 ～ 33	srcport	レイヤ 4 送信元ポート番号または同等の内容	**0**	**0**	**X**	**X**
34 ～ 35	dstport	レイヤ 4 宛先ポート番号または同等の内容	**0**	**0**	**X**	**X**
36	pad1	使用しない（0 の）バイト				
37	tcp_flags	TCP フラグの累積 OR	**0**	**0**	**0**	**0**
38	prot	レイヤ 4 プロトコル（たとえば、6 = TCP、17 = UDP）	**0**	**0**	**X**	**X**
39	tos	IP ToS のバイト	**X**	**X**	**X**	**X**
40 ～ 41	src_as	送信元の Autonomous System（AS; 自律システム）番号（オリジンまたはピア）	**0**	**0**	**0**	**0**
42 ～ 43	dst_as	宛先の AS 番号（オリジンまたはピア）	**0**	**0**	**0**	**0**
44 ～ 45	src_mask	送信元アドレスのプレフィクス マスク ビット	**0**	**0**	**0**	**0**
46 ～ 47	dst_mask	宛先アドレスのプレフィクス マスク ビット	**0**	**0**	**0**	**0**
48	pad2	使用しない（0 の）バイト				

1. このフロー マスクは CLI（コマンドライン インターフェイス）から設定できません。再帰 Access Control List（ACL; アクセス制御リスト）などの一部の機能を設定した場合のみオンになります。

表 16-3　NDE バージョン 7 ヘッダー フォーマット

バイト	内容	説明
0 ～ 1	version	NetFlow エクスポートのフォーマット バージョン番号
2 ～ 3	count	このパケットでエクスポートされるフローの数（1 ～ 30）
4 ～ 7	SysUptime	ルータ起動以降の現在時間（ミリ秒）
8 ～ 11	unix_secs	0000 UTC 1970 以降の現在秒数
12 ～ 15	unix_nsecs	0000 UTC 1970 以降の残余ナノ秒数
16 ～ 19	flow_sequence	検知された総フローのシーケンス カウンタ
20 ～ 24	reserved	使用しない（0 の）バイト

表 16-4　NDE バージョン 7 フロー レコード フォーマット

			フロー マスク：X = 実装			
バイト	内容	説明	宛先	宛先 送信元	フル	フル VLAN[1]
0 ～ 3	srcaddr	送信元 IP アドレス	**0**	**X**	**X**	**X**
4 ～ 7	dstaddr	宛先 IP アドレス	**X**	**X**	**X**	**X**
8 ～ 11	nexthop	ネクスト ホップ ルータの IP アドレス	**X**	**X**	**X**	**X**
12 ～ 13	input	入力インターフェイスの SNMP ifIndex	**0**	**X**	**X**	**X**
14 ～ 15	output	出力インターフェイスの SNMP ifIndex	**X**	**X**	**X**	**X**
16 ～ 19	dPkts	フロー内のパケット	**X**	**X**	**X**	**X**
20 ～ 23	dOctets	フロー内のオクテット（バイト）	**X**	**X**	**X**	**X**
24 ～ 27	First	フロー開始時の SysUptime（ミリ秒）	**X**	**X**	**X**	**X**
28 ～ 31	Last	フローの最終パケット受信時の SysUptime（ミリ秒）	**X**	**X**	**X**	**X**
32 ～ 33	srcport	レイヤ 4 送信元ポート番号または同等の内容	**0**	**0**	**X**	**X**
34 ～ 35	dstport	レイヤ 4 宛先ポート番号または同等の内容	**0**	**0**	**X**	**X**
36	flags	使用中のフロー マスク	**X**	**X**	**X**	**X**
37	tcp_flags	TCP フラグの累積 OR	**0**	**0**	**0**	**0**
38	prot	レイヤ 4 プロトコル（たとえば、6 = TCP、17 = UDP）	**0**	**0**	**X**	**X**
39	tos	IP ToS のバイト	**X**	**X**	**X**	**X**
40 ～ 41	src_as	送信元の AS 番号（オリジンまたはピア）	**0**	**0**	**0**	**0**
42 ～ 43	dst_as	宛先の AS 番号（オリジンまたはピア）	**0**	**0**	**0**	**0**
44	src_mask	送信元アドレスのプレフィクス マスク ビット	**0**	**0**	**0**	**0**
45	dst_mask	宛先アドレスのプレフィクス マスク ビット	**0**	**0**	**0**	**0**
46 ～ 47	pad2	Pad 2 は 2 バイト使用				
48 ～ 51	MLS RP	MLS ルータの IP アドレス	**X**[2]	**X**[2]	**X**[2]	**X**[2]

1. このフロー マスクは CLI から設定できません。再帰 ACL などの一部の機能を設定した場合のみオンになります。
2. スイッチド エントリ用です。

NDE のデフォルト設定

表 16-5 に、NDE のデフォルト設定を示します。

表 16-5　NDE のデフォルト設定

機能	デフォルト値
NDE	ディセーブル
NDE データ コレクタのアドレスおよび UDP ポート	指定なし
NDE フィルタ	設定なし

スイッチ上での NDE の設定

ここでは、NDE を設定する手順について説明します。

NDE 設定時の注意事項

ここでは、NetFlow テーブルのエントリが多すぎる場合の注意事項について説明します。

- ソフトウェア リリース 8.5(1) 以降のリリースでは、複数のフロー マスク機能が Supervisor Engine 720 上でサポートされます。この機能は、NDE 機能にいくつかの変更をもたらします。NDE での複数のフロー マスク機能の使用については、「フロー マスク モード ― Release 8.5(1) 以降のソフトウェア リリース」（p.14-7）を参照してください。
- MLS エージング タイムを短縮します。Policy Feature Card 2（PFC2; ポリシー フィーチャ カード 2）の場合、エージング タイムを設定して、PFC2 の 32,000 フロー範囲内にエントリ数を余裕をもって保てるようにします。PFC3A の場合、エージング タイムを設定して、PFC3A の 64,000 フロー範囲内にエントリ数を余裕をもって保てるようにします。

  Supervisor Engine 2 でブリッジド フロー統計を使用する場合は、エージング タイムを 1 秒に設定します。MLS エージング タイムの変更方法については、第 14 章「MLS の設定」の「MLS エージング タイム値の指定」（p.14-21）を参照してください。

(注) ブリッジド フロー統計は、Supervisor Engine 720 または Supervisor Engine 32 ではサポートされません。

- フローあたりの実行パケットが少ないプロトコルがある場合は、MLS ファスト エージング タイムを削減します。MLS ファスト エージング タイムの変更方法については、第 14 章「MLS の設定」の「IP MLS の長期エージング タイム、ファスト エージング タイム、およびパケット スレッシュホールド値の指定」（p.14-23）を参照してください。
- 必要な種類の情報を取得するのに必要なフロー マスクを使用します。full flow マスクによりさらに情報が表示されますが、フロー数が増えるにつれて、レイヤ 3 エージングに対する負荷も増えます。必要なデータを取得するのに必要な最小粒度のフロー マスクを使用してみてください。full flow マスクの場合は、full flow マスクが 1 秒あたりのフロー数を増やすので、MLS エージング タイムを減らすことが必要な場合もあります。フロー マスクの設定手順については、第 14 章「MLS の設定」の「最小 IP MLS フロー マスクの設定」（p.14-24）を参照してください。
- フローあたりのパケットの少ないエントリを除外します。Domain Name System（DNS; ドメイン ネーム システム）のような一部のクエリ プロトコルは、生成するフローあたりのパケットが少なく、**set mls exclude protocol** コマンドで NetFlow テーブルから除外することができます。最大 4 つのプロトコル フィルタを指定できますが、フィルタが実行されたプロトコルからのパケットは MSFC に進みます。
- **set mls nde flow exclude** コマンドで、NetFlow テーブルに特定のフローが追加されないようにしてください。
- レイヤ 3 フローに見える VLAN のブリッジド フローで NetFlow テーブル内のフロー数を増加するために、VLAN に対するブリッジド フロー統計をイネーブルにします。NetFlow テーブル内の NetFlow エントリが増えると、パフォーマンスが低下します。

  Supervisor Engine 1 では、ハードウェアの NetFlow テーブル内に VLAN フローについてレポートする容量がない場合、パケットは MSFC に送信されてソフトウェアによって転送され、NetFlow Full Errors レジスタが加算されます。

  Supervisor Engine 2 では、NetFlow テーブル内にフロー エントリが 1 つもない場合、パケットが転送され、NetFlow Full Errors レジスタが加算されて、統計情報は失われます。

  NetFlow テーブルがオーバーフローするのを防ぐには、次のようにします

  - フロー マスクを最小粒度値にします。たとえば、プロトコルおよびレイヤ 4 ポートの情報が必要ない場合は、フロー マスクを full flow ではなく、destination-source または destination に設定します。
  - トラフィック プロファイルに応じて、エージング タイムを設定可能な最小値（1 秒）にします。
  - ブリッジド フロー統計をイネーブルにするのは、VLAN 内の統計情報が必要な VLAN に対してだけにします。VLAN 間の統計情報はデフォルトでレポートされます。
- NetFlow テーブル エントリ作成は VLAN 単位でイネーブルにできます。ただし、ブリッジド フロー統計および VLAN 単位エントリ作成は同じメカニズムを使用して統計情報を収集するため、VLAN エントリが重複することがあります。「インターフェイス単位での NetFlow テーブル エントリの指定」（p.13-27）を参照してください。

NDE コレクタの指定

NDE を初めてイネーブルにする前に、エクスポートされた統計情報を受信する NDE コレクタおよび UDP ポートを指定する必要があります。コレクタのアドレスおよび UDP ポート番号は NVRAM に保存され、NDE をディセーブルにして再びイネーブルにした場合、またはスイッチの電源を切って再び電源投入した場合にも、削除されずに保存されています。

(注) NetFlow FlowCollector アプリケーションをデータ収集に使用する場合は、指定する UDP ポート番号が、FlowCollector の nfconfig.file で指定されているポート番号と同じであることを確認してください。このファイルは、FlowCollector アプリケーションの /opt/csconfc/config/nfconfig.file に格納されています。

Release 8.3(1) 以降のソフトウェアでは、二重宛先機能により NetFlow は 2 つの宛先へ同時にデータをエクスポートできます。この拡張により、2 つの個別のコレクタを設定できます。同じ NetFlow データが両方の宛先にエクスポートされます。ただし、2 つのコレクタに送信されるパケットのカウントは、2 つの宛先が作成された時間によって異なる可能性があります。個々のコレクタに送信されるパケットのカウントは別々に保持されます。両方の宛先における他の NetFlow パラメータは同じです。

コレクタが設定されていないと NDE をイネーブルにできません。NDE をイネーブルにする前に、プライマリおよびセカンダリ宛先を設定する必要があります。

セカンダリ宛先 IP アドレスおよびポート番号は、プライマリ宛先 IP アドレスおよびポート番号と同一にはできません。

NDE コレクタを指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
ハードウェア スイッチングされるパケットのデータ エクスポート用の NDE コレクタおよび UDP ポートを指定します。	**set mls nde** {*collector_ip* | *collector_name*} {*udp_port_number*}

次に、他のコレクタが設定されていない場合に NDE コレクタを指定する例を示します。

```
Console> (enable) set mls nde 10.6.1.10 7772
Number of collectors configured is 1
Netflow export configured for port 7772 on host 10.6.1.10
Netflow export is not enabled. Please enable it now.
Console> (enable)
```

次に、1 つのコレクタがすでに設定されいる場合に NDE コレクタを指定する例を示します。

```
Console> (enable) set mls nde 10.6.1.10 7775
Number of collectors configured is 2
Netflow export configured for port 7775 on host 10.6.1.10
Netflow export is not enabled. Please enable it now.
Console> (enable)
```

NDE コレクタの消去

clear mls nde コマンドを入力すると、プライマリおよびセカンダリ コレクタを消去して NDE をディセーブルにすることができます。特定のコレクタ宛先を消去するには、コレクタの IP アドレスおよびポート番号を指定します。

NDE コレクタを消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
すべての NDE コレクタ、または特定の NDE コレクタを消去します。	**clear mls nde** {*ip_address port*}

次に、プライマリおよびセカンダリ コレクタを消去する例を示します。

```
Console> (enable) clear mls nde
Collector's IP address cleared.
Secondary Collector IP address cleared.
Console> (enable)
```

次に、特定のコレクタ宛先を消去する例を示します。

```
Console> (enable) clear mls nde 10.6.1.10 9939
Cleared Collector IP 10.6.1.10 port 9939
Console> (enable)
```

MSFC 上での NetFlow の設定

(注)　MSFC が存在しない場合、ブリッジド フローの統計情報しか収集（およびエクスポート）できません（ブリッジド フローの統計情報機能がイネーブルの場合）。ルーテッドおよびレイヤ 3 スイッチド トラフィックの NDE をサポートするには、MSFC レイヤ 3 インターフェイスで NetFlow をイネーブルにする必要があります。

MSFC 上での NetFlow の設定に関する詳細は、次の資料を参照してください。

- 『*Cisco IOS Switching Services Configuration Guide*』Release 12.1 の「NetFlow 」
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/switch_c/xcprt3/index.htm
- 『*Cisco IOS Switching Services Command Reference*』Release 12.1
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/switch_r/index.htm

ここでは、MSFC 上で NetFlow を設定する手順について説明します。

- NetFlow のイネーブル化（p.16-11）
- MSFC NDE 送信元インターフェイスの設定（p.16-11）
- NDE の宛先の設定（p.16-11）

NetFlow のイネーブル化

NetFlow をイネーブルにするには、各レイヤ 3 インターフェイスで次の作業を行います。

	作業	コマンド
ステップ 1	設定する VLAN インターフェイスを選択します。	Router(config)# **interface vlan** *vlan_ID*
ステップ 2	NetFlow をイネーブルにします。	Router(config-if)# **ip route-cache flow**

MSFC NDE 送信元インターフェイスの設定

MSFC からの統計情報が含まれた NDE パケットの送信元として使用されるインターフェイスを設定するには、次の作業を行います。

作業	コマンド
MSFC からの統計情報が含まれた NDE パケットの送信元として使用されるインターフェイスを設定します。 • IP アドレスによって設定するインターフェイスを選択します。 • ループバック インターフェイスを使用します。	Router(config)# **ip flow-export source** {**vlan** | **loopback**} *number*

次に、NDE フローの送信元としてループバック インターフェイスを設定する例を示します。

```
Router(config)# ip flow-export source loopback 0
Router(config)#
```

NDE の宛先の設定

NDE フロー宛先 IP アドレスおよび UDP ポートを設定するには、次の作業を行います。

作業	コマンド
NDE の宛先 IP アドレスと UDP ポートを設定します。	Router(config)# **ip flow-export destination** *ip_address udp_port_number*

次に、NDE フローの宛先 IP アドレスと UDP ポートを設定する例を示します。

```
Router(config)# ip flow-export destination 172.20.52.37 200
Router(config)#
```

NDE のイネーブル化

NDE をイネーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
スイッチ上で NDE をイネーブルにします。	**set mls nde enable**

次に、スイッチ上で NDE をイネーブルにする例を示します。

```
Console> (enable) set mls nde enable
Netflow data export enabled.
Netflow data export to port 9996 on 172.20.15.1 (Stargate)
Console> (enable)
```

事前にコレクタを指定せずに NDE をイネーブルにしようとすると、次のメッセージが表示されます。

```
Console> (enable) set mls nde enable
Please set host name and UDP port number with 'set mls nde <collector_ip>
<udp_port_number>'.
Console> (enable)
```

VLAN に対するブリッジド フロー統計のイネーブル化およびディセーブル化

(注)　この機能は Supervisor Engine 1 または 1A/PFC、Supervisor Engine 2/PFC2 でサポートされていて、MSFC/MSFC2 は不要です。この機能は、Supervisor Engine 720 または Supervisor Engine 32 ではサポートされていません。

特定の VLAN に対するブリッジド フロー統計をイネーブルまたはディセーブルに設定するには、**set mls bridged-flow-statistics** コマンドを使用します。1 つまたは複数の VLAN を入力できます。

(注)　NetFlow テーブル エントリ作成は VLAN 単位でイネーブルにできます。ただし、ブリッジド フロー統計および VLAN 単位エントリ作成は同じメカニズムを使用して統計情報を収集するため、VLAN エントリが重複することがあります。「インターフェイス単位での NetFlow テーブル エントリの指定」（p.13-27）を参照してください。

特定の VLAN または VLAN 範囲に対するブリッジド フロー統計をイネーブルまたはディセーブルに設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
特定の VLAN または VLAN 範囲に対するブリッジド フロー統計をイネーブルまたはディセーブルに設定します。	**set mls bridged-flow-statistics** {**enable** | **disable**} {*vlanlist*}

次に、特定の VLAN に対するブリッジド フロー統計をイネーブルにする例を示します。

```
Console> (enable) set mls bridged-flow-statistics enable 1,20-21
Netflow statistics is enabled for bridged packets on vlan(s) 1,20-21.
Console> show mls nde
Netflow Data Export version: 7
Netflow Data Export enabled
Netflow Data Export configured for port 9991 on host 21.0.0.1
Total packets exported = 0
Bridged flow statistics is enabled on vlan(s) 1,20-21.
Console>
```

宛先ホスト フィルタの指定

宛先ホスト フィルタを指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
NDE フローの宛先ホスト フィルタを指定します。	**set mls nde flow destination** [*ip_addr_spec*]

次に、ホスト 171.69.194.140 への期限切れになったフローだけがエクスポートされるように、宛先ホスト フィルタを指定する例を示します。

```
Console> (enable) set mls nde flow destination 171.69.194.140
Netflow Data Export successfully set
Destination filter is 171.69.194.140/255.255.255.255
Filter type: include
Console> (enable)
```

宛先および送信元サブネット フィルタの指定

宛先および送信元サブネット フィルタを指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
NDE フローの宛先および送信元サブネット フィルタを指定します。	**set mls nde flow destination** [*ip_addr_spec*] **source** [*ip_addr_spec*]

次に、サブネット 171.69.173.0 からサブネット 171.69.194.0 への期限切れになったフローだけがエクスポートされるように、宛先および送信元サブネット フィルタを指定する例を示します（フロー マスクは source-destination-ip に設定されているものと想定します）。

```
Console> (enable) set mls nde flow destination 171.69.194.140/24 source
171.69.173.5/24
Netflow Data Export successfully set
Source filter is 171.69.173.0/24
Destination filter is 171.69.194.0/24
Filter type: include
Console> (enable)
```

宛先 TCP/UDP ポート フィルタの指定

宛先 TCP/UDP ポート フィルタを指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
NDE フローの宛先 TCP/UDP ポート フィルタを指定します。	**set mls nde flow dst_prt** [*port_number*]

次に、宛先ポート 23 への期限切れになったフローだけがエクスポートされるように、宛先 TCP/UDP ポート フィルタを指定する例を示します（フロー マスクは ip-flow に設定されているものと想定します）。

```
Console> (enable) set mls nde flow dst_port 23
Netflow Data Export successfully set
Destination port filter is 23
Filter type: include
Console> (enable)
```

送信元ホストおよび宛先 TCP/UDP ポート フィルタの指定

送信元ホストおよび宛先 TCP/UDP ポート フィルタを指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
NDE フローの送信元ホストおよび宛先 TCP/UDP ポート フィルタを指定します。	**set mls nde flow source** [*ip_addr_spec*] **dst_prt** [*port_number*]

次に、ホスト 171.69.194.140 から宛先ポート 23 への期限切れになったフローだけがエクスポートされるように、送信元ホストおよび宛先 TCP/UDP ポート フィルタを指定する例を示します（フローマスクは ip-flow に設定されているものと想定します）。

```
Console> (enable) set mls nde flow source 171.69.194.140 dst_port 23
Netflow Data Export successfully set
Source filter is 171.69.194.140/255.255.255.255
Destination port filter is 23
Filter type: include
Console> (enable)
```

プロトコル フィルタの指定

プロトコル フィルタを指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
NDE フローのプロトコル フィルタを指定します。	**set mls nde flow protocol** *protocol*

次に、プロトコル 17 からの期限切れになったフローだけがエクスポートされるように、プロトコル フィルタを指定する例を示します。

```
Console> (enable) set mls nde flow protocol 17
Netflow Data Export filter successfully set.
Protocol filter is 17
Filter type: include
Console> (enable)
```

統計収集対象プロトコルの指定

set mls statistics protocol *protocol port* コマンドを使用すると、NDE によってエクスポートされる統計情報の収集対象になるプロトコルを 64 個まで指定できます。*protocol* 引数には、**ip**、**ipinip**、**icmp**、**igmp**、**tcp**、**udp**、またはその他のプロトコル ファミリーを表す 10 進数を指定できます。*port* 引数には、プロトコル ポートを指定します。

プロトコルを統計収集の対象に指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
プロトコルを統計収集の対象として指定します。	**set mls statistics protocol** *protocol port*

次に、プロトコルを統計収集の対象として指定する例を示します。

```
Console> (enable) set mls statistics protocol 17 1934
Protocol 17 port 1934 is added to protocol statistics list.
Console> (enable)
```

統計収集対象プロトコルの削除

clear mls statistics protocol {*protocol port* | **all**} コマンドを使用すると、NDE によってエクスポートされる統計情報の収集対象から削除するプロトコルを 64 個まで指定できます。*protocol* 引数には、**tcp**、**udp**、**icmp**、またはその他のプロトコル ファミリーを表す 10 進数を指定できます。*port* 引数には、プロトコル ポートを指定します。すべてのプロトコルを統計収集対象から削除するには、**all** キーワードを指定します。

プロトコルを統計収集の対象から削除するには、イネーブル モードで次の作業を行います。

作業	コマンド
プロトコルを統計収集の対象から削除します。	**clear mls statistics protocol** {*protocol port* | **all**}

次に、プロトコルを統計収集の対象から削除する例を示します。

```
Console> (enable) clear mls statistics protocol 17 1934
Protocol 17 port 1934 cleared from protocol statistics list.
Console> (enable)
```

NDE フロー フィルタの消去

NDE フロー フィルタを消去し、フィルタをデフォルト（すべてのフローをエクスポート）に戻すには、イネーブル モードで次の作業を行います。

作業	コマンド
NDE フロー フィルタを消去します。	**clear mls nde flow**

次に、NDE フロー フィルタを消去して、すべてのフローがエクスポートされるようにする例を示します。

```
Console> (enable) clear mls nde flow
Netflow data export filter cleared.
Console> (enable)
```

NDE のディセーブル化

（注） Supervisor Engine 1 および PFC で、NDE がイネーブルに設定されているときに MLS をディセーブルにすると、統計情報がエクスポートされなくなるため、既存のキャッシュ エントリの統計情報が失われます。

スイッチ上で NDE をディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
スイッチ上で NDE をディセーブルにします。	**set mls nde disable**

次に、スイッチ上で NDE をディセーブルにする例を示します。

```
Console> (enable) set mls nde disable
Netflow data export disabled.
Console> (enable)
```

NDE IP アドレスの削除

MSFC から NDE IP アドレスを削除するには、グローバル コンフィギュレーション モードで次の作業を行います。

作業	コマンド
MSFC から NDE IP アドレスを削除します。	Router(config)# **no mls nde-address** [*ip_addr*]

次に、MSFC から NDE IP アドレスを削除する例を示します。

```
Router(config)# no mls nde-address 170.170.2.1
Router(config)#
```

NDE 設定の表示

スイッチ上の NDE 設定を表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
スイッチ上の NDE 設定を表示します。	**show mls nde**

次に、スイッチ上で NDE 設定を表示する方法を示します。

```
Console> (enable) show mls nde
Netflow Data Export enabled
Netflow Data Export configured for port 7772 on host 10.6.1.10
Secondary Data Export configured for port 7775 on host 10.6.1.10
Source filter is 171.69.194.140/255.255.255.0
Destination port filter is 23
Total packets exported = 26784
Console> (enable)
```

次に、スイッチ上でブリッジド フロー統計がイネーブルに設定されている場合の NDE 設定を表示する例を示します。

```
Console> (enable) show mls nde
Netflow Data Export version:7
Netflow Data Export enabled
Netflow Data Export configured for port 7772 on host 10.6.1.10
Secondary Data Export configured for port 7775 on host 10.6.1.10
Total packets exported = 0
Bridged flow statistics is enabled on vlan(s) 1,20-21.
```

CHAPTER 17

GVRP の設定

この章では、Catalyst 6500 シリーズ スイッチ上で Generic Attribute Registration Protocol（GARP）VLAN Registration Protocol（GVRP）を設定する手順について説明します。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

この章で説明する内容は、次のとおりです。

(注) GVRP を使用するには、Release 5.2 以降のスーパバイザ エンジン ソフトウェア リリースが必要です。Supervisor Engine 720 の場合、Release 8.3(1) 以降のソフトウェア リリースが必要です。Supervisor Engine 32 の場合、Release 8.4(1) 以降のソフトウェア リリースが必要です。

GVRP の機能概要

GVRP は、802.1Q トランク ポート上で IEEE 802.1Q 準拠 VLAN（仮想 LAN）プルーニングおよびダイナミック VLAN 構成を提供する GARP アプリケーションです。

GVRP を使用することで、スイッチは他の GVRP スイッチと VLAN 設定情報を交換し、不要なブロードキャストや未知のユニキャスト トラフィックを削除し、802.1Q トランク ポートによって接続されているスイッチ上で VLAN を動的に構成および管理します。

(注)　GARP および GVRP は、IEEE 802.1p で規定されている業界標準プロトコルです。

GVRP のデフォルト設定

表 17-1 に、GVRP のデフォルト設定を示します。

表 17-1　GVRP のデフォルト設定

機能	デフォルト値
GVRP のグローバル イネーブル ステート	ディセーブル
GVRP のトランクごとのイネーブル ステート	すべてのポート上でディセーブル
GVRP VLAN のダイナミック構成	ディセーブル
GVRP 登録モード	**normal**、すべてのポートに対して VLAN 1 を **fixed** に設定する場合
GVRP 加入者（アプリカント）ステート	**normal**（STP[1] ブロッキング ステートの場合、ポートは VLAN を宣言しない）
GARP タイマー	• Join 時間：200 ミリ秒 • Leave 時間：600 ミリ秒 • Leaveall 時間：10,000 ミリ秒

1. STP = Spanning-Tree Protocol（スパニングツリー プロトコル）

GVRP 設定時の注意事項

ここでは、GVRP 設定時の注意事項について説明します。

- ポートごとの GVRP ステートを設定できるのは、802.1Q 対応のポート上だけです。
- 802.1Q トランク リンクの両端で GVRP をイネーブルにする必要はあります。
- VLAN 1 の GVRP 登録モードは常に **fixed** であり、変更できません。
- VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）プルーニングはイネーブルになると、GVRP がディセーブルに設定されているすべての 802.1Q トランク ポート上で実行されます。

スイッチ上での GVRP の設定

ここでは、GVRP の設定手順について説明します。

GVRP のグローバルなイネーブル化

スイッチ上で GVRP 処理を行う前に、GVRP をグローバルにイネーブルにする必要があります。GVRP をグローバルにイネーブルにすると、GVRP は 802.1Q トランク リンク上で VLAN プルーニングを実行できるようになります。プルーニングが行われるのは、GVRP がイネーブル化されたトランク上だけです。トランク ポートごとの GVRP イネーブル ステートを設定する手順については、「個々の 802.1Q トランク ポート上での GVRP のイネーブル化」（p.17-4）を参照してください。

ダイナミック VLAN 構成をイネーブルにするには、スイッチ上でもグローバルかつ明示的にダイナミック VLAN 構成をイネーブルにする必要があります。ダイナミック VLAN 構成をイネーブルにする手順については、「GVRP ダイナミック VLAN 構成のイネーブル化」（p.17-4）を参照してください。

スイッチ上で GVRP をグローバルにイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチ上で GVRP をイネーブルにします。	**set gvrp enable**
ステップ 2	設定を確認します。	**show gvrp configuration**

次に、GVRP をイネーブルにして設定を確認する例を示します。

```
Console> (enable) set gvrp enable
GVRP enabled
Console> (enable) show gvrp configuration
Global GVRP Configuration:
GVRP Feature is currently enabled on the switch.
GVRP dynamic VLAN creation is disabled.
GVRP Timers(milliseconds)
Join = 200
Leave = 600
LeaveAll = 10000

Port based GVRP Configuration:
Port                                                GVRP Status Registration
--------------------------------------------------- ----------- ------------
2/1-2,3/1-8,7/1-24,8/1-24                           Enabled     Normal

GVRP Participants running on 3/7-8.
Console>
```

個々の 802.1Q トランク ポート上での GVRP のイネーブル化

(注)　GVRP がグローバルにイネーブルになっているかどうかに関係なく、トランクごとの GVRP 設定を変更できます。ただし、グローバルにイネーブル化されないかぎり、GVRP はどのポートでも機能しません。スイッチ上で GVRP をグローバルにイネーブル化する手順については、「GVRP のグローバルなイネーブル化」（p.17-3）を参照してください。

ポートごとの GVRP ステートには 2 種類あります。

- CLI（コマンドライン インターフェイス）で設定され、NVRAM（不揮発性 RAM）に保存されているスタティック GVRP ステート
- ポートの実際の GVRP ステート（アクティブ GVRP 加入者）

スタティック GVRP ポート ステートは、グローバル GVRP イネーブル ステートや、ポートが 802.1Q トランクかどうかに関係なく、どの 802.1Q 対応スイッチ ポート上でも設定できます。ただし、ポートをアクティブ GVRP 加入者にするには、CLI 設定または Dynamic Trunking Protocol（DTP）ネゴシエーションのいずれかにより、GVRP をグローバルにイネーブルにする必要があり、ポートは 802.1Q トランク ポートでなければなりません。

個々の 802.1Q 対応ポート上で GVRP をイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	個々の 802.1Q 対応ポート上で GVRP をイネーブルにします。	**set port gvrp** *mod/port* **enable**
ステップ 2	設定を確認します。	**show gvrp configuration**

次に、802.1Q 対応ポート 1/1 上で GVRP をイネーブルにする例を示します。

```
Console> (enable) set port gvrp 1/1 enable
GVRP enabled on 1/1.
Console> (enable)
```

GVRP ダイナミック VLAN 構成のイネーブル化

GVRP ダイナミック VLAN 構成をイネーブルにできるのは、次の条件を満たす場合のみです。

- スイッチが VTP トランスペアレント モードである。
- スイッチ上のすべてのトランク ポートが 802.1Q トランクである（ただし、MSFC へのトランク接続は例外）。
- すべてのトランク ポート上で GVRP がイネーブルになっている。

ダイナミック VLAN 構成をイネーブルにする場合、設定に関する次の制限事項に注意してください。

- スイッチは、VTP サーバやクライアント モードには変更できません。
- GVRP を実行しているトランク ポート上で GVRP をディセーブルにできません。

ダイナミック VLAN 構成がイネーブル状態の場合、（CLI 設定または DTP を使用したネゴシエーションのいずれかにより）スイッチ上のポートが ISL（スイッチ間リンク）トランクになると、ダイナミック VLAN 構成をイネーブルにできる状態に回復するまで、ダイナミック VLAN 構成は自動的にディセーブル状態になります。

(注)　802.1Q トランク上で VLAN を動的に構成できるのは、**normal** 登録モードのときだけです。

(注)　ダイナミック VLAN 構成は、すべての VLAN タイプをサポートしています。

スイッチ上で GVRP ダイナミック VLAN 構成をイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチ上でダイナミック VLAN 構成をイネーブルにします。	**set gvrp dynamic-vlan-creation enable**
ステップ 2	設定を確認します。	**show gvrp configuration**

次に、スイッチ上でダイナミック VLAN 構成をイネーブルにする例を示します。

```
Console> (enable) set gvrp dynamic-vlan-creation enable
Dynamic VLAN creation enabled.
Console> (enable)
```

GVRP 登録の設定

ここでは、スイッチ ポート上で GVRP 登録モードを設定する手順について説明します。

- GVRP normal（標準）登録の設定（p.17-5）
- GVRP fixed（固定）登録の設定（p.17-6）
- GVRP forbidden（禁止）登録の設定（p.17-6）

GVRP normal（標準）登録の設定

normal 登録モードで 802.1Q トランク ポートを設定すると、トランク ポート上の VLAN を動的に構成し（ダイナミック VLAN 構成がイネーブルの場合）、登録および登録解除することが可能になります。デフォルトは normal モードです。

802.1Q トランク ポート上で GVRP normal 登録を設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	802.1Q トランク ポート上で normal 登録を設定します。	**set gvrp registration normal** *mod/port*
ステップ 2	設定を確認します。	**show gvrp configuration**

次に、802.1Q トランク ポート上で normal 登録を設定する例を示します。

```
Console> (enable) set gvrp registration normal 1/1
Registrar Administrative Control set to normal on port 1/1.
Console> (enable)
```

GVRP fixed（固定）登録の設定

fixed 登録モードで 802.1Q トランク ポートを設定すると、手動による VLAN 構成および登録が可能になり、VLAN の登録解除を防止し、トランク ポート上のその他の既知の VLAN をすべて登録することができます。

802.1Q トランク ポート上で GVRP fixed 登録を設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	802.1Q トランク ポート上で fixed 登録を設定します。	**set gvrp registration fixed** *mod/port*
ステップ 2	設定を確認します。	**show gvrp configuration**

次に、802.1Q トランク ポート上で fixed 登録を設定する例を示します。

```
Console> (enable) set gvrp registration fixed 1/1
Registrar Administrative Control set to fixed on port 1/1.
Console> (enable)
```

GVRP forbidden（禁止）登録の設定

forbidden 登録モードで 802.1Q トランク ポートを設定すると、すべての VLAN（VLAN 1 を除く）を登録解除し、トランク ポート上での以降の VLAN 構成や登録を防止することができます。

802.1Q トランク ポート上で GVRP forbidden 登録を設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	802.1Q トランク ポート上で forbidden 登録を設定します。	**set gvrp registration forbidden** *mod/port*
ステップ 2	設定を確認します。	**show gvrp configuration**

次に、802.1Q トランク ポート上で forbidden 登録を設定する例を示します。

```
Console> (enable) set gvrp registration forbidden 1/1
Registrar Administrative Control set to forbidden on port 1/1.
Console> (enable)
```

ブロッキング ポートからの GVRP VLAN 宣言の設定

VLAN ごとの Per-VLAN STP+（PVST+）をサポートしていない装置の接続ポート上で、Spanning-Tree Protocol（STP; スパニングツリー プロトコル）トポロジーの不要な再編成を避けるには、ポート上で GVRP アクティブ加入者ステートを設定します。GVRP アクティブ加入者ステートのポートは、STP ブロッキング ステートのときに GVRP VLAN 宣言を送信します。これにより、STP の Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）がその他のポートからプルーニングされなくなります。

（注） 他の装置のポート上で fixed 登録を設定しても、STP トポロジーの不要な再編成を防止できます。

ブロッキング ステート時に VLAN 宣言を送信するように 802.1Q トランク ポートを設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
ブロッキング ステート時に VLAN 宣言を送信するように、802.1Q トランク ポートを設定します。	**set gvrp applicant state** {**normal** | **active**} *mod/port*

次に、ブロッキング ステート時に VLAN 宣言を送信するように、802.1Q トランク ポートのグループを設定する例を示します。

```
Console> (enable) set gvrp applicant state active 4/2-3,4/9-10,4/12-24
Applicant was set to active on port(s) 4/2-3,4/9-10,4/12-24.
Console> (enable)
```

デフォルト ステート（アクティブ モードがディセーブル状態）に戻るには、**normal** キーワードを使用します。

GARP タイマーの設定

（注） **set gvrp timer** コマンドおよび **show gvrp timer** コマンドは、**set garp timer** コマンドおよび **show garp timer** コマンドのエイリアスです。必要に応じてこれらのエイリアスを使用できます。

（注） GARP タイマーの値を変更すると、GVRP だけではなく、スイッチ上で実行している *すべての* GARP アプリケーションに影響を及ぼします（たとえば、GMRP は同じタイマーを使用します）。

デフォルトの GARP タイマー値は、スイッチ上で変更できます。

タイマー値を設定する場合には、**leave** の値を **join** の値の 3 倍以上にしなければなりません（**leave >= join** × 3）。また、**leaveall** の値は、**leave** の値より大きくなければなりません（**leaveall** > **leave**）。

このルールから外れたタイマー値を設定しようとすると、エラーが返されます。たとえば、**leave** タイマーを 600 ミリ秒に設定し、**join** タイマーを 350 ミリ秒に設定しようとすると、エラーになります。この場合、**leave** タイマーを 1050 ミリ秒以上に設定してから、**join** タイマーを 350 ミリ秒に設定してください。

注意 レイヤ 2 で接続されたすべての装置に、同じ GARP タイマー値を設定してください。レイヤ 2 で接続された装置間で GARP タイマーが異なっていると、GARP アプリケーション（たとえば、GMRP および GVRP）が正常に動作しません。

GARP タイマーの値を設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	GARP タイマーの値を設定します。	**set garp timer** {**join** | **leave** | **leaveall**} *timer_value*
ステップ 2	設定を確認します。	**show garp timer**

次に、GARP タイマーを設定し、設定を確認する例を示します。

```
Console> (enable) set garp timer leaveall 10000
GMRP/GARP leaveAll timer value is set to 10000 milliseconds.
Console> (enable) set garp timer leave 600
GMRP/GARP leave timer value is set to 600 milliseconds.
Console> (enable) set garp timer join 200
GMRP/GARP join timer value is set to 200 milliseconds.
Console> (enable) show garp timer
Timer     Timer Value (milliseconds)
--------  --------------------------
Join      200
Leave     600
LeaveAll  10000
Console> (enable)
```

GVRP 統計情報の表示

スイッチ上の GVRP 統計情報を表示するには、次の作業を行います。

作業	コマンド
GVRP 統計情報を表示します。	**show gvrp statistics** [*mod/port*]

次に、ポート 1/1 の GVRP 統計情報を表示する例を示します。

```
Console> (enable) show gvrp statistics 1/1
Join Empty Received:     0
Join In Received:        0
Empty Received:          0
LeaveIn Received:        0
Leave Empty Received:    0
Leave All Received:      40
Join Empty Transmitted:  156
Join In Transmitted:     0
Empty Transmitted:       0
Leave In Transmitted:    0
Leave Empty Transmitted: 0
Leave All Transmitted:   41
VTP Message Received:    0
Console> (enable)
```

GVRP 統計情報の消去

スイッチ上のすべての GVRP 統計情報を消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
GVRP 統計情報を消去します。	**clear gvrp statistics** {*mod/port* | **all**}

次に、スイッチ上のすべての GVRP 統計情報を消去する例を示します。

```
Console> (enable) clear gvrp statistics all
GVRP Statistics cleared for all ports.
Console> (enable)
```

個々の 802.1Q トランク ポート上での GVRP のディセーブル化

個々の 802.1Q トランク ポート上で GVRP をディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	個々の 802.1Q トランク ポート上で GVRP をディセーブルにします。	**set port gvrp disable** *mod/port*
ステップ 2	設定を確認します。	**show gvrp configuration**

次に、802.1Q トランク ポート 1/1 上で GVRP をディセーブルにする例を示します。

```
Console> (enable) set gvrp disable 1/1
GVRP disabled on 1/1.
Console> (enable)
```

GVRP のグローバルなディセーブル化

スイッチ上で GVRP をグローバルにディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
スイッチ上で GVRP をディセーブルにします。	**set gvrp disable**

次に、スイッチ上で GVRP をグローバルにディセーブルにする例を示します。

```
Console> (enable) set gvrp disable
GVRP disabled
Console> (enable)
```

CHAPTER 18

VMPS によるダイナミック ポート VLAN メンバーシップの設定

この章では、Catalyst 6500 シリーズ スイッチ上で VLAN Management Policy Server（VMPS; VLAN マネジメント ポリシー サーバ）を使用して、ダイナミック ポート VLAN（仮想 LAN）メンバーシップを設定する手順について説明します。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

この章で説明する内容は、次のとおりです。

VMPS の機能概要

VMPS により、ポートに接続された装置の送信元 MAC（メディア アクセス制御）アドレスに基づいて、VLAN にスイッチ ポートを動的に割り当てることができます。ネットワーク上のあるスイッチのポートから別のスイッチのポートへホストを移動させると、スイッチによって、そのホストに対応する適切な VLAN に新しいポートが動的に割り当てられます。

VMPS をイネーブルにすると、Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバから MAC アドレス /VLAN マッピング データベースがダウンロードされ、VMPS がクライアント要求の受け入れを開始します。そのあと、スイッチをリセットまたはいったん電源を切ってから再投入した場合には、VMPS データベースが TFTP サーバから自動的にダウンロードされ、VMPS が再びイネーブルになります。

VMPS は、UDP ソケットをオープンにしてクライアントと通信し、クライアント要求を待機します。VMPS サーバは有効なクライアント要求を受け取ると、VMPS データベースで MAC アドレス /VLAN マッピングを検索します。

割り当てられた VLAN が、あるポート グループに制限されている場合、VMPS はそのグループと要求側ポートを比較して確認します。そのポート上で VLAN が有効であれば、VLAN 名をクライアントに返します。VLAN がそのポート上で無効で、かつ VMPS がセキュア モードではない場合には、「アクセス拒否」の応答をホストに送ります。VMPS がセキュア モードの場合には、ポートがシャットダウンされます。

データベースの VLAN とポート上の現在の VLAN が一致せず、かつポート上にアクティブなホストがある場合には、VMPS のセキュア モードに基づいて、VMPS からアクセス拒否またはポート シャットダウン応答を送信します。

代替 VLAN 名を設定できます。データベースに登録されていない MAC アドレスを持つ装置を接続する場合、VMPS は代替 VLAN 名をクライアントに送信します。代替 VLAN 名を設定していない場合で、かつ MAC アドレスがデータベースに含まれていない場合には、VMPS からアクセス拒否応答を送信します。VMPS がセキュア モードの場合には、ポート シャットダウン応答を送信します。

コンフィギュレーション テーブルで、明示的なエントリを作成し、セキュリティ上の理由で特定の MAC アドレスに対するアクセスを禁止することもできます。その場合には、VLAN 名に対して **--NONE--** キーワードを指定します。VMPS からアクセス拒否またはポート シャットダウン応答が送信されます。

Release 6.2(1) より前のソフトウェア リリースでは、ダイナミック ポートは 1 つの*ネイティブ* VLAN にしか属することができませんが、Release 6.2(1) のソフトウェアでは、1 つのポートはネイティブ VLAN と補助 VLAN に属することができます。詳細については、「補助 VLAN によるダイナミック ポート VLAN メンバーシップ」（p.18-16）を参照してください。

リンクをアクティブにすると、ダイナミック ポートはスタティック VLAN から切り離されます。ダイナミック ポート上の新しいホストの最初のパケットの送信元 MAC アドレスが VMPS に送信され、VMPS は、その MAC アドレスを VMPS データベースの VLAN と照合します。MAC アドレスと VLAN が一致すると、VMPS はダイナミック ポートに VLAN 番号を割り当てます。一致しない場合、VMPS は（VMPS セキュア モードの設定に応じて）要求を拒否するか、またはポートをシャットダウンします。

同じ VLAN 上のホストであれば、ダイナミック ポート上で複数のホスト（MAC アドレス）をアクティブにすることができます。ダイナミック ポート上のリンクがダウンすると、ポートは再び切り離された状態になります。そのポート上でホストが再びオンラインになると、VMPS によりホストが再び照合されたあと、ポートが VLAN に割り当てられます。

VMPS およびダイナミック ポートのデフォルト設定

表 18-1 に、VMPS およびダイナミック ポートのデフォルト設定を示します。

表 18-1　VMPS およびダイナミック ポートのデフォルト設定

機能	デフォルト設定
VMPS サーバ	
VMPS のイネーブル ステート	ディセーブル
VMPS 管理ドメイン	ヌル
VMPS TFTP サーバ	none
VMPS データベース コンフィギュレーション ファイル名	*vmps-config-database.1*
VMPS 代替 VLAN	ヌル
VMPS セキュア モード	オープン
VMPS no domain 要求	可能
VMPS クライアント	
VMPS ドメイン サーバ	none
VMPS 再確認間隔	60 分
VMPS サーバ再試行回数	3
ダイナミック ポート	ダイナミック ポートの設定なし

VMPS およびダイナミック ポート VLAN メンバーシップ設定時の注意事項

ダイナミック ポート VLAN メンバーシップ設定時の注意事項について説明します。

- VMPS を設定してから、ダイナミック ポートを設定する必要があります。
- ポートをダイナミックとして設定すると、そのポートに対してスパニングツリーの PortFast が自動的にイネーブルになります。スパニングツリー PortFast が自動的にイネーブルになることにより、不適切な設定が原因で、ホスト上のアプリケーションがタイムアウトし、ループ状態になるのを防止します。ダイナミック ポート上でスパニングツリー PortFast をディセーブルにすることもできます。
- 同一 VLAN 上でスタティック ポートからダイナミック ポートに設定を変更すると、ポートがただちにその VLAN に接続します。ただし、VMPS がダイナミック ポート上の指定ホストの有効性を確認するのは、一定時間経ってからです。
- スタティック セキュア ポートをダイナミック ポートにすることはできません。事前にスタティック セキュア ポートのセキュリティをオフにしてから、ダイナミックにする必要があります。
- トランキングを行っているスタティック ポートをダイナミック ポートにすることはできません。トランク ポートのトランキングをオフにしたあとに、ポートをスタティックからダイナミックに変更する必要があります。

（注） VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）管理ドメインおよび VMPS クライアントと VMPS サーバの管理 VLAN は同じでなければなりません。詳細については、第 10 章「VTP の設定」および第 11 章「VLAN の設定」を参照してください。

スイッチ上での VMPS およびダイナミック ポート VLAN メンバーシップの設定

ここでは、VMPS を設定し、クライアント上でダイナミック ポートを定義する手順について説明します。

VMPS データベースの作成

VMPS を使用するには、VMPS データベースを作成し、TFTP サーバに保存する必要があります。VMPS のパーサは行単位です。ファイルのエントリごとに、行を改める必要があります。ポート番号を範囲で指定することはできません。

（注） ASCII テキストの VMPS データベース コンフィギュレーション ファイルの例については、「VMPS データベース コンフィギュレーション ファイルの例」（p.18-12）を参照してください。

VMPS データベース ファイルを作成する際は、次の注意事項に従ってください。

- VMPS サーバが、異なるタイプのコンフィギュレーション ファイルを誤って読み込むことがないように、コンフィギュレーション ファイルは必ず [VMPS] で開始してください。
- VMPS ドメインの定義 — VMPS ドメインは、スイッチ上で設定されている VTP ドメイン名と対応させる必要があります。
- セキュリティ モードの定義 — VMPS は、オープン モードまたはセキュア モードで動作可能です。
- （任意）代替 VLAN の定義 — 接続ホストの MAC アドレスがデータベースで定義されていない場合、代替 VLAN が割り当てられます。
- MAC アドレス /VLAN 名マッピングの定義 — 各ホストの MAC アドレスと、それぞれが所属する VLAN を入力します。指定したホストのネットワーク接続を禁止するには、VLAN 名として **--NONE--** キーワードを使用します。ポートは、スイッチの IP アドレスとポートのモジュール / ポート番号（*mod/port* の形式）で指定します。
- ポート グループの定義 — ポート グループは、ポートの論理グループです。個々のポートまたはポート グループに VMPS ポリシーを適用できます。キーワード **all-ports** を使用すると、指定したスイッチのすべてのポートを指定することができます。
- VLAN グループの定義 — VLAN グループで、VLAN の論理グループを定義します。論理グループでは、VLAN ポート ポリシーを定義します。
- VLAN ポート ポリシーの定義 — VLAN ポート ポリシーで、制限付き VLAN と対応付けるポートを定義します。制限付き VLAN は、その VLAN が存在できる一連のダイナミック ポートを定義することによって設定します。

VMPS データベースを作成するには、次の作業を行います。

	作業	コマンド
ステップ 1	VLAN に動的に割り当てるホストの MAC アドレスを調べます。	**show cam**
ステップ 2	ワークステーションまたは PC 上で、MAC アドレス /VLAN マッピングを指定した ASCII テキスト ファイルを作成します。	–
ステップ 3	ASCII テキスト ファイルを TFTP サーバに転送し、スイッチにダウンロードできるようにします。	–

VMPS の設定

VMPS をイネーブルに設定すると、TFTP サーバまたは Remote Copy Protocol（RCP）サーバから VMPS データベースがダウンロードされ、VMPS 要求の受け入れが開始されます。

VMPS を設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ダウンロード方式を指定します。	**set vmps downloadmethod rcp** | **tftp** [*username*]
ステップ 2	ASCII テキストの VMPS データベース コンフィギュレーション ファイルを保存する TFTP サーバまたは RCP サーバの IP アドレスを設定します。	**set vmps downloadserver** *ip_addr* [*filename*]
ステップ 3	VMPS をイネーブルにします。	**set vmps state enable**
ステップ 4	VMPS の設定を確認します。	**show vmps**

次に、スイッチ上で VMPS をイネーブルにする例を示します。

```
Console> (enable) set vmps state enable
Vlan Membership Policy Server enable is in progress.
Console> (enable)
```

VMPS をディセーブルするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	VMPS をディセーブルにします。	**set vmps state disable**
ステップ 2	VMPS がディセーブルに設定されていることを確認します。	**show vmps**

次に、スイッチ上で VMPS をディセーブルにする例を示します。

```
Console> (enable) set vmps state disable
All the VMPS configuration information will be lost and the resources released on
disable.
Do you want to continue (y/n[n]): y
Vlan Membership Policy Server disabled.
Console> (enable)
```

VMPS クライアント上でのダイナミック ポートの設定

VMPS クライアント スイッチ上でダイナミック ポートを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	VMPS サーバ（VMPS がイネーブルに設定されているスイッチ）の IP アドレスを指定します。	**set vmps server** *ip_addr* [**primary**]
ステップ 2	VMPS サーバの指定を確認します。	**show vmps server**
ステップ 3	ポートにダイナミック VLAN メンバーシップの割り当てを設定します。	**set port membership** *mod*/*port* **dynamic**
ステップ 4	ダイナミック ポートの割り当てを確認します。	**show port** [*mod*[*/port*]]

次に、VMPS サーバを指定および確認し、ダイナミック ポートを割り当て、設定を確認する例を示します。

```
Console> (enable) show vmps server
VMPS domain server VMPS Status
--------------------------------------
192.0.0.6
192.0.0.1       primary
192.0.0.9
Console> (enable) set port membership 3/1-3 dynamic
Ports 3/1-3 vlan assignment set to dynamic.
Spantree port fast start option enabled for ports 3/1-3.
Console> (enable) set port membership 1/2 dynamic
Trunking port 1/2 vlan assignment cannot be set to dynamic.
Console> (enable) set port membership 2/1 dynamic
ATM LANE port 2/1 vlan assignment can not be set to dynamic.
Console> show port
Port   Name     Status   Vlan    Level     Duplex       Speed       Type
1/1             connect  dyn-3   normal    full         100         100 BASE-TX
1/2             connect  trunk   normal    half         100         100 BASE-TX
2/1             connect  trunk   normal    full         155         OC3 MMF ATM
3/1             connect  dyn-5   normal    half         10          10 BASE-T
3/2             connect  dyn-5   normal    half         10          10 BASE-T
3/3             connect  dyn-5   normal    half         10          10 BASE-T
Console> (enable)
```

（注） ポートに対応する VLAN が割り当てられていない場合には、**show port** コマンドの出力で、VLAN の欄に *dyn-* が表示されます。

VMPS の管理およびモニタ

MAC アドレス /VLAN マッピング情報を表示するには、イネーブル モードで次のいずれかの作業を行います。

作業	コマンド
データベースで MAC アドレスがマッピングされている VLAN を表示します。	**show vmps mac** [*mac_address*]
データベースで VLAN にマッピングされている MAC アドレスを表示します。	**show vmps vlan** [*vlan_name*]
制限付き VLAN に属するポートを表示します。	**show vmps vlanports** [*vlan_name*]

VMPS 統計情報を表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
VMPS 統計情報を表示します。	**show vmps statistics**

VMPS 統計情報を消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
VMPS 統計情報を消去します。	**clear vmps statistics**

VMPS サーバ エントリを消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
VMPS サーバ エントリを消去します。	**clear vmps server** *ip_addr*

ダイナミック ポート VLAN メンバーシップの割り当てを再確認するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ダイナミック ポート VLAN メンバーシップを再確認します。	**reconfirm vmps**
ステップ 2	ダイナミック VLAN 再確認ステータスを表示します。	**show dvlan statistics**

次に、ダイナミック ポート VLAN メンバーシップの割り当てを再確認する例を示します。

```
Console> (enable) reconfirm vmps
reconfirm process started
Use 'show dvlan statistics' to see reconfirm status
Console> (enable)
```

VMPS データベースを手動でダウンロードするには（変更されたデータベース コンフィギュレーション ファイルをダウンロードする、またはダウンロードの失敗後に再試行するには）、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	TFTP サーバから VMPS データベースをダウンロードするか、異なる VMPS データベース コンフィギュレーション ファイルを指定します。	**download vmps**
ステップ 2	VMPS データベース コンフィギュレーション ファイルを確認します。	**show vmps**

スタティック VLAN ポート メンバーシップの設定

ポートをスタティック VLAN ポート メンバーシップに戻すには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポートにスタティック VLAN メンバーシップの割り当てを設定します。	**set port membership** *mod*/*port* **static**
ステップ 2	スタティック ポートの割り当てを確認します。	**show port** [*mod*[/*port*]]

次に、ポートをスタティック VLAN ポート メンバーシップに戻す例を示します。

```
Console> (enable) set port membership 3/1 static
Port 3/1 vlan assignment set to static.
Console> (enable)
```

VMPS コンフィギュレーション ファイルのバックアップ

VMPS クライアントおよびサーバがオンラインに戻る際に電源のシャットダウン後の遅延を避けるには、VMPS コンフィギュレーション ファイルのバックアップ機能を使用します。電源のシャットダウン後、クライアントが送信した VMPS 要求は、VMPS サーバが VMPS コンフィギュレーション ファイルを VMPS サーバからダウンロードするまで、TFTP サーバによってキューに入れられます。クライアント アクセスがシステム再起動時に確実に遅延しないようにするために、VMPS コンフィギュレーションをローカルにバックアップして、現在の VMPS コンフィギュレーション ファイルをリモート TFTP サーバからダウンロードするまで、そのファイルを使用するようにスイッチを設定できます。

VMPS コンフィギュレーション ファイルをバックアップするようにスイッチを設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
手動で VMPS コンフィギュレーション ファイルをバックアップします。 **（注）** ファイル名を指定しない場合、VMPS コンフィギュレーション ファイルは **vmps-backup-config-database.1** として保存されます。	**set vmps config-file device:**[**filename**]
VMPS コンフィギュレーション ファイルの自動バックアップをイネーブルにします。	**set vmps config-file auto-save enable | disable**
設定を確認します。	**show vmps**

次に、VMPS コンフィギュレーション ファイルを手動でバックアップする例を示します。

```
Console> (enable) set vmps config-file disk0:
Vlan Membership Policy Server back-up file name is set to disk0:vmps-backup-conf
ig-database.1.
Console> (enable)
```

次に、VMPS コンフィギュレーション ファイルを自動的にバックアップするようにシステムを設定する例を示します。

```
Console> (enable) set vmps config-file auto-save enable
Auto save to store Vlan Membership Policy Server configuration file is enabled.
Console> (enable)
```

次に、設定を確認する例を示します。

```
Console> show vmps
VMPS Server Status:
-------------------
Management Domain        (null)
State                    disabled
Operational Status       inactive
TFTP Server              default
TFTP File                vmps-config-database.1
Fallback VLAN            (null)
Secure Mode              open
VMPS No Domain Req       allow
VMPS Backup file name    disk0:vmps-backup-config-database.1
VMPS Auto-Save state     enabled

VMPS Client Status:
---------------------
VMPS VQP Version:     1
Reconfirm Interval:   60 min
Server Retry Count:   3
VMPS domain server:

No dynamic ports configured.
Console>
```

VMPS およびダイナミック ポート VLAN メンバーシップのトラブルシューティング

ここでは、VMPS およびダイナミック ポート VLAN メンバーシップのトラブルシューティング方法について説明します。

VMPS のトラブルシューティング

表 18-2 に、**set vmps state enable** コマンドまたは **download vmps** コマンドを入力したときに表示される VMPS エラー メッセージを示します。

表 18-2　VMPS のエラー メッセージ

VMPS のエラー メッセージ	対処方法
`TFTP server IP address is not configured.`	**set vmps tftpserver** *ip_addr* [*filename*] コマンドを使用して TFTP サーバのアドレスを指定します。
`Unable to contact the TFTP server 172.16.254.222.`	（**set ip route** コマンドを使用して）TFTP サーバへのスタティック ルートを入力します。
`File "vmps_configuration.db" not found on the TFTP server 172.16.254.222.`	TFTP サーバで VMPS データベース コンフィギュレーション ファイルのファイル名を確認します。アクセス権が正しく設定されているかどうかを確認します。
`Enable failed due to insufficient resources.`	スイッチのリソース不足が原因で、データベースを実行できません。DRAM を拡張することによって、この問題を解決できます。

VMPS は、VMPS データベース コンフィギュレーション ファイルが正常にダウンロードされたあとで、ファイルを解析し、データベースを作成します。解析が完了すると、解析した総行数および解析エラーの数を示した統計情報が出力されます。

VMPS 解析エラーの詳細を調べるには、**set logging level vmps 3** コマンドを使用して、VMPS の Syslog レベルを 3 に設定します。

ダイナミック ポート VLAN メンバーシップのトラブルシューティング

次の状況が発生すると、ダイナミック ポートはシャットダウンする可能性があります。

- VMPS　がセキュア　モードで、かつホストがポートへ接続することが認められていない場合。ポートは、ホストをネットワークへ接続させないためにシャットダウンします。
- ダイナミック ポート上のアクティブ ホストが 50 を超過している場合。

シャットダウンしたダイナミック ポートを再びイネーブルにするには、**set port enable** *mod/port* コマンドを使用します。

VMPS によるダイナミック ポート VLAN メンバーシップの設定例

ここでは、VMPS およびダイナミック ポートを設定する例を紹介します。

VMPS データベース コンフィギュレーション ファイルの例

次に、VMPS データベース コンフィギュレーション ファイルの例を示します。VMPS データベース コンフィギュレーション ファイルは、ASCII テキスト ファイルであり、VMPS サーバとして動作するスイッチからアクセスできる TFTP サーバ上に保存します。この設定例の概要は次のとおりです。

- セキュリティ モードがオープンしています。
- 代替 VLAN には、デフォルトを使用します。
- MAC アドレス /VLAN 名のマッピング ― 各ホストの MAC アドレスと、それぞれが所属する VLAN を定義します。
- ポート グループを定義します。
- VLAN グループを定義します。
- 制限付き VLAN に対応付けるポートの VLAN ポート ポリシーを定義します。

```
!VMPS File Format, version 1.1
! Always begin the configuration file with
! the word "VMPS"
!
!vmps domain <domain-name>
! The VMPS domain must be defined.
!vmps mode {open | secure}
! The default mode is open.
!vmps fallback <vlan-name>
!vmps no-domain-req { allow | deny }
!
! The default value is allow.
vmps domain WBU
vmps mode open
vmps fallback default
vmps no-domain-req deny
!
!
!MAC Addresses
!
vmps-mac-addrs
!
! address <addr> vlan-name <vlan_name>
!
address 0012.2233.4455 vlan-name hardware
address 0000.6509.a080 vlan-name hardware
address aabb.ccdd.eeff vlan-name Green
address 1223.5678.9abc vlan-name ExecStaff
address fedc.ba98.7654 vlan-name --NONE--
address fedc.ba23.1245 vlan-name Purple
!
!Port Groups
!
!vmps-port-group <group-name>
! device <device-id> { port <port-name> | all-ports }
!
vmps-port-group WiringCloset1
 device 198.92.30.32 port 3/2
 device 172.20.26.141 port 2/8
vmps-port-group "Executive Row"
```

```
 device 198.4.254.222 port 1/2
 device 198.4.254.222 port 1/3
 device 198.4.254.223 all-ports
!
!
!VLAN groups
!
!vmps-vlan-group <group-name>
! vlan-name <vlan-name>
!
vmps-vlan-group Engineering
vlan-name hardware
vlan-name software
!
!
!VLAN port Policies
!
!vmps-port-policies {vlan-name <vlan_name> | vlan-group <group-name> }
! { port-group <group-name> | device <device-id> port <port-name> }
!
vmps-port-policies vlan-group Engineering
 port-group WiringCloset1
vmps-port-policies vlan-name Green
 device 198.92.30.32 port 4/8
vmps-port-policies vlan-name Purple
 device 198.4.254.22 port 1/2
 port-group "Executive Row"
```

ダイナミック ポート VLAN メンバーシップの設定例

図 18-1 に、VMPS サーバ スイッチと、ダイナミック ポートのある VMPS クライアント スイッチで構成されるネットワークを示します。この例の前提条件は次のとおりです。

- VMPS サーバおよび VMPS クライアントは、それぞれ別個のスイッチです。
- スイッチ 1 は、プライマリ VMPS サーバです。
- スイッチ 3 およびスイッチ 10 は、セカンダリ VMPS サーバです。
- エンド ステーションは次のクライアントに接続されています。
  - スイッチ 2
  - スイッチ 9
- データベース コンフィギュレーション ファイルは、Bldg-G.db という名前で、IP アドレスが 172.20.22.7 の TFTP サーバ上に保存されています。

VMPS とダイナミック ポートを設定するには、次の手順を実行します。

ステップ 1　スイッチ 1 をプライマリ VMPS サーバとして設定します。

a. ASCII ファイルを保存する TFTP サーバの IP アドレスを設定します。

```
Console> (enable) set vmps tftpserver 172.20.22.7 Bldg-G.db
```

b. VMPS をイネーブルにします。

```
Console> (enable) set vmps state enable
```

これらのコマンドを入力すると、ファイル Bldg-G.db がスイッチ 1 にダウンロードされます。スイッチ 1 が VMPS サーバになります。

ステップ 2　各 VMPS クライアント上で VMPS サーバ アドレスを設定します。

a. プライマリ VMPS サーバの IP アドレスを設定します。

```
Console> (enable) set vmps server 172.20.26.150 primary
```

b. セカンダリ VMPS サーバの IP アドレスを設定します。

```
Console> (enable) set vmps server 172.20.26.152

Console> (enable) set vmps server 172.20.26.159
```

c. VMPS サーバのアドレスを確認します。

```
Console> (enable) show vmps server
```

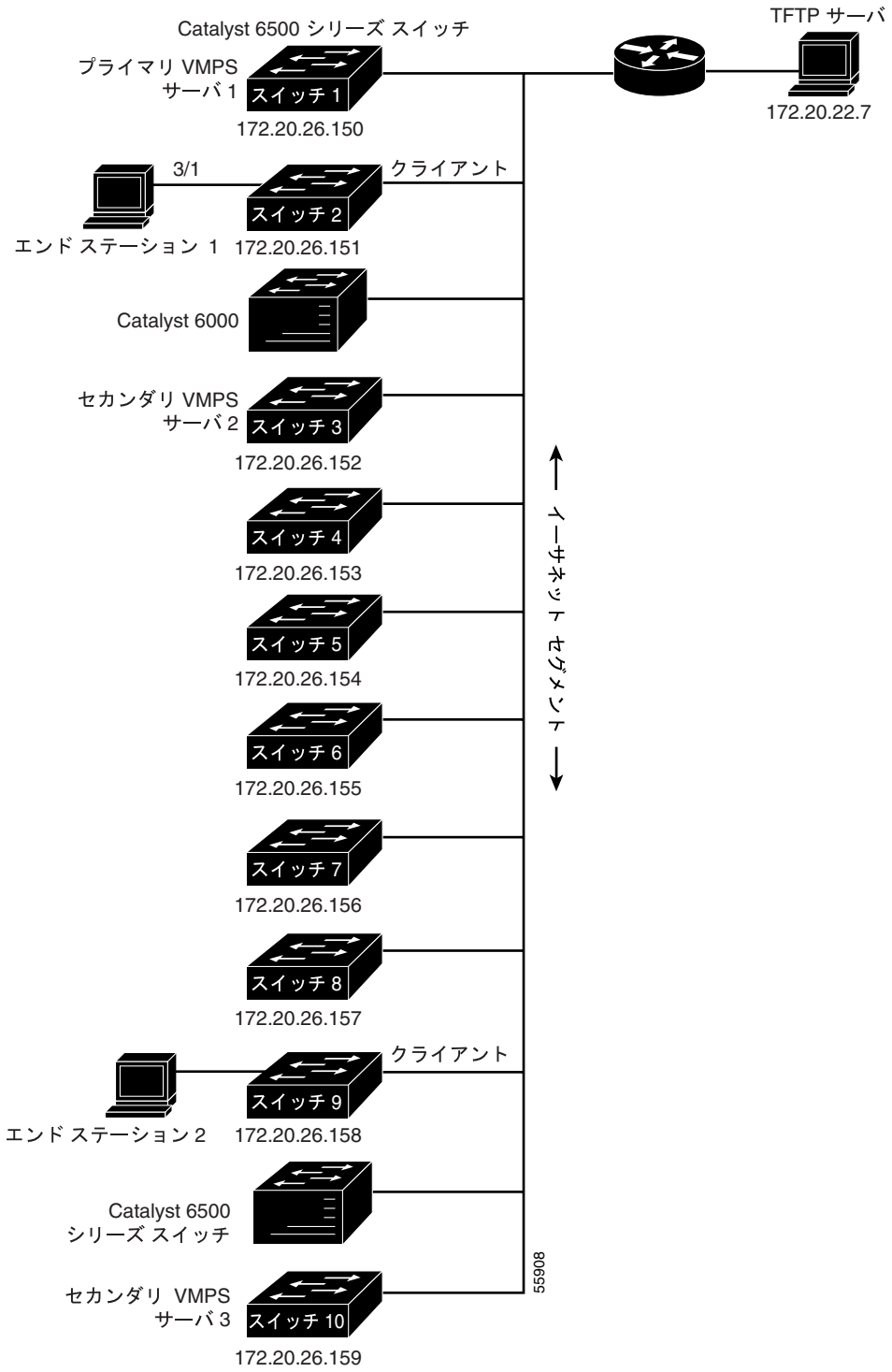
ステップ 3　スイッチ 2 上のポート 3/1 をダイナミック ポートとして設定します。

```
Console> (enable) set port membership 3/1 dynamic
```

ステップ 4　ポート 3/1 上のエンド ステーション 2 を接続します。エンド ステーション 2 がパケットを送信すると、スイッチ 2 がプライマリ VMPS サーバであるスイッチ 1 にクエリを送ります。スイッチ 1 は、ポート 3/1 に割り当てる VLAN を応答として返します。ダイナミック ポートではデフォルトとして、スパニングツリー PortFast モードがイネーブルなので、ポート 3/1 はただちに接続されて転送モードになります。

ステップ 5　ステップ 2 およびステップ 3 を繰り返して、VMPS サーバ アドレスを設定し、各 VMPS クライアント スイッチ上にダイナミック ポートを割り当てます。

図 18-1　ダイナミック ポート VLAN メンバーシップの構成



補助 VLAN によるダイナミック ポート VLAN メンバーシップ

(注)　この機能では Release 6.2(1) 以降のソフトウェア リリースが必要です。

ここでは、ネイティブと外部の 2 つの VLAN に属するように、ダイナミック ポートを設定する手順について説明します。ここでは、次の用語を使用します。

- 補助 VLAN ― IP Phone 用の個別の VLAN
- ネイティブ VLAN ― データ用の従来の VLAN
- 補助 VLAN ID ― 補助 VLAN の VLAN ID
- ネイティブ VLAN ID ― ネイティブ VLAN の VLAN ID

Release 6.2(1) より前のソフトウェア リリースでは、ダイナミック ポートは 1 つの VLAN にしか属することができませんでした。また、ネイティブ VLAN と補助 VLAN を備えたポートに対してダイナミック ポート VLAN 機能をイネーブルに設定できませんでした。

一方、Release 6.2(1) 以降のソフトウェア リリースでは、ダイナミック ポートは 2 つの VLAN に属することができます。IP Phone との接続を設定するスイッチ ポートで、次のトラフィックを伝送するように、個別の VLAN を設定できます。

- IP Phone との間の音声トラフィック（補助 VLAN）
- IP Phone（ネイティブ VLAN）の *アクセス ポート*を介してスイッチに接続する PC との間のデータ トラフィック

ここでは、設定時の注意事項および制限事項について説明します。

- 補助 VLAN によるダイナミック ポート VLAN メンバーシップの注意事項（p.18-16）
- 補助 VLAN によるダイナミック ポート VLAN メンバーシップの設定（p.18-17）

(注)　補助 VLAN および Cisco Voice over IP（VoIP）ネットワークの詳細については、第 53 章「VoIP ネットワークの設定」を参照してください。

補助 VLAN によるダイナミック ポート VLAN メンバーシップの注意事項

ここでは、補助 VLAN 用にダイナミック ポート VLAN メンバーシップを設定する際の注意事項と制限事項について説明します。

- ネイティブ VLAN ID の設定は、IP Phone のアクセス ポートに接続した PC に対しては動的です。一方、補助 VLAN ID の設定は動的ではないので、手動で設定する必要があります。補助 VLAN ID の設定は手動で行われるので、VMPS サーバは、IP Phone から着信するパケットではなく PC から着信するパケットに対して照会されます。
- Cisco Discovery Protocol（CDP）パケットを除いた IP Phone からのすべてのパケットは、補助 VLAN ID でタグが付けられます。補助 VLAN ID でタグが付けられたパケットはすべて、IP Phone からのパケットとみなされ、残りのパケットは PC からのパケットとみなされます。
- 802.1p またはタグなしフレームで補助 VLAN ID を設定する場合は、IP Phone の MAC アドレスで VMPS サーバを設定する必要があります（VMPS の設定については、「VMPS によるダイナミック ポート VLAN メンバーシップの設定例」[p.18-12] を参照）。
- ダイナミック ポートの場合、補助 VLAN ID は、ダイナミック ポート用に VMPS によって割り当てられたネイティブ VLAN ID と同じ設定にすることはできません。
- ポートの設定に際しては、事前に「VMPS およびダイナミック ポート VLAN メンバーシップ設定時の注意事項」（p.18-3）を参照してください。

補助 VLAN によるダイナミック ポート VLAN メンバーシップの設定

補助 VLAN でダイナミック ポート VLAN メンバーシップを設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
補助 VLAN でダイナミック ポート VLAN メンバーシップを設定します。	**set port auxiliaryvlan** *mod*[/*port*] {*vlan* | **untagged** | **dot1p** | **none**} **[cdpverify** {**enable** | **disable**}]

次に、補助 VLAN に音声ポートを追加し、カプセル化タイプを指定する方法を示します。

```
Console> (enable) set port auxiliaryvlan 5/9 222
Auxiliaryvlan 222 configuration successful.
AuxiliaryVlan AuxVlanStatus Mod/Ports
------------- ------------- ------------------------
222           active        5/9
Console> (enable)

Console> (enable) set port auxiliaryvlan 5/9 dot1p
Port 5/9 allows the connected device send and receive packets with 802.1p priority.
Console> (enable)
```

次に、ダイナミック ポートとしてポート 5/9 を指定する例を示します。

```
Console> (enable) set port membership 5/9 dynamic
Warning: Auxiliary Vlan set to dot1p|untagged on dynamic port. VMPS will be queried
for IP phones.
Port 5/9 vlan assignment set to dynamic.
Spantree port fast start option enabled for ports 5/9.
Console> (enable)
```

次に、指定された補助 VLAN ID をネイティブ VLAN ID と同じ設定にできない例を示します。

```
Console> (enable) set port auxiliaryvlan 5/10 223
Auxiliary vlan cannot be set to 223 as PVID=223.
Console> (enable)
```

■ 補助 VLAN によるダイナミック ポート VLAN メンバーシップ

CHAPTER 19

ステータスおよび接続の確認

この章では、Catalyst 6500 シリーズ スイッチ上でステータスおよび接続を確認する方法について説明します。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

この章で説明する内容は、次のとおりです。

モジュール ステータスの確認

Catalyst 6500 シリーズ スイッチは、マルチモジュール システムです。スイッチに搭載されているモジュール、MAC（メディア アクセス制御）アドレス範囲、および各モジュールのバージョン番号を調べるには、**show module** [*mod*] コマンドを使用します。各モジュールの詳細情報を表示するには、そのモジュールの番号を指定します。

モジュールのステータスを確認するには、ユーザ モードで次の作業を行います。

作業	コマンド
モジュール ステータスを確認します。	**show module** [*mod*]

次に、モジュール ステータスを確認する例を示します。出力では、シャーシにはスーパバイザ エンジンが 1 つ、他のモジュールが 4 つ搭載されていることを示しています。

```
Console> (enable) show module
Mod Slot Ports Module-Type               Model               Status
--- ---- ----- ------------------------- ------------------- --------
1   1    2     1000BaseX Supervisor      WS-X6K-SUP1-2GE     ok
2   2    24    100BaseFX MM Ethernet     WS-X6224-100FX-MT   ok
3   3    8     1000BaseX Ethernet        WS-X6408-GBIC       ok
4   4    48    10/100BaseTX (Telco)      WS-X6248-TEL        ok
5   5    48    10/100BaseTX (RJ-45)      WS-X6248-RJ-45      ok

Mod Module-Name         Serial-Num
--- ------------------- -----------
1                       SAD03040546
2                       SAD03110020
3                       SAD03070194
4                       SAD03140787
5                       SAD03181291

Mod MAC-Address(es)                         Hw     Fw          Sw
--- --------------------------------------- ------ ----------- ------------------
1   00-50-f0-a8-26-b2 to 00-50-f0-a8-26-b3 1.4    5.1(1)      5.2(1)CSX
    00-50-f0-a8-26-b0 to 00-50-f0-a8-26-b1
    00-50-3e-8d-64-00 to 00-50-3e-8d-67-ff
2   00-50-54-6c-e9-a8 to 00-50-54-6c-e9-bf 1.3    4.2(0.24)V 5.2(1)CSX
3   00-50-54-6c-93-6c to 00-50-54-6c-93-73 1.4    4.2(0.24)V 5.2(1)CSX
4   00-50-54-bf-59-64 to 00-50-54-bf-59-93 0.103  4.2(0.24)V 5.2(1)CSX
5   00-50-f0-ac-30-54 to 00-50-f0-ac-30-83 1.0    4.2(0.24)V 5.2(1)CSX

Mod Sub-Type                Sub-Model           Sub-Serial  Sub-Hw
--- ----------------------- ------------------- ----------- ------
1   L2 Switching Engine I   WS-F6020            SAD03040312 1.0
Console> (enable)
```

次に、特定のモジュールのステータスを確認する例を示します。

```
Console> (enable) show module 4
Mod Slot Ports Module-Type               Model               Status
--- ---- ----- ------------------------- ------------------- --------
4   4    48    10/100BaseTX (Telco)      WS-X6248-TEL        ok

Mod Module-Name         Serial-Num
--- ------------------- -----------
4                       SAD03140787

Mod MAC-Address(es)                         Hw     Fw          Sw
--- --------------------------------------- ------ ----------- ------------------
4   00-50-54-bf-59-64 to 00-50-54-bf-59-93 0.103  4.2(0.24)V 5.2(1)CSX
Console> (enable)
```

ポート ステータスの確認

スイッチ ポート上のサマリーまたは詳細情報を表示するには、**show port** [*mod*[/*port*]] コマンドを使用します。引数を指定せずに **show port** コマンドを入力すると、スイッチ上のすべてのポートのサマリー情報が表示されます。特定のモジュール番号を指定すると、そのモジュールのポート情報だけが表示されます。モジュール番号およびポート番号の両方を指定すると、指定したポートの詳細情報が表示されます。

特定のポートにコンフィギュレーション コマンドを適用するには、対応する論理モジュールを指定する必要があります。詳細については、「モジュール ステータスの確認」（p.19-2）を参照してください。

ポートのステータスを確認するには、ユーザ モードで次の作業を行います。

作業	コマンド
ポート ステータスを確認します。	**show port** [*mod*[/*port*]]

次に、特定モジュールだけのポート情報を表示する例を示します。

```
Console> (enable) show port 1
Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 1/1                     connected  1            full  1000 1000BaseSX
 1/2                     notconnect 1            full  1000 1000BaseSX

Port  Security Secure-Src-Addr   Last-Src-Addr     Shutdown Trap     IfIndex
----- -------- ----------------- ----------------- -------- -------- -------
 1/1  disabled                                     No       disabled 3
 1/2  disabled                                     No       disabled 4

Port     Broadcast-Limit Broadcast-Drop
-------- --------------- --------------------
 1/1                   -                    0
 1/2                   -                    0

Port   Send FlowControl    Receive FlowControl   RxPause    TxPause
       admin    oper       admin    oper
-----  -------- --------   -------- --------     ---------- ----------
 1/1   desired  off        off      off          0          0
 1/2   desired  off        off      off          0          0

Port  Status     Channel    Admin Ch    Neighbor                            Neighbor
                 Mode       Group Id    Device                                 Port
----- ---------- ---------  ----- ----- ----------------------------------- -----
 1/1  connected  auto       65    0
 1/2  notconnect auto       65    0

Port  Align-Err  FCS-Err    Xmit-Err   Rcv-Err    UnderSize
----- ---------- ---------- ---------- ---------- ---------
 1/1           0          0          0          0         0
 1/2           0          0          0          0         0

Port  Single-Col Multi-Coll Late-Coll  Excess-Col Carri-Sen Runts     Giants
----- ---------- ---------- ---------- ---------- --------- --------- ---------
 1/1           0          0          0          0         0         0         0
 1/2           0          0          0          0         0         0         0

Last-Time-Cleared
--------------------------
Tue Jun 8 1999, 10:01:35
Console> (enable)
```

次に、個々のポートの詳細情報を表示する例を示します。

```
Console> (enable) show port 1/1
Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 1/1                     connected  1            full  1000 1000BaseSX

Port  Security Secure-Src-Addr   Last-Src-Addr     Shutdown Trap     IfIndex
----- -------- ----------------- ----------------- -------- -------- -------
 1/1  disabled                                     No       disabled 3

Port     Broadcast-Limit Broadcast-Drop
-------- --------------- --------------------
 1/1                   -                    0
Port   Send FlowControl    Receive FlowControl   RxPause    TxPause
       admin    oper       admin    oper
-----  -------- --------   -------- --------     ---------- ----------
 1/1   desired  off        off      off          0          0

Port  Status     Channel   Admin Ch    Neighbor                            Neighbor
                 Mode      Group Id    Device                                 Port
----- ---------- --------- ----- ----- ----------------------------------- -----
 1/1  connected  auto      65    0

Port  Align-Err  FCS-Err    Xmit-Err   Rcv-Err    UnderSize
----- ---------- ---------- ---------- ---------- ---------
 1/1           0          0          0          0         0

Port  Single-Col Multi-Coll Late-Coll  Excess-Col Carri-Sen Runts     Giants
----- ---------- ---------- ---------- ---------- --------- --------- ---------
 1/1           0          0          0          0         0         0         0

Last-Time-Cleared
--------------------------
Tue Jun 8 1999, 10:01:35
Console> (enable)
```

ポートの MAC アドレスの表示

show module コマンドを使用してモジュールの MAC アドレス範囲を表示するほかに、**show port mac-address** [*mod*[/*port*]] コマンドで、特定のスイッチ ポートの MAC アドレスを表示することもできます。

特定のポートの MAC アドレスを表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
特定のポートの MAC アドレスを表示します。	**show port mac-address** [*mod*[/*port*]]

次に、特定のポートの MAC アドレスを表示する例を示します。

```
Console> show port mac-address 4/1
Port  Mac address
----- -----------------------
 4/1  00-50-54-bf-59-64
```

次に、モジュール上のすべてのポートの MAC アドレスを表示する例を示します。

```
Console> show port mac-address 4
Port  Mac address
----- -----------------------
 4/1  00-50-54-bf-59-64
 4/2  00-50-54-bf-59-65
 4/3  00-50-54-bf-59-66
 4/4  00-50-54-bf-59-67

...

 4/47 00-50-54-bf-59-92
 4/48 00-50-54-bf-59-93
```

ポート機能の表示

スイッチのポート機能を表示するには、**show port capabilities** [[*mod*][/*port*]] コマンドを使用します。

特定のポートの機能を表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
特定のポートの機能を表示します。	**show port capabilities** [*mod*[/*port*]]

次に、スイッチ ポートの機能を表示する例を示します。

```
Console> (enable) show port capabilities 1/1
Model                     WS-X6K-SUP1A-2GE
Port                      1/1
Type                      No Connector
Speed                     1000
Duplex                    full
Trunk encap type          802.1Q,ISL
Trunk mode                on,off,desirable,auto,nonegotiate
Channel                   yes
Broadcast suppression     percentage(0-100)
Flow control              receive-(off,on,desired),send-(off,on,desired)
Security                  yes
Membership                static,dynamic
Fast start                yes
QOS scheduling            rx-(1p1q4t),tx-(1p2q2t)
CoS rewrite               yes
ToS rewrite               DSCP
UDLD                      yes
Inline power              no
AuxiliaryVlan             no
SPAN                      source,destination
COPS port group           1/1-2
Console> (enable)
```

10 ギガビット イーサネット リンクのステータスの確認

ケーブル診断機能で、10 ギガビット イーサネット リンクの Pseudo Random Binary Sequence（PRBS）テストをアクティブにできます。

（注） PRBS テストは、現在、1 ポート 10GBASE-E シリアル 10 ギガビット イーサネット モジュール（WS-X6502-10GE）で使用できます。

2 つの装置間で PRBS テストを適切に実行するには、ケーブルの両端でテストを開始する必要があります。ケーブルがループ バックの場合、単一エンドでテスト シーケンスを生成し（Tx）、テスト シーケンスを確認し、エラーをカウントします（Rx）。

PRBS テストの開始前に、ポートは自動的に errdisable ステートになります。errdisable タイムアウトはポートでディセーブルなので、タイムアウト インターバルの経過後もポートは自動的に再びイネーブルになりません。errdisable タイムアウトは、PRBS テストの終了後に自動的に再びイネーブルになります。

PRBS テストを実行中、システムは **set port enable** および **set port disable** コマンドの入力を許可しません。

PRBS エラー カウンタは、ケーブルの信頼性を測定します。エラー カウンタの範囲は、0 ～ 255 です。値が 0 の場合はリンク接続が完全であることを示し、値が 255 の場合はポートが不良か、接続されていないか、またはリンクを介した通信がないことを示します。あらかじめ決められた時間カウンタが 0 のままでない場合、リンクは不良です。たとえば、Baud Error Rate（BER）が 10^-12 の場合、カウンタは 100 秒間 0 にならなければなりません。

show port prbs コマンドで PRBS にアクセスするたびに、PRBS エラー カウンタ値は 0 にリセットされ、再びエラーの累算を開始します。

（注） PRBS　カウンタは「読み取りおよび消去」レジスタです。シーケンスにおける最初の読み取りは、通常信頼性が低くカウンタを消去するためのもので、次の読み取りが正確なものです。

PRBS テストを開始または停止するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	PRBS テストを開始または停止します。	**test cable-diagnostics prbs** {**start** | **stop**} *mod/port*
ステップ 2	PRBS テスト カウンタ情報を表示します。	**show port prbs**

次に、モジュール 5 のポート 1 上で、PRBS テストを開始する例を示します。

```
Console> (enable) test cable-diagnostics prbs start 5/1
PRBS cable-diagnostic test started on port 5/1.
Console> (enable)
```

次に、モジュール 5 のポート 1 上で、PRBS テストを停止する例を示します。

```
Console> (enable) test cable-diagnostics prbs stop 5/1
PRBS cable-diagnostic test stopped on port 5/1.
Console> (enable)
```

次に、PRBS テストがモジュール上でサポートされていない場合に表示されるメッセージの例を示します。

```
Console> (enable) test cable-diagnostics prbs start 6/1
Feature not supported on module 6.
Console> (enable)
```

次に、PRBS カウンタ値および PRBS テストを実行しているポートを表示する例を示します。

```
Console> (enable) show port prbs
Port PRBS state Error Counters
6/1 start 30
7/1 stop -
Console> (enable)
```

TDR によるケーブル ステータスの確認

銅ケーブルのステータスを確認するには、モジュールで Time Domain Reflectometer（TDR; タイムドメイン反射率計）を使用します。TDR をサポートするモジュールは、WS-X6148-GE-TX、WS-X6148V-GE-TX、WS-X6548-GE-TX、WS-X6548V-GE-TX, WS-X6548-GE-45AF、WS-X6748-GE-TX、WS-X6148A-GE-TX、WS-X6148-GE-45AF、WS-X6148A-GE-45AF、WS-X6148A-RJ-45、および WS-X6148A-45AF です。TDR は、まず信号をケーブルに送信し、反射して戻ってきた信号を読み取ることでケーブルの不良を検出します。信号の全部または一部が、ケーブルの不良箇所またはケーブルの終端から反射して戻ってきます。

リンクを確立できない場合、TDR を使用してケーブルが不良であるかどうかを判定します。このテストは、既存スイッチの交換、ギガビット イーサネットへのアップグレード、または新しいケーブル プラントを導入する際に特に重要になります。

TDR テストを開始または停止するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	TDR テストを開始または停止します。	**test cable-diagnostics tdr** {**start** | **stop**} *mod/port*
ステップ 2	TDR テスト カウンタ情報を表示します。	**show port tdr**

次に、モジュール 2 のポート 1 上で、TDR テストを開始する例を示します。

```
Console> (enable) test cable-diagnostics tdr start 2/1
TDR test started on port 2/1. Use show port tdr <m/p> to see the results
Console> (enable)
```

次に、モジュール 2 のポート 1 上で、TDR テストを停止する例を示します。

```
Console> (enable) test cable-diagnostics tdr stop 2/1
tdr cable-diagnostic test stopped on port 2/1.
Console> (enable)
```

次に、TDR テストがモジュール上でサポートされていない場合に表示されるメッセージの例を示します。

```
Console> (enable) test cable-diagnostics tdr start 2/1
Feature not supported on module 2.
Console> (enable)
```

次に、ポートの TDR テスト結果を表示する例を示します。

```
Console> (enable) show port tdr 2/1
TDR test last run on Mon, March 10 2003 at 1:35:00 pm
Port  Speed  Local pair  Pair length         Remote pair  Pair status
----- ------ ----------- ------------------- ------------ ------------
2/1   1000   Pair A      12  +/- 3 meters    Pair A       Terminated
             Pair B      12  +/- 3 meters    Pair B       Terminated
             Pair C      12  +/- 3 meters    Pair C       Terminated
             Pair D      12  +/- 3 meters    Pair D       Terminated
```

Telnet の使用方法

Telnet を使用して、スイッチの CLI（コマンドライン インターフェイス）にアクセスできます。また、Telnet を使用して、スイッチからネットワーク上の他の装置にアクセスできます。同時に最大 8 つの Telnet セッションを実行できます。

スイッチからネットワーク上の他の装置に Telnet 接続するには、イネーブル モードで次の作業を行います。

作業	コマンド
リモート ホストとの Telnet セッションを開始します。	**telnet** *host* [*port*]

次に、スイッチからリモート ホストに Telnet で接続する例を示します。

```
Console> (enable) telnet labsparc
Trying 172.16.10.3...
Connected to labsparc.
Escape character is '^]'.

UNIX(r) System V Release 4.0 (labsparc)

login:
```

Telnet セッションの SSH 暗号化の使用方法

（注） Secure Shell（SSH; セキュア シェル）暗号化コマンドを使用するには、暗号化イメージを実行している必要があります。暗号化イメージに使用されるソフトウェア イメージの命名規約については、第 26 章「システム ソフトウェア イメージの操作」を参照してください。

（注） Secure Shell 暗号化機能には、Eric Young（eay@cryptsoft.com）が記述した暗号化ソフトウェアが含まれています。

SSH 暗号化は、スイッチへの Telnet セッションまたはその他のリモート接続に対してセキュリティを提供します。SSH 暗号化がサポートされるのは、スイッチにリモート ログインする場合だけです。スイッチから開始される Telnet セッションの場合は、暗号化はサポートされません。SSH 暗号化機能を使用するには、スイッチにアクセスするクライアント上にアプリケーションをインストールし、スイッチ上に SSH 暗号化を設定する必要があります。

現在実装されている SSH 暗号化は、SSH バージョン 1 およびバージョン 2 をサポートしています。SSH バージョン 1 は DES（データ暗号化規格）および 3DES 暗号化方式を、SSH バージョン 2 は 3DES および AES 暗号化方式をサポートしています。SSH 暗号化は、Remote Access Dial-In User Service（RADIUS）および Terminal Access Controller Access Control System Plus（TACACS+）認証と組み合わせて使用できます。SSH 暗号化を使用する認証を設定するには、**set authentication** コマンドに **telnet** キーワードを入力します。

（注） スイッチへのアクセス認証に Kerberos を使用する場合には、SSH 暗号化を使用することはできません。

スイッチ上で SSH 暗号化をイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	RSA ホスト鍵を作成します。	**set crypto key rsa** *nbits* [**force**]
ステップ 2	SSH バージョンを設定します。 **(注)** **v1** または **v2** キーワードを設定しない場合、SSH は互換モードで動作します。	**set ssh mode** {**v1** | **v2**}
ステップ 3	SSH モード設定を消去します。	**clear ssh mode**
ステップ 4	SSH 設定情報を表示します。	**show ssh**

次に、RSA ホスト鍵を作成する例を示します。

```
Console> (enable) set crypto key rsa 1024
Generating RSA keys.... [OK]
Console> (enable) set ssh mode v2
SSH protocol mode set to SSHv2 Only.
Console> (enable) show ssh
Session      Protocol       Cipher     State           PID     Userid       Host
-------      --------       ------     -----           ---     --------     -----
0            V2             3DES       SESSION_OPEN    146     dkoya        171.69.66.
45
1            V1             3DES       SESSION_OPEN    147     -
dove.cisco.com
SSH server mode : V1 and V2
Console> (enable)
```

nbits の値により、RSA 鍵のサイズを指定します。有効な鍵のサイズは、512 ～ 2048 ビットです。SSH バージョン 2 の場合、最小推奨鍵サイズは 768 ビットです。鍵のサイズが大きいほど高いセキュリティが提供されますが、生成時間は長くなります。

オプションの **force** キーワードを入力して鍵を再生成すると、既存の鍵の上書きを警告するプロンプトは表示されなくなります。

ユーザ セッションのモニタ

show users コマンドを使用すると、スイッチ上で現在アクティブなユーザ セッションを表示できます。コマンド出力には、スイッチ上のすべてのアクティブ コンソール ポートおよび Telnet セッションが表示されます。

スイッチ上のアクティブ ユーザ セッションを表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
スイッチ上で現在アクティブなユーザ セッションを表示します。	**show users** [**noalias**]

次に、コンソール セッションおよび Telnet セッションに対して、ローカル認証がイネーブルに設定されているときの **show users** コマンドの出力例を示します（アスタリスク [*] は現在のセッションを示しています）。

```
Console> (enable) show users
  Session  User             Location
  -------- ---------------- -------------------------
  console
  telnet                    sam-pc.bigcorp.com
* telnet                    jake-mac.bigcorp.com
Console> (enable)
```

次に、コンソール セッションおよび Telnet セッションに対して、TACACS+ 認証がイネーブルに設定されているときの **show users** コマンドの出力例を示します。

```
Console> (enable) show users
  Session  User             Location
  -------- ---------------- -------------------------
  console  sam
  telnet   jake             jake-mac.bigcorp.com
  telnet   tim              tim-nt.bigcorp.com
* telnet   suzy             suzy-pc.bigcorp.com
Console> (enable)
```

次に、**noalias** キーワードを使用して、接続ホストの IP アドレスを表示し、ユーザ セッションに関する情報を表示する例を示します。

```
Console> (enable) show users noalias
  Session  User             Location
  -------- ---------------- -------------------------
  console
  telnet                    10.10.10.12
* telnet                    10.10.20.46
Console> (enable)
```

アクティブ ユーザ セッションを切断するには、イネーブル モードで次の作業を行います。

作業	コマンド
スイッチ上のアクティブ ユーザ セッションを切断します。	**disconnect** {**console** | *ip_addr*}

次に、アクティブ コンソール ポート セッションおよびアクティブ Telnet セッションを切断する例を示します。

```
Console> (enable) show users
  Session  User             Location
  -------- ---------------- -------------------------
  console  sam
  telnet   jake             jake-mac.bigcorp.com
  telnet   tim              tim-nt.bigcorp.com
* telnet   suzy             suzy-pc.bigcorp.com
Console> (enable) disconnect console
Console session disconnected.
Console> (enable) disconnect tim-nt.bigcorp.com
Telnet session from tim-nt.bigcorp.com disconnected. (1)
Console> (enable) show users
  Session  User             Location
  -------- ---------------- -------------------------
  telnet   jake             jake-mac.bigcorp.com
* telnet   suzy             suzy-pc.bigcorp.com
Console> (enable)
```

ping の使用方法

ここでは、IP ping の使用方法について説明します。

ping の機能

IP ping を使用すると、リモート ホストとの接続をテストできます。異なる IP サブネットワーク上のホストに ping を実行する場合は、そのネットワークへのスタティック ルートを定義するか、両サブネット間でルーティングが行われるようにルータを設定する必要があります。

ping コマンドは、ユーザ EXEC モードおよびイネーブル EXEC モードで設定することができます。ユーザ EXEC モードの **ping** コマンドは、パケット サイズおよびパケット カウントを指定できる **-s** パラメータをサポートしています。イネーブル EXEC モードの **ping** コマンドでは、パケット サイズ、パケット カウント、および待機時間を指定することができます。

表 19-1 に、**ping-s** コマンドのデフォルト値を示します。

表 19-1　ping コマンドのデフォルト値

説明	ping	ping-s
パケット数	5	0 = 連続 ping
パケット サイズ	56	56
待機時間	2	2
送信元アドレス	ホスト IP アドレス	該当なし

実行中の ping を中止するには、**Ctrl-C** キーを押します。

ping を実行すると、次のいずれかの応答が戻ります。

- 正常な応答 — 正常な応答（*hostname* is alive）は、ネットワーク トラフィックに応じて 1 ～ 10 秒で戻ります。
- 宛先からの応答なし — ホストが応答しない場合、応答メッセージは戻りません。

- unknown ホスト ― ホストが存在しない場合、unknown ホスト メッセージが戻ります。
- 宛先への到達不能 ― デフォルト ゲートウェイが指定されたネットワークに到達できない場合、destination unreachable メッセージが戻ります。
- ネットワークまたはホストへの到達不能 ― ルート テーブルにホストまたはネットワークのエントリがない場合、network/host unreachable メッセージが戻ります。

ping の実行

スイッチからネットワーク上の他の装置に ping を実行するには、ユーザ モードまたはイネーブル モードで次のいずれかの作業を行います。

作業	コマンド
リモート ホストに ping を実行します。	**ping** *host*
ping オプションを使用してリモート ホストに ping を実行します。	**ping -s** *host* [*packet_size*] [*packet_count*]

次に、ユーザ EXEC モードで、リモート ホストに ping を実行する例を示します。

```
Console> ping labsparc
labsparc is alive
Console> ping 72.16.10.3
12.16.10.3 is alive
Console>
```

次に、ping **-s** オプションを使用してリモート ホストに ping を実行する例を示します。

```
Console> ping -s 12.20.5.3 800 10
PING 12.20.2.3: 800 data bytes
808 bytes from 12.20.2.3: icmp_seq=0. time=2 ms
808 bytes from 12.20.2.3: icmp_seq=1. time=3 ms
808 bytes from 12.20.2.3: icmp_seq=2. time=2 ms
808 bytes from 12.20.2.3: icmp_seq=3. time=2 ms
808 bytes from 12.20.2.3: icmp_seq=4. time=2 ms
808 bytes from 12.20.2.3: icmp_seq=5. time=2 ms
808 bytes from 12.20.2.3: icmp_seq=6. time=2 ms
808 bytes from 12.20.2.3: icmp_seq=7. time=2 ms
808 bytes from 12.20.2.3: icmp_seq=8. time=2 ms
808 bytes from 12.20.2.3: icmp_seq=9. time=3 ms

----17.20.2.3 PING Statistics----
10 packets transmitted, 10 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 2/2/3
Console>
```

次に、イネーブル モードで **ping** コマンドを入力し、パケット数、パケット サイズ、およびタイムアウトの秒数を指定する例を示します。

```
Console> (enable) ping
Target IP Address []: 12.20.5.19
Number of Packets [5]: 10
Datagram Size [56]: 100
Timeout in seconds [2]: 10
Source IP Address [12.20.2.18]: 12.20.2.18
!!!!!!!!!!

----12.20.2.19 PING Statistics----
10 packets transmitted, 10 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 1/1/1
Console> (enable)
```

レイヤ 2 traceroute の使用方法

レイヤ 2 traceroute ユーティリティにより、送信元から宛先に到達するまでのパケットの物理パスを識別することができます。レイヤ 2 traceroute ユーティリティは、パス上のスイッチのフォワーディング エンジン テーブルを検索して、パスを判別します。

送信元から宛先までのパス上にあるすべての Catalyst 6500 シリーズ スイッチの情報が表示されます。

ここでは、レイヤ 2 traceroute の使用方法について説明します。

レイヤ 2 traceroute 使用上の注意事項

ここでは、レイヤ 2 traceroute ユーティリティを使用する場合の注意事項を示します。

- レイヤ 2 traceroute ユーティリティを適用できるのは、ユニキャスト トラフィックだけです。
- ネットワーク内のすべての Catalyst 5000 および Catalyst 6500 シリーズ スイッチ上で、Cisco Discovery Protocol（CDP）をイネーブルにする必要があります（CDP のイネーブル化の詳細については、第 30 章「CDP の設定」を参照）。パス上のいずれかの装置が CDP に対してトランスペアレントに設定されている場合、**l2trace** コマンドで、これらの装置を通過するレイヤ 2 パスをトレースすることはできません。
- このユーティリティは、送信元から宛先までのレイヤ 2 パス上に置かれていないスイッチから実行することができます。ただし、送信元および宛先を含むパス上のすべてのスイッチが、ユーティリティ実行スイッチに到達できる必要があります。
- パス上のすべてのスイッチは、相互に到達できる必要があります。
- レイヤ 2 パスをトレースするには、送信元 / 宛先 IP アドレス（または IP エイリアス、または MAC アドレスを指定します。送信元と宛先が複数の VLAN（仮想 LAN）に属していて、MAC アドレスを指定している場合、VLAN も指定することができます。
- 送信元および宛先スイッチは、同じ VLAN に属している必要があります。
- **l2trace** クエリを実行できる最大ホップ数は 10 です。これには、送信元トレースの関連ホップ数も含まれています。
- レイヤ 2 traceroute ユーティリティは、トークンリング VLAN の場合、複数の装置がハブ経由で 1 つのポートに接続している場合、またはポート上の複数のネイバが存在する場合には、機能しません。

レイヤ 2 パスの識別

レイヤ 2 パスを識別するには、イネーブル モードで次のいずれかの作業を実行します。

作業	コマンド
（任意）MAC アドレスを使用してレイヤ 2 パスをトレースします。	**l2trace** {*src-mac-addr*} {*dest-mac-addr*} [*vlan*] [**detail**]
（任意）IP アドレスまたは IP エイリアスを使用してレイヤ 2 パスをトレースします。	**l2trace** {*src-ip-addr*} {*dest-ip-addr*} [**detail**]

次に、送信元と宛先の MAC アドレスを指定し、VLAN を指定せずに、detail オプションを指定する例を示します。パス上で検索された各 Catalyst 5000/6500 シリーズ スイッチについて、装置のタイプ、装置名、装置 IP アドレス、着信ポート名、着信ポート速度、着信ポートのデュプレックス モード、発信ポート名、発信ポート速度、および発信ポートのデュプレックス モードが表示されます。

```
Console> (enable) l2trace 00-01-22-33-44-55 10-22-33-44-55-66 detail

l2trace vlan number is 10.

00-01-22-33-44-55 found in C5500 named wiring-1 on port 4/1 10Mb half duplex
C5500:wiring-1:192.168.242.10:4/1 10Mb half duplex -> 5/2 100MB full duplex
C5000:backup-wiring-1:192.168.242.20:1/1 100Mb full duplex -> 3/1 100MB full duplex
C5000:backup-core-1:192.168.242.30:4/1 100 MB full duplex -> 1/1 100MB full duplex
C6000:core-1:192.168.242.40:1/1 100MB full duplex -> 2/1 10MB half duplex.
10-22-33-44-55-66 found in C6000 named core-1 on port 2/1 10MB half duplex.
```

IP traceroute の使用方法

IP traceroute ユーティリティにより、ネットワークを通過するパケットのパスを、レイヤ 3 のホップ単位で調べることができます。コマンド出力には、宛先までのトラフィック パスについて、ルータなどを含むネットワーク レイヤ（レイヤ 3）のすべての装置が表示されます。

ここでは、IP traceroute の使用方法について説明します。

IP traceroute の機能

traceroute コマンドを実行すると、IP ヘッダーの Time To Live（TTL）フィールドにより、ルータおよびサーバで特定の戻りメッセージが生成されます。traceroute コマンドは、まず、宛先ホストに対して、TTL フィールドを 1 に設定した UDP データグラムを送信します。ルータは 1 または 0 の TTL 値を検出すると、データグラムを廃棄し、送信元に Internet Control Message Protocol（ICMP）の time-exceeded メッセージを戻します。traceroute 機能は、ICMP time-exceeded メッセージの送信元アドレス フィールドを調べ、最初のホップのアドレスを判別します。

続いて、次のホップを識別するために、TTL 値を 2 に設定した UDP パケットが送信されます。最初のルータは、TTL フィールドを 1 だけ減らし、2 番めのルータにデータグラムを送信します。2 番めのルータは、TTL 値が 1 の UDP パケットを受け取り、データグラムを廃棄して、送信元に time-exceeded メッセージを戻します。このように、宛先ホストに到達するまで（または TTL の最大値に達するまで）、TTL の値が増分され、処理が続けられます。

データグラムが宛先に到達したことを確認するために、traceroute 機能は、データグラムの UDP 宛先ポートに、宛先ホストが使用する可能性のない非常に大きい値を設定します。ホストは、この未知のポート番号を持つデータグラムを受信すると、送信元に ICMP port unreachable error メッセージを戻します。このメッセージにより、宛先に到達したことを traceroute 機能に伝えます。

スイッチは、**traceroute** コマンドの送信元または宛先として指定できますが、**traceroute** コマンドの出力に 1 つのホップとして表示されることはありません。

IP traceroute の実行

パケットがネットワークを通過するパスを追跡するには、イネーブル モードで次の作業を行います。

作業	コマンド
IP traceroute を実行して、ネットワークを通過するパケットのレイヤ 3 パスをトレースします。	**traceroute** [**-n**] [**-w** *wait_time*] [**-i** *initial_ttl*] [**-m** *max_ttl*] [**-p** *dest_port*] [**-q** *nqueries*] [**-t** *tos*] *host* [*data_size*]

次に、**traceroute** コマンドの使用例を示します。

```
Console> (enable) traceroute 10.1.1.100
traceroute to 10.1.1.100 (10.1.1.100), 30 hops max, 40 byte packets
 1 10.1.1.1 (10.1.1.1)  1 ms  2 ms  1 ms
 2 10.1.1.100 (10.1.1.100)  2 ms  2 ms  2 ms
Console> (enable)
```

次に、**traceroute** コマンドを使用して、それぞれ 1400 バイトのパケットで、各ホップに 6 回のクエリを送信する例を示します。

```
Console> (enable) traceroute -q 6 10.1.1.100 1400
traceroute to 10.1.1.100 (10.1.1.100), 30 hops max, 1440 byte packets
 1 10.1.1.1 (10.1.1.1)  2 ms  2 ms  2 ms  1 ms  2 ms  2 ms
 2 10.1.1.100 (10.1.1.100)  2 ms  4 ms  3 ms  3 ms  3 ms  3 ms
Console> (enable)
```

ポート カウンタのシステム警告を使用する方法

すべてのポート上で特定のエラー カウンタをポーリングし、システム エラー メッセージを記録することによって、Catalyst 6500 シリーズ スイッチをモニタし、トラブルシューティングを行うことができます。システム、ハードウェア、およびスパニングツリー ポートについて、次の条件でメッセージが記録されます。

- 設定可能なスレッシュホールドを超過したバックプレーン トラフィック レベル
- 残りメモリの不足
- メモリ破損の検出
- NVRAM（不揮発性 RAM）のログ
- 着信エラー
- UDP および TCP エラー

ハードウェア エラー情報は 30 分間隔で記録され、ポート カウンタのデバッグに必要な情報が得られます。カウンタ値が増えると、メッセージが記録されます。

次のスパニングツリー エラー情報が得られます。

- ブロッキング ステートからフォワーディング ステートに移行するポート
- 設定スレッシュホールドを超過した Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）スキュー

ここでは、Catalyst6500 シリーズ スイッチ上でシステム警告機能を使用する手順について説明します。

- ポート カウンタのシステム警告の実行（p.19-18）
- ポート カウンタのハードウェア レベル警告の実行（p.19-21）
- ポート カウンタのスパニングツリー警告の実行（p.19-21）

ポート カウンタのシステム警告の実行

ここでは、ポート カウンタのシステム警告を実行する方法について説明します。

- バックプレーン トラフィック（p.19-18）
- 残りメモリの不足（p.19-19）
- メモリ破損の検出（p.19-20）
- NVRAM のログ（p.19-20）
- 着信エラー（p.19-20）
- UDP エラー（p.19-21）

バックプレーン トラフィック

上限スレッシュホールドを割合で指定することによって、バックプレーン スレッシュホールド検知を設定できます。バックプレーン トラフィックが指定のスレッシュホールドを超えると、以前のトラフィック ポーリングと比較して、Syslog メッセージが生成されます。ただし、スレッシュホールドを 100%（デフォルト）に設定した場合、Syslog メッセージは生成されません。

スイッチング バスを 3 つ使用するスイッチの場合、3 つのスイッチング バス全体の平均トラフィックを設定する代わりに、バスごとにスレッシュホールドおよび（Syslog イベント ポーリングおよびメッセージの生成を制御する）Syslog スロットリングを設定できます。スロットルの間隔は 5 分です。

次に、スレッシュホールドを設定する例を示します。

```
Console> (enable) set traffic monitor help
Usage: set traffic monitor <threshold>
       (threshold = 0..100 in percentage)
Console> (enable) set traffic monitor 60
Traffic monitoring threshold set to 60%.
Console> (enable) show traffic
Threshold: 60%

Backplane-Traffic Peak Peak-Time
----------------- ---- -------------------------
  0%                0% Tue Apr 16 2002, 08:01:53

Fab Chan Input Output
-------- ----- ------
       0    0%     0%
       1    0%     0%
       2    0%     0%
       3    0%     0%
       4    0%     0%
       5    0%     0%
       6    0%     0%
       7    0%     0%
       8    0%     0%
       9    0%     0%
      10    0%     0%
      11    0%     0%
      12    0%     0%
      13    0%     0%
      14    0%     0%
      15    0%     0%
      16    0%     0%
      17    0%     0%
Console> (enable)
```

次に、Syslog メッセージの例を示します。

```
2000 Jan 11 06:00:27 PST -07:00 %SYS-4-SYS_HITRFC: 62% traffic detected on switching
bus (A)
2000 Feb 21 12:00:27 PST -07:00 %SYS-4-SYS_HITRFC: 65% traffic detected on switching
bus
```

残りメモリの不足

Catalyst 6500 シリーズ スイッチ上のクラスタおよびバッファに対するメモリ割り当てが 90% のハイ ウォーターマークを超えると、Syslog メッセージが生成されます。Syslog メッセージは次の状況で生成されます。

- クラスタに割り当てられた使用率がハイ ウォーターマークである 90% を超え、スロットル間隔が 1 時間のとき
- mbufs に割り当てられた使用率がハイ ウォーターマークである 90% を超え、スロットル間隔が 1 時間のとき
- malloc に割り当てられた使用率がハイ ウォーターマークである 90% を超え、スロットル間隔が 1 時間のとき

次に、Syslog メッセージの例を示します。

```
1999 Sep 9 00:00:00 PDT -07:00 %SYS-3-SYS_MEMLOW: Memory cluster usage exceeded 90%
1999 Sep 9 00:00:00 PDT -07:00 %SYS-3-SYS_MEMLOW: Mbuf usage exceeded 90%
1999 Sep 9 00:00:00 PDT -07:00 %SYS-3-SYS_MEMLOW: Malloc usage exceeded 90%
```

メモリ破損の検出

デフォルトでは、Memory Management Module（MMU）によるメモリ破損検出はイネーブルです。次に、メモリ破損検出をイネーブルにする例を示します。

```
Console> (enable) set errordetection memory
Usage: set errordetection memory <enable|disable>
Console> (enable) set errordetection memory enable
Memory error detection enabled.
Console> (enable) show errordetection
Inband error detection:              disabled
Memory error detection:              enabled
Packet buffer error detection:       errdisable
Port counter error detection:        disabled
Port link-errors action:             port-failover
Port link-errors interval:           30 seconds
Port link-errors high rx-threshold: 1000 packets
Port link-errors low rx-threshold:  1000 packets
Port link-errors high tx-threshold: 1000 packets
Port link-errors low tx-threshold:  1000 packets
Port link-errors sampling:           3
Console> (enable)
```

次に、Syslog メッセージの例を示します。

```
1999 Nov 23 16:32:21 PDT -07:00 %SYS-3-SYS_MEMERR: Out of range while freeing address
0xabcdefab
```

NVRAM のログ

コンフィギュレーション関連の NVRAM ログ イベントごとに、Syslog エラーが生成されます。このイベントは、設定またはハードウェアのエラーを意味する場合も、ユーザ側に通告なく行われた NVRAM 設定を意味する場合もあります。ハードウェア エラーの NVRAM ログは Syslog に記録されません。NVRAM ログのタイムスタンプは、メッセージに含まれません。

次に、Syslog メッセージの例を示します。

```
1999 Nov 23 16:37:21 PDT -07:00 %SYS-4-SYS_NVLOG: convert_post_SAC_CiscoMIB:Block 63
converted from version 0 to 1

1999 Nov 23 16:37:25 PDT -07:00 %SYS-4-SYS_NVLOG: StartupConfig:Auto config started
```

着信エラー

着信 Syslog メッセージは、送受信エラーが検出された場合に生成されます。デフォルトでは、着信 Syslog メッセージはイネーブルです。次に、着信エラー検出をイネーブルにする例を示します。

```
Console> (enable) set errordetection inband
Usage: set errordetection inband <enable|disable>
Conosle> (enable) set errordetection inband enable
Inband errordetection enabled.
```

受信側のリソース エラーが 500 回に達すると、次の Syslog エラーが生成されます。

```
2000 Jun 24 06:37:25 PDT -07:00 %SYS-3-INBAND_NORESOURCE: inband resource error
warning (500)
2000 Jun 24 08:12:03 PDT -07:00 %SYS-3-INBAND_NORESOURCE: inband resource error
warning (1000)
```

擬似割り込みのたびに、次のようなメッセージが記録されます。

```
1999 Dec 25 18:22:08 PDT -07:00 %SYS-3-INBAND_SPRINTR: inband spurious interrupt
occurred (2)
```

着信ポートで送受信エラーが発生するたびに、次のようなメッセージが記録されます。

(注)　カッコ内の数字は、送受信エラーの回数ではなく、着信ポートがリセットされた回数を示しています。

```
1999 Dec 25 18:22:08 PDT -07:00 %SYS-3-INBAND_TXRXFAIL: inband driver stuck/reset (2)
```

UDP エラー

show netstat upd コマンドを入力すると、ソケット オーバーフローのたびに、次のようなメッセージが生成されます。

```
1999 Oct 31 23:59:59 PDT -07:00 %IP-3-UDP_SOCKOVFL: UDP socket overflow
```

show netstat udp/tcp コマンドを入力すると、UDP/TCP チェックサム不良が発生するたびに、次のようなメッセージが生成されます。

```
1999 Oct 31 23:59:59 PDT -07:00 %IP-3-UDP_BADCKSUM: UDP bad checksum
1999 Oct 31 23:59:59 PDT -07:00 %IP-3-TCP_BADCKSUM: TCP bad checksum
```

ポート カウンタのハードウェア レベル警告の実行

各スイッチ ポートの特定のエラー カウンタを 30 分間隔でポーリングすることができます。同一ポート上での連続する 2 回のポーリングで、カウンタの値が増えていた場合は、イベントが記録されます。バックグラウンド ポーリングのイネーブルまたはディセーブルには、**set errordetection portcounters** コマンドを使用します。デフォルトでは、ポーリングはイネーブルです。

次のように、**set errordetection portcounters** コマンドを入力します。

```
Console> (enable) set errordetection portcounters
Usage: set errordetection portcounters <enable|disable>
Console> (enable) set errordetection portcounters disable
Port Counters error detection disabled.
```

次に、Syslog メッセージの例を示します。

```
1999 Jan 11 08:02:59 PDT -07:00 %SYS-3-PORT_ERR: Port 3/4 swBusResultEvent (12)
1999 Jan 11 09:03:03 PDT -07:00 %SYS-3-PORT_ERR: Port 3/4 swBusResultEvent (223)
1999 Jan 11 09:03:03 PDT -07:00 %SYS-4-PORT_WARN: Port 3/4 dmaTxFull (7) dmaRetry (33)
dmaLevel2Request(21)
```

ポート カウンタのスパニングツリー警告の実行

ここでは、ポート カウンタのスパニングツリー警告を実行する方法について説明します。

- ブロッキングからリスニングへの移行（p.19-22）
- BPDU スキューイング（p.19-22）
- SNMP（p.19-22）

ブロッキングからリスニングへの移行

ポートがブロッキングからリスニングに移行するたびに、Syslog メッセージが生成されます。スパニングツリー ステート変化には、既存の Syslog メッセージがあります。

次に、Syslog メッセージの例を示します。

```
1999 Jan 03 00:02:59 PDT -07:00 %SPANTREE-5-PORTLISTEN: Port 3/4 state in vlan 1
changed to listening
1999 Jan 03 00:02:59 PDT -07:00 %SPANTREE-5-TR_PORTLISTEN: Trcrf 101 in trbrf 102
state changed to listening
```

BPDU スキューイング

ポート上で連続して 2 回受信した BPDU の受信間隔が hello タイムを 10 秒超えていた場合に、Syslog メッセージが生成されます。スロットル間隔については、すべての VLAN 番号で、ポート別に毎分 1 つずつメッセージが生成されます。

次に、Syslog メッセージの例を示します。

```
1999 Jan 01 00:01:19 PDT -07:00 %SPANTREE-3-BPDUSKEW: Port 2/1 vlan 1 BPDU skewed
1999 Jan 01 00:05:19 PDT -07:00 %SPANTREE-3-BPDUSKEW: Port 2/5 vlan 1 BPDU skewed
1999 Jan 01 00:05:23 PDT -07:00 %SPANTREE-3-BPDUSKEW: Port 2/5 vlan 3 BPDU skewed
```

SNMP

Syslog 警告ごとに、既存の clogMessageGenerated トラップを使用して生成された、対応する SNMP（簡易ネットワーク管理プロトコル）トラップが、Syslog メッセージが生成されるたびに送信されます。

パケットバッファ エラー処理の設定

set errordetection packet-buffer {**errdisable** | **powercycle** | **supervisor** {**errdisable** | **shutdown**}} コマンドを使用すると、次のようにパケットバッファ エラー処理を指定できます（デフォルトは **errdisable**）。

- **errdisable** ― **errdisable** キーワードを入力した場合、パケットバッファ エラーが発生したポートは errdisable ステートになります。
- **powercycle** ― **powercycle** キーワードを入力した場合、このオプションをサポートするモジュールは、パケットバッファ エラーが発生すると電源がオフ / オンになります。このオプションを選択した場合、モジュール上で ROMMON アップグレードが（必要に応じて）自動実行され、標準の起動シーケンスが省略されて、モジュールのダウンタイムが短縮されます（この機能は高速起動機能ともいいます）。
- **supervisor** ― **supervisor errdisable** キーワードを入力した場合、パケットバッファ エラーが発生したスーパバイザ エンジン ポートは errdisable ステートになります。**supervisor shutdown** キーワードを入力した場合、パケットバッファ エラーが発生したスーパバイザ エンジン ポートはシャット ダウンされます。

注意　ROMMON イメージのダウンロード中は、モジュールの電源をオフ / オンにしないでください。モジュールが破損することがあります。

パケットバッファ エラー処理は、次のモジュールで使用できます。

- WS-X6248-RJ45
- WS-X6248-TEL
- WS-X6348-RJ45
- WS-X6348-RJ21
- WS-X6148-RJ45
- WS-X6148-RJ21

（注）　エラー検出設定に関する情報を表示するには、**show errordetection** コマンドを入力します。

EtherChannel/ リンク エラー処理の設定

この機能を使用すると、指定期間内に EtherChannel 内のポートの 1 つが設定可能なエラー スレッシュホールドを超過した場合に、EtherChannel 内のポート間でトラフィックが自動的にフェールオーバーされます。ポート フェールオーバーが発生するのは、EtherChannel に動作可能なポートが存在する場合のみです。障害の発生したポートが EtherChannel 内の最終ポートである場合、ポートは「ポート フェールオーバー」ステートにならないで、受信中のエラー タイプに関係なくトラフィックを引き続き送受信します。単一の非チャネリング ポートはポート フェールオーバー ステートになりません。指定期間内にエラー スレッシュホールドを超過した場合、これらのポートは errdisable ステートになります。

(注) リンク エラーは、Inerrors、RXCRC（CRCAlignErrors）、および TXCRC の 3 つのカウンタに基づいてモニタされます。リンクの errdisable タイマーがイネーブルの場合（**set errdisable-timeout enable** コマンドを使用）、errdisable ステートのポートはタイムアウト インターバルの経過後に自動的に再イネーブルになります（タイムアウト インターバルは **set errdisable-timeout interval** {*interval*} コマンドを使用して指定します）。これらのコマンドの詳細については、「ポートの errdisable ステートにおけるタイムアウト設定」（p.4-13）を参照してください。

set errordetection link-errors グローバル コマンドを使用すると、EtherChannel/ リンク エラー処理を次のように指定できます。

- **set errordetection link-errors action** {**errordisable** | **port-failover**}

  ポートのエラー カウンタが設定可能なスレッシュホールドの上限値に到達すると（指定されたサンプリング カウント期間内）、errordisable または port-failover のいずれかの *action* が実行されます。**errordisable** を選択した場合、上限スレッシュホールドに到達したポートは errdisable ステートになります。**port-failover** を選択した場合は、ポートのチャネル ステータスが考慮されます。ポートがチャネルに属していて、チャネル内の動作可能な最終ポートでない場合、ポートは errdisable ステートになります（ポートが単一ポートの場合も、errdisable ステートになります）。**action** のデフォルト設定は **port-failover** です。

- **set errordetection link-errors interval** {*timer-value*}

  指定された **interval** *timer-value* は、ポートのエラー カウンタの読み取り頻度を決定します。指定されたデフォルトタイマー値は 30 秒で、有効範囲は 30 ～ 1800 秒です。

  (注) EtherChannel/ リンク エラー処理機能がディセーブルの場合も、インターバルを設定できます。この機能がイネーブルの場合に、インターバルを指定すると、タイマーは新しい値を使用して再起動します。

- **set errordetection link-errors** {**inerrors** | **rxcrc** | **txcrc**} {[**high** *value*] | [**low** *value*]}

  指定された **rxcrc** 値および **txcrc** 値は、**interval** *timer-value* コマンドを入力して指定されたインターバル中に許可されるリンク エラー数を決定します。下限スレッシュホールドに到達すると（指定されたサンプリング カウント期間内）、Syslog メッセージが表示されます。上限スレッシュホールドに到達すると（指定されたサンプリング カウント期間内）、Syslog メッセージが表示されるとともに、ポートが errdisable ステートになるか、またはポート フェールオーバー メカニズムがトリガーされます。上限スレッシュホールドの範囲は 2 ～ 65535、下限スレッシュホールドの範囲は 1 ～ 65534 です。指定された **inerrors** 値は、inerrors スレッシュホールドを決定します。デフォルトのスレッシュホールド値は、次のとおりです。

  — **inerrors** スレッシュホールドの上限値 — 1001 パケット

  — **inerrors** スレッシュホールドの下限値 — 1000 パケット

- ― **rxcrc** スレッシュホールドの上限値 ― 1001 パケット
- ― **rxcrc** スレッシュホールドの下限値 ― 1000 パケット
- ― **txcrc** スレッシュホールドの上限値 ― 1001 パケット
- ― **txcrc** スレッシュホールドの下限値 ― 1000 パケット

- **set errordetection link-errors sampling** {*sampling_count*}

  実際のシステム エラー条件でないワンタイム イベントによってポートが偶然に errdisable ステートになる可能性を最小限にするには、*sampling_count* を指定してください。*sampling_count* は、ポートが errdisable ステートになるまでに上限 / 下限スレッシュホールド値に到達しなければならない回数を決定します。たとえば、ポートの上限スレッシュホールド値が 1000 で、サンプリング カウントが 3 の場合、ポートが errdisable ステートになるのは、ポートが 1000 のスレッシュホールドに 3 回到達した場合のみです。デフォルトのサンプリング カウント値は 3、有効範囲は 1 ～ 255 回です。

(注)　エラー検出設定に関する情報を表示するには、**show errordetection** コマンドを入力します。

IEEE 802.3ah イーサネット OAM の設定

イーサネット Operation, Administration, and Maintenance（OAM）機能は、IEEE 802.3ah の資料にある仕様に従います。このプロトコルによって扱われる主な イーサネット OAM 機能は、リンク モニタリング、リモート失敗指示、およびリモート ループバック テストです。

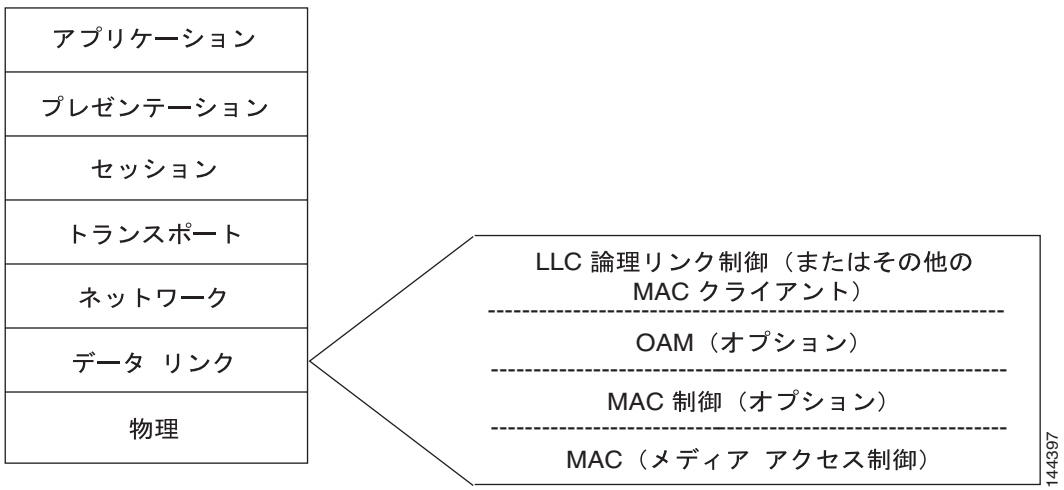
(注)　シスコでは、リモート失敗指示をサポートしていません。

ここでは、IEEE 802.3ah イーサネット OAM の設定方法について説明します。

概要

Open Systems Interconnection（OSI; 開放型システム間相互接続）参照モデルでは、イーサネット OAM は、データ リンク レイヤの Logical Link Control（LLC; 論理リンク制御）サブレイヤと MAC サブレイヤ間に実装されるオプションのサブレイヤです（図 19-1 を参照）。

図 19-1　OSI 参照モデルの イーサネット OAM の位置



(注)　OAM は、広帯域幅を必要としない（フレーム転送速度が最大 10 フレーム / 秒に制限されている）比較的低速のプロトコルで、通常のリンク動作では必要ありません。OAM フレーム（別名 OAM Protocol Data Unit [OAMPDU]）は、低速プロトコル宛先 MAC アドレス（0180.c200.0002）を使用して、MAC サブレイヤで代行受信され、イーサネット ネットワーク内の複数のホップに伝播されません。

任意の全二重ポイントツーポイント イーサネット リンクまたはエミュレート ポイントツーポイント イーサネット リンクで OAM を実装できます。OAM はポート単位で設定できます。OAM 設定はポートの他の設定とは無関係です。ポートは、トランク ポート、アクセス ポート、または EhterChannel の一部とすることができます。ポート上で OAM を設定する場合、このポートの OAM 機能は他のポートで設定された OAM 機能とは無関係です。

イーサネット OAM 設定時の注意事項および制限事項

イーサネット OAM を設定する場合、次の設定時の注意事項および制限事項に従ってください。

- OAM 機能は、物理的な外部イーサネット ポート上でのみサポートされます。
- OAM を実行するポートは、全二重モードにする必要があります。
- リモート失敗指示は、サポートされません。
- OAM リモート ループバック モードは、トランク ポート、EtherChannel ポート、およびプライベート VLAN ポートではサポートされません。
- MIB（管理情報ベース）変数要求および応答は、サポートされません。

イーサネット OAM の実行

ここでは、イーサネット OAM の実行方法について説明します。

- イーサネット OAM のイネーブル化またはディセーブル化（p.19-28）
- イーサネット OAM ポート モードの指定（p.19-28）
- イーサネット OAM リモート ループバック テストの拒否または許可（p.19-29）
- イーサネット OAM リモート ループバック テストのイネーブル化またはディセーブル化（p.19-29）
- イーサネット OAM リモート ループバック テストのパケット数およびパケット サイズの指定とテストの実行（p.19-30）
- イーサネット OAM リンク モニタリングのイネーブル化またはディセーブル化（p.19-30）
- イーサネット OAM リンク モニタリング用のリンク イベントのウィンドウ サイズの指定（p.19-31）
- イーサネット OAM リンク モニタリングの下限スレッシュホールド エラー カウントおよび関連アクションの指定（p.19-31）
- イーサネット OAM リンク モニタリングの上限スレッシュホールド エラー カウントおよび関連アクションの指定（p.19-32）
- OAM クリティカル リンク イベントの関連アクションの指定（p.19-32）
- イーサネット OAM 統計情報およびイーサネット OAM 設定の消去（p.19-33）
- OAM リンク モニタリング用のユーザ設定パラメータの消去（p.19-33）
- OAM クリティカル リンク イベント用のユーザ設定アクションの消去（p.19-34）
- イーサネット OAM 関連情報の表示（p.19-34）
- イーサネット OAM ネイバ情報の表示（p.19-35）
- イーサネット OAM リモート ループバック テスト情報の表示（p.19-36）
- イーサネット OAM 統計情報の表示（p.19-37）

イーサネット OAM のイネーブル化またはディセーブル化

次のコマンドを使用すると、特定のポート上で OAM をイネーブルまたはディセーブルにできます。デフォルトでは、OAM はすべてのポート上でディセーブルです。

指定のポート上で OAM をイネーブルまたはディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
指定のポート上で OAM をイネーブルまたはディセーブルにします。	**set port ethernet-oam** *mod/port* {**disable** | **enable**}

次に、指定のポート上で OAM をイネーブルにする例を示します。

```
Console> (enable) set port ethernet-oam 3/1 enable
Successfully enabled OAM on port(s) 3/1.
Console> (enable)
```

イーサネット OAM ポート モードの指定

以下のコマンドを使用すると、指定のポート上での OAM ポート モードを指定できます。表 19-2 に、アクティブおよびパッシブ モードで許可される OAM ポート機能を示します。デフォルトでは、OAM モードはすべてのポートでアクティブです。

表 19-2　イーサネット OAM ポート モード

機能	アクティブ	パッシブ
OAM 検出プロセスを開始します。	あり	なし
OAM 検出プロセスの開始に応答します。	あり	あり
情報 OAMPDU を送信する必要があります。	あり	あり
イベント通知 OAMPDU の送信が許可されます。	あり	あり
変数要求 OAMPDU の送信が許可されます。	あり	なし
変数応答 OAMPDU の送信が許可されます。	あり[1]	あり
ループバック制御 OAMPDU の送信が許可されます。	あり	なし
ループバック制御 OAMPDU に応答します。	あり[1]	あり
構成に固有の OAMPDU の送信が許可されます。	あり	あり

1. ピア ポートをアクティブ モードにする必要があります。

指定ポート上で OAM ポート モードを指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
指定ポート上で OAM ポート モードを指定します。	**set port ethernet-oam** *mod/port* **mode** {**active** | **passive**}

次に、指定ポート上で OAM ポート モードをアクティブに指定する例を示します。

```
Console> (enable) set port ethernet-oam 3/1 mode active
Successfully updated OAM mode to active on port(s) 3/1.
Console> (enable)
```

イーサネット OAM リモート ループバック テストの拒否または許可

以下のコマンドを使用すると、指定ポート上で OAM リモート ループバック要求を拒否または許可できます。デフォルトの設定は許可です。

指定ポートで OAM リモート ループバック要求を拒否または許可するには、イネーブル モードで次の作業を行います。

作業	コマンド
指定ポートで OAM リモート ループバック要求を拒否または許可します。	**set port ethernet-oam** *mod/port* **remote-loopback** {**deny** | **permit**}

次に、指定ポートで OAM リモート ループバック要求を拒否する例を示します。

```
Console> (enable) set port ethernet-oam 3/1 remote-loopback deny
Successfully updated OAM remote-loopback capability to deny on port(s) 3/1.
Console> (enable)
```

イーサネット OAM リモート ループバック テストのイネーブル化またはディセーブル化

以下のコマンドを使用すると、指定ポート上で OAM リモート ループバック テストをイネーブルまたはディセーブルにできます。このテストを実行するように指定したポートは、OAM リモート ループバック モードを開始できるピア OAM デバイスと接続している必要があります。

（注） 以下のコマンドは、コンフィギュレーション ファイルまたは NVRAM に保存されません。

（注） リモート ループバック テストの動作中に、リモート ループバックがイネーブルになった場合、データ パケットを含むすべてのパケットがそのポートで廃棄されます。この動作により、多くのプロトコル（Spanning-Tree Protocol [STP; スパニングツリー プロトコル]、Etherchannel プロトコルなど）でステート マシンがリセットされます。

指定ポートで OAM リモート ループバック テストをイネーブルまたはディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
指定ポートで OAM リモート ループバックテストをイネーブルまたはディセーブルにします。	**set port ethernet-oam** *mod/port* **remote-loopback** {**disable** | **enable**}

次に、指定ポートで OAM リモート ループバックテストをイネーブルにする例を示します。

```
Console> (enable) set port ethernet-oam 3/1 remote-loopback enable
Successfully initiated OAM remote-loopback on port(s) 1/1.
Port status set to inactive
Console> (enable)
```

イーサネット OAM リモート ループバック テストのパケット数およびパケット サイズの指定とテストの実行

以下のコマンドを使用すると、OAM リモート ループバック テストのパケット数および パケット サイズを指定し、指定のポート上でテストを実行できます。このコマンドは、OAM リモート ループバック テストがイネーブルのポートでのみ使用できます。このコマンドの入力後、リモート ループバック テストが実行され、テスト終了後にテスト結果の要約が表示されます。デフォルトでは、64 バイトのパケット 10,000 個が送信されます。許容パケット数は、1 ～ 99999999 パケットです。許容パケットサイズは、64 ～ 1518 バイトです。

(注)　以下のコマンドは、コンフィギュレーション ファイルまたは NVRAM に保存されません。

OAM リモート ループバック テストのパケット数および パケット サイズを指定し、指定ポートでテストを実行するには、イネーブル モードで次の作業を実行します。

作業	コマンド
OAM リモート ループバック テストのパケット数および パケット サイズを指定して、指定ポート上でテストを実行します。	**set port ethernet-oam** *mod/port* **remote-loopback test** [*no of packets* [*packet size*]]

次に、OAM リモート ループバック テストのパケット数を指定して、指定ポート上でテストを実行する例を示します。

```
Console> (enable) set port ethernet-oam 1/1 remote-loopback test 999999
Transmitting 999999 (64 byte) packets on port 1/1 Ö
OAM Remote Loopback Test 1/1: 999999 transmitted, 999999 received
Console> (enable)
```

イーサネット OAM リンク モニタリングのイネーブル化またはディセーブル化

以下のコマンドを使用すると、指定ポート上で OAM リンク モニタリングをイネーブルまたはディセーブルにできます。デフォルトでは、イネーブルです。

指定ポートで OAM リンク モニタリングをイネーブルまたはディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
指定ポートで OAM リンク モニタリングをイネーブルまたはディセーブルにします。	**set port ethernet-oam** *mod/port* **link-monitor** {**disable** | **enable**}

次に、指定ポート上で OAM リンク モニタリングをイネーブルにする例を示します。

```
Console> (enable) set port ethernet-oam 3/1 link-monitor enable
Successfully enabled OAM link-monitor on port(s) 3/1.
Console> (enable)
```

イーサネット OAM リンク モニタリング用のリンク イベントのウィンドウ サイズの指定

以下のコマンドを使用すると、対応するリンク イベントの OAM リンク モニタリング ウィンドウ サイズを指定できます。ウィンドウ サイズのデフォルトおよび範囲は、次のとおりです。

- **symbol-period** ― デフォルトでは 625,000,000 記号です。範囲は、1 ～ 1,000,000 で、100 万記号単位です。
- **frame** ― デフォルトの設定は 30 秒です。範囲は、10 ～ 65535 ミリ秒（1 ～ 6553.5 秒）で、100 ミリ秒単位です。
- **frame-period** ― デフォルトでは 10,000,000 フレームです。範囲は、200 ～ 2,000,000,000 フレームです。

指定のポート上で対応するリンク イベントの OAM リンク モニタリング ウィンドウ サイズを指定するには、イネーブル モードで次の作業を実行します。

作業	コマンド
指定ポートで対応するリンク イベントの OAM リンク モニタリング ウィンドウ サイズを指定します。	**set port ethernet-oam** *mod/port* **link-monitor** {**symbol-period** | **frame** | **frame-period**} **window** *size*

次に、リンク モニタリングの **symbol-period** ウィンドウ サイズを 1000 に指定する例を示します。

```
Console> (enable) set port ethernet-oam 3/1 link-monitor symbol-period window 10000
Successfully updated OAM symbol-period window on port(s) 3/1.
Console> (enable)
```

次に、リンク モニタリングの **frame** ウィンドウ サイズを 100 に指定する例を示します。

```
Console> (enable) set port ethernet-oam 3/1 link-monitor frame window 100
Successfully updated OAM frame window on port(s) 3/1.
Console> (enable)
```

次に、リンク モニタリングの **frame-period** ウィンドウ サイズを 1000 に指定する例を示します。

```
Console> (enable) set port ethernet-oam 3/1 link-monitor frame-period window 1000
Successfully updated OAM frame-period window on port(s) 3/1.
Console> (enable)
```

イーサネット OAM リンク モニタリングの下限スレッシュホールド エラー カウントおよび関連アクションの指定

以下のコマンドを使用すると、指定ポート上で OAM リンク モニタリングの下限スレッシュホールド エラー カウントおよび関連アクションを指定できます。デフォルトの下限スレッシュホールド エラー カウントは、1 エラーです。デフォルトのアクションは、警告です。

下限スレッシュホールド エラー カウントは、OAM リンク モニタリングのモニタリング スレッシュホールドとしても機能します。指定の下限スレッシュホールド エラー カウントに到達するかまたは超過すると、OAM リンク イベントの Type-Length-Value（TLV）が生成され、IEEE 802.3ah の資料に記載されているように送信されます。

指定ポートで OAM リンク モニタリングの下限スレッシュホールド エラー カウントおよび関連アクションを指定するには、イネーブル モードで次の作業を実行します。

作業	コマンド
指定ポートで OAM リンク モニタリングの下限スレッシュホールド エラー カウントおよび関連アクションを指定します。	**set port ethernet-oam** *mod/port* **link-monitor** {**symbol-period** | **frame** | **frame-period**} **low-threshold** *count* [**action** {**none** | **warning**}]

次に、指定ポートで OAM リンク モニタリングの下限スレッシュホールド エラー カウントおよび関連アクションを指定する例を示します。

```
Console> (enable) set port ethernet-oam 3/1 link-monitor frame low-threshold 2 action
none
Successfully updated OAM frame low threshold on port(s) 3/1.
Console> (enable)
```

イーサネット OAM リンク モニタリングの上限スレッシュホールド エラー カウントおよび関連アクションの指定

以下のコマンドを使用すると、指定ポート上で OAM リンク モニタリングの上限スレッシュホールド エラー カウントおよび関連アクションを指定できます。デフォルトの上限スレッシュホールド エラー カウントは、65535 エラーです。デフォルトのアクションは、警告です。

指定ポートでの OAM リンク モニタリングの上限スレッシュホールド エラー カウントおよび関連アクションを指定するには、イネーブル モードで次の作業を実行します。

作業	コマンド
指定ポートで OAM リンク モニタリングの上限スレッシュホールド エラー カウントおよび関連アクションを指定します。	**set port ethernet-oam** *mod/port* **link-monitor** {**symbol-period** | **frame** | **frame-period**} **high-threshold** *count* [**action** {**errordisable** | **none** | **warning**}]

次に、指定ポートで OAM リンク モニタリングの上限スレッシュホールド エラー カウントおよび関連アクションを指定する例を示します。

```
Console> (enable) set port ethernet-oam 3/1 link-monitor frame high-threshold 100
action none
Successfully updated OAM frame-period high threshold on port(s) 3/1.
Console> (enable)
```

OAM クリティカル リンク イベントの関連アクションの指定

以下のコマンドを使用すると、指定ポートで OAM クリティカル リンク イベントの関連アクション（**critical-event**、**dying-gasp**、または **link-fault**）を指定できます。デフォルトでは警告です。**dying-gasp** キーワードを指定すると、**errordisable** オプションは使用できません。

指定ポート上で OAM クリティカル リンク イベントの関連アクションを指定するには、イネーブル モードで次の作業を実行します。

作業	コマンド
指定ポートで OAM クリティカル リンク イベントの関連アクションを指定します。	**set port ethernet-oam** *mod/port* {**critical-event** | **dying-gasp** | **link-fault**} **action** {**errordisable** | **none** | **warning**}

次に、指定ポートで OAM クリティカル リンク イベントの関連アクションを指定する例を示します。

```
Console> (enable) set port ethernet-oam 3/1 link-fault action errdisable
Successfully updated OAM link-fault action on port(s) 3/1.
Console> (enable)
```

イーサネット OAM 統計情報およびイーサネット OAM 設定の消去

以下のコマンドを使用すると、すべてのポートまたは個々のポート上で OAM 統計情報および OAM 関連の設定を消去できます。

すべてのポートまたは個々のポート上で OAM 統計情報および OAM 関連の設定を消去するには、イネーブル モードで次の作業を実行します。

作業	コマンド
すべてのポートまたは個々のポート上で OAM 統計情報および OAM 関連の設定を消去します。	**clear port ethernet-oam** [*mod/port*] [**statistics**]

次に、すべてのポートの OAM 設定を消去する例を示します。

```
Console> (enable) clear port ethernet-oam
Successfully cleared OAM config on port(s) 2/1-2,3/1-48,8/1-8.
Console> (enable)
```

次に、特定のポートの OAM 設定を消去する例を示します。

```
Console> (enable) clear port ethernet-oam 3/1
Successfully cleared OAM config on port(s) 3/1.
Console> (enable)
```

次に、すべてのポートの OAM 統計情報を消去する例を示します。

```
Console> (enable) clear port ethernet-oam statistics
Successfully cleared OAM statistics on port(s) 2/1-2,3/1-48,8/1-8.
Console> (enable)
```

次に、特定のポートの OAM 統計情報を消去する例を示します。

```
Console> (enable) clear port ethernet-oam 3/1 statistics
Successfully cleared OAM statistics on port(s) 3/1.
Console> (enable)
```

OAM リンク モニタリング用のユーザ設定パラメータの消去

以下のコマンドを使用すると、指定ポート上で OAM リンク モニタリング用のユーザ設定パラメータを消去できます。上限スレッシュホールドまたは下限スレッシュホールドを消去すると、関連アクションも消去されます。

指定ポートで OAM リンク モニタリング用のユーザ設定パラメータを消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
指定ポート上で OAM リンク モニタリング用のユーザ設定パラメータを消去します。	**clear port ethernet-oam** *mod/port* **link-monitor** {**symbol-period** | **frame** | **frame-period**} {**high-threshold** | **low-threshold** | **window**}

次に、指定ポート上で OAM リンク モニタリング用のユーザ設定パラメータを消去する例を示します。

```
Console> (enable) clear port ethernet-oam 3/1 link-monitor frame high-threshold
Successfully cleared OAM frame-period high-threshold on port(s) 3/1.
Console> (enable)

Console> (enable) clear port ethernet-oam 3/1 link-monitor frame-period window
Successfully cleared OAM frame-period window on port(s) 3/1.
Console> (enable)
```

OAM クリティカル リンク イベント用のユーザ設定アクションの消去

以下のコマンドを使用すると、指定ポート上で OAM クリティカル リンク イベント用のユーザ設定アクションを消去できます。

指定ポートで OAM クリティカル リンク イベント用のユーザ設定アクションを消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
指定ポート上で OAM クリティカル リンク イベント用のユーザ設定アクションを消去します。	**clear port ethernet-oam** *mod/port* {**critical-event** | **dying-gasp** | **link-fault**} **action**

次に、指定ポート上で OAM クリティカル リンク イベント用のユーザ設定アクションを消去する例を示します。

```
Console> (enable) clear port ethernet-oam 3/1 link-fault action
Successfully cleared OAM link-fault action on port(s) 3/1.
Console> (enable)

Console> (enable) clear port ethernet-oam 3/1 critical-event action
Successfully cleared OAM critical-event action on port(s) 3/1.
Console> (enable)
```

イーサネット OAM 関連情報の表示

以下のコマンドを使用すると、すべての OAM ポートまたは指定の OAM ポートの OAM 設定およびステータスを表示できます。

すべての OAM ポートまたは指定の OAM ポートの OAM 設定およびステータスを表示するには、ユーザ モードで次の作業を実行します。

作業	コマンド
すべての OAM ポートまたは指定の OAM ポートの OAM 設定およびステータスを表示します。	**show port ethernet-oam** [*mod* | *mod/port*]

次に、指定ポートで OAM 設定およびステータスを表示する例を示します。

```
Console> (enable) show port ethernet-oam 1/1,3/5,4/6

Port  State    Mode    Status       LinkMonitor ConfigRev MaxPdu
----- -------- ------- ------------ ----------- --------- ------
1/    enable   active  R-Loopback   enable      11        1518
3/5   enable   passive Connecting   enable      38        1518
4/6   disable  active  Operational  disable     0         1518

Port  Remote   Link    UniDir  Variable
      Loopback Event           retrieval
----- -------- ------- ------- ---------
1/1   Permit   enable  disable disable
3/5   Permit   enable  enable  disable
4/6   Deny     enable  disable disable

Port  ErrSymbol Period  ErrSymbol Period    ErrSymbol Period
      Window              LowThreshold        HighThreshold
      (millions)        Count     Action    Count     Action
----- ----------------- --------- --------- --------- ---------
1/1   625               1         None      10        Warning
3/5   65535             1         Warning   1000      ErrDisable
4/6   1                 1         None      1         ErrDisable

Port   Errored Frame    Errored Frame       Errored Frame
       Window            LowThreshold       HighThreshold
       (100 msec)       Count     Action    Count     Action
----- ----------------- --------- --------- --------- ---------
1/1   300               1         None      10        Warning
3/5   65535             1         Warning   1000      ErrDisable
4/6   1000              1         Warning   1         ErrDisable

Port  ErrFrame Period   ErrFrame Period     ErrFrame Period
      Window              LowThreshold        HighThreshold
                        Count     Action    Count     Action
----- ----------------- --------- --------- --------- ---------
1/1   10000             1         None      10        Warning
3/5   1294967000        1         Warning   1000      ErrDisable
4/6   200               1         Warning   1         ErrDisable

Port  LinkFaultAction   DyingGaspAction CriticalEventAction
----- ----------------- --------------- -------------------
1/1   ErrDisable        Warning         Warning
3/5   None              Warning         None
4/6    ErrDisable          None             None
Console> (enable)
```

イーサネット OAM ネイバ情報の表示

以下のコマンドを使用すると、OAM ネイバ情報を表示できます。*ネイバ*は、接続している OAM ピアです。

指定のネイバまたはすべてのネイバの OAM 情報を表示するには、ユーザ モードで次の作業を実行します。

作業	コマンド
指定のネイバまたはすべてのネイバの OAM 情報を表示します。	**show port ethernet-oam** [*mod* | *mod/port*] **neighbor**

次に、すべてのネイバの OAM 情報を表示する例を示します。

```
Console> (enable) show port ethernet-oam neighbor
Port  MAC Addr           OUI    VendorInfo Mode    ConfigRev MaxPDU
----- ----------------- ------ ---------- ------- --------- ------
1/1   00-50-54-6c-b5-20 00000C 0000018C   passive 3         1518
3/5   00-0b-fc-fb-4a-10 00000C 0000018D   active  7         1518

Port  Remote   Link    UniDir  Variable
      Loopback Event           retrieval
----- -------- ------- ------- ---------
1/1   permit   enable  disable disable
3/5    deny      enable  enable   disable
Console> (enable)
```

イーサネット OAM リモート ループバック テスト情報の表示

以下のコマンドを使用すると、指定ポート上で OAM リモート ループバック テストの情報を表示できます。**current-session** キーワードにより、現在の OAM リモート ループバック セッションの統計情報が表示されます。**detail** キーワードおよび **current-session** キーワードを指定すると、MAC 統計情報が表示されます。**last-session** キーワードにより、最後の OAM リモート ループバック セッションの統計情報が表示されます。**detail** キーワードおよび **last-session** キーワードを指定すると、MAC 統計情報およびリモート ピア（サポートされる場合）により報告された統計情報が表示されます。ポートで新しいリモート ループバック セッションを開始すると、最後のセッション情報が使用不可能になります。

指定ポートの OAM リモート ループバック テストの情報を表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
指定ポートの OAM リモート ループバック テストを表示します。	**show port ethernet-oam** [*mod* | *mod/port*] {**remote-loopback**} {**current-session** | **last-session**} [**detail**]

次に、OAM リモート ループバック テストの現在のセッションの情報を表示する例を示します。

```
Console> (enable) show port ethernet-oam 1/2 remote-loopback current-session

Port Loopback at OAM Rx     OAM Tx
---- ------------ ---------- ----------
1/2  Remote           33333      55555

Console> (enable) show port ethernet-oam 1/2 remote-loopback current-session detail
Port: 1/2
Loopback: Remote OAM in loopback mode
Start: Mon Aug 1 2005, 07:30:59
End: Still running
Test statistics:
OAM Rx: 10000
OAM Tx: 10000
MAC Rx: 13415
MAC Tx: 13403
OAMPDU Rx: 3415
OAMPDU Tx: 3403
MAC Rx Drop: 0

Console> (enable)
```

次に、OAM リモート ループバック テストの最後のセッションの情報を表示する例を示します。

```
Console> (enable) show port ethernet-oam 1/2 remote-loopback last-session

Port Last Loopback at   OAM Rx     OAM Tx
---- ----------------   ---------- ----------
1/2  Remote                  33333      55555

Console> (enable) show port ethernet-oam 1/2 remote-loopback last-session detail

Port: 1/2
Last Loopback: Remote OAM in loopback mode
Start: Mon Aug 1 2005, 07:30:59
End: Mon Aug 1 2005, 08:29:07
Test statistics:
       OAM Rx: 10000
       OAM Tx: 10000
       MAC Rx: 13459
       MAC Tx: 13448
    OAMPDU Rx: 3459
    OAMPDU Tx: 3448
  MAC Rx Drop: 0
Test statistics reported by remote peer:
       OAM Rx: 10000
       OAM Tx: 10000
       MAC Rx: 13448
    OAMPDU Rx: 3448
  MAC Rx Drop: 0
Console> (enable)
```

イーサネット OAM 統計情報の表示

以下のコマンドを使用すると、OAM 統計情報を表示できます。

OAM 統計情報を表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
OAM 統計情報を表示します。	**show port ethernet-oam** [*mod* | *mod/port*] **statistics**

次に、ポート 1/2 の OAM 統計情報を表示する例を示します。

```
Console> (enable) show port ethernet-oam 1/2 statistics
Port  InfoPduRx  UniEventRx DupEventRx RLBCtrlRx  VarReqRx   VarResRx
----- ---------- ---------- ---------- ---------- ---------- ----------
1/2   2579       0          0          0          0          0
Port  InfoPduTx  UniEventTx DupEventTx RLBCtrlTx  VarReqTx   VarResTx
----- ---------- ---------- ---------- ---------- ---------- ----------
1/2   2571       0          0          1          0          0
Port  OrgSpecRx  UnknownRx  CiscoPduRx CiscoTLVRx
----- ---------- ---------- ---------- ----------
1/2   0          0          0          1
Port  OrgSpecTx  UnknownTx  CiscoPduTx CiscoTLVTx
----- ---------- ---------- ---------- ----------
1/2   0          0          0          0
Console> (enable)
```

CHAPTER 20

GOLD の設定

この章では、Catalyst 6500 シリーズ スイッチ上で Generic Online Diagonostics（GOLD）を設定する方法について説明します。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

この章で説明する内容は、次のとおりです。

オンライン診断の機能概要

(注) GOLD は、Supervisor Engine 720 および Supervisor Engine 32 上でのみサポートされます。ただし、以前の診断コマンドは Supervisor Engine 1 および Supervisor Engine 2 上でもサポートされます。

オンライン診断では、次の機能を実行します。

- スイッチが稼働中のネットワークに接続している間に、スーパバイザ エンジン、モジュール、およびスイッチのハードウェア機能をテストおよび検証します。
- 各種ハードウェア コンポーネントをチェックするパケット スイッチング テストを実行して、データ パスおよび制御信号を検証します。
- 問題の検出箇所は、次のとおりです。
  - ハードウェア コンポーネント
  - インターフェイス（GBIC [ギガビット インターフェイス コンバータ]、イーサネット ポートなど）
  - コネクタ（接触不良コネクタ、曲がったピンなど）
  - はんだ接合
  - メモリ（経時的な障害）

オンライン診断は、次のように分類されます。

- 起動 — 起動診断は、起動、モジュールの Online Insertion and Removal（OIR; ホットスワップ）、またはバックアップ スーパバイザ エンジンへのスイッチオーバーの間に実行されます。
- オンデマンド — オンデマンド診断は、CLI（コマンドライン インターフェイス）から実行されます。
- スケジュール診断 — スケジュール診断は、スイッチが稼働中のネットワークへ接続中に、ユーザ指定の間隔または指定時間に実行されます。
- ヘルス モニタリング — ヘルス モニタリング診断は、バックグラウンドで実行されます。

オンライン診断テストには、次の 2 種類があります。

- 中断を伴うオンライン診断テスト — このテストには、Built-in self test（BIST）および中断を伴うループバック テストが含まれます。
- 中断を伴わないオンライン診断テスト — このテストにはパケット スイッチングが含まれ、起動、ライン カードの OIR、およびシステム再設定診断テストの間に実行されます。中断を伴わない診断テストは、バックグラウンドのヘルス モニタリングの一部として、またはユーザ要求（オンデマンド）で実行されます。

オンライン診断は、ハイアベイラビリティ機能の要件の 1 つです。ハイアベイラビリティは、ネットワーク上の機器障害による影響を制限しようとする一連の品質標準です。ハイアベイラビリティの中核となるのは、スイッチが稼働中のネットワークで動作している間に、ハードウェア障害を検出し、改善処置を行うことです。ハイアベイラビリティのオンライン診断では、ハードウェア障害を検出し、ハイアベイラビリティ ソフトウェア コンポーネントにフィードバックして、スイッチオーバーの判断をします。

オンライン診断の設定

ここでは、オンライン診断を設定する手順について説明します。

起動オンライン診断レベルの指定

起動オンライン診断レベルを最低限または完全に指定するか、またはすべての起動診断を省略できます。すべての診断を実行するには、**complete** キーワードを入力します。スーパバイザ エンジンの Policy Feature Card（PFC; ポリシー フィーチャ カード）テストおよびスイッチのすべてのポートのループバック テストのみを実行するには、**minimal** キーワードを入力します。すべての診断テストを省略するには、**bypass** キーワードを入力します。デフォルトの起動診断レベルは、省略です。

（注） 起動診断レベルは、スイッチ全体に適用され、モジュール単位では設定できません。

起動診断レベルを指定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	起動診断レベルを指定します。	**set diagnostic bootup level** [**bypass** | **minimal** | **complete**]
ステップ 2	起動診断レベルを表示します。	**show diagnostic bootup level**

次に、起動診断レベルを省略に指定する例を示します。

```
Console> (enable) set diagnostic bootup level bypass
Diagnostic level set to bypass
Console> (enable)

Console> (enable) show diagnostic bootup level
Current bootup diagnostic level: bypass
Console> (enable)
```

オンデマンド オンライン診断の設定

注意 ほとんどのオンライン診断メモリ テストは、中断を伴ううえに時間がかかるために、オンデマンド テストとなります。メモリ テストは、ハードウェアの問題の可能性がある場合、および運用中のネットワーク環境とシステムが分離されたあとでのみ使用してください。

(注)　オンライン診断テストでは EOBC チャネルを使用して、残りのシステムと通信します。オンライン診断テストの実行には、スーパバイザ エンジンと SLCP、Link Control Protocol（LCP; リンク制御プロトコル）、およびモジュール プロセッサ間の EOBC チャネルの適切な動作が必要です。

オンデマンド オンライン診断の設定については、次を参照してください。

- オンデマンド オンライン診断テストの実行（p.20-4）
- オンデマンド オンライン診断の設定上の注意事項および制限事項（p.20-4）
- オンデマンド オンライン診断の設定手順（p.20-5）
- オンデマンド オンライン診断の action-on-failure キーワードおよび iterations キーワード コマンド（p.20-8）

オンデマンド オンライン診断テストの実行

注意　ここでは、オンデマンドの **diagnostic start** および **diagnostic stop** コマンドについて説明します。いずれのオンデマンド オンライン診断テストを実行する場合でも、「オンデマンド オンライン診断の設定手順」（p.20-5）の手順を使用します。これらのテストは、事前にオンデマンド オンライン診断設定手順を行ってから実行してください。

テスト ID に基づいて特定のテストを開始するには、**diagnostic start** コマンドを使用します。このコマンドは、1 つのテスト ID、テスト ID の範囲、テストのサブグループ、またはすべてのテストを指定する **all** を指定できます。特定テストのテスト ID は、モジュール タイプ別、またはソフトウェア リリース別によっても変えられます。**show diagnostic content** コマンドを使用して、正確なテスト ID および関連するテスト名を入手することが重要です。指定モジュールで実行中のテストを停止するには、**diagnostic stop module** *mod* コマンドを使用します。**diagnostic start** および **diagnostic stop** コマンドの完全な構文は、次のとおりです。

diagnostic start module *mod_num* ***test*** {***all*** | *test_ID_num* | *test_list* | ***complete*** | ***minimal*** | ***non-disruptive*** | ***per-port***} [***port*** {***all*** | *port_num* | *port_list*}]

diagnostic stop module *mod*

オンデマンド オンライン診断の設定上の注意事項および制限事項

ここでは、「オンデマンド オンライン診断の設定手順」（p.20-5）に記載されたオンデマンド テスト設定手順を実行する場合の、設定上の注意事項および制限事項について説明します。

- 特定の手順でテストを実行したあとは、それ以前の手順のテストは機能しません。
- テストの実行前後には、特定の作業を行う必要がある場合があります。これらの作業は、設定手順で説明されています。
- テストには、中断を伴うものもあります。設定手順では、すべての中断を伴うテストの実行に関するガイダンスを提供しています。
- メモリ テストを実行する前に、パケットスイッチング テストを実行する必要があります。
- メモリ テストは常に、まずモジュール上で実行してからスーパバイザ エンジンで実行する必要があります。これは、スーパバイザ エンジン上でのメモリ テスト実行後、システムは使用不可能ステートになり、通常の動作を行うためにすぐ再起動する必要があるためです。

(注)　Release 8.5(1) では、メモリ テストはスーパバイザ エンジンに対してのみ使用できます。他のモジュールに対するメモリ テストは、次のリリースで予定されています。

オンデマンド オンライン診断の設定手順

オンデマンド オンライン診断テストを実行するには、次の手順を行います。

ステップ 1　中断を伴わないテストを実行します。中断を伴わないテストは、パケット スイッチング テストで、システム動作は中断しません。これらのテストは、わずか数秒で終了します。

その他のテスト要件は、次のとおりです。

- テスト実行前のユーザ作業 — なし
- テスト実行後のユーザ作業 — なし

ステップ 2　パケット スイッチング テストは、各種機能テスト グループに分類されます。次の表を使用して、テストする機能テスト グループを決定し、その機能テスト グループのテストを実行します。

- 表 20-1 オンデマンド テスト：スーパバイザ エンジン
- 表 20-2 オンデマンド テスト：ファブリックがイネーブルのモジュール
- 表 20-3 オンデマンド テスト：ファブリックがイネーブルでないモジュール

(注)　サポート対象の機能テスト グループはモジュール タイプによって異なるため、すべてのモジュールにすべての機能テスト グループが存在するわけではありません。選択する機能テスト グループが不明な場合は、**diagnostic start module** *mod/num* **test complete** コマンドにより診断レベルが [complete] に設定された場合に、起動中に実行されるすべてのパケット スイッチング テストを行います。

(注)　ループバック テストを実行して、1 つまたは複数のモジュール ポート上に障害がある場合、そのモジュール上のポートに接続されたケーブルをすべて切断し、モジュール上のすべてのポートをシャット ダウンしてから、ループバック テストに戻ります。何らかのスプリアス パケットがループバック テストに干渉して、失敗の原因となる場合があります。また、モジュールにインラインパワー ドータ カードが搭載されている場合も、テスト実行前にインラインパワー ドータ カードの電源をディセーブルにしてください。

その他のテスト要件は、次のとおりです。

- テスト実行前のユーザ作業 — なし
- テスト実行後のユーザ作業 — なし

表 20-1　オンデマンド テスト：スーパバイザ エンジン

機能テスト グループ	個々のテスト
ポート単位のテスト	TestLoopback
レイヤ 2 フォワーディング テスト	TestNewIndexLearn TestMatchCapture TestDontConditionalLearn TestProtocolMatchChannel TestBadBpduTrap
NetFlow 機能	TestNetflowInlineRewrite
ACL/QoS 機能	TestAclPermit TestQosTcam TestAclDeny
IP バージョン 4 機能	TestIPv4FibShortcut TestFibDevices TestL3Capture2 TestNATFibShortcut
マルチキャスト機能	TestL3VlanMet
Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）機能	TestIngressSpan TestEgressSpan
ファブリック接続	TestFabricSnakeForward TestFabricSnakeBackward
EOBC 接続	ステップ 3 に進む
パケット バッファ問題	ステップ 4 に進む

表 20-2　オンデマンド テスト：ファブリックがイネーブルのモジュール

機能テスト グループ	個々のテスト
ポート単位のテスト	TestLoopback
マルチキャスト機能	TestL3VlanMet
SPAN 機能	TestIngressSpan TestEgressSpan
ファブリック テスト	TestSynchedFabChannel

表 20-3　オンデマンド テスト：ファブリックがイネーブルでないモジュール

機能テスト グループ	個々のテスト
ポート単位のテスト	TestLoopback TestNetflowInlineRewrite

ステップ 3　TestTrafficStress テストを実行します。

（注） Release 8.5(1) では、TestTrafficStress テストは使用できません。このテストは、次のリリースで使用可能になる予定です。テストが使用できない場合は、次の手順に進んでください。

この中断を伴うパケット スイッチング テストは、スーパバイザ エンジン上でのみ使用できます。このテストではシステム上のポートをペアにして、パケットがこれらのポート間でシステムのストレステスト用の回線速度でスイッチングされるようにします。テストを終了するには数分かかります。テスト中に、すべてのポートはシャット ダウンされたり、ポートの一部がアップ / ダウン（フラップ）する場合もありますが、テスト終了後にはポートが回復します。その他のテスト要件は、次のとおりです。

- テスト実行前のユーザ作業 — このテストの前には、モジュールのすべてのヘルス モニタリング テストをディセーブルにする必要があります。
- テスト実行後のユーザ作業 — なし

ステップ 4　TestEobcStressPing テストを実行します。

（注） Release 8.5(1) では、TestEobcStressPing テストは使用できません。このテストは、次のリリースで使用可能になる予定です。テストが使用できない場合は、次の手順に進んでください。

この中断を伴うテストでは、指定のモジュールの EOBC 接続を確認します。テストを終了するには 2 ～ 3 分かかります。このテスト終了後は、前述の手順で説明されたパケット スイッチング テストを実行できません。ただし、ステップ 5 で説明するテストは実行できます。その他の要件は、次のとおりです。

- テスト前のユーザ作業 — このテストの実行前は、モジュールのすべてのヘルス モニタリング テストをディセーブルにする必要があります。これは、EOBC 接続が中断され、ヘルス モニタリング テストが失敗する原因となるからです。
- テスト実行後のユーザ作業 — ステップ 5 で記述されたテストを実行するか、またはモジュールをオン / オフして、通常の動作に戻します。モジュールがオンラインになったあと、ディセーブルにしたヘルス モニタリング テストを再びイネーブルにします。

ステップ 5　包括的メモリ テストを実行します。

包括的メモリ テストは、スーパバイザ エンジンおよびほかのモジュールで実行できます。スーパバイザ エンジン上でのメモリ テストは、他のモジュールでのメモリ テストが実行されたあとでのみ実行する必要があるので注意してください。スーパバイザ エンジンのメモリ テストの実行後、システムは使用不可能ステートになり、通常の動作ステートに戻すには再起動する必要があるため、この順番が必須となります。

（注） Release 8.5(1) では、メモリ テストはスーパバイザ エンジンに対してのみ使用できます。他のモジュールに対するメモリ テストは、次のリリースで予定されています。

（注） 包括的メモリ テストの実行後は、スーパバイザ エンジンまたは他のモジュール上でその他のテストを実行できません。

注意　いずれのメモリ テストも実行前に、以下の「テスト実行前のユーザ作業」に示されるすべての要件に従っていることを確認してください。

包括的メモリ テストは、個々に実行できます。メモリ サイズによっては、テスト終了までに数時間かかるものもあります。モジュールごとに複数のメモリ テストがあり、それらは相互依存しているため、各モジュールでのテストの実行順序が重要となります。これらのテストの実行順序は、次のとおりです。

（注） Release 8.5(1) では、TestFibTcamSSRAM テストのみが使用可能な包括的メモリ テストです。その他のメモリ テスト（以下の項目 2 ～ 5）は、次のリリースで予定されています。

1. TestFibTcamSSRAM
2. TestAclQosTcam
3. TestNetflowTcam
4. TestAsicMemory
5. TestLinecardMemory

モジュールに特定のテストが存在しない場合は、省略できます。その他の要件は、次のとおりです。

- テスト実行前のユーザ作業
  - **clear diagnostic monitor module** *num* **test all** コマンドを使用して、スーパバイザ エンジンおよびスイッチング モジュール上でのすべてのバックグラウンド ヘルスモニタリング テストをオフにします。
  - 接続されているすべてのポートをディセーブルにして、ネットワーク トラフィックを切り離します。
  - メモリ テスト中は、テスト パケットを送信しないでください。
  - スーパバイザ エンジンの PFC 上の Forwarding Information Base（FIB; 転送情報ベース）Ternary CAM（TCAM）および SSRAM をテストするために、すべてのスイッチング モジュールを取り外します。
  - システムまたはテスト中のモジュールをリセットしてから、システムを通常の動作モードに戻します。
- テスト実行後のユーザ作業
  - スーパバイザ エンジン ― スイッチを再起動しますが、テスト中に設定が変更されているため、再起動中に設定を保存しないでください。
  - 他のモジュール ― モジュールをオン / オフします。モジュールがオンラインになったあと、ディセーブルだったヘルス モニタリング テストを再びイネーブルにします。

オンデマンド オンライン診断の action-on-failure キーワードおよび iterations キーワード コマンド

continue *failure_limit* キーワードを入力すると、設定可能な数の障害が発生するまでオンデマンド オンライン診断を実行し続けるように指定できます。*failure_limit* の範囲は、0 ～ 65534 障害です。**stop** キーワードを入力すると、単一の障害が発生した場合にオンデマンド オンライン診断の実行を中止するように指定できます。**iterations** *number_of_iterations* キーワードを入力すると、オンデマンド テストを複数回実行するように指定できます。*number_of_iterations* の範囲は、1 ～ 999 です。これらのキーワードの完全な構文は、次のとおりです。

set diagnostic ondemand action-on-failure [**continue** *failure_limit* | **stop**]

set diagnostic ondemand iterations *number_of_iterations*

オンライン診断ヘルス モニタリング テストの設定

スイッチが稼働中のネットワークに接続している間に、指定のモジュール上でヘルスモニタリング診断テストを設定できます。各ヘルスモニタリング テストの実行間隔、テスト失敗時にシステム メッセージを生成するかどうか、または個々のテストをイネーブル / ディセーブルにするかどうかを指定できます。

デフォルトでは、中断を伴うテストがディセーブルです。特定数の中断を伴わないテスト（すべてではない）は、デフォルトでイネーブルです。中断を伴う（D）および中断を伴わない（N）テストを判別するには、**show diagnostic content module** *mod_list* コマンドを使用して、[Attributes] カラムを確認します。この情報は、その他のヘルス モニタリング テストを設定するのに使用します。ヘルス モニタリングには、中断を伴わないテストのみを使用することを推奨します。

オンライン診断ヘルスモニタリング テストを設定するには、イネーブル モードで次の作業を実行します。

	作業	コマンド
ステップ 1	オンライン診断モニタリング インターバルを指定します。	**set diagnostic monitor interval module** *mod_num* **test** {**all** | *test_ID_num* | *test_list*} *hh:mm:ss*[1]
ステップ 2	（任意）ヘルスモニタリング診断テストをイネーブルにします。	**set diagnostic monitor module** *mod_num* **test** {*test-id* | *test-id-range* | **all**}
ステップ 3	テスト失敗時の Syslog の生成をイネーブルにします。	**set diagnostic monitor syslog**
ステップ 4	オンライン診断モニタリング設定を表示します。	**show diagnostic content module** {*mod_list* | **all**}

1. **interval** キーワードには、0 ～ 999（ミリ秒）の範囲および 0 ～ 20（日）を指定できます。

次に、オンライン診断ヘルスモニタリング テスト（テスト 18）をモジュール 7 上で、10 日ごとの 12 時 12 分 12.1 秒に実行するよう指定する例を示します。

```
Console> (enable) set diagnostic monitor interval module 7 test 18 12:12:12 100 10
Diagnostic monitor interval set at 12:12:12 100 10 for module 7 test 18
Console> (enable)
```

次に、モジュール 7 でテスト 18 をイネーブルにする例を示します。

```
Console> (enable) set diagnostic monitor module 7 test 18
Module 7 test 18 diagnostic monitor enable.
Console> (enable)
```

次に、テスト失敗時の Syslog 生成をイネーブルにする例を示します。

```
Console> (enable) set diagnostic monitor syslog
Diagnostic monitor syslog enable.
Console> (enable)
```

オンライン診断のスケジューリング

特定のモジュールについて、指定時間、または毎日、毎週、毎月のペースでオンライン診断を実行できます。すべてのテストを実行するか、または個々のテストを実行するかを指定できます。テストは、一度だけ、または指定間隔で繰り返し実行するかをスケジュールできます。

（注） オンライン診断を指定時間に実行するようにスケジュールしたあとに、**set time** コマンドを使用してシステム時間を変更した場合は、オンライン診断は指定時間に実行されません。たとえば、オンライン診断を 3:00 pm に実行するようスケジュールした場合に、システム時間を 2:59 に変更すると、オンライン診断は 3:00 pm に実行されません。

オンライン診断をスケジュールするには、イネーブル モードで次の作業を実行します。

	作業	コマンド
ステップ 1	オンライン診断をスケジュールします。	**set diagnostic schedule module** *slot_num* **test** {*test-id* | *test-id-range* | **all**} {[**port** {*port_num* | *port_num_range* | **all**}] | [**daily** *hh*:*mm*] [**on** *month day_of_month year hh*:*mm*] [**weekly** *day hh*:*mm*]}
ステップ 2	オンライン診断のスケジューリングを表示します。	**show diagnostic schedule module** *mod_list*

次に、特定の日時に特定のモジュールで行われるように、診断テスト（テスト 1 および 2 を指定）をスケジュールする例を示します。

```
Console> (enable) set diagnostic schedule module 7 test 1 daily 12:12
Diagnostic schedule set at daily 12:12 for module 7 test 1
Console> (enable)
```

次に、毎日特定の時間に、特定のポートおよびモジュールで診断テスト（テスト 1 を指定）をスケジュールする例を示します。

```
Console> (enable) set diagnostic schedule module 7 test 3 port 1 daily 16:16
Diagnostic schedule set at daily 16:16 for module 7 test 3
Console> (enable)

Console> (enable) show diagnostic schedule module 7

Current Time = Fri Apr 15 2005, 16:56:06

Diagnostic for Module 7:

Schedule #1:
        To be run daily 12:12
        Test ID(s) to be executed: 1-2.

Schedule #2:
        To be run daily 16:16
        Test ID(s) to be executed: 3.
        Port(s) to be tested: 1.

Console> (enable)
```

オンライン診断失敗応答の指定

スーパバイザ エンジンにオンライン診断失敗応答を指定できます。**ignore** キーワードを指定した場合、スーパバイザ エンジンはオンライン診断失敗後起動します。**system** キーワードを指定した場合（デフォルト）、スーパバイザ エンジンはオフラインのまま維持され、モジュール固有の改善処置が行われます。

スーパバイザ エンジンにオンライン診断失敗応答を指定するには、イネーブル モードで次の作業を実行します。

	作業	コマンド
ステップ 1	スーパバイザ エンジンにオンライン診断失敗応答を指定します。	**set diagnostic diagfail-action** {**ignore** | **system**}
ステップ 2	スーパバイザ エンジンのオンライン診断失敗応答の設定値を表示します。	**show diagnostic diagfail-action**

次に、オンライン診断の失敗後、スーパバイザ エンジンがオフラインになるように指定する例を示します。

```
Console> (enable) set diagnostic diagfail-action system
Diagnostic failure action set to system.
Console> (enable) show diagnostic diagfail-action
Diagnostic failure action at last bootup : system
Diagnostic failure action at next reset  : system
Console> (enable)
```

オンライン診断のイベント ログ サイズの指定

デフォルトの設定は 500 エントリで、有効範囲は 1 ～ 10,000 エントリです。

オンライン診断のイベント ログ サイズを指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
オンライン診断のイベントログ サイズを指定します。	**set diagnostic event-log size** [*size*]

次に、オンライン診断のイベントログ サイズを 1000 エントリに指定する例を示します。

```
Console> (enable) set diagnostic event-log size 1000
Diagnostic event-log size set to 1000
Console> (enable)
```

オンライン診断テストおよびテスト結果の表示

show コマンドにより、特定のモジュールに設定されたオンライン診断テストを表示して、テスト結果を確認できます。

オンライン診断テスト情報を表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
起動診断レベルを表示します。	**show diagnostic bootup level**
指定されたモジュールまたはすべてのモジュールのテスト内容を表示します。	**show diagnostic content module** [*mod_num* | **all**]

作業	コマンド
スーパバイザ エンジンのオンライン診断失敗応答の設定値を表示します。	**show diagnostic diagfail-action**
診断イベント ログを表示します。	**show diagnostic events** [**event-type** {**error** | **info** | **warning**}] **show diagnostic events** [**module** {*mod_list* | **all**}] **show diagnostic events**
オンライン診断のオンデマンド設定値を表示します。	**show diagnostic ondemand settings**
指定されたモジュールまたはすべてのモジュールの診断テスト結果を表示します。	**show diagnostic result module** *mod_list* | **all** [**detail** | **test**] [*test_list*] [**detail**]
オンライン診断のスケジューリングを表示します。	**show diagnostic schedule module** *mod_list*
すべてのモジュールの現在のオンライン診断ステータスを表示します。	**show diagnostic status**

オンライン診断設定の消去

オンライン診断の設定パラメータを消去するには、ユーザ モードで次の作業を行います。

作業	コマンド
起動オンライン診断レベルを消去します。	**clear diagnostic bootup level**
オンライン診断のイベントログ サイズを消去します。	**clear diagnostic event-log size**
オンライン診断のヘルスモニタリング設定を消去します。	**clear diagnostic monitor interval module** *mod_list* **test** [*test_list* | **all**] **clear diagnostic monitor module** *mod* **test** *test_list* **clear diagnostic monitor syslog**
テスト失敗時の Syslog の生成をディセーブルにします。	**clear diagnostic monitor syslog**
オンライン診断のスケジューリング情報を消去します。	**clear diagnostic schedule module** *mod_num* **test** {*test-id* | *test-id-range* | **all**} {[**port** {*port_num* | *port_range* | **all**}] | [**device** {*device_num* | *device_range* | **all**}]}

次に、起動オンライン診断レベルを消去する例を示します。

```
Console> (enable) clear diagnostic bootup level
Diagnostic level set to bypass
Console> (enable)
```

次に、オンライン診断のイベントログ サイズを消去する例を示します。

```
Console> (enable) clear diagnostic event-log size
Diagnostic event-log size set to default(500)
Console> (enable)
```

次に、オンライン診断のモニタリング設定を消去する例を示します。

```
Console> (enable) clear diagnostic monitor interval module 7 test 3
Clear diagnostic monitor interval for module 7 test 3
Console> (enable)

Console> (enable) clear diagnostic monitor module 7 test 1
Module 7 test 1 diagnostic monitor disable.
Console> (enable)

Console> (enable) clear diagnostic monitor syslog
Diagnostic monitor syslog disable.
Console> (enable)
```

モジュール 7 上のテスト 1 および 2 に対するオンライン診断のスケジューリング設定を消去します。

```
Console> (enable) clear diagnostic schedule module 7 test 1-2 daily 12:12
Clear diagnostic schedule at daily 12:12 for module 7 test 1-2
Console> (enable)
```

CHAPTER 21

スイッチの管理

この章では、Catalyst 6500 シリーズ スイッチ上でさまざまな管理作業を実行する手順について説明します。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

この章で説明する内容は、次のとおりです。

スイッチ上でのシステム名およびシステム プロンプトの設定

スイッチのシステム名は、装置を識別するための文字列であり、ユーザ側で設定できます。デフォルト設定では、システム名は設定されていません。

システム名を手動で設定していない場合に、スイッチを次のように設定すると、Domain Name System（DNS; ドメイン ネーム システム）を使用してシステム名が割り当てられます。

- sc0 インターフェイスに、DNS サーバ上でスイッチ名にマッピングされている IP アドレスを指定
- スイッチ上で DNS をイネーブルに設定
- スイッチ上で少なくとも 1 つの有効な DNS サーバを指定

DNS 検索が正常に実行されると、スイッチの DNS ホスト名がスイッチのシステム名として設定され、NVRAM（不揮発性 RAM）に保存されます（ドメイン名は削除されます）。

システム プロンプトを設定しなかった場合、システム名の最初の 20 文字がシステム プロンプトとして使用されます（最後に大なり記号 [>] が付加されます）。システム名を変更するたびに、**set prompt** コマンドを使用して手動でプロンプトを設定している場合を除き、プロンプトも更新されます。

次のいずれかの操作を実行するたびに、DNS を使用してシステム名が検索されます。

- スイッチの初期化（電源投入またはリセット）
- CLI（コマンドライン インターフェイス）または SNMP（簡易ネットワーク管理プロトコル）を使用して、sc0 インターフェイスに IP アドレスを設定
- **set ip route** コマンドを使用してルートを設定
- **set system name** コマンドを使用してシステム名を消去
- DNS をイネーブルに設定または DNS サーバを指定

システム名を手動で設定した場合、DNS 検索は実行されません。

スタティックなシステム名およびプロンプトの設定

ここでは、スタティックなシステム名およびプロンプトを設定する手順について説明します。

スタティックなシステム名の設定

スタティックなシステム名を設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
スタティックなシステム名を設定します。	**set system name** *name_string*

（注）　システム名を設定すると、そのシステム名がシステム　プロンプトとして使用されます。プロンプトの文字列は、**set prompt** コマンドで上書きすることができます。

次に、スイッチ上にシステム名を設定する例を示します。

```
Console> (enable) set system name Catalyst 6500
System name set.
Catalyst 6500> (enable)
```

スタティックなシステム プロンプトの設定

スタティックなシステム プロンプトを設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
スタティックなシステム プロンプトを設定します。	**set prompt** *prompt_string*

次に、スイッチ上にスタティックなシステム プロンプトを設定する例を示します。

```
Console> (enable) set prompt Catalyst6509>
Catalyst6509> (enable)
```

システム名の消去

システム名を消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
システム名を消去します。	**set system name**

次に、システム名を消去する例を示します。

```
Console> (enable) set system name
System name cleared.
Console> (enable)
```

スイッチ上でのシステム コンタクトおよびロケーションの設定

リソース管理に役立つように、システムのコンタクト（連絡先）およびロケーション（設置場所）を設定できます。

システムのコンタクトおよびロケーションを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	システム コンタクトを設定します。	**set system contact** [*contact_string*]
ステップ 2	システム ロケーションを設定します。	**set system location** [*location_string*]
ステップ 3	グローバル システム情報を確認します。	**show system**

次に、システムのコンタクトおよびロケーションを設定し、その設定を確認する例を示します。

```
Catalyst 6500> (enable) set system contact sysadmin@corp.com
System contact set.
Catalyst 6500> (enable) set system location Sunnyvale CA
System location set.
Catalyst 6500> (enable) show system
PS1-Status PS2-Status Fan-Status Temp-Alarm Sys-Status Uptime d,h:m:s Logout
---------- ---------- ---------- ---------- ---------- -------------- ---------
ok         none       ok         off        ok         0,04:04:07     20 min

PS1-Type   PS2-Type   Modem   Baud  Traffic Peak Peak-Time
---------- ---------- ------- ----- ------- ---- -------------------------
other      none       disable  9600   0%      0% Tue Jun 23 1998, 16:51:36

System Name              System Location          System Contact
------------------------ ------------------------ ------------------------
Catalyst 6500            Sunnyvale CA             sysadmin@corp.com
Catalyst 6500> (enable)
```

スイッチ上でのシステム クロックの設定

（注） Network Time Protocol（NTP）を使用して日時を取得するようにスイッチを設定できます。NTP の設定手順については、第 33 章「NTP の設定」を参照してください。

システム クロックを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	システム クロックを設定します。	**set time** [*day_of_week*] [*mm/dd/yy*] [*hh:mm:ss*]
ステップ 2	現在の日時を表示します。	**show time**

次に、システム クロックを設定し、現在の日時を表示する例を示します。

```
Console> (enable) set time Mon 06/15/98 12:30:00
Mon Jun 15 1998, 12:30:00
Console> (enable) show time
Mon Jun 15 1998, 12:30:02
Console> (enable)
```

スイッチ上でのログイン バナーの作成

ユーザがスイッチにログインする際に、画面に表示される 1 つまたは複数行のメッセージ バナーを作成できます。**motd** キーワードの次に入力する 1 文字が、バナー テキストの開始と終了を示すデリミタになります。終了デリミタより後ろの文字は破棄されます。終了デリミタを入力し、**Return** キーを押します。バナー テキストの長さは 3,070 文字未満です。

ここでは、ログイン バナーを設定および消去する手順について説明します。

ログイン バナーの設定

ログイン バナーを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ログイン バナーを入力します。	**set banner motd** *c message_of_the_day c*
ステップ 2	ログアウトし、再度スイッチにログインして、ログイン バナーを表示します。	–

次に、開始および終了デリミタとして # 記号を使用し、スイッチのログイン バナーを設定する例を示します。

```
Console> (enable) set banner motd #
Welcome to the Catalyst 6500 Switch!
Unauthorized access prohibited.
Contact sysadmin@corp.com for access.
#
MOTD banner set
Console> (enable)
```

ログイン バナーの消去

ログイン バナーを消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
ログイン バナーを消去します。	**set banner motd** *cc*

次に、ログイン バナーを消去する例を示します。

```
Console> (enable) set banner motd ##
MOTD banner cleared
Console> (enable)
```

スイッチ上での Cisco Systems Console Telnet ログイン バナーの表示または抑制

[Cisco Systems Console] Telnet ログイン バナーを表示または抑制するには、イネーブル モードで次の作業を行います。

（注） デフォルトでは、Cisco Systems Console Telnet ログイン バナーはイネーブルです。

	作業	コマンド
ステップ 1	Cisco Systems Console Telnet ログイン バナーを表示または抑制します。	**set banner telnet** {**enable** | **disable**}
ステップ 2	Cisco Systems Console Telnet ログイン バナー設定を表示します。	**show banner**

次に、Cisco Systems Console Telnet ログイン バナーをイネーブルにする例を示します。

```
Console> (enable) set banner telnet enable
Cisco Systems Console banner will be printed at telnet.
Console> (enable)
```

次に、Cisco Systems Console Telnet ログイン バナーをディセーブルにする例を示します。

```
Console> (enable) set banner telnet disable
Cisco Systems Console banner will not be printed at telnet.
Console> (enable)
```

次に、Cisco Systems Console Telnet ログイン バナーの設定を表示する例を示します。

```
Console> (enable) show banner
MOTD banner:

LCD config:

Telnet Banner:
disabled
Console> (enable)
```

スイッチ上でのコマンド エイリアスの定義

set alias コマンドを使用すると、使用頻度の高いコマンドや長くて複雑なコマンドのエイリアス（コマンドの短縮形）を 100 個まで定義できます。コマンド エイリアスを作成すると、スイッチの設定またはモニタ時に手間が省けると同時に、入力ミスを防ぐこともできます。

コマンド エイリアスは、*name* 引数で定義します。コマンドラインにコマンド エイリアスを入力することによって実行されるコマンドを、*command* および *parameter* 引数で定義します。

スイッチ上でコマンド エイリアスを定義するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチ上でコマンド エイリアスを定義します。	**set alias** *name command* [*parameter*] [*parameter*]
ステップ 2	現在定義されているコマンド エイリアスを確認します。	**show alias** [*name*]

次に、2 つのコマンド エイリアス、**sm8** および **sp8** を定義する例を示します。**sm8** は **show module 8** コマンドを発行し、**sp8** は **show port 8** コマンドを発行します。この例では、さらに、現在定義されているコマンド エイリアスを確認し、コマンドラインにコマンド エイリアスを入力した場合の処理内容を表示しています。

```
Console> (enable) set alias sm8 show module 8
Command alias added.
Console> (enable) set alias sp8 show port 8
Command alias added.
Console> (enable) show alias
sm8             show module 8
sp8             show port 8
Console> (enable) sm8
Mod Module-Name          Ports Module-Type           Model    Serial-Num Status
--- ------------------- ----- --------------------- --------- --------- -------
8                       2     DS3 Dual PHY ATM      WS-X5166  007243262 ok

Mod MAC-Address(es)                         Hw     Fw          Sw
--- --------------------------------------- ------ ----------- ------------------
8   00-60-2f-45-26-2f                       2.0    1.3         51.1(103)
Console> (enable) sp8
Port  Name            Status  Vlan    Level Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
 8/1                     notconnect trunk      normal   full    45 DS3 ATM
 8/2                     notconnect trunk      normal   full    45 DS3 ATM

Port   ifIndex
-----  -------
 8/1   285
 8/2   286


Use 'session' command to see ATM counters.

Last-Time-Cleared
--------------------------
Thu Sep 10 1998, 16:56:08
Console> (enable)
```

スイッチ上での IP エイリアスの定義

set ip alias コマンドを使用して、IP アドレスに対応するエイリアスをテキストで定義できます。IP エイリアスを定義しておけば、DNS がイネーブルに設定されていなくても、**ping**、**telnet**、およびその他のコマンドを使用する際に、簡単に他のネットワーク装置を参照できます。

IP エイリアスは、*name* 引数で定義します。*ip_addr* 引数で、エイリアスに対応する IP アドレスを定義します。

スイッチ上で IP エイリアスを定義するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチ上で IP エイリアスを定義します。	**set ip alias** *name ip_addr*
ステップ 2	現在定義されている IP エイリアスを確認します。	**show ip alias** [*name*]

次に、2 つの IP エイリアス、**sparc** および **cat6509** を定義する例を示します。**sparc** は IP アドレス 172.20.52.3 を参照し、**cat6509** は IP アドレス 172.20.52.71 を参照します。この例ではさらに、現在定義されている IP エイリアスを確認し、IP エイリアスを使用して **ping** コマンドを実行した場合の処理内容を表示しています。

```
Console> (enable) set ip alias sparc 172.20.52.3
IP alias added.
Console> (enable) set ip alias cat6509 172.20.52.71
IP alias added.
Console> (enable) show ip alias
default         0.0.0.0
sparc           172.20.52.3
cat6509         172.20.52.71
Console> (enable) ping sparc
sparc is alive
Console> (enable) ping cat6509
cat6509 is alive
Console> (enable)
```

スイッチ上でのスタティック ルートの設定

（注）　デフォルト ゲートウェイ（デフォルト ルート）の設定手順については、「デフォルト ゲートウェイの設定」（p.3-9）を参照してください。

状況によっては、1 つまたは複数の宛先ネットワーク用として、スタティック ルーティング テーブルにエントリを追加する必要があります。スタティック ルートのエントリは、宛先 IP ネットワーク アドレス、ネクスト ホップ ルータの IP アドレス、およびそのルートのメトリック（ホップ カウント）から成ります。

宛先 IP ネットワーク アドレスを変数的にサブネット化して、Classless Interdomain Routing（CIDR）をサポートできます。サブネット ビット数またはドット付き 10 進表記を使用して、宛先ネットワークのサブネット マスク（*netmask*）を指定できます。サブネット マスクを指定しないと、デフォルト（classful）マスクが使用されます。

スイッチは、IP ルーティング テーブル内の最長一致アドレスを使用して、スイッチが生成した IP トラフィックを転送します。スイッチは、接続装置からのトラフィックの転送には IP ルーティング テーブルを使用しません。スイッチ本体が生成した IP トラフィック（Telnet、Trivial File Transfer Protocol [TFTP; 簡易ファイル転送プロトコル]、および ping など）の転送だけに使用します。

スタティック ルートを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	リモート ネットワークまでのスタティック ルートを設定します。	**set ip route** *destination*[/*netmask*] *gateway* [*metric*]
ステップ 2	IP ルーティング テーブルにスタティック ルートが正しく組み込まれていることを確認します。	**show ip route**

次に、スイッチ上のスタティック ルートを設定し、ルーティング テーブルにそのルートが正しく設定されていることを確認する例を示します。

```
Console> (enable) set ip route 172.16.16.0/20 172.20.52.127
Route added.
Console> (enable) show ip route
Fragmentation   Redirect   Unreachable
-------------   --------   -----------
enabled         enabled    enabled

The primary gateway: 172.20.52.121
Destination      Gateway          RouteMask    Flags   Use       Interface
---------------  ---------------  -----------  -----   --------  ---------
172.16.16.0      172.20.52.127    0xfffff000   UG      0           sc0
default          172.20.52.121    0x0          UG      0           sc0
172.20.52.120    172.20.52.124    0xffffffff8  U       1           sc0
default          default          0xff000000   UH      0           sl0
Console> (enable)
```

スイッチ上でのパーマネントおよびスタティック ARP エントリの設定

Catalyst LAN スイッチが Address Resolution Protocol（ARP; アドレス解決プロトコル）要求に応答しない装置と通信できるようにするために、それらの装置の IP アドレスを装置の MAC アドレスにマッピングする、スタティックまたはパーマネント ARP エントリを設定することができます。ARP エントリをスタティックまたはパーマネントのどちらかに設定すると、そのエントリが無効になるのを防ぎます。**set arp static** コマンドを使用してスタティックな ARP エントリを設定した場合、ARP エントリはシステム リセット後に ARP キャッシュから削除されます。**set arp permanent** コマンドを使用してパーマネント ARP エントリを設定した場合、そのエントリはシステム リセット後も保持されます。

大部分のホストはダイナミック レゾリューションをサポートしているので、通常はスタティックまたはパーマネント ARP キャッシュ エントリを指定する必要はありません。ARP 要求に応答しない装置がある場合、ARP キャッシュにスタティックまたはパーマネントに保存される ARP エントリを設定して、それらの装置が到達可能になるようにします。

スタティックまたはパーマネント ARP エントリを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スタティックまたはパーマネント ARP エントリを設定します。	**set arp** [**dynamic** | **permanent** | **static**] {*ip_addr hw_addr*}
ステップ 2	（任意）ARP エージング タイムを指定します。	**set arp agingtime** *seconds*
ステップ 3	ARP の設定を確認します。	**show arp**

次に、スタティック ARP エントリを定義する例を示します。

```
Console> (enable) set arp static 20.1.1.1 00-80-1c-93-80-40
Static ARP entry added as
20.1.1.1 at 00-80-1c-93-80-40 on vlan 1
Console> (enable)
```

次に、パーマネント ARP エントリを定義する例を示します。

```
Console> (enable) set arp permanent 10.1.1.1 00-80-1c-93-80-60
Permanent ARP entry added as
10.1.1.1 at 00-80-1c-93-80-60 on vlan 1
Console> (enable)
```

次に、ARP エージング タイムを設定する例を示します。

```
Console> (enable) set arp agingtime 300
ARP aging time set to 300 seconds.
Console> (enable)
```

次に、ARP キャッシュを表示する例を示します。

```
Console> (enable) show arp
ARP Aging time = 300 sec
+ - Permanent Arp Entries
* - Static Arp Entries
+ 10.1.1.1 at 00-80-1c-93-80-60 on vlan 1
172.20.52.1 at 00-60-5c-86-5b-28 port  8/1 on vlan 1
* 20.1.1.1 at 00-80-1c-93-80-40 port  8/1 on vlan 1
Console> (enable)
```

ARP エントリを消去するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ダイナミック、スタティック、またはパーマネント ARP エントリを消去します。	**clear arp** [**dynamic** | **permanent** | **static**] {*ip_addr hw_addr*}
ステップ 2	ARP の設定を確認します。	**show arp**

次に、すべてのパーマネント ARP エントリを消去し、設定を確認する例を示します。

```
Console> (enable) clear arp permanent
Permanent ARP entries cleared.
Console> (enable)
Console> (enable) show arp
ARP Aging time = 300 sec
+ - Permanent Arp Entries
* - Static Arp Entries
172.20.52.1 at 00-60-5c-86-5b-28 port  8/1 on vlan 1
* 20.1.1.1 at 00-80-1c-93-80-40 port  8/1 on vlan 1
Console> (enable)
```

スイッチ上でのシステム リセットのスケジューリング

ここでは、システム リセットをスケジュールする手順について説明します。

schedule reset コマンドを使用して、特定の時刻にシステムをリセットするようスケジュールすることができます。この機能を利用して、就業時間中にソフトウェアをアップグレードしておき、就業時間後にシステム アップグレードを行うスケジュールにすれば、ユーザに影響を及ぼさずに済みます。

さらに、スイッチで新しい機能を試す場合にも、スケジュール リセットを使用できます。設定上の誤りや装置のネットワーク接続の切断に備えて、スタートアップ コンフィギュレーション機能を設定し、30 分後にリセットが行われるようスケジュールします。その後設定を変更します。接続が切断された場合、システムは 30 分でリセットされ、元の設定に戻ります。

特定の時刻におけるリセットのスケジューリング

リセットが行われる絶対的な日時を指定するには、**reset at** コマンドを使用します。このコマンドでは、月日を表すパラメータは省略可能です。月日を指定しない場合、指定する時刻が現在時刻よりあとなら、リセットは当日行われます。現在時刻より前の時刻にリセットをスケジュールすると、リセットは翌日行われます。

（注） スケジュールできる最長のリセット時間は、24 日後です。

特定の時刻にリセットするようにスケジュールするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	特定の時刻にリセットをスケジュールします。	**reset** [**mindown**] **at** {*hh:mm*} [*mm/dd*] [*reason*]
ステップ 2	リセットのスケジュールを確認します。	**show reset**

（注） mindown（最小ダウンタイム）引数は、システムにスタンバイ スーパバイザ エンジンが装備されている場合に限って有効です。

次に、特定の時刻にリセットをスケジュールする例を示します。

```
Console> (enable) reset at 20:00
Reset scheduled at 20:00:00, Wed Aug 18 1999.
Proceed with scheduled reset? (y/n) [n]? y
Reset scheduled for 20:00:00, Wed Aug 18 1999 (in 0 day 5 hours 40 minutes).
Console> (enable)
```

次に、特定の時刻にリセットをスケジュールするとともに、リセットする理由を入力する例を示します。

```
Console> (enable) reset at 23:00 8/18 Software upgrade to 5.3(1).
Reset scheduled at 23:00:00, Wed Aug 18 1999.
Reset reason: Software upgrade to 5.3(1).
Proceed with scheduled reset? (y/n) [n]? y
Reset scheduled for 23:00:00, Wed Aug 18 1999 (in 0 day 8 hours 39 minutes).
Console> (enable)
```

次に、最小ダウンタイムでリセットをスケジュールする例を示します。

```
Console> (enable) reset mindown at 23:00 8/18 Software upgrade to 5.3(1).
Reset scheduled at 23:00:00, Wed Aug 18 1999.
Reset reason: Software upgrade to 5.3(1).
Proceed with scheduled reset? (y/n) [n]? y
Reset mindown scheduled for 23:00:00, Wed Aug 18 1999 (in 0 day 8 hours 39 minutes).
Console> (enable)
```

時間指定によるリセット スケジューリング

指定した時間内にリセットを行うようにスケジュールするには、**reset in** コマンドを使用します。たとえば、現在のシステム時刻が午前 9 時で、リセットが 1 時間後にスケジュールされている場合、スケジュールされたリセットは午前 10 時に発生します。手動または NTP によりシステム クロックを午前 10 時に進めた場合、リセットは午前 11 時に発生します。クロックをスケジュールされたリセット時刻より先に進めた場合、リセットは現在時刻の 5 分後に発生します。

指定した時間内にリセットするようスケジュールするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	指定した時間内にリセットをスケジュールします。	**reset** [**mindown**] **in** [*hh*] {*mm*} [*reason*]
ステップ 2	リセットのスケジュールを確認します。	**show reset**

（注） mindown（最小ダウンタイム）引数は、システムにスタンバイ スーパバイザ エンジンが装備されている場合に限って有効です。

次に、指定した時間にリセットをスケジュールする例を示します。

```
Console> (enable) reset in 5:20 Configuration update
Reset scheduled in 5 hours 20 minutes.
Reset reason: Configuration update
Proceed with scheduled reset? (y/n) [n]? y
Reset scheduled for 19:56:01, Wed Aug 18 1999 (in 5 hours 20 minutes).
Reset reason: Configuration update
Console> (enable)
```

電源の管理

ここでは、Catalyst 6500 シリーズ スイッチでの電源の管理について説明します。内容は次のとおりです。

（注） 冗長電源装置のあるシステムでは、両方の電源装置が同じワット数である必要があります。Catalyst 6500 シリーズ スイッチでは、同じシャーシ内に AC 入力および DC 入力電源装置を混在させることができます。各シャーシについてサポートされている電源構成の詳細については、『*Catalyst 6500 Series Switch Installation Guide*』を参照してください。

Catalyst 6500 シリーズ モジュールには、さまざまな電源要件があります。電源装置のワット数によって、一部のスイッチ構成には 1 台の電源装置では足りない容量の電力が必要になります。電源管理機能によって、搭載されたすべてのモジュールに 2 台の電源装置で電力を供給できますが、この構成では冗長構成はサポートされません。ここでは、冗長および非冗長の電源構成について説明します。

電源の冗長構成のイネーブル化またはディセーブル化

冗長構成をイネーブルまたはディセーブルにするには、**set power redundancy enable** | **disable** コマンドを使用します（デフォルトでは冗長構成がイネーブルに設定されています）。冗長構成がイネーブルで、ワット数の等しい 2 台の電源装置を搭載している場合、2 台の電源装置から供給される電力の総量は、どの時点でも 1 台分の容量を超えることはありません。1 台の電源装置が故障した場合、もう 1 台がシステムの負荷全体を引き継ぎます。ワット数の等しい 2 台の電源装置を搭載して電源をオンにすると、それぞれの電源装置がシステムに必要な電力の約半分を同時に供給します。負荷分散と冗長構成が自動的にイネーブルになるので、ソフトウェアによる設定は必要ありません。

冗長構成をイネーブルにして、ワット数の異なる 2 台の電源装置でシステムに電力を供給すると、両方の電源がオンラインになりますが、ワット数の小さい方の電源装置がディセーブルになることを示す Syslog メッセージが表示されます。アクティブな電源装置が故障した場合には、ディセーブルになっていたワット数の小さい電源装置がオンラインになり、必要に応じてワット数の低下に対応するためにモジュールの電源が切断されます。

非冗長構成では、システムで使用できる電力量は、2 台の電源装置で供給できる電力の総和です。システムは総電力量の許すかぎり、何個のモジュールにも電力を供給できます。ただし、1 台の電源装置が故障し、それまでに電力が供給されていたすべてのモジュールに供給できるだけの電力がなくなった場合には、システムは一部のモジュールの電源を切断します。それらのモジュールについては、**show module** コマンドの Status フィールドに *power-deny* とマークされます。

電源の構成は、いつでも冗長または非冗長に変更できます。冗長構成から非冗長構成に切り替えると、両方の電源装置がイネーブルになります（ワット数が小さいためにディセーブルになっていた電源装置もイネーブルになります）。非冗長構成から冗長構成に切り替えると、最初は両方の電源装置がイネーブルになります。2 台ともワット数が同じであれば、そのままイネーブルの状態が続きます。ワット数が異なる場合には、Syslog メッセージが表示され、ワット数が小さい方の電源装置がディセーブルになります。

表 21-1 で、電源の構成を変更した場合のシステムへの影響を説明します。

表 21-1　電源構成の変更時の影響

構成の変更内容	影響
冗長構成から非冗長構成へ	• システム ログおよび Syslog メッセージが表示されます。 • システムの電力は増え、両方の電源装置で供給できる電力の総和になります。 • 十分な電力がある場合、**show module** コマンドの Status フィールドに *power-deny* とマークされていたモジュールの電源が入ります。
非冗長構成から冗長構成へ	• システム ログおよび Syslog メッセージが表示されます。 • システムの電力は、ワット数の大きい方の電源装置の電力供給可能量です。 • それまでに電力が供給されていたすべてのモジュールに供給できる十分な電力がない場合は、一部のモジュールの電源が切断され、そのモジュールについては **show module** コマンドの Status フィールドに *power-deny* とマークされます。
冗長構成がイネーブルで、同じワット数の電源装置を挿入した場合	• システム ログおよび Syslog メッセージが表示されます。 • システムの電力は、1 台の電源装置の電力供給可能量に等しくなります。 • 供給できる電力量には変化がないので、モジュールのステータスは変化しません。
冗長構成がディセーブルで、同じワット数の電源装置を挿入した場合	• システム ログおよび Syslog メッセージが表示されます。 • システムの電力は、両方の電源装置で供給できる電力の総和になります。 • 十分な電力がある場合、**show module** コマンドの Status フィールドに *power-deny* とマークされていたモジュールの電源が入ります。
冗長構成がイネーブルで、ワット数の大きい電源装置を挿入した場合	• システム ログおよび Syslog メッセージが表示されます。 • システムはワット数の小さい電源装置をディセーブルにします。ワット数の大きい電源装置がシステムに電力を供給します。
冗長構成がイネーブルで、ワット数の小さい電源装置を挿入した場合	• システム ログおよび Syslog メッセージが表示されます。 • システムはワット数の小さい電源装置をディセーブルにします。ワット数の大きい電源装置がシステムに電力を供給します。
冗長構成がディセーブルで、ワット数が大きいか、または小さい電源装置を挿入した場合	• システム ログおよび Syslog メッセージが表示されます。 • システムの電力は増え、両方の電源装置で供給できる電力の総和になります。 • 十分な電力がある場合、**show module** コマンドの Status フィールドに *power-deny* とマークされていたモジュールの電源が入ります。

表 21-1　電源構成の変更時の影響（続き）

構成の変更内容	影響
冗長構成がイネーブルで、電源装置を取り外した場合	• システム ログおよび Syslog メッセージが表示されます。 • 電源装置のワット数が同じであれば、供給できる電力量には変化がないので、モジュールのステータスは変化しません。 電源装置のワット数が異なっており、ワット数の小さい方の電源装置を取り外した場合には、モジュールのステータスは変化しません。 電源装置のワット数が異なっており、ワット数の大きい方の電源装置を取り外した場合には、それまでに電力が供給されていたすべてのモジュールに供給できる十分な電力がなければ、一部のモジュールの電源が切断され、そのモジュールについては **show module** コマンドの Status フィールドに *power-deny* とマークされます。
冗長構成がディセーブルで、電源装置を取り外した場合	• システム ログおよび Syslog メッセージが表示されます。 • システムの電力は減り、1 台の電源装置の容量になります。 • それまでに電力が供給されていたすべてのモジュールに供給できる十分な電力がない場合は、一部のモジュールの電源が切断され、そのモジュールについては **show module** コマンドの Status フィールドに *power-deny* とマークされます。
ワット数の異なる電源装置を搭載し、冗長構成がイネーブルで、システムを起動した場合	• システム ログおよび Syslog メッセージが表示されます。 • ワット数の小さい電源装置がディセーブルになります。
ワット数の等しい、または異なる電源装置を搭載し、冗長構成がディセーブルで、システムを起動した場合	• システム ログおよび Syslog メッセージが表示されます。 • システムの電力は、両方の電源装置で供給できる電力の総和になります。 • システムは総電力量の許すかぎり、何個のモジュールにも電力を供給できます。

CLI によるモジュールの電源投入または切断

CLI から、正常に稼働しているモジュールの電源を切断するには、**set module power down** *mod* コマンドを使用します。そのモジュールについては、**show module** コマンドの Status フィールドに *power-down* とマークされます。電源を切断したモジュールの電源を再び入れるために、システムに電力の余裕が十分にあるかどうかを確認するには、**set module power up** *mod* コマンドを使用します。十分な電力がない場合には、モジュールのステータスは *power-down* から *power-deny* に変化します。

環境モニタ

シャーシ コンポーネントの環境をモニタすることにより、コンポーネント故障の兆候を早期に発見し、安全で信頼性の高いシステム稼働を実現するとともに、ネットワークの中断を防止することができます。ここでは、これらの重要なシステム コンポーネントをモニタし、システム内でハードウェア関連の問題点を特定し、速やかに改善するための方法を説明します。

ここでは、環境モニタについて説明します。

CLI コマンドによる環境モニタ

診断テストで報告されたエラーを表示するには、**show test** [*mod*] コマンドを使用します。モジュール番号を指定しない場合は、システム全般およびスロット 1 のモジュールに関するテスト統計が表示されます。エラーがなければ、Line Card Status フィールドに PASS と表示されます。

システム ステータス情報を表示するには、**show environment** [**temperature** | **all** | **power**] コマンドを使用します。各キーワードの意味は次のとおりです。

- **temperature** ― （任意）温度の情報を表示します。
- **all** ― （任意）環境ステータス情報（電源、ファン ステータス、温度情報など）およびシステムで使用できる電力量を表示します。
- **power** ― （任意）電力に関する環境情報を表示します。

LED 表示

アラームの種類には、メジャーおよびマイナーの 2 種類があります。メジャー アラームは、システムのシャットダウンを引き起こす可能性のある、重大な問題を表します。マイナー アラームは、もし改善措置を行わなければ、重大な問題に発展する可能性のある問題を通知するメッセージです。

過熱状態が発生し、システムが（メジャーまたはマイナー）アラームを表示した場合、5 分間そのアラームはキャンセルされず、（モジュールのリセットまたはシャットダウンなどの）措置も行われません。この間に温度がアラーム スレッシュホールドより 5°C（41°F）下がると、アラームはキャンセルされます。

表 21-2 に、スーパバイザ エンジンおよびスイッチング モジュールに関する環境インジケータを示します。

（注） LED インジケータの詳細については、『*Catalyst 6500 Series Switch Module Installation Guide*』を参照してください。

表 21-2　スーパバイザ エンジンおよびスイッチング モジュールの環境モニタ

コンポーネント	アラームの種類	LED インジケータ	アクション
スーパバイザ エンジンの温度センサがメジャー スレッシュホールドを超過[1]	メジャー	STATUS[2] LED レッド[3]	Syslog メッセージおよび SNMP トラップが生成されます。 冗長構成の場合、システムは冗長スーパバイザ エンジンに切り替え、アクティブなスーパバイザ エンジンはシャットダウンします。 冗長構成ではなく、かつ過熱状態が改善されない場合、システムは 5 分後にシャットダウンします。
スーパバイザ エンジンの温度センサが、マイナー スレッシュホールドを超過	マイナー	STATUS LED オレンジ	Syslog メッセージおよび SNMP トラップが生成されます。 状況をモニタします。
冗長スーパバイザ エンジンの温度センサがメジャーまたはマイナー スレッシュホールドを超過	メジャー	STATUS LED レッド	Syslog メッセージおよび SNMP トラップが生成されます。 メジャー アラームおよび過熱状態が改善されない場合、システムは 5 分後にシャットダウンします。
	マイナー	STATUS LED オレンジ	マイナー アラームの場合は、状況をモニタします。
スイッチング モジュールの温度センサがメジャー　スレッシュホールドを超過	メジャー	STATUS LED レッド	Syslog メッセージおよび SNMP トラップが生成されます。 モジュールの電源を切断します。[4]
スイッチング モジュールの温度センサがマイナー　スレッシュホールドを超過	マイナー	STATUS LED オレンジ	Syslog メッセージおよび SNMP トラップが生成されます。 状況をモニタします。

1. 温度センサは、主要なスーパバイザ エンジン コンポーネント（ドータカードも含む）をモニタします。
2. STATUS LED は、スーパバイザ エンジンの前面パネルおよびすべてのモジュールの前面パネルにあります。
3. STATUS LED は、スーパバイザ エンジンが故障するとレッドになります。冗長構成のスーパバイザ エンジンがない場合は、SYSTEM LED もレッドになります。
4. 手順については、「電源の管理」（p.21-14）を参照してください。

テクニカル サポート用のシステム ステータス情報の表示

ここでは、テクニカル サポート用のシステム ステータス情報を表示する手順について説明します。

システム ステータス レポートの生成

1 つのコマンドを使用して、スイッチのステータス情報を含むレポートを生成することができます。生成された情報は、Cisco Technical Assistance Center（TAC）に問題を報告するときに役立ちます。このコマンドは、いくつかの **show system status** コマンドを組み合わせたものです。このコマンドの出力を TFTP サーバにアップロードして、TAC に送信することができます。

キーワードを使用して、特定のモジュール、VLAN（仮想 LAN）、ポートなど、出力する情報の範囲を限定できます。キーワードを指定しないと、システム全体のレポートが生成されます。

レポートを生成して TFTP サーバにアップロードするには、イネーブル モードで次の作業を行います。

作業	コマンド
TAC に送信するためのシステム ステータス レポートを生成します。	**write tech-support** {*host*} {*filename*} [**module** *mod*] [**port** *mod*/*port*] [**vlan** *vlan*] [**memory**] [**config**]

次に、指定したファイル名で、ホスト 172.20.32.10 にレポートを送信する例を示します。キーワードが指定されていないので、レポートにはスイッチ全体のステータス情報が含まれます。

```
Console> (enable) write tech-support 172.20.32.10 tech.txt
Upload tech-report to tech.txt on 172.20.32.10 (y/n) [n]? y
/
Finished network upload.  (67784 bytes)
Console> (enable)
```

システム ダンプ ファイルの使用

コア ダンプおよびスタック ダンプにより、スイッチのシステム ステータス情報を含んだレポートが生成されます。コア ダンプまたはスタック ダンプによってキャプチャされたイメージを、解析のために Cisco TAC に送ります。

コア ダンプのイネーブル化およびディセーブル化

ソフトウェア エラーによってシステムに障害が発生したときに、コア ダンプはイメージの包括的なレポートを作成します。このレポートには、テキスト、コード、スタック セグメントなどシステム メモリの内容が含まれています。コア イメージはシスコ製コア ファイル形式で作成され、ファイル システムに保存されます。TAC は、コア ダンプ ファイルを調べて、打ち切られたプロセスのエラー条件を解析します。

コア ダンプをイネーブルまたはディセーブルにするには、**set system core-dump** コマンドを使用します。スイッチに冗長スーパバイザ エンジンが搭載されている場合は、コア ダンプが発生する前にスタンバイ スーパバイザ エンジンが自動的に引き継ぎます。これまでアクティブだったスーパバイザ エンジンは、コア ダンプ終了後にリセットします。

コア ダンプをイネーブルまたはディセーブルに設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
コア ダンプをイネーブルまたはディセーブルに設定します。	**set system core-dump** {**enable** | **disable**}

次に、コア ダンプをイネーブルにする例を示します。

```
Console> (enable) set system core-dump enable
(1) In the event of a system crash, this feature will
     cause a core file to be written out.
(2) Core file generation may take up to 20 minutes.
(3) Selected core file is slot0:crash.hz
(4) Please make sure the above device has been installed,
    and ready to use
Core-dump enabled
Console> (enable)
```

次に、コア ダンプをディセーブルにする例を示します。

```
Console> (enable) set system core-dump disable
Core-dump disabled
Console> (enable)
```

ファイル システムのサイズは、メモリ カードのサイズによって異なります。エラー プロセスにより、システム DRAM のサイズに比例したコア イメージが生成されます。コア ダンプ ファイルを保存できるだけのメモリを確保するようにしてください。

コア イメージ ファイル名の指定

コア イメージ ファイル名を指定するには、**set system core-file** コマンドを使用します。デフォルトのファイル名は、[slot0:crash.hz] です。このコマンドは、入力されたデバイス名の妥当性を自動的に確認します。

コア イメージ ファイル名を指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
コア イメージ ファイル名を指定します。	**set system core-file** {*device:filename*}

次に、コア イメージ ファイル名を指定する例を示します。

```
Console> (enable) set system core-file slot0:core.hz
System core-file set.
Console> (enable)
```

スタック ダンプの表示

スタック ダンプが生成するイメージは、システムの障害を引き起こした特定のプロセスに関するものだけです。このイメージ スタックはコンソール上に表示され、ログ領域にも保存されます。スタック ダンプは自動で、システムの再起動後に **show log** コマンドを実行すると有効になります。

ログ情報を表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
スタック ダンプを表示します。	**show log**

次に、**show log** コマンドの実行後に表示されるイメージ スタックの例を示します。

```
Breakpoint Exception occurred.
Software version =  6.2(0.83)
Process ID #52, Name
= Console
             EPC: 807523F4
    Stack content:
    sp+00: 00000000 80A75698 00000005 00000005
    sp+10: BE000A00 00000000 83F84150 801194B8
    sp+20: 80A75698 80A74BC8 80C8DBDC 000006E8
    sp+30: 8006AF30 8006AE98 82040664 00000630
    sp+40: 801AC744 801AC734 80A32488 80A32484
    sp+50: 80A3249C 00000000 00000002 000009E4
    sp+60: 8204067B 82040670 8011812C 81CAFC98
    sp+70: 8011814C 82040670 8011812C 81CAFC98
    sp+80: 00000002 000009E4 80110160 80110088
    sp+90: 82040670 80A71EB4 81F1E9F8 00000004
    sp+A0: 00000000 81F25EAC 81FF5750 00000000
    sp+B0: 00000000 00000000 81F1E314 800840BC
    sp+C0: 0000000B 80084EB0 00000001 8073A358
    sp+D0: 00000003 0000000D 00000000 0000000A
    sp+E0: 00000020 00000000 800831B4 0000001A
    sp+F0: 00000000 00000000 00000000 000D84F0
    Register content:
      Status: 3401FC23    Cause: 00000024
AT: 81640000
          V0: 00000007       V1: 00000007
          A0: 00000000       A1: 80A756A6
          A2: 00000011       A3: BE000BD0
          T0: BFFFFFFE       T1: 80000000
          T2: 00000000       T3: 00000001
          T4: 00000000       T5: 00000007
          T6: 00000000       T7: 00000000
          S0: 00000001       S1: 00000032
          S2: 81F1E9F8       S3: 80A74BC8
          S4: 80C8DBDC       S5: 000006E8
          S6: 00000000       S7: 00000000
          T8: F0D09E3A       T9: 82940828
          K0: 3041C001       K1: 80C73038
          GP: 811F39C0       SP: 83F84010
          S8: 83F84010       RA: 807523F4
        HIGH: 00000001      LOW: D5555559
    BADVADDR: 7DFF7FFF  ERR EPC: 58982466
GDB: Breakpoint Exception
GDB: The system has trapped into the debugger.
GDB: It will hang until examined with gdb.
```

システム クラッシュ情報ファイルの使用

クラッシュ情報ファイルには、エラーによる再ロード時に取り込まれる拡張システム情報が格納されます。クラッシュ ダンプ ファイルと同様に、クラッシュ情報ファイルはファイル システム内に保存されます。コア ダンプ情報に加えて、クラッシュ情報ファイル内の情報を確認する必要があります。クラッシュ情報ファイルおよびコア ダンプ ファイルを検査することで、Cisco TAC ではより良いエラーの解析が可能になります。

クラッシュ情報ファイルのイネーブル化とディセーブル化

エラーによるシステム リロードの発生後のクラッシュ情報ファイル書き込みをイネーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
クラッシュ情報ファイルの作成をイネーブルまたはディセーブルにします。 **（注）** この機能は、デフォルトではディセーブルです。	**set system crashinfo enable | disable**

次に、クラッシュ情報ファイルの書き込みをシステムでイネーブルにする例を示します。

```
Console> (enable) set system crashinfo enable
Crashinfo enabled
```

クラッシュ情報ファイル名の指定

クラッシュ情報ファイル名を指定するには、**set system crash-info-file** コマンドを使用します。このコマンドは、入力されたデバイス名の妥当性を自動的に確認します。

クラッシュ情報ファイル名を指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
クラッシュ情報ファイル名を指定します。デフォルトのファイル名は **crashinfo** です。	**set system crashinfo-file** {*device:filename*}

次に、クラッシュ情報ファイル名を指定する例を示します。

```
Console> (enable) set system crashinfo-file slot0:crashinfo
System crashinfo-file set.
Console> (enable)
```

システム情報の TFTP または RCP サーバへのロギング

システムを設定して、最大 15 個の **show** コマンドを実行し、指定したサーバ上のファイルにその出力をロギングすることができます。その出力情報は、デバッグやトラブルシューティングに使用できます。

ここでは、スイッチ上でシステム情報ロギングを設定する手順について説明します。

システム情報ロギングのイネーブル化

デフォルトでは、システム情報ロギングはディセーブルです。

スイッチ上でシステム情報ロギングをイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	システム情報ロギングをイネーブルにします。	**set system info-log enable**
ステップ 2	システム情報ロギングがイネーブルであることを確認します。	**show system info-log**

次に、システム情報ロギングをイネーブルにし、イネーブルになったことを確認する例を示します。

```
Console> (enable) set system info-log enable
Successfully enabled system information logging.
Console> (enable) show system info-log
System Logging  Host            File                                Interval
--------------  --------------  ----------------------------------  --------
Enabled         -               tftp:sysinfo                        1440
Index        System Command
-----        ------------------------------------------------------------
Console> (enable)
```

システム情報ロギングを行う show コマンドの指定

最大 15 個の **show** コマンドについて、その出力が定期的に指定したサーバ上のファイルにロギングされるように指定できます。**show** コマンドの両側にはデリミタ文字が必要です。一度に入力できる **show** コマンドは 1 つだけです。

position 引数を入力すれば、**show** コマンドの実行順序を指定できます。有効な値は 1 ～ 15 です。*position* 引数はシステム情報ロギング インデックス内の **show** コマンドの番号です。

出力をファイルにロギングする **show** コマンドを指定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	出力をロギングする **show** コマンドを指定します。	**set system info-log command** {*command_string*} [*position*]
ステップ 2	システム情報ロギングがイネーブルであることを確認します。	**show system info-log**

次に、**show** コマンドを指定し、そのコマンドがシステム情報ロギングに含まれたことを確認する例を示します。

```
Console> (enable) set system info-log command $show version$
System command was successfully added to the list.
Console> (enable) set system info-log command $show module$
System command was successfully added to the list.
Console> (enable) set system info-log command $show environment$
System command was successfully added to the list.
Console> (enable) set system info-log command $show config$
System command was successfully added to the list.
Console> (enable) show system info-log
System Logging  Host            File                                Interval
--------------  --------------  ----------------------------------  --------
Enabled         -               tftp:sysinfo                        1440
Index        System Command
-----        ------------------------------------------------------------
    1        show version
    2        show module
    3        show environment
    4        show config
Console> (enable)
```

システム情報ロギングの実行頻度の指定

システム情報ロギングの実行間隔を時間指定できます。この時間間隔は分単位で指定します。有効な値は 1 ～ 35000 分（25 日）です。デフォルトでは、ロギング実行間隔は 1440 分（1 日）です。

ロギングの時間間隔を指定して確認するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	システム情報ロギングを実行する時間間隔を指定します。	**set system info-log interval** *mins*
ステップ 2	時間間隔を確認します。	**show system info-log**

次に、ロギングの時間間隔を指定して確認する例を示します。

```
Console> (enable) set system info-log interval 4320
Successfully set system information logging interval to 4320 minutes.
Console> (enable) show system info-log
System Logging  Host            File                                Interval
--------------  --------------  ----------------------------------  -------
Enabled         -               tftp:sysinfo                        4320
Index        System Command
-----        ------------------------------------------------------------
    1        show config
    2        show version
    3        show module
    4        show environment
Console> (enable)
```

システム情報ロギング用のファイル名およびサーバの指定

システム情報ロギング用にファイル名およびサーバを指定できます。ファイルへのパスを指定しなければ、TFTP 用のデフォルト ディレクトリは tftpboot、RCP 用のデフォルト ディレクトリはユーザのホーム ディレクトリとなります。

システム情報ロギング用のファイル名およびサーバを指定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	システム情報ロギング用のファイル名およびサーバを指定します。	**set system info-log** {**tftp** | **rcp** *username*} *host filename*
ステップ 2	時間間隔を確認します。	**show system info-log**

次に、ファイル名およびサーバを指定し、その設定を確認する例を示します。

```
Console> (enable) set system info-log rcp hcavende 10.5.2.10 sysinfo
Successfully set the system information logging file to rcp:sysinfo
Console> (enable) show system info-log
System Logging  Host            File                                Interval
--------------  --------------  ----------------------------------  --------
Enabled         10.5.2.10       rcp:sysinfo                         4320
Index        System Command
-----        ------------------------------------------------------------
    1        show config
    2        show version
    3        show module
    4        show environment
Console> (enable)
```

システム情報ロギングからの show コマンドの消去

すべての **show** コマンド、または特定の **show** コマンドをシステム情報ロギングから消去し、消去されたことを確認するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	システム情報ロギングから **show** コマンドを消去します。	**clear system info-log command** {**all** | *index*}
ステップ 2	**show** コマンドの消去を確認します。	**show system info-log**

次に、**show** コマンド番号 1 を、システム情報ロギング インデックスから消去する例を示します。

```
Console> (enable) clear system info-log command 2
Successfully cleared the configured command.
Console> (enable) show system info-log
System Logging  Host            File                                Interval
--------------  --------------  ----------------------------------  --------
Enabled         10.5.2.10       rcp:sysinfo                         4320
Index        System Command
-----        ------------------------------------------------------------
    1        show config
    2        show module
    3        show environment
Console> (enable)
```

システム情報ロギング設定の消去

システム情報ロギング設定を消去し、デフォルト設定に戻すには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	システム情報ロギング設定を消去します。	**clear config sysinfo-log**
ステップ 2	設定が消去されたことを確認します。	**show system info-log**

次に、システム情報ロギング設定を消去し、デフォルトに戻す例を示します。

```
Console> (enable) clear config sysinfo-log
Successfully cleared the system information logging configuration.
Console> (enable) show system info-log
System Logging  Host             File                                Interval
--------------  ---------------  ----------------------------------  --------
Disabled        -                tftp:sysinfo                        1440
Index        System Command
-----        ------------------------------------------------------------
Console> (enable)
```

システム情報ロギングのディセーブル化

システム情報ロギングをディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	システム情報ロギングをディセーブルにします。	**set system info-log disable**
ステップ 2	システム情報ロギングがディセーブルであることを確認します。	**show system info-log**

次に、システム情報ロギングをディセーブルにし、ディセーブルになったことを確認する例を示します。

```
Console> (enable) set system info-log disable
Successfully disabled system information logging.
Console> (enable) show system info-log
System Logging  Host             File                                Interval
--------------  ---------------  ----------------------------------  --------
Disabled        -                tftp:sysinfo                        1440
Index        System Command
-----        ------------------------------------------------------------
Console> (enable)
```

TCL スクリプティング

Tool Command Language（TCL）はプログラミング可能な、テキスト ベースの簡易言語であり、コマンド プロシージャを記述することにより組み込みコマンド群の機能を拡張できます。これは、テキスト エディタ、デバッガ、イラストレータやシェルなどのインタラクティブ プログラムとともに使用します。Catalyst 6500 シリーズ スイッチ ソフトウェアは、TCL バージョン 7.4 をサポートしています。

TCL はオープン ソースコードです。TCL コマンド、および TCL の使用法、ライセンス、プログラミングの詳細については、次の URL を参照してください。

http://www.tcl.tk

表 21-3 に、サポートされている TCL コマンドを示します。*t* プレフィクス付きのコマンド（**tformat**、**trename**、**tset**、**tswitch**）は、標準 TCL コマンドからカスタマイズされており、Catalyst 6500 シリーズ スイッチ ソフトウェアと競合しないようになっています。このソフトウェアには、特に次の 2 つのコマンドが追加されています。

- **auto answer** {**on** | **off**}

  on に設定すると、スイッチが yes/no 形式の応答を要求する場合、TCL シェルは *yes* と応答します。デフォルトの設定は **off** です。

- **echo** {**on** | **off**}

  off に設定した場合、スイッチ コマンドの出力は画面に表示されません。デフォルトの設定は **on** です。

表 21-3　TCL コマンド

append	array	auto answer	break
case	catch	concat	continue
echo	error	eval	expr
for	foreach	global	if
incr	info	join	lappend
lindex	linsert	list	llength
lrange	lreplace	lsearch	lsort
proc	puts	regexp	regsub
return	scan	source	split
string	subst	tformat	trename
tset	tswitch	unset	uplevel
upvar	while		

TCL コマンドの入力

TCL コマンドの入力には、TCL シェルを使用する必要があります。TCL シェルをオープンするには、イネーブル モードで次の作業を行います。

作業	コマンド
TCL シェルをオープンします。	**tclsh**

次に、TCL シェルをオープンする例を示します。

```
Console> (enable) tclsh
Console> (tclsh)(enable)
```

TCL シェルをクローズするには、イネーブル モードで次の作業を行います。

作業	コマンド
TCL シェルをクローズします。	**tclquit**

次に、TCL シェルをクローズする例を示します。

```
Console> (enable) tclquit
Console> (enable)
```

CHAPTER 22

冗長機能の設定

この章では、Catalyst 6500 シリーズ スイッチ上で冗長スーパバイザ エンジンを設定する手順、および Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）の冗長機能を設定する手順について説明します。

この章で説明する内容は、次のとおりです。

（注） Cisco Nonstop Forwarding（NSF）/Stateful Switchover（SSO）を使用した MSFC 冗長機能の設定については、第 23 章「NSF/SSO MSFC 冗長機能の設定」を参照してください。

注意 単一シャーシに搭載のデュアル MSFC は、冗長モードのみでの使用を目的に設計されており、同一の設定でなければなりません。詳細については、「MSFC 冗長機能」（p.22-22）を参照してください。

MSFC の設定が異なる構成はサポートしていません。

（注） 特に明記されていないかぎり、この章で説明する情報および手順は、Policy Feature Card 3B/3BXL（PFC3B/PFC3BXL; ポリシー フィーチャ カード 3B/3BXL）を搭載した Supervisor Engine 32、PFC3A/PFC3B/PFC3BXL を搭載した Supervisor Engine 720、PFC2 を搭載した Supervisor Engine 2、および PFC を搭載した Supervisor Engine 1 に適用されます。

（注） *MSFC* という用語は、このマニュアルを通じて特に明記されていないかぎり、MSFC、MSFC2、MSFC2A、および MSFC3 を指します。

Catalyst 6500 シリーズ冗長スーパバイザ エンジンのインストレーションの詳細については、『*Catalyst 6500 Series Switch Module Installation Guide*』を参照してください。この章で使用しているコマンドの構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

スーパバイザ エンジンの冗長機能

(注) 冗長スーパバイザ エンジンには、同じモデルのフィーチャ カードと同タイプのものを使用する必要があります。WS-X6K-SUP1-2GE および WS-X6K-SUP1A-2GE（両方とも PFC を非搭載）は互換性があり、冗長構成が可能です。PFC が搭載されたスーパバイザ エンジンの場合、冗長構成にするには PFC が同一でなければなりません（2 つの PFC、2 つの PFC2、2 つの PFC3A、または 2 つの PFC3BXL）。

2 つのスーパバイザ エンジンを搭載している場合、先に起動したスーパバイザ エンジンがアクティブ モジュールになり、2 番めのスーパバイザ エンジンはスタンバイ モードになります。SNMP（簡易ネットワーク管理プロトコル）、CLI（コマンドライン インターフェイス）コンソール、Telnet、Spanning-Tree Protocol（STP; スパニングツリー プロトコル）、Cisco Discovery Protocol（CDP）、VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）などの管理機能およびネットワーク管理機能はすべて、アクティブ スーパバイザ エンジン上で処理されます。

スタンバイ スーパバイザ エンジンのコンソール ポートは非アクティブで、モジュール ステータスは [standby] で示されます。ただし、アップリンク ポートのステータス表示は通常どおりです。

Supervisor Engine 1 および Supervisor Engine 2 の場合、冗長スーパバイザ エンジンはシャーシのスロット 1 および 2 に搭載する必要があります。Supervisor Engine 720 および Supervisor Engine 32 のスロット要件は、次のとおりです。3 スロット シャーシの場合は、Supervisor Engine 720 および Supervisor Engine 32 をスロット 1 または 2 に搭載します。6 スロットまたは 9 スロット シャーシの場合は、Supervisor Engine 720 および Supervisor Engine 32 をスロット 5 または 6 に搭載します。13 スロット シャーシの場合は、Supervisor Engine 720 および Supervisor Engine 32 をスロット 7 または 8 に搭載します。冗長スーパバイザ エンジンは両方のスロットに搭載する必要があります。

冗長スーパバイザ エンジンはホットスワップ対応です。システムは冗長スーパバイザ エンジンに切り替えたあとも、同じ設定で稼働を続けます。

(注) 各スーパバイザ エンジンを個別に起動できるようにするため、コンフィギュレーション レジスタは、スーパバイザ エンジン間で同期化されていません。

(注) アクティブ スーパバイザ エンジンからスタンバイ スーパバイザ エンジンへの切り替えに要する時間に、スパニングツリーのコンバージェンス タイムは含まれていません。

スイッチの起動時には、両方のスーパバイザ エンジンで初期モジュール レベルの診断が実行されます。両方のスーパバイザ エンジンがこのレベルの診断をパスした場合、2 つのスーパバイザ エンジンはバックプレーンを介して通信し、スイッチングバス診断時に協調するようになります。スロット 1 に搭載されたスーパバイザ エンジンがアクティブになり、スロット 2 のスーパバイザ エンジンがスタンバイ モードになります。2 つのスーパバイザ エンジンのソフトウェア バージョンが異なる場合、または NVRAM（不揮発性 RAM）設定が異なっている場合には、アクティブ スーパバイザ エンジンのソフトウェア イメージおよび設定がスタンバイ スーパバイザ エンジンに自動的にダウンロードされます。

(注)　*スロット 1* および *スロット 2* は、冗長スーパバイザ エンジンを指します。上記のように、Supervisor Engine 720 および Supervisor Engine 32 ではスロット要件が異なります。

アクティブ スーパバイザ エンジンのバックグラウンド診断によって重大な問題が検出された場合、または例外が発生した場合には、アクティブ スーパバイザ エンジンがリセットされます。スタンバイ スーパバイザ エンジンは、アクティブ スーパバイザ エンジンが稼働しなくなったことを検出し、アクティブになります。スタンバイ スーパバイザ エンジンは、アクティブ スーパバイザ エンジンが正常に機能していない場合にそれを検出し、必要に応じてアクティブ スーパバイザを強制的にリセットすることもできます。リセットされたスーパバイザ エンジンは、復旧するとスタンバイ モードになります。

2 番めのスーパバイザ エンジンをオンラインの状態で挿入すると、初期モジュール レベルの診断が完了した時点で、2 番めのモジュールはアクティブ スーパバイザ エンジンと通信します。アクティブ スーパバイザ エンジンがすでにバックプレーン上のトラフィックをスイッチングしているので、2 番めのスーパバイザ エンジンについてはスイッチングバス診断は実行されません。診断を実行すると通常のトラフィックが中断される可能性があるためです。2 番めのスーパバイザエンジンは、ただちにスタンバイ モードになります。この時点で、アクティブ スーパバイザ エンジンのソフトウェア イメージおよび設定が、必要に応じてスタンバイ スーパバイザ エンジンにダウンロードされます。

スーパバイザ エンジンは、*ブート イメージ*と *ランタイム イメージ*という 2 つのフラッシュ イメージを使用します。ブート イメージのファイル名は、BOOT 環境変数で指定し、NVRAM に保存します。ランタイム イメージは、ROM モニタがスーパバイザ エンジンを起動するために使用するブート イメージです。システム起動後は、ランタイム イメージは DRAM に常駐します。

冗長スーパバイザ エンジンを搭載したスイッチの電源を入れるか、リセットすると、スタンバイ スーパバイザ エンジン上のランタイム イメージとブート イメージがアクティブ スーパバイザ エンジン上のイメージと同じになるように同期化が行われます。

スーパバイザ エンジンのランタイム イメージとブート イメージは、異なる場合があります。ブート イメージとランタイム イメージが同じであるときに、BOOT 環境変数を変更したり、システム起動に使用されたフラッシュ デバイス上の現在のブート イメージを上書きしたり破棄したりすると、ランタイム イメージとブート イメージは異なったものになります。ブートイメージを再設定すると、アクティブ スーパバイザ エンジンは、現在のブート イメージをスタンバイ スーパバイザ エンジンと同期化させます。

ブート イメージは、フラッシュ ファイル システムに直接読み込まれます。フラッシュ メモリ装置に保存されたファイルに対しては、（**copy**、**delete**、**undelete** などの）操作を実行できます。また、アクティブ スーパバイザ エンジンのブート イメージを、スタンバイ スーパバイザ エンジンのブートフラッシュに保存できます。フラッシュ ファイル システムの詳しい使用手順は、第 25 章「フラッシュ ファイル システムの使用」を参照してください。

Supervisor Engine 1 および Supervisor Engine 2 には、オンボード フラッシュ メモリのほかにフラッシュ PC カード（PCMCIA［パーソナル コンピュータ メモリ カード国際協会 ］）スロット（slot0）があります。このスロットにフラッシュ PC カードを挿入し、そこに追加のブート イメージを保存することができます。スロットのキーワードは、**slot0:**（リニア フラッシュ デバイスの場合）、および **disk0:**（ATA フラッシュ デバイスの場合）です。

(注)　このマニュアルでは、「*PCMCIA カード*」という用語の代わりに「*フラッシュ PC カード*」を使用しています。

Supervisor Engine 720 には、コンパクトフラッシュ Type II スロットが 2 つあります。コンパクトフラッシュ Type II スロットは、コンパクトフラッシュ Type II フラッシュ PC カードをサポートしています。アクティブな Supervisor Engine 720 上のスロットのキーワードは、**disk0:** および **disk1:** です。冗長 Supervisor Engine 720 上のスロットのキーワードは、**slavedisk0:** および **slavedisk1:** です。Supervisor Engine 32 には、コンパクトフラッシュ Type II スロットが 1 つあります。コンパクトフラッシュ Type II スロットは、コンパクトフラッシュ Type II フラッシュ PC カードをサポートしています。アクティブな Supervisor Engine 32 上のスロットのキーワードは、**disk0:** 冗長 Supervisor Engine 32 上のスロットのキーワードは、**slavedisk0:**

複数のブート イメージを保存できるという理由から、起動および同期化が正しく行われるようにするため、ブート ファイル イメージの名前およびイメージ ファイルのフラッシュ ファイル システムでの保存場所を指定する必要があります。ブート イメージの名前および場所の指定方法については、第 24 章「スイッチの起動設定の変更」を参照してください。

同期化プロセス中、アクティブ スーパバイザ エンジンはスタンバイ スーパバイザ エンジンのランタイム イメージをチェックし、自身のランタイム イメージと一致していることを確認します。アクティブ スーパバイザ エンジンがチェックする条件は、次の 3 つです。

- アクティブ スーパバイザ エンジンのブート イメージを、スタンバイ スーパバイザ エンジンにコピーする必要があるかどうか。
- スタンバイ スーパバイザ エンジンのブートストリングを変更する必要があるかどうか。
- スタンバイ スーパバイザ エンジンをリセットする必要があるかどうか。

ここでは、フラッシュの同期化が開始される条件について説明します。さまざまな設定でスーパバイザ エンジンのフラッシュ イメージを同期化する例は、「スーパバイザ エンジンの同期化の例」（p.22-17）を参照してください。

スイッチ上での冗長スーパバイザ エンジンの設定

ここでは冗長スーパバイザ エンジンの設定方法について説明します。

同期化プロセスの開始

アクティブおよびスタンバイ スーパバイザ エンジン上のランタイム イメージおよびブート イメージの同期化が開始される条件は、次のとおりです。

- アクティブおよびスタンバイ スーパバイザ エンジン間でのランタイム イメージのタイムスタンプの不一致 — システムの起動時またはリセット時に、それぞれのランタイム イメージのタイムスタンプが異なっている場合、アクティブ スーパバイザ エンジンが自分のランタイム イメージに合わせて、スタンバイ スーパバイザ エンジンを同期化させます。
- アクティブおよびスタンバイ スーパバイザ エンジン間でのブート イメージのタイムスタンプの不一致 — システムの起動時またはリセット時に、それぞれのブート イメージのタイムスタンプが異なっている場合、または BOOT 環境変数が変更された場合には、アクティブ スーパバイザ エンジンが自分のブート イメージに合わせて、スタンバイ スーパバイザ エンジンを同期化させます。
- 現在のブート イメージの上書き — いずれかのフラッシュ デバイス上で保存されている現在のブート イメージが上書きされた場合、ファイル システム管理モジュールがそのイベントを検出し、同期化を開始します。アクティブ スーパバイザ エンジンが自分の新しいブート イメージに合わせて、スタンバイ スーパバイザ エンジンを同期化させます。
- BOOT 環境変数の変更 — BOOT 環境変数を変更して、異なるデフォルトブート イメージを指定した場合、アクティブ スーパバイザ エンジンによってブート イメージの同期化が開始されます。NVRAM 設定モジュールがそのイベントを検出し、起動設定パラメータを調べることにより、次に可能性の高いブート ファイル名を指定して、フラッシュ同期機能を呼び出します。
- 同じブート イメージ ファイル名が使用されているフラッシュ PC カード — アクティブまたはスタンバイのどちらかのスーパバイザ エンジンのフラッシュ デバイスを交換し、新しいフラッシュ デバイスに以前のフラッシュ デバイスのブート イメージと同じ名前の（タイムスタンプの異なる）ブート イメージが格納されている場合、フラッシュ ファイル管理モジュールが同期機能を開始します。
- 現在のランタイム イメージの削除 — フラッシュ デバイスから現在のランタイム イメージを削除する場合、フラッシュ ファイル管理モジュールから削除の確認を求められます。確認すると、フラッシュ ファイル管理モジュールがフラッシュの同期化を開始し、NVRAM 設定モジュールに変更を通知します。NVRAM 設定モジュールは、BOOT 環境変数を調べ、次に起動できるイメージを特定し、新しいイメージ名を使用してフラッシュ同期機能を呼び出します。

スーパバイザ エンジンの冗長構成に関する注意事項および制限事項

次に挙げる条件またはイベントは、冗長構成のスーパバイザ エンジン間でイメージが正しく同期化されず、予想外の結果が生じる原因になります。

- アクティブ スーパバイザ エンジンへの新しいイメージのダウンロード

  アクティブ スーパバイザ エンジンに新しいイメージをダウンロードすると、新しいイメージが（ブートフラッシュまたはフラッシュ PC カードの）ファイル システムにコピーされます。このイメージはブート イメージとして設定されていない場合もあるので、新しくダウンロードしたイメージは、スタンバイ スーパバイザ エンジンに自動的にはコピーされません。

  アクティブおよびスタンバイのスーパバイザ エンジン間で同期機能を開始するには、新しくダウンロードしたイメージを、アクティブ スーパバイザ エンジン上でブート イメージとして設定する必要があります。同期化は、ブート変数を変更したときに行われます。新しいイメージを実行するには、システムのリセットが必要です。

- 現在のランタイム イメージが見つからない場合

  アクティブ スーパバイザ エンジンがフラッシュ デバイス上で現在のランタイム イメージを見つけることができない場合には、エラー状態が伝えられます。スタンバイ スーパバイザ エンジンが搭載またはリセットされても、フラッシュの同期化は実行されません。さらに、スタンバイ スーパバイザ エンジン上の STATUS LED がレッドに点灯し、Syslog エラー メッセージが生成されます。

- スロット 2 にアクティブ スーパバイザ エンジンが搭載されている場合

  アクティブ スーパバイザ エンジンがスロット 2 に搭載されている場合、スタンバイ スーパバイザ エンジンはスロット 1 にあります。設定を変更して新しいブート イメージを指定し、システムをリセットすると、スロット 1 のスーパバイザ エンジンがアクティブ スーパバイザ エンジンになり、対応するデフォルトのブート イメージがロードされて、変更した設定内容が取り消されます。この問題を回避するために、ブート ファイル設定を変更すると、スイッチはただちに、フラッシュの同期化を要求するプロンプトを表示します。

スタンバイ スーパバイザ エンジン ステータスの確認

ここで説明される CLI コマンドを使用して、スタンバイ スーパバイザ エンジンのステータスを確認することができます。

（注） **show module** コマンドは、搭載されたドータカードについての情報を出力します。**show test** コマンドは、オンボードの Application-Specific Integrated Circuit（ASIC; 特定用途向け IC）についての情報を出力します。

スタンバイ スーパバイザ エンジンのステータスを調べるには、次の作業のうち 1 つまたは複数を行います。

作業	コマンド
スタンバイ スーパバイザ エンジンのステータスを表示します。	**show module** [*mod*]
スタンバイ スーパバイザ エンジンのアップリンク ポート ステートを表示します。	**show port** [*mod*[*/port*]]
スタンバイ スーパバイザ エンジンについて、診断テスト結果を表示します。	**show test** [*mod*]

次に、**show module** および **show test** コマンドを入力して、スタンバイ スーパバイザ エンジンのステータスを調べる例を示します。

```
Console> (enable) show module 2
Mod Slot Ports Module-Type               Model               Status
--- ---- ----- ------------------------- ------------------- --------
2   2    2     1000BaseX Supervisor      WS-X6K-SUP1-2GE     ok

Mod Module-Name         Serial-Num
--- ------------------- -----------
2                       SAD02330231

Mod MAC-Address(es)                         Hw     Fw          Sw
--- --------------------------------------- ------ ----------- ------------------
2   00-e0-14-0e-f5-6c to 00-e0-14-0e-f5-6d 0.404  4.2(2038)  4.2(0.24)VAI50
    00-e0-14-0e-f5-6e to 00-e0-14-0e-f5-6f
    00-10-7b-bb-2b-00 to 00-10-7b-bb-2e-ff

Mod Sub-Type            Sub-Model           Sub-Serial  Sub-Hw
--- ------------------- ------------------- ----------- ------
2   L2 Switching Engine WS-F6020            SAD02350211 0.101
Console> (enable)

Console> (enable) show test 2
Module 2 : 2-port 1000BaseX Supervisor
Network Management Processor (NMP) Status: (. = Pass, F = Fail, U = Unknown)
  ROM:  .   Flash-EEPROM: .   Ser-EEPROM: .   NVRAM: .   EOBC Comm: .

Line Card Status for Module 1 : PASS

Port Status :
  Ports 1  2
  -----------
        .  .
Line Card Diag Status for Module 2  (. = Pass, F = Fail, N = N/A)

 Module 2
  Cafe II Status :
        NewLearnTest:             .
        IndexLearnTest:           .
        DontForwardTest:          .
        DontLearnTest:            .
        ConditionalLearnTest:     .
        BadBpduTest:              .
        TrapTest:                 .
 Loopback Status [Reported by Module 2] :
  Ports 1  2
  -----------
        .  .
Console> (enable)
```

スタンバイ スーパバイザ エンジンへの強制切り替え

アクティブ スーパバイザ エンジンをリセットすることによって、スタンバイ スーパバイザ エンジンに強制的に切り替えることができます。

（注） アクティブ スーパバイザ エンジンをリセットすると、オープンしている Telnet セッションが切断されます。

スタンバイ スーパバイザ エンジンに強制的に切り替えるには、イネーブル モードで次の作業を行います。

作業	コマンド
アクティブ スーパバイザ エンジンをリセットします（*mod* はアクティブ スーパバイザ エンジンの番号を示します）。	**reset** *mod*

また、アクティブ スーパバイザ エンジン上で CISCO-STACK-MIB moduleAction 変数を reset（2）に設定することによって、スタンバイ スーパバイザ エンジンに強制的に切り替えることもできます。切り替えが行われると、システムから標準の SNMP ウォームスタート トラップが、設定されているトラップ レシーバーに送信されます。

次に、アクティブ スーパバイザ エンジンからスタンバイ スーパバイザ エンジンに強制的に切り替えたときの、アクティブ スーパバイザ エンジンのコンソール出力例を示します。

```
Console> (enable) reset 1
This command will force a switch-over to the standby Supervisor module.
Do you want to continue (y/n) [n]? y
Console> (enable) 12/07/1998,17:04:39:SYS-5:Module 1 reset from Console//

System Bootstrap, Version 3.1(2)
Copyright (c) 1994-1997 by cisco Systems, Inc.

System Bootstrap, Version 3.1(2)
Copyright (c) 1994-1997 by cisco Systems, Inc.
Presto processor with 32768 Kbytes of main memory

Autoboot executing command: "boot bootflash:cat6000-sup.5-4-1a.bin"
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Uncompressing file:  ###########################################################

System Power On Diagnostics
NVRAM Size .. .................512KB
ID Prom Test ..................Passed
DPRAM Size ....................16KB
DPRAM Data 0x55 Test ..........Passed
DPRAM Data 0xaa Test ..........Passed
DPRAM Address Test ............Passed
Clearing DPRAM ................Done
System DRAM Memory Size .......32MB
DRAM Data 0x55 Test ...........Passed
DRAM Data 0xaa Test ...........Passed
DRAM Address Test  ............Passed
Clearing DRAM .................Done
EARLII ........................Present
EARLII RAM Test ...............Passed
EARL Serial Prom Test .........Passed
Level2 Cache ..................Present
Level2 Cache test..............Passed

Boot image: bootflash:cat6000-sup.5-4-1a.bin
Downloading epld sram device please wait ...
Programming successful for Altera 10K50 SRAM EPLD
This module is now in standby mode.
Console is disabled for standby supervisor
```

次に、アクティブ スーパバイザ エンジンからスタンバイ スーパバイザ エンジンに強制的に切り替えたときの、スタンバイ スーパバイザ エンジンのコンソール出力例を示します。

```
Cisco Systems Console

Enter password:
12/07/1998,17:04:43:MLS-5:Multilayer switching is enabled
12/07/1998,17:04:43:MLS-5:Netflow Data Export disabled
12/07/1998,17:04:44:SYS-5:Module 2 is online
12/07/1998,17:04:45:SYS-5:Module 5 is online
12/07/1998,17:04:45:SYS-5:Module 7 is online
12/07/1998,17:04:45:SYS-5:Module 3 is online
12/07/1998,17:04:52:MLS-5:Route Processor 172.20.52.6 added
12/07/1998,17:05:10:SYS-5:Module 8 is online
12/07/1998,17:05:14:SYS-5:Module 9 is online
12/07/1998,17:05:22:SYS-5:Module 4 is online
12/07/1998,17:06:13:SYS-5:Module 1 is in standby mode
Supervisor image synchronization process will start in 10 seconds
12/07/1998,17:06:37:SYS-5:Ports on standby supervisor(Module 1) are UP
12/07/1998,17:06:41:SYS-5:Active supervisor is synchronizing the NMP image.
12/07/1998,17:06:44:SYS-5:The active supervisor has synchronized the NMP image.

Console>
```

ハイ アベイラビリティ機能

ハイ アベイラビリティ機能により、アクティブ スーパバイザ エンジンの故障時にアクティブ スーパバイザ エンジンからスタンバイ スーパバイザ エンジンへの切り替え時間を最小限に抑えることができます。

ハイ アベイラビリティ機能がリリースされる以前は、高速スイッチオーバーによってスタンバイ スーパバイザ エンジンへの切り替えが速やかに行われていました。ただし、高速スイッチオーバーでは、スイッチオーバー以前のスイッチ機能のステートが不明なため、スタンバイ スーパバイザエンジンをアクティブにする際にすべてのスイッチ機能を再度初期化し、スイッチを再起動する必要がありました。

ハイ アベイラビリティ機能では、このような制約がなくなっています。アクティブ スーパバイザ エンジンがスタンバイ スーパバイザ エンジンと通信し、機能のプロトコル ステートの同期化を保つためです。スーパバイザ エンジン間の同期化により、障害時にスタンバイ スーパバイザ エンジンが速やかに機能を引き継ぎます。

さらに、ハイ アベイラビリティ機能では、アクティブおよびスタンバイ スーパバイザ エンジン上で異なるソフトウェア イメージを実行できるバージョニングオプションも提供されています。

次に、これらの機能について説明します。

- ハイ アベイラビリティの概要（p.22-10）
- ハイ アベイラビリティでサポートされる機能（p.22-11）
- ハイ アベイラビリティ設定時の注意事項（p.22-11）
- バージョニングの概要（p.22-12）
- CLI コマンド（p.22-13）
- スタンバイ スーパバイザ エンジンへの異なる（ただし互換性のある）イメージのロード（p.22-15）

ハイ アベイラビリティの概要

ハイ アベイラビリティを可能にするために、アクティブ スーパバイザ エンジン上でシステム データベースが保守され、そのデータベース内のデータに変更があると、スタンバイ スーパバイザ エンジンに最新情報が送られます。アクティブ スーパバイザ エンジンは、何らかのステートの変更が発生すると、スタンバイ スーパバイザ エンジンと通信して情報を更新し、サポートされる機能の現在のプロトコル ステートをスタンバイ スーパバイザ エンジンが認識できるようにします。スタンバイ スーパバイザ エンジンは、すべてのモジュール、ポート、および VLAN（仮想 LAN）について現在のプロトコル ステートを認識しています。このステート情報を使用して各プロトコルが初期化され、ただちに動作を開始できます。

アクティブ スーパバイザ エンジンは、システム バス（バックプレーン）を制御し、ネットワークとの間でパケットを送受信し、すべてのモジュールを制御します。プロトコルはアクティブ スーパバイザ エンジン上でだけ動作します。

スタンバイ スーパバイザ エンジンはシステム バスから切り離されていて、パケットのスイッチングは行いません。ただし、スイッチング バスからパケットを受信して、レイヤ 2 スイッチド フローのために学習し、レイヤ 2 転送テーブルに入力します。さらにスタンバイ スーパバイザ エンジンは、スイッチング バスからパケットを受信して、レイヤ 3 スイッチド フローのために学習し、テーブルに入力します。スタンバイ スーパバイザ エンジンは、パケットの転送にはまったく参加せず、どのモジュールとも通信しません。

スタンバイ スーパバイザ エンジンの稼働時にハイ アベイラビリティをイネーブルに設定すると、イメージのバージョン互換性がチェックされます。互換性がある場合、データベースの同期化が開始されます。ハイ アベイラビリティ互換の各機能は、切り替え後、スタンバイ スーパバイザ エンジンに保存されていたステートから処理を続行します。

ハイ アベイラビリティをディセーブルにすると、データベースの同期化は実行されず、切り替え後はスタンバイ スーパバイザ エンジン上ですべての機能を再起動しなければなりません。

ハイ アベイラビリティをイネーブルからディセーブルに変更すると、アクティブ スーパバイザ エンジンからの同期化は停止され、スタンバイ スーパバイザ エンジンはその時点での同期データをすべて廃棄します。

ハイ アベイラビリティをディセーブルからイネーブルに変更すると、（スタンバイ スーパバイザ エンジンが存在し、しかもそのイメージ バージョンが互換である場合）アクティブからスタンバイ スーパバイザ エンジンへの同期化が開始されます。

NVRAM の同期化は、（2 つのスーパバイザ エンジンの NVRAM バージョンが互換である場合）ハイ アベイラビリティがイネーブルとディセーブルのどちらであっても行われます。

スタンバイ スーパバイザ エンジンがシステム ブート時に搭載されていなかった場合、アクティブ スーパバイザ エンジンはこの状況を検知し、同期化のためのデータベースの最新情報をキューに入れません。同様に、スタンバイ スーパバイザ エンジンをリセットまたは取り外した場合、同期化のための最新情報はキューに入れられず、同期化キュー内の未処理の更新データは廃棄されます。スタンバイ スーパバイザ エンジンになる 2 番めのスーパバイザ エンジンをオンラインの状態で挿入するか再起動すると、アクティブ スーパバイザ エンジンはシステム データベース全体をスタンバイ スーパバイザ エンジンにダウンロードします。これで初めてグローバルな同期化が成立し、アクティブ スーパバイザ エンジンは個々の最新情報をキューに入れ、スタンバイ スーパバイザ エンジンとの同期化を図るようになります。

（注） 2 番めのスーパバイザ エンジンをオンラインの状態で挿入するか再起動した場合、グローバルな同期が成立するまでに数分かかることがあります。

ハイ アベイラビリティでサポートされる機能

Catalyst 6500 シリーズ スイッチのハイ アベイラビリティ機能は、次の 3 つのカテゴリに分類されます（表 22-1 を参照）。

- サポートされる機能 — ハイ アベイラビリティが完全にサポートされています。この機能のデータベースは、アクティブ スーパバイザ エンジンからスタンバイ スーパバイザ エンジンに同期化されます。
- 互換機能 — ハイ アベイラビリティがサポートされていません。この機能のデータベースは、アクティブ スーパバイザ エンジンからスタンバイ スーパバイザ エンジンに同期化されません。ただし、ハイ アベイラビリティをイネーブルにすると、互換機能をイネーブルにできます。
- 非互換機能 — ハイ アベイラビリティがサポートされていません。この機能のデータベースは、アクティブ スーパバイザ エンジンからスタンバイ スーパバイザ エンジンに同期化されません。ハイ アベイラビリティをイネーブルにしても、非互換機能をイネーブルにできません。また、この非互換機能をイネーブルにすると、ハイ アベイラビリティをイネーブルにできません。

表 22-1　ハイ アベイラビリティ機能のサポート

サポートされる機能	互換機能	非互換機能
CEF	ASLB	ダイナミック VLAN
COPS-DS	CDP	GVRP
COPS-PR	GMRP	プロトコル フィルタリング
DTP	IGMP スヌーピング	
EtherChannel	RMON	
Cisco IOS ACL	RSVP	
MLS	SNMP	
PAgP	Telnet セッション	
QoS	UplinkFast	
SPAN	VTP プルーニング	
STP		
トランキング		
UDLD		
VACL		
VTP		
ポート セキュリティ		
802.1x		

ハイ アベイラビリティ設定時の注意事項

ここでは、ハイ アベイラビリティ設定時の注意事項について説明します。

- Cisco IOS ソフトウェアではハイ アベイラビリティは実行されないので、アクティブ MSFC のルーティング テーブル エントリは維持されません。ただし、アクティブおよびスタンバイの両方のスーパバイザ エンジン上で MSFC を同じコンフィギュレーションに設定し、アクティブ MSFC とスタンバイ MSFC の間でルーティング テーブル エントリを維持することはできます。MSFC 上に Hot Standby Router Protocol（HSRP）を設定すると、ルーティングが自動的にバックアップされます。詳細については、「MSFC 冗長機能」（p.22-22）を参照してください。
- タイマーおよび統計情報は、アクティブ スーパバイザ エンジンからスタンバイ スーパバイザ エンジンに同期化されません。
- Multilayer Switching（MLS; マルチレイヤ スイッチング）フローは、アクティブ スーパバイザ エンジンからスタンバイ スーパバイザ エンジンへ維持されます。

- 802.1X ポートでは、許可および未許可のステートだけがアクティブ スーパバイザ エンジンからスタンバイ スーパバイザ エンジンに同期化されます。その他のステートにあるポートは、スイッチオーバー発生後初期化されるか、再起動されます。
- 802.1X レコードの更新は、同様なタイプの更新を 1 つのレコードにまとめることによって最小化されています。
  レコードの変数が変更されると、アクティブ スーパバイザ エンジンは、スタンバイ スーパバイザ エンジンにレコードを送ります。
- 許可済みポートの 802.1X 再認証タイマーは、スイッチオーバー発生後に再始動します。
- ポート セキュリティ統計情報は、アクティブ スーパバイザ エンジンからスタンバイ スーパバイザ エンジンに同期化されません。
- ハイ アベイラビリティをイネーブルにするか、セキュア ポートを備えたスイッチ上でスタンバイ スーパバイザ エンジンをオンラインの状態で取り付けると、ポート単位および MAC（メディア アクセス制御）関連情報はすべてアクティブ スーパバイザ エンジンからスタンバイ スーパバイザ エンジンに同期化されます。

バージョニングの概要

ハイ アベイラビリティのバージョニング機能をイネーブルに設定した場合、アクティブ スーパバイザ エンジンおよびスタンバイ スーパバイザ エンジン上に、異なるが互換性のある 2 つのイメージを保持することができます。アクティブ スーパバイザ エンジンはスタンバイ スーパバイザ エンジンとイメージのバージョン情報を交換し、イメージの互換性によってハイ アベイラビリティ機能がイネーブルになるかを判別します。アクティブおよびスタンバイ スーパバイザ エンジンの実行するイメージ バージョンに互換性がない場合、ハイ アベイラビリティをイネーブルにすることはできません。

イメージ バージョニングは、Release 5.4(1) 以降のスーパバイザ エンジン ソフトウェア リリースでサポートされています。バージョニングをイネーブルに設定した場合、アクティブ スーパバイザ エンジンとスタンバイ スーパバイザ エンジンが異なるイメージを実行していても、それらのイメージに互換性があれば、ハイ アベイラビリティは完全にサポートされます。完全に互換性のあるイメージは、次に示すものだけです。

（注） 8.x ソフトウェア リリース トレインでは、ソフトウェア イメージ バージョンの互換性がありません。これには、8.1(x)、8.2(x)、8.3(x) 間などのメジャー リリースが含まれます。また、8.1(1) と 8.1(2) 間、8.2(1) と 8.2(2) 間などのサブリリースも含まれます。

- Supervisor Engine 1
  - 5.5(3) と 5.5(4)
  - 6.1(3) と 6.1(4)
  - 6.2(2) と 6.2(3)
  - 6.3(2) と 6.3(3)
  - 6.3(4) と 6.3(5)
  - 6.3(6) と 6.3(7)
- Supervisor Engine 2
  - 6.1(3) と 6.1(4)
  - 6.2(2) と 6.2(3)
  - 6.3(2) と 6.3(3)

ギガビット イーサネット スイッチング モジュールを除くすべてのモジュールと互換性のあるイメージは、次のとおりです。

- Supervisor Engine 1
  - 5.4(3) と 5.4(4)
  - 5.5(3) と 5.5(5)
  - 5.5(4) と 5.5(5)

ギガビット イーサネット スイッチング モジュールとは互換性があるが、10/100BASE-T モジュールとは互換性のないイメージは、次のとおりです。

- Supervisor Engine 1
  - 5.5(6a) と 5.5(7)

SFM/SFM2 およびファブリック対応モジュールを除くすべてのモジュールと互換性のあるイメージは、次のとおりです。

- Supervisor Engine 2
  - 6.3(4) と 6.3(5)
  - 6.3(6) と 6.3(7)

(注) 互換性のないバージョンのイメージを実行すると設定情報が失われます。

(注) 2 つのスーパバイザ エンジンを搭載している場合、先に起動したスーパバイザ エンジンがアクティブ モジュールになり、2 番めのスーパバイザ エンジンはスタンバイ モードになります。2 つのスーパバイザ エンジンがシステムに搭載されている場合は、起動時にスロット 1 のスーパバイザ エンジンがアクティブになり、スロット 2 のスーパバイザ エンジンがスタンバイ モードになります。このとき、2 つのスーパバイザ エンジンのソフトウェア バージョンが異なっているか、2 つのスーパバイザ エンジンの NVRAM 設定が異なっており、しかもバージョニングがイネーブルに設定されていない場合には、アクティブ スーパバイザ エンジンのソフトウェア イメージおよび設定がスタンバイ スーパバイザ エンジンに自動的にダウンロードされます。

CLI コマンド

ここでは、ハイ アベイラビリティおよびバージョニングに関連する CLI コマンドについて説明します。

ハイ アベイラビリティのイネーブル化またはディセーブル化

デフォルトでは、ハイ アベイラビリティはディセーブルに設定されています。ハイ アベイラビリティをイネーブルまたはディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
ハイ アベイラビリティをイネーブルまたはディセーブルにします。	**set system highavailability** {**enable** | **disable**}

次に、ハイ アベイラビリティをイネーブルにする例を示します。

```
Console> (enable) set system highavailability enable
System high availability enabled.
Console> (enable)
```

次に、ハイ アベイラビリティをディセーブルにする例を示します。

```
Console> (enable) set system highavailability disable
System high availability disabled.
Console> (enable)
```

ハイ アベイラビリティ バージョニングのイネーブル化またはディセーブル化

デフォルトでは、ハイ アベイラビリティ バージョニングはディセーブルに設定されています。ハイ アベイラビリティ バージョニングをイネーブルまたはディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
ハイ アベイラビリティ バージョニングをイネーブルまたはディセーブルにします。	**set system highavailability versioning** {**enable** | **disable**}

次に、ハイ アベイラビリティ バージョニングをイネーブルにする例を示します。

```
Console> (enable) set system highavailability versioning enable
Image versioning enabled.
Console> (enable)
```

次に、ハイ アベイラビリティ バージョニングをディセーブルにする例を示します。

```
Console> (enable) set system highavailability versioning disable
Image versioning disabled.
Console> (enable)
```

ハイ アベイラビリティの設定および稼働ステータスの表示

show system highavailability コマンドを実行すると、次の情報が表示されます。

- ハイ アベイラビリティの設定（イネーブルまたはディセーブル）
- バージョニングの設定（イネーブルまたはディセーブル）
- ハイ アベイラビリティの稼働ステータス（スタンバイ スーパバイザ エンジンが搭載されて稼働しているかどうかに基づく）。稼働ステータス フィールドには、次のいずれかが表示されます。
  - OFF（high-availability-not-enabled）：NVRAM のハイ アベイラビリティ オプションがディセーブルに設定されています。
  - OFF（standby-supervisor-not-present）：スタンバイ スーパバイザ エンジンが搭載されていません。
  - OFF（standby-supervisor-image-incompatible）：スタンバイ スーパバイザ エンジンがアクティブ スーパバイザ エンジンとは異なるイメージを実行しており、しかもイメージがバージョン互換ではありません（NVRAM のバージョニング オプションはイネーブルに設定されています）。同期化は一切行われません（アクティブ スーパバイザ エンジン上の NVRAM で設定が変更されても、バージョン間に互換性がないので、スタンバイ スーパバイザ エンジンには伝播されません）。
  - OFF（standby-supervisor-image-nvram-only-compat）：スタンバイ スーパバイザ エンジンがアクティブ スーパバイザ エンジンとは異なるイメージを実行しており（NVRAM のバージョニング オプションはイネーブルに設定されています）、そのイメージは NVRAM 互換性が

あるだけです（したがって、アクティブ スーパバイザ エンジン上の NVRAM で設定が変更されると、スタンバイ スーパバイザ エンジンに伝播されます）。ただし、ハイ アベイラビリティはサポートできません。

- OFF（standby-supervisor-not-operational-yet）：スタンバイ スーパバイザ エンジンが検出されましたが稼働していません（まだオンラインではありません）。
- OFF（high-availability-not-operational-yet）：スタンバイ スーパバイザ エンジンは稼働しています（オンラインです）が、ハイ アベイラビリティはまだ稼働していません（システムがリセット後に起動したとき、ハイ アベイラビリティが稼働するまでに数分かかります）。
- ON：ハイ アベイラビリティが稼働しています。アクティブ スーパバイザ エンジンの各機能は、スタンバイ スーパバイザ エンジンとの同期をとるため、ステータス変更のキューイングを開始しました。

ハイ アベイラビリティの設定および稼働ステートを表示するには、次の作業を行います。

作業	コマンド
ハイ アベイラビリティの設定および稼働ステートを表示します。	**show system highavailability**

次に、ハイ アベイラビリティの設定および稼働ステートを表示する例を示します。

```
Console> (enable) show system highavailability
Highavailability: disabled
Highavailability versioning: disabled
Highavailability Operational-status: OFF (high-availability-not-enabled)
Console> (enable)
```

次に、ハイ アベイラビリティをイネーブルにする例を示します。

```
Console> (enable) set system highavailability enable
System high availability enabled.
Console> (enable)

Console> (enable) show system highavailability
Highavailability: enabled
Highavailability versioning: disabled
Highavailability Operational-status: ON
Console> (enable)
```

スタンバイ スーパバイザ エンジンへの異なる（ただし互換性のある）イメージのロード

スタンバイ スーパバイザ エンジンに、アクティブ スーパバイザ エンジン上のイメージとは異なる新しいイメージをロードする手順は、次のとおりです。アクティブ スーパバイザ エンジンのコンソール ポートから、次の作業を実行します（アクティブ スーパバイザ エンジンはスロット 1 に搭載されています）。

ステップ 1　ハイ アベイラビリティをイネーブルにします。

```
Console> (enable) set system highavailability enable
System high availability enabled.
Console> (enable)
```

ステップ 2　アクティブ スーパバイザ エンジンのブートフラッシュに、新しいイメージをダウンロードします。

```
Console> (enable) copy tftp:image2.bin bootflash
IP address or name of remote host []? 172.20.52.3

8763532 bytes available on device bootflash, proceed (y/n) [n]? y
.
.
.
Console> (enable)
```

ステップ 3　スタンバイ スーパバイザ エンジンのブートフラッシュに、新しいイメージをコピーします。

```
Console> (enable) copy bootflash:image2.bin 2/bootflash:

5786532 bytes available on device bootflash, proceed (y/n) [n]? y
.
.
.
Console> (enable)
```

ステップ 4　スタンバイ スーパバイザ エンジンが新しいイメージを起動するように、BOOT 環境変数を変更します。

```
Console> (enable) set boot system flash bootflash:image2.bin prepend 2
BOOT variable = bootflash:image2.bin,1;slot0:image1.bin,1
Console> (enable)
```

ステップ 5　スタンバイ スーパバイザ エンジンをリセットして、新しいイメージを起動します。

```
Console> (enable) reset 2
This command will reset the system.
Do you want to continue (y/n) [n]? y
.
.
.
Console> (enable)
```

NSF および SSO を使用したスーパバイザ エンジンの冗長構成

Cisco NSF は SSO と連携することにより、スイッチオーバー後にユーザがネットワークを使用できなくなる期間を最小にしながら、IP パケットの転送を継続します。

NSF に SSO を設定する手順については、次の URL にある『*Catalyst 6500 Series Cisco IOS Software Configuration Guide, 12.2SX*』の「Configuring Supervisor Engine Redundancy using NSF with SSO」を参照してください。
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/nsfsso.htm

スーパバイザ エンジンの同期化の例

ここでは、同期機能が特定の条件を検出した場合の現象について説明します。

- ランタイム イメージとブートストリングの同期化（p.22-17）
- アクティブおよびスタンバイ スーパバイザ エンジンのブート イメージの同期化（p.22-19）

（注） ここで示す一連の例で、ブートストリングの中のファイル名の後ろの　**1**　という数字（たとえば **bootflash:f1,1**）は、Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）起動の試行回数を表します。ただし、スーパバイザ エンジンでは TFTP による起動はサポートされていません。Cisco IOS の表記との一貫性のため、この数字を含めています。

（注） ここで紹介する例は、考えられるすべての事例を含んでいるわけではありません。

ランタイム イメージとブートストリングの同期化

ここでは、アクティブ スーパバイザ エンジンのランタイム イメージとスタンバイ スーパバイザ エンジンとの同期化について、4 つの例を紹介します。

例 1：ランタイム イメージの同期化が行われない場合

例 1 の設定は、次のとおりです。

- アクティブ スーパバイザ エンジンの設定は、次のとおりです（スタンバイ スーパバイザ エンジンのイメージがアクティブ スーパバイザ エンジンのイメージと同じである場合、出力は同じになります）。
  - ランタイム イメージ：`bootflash:f1`
  - ブートストリング：`bootflash:f1,1`
  - ブートフラッシュ：`f1`
- アクティブ スーパバイザ エンジン上の **f1** のタイムスタンプは、スタンバイ スーパバイザ エンジン上の **f1** と同じです。
- 予測される結果は、次のとおりです。
  - アクティブ スーパバイザ エンジンの **f1** イメージは、スタンバイ スーパバイザ エンジンにコピーされません。
  - スタンバイ スーパバイザ エンジンのブートストリングは変更されません。
  - スタンバイ スーパバイザ エンジンはリセットされません。

例 2：ファイルのコピー、ブートストリングの変更、スタンバイ スーパバイザ エンジンのリセットが行われる場合

例 2 の設定は、次のとおりです。

- アクティブ スーパバイザ エンジンの設定は、次のとおりです。
  - ランタイム イメージ：`bootflash:f1`
  - ブートストリング：`bootflash:f1,1`
  - ブートフラッシュ：`f1`

- スタンバイ スーパバイザ エンジンの設定は、次のとおりです。
  - ランタイム イメージ：bootflash:f2
  - ブートストリング：bootflash:f2,1
  - ブートフラッシュ：f2
- アクティブ スーパバイザ エンジン上の **f1** のタイムスタンプは、スタンバイ スーパバイザ エンジン上の **f2** と同じではありません。
- 予測される結果は、次のとおりです。
  - アクティブ スーパバイザ エンジンが **f1** イメージをスタンバイ スーパバイザ エンジンにコピーし、ファイル名を **RTSYNC_f1** に変更します。
  - スタンバイ スーパバイザ エンジンのブートフラッシュが次のように変更されます。**f2, RTSYNC_f1**
  - スタンバイ スーパバイザ エンジンのブートストリングが次のように変更されます。**bootflash:RTSYNC_f1,1;f2,1;**
  - スタンバイ スーパバイザ エンジンがリセットされます。

例 3：ファイルがコピーされず、ブートストリングが変更され、スタンバイ スーパバイザ エンジンがリセットされる場合

例 3 の設定は、次のとおりです。

- アクティブ スーパバイザ エンジンの設定は、次のとおりです。
  - ランタイム イメージ：bootflash:f1
  - ブートストリング：bootflash:f1,1
  - ブートフラッシュ：f1
- スタンバイ スーパバイザ エンジンの設定は、次のとおりです。
  - ランタイム イメージ：bootflash:f2
  - ブートストリング：bootflash:f2,1
  - ブートフラッシュ：f1,f2
- アクティブ スーパバイザ エンジン上の **f1** のタイムスタンプは、スタンバイ スーパバイザ エンジン上の **f1** と同じですが、スタンバイ スーパバイザ エンジン上の **f2** とは同じではありません。
- 予測される結果は、次のとおりです。
  - アクティブ スーパバイザ エンジンのランタイム イメージとスタンバイ スーパバイザ エンジンが同期化されます。
  - アクティブ スーパバイザ エンジンの **f1** イメージは、スタンバイ スーパバイザ エンジンにコピーされません。
  - スタンバイ　スーパバイザ　エンジンのブートストリングが次のように変更されます。**f1,1;f2,1;**
  - スタンバイ スーパバイザ エンジンがリセットされます。

例 4：最も古いブートフラッシュ ファイルが削除され、ブートフラッシュのスクイーズが実行される場合

例 4 の設定は、次のとおりです。

- アクティブ スーパバイザ エンジンの設定は、次のとおりです。
  - ランタイム イメージ：bootflash:f1
  - ブートストリング：bootflash:f1,1
  - ブートフラッシュ：f1
- スタンバイ スーパバイザ エンジンの設定は、次のとおりです。
  - ランタイム イメージ：bootflash:f2

- ブートストリング：`bootflash:f2,1;`
- ブートフラッシュ：`f2, f3, f4`（メモリの空きスペースは 1 MB 未満）

- アクティブ スーパバイザ エンジン上の **f1** のタイムスタンプは、スタンバイ スーパバイザ エンジン上の **f2** と同じではありません。**f2** のタイムスタンプは **f3** より古く、**f3** のタイムスタンプは **f4** より古くなっています。
- 予測される結果は、次のとおりです。
  - アクティブ スーパバイザ エンジンのランタイム イメージとスタンバイ スーパバイザ エンジンが同期化されます。
  - アクティブ スーパバイザ エンジンは、スタンバイ スーパバイザ エンジンへ **f1** イメージのコピーを試みます。
  - スタンバイ スーパバイザ エンジンのブートフラッシュがスペース不足なので、冗長同期化機能が最も古いファイルを見つけて削除し、ブートフラッシュのスクイーズを実行します。
  - アクティブ スーパバイザ エンジンが **f1** イメージをスタンバイ スーパバイザ エンジンにコピーし、ファイル名を **RTSYNC_f1** に変更します。
  - スタンバイ スーパバイザ エンジンのブートフラッシュが次のように変更されます。**f3, f4, RTSYNC_f1**
  - スタンバイ スーパバイザ エンジンのブートストリングが次のように変更されます。**RTSYNC_f1,1;f2,1;**
  - スタンバイ スーパバイザ エンジンがリセットされます。

アクティブおよびスタンバイ スーパバイザ エンジンのブート イメージの同期化

ここでは、アクティブおよびスタンバイ スーパバイザ エンジン上のブートストリングの同期化について、4 つの例を紹介します。

例 1：ブート イメージを割り当てられない場合

この例の設定は、次のとおりです。

- アクティブ スーパバイザ エンジンの設定は、次のとおりです。
  - ランタイム イメージ：`bootflash:f1`
  - ブートストリング：`bootflash:f1,1;`
  - ブートフラッシュ：`f1`
- スタンバイ スーパバイザ エンジンの設定は、次のとおりです。
  - ランタイム イメージ：`bootflash:f1`
  - ブートストリング：`bootflash:f1,1;`
  - ブートフラッシュ：`f1`
- アクティブ スーパバイザ エンジン上の **f1** のタイムスタンプは、スタンバイ スーパバイザ エンジン上の **f1** と同じです。
- システムはアクティブ スーパバイザ エンジンのブートストリングを次のように変更しようと試みます。**f2,1;**
- 予測される結果は、次のとおりです。
  - アクティブ スーパバイザ エンジンは **f2** を割り当てることができず、同期化が失敗します。
  - Syslog にエラーが記録されます。
  - アクティブ スーパバイザ エンジンの **f1** イメージは、スタンバイ スーパバイザ エンジンにコピーされません。
  - スタンバイ スーパバイザ エンジンのブートストリングは変更されません。
  - スタンバイ スーパバイザ エンジンはリセットされません。

例 2：ファイルがコピーされ、ブートフラッシュが変更され、スタンバイ スーパバイザ エンジンがリセットされない場合

この例の設定は、次のとおりです。

- アクティブ スーパバイザ エンジンの設定は、次のとおりです。
  - ランタイム イメージ：`bootflash:f1`
  - ブートストリング：`bootflash:f1,1;`
  - ブートフラッシュ：`f1,f2`
- スタンバイ スーパバイザ エンジンの設定は、次のとおりです。
  - ランタイム イメージ：`bootflash:f1`
  - ブートストリング：`bootflash:f1,1;`
  - ブートフラッシュ：`f1`
- アクティブ スーパバイザ エンジン上の **f1** のタイムスタンプは、スタンバイ スーパバイザ エンジン上の **f1** と同じです。
- アクティブ スーパバイザ エンジンのブートストリングを次のように変更します。**f2,1;**
- 予測される結果は、次のとおりです。
  - アクティブ スーパバイザ エンジンが **f2** イメージをスタンバイ スーパバイザ エンジンにコピーし、ファイル名を **BTSYNC_f2** に変更します。
  - スタンバイ スーパバイザ エンジンのブートフラッシュが次のように変更されます。**f1, BTSYNC_f2**
  - スタンバイ スーパバイザ エンジンのブートストリングが次のように変更されます。**bootflash:BTSYNC_f2,1;f1,1;**
  - スタンバイ スーパバイザ エンジンはリセットされません。

例 3：ファイルがコピーされず、ブートストリングが変更され、スタンバイ スーパバイザ エンジンがリセットされない場合

この例の設定は、次のとおりです。

- アクティブ スーパバイザ エンジンの設定は、次のとおりです。
  - ランタイム イメージ：`bootflash:f1`
  - ブートストリング：`bootflash:f1,1;`
  - ブートフラッシュ：`f1,f2`
- スタンバイ スーパバイザ エンジンの設定は、次のとおりです。
  - ランタイム イメージ：`bootflash:f1`
  - ブートストリング：`bootflash:f1,1;`
  - ブートフラッシュ：`f1,f2`
- アクティブ スーパバイザ エンジン上の **f1** のタイムスタンプは、スタンバイ スーパバイザ エンジン上の **f1** と同じです。アクティブ スーパバイザ エンジン上の **f2** のタイムスタンプは、スタンバイ スーパバイザ エンジン上の **f2** と同じです。
- アクティブ スーパバイザ エンジンのブートストリングが次のように変更されます。**f2,1; f1,1;**
- 予測される結果は、次のとおりです。
  - アクティブ スーパバイザ エンジンの **f1** イメージは、スタンバイ スーパバイザ エンジンにコピーされません。
  - スタンバイ スーパバイザ エンジンのブートストリングが次のように変更されます。**bootflash:f2,1;bootflash:f1,1;**
  - スタンバイ スーパバイザ エンジンはリセットされません。

例 4：ファイルのコピー、最も古いファイルの削除、ブートフラッシュのスクイーズ、ブートストリングの変更が行われ、スタンバイ スーパバイザ エンジンがリセットされない場合

この例の設定は、次のとおりです。

- アクティブ スーパバイザ エンジンの設定は、次のとおりです。
  - ランタイム イメージ：`bootflash:f1`
  - ブートストリング：`bootflash:f1,1;`
  - ブートフラッシュ：`f1,f2`
- スタンバイ スーパバイザ エンジンの設定は、次のとおりです。
  - ランタイム イメージ：`bootflash:f1`
  - ブートストリング：`bootflash:f1,1;`
  - ブートフラッシュ：`f0,f1,f3`（メモリの空きスペースは 1 MB 未満）
- アクティブ スーパバイザ エンジン上の **f1** のタイムスタンプは、スタンバイ スーパバイザ エンジン上の **f1** と同じです。**f0** のタイムスタンプは **f1** より古く、**f1** のタイムスタンプは **f3** より古くなっています。
- アクティブ スーパバイザ エンジンのブートストリングが次のように変更されます。
  bootflash:f2,1;bootflash:f1,1;
- 予測される結果は、次のとおりです。
  - アクティブ スーパバイザ エンジンは、スタンバイ スーパバイザ エンジンへ **f2** イメージのコピーを試みます。
  - スタンバイ スーパバイザ エンジンのブートフラッシュがスペース不足なので、冗長同期化機能が最も古いファイル（**f0**）を見つけて削除し、ブートフラッシュのスクイーズを実行します。
  - アクティブ スーパバイザ エンジンが **f2** イメージをスタンバイ スーパバイザ エンジンにコピーし、ファイル名を **BTSYNC_f2** に変更します。
  - スタンバイ スーパバイザ エンジンのブートフラッシュが次のように変更されます。
    f1, f3, BTSYNC_f2
  - スタンバイ スーパバイザ エンジンのブートストリングが次のように変更されます。
    bootflash:BTSYNC_f2,1;bootflash:f1,1;

MSFC 冗長機能

ここでは、次の内容で MSFC 冗長機能について説明します。

（注） NSF/SSO を使用した MSFC 冗長機能の設定については、第 23 章「NSF/SSO MSFC 冗長機能の設定」を参照してください。

（注） SRM の冗長機能は、Supervisor Engine 720 および Supervisor Engine 32 でサポートされる唯一の MSFC 冗長機能オプションです。

デュアル MSFC 冗長機能

注意 両方の MSFC は同一設定にしておく必要があります。表 22-2（p.22-23）に、同一設定の要件、および単一スイッチ シャーシでのレイヤ 3 冗長機能の例外を示します。

MSFC が同一設定でない構成は、サポートされていません。

ここでは、MSFC 冗長機能の設定手順について説明します。

ハードウェアおよびソフトウェアの要件

レイヤ 3 の冗長機能を設定するには、少なくとも次のいずれかの構成が必要です。

- 2 つの同一スーパバイザ エンジン ドータカードから構成される 1 つのシャーシ
  - PFC および MSFC または MSFC2 搭載の Supervisor Engine 1（両方のスーパバイザ エンジンに同一タイプの MSFC を搭載することが必要）
  - PFC2 および MSFC2 搭載の Supervisor Engine 2
- それぞれスーパバイザ エンジンを搭載したシャーシ ― 各シャーシに少なくとも 1 つはスーパバイザ エンジンを搭載しておく必要があります。各スーパバイザ エンジンに、PFC および MSFC を取り付けておく必要があります。

（注） 各 MSFC は、同じ Cisco IOS ソフトウェア リリースを実行している必要があります。

単一シャーシによるレイヤ 3 冗長設定

単一の Catalyst 6500 シリーズ シャーシに、それぞれ MSFC を搭載した冗長スーパバイザ エンジンを取り付けることができます。MSFC 上に HSRP を設定すると、ネットワークで IP ホストに対するトランスペアレントなデフォルト ゲートウェイ冗長機能が実現します。HSRP コンフィギュレーションは、同じインターフェイス上で IPX および AppleTalk コンフィギュレーションと共存できます。

1 つの MSFC で障害が起きると、HSRP により、他方の MSFC（ルータ）が自動的に障害のある MSFC の機能を受け継ぎます。Release 5.4(1) のスーパバイザ エンジン ソフトウェア リリースのハイ アベイラビリティ機能を併用すると、ネットワークの冗長レベルがさらに向上します。

注意　両方の MSFC は同一設定にしておく*必要*があります。表 22-2 に、同一設定の要件、および単一スイッチ シャーシでのレイヤ 3 冗長機能の例外を示します。

表 22-2　単一シャーシのレイヤ 3 冗長機能の要件

同一設定の要件 ―グローバルおよびインターフェイス レベル	例外 ― インターフェイス レベル	例外 ― グローバル レベル
• 両方の MSFC に次の設定が*必要*です。 ― 同じルーティング プロトコル ― 同じスタティック ルート ― 同じデフォルト ルート ― 同じポリシー ルート ― 同じ VLAN インターフェイス ― 同じ Cisco IOS ACL[1、2] • すべてのインターフェイスが同じ管理ステータスでなければ*なりません*。	• HSRP スタンバイ コマンド • IP アドレス コマンド[3] • IPX ネットワーク[3]	• IP デフォルト ゲートウェイ • IPX インターナル ネットワーク • IPX デフォルト ルート

1. 実データ フローに基づくダイナミック ACL および再帰 ACL は、各 MSFC で設定することができます。
2. 両方の MSFC に同一の ACL を定義するだけではなく、ACL を両方の MSFC 上の同じ VLAN インターフェイスの同じ方向に適用する必要があります。
3. IP または IPX アドレスを両方の MSFC 上で同じにする必要はありませんが、両方の MSFC 上で IP または IPX アドレスを設定することが必要です。

表 22-2 に示したインターフェイスおよびグローバル レベルの例外に関して、代替コンフィギュレーションを指定する方法については、「alt キーワードの使用方法」（p.22-38）を参照してください。

冗長スーパバイザ エンジンには、同一のハードウェア（MSFC および PFC）が搭載されている*必要*があります。詳細については、「ハードウェアおよびソフトウェアの要件」（p.22-22）を参照してください。

（注）　MSFC および MSFC2 のメモリ要件については、次の URL の『Release Notes for MSFC』を参照してください。
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/index.htm

ルーティング プロトコルのピア設定

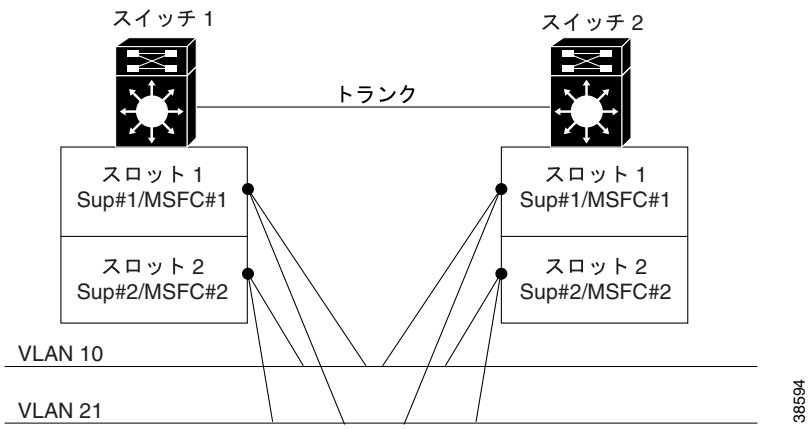
冗長スーパバイザ エンジンおよびデュアル MSFC 設定では、1 つのスーパバイザ エンジンが完全に稼働している状態（アクティブ）で、もう 1 つのスーパバイザ エンジンがスタンバイ モードになります。ただし、（アクティブ スーパバイザ エンジン上の PFC をプログラミングするため）MSFC は両方とも稼働し、独立ルータとして運用されます。

(注)　**PFC**：PFC を使用すると、MLS エントリをどちらかの MSFC に対応付けられます（最初のパケットをどちらの MSFC がルーティングするかに基づきます）。アクティブ スーパバイザ エンジン上の PFC だけが、パケットをスイッチングします。

(注)　**PFC2**：PFC2 では、メイン MSFC のみが、アクティブ スーパバイザ エンジン上で Forwarding Information Base（FIB; 転送情報ベース）、隣接テーブル、Cisco IOS ソフトウェア、およびポリシー ルーティング ACL をプログラミングします。スタティック ルートまたはポリシー ルーティングを設定した場合は、両方の MSFC で*同一*の設定にする必要があります。メイン MSFC 上にない非メイン MSFC にスタティック ルートがある場合は、そのルートは PFC2 ではプログラミング*されません*。

両方の MSFC は、ルーティング プロトコルのピア設定の観点から運用可能です。たとえば、単一の Catalyst 6500 シリーズ スイッチ シャーシに 2 つの MSFC を搭載し、両方に VLAN 10 および VLAN 21 のインターフェイスを設定した場合、2 つの MSFC はこれらの VLAN 上で相互にピアを形成します。デュアル シャーシおよびデュアル MSFC の構成で同じ VLAN を設定した場合には、各 MSFC に 6 つのピア（VLAN 10 に 3 つ、VLAN 21 に 3 つ）が形成されます。同じシャーシ内のピアのほか、2 つめのシャーシ内の 2 つの MSFC に対応するピアが形成されるためです（VLAN 10 の 3、VLAN 21 の 3）。図 22-1 を参照してください。

図 22-1　デュアル シャーシおよびデュアル MSFC のピア設定



各 MSFC は（ピア設定という観点では）独立ルータとして動作しますが、シャーシ上の 2 つの MSFC は同時に稼働し、同じインターフェイスを運用し、同じルーティング プロトコルを実行します。

スーパバイザ エンジンのハイ アベイラビリティ機能と MSFC 上の HSRP を併用すると、次のレイヤ 2 およびレイヤ 3 の冗長機能が提供されます。

- スーパバイザ エンジンのレイヤ 2 冗長機能（アクティブおよびスタンバイ）― アクティブ スーパバイザ エンジン（および搭載されている MSFC）に障害が発生すると、レイヤ 2 およびレイヤ 3 の両方の機能がスタンバイ スーパバイザ エンジンと搭載 MSFC に切り替わります。
- 2 つの MSFC のレイヤ 3 冗長機能および負荷分散 ― 1 つの MSFC に障害が発生すると、他方の MSFC が（HSRP により）ただちに機能を受け継ぎます。レイヤ 2 の運用は妨げられません（アクティブ スーパバイザ エンジンはレイヤ 2 トラフィックの転送を続けます）。

アクティブ スーパバイザ エンジン上の障害のある MSFC によってプログラミングされたレイヤ 3 エントリは、エージング アウトし、新しいアクティブ MSFC により移植されたレイヤ 3 エントリに置き換えられるまで、そのまま使用されます。エージングには 4 分かかるので、新しいアクティブ MSFC は、ハードウェアのスイッチング フローを妨げずに、XTAG 値を使用して MLS エントリを移植することができます。また、このプロセスは、新しいアクティブ MSFC に初期トラフィック フローが大量に送り込まれるのを防ぎます。

（注） 各 MSFC には、MLS ルート プロセッサであることを示す独自の XTAG 値が設定されています。MSFC #1（アクティブ スーパバイザ エンジン上）の XTAG は 1、MSFC #2（スタンバイ スーパバイザ エンジン上）の XTAG は 2 です。

XTAG 値を使用するのは、Supervisor Engine 1 のみです。Supervisor Engine 2 では XTAG 値が使用されません。

注意 同一シャーシ上のレイヤ 3 冗長機能を正常に動作させるには、両方の MSFC の設定が同じでなければなりません（表 22-2 [p.22-23] を参照）。

（注） 表 22-2 に、設定の例外が示されています。たとえば、図 22-1 では、VLAN10 上に 4 つの MSFC が関与しています。各 MSFC に異なる IP アドレスおよび HSRP プライオリティが設定されています。

ACL の設定

MSFC 上で Cisco IOS Access Control List（ACL; アクセス制御リスト）を使用する場合には、グローバル レベルおよびインターフェイス レベルで、両方の MSFC 上に同じ ACL を設定する*必要*があります。メイン MSFC（最初にオンラインになる MSFC、またはオンライン時間が長い MSFC）だけが、ACL 情報を備えた PFC をプログラミングします。

アクティブ スーパバイザ エンジン上の PFC のマルチレイヤ機能（CEF [Cisco Express Forwarding] for PFC2）は、ACL ASIC を照会し、設定されている Cisco IOS ACL に応じてパケットを転送するかどうか判別してから、パケットをスイッチングします。メイン MSFC に障害が発生した場合、新たにメインとなった MSFC は、スタティック ACL 用の PFC を再プログラミングする必要があります。一貫した結果を得るには、両方の MSFC に、スタティック ACL など、同一の ACL を設定する*必要があります*。

（注） 両方の MSFC 上に同一の ACL を定義するだけではなく、ACL を両方の MSFC 上の同じ VLAN インターフェイスに適用する必要があります。

（注） 実データ フローに基づくダイナミック ACL および再帰 ACL は、各 MSFC で設定することができます。

（注） **PFC**：PFC でのハードウェアおよびソフトウェアによる Cisco IOS ACL の処理の詳細については、「PFC でのハードウェアおよびソフトウェアによる Cisco IOS ACL の処理」（p.15-11）を参照してください。

（注） **PFC2**：PFC2 でのハードウェアおよびソフトウェアによる Cisco IOS ACL の処理の詳細については、「PFC2 および PFC3A/PFC3B/PFC3BXL でのハードウェアおよびソフトウェアによる Cisco IOS ACL の処理」（p.15-13）を参照してください。

メイン MSFC のステータスを判別するには、**show fm features** コマンドまたは **show redundancy** コマンドを使用します。

```
Router-15# show redundancy
Designated Router: 1 Non-designated Router:2
Redundancy Status: non-designated
Config Sync AdminStatus  : enabled
Config Sync RuntimeStatus: enabled

Router-16# show redundancy
Designated Router: 1 Non-designated Router:2
Redundancy Status: designated
Config Sync AdminStatus  : enabled
Config sync RuntimeStatus: enabled
```

デュアル MSFC 運用モデルの冗長機能および負荷分散

図 22-2 に、アクセス レイヤ スイッチの複数の VLAN による一般的なアクセスおよび分散レイヤ構築ブロックを示します。レイヤ 2 ループは設定されていないので、コンバージェンスおよび負荷分散には HSRP が使用されます。スイッチ S1 およびスイッチ S2 には、スロット 1（Sup #1/MSFC #1）およびスロット 2（Sup #2/MSFC #2）に MSFC 搭載スーパバイザ エンジンが取り付けられています。両スイッチとも、Sup #1 がアクティブで、Sup #2 はスタンバイ モードです。スーパバイザ エンジンのハイ アベイラビリティはイネーブルに設定されています。スーパバイザ エンジンのイメージおよび設定は自動的に同期化されますが、MSFC 上のイメージおよび設定は手動で同期化する必要があります。

図 22-2　デュアル MSFC 運用モデルの冗長機能および負荷分散 — VLAN10 および VLAN21

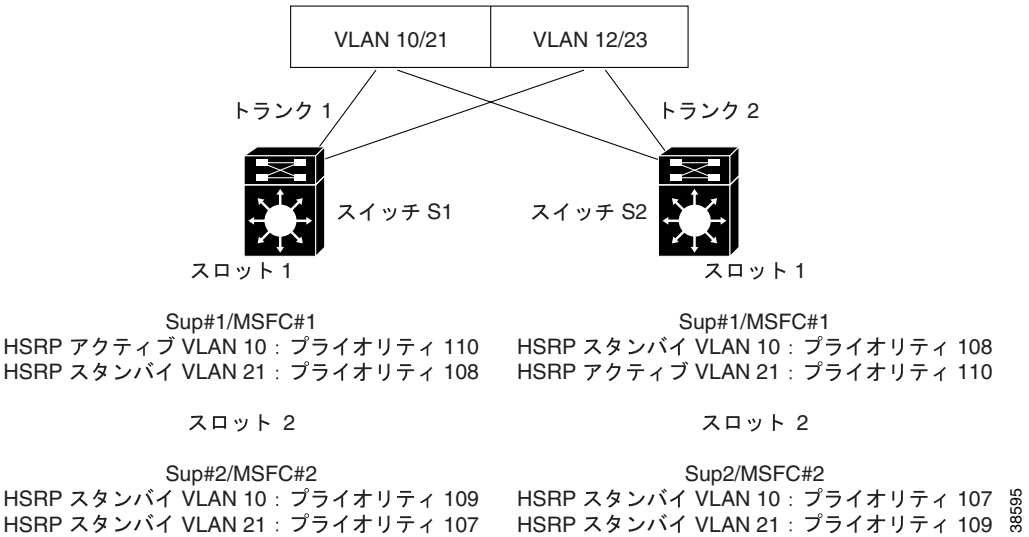


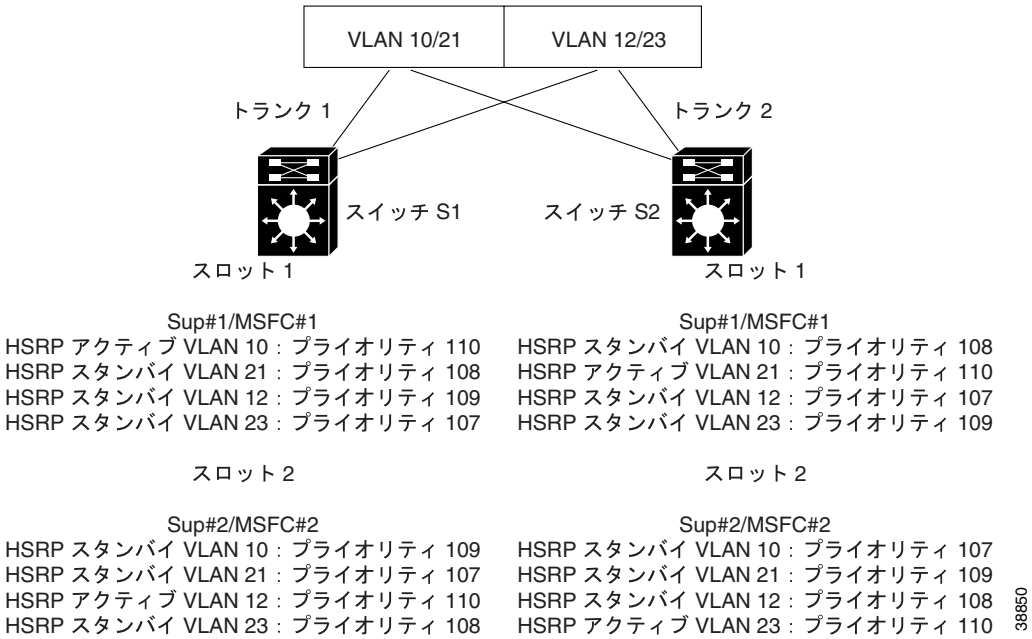
図 22-2 では、冗長機能および負荷分散を次のように設定します。

- VLAN10（偶数番号の VLAN）— スイッチ S1 の MSFC #1 をプライマリ HSRP ルータ（プライオリティ 110）として設定し、MSFC #2 をスタンバイ ルータ（プライオリティ 109）として設定します。
- VLAN21（奇数番号の VLAN）— スイッチ S2 の MSFC #1 をプライマリ HSRP ルータ（プライオリティ 110）として設定し、MSFC #2 をスタンバイ ルータ（プライオリティ 109）として設定します。

スイッチ S1 が偶数番号の VLAN をルーティングし、スイッチ S2 が奇数番号の VLAN をルーティングすることによって、負荷分散がサポートされます。一方のスイッチに障害が発生すると、他方のスイッチが奇数 VLAN と偶数 VLAN の両方のサービスを実行します。

スイッチ S1 の MSFC #2 を VLAN 12 のプライマリ HSRP ルータに、スイッチ S2 の MSFC #2 を VLAN 23 のプライマリ HSRP ルータに設定すれば、より高度な負荷分散を達成できます（図 22-3 を参照）。

図 22-3　デュアル MSFC 運用モデルの冗長機能および負荷分散 ― VLAN 10、12、21 および 23



VLAN のアクティブ HSRP ルータだけが、HSRP IP アドレスの Address Resolution Protocol（ARP）要求に対して、HSRP MAC アドレスを戻します。アクティブ HSRP ルータは、エンド ステーションの MAC アドレスに順番に ARP を適用し、ARP キャッシュを伝播します。単一シャーシ上の両方の MSFC を使用して偶数 VLAN の HSRP 処理を分散することによって、制御プレーンの ARP トラフィックを分散できます。いずれかの MSFC に障害が発生した場合、再学習が必要になるのは、影響を受けた VLAN の ARP エントリだけです。

このレベルの冗長機能および負荷分散では、Catalyst 6500 シリーズ スイッチ シャーシ上の MSFC の偶数および奇数 VLAN の追跡が複雑になるという欠点があります。

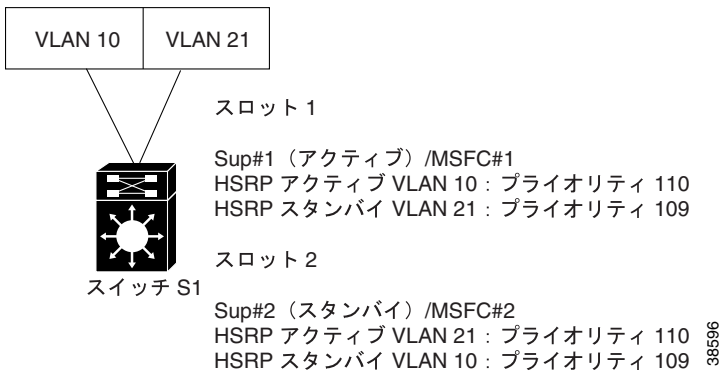
HSRP MAC アドレスに到達したパケット、およびルータの実 MAC アドレスを持つパケットには、MLS エントリが作成されます。ユニキャスト トラフィックの最初のホップの冗長機能には、HSRP が使用されます。たとえば、VLAN10 に接続している他のルータ経由で受信したトラフィックには、Sup #1/MSFC #1 の実 MAC アドレスが使用されます。

障害の例

ここでは、デュアル MSFC 搭載の 2 つのスーパバイザ エンジンを備えた単一シャーシ上で（図 22-4 を参照）ハイ アベイラビリティをイネーブルに設定した場合、発生する可能性のある 5 つの障害の例を示します。メイン MSFC が、スタティック ACL の ACL ASIC をプログラミングしています。

（注） この例は PFC 特有のものですが、PFC2/MSFC2 のフェールオーバーの例は、ACL および CEF テーブル エントリの処理に対するものと同じです。Supervisor Engine 2 では、メイン MSFC2 は、CEF テーブルの作成など PFC2 上で多数の ASIC をプログラミングします。非メイン MSFC2 に対するメイン MSFC2 HSRP フェールオーバーでは、PFC2 はこれまでのメイン MSFC2 によってプログラミングされた CEF テーブルで機能し続けます。Supervisor Engine 1/MSFC コンフィギュレーションでの MLS キャッシュによるプロセスと同様に、新しいメイン MSFC2 は固有のエントリで CEF テーブルを再度プログラミングし、古いエントリはエージング アウトします。

図 22-4　デュアル MSFC 搭載の 2 つのスーパバイザ エンジンを備えた単一シャーシ



障害ケース 1: メイン MSFC #1 の障害

メイン MSFC #1 に障害が起きると、次のシーケンスが実行されます。

1. MSFC #1 の MLS エントリが Sup #1 レイヤ -3 キャッシュでエージング アウトし、MSFC #2 は独自の XTAG 値を使用して、これらの MLS エントリを一時的に所有します。
2. MSFC #2 の MLS エントリは影響を受けません。
3. MSFC #2 は、MSFC #1 によってプログラミングされたハードウェア上のすべてのダイナミックおよび再帰 ACL を削除します。
4. MSFC #2 が新しいメイン MSFC となり、Sup #1 ACL ASIC のスタティック ACL を再プログラミングします。

障害ケース 2: 非メイン MSFC #2 の障害

非メイン MSFC #2 に障害が起きると、次のシーケンスが実行されます。

1. MSFC #2 の MLS エントリが Sup #1 レイヤ 3 キャッシュでエージング アウトし、MSFC #1 は独自の XTAG 値を使用して、これらの MLS エントリを一時的に所有します。
2. MSFC #1 の MLS エントリは影響を受けません。
3. MSFC #1 は、MSFC #2 によってプログラミングされたハードウェア上のすべてのダイナミックおよび再帰 ACL を削除します。
4. MSFC #1 は、そのままメイン MSFC として動作します。

障害ケース 3: アクティブ Sup #1 の障害

アクティブ スーパバイザ エンジン（Sup #1）に障害が起きると、次のシーケンスが実行されます。

1. レイヤ 3 のステートは保持されているので、MSFC #1 の MLS エントリは Sup #2 のレイヤ 3 キャッシュでエージング アウトし、MSFC #2 が独自の XTAG 値を使用して、これらの MLS エントリを一時的に所有します。
2. スタンバイ スーパバイザ エンジンはレイヤ 2 ステートを保持するので、レイヤ 2 のコンバージェンスは発生しません。
3. MSFC #2 は、MSFC #1 によってプログラミングされたハードウェア上のすべてのダイナミックおよび再帰 ACL を削除します。
4. MSFC #2 が、Sup #2 ACL ASIC のスタティック ACL を再プログラミングします。MSFC #2 が新しいメイン MSFC になります。

障害ケース 4: スタンバイ Sup #2 の障害

スタンバイ スーパバイザ エンジン（Sup #2）に障害が起きると、次のシーケンスが実行されます。

1. MSFC #2 の MLS エントリが Sup #1 レイヤ 3 キャッシュでエージング アウトし、MSFC #1 が独自の XTAG 値を使用して、これらの MLS エントリを一時的に所有します。
2. MSFC #1 の MLS エントリは影響を受けません。
3. MSFC #1 は、MSFC #2 によってプログラミングされたハードウェア上のすべてのダイナミックおよび再帰 ACL を削除します。MSFC #1 は、そのままメイン MSFC として動作します。

障害ケース 5: 新しいスーパ バイザまたは障害のあったスーパバイザをオンラインに戻したとき

障害のあったスーパバイザ エンジン（Sup #2）をオンラインに戻すと、次のシーケンスが実行されます。

1. Sup #1 は、引き続きアクティブ スーパバイザ エンジンとして動作します。
2. Sup #2 は、イメージおよびコンフィギュレーションを Sup #1 と同期化します（ハイ アベイラビリティ バージョニングがイネーブルに設定されていない場合）。
3. （Sup #2 上の）MSFC #2 がアップになります。VLAN21 の HSRP preempt が設定されている場合は、MSFC #2 の HSRP がアクティブになります。MSFC #1 の MLS エントリが削除され、MSFC #2 経由で再学習されます。
4. MSFC #1 は、引き続きスタティック ACL のメイン MSFC として動作します。

HSRP を使用した冗長機能の設定

スーパバイザ エンジン ハイ アベイラビリティ機能は、冗長スーパバイザ エンジンの間でプロトコル ステートを維持しますが、冗長 MSFC の間でフェールオーバー用に HSRP を設定する必要があります。HSRP を使用して、ユニキャスト トラフィックの最初のホップの冗長機能を実現します。MSFC の VLAN インターフェイスについて、1 つまたは複数の HSRP グループを設定することにより、ネットワークのルーティングを自動的にバックアップすることができます。HSRP グループの各 VLAN インターフェイスは、仮想 IP アドレスおよび MAC アドレスを共有します。HSRP アドレスをデフォルト ゲートウェイとして使用するようにエンド ステーションおよび他のデバイスを設定しておくと、1 つのルータ インターフェイスに障害が起きても、これらの装置のサービスは中断されません。

HSRP プライオリティが最も高いインターフェイスが、その HSRP グループのアクティブ インターフェイスになります。

（注） **PFC2：**PFC2 は、一意の番号を持つ HSRP グループを 16 個までサポートしています。異なる VLAN 上で同じ HSRP グループ番号を使用できます。16 を超える HSRP グループを設定すると、この制限により HSRP グループ番号として VLAN 番号を使用できなくなります。

（注） **PFC2：**同じ番号の HSRP グループは、同じ仮想 MAC アドレスを使用しますが、このことにより、MSFC でブリッジを設定する場合にエラーが発生する可能性があります。

HSRP 設定では、**standby use-bia** オプションを入力しないでください。**standby use-bia** オプションを入力すると、MLS エントリは作成されません。**standby use-bia** オプションを設定すると、HSRP アクティブ インターフェイスがアップまたはダウンになった場合、スタンバイ VLAN インターフェイスのルータ CAM（連想メモリ）アドレスはありません。ルータ CAM アドレスがなければショートカットは作成されません。この問題は、MSFC Cisco IOS のリリースとは無関係です（この問題については警告 CSCdz17169 を参照してください）。

MSFC の VLAN インターフェイス上に HSRP を設定するには、インターフェイス コンフィギュレーション モードで次の作業を行います。

	作業	コマンド
ステップ 1	HSRP をイネーブルにし、HSRP IP アドレスを指定します。*group_number* を指定しない場合、group 0 が使用されます。トラブルシューティングを容易にするため、グループ番号は VLAN 番号と一致するように設定してください。	Router(config-if)# **standby** [*group_number*] **ip** [*ip_address*]
ステップ 2	HSRP インターフェイスのプライオリティを指定します。HSRP グループ内の少なくとも 1 つのインターフェイスに、高いプライオリティを設定します（デフォルトは 100 です）。プライオリティの最も高いインターフェイスが、その HSRP グループのアクティブ インターフェイスになります。	Router(config-if)# **standby** [*group_number*] **priority** *priority*
ステップ 3	インターフェイスが現在のアクティブ HSRP インターフェイスを先取（preempt）し、現在のアクティブ インターフェイスよりもプライオリティが高い場合、そのインターフェイスがアクティブになるように設定します。	Router(config-if)# **standby** [*group_number*] **preempt** [**delay** *delay*]
ステップ 4	（任意）インターフェイスの HSRP hello タイマーおよび holdtime タイマーを設定します。デフォルト値は、3（hello）および 10（holdtime）です。HSRP グループのすべてのインターフェイスで、同じタイマー値を使用する必要があります。	Router(config-if)# **standby** [*group_number*] **timers** *hellotime holdtime*
ステップ 5	（任意）インターフェイスのクリア テキスト HSRP 認証ストリングを指定します。HSRP グループのすべてのインターフェイスで、同じ認証ストリングを使用する必要があります。	Router(config-if)# **standby** [*group_number*] **authentication** *string*

次に HSRP グループ 100 に属するインターフェイスを設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface vlan100
Router(config-if)# standby 100 ip 172.20.100.10
Router(config-if)# standby 100 priority 110
Router(config-if)# standby 100 preempt
Router(config-if)# standby 100 timers 5 15
Router(config-if)# standby 100 authentication Secret
Router(config-if)# ^Z
Router#
```

設定例

ここでは、冗長機能を実行する 3 つの設定例を紹介します。

- 例 1：スーパバイザ エンジンおよび MSFC を 1 つずつ搭載した 2 つのシャーシ（p.22-32）
- 例 2：スーパバイザ エンジンおよび MSFC を 2 つずつ装備した単一シャーシ（p.22-33）
- 例 3：スーパバイザ エンジンおよび MSFC を 2 つずつ装備したデュアル シャーシ（p.22-34）

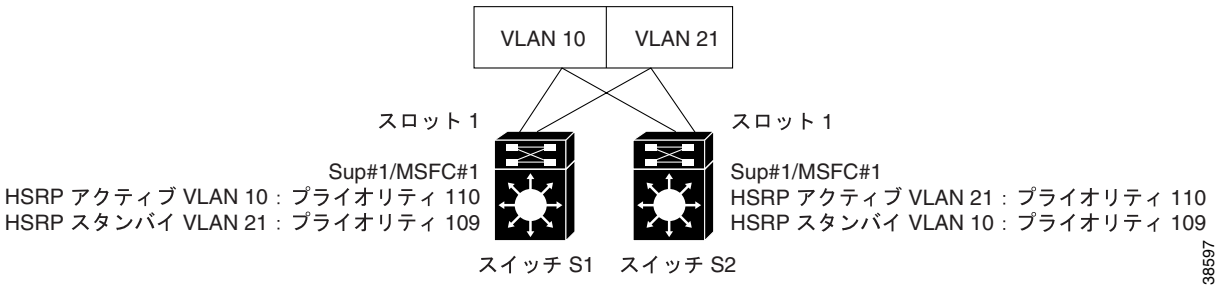
これらの例では、メイン MSFC はアクティブ スーパバイザ エンジンに搭載されています。メイン MSFC のステータスを判別するには、**show fm features** コマンドまたは **show redundancy** コマンドを使用します。次の例では、Router-16 がメイン MSFC です。

```
Router-15# show redundancy
Designated Router: 1 Non-designated Router:2

Redundancy Status: non-designated
Config Sync AdminStatus  : enabled
Config Sync RuntimeStatus: enabled

Router-16# show redundancy
Designated Router: 1 Non-designated Router:2

Redundancy Status: designated
Config Sync AdminStatus  : enabled
Config sync RuntimeStatus: enabled
```

例 1：スーパバイザ エンジンおよび MSFC を 1 つずつ搭載した 2 つのシャーシ

図 22-5 では、スーパバイザ エンジン上にハイ アベイラビリティを設定することはできませんが、MSFC 上に HSRP を設定することができます。

図 22-5　1 つのスーパバイザ エンジンと 1 つの MSFC が搭載された 2 つのシャーシ



次に、スイッチ S1 の MSFC 上に HSRP を設定する例を示します。

```
Console> (enable) switch console 15
Trying Router-15...
Connected to Router-15.
Type ^C^C^C to switch back...
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface vlan10
Router(config-if)# standby 10 ip 172.20.100.10
Router(config-if)# standby 10 priority 110
Router(config-if)# standby 10 preempt
Router(config-if)# standby 10 timers 5 15
Router(config-if)# standby 10 authentication Secret
Router(config-if)# interface vlan21
Router(config-if)# standby 21 ip 192.20.100.21
Router(config-if)# standby 21 priority 109
Router(config-if)# standby 21 preempt
Router(config-if)# standby 21 timers 5 15
Router(config-if)# standby 21 authentication Secret
Router(config-if)# ^Z
Router# ^C^C^C
```

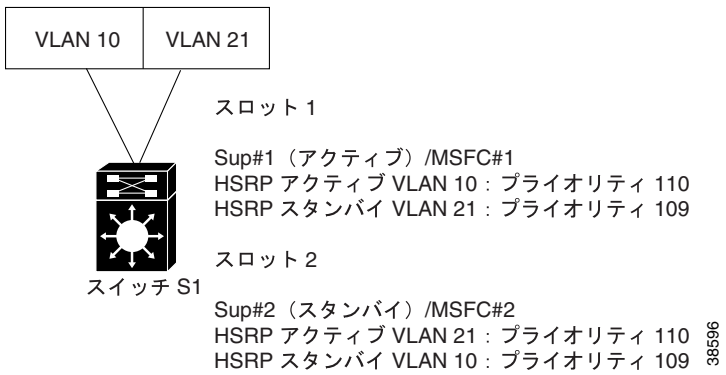
次に、スイッチ S2 の MSFC 上に HSRP を設定する例を示します。

```
Console> (enable) switch console 15
Trying Router-15...
Connected to Router-15.
Type ^C^C^C to switch back...
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface vlan10
Router(config-if)# standby 10 ip 172.20.100.10
Router(config-if)# standby 10 priority 109
Router(config-if)# standby 10 preempt
Router(config-if)# standby 10 timers 5 15
Router(config-if)# standby 10 authentication Secret
Router(config-if)# interface vlan21
Router(config-if)# standby 21 ip 192.20.100.21
Router(config-if)# standby 21 priority 110
Router(config-if)# standby 21 preempt
Router(config-if)# standby 21 timers 5 15
Router(config-if)# standby 21 authentication Secret
Router(config-if)# ^Z
Router# ^C^C^C
```

例 2：スーパバイザ エンジンおよび MSFC を 2 つずつ装備した単一シャーシ

図 22-6 では、スーパバイザ エンジン上にハイ アベイラビリティを設定し、MSFC 上に HSRP を設定しています。

図 22-6　冗長スーパバイザ エンジンおよび MSFC が搭載された単一シャーシ



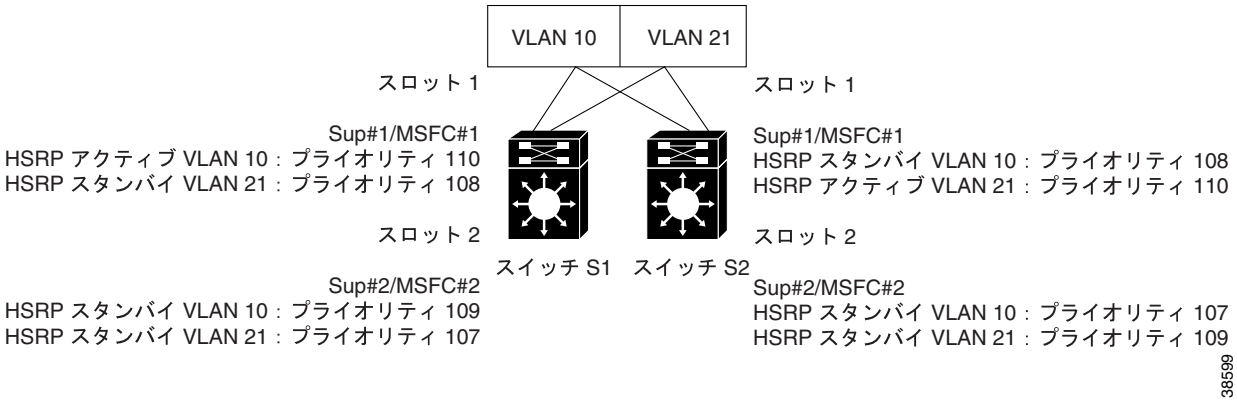
次に、スイッチ S1 の MSFC 上に HSRP を設定する例を示します。

```
Console> (enable) switch console 15
Trying Router-15...
Connected to Router-15.
Type ^C^C^C to switch back...
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface vlan10
Router(config-if)# standby 10 ip 172.20.100.10
Router(config-if)# standby 10 priority 110
Router(config-if)# standby 10 preempt
Router(config-if)# standby 10 timers 5 15
Router(config-if)# standby 10 authentication Secret
Router(config-if)# interface vlan21
Router(config-if)# standby 21 ip 192.20.100.21
Router(config-if)# standby 21 priority 109
Router(config-if)# standby 21 preempt
Router(config-if)# standby 21 timers 5 15
Router(config-if)# standby 21 authentication Secret
Router(config-if)# ^Z
Router# ^C^C^C

Console> (enable) switch console 16
Trying Router-16...
Connected to Router-16.
Type ^C^C^C to switch back...
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface vlan10
Router(config-if)# standby 10 ip 172.20.100.10
Router(config-if)# standby 10 priority 109
Router(config-if)# standby 10 preempt
Router(config-if)# standby 10 timers 5 15
Router(config-if)# standby 10 authentication Secret
Router(config-if)# interface vlan21
Router(config-if)# standby 21 ip 192.20.100.21
Router(config-if)# standby 21 priority 110
Router(config-if)# standby 21 preempt
Router(config-if)# standby 21 timers 5 15
Router(config-if)# standby 21 authentication Secret
Router(config-if)# ^Z
Router# ^C^C^C
```

例 3：スーパバイザ エンジンおよび MSFC を 2 つずつ装備したデュアル シャーシ

図 22-7 の 2 つの Catalyst 6500 シリーズ スイッチ（S1 および S2）は、それぞれスロット 1（Sup #1/MSFC #1）とスロット 2（Sup #2/MSFC #2）に MSFC およびスーパバイザ エンジンが搭載されています。レイヤ -2 ループは設定されていないので、コンバージェンスおよび負荷分散には HSRP が使用されます。両スイッチとも、Sup #1 がアクティブ スーパバイザ エンジンで、Sup #2 はスタンバイ スーパバイザ エンジンです。

図 22-7　デュアル MSFC 運用モデルの冗長機能および負荷分散



次に、スイッチ S1 の MSFC 上に HSRP を設定する例を示します。

```
Console> (enable) switch console 15
Trying Router-15...
Connected to Router-15.
Type ^C^C^C to switch back...
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface vlan10
Router(config-if)# standby 10 ip 172.20.100.10
Router(config-if)# standby 10 priority 110
Router(config-if)# standby 10 preempt
Router(config-if)# standby 10 timers 5 15
Router(config-if)# standby 10 authentication Secret
Router(config-if)# interface vlan21
Router(config-if)# standby 21 ip 192.20.100.21
Router(config-if)# standby 21 priority 108
Router(config-if)# standby 21 preempt
Router(config-if)# standby 21 timers 5 15
Router(config-if)# standby 21 authentication Secret
Router(config-if)# ^Z
Router# ^C^C^C

Console> (enable) switch console 16
Trying Router-16...
Connected to Router-16.
Type ^C^C^C to switch back...
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface vlan10
Router(config-if)# standby 10 ip 172.20.100.10
Router(config-if)# standby 10 priority 109
Router(config-if)# standby 10 preempt
Router(config-if)# standby 10 timers 5 15
Router(config-if)# standby 10 authentication Secret
Router(config-if)# interface vlan21
Router(config-if)# standby 21 ip 192.20.100.21
Router(config-if)# standby 21 priority 107
Router(config-if)# standby 21 preempt
Router(config-if)# standby 21 timers 5 15
Router(config-if)# standby 21 authentication Secret
Router(config-if)# ^Z
Router# ^C^C^C
```

次に、スイッチ S2 の MSFC 上に HSRP を設定する例を示します。

```
Console> (enable) switch console 15
Trying Router-15...
Connected to Router-15.
Type ^C^C^C to switch back...
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface vlan10
Router(config-if)# standby 10 ip 172.20.100.10
Router(config-if)# standby 10 priority 108
Router(config-if)# standby 10 preempt
Router(config-if)# standby 10 timers 5 15
Router(config-if)# standby 10 authentication Secret
Router(config-if)# interface vlan21
Router(config-if)# standby 21 ip 192.20.100.21
Router(config-if)# standby 21 priority 110
Router(config-if)# standby 21 preempt
Router(config-if)# standby 21 timers 5 15
Router(config-if)# standby 21 authentication Secret
Router(config-if)# ^Z
Router# ^C^C^C

Console> (enable) switch console 16
Trying Router-16...
Connected to Router-16.
Type ^C^C^C to switch back...
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface vlan10
Router(config-if)# standby 10 ip 172.20.100.10
Router(config-if)# standby 10 priority 107
Router(config-if)# standby 10 preempt
Router(config-if)# standby 10 timers 5 15
Router(config-if)# standby 10 authentication Secret
Router(config-if)# interface vlan21
Router(config-if)# standby 21 ip 192.20.100.21
Router(config-if)# standby 21 priority 109
Router(config-if)# standby 21 preempt
Router(config-if)# standby 21 timers 5 15
Router(config-if)# standby 21 authentication Secret
Router(config-if)# ^Z
Router# ^C^C^C
```

MSFC 設定同期化の概要

MSFC ハイ アベイラビリティにより、メイン MSFC（最初にオンラインになる MSFC、またはオンライン時間が最も長い MSFC）と、非メイン MSFC との間で、スタートアップ コンフィギュレーションおよび実行コンフィギュレーションを自動的に同期化することができます。ハイ アベイラビリティ冗長機能は、デフォルトではディセーブルです。

注意　設定同期化がサポートされているのは、IP および IPX コンフィギュレーションに対してだけです。同期化をイネーブルにする前に、両方の MSFC がすべてのプロトコルについて同じ設定を持つようにする必要があります。AppleTalk、DECnet、VINES、またはその他のルーティングを使用している場合は、両方の MSFC ですべてのプロトコルについて同じ設定を持つように手動で設定する必要があります。

メイン MSFC のステータスを判別するには、**show fm features** コマンドまたは **show redundancy** コマンドを使用します。

```
Router-15# show redundancy
Designated Router: 1 Non-designated Router:2

Redundancy Status: non-designated
Config Sync AdminStatus  : enabled
Config Sync RuntimeStatus: enabled

Router-16# show redundancy
Designated Router: 1 Non-designated Router:2

Redundancy Status: designated
Config Sync AdminStatus  : enabled
Config sync RuntimeStatus: enabled
```

ハイ アベイラビリティ冗長機能は、スタートアップ コンフィギュレーションおよび実行コンフィギュレーションを同期化します。

ハイ アベイラビリティ冗長機能をイネーブルにすると、メイン MSFC 上で次のいずれかのコマンドを入力した場合、両方の MSFC のスタートアップ コンフィギュレーションが更新されます。

- **write mem**
- **copy** *source* **startup-config**

ハイ アベイラビリティ冗長機能をイネーブルにすると、メイン MSFC 上で実行したすべてのコンフィギュレーション コマンドが、非メイン MSFC に送信されます。また、メイン MSFC 上で **copy** *source* **running-config** コマンドを入力すると、実行コンフィギュレーションの同期化が更新されます。

ここでは、MSFC 設定同期化について説明します。

- 設定同期化のステート（p.22-37）
- alt キーワードの使用方法（p.22-38）

設定同期化のステート

設定同期化には、次の 2 つのステートがあります。

- Config Sync AdminStatus ― ユーザが設定した機能が、ただちに反映されます。
- Config Sync RuntimeStatus ― 次の場合に限り、イネーブルになります。
  - ― メインおよび非メイン MSFC の両方で、Config Sync AdminStatus がイネーブルになっている場合
  - ― メインおよび非メイン MSFC が互換イメージを実行している場合

Config Sync RuntimeStatus がイネーブルの場合には、次の状態になります。

- 非メイン MSFC の CLI では、コンフィギュレーション モードを使用できません。EXEC モードは使用できます。
- **alt** キーワードが使用でき、必要になります（**alt** キーワードの詳細については、「alt キーワードの使用方法」[p.22-38] を参照）。
- 実行コンフィギュレーションとスタートアップ コンフィギュレーションが同期化されます。

Config Sync RuntimeStatus がディセーブルの場合には、次の状態になります。

- 両方の MSFC の CLI 上で、コンフィギュレーション モードを使用できます。
- **alt** キーワードを使用できますが、使用は任意です。
- 実行コンフィギュレーションとスタートアップ コンフィギュレーションは同期化されません。

各種のコンフィギュレーションおよび運用例は、「ハイ アベイラビリティ冗長機能の設定例」（p.22-39）を参照してください。

alt キーワードの使用方法

Config Sync RuntimeStatus がイネーブルの場合、非メイン MSFC 上では、EXEC モードだけは使用できますが、コンフィギュレーション モードは使用できません。両方の MSFC のコンフィギュレーションは、メイン MSFC のコンソールまたは Telnet セッション経由で行います。

単一コンソールから両方の MSFC を設定するには、**alt** キーワードを使用して、代替コンフィギュレーションを行うことを指定します。代替コンフィギュレーションを指定した場合、**alt** キーワードの前に入力したコンフィギュレーションはスイッチのスロット 1 のスーパバイザ エンジン上の MSFC に適用され、**alt** キーワードのあとに入力したコンフィギュレーションはスロット 2 のスーパバイザ エンジン上の MSFC に適用されます。

（注）　Config Sync AdminStatus をイネーブルにするときは、**alt** キーワードを入力する必要があります。

表 22-3 に、**alt** キーワードの含まれるインターフェイスおよびグローバル コンフィギュレーション コマンドを示します。

表 22-3　alt キーワードの含まれるインターフェイスおよびグローバル コンフィギュレーション コマンド

インターフェイス コンフィギュレーション コマンド	グローバル コンフィギュレーション コマンド
• [**no**] **standby** [*group_number*] **ip** [*ip_address* [**secondary**]] **alt** [**no**] **standby** [*group_number*] **ip** [*ip_address* [**secondary**]] • [**no**] **standby** [*group_number*] **priority** *priority* [**preempt** [**delay** *delay*]] **alt** [**no**] **standby** [*group_number*] **priority** *priority* [**preempt** [**delay** *delay*]] • [**no**] **ip address** *ip_address mask* [**secondary**] **alt** [**no**] **ip address** *ip_address mask* [**secondary**] • [**no**] **ipx network** *network* [**encapsulation** *encapsulation_type* [**secondary**]] [**alt** [**no**] **ipx network** *network* [**encapsulation** *encapsulation_type* [**secondary**]]]	• [**no**] **hostname** *hostname* **alt hostname** *hostname* • [**no**] **ip default-gateway** *ip_address* **alt** [**no**] **ip default-gateway** *ip_address* • **router bgp** *autonomous_system* **bgp router-id** *ip_address* [**alt** *ip_address*] • **router ospf** *process_id* **router-id** *ip_address* [**alt** *ip_address*]

次に、**ip address** コマンドでの **alt** キーワードの使用例を示します。

```
Router-1(config-if)# ip address 1.2.3.4 255.255.255.0 alt ip address 1.2.3.5
255.255.255.0
```

設定同期化のイネーブル化およびディセーブル化

ハイ アベイラビリティ冗長機能をイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	冗長機能をイネーブルにします。	**redundancy**
ステップ 2	ハイ アベイラビリティをイネーブルにします。	**high-availability**
ステップ 3	設定同期化をイネーブルまたはディセーブルにします。	[**no**] **config-sync**

次に、ハイ アベイラビリティ冗長機能および設定同期化をイネーブルにする例を示します（Router-15 がメイン MSFC です）。

```
Console>(enable) session 15
Trying Router-15...
Connected to Router-15.
Escape character is '^]'.

Router-15> enable
Router-15# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router-15(config)# redundancy
Router-15(config-r)# high-availability
Router-15(config-r-ha)# config-sync
Router-15(config-r-ha)# end
```

(注)　ハイ　アベイラビリティ冗長機能をイネーブルにすると、非メイン　MSFC　上のコンフィギュレーション モードはディセーブルになり、使用できるのは EXEC モードだけになります。

次の例では、Router-16 は非メイン MSFC です。ハイ アベイラビリティ冗長機能および設定同期化がイネーブルに設定されています。

```
Console>(enable) session 16
Trying Router-16...
Connected to Router-16.
Escape character is '^]'.

Router-16> enable
Router-16# configure terminal
Config mode is disabled on non-designated Router, please configure from designated
Router
```

ハイ アベイラビリティ冗長機能の設定例

ここでは、ハイ アベイラビリティおよび設定同期化をイネーブルにする例を、いくつか紹介します。

- 例 1：両方の MSFC 上で設定同期化をイネーブル化（p.22-39）
- 例 2：メイン MSFC 上で設定同期化をディセーブル化（p.22-43）
- 例 3：メイン MSFC をアップにする場合（p.22-43）
- 例 4：非メイン MSFC をアップにする場合（p.22-43）
- 例 5：メイン MSFC がダウンした場合（p.22-45）

例 1：両方の MSFC 上で設定同期化をイネーブル化

両方の MSFC がアップになっていることが前提です。

両方の MSFC の設定同期化をイネーブルにすると、最初にすべてのインターフェイス上の IP アドレスがチェックされます。メイン MSFC に IP アドレスが設定され、非メイン MSFC に指定されていないと、代替 IP アドレスが指定されていない最初のインターフェイスを示すメッセージが表示されます。

IP アドレスのチェックが終了すると、HSRP のアドレスがチェックされます。メイン MSFC に HSRP アドレスが設定され、非メイン MSFC に指定されていないと、代替 HSRP（スタンバイ）アドレスが指定されていない最初のインターフェイスを示すメッセージが表示されます。

HSRP アドレスのチェックが終了すると、IPX ネットワーク アドレスがチェックされます。

メイン MSFC を最初に設定します。次の例は、VLAN 1 インターフェイスの代替コンフィギュレーションが設定されていないことを示しています。

```
Router-16# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router-16(config)# redundancy
Router-16(config-r)# high-availability
Router-16(config-r-ha)# config-sync

Alternate IP address missing for Vlan1
The alternate configuration is missing. The auto-config sync can not be enabled
```

(注)　代替 IP コンフィギュレーションを指定する場合、**alt** キーワードの前に入力したコンフィギュレーションはスイッチのスロット 1 のスーパバイザ エンジン上の MSFC に適用され、**alt** キーワードのあとに入力したコンフィギュレーションはスロット 2 のスーパバイザ エンジン上の MSFC に適用されます。詳細については、「alt キーワードの使用方法」（p.22-38）を参照してください。

次に、VLAN 1 の代替コンフィギュレーションを指定する例を示します。

```
Router-16(config)# interface vlan 1
Router-16(config-if)# ip address 70.0.70.4 255.255.0.0 alt ip address 70.0.70.5
255.255.0.0
Router-16(config-if)# exit
```

次に、ハイ アベイラビリティ冗長機能を設定する例を示します。

```
Router-16(config)# redundancy
Router-16(config-r)# high-availability
Router-16(config-r-ha)# config-sync
Router-16(config-r-ha)# end
Router-16#
00:03:31: %SYS-5-CONFIG_I: Configured from console by console
```

非メイン MSFC の Config Sync AdminStatus がディセーブルになっているので、メイン MSFC の Config Sync RuntimeStatus はディセーブル モードのままです。メイン MSFC に、次のメッセージが表示されます。

```
00:17:05: %RUNCFGSYNC-6-SYNCEVENT:
Non-Designated Router is now online
High-Availability Redundancy Feature is not enabled on the Non-Designated Router
```

次に、非メイン MSFC 上で設定同期化をイネーブルにする例を示します。

```
Router-151(config)# redundancy
Router-15(config-r)# high-availability
Router-15(config-r-ha)# config-sync
Router-15(config-r-ha)# end
Router-15#
00:03:31: %SYS-5-CONFIG_I: Configured from console by console
```

(注)　ハイ アベイラビリティ冗長機能をイネーブルにすると、非メイン MSFC のコンソールのコンフィギュレーション モードはディセーブルになり、使用できるのは EXEC モードだけになります。

非メイン MSFC 上に、ハイ アベイラビリティ機能がイネーブルになり、コンフィギュレーション モードが自動的に終了することを示す、次のメッセージが表示されます。

```
00:18:57: %RUNCFGSYNC-6-SYNCEVENT:
The High-Availability Redundancy Feature is enabled
The config mode is no longer accessible

Router-15#

00:19:41: %RUNCFGSYNC-6-SYNCEVENT:
Non-Designated Router is now online
Running Configuration Synchronization will begin in 1 minute
```

非メイン MSFC を安定させるため、1 分間のタイマーがスタートします。タイマーが切れると、現在の実行コンフィギュレーションのスナップショットが非メイン MSFC に送信されます。実行コンフィギュレーションが同期化される前に、次のメッセージが表示されます。

```
00:20:41: %RUNCFGSYNC-6-SYNCEVENT:
Syncing Running Configuration to the Non-Designated Router

00:20:41: %RUNCFGSYNC-6-SYNCEVENT:
Syncing Startup Configuration to the Non-Designated Router
```

以下の例は、メイン MSFC と非メイン MSFC が同期化され、同じ実行コンフィギュレーションが設定されていることを示しています。

```
<designated MSFC>
Router-16# show running-config
Building configuration...

Current configuration:
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router-15 alt hostname Router-16
!
boot bootldr bootflash:c6msfc-boot-mz.120-7.XE1
!
ip subnet-zero
!
ip cef
redundancy
 high-availability
 config-sync
cns event-service server
!
!
!
interface Vlan1
 ip address 70.0.70.4 255.255.0.0 alt ip address 70.0.70.5 255.255.0.0
!
interface Vlan10
ip address 192.10.10.1 255.255.255.0 alt ip address 192.10.10.2 255.255.255.0
 no ip redirects
 shutdown
 standby ip 192.20.20.1 alt standby ip 192.20.20.1
!
ip classless
ip route 223.255.254.0 255.255.255.0 70.0.100.0
no ip http server
!
!
!
```

```
line con 0
 transport input none
line vty 0 4
 login
 transport input lat pad mop telnet rlogin udptn nasi
!
end


<nondesignated MSFC>
Router-15# show running-config
Building configuration...

Current configuration:
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router1 alt hostname Router2
!
boot bootldr bootflash:c6msfc-boot-mz.120-7.XE1
!
ip subnet-zero
!
ip cef
redundancy
 high-availability
 config-sync
cns event-service server
!
!
!
interface Vlan1
 ip address 70.0.70.4 255.255.0.0 alt ip address 70.0.70.5 255.255.0.0
!
interface Vlan10
ip address 192.10.10.1 255.255.255.0 alt ip address 192.10.10.2 255.255.255.0
 no ip redirects
 shutdown
 standby ip 192.20.20.1 alt standby ip 192.20.20.1
!
ip classless
ip route 223.255.254.0 255.255.255.0 70.0.100.0
no ip http server
!
!
!
line con 0
 transport input none
line vty 0 4
 login
 transport input lat pad mop telnet rlogin udptn nasi
!
end
```

例 2：メイン MSFC 上で設定同期化をディセーブル化

この例では、設定同期化がすでにイネーブルに設定されています。設定同期化をディセーブルにする例を示します。

```
Router-16# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router2(config)# redundancy
Router2(config-r)# high-availability
Router2(config-r-ha)# no config-sync
```

設定同期化をディセーブルにすると、非メイン MSFC 上に次のメッセージが表示されます。

```
00:13:00: %RUNCFGSYNC-6-SYNCEVENT:
The High-Availability Redundancy Feature is now disabled
The config mode is now accessible
```

メインおよび非メイン MSFC の両方で、CLI のコンフィギュレーション モードを使用することができます。

例 3：メイン MSFC をアップにする場合

この例では、Config Sync AdminStatus がすでにイネーブルに設定されています。メイン MSFC は代替コンフィギュレーションを検証し、非メイン MSFC がアップになった時点で、コンフィギュレーションを同期化します。

非メイン MSFC はまだアップになっていないので、Config Sync RuntimeStatus はディセーブルです。したがって、設定同期化は実行されません。非メイン MSFC の情報については、「例 4：非メイン MSFC をアップにする場合」（p.22-43）を参照してください。

次の例では、Router-16 がメイン MSFC です。Config Sync AdminStatus はイネーブル、Config Sync RuntimeStatus はディセーブルに設定されています。

```
Router-16# show redundancy
Designated Router: 1 Non-designated Router:0

Redundancy Status: designated
Config Sync AdminStatus  : enabled
Config Sync RuntimeStatus: disabled
```

例 4：非メイン MSFC をアップにする場合

Config Sync AdminStatus がイネーブルの場合

この例では、非メイン MSFC がメイン MSFC に対して、非メイン MSFC がアップになり、Config Sync AdminStatus がイネーブルになったことを通知しています。メイン MSFC は非メイン MSFC に、Config Sync RuntimeStatus をイネーブルにするように要求しています。非メイン MSFC の Config Sync RuntimeStatus がイネーブルになります。

非メイン MSFC には、次のメッセージが表示されます。

```
00:00:07: %RUNCFGSYNC-6-SYNCEVENT:
The High-Availability Redundancy Feature is enabled
The config mode is no longer accessible

00:00:51: %RUNCFGSYNC-6-SYNCEVENT:
Non-Designated Router is now online
Running Configuration Synchronization will begin in 1 minute
```

非メイン MSFC を安定させるため、1 分間のタイマーがスタートします。タイマーが切れると、現在の実行コンフィギュレーションのスナップショットが非メイン MSFC に送信されます。実行コンフィギュレーションが同期化される前に、次のメッセージが表示されます。

```
00:01:51: %RUNCFGSYNC-6-SYNCEVENT:
Syncing Running Configuration to the Non-Designated Router
```

Config Sync AdminStatus がディセーブルの場合

この例では、非メイン MSFC がメイン MSFC に対し、アップになったことを通知しています。非メイン MSFC の Config Sync AdminStatus はディセーブルなので、メイン MSFC に、非メイン MSFC のハイ アベイラビリティ冗長機能をイネーブルにする必要があることを示す次のメッセージが表示されます。

```
Router-16#
Non-Designated Router came up.
High-Availability Redundancy Feature is not enabled on the Non-Designated Router
```

次に、非メイン MSFC 上で、ハイ アベイラビリティ冗長機能をイネーブルにする例を示します。

```
Router-15# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router-15(config)# redundancy
Router-15(config-r)# high-availability
Router-15(config-r-ha)# config-sync
Router-15(config-r-ha)#
00:03:47: %SYS-5-CONFIG_I: Configured from console by console
00:03:47: %RUNCFGSYNC-6-SYNCEVENT:
The High-Availability Redundancy Feature is enabled
The config mode is no longer accessible

00:00:51: %RUNCFGSYNC-6-SYNCEVENT:
Non-Designated Router is now online
Running Configuration Synchronization will begin in 1 minute
```

非メイン MSFC を安定させるため、1 分間のタイマーがスタートします。タイマーが切れると、現在の実行コンフィギュレーションのスナップショットが非メイン MSFC に送信されます。実行コンフィギュレーションが同期化される前に、次のメッセージが表示されます。

```
00:01:51: %RUNCFGSYNC-6-SYNCEVENT:
Syncing Running Configuration to the Non-Designated Router
```

次の例は、メイン MSFC および非メイン MSFC 上の Config Sync AdminStatus および Config Sync RuntimeStatus がイネーブルに設定されていることを示しています。

```
Router-15# show redundancy
Designated Router: 1 Non-designated Router:2

Redundancy Status: non-designated
Config Sync AdminStatus  : enabled
Config Sync RuntimeStatus: enabled


Router-16# show redundancy
Designated Router: 1 Non-designated Router:2

Redundancy Status: designated
Config Sync AdminStatus  : enabled
Config sync RuntimeStatus: enabled
```

例 5：メイン MSFC がダウンした場合

この例では、非メイン MSFC がメイン MSFC に切り替わります。設定の同期化がディセーブルになり、CLI でのコンフィギュレーション モードが利用できるようになります。

元のメイン MSFC を再びアップにすると、この MSFC は非メイン MSFC になります。「例 4：非メイン MSFC をアップにする場合」（p.22-43）を参照してください。

SRM の冗長機能

ここでは、SRM 冗長機能の設定手順について説明します。

SRM 冗長機能は、両方の MSFC2 が同時にアクティブな内部冗長（デュアル）MSFC2 コンフィギュレーションに代わるものです。SRM 冗長機能では、ネットワークから見えるのは常に指定ルータのみです。非指定ルータは完全に起動され、SRM 開始時にイネーブルに自動設定される設定同期化に参加します。SRM では、[alt] キーワード以後のコンフィギュレーションはすべて無視されます。したがって、非指定ルータの設定は指定ルータのものとまったく同じですが、そのインターフェイスは回線ダウン ステートのままでネットワークからは見えません。ルーティング プロトコルなどのプロセスは、非指定および指定ルータ上で作成されますが、非指定ルータのインターフェイスはすべて回線ダウン ステートにあります。このためネットワークからのアップデートの送受信は行いません。

指定ルータに障害が発生すると、非指定ルータは、非指定ルータから指定ルータにステートを変更し、そのインターフェイスのステートがリンク アップに変わります。新しい指定ルータは、既存のスーパバイザ エンジン スイッチ プロセッサ エントリを使用してレイヤ 3 トラフィックを転送しながら、ルーティング テーブルを構築します。スイッチ プロセッサは引き続き古いエントリを使用して、レイヤ 3 パケットを転送します。事前に定義された時間が経過したあと、新規の指定ルータは新しいレイヤ 3 スイッチング情報をスイッチ プロセッサにダウンロードします。

（注） Cisco IOS Release 12.1(11b)E 以降のリリースでは、新しい指定ルータがスーパバイザ エンジンのスイッチ プロセッサに新しいレイヤ 3 スイッチング情報をダウンロードする前に待機する移行時間を指定できます。設定の詳細については、「新しいアクティブ指定ルータに対する移行時間の指定」（p.22-49）を参照してください。

ハードウェアおよびソフトウェアの要件

SRM 冗長機能を設定するには、次のハードウェアおよびソフトウェアが必要です。

- 2 つの同一スーパバイザ エンジン ドータカードから構成される 1 つのシャーシ
  - PFC3B/PFC3BXL および MSFC2A 搭載の Supervisor Engine 32
  - PFC3A/PFC3B/PFC3BXL および MSFC3 搭載の Supervisor Engine 720
  - PFC2 および MSFC2 搭載の Supervisor Engine 2
  - PFC および MSFC または MSFC2 搭載の Supervisor Engine 1

（注） Cisco IOS Release 12.1(8a)E4 は、Supervisor Engine 1 および MSFC を使用する SRM 冗長構成の初期サポートを提供します。

（注） **マルチキャスト サポート：**Release 7.1(1) より前のソフトウェア リリースでは、MSFC または MSFC2 搭載の Supervisor Engine 1 を SRM 冗長構成で使用する場合、2 番めの MSFC へのフェールオーバーがマルチキャスト MLS に関してステートフルにならない点に注意してください。プライマリ MSFC でエラーが発生すると、すべてのマルチキャスト MLS エントリが削除され、新しくアクティブになった MSFC によって再作成されて再インストールされます。

（注） **マルチキャスト サポート：**Release 7.1(1) 以降のソフトウェア リリースでは、PFC および MSFC2 搭載の Supervisor Engine 1 および PFC2 および MSFC2 搭載の Supervisor Engine 2 に関して、マルチキャスト トラフィックの SRM 冗長性サポートが改善されています。マルチキャストに関する改善は、MSFC 搭載の Supervisor Engine 1 には当てはまりません。

SRM 冗長機能をイネーブルにすると、コンバージェンス タイムが向上し、切り替え時のマルチキャスト トラフィックの停止が短縮されます。MSFC2 は、切り替え時にマルチキャスト トラフィックで過負荷にならないように保護されます。スイッチは停止した MSFC2 からのフローをキャッシュし、新しくアクティブになった MSFC2 がルータを認識するまで、キャッシュのフローを使用してトラフィックを転送します。一度に少数のフローだけが MSFC2 に与えられるので、あふれることはありません。

- Release 6.3(1) 以降のスーパバイザ エンジン ソフトウェア リリース（Supervisor Engine 720 では Release 8.1(1) 以降のスーパバイザ エンジン ソフトウェア リリース、Supervisor Engine 32 では Release 8.4(1) 以降のスーパバイザ エンジン ソフトウェア リリースが必要）
- Cisco IOS Release12.1(8a)E2 以降（Supervisor Engine 720 MSFC3 では、Cisco IOS Release12.2(14)SX2 以降が必要）

SRM 冗長性設定時の注意事項

ここでは、SRM 冗長性設定時の注意事項について説明します。

- 指定ルータおよび非指定ルータが同じ Cisco IOS イメージを実行している必要があります。
- 指定ルータおよび非指定ルータの両方のブートフラッシュに、Cisco IOS イメージが必要です。
- 非指定ルータは外部ネットワークに接続できません。
- 外部ネットワークから指定ルータで起動しないでください。外部ネットワークから起動すると、SRM の機能が大幅に低下します。
- SRM 冗長機能を使用すると、指定ルータは外部ネットワークにアクセスし、**copy tftp:** などのコピー コマンドを制約なしで使用できます。
- スーパバイザ エンジン上でハイ アベイラビリティをイネーブルに設定する必要があります。
- RADIUS や TACACS+ などの認証方式を使用してスイッチへのアクセスを制御する場合、**switch console** または **session** コマンドで非指定ルータにアクセスできるようにするときは、フォールバック オプションを設定してローカルのユーザ名とパスワードでログインする必要があります。

  フォールバック オプションの設定手順については、第 38 章「AAA によるスイッチ アクセスの設定」を参照してください。

Supervisor Engine 720 における SRM 冗長機能の設定

（注） SRM の冗長機能は、Supervisor Engine 720 および Supervisor Engine 32 でサポートされる唯一の MSFC 冗長機能オプションです。

Supervisor Engine 720 および Supervisor Engine 32 では、MSFC で SRM を明示的にイネーブルにする必要はありません。SRM はデフォルトでイネーブルです。SRM が正常に動作しているか判断するため、両方の MSFC が同一のスタートアップ コンフィギュレーションを保有していることを確認する必要があります。

1. システムをリセットしてリロードしたあと、**write erase** コマンドを非メイン MSFC 上で実行し、非メイン MSFC をリロードします。
2. システムをリセットしてリロードしたあと、**show redundancy** コマンドを入力して、SRM ランタイム ステータスがイネーブルであることを確認します。SRM ランタイム ステータスがイネーブルであることを確認したあと、**write memory** コマンドをメイン MSFC 上で実行し、非メイン MSFC をリロードします（非メイン MSFC の設定をリロード プロンプトで保存しないでください）。

ヒント 非メイン MSFC がメイン MSFC と同じ設定で起動する場合は、第 2 の方法を推奨します。その方が、予期しない問題が発生する可能性が小さくなります。

（注） システム起動時に、非メイン MSFC のスタートアップ コンフィギュレーションにメイン MSFC 設定にはない設定項目があった場合、MSFC は実行コンフィギュレーションで一貫性がなくなります。上記の 2 つの手順により、非メイン MSFC が常に MSFC と同じ実行コンフィギュレーションを持つことができます。

Supervisor Engine 1 または Supervisor Engine 2 における SRM 冗長機能の設定

SRM 冗長機能を設定するには、次の手順を実行します。

注意 デュアル ルータ モードから SRM 冗長機能に移行する前に、MSFC の **copy running-config** コマンドを使用し、非 SRM コンフィギュレーションをブートフラッシュに保存するようにしてください。SRM 冗長機能に移行すると、代替コンフィギュレーション（**alt** キーワードのあとのコンフィギュレーション）は失われます。SRM 冗長機能をイネーブルにする前に、両方の MSFC に **copy running-config bootflash:***nosrm_dual_router_config* コマンドを入力し、デュアル ルータ モード コンフィギュレーションをブートフラッシュに保存してください。

詳細については、「SRM の終了」（p.22-51）を参照してください。

（注） この手順は、指定ルータがスロット 1 に搭載の MSFC2 で、非指定ルータがスロット 2 に搭載の MSFC2 であり、さらにアクティブ スーパバイザ エンジンはスロット 1 にあり、スタンバイ スーパバイザ エンジンはスロット 2 にあると仮定しています。

ステップ 1　**show version** コマンドを使用して、両方のスーパバイザ エンジンが、スーパバイザ エンジン Release 6.3(1) 以降のソフトウェア リリースを実行していることを確認します。

ステップ 2　**set system highavailability enable** コマンドを使用して、アクティブ スーパバイザ エンジン上でハイ アベイラビリティ機能をイネーブルにします。**show system highavailability** コマンドを使用して、ハイ アベイラビリティ機能がイネーブルになっていることを確認します。

ステップ 3　コンソール接続を行っている場合は、**switch console** コマンドを使用して指定ルータにアクセスします。Telnet セッションを使用して接続している場合は、**session** *mod* コマンドを使用して指定ルータにアクセスします。

ステップ 4　Cisco IOS Release 12.1(8a)E2 以降のイメージを指定ルータおよび非指定ルータのブートフラッシュにコピーします。

ステップ 5　指定ルータおよび非指定ルータに対してブート イメージとコンフィギュレーション レジスタを設定して、リロード時に新しいイメージを起動します。

指定ルータの場合は、**boot system flash bootflash:***image_name* コマンドを使用してこのイメージがブート リストの最初にあることを確認します。**boot system** コマンドの **no** 形式を使用して、実行コンフィギュレーションに表示されている（**show running-config**）すべての既存の **boot system** コマンドを削除します。

非指定ルータの場合は、**config-register 0x102** コマンドを入力して、自動起動するようにコンフィギュレーション レジスタを設定します。

（注）　SRM 対応 Cisco IOS イメージがロード済みの場合、ステップ 6 の手順は不要です。

ステップ 6　**reload** コマンドを使用して、指定ルータおよび非指定ルータをリロードします。

ステップ 7　コマンドの **no** 形式を入力して、指定ルータ上で設定の同期化（**config-sync**）をディセーブルにします。**write memory** コマンドを入力します。これにより、指定ルータと非指定ルータの両方でコンフィギュレーション モードにアクセスできるようになります。

ステップ 8　最初に指定ルータ上で SRM をイネーブルにしてから、次のように非指定ルータ上で SRM をイネーブルにします。

```
Router(config)#redundancy
Router(config-r)#high-availability
Router(config-r-ha)#single-router-mode
```

（注）　Cisco IOS Release 12.1(11b)E 以降のリリースでは、新しい指定ルータがスーパバイザ エンジンのスイッチ プロセッサに新しいレイヤ 3 スイッチング情報をダウンロードする前に待機する移行時間を指定できます。設定の詳細については、「新しいアクティブ指定ルータに対する移行時間の指定」（p.22-49）を参照してください。

ステップ 9　指定ルータ上で **write memory** コマンドを実行し、非指定ルータのスタートアップ コンフィギュレーションが SRM をイネーブルに設定していることを確認します。

ステップ 10 非指定ルータ上で **show startup-config** コマンドを実行し、非指定ルータが次のコンフィギュレーション ステートメントを持っていることを確認します。

```
redundancy
 high-availability
 single-router-mode
```

ステップ 11 指定ルータおよび非指定ルータ上で **show redundancy** コマンドを実行し、いずれのルータにも次のコンフィギュレーション ステートメントがあることを確認します。

```
Single Router Mode RuntimeStatus: enabled
```

ない場合は、ステップ 9 および 10 をステップ間で十分な時間を取りながら繰り返します。

ステップ 12 **reload** コマンドを使用して、非指定ルータをリロードします。設定を保存するかどうかの問い合せには、**no** を入力します。

次の出力は、SRM 冗長機能をイネーブルにするために指定ルータおよび非指定ルータに対して使用したコンフィギュレーション コマンドの要約です。

```
Time   Designated Router                      Nondesignated Router
  ----   ---                                   ----
  t0:    conf t->red->hi->no config-sync
  t1:                                          conf t->red->hi->no config-sync
  t2:    conf t->red->hi->single-router-mode
  t3:                                          conf t->red->hi->single-router-m
  t4:    write mem
  t5:                                          reload
```

新しいアクティブ指定ルータに対する移行時間の指定

Release 12.1(11b)E より前の Cisco IOS リリースでは、移行時間は 120 秒に定められ、ユーザは設定できませんでした。ルーティング コンバージェンス時間が異なるので、120 秒では足りないことがあります。古いレイヤ 3 スイッチング エントリは消去され、新たにダウンロードしたレイヤ 3 スイッチング情報が不完全なことがあります。

Cisco IOS Release 12.1(11b)E 以降のリリースでは、新しい指定ルータがスイッチ プロセッサに新しいレイヤ 3 スイッチング情報をダウンロードする前に待機する移行時間を指定できます。切り替え時には、スイッチ プロセッサに新しいレイヤ 3 スイッチング情報がダウンロードされる前に、設定した秒数の間、古いレイヤ 3 スイッチング情報が使用されます。

ノンストップの転送が必要な場合、移行時間をデフォルト値（120 秒）より小さい値に設定することは推奨できません。ルートのコンバージェンスには最低限 30 ～ 60 秒かかります。

移行時間を指定するには、以下のコマンドを入力します（この例では移行時間は 240 秒に設定されています）。

```
Router(config)#redundancy
Router(config-r)#high-availability
Router(config-r-ha)#single-router-mode
Router(config-r-ha)#single-router-mode failover ?
   table-update-delay  Adjust for routing convergence time
Router(config-r-ha)#single-router-mode failover table-update-delay ?
   <0-4294967295>  Delay in seconds between switch over detection and h/w FIB reload
Router(config-r-ha)#single-router-mode failover table-update-delay 240
Router(config-r-ha)#
```

移行時間をデフォルトの 2 分に設定する場合は、次のように、このコマンドの **no** 形式を使用します。

```
Router(config-r-ha)#no single-router-mode failover table-update-delay
```

移行時間を表示するには、次のようにします。

```
Router-16#show redundancy
 Designated Router: 2 Non-designated Router: 1

 Redundancy Status: designated

 Config Sync AdminStatus  : enabled

 Config Sync RuntimeStatus: enabled

 Single Router Mode AdminStatus  : enabled

 Single Router Mode RuntimeStatus: enabled

 Single Router Mode transition timer : 240 seconds    <---- 移行時間

Router-16#
```

SRM をイネーブルに設定したイメージのアップグレード

ここでは、SRM の稼働時にアクティブおよびスタンバイ MSFC 上で Cisco IOS イメージをアップグレードする方法について説明します。新しいイメージの名前は c6msfc2-jsv-mz.9E です。スタンバイ MSFC は TFTP でイメージをロードすることはできませんが、スーパバイザ エンジン フラッシュ PC カード（sup-slot0:）からイメージをロードすることができます。

（注） この手順はデータ トラフィックに影響します。スケジュールされているメンテナンス ウィンドウで実行することを推奨します。

イメージをアップグレードする手順は、次のとおりです。

ステップ 1　アクティブ スーパバイザ エンジン上で、**copy tftp sup-slot0:** コマンドを実行し、表示されるプロンプトに従って新しい（c6msfc2-jsv-mz.9E）イメージをスーパバイザ エンジン フラッシュ PC カードにロードします。

ステップ 2　コンソール接続を行っている場合は、**switch console** コマンドを使用してアクティブ MSFC にアクセスします。Telnet セッションを使用して接続している場合は、**session** *mod* コマンドを使用してアクティブ MSFC にアクセスします。

ステップ 3　アクティブ MSFC 上で、スーパバイザ エンジン フラッシュ PC カードから新しいイメージを MSFC ブートフラッシュにコピーします。

```
copy sup-slot0:c6msfc2-jsv-mz.9E bootflash:c6msfc2-jsv-mz.9E
```

ステップ 4　スタンバイ MSFC にアクセスするには、**switch supervisor** コマンドを入力し、そのあとにアクティブ スーパバイザ エンジンに **switch console** コマンドを入力します。

(注)　スタンバイ MSFC は、アクティブ スーパバイザ エンジンから発行された **show module** コマンドの出力には表示されません。

ステップ 5　スタンバイ MSFC 上で、スーパバイザ エンジン フラッシュ PC カードから新しいイメージを MSFC ブートフラッシュにコピーします。

```
copy sup-slot0:c6msfc2-jsv-mz.9E bootflash:c6msfc2-jsv-mz.9E
```

ステップ 6　アクティブ MSFC 上で、MSFC のリロード時に新しいイメージを起動するように指定します。

```
boot system flash bootflash:c6msfc2-jsv-mz.9E
```

ステップ 7　アクティブ MSFC 上で、**write memory** コマンドを実行して、スタンバイ MSFC スタートアップ コンフィギュレーションが起動情報を取得していることを確認します。

ステップ 8　**reload** コマンドを実行して、スタンバイ MSFC をリロードします。

ステップ 9　アクティブおよびスタンバイ MSFC 上で **show redundancy** コマンドを実行し、ともに次のコンフィギュレーション ステートメントを持っていることを確認します。

```
Single Router Mode RuntimeStatus: enabled
```

ステップ 10　**reload** コマンドを実行して、アクティブ MSFC をリロードします。

これで、どちらの MSFC も c6msfc2-jsv-mz.9E イメージを実行している状態になります。

SRM の終了

(注)　SRM 冗長機能を設定する前に、デュアル ルータ モードで使用される実行コンフィギュレーションのコピーを保存した場合は、以下に記載する手順を実行する必要はありません。SRM 冗長機能を終了してデュアル ルータ モードに戻るには、両方の MSFC 上で **copy bootflash:***nosrm_dual_router_config startup-config* コマンドを入力します。コンフィギュレーションのコピー後、**reload** コマンドで MSFC をリロードします。

SRM を終了する手順は、次のとおりです。

ステップ 1　指定ルータ上で、コマンドの **no** 形式を入力して SRM をディセーブルにします。

```
Router(config)#redundancy
Router(config-r)#high-availability
Router(config-r-ha)#no single-router-mode
```

ステップ 2　指定ルータおよび非指定ルータ上で **write memory** コマンドを実行します。

ステップ 3　指定ルータおよび非指定ルータ上で **show startup-config** コマンドを実行し、スタートアップ コンフィギュレーションに [single-router mode] がないことを確認します。

ステップ 4　**reload** コマンドを実行して、指定ルータおよび非指定ルータをリロードします。

これで、指定ルータおよび非指定ルータ上で SRM がディセーブルの状態になります。

手動モード MSFC 冗長機能

(注)　SRM 機能を含む Release 6.3(1) スーパバイザ エンジン ソフトウェア リリースの投入により、手動モード MSFC 冗長機能のサポートは 2002 年 12 月までとなります。手動モード MSFC 冗長機能ではなく SRM を使用することを推奨します。この場合、機能のサポートに期限はなく、また、自動レイヤ 3 フェールオーバー機能も得られます。

ここでは、一方の MSFC をアクティブに、もう一方の MSFC を ROM モニタ モードにした状態で冗長 MSFC を設定する方法について説明します。

ハードウェアおよびソフトウェアの要件

レイヤ 3 の冗長機能を設定するには、少なくとも次のいずれかの構成が必要です。

- 2 つの同一スーパバイザ エンジン ドータカードから構成される 1 つのシャーシ
  - PFC および MSFC または MSFC2 搭載の Supervisor Engine 1（両方のスーパバイザ エンジンに同一タイプの MSFC を搭載することが必要）
  - PFC2 および MSFC2 搭載の Supervisor Engine 2
- それぞれスーパバイザ エンジンを搭載したシャーシ ― 各シャーシに少なくとも 1 つはスーパバイザ エンジンを搭載しておく必要があります。各スーパバイザ エンジンに、PFC および MSFC を取り付けておく必要があります。
- 手動モード MSFC 冗長機能では、次のソフトウェアが必要です。
  - Release 6.1(3) 以降のスーパバイザ エンジン ソフトウェア リリースおよび Cisco IOS Release 12.1(7)E 以降のリリース
  - Release 5.5.8 以降のスーパバイザ エンジン ソフトウェア リリースおよび Cisco IOS Release 12.1(7a)E1 以降のリリース

(注)　各 MSFC は、同じ Cisco IOS ソフトウェア リリースを実行している必要があります。

手動モード MSFC 冗長機能設定時の注意事項

ここでは、手動モード MSFC 冗長機能設定時の注意事項について説明します。

- MSFC の切り替えは手動なので、外部冗長ルータが存在する環境、および HSRP が使用されているか、何らかの形式のゲートウェイ検出がホスト上に実装されている環境でのみ手動モード MSFC 冗長機能を使用することを推奨します。
- アクティブ MSFC（MSFC-15）上のコンフィギュレーション レジスタが 0x2102 に、ROM モニタ モードの MSFC（MSFC-16）上のコンフィギュレーション レジスタが 0x0 に設定されていることを確認します。この設定により、両方の MSFC が同時にアクティブになるのを防止し、アクティブ MSFC をリセット後にオンラインにすることができます。コンフィギュレーション レジスタの設定の詳細については、「MSFC コンフィギュレーション レジスタの設定」（p.22-54）を参照してください。

（注） 両方の MSFC を 0x0 に設定することはオプションとしてサポートされていますが、スイッチをリセットする場合はユーザによる設定が必要です。

- IP アドレスの領域を保護し、レイヤ 3 の全体的な複雑性を緩和するには、両方の MSFC 上で設定同期化をディセーブルにし、すべての [alt] アドレスを削除するようにします。alt アドレスが使用されていると、IP アドレス領域が保護されず、（BGP などの）リンクレベルのピアリングが存在する場合にレイヤ 3 の複雑性が増します。
- メンテナンス ウィンドウで ROM モニタ モードの MSFC を起動した場合、アクティブ MSFC と完全に同じ設定かどうかを確認してください。表 22-2（p.22-23）に記載されている設定時の注意事項を参照してください。
- 手動モード MSFC 冗長機能の間、スーパバイザ エンジン上でハイ アベイラビリティをイネーブルにして、MSFC 切り替え実行時のレイヤ 2 ダウンタイムを最小限に抑えます。ハイ アベイラビリティはプロトコル フィルタリング、ポート セキュリティ、Dynamic VLAN（DVLAN）、Generic Attribute Registration Protocol（GARP）VLAN Registration Protocol（GVRP）には対応していないので、手動モード MSFC 冗長機能使用時は、これらの機能をディセーブルに設定することを推奨します。
- 両方のスーパバイザ エンジン上のコンソール ポートに運用担当者がアクセスできるようにします（端末サーバまたはモデムによる帯域外アクセス）。

（注） ここでの手順は、**switch console** コマンドを使用してスーパバイザ エンジンから MSFC にアクセスします。Telnet セッションでは、**switch console** コマンドはサポートされていません。

スタンバイ MSFC のアクセス

スタンバイ MSFC にアクセスするには、**switch supervisor** コマンドを入力し、そのあとに **switch console** コマンドを入力します。

（注） スタンバイ MSFC は、アクティブ スーパバイザ エンジンから発行された **show module** コマンドの出力には表示されません。

手動による MSFC の起動

両方の MSFC のコンフィギュレーション レジスタが 0x0 に設定されている場合、MSFC 手動モードでは、スイッチをリセットするたびに MSFC を手動で起動する必要があります。MSFC を手動で起動するには、次の作業を行います。

ステップ 1　**switch console** コマンドを使用して MSFC ROMMON プロンプトにアクセスします。

ステップ 2　**boot bootflash:***image* コマンドを入力します。

ステップ 3　MSFC の起動後、Router> プロンプトに **Ctrl-C** を 3 回入力すると、スーパバイザ エンジン プロンプトに戻ります。**session** コマンドを実行して、MSFC にアクセスします。

MSFC コンフィギュレーション レジスタの設定

手動モード MSFC 冗長機能では、次のようにコンフィギュレーション レジスタを設定します。

ステップ 1　アクティブ MSFC（MSFC-15）上で Cisco IOS コンフィギュレーション モードから、**config-register 0x2102** コマンドを入力します。

ステップ 2　ROM モニタ モードの MSFC（MSFC-16）上で、**config-register 0x0** コマンドを入力します。

（注）　両方の MSFC コンフィギュレーションの **boot** システム コマンドがブートフラッシュの有効なイメージをポイントするようにし、かつ、これらの **boot** コマンドを無視するようにはコンフィギュレーション レジスタを設定しないことを推奨します。

MSFC 回復手順

ここでは、一時的または永続的な MSFC 障害から回復する手順について説明します。

アクティブ MSFC の一時的な障害が発生した場合、コンフィギュレーション レジスタが 0x2102 に設定されているため、MSFC が再起動します。

永続的な障害の疑いがあるアクティブな MSFC は確認する必要があります。それには、アクティブ スーパバイザ エンジンのコンソール ポートから **reset 15** コマンドを実行し、アクティブ MSFC が正常に再起動するかどうかを確認します。再起動しない場合は、次の 2 つの方法でスタンバイ MSFC に切り替えることができます。

方法 1：スイッチに物理的にアクセスする場合

スイッチに物理的にアクセスする場合は、この方法を使用します。問題のある MSFC を装備しているアクティブ スーパバイザ エンジンを取り外すことにより、冗長スーパバイザ エンジンが動作を引き継ぎます。冗長スーパバイザ エンジンの物理コンソール ポートで、次の手順を実行します。

ステップ 1　**switch console** コマンドを実行します。

ステップ 2　ROMMON プロンプトで、**boot bootflash:***image* コマンドを実行します。

ステップ 3　スタンバイ MSFC の起動後、Cisco IOS コンフィギュレーション モードで **config-register 0x2102** コマンドを実行して、スイッチのリセット時に MSFC が起動するようにします。

方法 2：スイッチにリモート アクセスだけが可能な場合

スイッチにリモート アクセスしかできない場合は、この方法を使用します。問題のある MSFC を装備しているアクティブ スーパバイザ エンジンで、次の手順を実行します。

（注）　問題のある MSFC がスタンバイ スーパバイザ エンジン上にある場合は、**switch supervisor** コマンドを実行します。

ステップ 1　**switch console** コマンドを実行します。

ステップ 2　ブレーク信号を送信して問題のある MSFC の ROMMON に入ります（ブレークが有効なのは MSFC が引き続き再起動している場合に限ります）。システムのブートストラップ メッセージが出力されてから、メイン Cisco IOS イメージが解凍されるまでの間に発行されるように、ブレークのタイミングを決める必要があります（次の出力の 2 つの矢印を参照）。

```
System Bootstrap, Version 12.0(3)XE, RELEASE SOFTWARE
Copyright (c) 1998 by cisco Systems, Inc.
Cat6k-MSFC platform with 131072 Kbytes of main memory <======= ISSUE BREAK AFTER THIS
POINT


Self decompressing the image :
########################################################################################
[OK]

<==========BUT BEFORE THIS POINT

Self decompressing the image :
########################################################################################
########################################################################################
########################################################################################
########################################################################################
########################################################################################
########################################################################################
########################################################################################
########################################################################################
################################### [OK]
```

ステップ 3　ROMMON プロンプトで、**confreg** コマンドを入力します。

a.　[do you wish to change the configuration? y/n [n]:] のプロンプトに、**y** と入力します。

b.　**Enter** を押してすべての質問に対してデフォルトの設定を受け入れると、次のプロンプトが表示されます。[change the boot characteristics? y/n [n]:]

c.　**y** と入力します。

d. **0** と入力して、次のプロンプトで 0 = ROM Monitor オプションを選択します。

e. Configuration Summary を調べて、boot:the ROM Monitor の値を確認します。

f. 再度、[do you wish to change the configuration? y/n [n]:] というプロンプトが表示されます。

g. **n** と入力します。

h. ROMMON プロンプトに戻ります。

ステップ 4　**reset** コマンドを実行して、MSFC が ROMMON で起動していることを確認します。このステップにより、この MSFC とアクティブ MSFC が同時に起動しないようになります。

ステップ 5　**Ctrl-C** を 3 回入力して、スーパバイザ エンジン プロンプトに戻ります。

ステップ 6　ハイ アベイラビリティがスーパバイザ エンジンのステートを同期化していることを確認します。そのためには、**show system highavailability** コマンドを実行して、ハイ アベイラビリティの [Operational-status] が ON であることを確認します。

ステップ 7　**switch supervisor** コマンドを実行します。

ステップ 8　**switch console** コマンドを実行します。

ステップ 9　スタンバイ MSFC の ROMMON プロンプトで、ステップ 3 を繰り返しますが、ステップ 3d ではオプション 2 の [boot system] を選択します。

```
change the boot characteristics? y/n  [n]:  y
enter to boot:
 0 = ROM Monitor
 1 = the boot helper image
 2-15 = boot system
    [2]:  2   <========================


    Configuration Summary
enabled are:
load rom after netboot fails
console baud: 9600
boot: the ROM Monitor

do you wish to change the configuration? y/n  [n]:  n


You must reset or power cycle for new config to take effect
rommon 2 >
```

ステップ 10　ROMMON プロンプトで **reset** コマンドを入力してシステムを起動します。

ステップ 11　MSFC が起動したら、新しいアクティブ MSFC のコンソール ポート上の Cisco IOS コンフィギュレーション モードで **config-register 0x2102** コマンドを実行します。

ステップ 12　**Ctrl-C** を 3 回入力して、スーパバイザ エンジン プロンプトに戻ります。

CHAPTER 23

NSF/SSO MSFC 冗長機能の設定

この章では、Catalyst 6500 シリーズ スイッチ上で Cisco Nonstop Forwarding（NSF）/Stateful Switchover（SSO）を使用して Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）冗長機能を設定する手順について説明します。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series MSFC Cisco IOS Command Reference*』を参照してください。

(注) *MSFC* という用語は、この章を通じて特に明記されていないかぎり、MSFC2、MSFC2A、および MSFC3 を指します。

(注) 特に明記されていないかぎり、この章で説明する情報および手順は、Policy Feature Card（PFC; ポリシー フィーチャ カード）3B/3BXL を搭載した Supervisor Engine 32、PFC3A/PFC3B/PFC3BXL を搭載した Supervisor Engine 720、および PFC2 を搭載した Supervisor Engine 2 に適用されます。

この章で説明する内容は、次のとおりです。

ハードウェアおよびソフトウェアの要件

ここでは、NSF/SSO を設定する場合のハードウェアおよびソフトウェア要件について説明します。

- サポート対象スーパバイザ エンジン ― Supervisor Engine 2、Supervisor Engine 720、および Supervisor Engine 32（Supervisor Engine 1 では NSF/SSO はサポートされません）。
- サポート対象 MSFC ― MSFC2、MSFC2A、および MSFC3（MSFC はサポートされません）。
- 冗長スーパバイザ エンジンには、同じモデルの PFC と MSFC を搭載した同じタイプのスーパバイザ エンジンを使用する必要があります。
- Rlease 8.5(1) 以降の Catalyst ソフトウェア リリース

（注） SSO が MSFC 上でイネーブルな場合、Release 8.5(1) 以降のスーパバイザ エンジン ソフトウェア リリースにアップグレードする前に、スーパバイザ エンジン上でハイ アベイラビリティをイネーブルにする必要があります。**set system highavailability enable** コマンドを使用して、スーパバイザ エンジン上でハイ アベイラビリティ機能をイネーブルにします。

- Cisco IOS Release 12.2(18)SXF 以降のリリース

NSF/SSO の機能概要

（注） SSO は、Single Router Mode（SRM）と Dual Router Mode（DRM）に代わる機能です。これらのハイ アベイラビリティ モードは、サポートされません。SRM および DRM の CLI（コマンドライン インターフェイス）処理の詳細については、「設定時の注意事項および制限事項」（p.23-5）を参照してください。

スーパバイザ エンジン上で稼働する Catalyst オペレーティング システムにより、冗長スーパバイザ エンジンのレイヤ 2 ハイ アベイラビリティが提供されます。MSFC 上で稼働する NSF/SSO を備えた Cisco IOS Release 12.2(18)SXF 以降のリリースでは、冗長 MSFC にレイヤ 3 以上のハイ アベイラビリティ機能を提供します。MSFC SSO のハイ アベイラビリティの利点は、次のとおりです。

- ダウンタイムの軽減
- MSFC をシャット ダウンせずにソフトウェアをアップグレード可能
- アクティブ MSFC の障害を検出し、スタンバイ MSFC が既存トラフィック フローの廃棄を最少限にして、システムをテイクオーバー可能

システムが起動し、スーパバイザ エンジンが初期化を完了し動作準備が整ったあと、スーパバイザ エンジンは両方の MSFC に SCP インベントリ メッセージを送信します。インベントリ メッセージには、システム内にどの MSFC が存在するかという情報および他の動作ステート情報が含まれます。ハイ アベイラビリティという観点では、インベントリ メッセージには、アクティブ MSFC となる MSFC およびスタンバイ MSFC となる MSFC を指示する情報が含まれるので、重要です。

スタンバイ MSFC の起動中、イメージ バージョン情報は MSFC 間で交換され、次のいずれかの処理が行われます。

- イメージ バージョン情報が一致し、両方の MSFC が SSO として設定されるか、またはデフォルトに（SSO）設定されると、システムは SSO モードで稼働します。
- イメージ バージョン情報が一致しないか、または MSFC のどちらかで Route Processor Redundancy（RPR）が設定されると、システムは RPR モードで稼働します。

NSF/SSO モードでは、一方の MSFC がアクティブ モードでもう一方の MSFC はホットスタンバイ モードになります。ホットスタンバイ MSFC は、アクティブ MSFC からステート情報を受信することにより、一定の準備ステートを維持します。スーパバイザ エンジンは、スタンバイ MSFC にアクティブ MSFC が行っている処理を引き継ぐように要求する場合があります。スーパバイザ エンジンはアクティブ MSFC をモニタします。MSFC が応答しない場合は、スーパバイザ エンジンは MSFC に切断またはダウンを宣告し、MSFC のリセットを行います。スタンバイ MSFC には、処理を開始するのに必要な最新のステート情報があります（スタンバイ MSFC は完全に初期化されますが、スイッチオーバーが発生するまでは、VLAN［仮想 LAN］は管理上のダウン ステートのままです）。

NSF により、スイッチング モジュールおよびスイッチ ファブリックは、MSFC スイッチオーバーの実行中もパケット転送を継続します。

（注） 検出されたハードウェア障害または CLI コマンドによっても、スイッチオーバーは発生します。

（注） スーパバイザ エンジン上のハイ アベイラビリティ機能は、MSFC のハイ アベイラビリティ機能とは無関係です。ただし、確実に MSFC SSO 機能を適切に動作させるように、スーパバイザ エンジン上でハイ アベイラビリティをイネーブルにする必要があります。

SSO モードで MSFC を稼働中に、スーパバイザ エンジンのハイ アベイラビリティ機能を実行していない場合、スイッチオーバーは非ステートフル スイッチオーバーとなり、スタンバイ MSFC はスイッチオーバー時にリセットされ、再起動されます。スーパバイザ エンジン上に MSFC の SSO をサポートするのに十分なステート情報がないため、スタンバイ MSFC のリセット / 再起動が発生します。スタンバイ MSFC のリセット / 再起動により、サービスは中断されます。

RPR の概要

（注） RPR+ モードはサポートされません。

RPR は、*コールド*スタンバイ モードです。スイッチオーバーが発生すると、スタンバイ MSFC は完全に初期化する必要があります。RPR モードは、主として Fast Software Upgrade（FSU）用に使用されます（「高速ソフトウェア アップグレード」[p.23-16] を参照）。RPR モードでは、スタートアップ コンフィギュレーションがスタンバイ MSFC に同期化されますが、スイッチオーバーが発生するまでは一切処理されません。実行コンフィギュレーションは、スタンバイ MSFC に同期化されません。

アクティブ MSFC が完全に起動すると、MSFC 間でのステート情報の交換は行われません。アクティブ MSFC が故障すると、スタンバイ MSFC がスタートアップ コンフィギュレーション ファイルを処理して、初期化を開始します。

イメージの互換性に問題がある場合は、アクティブ MSFC は完全に起動しますが、スタートアップ コンフィギュレーション ファイルを処理する前に、スタンバイ MSFC は起動を中断します。アクティブ MSFC が故障すると、スイッチオーバーがトリガーされ、中断されたスタンバイ MSFC が初期化を開始し、アクティブ MSFC となります。

（注） MSFC 上で RPR を実行する場合、スーパバイザ エンジン上のハイ アベイラビリティをイネーブルにする必要はありません。

MSFC スイッチオーバーのタイプ

MSFC スイッチオーバーのタイプは、次のとおりです。

- フェールオーバー ― アクティブ MSFC が故障するか、または重大なシステム障害が検出され、最終的に ROMMON に入ると、MSFC フェールオーバーが発生します。
- 強制スイッチオーバー ― 強制スイッチオーバーは、CLI コマンドを入力するか、またはシャーシからアクティブ MSFC 搭載のスーパバイザ エンジンを取り外すことにより発生します。強制的にスイッチオーバーを実行する MSFC の CLI コマンドは、**redundancy force-switchover** および **reload** コマンドです。強制的にスイッチオーバーを実行するスーパバイザ エンジンの CLI コマンドは、**reset** *mod* コマンドです。この場合 *mod* は、**show module** コマンド表示で示される MSFC のモジュール番号です。

設定時の注意事項および制限事項

ここでは、NSF/SSO を設定する際の設定時の注意事項と制限事項を説明します。

- SSO が MSFC 上でイネーブルな場合、Release 8.5(1) 以降のスーパバイザ エンジン ソフトウェア リリースにアップグレードする前に、スーパバイザ エンジン上でハイ アベイラビリティをイネーブルにする必要があります。**set system highavailability enable** コマンドを使用して、スーパバイザ エンジン上でハイ アベイラビリティ機能をイネーブルにします。
- SSO は、SRM および DRM に代わる機能です。これらのハイ アベイラビリティ モードは、サポートされません。詳細は、次のとおりです。
  - SRM CLI 処理 ― Cisco IOS Release 12.2(18)SXF 以降のソフトウェア リリースには、SRM CLI が含まれます。CLI は入力時に受け入れられますが、機能はしません。SRM CLI は、Cisco IOS Release 12.2(18)SXF 以降のソフトウェア リリースで維持され、NSF/SSO への移行を容易にします。ただし、SRM CLI により NVRAM（不揮発性 RAM）のアップデートは行われません。SRM CLI が設定されていて、**write mem** コマンドを入力して SRM 設定を変更しようとする場合、設定内の SRM CLI コマンドは失われます。SRM を持つイメージにダウングレードする場合、元の SRM CLI 設定は失われるため、SRM を再設定する必要があります。このため、SRM から NSF/SSO にアップグレードする前に設定を保存することを推奨します。
  - DRM CLI 処理 ― SRM CLI とは異なり、NSF/SSO へのアップグレード後のコンフィギュレーション ファイルには、既存の DRM CLI がシステム起動時のエラーとしてフラグ付けされます。スイッチを再設定して、DRM 設定を削除する必要があります。DRM から NSF/SSO にアップグレードする前に設定を保存することを推奨します。
- スイッチオーバー中は、MSFC によりルーティングされたトラフィックのトラフィック損失が発生します。NSF は、モジュールおよびスイッチ ファブリックによりハードウェア スイッチングされたトラフィックにのみ適用されます。スイッチオーバーが完了するまで、新しいフローは許可されません。
- MSFC に障害があり、スーパバイザ エンジンにこの障害を通知できない場合、スーパバイザ エンジンが MSFC の障害を認識し、スイッチオーバーがトリガーされるまで 30 ～ 40 秒かかる可能性があります。スーパバイザ エンジンが障害通知を受信した場合、スイッチオーバーは直ちにトリガーされます。
- フレーム リレー、Asynchronous Transfer Mode（ATM; 非同期転送モード）、および PPP（ポイントツーポイント プロトコル）の各プロトコルは、SSO モードでサポートされません。
- WAN モジュールは、SSO スイッチオーバーに対して次のように動作します。
  - SSO スイッチオーバーの場合、WAN モジュールは再起動しません。
  - WAN モジュール インターフェイスは、SSO スイッチオーバー中にダウンして、その後アップに戻ります。
  - NSF が WAN インターフェイスで設定されている場合、すべてのルーティング プロトコルは NSF を実行しません。
  - WAN インターフェイスのすべての機能は、SSO スイッチオーバー後に動作を再開します。

- スタンバイ スーパバイザ エンジン /MSFC 挿入 ― NSF/SSO 冗長性では、メンテナンスのためのスタンバイ スーパバイザ エンジン /MSFC のホット スワップが可能です。スタンバイ MSFC をホット インサートすると、アクティブ MSFC がスタンバイ MSFC の存在を検出し、スタンバイ MSFC ステートをホットスタンバイに移行させます。スタンバイ MSFC を取り外すと、アクティブ MSFC とスタンバイ MSFC 間の同期化が中断され、スタンバイ MSFC への保留状態のアップデートはすべて廃棄され、シンプレックス モードが開始されます。スタンバイ MSFC ステートは、**show redundancy states** コマンドにより表示されます。
- カウンタおよび統計情報 ― MSFC により維持される各種カウンタおよび統計情報は、MSFC 間で同期化されません。
- すべてのサブシステムがハイアベイラビリティ対応であるわけではなく、ハイアベイラビリティ アウェアであるサブシステムでも、それぞれ一連の制限があります。
- 一部のサブシステムでは、それぞれハイ アベイラビリティ固有の設定およびステータス コマンド（ **show isis nsf** など）があります。
- MSFC ソフトウェア イメージは、現在 In-Service Software Upgrade（ISSU）をサポートしません。
- 診断は、ハイ アベイラビリティに統合されません。MSFC 上の診断失敗によるスイッチオーバーは、サポートされません。

CLI を使用した NSF/SSO の設定

ここでは、NSF/SSO を設定する手順について説明します。

SSO の設定

SSO は、デフォルト モードです。デフォルトでは、明示的に SSO として設定されない場合でも、システムは SSO モードでアップします。ただし、明示的に SSO モードを設定することを推奨します。

（注） 次の作業は、RPR モードの設定でも使用できます（**mode sso** の代わりに **mode rpr** を使用）。

SSO モードを設定するには、次の作業を実行します。

	作業	コマンド
ステップ 1	冗長コンフィギュレーション モードを開始します。	`Router(config)# redundancy`
ステップ 2	SSO を設定します。このコマンドにより、冗長 MSFC が再起動され、SSO モードで機能を開始します。	`Router(config-red)# mode sso`
ステップ 3	SSO がイネーブルに設定されたことを確認します。	`Router# show running-config`
ステップ 4	動作冗長モードを表示します。	`Router# show redundancy states`

次に、システムで SSO を設定して、冗長ステートを表示する例を示します。

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# redundancy
Router(config-red)# mode sso
Router(config-red)# end
Router# show redundancy states
my state = 13 -ACTIVE
     peer state = 1  -DISABLED
           Mode = Simplex
           Unit = Primary
        Unit ID = 7
Redundancy Mode (Operational) = Stateful SwitchOver - SSO
Redundancy Mode (Configured)  = Stateful SwitchOver - SSO
Redundancy State              = Non Redundant

     Split Mode = Disabled
   Manual Swact = Disabled  Reason: Simplex mode
 Communications = Down      Reason: Simplex mode

   client count = 18
 client_notification_TMR = 30000 milliseconds
          keep_alive TMR = 9000 milliseconds
        keep_alive count = 0
    keep_alive threshold = 18
           RF debug mask = 0x0
Router#
```

CEF NSF の設定

デフォルトでは、Cisco Express Forwarding（CEF) NSF は、ネットワーキング装置が SSO モードで稼働している場合に動作します。設定作業は必要ありません。

CEF NSF の確認

CEF が NSF 対応であることを確認するには、次の作業を実行します。

作業	コマンド
CEF が NSF 対応であることを確認します。	Router# **show cef state**

次に、CEF が NSF 対応であることを確認する例を示します。

```
router# show cef state
CEF Status [RP]
 CEF enabled/running
 dCEF enabled/running
 CEF switching enabled/running
 CEF default capabilities:
  Always CEF switching:               yes
  Always dCEF switching:              yes
  Default CEF switching:              yes
  Default dCEF switching:             yes
  Drop multicast packets:             no
  OK to punt packets:                 yes
  NVGEN CEF state:                    yes
  fastsend() used:                    no
  CEF NSF capable:                    yes
  RPR+/SSO standby capable:           yes
  IPC delayed func on SSO:            no
  FIB auto repair supported:          yes
  LCs not running at init time:       yes
  Hardware forwarding supported:      yes
  Hardware forwarding in use:         yes
  Load-sharing pr. packet supported:  no
 RRP state:
  I am standby RRP:                   no
  RF Peer Presence:                   no
  RF PeerComm reached:                no
  Config Redundancy mode:             Stateful SwitchOver - SSO(7)
  Operating Redundancy mode:          Stateful SwitchOver - SSO(7)
  CEF NSF:                            enabled/not running
 RP state:
  Expanded LC ipc memory:             0 Kbytes
  Linecard reloader type:             aggressive (Default)
  Linecard dFIB structures:           initialized
Router#
```

BGP NSF の設定

（注） Border Gateway Protocol（BGP）NSF に参加するすべてのピア デバイス上では、BGP の適切な再起動を設定する必要があります。

NSF に BGP を設定するには、次の作業を実行します（この作業を各 BGP NSF ピア デバイス上で繰り返します）。

	目的	コマンド
ステップ 1	グローバル コンフィギュレーション モードを開始します。	`Router# configure terminal`
ステップ 2	BGP ルーティング プロセスをイネーブルにし、ルータをルータ コンフィギュレーション モードにします。	`Router(config)# router bgp` *as-number*
ステップ 3	BGP の適切な再起動機能をイネーブルにして、BGP NSF を開始します。 BGP セッションの確立後にこのコマンドを入力する場合、BGP ネイバと機能を交換できるよう、セッションを再起動する必要があります。 再起動するルータおよびすべてのピアでこのコマンドを使用します。	`Router(config-router)# bgp graceful-restart`

BGP NSF の確認

BGP NSF を確認するには、SSO 対応のネットワーキング装置および近接装置上で、適切な再起動機能が設定されていることを確認する必要があります。確認するには、次の手順を実行します。

ステップ 1　**show running-config** コマンドを入力して、SSO 対応ルータの BGP 設定で [bgp graceful-restart] が表示されることを確認します。

```
Router# show running-config

.
.
.
router bgp 120
.
.
.
bgp graceful-restart
 neighbor 10.2.2.2 remote-as 300
.
.
.
```

ステップ 2　各 BGP ネイバ上でステップ 1 を繰り返します。

ステップ 3　SSO 装置および近接装置上で、適切な再起動機能がアドバタイズ済み、受信済みの両方で表示されることを確認して、適切な再起動機能のあるアドレス ファミリーを確認します。

（注）　アドレス ファミリーが表示されない場合、BGP NSF も発生しません。

```
Router# show ip bgp neighbors x.x.x.x

BGP neighbor is 192.168.2.2,  remote AS YY, external link
  BGP version 4, remote router ID 192.168.2.2
  BGP state = Established, up for 00:01:18
  Last read 00:00:17, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh:advertised and received(new)
    Address family IPv4 Unicast:advertised and received
    Address famiiy IPv4 Multicast:advertised and received
    Graceful Restart Capabilty:advertised and received
      Remote Restart timer is 120 seconds
      Address families preserved by peer:
        IPv4 Unicast, IPv4 Multicast
  Received 1539 messages, 0 notifications, 0 in queue
  Sent 1544 messages, 0 notifications, 0 in queue
  Default minimum time between advertisement runs is 30 seconds
```

OSPF NSF の設定

（注）　OSPF NSF に参加するすべてのピア装置では、OSPF NSF 対応にする必要があります。これは、装置に NSF ソフトウェアをインストールすると自動的に実行されます。

OSPF NSF を設定するには、次の作業を実行します。

	目的	コマンド
ステップ 1	グローバル コンフィギュレーション モードを開始します。	`Router# configure terminal`
ステップ 2	OSPF ルーティング プロセスをイネーブルにし、ルータをルータ コンフィギュレーション モードにします。	`Router(config)# router ospf processID`
ステップ 3	OSPF の NSF 動作をイネーブルにします。	`Router(config-router)# nsf`

OSPF NSF の確認

OSPF NSF を確認するには、NSF 機能が SSO 対応のネットワーキング装置に設定されていることを確認する必要があります。OSPF NSF を確認するには、次の手順を実行します。

ステップ 1　**show running-config** コマンドを入力して、SSO 対応装置の OSPF 設定で [nsf] が表示されることを確認します。

```
Router# show running-config

router ospf 120
log-adjacency-changes
nsf
network 192.168.20.0 0.0.0.255 area 0
network 192.168.30.0 0.0.0.255 area 1
network 192.168.40.0 0.0.0.255 area 2
.
.
.
```

ステップ 2　**show ip ospf** コマンドを入力して、NSF が装置上でイネーブルであることを確認します。

```
router> show ip ospf

Routing Process "ospf 1" with ID 192.168.2.1 and Domain ID 0.0.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x0
Number of opaque AS LSA 0. Checksum Sum 0x0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
Non-Stop Forwarding enabled, last NSF restart 00:02:06 ago (took 44 secs)
Area BACKBONE(0)
Number of interfaces in this area is 1 (0 loopback)
 Area has no authentication
 SPF algorithm executed 3 times
```

IS-IS NSF の設定

Intermediate System-to-Intermediate System（IS-IS）NSF を設定するには、次の作業を実行します。

	目的	コマンド
ステップ 1	グローバル コンフィギュレーション モードを開始します。	`Router# configure terminal`
ステップ 2	IS-IS ルーティング プロセスをイネーブルにし、ルータをルータ コンフィギュレーション モードにします。	`Router(config)# router isis [tag]`
ステップ 3	IS-IS の NSF 動作をイネーブルにします。 IETF ドラフトベースの再起動性をサポートするネットワーキング装置との隣接関係が保証されている場合は、**ietf** キーワードを入力して、同種ネットワークで IS-IS をイネーブルにします。 NSF 対応のネットワーキング装置と隣接関係にない場合は、**cisco** キーワードを入力して、異種ネットワークで IS-IS を実行します。	`Router(config-router)# nsf [cisco | ietf]`
ステップ 4	（任意）NSF 再起動試行間の最少時間を指定します。*連続する* NSF 再起動試行間のデフォルト時間は、5 分です。	`Router(config-router)# nsf interval [minutes]`
ステップ 5	（任意）IS-IS 自身のリンクステート情報が一杯になり、その情報がネイバにフラッディングされるまで、IS-IS が IS-IS データベースの同期を待機する時間を指定します。 **t3** キーワードは、IETF 動作を選択した場合にのみ、適用されます。**adjacency** キーワードを指定すると、再起動中のルータは近接装置から待機時間を取得します。	`Router(config-router)# nsf t3 {manual [seconds] | adjacency}`
ステップ 6	（任意）再起動が完了する前に、IS-IS 隣接関係にあるすべてのインターフェイスがアップするまで IS-IS NSF の再起動を待機する時間を指定します。デフォルトは 10 秒です。	`Router(config-router)# nsf interface wait seconds`

IS-IS NSF の確認

IS-IS NSF を確認するには、NSF 機能が、SSO 対応のネットワーキング装置に設定されていることを確認する必要があります。IS-IS NSF を確認するには、次の作業を実行します。

ステップ 1　**show running-config** コマンドを入力して、SSO 対応装置の IS-IS 設定で [nsf] が表示されることを確認します。Cisco IS-IS または IETF IS-IS 設定のいずれかが表示されます。次に、装置が IS-IS NSF の Cisco 実装 を使用する例を示します。

```
Router# show running-config
（テキスト出力は省略）
router isis
nsf cisco
（テキスト出力は省略）
```

ステップ 2　NSF 設定が **cisco** に設定されている場合、**show isis nsf** コマンドを入力して、NSF が装置上でイネーブルであることを確認します。Cisco 設定を使用すると、表示出力はアクティブ MSFC（Route Processor［RP; ルート プロセッサ］）と冗長 MSFC で異なります。次に、アクティブ MSFC（RP）上の Cisco 設定の出力例を示します。この例で、[NSF restart enabled] があることに注意してください。

```
router# show isis nsf

NSF is ENABLED, mode 'cisco'

RP is ACTIVE, standby ready, bulk sync complete
NSF interval timer expired (NSF restart enabled)
Checkpointing enabled, no errors
Local state:ACTIVE,  Peer state:STANDBY HOT,  Mode:SSO
```

次に、スタンバイ RP 上の Cisco 設定の出力例を示します。この例で、[NSF restart enabled] があることに注意してください。

```
router# show isis nsf

NSF enabled, mode 'cisco'
RP is STANDBY, chkpt msg receive count:ADJ 2, LSP 7
NSF interval timer notification received (NSF restart enabled)
Checkpointing enabled, no errors
Local state:STANDBY HOT,  Peer state:ACTIVE,  Mode:SSO
```

ステップ 3　NSF 設定が **ietf** に設定されている場合、**show isis nsf** コマンドを入力して、NSF が装置上でイネーブルであることを確認します。次に、ネットワーキング装置上の IETF IS-IS 設定の出力例を示します。

```
router# show isis nsf

NSF is ENABLED, mode IETF
NSF pdb state:Inactive
NSF L1 active interfaces:0
NSF L1 active LSPs:0
NSF interfaces awaiting L1 CSNP:0
Awaiting L1 LSPs:
NSF L2 active interfaces:0
NSF L2 active LSPs:0
NSF interfaces awaiting L2 CSNP:0
Awaiting L2 LSPs:
Interface:Serial3/0/2
    NSF L1 Restart state:Running
    NSF p2p Restart retransmissions:0
    Maximum L1 NSF Restart retransmissions:3
    L1 NSF ACK requested:FALSE
    L1 NSF CSNP requested:FALSE
    NSF L2 Restart state:Running
    NSF p2p Restart retransmissions:0
    Maximum L2 NSF Restart retransmissions:3
    L2 NSF ACK requested:FALSE
Interface:GigabitEthernet2/0/0
    NSF L1 Restart state:Running
    NSF L1 Restart retransmissions:0
    Maximum L1 NSF Restart retransmissions:3
    L1 NSF ACK requested:FALSE
    L1 NSF CSNP requested:FALSE
    NSF L2 Restart state:Running
    NSF L2 Restart retransmissions:0
    Maximum L2 NSF Restart retransmissions:3
    L2 NSF ACK requested:FALSE
    L2 NSF CSNP requested:FALSE
Interface:Loopback1
    NSF L1 Restart state:Running
    NSF L1 Restart retransmissions:0
    Maximum L1 NSF Restart retransmissions:3
    L1 NSF ACK requested:FALSE
    L1 NSF CSNP requested:FALSE
    NSF L2 Restart state:Running
    NSF L2 Restart retransmissions:0
    Maximum L2 NSF Restart retransmissions:3
    L2 NSF ACK requested:FALSE
    L2 NSF CSNP requested:FALSE
```

冗長関連情報の表示

冗長関連情報を表示するには、**show redundancy** [qualifier] コマンドを使用します。サポートされる修飾詞は、次のとおりです。

```
Router# show redundancy ?
  clients          Redundancy Facility (RF) client list
  counters         Redundancy Facility (RF) operational counters
  events           Redundancy Facility (RF) events list
  history          Redundancy Facility (RF) history
  linecard-group   Line card redundancy group information
  states           Redundancy Facility (RF) states
  switchover       Redundancy Facility (RF) switchover
  |                Output modifiers
  <cr>

Router#
```

MSFC スイッチオーバーの実行

スタンバイ MSFC にスイッチオーバーを行うには、**redundancy switch-activity** [**force**] コマンドを使用します。**force** キーワードにより、すべての制限事項が無効になります。

MSFC ソフトウェアのリロードの実行

スタンバイ MSFC（**peer** キーワード）またはシャーシ内のすべてのモジュール（**shelf** キーワード）をリロードするには、**redundancy reload** {**peer** | **shelf**} コマンドを使用します。

冗長関連のデバッグ コマンドの使用

冗長関連のデバッグ情報を表示するには、**debug redundancy** [qualifier] コマンドを使用します。サポートされる修飾詞は、次のとおりです。

```
Router# debug redundancy ?
  config-sync  HA config sync debug option
  ehsa         Redundancy Facility (RF) EHSA
  errors       Redundancy Facility (RF) Errors
  fsm          Redundancy Facility (RF) FSM events
  kpa          Redundancy Facility (RF) keep alive
  msg          Redundancy Facility (RF) Messaging events
  progression  Redundancy Facility (RF) Progression events
  status       Redundancy Facility (RF) Status events
  timer        Redundancy Facility (RF) Timer events

Router#
```

NSF/SSO 固有の冗長情報を表示するには、**debug hybrid-ha** [qualifier] コマンドを使用します。サポートされる修飾詞は、次のとおりです。

```
Router# debug hybrid-ha ?
  all     All Hybrid HA SSO/NSF platform specific debugging messages
  errors  Hybrid HA SSO/NSF platform specific warnings and errors
  events  Hybrid HA SSO/NSF platform specific events
  ipc     Hybrid HA SSO/NSF platform specific IPC related events
  kpa     Hybrid HA SSO/NSF platform specific Keep-Alive related events

Router#
```

ソフトウェアのアップグレード

ここでは、MSFC ソフトウェアをアップグレードする手順について説明します。

（注） いずれのソフトウェア　アップグレードの手順を実行する場合も、事前に「設定時の注意事項および制限事項」（p.23-5）を参照してください。

高速ソフトウェア アップグレード

（注） 高速ソフトウェア アップグレード中は、システムは RPR モードとなるため、サービスは中断されます。スイッチオーバーは、ステートフルではありません。インターフェイスはダウンしますが、MSFC の初期化で再びアップし、RPR モードでアップになります。さらに、保存されていない設定変更はすべて失われます。

（注） この手順では、両方の MSFC 上で Cisco IOS リリースが RPR（最低）をサポートする必要があり、両方の MSFC では同じソフトウェア バージョンを稼働する必要があります。アクティブ MSFC は、スタンバイ MSFC がアップすると、スタンバイ イメージ バージョンを確認します。スタンバイ イメージ バージョンがアクティブ イメージ バージョンと異なる場合、冗長モードは RPR に戻ります。

（注） この手順は、SRM および DRM イメージとは連動しません。

（注） 冗長スーパバイザ エンジンには、同じモデルの PFC と MSFC を搭載した同じタイプのスーパバイザ エンジンを使用する必要があります。

高速ソフトウェア アップグレードにより、ソフトウェアのアップグレードまたはダウングレードに予定されていたダウンタイムが短縮されます。高速ソフトウェア アップグレードの手順には、スタンバイ MSFC およびアクティブ MSFC への新しいイメージのロード、およびスタンバイ MSFC の再起動が含まれます。スタンバイ MSFC 上で稼働する新しいイメージは、アクティブ MSFC 上で現在稼働中のイメージとの互換性がありません。そのため、スタンバイ MSFC は RPR モードでアップします。高速ソフトウェア アップグレードは、アップグレード プロセス中のイメージの非互換性を避けるため、RPR モードで実行されます。

新しいイメージの実行を開始するには、アクティブ MSFC の実行を中断することにより、スタンバイ MSFC に強制的に切り替えます。これで、スタンバイ MSFC はアクティブ MSFC となります。次に、中断していた MSFC の起動が許可されます。これは、スタンバイ MSFC となりますが、新しく

アップグレードされたイメージを実行します。新しいイメージは、両方の MSFC 上で稼働し、スタンバイ MSFC はホットスタンバイ モードでアップします。この時点で、両方の MSFC が同じイメージ バージョンを実行しているため、システムは SSO モードで稼働します。

（注） スタンバイ MSFC がアクティブ MSFC となるスイッチオーバーをもう一度強制的に行うことにより、MSFC の元の役割（アクティブおよびパッシブ ステータス）に戻すこともできます。

高速ソフトウェア アップグレードを実行するには、次の手順を実行します。

ステップ 1　両方の MSFC に新しいイメージをコピーします。

ステップ 2　起動変数を設定して、**write memory** コマンドにより設定を保存します。

ステップ 3　スタンバイ MSFC をリセットし、オンラインに戻し、新しいイメージを実行します。**show redundancy states** コマンドを入力して、スタンバイ MSFC が完全にオンラインであることを確認します。

ステップ 4　**redundancy force-switchover** コマンドを入力して、手動のスイッチオーバーを実行します。スタンバイ MSFC は、新しいイメージを実行する新しいアクティブ MSFC となります。スイッチオーバー前のシステムは RPR モードであったため、搭載されたモジュールはスイッチオーバー中に新しいソフトウェアによりリセットされ、再度ダウンロードされます。

ステップ 5　新しいスタンバイ MSFC が再起動してオンラインに戻されると、両方の MSFC および搭載されたモジュールは、新しいバージョンのソフトウェアを実行します。

SSO の SRM および DRM からのアップグレード

（注） このアップグレードにより、サービスは中断されます。実際のダウンタイムはスイッチの設定により変化しますが、システムを起動してオンラインにするのに所要される時間ほど長くはかかりません。

（注） SSO を SRM および DRM からアップグレードする場合は、アップグレードを実行する前に設定を保存する必要があります。システムが新しいイメージをリロードする際、DRM 設定により解析エラーが生成されます。アップグレード後、SSO を使用するには DRM 設定を再設定する必要があります。

Cisco IOS Release 12.2(18)SXF 以前の Cisco IOS ソフトウェアは、SRM および（または）DRM 対応ですが、SSO へのアップグレードはサポートされていません。これらのソフトウェア イメージは、高速ソフトウェア アップグレード手順ではアップグレードできません。このソフトウェアをアップグレードするには、各 MSFC 上で新しいイメージをロードし、同時に両方の MSFC を起動する必要があります。

MSFC で新しいイメージがロードされたあと、システムを再起動して新しいイメージをロードする必要があります。この起動時間中にスイッチはオフラインになるため、新しいイメージをロードするまでは SSO の利点を確認できません。

混在モードの動作

ソフトウェアのアップグレードで誤りがあると、MSFC 上で SSO ベースのイメージが稼働し、もう一方の MSFC 上で SRM および（または）DRM ベースのイメージが稼働する混在モードの状態となります。この状態は、システムの安定性の問題につながります。

この混在モードでは、アクティブ MSFC 上で SSO ベースのイメージが稼働している場合、アクティブ MSFC は完全に起動し、シンプレックス（非冗長）ステートでアップします。また、SRM および（または）DRM ベースのイメージも起動しますが、スタンバイ ステートのままです。

混在モードのアップグレードとなるもう一つの例は、アクティブ MSFC 上で SRM および（または）DRM イメージが稼働し、スタンバイ MSFC 上で SSO ベースのイメージが稼働する場合です。このモードでは、SRM および（または）DRM イメージが稼働するアクティブ MSFC は完全に起動しますが、スタンバイ MSFC 上で稼働する SSO ベースのイメージは、誤ってその MSFC はアクティブ MSFC で、アクティブ MSFC として起動しようとしていると判断します。スーパイザ エンジンからスタンバイ MSFC であることを示すインベントリ メッセージを受信すると、MSFC の役割不一致エラーを報告して、自身をリロードします。この問題は、アクティブ MSFC 上で SRM、DRM、または boothelper イメージが稼働していて、スタンバイ MSFC 上で SSO 対応のイメージをロードしようとすると発生します。

両方の状況を解決するには、SRM および（または）DRM ソフトウェアを SSO ベースのソフトウェアと同じレベルにアップグレードするか、または SSO ベースのソフトウェアを SRM および（または）DRM イメージのレベルまでダウングレードする必要があります。

CHAPTER 24

スイッチの起動設定の変更

この章では、Catalyst 6500 シリーズ スイッチ上で、BOOT 環境変数、CONFIG_FILE 環境変数、およびコンフィギュレーション レジスタを含むスイッチの起動設定を変更する方法について説明します。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

この章で説明する内容は、次のとおりです。

スイッチの起動設定の機能

ここでは、起動設定の機能について説明します。

ブート プロセスの概要

ブート プロセスには、ROM モニタとスーパバイザ エンジン システム コードの 2 つのソフトウェア イメージが関与します。スイッチを起動またはリセットすると、ROM モニタ コードが実行されます。NVRAM（不揮発性 RAM）内の設定に応じて、スイッチは ROM モニタ モードのままの場合と、スーパバイザ エンジン システム コードをロードする場合とがあります。

スイッチを起動する方法は、コンフィギュレーション レジスタと BOOT 環境変数という、ユーザ側で設定できる 2 つのパラメータによって決まります。コンフィギュレーション レジスタについては、「コンフィギュレーション レジスタの概要」（p.24-3）を参照してください。BOOT 環境変数については、「BOOT 環境変数の概要」（p.24-3）を参照してください。

ROM モニタの概要

ROM モニタ コードは、スイッチの起動時、リセット時、または重大な例外が発生したときに実行されます。ROM モニタ モードが開始されるのは、スイッチが有効なシステム イメージを見つけることができなかった場合、NVRAM 内の設定が壊れていた場合、またはコンフィギュレーション レジスタが ROM モニタ モードを開始するように設定されていた場合です。ROM モニタ モードで、フラッシュ メモリ、ネットワーク サーバ ファイル、またはブートフラッシュからシステム イメージを手動でロードできます。

スイッチを再起動し、起動から 60 秒以内に **Break** キーを押すことにより、ROM モニタ モードを開始できます。端末サーバから接続している場合は、エスケープによって Telnet プロンプトを表示し、**send break** コマンドを入力すると、ROM モニタ モードが開始されます。

（注） コンフィギュレーション レジスタの設定値で **Break** キーがオフに設定されているかどうかに関係なく、システムの再起動から 60 秒間は、**Break** キーが必ず有効です。

ROM モニタには、次の機能が組み込まれています。

- 電源投入時の信頼性テスト
- ハードウェアの初期化
- 起動（手動起動および自動起動が可能）
- デバッグ ユーティリティおよびクラッシュ分析機能
- モニタ呼び出しインターフェイス（EMT コール ― ROM モニタは EMT コールを使用して、実行システム イメージに情報およびある種の機能を提供します）
- ファイル システム（ROM モニタは、単純なファイル システムを認識し、動的にリンクされたファイル システム ライブラリ [MONLIB] によって新しく作成されたファイル システムをサポートします）
- 例外処理

コンフィギュレーション レジスタの概要

コンフィギュレーション レジスタによって、スイッチが OS（オペレーティング システム）イメージをロードするかどうか、また、どこにシステム イメージを保存するかが決まります。コンフィギュレーション レジスタのブート フィールドによって、起動時に ROM モニタがスーパバイザ エンジンのシステム イメージをロードするかどうかが、また、ロードする場合にはその方法が決まります。ブート フィールドを変更することにより、起動時にデフォルトのシステム イメージを使用するのではなく、強制的に特定のシステム イメージを起動させることができます。

ブート フィールドは、16 ビットのコンフィギュレーション レジスタの下位 4 ビット（ビット 3、2、1、および 0）で形成されます。デフォルトのブート フィールド値は 0x10F です。次に挙げるコンフィギュレーション レジスタのブート フィールド設定を使用できます。

- ブート フィールドが 0000 の場合、スイッチはシステム イメージをロードしません。その代わりに、ROM モニタ モードを開始します。ROM モニタ モードでは、ROM モニタ コマンドを入力して、システム イメージを手動でロードできます。
- ブート フィールドが 0001 の場合、スイッチはオンボード フラッシュ メモリ上で見つけた最初に有効なシステム イメージをロードします。
- ブート フィールドの値が 0010 ～ 1111 の場合、スイッチは NVRAM 設定の **boot system** コマンドで指定されたシステム イメージをロードします。**boot system** コマンドの入力順に、イメージの起動を試行します。BOOT 環境変数リストの中のどのイメージも起動できなかった場合は、ROM モニタ モードのままになります。正確なブート シーケンスは、ROM モニタによって定義されます。

コンフィギュレーション レジスタの他のビットを設定する場合、次のような機能を持ちます。

- ビット 5（0x0020）― CONFIG_FILE の反復がイネーブルになります。
- ビット 6（0x0040）― システム ソフトウェアによって NVRAM の内容が消去されます。
- ビット 7（0x0080）― OEM ビットがイネーブルになります（未使用）。
- ビット 8（0x0100）― ブレークがディセーブルになります。
- ビット 9（0x0200）― セカンダリ ブートストラップが使用されます（ROM モニタでは未使用）。
- ビット 10（0x0400）― すべてゼロで IP ブロードキャストを行います（未使用）。
- ビット 11/12（0x0800/0x1000）― コンソールの回線速度を次のように指定します。0/0=9600、0/1=1200、1/0=4800、1/1=2400（デフォルトの設定は 9600）です。
- ビット 13（0x2000）― ネットワーク ブートができなかった場合に、デフォルトのフラッシュ ソフトウェアを起動します（未使用）。
- ビット 14（0x4000）― IP ブロードキャストにネットワーク番号がありません（未使用）。
- ビット 15（0x8000）― 診断メッセージをイネーブルにし、NVRAM の内容を無視します（未使用）。

BOOT 環境変数の概要

BOOT 環境変数では、起動時にスイッチの起動元となる各種デバイス上のイメージ ファイルをリスト形式で指定します。

BOOT 環境変数に複数のイメージを追加すると、フェールセーフ起動設定が得られます。最初のファイルでスイッチを起動できなかった場合、BOOT 環境変数で次に指定されているイメージが試行され、スイッチが起動するか起動を試行するイメージがなくなるまで、この作業が順番に繰り返されます。最終的に、起動できる有効なイメージがなかった場合、システムは ROM モニタ モードを開始して、ユーザが手動でブート イメージを指定できるようにします。

システムは、BOOT 環境変数に入力された順序で、イメージを保存および実行します。起動時のイメージ試行順序を変更する場合は、BOOT 環境変数のイメージを追加または消去して、適切な順序になるようにするか、BOOT 環境変数全体をいったん消去して、適切な順序でリストを再度定義します。

CONFIG_FILE 環境変数の概要

CONFIG_FILE 環境変数を使用することにより、起動時のスイッチ設定に使用する各種装置のコンフィギュレーション ファイル（auto-config ファイル）のリストを指定できます。次の動作を指定できます。

- 反復不能 — CONFIG_FILE 環境変数にコンフィギュレーション ファイルのリストを追加すると、次回のスイッチ再起動時に、システムによって NVRAM 内の設定が消去され、指定されたファイルを使用してスイッチが設定されます。CONFIG_FILE 環境変数は、スイッチの設定前に消去されます。反復不能がデフォルトの設定です。
- 反復可能 — CONFIG_FILE 環境変数にコンフィギュレーション ファイルのリストを追加すると、リストが NVRAM に無期限に保存されます。スイッチを再起動するたびに、システムによって NVRAM 内の設定が消去され、指定されたコンフィギュレーション ファイルを使用してスイッチが設定されます。CONFIG_FILE 環境変数は消去されません。

  反復または反復不能の指定方法については、「CONFIG_FILE 反復の設定」（p.24-7）を参照してください。
- 上書き — CONFIG_FILE 環境変数にコンフィギュレーション ファイルのリストを追加すると、NVRAM 内の設定が消去され、そのあとでコンフィギュレーション ファイルが実行されます。上書きがデフォルトの設定です。
- 追加 — NVRAM を消去せずに、コンフィギュレーション ファイルが実行されます。

  上書きまたは追加の指定方法については、「CONFIG_FILE 上書きの設定」（p.24-8）を参照してください。
- 同期イネーブル — コンフィギュレーション ファイルが自動的にスタンバイ スーパバイザ エンジンと同期するよう同期化をイネーブルにします。ファイルはアクティブ スーパバイザ エンジン上のファイルと同じ状態に保たれます。
- 同期ディセーブル — 同期化をディセーブルにします。

  同期化を指定する方法については、「CONFIG_FILE 同期の設定」（p.24-8）を参照してください。

ヒント　CONFIG_FILE 環境変数は変更可能です。また、起動時にスイッチを設定するコンフィギュレーション ファイル内のコマンドによってプロパティが変更される可能性があります。

CONFIG_FILE 環境変数には、複数のコンフィギュレーション ファイルを追加できます。ローカル フラッシュ デバイス（bootflash: または slot0:）に保存されている任意の有効なコンフィギュレーション ファイルを指定できます。

スイッチの起動時に、CONFIG_FILE 環境変数で指定されたファイルのいずれかが有効なコンフィギュレーション ファイルであった場合、NVRAM 内の設定が消去され、指定のコンフィギュレーション ファイルを使用してスイッチが設定されます。有効なコンフィギュレーション ファイルが複数指定されていた場合、CONFIG_FILE 環境変数に指定された順に、1 つずつコンフィギュレーション ファイルが実行されます。

指定されたファイルが有効なコンフィギュレーション ファイルではなかった場合、そのエントリを無視して次のファイルが試行されます。指定されたイメージがほかになくなるまで、この動作が繰り返されます。有効なコンフィギュレーション ファイルが 1 つも指定されていなかった場合、NVRAM に最後に保存された設定が使用されます。

スイッチのデフォルト起動設定

表 24-1 に、スイッチのデフォルト起動設定を示します。

表 24-1　スイッチのデフォルト起動設定

機能	デフォルト設定
コンフィギュレーション レジスタの値	0x10f
起動方式	BOOT 環境変数で指定されたイメージからシステムを起動
ROM モニタ コンソール ポートのボーレート	9600 ボー
ignore-config パラメータ	ディセーブル
BOOT 環境変数	空
CONFIG_FILE 環境変数	slot0:switch.cfg
CONFIG_FILE 反復に関するコンフィギュレーション レジスタ パラメータ	反復不能
CONFIG_FILE　上書きに関するコンフィギュレーション レジスタ パラメータ	上書き
CONFIG_FILE 同期に関するコンフィギュレーション レジスタ パラメータ	同期ディセーブル

コンフィギュレーション レジスタの設定

(注)　コンフィギュレーション レジスタの設定が、冗長スーパバイザ エンジンに自動的にコピーされることはありません。スイッチ内の各スーパバイザ エンジンに、個別にコンフィギュレーション レジスタを設定する必要があります。

ここでは、コンフィギュレーション レジスタを変更する方法について説明します。

- コンフィギュレーション レジスタのブート フィールドの設定（p.24-6）
- ROM モニタ コンソール ポートのボーレートの設定（p.24-6）
- CONFIG_FILE 反復の設定（p.24-7）
- CONFIG_FILE 上書きの設定（p.24-8）
- CONFIG_FILE 同期の設定（p.24-8）
- スイッチに NVRAM 内の設定情報を無視させる設定（p.24-9）
- コンフィギュレーション レジスタ値の設定（p.24-10）

コンフィギュレーション レジスタのブート フィールドの設定

コンフィギュレーション レジスタのブート フィールドを設定することにより、次回の起動時にスイッチが使用するブート方式を指定できます。このコマンドが作用するのは、ブート フィールドを制御するコンフィギュレーション レジスタ ビットだけです。他のビットの設定は変わりません。使用できる起動方式は次のとおりです。

- ROM モニタ — **rommon** キーワードを使用して、起動時にスイッチが ROM モニタ モードにとどまるようにします。
- ブートフラッシュ — **bootflash** キーワードを使用して、オンボード フラッシュ メモリ上の最初のイメージからスイッチを起動させます。
- システム — **system** キーワードを使用して、BOOT 環境変数で指定されたイメージから起動させます（デフォルトの設定）。

（注） **set boot config-register boot** コマンドで使用するキーワードは、**rommon** および **system** に限定することを推奨します。

コンフィギュレーション レジスタのブート フィールドを設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
コンフィギュレーション レジスタのブート フィールドを設定します。	**set boot config-register boot** {**rommon** | **bootflash** | **system**} [*mod*]

次に、コンフィギュレーション レジスタのブート フィールドを設定する例を示します。

```
Console> (enable) set boot config-register boot rommon
Configuration register is 0x0
ignore-config: disabled
auto-config: non-recurring
console baud: 9600
boot: the ROM monitor
Console> (enable)
```

ROM モニタ コンソール ポートのボーレートの設定

ROM モニタが使用するコンソール ポートのボーレートを設定できます。新しいボーレートが使用されるのは、次にスイッチを再起動したときです。このコマンドの作用を受けるのは、ボーレートを制御するコンフィギュレーション レジスタ ビットだけです。他のビットの設定は変わりません。

（注） コンフィギュレーション レジスタで指定したボーレートを使用するのは、ROM モニタだけです。**set system baud** コマンドで指定するボーレートとは異なります。

コンフィギュレーション レジスタで ROM モニタ コンソール ポートのボーレートを設定するには、イネーブル モードで次のコマンドを入力します。

作業	コマンド
コンフィギュレーション レジスタで ROM モニタ コンソール ポートのボーレートを設定します。	**set boot config-register baud** {**1200** | **2400** | **4800** | **9600**} [*mod*]

次に、コンフィギュレーション レジスタで ROM モニタ コンソール ポートのボーレートを 2400 に設定する例を示します。

```
Console> (enable) set boot config-register baud 2400
Configuration register is 0x1800
ignore-config: disabled
auto-config: non-recurring
console baud: 2400
boot: the ROM monitor
Console> (enable)
```

CONFIG_FILE 反復の設定

デフォルトでは、CONFIG_FILE 環境変数を設定した場合に、起動時に使用するコンフィギュレーション ファイルのリストが維持されるのは、次にスイッチを再起動するまでの間だけです。

システム ソフトウェアに CONFIG_FILE 環境変数の設定値を無期限に維持させ、スイッチを再起動するたびに、指定のコンフィギュレーション ファイルを使用してスイッチが設定されるようにすることができます。

このコマンドが作用するのは、CONFIG_FILE 環境変数の設定が反復か反復不能かを制御するコンフィギュレーション レジスタ ビットだけです。他のコンフィギュレーション レジスタ ビットは変更されません。

注意　CONFIG_FILE 環境変数を **recurring** に設定すると、スイッチを再起動するたびに NVRAM の現在の設定が消去され、指定のコンフィギュレーション ファイルを使用してスイッチが設定されます。CONFIG_FILE 環境変数を **non-recurring** に設定すると、次回スイッチを再起動したときに NVRAM の現在の設定が消去され、指定のコンフィギュレーション ファイルを使用してスイッチが設定されます。NVRAM 設定は、（再び CONFIG_FILE 変数を設定しないかぎり）その後の再起動後も維持されます。

スイッチが現在の CONFIG_FILE 環境変数を無期限に維持するように設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
現在の CONFIG_FILE 環境変数が無期限に維持されるようにスイッチを設定します。	**set boot config-register auto-config {recurring | non-recurring}**

次に、現在の CONFIG_FILE 環境変数が無期限に維持されるようにスイッチを設定する例を示します。

```
Console> (enable) set boot config-register auto-config recurring
Configuration register is 0x1820
ignore-config: disabled
auto-config: recurring, overwrite, sync disabled
console baud: 2400
boot: the ROM monitor
Console> (enable)
```

CONFIG_FILE 上書きの設定

このコマンドでは、auto-config ファイルを使用して NVRAM 内の設定を上書きするか、NVRAM の現在の内容にファイルの設定を追加するかを指定できます。上書きを指定すると、NVRAM 内の設定が消去されてから、auto-config ファイルが実行されます。追加を指定すると、NVRAM を消去せずに auto-config ファイルが実行されます。デフォルトの設定は **overwrite** です。

auto-config ファイルで NVRAM 内の設定を上書きするか、それとも NVRAM の現在の内容にファイルの設定を追加するかを指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
auto-config ファイルで NVRAM 内の設定を上書きするか、それとも NVRAM の現在の内容にファイルの設定を追加するかを指定します。	**set boot config-register auto-config** {**overwrite** | **append**}

次に、auto-config ファイルを使用して NVRAM 内の設定を上書きするように指定する例を示します。

```
Console> (enable) set boot config-register auto-config overwrite
Configuration register is 0x12F
ignore-config: disabled
auto-config: recurring, overwrite, sync disabled
console baud: 9600
boot: image specified by the boot system commands
Console> (enable)
```

次に、NVRAM の現在の内容に auto-config ファイルを追加するように指定する例を示します。

```
Console> (enable) set boot config-register auto-config append
Configuration register is 0x12F
ignore-config: disabled
auto-config: recurring, append, sync disabled
console baud: 9600
boot: image specified by the boot system commands
Console> (enable)
```

CONFIG_FILE 同期の設定

set boot config-register auto-config sync コマンドは、auto-config ファイルを強制的にスタンバイ スーパバイザ エンジンと自動的に同期化するために同期化をイネーブルにします。ファイルはアクティブ スーパバイザ エンジン上のファイルと同じ状態に保たれます。デフォルトの設定は **disabled** です。同期化チェックおよび（必要な場合）同期化をトリガするイベントは、次のとおりです。

- どちらかのスーパバイザ エンジン上での auto-config ファイルの変更（アクティブ スーパバイザ エンジン上でファイルが削除された場合は、スタンバイ スーパバイザ エンジン上でも削除されます）
- ブート ストリングの CONFIG_FILE 変数の設定変更
- 新しいスーパバイザ エンジンの搭載
- システムの起動

アクティブ スーパバイザ エンジンの CONFIG_FILE 変数が、スタンバイ スーパバイザ エンジン上でも同一に保持されます。アクティブ スーパバイザ エンジンの各 auto-config ファイルが、スタンバイ スーパバイザ エンジンの対応する auto-config ファイルと比較されます。2 つのファイルの長さおよび Cyclic Redundancy Check（CRC; 巡回冗長検査）が同じであれば、それらのファイルは同一とみなされます。スタンバイ スーパバイザ エンジン上のファイルがアクティブ スーパバイザ エン

ジン上のファイルと同じでなければ、アクティブ スーパバイザ エンジン上のファイル名を使用して、スタンバイ スーパバイザ エンジン上に新しいファイルが作成されます。スタンバイ スーパバイザ エンジン上に同名のファイルが存在する場合には、上書きされます。

同期化をイネーブルまたはディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
同期化をイネーブルにするか、ディセーブルにするかを指定します。	**set boot config-register auto-config sync** {**enable** | **disable**}

次に、同期化をイネーブルにする例を示します。

```
Console> (enable) set boot config-register auto-config sync enable
Configuration register is 0x12F
ignore-config: disabled
auto-config: recurring, append, sync enabled
console baud: 9600
boot: image specified by the boot system commands
Console> (enable)
```

次に、同期化をディセーブルにする例を示します。

```
Console> (enable) set boot config-register auto-config sync disable
Configuration register is 0x12F
ignore-config: disabled
auto-config: recurring, append, sync disabled
console baud: 9600
boot: image specified by the boot system commands
Console> (enable)
```

スイッチに NVRAM 内の設定情報を無視させる設定

次にスイッチを再起動するときに、NVRAM に保存されている設定情報をシステム ソフトウェアに無視させることができます。**set boot config-register ignore-config enable** コマンドが作用するのは、スイッチに NVRAM 内の設定を無視させるかどうかを制御するコンフィギュレーション レジスタ ビットだけです。他のビットの設定は変わりません。このコマンドは、次にスイッチを再起動したときにだけ作用します。

注意　**ignore-config** パラメータをイネーブルにすることは、**clear config all** コマンドを入力するのと同じことです。次回のスイッチ再起動時に、NVRAM に保存されているすべての設定が消去されます。

次回の再起動時に NVRAM 内の設定をスイッチに無視させるには、イネーブル モードで次のコマンドを入力します。

作業	コマンド
起動時に NVRAM の内容を無視するようにスイッチを設定します。	**set boot config-register ignore-config enable**

次に、次回の再起動時に NVRAM 内の設定を無視するようにスイッチを設定する例を示します。

```
Console> (enable) set boot config-register ignore-config enable
Configuration register is 0x1860
ignore-config: enabled
auto-config: recurring
console baud: 2400
boot: the ROM monitor
Console> (enable)
```

コンフィギュレーション レジスタ値の設定

コンフィギュレーション レジスタ値を設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
コンフィギュレーション レジスタを設定します。	**set boot config-register 0x***value* [*mod*]

次に、コンフィギュレーション レジスタ値を 0x90f に設定する例を示します。

```
Console> (enable) set boot config-register 0x90f
Configuration register is 0x90f
ignore-config: disabled
auto-config: non-recurring
console baud: 4800
boot: image specified by the boot system commands
Console> (enable)
```

BOOT 環境変数の設定

（注）　BOOT 環境変数の設定値が冗長スーパバイザ エンジン（存在する場合）に自動的にコピーされることはありません。スイッチ内の各スーパバイザ エンジンに、個別に BOOT 変数を設定する必要があります。

ここでは、BOOT 環境変数を変更する方法について説明します。

BOOT 環境変数の設定

BOOT 環境変数を設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
BOOT 環境変数を設定します。	**set boot system flash** *device:*[*filename*] [**prepend**] [*mod*]

次に、BOOT 環境変数を設定する例を示します。

```
Console> (enable) set boot system flash bootflash:cat6000-sup.5-5-1.bin
BOOT variable = bootflash:cat6000-sup.5-5-1.bin,1;
Console> (enable) set boot system flash bootflash:cat6000-sup.4-5-2.bin
BOOT variable = bootflash:cat6000-sup.5-1-1.bin,1;bootflash:cat6000-sup.4-5-2.
bin,1;
Console> (enable) set boot system flash bootflash:cat6000-sup.5-2-1.bin prepend
BOOT variable = bootflash:cat6000-sup.5-2-1.bin,1;bootflash:cat6000-sup.5-5-1.
bin,1;bootflash:cat6000-sup.4-5-2.bin,1;
Console> (enable)
```

BOOT 環境変数の設定値の消去

BOOT 環境変数からエントリを消去するには、イネーブル モードで次のいずれかの作業を行います。

作業	コマンド
BOOT 環境変数から特定のイメージを消去します。	**clear boot system flash** *device:*[*filename*] [*mod*]
BOOT 環境変数全体を消去します。	**clear boot system all** [*mod*]

次に、BOOT 環境変数から特定のエントリを消去する例を示します。

```
Console> (enable) clear boot system flash bootflash:cat6000-sup.5-1-1.bin
BOOT variable = bootflash:cat6000-sup.5-2-1.bin,1;bootflash:cat6000-sup.4-5-2.
bin,1;
Console> (enable)
```

次に、BOOT 環境変数全体を消去する例を示します。

```
Console> (enable) clear boot system all
BOOT variable =
Console> (enable)
```

CONFIG_FILE 環境変数の設定

ここでは、CONFIG_FILE 環境変数を変更する方法について説明します。

CONFIG_FILE 環境変数の設定

set boot auto-config コマンドを使用し、セミコロン（;）で区切ることにより、複数のコンフィギュレーション ファイルを指定できます。各コンフィギュレーション ファイルに、装置名とファイル名の両方を指定する必要があります。

(注)　CONFIG_FILE 環境変数の前後にコンフィギュレーション ファイルを付加することはできません。**set boot auto-config** コマンドを入力すると、それまで **set boot auto-config** コマンドによって指定されていたコンフィギュレーション ファイル リストが消去されます。

CONFIG_FILE 環境変数を設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
CONFIG_FILE 環境変数を設定します。	**set boot auto-config** *device:filename*[**;***device:filename*...]

次に、CONFIG_FILE 環境変数を設定する例を示します。

```
Console> (enable) set boot auto-config bootflash:generic.cfg;bootflash:6509_1_noc.cfg
CONFIG_FILE variable = bootflash:generic.cfg;bootflash:6509_1_noc.cfg
WARNING: nvram configuration may be lost during next bootup,
         and re-configured using the file(s) specified.
Console> (enable)
```

CONFIG_FILE 環境変数の設定値の消去

CONFIG_FILE 環境変数からエントリを消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
CONFIG_FILE 環境変数のエントリを消去します。	**clear boot auto-config**

次に、CONFIG_FILE 環境変数のエントリを消去する例を示します。

```
Console> (enable) clear boot auto-config
CONFIG_FILE variable =
Console> (enable)
```

スイッチの起動設定の表示

現在のコンフィギュレーション レジスタ、BOOT 環境変数、および CONFIG_FILE 環境変数の設定値を表示するには、次の作業を行います。

作業	コマンド
現在のコンフィギュレーション レジスタ、BOOT 環境変数、および CONFIG_FILE 環境変数の設定値を表示します。	**show boot** [*mod*]

次に、現在のコンフィギュレーション レジスタ、BOOT 環境変数、および CONFIG_FILE 環境変数の設定値を表示する例を示します。

```
Console> (enable) show boot
BOOT variable = bootflash:cat6000-sup.5-2-1.bin,1;
CONFIG_FILE variable = bootflash:generic.cfg;bootflash:6509_1_noc.cfg

Configuration register is 0x12f
ignore-config: disabled
auto-config: recurring
console baud: 9600
boot: image specified by the boot system commands

Console> (enable)
```

CHAPTER 25

フラッシュ ファイル システムの使用

この章では、Catalyst 6500 シリーズ スイッチ上でフラッシュ ファイル システムを使用する手順について説明します。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

この章で説明する内容は、次のとおりです。

フラッシュ ファイル システムの機能

Catalyst 6500 シリーズ スーパバイザ エンジンのフラッシュ ファイル システムには、ソフトウェア イメージおよびコンフィギュレーション ファイルの管理を容易に行うために役立つ多くのコマンドがあります。スーパバイザ エンジン上のフラッシュ ファイル システムは、次のフラッシュ デバイスから構成されています。どちらのデバイスにもファイルを保存できます。

- Supervisor Engine 1 および Supervisor Engine 2
  - **bootflash**：オンボード フラッシュ メモリ
  - **slot0**：リニア フラッシュ PC カード（PCMCIA スロット）
  - **disk0**：ATA フラッシュ PC カード（PCMCIA スロット）
- Supervisor Engine 720
  - **bootflash**：オンボード フラッシュ メモリ
  - **disk0**：CompactFlash Type II カードのみ（DISK 0 スロット）
  - **disk1**：CompactFlash Type II カード（DISK 1 スロット）
- Supervisor Engine 32
  - **bootflash**：オンボード フラッシュ メモリ
  - **disk0**：CompactFlash Type II カードのみ（DISK 0 スロット）

スイッチ上のフラッシュ ファイル システムの使用方法

ここでは、フラッシュ ファイル システムに関連するさまざまな手順について説明します。

デフォルト フラッシュ デバイスの設定

スイッチのデフォルト フラッシュ デバイスを設定しておくと、フラッシュ ファイル システム コマンドの入力時にフラッシュ デバイスを指定しなかった場合、デフォルトのデバイスが使用されます。

デフォルトのフラッシュ デバイスを設定するには、次の作業を行います。

	作業	コマンド
ステップ 1	スイッチのデフォルト フラッシュ デバイスを設定します。	**cd** [[*m*/][**bootflash:**| **slot0:**]]
ステップ 2	スイッチのデフォルト フラッシュ デバイスを確認します。	**pwd** [*mod*]

次に、デフォルト フラッシュ デバイスを **slot0:** に変更し、デフォルト デバイスを確認する例を示します。

```
Console> (enable) cd slot0:
Console> (enable) pwd
slot0
Console> (enable)
```

テキスト ファイル コンフィギュレーション モードの設定

テキスト ファイル コンフィギュレーション モードを使用した場合、スイッチはその設定をテキスト ファイルとして、NVRAM（不揮発性 RAM）またはフラッシュ メモリのいずれかの不揮発性記憶装置に保存します。このテキスト ファイルは、各種の機能を設定するようにユーザによって入力されたコマンドで構成されます。たとえば、ポートをディセーブルにする場合、そのポートをディセーブルにするコマンドをテキスト コンフィギュレーション ファイルに格納します。

テキスト ファイルにはスイッチを設定するために使用したコマンドしか含まれていないので、通常、バイナリ コンフィギュレーション モードよりも NVRAM またはフラッシュ メモリのメモリ容量が少なくてすみます。テキスト ファイルは通常、必要な容量が少ないので、NVRAM はファイルを保存するのに適した場所です。テキスト ファイルが NVRAM の容量を超える場合は、フラッシュ メモリに保存することもできます。

スイッチがテキスト ファイル コンフィギュレーション モードで稼働している場合、大部分のユーザ設定はすぐには NVRAM に保存されません。設定の変更は、DRAM に書き込まれるだけです。設定を不揮発性記憶装置に保存するには、**write memory** コマンドを実行する必要があります。

（注） VLAN Trunking Protocol（VTP;VLAN トランキング プロトコル）モードをサーバに設定した状態で、テキスト モードでスイッチを動作させている場合、VLAN（仮想 LAN）コマンドはコンフィギュレーション ファイルの一部としては保存されません。

テキスト ファイル コンフィギュレーション モードを設定するには、次の作業を行います。

	作業	コマンド
ステップ 1	システムのファイル コンフィギュレーション モードをテキストに設定します。	**set config mode text** {**nvram** | *device:file-id*}
ステップ 2	システムのファイル コンフィギュレーション モードを確認します。	**show config mode**
ステップ 3	テキスト ファイル コンフィギュレーションを保存します。	**write memory**
ステップ 4	現在の実行コンフィギュレーションを表示します。	**show running-config all**
ステップ 5	次のリセット後に使用されるスタートアップ コンフィギュレーションを表示します。	**show config**

次に、設定をテキスト ファイルとして NVRAM に保存するようにシステムを設定し、コンフィギュレーション モードを確認し、現在の実行コンフィギュレーションを表示する例を示します。

```
Console> (enable) set config mode text nvram
Console> (enable) show config mode
Console> (enable) show running-config all
Console> (enable) show config
Console> (enable)
```

テキスト ファイル コンフィギュレーション モードの Auto-Save 設定

set config mode text auto-save コマンドを使用して、テキスト コンフィギュレーションの NVRAM への自動保存を設定します。**interval** キーワードを使用して、テキスト コンフィギュレーションが NVRAM に保存される間隔を設定します。テキスト コンフィギュレーションが NVRAM に保存される間隔の設定は、システムがバイナリ モードであっても可能です。**interval** キーワードのあとに数値（分）を指定しなければ、間隔はデフォルトの 30 秒に設定されます。

テキスト コンフィギュレーションは、Auto-Save がイネーブルでなければ、NVRAM に自動保存されません。Auto-Save をイネーブルにするには、まずシステム コンフィギュレーション モードをテキストに設定し、さらにテキスト コンフィギュレーションを NVRAM に保存するようにシステムを設定する必要があります。システム コンフィギュレーション モードがバイナリ モードに設定されている場合は、Auto-Save をイネーブルにすることはできません。

テキスト ファイル コンフィギュレーション モードを Auto-Save に設定するには、次の作業を行います。

	作業	コマンド
ステップ 1	システムのファイル コンフィギュレーション モードをテキストに設定します。	**set config mode text** {**nvram** | *device:file-id*}
ステップ 2	**auto-save** キーワードを指定します。	**set config mode text auto-save** {**enable** | **disable**}
ステップ 3	（任意）**interval** キーワードを設定します。	**set config mode text auto-save interval** *mins*
ステップ 4	システムのファイル コンフィギュレーション モードを確認します。	**show config mode**
ステップ 5	テキスト ファイル コンフィギュレーションを保存します。	**write memory**
ステップ 6	現在の実行コンフィギュレーションを表示します。	**show running-config all**
ステップ 7	次のリセット後に使用されるスタートアップ コンフィギュレーションを表示します。	**show config**

次に、コンフィギュレーション モードをテキストに設定し、テキスト コンフィギュレーション ファイルを保存する場所とファイル名を指定する例を示します。

```
Console> (enable) set config mode text bootflash:switch.cfg
Binary system configuration has been deleted from NVRAM. Configuration mode set to
text. Use the write memory command to save configuration
changes. System configuration file set to: bootflash:switch.cfg
The file specified will be used for configuration during the next bootup.
Console> (enable)
```

次に、コンフィギュレーションがテキスト モードに設定され、システムがテキスト コンフィギュレーションを NVRAM に保存するように設定されている場合に、Auto-Save をイネーブルにする例を示します。

```
Console> (enable) set config mode text auto-save enable
auto-save feature has been enabled
auto-save feature has started
Please do a write mem manually if you plan to reboot the switch or any card before
first expiry of the timer
Console> (enable)
```

次に、コンフィギュレーションがテキスト モードに設定されておらず、システムがテキスト コンフィギュレーションを NVRAM に保存するように設定されていない場合に、Auto-Save をイネーブルにしようとした場合に表示されるメッセージの例を示します。

```
Console> (enable) set config mode text auto-save enable
auto-save cannot be enabled unless config mode is set to text and config file is
stored in nvram.
Use the 'set config mode text nvram' command to enable automatic saving of the system
configuration to nvram
Console> (enable)
```

次に、保存する間隔を 2,880 分に設定する例を示します。

```
Console> (enable) set config mode text auto-save interval 2880
auto-save interval set to 2880 minutes
Console> (enable)
```

次に、保存する間隔をデフォルト設定である 30 分に設定する例を示します。

```
Console> (enable) set config mode text auto-save interval
auto-save interval set to 30 minutes
Console> (enable)
```

フラッシュ デバイス上のファイルのリスト表示

フラッシュ デバイス上のファイルのリストを表示するには、次のいずれかの作業を行います。

作業	コマンド
フラッシュ デバイス上のファイルのリストを表示します。	**dir** [[*m*/]*device:*][*filename*]
フラッシュ デバイスから削除されたファイルのリストを表示します。	**dir** [[*m*/]*device:*][*filename*] **deleted**
削除されたファイルを含むフラッシュ デバイス上のすべてのファイルのリストを表示します。	**dir** [[*m*/]*device:*][*filename*] **all**
フラッシュ デバイス上のファイルの詳細リストを表示します。	**dir** [[*m*/]*device:*][*filename*] **long**

次に、デフォルト フラッシュ デバイス上のファイルのリストを表示する例を示します。

```
Console> (enable) dir
-#- -length- -----date/time------ name
  4  3134688 Mar 15 1999 08:27:01 cat6000-sup.5-2-1-CSX.bin
  5  3231989 Jan 24 1999 12:04:40 cat6000-sup.5-1-1-CSX.bin
  6      135 Feb 17 1999 11:30:05 dns_config.cfg

1213952 bytes available (6388224 bytes used)
Console> (enable)
```

次に、デフォルト デバイス以外のフラッシュ デバイス上に置かれているファイルのリストを表示する例を示します。

```
Console> (enable) dir slot0:
-#- -length- -----date/time------ name
  1  3209261 Jun 16 1998 13:18:19 cat6000-sup.5-2-1-CSX.bin
  2      135 Jul 17 1998 11:32:53 dns-config.cfg
  3  3231989 Jul 17 1998 16:54:23 cat5000-sup3.4-1-2.bin
  4     8589 Jul 17 1998 17:02:52 6000_config.cfg

9933504 bytes available (6450496 bytes used)
Console> (enable)
```

次に、デフォルト フラッシュ デバイス上の削除されたファイルのリストを表示する例を示します。

```
Console> (enable) dir deleted
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
  1 .D ffffffff 81a027ca   41bdc   22     7004 Apr 01 1998 15:27:45 5002.config.
4.1.98.cfg
  2 .D ffffffff ccce97a3   43644   23     6630 Apr 01 1998 15:36:47 5002.default
.config.cfg
  3 .D ffffffff 81a027ca   45220   15     7004 Apr 19 1998 10:05:59 5002_config.
cfg

1213952 bytes available (6388224 bytes used)
Console> (enable)
```

ファイルのコピー

ファイルをコピーするには、イネーブル モードで次のいずれかの作業を行います。

作業	コマンド
フラッシュ ファイルを Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバ、Remote Copy Protocol（RCP）サーバ、フラッシュ メモリ、別のフラッシュ デバイス、または実行コンフィギュレーションにコピーします。	**copy** *file-id* {**tftp** | **rcp** | **flash** | *file-id* | **config**}
TFTP サーバまたは RCP サーバからフラッシュ メモリ、フラッシュ デバイス、または実行コンフィギュレーションにファイルをコピーします。	**copy** {**tftp** | **rcp**} {**flash** | *file-id* | **config**}
フラッシュ メモリから TFTP サーバ、RCP サーバ、フラッシュ デバイス、または実行コンフィギュレーションにファイルをコピーします。	**copy flash** {**tftp** | **rcp** | *file-id* | **config**}
実行コンフィギュレーションをフラッシュ メモリ、別のフラッシュ デバイス、TFTP サーバ、または RCP サーバにコピーします。	**copy config** {**flash** | *file-id* | **tftp** | **rcp**}

次に、デフォルトのフラッシュ デバイスから別のフラッシュ デバイスにファイルをコピーする例を示します。

```
Console> (enable) copy cat6000-sup.5-2-1-CSX.bin slot0:

13174216 bytes available on device slot0, proceed (y/n) [n]? y
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCcccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
File has been copied successfully.
Console> (enable)
```

次に、TFTP サーバから実行コンフィギュレーションにファイルをコピーする例を示します。

```
Console> (enable) copy tftp config
IP address or name of remote host []? 172.20.52.3
Name of file to copy from []? dns_config.cfg

Configure using tftp:dns_config.cfg (y/n) [n]? y
/
Finished network download.  (135 bytes)
>>
>> set ip dns server 172.16.10.70 primary
172.16.10.70 added to DNS server table as primary server.
>> set ip dns server 172.16.10.140
172.16.10.140 added to DNS server table as backup server.
>> set ip dns enable
DNS is enabled
>> set ip dns domain corp.com
Default DNS domain name set to corp.com
Console> (enable)
```

次に、TFTP サーバからコンフィギュレーション ファイルをダウンロードして、フラッシュ デバイス上に保存する例を示します。

```
Console> (enable) copy tftp flash
IP address or name of remote host []? 172.20.52.3
Name of file to copy from []? dns-config.cfg
Flash device [slot0]?
Name of file to copy to [dns-config.cfg]?

9932056 bytes available on device slot0, proceed (y/n) [n]? y
/
File has been copied successfully.
Console> (enable)
```

次に、フラッシュ メモリに実行コンフィギュレーションをコピーする例を示します。

```
Console> (enable) copy config flash
Flash device [bootflash]? slot0:
Name of file to copy to []? 6000_config.cfg

Upload configuration to slot0:6000_config.cfg
9942096 bytes available on device slot0, proceed (y/n) [n]? y
.....
..........
.......

..........
...........
..

Configuration has been copied successfully.
Console> (enable)
```

次に、TFTP サーバにフラッシュ デバイス上のコンフィギュレーション ファイルをアップロードする例を示します。

```
Console> (enable) copy slot0:6000_config.cfg tftp
IP address or name of remote host []? 172.20.52.3
Name of file to copy to [6000_config.cfg]?
/
File has been copied successfully.
Console> (enable)
```

次に、RCP を使用して、リモート ホストからフラッシュにイメージをアップロードする例を示します。

```
Console> (enable) copy rcp flash
IP address or name of remote host []? 172.20.52.3
Name of file to copy from []? 6000_config.cfg
Flash device [bootflash]?
Name of file to copy to [6000_config.cfg]?

4369664 bytes available on device bootflash, proceed (y/n) [n]? y
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCC
File has been copied successfully.
Console> (enable)
```

ファイルの削除

注意　フラッシュ デバイス上で **squeeze** コマンドを実行すると、**squeeze** コマンドの実行前に削除したファイルは復元できなくなります。

フラッシュ デバイス上のファイルを削除するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	フラッシュ デバイス上のファイルを削除します。	**delete** [[*m*/]*device:*]*filename*
ステップ 2	必要に応じて、フラッシュ デバイス上のすべての削除ファイルを永久に削除します（この処理には数分かかることがあります)。	**squeeze** [*m*/]*device:*
ステップ 3	ファイルが削除されたことを確認します。	**dir** [[*m*/]*device***:**][*filename*]

次に、フラッシュ デバイスからファイルを削除する例を示します。

```
Console> (enable) delete dns_config.cfg
Console> (enable)
```

次に、フラッシュ デバイスからすべての削除されたファイルを永久に削除する例を示します。

```
Console> (enable) squeeze slot0:
All deleted files will be removed, proceed (y/n) [n]? y
Squeeze operation may take a while, proceed (y/n) [n]? y
Erasing squeeze log
Console> (enable)
```

削除されたファイルの復元

復元するファイルを特定するには、削除されたファイルのインデックス番号を指定する必要があります。各ファイルのインデックス番号は、**dir** コマンド出力の最初のカラムに表示されます。同名の有効ファイルがすでに存在している場合、ファイルを復元することはできません。既存のファイルを削除してから、同名のファイルを復元してください。1 ファイルにつき、15 回まで削除と復元を繰り返すことができます。

フラッシュ デバイス上の削除されたファイルを復元するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	フラッシュ デバイス上の削除されたファイルのインデックス番号を調べます。	**dir** [[*m*/]*device*:][*filename*] **deleted**
ステップ 2	フラッシュ デバイス上の削除されたファイルを復元します。	**undelete** *index* [[*m*/]*device*:]
ステップ 3	ファイルが復元されたことを確認します。	**dir** [[*m*/]*device*:][*filename*]

次に、削除されたファイルを復元する例を示します。

```
Console> (enable) dir deleted
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
6 .D ffffffff 42da7f71  657a00   14      135 Jul 17 1998 11:30:05 dns_config.cfg

1213952 bytes available (6388224 bytes used)
Console> (enable) undelete 6
Console> (enable) dir
-#- -length- -----date/time------ name
  4  3134688 Apr 27 1998 08:27:01 cat6000-sup.5-2-1.bin
  5  3231989 Jun 24 1998 12:04:40 cat6000-sup.5-2-1.bin
  6      135 Jul 17 1998 11:30:05 dns_config.cfg

1213952 bytes available (6388224 bytes used)
Console> (enable)
```

ファイルのチェックサムの確認

フラッシュ デバイス上のファイルのチェックサムを確認するには、イネーブル モードで次の作業を行います。

作業	コマンド
フラッシュ デバイス上のファイルのチェックサムを確認します。	**verify** [[*m*/]*device:*]*filename*

次に、ファイルのチェックサムを確認する例を示します。

```
Console> (enable) verify cat6000-sup.5-2-1-CSX.bin
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCC
File bootflash:cat6000-sup.5-2-1-CSX.bin verified OK
Console> (enable)
```

フラッシュ デバイスのフォーマット

一部のフラッシュ デバイスはフォーマットしてからでないと使用できません。設定したセクタが使用できなくなった場合に備えて、最大 16 の予備セクタを確保できます（デフォルトの設定では確保されません）。予備セクタを確保していないと、一部のセクタで問題が生じた場合、フラッシュ メモリ全体を再フォーマットする必要があり、既存のすべてのデータが消去されます。

（注） Supervisor Engine 2 および Supervisor Engine 1 では、フラッシュ PC カードのフォーマットが異なります。Supervisor Engine 2 で使用するフラッシュ PC カードは、Supervisor Engine 2 でフォーマットする必要があります。Supervisor Engine 1 で使用するフラッシュ PC カードは、Supervisor Engine 1 でフォーマットする必要があります。

(注) Supervisor Engine 1 または Route-Switch Processor（RSP）ベースの Cisco 7500 シリーズ ルータ上でフォーマットしたフラッシュ PC カードは、ルータでスーパバイザ エンジンと同じレベルまたはそれ以上のソフトウェアが稼働していれば、相互に交換できます。Route Processor（RP; ルート プロセッサ）ベースの Cisco 7000 シリーズ ルータでフォーマットしたフラッシュ PC カードを使用するには、再フォーマットが必要です。

フラッシュ デバイスのフォーマット時に、ROM モニタからフラッシュ ファイル システムのファイルにアクセスするための *monlib* ファイル（ROM モニタ ライブラリ）を指定できます。monlib ファイルは、ソフトウェア イメージにも組み込まれます。

format コマンドの引数 *device2* で、使用する monlib ファイルが保存されているデバイスを指定します。*device2* 引数全体を省略すると、スイッチはソフトウェアにバンドルされた monlib ファイルを使用してデバイスをフォーマットします。[[*device2:*][*monlib-filename*]] 引数でデバイス名（*device2*）だけを省略すると、スイッチはデフォルト フラッシュ デバイスに保存されている指定の monlib ファイルを使用してデバイスをフォーマットします。[[*device2:*][*monlib-filename*]] 引数で *monlib-filename* を省略すると、スイッチは *device2* の monlib ファイルを使用してデバイスをフォーマットします。[[*device2:*][*monlib-filename*]] 引数全体を指定すると、スイッチは指定されたデバイスの指定された monlib ファイルを使用してデバイスをフォーマットします。monlib ファイルが見つからない場合には、フォーマット処理が打ち切られます。

(注) フラッシュ デバイスにボリューム ID がある場合は、ボリューム ID を指定してデバイスをフォーマットする必要があります。ボリューム ID は、**show flash** *m/device*:**filesys** コマンドで表示されます。

フラッシュ デバイスをフォーマットするには、イネーブル モードで次の作業を行います。

作業	コマンド
フラッシュ デバイスをフォーマットします。	**format** [**spare** *spare-number*] [*m/*]*device1:*[[*device2:*][*monlib-filename*]]

次に、slot0: のフラッシュ デバイスをフォーマットする例を示します。

```
Console> (enable) format slot0:
All sectors will be erased, proceed (y/n) [n]?y
Enter volume id (up to 31 characters):
Formatting sector 1
Format device slot0 completed.
Console> (enable)
```

CHAPTER 26

システム ソフトウェア イメージの操作

この章では、Catalyst 6500 シリーズ スイッチ上でシステム ソフトウェア イメージ ファイルを操作する方法について説明します。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

この章で説明する内容は、次のとおりです。

ソフトウェア イメージの命名規則

Catalyst 6500 シリーズ スイッチ上のソフトウェア イメージでは、次の命名規則を使用します（例では Supervisor Engine 2 Release 7.3(1) のソフトウェア リリース イメージを使用）。

- 7.3(1) フラッシュ イメージ（標準）— cat6000-sup2k8.7-3-1.bin
- 7.3(1) フラッシュ イメージ（CiscoView）— cat6000- sup2cvk8.7-3-1.bin
- 7.3(1) フラッシュ イメージ（Secure Shell [SSH; セキュア シェル]）— cat6000-sup2k9.7-3-1.bin
- 7.3(1) フラッシュ イメージ（SSH および CiscoView）— cat6000-sup2cvk9.7-3-1.bin

（注） sup2cvk8、sup2k9、および sup2cvk9 の指定は次のとおりです。sup2cvk8 は CiscoView イメージ、sup2k9 は SSH イメージ、sup2cvk9 は SSH および CiscoView イメージです。

EPLD イメージのアップグレード

（注） スーパバイザ エンジン EPLD アップグレードは、Supervisor Engine 2 および Supervisor Engine 720 でしかサポートされていません。スーパバイザ エンジン以外のモジュール（スイッチング モジュールおよびサービス モジュール）の EPLD アップグレードは、Supervisor Engine 1、Supervisor Engine 2、または Supervisor Engine 720 を使用してサポートされています。

Supervisor Engine 2 および Supervisor Engine 720 の EPLD イメージは、Catalyst スーパバイザ エンジン ソフトウェア イメージに組み込まれています。スーパバイザ エンジン以外のモジュールの EPLD イメージは、個別のダウンロード可能イメージで提供されます。

スーパバイザ エンジン EPLD イメージのアップグレード

スーパバイザ エンジン EPLD のアップグレードは、スイッチをリセットするかいったん電源を切ってから再投入すると、自動的に実行されます。EPLD アップグレードのプロセスは、**set system supervisor-update** コマンドを使用して変更できます。スーパバイザ エンジン EPLD のアップグレードは、デフォルトでは、ディセーブルに設定されています。**automatic** モードでは、システムはバンドルされた EPLD イメージのバージョン レベルを調べ、そのバージョンが既存のイメージのものより新しい場合はアップグレードを実行します。キーワード **force** を指定すると、バージョン レベルに関係なく既存の EPLD イメージがバンドルされた EPLD イメージにアップグレードされます。強制アップグレード後、設定はデフォルト設定の **automatic** に戻ります。キーワード **disable** は、自動 EPLD アップグレードのプロセスをディセーブルにします。

スーパバイザ エンジン EPLD イメージをアップグレードするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スーパバイザ エンジン EPLD イメージをアップグレードします。	**set system supervisor-update** {**automatic** | **disable** | **force**}
ステップ 2	スーパバイザ エンジン EPLD イメージのアップグレードを確認します。	**show system supervisor-update**

次に、EPLD のアップグレードに **automatic** キーワードを指定する例を示します。

```
Console> (enable) set system supervisor-update automatic
Down-rev supervisor EPLD's will be re-programmed next reset.
Console> (enable)
```

次に、EPLD のアップグレードに **force** キーワードを指定する例を示します。

```
Console> (enable) set system supervisor-update force
Supervisor EPLD's will synchronize to the image bundle during the next reset.
Console> (enable)
```

次に、EPLD のアップグレードをディセーブルにする例を示します。

```
Console> (enable) set system supervisor-update disable
Supervisor EPLD update during reset is disabled.
Console> (enable)
```

次に、EPLD のアップグレード設定を表示する例を示します。

```
Console> (enable) show system supervisor-update
Supervisor EPLD update: disabled
Console> (enable)
```

スーパバイザ エンジン以外のモジュールの EPLD イメージのアップグレード

注意　アップグレード プロセスの間は、スイッチやモジュールの電源を切ったり、リセットしたりしないでください。モジュールが使用できない状態になることがあります。

（注）　この章の手順を開始する前に、スーパバイザ エンジンのフラッシュ メモリ（bootflash: または slot0:）に新しい EPLD アップグレード イメージをダウンロード済みであることを確認してください。

download コマンドにキーワード **epld** を指定することで、スーパバイザ エンジン以外のモジュールの EPLD イメージをアップグレードできます。モジュールを指定しないで **download epld** *file* コマンドを入力すると、モジュールの既存の EPLD イメージのバージョンより新しいバージョンの EPLD イメージが、すべての互換モジュールにダウンロードされます。キーワード **force** を指定して **download epld** *file mod* コマンドを実行すると、モジュールの既存の EPLD イメージは、既存のバージョン レベルに関係なく新しい EPLD イメージにアップグレードされます。

スーパバイザ エンジン以外のモジュール（スイッチング モジュールおよびサービス モジュール）の EPLD をアップグレードするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スーパバイザ エンジン以外の EPLD イメージをアップグレードします。	**download epld** *file* **download epld** *file mod* [**force**]
ステップ 2	EPLD アップグレード プロセスの設定を確認します。	**show version epld** *mod*

次に、スロット 5 にあるモジュール上の EPLD イメージをアップグレードする例を示します。

```
Console> (enable) download epld aq_cr128_art.bin 5 force
CCCCCC
Device found requiring upgrade in slot 5.

##########################################################
#                   W A R N I N G                        #
#                                                        #
# Any disruptions to the module during programming may   #
# leave the module or system in an inconsistent state.   #
# Please ensure that the system or module does not get   #
# switched off or reset during the programming process.  #
# Programming may take a minute or two, depending on     #
# the number of devices updated.  Please wait for the    #
# module to come back online before continuing.          #
#                                                        #
#                   W A R N I N G                        #
##########################################################
This command may reset module 5.
Updating fabric modules may significantly affect system performance while the update
is occurring.

Do you wish to update the devices in slot 5 (y/n) [n]? y

Updating programmable devices in slot 5.  This may take a minute...
Programming successful, updating EPLD revisions.
2002 Aug 09 06:32:22 %SYS-4-NVLOG:EpldUpdate:Module 5 EPLD A updated from rev 1 to rev
1
Waiting for module to come online.
.........2002 Aug 09 06:32:33 %SYS-5-MOD_OK:Module 5 is online
.

###############################################################################

               E P L D   P R O G R A M M I N G   C O M P L E T E

    Found 1 devices requiring upgrades, 1 attempted, 1 updated, 0 failed

###############################################################################
Console> (enable) 2002 Aug 09 06:32:34 %SYS-4-NVLOG:EpldUpdate:Module 5 EPLD A s
prom updated to rev 1
Console> (enable)
```

FTP または TFTP によるソフトウェア イメージのスイッチへのダウンロード

ここでは、スイッチのスーパバイザ エンジンおよびインテリジェント モジュールに、システム ソフトウェア イメージをダウンロードする方法について説明します。

FTP および TFTP によるソフトウェア イメージのダウンロードの概要

FTP（ファイル転送プロトコル）または Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）を使用して、システム ソフトウェア イメージをスイッチにダウンロードできます。TFTP を使用すると、TFTP サーバからネットワーク経由でシステム イメージ ファイルをダウンロードできます。FTP を使用すると、FTP サーバからネットワーク経由でシステム イメージ ファイルをダウンロードできます。

Asynchronous Tranfer Mode（ATM; 非同期転送モード）モジュールなど、一部のモジュールには専用のオンボード フラッシュ メモリがあります。ソフトウェア イメージ ファイルをダウンロードすると、スイッチはイメージ ファイルのヘッダーをチェックし、ソフトウェア イメージのタイプを判別します。

ダウンロードするソフトウェア イメージのタイプに応じて、次のいずれかの処理が実行されます。

- スーパバイザ エンジン ソフトウェア イメージの場合 — イメージ ファイルは、スーパバイザ エンジンのフラッシュ メモリにダウンロードされます。フラッシュ メモリ システム デバイス（ブート フラッシュ、フラッシュ PC カードなど）に、複数のイメージ ファイルを保存できます。
- インテリジェント モジュール ソフトウェア イメージの場合 — モジュール番号を指定すると、指定したモジュールだけにイメージ ファイルがダウンロードされます（ただし、イメージ ファイルが指定したモジュールのタイプである場合）。モジュール番号を指定しないと、該当タイプのすべてのモジュールにイメージ ファイルがダウンロードされます。ファイルは、システム内部のプロセス間通信プロトコルにより、スイッチング バスを経由して、パケット単位で各モジュールにリレーされます。イメージ ファイルが複数のモジュールにダウンロードされるので、同一タイプの複数のモジュール ソフトウェアをアップデートする場合、非常に短時間で処理できます。

（注）　フラッシュ ファイル システムにおけるシステム ソフトウェア イメージ ファイルの詳しい使用手順については、第 25 章「フラッシュ ファイル システムの使用」を参照してください。

FTP ユーザ名とパスワードの指定

FTP を使用する場合は、FTP 接続に使用するユーザ名とパスワードを指定できます。

ユーザ名とパスワードを指定するには、次の手順を実行します。

ステップ 1　**set ftp username** *new_ftp_username* コマンドを入力します。

ステップ 2　**set ftp password** コマンドを入力します。

次に、FTP ユーザ名を設定する例を示します。

```
Console> (enable) set ftp username doc_people
ftp username set to doc_people
```

次に、FTP パスワードを設定する例を示します。

```
Console> (enable) set ftp password
Enter password for User 'doc_people':
Retype password for User 'doc_people':
ftp password set.
```

次に、FTP ユーザ名を消去する例を示します。

```
Console> (enable) clear ftp username
```

次に、FTP パスワードを消去する例を示します。

```
Console> (enable) clear ftp password
```

パッシブ モードを使用して FTP サーバに接続することもできます。パッシブ モードでは、クライアントがサーバへの接続を開始します。パッシブ モードを使用するには、**set ftp passive** コマンドを実行します。

FTP または TFTP によるイメージ ダウンロードの準備

FTP または TFTP を使用してソフトウェア イメージをダウンロードする前に、次の作業が必要です。

- TFTP サーバとして動作するワークステーションが、正しく設定されていることを確認します。Sun ワークステーション上で TFTP を使用する場合、/etc/inetd.conf ファイルに次の行が含まれていることを確認します。

  ```
  tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot
  ```

  /etc/services ファイルに次の行が含まれていることを確認します。

  ```
  tftp 69/udp
  ```

  Sun ワークステーション上で FTP を使用する場合、/etc/inetd.conf ファイルに次の行が含まれていることを確認します。

  ```
  ftp stream tcp nowait root /usr/sbin/tcpd in.ftpd
  ```

  /etc/services ファイルに次の行が含まれていることを確認します。

  ```
  ftp 21/udp
  ```

（注） /etc/inetd.conf ファイルおよび /etc/services ファイルを変更したあとで、inetd デーモンを再起動する必要があります。デーモンを再起動するには、inetd プロセスをいったん中止してから再起動するか、**fastboot** コマンド（SunOS 4.x）または **reboot** コマンド（Solaris 2.x または SunOS 5.x）を入力します。FTP または TFTP デーモンの詳しい使用方法については、使用しているワークステーションのマニュアルを参照してください。

- スイッチに FTP または TFTP サーバへのルートが設定されていることを確認します。サブネット間でトラフィックをルーティングするルータを設定していない場合、スイッチと FTP または TFTP サーバは同じサブネットに置かれていなければなりません。**ping** コマンドを入力して、FTP または TFTP サーバに接続できるかどうかを確認してください。
- ダウンロードするソフトウェア イメージが、FTP または TFTP サーバの正しいディレクトリに存在することを確認します。
- ファイルに対する許可が正しく設定されていることを確認します。ファイルの許可は world-read に設定されていなければなりません。
- ダウンロードの処理中に停電（または他の問題）が生じると、フラッシュ コードが壊れることがあります。フラッシュ コードが壊れた場合には、コンソール ポートを通じてスイッチに接続し、フラッシュ PC カード上の壊れていないシステム イメージを使用して起動することができます。

FTP または TFTP によるスーパバイザ エンジン イメージのダウンロード

（注） スーパバイザ エンジンを冗長構成にしている場合、FTP または TFTP サーバからスタンバイ スーパバイザ エンジンのフラッシュ メモリに、システム イメージを直接ダウンロードすることはできません。アクティブ スーパバイザ エンジンにイメージをダウンロードすると、スタンバイ スーパバイザ エンジンが新しいイメージで自動的に同期されます。また、スタンバイ スーパバイザ エンジンのイメージを、アクティブ スーパバイザ エンジンにコピーすることはできません。

FTP または TFTP サーバからスイッチにスーパバイザ エンジン ソフトウェア イメージをダウンロードするには、次の手順を実行します。

ステップ 1　ソフトウェア イメージ ファイルをワークステーションの適切な FTP または TFTP ディレクトリにコピーします。

ステップ 2　コンソール ポートから、または Telnet セッションを使用して、スイッチにログインします。Telnet でログインした場合、新しいソフトウェアを実行するために、スイッチをリセットした時点で、Telnet セッションが切断されます。

ステップ 3　**copy ftp flash** または **copy tftp flash** コマンドを実行します。プロンプトに、TFTP サーバの IP アドレスまたはホスト名、およびダウンロードするファイル名を入力します。フラッシュ ファイル システムをサポートするプラットフォームでは、ファイルのコピー先となるフラッシュ デバイスおよび宛先ファイル名を入力することも必要です。

スイッチは FTP または TFTP サーバから指定されたフラッシュ デバイスにイメージ ファイルをダウンロードします。

(注)　イメージのダウンロード中も、スイッチは稼働しています。

ステップ 4　**set boot system flash** *device*:*filename* **prepend** コマンドを使用して BOOT 環境変数を変更し、スイッチのリセット時に新しいイメージが起動するようにします。フラッシュ デバイス（*device*:）およびダウンロードされたイメージのファイル名（*filename*）を指定します。

ステップ 5　**reset system** コマンドを入力してスイッチをリセットします。Telnet 接続の場合には、Telnet セッションが切断されます。

起動時にスーパバイザ エンジンのフラッシュ メモリが、新しいフラッシュ コードを使用して書き換えられます。

ステップ 6　スイッチの再起動後、**show version** コマンドを入力して、スイッチ コードのバージョンを確認します。

(注)　各種スーパバイザ エンジンおよびスイッチ タイプの FTP または TFTP ダウンロード手順の例については、「FTP および TFTP によるダウンロード手順の例」（p.26-9）を参照してください。

FTP または TFTP によるスイッチング モジュール イメージのダウンロード

インテリジェント モジュールにソフトウェア イメージをダウンロードするには、次の手順を実行します。

ステップ 1　ソフトウェア イメージ ファイルをワークステーションの適切な FTP または TFTP ディレクトリにコピーします。

ステップ 2　コンソール ポートまたは Telnet セッションを使用して、スイッチにログインします。Telnet でログインした場合、新しいソフトウェアを実行するためにモジュールをリセットした時点で、Telnet セッションが切断される可能性があります。

ステップ 3　イメージに対応するタイプのモジュールが 1 つだけの場合、または対応するタイプのすべてのモジュールのイメージをアップデートする場合は、**copy ftp flash** または **copy tftp flash** コマンドを入力します。プロンプトに、TFTP サーバの IP アドレスまたはホスト名、ダウンロードするファイル名、ファイルのコピー先フラッシュ デバイス、および宛先ファイル名を指定します。

ステップ 4　イメージに対応するタイプのモジュールが複数あり、その中の 1 つのモジュールのイメージだけをアップデートする場合は、**copy ftp** *m*/**bootflash:** または **copy tftp** *m*/**bootflash:** コマンドを実行します。*m* には、ソフトウェア イメージをダウンロードするモジュールの番号を指定します。

(注)　モジュール番号を指定しなかった場合、イメージ ファイルのヘッダー情報から、ソフトウェアのダウンロード先モジュールが判別されます。この場合、イメージは対応するタイプのすべてのモジュールにダウンロードされます。

イメージ ファイルをダウンロードすると、対応するモジュールのフラッシュ メモリが消去され、ダウンロードしたフラッシュ コードに書き換えられます。

（注） イメージのダウンロード中も、スイッチのすべてのモジュールは稼働しています。

ステップ 5 **reset** *mod* コマンドを入力して、該当するモジュールをリセットします。Telnet で接続している場合、接続に使用したモジュールをリセットすると、Telnet セッションが切断されます。

ステップ 6 アップグレードしたモジュールがオンラインになってから、**show version** [*mod*] コマンドを使用して、スイッチ コードのバージョンを確認します。

（注） FTP および TFTP を使用してインテリジェント モジュールにダウンロードする手順の例については、「単一モジュールにイメージをダウンロードする例」（p.26-12）および「複数モジュールにイメージをダウンロードする例」（p.26-14）を参照してください。

FTP および TFTP によるダウンロード手順の例

ここでは、FTP および TFTP によるダウンロード手順の例を紹介します。

スーパバイザ エンジン イメージをダウンロードする例

（注） スーパバイザ エンジン ソフトウェア イメージを FTP または TFTP サーバからダウンロードする手順については、「FTP または TFTP によるスーパバイザ エンジン イメージのダウンロード」（p.26-7）を参照してください。

次に、Catalyst 6500 シリーズ スイッチにスーパバイザ エンジン ソフトウェア イメージを TFTP でダウンロードする例を示します。

```
Console> (enable) copy tftp flash
IP address or name of remote host []? 172.20.52.3
Name of file to copy from []? cat6000-sup.5-2-1-CSX.bin
Flash device [bootflash]?
Name of file to copy to [cat6000-sup.5-2-1-CSX.bin]?

4369664 bytes available on device bootflash, proceed (y/n) [n]? y
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCC
File has been copied successfully.

Console> (enable) set boot system flash bootflash:cat6000-sup.5-2-1-CSX.bin
BOOT variable = bootflash:cat6000-sup.5-2-1-CSX.bin,1;
Console> (enable) reset system
```

```
This command will reset the system.
Do you want to continue (y/n) [n]? y
Console> (enable) 07/21/1998,13:51:39:SYS-5:System reset from Console//

System Bootstrap, Version 4.2
Copyright (c) 1994-1998 by cisco Systems, Inc.
c6k_sup1 processor with 32768 Kbytes of main memory

Autoboot executing command: "boot bootflash:cat6000-sup.5-2-1-CSX.bin"
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCC
Uncompressing file:  ###########################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
#############

System Power On Diagnostics
DRAM Size ....................32 MB
Testing DRAM..................Passed
Verifying Text segment .......Passed
NVRAM Size ...................512 KB
Saving NVRAM .................
Testing NVRAM ................Passed
Restoring NVRAM...............
Level2 Cache ..................Present
Level2 Cache test..............Passed

Leaving power_on_diags

Cafe Daughter Present.

EOBC link up

Boot image: bootflash:cat6000-sup.5-2-1-CSX.bin
Flash Size = 0X1000000, num_flash_sectors = 64
readCafe2Version: 0x00000001
RIn Local Test Mode, Pinnacle Synch Retries: 2
Running System Diagnostics from this Supervisor (Module 1)
This may take up to 2 minutes....please wait

Cisco Systems Console



Enter password:
07/21/1998,13:52:51:SYS-5:Module 1 is online
07/21/1998,13:53:11:SYS-5:Module 4 is online
07/21/1998,13:53:11:SYS-5:Module 5 is online
07/21/1998,13:53:14:PAGP-5:Port 1/1 joined bridge port 1/1.
07/21/1998,13:53:14:PAGP-5:Port 1/2 joined bridge port 1/2.
07/21/1998,13:53:40:SYS-5:Module 2 is online
07/21/1998,13:53:45:SYS-5:Module 3 is online

Console>
```

次に、Catalyst 6500 シリーズ スイッチにスーパバイザ エンジン ソフトウェア イメージを FTP でダウンロードする例を示します。

```
Console> (enable) copy ftp flash
IP address or name of remote host []? 172.20.52.3
Name of file to copy from []? cat6000-sup2k8.7-7-1.bin
Flash device [bootflash]?
Name of file to copy to [cat6000-sup2k8.7-7-1.bin ]?

4369664 bytes available on device bootflash, proceed (y/n) [n]? y
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCC
File has been copied successfully.
Console> (enable) set boot system flash bootflash: cat6000-sup2k8.7-7-1.bin
BOOT variable = bootflash:cat6000-sup2k8.7-7-1.bin,1;
Console> (enable) reset system
This command will reset the system.
Do you want to continue (y/n) [n]? y
Console> (enable) 04/29/2003,13:51:39:SYS-5:System reset from Console//

System Bootstrap, Version 4.2
Copyright (c) 1994-1998 by cisco Systems, Inc.
c6k_sup1 processor with 32768 Kbytes of main memory

Autoboot executing command: "boot bootflash:cat6000-sup2k8.7-7-1.bin,1"
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCC
Uncompressing file:  ###########################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
#############

System Power On Diagnostics
DRAM Size ...................32 MB
Testing DRAM.................Passed
Verifying Text segment .......Passed
NVRAM Size ..................512 KB
Saving NVRAM ................
Testing NVRAM ................Passed
Restoring NVRAM..............
Level2 Cache ..................Present
Level2 Cache test.............Passed

Leaving power_on_diags

Cafe Daughter Present.

EOBC link up

Boot image: bootflash:cat6000-sup2k8.7-7-1.bin,1
Flash Size = 0X1000000, num_flash_sectors = 64
readCafe2Version: 0x00000001
RIn Local Test Mode, Pinnacle Synch Retries: 2
Running System Diagnostics from this Supervisor (Module 1)
This may take up to 2 minutes....please wait

Cisco Systems Console



Enter password:
07/21/1998,13:52:51:SYS-5:Module 1 is online
```

```
07/21/1998,13:53:11:SYS-5:Module 4 is online
07/21/1998,13:53:11:SYS-5:Module 5 is online
07/21/1998,13:53:14:PAGP-5:Port 1/1 joined bridge port 1/1.
07/21/1998,13:53:14:PAGP-5:Port 1/2 joined bridge port 1/2.
07/21/1998,13:53:40:SYS-5:Module 2 is online
07/21/1998,13:53:45:SYS-5:Module 3 is online
Console>
```

単一モジュールにイメージをダウンロードする例

(注)　インテリジェント モジュールにソフトウェア イメージをダウンロードする手順については、「FTP または TFTP によるスイッチング モジュール イメージのダウンロード」（p.26-8）を参照してください。

次に、単一の ATM モジュールに ATM ソフトウェア イメージを TFTP でダウンロードする例を示します。

```
Console> (enable) show version 4
Mod Port Model      Serial #  Versions
--- ---- ---------- --------- ----------------------------------------
4   1    WS-X6101   003414855 Hw : 1.2
                               Fw : 1.3
                               Sw : 3.2(6)

Console> (enable) copy tftp 4/flash
IP address or name of remote host []? 172.20.52.3
Name of file to copy from []? cat6000-atm.3-2-7.bin
Download image tftp:cat6000-atm.3-2-7.bin to Module 4 FLASH (y/n) [n]? y
This command will reset Download Module(s) you selected.

Do you wish to continue download flash (y/n) [n]? y
-
Download done for module 4, please wait for it to come online

File has been copied successfully.
Console> (enable) 07/21/1998,13:13:54:SYS-5:Module 4 is online

Console> (enable) show version 4
Mod Port Model      Serial #  Versions
--- ---- ---------- --------- ----------------------------------------
4   1    WS-X6101   003414855 Hw : 1.2
                               Fw : 1.3
                               Sw : 3.2(7)
Console> (enable)
```

次に、単一の ATM モジュールに ATM ソフトウェア イメージを FTP でダウンロードする例を示します。

```
Console> (enable) show version 4
Mod Port Model      Serial #  Versions
--- ---- ---------- --------- -----------------------------------------
4   1    WS-X6101   003414855 Hw : 1.2
                               Fw : 1.3
                               Sw : 3.2(6)

Console> (enable) copy ftp 4/flash
IP address or name of remote host []? 172.20.52.3
Name of file to copy from []? c6atm-lc-mz.121-14.E1.bin
Download image tftp:c6atm-lc-mz.121-14.E1.bin to Module 4 FLASH (y/n) [n]? y
This command will reset Download Module(s) you selected.

Do you wish to continue download flash (y/n) [n]? y
-
Download done for module 4, please wait for it to come online

File has been copied successfully.
Console> (enable) 04/29/2003,13:13:54:SYS-5:Module 4 is online

Console> (enable) show version 4
Mod Port Model      Serial #  Versions
--- ---- ---------- --------- -----------------------------------------
4   1    WS-X6101   003414855 Hw : 1.2
                               Fw : 1.3
                               Sw : 3.2(7)
Console> (enable)
```

複数モジュールにイメージをダウンロードする例

(注)　インテリジェント モジュールにソフトウェア イメージをダウンロードする手順については、「FTP または TFTP によるスイッチング モジュール イメージのダウンロード」（p.26-8）を参照してください。

次に、複数の ATM モジュールに ATM ソフトウェア イメージを TFTP でダウンロードする例を示します。

```
Console> (enable) show version 4
Mod Port Model      Serial #  Versions
--- ---- ---------- --------- -----------------------------------------
4   1    WS-X6101   003414855 Hw : 1.2
                               Fw : 1.3
                               Sw : 3.2(6)
Console> (enable) show version 5
Mod Port Model      Serial #  Versions
--- ---- ---------- --------- -----------------------------------------
5   1    WS-X6101   003414463 Hw : 1.2
                               Fw : 1.3
                               Sw : 3.2(6)
Console> (enable) copy tftp flash
IP address or name of remote host []? 172.20.52.3
Name of file to copy from []? cat6000-atm.3-2-7.bin
Download image tftp:cat6000-atm.3-2-7.bin to Module 4 FLASH (y/n) [n]? y
Download image tftp:cat6000-atm.3-2-7.bin to Module 5 FLASH (y/n) [n]? y
This command will reset Download Module(s) you selected.

Do you wish to continue download flash (y/n) [n]? y
-
Download done for module 4, please wait for it to come online

Download done for module 5, please wait for it to come online

File has been copied successfully.
Console> (enable) 07/21/1998,12:25:10:SYS-5:Module 4 is online
07/21/1998,12:25:10:SYS-5:Module 5 is online

Console> (enable) show version 4
Mod Port Model      Serial #  Versions
--- ---- ---------- --------- -----------------------------------------
4   1    WS-X6101   003414855 Hw : 1.2
                               Fw : 1.3
                               Sw : 3.2(7)
Console> (enable) show version 5
Mod Port Model      Serial #  Versions
--- ---- ---------- --------- -----------------------------------------
5   1    WS-X6101   003414463 Hw : 1.2
                               Fw : 1.3
                               Sw : 3.2(7)
Console> (enable)
```

FTP または TFTP サーバへのシステム ソフトウェア イメージのアップロード

ここでは、スイッチから FTP または TFTP サーバにシステム ソフトウェア イメージをアップロードする手順について説明します。

（注）　フラッシュ ファイル システムにおけるシステム ソフトウェア イメージ ファイルの詳しい使用手順については、第 25 章「フラッシュ ファイル システムの使用」を参照してください。

FTP または TFTP サーバへのイメージ アップロードの準備

FTP または TFTP サーバにソフトウェア イメージをアップロードする前に、次の作業が必要です。

- FTP または TFTP サーバとして動作するワークステーションが、正しく設定されていることを確認します。Sun ワークステーション上で FTP を使用する場合、/etc/inetd.conf ファイルに次の行が含まれていることを確認します。

  ```
  ftp stream tcp nowait root /usr/sbin/tcpd in.ftpd
  ```

  /etc/services ファイルに次の行が含まれていることを確認します。

  ```
  ftp 21/udp
  ```

  Sun ワークステーション上で TFTP を使用する場合、/etc/inetd.conf ファイルに次の行が含まれていることを確認します。

  ```
  tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot
  ```

  /etc/services ファイルに次の行が含まれていることを確認します。

  ```
  tftp 69/udp
  ```

  （注）　/etc/inetd.conf ファイルおよび /etc/services ファイルを変更したあとで、inetd デーモンを再起動する必要があります。デーモンを再起動するには、inetd プロセスをいったん中止してから再起動するか、**fastboot** コマンド（SunOS 4.x）または **reboot** コマンド（Solaris 2.x または SunOS 5.x）を入力します。TFTP デーモンの詳しい使用手順については、使用しているワークステーションのマニュアルを参照してください。

- スイッチに FTP または TFTP サーバへのルートが設定されていることを確認します。サブネット間でトラフィックをルーティングするルータを設定していない場合、スイッチと FTP または TFTP サーバは同じサブネットに置かれていなければなりません。**ping** コマンドを入力して、FTP または TFTP サーバに接続できるかどうかを確認してください。
- 必要に応じて、イメージをアップロードする前に、FTP または TFTP サーバ上に空のファイルを作成します。空のファイルを作成するには、**touch** *filename* コマンドを入力します。*filename* は、サーバにイメージをアップロードするときに使用するファイル名です。
- 既存ファイル（作成済みの空のファイルを含む）を上書きする場合は、ファイル許可が正しく設定されていることを確認します。ファイルの許可は world-write に設定されていなければなりません。

FTP または TFTP サーバへのソフトウェア イメージのアップロード

スイッチ上のソフトウェア イメージを FTP または TFTP サーバにアップロードするには、次の手順を実行します。

ステップ 1 コンソール ポートまたは Telnet セッションを使用して、スイッチにログインします。

ステップ 2 **copy flash ftp** または **copy flash tftp** コマンドを使用して、FTP または TFTP サーバにソフトウェア イメージをアップロードします。プロンプトに、FTP または TFTP サーバのアドレスおよび宛先ファイル名を指定します。フラッシュ ファイル システムをサポートするプラットフォーム上では、フラッシュ デバイスおよびソース ファイル名を尋ねるプロンプトが最初に表示されます。これらのプラットフォームでは、希望する場合 **copy** *file-id* **ftp** または **copy** *file-id* **tftp** コマンドを入力できます。

FTP または TFTP サーバにソフトウェア イメージがアップロードされます。

次に、TFTP を使用して、スーパバイザ エンジンのソフトウェア イメージをアップロードする例を示します。

```
Console> (enable) copy flash tftp
Flash device [bootflash]? slot0:
Name of file to copy from []? cat6000-sup.5-4-1.bin
IP address or name of remote host [172.20.52.3]? 172.20.52.10
Name of file to copy to [cat6000-sup.5-4-1.bin]?
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC|
File has been copied successfully.
Console> (enable)
```

RCP によるシステム ソフトウェア イメージのダウンロード

ここでは、スイッチのスーパバイザ エンジンおよびインテリジェント モジュールに、システム ソフトウェア イメージをダウンロードする方法について説明します。

RCP によるイメージ ダウンロードの準備

Remote Copy Protocol（RCP）を使用してソフトウェア イメージをダウンロードする前に、次の作業が必要です。

- RCP サーバとして動作するワークステーションが、Remote Shell（RSH）をサポートしていることを確認します。
- スイッチに RCP サーバへのルートが設定されていることを確認します。サブネット間でトラフィックをルーティングするルータを設定していない場合、スイッチと RCP サーバは同じサブネットに置かれていなければなりません。**ping** コマンドを入力して、RCP サーバに接続できるかどうかを確認してください。
- 有効なユーザ名を使用しないでコンソールまたは Telnet セッション経由でスイッチにアクセスしている場合、現在の RCP ユーザ名が RCP ダウンロードに使用する名前であることを確認してください。**show users** コマンドを入力すると、現在の有効なユーザ名を調べることができます。現在のユーザ名を使用しない場合は、**set rcp username** コマンドを入力して新しい RCP ユーザ名を作成します。新しいユーザ名は NVRAM（不揮発性 RAM）に保存されます。有効なユーザ名を使用して Telnet セッション経由でスイッチにアクセスしている場合、このユーザ名が使用されるので、RCP ユーザ名を設定する必要はありません。
- ダウンロードの処理中に停電（または他の問題）が生じると、フラッシュ コードが壊れることがあります。フラッシュ コードが壊れた場合には、コンソール ポートを通じてスイッチに接続し、フラッシュ PC カード上の壊れていないシステム イメージを使用して起動することができます。

RCP によるスーパバイザ エンジン イメージのダウンロード

RCP サーバからスイッチにスーパバイザ エンジン ソフトウェア イメージをダウンロードするには、次の手順を実行します。

ステップ 1　ソフトウェア イメージ ファイルをワークステーション上の適切な RCP ディレクトリにコピーします。

ステップ 2　コンソール ポートから、または Telnet セッションを使用して、スイッチにログインします。Telnet でログインした場合、新しいソフトウェアを実行するために、スイッチをリセットした時点で、Telnet セッションが切断されます。

ステップ 3　**copy rcp flash** コマンドを使用して、RCP サーバからソフトウェア イメージをダウンロードします。プロンプトに、RCP サーバの IP アドレスまたはホスト名、およびダウンロードするファイル名を入力します。フラッシュ ファイル システムをサポートするプラットフォームでは、ファイルのコピー先となるフラッシュ デバイスおよび宛先ファイル名を入力することも必要です。

スイッチは、RCP サーバからイメージ ファイルをダウンロードします。

(注)　イメージのダウンロード中も、スイッチは稼働しています。

ステップ 4　**set boot system flash** *device*:*filename* **prepend** コマンドを入力して BOOT 環境変数を変更し、スイッチのリセット時に新しいイメージが起動するようにします。フラッシュ デバイス（*device*:）およびダウンロードされたイメージのファイル名（*filename*）を指定します。

ステップ 5　**reset system** コマンドを入力してスイッチをリセットします。Telnet 接続の場合には、Telnet セッションが切断されます。

起動時にスーパバイザ エンジンのフラッシュ メモリが、新しいフラッシュ コードを使用して書き換えられます。

ステップ 6　スイッチの再起動後、**show version** コマンドを入力して、スイッチ コードのバージョンを確認します。

RCP によるスイッチング モジュール イメージのダウンロード

Catalyst 6500 シリーズ スイッチ上のインテリジェント モジュールにソフトウェア イメージをダウンロードするには、次の手順を実行します。

ステップ 1　ソフトウェア イメージ ファイルをワークステーション上の適切な RCP ディレクトリにコピーします。

ステップ 2　コンソール ポートまたは Telnet セッションを使用して、スイッチにログインします。Telnet でログインした場合、新しいソフトウェアを実行するためにモジュールをリセットした時点で、Telnet セッションが切断される可能性があります。

ステップ 3　各スイッチおよびスーパバイザ エンジンに対応するコマンドを使用して、RCP サーバからソフトウェア イメージをダウンロードします。

- イメージに対応するタイプのモジュールが 1 つだけの場合、または対応するタイプのすべてのモジュールのイメージをアップデートする場合は、**copy rcp flash** コマンドを入力します。プロンプトに、RCP サーバの IP アドレスまたはホスト名、ダウンロードするファイル名、ファイルのコピー先フラッシュ デバイス、および宛先ファイル名を指定します。
- イメージに対応するタイプのモジュールが複数あり、その中の 1 つのモジュールのイメージだけをアップデートする場合は、**copy rcp** | *m*/**bootflash:** コマンドを実行します。*m* には、ソフトウェア イメージをダウンロードするモジュールの番号を指定します。モジュールを指定しなかった場合は、同一タイプのモジュールがすべてアップデートされます。

(注)　モジュール番号を指定しなかった場合、イメージ ファイルのヘッダー情報から、ソフトウェアのダウンロード先モジュールが判別されます。この場合、イメージは対応するタイプのすべてのモジュールにダウンロードされます。

イメージ ファイルをダウンロードすると、対応するモジュールのフラッシュ メモリが消去され、ダウンロードしたフラッシュ コードに書き換えられます。

(注)　イメージのダウンロード中も、スイッチのすべてのモジュールは稼働しています。

ステップ 4　**reset** *mod* コマンドを使用して、該当するモジュールをリセットします。Telnet で接続している場合、接続に使用したモジュールをリセットすると、Telnet セッションが切断されます。

ステップ 5　アップグレードしたモジュールがオンラインになってから、**show version** [*mod*] コマンドを使用して、スイッチ コードのバージョンを確認します。

RCP によるダウンロード手順の例

ここでは、RCP によるダウンロード手順の例を紹介します。

- RCP でスーパバイザ エンジン イメージをダウンロードする例（p.26-19）
- RCP で単一モジュールにイメージをダウンロードする例（p.26-21）
- RCP で複数のモジュールにイメージをダウンロードする例（p.26-22）

RCP でスーパバイザ エンジン イメージをダウンロードする例

(注)　スーパバイザ エンジン ソフトウェア イメージを RCP サーバからダウンロードする手順については、「RCP によるスーパバイザ エンジン イメージのダウンロード」（p.26-17）を参照してください。

次に、Catalyst 6500 シリーズ スイッチにスーパバイザ エンジン ソフトウェア イメージを RCP でダウンロードする例を示します。

```
Console> (enable) copy rcp flash
IP address or name of remote host []? 172.20.52.3
Name of file to copy from []? cat6000-sup.5-2-1-csx.bin
Flash device [bootflash]?
Name of file to copy to [cat6000-sup.5-2-1-csx.bin]?

4369664 bytes available on device bootflash, proceed (y/n) [n]? y
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCC
File has been copied successfully.
Console> (enable) set boot system flash bootflash:cat6000-sup.5-2-1-csx.bin prepend
BOOT variable = bootflash:cat6000-sup.5-2-1-csx.bin,1;bootflash:cat6000-sup.5-2-
1-csx.bin,1;
Console> (enable) reset system
This command will reset the system.
Do you want to continue (y/n) [n]? y
Console> (enable) 09/2/1999,13:51:39:SYS-5:System reset from Console//

System Bootstrap, Version 4.2
Copyright (c) 1994-1999 by cisco Systems, Inc.
Presto processor with 32768 Kbytes of main memory

Autoboot executing command: "boot bootflash:cat6000-sup.5-2-1-csx.bin"
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCC
Uncompressing file:  ###########################################################
################################################################################
```

```
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
#############


System Power On Diagnostics
DRAM Size .....................32 MB
Testing DRAM...................Passed
Verifying Text segment .......Passed
NVRAM Size ....................512 KB
Saving NVRAM ..................
Testing NVRAM .................Passed
Restoring NVRAM................
Level2 Cache ..................Present
Level2 Cache test..............Passed

Leaving power_on_diags

Cafe Daughter Present.

EOBC link up

Boot image: bootflash:cat6000-sup.5-2-1-CSX.bin
Flash Size = 0X1000000, num_flash_sectors = 64
readCafe2Version: 0x00000001
RIn Local Test Mode, Pinnacle Synch Retries: 2
Running System Diagnostics from this Supervisor (Module 1)
This may take up to 2 minutes....please wait

Cisco Systems Console

Enter password:
09/2/1999,13:52:51:SYS-5:Module 1 is online
09/2/1999,13:53:11:SYS-5:Module 4 is online
09/2/1999,13:53:11:SYS-5:Module 5 is online
09/2/1999,13:53:14:PAGP-5:Port 1/1 joined bridge port 1/1.
09/2/1999,13:53:14:PAGP-5:Port 1/2 joined bridge port 1/2.
09/2/1999,13:53:40:SYS-5:Module 2 is online
09/2/1999,13:53:45:SYS-5:Module 3 is online
Console> (enable)
```

RCP で単一モジュールにイメージをダウンロードする例

(注) インテリジェント モジュールにソフトウェア イメージをダウンロードする手順については、「RCP によるスイッチング モジュール イメージのダウンロード」（p.26-18）を参照してください。

次に、単一の ATM モジュールに ATM ソフトウェア イメージを RCP でダウンロードする例を示します。

```
Console> (enable) show version 4
Mod Port Model      Serial #  Versions
--- ---- ---------- --------- -----------------------------------------
4   1    WS-X6101   003414855 Hw : 1.2
                               Fw : 1.3
                               Sw : 3.2(6)
Console> (enable) copy rcp 4/flash
IP address or name of remote host []? 172.20.52.3
Name of file to copy from []? cat6000-atm.3-2-7.bin
Download image rcp:cat6000-atm.3-2-7.bin to Module 4 FLASH (y/n) [n]? y
This command will reset Download Module(s) you selected.

Do you wish to continue download flash (y/n) [n]? y

Download done for module 4, please wait for it to come online

File has been copied successfully.
Console> (enable) 09/2/1999,13:13:54:SYS-5:Module 4 is online

Console> (enable) show version 4
Mod Port Model      Serial #  Versions
--- ---- ---------- --------- -----------------------------------------
4   1    WS-X6101   003414855 Hw : 1.2
                               Fw : 1.3
                               Sw : 3.2(7)
Console> (enable)
```

RCP で複数のモジュールにイメージをダウンロードする例

(注) インテリジェント モジュールにソフトウェア イメージをダウンロードする手順については、「RCP によるスイッチング モジュール イメージのダウンロード」（p.26-18）を参照してください。

次に、複数の ATM モジュールに ATM ソフトウェア イメージを RCP でダウンロードする例を示します。

```
Console> (enable) show version 4
Mod Port Model      Serial #  Versions
--- ---- ---------- --------- -----------------------------------------
4   1    WS-X6101   003414855 Hw : 1.2
                               Fw : 1.3
                               Sw : 3.2(6)
Console> (enable) show version 5
Mod Port Model      Serial #  Versions
--- ---- ---------- --------- -----------------------------------------
5   1    WS-X6101   003414463 Hw : 1.2
                               Fw : 1.3
                               Sw : 3.2(6)
Console> (enable) copy rcp flash
IP address or name of remote host []? 172.20.52.3
Name of file to copy from []? cat6000-atm.3-2-7.bin
Download image rcp:cat6000-atm.3-2-7.bin to Module 4 FLASH (y/n) [n]? y
Download image rcp:cat6000-atm.3-2-7.bin to Module 5 FLASH (y/n) [n]? y
This command will reset Download Module(s) you selected.

Do you wish to continue download flash (y/n) [n]? y
-
Download done for module 4, please wait for it to come online
Download done for module 5, please wait for it to come online

File has been copied successfully.
Console> (enable) 09/2/1999,12:25:10:SYS-5:Module 4 is online
09/2/1999,12:25:10:SYS-5:Module 5 is online

Console> (enable) show version 4
Mod Port Model      Serial #  Versions
--- ---- ---------- --------- -----------------------------------------
4   1    WS-X6101   003414855 Hw : 1.2
                               Fw : 1.3
                               Sw : 3.2(7)
Console> (enable) show version 5
Mod Port Model      Serial #  Versions
--- ---- ---------- --------- -----------------------------------------
5   1    WS-X6101   003414463 Hw : 1.2
                               Fw : 1.3
                               Sw : 3.2(7)
Console> (enable)
```

RCP サーバへのシステム ソフトウェア イメージのアップロード

ここでは、スイッチから RCP サーバにシステム ソフトウェア イメージをアップロードする手順について説明します。

- RCP サーバへのイメージ アップロードの準備（p.26-23）
- RCP サーバへのソフトウェア イメージのアップロード（p.26-23）

（注） フラッシュ ファイル システムにおけるシステム ソフトウェア イメージ ファイルの詳しい使用手順については、第 25 章「フラッシュ ファイル システムの使用」を参照してください。

RCP サーバへのイメージ アップロードの準備

RCP サーバにソフトウェア イメージをアップロードする前に、次の作業が必要です。

- RCP サーバとして動作するワークステーションが、正しく設定されていることを確認します。
- スイッチに RCP サーバへのルートが設定されていることを確認します。サブネット間でトラフィックをルーティングするルータを設定していない場合、スイッチと RCP サーバは同じサブネットに置かれていなければなりません。**ping** コマンドを入力して、RCP サーバに接続できるかどうかを確認してください。
- 既存ファイル（作成済みの空のファイルを含む）を上書きする場合は、ファイル許可が正しく設定されていることを確認します。特定のユーザ名に関して、ファイルへの書き込み権限が必要です。

RCP サーバへのソフトウェア イメージのアップロード

スイッチ上のソフトウェア イメージを RCP サーバにアップロードするには、次の手順を実行します。

ステップ 1 コンソール ポートまたは Telnet セッションを使用して、スイッチにログインします。

ステップ 2 **copy flash rcp** コマンドを使用して、RCP サーバにソフトウェア イメージをアップロードします。プロンプトに、RCP サーバのアドレスおよび宛先ファイル名を指定します。フラッシュ ファイル システムをサポートするプラットフォーム上では、フラッシュ デバイスおよびソース ファイル名を尋ねるプロンプトが最初に表示されます。これらのプラットフォーム上では、希望する場合 **copy** *file-id* **rcp** コマンドを使用できます。

RCP サーバにソフトウェア イメージがアップロードされます。

次に、RCP サーバにスーパバイザ エンジン ソフトウェア イメージをアップロードする例を示します。

```
Console> (enable) copy flash rcp
Flash device [bootflash]? slot0:
Name of file to copy from []? cat6000-sup.5-3-1.bin
IP address or name of remote host [172.20.52.3]? 172.20.52.10
Name of file to copy to [cat6000-sup.5-3-1.bin]?
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC|
File has been copied successfully.
Console> (enable)
```

SCP を使用した暗号化イメージのダウンロード

Secure Copy（SCP; セキュア コピー）では、暗号化イメージ ファイルを安全にコピーし、認証を実行します。SCP は、SSH に依存していて、ユーザが正しい特権レベルを持っているかどうかをシステムが判断するために、AAA 認証を設定する必要があります。

SCP により、適切な許可を持つユーザが **copy** コマンドを使用してシステムとの間で暗号化ファイルをコピーできます。許可されたネットワーク管理者も、ワークステーションからこの動作を実行できます。

SCP は SSH に依存して安全な伝送を行っているため、システムには RSA 鍵ペアが必要です。SCP をイネーブルにする前に、SSH をイネーブルにし、認証と許可を正しく設定する必要があります。AAA の設定手順については、第 38 章「AAA によるスイッチ アクセスの設定」を参照してください。

ここでは、スイッチのスーパバイザ エンジンにシステム ソフトウェアの暗号化イメージをダウンロードする方法について説明します。

SCP よるイメージ ダウンロードの準備

SCP を使用してソフトウェア イメージをダウンロードする前に、次の作業が必要です。

- SCP サーバとして動作するワークステーションが、SSH をサポートしていることを確認します。
- SSH v1 と互換性のある **scp** コマンドを使用できるコマンド シェルを、サーバがサポートしていることを確認します。
- スイッチに SCP サーバへのルートが設定されていることを確認します。サブネット間でトラフィックをルーティングするルータを設定していない場合、スイッチと SCP サーバは同じサブネットに置かれていなければなりません。**ping** コマンドを使用して、SCP サーバに接続できるかどうかを確認してください。
- ダウンロードの処理中に停電（または他の問題）が生じると、フラッシュ コードが壊れることがあります。フラッシュ コードが壊れた場合には、コンソール ポートを通じてスイッチに接続し、フラッシュ PC カード上の壊れていないシステム イメージを使用して起動することができます。

SCP を使用した暗号化イメージのダウンロード

SCP サーバからスイッチにスーパバイザ エンジン ソフトウェア イメージをダウンロードするには、次の手順を実行します。

ステップ 1　ソフトウェア イメージ ファイルをワークステーション上の適切な SCP ディレクトリにコピーします。

ステップ 2　コンソール ポートから、または SSH セッションを使用して、スイッチにログインします。Telnet でログインした場合、新しいソフトウェアを実行するために、スイッチをリセットした時点で、Telnet セッションが切断されます。

ステップ 3　**copy scp flash** コマンドを使用して、SCP サーバからソフトウェア イメージをダウンロードします。プロンプトに、SCP サーバの IP アドレスまたはホスト名、およびダウンロードするファイル名を入力します。フラッシュ ファイル システムをサポートするプラットフォームでは、ファイルのコピー先となるフラッシュ デバイスおよび宛先ファイル名を入力することも必要です。

スイッチは、SCP サーバからイメージ ファイルをダウンロードします。

（注）　イメージのダウンロード中も、スイッチは稼働しています。

ステップ 4　**set boot system flash** *device***:***filename* **prepend** コマンドを入力して BOOT 環境変数を変更し、スイッチのリセット時に新しいイメージが起動するようにします。フラッシュ デバイス（*device***:**）およびダウンロードされたイメージのファイル名（*filename*）を指定します。

ステップ 5　**reset system** コマンドを入力してスイッチをリセットします。Telnet 接続の場合には、Telnet セッションが切断されます。

起動時にスーパバイザ エンジンのフラッシュ メモリが、新しいフラッシュ コードを使用して書き換えられます。

ステップ 6　スイッチの再起動後、**show version** コマンドを入力して、スイッチ コードのバージョンを確認します。

SCP ダウンロード手順の例

次に、Catalyst6500 シリーズ スイッチに暗号化イメージを SCP でダウンロードするすべての手順の例を示します。

```
Console> (enable) copy scp flash
IP address or name of remote host []? 172.20.52.3
Name of file to copy from []? cat6000-sup720cvk9.8-3-1.bin
Username for scp[bob]?
Password for User bob[]:
Flash device [bootflash]?
Name of file to copy to [cat6000-sup720cvk9.8-3-1.bin]?

4369664 bytes available on device bootflash, proceed (y/n) [n]? y
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCC
File has been copied successfully.
Console> (enable) set boot system flash bootflash:cat6000-sup720cvk9.8-3-1.bin prepend
BOOT variable =
bootflash:cat6000-sup720cvk9.8-3-1.bin,1;bootflash:cat6000-sup720cvk9.8-3-1.bin
1-csx.bin,1;
Console> (enable) reset system
This command will reset the system.
Do you want to continue (y/n) [n]? y
Console> (enable) 11/25/2003,13:51:39:SYS-5:System reset from Console//

System Bootstrap, Version 4.2
Copyright (c) 1994-2003 by cisco Systems, Inc.
Presto processor with 32768 Kbytes of main memory

Autoboot executing command: "boot bootflash:cat6000-sup720cvk9.8-3-1.bin"
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCC
Uncompressing file:  ###########################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
#############


System Power On Diagnostics
DRAM Size ....................32 MB
Testing DRAM..................Passed
Verifying Text segment .......Passed
NVRAM Size ...................512 KB
Saving NVRAM .................
Testing NVRAM ................Passed
Restoring NVRAM...............
Level2 Cache ..................Present
Level2 Cache test..............Passed

Leaving power_on_diags

Cafe Daughter Present.

EOBC link up

Boot image: cat6000-sup720cvk9.8-3-1.bin
Flash Size = 0X1000000, num_flash_sectors = 64
readCafe2Version: 0x00000001
RIn Local Test Mode, Pinnacle Synch Retries: 2
Running System Diagnostics from this Supervisor (Module 1)
This may take up to 2 minutes....please wait
```

```
Cisco Systems Console

Enter password:
11/25/2003,13:52:51:SYS-5:Module 1 is online
11/25/2003,13:53:11:SYS-5:Module 4 is online
11/25/2003,13:53:11:SYS-5:Module 5 is online
11/25/2003,13:53:14:PAGP-5:Port 1/1 joined bridge port 1/1.
11/25/2003,13:53:14:PAGP-5:Port 1/2 joined bridge port 1/2.
11/25/2003,13:53:40:SYS-5:Module 2 is online
11/25/2003,13:53:45:SYS-5:Module 3 is online
Console> (enable)
```

SCP サーバへのソフトウェア イメージのアップロード

ここでは、スイッチから SCP サーバにシステム ソフトウェア イメージをアップロードする手順について説明します。

（注）フラッシュ ファイル システムにおけるシステム ソフトウェア イメージ ファイルの詳しい使用手順については、第 25 章「フラッシュ ファイル システムの使用」を参照してください。

SCP サーバへのイメージ アップロードの準備

SCP サーバにソフトウェア イメージをアップロードする前に、次の作業が必要です。

- SCP サーバとして動作するワークステーションが、正しく設定されていることを確認します。
- スイッチに SCP サーバへのルートが設定されていることを確認します。サブネット間でトラフィックをルーティングするルータを設定していない場合、スイッチと SCP サーバは同じサブネットに置かれていなければなりません。**ping** コマンドを入力して、RCP サーバに接続できるかどうかを確認してください。
- 既存ファイル（作成済みの空のファイルを含む）を上書きする場合は、ファイル許可が正しく設定されていることを確認します。特定のユーザ名に関して、ファイルへの書き込み権限が必要です。

SCP サーバへのソフトウェア イメージのアップロード

スイッチ上の暗号化イメージを SCP サーバにアップロードして保存するには、次の手順を実行します。

ステップ 1 コンソール ポートから、または SSH セッションを使用して、スイッチにログインします。

ステップ 2 **copy flash scp** コマンドを入力して、SCP サーバにソフトウェア イメージをアップロードします。プロンプトに、SCP サーバのアドレスおよび宛先ファイル名を指定します。フラッシュ ファイル システムをサポートするプラットフォーム上では、フラッシュ デバイスおよびソース ファイル名を尋ねるプロンプトが最初に表示されます。これらのプラットフォーム上では、希望する場合 **copy** *file-id* **scp** コマンドを入力できます。

SCP サーバにイメージがアップロードされます。

次に、暗号化イメージを SCP サーバにアップロードする例を示します。

```
Console> (enable) copy bootflash scp
Flash device [bootflash]? slot0:
Name of file to copy from []? cat6000-sup720cvk9.8-3-1.bin
Username for scp[bob]?
Password for User bob[]:
IP address or name of remote host [172.20.52.3]? 172.20.52.10
Name of file to copy to [cat6000-sup720cvk9.8-3-1.bin]?
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC|
File has been copied successfully.
Console> (enable) .
```

コンソール ポートのシリアル接続によるソフトウェア イメージのダウンロード

ここでは、スーパバイザ エンジンのコンソール ポートから、Kermit を使用して、ソフトウェア イメージをシリアル ダウンロードする手順について説明します。Kermit は、広く普及しているファイル転送および端末エミュレーション ソフトウェア プログラムです。

Kermit によるイメージ ダウンロードの準備

Kermit を使用してソフトウェア イメージをシリアル ダウンロードする前に、次の作業が必要です。

- UNIX ワークステーションの場合、シェル ウィンドウがローカルである（別のワークステーションへの **rlogin** ウィンドウではない）ことを確認します。
- スーパバイザ エンジンのコンソール ポートが、シリアル ケーブルにより、PC またはワークステーション上のシリアル ポートに接続されていることを確認します。
- PC またはワークステーション上で Kermit ソフトウェアがインストールされていることを確認します。
- PC またはワークステーションとスイッチの回線速度設定が一致していることを確認します。
  - スイッチのコンソール ポートの速度を変更するには、**set system baud** *rate* コマンドを入力します。デフォルトのボーレートは 9600 ボーです。
  - PC またはワークステーションのシリアル ポートのボーレートを変更するには、Kermit> プロンプトに **set speed** *rate* コマンドを入力します。

注意　通信上の問題が起きないように、19,200 ボー以上の回線速度は使用しないでください。

- 次の作業を行って、Kermit が正しいシリアル ポートを使用していることを確認します。
  - PC 上では、**set port com***x* コマンドを入力してシリアル ポートを指定します。*x* に、スイッチに接続する PC シリアル ポート番号（1 ～ 8）を指定します。
  - UNIX ワークステーション上では、**set port/dev/tty***x* コマンドを入力してシリアル ポートを指定します。*x* には、スイッチに接続するシリアル ポート（a または b）を指定します。

Kermit によるソフトウェア イメージのダウンロード（PC の場合）

（注）　この手順が当てはまるのは、PC を使用するシリアル ダウンロードの場合だけです。UNIX ワークステーション上でのシリアル ダウンロード手順については、「Kermit によるソフトウェア イメージのダウンロード（UNIX の場合）」（p.26-31）を参照してください。

スーパバイザ エンジンのコンソール ポートを使用してソフトウェア イメージをシリアル ダウンロードするには、次の手順を実行します。

ステップ 1　Kermit がロードされているディレクトリに、ソフトウェア イメージ ファイルをコピーします。

ステップ 2　PC 上で Kermit を起動します。

（注）　作業を続ける前に、「Kermit によるイメージ ダウンロードの準備」（p.26-29）の説明に従って、回線速度が正しく設定されていること、および正しいシリアル回線が選択されていることを確認してください。

ステップ 3　Kermit> プロンプトに **connect** コマンドを入力し、スイッチに接続します。回線および速度が正しく設定されていれば、スイッチの Console> プロンプトが表示されます。

ステップ 4　**enable** コマンドを入力してイネーブル モードを開始します。

ステップ 5　**download serial** コマンドを入力します。デフォルトではモジュール 1 にファイルがダウンロードされます。

ステップ 6　プロンプトが表示されたら、ダウンロードを確認します。

ステップ 7　**Ctrl** キーを押しながら **]** キーと **c** キーを押すことにより、エスケープ シーケンスの **Ctrl-]-c** を入力します。

ステップ 8　Kermit> プロンプトに、**send** *filename* コマンドを入力し、スイッチにファイルを送信します。

スイッチにイメージ ファイルがダウンロードされ、スーパバイザ エンジンまたは対応するモジュールのフラッシュ メモリが消去され、ダウンロードしたフラッシュ コードによってフラッシュ メモリが書き換えられます。

（注）　イメージのダウンロード中も、スイッチは稼働しています。

ステップ 9　C-Kermit> プロンプトが再び表示されたら、**connect** コマンドを入力し、スイッチの Console> プロンプトに戻ります。スイッチのフラッシュ メモリが消去され、内容が書き換えられると、ステータス情報が表示されます。

（注）　Kermit> プロンプトが再表示されたあと、2 分以上経過してから **connect** コマンドを入力した場合は、Console> プロンプトだけが表示され、フラッシュ コードの消去と書き換えを示すステータス情報は表示されません。

ステップ 10　**reset system** コマンドを入力してスイッチをリセットします。

ステップ 11　スイッチの再起動後、**show version** [*mod*] コマンドを入力し、スイッチ コードのバージョンを確認します。

(注)　PC 上で Kermit を使用してシリアル ダウンロードを実行する手順の例については、「PC でのシリアル ダウンロード手順の例」（p.26-33）を参照してください。

Kermit によるソフトウェア イメージのダウンロード（UNIX の場合）

(注)　この手順が当てはまるのは、UNIX を使用するシリアル ダウンロードの場合だけです。PC 上でのシリアル ダウンロード手順については、「Kermit によるソフトウェア イメージのダウンロード（PC の場合）」（p.26-29）を参照してください。

次の手順で、スーパバイザ エンジンのコンソール ポートを使用して、ソフトウェア イメージのシリアル ダウンロードを実行します。

ワークステーションにソフトウェアをコピーするには、root としてログインし、次の手順を実行します。

ステップ 1　ホーム ディレクトリにソフトウェア イメージ ファイルをコピーします。

ステップ 2　UNIX コマンド プロンプトに **kermit** コマンドを入力し、Kermit を起動します（Kermit がインストールされたディレクトリが、ワークステーション上の $PATH 環境変数に指定されていることを確認してください）。

(注)　作業を続ける前に、「Kermit によるイメージ ダウンロードの準備」（p.26-29）の説明に従って、回線速度が正しく設定されていること、および正しいシリアル回線が選択されていることを確認してください。

ステップ 3　C-Kermit> プロンプトに **connect** コマンドを入力し、スイッチに接続します。回線および速度が正しく設定されていれば、スイッチの Console> プロンプトが表示されます。

ステップ 4　**enable** コマンドを入力してイネーブル モードを開始します。

ステップ 5　**download serial** コマンドを入力します。デフォルトではモジュール 1 にファイルがダウンロードされます。

ステップ 6　プロンプトが表示されたら、ダウンロードを確認します。

ステップ 7　**Ctrl** キーを押しながら \ キーと **c** キーを押すことにより、エスケープ シーケンスの **Ctrl-\-c** を入力します。

ステップ 8　Kermit> プロンプトに、**send** *filename* コマンドを入力し、スイッチにファイルを送信します。

Kermit ダウンロードの実行中に **a** キーを押すと、ダウンロードの進行状況をモニタできます。4 パケットが転送されるたびに、1 ドットが画面に表示されます。ファイルの転送中に問題が発生すると、次の文字コードが 1 つまたは複数表示されます。

- T ― Kermit のタイムアウトが発生しました。

- N ― Kermit が、スイッチのダウンロード プロセスを確認応答していません。
- E ― 処理の進行中に Kermit によってエラーが検出されました。

スイッチにイメージ ファイルがダウンロードされ、スーパバイザ エンジンまたは対応するモジュールのフラッシュ メモリが消去され、ダウンロードしたフラッシュ コードによってフラッシュ メモリが書き換えられます。

(注) イメージのダウンロード中も、スイッチは稼働しています。

ステップ 9　**Return** キーを押して、C-Kermit> プロンプトに戻ります。C-Kermit> プロンプトが再び表示されたら、**connect** コマンドを入力し、スイッチの Console> プロンプトに戻ります。スイッチのフラッシュ メモリが消去され、内容が書き換えられると、ステータス情報が表示されます。

(注) Kermit> プロンプトが再表示されたあと、2 分以上経過してから **connect** コマンドを入力した場合は、Console> プロンプトだけが表示され、フラッシュ コードの消去と書き換えを示すステータス情報は表示されません。

ステップ 10　**reset system** コマンドを入力してスイッチをリセットします。

ステップ 11　スイッチの再起動後、**show version** [*mod*] コマンドを入力し、スイッチ コードのバージョンを確認します。

(注) UNIX ワークステーション上で Kermit を使用してシリアル ダウンロードを実行する手順の例については、「UNIX ワークステーションでのシリアル ダウンロード手順の例」（p.26-34）を参照してください。

ソフトウェア イメージのシリアル ダウンロード手順の例

ここでは、スーパバイザ エンジンのコンソール ポートを使用し、Kermit によってイメージをシリアル ダウンロードする例を紹介します。

- PC でのシリアル ダウンロード手順の例（p.26-33）
- UNIX ワークステーションでのシリアル ダウンロード手順の例（p.26-34）

PC でのシリアル ダウンロード手順の例

次に、PC 上でシリアル ダウンロードを実行したときの、出力全体の例を示します。

```
C:\ copy A:\*.*
copying c6509_xx.bin
C:\ kermit
Kermit, 4C(057) 06 Apr 98, 4.2 BSD
Type ? for help
Kermit> set port com1
Kermit> set speed 9600
Kermit> connect
Connecting to com1,speed 9600.
The escape character is ^] (ASCII 29).
Type the escape character followed by C to get back,
or followed by ? to see other options

Console> enable
Console> (enable) download serial
Download CBI image via console port (y/n) [n]? y

Waiting for DOWNLOAD!
Return to your local Machine by typing its escape sequence
Issue Kermit send command from there[ Send `Filename`]

<CONTROL-] c to return to Local Machine>

Kermit> send c6509_xx.bin


          File name: c6509_xx.bin
 KBytes transferred: xxxx
Percent transferred: 100%
            Sending: Complete

  Number of Packets: xxxx
  Number of retries: None
         Last error: None
       Last warning: None
Kermit> connect

Finished network download.  (1136844 bytes)
Flash erase in progress ... Erase done
Programming Flash:  Flash Programming Complete
Flash erase in progress ... Erase done
Programming Flash:  Flash Programming Complete
Flash erase in progress ... Erase done
Programming Flash:  Flash Programming Complete
Flash erase in progress ... Erase done
Programming Flash:  Flash Programming Complete
Flash erase in progress ... Erase done
Programming Flash:  Flash Programming Complete
Flash erase in progress ... Erase done
Programming Flash:  Flash Programming Complete
Flash erase in progress ... Erase done
Programming Flash:  Flash Programming Complete
The system needs to be reset to run the new image.

Cisco Systems Console
Enter password:
Mon Apr 06, 1998, 14:35:08
Console>
```

UNIX ワークステーションでのシリアル ダウンロード手順の例

次に、UNIX ワークステーション上でシリアル ダウンロードを実行したときの、出力全体の例を示します。

```
workstation% cd /tmp
workstation% tar -xvfp /dev/rfd0
c5009_xx.bin, 1156046 bytes, 2258 tape blocks
workstation% ls -la
total 1150
drwxrwsrwt  5 bin           512 Sep 28 04:15 .
drwxr-xr-x 18 root         1536 Sep 27 15:41 ..
-r--r--r--  1 60000     1156046 Jul 18 10:32 c5009_xx.bin
workstation% kermit
C-Kermit, 4E(072) 06 Apr 98, SUNOS 4.x
Type ? for help
C-Kermit> set line /dev/ttya
C-Kermit> set speed 9600
/dev/ttya: 9600 baud
C-Kermit> connect
Connecting thru /dev/ttya, speed 9600.
The escape character is CTRL-\ (28).

Type the escape character followed by C to get back,
or followed by ? to see other options.

Console> enable
Console> (enable) download serial c5009_xx.bin

Download CBI image via console port (y/n) [n]? y

Waiting for DOWNLOAD!
Return to your local Machine by typing its escape sequence
Issue Kermit send command from there[ Send `Filename`]
[Back at Local System]
C-Kermit> send c5009_xx.bin
SF
c5009_xx.bin => c5009_xx.bin, Size: 1156046

CTRL-F to cancel file,  CTRL-R to resend current packet
CTRL-B to cancel batch, CTRL-A for status report:
.....................................................................................
.....................................
(テキスト出力は省略)
.............................................................
.................................. [OK]
ZB?
C-Kermit> connect
Connecting thru /dev/ttya, speed 9600.
The escape character is CTRL-\ (28).
Type the escape character followed by C to get back,
or followed by ? to see other options.

Download OK
Initializing Flash
Programming Flash
Base....Code....Length....Time....Done

Cisco Systems Console
Enter password:
Mon Apr 06, 1998, 17:35:08
Console>
```

Xmodem または Ymodem によるシステム イメージのダウンロード

スイッチにシステム イメージが必要であるにもかかわらず、スイッチがネットワークにアクセスしておらず、フラッシュ PC カード上にソフトウェア イメージがない場合、ローカルまたはリモート コンピュータ（PC、UNIX ワークステーション、Macintosh など）から Xmodem または Ymodem プロトコルを使用し、コンソール ポートを通じてイメージをダウンロードできます。

Xmodem および Ymodem プロトコルはファイル転送用に普及しており、Windows 3.1（TERMINAL.EXE）、Windows 95（HyperTerminal）、Windows NT 3.5x（TERMINAL.EXE）、Windows NT 4.0（HyperTerminal）、および Linux UNIX フリーウェア（minicom）などのアプリケーションに含まれています。

Xmodem および Ymodem によるダウンロードは低速です。これらのプロトコルは、スイッチがネットワークにアクセスしていない場合にだけ使用してください。コンソール ポートの速度を 38400 bps に設定すれば、転送を高速化できます。

Xmodem および Ymodem によるファイル転送は、ROM モニタから次のコマンドを使用して行います。

```
xmodem [-y] [-c] [-s data-rate]
```

この例では、**-y** キーワードを指定すると Ymodem プロトコルが使用され、**-c** キーワードを指定すると CRC-16 チェックサムが行われ、**-s** キーワードを指定するとコンソール ポートのデータ速度を設定できます。

スーパバイザ エンジン ソフトウェア イメージの転送元となるコンピュータでは、Xmodem または Ymodem プロトコルをサポートする端末エミュレーション ソフトウェアが稼働している必要があります。

Xmodem プロトコルを使用したファイル転送の手順を次に示します。Ymodem プロトコルを使用するには、**xmodem** コマンドに **-y** キーワードを指定します。

注意　電話回線網からコンソール ポートへのモデム接続を行う場合には、前もって考慮しておくべきセキュリティ上の問題があります。たとえば、リモート ユーザがモデムにダイヤルインし、スイッチの設定情報にアクセスする可能性があります。

注意　冗長構成のスーパバイザ エンジンを使用している場合は、2 番めの（冗長）スーパバイザ エンジンを取り外してからこの手順を実行してください。Xmodem を使用してダウンロードされたイメージは、メモリに保存されていません。したがって、ダウンロード後、2 つのスーパバイザ エンジンがインストールされており、ダウンロードされたイメージでアクティブ スーパバイザ エンジンを再起動する場合、冗長スーパバイザ エンジンはアクティブなスーパバイザ エンジンを引き継いで同期化します。ダウンロード イメージは起動されません。

ステップ 1　コンピュータのハード ドライブに、スーパバイザ エンジン ソフトウェア イメージを入れます。イメージは、Cisco.com からダウンロードできます（詳細は「はじめに」の章を参照してください）。

ステップ 2　ローカル コンピュータからダウンロードするために、ヌルモデム ケーブルを使用してコンソール ポート（ポートのモード スイッチは *in* の位置に設定）をコンピュータのシリアル ポートに接続します。コンソール ポートの速度は、ローカル コンピュータで設定されている速度と一致させる必要があります。

（注）　ローカル コンピュータから転送するときは、RTS/DTR シグナルを無視するよう端末エミュレーション プログラムを設定しなければならない場合があります。

ステップ 3　リモート コンピュータからダウンロードする手順は、次のとおりです。

a.　コンソール ポートにモデムを接続し、電話回線網に接続します。

b.　モデムとコンソール　ポートは、モデムがサポートする速度によって異なりますが、1200　～ 38400 bps の範囲の同じ速度で通信する必要があります。コンソール ポートの伝送速度を設定するには、ROM モニタ コマンド **confreg** を入力します。

c.　モデムをリモート コンピュータおよび電話回線網に接続し、スーパバイザ エンジンと同じ速度に設定します。

d.　リモート コンピュータからスーパバイザ エンジン モデムの番号をダイヤルします。

ステップ 4　端末エミュレーション ウィンドウの ROM モニタ プロンプトに、**xmodem** コマンドを入力します。

```
rommon > xmodem -s 38400 -c
```

ステップ 5　コンピュータの端末エミュレーション ソフトウェアを使用して、Xmodem または Ymodem による送信を開始します。コンピュータがスーパバイザ エンジンにシステム イメージをダウンロードします。Xmodem または Ymodem によるファイル転送の実行方法については、端末エミュレーション ソフトウェアのマニュアルを参照してください。

新しいイメージが完全にダウンロードされると、ROM モニタによってそのイメージが起動されます。

（注）　コンソール ポートを通じてイメージをダウンロードした場合、フラッシュ デバイスにはイメージ ファイルは作成されません。ダウンロードされたイメージは、メモリだけに保存されます。イメージはメモリ内にファイルとして保存できません。

ステップ 6　ダウンロードが終了すると、コンソール ポートはデフォルトのボーレート 9600 に戻ります。9600 ボー以外の速度でダウンロードを行った場合には、リモート コンピュータのボーレートを 9600 に戻す必要があります。

ステップ 7　TFTP サーバのイメージ ファイルをいずれかのフラッシュ デバイスにコピーするには、スイッチへのネットワーク接続を確立してください。

ソフトウェア イメージの確認

（注） この機能は、Supervisor Engine 1 ではサポートされていません。

ソフトウェア イメージは一連の転送を経てから、スイッチのメモリにコピーされるため、Cisco.com からのダウンロードのたびに、イメージの完全性は不安定になります。イメージ サイズおよびチェックサムはイメージのコピー時に自動的に確認されますが、このタイプのチェックではダウンロードされたイメージが壊れていたかどうか確認できません。ダウンロードしたイメージの完全性を保証するには、**set image-verification** コマンドを使用します。ブート時、イメージのコピー後、またはシステムのリセット前にイメージ検査が機能するように設定できます。

イメージ検査をイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	イメージ検査をイネーブルにします。	**set image-verification** [**boot** | **copy** | **reset**] **enable**
ステップ 2	イメージ検査設定を確認します。	**show image-verification**

次に、スイッチのリセット時にイメージ検査をイネーブルにする例を示します。

```
Console> (enable) set image-verification reset enable
Console> (enable)
```

次に、イメージ検査設定を確認する例を示します。

```
Console> (enable) show image-verification
Image Verification Status:
Boot:  Disable
Copy:  Disable
Reset: Enable
Console> (enable)
```

CHAPTER 27

コンフィギュレーション ファイルの操作

この章では、Catalyst 6500 シリーズ スイッチ上でのスイッチ コンフィギュレーション ファイルの操作方法について説明します。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

(注) フラッシュ デバイス名（**slot0:** など）はスーパバイザ エンジンのタイプによって変わります。詳細については、「フラッシュ ファイル システムの機能」（p.25-2）を参照してください。

この章で説明する内容は、次のとおりです。

スイッチ上でのコンフィギュレーション ファイルの操作

ここでは、スイッチ上でのコンフィギュレーション ファイルの操作方法について説明します。

（注） フラッシュ ファイル システムでのコンフィギュレーション ファイルの操作については、第 25 章「フラッシュ ファイル システムの使用」を参照してください。

コンフィギュレーション ファイルの作成および使用上の注意事項

コンフィギュレーション ファイルを作成することにより、各スイッチの設定が容易になります。コンフィギュレーション ファイルには、1 台または複数のスイッチの設定に必要な一部またはすべてのコマンドを登録することができます。たとえば、同じハードウェア構成の複数のスイッチに同じコンフィギュレーション ファイルをダウンロードすることにより、モジュールおよびポートを同じ設定にすることができます。

ここでは、コンフィギュレーション ファイル作成時の注意事項について説明します。

- コンフィギュレーション ファイルを使用してスイッチを設定する場合、コンソール ポートから接続することを推奨します。Telnet セッションによる接続では、スイッチの設定時に IP アドレスを変更できません。また、ポートおよびモジュールをディセーブルにできません。
- スイッチにパスワードを設定していない場合、**set password** および **set enablepass** コマンドを入力して、各スイッチにパスワードを設定する必要があります。**set password** および **set enablepass** コマンドの後ろに空白行を作成してください。パスワードが空テキストとしてコンフィギュレーション ファイルに保存されます。

  すでにパスワードを設定している場合は、**set password** および **set enablepass** コマンドは入力できません。パスワード検証エラーになるためです。コンフィギュレーション ファイルにパスワードを入力すると、ファイルの実行時に、パスワードが誤ってコマンドとして実行されます。
- コンフィギュレーション ファイルに指定するコマンドによっては、コマンドの後ろに空白行を入力する必要があります。空白行を入力しないと、これらのコマンドによって Telnet セッションが切断される可能性があります。セッションを切断する前に、スイッチから確認を求めるプロンプトが出されます。空白行は、CR（復帰）の役割を果たすので、プロンプトに対する否定応答となり、Telnet セッションを継続することができます。

  コンフィギュレーション ファイルに次のコマンドを指定する場合は、各コマンドを入力するたびに、空白行を挿入してください。

  - **set interface sc0** *ip_addr netmask*
  - **set interface sc0 disable**
  - **set module disable** *mod*
  - **set port disable** *mod/port*

コンフィギュレーション ファイルの作成

コンフィギュレーション ファイルを作成するときには、システムが正しく応答できるように、論理的な順序でコマンドを指定する必要があります。コンフィギュレーション ファイルを作成するには、次の手順を実行します。

ステップ 1　スイッチから既存の設定をダウンロードします。

ステップ 2　UNIX の vi または emacs、PC のメモ帳などのテキスト エディタで、コンフィギュレーション ファイルを開きます。

ステップ 3　コンフィギュレーション ファイルから必要なコマンドの部分を抜き出し、新しいファイルとして保存します。ファイルの先頭に独立した行として **begin**、ファイルの末尾に **end** を指定する必要があります。

ステップ 4　ワークステーションの適切な Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）ディレクトリ（UNIX ワークステーション上の /tftpboot）に、新しいコンフィギュレーション ファイルをコピーします。

ステップ 5　ファイルに対する許可が world-read に設定されていることを確認します。

次に、コンフィギュレーション ファイルの例を示します。このファイルを使用して、複数のスイッチに Domain Name System（DNS; ドメイン ネーム システム）を設定できます。

```
begin

!
#dns
set ip dns server 172.16.10.70 primary
set ip dns server 172.16.10.140
set ip dns enable
set ip dns domain corp.com
end
```

TFTP によるコンフィギュレーション ファイルのスイッチへのダウンロード

各スイッチは、作成したコンフィギュレーション ファイルを使用して設定することも、別のスイッチからコンフィギュレーション ファイルをダウンロードして設定することもできます。また、フラッシュ ファイル システムをサポートしているハードウェア上のフラッシュ デバイスにコンフィギュレーション ファイルを保存しておき、フラッシュ デバイス上のコンフィギュレーション ファイルを使用してスイッチを設定することもできます。

ここでは、TFTP サーバからダウンロードしたコンフィギュレーション ファイル、またはフラッシュ デバイス上のコンフィギュレーション ファイルを使用して、スイッチを設定する手順について説明します。

- TFTP によるコンフィギュレーション ファイルのダウンロードの準備（p.27-4）
- TFTP サーバ上のファイルを使用したスイッチの設定（p.27-4）
- フラッシュ デバイス上のファイルを使用したスイッチの設定（p.27-5）

TFTP によるコンフィギュレーション ファイルのダウンロードの準備

TFTP を使用してコンフィギュレーション ファイルをダウンロードする前に、次の作業が必要です。

- TFTP サーバとして動作するワークステーションが、正しく設定されていることを確認します。Sun ワークステーション上で、/etc/inetd.conf ファイルに次の行が含まれていることを確認します。

  ```
  tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot
  ```

  /etc/services ファイルに次の行が含まれていることを確認します。

  ```
  tftp 69/udp
  ```

  （注） /etc/inetd.conf ファイルおよび /etc/services ファイルを変更したあとで、inetd デーモンを再起動する必要があります。デーモンを再起動するには、inetd プロセスをいったん中止してから再起動するか、**fastboot** コマンド（SunOS 4.x）または **reboot** コマンド（Solaris 2.x または SunOS 5.x）を入力します。TFTP デーモンの詳しい使用手順については、使用しているワークステーションのマニュアルを参照してください。

- スイッチに TFTP サーバへのルートが設定されていることを確認します。サブネット間でトラフィックをルーティングするルータを設定していない場合、スイッチと TFTP サーバは同じサブネットに置かれていなければなりません。**ping** コマンドを使用して、TFTP サーバに接続できるかどうかを確認してください。
- ダウンロードするコンフィギュレーション　ファイルが、TFTP　サーバの正しいディレクトリ（UNIX ワークステーションでは /tftpboot）に存在していることを確認します。
- ファイルに対する許可が正しく設定されていることを確認します。ファイルの許可は world-read に設定されていなければなりません。

TFTP サーバ上のファイルを使用したスイッチの設定

TFTP サーバからダウンロードしたコンフィギュレーション ファイルを使用してスイッチを設定するには、次の手順を実行します。

ステップ 1　コンフィギュレーション　ファイルをワークステーション上の適切な TFTP ディレクトリにコピーします。

ステップ 2　コンソール ポートまたは Telnet セッションを使用して、スイッチにログインします。

ステップ 3　**copy tftp config** コマンドを入力し、TFTP　サーバからダウンロードしたコンフィギュレーション ファイルを使用してスイッチを設定します。TFTP サーバの IP アドレスまたはホスト名、およびダウンロードするファイル名を指定します。

コンフィギュレーション ファイルがダウンロードされ、ファイルの各行に指定されているコマンドが、順に実行されます。

次に、TFTP サーバからダウンロードしたコンフィギュレーション ファイルを使用してスイッチを設定する例を示します。

```
Console> (enable) copy tftp config
IP address or name of remote host []? 172.20.52.3
Name of file to copy from []? dns-config.cfg

Configure using tftp:dns-config.cfg (y/n) [n]? y
/
Finished network download.  (134 bytes)
>>
>> set ip dns server 172.16.10.70 primary
172.16.10.70 added to DNS server table as primary server.
>> set ip dns server 172.16.10.140
172.16.10.140 added to DNS server table as backup server.
>> set ip dns enable
DNS is enabled
>> set ip dns domain corp.com
Default DNS domain name set to corp.com
Console> (enable)
```

フラッシュ デバイス上のファイルを使用したスイッチの設定

フラッシュ デバイス上のフラッシュ ファイル システムに保存されているコンフィギュレーション ファイルを使用してスイッチを設定するには、次の手順を実行します。

ステップ 1　コンソール ポートまたは Telnet セッションを使用して、スイッチにログインします。

ステップ 2　**cd** および **dir** コマンドを使用して、コンフィギュレーション ファイルを検索します（詳細については、第 25 章「フラッシュ ファイル システムの使用」を参照）。

ステップ 3　**copy** *file-id* **config** コマンドを使用し、フラッシュ デバイスに保存されているコンフィギュレーション ファイルを使用してスイッチを設定します。

ファイルが行単位で読み取られ、指定されているコマンドが実行されます。

次に、フラッシュ デバイスに保存されているコンフィギュレーション ファイルを使用してスイッチを設定する例を示します。

```
Console> (enable) copy slot0:dns-config.cfg config

Configure using slot0:dns-config.cfg (y/n) [n]? y

Finished network download.  (134 bytes)
>>
>> set ip dns server 172.16.10.70 primary
172.16.10.70 added to DNS server table as primary server.
>> set ip dns server 172.16.10.140
172.16.10.140 added to DNS server table as backup server.
>> set ip dns enable
DNS is enabled
>> set ip dns domain corp.com
Default DNS domain name set to corp.com
Console> (enable)
```

TFTP サーバへのコンフィギュレーション ファイルのアップロード

ここでは、実行コンフィギュレーションまたはフラッシュ デバイスに保存されているコンフィギュレーション ファイルを、TFTP サーバにアップロードする手順について説明します。

TFTP サーバへのコンフィギュレーション ファイルのアップロードの準備

TFTP サーバにコンフィギュレーション ファイルをアップロードする前に、次の作業が必要です。

- TFTP サーバとして動作するワークステーションが、正しく設定されていることを確認します。Sun ワークステーション上で、/etc/inetd.conf ファイルに次の行が含まれていることを確認します。

  ```
  tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot
  ```

  /etc/services ファイルに次の行が含まれていることを確認します。

  ```
  tftp 69/udp
  ```

  （注） /etc/inetd.conf ファイルおよび /etc/services ファイルを変更したあとで、inetd デーモンを再起動する必要があります。デーモンを再起動するには、inetd プロセスをいったん中止してから再起動するか、**fastboot** コマンド（SunOS 4.x）または **reboot** コマンド（Solaris 2.x または SunOS 5.x）を入力します。TFTP デーモンの詳しい使用手順については、使用しているワークステーションのマニュアルを参照してください。

- スイッチに TFTP サーバへのルートが設定されていることを確認します。サブネット間でトラフィックをルーティングするルータを設定していない場合、スイッチと TFTP サーバは同じサブネットに置かれていなければなりません。**ping** コマンドを使用して、TFTP サーバに接続できるかどうかを確認してください。
- 必要に応じて、コンフィギュレーション ファイルをアップロードする前に、TFTP サーバ上に空のファイルを作成します。空のファイルを作成するには、**touch** *filename* コマンドを入力します。*filename* は、サーバにコンフィギュレーション ファイルをアップロードするときに使用するファイル名です。
- 既存ファイル（作成済みの空のファイルを含む）を上書きする場合は、ファイル許可が正しく設定されていることを確認します。ファイルの許可は world-write に設定されていなければなりません。

TFTP サーバへのコンフィギュレーション ファイルのアップロード

スイッチから TFTP サーバにコンフィギュレーション ファイルをアップロードして保存するには、次の手順を実行します。

ステップ 1　コンソール ポートまたは Telnet セッションを使用して、スイッチにログインします。

ステップ 2　**copy config tftp** コマンドを使用して、TFTP にスイッチ コンフィギュレーションをアップロードします。TFTP サーバの IP アドレスまたはホスト名、および宛先ファイル名を指定します。

TFTP サーバにファイルがアップロードされます。

次に、TFTP サーバに実行コンフィギュレーションをアップロードして保存する例を示します。

```
Console> (enable) copy config tftp
IP address or name of remote host []? 172.20.52.3
Name of file to copy to []? cat6000_config.cfg

Upload configuration to tftp:cat6000_config.cfg, (y/n) [n]? y
.....
.........
.......

.........
..........
..
/
Configuration has been copied successfully.
Console> (enable)
```

SCP または RCP を使用したコンフィギュレーションファイルのコピー

ここでは、SCP または RCP を使用してファイルをコピーする方法について説明します。

- RCP の概要（p.27-7）
- SCP の概要（p.27-7）

RCP の概要

Remote Copy Protocol（RCP）を使用して、リモート ホストとスイッチ間でコンフィギュレーションのダウンロード、アップロード、およびコピーを行うこともできます。UDP を使用する TFTP と異なり、コネクションレス プロトコルである RCP は、コネクション型の TCP を使用します。

RCP を使用してファイルをコピーするには、ファイルのコピー先またはコピー元となるサーバが RCP をサポートしていなければなりません。RCP の **copy** コマンドは、リモート システムの Remote Shell（RSH）サーバ（またはデーモン）に依存します。RCP を使用してファイルをコピーする場合、TFTP と異なり、ファイル配布用のサーバを作成する必要はありません。RSH をサポートするサーバにアクセスするだけです（大部分の UNIX システムは RSH をサポートしています）。ある場所から別の場所へファイルをコピーするので、コピー元ファイルに対して読み取り権限、コピー先ファイルに対して書き込み権限が必要です。コピー先ファイルが存在していない場合は、RCP がユーザに代わってファイルを作成します。

SCP の概要

Secure Copy（SCP; セキュア コピー）は、暗号化イメージ ファイルのコピーを安全に行います。SCP は Secure Shell（SSH; セキュア シェル）に依存していて、暗号化チャネルを使用してシステムで暗号化ファイルをコピーできます。

RCP または SCP サーバからのコンフィギュレーション ファイルのダウンロード

ここでは、RCP または SCP サーバから実行コンフィギュレーションまたはフラッシュ デバイスに、コンフィギュレーション ファイルをダウンロードする方法について説明します。

- RCP または SCP によるコンフィギュレーション ファイルのダウンロードの準備（p.27-8）
- RCP または SCP サーバ上のファイルを使用したスイッチの設定（p.27-8）

RCP または SCP によるコンフィギュレーション ファイルのダウンロードの準備

RCP または SCP を使用してコンフィギュレーション ファイルをダウンロードする前に、次の作業が必要です。

- RCP サーバとして動作するワークステーションが、RSH をサポートしていることを確認します。
- SCP サーバとして動作するワークステーションが、SSH をサポートしていることを確認します。
- スイッチに RCP または SCP サーバへのルートが設定されていることを確認します。サブネット間でトラフィックをルーティングするルータを設定していない場合、スイッチとサーバが同じサブネットに置かれていなければなりません。**ping** コマンドを使用して、RCP サーバに接続できるかどうかを確認してください。
- 有効なユーザ名を使用しないでコンソールまたは Telnet セッション経由でスイッチにアクセスしている場合、現在の RCP ユーザ名が RCP ダウンロードに使用する名前であることを確認してください。**show users** コマンドを入力すると、現在の有効なユーザ名を調べることができます。現在のユーザ名を使用しない場合は、**set rcp username** コマンドで新しいユーザ名を作成します。新しいユーザ名は NVRAM（不揮発性 RAM）に保存されます。有効なユーザ名を使用して Telnet セッション経由でスイッチにアクセスしている場合、このユーザ名が使用されるので、RCP ユーザ名を設定する必要はありません。

RCP または SCP サーバ上のファイルを使用したスイッチの設定

RCP または SCP サーバからダウンロードしたコンフィギュレーション ファイルを使用して、Catalyst 6500 シリーズ スイッチを設定するには、次の手順を実行します。

ステップ 1　コンフィギュレーション ファイルをワークステーション上の適切な RCP ディレクトリにコピーします。

ステップ 2　コンソール ポートまたは Telnet セッションを使用して、スイッチにログインします。SCP を使用している場合、SSH セッションを使用してログインします。

ステップ 3　**copy rcp | scp config** コマンドを入力し、サーバからダウンロードしたコンフィギュレーション ファイルを使用してスイッチを設定します。サーバの IP アドレスまたはホスト名、およびダウンロードするファイル名を指定します。

コンフィギュレーション ファイルがダウンロードされ、ファイルの各行に指定されているコマンドが、順に実行されます。

次に、サーバからダウンロードしたコンフィギュレーション ファイルを使用して、Catalyst 6500 シリーズ スイッチを設定する例を示します。

```
Console> (enable) copy rcp config
IP address or name of remote host []? 172.20.52.3
Name of file to copy from []? dns-config.cfg

Configure using rcp:dns-config.cfg (y/n) [n]? y
/
Finished network download.  (134 bytes)
>>
>> set ip dns server 172.16.10.70 primary
172.16.10.70 added to DNS server table as primary server.
>> set ip dns server 172.16.10.140
172.16.10.140 added to DNS server table as backup server.
>> set ip dns enable
DNS is enabled
>> set ip dns domain corp.com
Default DNS domain name set to corp.com
Console> (enable)
```

RCP または SCP サーバへのコンフィギュレーション ファイルのアップロード

ここでは、実行コンフィギュレーションまたはフラッシュ デバイスに保存されているコンフィギュレーション ファイルを、RCP または SCP サーバにアップロードする手順について説明します。

RCP または SCP サーバへのコンフィギュレーション ファイルのアップロードの準備

RCP または SCP サーバにコンフィギュレーション ファイルをアップロードする前に、次の作業が必要です。

- RCP または SCP サーバとして動作するワークステーションが、正しく設定されていることを確認します。
- スイッチに RCP または SCP サーバへのルートが設定されていることを確認します。サブネット間でトラフィックをルーティングするルータを設定していない場合、システムとサーバが同じサブネットに置かれていなければなりません。**ping** コマンドを使用して、サーバに接続できるかどうかを確認してください。
- 既存ファイル（作成済みの空のファイルを含む）を上書きする場合は、ファイル許可が正しく設定されていることを確認します。ファイルの許可は user-write に設定されていなければなりません。

RCP または SCP サーバへのコンフィギュレーション ファイルのアップロード

スイッチから RCP または SCP サーバにコンフィギュレーション ファイルをアップロードして保存するには、次の手順を実行します。

ステップ 1　コンソール ポートまたは Telnet セッションを使用して、スイッチにログインします。SCP を使用している場合、SSH セッションを使用してスイッチにログインします。

ステップ 2　**copy config rcp | scp** コマンドを入力して、RCP サーバにスイッチの設定をアップロードします。RCP サーバの IP アドレスまたはホスト名、および宛先ファイル名を指定します。

サーバにファイルがアップロードされます。

次に、RCP サーバに Catalyst 6500 シリーズ スイッチの実行コンフィギュレーションをアップロードして保存する例を示します。

```
Console> (enable) copy config rcp
IP address or name of remote host []? 172.20.52.3
Name of file to copy to []? cat6000_config.cfg

Upload configuration to rcp:cat6000_config.cfg, (y/n) [n]? y
.....
.........
.......

.........
...........
..
/
Configuration has been copied successfully.
Console> (enable)
```

次に、SCP サーバに Catalyst 6500 シリーズ スイッチの実行コンフィギュレーションをアップロードして保存する例を示します。

```
Console> (enable) copy scp flash scp
IP address or name of remote host []? 172.20.52.3
Name of file to copy from []? cat6000-sup720cvk9.8-3-1.bin
Username for scp[bob]?
Password for User bob[]:
CCC/
File has been copied successfully.
```

設定の消去

スイッチ全体の設定を消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
スイッチの設定を消去します。	**clear config all**

次に、スイッチ全体の設定を消去する例を示します。

```
Console> (enable) clear config all
This command will clear all configuration in NVRAM.
This command will cause ifIndex to be reassigned on the next system startup.
Do you want to continue (y/n) [n]? y
........
.............................

System configuration cleared.
Console> (enable)
```

個々のモジュールの設定を消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
個々のモジュールの設定を消去します。	**clear config** *mod*

（注） モジュールを取り外して、異なるタイプのモジュールに交換すると（10/100 イーサネット モジュールからギガビット イーサネット モジュールに交換する場合など）、モジュールの設定の不一致が生じます。**show module** コマンドを実行すると、出力結果から問題がわかります。この不一致を解消するには、モジュール上の設定を消去する必要があります。

次に、個々のモジュールの設定を消去する例を示します。

```
Console> (enable) clear config 2
This command will clear module 2 configuration.
Do you want to continue (y/n) [n]? y
.............................
Module 2 configuration cleared.
Console> (enable)
```

個々のモジュール ポートの設定を消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
個々のモジュール ポートの設定を消去します。	**clear config** {*mod* | *mod/port*}

コンフィギュレーション ファイルの比較

コンフィギュレーション ファイル間の違いを判断したり、システム コンフィギュレーションが変更されたかどうかをチェックするために、システムに保存されているコンフィギュレーション ファイルを比較できます。コンフィギュレーション ファイルを比較するには、イネーブル モードで次の作業を行います。

作業	コマンド
コンフィギュレーション ファイル間の違いを比較します。	**show config differences** {**all** *file* | **context** *val* | *file* | **ignorecase**}

次に、2 つの異なるコンフィギュレーション ファイルの違いを比較する例を示します。

```
Console> (enable) show config differences 1.cfg 2.cfg
--- bootflash:1.cfg
+++ bootflash:2.cfg
@@ -8,1 +8,1 @@
-#version 8.2(0.11-Eng)DEL
+#VERSION 8.2(0.11-eNG)del
@@ -11,1 +11,1 @@
-set config mode text auto-save interval 1
+SET CONFIG MODE TEXT AUTO-SAVE INTERVAL 1
Console> (enable)
```

次に、大文字と小文字の違いは無視してコンフィギュレーション ファイルの違いを比較する例を示します。

```
Console> (enable) show config differences ignorecase 1.cfg 2.cfg
Files bootflash:1.cfg and bootflash:2.cfg are identical
Console> (enable)
```

コンフィギュレーション ロールバック用のコンフィギュレーション チェックポイント ファイルの作成

現在のファイルによって望ましくない結果がシステムで生じる場合、現在のスイッチ コンフィギュレーション ファイルを前に保存したコンフィギュレーション ファイル（別名「チェックポイント」ファイル）にロール バックできます。このロールバック機能によって、1 つのコマンドに複数のコンフィギュレーション「チェックポイント」ファイルを設定できます。現在のコンフィギュレーション ファイルをスイッチ上で実行したくない場合、速やかにコンフィギュレーション チェックポイント ファイルのいずれかに戻し、スイッチ機能への障害をできるだけ少なくすることができます。

コンフィギュレーション チェックポイント ファイルの作成時には、次の注意事項に従ってください。

- コンフィギュレーション チェックポイント ファイルは、ファイルの作成時に指定する名前によって特定されます。コンフィギュレーション チェックポイント ファイル名は、15 文字以内にする必要があります。名前を指定しない場合、システムによって名前が生成されます。システムによって生成される名前は、CKPi_MMDDYYHHMM の形式になります。「i」はチェックポイント番号を表します。
- チェックポイント ファイルは、ブートフラッシュまたは slotX/diskX に保存されます。装置を指定しない場合、ファイルは現在のデフォルト装置に保存されます。
- コンフィギュレーション チェックポイント ファイルは、読み取りおよび編集が可能なテキスト ファイルに保存されます。ファイルを編集しないことを強く推奨します。

- チェックポイント ファイル名がシステムから消去されると、関連するコンフィギュレーション チェックポイント ファイルが削除されます。スペースを確保するために装置をスクイーズする必要があります。
- システム上に最大 5 つのコンフィギュレーション チェックポイント ファイルを作成できます。保存されたすべてのコンフィギュレーション チェックポイント ファイルに任意の順序でロール バックできます。これらのファイルは完全なコンフィギュレーションを使用して生成されるので、相互に独立しています。
- チェックポイント コンフィギュレーションは NVRAM に保存されます。**clear config all** コマンドを入力した場合、コンフィギュレーションは消去されません。
- この機能は、冗長スーパバイザ エンジンを搭載したシステムでサポートされています。チェックポイント コンフィギュレーション ファイルおよび関連するファイルはスタンバイ スーパバイザ エンジンに同期化されます。

コンフィギュレーション チェックポイント ファイルを作成するには、イネーブル モードで次の作業を行います。

作業	コマンド
コンフィギュレーション チェックポイント ファイルを作成します。	**set config checkpoint** [**name** *name*] [**device** *device*]
コンフィギュレーション チェックポイント ファイル名を確認します。	**show config checkpoints**

次に、コンフィギュレーション チェックポイント ファイルを作成し、作成されたことを確認する例を示します。

```
Console> (enable) set config checkpoint
Configuration checkpoint CKP0_0722040905 creation successful.
Console> (enable) show config checkpoints
Checkpoint          File id                                  Date
==========          =======                                  ====
CKP0_0722040905     bootflash:CKP0_07220409058.4(0.79)COC    Thu Jul 22 2000, 09:05:31
Console> (enable)
```

現在のコンフィギュレーション ファイルを前に作成されたコンフィギュレーション チェックポイント ファイルにロール バックするには、イネーブル モードで次の作業を行います。

作業	コマンド
現在のコンフィギュレーション ファイルをコンフィギュレーション チェックポイント ファイルにロール バックします。	**set config rollback** *name*

すべてのコンフィギュレーション チェックポイント ファイルまたは特定のコンフィギュレーション チェックポイント ファイルを消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
すべてのコンフィギュレーション チェックポイント ファイルまたは特定のコンフィギュレーション チェックポイント ファイルを消去します。	**clear config checkpoint** {**all** | *name*}
コンフィギュレーション チェックポイント ファイル名を確認します。	**show config checkpoints**

次に、すべてのコンフィギュレーション チェックポイント ファイルを消去し、消去されたことを確認する例を示します。

```
Console> (enable) clear config checkpoint all
All configuration checkpoints cleared.
Console> (enable) show config checkpoints
No Checkpoints defined.
Console> (enable)
```

MSFC 上でのコンフィギュレーション ファイルの操作

ここでは、Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）上のコンフィギュレーション ファイルの操作について説明します。

MSFC の稼働時は、設定情報は 2 つの場所にあります。NVRAM 内のデフォルト（永続的）設定と RAM 内の実行（一時的）メモリです。NVRAM の情報は電源を切断しても保持されるので、デフォルト設定は常時、使用できます。現在の実行メモリは、システムの電源を切断すると失われます。現在の設定には、**configure** または **setup** コマンドを入力することにより、またはコンフィギュレーション ファイルを編集することにより追加された、デフォルト以外のすべての設定情報が含まれています。

電源を切断しても現在の設定が失われないようにするには、**copy running-config startup-config** コマンドを使用して現在の設定を NVRAM のデフォルト設定に追加します。システムの設定を変更する場合は、必ず **copy running-config startup-config** コマンドを実行し、新しい設定を保存してください。

MSFC を交換する場合には、設定全体を交換する必要があります。MSFC を取り外す前にコンフィギュレーション ファイルをリモート サーバにアップロード（コピー）しておけば、新しい MSFC を取り付けたあと、元の設定を NVRAM に戻すことができます。コンフィギュレーション ファイルをアップロードしない場合には、新しい MSFC を取り付けたあと、**configure** コマンドを入力して設定情報を再入力する必要があります。

MSFC を一時的に取り外して再び取り付ける場合には、コンフィギュレーション ファイルを保存して戻す必要はありません。リチウム電池により、設定情報がメモリに保存されています。この作業では、EXEC コマンド インタープリタのイネーブル レベルにアクセスする必要があり、通常、パスワードが必要になります。

TFTP サーバへのコンフィギュレーション ファイルのアップロード

TFTP ファイル サーバに実行コンフィギュレーションをアップロードする前に、次のことを確認してください。

- コンソール端末から、または Telnet セッションによりリモートで MSFC に接続できること。
- MSFC がファイル サーバ（リモート ホスト）をサポートしているネットワークに接続していること。
- リモート ホストが TFTP アプリケーションをサポートしていること。
- 使用できるリモート ホストの IP アドレスまたはホスト名がわかっていること。

リモート ホストに情報を保存するには、**write network** イネーブル EXEC コマンドを使用します。このコマンドに、宛先ホストのアドレスおよびファイル名を入力し、指示した情報を確認します。情報を確認すると、MSFC により、現在の実行コンフィギュレーションがリモート ホストに送信されます。システムのデフォルトでは、設定は MSFC の名前に *-confg* が付加されたファイル名で保存されます。**Return** キーを押してデフォルト ファイル名を使用するか、別のファイル名を入力して **Return** キーを押します。

現在の実行コンフィギュレーションをリモート ホストにアップロードするには、次の手順を実行します。

ステップ 1　システム プロンプトに、EXEC コマンド インタープリタのイネーブル レベルを示すポンド記号（#）が表示されていることを確認します。

ステップ 2　**ping** コマンドを入力して、MSFC とリモート ホストとの接続を確認します。

ステップ 3　**write term** コマンドを入力して、現在の実行コンフィギュレーションを端末に表示し、設定情報が完全で正しいことを確認します。情報が正しくない場合には、**configure** コマンドを使用して既存の設定に追加または変更を行います。

ステップ 4　**write net** コマンドを入力します。EXEC コマンド インタープリタによって、コンフィギュレーション ファイルを受信するリモート ホストの名前または IP アドレスの入力を求めるプロンプトが表示されます（プロンプトにデフォルトのファイル サーバの名前またはアドレスが示されていることもあります）。

```
Router# write net
Remote host []?
```

ステップ 5　リモート ホストの名前または IP アドレスを入力します。次の例では、リモート サーバ名 *servername* を入力しています。

```
Router# write net
Remote host []? servername
Translating "servername"...domain server (1.1.1.1) [OK]
```

ステップ 6　設定を保存するファイル名を指定するように要求されます。デフォルトでは、MSFC 名に *-confg* を付加した新しいファイル名が作成されます。**Return** キーを押してデフォルト ファイル名を使用するか、別のファイル名を入力して **Return** を押します。次の例ではデフォルトがそのまま使用されています。

```
Name of configuration file to write [Router-confg]?
Write file Router-confg on host 1.1.1.1? [confirm]
Writing Router-confg .....
```

ステップ 7　MSFC によりコピー処理が開始される前に、指定した情報が表示されるので確認します。指定した内容が正しくない場合には、**n**（no）を入力し、**Return** キーを押して処理を中止します。指定した内容を確定するには、**Return** キーを押すか、**y**（yes）を入力して **Return** キーを押します。コピー処理が開始されます。次の例ではデフォルトがそのまま使用されています。

```
Write file Router-confg on host 1.1.1.1? [confirm]
Writing Router-confg: !!!! [ok]
```

MSFC がリモート ホストに設定をコピーしている間、一連の感嘆符（!!!）またはピリオド（...）を表示します。!!! および [ok] は、処理が成功したことを示しています。失敗すると、ピリオドの連続（...）と [timed out] または [failed] が表示されます。この場合、ネットワークに障害があるか、リモート ファイル サーバ上に読み書き可能なファイルが存在しない可能性があります。

ステップ 8　処理が成功していれば（!!! および [ok] が表示されている状態）、アップロードは完了です。設定は、リモート ファイル サーバ上の一時ファイルに保存されます。

処理が失敗すると、次の例のようにピリオドの連続（...）が表示されます。

```
Writing Router-confg .....
```

この場合、設定は保存されていません。上記の手順を再度実行するか、別のリモート ファイル サーバを選択して同じ手順を繰り返してください。

リモート ホストに設定を正常にコピーできない場合には、ネットワーク管理者に連絡してください。

スーパバイザ エンジンのフラッシュ PC カードへのコンフィギュレーション ファイルのアップロード

スーパバイザ エンジンのフラッシュ PC カードにコンフィギュレーション ファイルをアップロードするには、次の作業を行います。

	作業	コマンド
ステップ 1	EXEC プロンプトで、イネーブル モードを開始します。	Router> **enable**
ステップ 2	スタートアップ コンフィギュレーション ファイルをスロット 0 にコピーします。	Router# **copy startup-config sup-slot0:***file_name*
ステップ 3	実行コンフィギュレーション ファイルをスロット 0 にコピーします。	Router# **copy running-config sup-slot0:***file_name*

リモート ホストからのコンフィギュレーション ファイルのダウンロード

新しい MSFC を搭載したあと、保存した設定を検索して、NVRAM にコピーすることができます。コンフィギュレーション モードを開始し、ネットワーク経由で MSFC の設定を行います。システム プロンプトにホスト名、アドレス、およびホストに保存されているコンフィギュレーション ファイル名を入力し、リモート ファイルを使用した再起動を指示します。

リモート ホストから現在の実行コンフィギュレーションをダウンロードするには、次の手順を実行します。

ステップ 1　システム プロンプトに、EXEC コマンド インタープリタのイネーブル レベルを示すポンド記号（#）が表示されていることを確認します。

（注）　元の設定を検索して戻すまで、MSFC は NVRAM 上のデフォルト設定を実行します。設定を戻すまでは、システムに設定していたパスワードは無効になります。

ステップ 2　**ping** コマンドを入力して、ルータとリモート ホストとの接続を確認します。

ステップ 3　システム プロンプトに **configure network** コマンドを入力し、**Return** キーを押してコンフィギュレーション モードを開始します。(デフォルトのコンソール端末を使用するのではなく)ネットワーク装置からシステムの設定を行うことを指定します。

```
Router# configure network
```

ステップ 4　ホストまたはネットワーク上のコンフィギュレーション ファイルを選択するように要求されます。デフォルトはホスト上のファイルです。デフォルトを確定するには、**Return** キーを押します。

```
Host or network configuration file [host]?
```

ステップ 5　ホストの IP アドレスを入力するように要求されます。リモート ホスト（コンフィギュレーション ファイルをアップロードしたリモート ファイル サーバ）の IP アドレスまたは名前を入力します。

```
IP address of remote host [255.255.255.255]? 1.1.1.1
```

ステップ 6　コンフィギュレーション ファイル名を入力します。ファイルのアップロード時のデフォルト名は、MSFC 名に *-confg* を付けたファイル名（次の例では *router-confg*）です。設定のアップロード時にデフォルト以外のファイル名を指定した場合は、そのファイル名を入力します。デフォルト名を使用した場合には、**Return** キーを押します。

```
Name of configuration file [router-confg]?
```

ステップ 7　新しい設定でシステムを再起動する前に、指定した情報が表示されるので確認します。指定した内容が正しくない場合には、**n**（no）を入力し、**Return** キーを押して処理を中止します。指定した内容を確定するには、**Return** キーを押すか、**y** を入力して **Return** キーを押します。

```
Configure using router-confg from 1.1.1.1? [confirm]
Booting router-confg from 1.1.1.1: ! ! [OK - 874/16000 bytes]
```

MSFC がリモート ホスト上の設定の検索およびシステム再起動を開始すると、コンソールに処理が成功したかどうかが示されます。一連の !!! および [ok]（前述の例を参照）は、処理が成功したことを示します。ピリオドの連続（ ...）と [timed out] または [failed] は、処理が失敗したことを示します（ネットワークに障害があるか、指定したサーバ名、アドレス、またはファイル名が間違っている可能性があります)。次に、リモート サーバからのシステム再起動に失敗した例を示します。

```
Booting Router-confg ..... [timed out]
```

ステップ 8　処理に成功した場合は、次の手順に進みます。

処理に失敗した場合は、リモート サーバの名前またはアドレスおよびファイル名が正しいかどうか確認し、前の手順を繰り返してください。設定を正常に検索できない場合には、ネットワーク管理者に連絡してください。

ステップ 9　**write term** コマンドを入力して、現在の実行コンフィギュレーションを端末に表示します。表示されたコンフィギュレーション情報が完全で、正しいことを確認します。正しくない場合は、ファイル名を確認してから前の手順を繰り返して正しいファイルを検索するか、**configure** コマンドを入力して既存の設定に追加または変更を行います（システム、各インターフェイス、特定の設定手順で利用できる設定オプションについては、該当するソフトウェアのマニュアルを参照してください）。

ステップ 10　現在の実行コンフィギュレーションが正しいことを確認したら、**copy running-config startup-config** コマンドを入力して、検索した設定を NVRAM に保存します。保存しないと、システムを再起動した場合に、検索した設定は失われます。

スーパバイザ エンジンのフラッシュ PC カードからのコンフィギュレーション ファイルのダウンロード

スーパバイザ エンジンのフラッシュ PC カードからコンフィギュレーション ファイルをダウンロードするには、次の作業を行います。

	作業	コマンド
ステップ 1	EXEC プロンプトで、イネーブル モードを開始します。	Router> **enable**
ステップ 2	保存されている実行コンフィギュレーション ファイルを、MSFC 実行コンフィギュレーションにコピーします。	Router# **copy sup-slot0:***file_name* **running-config**
ステップ 3	保存されているスタートアップ コンフィギュレーション ファイルを、MSFC 実行コンフィギュレーションにコピーします。	Router# **copy sup-slot0:***file_name* **startup-config**

プロファイル ファイルの操作

プロファイル ファイルによって、スイッチのデフォルト コンフィギュレーションとしてカスタマイズされたコンフィギュレーションを持つことができます。また、起動時または新規のモジュールが搭載された場合に、特定の機能をイネーブルまたはディセーブルにするカスタム デフォルト コンフィギュレーションをロードすることができます。プロファイル ファイルを使用すれば、スイッチにセキュリティ リスク（たとえば、CDP のディセーブル化またはポート上の自動トランキングの切断）をもたらす可能性がある機能または処理を排除できます。

セキュリティ リスクのほとんどを無効にしたプロファイル ファイルは、「ロックダウン」プロファイルともいいます。ロックダウン プロファイルは、デフォルトでスイッチの機能をアクセスのイネーブルからアクセスの阻止に変更します。ロックダウン プロファイルが適用されている場合、プロファイル ファイルによってディセーブルにされた機能を手動でイネーブルにする必要があります。

プロファイル ファイルの作成

プロファイル ファイル形式は、コンフィギュレーション ファイル形式と類似しています。新規のプロファイル ファイルを作成することもできますし、システムによって生成されたコンフィギュレーション ファイルを編集することもできます。

注意　要素を失ったり、置き違えるとコンフィギュレーションが失敗する原因になるので、コンフィギュレーション ファイルに不慣れな場合は新規のプロファイル ファイルを作成しないことを推奨します。

システムによって生成されたコンフィギュレーション ファイルを編集してプロファイル ファイルを作成する場合、必須の表記のほとんどがすでにファイルに存在します。現在サポートされているキーワードは、ALL_MODULES、ALL_PORTS、ALL_MODULE_PORTS、および ALL_VLANS です。**copy config all** コマンドを入力した結果生じた出力をテンプレートとして使用してプロファイル ファイルを作成しないでください。出力には、ファイルのサイズと処理時間を増やすデフォルトのコンフィギュレーション情報が含まれているからです。

使用するシステム プロファイル ファイルを指定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	装置および使用するプロファイル ファイル名を指定します。	**set system profile** *device*:*filename*
ステップ 2	指定したモジュールのシステム プロファイル ファイルをイネーブルまたはディセーブルにします。	**set system profile** {**enable** | **disable**} *mod_list*

次に、装置名およびプロファイル ファイル名を指定する例を示します。

```
Console> (enable) set system profile bootflash:test.cfg
System is set to be configured with profile file bootflash:test.cfg.
Console> (enable)
```

次に、指定されたモジュールのシステム プロファイルのロードをディセーブルにする例を示します。

```
Console> (enable) set system profile disable 2
System profile loading is disabled for module 2.
Console> (enable)
```

次に、ロックダウン プロファイル ファイルの例を示します。一般的であると考えられるロックダウン プロファイル ファイルをデフォルト コンフィギュレーションとして使用する場合、このファイルのコピーをそのまま使用できます。このロックダウン プロファイル ファイルのパラメータがニーズに合わない場合は、ファイルを変更し、ファイルを変更したものを使用することもできます。

```
begin
!
# ***** DEFAULT PROFILE *****
!
!
##################################
# Lockdown Profile version 1.0.3 #
##################################
!
# set system prompt (edit as needed)
set prompt locked_down>
!
# system attributes to be customized (edit as needed)
set system name locked_down
set system contact locked_down
set system location locked_down
!
# set a strong banner (edit as needed)
set banner motd ^
Access to this device or the attached networks is prohibited
without express permission from the network administrator.

Violators will be prosecuted to the fullest extent of both civil
and criminal law.

^
!
!
#
# vtp mode off, enable password and dummy domain (edit as needed)
set vtp domain locked_down
set vtp mode off
set vtp passwd locked_down
!
# default VLAN is "Quarantine" (edit as needed)
set vlan 999 name Quarantine
!
# Management VLAN is "Management" (edit as needed)
set vlan 1000 name Management
# Alternate management vlan is "OtherMgmt" (edit as needed)
set vlan 1001 name OtherMgmt
!
# sc0 and sc1 off (edit as needed)
set interface sc0 down
set interface sc0 1000
set interface sc1 down
set interface sc1 1001
!
# default port status is disabled
set port disable ALL_PORTS
!
# default cdp status is disabled
set cdp disable ALL_PORTS
!
# default STP status is with BPDU guard enabled
set spantree portfast bpdu-guard ALL_PORTS enable
!
# default PAgP/LACP status is disabled
set port channel ALL_PORTS mode off
!
# Default DTP status is disabled, no allowed vlans and dot1q-all-tagged mode on.
# Warning: A max of 128 trunks can have non-default configuration in CatOS 8.4
# Warning: Edit port list as needed.
```

```
set trunk ALL_PORTS off none
set dot1q-all-tagged enable
!
# default is CPU rate limiters enabled
set rate-limit l2pdu enable
!
# default SSH version is 2
set ssh mode v2
!
# default VLAN is "Quarantine" (edit as needed)
set vlan 999 ALL_PORTS
!
# Enable image checksum verification by default
set image-verification enable
!
# Set a more aggressive default logout timeout
set logout 10
#
#
# Anti-spoofing ACL
#
!
! Deny any packets from the RFC 1918, IANA reserved, ranges,
! multicast as a source, and loopback netblocks to block
! attacks from commonly spoofed IP addresses.
!
! Bogons
!
set security acl ip Anti-spoofing deny ip 0.0.0.0 0.255.255.255  any log
set security acl ip Anti-spoofing deny ip 1.0.0.0 0.255.255.255  any log
set security acl ip Anti-spoofing deny ip 2.0.0.0 0.255.255.255  any log
set security acl ip Anti-spoofing deny ip 5.0.0.0 0.255.255.255  any log
set security acl ip Anti-spoofing deny ip 7.0.0.0 0.255.255.255  any log
set security acl ip Anti-spoofing deny ip 10.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 23.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 27.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 31.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 36.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 37.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 39.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 41.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 42.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 49.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 50.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 73.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 74.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 75.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 76.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 77.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 78.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 79.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 89.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 90.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 91.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 92.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 93.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 94.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 95.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 96.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 97.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 98.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 99.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 100.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 101.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 102.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 103.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 104.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 105.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 106.0.0.0 0.255.255.255 any log
```

```
set security acl ip Anti-spoofing deny ip 107.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 108.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 109.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 110.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 111.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 112.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 113.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 114.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 115.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 116.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 117.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 118.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 119.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 120.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 121.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 122.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 123.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 124.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 125.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 126.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 127.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 169.254.0.0 0.0.255.255 any log
set security acl ip Anti-spoofing deny ip 172.16.0.0 0.15.255.255 any log
set security acl ip Anti-spoofing deny ip 173.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 174.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 175.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 176.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 177.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 178.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 179.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 180.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 181.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 182.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 183.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 184.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 185.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 186.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 187.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 189.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 190.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 192.0.2.0 0.0.0.255     any log
set security acl ip Anti-spoofing deny ip 192.168.0.0 0.0.255.255 any log
set security acl ip Anti-spoofing deny ip 197.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 223.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 224.0.0.0 31.255.255.255 any log
# Add here a specific list of permits as needed
set security acl ip Anti-spoofing deny any any log
!
# Set protection to VLAN list (edit as needed)
# You can use ALL_VLANS but that will
# take some time to finish.
# Use the "show security acl" cmd to verify when
# the ACL mapping process is completed.
commit security acl all
set security acl map Anti-spoofing ALL_VLANS
!
!
end
```

CHAPTER 28

システム メッセージ ロギングの設定

この章では、Catalyst 6500 シリーズ スイッチ上でシステム メッセージ ロギングを設定する方法について説明します。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

(注) システム メッセージの詳細については、『*System Message Guide — Catalyst 6500 Series, Catalyst 2948G, Catalyst 2980G Switches*』を参照してください。

この章で説明する内容は、次のとおりです。

システム メッセージ ロギングの機能

システム メッセージ ロギング ソフトウェアは、メッセージをログ ファイルに保存するか、または他の装置に転送します。システム メッセージ ロギングには次の機能があります。

- モニタおよびトラブルシューティングのためのログ情報を提供します。
- 収集したログ情報のタイプを選択できます。
- 収集したログ情報の宛先を選択できます。

スイッチはデフォルトの設定として、正常ではあるが重要なイベントを通知するシステム メッセージを内部バッファに記録し、さらにシステム コンソールに送信します。ファシリティ タイプ（表 28-1 を参照）および重大度（表 28-2 を参照）に基づいて、保存するシステム メッセージを指定できます。メッセージにはタイムスタンプが付加されるので、リアルタイムのデバッグおよび管理に有効です。

スイッチの CLI（コマンドライン インターフェイス）を使用するか、適切に設定した Syslog サーバに保存することにより、記録されたシステム メッセージを表示できます。スイッチ ソフトウェアは、内部バッファに最大 500 の Syslog メッセージを保存します。したがって、スイッチに Telnet またはコンソール ポートを使用してアクセスするか、または Syslog サーバ上のログを調べることにより、離れた場所でシステム メッセージをモニタできます。

システム障害が発生した場合、システム Syslog ダンプにより、Syslog バッファ内のシステム メッセージをフラッシュ ファイルに書き込み、障害発生前の関連する Syslog 情報を取り込むことができます。システムのコア ダンプ機能がイネーブルになっている場合、Syslog のダンプはコア ダンプの前に行われます。

（注） Syslog サーバにリダイレクトされるメッセージは、最大で 90 秒遅れます。

表 28-1 に、システム メッセージ ログでサポートされるファシリティ タイプを示します。

表 28-1　システム メッセージ ログのファシリティ タイプ

ファシリティ名	定義
all	すべてのファシリティ
acl	ACL ファシリティ
cdp	Cisco Discovery Protocol
cops	Common Open Policy Server
dtp	Dynamic Trunking Protocol
dvlan	ダイナミック VLAN
earl	Enhanced Address Recognition Logic
filesys	ファイル システム
gvrp	GARP VLAN Registration Protocol
ip	Internet Protocol
kernel	カーネル
ld	ASLB ファシリティ
mcast	マルチキャスト
mgmt	管理
mls	Multilayer Switching（マルチレイヤ スイッチング）

表 28-1　システム メッセージ ログのファシリティ タイプ（続き）

ファシリティ名	定義
pagp	Port Aggregation Protocol（ポート集約プロトコル）
protfilt	プロトコル フィルタ
pruning	VTP プルーニング
privatevlan	プライベート VLAN ファシリティ
qos	サービス品質
radius	Remote Access Dial-In User Service
rsvp	ReSerVation Protocol
security	セキュリティ
snmp	Simple Network Management Protocol（簡易ネットワーク管理プロトコル）
spantree	Spanning-Tree Protocol（スパニングツリー プロトコル）
sys	システム
tac	ターミナル アクセス コントローラ
tcp	Transmission Control Protocol
telnet	端末エミュレーション プロトコル
tftp	Trivial File Transfer Protocol（簡易ファイル転送プロトコル）
udp	User Datagram Protocol
vmps	VLAN Membership Policy Server（VLAN メンバーシップ ポリシー サーバ）
vtp	VLAN トランク プロトコル

表 28-2 に、システム メッセージ ログがサポートしている重大度を示します。

表 28-2　重大度の定義

重大度	説明
0 — emergencies（緊急）	システムは使用不可能
1 — alerts（アラート）	即時処置が必要
2 — critical（クリティカル）	クリティカル
3 — errors（エラー）	エラー
4 — warnings（警告）	警告
5 — notifications（通知）	通常のバグ
6 — informational（情報）	通知メッセージ
7 — debugging（デバッグ）	デバッグ メッセージ

システム ログ メッセージの形式

システム ログ メッセージは、パーセント記号（%）から始まる最大 80 文字のメッセージです。メッセージは、次の形式で表示されます。

mm/dd/yyy:hh/mm/ss:facility-severity-MNEMONIC:description

表 28-3 に、Syslog メッセージの要素を示します。

表 28-3　システム ログ メッセージの要素

要素	説明
mm/dd/yyy:hh/mm/ss	エラーまたはイベントが発生した日時。この情報は、**set logging timestamp enable** コマンドで設定した場合に限って表示されます。
facility	メッセージが指し示すファシリティ（SNMP、SYS など）です。
severity	メッセージの重大度を示す 0 ～ 7 の 1 桁のコード
MNEMONIC	エラー メッセージを独自に説明するテキスト
description	報告対象のイベントの詳細情報を含むテキスト

次に、スイッチの一般的なシステム メッセージの例を示します（システム起動時）。

```
1999 Apr 16 10:01:26 %MLS-5-MLSENABLED:IP Multilayer switching is enabled
1999 Apr 16 10:01:26 %MLS-5-NDEDISABLED:Netflow Data Export disabled
1999 Apr 16 10:01:26 %SYS-5-MOD_OK:Module 1 is online
1999 Apr 16 10:01:47 %SYS-5-MOD_OK:Module 3 is online
1999 Apr 16 10:01:42 %SYS-5-MOD_OK:Module 6 is online
1999 Apr 16 10:02:27 %PAGP-5-PORTTOSTP:Port 3/1 joined bridge port 3/1
1999 Apr 16 10:02:28 %PAGP-5-PORTTOSTP:Port 3/2 joined bridge port 3/2
```

システム メッセージ ロギングのデフォルト設定

表 28-4 に、システム メッセージ ロギングのデフォルト設定を示します。

表 28-4　システム メッセージ ロギングのデフォルト設定

設定パラメータ	デフォルト設定
コンソールへのシステム メッセージ ロギング	イネーブル
Telnet セッションへのシステム メッセージ ロギング	イネーブル
ロギング バッファ サイズ	500（デフォルトであり最大値）
ロギング ヒストリ サイズ	1
ロギング ヒストリ重大度	warnings（4）
タイムスタンプ オプション	イネーブル
ロギング サーバ	ディセーブル
Syslog サーバの IP アドレス	設定なし
サーバ ファシリティ	LOCAL7
サーバ重大度	warnings（4）
システム メッセージのファシリティ / 重大度	**sys/5** **dtp/5** **pagp/5** **mgmt/5** **mls/5** **cdp/4** **udld/4** *その他のファシリティ* **/2**
システム Syslog ダンプ	ディセーブル
システム Syslog ダンプ用のデバイスおよびファイル名の指定	フラッシュ デバイスは slot0: ファイル名は sysloginfo

スイッチ上でのシステム メッセージ ロギングの設定

ここでは、スイッチ上でシステム メッセージ ロギングを設定する手順について説明します。

セッション ロギングのイネーブル化およびディセーブル化

特に設定しなかった場合、システム ロギング メッセージはデフォルトのロギング ファシリティおよび重大度に基づいて、コンソールおよび Telnet セッションに送信されます。状況に応じて、コンソールへのロギング、または特定の Telnet セッションへのロギングをディセーブルにすることができます。

コンソール セッションへのロギングをディセーブルまたはイネーブルにすると、そのイネーブル ステートが以後すべてのコンソール セッションに適用されます。たとえば、コンソールへのロギングをディセーブルにして、コンソール ポートを切り離し、その後再接続しても、そのコンソールへのロギングはディセーブルのままです。

Telnet セッションへのロギングをディセーブルまたはイネーブルにすると、そのセッションに限ってイネーブル ステートが適用されます。Telnet セッションへのロギングをディセーブルにして、セッションを切断し、その後再接続した場合、新しいセッションではロギングがイネーブルになります。

（注） コンソール ポートから接続しているときに、**set logging session** コマンドを入力すると、**set logging console** コマンドを入力した場合と同じ結果になります。ただし、Telnet セッションを使用して接続しているときに、**set logging console** コマンドを入力した場合は、デフォルトのコンソール ロギング イネーブル ステートが変更されます。

コンソール セッションのロギング ステートをイネーブルまたはディセーブルに設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	コンソール セッションでデフォルトのロギング ステートをイネーブルまたはディセーブルに設定します。	**set logging console** {**enable** | **disable**}
ステップ 2	ロギングの設定を確認します。	**show logging** [**noalias**]

次に、現在および今後のコンソール セッションへのロギングをディセーブルにする例を示します。

```
Console> (enable) set logging console disable
System logging messages will not be sent to the console.
Console> (enable)
```

現在の Telnet セッションのロギング ステートをイネーブルまたはディセーブルに設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	Telnet セッションのロギング ステートをイネーブルまたはディセーブルに設定します。	**set logging session** {**enable** | **disable**}
ステップ 2	ロギングの設定を確認します。	**show logging** [**noalias**]

次に、現在の Telnet セッションへのロギングをディセーブルにする例を示します。

```
Console> (enable) set logging session disable
System logging messages will not be sent to the current login session.
Console> (enable)
```

システム メッセージ ロギングの重大度の設定

set logging level コマンドを使用すると、ロギング ファシリティごとに重大度を設定できます。すべてのファシリティを指定する場合は、**all** キーワードを入力します。指定した重大度を特定のファシリティのデフォルト値にする場合は、**default** キーワードを入力します。**default** キーワードを使用しなかった場合、指定した重大度は現在のセッションに限って有効です。

ロギング ファシリティに関するシステム メッセージ ロギングの重大度を設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ロギング ファシリティの重大度を設定します。	**set logging level** {**all** | *facility*} *severity* [**default**]
ステップ 2	システム メッセージ ロギングの設定を確認します。	**show logging** [**noalias**]

次に、すべてのファシリティで（現在のセッションに限り）ロギング重大度を 5 に設定する例を示します。

```
Console> (enable) set logging level all 5
All system logging facilities for this session set to severity 5(notifications)
Console> (enable)
```

次に、**cdp** ファシリティでデフォルトのロギング重大度を 3 に設定する例を示します。

```
Console> (enable) set logging level cdp 3 default
System logging facility <cdp> set to severity 3(errors)
Console> (enable)
```

ロギング タイムスタンプ イネーブル ステートのイネーブル化およびディセーブル化

ロギング タイムスタンプ ステートをイネーブルまたはディセーブルに設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ロギング タイムスタンプ ステートをイネーブルまたはディセーブルに設定します。	**set logging timestamp** {**enable** | **disable**}
ステップ 2	ロギング タイムスタンプのステートを確認します。	**show logging** [**noalias**]

次に、システム ロギング メッセージにタイムスタンプを表示できるようにする例を示します。

```
Console> (enable) set logging timestamp enable
System logging messages timestamp will be enabled.
Console> (enable)
```

ロギング バッファ サイズの指定

ロギング バッファに記録するメッセージ数を設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ロギング バッファに記録するメッセージ数を設定します。	**set logging buffer** *buffer_size*
ステップ 2	システム メッセージ ロギングの設定を確認します。	**show logging** [**noalias**]

次に、ロギング バッファ サイズを 200 メッセージに設定する例を示します。

```
Console> (enable) set logging buffer 200
System logging buffer size set to <200>
Console> (enable)
```

Syslog メッセージ数の制限

重大度に基づいてヒストリ テーブルと SNMP ネットワーク管理ステーションに送信する Syslog メッセージ数を制限できます。デフォルトの重大度は warnings（4）に設定されています。

Syslog メッセージ数を制限するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	Syslog メッセージ数を制限します。	**set logging history severity** *severity_level*
ステップ 2	システム メッセージ ロギングの設定を確認します。	**show logging**

次に、Syslog メッセージ数を notifications（5）の重大度を持つメッセージに制限する例を示します。

```
Console> (enable) set logging history severity 5
System logging history set to severity <5>
Console> (enable)
```

UNIX Syslog サーバ上での Syslog デーモンの設定

UNIX Syslog サーバにシステム ログ メッセージを送信するには、あらかじめ UNIX サーバ上で Syslog デーモンを設定しておく必要があります。root としてログインし、次の手順を実行します。

ステップ 1　/etc/syslog.conf ファイルに次のような行を追加します。

```
user.debug                      /var/log/myfile.log
```

（注）　**user.debug** と **/var/log/**myfile.log の間に 5 個のタブ文字を入れる必要があります。/etc/syslog.conf ファイルのエントリを参照してください。

スイッチは、指定されたファシリティ タイプと重大度に従って、メッセージを送信します。**user** キーワードで、使用する UNIX ロギング ファシリティを指定します。スイッチのメッセージがユーザ プロセスによって生成されます。**debug** キーワードで、記録する状況の重大度を指定します。UNIX システムがスイッチからすべてのメッセージを受信するように設定することもできます。

ステップ 2　UNIX シェル プロンプトに次のコマンドを入力し、ログ ファイルを作成します。

```
$ touch /var/log/myfile.log
$ chmod 666 /var/log/myfile.log
```

ステップ 3　次のコマンドを入力し、Syslog デーモンに変更が反映されたことを確認します。

```
$ kill -HUP `cat /etc/syslog.pid
```

Syslog サーバの設定

（注）　システム ログ メッセージを UNIX Syslog サーバに送信するには、「UNIX Syslog サーバ上での Syslog デーモンの設定」（p.28-9）の説明に従って、UNIX サーバ上であらかじめ Syslog デーモンを設定しておく必要があります。

Syslog サーバにメッセージを記録するようにスイッチを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	1 つまたは複数の Syslog サーバの IP アドレスを指定します。[1]	**set logging server** *ip_addr*
ステップ 2	Syslog サーバ メッセージのファシリティおよび重大度を設定します。	**set logging server facility** *server_facility_parameter* **set logging server severity** *server_severity_level*
ステップ 3	設定した Syslog サーバへのシステム メッセージ ロギングをイネーブルにします。	**set logging server enable**
ステップ 4	設定を確認します。	**show logging** [**noalias**]

1. 最大 3 つの Syslog サーバを設定できます。

次に、Syslog サーバを指定して、ファシリティおよび重大度を設定し、サーバへのロギングをイネーブルにする例を示します。

```
Console> (enable) set logging server 10.10.10.100
10.10.10.100 added to System logging server table.
Console> (enable) set logging server facility local5
System logging server facility set to <local5>
Console> (enable) set logging server severity 5
System logging server severity set to <5>
Console> (enable) set logging server enable
System logging messages will be sent to the configured syslog servers.
Console> (enable)
```

Syslog サーバ テーブルから Syslog サーバを削除するには、イネーブル モードで次の作業を行います。

作業	コマンド
Syslog サーバ テーブルから Syslog サーバを削除します。	**clear logging server** *ip_addr*

次に、Syslog サーバ テーブルから Syslog サーバを削除する例を示します。

```
Console> (enable) clear logging server 10.10.10.100
System logging server 10.10.10.100 removed from system logging server table.
Console> (enable)
```

Syslog サーバへのロギングをディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
設定した Syslog サーバへのシステム メッセージ ロギングをディセーブルにします。	**set logging server disable**

次に、Syslog サーバへのロギングをディセーブルにする例を示します。

```
Console> (enable) set logging server disable
System logging messages will not be sent to the configured syslog servers.
Console> (enable)
```

ロギングの設定の表示

show logging コマンドを使用して、現在のシステム メッセージ ロギングの設定を表示します。設定されている Syslog サーバのホスト名ではなく IP アドレスを表示する場合は、**noalias** キーワードを使用します。

システム メッセージ ロギングに関する現在の設定を表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
現在のシステム メッセージ ロギングの設定を表示します。	**show logging** [**noalias**]

次に、システム メッセージ ロギングの現在の設定を表示する例を示します。

```
Console> (enable) show logging
Logging buffered size:       500
        timestamp option:    enabled
Logging history size:        1
            severity:        notifications(5)
Logging console:             enabled
Logging server:              disabled
        server facility:     LOCAL7
        server severity:     warnings(4
Current Logging Session:     enabled


Facility            Default Severity         Current Session Sever
-------------       -----------------------  ---------------------
acl                 5                        5
cdp                 4                        4
cops                3                        3
dtp                 5                        5
dvlan               2                        2
earl                2                        2
filesys             2                        2
gvrp                2                        2
ip                  2                        2
kernel              2                        2
ld                  3                        3
mcast               2                        2
mgmt                5                        5
mls                 5                        5
pagp                5                        5
protfilt            2                        2
pruning             2                        2
privatevlan         3                        3
qos                 3                        3
radius              2                        2
rsvp                3                        3
security            2                        2
snmp                2                        2
spantree            2                        2
sys                 5                        5
tac                 2                        2
tcp                 2                        2
telnet              2                        2
tftp                2                        2
udld                4                        4
vmps                2                        2
vtp                 2                        2

0(emergencies)        1(alerts)             2(critical)
3(errors)             4(warnings)           5(notifications)
6(information)        7(debugging)
Console> (enable)
```

システム メッセージの表示

show logging buffer コマンドを使用して、スイッチのロギング バッファ内のメッセージを表示します。*number_of_messages* を指定しなかった場合、デフォルトとして、バッファ内に格納された最後の 20 個のメッセージ（-20）が表示されます。

スイッチのロギング バッファ内のメッセージを表示するには、次のいずれかの作業を行います。

作業	コマンド
バッファ内の最初の *number_of_messages* 指定数のメッセージを表示します。	**show logging buffer** [*number_of_messages*]
バッファ内の最後の *number_of_messages* 指定数のメッセージを表示します。	**show logging buffer -**[*number_of_messages*]

次に、バッファ内の最初の 5 つのメッセージを表示する例を示します。

```
Console> (enable) show logging buffer 5
1999 Apr 16 08:40:11 %SYS-5-MOD_OK:Module 1 is online
1999 Apr 16 08:40:14 %SYS-5-MOD_OK:Module 3 is online
1999 Apr 16 08:40:14 %SYS-5-MOD_OK:Module 2 is online
1999 Apr 16 08:41:15 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1
1999 Apr 16 08:41:15 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/2
```

次に、バッファ内の最後の 5 つのメッセージを表示する例を示します。

```
Console> (enable) show logging buffer -5
%PAGP-5-PORTFROMSTP:Port 3/1 left bridge port 3/1
%SPANTREE-5-PORTDEL_SUCCESS:3/2 deleted from vlan 1 (PAgP_Group_Rx)
%PAGP-5-PORTFROMSTP:Port 3/2 left bridge port 3/2
%PAGP-5-PORTTOSTP:Port 3/1 joined bridge port 3/1-2
%PAGP-5-PORTTOSTP:Port 3/2 joined bridge port 3/1-2
Console> (enable)
```

システム Syslog ダンプのイネーブル化およびディセーブル化

システム障害が発生した場合、Syslog バッファ内のシステム メッセージ（**show logging buffer** コマンド実行時の出力）を格納したファイルが生成されます。

システム Syslog ダンプをイネーブルまたはディセーブルにするには、イネーブル モードで次の作業を行います（デフォルトでは Syslog ダンプはディセーブル）。

	作業	コマンド
ステップ 1	システム Syslog ダンプをイネーブルまたはディセーブルにします。	**set system syslog-dump** {**enable** | **disable**}
ステップ 2	システム Syslog ダンプのステータスを確認します。	**show system**

次に、システム Syslog ダンプをイネーブルにする例を示します。

```
Console> (enable) set system syslog-dump enable
(1) In the event of a system crash, this feature will
cause a syslog file to be written out.
(2) Selected syslog file is slot0:sysloginfo
(3) Please make sure the above device has been installed,
and ready to use.
Syslog-dump enabled
Console> (enable)
```

次に、システム Syslog ダンプをディセーブルにする例を示します。

```
Console> (enable) set system syslog-dump disable
Syslog-dump disabled
Console> (enable)
```

次に、システム Syslog ダンプのステータスを表示する例を示します。

```
Console> (enable) show system
PS1-Status PS2-Status
---------- ----------
ok         none

Fan-Status Temp-Alarm Sys-Status Uptime d,h:m:s Logout
---------- ---------- ---------- -------------- ---------
ok         off        ok         1,00:03:18     20 min
.
.
.
Core Dump                Core File
------------------------ ----------------------
disabled                 slot0:crashinfo


Syslog Dump              Syslog File
------------------------ ----------------------
enabled                  slot0:sysloginfo
Console> (enable)
```

システム Syslog ダンプ用のフラッシュ デバイスおよびファイル名の指定

Syslog ダンプをイネーブルまたはディセーブルにする際、フラッシュ デバイスおよびファイル名を変更できます。フラッシュ デバイスのみを指定した場合、ファイル名は自動的に sysloginfo に設定されます。フラッシュ デバイスおよびファイル名を指定しなければ、Syslog ダンプ用に設定済みのファイル名は削除され、デフォルトのフラッシュ デバイスとファイル名（slot0:sysloginfo）が使用されます。

システム Syslog ダンプ用のフラッシュ デバイスおよびファイル名を指定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	フラッシュ デバイスおよびファイル名を指定します。	**set system syslog-file** [*device*:[*filename*]]
ステップ 2	フラッシュ デバイスおよびファイル名の設定を確認します。	**show system**

次に、Syslog ダンプ用のフラッシュ デバイスを設定する例を示します。

```
Console> (enable) set system syslog-file bootflash:
Default filename sysloginfo added to the device bootflash:
System syslog-file set.
Console> (enable)
```

次に、フラッシュ デバイスおよびファイル名を設定する例を示します。

```
Console> (enable) set system syslog-file bootflash:sysmsgs1
System syslog-file set.
Console> (enable)
```

次に、フラッシュ デバイスおよびファイル名をデフォルト設定に戻す例を示します。

```
Console> (enable) set system syslog-file
System syslog-file set to the default file.
Console> (enable)
```

コールホームの設定

コールホーム機能を使用して、指定した重大度の Syslog メッセージを、指定した電子メール アドレスやポケベル アドレスに送るようにスイッチを設定できます。

コールホームは Syslog メッセージが生成されると起動されます。生成された Syslog メッセージの重大度が設定値より低い場合は、メッセージが指定の宛先アドレスに転送されることはありません。重大度が設定値より高い場合、スイッチは入力済みの一連の宛先アドレスに Syslog メッセージを転送します。

コールホームは Syslog メッセージとその重大度に関連付けられています。コールホームの重大度を設定する際は、既存の **set logging level** コマンド、および新規に導入された **set logging callhome severity** コマンドに必要な重大度を、十分に検討してください。

Syslog で alerts（レベル 1）のような非常に高い重大度を設定すると、コールホームで notifications（レベル 5）のような低い重大度を設定しても、宛先アドレスは alerts および emergencies（レベル 0 および 1）しか受信しません。宛先アドレスは、指定した残りのコールホーム重大度の通知（レベル 2、3、4）を受け取りません。宛先アドレスが、設定したすべての重大度の警告および通知を受信するようにするには、コールホームの重大度を、使用する Syslog メッセージの重大度以上に設定します。

複数の Simple Mail Transfer Protocol（SMTP）サーバを設定すれば、いずれのサーバが障害を起こしてもコールホーム機能は中断しません。SMTP サーバが障害を起こした場合、スイッチは次の設定済みサーバに連絡します。複数の SMTP サーバを設定している場合、スイッチは最初に発見した使用可能な SMTP サーバを使用します。

スイッチ上でコールホームを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	コールホームをイネーブルにします。	**set logging callhome** {**enable** | **disable**}
ステップ 2	Syslog メッセージおよび（必要に応じて）フラグメント サイズを受信させる宛先の電子メールまたはポケベル アドレスを指定します。	**set logging callhome destination** *Email or Epage Address* [**fragment** *size in bytes*]
ステップ 3	スイッチが Syslog メッセージを送信する SMTP サーバの IP アドレスを指定します。	**set logging callhome smtp-server** *IP Address*
ステップ 4	コールホームの重大度を指定します。 **（注）** デフォルトでは、この重大度は critical メッセージのみ（レベル 2）に設定されています。	**set logging callhome severity** *level*
ステップ 5	（任意）SMTP サーバが Syslog メッセージを転送できない場合のために [from] 電子メール アドレスを設定します。 **（注）** 配信に失敗した場合、SMTP　サーバはメッセージをこの [from] アドレスに送信します。	**set logging callhome from** *Email Address*
ステップ 6	（任意）受信側に [from] アドレス以外のアドレスに応答させたい場合、[reply to] 電子メール アドレスを設定します。	**set logging callhome reply-to** *Email address*
ステップ 7	設定を確認します。	**show logging callhome**

次に、コールホームをイネーブルにする例を示します。

```
Console> (enable) set logging callhome enable
Callhome functionality is enabled.
Callhome messages will be sent to the configured destination addresses.
Console> (enable)
```

次に、以下のアドレスがコールホーム メッセージを受信するように設定する例を示します。

- ポケベル：adminjoe@epage.cisco（128 バイトのフラグメント サイズを使用）
- 電子メール：adminboss@cisco.com および adminjane@cisco.com

```
Console> (enable) set logging callhome destination adminjoe@epage.cisco fragment 128
Included adminjoe@epage.cisco in the table of callhome destination addresses.
Messages will be sent to this address in fragments of 128 bytes.
Console> (enable) set logging callhome destination adminjane@cisco.com
Included adminjane@cisco.com in the table of callhome destination addresses.
Messages will be sent to this address without fragmentation.
Console> (enable) set logging callhome destination adminboss@cisco.com
Included adminboss@cisco.com in the table of callhome destination addresses.
Messages will be sent to this address without fragmentation.
Console> (enable)
```

次に、IP アドレス 172.20.8.16 の SMTP サーバを設定する例を示します。

```
Console> (enable) set logging callhome smtp-server 172.20.8.16
Included 172.20.8.16 in the table of callhome SMTP servers.
Console> (enable)
```

次に、重大度を 3（critical および error メッセージ）に設定する例を示します。

```
Console> (enable) set logging callhome severity 3
Callhome severity level set to 3
Console> (enable)
```

次に、From アドレスを adminjoe@cisco.com に設定する例を示します。

```
Console> (enable) set logging callhome from adminjoe@cisco.com
From address of callhome messages is set to adminjoe@cisco.com
Console> (enable)
```

次に、Reply to アドレスを adminjane@cisco.com に設定する例を示します。

```
Console> (enable) set logging callhome reply-to adminjane@cisco.com
Reply-To address of callhome messages is set to adminjane@cisco.com
Console> (enable)
```

次に、設定を確認する例を示します。

```
Console> (enable) show logging callhome
Callhome Functionality:       enabled
Callhome Severity:            LOG_ERR (3)

SMTP Server
-----------
172.20.8.16

Destination Address                                                 Message Size
--------------------                                                ------------
adminboss@cisco.com                                                 No Fragmentation
adminjane@cisco.com                                                 No Fragmentation
adminjoe@epage.cisco                                                128 bytes

From: adminjoe@cisco.com
Reply-To: adminjane@cisco.com
Console> (enable)
```

コールホームのディセーブル化

コールホームをディセーブルにしても、設定した他のコールホーム パラメータは消去されません。各パラメータを個別に消去する必要があります。

スイッチ上でコールホームをディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
コールホームをディセーブルにします。	**set logging callhome disable**

次に、コールホームをディセーブルにする例を示します。

```
Console> (enable) set logging callhome disable
Callhome functionality is disabled.
Callhome messages will not be sent to the configured destination addresses.
Console> (enable)
```

コールホーム メッセージを受信するアドレス リストからアドレスを消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
コールホーム メッセージを受信するアドレス リストから宛先アドレスを消去します。	**clear logging callhome destination** *Email or Epage Address*

次に、宛先アドレス adminboss@cisco.com をコールホーム メッセージを受信するアドレス リストから消去する例を示します。

```
Console> (enable) clear logging callhome destination adminboss@cisco.com
Removed adminboss@cisco.com from the table of callhome destination addresses.
Console> (enable)
```

[from] アドレスを消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
[from] アドレスを消去します。	**clear logging callhome from**

[from] アドレスを消去する例を示します。

```
Console> (enable) clear logging callhome from
Cleared the from address field of callhome messages.
Console> (enable)
```

[reply to] アドレスを消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
[reply to] アドレスを消去します。	**clear logging callhome reply-to**

[reply to] アドレスを消去する例を示します。

```
Console> (enable) clear logging callhome reply-to
Cleared the reply-to address field of callhome messages.
Console> (enable)
```

コールホーム SMTP サーバ リストから SMTP サーバを消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
SMTP サーバを消去します。	**clear logging callhome smtp-server** *IP Address*

次に、SMTP サーバ 172.20.8.16 をコールホーム サーバ リストから削除する例を示します。

```
Console> (enable) clear logging callhome smtp-server 172.20.8.16
Removed 172.20.8.16 from the table of callhome SMTP servers.
Console> (enable)
```

コールホームの重大度を消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
コールホームの重大度を消去します。	**clear logging callhome severity**

次に、コールホームの重大度を消去する例を示します。

```
Console> (enable) clear logging callhome severity
Cleared callhome severity level to its default value of 2(LOG_CRIT).
Console> (enable)
```

CHAPTER 29

DNS の設定

この章では、Catalyst 6500 シリーズ スイッチ上で Domain Name System（DNS; ドメイン ネーム システム）を設定する方法について説明します。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

この章で説明する内容は、次のとおりです。

DNS の機能

DNS は、DNS サーバから DNS プロトコルを使用して、ホスト名を IP アドレスにマッピングすることができる分散データベースです。スイッチに DNS を設定すると、**ping**、**telnet**、**upload**、**download** など、すべての IP コマンドにおいて、IP アドレスの代わりにホスト名を使用できます。

DNS を使用するには、ネットワーク上に DNS ネーム サーバが設定されていなければなりません。

スイッチには、プライマリ DNS ネーム サーバのほかに、2 台のバックアップ サーバを指定できます。プライマリ サーバを明示的に特定しないと、最初に指定したサーバがプライマリ サーバになります。スイッチは、最初にプライマリ サーバに対して DNS クエリを送信します。プライマリ サーバへのクエリに失敗すると、バックアップ サーバにクエリが送信されます。

DNS のデフォルト設定

表 29-1 に、DNS のデフォルト設定を示します。

表 29-1　DNS のデフォルト設定

機能	デフォルト値
DNS イネーブル ステート	ディセーブル
DNS デフォルト ドメイン名	ヌル
DNS サーバ	指定なし

スイッチ上での DNS の設定

ここでは、DNS を設定する手順について説明します。

- DNS の設定およびイネーブル化（p.29-2）
- DNS サーバの消去（p.29-3）
- DNS ドメイン名の消去（p.29-3）
- DNS のディセーブル化（p.29-4）

DNS の設定およびイネーブル化

スイッチ上で DNS を設定してイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	1 つまたは複数の DNS サーバの IP アドレスを指定します。	**set ip dns server** *ip_addr* [**primary**]
ステップ 2	ドメイン名を設定します。	**set ip dns domain** *name*
ステップ 3	DNS をイネーブルにします。	**set ip dns enable**
ステップ 4	DNS の設定を確認します。	**show ip dns** [**noalias**]

次に、スイッチ上で DNS を設定してイネーブルにし、設定を確認する例を示します。

```
Console> (enable) set ip dns server 10.2.2.1
10.2.2.1 added to DNS server table as primary server.
Console> (enable) set ip dns server 10.2.24.54 primary
10.2.24.54 added to DNS server table as primary server.
Console> (enable) set ip dns server 10.12.12.24
10.12.12.24 added to DNS server table as backup server.
Console> (enable) set ip dns domain corp.com
Default DNS domain name set to corp.com
Console> (enable) set ip dns enable
DNS is enabled
Console> (enable) show ip dns
DNS is currently enabled.
The default DNS domain name is: corp.com

DNS name server                          status
---------------------------------------  -------
dns_serv2
dns_serv1                                primary
dns_serv3
Console> (enable)
```

DNS サーバの消去

DNS サーバ テーブルから DNS サーバを消去するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	DNS サーバ テーブルから 1 つまたはすべての DNS サーバを消去します。	**clear ip dns server** [*ip_addr* | **all**]
ステップ 2	DNS の設定を確認します。	**show ip dns** [**noalias**]

次に、DNS サーバ テーブルから DNS サーバを消去する例を示します。

```
Console> (enable) clear ip dns server 10.12.12.24
10.12.12.24 cleared from DNS table
Console> (enable)
```

次に、DNS サーバ テーブルからすべての DNS サーバを消去する例を示します。

```
Console> (enable) clear ip dns server all
All DNS servers cleared
Console> (enable)
```

DNS ドメイン名の消去

デフォルトの DNS ドメイン名を消去するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	デフォルトの DNS ドメイン名を消去します。	**clear ip dns domain**
ステップ 2	DNS の設定を確認します。	**show ip dns** [**noalias**]

次に、デフォルトの DNS ドメイン名を消去する例を示します。

```
Console> (enable) clear ip dns domain
Default DNS domain name cleared.
Console> (enable)
```

DNS のディセーブル化

DNS をディセーブルするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチ上で DNS をディセーブルにします。	**set ip dns disable**
ステップ 2	DNS の設定を確認します。	**show ip dns** [**noalias**]

次に、スイッチ上で DNS をディセーブルにする例を示します。

```
Console> (enable) set ip dns disable
DNS is disabled
Console> (enable)
```

CHAPTER 30

CDP の設定

この章では、Catalyst 6500 シリーズ スイッチ上で Cisco Discovery Protocol（CDP）を設定する方法について説明します。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

この章で説明する内容は、次のとおりです。

CDP の機能

CDP は Release 8.1(1) のソフトウェア リリースで機能強化されているため、高出力の新しい Cisco IP Phone との下位互換性を簡単に確保できます。この機能強化した CDP により、Cisco IP Phone はスイッチへの電源要求を CDP パケット内でネゴシエーションします。スイッチはこの情報を使用して、使用可能な電力をオーバーサブスクライブしないようにします。

CDP は、ルータ、ブリッジ、アクセス サーバ、通信サーバ、スイッチなど、すべてのシスコ製装置上で実行できる、メディアやプロトコルに依存しないプロトコルです。CDP を使用して、スイッチに直接接続しているすべてのシスコ製装置の情報を表示することができます。CDP はさらに、ネイティブ VLAN（仮想 LAN）とポート デュプレックスの不一致を検出します。

CDP を使用することにより、ネットワーク管理アプリケーションで、近接するシスコ製装置のタイプおよび SNMP（簡易ネットワーク管理プロトコル）エージェント アドレスを検索できます。この機能により、アプリケーションから近接装置に SNMP クエリを送信できます。CDP により、ネットワーク管理アプリケーションは、既知の装置に近接しているシスコ製装置、特にプロトコルに関係なく下位レイヤの近接装置を検索できます。

CDP は、Subnetwork Access Protocol（SNAP）をサポートしているすべてのメディア上で稼働します。CDP が稼働するのはデータリンク層だけです。

シスコ製装置は CDP パケットを転送しません。新しい CDP 情報を受信すると、古い情報は破棄されます。

CDP のデフォルト設定

表 30-1 に、CDP のデフォルト設定を示します。

表 30-1　CDP のデフォルト設定

機能	デフォルト値
CDP グローバル イネーブル ステート	イネーブル
CDP ポート イネーブル ステート	すべてのポート上でイネーブル
CDP メッセージ インターバル	60 秒
CDP 保持時間	180 秒

スイッチ上での CDP の設定

ここでは、CDP を設定する手順について説明します。

CDP グローバル イネーブルおよびディセーブル ステートの設定

CDP グローバル イネーブル ステートを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチ上で CDP グローバル イネーブル ステートを設定します。	**set cdp** {**enable** | **disable**}
ステップ 2	CDP の設定を確認します。	**show cdp**

次に、CDP をグローバルにイネーブルにし、設定を確認する例を示します。

```
Console> (enable) set cdp enable
CDP enabled globally
Console> (enable) show cdp
CDP                : enabled
Message Interval   : 60
Hold Time          : 180
Console> (enable)
```

次に、CDP をグローバルにディセーブルにし、設定を確認する例を示します。

```
Console> (enable) set cdp disable
CDP disabled globally
Console> (enable) show cdp
CDP                : disabled
Message Interval   : 60
Hold Time          : 180
Console> (enable)
```

ポート上での CDP イネーブルおよびディセーブル ステートの設定

CDP は、ポート単位でイネーブルまたはディセーブルに設定できます。CDP をグローバルにイネーブルにしてからでなければ、スイッチはポートに CDP メッセージを送信できません。

ポート単位で CDP イネーブル ステートを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	個々のポートに CDP イネーブル ステートを設定します。	**set cdp** {**enable** | **disable**} [*mod/port*]
ステップ 2	CDP の設定を確認します。	**show cdp port** [*mod*[/*port*]]

次に、ポート 3/1 ～ 2 上で CDP をイネーブルにし、設定を確認する例を示します。

```
Console> (enable) set cdp enable 3/1-2
CDP enabled on ports 3/1-2.
Console> (enable) show cdp port 3
CDP               : enabled
Message Interval  : 60
Hold Time         : 180

Port      CDP Status
--------  ----------
 3/1      enabled
 3/2      enabled
 3/3      disabled
 3/4      disabled
 3/5      disabled
 3/6      disabled
 3/7      enabled
 3/8      enabled
 3/9      enabled
 3/10     enabled
 3/11     enabled
 3/12     enabled
Console> (enable)
```

次に、ポート 3/1 ～ 6 上で CDP をディセーブルにし、設定を確認する例を示します。

```
Console> (enable) set cdp disable 3/1-6
CDP disabled on ports 3/1-6.
Console> (enable) show cdp port 3
CDP               : enabled
Message Interval  : 60
Hold Time         : 180

Port      CDP Status
--------  ----------
 3/1      disabled
 3/2      disabled
 3/3      disabled
 3/4      disabled
 3/5      disabled
 3/6      disabled
 3/7      enabled
 3/8      enabled
 3/9      enabled
 3/10     enabled
 3/11     enabled
 3/12     enabled
Console> (enable)
```

CDP メッセージ インターバルの設定

CDP メッセージ インターバルでは、スイッチが直接接続されたシスコ製装置へ CDP メッセージを送信する間隔を指定します。

デフォルトの CDP メッセージ インターバルを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	デフォルトの CDP メッセージ インターバルを設定します。設定範囲は、5 ～ 900 秒です。	**set cdp interval** *interval*
ステップ 2	CDP の設定を確認します。	**show cdp**

次に、デフォルトの CDP メッセージ インターバルを 100 秒に設定し、設定を確認する例を示します。

```
Console> (enable) set cdp interval 100
CDP message interval set to 100 seconds for all ports.
Console> (enable) show cdp
CDP               : enabled
Message Interval  : 100
Hold Time         : 180
Console> (enable)
```

CDP 保持時間の設定

CDP 保持時間では、近接装置からの CDP メッセージが受信されてから、その装置がすでに接続されていないとみなされてネイバ エントリが期限切れになるまでの時間を指定します。

デフォルトの CDP 保持時間を設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	デフォルトの CDP 保持時間を設定します。設定範囲は、10 ～ 255 秒です。	**set cdp holdtime** *interval*
ステップ 2	CDP の設定を確認します。	**show cdp**

次に、デフォルトの CDP 保持時間を 225 秒に設定し、設定を確認する例を示します。

```
Console> (enable) set cdp holdtime 225
CDP holdtime set to 225 seconds.
Console> (enable) show cdp
CDP               : enabled
Message Interval  : 100
Hold Time         : 225
Console> (enable)
```

CDP 近接情報の表示

直接接続されたシスコ製装置についての情報を表示するには、**show cdp neighbors** コマンドを入力します。接続ポートのネイティブ VLAN を表示するには、**vlan** キーワードを入力します。接続ポートのデュプレックス モードを表示するには、**duplex** キーワードを入力します。接続装置の装置機能コードを表示するには、**capabilities** キーワードを入力します。近接装置の詳細情報を表示するには、**detail** キーワードを入力します。

（注） 旧バージョンの CDP をサポートしているデバイスに対して **show cdp neighbors** コマンドを入力すると、VLAN Trunking Protocol（VTP;VLAN トランキング プロトコル）Management Domain、Native VLAN、Duplex の各フィールドには [unknown]（確認不能）と表示されます。

直接接続されたシスコ製装置の情報を表示するには、次の作業を行います。

作業	コマンド
CDP 近接装置の情報を表示します。	**show cdp neighbors** [*mod*[*/port*]] [**vlan** | **duplex** | **capabilities** | **detail**]

次に、接続されたシスコ製装置の CDP 近接情報を表示する例を示します。

```
Console> (enable) show cdp neighbors
* - indicates vlan mismatch.
# - indicates duplex mismatch.
Port     Device-ID                      Port-ID                   Platform
-------- ------------------------------ ------------------------- ------------
 2/3     JAB023807H1(2948)              2/2                       WS-C2948
 3/1     JAB023806JR(4003)              2/1                       WS-C4003
 3/2     JAB023806JR(4003)              2/2                       WS-C4003
 3/5     JAB023806JR(4003)              2/5                       WS-C4003
 3/6     JAB023806JR(4003)              2/6                       WS-C4003
Console> (enable)
```

次に、近接装置の各接続ポートのネイティブ VLAN を表示する例を示します（アスタリスク [*] は、ローカル スイッチのポート 3/6 と近接装置のポート 2/6 間にネイティブ VLAN の不一致があることを示しています）。

```
Console> (enable) show cdp neighbors vlan
* - indicates vlan mismatch.
# - indicates duplex mismatch.
Port     Device-ID                      Port-ID                   NativeVLAN
-------- ------------------------------ ------------------------- ----------
 2/3     JAB023807H1(2948)              2/2                       522
 3/1     JAB023806JR(4003)              2/1                       100
 3/2     JAB023806JR(4003)              2/2                       100
 3/5     JAB023806JR(4003)              2/5                       1
 3/6     JAB023806JR(4003)              2/6*                      1
Console> (enable)
```

次に、近接装置の詳細情報を表示する例を示します。

```
Console> (enable) show cdp neighbors 2/3 detail
Port (Our Port): 2/3
Device-ID: JAB023807H1(2948)
Device Addresses:
  IP Address: 172.20.52.36
Holdtime: 132 sec
Capabilities: TRANSPARENT_BRIDGE SWITCH
Version:
  WS-C2948 Software, Version McpSW: 5.1(57) NmpSW: 5.1(1)
  Copyright (c) 1995-1999 by Cisco Systems, Inc.
Platform: WS-C2948
Port-ID (Port on Neighbors's Device): 2/2
VTP Management Domain: Lab_Network
Native VLAN: 522
Duplex: full
Console> (enable)
```

CHAPTER 31

UDLD の設定

この章では、Catalyst 6500 シリーズ スイッチ上で UniDirectional Link Detection（UDLD; 単一方向リンク検出）プロトコルを設定する方法について説明します。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

この章で説明する内容は、次のとおりです。

UDLD の機能

UDLD プロトコルにより、光ファイバまたは銅（たとえば、カテゴリ 5 のケーブルなど）イーサネット ケーブルを使用して接続された装置で、ケーブルの物理構成をモニタし、単一方向のリンクの存在を検出することができます。単一方向リンクが検出されると、UDLD が関係のあるポートをシャットダウンし、ユーザに通知します。単一方向リンクは、スパニングツリー トポロジー ループをはじめ、さまざまな問題を引き起こす可能性があります。

UDLD は、レイヤ 1 メカニズムとともに作用し、リンクの物理的ステータスを判別するレイヤ 2 プロトコルです。レイヤ 1 では、物理的シグナリングおよび障害検出は、自動ネゴシエーションによって処理されます。UDLD は、ネイバの識別情報の検知、不正に接続されたポートのシャットダウンなど、自動ネゴシエーションでは実行不可能な処理を実行します。自動ネゴシエーションと UDLD の両方をイネーブルにすると、レイヤ 1 とレイヤ 2 の検知機能が協調して作用し、物理的および論理的な単一方向接続、および他のプロトコルの不正な動作を防止します。

リンク上でローカル装置が送信したトラフィックをネイバが受信するにもかかわらず、ネイバから送信されたトラフィックをローカル装置が受信しない場合に、単一方向リンクが発生します。対になっているファイバ ストランドのどちらかの接続が切れた場合、自動ネゴシエーションがアクティブであるかぎり、そのリンクは存続できません。この場合、論理リンクは不確定であり、UDLD は何の措置も行いません。レイヤ 1 の観点から両方のファイバが正常に稼働していれば、レイヤ 2 の UDLD はそれらのファイバが正しく接続しているかどうか、トラフィックが正しいネイバ間で双方向に流れているかどうかを判別します。自動ネゴシエーションはレイヤ 1 のメカニズムであるため、このチェックは自動ネゴシエーションでは不可能です。

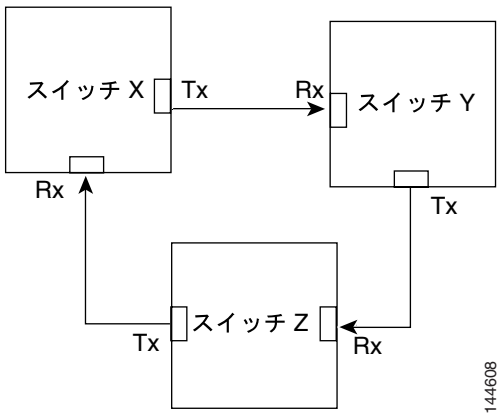
スイッチは、近接装置の UDLD がイネーブルのポートに、UDLD メッセージ（パケット）を定期的に送信します。このメッセージが一定時間内に送信元にエコー バックされ、特定の確認応答（エコー）が欠落している場合には、そのリンクは単一方向リンクとしてフラグ付けされ、ポートがシャットダウンされます。プロトコルが単一方向リンクを正しく識別して使用を禁止できるようにするには、リンクの両端の装置で UDLD をサポートしている必要があります。

（注） Release 5.4(3) 以降のスーパバイザ エンジン ソフトウェア リリースでは、UDLD メッセージのインターバルを指定できます。旧リリースでは、メッセージ インターバルは 60 秒に固定されていました。メッセージ インターバルが設定可能になったため、UDLD がリンク障害に対して迅速に反応します。

（注） デフォルトでは、UDLD は銅ポート上ではローカルにディセーブルに設定されています。この種のメディアは、アクセス ポートに使用されることが多いので、メディアに不要な制御トラフィックを送信しないようにするためです。

図 31-1 に、単一方向リンク条件の例を示します。各スイッチは、近接スイッチにパケットを送信しますが、これと同じスイッチからのパケットを受信できません。UDLD は、これらの一方向接続を検出し、ディセーブルにします。

図 31-1　単一方向リンク



UDLD のデフォルト設定

表 31-1 に、UDLD のデフォルト設定を示します。

表 31-1　UDLD のデフォルト設定

機能	デフォルト値
UDLD グローバル イネーブル ステート	グローバルにディセーブル
UDLD ポート別イネーブル ステート（光ファイバ メディア）	すべてのイーサネット光ファイバ ポート上でイネーブル
UDLD ポート別イネーブル ステート（ツイストペア［銅］メディア）	すべてのイーサネット 10/100 および 1000BASE-TX ポート上でディセーブル
UDLD メッセージ インターバル	15 秒
UDLD アグレッシブ モード	ディセーブル

スイッチ上での UDLD の設定

ここでは、UDLD を設定する手順について説明します。

UDLD のグローバルなイネーブル化

スイッチ上で UDLD をグローバルにイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチ上で UDLD をグローバルにイネーブルにします。	**set udld enable**
ステップ 2	設定を確認します。	**show udld**

次に、UDLD をグローバルにイネーブルにし、設定を確認する例を示します。

```
Console> (enable) set udld enable
UDLD enabled globally
Console> (enable) show udld
UDLD      : enabled
Console> (enable)
```

ポート単位での UDLD のイネーブル化

個々のポート上で UDLD をイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	特定のポート上で UDLD をイネーブルにします。	**set udld enable** *mod/port*
ステップ 2	設定を確認します。	**show udld port** [*mod*[*/port*]]

次に、ポート 4/1 上で UDLD をイネーブルにし、設定を確認する例を示します。

```
Console> (enable) set udld enable 4/1
UDLD enabled on port 4/1
Console> (enable) show udld port 4/1
UDLD      : enabled
Message Interval: 15 seconds
Port      Admin Status  Aggressive Mode Link State
--------  ------------  --------------- ---------
 4/1      enabled       disabled        bidirectional
Console> (enable)
```

ポート単位での UDLD のディセーブル化

個々のポート上で UDLD をディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	特定のポート上で UDLD をディセーブルにします。	**set udld disable** *mod/port*
ステップ 2	設定を確認します。	**show udld port** [*mod*[*/port*]]

次に、ポート 4/1 上で UDLD をディセーブルにする例を示します。

```
Console> (enable) set udld disable 4/1
UDLD disabled on port 4/1.
Console> (enable)
```

UDLD のグローバルなディセーブル化

スイッチ上で UDLD をグローバルにディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチ上で UDLD をグローバルにディセーブルにします。	**set udld disable**
ステップ 2	設定を確認します。	**show udld**

次に、スイッチ上で UDLD をグローバルにディセーブルにする例を示します。

```
Console> (enable) set udld disable
UDLD disabled globally
Console> (enable)
```

UDLD メッセージ インターバルの指定

UDLD のメッセージ インターバルを指定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	UDLD メッセージ インターバルを指定します。	**set udld interval** *interval*
ステップ 2	設定を確認します。	**show udld**

次に、スイッチ上で UDLD メッセージ インターバルを指定する例を示します。

```
Console> (enable) set udld interval 20
UDLD message interval set to 20 seconds
Console> (enable)
```

次に、スイッチ上で UDLD メッセージ インターバルを確認する例を示します。

```
Console> (enable) show udld
UDLD              : enabled
Message Interval  : 20 seconds
Console> (enable)
```

UDLD アグレッシブ モードのイネーブル化

Release 5.4(3) 以降のソフトウェア リリースでは、UDLD アグレッシブ モードがあります。UDLD アグレッシブ モードは、デフォルトではディセーブルに設定されています。このモードは、Release 5.4(3) 以降のソフトウェア リリースが稼働しているシスコ製スイッチ間のポイントツーポイント リンクに限って使用してください。アグレッシブ モードをイネーブルに設定した場合、双方向リンク上のポートが UDLD パケットを受信しなくなったとき、UDLD はネイバとの接続を再確立しようとします。この試行に 8 回失敗すると、ポートは errdisable ステートになります。

スパニングツリー ループを防止するため、デフォルトである 15 秒インターバルを使用する通常の UDLD により、（デフォルトのスパニングツリー パラメータを使用している場合）ブロッキング ポートがフォワーディング ステートに移行する前に、速やかに単一方向リンクをシャットダウンすることができます。

UDLD アグレッシブ モードは、次のような場合に利点をもたらします。

- リンクの一方の側でポート スタック（Tx および Rx）を使用している場合
- リンクの一方の側がダウンしているにもかかわらず、もう一方の側がアップしたままの場合

こういった状況では、UDLD アグレッシブ モードにより、リンク上のポートの 1 つが errdisable になり、トラフィックの廃棄を中止します。アグレッシブ モードをディセーブルに設定しても、1 つのポートが双方向にトラフィックを流すことはできないので、スパニングツリー ループに起因するブロードキャスト ストームの危険性はありません。

UDLD アグレッシブ モードをイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	UDLD アグレッシブ モードをイネーブルにします。	**set udld aggressive-mode enable** *mod/port*
ステップ 2	設定を確認します。	**show udld**

次に、スイッチ上で UDLD アグレッシブ モードをイネーブルにする例を示します。

```
Console> (enable) set udld aggressive-mode enable 4/1
Aggressive UDLD enabled on port 4/1.
Console> (enable)
```

次に、スイッチ上で UDLD アグレッシブ モードがイネーブルであることを確認する例を示します。

```
Console> (enable) show udld port 4/1
UDLD      : enabled
Message Interval: 30 seconds
Port      Admin Status  Aggressive Mode Link State
--------  ------------  --------------- ---------
 4/1      enabled       Enabled         bidirectional
Console> (enable)
```

UDLD の設定の表示

UDLD イネーブル ステートを表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
UDLD イネーブル ステートを表示します。	**show udld**

次に、UDLD イネーブル ステートを表示する例を示します。

```
Console> (enable) show udld
UDLD               : enabled
Message Interval   : 15 seconds
Console> (enable)
```

モジュールまたはポートの、UDLD の設定を表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
モジュールまたはポートの UDLD の設定を表示します。	**show udld port** [*mod*] [*mod/port*]

次に、モジュール 4 のポートについて、UDLD の設定を表示する例を示します。

```
Console> (enable) show udld port 4
UDLD      : enabled
Message Interval: 15 seconds
Port      Admin Status  Aggressive Mode Link State
--------  ------------  --------------- ---------
 4/1      enabled       disabled        bidirectional
 4/2      enabled       disabled        bidirectional
 4/3      enabled       disabled        undetermined
 4/4      enabled       disabled        bidirectional

.
.

Console> (enable)
```

表 31-2 に、**show udld** コマンドの出力に含まれるフィールドを説明します。

表 31-2　show udld コマンドの出力フィールド

フィールド	説明
UDLD	UDLD がイネーブルまたはディセーブルのどちらに設定されているかを示すステータス
Message Interval	メッセージ インターバル（秒数）
Port	モジュールおよびポート番号
Admin Status	管理ステータスがイネーブルまたはディセーブルのどちらに設定されているかを示すステータス
Aggressive Mode	アグレッシブ モードがイネーブルまたはディセーブルのどちらに設定されているかを示すステータス
Link State	リンクのステータス ― undetermined（検出中またはネイバの UDLD がディセーブルにされている）、not applicable（UDLD およびローカル ポートの両方または一方が手動でディセーブルにされている）、shutdown（単一方向リンクが検出され、ポートが errdisable にされた）、bidirectional（双方向リンクが検出され、ポートが双方向で正常に機能している）

CHAPTER 32

DHCP スヌーピングおよび IP ソース ガードの設定

この章では、Catalyst 6500 シリーズ スイッチで Dynamic Host Configuration Protocol（DHCP; ダイナミック ホスト コンフィギュレーション プロトコル）スヌーピングおよびソース ガードを設定する方法について説明します。

この章で説明する内容は、次のとおりです。

(注) この章で使用しているスイッチ コマンドの完全構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。また、次の関連資料も参照してください。
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_8_3/cmd_ref/index.htm

DHCP スヌーピングの機能概要

DHCP スヌーピングは、DHCP パケットをフィルタリングし、DHCP スヌーピング バインディング テーブルを作成し維持することにより、DHCP メッセージを使用して開始された DoS 攻撃に対するセキュリティを提供します。DHCP スヌーピングは、trusted（信頼性のある）および untrusted（信頼性のない）ポートの両方を使用します。

trusted ポートから受信した DHCP パケットは、検証なしで転送されます。一般的に、trusted ポートは DHCP サーバまたはリレー エージェントに到達するのに使用します。スイッチが untrusted ポートから DHCP パケットを受信すると、DHCP スヌーピングは、クライアントからの DHCP パケットのみが許可されて、情報のスヌーピングが実行されていないことを確認します。

DHCP スヌーピング バインディング テーブルには、スイッチの untrusted ポート上にある DHCP クライアントに関する MAC（メディア アクセス制御）アドレス、IP アドレス、リース期間（秒）、および VLAN（仮想 LAN）ポート情報が含まれています。DHCP スヌーピング バインディング テーブルに含まれる情報は、リース期間が終了するか DHCP スヌーピングが VLAN でディセーブルになると、バインディング テーブルから削除されます。

これらの DHCP メッセージは、DHCP バインディング テーブルを作成するのに使用します。

- DHCPACK ― バインディング エントリがない場合、新しいダイナミック DHCP バインディング エントリを追加します。
- DHCPNAK ― 既存の DHCP バインディング エントリを削除します。
- DHCPRELEASE ― バインディング エントリがある場合にダイナミック DHCP エントリを削除します。
- DHCPDECLINE ― バインディング エントリがある場合にダイナミック DHCP バインディング エントリを削除します。

各スイッチでは、ローカルの untrusted ポートだけに対する DHCP スヌーピング バインディング テーブルを保持しています。テーブルには、他のスイッチに直接接続されているホストの DHCP スヌーピング バインディング テーブルに関する情報は格納されず、trusted ポート経由で接続されているホストの情報も含まれていません。trusted ポートには、リレー エージェントまたは DHCP サーバなどの直接接続されているエンティティや、そのようなエンティティへの転送パスがあります。リレー エージェントまたは DHCP サーバへのパスは、信頼されている必要があります。

DHCP スヌーピング設定時の注意事項

ここでは、ネットワークに DHCP を設定する際の注意事項について説明します。

- DHCP スヌーピングをイネーブルにしてハイ アベイラビリティではないスイッチオーバーを実行した場合、DHCP スヌーピング バインディング テーブルの内容が消失します。この設定を使用することは推奨しません。
- DHCP スヌーピングは、Policy Feature Card（PFC; ポリシー フィーチャ カード）およびこれ以降のバージョンでサポートされます。
- DHCP スヌーピング バインディング テーブルは、16,384 エントリに制限されています。制限に到達すると、古いエントリがリース期間に到達するまで新しいエントリを追加できません。
- 802.1X-DHCP および DHCP スヌーピングは相互に排他的です。802.1X-DHCP と DHCP スヌーピングの両方に VLAN を設定できません。Access Control List（ACL; アクセス制御リスト）に 802.1X および DHCP スヌーピングの両方を設定した場合、ACL 内で高い位置にいる方がもう一方の機能を上書きします。
- Dynamic ARP Inspection（DAI）、DHCP スヌーピング、および IP ソース ガードを使用する場合、ハイ アベイラビリティをイネーブルにすることを推奨します。ハイ アベイラビリティがイネーブルでない場合、スイッチオーバー後にこれらの機能が動作するようにクライアントは IP アドレスを更新する必要があります。設定の詳細については、「ダイナミック ARP 検査」（p.15-40）を参照してください。

VLAN での DHCP スヌーピングの設定

一般的に、DHCP スヌーピングは、配線クローゼットなどのアクセスレベル ネットワークで使用されます。VLAN で DHCP スヌーピングをイネーブルにするには、その VLAN 上の DHCP クライアントに対する IP アドレスと MAC アドレスとのバインディング テーブルを作成します。

(注)　管理 VLAN sc0 および sc1 で DHCP をイネーブルにできません。

ここでは、DHCP スヌーピングを設定する手順について説明します。

DHCP スヌーピングのデフォルト設定

デフォルトでは、DHCP スヌーピングはディセーブルに設定されています。表 32-1 に、各 DHCP スヌーピング オプションのデフォルト設定値を示します。デフォルトの設定値を変更したい場合、「DHCP スヌーピングのイネーブル化」（p.32-4）を参照してください。

表 32-1　DHCP スヌーピングのデフォルト設定値

オプション	デフォルト値 / ステート
DHCP スヌーピング ホストのトラッキング情報オプション	ディセーブル
DHCP スヌーピング制限レート	Address Resolution Protocol（ARP; アドレス解決プロトコル）検査および 802.1X-DHCP で 1000 pps を共有します。レート制限は、PFC2 およびこれ以降のバージョンでサポートされます。
ポートでの DHCP スヌーピングの信頼	信頼しない
VLAN での DHCP スヌーピング	ディセーブル
DHCP スヌーピング バインディング データベースの自動保存オプション	ディセーブル
DHCP スヌーピング バインディング データベースのストレージ デバイスおよびファイル名	bootflash：dhcp-snooping-binding-database

DHCP スヌーピングのイネーブル化

DHCP スヌーピングは、セキュリティ VLAN ACL（VACL）を介して VLAN でイネーブルになっています。DHCP スヌーピング Access Control Entry（ACE; アクセス制御エントリ）を新規または既存のセキュリティ ACL に追加することにより、DHCP スヌーピングは VLAN でイネーブルに設定します。DHCP パケットのポリシーにしたがって、ACL 内の DHCP スヌーピングの位置を決定する必要があります。たとえば、特定のホストから DHCP パケットを拒否して他の DHCP パケットに対して DHCP スヌーピングを実行したい場合、DHCP スヌーピング ACE の前に拒否 ACE を配置する必要があります。

VLAN で DHCP スヌーピングをイネーブルにするには、次の作業を行います。

	作業	コマンド
ステップ 1	VACL に DHCP スヌーピングを追加します。	**set security acl ip** *acl_name* **permit dhcp-snooping**
ステップ 2	すべてのホストからの DHCP スヌーピングを許可するように VACL を設定します。	**set security acl ip** *acl_name* **permit ip any any**
ステップ 3	VACL を保存します。	**commit security acl** *acl_name*
ステップ 4	ACL を VLAN に追加します。	**set security acl map** *acl_name* **10**

次に、VLAN 上で DHCP スヌーピングを設定する例を示します。

```
Console> (enable) set security acl ip dhcpsnoop permit dhcp-snooping
Successfully configured DHCP Snooping for ACL dhcpsnoop. Use 'commit' command to
 save changes.
Console> (enable) set security acl ip dhcpsnoop permit ip any any
dhcpsnoop editbuffer modified. Use 'commit' command to apply changes.
Console> (enable) commit security acl dhcpsnoop
ACL commit in progress.

ACL 'dhcpsnoop' successfully committed.
Console> (enable) set security acl map dhcpsnoop 10
Mapping in progress.

ACL dhcpsnoop successfully mapped to VLAN 10.
Console> (enable)
```

（注） DHCP スヌーピングをイネーブルにするためだけに VACL を作成する場合、VACL にはリストの最後に暗黙の拒否があり、他のパケットは暗黙の許可がないかぎり許可されません。

（注） 802.1X-DHCP および DHCP スヌーピングは相互に排他的です。VLAN に両方の機能を設定しないでください。

プライベート VLAN での DHCP スヌーピングのイネーブル化

プライマリおよびセカンダリ（隔離またはコミュニティ）Private VLAN（PVLAN; プライベート VLAN）で別々に DHCP スヌーピングをイネーブルにする必要があります。DHCP スヌーピング バインディング テーブルには、プライマリ VLAN のバインディング情報のみが含まれていてセカンダリ VLAN の情報は含まれていません。DHCP スヌーピングを PVLAN でイネーブルにしてセカンダリ VLAN でイネーブルにしない場合、パケットは PVLAN で確認されていても、DHCP スヌーピング バインディング テーブル エントリは追加されません。

DHCP スヌーピング ホスト トラッキング情報オプションのイネーブル化

ホスト トラッキング情報オプションをイネーブルにする場合、DHCP リレー エージェント情報オプション（オプション 82）が転送されるクライアント パケットに追加されます。リレー エージェント オプションにはエージェント回線 ID およびエージェント リモート ID 情報が含まれています。回線 ID サブオプションには、クライアントのポートおよび VLAN 番号が含まれています。リモート ID サブオプションにはスイッチの MAC アドレスが含まれています。ホストトラッキング情報を挿入する前に、スイッチは DHCP メッセージに既存のリレー情報オプションやゼロ以外の giaddr フィールドがないことを確認します。ホストトラッキング情報を削除する前に、スイッチは、DHCP 応答メッセージが trusted ポートからのもので、リモート ID とローカル スイッチの MAC アドレスが一致することを確認します。パケットが trusted ポートからきたものでアドレスが一致しない場合、パケットは転送されます。

DHCP スヌーピングのホストトラッキング情報オプションを設定するには、次の作業を行います。

	作業	コマンド
ステップ 1	DHCP スヌーピング ホストのトラッキング情報オプションをイネーブルにします。	**set dhcp-snooping information host-tracking enable**
ステップ 2	ホストトラッキング情報オプションの MAC アドレスを表示します。	**show dhcp-snooping config**

次に、DHCP スヌーピング ホストトラッキング情報オプションを設定する例を示します。

```
Console> (enable) set dhcp-snooping information host-tracking enable
DHCP Snooping Information Option Enabled.
Console> (enable) show dhcp-snooping config
DHCP Snooping MAC address matching is enabled.
DHCP Snooping host-tracking information option is disabled.
Remote ID used in information option is 00-d0-00-4c-1b-ff.
Console> (enable)
```

DHCP スヌーピングの MAC アドレス一致オプションのイネーブル化

MAC アドレス一致オプションをイネーブルにする場合、イーサネット ヘッダーの送信元 MAC アドレスが、untrusted ポートからくる DHCP パケットの DHCP ペイロードにある chaddr フィールドと一致します。一致しない場合、パケットは廃棄されて untrusted ポートで廃棄されたパケットのカウンタが増加します。この機能は、デフォルトではイネーブルです。

DHCP スヌーピングの MAC アドレス一致オプションを設定するには、次の作業を行います。

	作業	コマンド
ステップ 1	DHCP スヌーピングの MAC アドレス一致オプションをイネーブルにします。	**set dhcp-snooping match-mac enable**
ステップ 2	DHCP スヌーピング設定を表示します。	**show dhcp-snooping config**

次に、DHCP スヌーピングの MAC アドレス一致オプションを設定する例を示します。

```
Console> (enable) set dhcp-snooping match-mac enable
DHCP Snooping MAC address matching enabled.
Console> (enable) show dhcp-snooping config
DHCP Snooping MAC address matching is enabled.
DHCP Snooping host-tracking information option is disabled.
Remote ID used in information option is 00-d0-00-4c-1b-ff.
Console> (enable)
```

DHCP スヌーピングの設定例

これらの設定例は、DHCP スヌーピングをイネーブルにする例を示したものです。

例 1：DHCP スヌーピングのイネーブル化

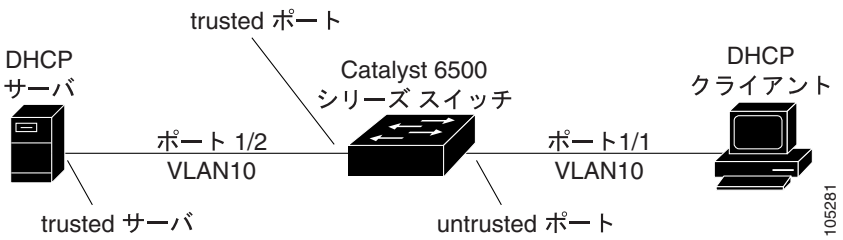
次に、DHCP サーバがポート 1/2 にある VLAN 10 の DHCP スヌーピングをイネーブルにする例を示します。

```
Console> (enable) set security acl ip dhcpsnoop permit dhcp-snooping
Successfully configured DHCP Snooping for ACL dhcpsnoop. Use 'commit' command to
 save changes.
Console> (enable) set security acl ip dhcpsnoop permit ip any any
dhcpsnoop editbuffer modified. Use 'commit' command to apply changes.
Console> (enable) commit security acl dhcpsnoop
ACL commit in progress.

ACL 'dhcpsnoop' successfully committed.
Console> (enable) set security acl map dhcpsnoop 10
Mapping in progress.

ACL dhcpsnoop successfully mapped to VLAN 10.
Console> (enable) set port dhcp-snooping 1/2 trust enable
Port(s)  1/2 state set to trusted for DHCP Snooping.
Console> show dhcp-snooping config
DHCP Snooping MAC address matching is enabled.
DHCP Snooping host-tracking information option is disabled.
Remote ID used in information option is 00-d0-00-4c-1b-ff.
Console> show port dhcp-snooping 1/1-2
Port     Trust
----     ------
1/1     untrusted
1/2     trusted
Console> (enable)
```

(注)　DHCP スヌーピングをイネーブルにしたあとに DHCP スヌーピング ホスト トラッキングを設定したい場合、**set dhcp-snooping information-option host-tracking** コマンドを入力します。

図 32-1 に、クライアント / サーバ ネットワークに DHCP スヌーピングを設定するのに使用する一般的なトポロジーを示します。

図 32-1　クライアントおよびサーバ用に設定された DHCP スヌーピング



例 2：MSFC を DHCP リレー エージェントとして使用した DHCP スヌーピングのイネーブル化

次に、DHCP ホスト トラッキングをイネーブルにして Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）をリレー エージェントとして設定する例を示します。

（注） この例では、クライアントは信頼性がなく、MSFC をリレー エージェントとするスイッチにアクセスします。MFSC リレー エージェント スイッチは、信頼できるトランク ポートを介して MSFC DHCP サーバ スイッチに接続します。

次に、MFSC を DHCP リレー エージェントとして設定する例を示します。

```
service dhcp
on int vlan 810
    ip address 192.168.80.241 255.255.255.0
    ip helper-address 192.168.94.247
    ip dhcp relay information trusted
on int vlan 4094
    ip address 192.168.94.241 255.255.255.0
```

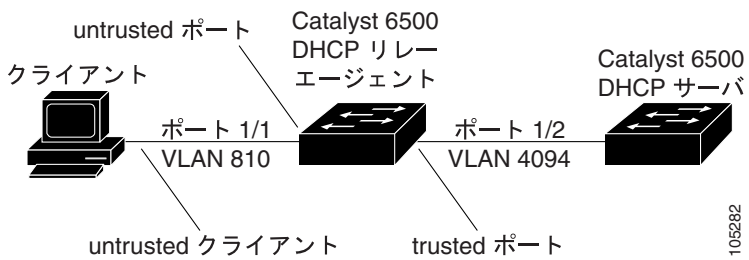
次に、MFSC を DHCP サーバとして設定する例を示します。

```
service dhcp
ip dhcp excluded-address 192.168.80.241
!
ip dhcp pool net810
   network 192.168.80.0 255.255.255.0
on int vlan 4094
   ip address 192.168.94.247 255.255.255.0
```

（注） MSFC ポートは、DHCP スヌーピングの trusted ポートとしてシステムに設定されています。

図 32-2 に、MSFC をリレー エージェントとして設定した場合の一般的なトポロジーを示します。

図 32-2　リレー エージェントとしての MSFC



DHCP スヌーピング情報の表示

ここにあるコマンドを使用して DHCP スヌーピング バインディング テーブルと設定情報を表示できます。

バインディング テーブルの表示

各スイッチの DHCP スヌーピング バインディング テーブルには、untrusted ポートに対応するバインディング エントリがあります。各相互接続スイッチには独自のバインディング テーブルがあるため、このテーブルには trusted ポートと相互接続しているホストに関する情報はありません。

作業	コマンド
DHCP スヌーピング バインディング テーブル情報を表示します。	**show dhcp-snooping bindings**

次に、スイッチの DHCP スヌーピング バインディング情報を表示する例を示します。

```
Console# show dhcp-snooping bindings
MacAddress          IpAddress        Lease(sec)    VLAN  Port
------------------  ---------------  ----------    ----  -----

00-01-7b-9b-05-3f   192.168.80.221   86377         810   1/8
```

表 32-2 に、**show dhcp-snooping binding** コマンドの出力に含まれるフィールドを説明します。

表 32-2　show dhcp-snooping bindings コマンド出力

フィールド	説明
MAC Address	クライアントのハードウェア MAC アドレス
IP Address	DHCP サーバから割り当てられたクライアントの IP アドレス
Lease (seconds)	IP アドレス リース期間
VLAN	クライアント ポートの VLAN 番号
Port	DHCP クライアント ホストに接続しているポート

DHCP スヌーピング設定と統計情報の表示

作業	コマンド
スイッチの DHCP スヌーピング設定を表示します。	**show dhcp-snooping config**

次に、DHCP スヌーピング ホスト トラッキングおよび一致 MAC 設定を表示する例を示します。

```
Console# show dhcp-snooping config
DHCP Snooping MAC address matching is enabled.
DHCP Snooping host-tracking information option is disabled.
Remote ID used in information option is 00-d0-00-4c-1b-ff.
Console#
```

作業	コマンド
スイッチの DHCP スヌーピング統計情報を表示します。	**show dhcp-snooping statistics**

次に、スイッチの DHCP スヌーピング統計情報を表示する例を示します。

```
Console# show dhcp-snooping statistics
Packets forwarded                             =          125
Packets dropped                               =          3
Packets dropped from untrusted ports          =          0
Number of bindings entries                    =          5
Console#
```

作業	コマンド
スイッチの DHCP スヌーピング ポート設定を表示します。	**show port dhcp-snooping**

次に、スイッチの DHCP スヌーピング ポート設定を表示する例を示します。

```
Console# show port dhcp-snooping
Port     Trust
-----  -----------
 3/1   untrusted
 3/2   trusted
 3/3   untrusted
 3/4   trusted
 3/5   trusted
 3/6   untrusted
 3/7   untrusted
 3/8   untrusted
(テキスト出力は省略)
 3/31  untrusted
 3/32  untrusted
 3/33  untrusted
 3/34  untrusted
 3/35  untrusted
 3/36  untrusted
 3/37  untrusted
 3/38  untrusted
 3/39  untrusted
 3/40  untrusted
 3/41  trusted
 3/42  trusted
 3/43  trusted
 3/44  untrusted
 3/45  untrusted
 3/46  untrusted
 3/47  untrusted
 3/48  untrusted
Console>
```

フラッシュ デバイスへの DHCP スヌーピング バインディング エントリの保存

DHCP スヌーピング バインディング エントリは、フラッシュ デバイスに保存できるため、スイッチの再設定後すぐにバインディングを復元できます。

auto-save *interval* オプションは、DHCP スヌーピング バインディングの自動保存インターバルの設定用です。インターバルの有効範囲は、1 ～ 35000（分）です。0 を指定すると、フラッシュ デバイスへのバインディングの定期的保存がディセーブルとなり、フラッシュに保存されているバインディング ファイルが削除されます。0 を指定しても、ユーザが指定したファイル名は消去されません。ユーザが指定したファイル名は、**clear config all** コマンドを入力すると、消去され、デフォルトのファイル名に戻ります。

device:filename オプションは、バインディングを保存するフラッシュ デバイスおよびファイル名の指定用です。デフォルトでは、フラッシュ デバイスは bootflash で、デフォルト ファイル名は、[dhcp-snooping-bindings-database] です。ファイル名が設定されていない場合、バインディングはフラッシュ デバイスにデフォルト ファイル名で自動的に保存されます。

DHCP スヌーピング バインディング エントリの **auto-save** オプションをイネーブルにして、バインディングを定期的に保存するインターバルを指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
DHCP スヌーピング バインディング エントリの **auto-save** オプションをイネーブルにして、バインディングを定期的に保存するインターバルを指定します。	**set dhcp-snooping bindings-database auto-save** *interval*

次に、DHCP スヌーピング バインディング エントリの **auto-save** オプションをイネーブルにして、バインディングを定期的に保存するインターバルを 600 分に指定する例を示します。

```
Console> (enable) set dhcp-snooping bindings-database auto-save 600
DHCP Snooping auto-save interval set to 600 minutes.
Console> (enable)
```

バインディング保存用のフラッシュ デバイスおよびファイル名を指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
バインディング保存用のフラッシュ デバイスおよびファイル名を指定します。	**set dhcp-snooping bindings-database** *device:*[*filename*]

次に、バインディング保存用のフラッシュ デバイスおよびファイル名を設定する例を示します。

```
Console> (enable) set dhcp-snooping bindings-database disk1:dhcp-bindings
DHCP Snooping bindings storage file set to disk1:dhcp-bindings.
Console> (enable)
```

次に、DHCP スヌーピング バインディング データベースの設定を表示する例を示します。

```
Console> (enable) show dhcp-snooping config
DHCP Snooping MAC address matching is enabled.
DHCP Snooping host-tracking information option is disabled.
Remote ID used in information option is 00-01-64-41-60-ff.
DHCP Snooping auto save interval is 600.
DHCP Snooping bindings storage file is disk1:dhcp-bindings.
Console> (enable)
```

IP ソース ガードの機能概要

IP ソース ガードは、特定のポートの DHCP スヌーピングを介して取得した IP アドレスのみを許可することで、IP スプーフィングを回避します。最初に、DHCP スヌーピングでキャプチャされた DHCP パケットを除く、ポート上のすべての IP トラフィックがブロックされます。クライアントが DHCP サーバから有効な IP アドレスを受信する場合、Port Access Control List（PACL; ポートアクセス制御リスト）がその IP アドレスからのトラフィックを許可するポートにインストールされます。このプロセスでは、クライアント IP トラフィックを、DHCP サーバから取得した送信元 IP アドレスに制限します。PACL 許可リストにない送信元 IP アドレスを持つ IP トラフィックはフィルタリングで除外されます。このフィルタリングによって、隣接ホストの IP アドレスを要求することによるホストのネットワーク攻撃能力を制限できます。

（注）　DHCP スヌーピングをイネーブルにしている VLAN が大量にあるトランク ポートで、IP ソース ガードをイネーブルにする場合、ACL ハードウェア リソースが不足し、そのポートに接続しているクライアントがトラフィックを送信できなくなる可能性があります。ポートごとに 10 個の IP アドレスに制限されているため、このような設定は推奨しません。

IP ソース ガードは、送信元 IP アドレス フィルタリングを使用します。これは、その送信元 IP アドレスに基づいた IP トラフィックをフィルタリングするものです。IP 送信元バインディング エントリと一致する送信元 IP アドレスがある IP トラフィックのみが許可されます。

ポートの新しい DHCP スヌーピング バンディング エントリが作成されたり削除されたりする際に、ポートの IP 送信元アドレス フィルタが変更されます。IP 送信元バインディングの変更を反映させるために、ポート PACL がハードウェアで変更されて再び適用されます。デフォルトで、ポートで DHCP スヌーピング バインディングなしで IP ソース ガードをイネーブルにする場合、すべての IP トラフィックを拒否するデフォルトの PACL がポートにインストールされます。IP ソース ガードをディセーブルにする場合、IP 送信元フィルタ PACL がポートから削除されます。

IP ソース ガードの設定時の注意事項

ここでは、ネットワークで IP ソース ガードを設定する際の注意事項について説明します。

- IP ソース ガードは、PFC3 およびこれ以降のバージョンでサポートされます。
- ポートごとに 10 個の IP アドレスに制限されています。
- IP ソース ガードはトランク ポートでは推奨しません。
- IP ソース ガードは、PACL と共存できません。
- IP ソース ガードは、EtherChannel 対応ポートでサポートされていません。また EtherChannel は IP ソース ガード対応ポートではサポートされていません。
- IP ソース ガードをイネーブルにすると、スタティック ARP 検査などの VLAN ベースの ACL 機能はディセーブルになります。
- DAI、DHCP スヌーピング、および IP ソース ガードを使用する場合、ハイ アベイラビリティをイネーブルにすることを推奨します。ハイ アベイラビリティがイネーブルでない場合、スイッチオーバー後にこれらの機能が動作するようにクライアントは IP アドレスを更新する必要があります。設定の詳細については、「ダイナミック ARP 検査」（p.15-40）を参照してください。

ポートでの IP ソース ガードのイネーブル化

IP ソース ガードをイネーブルにするには、次の作業を行います。

	作業	コマンド
ステップ 1	ポートをポート ベースに設定します。	**set port security-acl 3/1 port-based**
ステップ 2	IP ソース ガードをイネーブルにします。	**set port dhcp-snooping 3/1 source-guard enable**
ステップ 3	DHCP スヌーピングをイネーブルにします。	**set security acl ip dhcpsnoop permit dhcp-snooping**
ステップ 4	ポートで他のトラフィックの転送を許可します。	**set security acl ip dhcpsnoop permit ip any any**
ステップ 5	ACL 設定を保存します。	**commit security acl dhcpsnoop**
ステップ 6	VLAN で ACL をイネーブルにします。	**set security acl map dhcpsnoop 10**
ステップ 7	ポートでの DHCP スヌーピングの信頼をイネーブルにします。	**set port dhcp-snooping 1/2 trust enable**

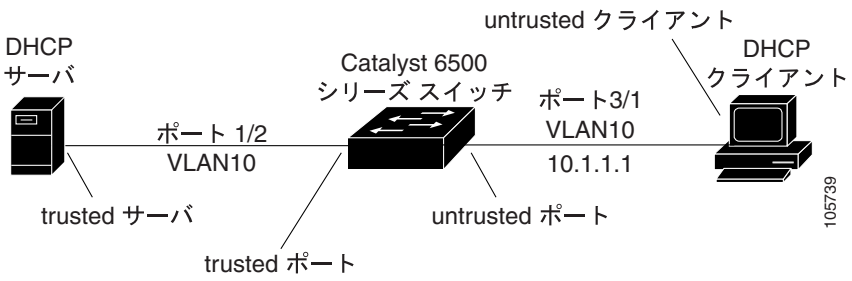
(注)　IP ソース ガードをイネーブルにする前に、ポートが属する VLAN の DHCP スヌーピングをイネーブルにする必要があります。ポートをセキュリティ ACL のポート ベースまたはマージ モードに設定する必要があります。DHCP スヌーピング untrusted ポートでのみ IP ソース ガードをイネーブルにします。

次に、IP ソース ガードをイネーブルにする例を示します。

```
Console> (enable) set port security-acl 3/1 port-based
Warning:Vlan-based ACL features will be disabled on port 3/1.
ACL interface is set to port-based mode for port(s) 3/1.
Console> (enable) set port dhcp-snooping 3/1 source-guard enable
IP Source Guard enabled on port(s)  3/1.

Console> (enable) set port dhcp-snooping 1/2 trust enable
Port(s)  1/2 state set to trusted for DHCP Snooping.
Console> (enable) set security acl ip dhcpsnoop permit dhcp-snooping
Successfully configured DHCP Snooping for ACL dhcpsnoop. Use 'commit' command to
 save changes.

Console> (enable) set security acl ip dhcpsnoop permit ip any any
dhcpsnoop editbuffer modified. Use 'commit' command to apply changes.
Console> (enable) commit security acl dhcpsnoop
ACL commit in progress.

ACL 'dhcpsnoop' successfully committed.
Console> (enable) set security acl map dhcpsnoop 10
Mapping in progress.

ACL dhcpsnoop successfully mapped to VLAN 10.
Console>
```

図 32-3 に、untrusted ポートで IP ソース ガードを設定する場合の一般的なトポロジーを示します。

図 32-3　untrusted ポートでイネーブルな IP ソース ガード



IP ソース ガード情報の表示

show port dhcp-snooping コマンドを使用して、スイッチ上のすべてのポートの IP ソース ガード情報を表示できます。モジュールで IP ソース ガードの情報を表示するには、次の作業を行います。

作業	コマンド
ポートで IP ソース ガードに関する情報を表示します。	**show port dhcp-snooping 4**

次に、ポートで IP ソース ガードの設定を表示する例を示します。

```
Console> (enable) show port dhcp-snooping 3/25
Port     Trust     Source-Guard    Source-Guarded IP Addresses
-----  ----------  ------------    ---------------------------
 3/25  untrusted      enabled      192.168.80.6, 192.168.80.5,
                                   192.168.80.4, 192.168.80.3,
                                   192.168.80.2, 192.168.80.1

Console> (enable)
```

CHAPTER 33

NTP の設定

この章では、Catalyst 6500 シリーズ スイッチ上で Network Time Protocol（NTP）を設定する方法について説明します。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

この章で説明する内容は、次のとおりです。

NTP の機能

NTP は、一連の分散タイム サーバおよびクライアント間でネットワーク時刻を同期化するプロトコルです。同期化により、システム ログ作成時または時間が重要であるイベントの発生時に、各イベントを関連付けることができます。

NTP サーバは、クライアント スイッチからアクセスできなければなりません。NTP は UDP 上で、UDP は IP 上で実行されます。NTP は RFC 1305 で規定されています。NTP 通信はすべて、GMT（グリニッジ標準時）と同じである Coordinated Universal Time（UTC; 協定世界時）を使用します。NTP ネットワークは通常、タイム サーバに接続されたラジオ クロックまたは原子時計などの確実な時刻ソースから時刻を入手します。この時刻が、NTP によりネットワーク上に配信されます。NTP はきわめて効率的で、1 分間に 1 パケットを使用するだけで、2 台の装置を 1 ミリ秒以内に同期化することができます。

NTP では、ストラタム（階層）を使用して、装置と正規時刻ソースとの間にある NTP ホップ数を識別します。ストラタム 1 は、ラジオ クロックまたは原子時計が直接接続されたタイム サーバです。ストラタム 2 のタイム サーバは、ストラタム 1 のタイム サーバから NTP により時刻を受信します。同様に、以降のストラタムも時刻を受信します。NTP を実行している装置は、NTP 通信用のストラタム番号が最小の装置を時刻ソースとして自動的に選択します。この手法により、NTP スピーカの自動編成型ツリーが適切に構築されます。

NTP では、2 つの方法により、時刻が正確でない装置との同期化が防止されます。

- 同期化されていないソース装置との同期化は実行されません。
- 複数の装置から報告された時刻が比較され、時刻が他の装置と著しく異なる装置との同期化は、たとえそのストラタム番号が小さくても実行されません。

NTP を実行している装置間の「アソシエーション」と呼ばれる通信は、通常、スタティックに設定されます。各装置に、すべての装置とのアソシエーションに使用する IP アドレスを設定します。アソシエーションのペアとなる装置間で NTP メッセージを交換することにより、正確な時刻が維持されます。ただし、LAN 環境では、NTP に IP ブロードキャスト メッセージを使用できます。この場合には、ブロードキャスト メッセージを送信または受信する装置を設定します。ただし、情報の流れが一方向に限られるので時刻管理の正確性は多少損なわれます。

シスコの NTP はストラタム 1 サービスをサポートしていないので、ラジオ クロックまたは原子時計に接続できません。ネットワークの時刻サービスは、IP インターネット上のパブリック NTP サーバから取得することを推奨します。インターネットから分離されたネットワークでは、シスコの NTP サポートにより、実際には別の手段で時刻を入手しているにもかかわらず、NTP を使用して同期をとっているかのような装置設定にすることができます。他の装置は、NTP によりこの装置と同期化されます。

ほとんどのホスト システムには NTP ソフトウェアが組み込まれており、UNIX システムなどでは市販のバージョンを入手できます。このソフトウェアにより、ホスト システムの時刻を同期化できます。

NTP のデフォルト設定

表 33-1 に、NTP のデフォルト設定を示します。

表 33-1　NTP のデフォルト設定

機能	デフォルト値
ブロードキャスト クライアント モード	ディセーブル
クライアント モード	ディセーブル
ブロードキャスト遅延	3000 マイクロ秒
タイム ゾーン	指定なし
UTC オフセット	0 時間
サマータイム調整	ディセーブル
NTP サーバ	指定なし
認証モード	ディセーブル

スイッチ上での NTP の設定

ここでは、NTP を設定する手順について説明します。

ブロードキャスト クライアント モードの NTP のイネーブル化

ルータなどの NTP ブロードキャスト サーバから、ネットワーク上の装置に時刻情報を定期的にブロードキャストする場合は、スイッチに NTP ブロードキャスト クライアント モードを設定します。サーバからクライアントへのパケット遅延を補正するには、NTP ブロードキャスト遅延（スイッチによるブロードキャスト パケット受信時の時刻調整係数）を指定します。

スイッチ上で NTP ブロードキャスト クライアント モードを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	NTP ブロードキャスト クライアント モードをイネーブルにします。	**set ntp broadcastclient enable**
ステップ 2	（任意）NTP ブロードキャスト パケット遅延の推定値を設定します。	**set ntp broadcast delay** *microseconds*
ステップ 3	NTP の設定を確認します。	**show ntp** [**noalias**]

次に、スイッチ上で NTP ブロードキャスト クライアント モードをイネーブルにして、ブロードキャスト遅延を 4000 マイクロ秒に設定し、設定を確認する例を示します。

```
Console> (enable) set ntp broadcastclient enable
NTP Broadcast Client mode enabled
Console> (enable) set ntp broadcastdelay 4000
NTP Broadcast delay set to 4000 microseconds
Console> (enable) show ntp

Current time: Tue Jun 23 1998, 20:25:43
Timezone: '', offset from UTC is 0 hours
Summertime: '', disabled
Last NTP update:
Broadcast client mode: enabled
Broadcast delay: 4000 microseconds
Client mode: disabled

NTP-Server
---------------------------------------
Console> (enable)
```

NTP クライアント モードの設定

クライアント スイッチから NTP サーバに対して定期的に時刻要求を送信する場合は、スイッチに NTP クライアント モードを設定します。1 台のクライアントに、最大 10 までのサーバ アドレスを設定できます。

スイッチに NTP クライアント モードを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	NTP サーバの IP アドレスを設定します。	**set ntp server** *ip_addr*
ステップ 2	NTP クライアント モードをイネーブルにします。	**set ntp client enable**
ステップ 3	NTP の設定を確認します。	**show ntp** [**noalias**]

次に、NTP サーバ アドレスを設定し、スイッチ上で NTP クライアント モードをイネーブルにし、設定を確認する例を示します。

```
Console> (enable) set ntp server 172.20.52.65
NTP server 172.20.52.65 added.
Console> (enable) set ntp client enable
NTP Client mode enabled
Console> (enable) show ntp

Current time: Tue Jun 23 1998, 20:29:25
Timezone: '', offset from UTC is 0 hours
Summertime: '', disabled
Last NTP update: Tue Jun 23 1998, 20:29:07
Broadcast client mode: disabled
Broadcast delay: 3000 microseconds
Client mode: enabled

NTP-Server
---------------------------------------
172.16.52.65
Console> (enable)
```

クライアント モードの認証の設定

認証により、NTP が稼働しているシステムのセキュリティを強化できます。認証をイネーブルにすると、クライアント スイッチは信頼できる NTP サーバだけに時刻要求を送ります。認証については、RFC 1305 に記述されています。

1 台のクライアントに、最大 10 個の認証鍵を設定できます。1 つの認証鍵は、実際には次の 2 つの鍵がペアになっています。

- 公開鍵番号 ― 1 ～ 4294967295 の 32 ビット整数
- 秘密鍵の文字列 ― 32 文字からなる任意の文字列（出力可能なすべての文字およびスペースを使用可能）

メッセージを認証するには、クライアントの認証鍵とサーバの認証鍵が一致しなければなりません。認証鍵を安全な方法で事前に配布しておく必要があります（クライアントの管理者は、サーバの管理者から鍵のペアを取得して、クライアントに設定する必要があります）。

認証を設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	NTP 用の認証鍵のペアを設定し、その鍵が信頼できるかどうかを指定します。	**set ntp key** *public_key* [*trusted* | *untrusted*] **md5** *secret_key*
ステップ 2	NTP サーバの IP アドレスおよび公開鍵を指定します。	**set ntp server** *ip_addr* [key *public_key*]
ステップ 3	NTP クライアント モードをイネーブルにします。	**set ntp client enable**
ステップ 4	NTP 認証をイネーブルにします。	**set ntp authentication enable**
ステップ 5	NTP の設定を確認します。	**show ntp** [**noalias**]

次に、NTP サーバ アドレスを設定し、スイッチ上で NTP クライアント モードおよび認証モードをイネーブルにし、設定を確認する例を示します。

```
Console> (enable) set ntp server 172.20.52.65 key 879
NTP server 172.20.52.65 with key 879 added.
Console> (enable) set ntp client enable
NTP Client mode enabled
Console> (enable) set ntp authentication enable
NTP authentication feature enabled
Console> (enable) show ntp

Current time: Tue Jun 23 1998, 20:29:25
Timezone: '', offset from UTC is 0 hours
Summertime: '', disabled
Last NTP update: Tue Jun 23 1998, 20:29:07
Broadcast client mode: disabled
Broadcast delay: 3000 microseconds
Client mode: enabled
Authentication: enabled

NTP-Server                                Server Key
----------------------------------------- ----------
172.16.52.65

Key Number  Mode       Key String
----------  ---------  --------------------------------

Console> (enable)
```

タイム ゾーンの設定

スイッチにタイム ゾーンを指定し、そのタイム ゾーンの時刻を表示することができます。タイム ゾーンを設定する前に、NTP をイネーブルにしておく必要があります。NTP がディセーブルの場合、このコマンドは無効です。NTP をイネーブルにし、タイム ゾーンを指定しないと、デフォルトの UTC が使用されます。

タイム ゾーンを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	タイム ゾーンを設定します。	**set timezone** *zone hours* [*minutes*]
ステップ 2	タイム ゾーンの設定を確認します。	**show timezone**

次に、スイッチ上でタイム ゾーンを設定する例を示します。

```
Console> (enable) set timezone Pacific -8
Timezone set to 'Pacific', offset from UTC is -8 hours
Console> (enable)
```

サマータイム調整のイネーブル化

米国の標準に従う場合、スイッチの時計を、4 月の第 1 日曜日の午前 2 時に 1 時間進め、10 月の最終日曜日の午前 2 時をもって元に戻し、サマータイムに適応させることができます。開始日時と終了日時、時刻調整を毎年繰り返すかどうかを明示的に指定することもできます。

米国の標準に従ってサマータイムの時刻調整をイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	サマータイム調整をイネーブルにします。	**set summertime enable** [*zone_name*] **set summertime recurring**
ステップ 2	設定を確認します。	**show summertime**

次に、米国の標準に従って、太平洋夏時間に合わせて時刻を設定する例を示します。

```
Console> (enable) set summertime enable PDT
Console> (enable) set summertime recurring
Summertime is enabled and set to 'PDT'
Console> (enable)
```

米国の標準とは別の日時で、または米国の標準とは異なる設定で、サマータイム時刻調整が毎年行われるようにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	サマータイム調整をイネーブルにします。	**set summertime recurring** *week day month hh:mm week day month hh:mm offset*
ステップ 2	設定を確認します。	**show summertime**

次に、サマータイム調整が毎年、2 月の第 3 月曜日の午前 3 時に開始され、8 月の第 2 土曜日の午後 3 時に終了し、2 月に 30 分進み、8 月に元に戻るように設定する例を示します。

```
Console> (enable) set summertime recurring 3 mon feb 3:00 2 saturday aug 15:00 30
Summer time is disabled and set to ''
    start: Sun Feb 13 2000, 03:00:00
    end: Sat Aug 26 2000, 14:00:00
    Offset: 30 minutes
    Recurring: yes, starting at 3:00am Sunday of the third week of February and ending
    14:00pm Saturday of the fourth week of August.
Console> (enable)
```

毎年繰り返すのではなく、一度だけ特定の日にサマータイム調整が行われるようにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	サマータイム調整をイネーブルにします。	**set summertime date** *month date year hh:mm month date year hh:mm offset*
ステップ 2	設定を確認します。	**show summertime**

次に、毎年ではなく、2000 年 4 月 13 日 4 時 30 分に、1440 分（1 日）サマータイム調整が開始され、2002 年 1 月 21 日午前 5 時 30 分に終了するように設定する例を示します。

```
Console> (enable) set summertime date apr 13 2000 4:30 jan 21 2002 5:30 1440
Summertime is disabled and set to ''
Start : Thu Apr 13 2000, 04:30:00
End   : Mon Jan 21 2002, 05:30:00
Offset: 1440 minutes (1 day)
Recurring: no
Console> (enable)
```

サマータイム調整のディセーブル化

サマータイム調整をディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	サマータイム調整をディセーブルにします。	**set summertime disable** [*zone_name*]
ステップ 2	設定を確認します。	**show summertime**

次に、サマータイム調整をディセーブルにする例を示します。

```
Console> (enable) set summertime disable Arizona
Summertime is disabled and set to 'Arizona'
Console> (enable)
```

タイム ゾーンの消去

タイム ゾーンの設定を消去し、デフォルトの UTC に戻すには、イネーブル モードで次の作業を行います。

作業	コマンド
タイム ゾーンの設定を消去します。	**clear timezone**

次に、タイム ゾーンの設定を消去する例を示します。

```
Console> (enable) clear timezone
Timezone name and offset cleared
Console> (enable)
```

NTP サーバの消去

スイッチの NTP サーバ テーブルから NTP サーバ アドレスを消去するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	消去する NTP サーバを指定します。	**clear ntp server** [*ip_addr* | **all**]
ステップ 2	NTP の設定を確認します。	**show ntp** [**noalias**]

次に、NTP サーバ テーブルから NTP サーバ アドレスを消去する例を示します。

```
Console> (enable) clear ntp server 172.16.64.10
NTP server 172.16.64.10 removed.
Console> (enable)
```

NTP のディセーブル化

スイッチの NTP ブロードキャスト クライアント モードをディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	NTP ブロードキャスト クライアント モードをディセーブルにします。	**set ntp broadcastclient disable**
ステップ 2	NTP の設定を確認します。	**show ntp** [**noalias**]

次に、スイッチ上で NTP ブロードキャスト クライアント モードをディセーブルにする例を示します。

```
Console> (enable) set ntp broadcastclient disable
NTP Broadcast Client mode disabled
Console> (enable)
```

スイッチ上で NTP クライアント モードをディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	NTP クライアント モードをディセーブルにします。	**set ntp client disable**
ステップ 2	NTP の設定を確認します。	**show ntp** [**noalias**]

次に、スイッチ上で NTP クライアント モードをディセーブルにする例を示します。

```
Console> (enable) set ntp client disable
NTP Client mode disabled
Console> (enable)
```

CHAPTER 34

ブロードキャスト抑制の設定

この章では、Catalyst 6500 シリーズ スイッチ上でブロードキャスト抑制を設定する方法について説明します。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

この章で説明する内容は、次のとおりです。

ブロードキャスト抑制の機能

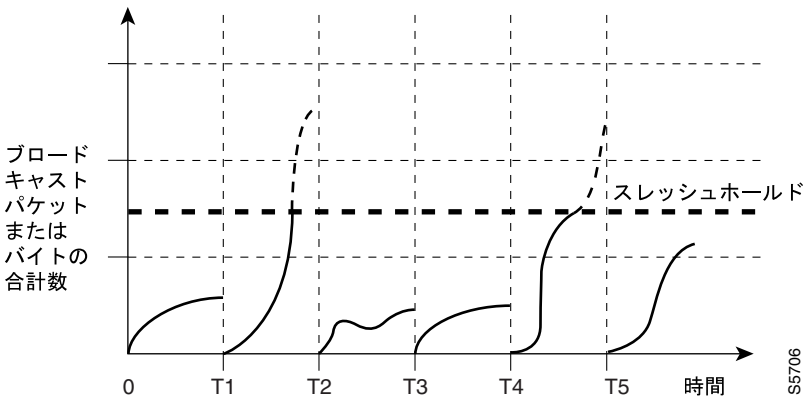
(注)　ブロードキャスト抑制およびマルチキャスト抑制は、WS-X6148A-GE-TX、WS-X6148A-GE-45A、および WS-X6548-GE-TX モジュール上でサポートされません。

ブロードキャスト抑制により、1 つのポート上でのブロードキャスト ストームによる LAN 上のスイッチド ポートの混乱を防ぐことができます。LAN ブロードキャスト ストームは、LAN 上でブロードキャストまたはマルチキャスト パケットのフラッディングが生じ、トラフィック過剰となって、ネットワークのパフォーマンスが低下した場合に発生します。また、プロトコル スタックまたはネットワーク設定のエラーも、ブロードキャスト ストームの原因になります。

ブロードキャスト抑制ではフィルタリングを使用して、LAN 上のブロードキャスト アクティビティを 1 秒間測定し、あらかじめ設定されたスレッシュホールドと測定値を比較します。スレッシュホールドに達している場合、次のブロードキャスト アクティビティを指定された時間だけ抑制します。ブロードキャスト抑制は、ディセーブルがデフォルトの設定です。

図 34-1 に、一定時間におけるポート上のブロードキャスト トラフィック パターンを示します。この例では、T1 ～ T2 間および T4 ～ T5 間において、ブロードキャスト抑制が機能しています。これらの間では、ブロードキャスト トラフィック量が、設定されたスレッシュホールドを超えているためです。

図 34-1　ブロードキャスト抑制



ブロードキャスト抑制スレッシュホールド値と時間の長さによって、さまざまなレベルの粒度でブロードキャスト抑制アルゴリズムが機能します。スレッシュホールドを上げるほど、多くのブロードキャスト パケットが通過します。

Catalyst 6500 シリーズ スイッチのブロードキャスト抑制は、ハードウェアで実行されます。スイッチの抑制回路がポートからスイッチング バスへ流れるパケットをモニタします。パケット宛先アドレスにある個別の、またはグループのビットにより、ブロードキャスト抑制回路はパケットのユニキャストまたはブロードキャストを判断します。1 秒単位でそのときのブロードキャスト カウントを追跡し、スレッシュホールドに達した場合は、以後のブロードキャスト パケットを排除します。

ハードウェアによるブロードキャスト抑制では帯域幅ベースの方式でブロードキャスト アクティビティを測定するため、実装で最も重要な要素は、ブロードキャスト トラフィックが使用できる全帯域幅の割合です。スレッシュホールド値を 100% にすると、ブロードキャスト トラフィックに関する制限はなくなります。**set port broadcast** コマンドを使用すると、ブロードキャスト抑制スレッシュホールド値を設定できます。

パケットは均一なインターバルで着信するわけではないので、ブロードキャスト アクティビティが測定される 1 秒間のインターバルがブロードキャストの抑制動作に影響を与える可能性があります。

ギガビット イーサネット ポートでは、ブロードキャスト抑制を使用してマルチキャストおよびユニキャスト トラフィックにフィルタをかけることができます。ポートでマルチキャストまたはユニキャスト トラフィックを個別に抑制できます。いずれの場合も、ブロードキャスト抑制を設定する必要があります。マルチキャストまたはユニキャスト トラフィックに使用する全帯域幅の割合を指定すると、同じ制限がブロードキャスト トラフィックにも適用されます。

（注） ブロードキャスト、マルチキャスト、またはユニキャストの抑制が行われた場合に、ポートが *errdisable* ステートになるように設定できます。詳細については、「errdisable ステートのイネーブル化」（p.34-5）を参照してください。

（注） マルチキャスト抑制では、Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）パケットは廃棄されません。

（注） マルチキャスト抑制が次のモジュール（WS-X6724-SFP、WS-X6748-GE-TX、WS-X6748-SFP、WS-X6704-10GE、WS-SUP32-GE-3B、および WS-SUP32-10GE-3B）上でイネーブルの場合、BPDU の受信は保証されません。これらのモジュール上でマルチキャスト抑制をイネーブルにすると、マルチキャスト抑制のスレッシュホールドを超過した場合に BPDU が抑制される原因となります。抑制スレッシュホールドを超過した場合、副次的にルート ポート損失またはスパニング ツリー ループが発生する可能性があるため、BPDU を受信する必要があるポートではマルチキャスト抑制を使用しないよう強く推奨します。

スイッチ上でのブロードキャスト抑制の設定

ここでは、Catalyst 6500 シリーズ スイッチ上でブロードキャスト抑制を設定する手順について説明します。

ブロードキャスト抑制のイネーブル化

1 つまたは複数のポートでブロードキャスト抑制をイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	1 つまたは複数のポートのブロードキャスト抑制スレッシュホールドを、全帯域幅の割合を指定してイネーブルにします。	**set port broadcast** *mod/port threshold***%** [**violation** {**drop-packets** | **errdisable**}] [**multicast** {**enable** | **disable**}] [**unicast** {**enable** | **disable**}]
ステップ 2	ブロードキャスト抑制の設定を確認します。	**show port broadcast** [*mod*[/*port*]]

（注） ブロードキャスト抑制のスレッシュホールドは、0.01% まで指定できますが、すべてのモジュールがその細かさで調整されるわけではありません。スレッシュホールドは通常、0.01 ～ 0.05% 程度の変動があります。スレッシュホールド値を細かく指定すると、スレッシュホールドの割合は可能なかぎり細密に調整されます。

次に、帯域幅ベースのブロードキャスト抑制をイネーブルにし、設定を確認する例を示します。

```
Console> (enable) set port broadcast 3/1-6 75.25%
Ports 3/1-6 broadcast traffic limited to 75.25%.
On broadcast suppression ports 3/1-6 are configured to drop-packets.
Console> (enable) show port broadcast 3

Port     Broadcast-Limit Multicast Unicast Total-Drop           Action
-------- --------------- --------- ------- -------------------- ------------
 3/1             75.25 %         -       -                    0 drop-packets
 3/2             75.25 %         -       -                    0 drop-packets
 3/3             75.25 %         -       -                    2 drop-packets
 3/4             75.25 %         -       -                    0 drop-packets
 3/5             75.25 %         -       -                    0 drop-packets
 3/6             75.25 %         -       -                    0 drop-packets
 3/7                   -         -       -                    0 drop-packets
 3/8                   -         -       -                    0 drop-packets
.
.<snip>
.
Console> (enable)
```

次に、モジュール 2 のポート 1 に対してマルチキャストおよびブロードキャスト トラフィックを 80% に制限し、その設定を確認する例を示します。

```
Console> (enable) set port broadcast 2/1 80% multicast enable
Port 2/1 broadcast and multicast traffic limited to 80.00%.
On broadcast suppression port 2/1 is configured to drop-packets.
Console> (enable) show port broadcast 2/1

Port     Broadcast-Limit Multicast Unicast Total-Drop           Action
-------- --------------- --------- ------- -------------------- ------------
 2/1             80.00 %   80.00 %       -                    0 drop-packets
Console> (enable)
```

ブロードキャスト抑制のディセーブル化

1 つまたは複数のポート上でブロードキャスト抑制をディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
1 つまたは複数のポート上で、ブロードキャスト抑制をディセーブルにします。	**clear port broadcast** *mod/port*

次に、1 つまたは複数のポート上でブロードキャスト抑制をディセーブルにする例を示します。

```
Console> (enable) clear port broadcast 2/1
Port 2/1 traffic unlimited.
Console> (enable)
```

errdisable ステートのイネーブル化

(注) ポートが NVRAM（不揮発性 RAM）ではイネーブルに設定されていても、実行時に何らかのプロセスによってディセーブルにされた場合、そのポートは errdisable ステートになります。たとえば、UniDirectional Link Detection（UDLD; 単一方向リンク検出）が単一方向リンクを検出すると、ポートは実行時にシャットダウンされます。ただし、そのポートの NVRAM 設定はイネーブルに設定されている（ユーザがポートをディセーブルにしていない）ので、ポートのステータスは errdisable として表示されます。

ブロードキャスト、マルチキャスト、またはユニキャストの抑制が行われた場合に、ポートにパケットを廃棄させるか、またはポートを errdisable ステートにするのかを設定できます。errdisable ステート機能は、ポート単位でイネーブルまたはディセーブルに設定できます。デフォルトではこの機能はディセーブルになります（デフォルトでは **drop-packets** オプションがイネーブルになります）。

(注) ブロードキャスト、マルチキャスト、またはユニキャストの抑制が行われて、ポートに errdisable 機能が設定されている場合、そのポートがパケットの廃棄を停止し、errdisable ステートになるまでに遅延時間が生じます。この遅延時間はスイッチによって異なる可能性があり、正確な遅延時間を判断することはできません。

1 つのポート上で errdisable ステート機能をイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	errdisable ステートをイネーブルにします。	**set port broadcast** *mod/port threshold***%** [**violation** {**drop-packets** | **errdisable**}] [**multicast** {**enable** | **disable**}] [**unicast** {**enable** | **disable**}]
ステップ 2	errdisable ステートがイネーブルに設定されたことを確認します。	**show port broadcast** [*mod*[/*port*]]

次に、ブロードキャスト トラフィックを 90% に制限し、ブロードキャスト抑制発生時にポートを errdisable ステートにする設定例を示します。

```
Console> (enable) set port broadcast 4/6 90% violation errdisable
Port 4/6 broadcast traffic limited to 90.00%.
On broadcast suppression port 4/6 is configured to move to errdisabled state.
Console> (enable)
```

（注） ブロードキャスト抑制に対する errdisable タイムアウト機能をイネーブルにするには、**set errdisable-timeout enable bcast-suppression** コマンドを入力します。

この機能によって、ポートが errdisable ステートになったあと、指定のタイムアウト時間が経過するとポートがイネーブルに戻るように設定できます。タイムアウト時間を指定するには、**set errdisable-timeout interval** コマンドを入力します。

errdisable ステートになったポートを一定期間後にイネーブルにするのか、または errdisable ステートのままにしておくのかをポート単位で制御するには、**set port errdisable-timeout** コマンドを入力します。

詳細については、「ポートの errdisable ステートにおけるタイムアウト設定」（p.4-13）を参照してください。

CHAPTER 35

レイヤ 3 プロトコル フィルタリングの設定

この章では、Catalyst 6500 シリーズ スイッチのイーサネット、ファスト イーサネット、およびギガビット イーサネット ポート上で、レイヤ 3 プロトコル フィルタリングを設定する手順について説明します。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

この章で説明する内容は、次のとおりです。

レイヤ 3 プロトコル フィルタリングの機能

レイヤ 3 プロトコル フィルタリングにより、スイッチ ポート上で特定プロトコルのトラフィック転送を禁止できます。レイヤ 3 プロトコル フィルタリングは、スーパバイザ エンジン上で実行されます。Policy Feature Card（PFC; ポリシー フィーチャ カード）または Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）が搭載されている必要はありません。ブロードキャストおよびユニキャスト フラッディング トラフィックは、異なるプロトコル グループ間でのポートのメンバーシップに基づいてフィルタリングされます。このフィルタリングは、ポート VLAN（仮想 LAN）メンバーシップによるフィルタリングに追加されます。レイヤ 3 プロトコル フィルタリングは、非トランクのイーサネット ポート、ファスト イーサネット ポート、およびギガビット イーサネット ポート上でのみサポートされています。

トランキング ポートは常に、すべてのプロトコル グループのメンバーになります。他のネットワーキング装置との互換性の問題を避けるため、レイヤ 3 プロトコル フィルタリングはトランク ポート上では実行されません。Spanning-Tree Protocol（STP; スパニングツリー プロトコル）、Cisco Discovery Protocol（CDP）などのレイヤ 2 プロトコルは、レイヤ 3 プロトコル フィルタリングの影響を受けません。ダイナミック ポートおよびポート セキュリティがイネーブルになっているポートは、すべてのプロトコル グループのメンバーになります。

各プロトコル グループについて、**on**、**off**、**auto** のいずれかのモードでポートを設定できます。

on に設定した場合、そのプロトコルに対応するすべてのフラッディング トラフィックが受信されます。**off** に設定した場合は、そのプロトコルに対応するフラッディング トラフィックは一切受信されません。

auto に設定した場合、ポートがグループに追加されるのは、指定したプロトコルのパケットがそのポートで受信されたあとです。自動学習機能を使用した場合、ポートがプロトコル グループのメンバーになるのは、そのポートに接続された装置から対応するプロトコルのパケットを受信したあとです。自動設定されたポートは、そのプロトコルに対応するパケットを 60 分以内に受信しなかった場合、プロトコル グループから削除されます。また、スーパバイザ エンジンにより、ポート上のリンク ダウンが検出された場合も、ポートはプロトコル グループから削除されます。

たとえば、IP と Internetwork Packet Exchange（IPX）の両方をサポートするホストをスイッチ ポートに接続し、ポートの IPX 処理を **auto** に設定した場合でも、ホストからの送信が IP トラフィックだけであれば、ホストの接続先ポートからホストに対して IPX フラッディング トラフィックは転送されません。ただし、ホストが IPX パケットを送信すると、スーパバイザ エンジン ソフトウェアによりプロトコル トラフィックが検出され、ポートが IPX グループに追加されるので、ポートは IPX フラッディング トラフィックを受信できるようになります。60 分以上、ホストから IPX トラフィックが送信されない場合、ポートは IPX プロトコル グループから削除されます。

デフォルトでは、ポートは IP プロトコル グループに関して **on** に設定されます。IP に関して **auto** を設定するのは、一般に、ポートに直接接続されたエンド ステーションがある場合だけです。IPX およびグループに関するデフォルト ポート設定は、**auto** です。

レイヤ 3 プロトコル フィルタリングがイネーブルになっている場合、ポートはプロトコルに基づいて識別されます。ポートは、1 つまたは複数のプロトコル グループのメンバーにすることができます。各プロトコル グループのフラッディング トラフィックが転送されるのは、適切なプロトコル グループに属しているポートからだけです。

パケットは次のプロトコル グループに分類されます。

- IP
- IPX
- AppleTalk、DECnet、および Banyan VINES（**group** モード）
- 上記のどのプロトコルにも属さないパケット

レイヤ 3 プロトコル フィルタリングのデフォルト設定

表 35-1 に、レイヤ 3 プロトコル フィルタリングのデフォルト設定を示します。

表 35-1　レイヤ 3 プロトコル フィルタリングのデフォルト設定

機能	デフォルト値
レイヤ 3 プロトコル フィルタリング	ディセーブル
ip モード	**on**
ipx モード	**auto**
group モード	**auto**

スイッチ上でのレイヤ 3 プロトコル フィルタリングの設定

ここでは、イーサネット タイプの VLAN およびすべてのタイプのイーサネット ポート上でレイヤ 3 プロトコル フィルタリングを設定する方法について説明します。

- レイヤ 3 プロトコル フィルタリングのイネーブル化（p.35-3）
- レイヤ 3 プロトコル フィルタリングのディセーブル化（p.35-4）

レイヤ 3 プロトコル フィルタリングのイネーブル化

（注） プロトコル フィルタリングは、イーサネット VLAN および非トランキング EtherChannel ポート上でのみサポートされています。**set protocolfilter** コマンドは、Network Analysis Module（NAM; ネットワーク解析モジュール）、Supervisor Engine 720、または Supervisor Engine 32 でサポートされていません。

イーサネット ポート上でレイヤ 3 プロトコル フィルタリングをイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチ上でレイヤ 3 プロトコル フィルタリングをイネーブルにします。	**set protocolfilter enable**
ステップ 2	該当するポートのプロトコル メンバーシップを設定します。	**set port protocol** *mod/port* {**ip** | **ipx** | **group**} {**on** | **off** | **auto**}
ステップ 3	ポート フィルタリングの設定を確認します。	**show port protocol** [*mod*[*/port*]]

次に、レイヤ 3 プロトコル フィルタリングをイネーブルにし、ポートのプロトコル メンバーシップを設定し、設定を確認する例を示します。

```
Console> (enable) set protocolfilter enable
Protocol filtering enabled on this switch.
Console> (enable) set port protocol 7/1-4 ip on
IP protocol set to on mode on ports 7/1-4.
Console> (enable) set port protocol 7/1-4 ipx off
IPX protocol disabled on ports 7/1-4.
Console> (enable) set port protocol 7/1-4 group auto
Group protocol set to auto mode on ports 7/1-4.
Console> (enable) show port protocol 7/1-4
Port     Vlan       IP       IP Hosts IPX      IPX Hosts Group    Group Hosts
-------- ---------- -------- -------- -------- --------- -------- -----------
7/1      4          on       1        off      0         auto-off 0
7/2      5          on       1        off      0         auto-on  1
7/3      2          on       1        off      0         auto-off 0
7/4      4          on       1        off      0         auto-on  1
Console> (enable)
```

レイヤ 3 プロトコル フィルタリングのディセーブル化

レイヤ 3 プロトコル フィルタリングをディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
スイッチ上でレイヤ 3 プロトコル フィルタリングをディセーブルにします。	**set protocolfilter disable**

次に、レイヤ 3 プロトコル フィルタリングをディセーブルにする例を示します。

```
Console> (enable) set protocolfilter disable

Protocol filtering disabled on this switch.
Console> (enable)
```

CHAPTER 36

IP 許可リストの設定

この章では、Catalyst 6500 シリーズ スイッチ上で IP 許可リストを設定する方法について説明します。

(注) IP 許可リストの機能は、VLAN Access Control List（VACL）を使用して実行することもできます。VACL はハードウェア（Policy Feature Card [PFC; ポリシー フィーチャ カード]）によって処理されるので、VACL のほうが IP 許可リストに比べて、高速に処理されます。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

この章で説明する内容は、次のとおりです。

IP 許可リストの機能

IP 許可リストは、許可されていない送信元 IP アドレスによるスイッチへの着信 Telnet および SNMP（簡易ネットワーク管理プロトコル）アクセスを防止します。他のすべての TCP/IP サービス（IP traceroute、IP ping など）は、IP 許可リストをイネーブルにしても、そのまま正常に動作します。発信 Telnet、Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）、およびその他の IP ベース サービスは、IP 許可リストの影響を受けません。

許可されていない送信元 IP アドレスによる Telnet アクセスでは、接続が拒否されます。許可されていない IP アドレスから SNMP 要求に応答が戻されないと、要求はタイムアウトになります。コンソールまたは Syslog サーバに対する無許可アクセスのロギングを希望する場合は、「IP 許可リストのイネーブル化」（p.36-3）の説明に従って IP のロギング重大度を変更する必要があります。無許可アクセスの試行時に SNMP トラップが生成されるようにするには、「IP 許可リストのイネーブル化」（p.36-3）の説明に従って IP 許可リスト（ippermit）SNMP トラップをイネーブルにする必要があります。同じ無許可ホストから複数のアクセスが試みられた場合は、10 分ごとに通知が生成されるだけです。

許可リストには最大 100 のエントリを設定できます。各エントリには、IP アドレスとサブネット マスクのペアをドット付き 10 進表記で指定するとともに、その IP アドレスを SNMP 許可リスト、Telnet 許可リスト、または両方のリストのどれに入れるかを指定します。マスクで 1 に設定したビットは、着信パケットの送信元 IP アドレスと一致するかどうかがチェックされます。ゼロに設定したビットはチェックされません。このプロセスでワイルドカード アドレスを指定できます。

IP 許可リストのエントリにマスクを指定しなかった場合、または IP アドレスの代わりにホスト名を指定した場合には、そのホストの IP アドレスとだけ一致するように、マスクのすべてのビットが 1 となる（255.255.255.255 または 0xffffffff）暗黙的な値になります。

IP アドレスの許可リストの種類として SNMP または Telnet を指定しない場合、その IP アドレスは、SNMP 許可リストおよび Telnet 許可リストの両方に追加されます。

マスクが異なっていれば、許可リストの複数エントリに同じ IP アドレスを指定できます。アドレスは、マスクが適用されてから NVRAM（不揮発性 RAM）に保存されるので、同じ結果になるアドレスは保存されません。IP 許可リストにこのようなアドレスを追加すると、マスクが適用されたアドレスが表示されます。

IP 許可リストのデフォルト設定

表 36-1 に、IP 許可リストのデフォルト設定を示します。

表 36-1　IP 許可リストのデフォルト設定

機能	デフォルト値
IP 許可リストのイネーブル ステート	ディセーブル
許可リストのエントリ	設定なし
IP Syslog メッセージの重大度	2
SNMP IP 許可トラップ（ippermit）	ディセーブル

スイッチ上での IP 許可リストの設定

ここでは、IP 許可リストを設定する方法について説明します。

IP 許可リストへの IP アドレスの追加

SNMP 許可リスト、Telnet 許可リスト、または両方のリストに特定の IP アドレスを追加できます。

IP 許可リストに IP アドレスを追加するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	IP 許可リストに追加する IP アドレスを指定します。	**set ip permit** *ip_address* [*mask*] [**telnet** | **snmp** | **ssh**]
ステップ 2	IP 許可リストの設定を確認します。	**show ip permit**

次に、IP 許可リストに IP アドレスを追加し、設定を確認する例を示します。

```
Console> (enable) set ip permit 172.16.0.0 255.255.0.0 telnet
172.16.0.0 with mask 255.255.0.0 added to telnet permit list.
Console> (enable) set ip permit 172.20.52.32 255.255.255.224 snmp
172.20.52.32 with mask 255.255.255.224 added to snmp permit list.
Console> (enable) set ip permit 172.20.52.3 all
172.20.52.3 added to IP permit list.
Console> (enable) show ip permit
Telnet permit list feature enabled.
Snmp permit list feature enabled.
Permit List        Mask               Access Type
----------------   ----------------   -------------
172.16.0.0         255.255.0.0        telnet
172.20.52.3                           snmp telnet
172.20.52.32       255.255.255.224    snmp
Denied IP Address   Last Accessed Time Type    Telnet Count   SNMP Count
-----------------   ------------------ ------  ------------   ----------
172.100.101.104     01/20/97,07:45:20  SNMP              14         1430
172.187.206.222     01/21/97,14:23:05  Telnet             7          236

Console> (enable)
```

IP 許可リストのイネーブル化

SNMP 許可リスト、Telnet 許可リスト、または両方のリストをイネーブルに設定できます。許可リストを指定しない場合は、SNMP 許可リストおよび Telnet 許可リストの両方がイネーブルに設定されます。

注意　特に SNMP を使用して設定する場合には、IP 許可リストをイネーブルにする前に、使用するワークステーションまたはネットワーク管理システムの IP アドレスが IP 許可リストに追加されていることを確認してください。IP アドレスが追加されていないと、スイッチにより接続が切断されます。IP 許可リストのエントリまたはホスト アドレスを削除する前に、IP 許可リストをディセーブルにしてください。

スイッチの IP 許可リストをイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	IP 許可リストをイネーブルにします。	**set ip permit enable** [**telnet** | **snmp** | **ssh**]
ステップ 2	必要な場合、IP 許可トラップをイネーブルにし、無許可アクセスの試行についてトラップを生成します。	**set snmp trap enable ippermit**
ステップ 3	必要な場合、無許可アクセスの Syslog メッセージが表示されるよう、ロギング レベルを設定します。	**set logging level ip 4 default**
ステップ 4	IP 許可リストの設定を確認します。	**show ip permit** **show snmp**

次に、IP 許可リストをイネーブルにし、設定を確認する例を示します。

```
Console> (enable) set ip permit enable
IP permit list enabled.
Console> (enable) set snmp trap enable ippermit
SNMP IP Permit traps enabled.
Console> (enable) set logging level ip 4 default
System logging facility <ip> set to severity 4(warnings)
Console> (enable) show ip permit
Telnet permit list feature enabled.
Snmp permit list feature disabled.

Permit List          Mask              Access-Type
---------------     ---------------   ---------------
172.16.0.0         255.255.0.0         telnet
172.20.52.3                            snmp telnet
172.20.52.32       255.255.255.224     snmp

Denied IP Address   Last Accessed Time Type    Telnet Count   SNMP Count
-----------------   ------------------ ------  ------------   ----------
172.100.101.104     01/20/97,07:45:20  SNMP              14         1430
172.187.206.222     01/21/97,14:23:05  Telnet             7          236

Console> (enable) show snmp
RMON:                         Disabled
Extended Rmon:                Extended RMON module is not present
Traps Enabled:
ippermit
Port Traps Enabled: None

Community-Access     Community-String
----------------     --------------------
read-only            public
read-write           private
read-write-all       secret

Trap-Rec-Address                            Trap-Rec-Community
------------------------------------------  --------------------
Console> (enable)
```

IP 許可リストのディセーブル化

スイッチの IP 許可リストをディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチの IP 許可リストをディセーブルにします。	**set ip permit disable** [**telnet** | **snmp** | **ssh**]
ステップ 2	IP 許可リストの設定を確認します。	**show ip permit**

次に、IP 許可リストをディセーブルにする例を示します。

```
Console> (enable) set ip permit disable
IP permit list disabled.
Console> (enable)
```

IP 許可リスト エントリの消去

SNMP 許可リスト、Telnet 許可リスト、または両方のリストから特定の IP アドレスを消去できます。どの許可リストから IP アドレスを消去するかを指定しない場合は、両方の許可リストから IP アドレスが削除されます。

注意　IP 許可リストのエントリまたはホスト アドレスを消去する前に、必ず IP 許可リストをディセーブルにしてください。現在使用中の IP アドレスを消去した場合に、設定対象のスイッチによって接続が切断されるのを防ぐためです。

IP 許可リストのエントリを消去するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	IP 許可リストをディセーブルにします。	**set ip permit disable** [**telnet** | **snmp** | **ssh**]
ステップ 2	IP 許可リストから削除する IP アドレスを指定します。	**clear ip permit** {*ip_address* [*mask*] | **all**} [**telnet** | **snmp** | **ssh**]
ステップ 3	IP 許可リストの設定を確認します。	**show ip permit**

次に、IP 許可リストからエントリを消去する例を示します。

```
Console> (enable) set ip permit disable all
Console> (enable) clear ip permit 172.100.101.102
172.100.101.102 cleared from IP permit list.
Console> (enable) clear ip permit 172.160.161.0 255.255.192.0 snmp
172.160.128.0 with mask 255.255.192.0 cleared from snmp permit list.
Console> (enable) clear ip permit 172.100.101.102 telnet
172.100.101.102 cleared from telnet permit list.
Console> (enable) clear ip permit all
IP permit list cleared.
Console> (enable)
```

CHAPTER 37

ポート セキュリティの設定

この章では、ポート セキュリティの設定方法と、Catalyst 6500 シリーズ スイッチで学習される MAC（メディア アクセス制御）アドレス数を制限する方法について説明します。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

(注) MAC（メディア アクセス制御）アドレス認証バイパスの設定については、第 40 章「MAC 認証バイパスの設定」を参照してください。

(注) 802.1X 認証の設定により、アクセスを許可されているポートから不正なデバイスが LAN 接続するのを制限する手順については、第 39 章「802.1X 認証の設定」を参照してください。

(注) Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）を設定して、Catalyst 6500 シリーズ スイッチの CLI（コマンドライン インターフェイス）へのアクセスをモニタおよび制御する方法については、第 38 章「AAA によるスイッチ アクセスの設定」を参照してください。

(注) Network Admission Control（NAC）の設定については、第 42 章「NAC の設定」を参照してください。

この章で説明する内容は、次のとおりです。

ポート セキュリティの機能

イーサネット、ファスト イーサネット、またはギガビット イーサネット ポートへのアクセスを試みたステーションの MAC アドレスが、そのポートに指定されている MAC アドレスと異なる場合、ポート セキュリティ機能を使用してポートへのアクセスをブロックできます。また、ホスト MAC アドレスに基づく指定ホストに送信、または指定ホストから受信したトラフィックをフィルタリングすることができます。

ここでは、トラフィック フィルタリング方式について説明します。

ホスト MAC アドレスに基づくトラフィックの許可

ポートあたりに指定できる MAC アドレスの総数には、次のような制限があります。

- Release 8.1(1) より前のソフトウェア リリースでは、1 つのポートにつき、指定できる MAC アドレスの総数は、グローバル リソースとしての 1024 に、デフォルトの MAC アドレス 1 つを加えた数です。1 ポート上の総 MAC アドレス数が 1025 を超えることはありません。
- Release 8.1(1) 以降のソフトウェア リリースでは、1 つのポートにつき、指定できる MAC アドレスの総数は、グローバル リソースとしての 4096 に、デフォルトの MAC アドレス 1 つを加えた数です。1 ポート上の総 MAC アドレス数が 4097 を超えることはありません。

各ポートに MAC アドレスの最大数を割り当てるかどうかは、ネットワーク構成によって決まります。次の組み合わせは、Release 8.1(1) より前のソフトウェア リリースで有効な割り当て例です。ロジックは Release 8.1(1) 以降のソフトウェア リリースでも同じです。

- 1 ポートに 1025（1 + 1024）個のアドレス、残りの各ポートに 1 アドレスずつ
- システム内の 2 ポートにそれぞれ 513（1 + 512）個、残りの各ポートに 1 アドレスずつ
- 1 ポートに 901（1 + 900）個、次のポートに 101（1 + 100）個、第 3 のポートに 25（1 + 24）個、残りの各ポートに 1 アドレスずつ

ポートに最大 MAC アドレス数を割り当てたあとで、そのポートに手動でセキュア MAC アドレスを指定するか、または接続装置の MAC アドレスをポートに動的に設定させることができます。ポートに割り当てられた最大数の MAC アドレスのうち、すべてを手動で設定するか、すべてを動的に学習するか、または一部を手動で設定し、残りを動的に学習することができます。手動または自動で設定したアドレスは、NVRAM（不揮発性 RAM）に保存され、リセット後も維持されます。動的に学習されたアドレスは保存されないので、スイッチのリセット後、それらはすべて消去されます。

ポートに最大 MAC アドレス数を割り当てたあとで、特定のポート上でアドレスの安全性が維持される期間を指定できます。エージング タイムが経過すると、そのポート上の MAC アドレスは非保護状態になります。デフォルトの設定では、ポート上のすべてのアドレスが永続的に保護されます。

セキュリティ違反が発生した場合に、ポートがシャットダウン モードまたは制限モードになるように設定できます。シャットダウン モードを使用すると、ポートを永続的にディセーブルにするのか、指定された期間だけディセーブルにするのかを指定できます。デフォルトの設定では、ポートは永続的にシャットダウンされます。制限モードを使用すると、セキュリティ違反が発生しても、ポートをイネーブルにしておき、非保護ホストから送られてきたパケットだけが廃棄されるように設定できます。

（注） 制限モードでセキュア ポートを設定していて、スイッチの別のポート上でセキュア MAC アドレスとして設定済みの MAC アドレスを持つポートにステーションを接続した場合、制限モードのポートはそのステーションからのトラフィックを制限するのではなく、シャットダウンしてしまいます。たとえば、ポート 2/1 のセキュア MAC アドレスとして MAC-1、ポート 2/2 のセキュア MAC アドレスとして MAC-2 を設定し、さらに、ポート 2/2 が制限モードとして設定されているときに、MAC-1 を指定してステーションとポート 2/2 を接続した場合、ポート 2/2 は MAC-1 からのトラフィックを制限するのではなく、シャットダウンします。

セキュア ポートがパケットを受信すると、そのパケットの送信元 MAC アドレスを、ポートに手動で設定された、または動的に学習された送信元セキュア アドレスのリストと比較します。ポートに接続された装置の MAC アドレスと、セキュア アドレス リストが異なる場合、ポートは永続的にシャットダウン（デフォルトのモード）するか、指定された期間だけシャットダウンするか、または非保護ホストからの着信パケットを廃棄します。ポートの動作は、セキュリティ違反に対してどのように対処するか、その設定によって決まります。

セキュリティ違反が発生すると、そのポートの LINK LED がオレンジに点灯し、SNMP（簡易ネットワーク管理プロトコル）マネージャにリンク ダウン トラップが送信されます。制限モードでポートを設定している場合は、SNMP トラップは送信されません。トラップが送信されるのは、セキュリティ違反時にシャットダウンするようにポートを設定している場合だけです。

ホスト MAC アドレスに基づくトラフィックの制限

ホスト MAC アドレスに基づいてトラフィックをフィルタリングし、特定の送信元 MAC アドレスを持つパケットを廃棄することができます。**set cam filter** コマンドを使用して MAC アドレス フィルタを指定すると、指定したホスト MAC アドレスからの着信トラフィックが廃棄されます。また、指定したホストを宛先とするパケットは転送されません。

（注） **set cam filter** コマンドでフィルタリングできるのは、ユニキャスト アドレスだけです。このコマンドでは、マルチキャスト アドレス用のトラフィックをフィルタリングすることはできません。

セキュア ポート上でのユニキャスト フラッディング パケットのブロック

ユニキャスト フラッディング機能をディセーブルにすることで、セキュア イーサネット ポート上でユニキャスト フラッディング パケットをブロックできます。ポートでユニキャスト フラッディング パケットをディセーブルにすると、ポートは、MAC アドレスの最大許容数に達すると、ユニキャスト フラッディング パケットを廃棄します。

MAC アドレス数が最大許容数を下回ると、ポートは自動的にユニキャスト フラッディング パケットの学習を再開します。学習された MAC アドレスのカウントは、設定された MAC アドレスが削除されるか、Time to Live（TTL）カウンタに達すると減少します。

MAC アドレス モニタリングの機能概要

Catalyst 6500 シリーズ スイッチでは送信元 MAC アドレスを自動的に学習するので、システムはスプーフィングされたトラフィックのフラッディングに弱く、DoS 攻撃を受けやすくなります。トラフィックのフラッディングや DoS 攻撃を避けるために、システムが学習した多くの MAC アドレスをポート単位、VLAN（仮想 LAN）単位、またはポート /VLAN 単位ベースでモニタできます。

MAC アドレス モニタリングはソフトウェアでサポートされています。

MAC アドレス モニタリングの設定については、「MAC アドレス モニタリングの設定」（p.37-15）を参照してください。

ポート セキュリティ設定時の注意事項

ここでは、ポート セキュリティ設定時の注意事項について説明します。

- SPAN 宛先ポートではポート セキュリティをイネーブルにしないでください。また、その逆の場合も同様です。
- セキュア ポートには、ダイナミック、スタティック、または永続 CAM（連想メモリ）エントリを設定しないでください。

スイッチ上でのポート セキュリティの設定

ここでは、ポート セキュリティを設定する手順について説明します。

- ポート セキュリティのイネーブル化（p.37-5）
- セキュア MAC アドレスの最大数の設定（p.37-6）
- 動的に学習された MAC アドレスの自動設定（p.37-7）
- ポート セキュリティ エージング タイムの設定（p.37-8）
- ポート セキュリティ エージング タイプの設定（p.37-8）
- MAC アドレスの消去（p.37-9）
- セキュア ポート上でのユニキャスト フラッディング ブロックの設定（p.37-10）
- セキュリティ違反時の処置の指定（p.37-11）
- シャットダウン タイムアウトの設定（p.37-11）
- ポート セキュリティのディセーブル化（p.37-12）
- ホスト MAC アドレスに基づくトラフィックの制限（p.37-12）
- ポート セキュリティの表示（p.37-13）

ポート セキュリティのイネーブル化

ポート上でポート セキュリティをイネーブルにすると、そのポートと対応付けられたスタティックまたはダイナミック CAM エントリは消去されます。その時点ですでに設定されている永続 CAM エントリは、安全とみなされます。

ポート セキュリティをイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポートを指定して、ポート セキュリティをイネーブルにします。セキュア MAC アドレスも指定できます。トランク ポートでポート セキュリティをイネーブルにするには、セキュア MAC アドレスが許可されている VLAN を指定します。	**set port security** *mod/port* **enable** [*mac_addr*] [*vlan_list*]
ステップ 2	セキュア アドレス リストに MAC アドレスを追加できます。	**set port security** *mod/port mac_addr* [*vlan_list*]
ステップ 3	設定を確認します。	**show port** [*mod*[*/port*]] [*mac_addr*][*vlan_list*]

次に、ポート上で学習した MAC アドレスを使用してポート セキュリティをイネーブルにし、設定を確認する例を示します。

```
Console> (enable) set port security 2/1 enable
Port 2/1 security enabled.
Console> (enable) show port 2/1
Port  Name               Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
 2/1                     connected  522        normal   half   100 100BaseTX

Port  Security Secure-Src-Addr   Last-Src-Addr     Shutdown Trap     IfIndex
----- -------- ----------------- ----------------- -------- -------- -------
 2/1  enabled  00-90-2b-03-34-08 00-90-2b-03-34-08 No       disabled 1081

Port     Broadcast-Limit Broadcast-Drop
-------- --------------- --------------
 2/1                   -              0

Port  Align-Err  FCS-Err    Xmit-Err   Rcv-Err    UnderSize
----- ---------- ---------- ---------- ---------- ---------
 2/1           0          0          0          0         0

Port  Single-Col Multi-Coll Late-Coll  Excess-Col Carri-Sen Runts     Giants
----- ---------- ---------- ---------- ---------- --------- --------- ---------
 2/1           0          0          0          0         0         0         0

Last-Time-Cleared
--------------------------
Fri Jul 10 1998, 17:53:38
```

次に、ポート上でポート セキュリティをイネーブルにし、セキュア MAC アドレスを手動で指定する例を示します。

```
Console> (enable) set port security 2/1 enable 00-90-2b-03-34-08
Port 2/1 port security enabled with 00-90-2b-03-34-08 as the secure mac address
Trunking disabled for Port 2/1 due to Security Mode
Console> (enable)
```

次に、トランク ポートでポート セキュリティを設定する例を示します。

```
Console> (enable) set port security 2/2 00-90-2b-03-34-09 1,20,30
Mac address 00-90-2b-03-34-09 set for port 2/2 on vlan 1,20,20
Console> (enable)
```

セキュア MAC アドレスの最大数の設定

ポート上で保護する MAC アドレスの数を設定できます。デフォルトの設定では、1 ポートに少なくとも 1 個の MAC アドレスを保護できます。このデフォルトに加えて、次のようにポートで共有するグローバル リソースが使用可能です。

- Release 8.1(1) より前のソフトウェア リリースでは、最大 1024 個の MAC アドレスを 1 つのポートで設定できます。1 ポート上の総 MAC アドレス数が 1025 を超えることはありません。
- Release 8.1(1) 以降のソフトウェア リリースでは、最大 4096 個の MAC アドレスを 1 つのポートで設定できます。1 ポート上の総 MAC アドレス数が 4097 を超えることはありません。

一部のポートで MAC アドレスのグローバル リソース全体を使用しても、残りのポートではまだ、1 ポートに最大 1 個の MAC アドレスを使用して、ポート セキュリティをイネーブルにできます。

MAC アドレスの最大数を少なくすると、システムによって指定された数の MAC アドレスが消去され、削除したアドレスのリストが表示されます。

8.1 および 8.2 のソフトウェア リリースでは、異なる VLAN にあるアクセス ポートに単一の MAC アドレスを設定できますが、そのポートにポート セキュリティを設定できません。Release 8.3(1) 以降のソフトウェア リリースでは、トランク ポートでポート セキュリティをサポートしていますが、異なる VLAN にある複数のポートに対して単一の MAC アドレスを設定しポート セキュリティを設定できます。たとえば、MAC アドレス [00-00-aa-00-00-aa] を VLAN 10 のポート 2/1 と VLAN 20 のポート 2/2 に設定し、いずれもポート セキュリティを設定できます。両方のポートが VLAN 10 にある場合、この MAC アドレスとポート セキュリティが設定できるのはいずれか一方になります。単一の MAC アドレスとポート セキュリティを設定できるのは、1 つの VLAN に属するポートのみです。

特定のポートで保護する MAC アドレスの数を設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
ポート上で保護する MAC アドレスの数を設定します。	**set port security** *mod/port* **maximum** *num_of_mac*

次に、保護する MAC アドレスの数を設定する例を示します。

```
Console> (enable) set port security 7/7 maximum 20
Maximum number of secure addresses set to 20 for port 7/7.
Console> (enable)
```

次に、MAC アドレスの数を減らし、消去された MAC アドレスを表示する例を示します。

```
Console> (enable) set port security 7/7 maximum 18
Maximum number of secure addresses set to 18 for port 7/7
00-11-22-33-44-55 cleared from secure address list for port 7/7
00-11-22-33-44-66 cleared from secure address list for port 7/7
Console> (enable)
```

動的に学習された MAC アドレスの自動設定

動的に学習された MAC アドレスの自動設定により、動的に学習された MAC アドレスを特定のポートに関連付けることができます。この機能は、システム内のすべてのセキュア ポートにグローバルに適用されます。

動的に学習されたアドレスは、手動で設定されたアドレスのように処理され、設定は NVRAM に保存されます。アドレスは、セキュリティ違反によるセキュア ポートのシャットダウン、ポート セキュリティのディセーブル化、またはセキュア ポートの管理上のディセーブル化といったイベントで保存されます。

（注） 自動設定オプションを使用して設定された動的に学習されたアドレスは、いかなる状況でも消去されません。これらのアドレスは、**clear port security** コマンドを入力して手動で消去する必要があります。

動的に学習された MAC アドレスの自動設定をイネーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
動的に学習された MAC アドレスの自動設定をイネーブルにします。	**set port security auto-configure enable | disable**

次に、動的に学習された MAC アドレスの自動設定をスイッチ上でグローバルにイネーブルにする例を示します。

```
Console> (enable)set port security auto-configure enable
Automatic configuration of secure learnt addresses enabled.
Console> (enable)
```

自動設定を確認するには、**show port security statistics system** コマンドを入力します。

```
Console> (enable) show port security statistics system

Auto-Configure Option: Enabled
Module 2:
  Total ports: 24
  Total secure ports: 0
  Total MAC addresses: 24
  Total global address space used (out of 4096): 0
  Status: installed
Module 3:
  Total ports: 48
  Total secure ports: 0
  Total MAC addresses: 48
  Total global address space used (out of 4096): 0
  Status: installed
Module 5:
  Total ports: 2
  Total secure ports: 0
  Total MAC addresses: 2
  Total global address space used (out of 4096): 0
  Status: installed
Total secure ports in the system: 0
Total secure MAC addresses in the system: 74
Total global MAC address resource used in the system (out of 4096): 0
Console> (enable)
```

ポート セキュリティ エージング タイムの設定

ポートのエージング タイムによって、そのポート上のすべてのアドレスの保護期間を指定します。このエージング タイムは、MAC アドレスがそのポート上のトラフィックを開始したときからアクティブになります。MAC アドレスに対応するエージング タイムが満了すると、ポート上のその MAC アドレスに対応するエントリがセキュア アドレス リストから削除されます。有効な範囲は 1 ～ 1440 分です。エージング タイムをゼロに設定すると、セキュア アドレスのエージングがディセーブルになります。

ポート上でエージング タイムを設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
ポート上の保護するアドレスにエージング タイムを設定します。	**set port security** *mod/port* **age** *time*

次に、ポート 7/7 上にエージング タイムを設定する例を示します。

```
Console> (enable) set port security 7/7 age 600
Secure address age time set to 600 minutes for port 7/7.
Console> (enable)
```

ポート セキュリティ エージング タイプの設定

(注) **set port security** *mod/port* **timer-type** {**absolute** | **inactivity**} コマンドは、Supervisor Engine 720 および Supervisor Engine 32 でのみサポートされています。

Release 8.2(1) 以降のソフトウェア リリースでは、ポート単位でエージングのタイプを設定し、動的に学習されたアドレスに適用できます。エージングのタイプには次の 2 つがあります。

- 絶対エージング ― *age_time* を超過すると、MAC アドレスはトラフィックのパターンに関係なく期限切れとなります。これはすべてのセキュア ポートでデフォルトであり、*age_time* は 0 に設定されます。
- 非アクティブ エージング ― 対応するホストが *age_time* を超過して非アクティブであった場合だけ、MAC アドレスは期限切れとなります。

動的に学習されたアドレスのポート セキュリティ エージング タイプをポートごとに設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
動的に学習されたアドレスのポート セキュリティ エージング タイプをポート単位で設定します。	**set port security** *mod/port* **timer-type** {**absolute** | **inactivity**}

次に、ポート 5/1 上に異なるポート セキュリティ エージング タイプを設定する例を示します。

```
Console> (enable) set port security 5/1 timer-type absolute
Port 5/1 security timer type absolute.
Console> (enable) set port security 5/1 timer-type inactivity
Port 5/1 security timer type inactive.
Console> (enable)
```

MAC アドレスの消去

clear port security コマンドを使用して、ポート上のセキュア アドレス リストから MAC アドレスを消去します。

（注） 使用中の MAC アドレスに **clear** コマンドを入力した場合、その MAC アドレスが学習されて、再び保護される可能性があります。ポート セキュリティをディセーブルにしてから、MAC アドレスを消去するようにしてください。

セキュア MAC アドレス リストからすべての MAC アドレス、または特定の MAC アドレスを消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
セキュア MAC アドレス リストから全部または特定の MAC アドレスを消去します。 **（注）** トランク ポートでは、VLAN リスト パラメータを使用して 1 つまたは複数の特定 VLAN のリストから MAC アドレスを消去できます。**all** キーワードを指定すると、トランク ポート上にあるすべての VLAN 用のセキュア MAC アドレス リストから MAC アドレスが消去されます。	**clear port security** *mod/port* **all** | *mac_addr* [**all** | *vlan_list*]

次に、ポート 3/37 上のセキュア アドレス リストから MAC アドレスを 1 つ消去する例を示します。

```
Console> (enable) clear port security 3/37 00-00-aa-00-00-aa 20,30
Secure MAC address 00-00-aa-00-00-aa cleared for port 3/37 and Vlan 20.
Secure MAC address 00-00-aa-00-00-aa cleared for port 3/37 and Vlan 30.
Console> (enable)
```

次に、ポート 3/37 からすべての MAC アドレスを消去する例を示します。

```
Console> (enable) clear port security 3/37 00-00-aa-00-00-aa all
Secure MAC address 00-00-aa-00-00-aa cleared for port 3/37 and Vlan 1.
Secure MAC address 00-00-aa-00-00-aa cleared for port 3/37 and Vlan 20.
Secure MAC address 00-00-aa-00-00-aa cleared for port 3/37 and Vlan 30.
Console> (enable)
```

次に、トランク ポート 2/2 の VLAN 1 から MAC アドレスをすべて消去する例を示します。

```
Console> (enable) clear port security 2/2  00-90-2b-03-34-09 1
Secure MAC address 00-90-2b-03-34-09 cleared for port 2/2 and Vlan 1.
Console> (enable)
```

セキュア ポート上でのユニキャスト フラッディング ブロックの設定

セキュア ポートでユニキャスト フラッディング ブロックを設定するには、ユニキャスト フラッディング機能をディセーブルにします。

（注） MAC アドレスの限度に達すると、ポートはユニキャスト フラッディングをディセーブルにします。

セキュア ポート上でユニキャスト フラッディング ブロックを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	指定のセキュア ポート上でユニキャスト フラッディング ブロックをディセーブルにします。	**set port security** *mod/port* **unicast-flood disable**
ステップ 2	ユニキャスト フラッディングの設定を確認します。	**show port security** *mod/port*
ステップ 3	ユニキャスト フラッディング ブロックのステータスを確認します。	**show port unicast-flood** *mod/port*

次に、ポート上でユニキャスト フラッディング パケットをディセーブルにするようにスイッチを設定し、設定を確認する例を示します。

```
Console> (enable) set port security 4/1 unicast-flood disable
Port 4/1 security flood mode set to disable.
Console> (enable) show port security 4/1
Port  Security Violation Shutdown-Time Age-Time Max-Addr Trap     IfIndex
----- -------- --------- ------------- -------- -------- -------- -------
 4/1  disabled  shutdown              0        0        1 disabled      50

Port  Num-Addr Secure-Src-Addr   Age-Left Last-Src-Addr     Shutdown/Time-Left
----- -------- ----------------- -------- ----------------- ------------------
 4/1        0                 -        -                 -        -          -

Port Flooding on Address Limit
---- -------------------------
 4/1                  Disabled
Console> (enable) show port unicast-flood 4/1
Port      Unicast Flooding
----      ----------------
4/1       Disabled
Console> (enable)
```

（注） **show port unicast-flood** コマンドにより、ユニキャスト フラッディング ブロックの実行時のステータスが表示されます。出力では、ポートがアドレスの限度を超えているかどうかに応じて、ユニキャスト フラッディングがイネーブルまたはディセーブルのいずれになっているかが表示されます。

セキュリティ違反時の処置の指定

ポートには、セキュリティ違反に対する処理として、次の 2 つのモードを設定できます。

- シャットダウン — ポートを永続的にまたは指定した期間だけシャットダウンします。永続的なシャットダウンがデフォルトのモードです。
- 制限 — 非保護ホストから送られてきたすべてのパケットを廃棄しますが、ポートは引き続きイネーブルです。

セキュリティ違反の発生時にとるべき処置を指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
ポート上での違反発生時の処置を指定します。	**set port security** *mod/port* **violation** {**shutdown** | **restrict**}

次に、ポート 7/7 上で、非保護ホストから送られたすべてのパケットを廃棄するように指定する例を示します。

```
Console> (enable) set port security 7/7 violation restrict
Port security violation on port 7/7 will cause insecure packets to be dropped.
Console> (enable)
```

(注) ポートのセキュア MAC アドレス数を 1 に制限して、他のホストがそのポートに接続しようとした場合、ポート セキュリティによって、他のホストからそのポートに接続することが禁止されるとともに、VLAN エージング タイムの間、同じ VLAN 内のすべてのポートへの接続が防止されます。デフォルトの設定では、VLAN エージング タイムは 5 分です。セキュア ポートであるために、同一 VLAN 内のポートにホストが接続できない場合は、VLAN エージング タイムが経過したあとで、もう一度ホストからポートに接続してください。

シャットダウン タイムアウトの設定

セキュリティ違反が発生した場合に、ポートをディセーブルにしておく時間を指定できます。デフォルトの設定では、ポートは永続的にシャットダウンされます。有効な範囲は 1 ～ 1440 分です。

この時間をゼロに設定すると、そのポートではシャットダウンがディセーブルになります。

(注) シャットダウン タイムが満了すると、ポートは再びイネーブルになり、ポート セキュリティ関連のすべての設定が維持されます。

シャットダウン タイムアウトを設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
ポート上でシャットダウン タイムアウトを設定します。	**set port security** *mod/port* **shutdown** *time*

次に、ポート 7/7 上でシャットダウン タイムアウト値を 600 分に設定する例を示します。

```
Console> (enable) set port security 7/7 shutdown 600
Secure address shutdown time set to 600 minutes for port 7/7.
Console> (enable)
```

ポート セキュリティのディセーブル化

ポート セキュリティをディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポートを指定して、ポート セキュリティをディセーブルにします。	**set port security** *mod/port* **disable**
ステップ 2	設定を確認します。	**show port security** [*mod/port*]

次に、ポート セキュリティをディセーブルにする例を示します。

```
Console> (enable) set port security 2/1 disable
Port 2/1 port security disabled.
Console> (enable)
Console> (enable) show port security 2/1
Port  Security Violation Shutdown-Time Age-Time Max-Addr Trap     IfIndex
----- -------- --------- ------------- -------- -------- -------- -------
 3/24 disabled  restrict             20      300       10 disabled     921

Port  Num-Addr Secure-Src-Addr   Age-Left Last-Src-Addr     Shutdown/Time-Left
----- -------- ----------------- -------- ----------------- ------------------
 3/24        1 00-e0-4f-ac-b4-00        -                 -         -          -
Console> (enable)
```

ホスト MAC アドレスに基づくトラフィックの制限

特定の MAC アドレスのトラフィックを制限するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	指定した MAC アドレスとの間の送信または受信トラフィックを制限します。	**set cam** {**static** | **permanent**} **filter** *unicast_mac vlan*
ステップ 2	フィルタを削除します。	**clear cam** *mac_address vlan*
ステップ 3	設定を確認します。	**show cam** {**static** | **permanent**}

次に、特定の MAC アドレスに対するトラフィックを制限するフィルタを作成する例を示します。

```
Console> (enable) set cam static filter 00-02-03-04-05-06 1
Filter entry added to CAM table.
Console> (enable)
```

次に、フィルタを消去する例を示します。

```
Console> (enable) clear cam 00-02-03-04-05-06 1
CAM entry cleared.
Console> (enable)
```

次に、スタティック CAM エントリを表示する例を示します。

```
Console> show cam static

VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs /[Protocol Type]
----  ------------------    -----  ----------------------------------------
3     04-04-05-06-07-08   *          FILTER
```

ポート セキュリティの表示

show port security コマンドを使用すると、次の情報が表示されます。

- ポートのセキュア MAC アドレス リスト
- ポート上で使用できる最大セキュア アドレス数
- セキュア MAC アドレスの総数
- エージング タイム
- 残っているエージング タイムおよびシャットダウンのタイムアウトまでの時間
- シャットダウン / セキュリティ モード
- ポート セキュリティ関連の統計情報

ポート セキュリティの設定情報および統計情報を表示するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	設定を表示します。	**show port security** [**statistics**] *mod/port*
ステップ 2	ポート セキュリティの統計情報を表示します。	**show port security statistics** [**system**] [*mod/port*]

次に、ポート セキュリティの設定情報および統計情報を表示する例を示します。

```
Console> (enable) show port security 4/1
* = Configured MAC Address

Port  Security Violation Shutdown-Time Age-Time Maximum-Addrs Trap     IfIndex
----- -------- --------- ------------- -------- ------------- -------- -------
 4/1  enabled  shutdown  120           1440     25            disabled 3

Port Secure-Src-Addrs  Age-Left Last-Src-Addr     Shutdown Shutdown-Time-Left
---- ----------------- -------- ----------------- -------- ------------------
 4/1 00-11-22-33-44-55 4        00-11-22-33-44-55 No       -
     00-10-14-da-77-f1 100
Port  Flooding on Address Limit
----- -------------------------
 4/1                    Enabled
Console> (enable) show port security statistics 4/1
Port  Total-Addrs Maximum-Addrs
----- ----------- -------------
 4/1            4            10
Console> (enable)
```

次に、モジュールに関してポート セキュリティの統計情報を表示する例を示します。

```
Console> (enable) show port security statistics 7
Port  Total-Addrs Maximum-Addrs
----- ----------- -------------
 7/1            0             1
 7/2            0             1
 7/3            0             1
 7/4            0             1
 7/5            0             1
 7/6            0             1
 7/7            0             1
 7/8            0             1
 7/9            0             1
 7/10           0           200
 7/11           0             1
 7/12           0             1
 7/13           0             1
 7/14           0             1
 7/15           0             1
 7/16           0             1
 7/17           0             1
 7/18           0             1
 7/19           0             1
 7/20           0             1
 7/21           0             1
 7/22           0             1
 7/23           0             1
 7/24           0             1
Module 7:
  Total ports: 24
  Total secure ports: 0
  Total MAC address(es): 223
  Total global address space used (out of 4096): 199
  Status: installed
Console> (enable)
```

次に、システムに関してポート セキュリティの統計情報を表示する例を示します。

```
Console> (enable) show port security statistics system

Auto-Configure Option: Enabled
Module 2:
  Total ports: 24
  Total secure ports: 0
  Total MAC addresses: 24
  Total global address space used (out of 4096): 0
  Status: installed
Module 3:
  Total ports: 48
  Total secure ports: 0
  Total MAC addresses: 48
  Total global address space used (out of 4096): 0
  Status: installed
Module 5:
  Total ports: 2
  Total secure ports: 0
  Total MAC addresses: 2
  Total global address space used (out of 4096): 0
  Status: installed
Total secure ports in the system: 0
Total secure MAC addresses in the system: 74
Total global MAC address resource used in the system (out of 4096): 0
Console> (enable)
```

MAC アドレス モニタリングの設定

ここでは、MAC アドレス モニタリングを設定する手順について説明します。

グローバル MAC アドレス モニタリングの設定

MAC アドレス モニタリングをグローバルにイネーブルまたはディセーブルにできます。MAC アドレス モニタリングをグローバルにディセーブルにしても設定は消去されません。

MAC アドレス モニタリングをグローバルにイネーブルまたはディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
MAC アドレス モニタリングをグローバルにイネーブルまたはディセーブルにします。 **（注）** デフォルトで、モニタリングはグローバルにイネーブルです。	**set cam monitor {disable | enable}**

次に、グローバル MAC アドレス モニタリング設定をディセーブルおよびイネーブルにする例を示します。

```
Console> (enable) set cam monitor disable
Cam monitor disabled
Console> (enable) set cam monitor enable
Cam monitor enabled
Console> (enable)
```

CAM テーブル内の MAC アドレスのモニタリング

学習されて CAM テーブルに保存された MAC アドレスをモニタするには、イネーブル モードで次の作業を行います。

作業	コマンド
ポート単位、VLAN 単位、またはポート /VLAN 単位ベースで学習されて CAM テーブルに保存されている MAC アドレスをモニタします。 (注) MAC アドレス モニタリングは、インターフェイス（ポート、VLAN、ポート /VLAN ベース）上でデフォルトでディセーブルです。	**set cam monitor** {**disable** | **enable**} [*mod*/*port* | {*mod*/*port vlan*} | *vlan*]

次に、特定のポートで学習されて CAM テーブルに保存されている MAC アドレスをモニタする例を示します。

```
Console> (enable) set cam monitor enable 3/1
Successfully enabled cam monitor on 3/1
Console> (enable)
```

次に、特定のポートで学習された MAC アドレスのモニタリングをディセーブルにする例を示します。

```
Console> (enable) set cam monitor disable 3/1
Successfully disabled cam monitor on 3/1
Console> (enable)
```

モニタリングのポーリング間隔の指定

MAC アドレス モニタリングはソフトウェアでサポートされています。CAM テーブルに多くの MAC アドレスと多くの設定済みインターフェイス（ポート、VLAN、またはポート VLAN）がある場合、CPU 使用率が上がります。**set cam monitor interval** コマンドを入力してソフトウェア ポーリング間隔を調整することで、CPU の負荷を低減できます。

CAM テーブルのポーリング間隔を指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
CAM テーブルのモニタリングに関するポーリング間隔を秒単位で指定します。有効な範囲は 5 ～ 30 秒です。 (注) デフォルトのポーリング間隔は 5 秒です。	**set cam monitor interval** *time_s*

次に、CAM テーブルのポーリング間隔を指定する例を示します。

```
Console> (enable) set cam monitor interval 20
Cam monitor interval set to 20 sec
Console> (enable)
```

MAC アドレス モニタリングの下限スレッシュホールドの指定

MAC アドレス モニタリングの下限スレッシュホールドを指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
MAC アドレス モニタリングの下限スレッシュホールドと、システムがこのスレッシュホールドを超過した場合に行う処置について指定します。下限スレッシュホールドの有効な範囲は 5 ～ 32000 です。 (注) **no-learn** キーワードを指定する場合、設定はポート /VLAN 設定で、違反発生時には、すべての VLAN 上のポートで MAC アドレスの学習を停止します。**warning** キーワードを指定した場合、下限スレッシュホールドを超過するとシステムはシステム メッセージを表示します。	**set cam monitor low-threshold** *value* [**action** {**no-learn** | **warning**}] {*mod/port* | {*mod/port vlan*} | *vlan*}

次に、ポートの下限スレッシュホールドとスレッシュホールドを超過した場合に行う処置を指定する例を示します。

```
Console> (enable) set cam monitor low-threshold 500 action warning 3/1
Successfully configured cam monitor on 3/1
Console> (enable)
```

MAC アドレス モニタリングの上限スレッシュホールドの指定

MAC アドレス モニタリングの上限スレッシュホールドを指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
MAC アドレス モニタリングの上限スレッシュホールドと、システムがこのスレッシュホールドを超過した場合に行う処置について指定します。上限スレッシュホールドの有効な範囲は 5 ～ 32000 です。 (注) **no-learn** キーワードを指定する場合、設定はポートと VLAN の組み合わせで、違反発生時には、VLAN 上のすべてのポートで MAC アドレスの学習を停止します。**shutdown** キーワードを指定し、設定がポートと VLAN の組み合わせの場合、違反発生時にはポートを errdisable にします。**warning** キーワードを指定した場合、上限スレッシュホールドを超過するとシステムはシステム メッセージを表示します。	**set cam monitor high-threshold** *value* [**action** {**no-learn** | **shutdown** | **warning**}] {*mod/port* | {*mod/port vlan*} | *vlan*}

次に、ポートの上限スレッシュホールドとスレッシュホールドを超過した場合に行う処置を指定する例を示します。

```
Console> (enable) set cam monitor high-threshold 28000 action shutdown 3/1
Successfully configured cam monitor on 3/1
Console> (enable)
```

MAC アドレス モニタリング設定の消去

MAC アドレス モニタリングの設定を消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
MAC アドレス モニタリングの設定を消去します。	**clear cam monitor** *mod/port* | *mod/port vlan* | *vlan* **clear cam monitor all** **clear cam monitor high-threshold** *mod/port* | *mod/port vlan* | *vlan* **clear cam monitorlow-threshold** *mod/port* | *mod/port vlan* | *vlan*

次に、ポート 3/1 上で上限スレッシュホールドを消去する例を示します。

```
Console> (enable) clear cam monitor high-threshold 3/1
Successfully cleared high-threshold on 3/1
```

次に、すべてのポートから CAM テーブル モニタリングおよび MAC アドレス モニタリング設定を消去する例を示します。

```
Console> (enable) clear cam monitor all
Cleared all cam monitor configuration
Console> (enable)
```

CAM モニタの設定の表示

CAM モニタの設定を表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
CAM モニタの設定を表示します。	**show cam monitor** [*mod/port* | *mod/port vlan* | *vlan* | **all**]

次に、CAM モニタの設定を表示する例を示します。

```
Console> (enable) show cam monitor all
Cam monitor global configuration:
status : enabled
interval : 5 seconds
* = violation occured

Port Status Low Low High High No. of
Threshold Action Threshold Action mac addrs
------ -------- --------- -------- --------- -------- ---------
3/1 enabled 500 warning 32000 warning 0
4/2 enabled 500 warning* 32000 warning 0

Total port entries = 2

Console> (enable)
```

CAM モニタのグローバル設定の表示

グローバル CAM モニタの設定を表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
CAM モニタのグローバル設定を表示します。	**show cam monitor**

```
Console> (enable) show cam monitor
Cam monitor global configuration:
status : enabled
interval : 5 seconds
Console> (enable)
```

CHAPTER 38

AAA によるスイッチ アクセスの設定

この章では、Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）を設定して、Catalyst 6500 シリーズ スイッチ上で CLI（コマンドライン インターフェイス）へのアクセスをモニタおよび制御する方法について説明します。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

(注) 802.1X 認証の設定により、アクセスを許可されているポートから不正なデバイスが LAN 接続するのを制限する手順については、第 39 章「802.1X 認証の設定」を参照してください。

(注) MAC（メディア アクセス制御）アドレス認証バイパスの設定については、第 40 章「MAC 認証バイパスの設定」を参照してください。

(注) ホスト MAC アドレスに基づいてトラフィックを許可または制限するようにポートを設定する手順については、第 37 章「ポート セキュリティの設定」を参照してください。

(注) Network Admission Control（NAC）の設定については、第 42 章「NAC の設定」を参照してください。

この章で説明する内容は、次のとおりです。

認証の機能

ここでは、各認証方式のメカニズムについて説明します。

認証の概要

次の認証方式を任意に組み合わせて設定することにより、スイッチに対するアクセスを制御できます。

- ログイン認証
- ローカル認証
- RADIUS 認証
- TACACS+ 認証
- Kerberos 認証

（注）　認証方式として TACACS+ を使用している場合、Kerberos 認証は機能しません。

ローカル認証を 1 つまたは複数の他の認証方式と併用してイネーブルにすると、ローカル認証は常に最後に試行されます。ただし、コンソール接続と Telnet 接続には異なる認証方式を指定することができます。たとえば、コンソール接続にローカル認証を使用して、Telnet 接続に RADIUS 認証を使用することができます。

ログイン認証の機能

ログイン認証は、不正ユーザにパスワードを推測させないようにすることで、セキュリティを向上させます。ユーザはスイッチに正常にログインするまでのログイン試行回数が制限されています。ユーザがパスワード認証に失敗した場合、システムはアクセスを延期し、Syslog および SNMP（簡易ネットワーク管理プロトコル）トラップにステーションのユーザ ID および IP アドレスを記録します。

ログイン試行回数の最大値は、**set authentication login attempt** *count* コマンドを使用して、CLI および SNMP で設定できます。イネーブル モードへのアクセスに対してログイン制限を設定するには、**set authentication enable attempt** *count* コマンドを入力します。設定範囲は 3（デフォルト）～ 10 回です。ログイン認証をゼロ（0）に設定すると、この機能はディセーブルになります。

すべての認証方式（Remote Access Dial-In User Service [RADIUS]、Terminal Access Controller Access Control System Plus [TACACS+]、Kerberos、またはローカル）がサポートされています。

ロックアウト（遅延）時間は、**set authentication login lockout** *time* コマンドを使用して、CLI および SNMP で設定できます。イネーブル モードへのアクセスに対して遅延時間を設定するには、**set authentication enable lockout** *time* コマンドを使用します。設定範囲は 30 ～ 43,200 秒です。ロックアウト時間をゼロ（0）に設定すると、この機能はディセーブルになります。

ユーザがコンソールでロックアウトされると、ロックアウト時間が経過するまで、コンソールにログインすることはできません。Telnet セッションでロックアウトされた場合は、制限時間に達すると接続が終了します。スイッチは、ロックアウト時間が経過するまで、そのステーションからの以降のアクセスを無効にし、適切な通知を表示します。

ローカル認証の機能

ローカル認証では、ローカルで設定されたログイン パスワードとイネーブル パスワードを使用して、ログイン試行を認証します。ログイン パスワードおよびイネーブル パスワードは、各スイッチにローカルであり、個々のユーザ名とは対応付けられません。

デフォルトでは、ローカル認証はイネーブルに設定されています。1 つまたは複数の他の認証方式をイネーブルにしたときだけ、ローカル認証をディセーブルにできます。ただし、ローカル認証がディセーブルのときに、その他すべての認証方式をディセーブルにすると、ローカル認証が自動的に再びイネーブルになります。

ローカル認証とともに、1 つまたは複数の他の認証方式を同時にイネーブルにできます。ローカル認証は、他の認証方式が失敗した場合に限って、スイッチによって試行されます。

ローカル ユーザ認証の機能

ローカル ユーザ認証では、ローカル ユーザのログイン試行の確認のために作成するローカル ユーザ アカウントとパスワードを使用します。各スイッチで最大 25 のローカル ユーザ アカウントを設定できます。ローカル ユーザ認証をイネーブルにするには、先に少なくとも 1 つのローカル ユーザ アカウントを定義します。

ローカル ユーザ アカウントを設定するには、ローカル ユーザごとに一意のユーザ名およびパスワードの組み合わせを作成します。各ユーザ名は 64 文字以内の英数字を使用できます（少なくとも 1 文字は英字であること）。

ローカル ユーザ アカウントごとに権限レベルを設定します。有効な権限レベルは 0 ～ 15 です。ユーザ名およびパスワードの組み合わせに割り当てられた権限レベルにより、認証成功後にユーザがユーザ モードまたはイネーブル モードのいずれでログインするかが決まります。権限レベルが 0 のユーザは、自動的にユーザ モードでログインします。権限レベルが 15 のユーザはイネーブル モードでログインします。権限レベルが 0 のユーザも、**enable** コマンドとパスワードの組み合わせを入力して、イネーブル モードにアクセスできます。ローカル ユーザがログインした場合、表示できるのは、その権限レベルで使用可能なコマンドのみです。

（注） CiscoView イメージを実行しているか、HTTP ログインを使用してログインしている場合は、システムの初期認証がユーザ名とパスワードの組み合わせで実行されます。ローカル ユーザに 15 の権限レベルが設定されていれば、権限パスワードを入力するかユーザ名とパスワードの組み合わせを使用するとイネーブル モードを開始できます。

TACACS+ 認証の機能

TACACS+ は、ネットワーク装置と中央データベースの間で Network Access Server（NAS）情報を交換し、ユーザまたはエンティティのアイデンティティを判別することにより、ネットワーク装置に対するアクセスを制御します。TACACS+ は、RFC 1492 で規定されている UDP ベースのアクセス制御プロトコル、TACACS の拡張バージョンです。TACACS+ は TCP を使用して、ネットワーク装置上の TACACS+ サーバと TACACS+ デーモン間のすべてのトラフィックを暗号化し、信頼性の高い配信を保証します。

TACACS+ は、固定パスワード、ワンタイム パスワード、チャレンジ応答認証など、多数の認証タイプをサポートしています。TACACS+ 認証は、通常、次の状況で実行されます。

- 装置への最初のログイン時
- 権限付きアクセス権が必要なサービス要求の送信時

権限が必要なサービスまたは制限付きのサービスを要求すると、TACACS+ により、MD5 暗号化アルゴリズムに基づいてユーザのパスワード情報が暗号化され、TACACS+ パケット ヘッダーが付加されます。このヘッダー情報には、送信パケットのタイプ（認証パケットなど）、パケット シーケンス番号、使用した暗号タイプ、パケット合計長が含まれています。このパケットが TACACS+ プロトコルによって TACACS+ サーバに転送されます。

TACACS+ サーバは、認証、許可、およびアカウンティングの機能を実行します。いずれのサービスも TACACS+ の機能ですが、それぞれ独立しているので、TACACS+ 設定ごとに任意の組み合わせで使用できます。

パケットを受信した TACACS+ サーバは、次のように動作します。

- ユーザ情報を認証し、認証の成否をクライアントに通知します。
- 認証処理が続けられること、および追加情報が必要なことをクライアントに通知します。このチャレンジ応答プロセスは、認証の成否が確定するまで繰り返されます。

クライアントおよびサーバに TACACS+ 鍵を設定できます。スイッチ上でこの鍵を設定する場合、TACACS+ サーバ上で設定されている鍵と一致させなければなりません。TACACS+ クライアント / サーバはこの鍵を使用して、送信対象のすべての TACACS+ パケットを暗号化します。TACACS+ 鍵を設定しなかった場合、パケットは暗号化されません。

スイッチ上で次の TACACS+ パラメータを設定できます。

- スイッチへのアクセスがユーザに許可されているかどうかを判別する TACACS+ 認証のイネーブル化およびディセーブル化
- イネーブル モードへのアクセスがユーザに許可されているかどうかを判別する TACACS+ 認証のイネーブル化およびディセーブル化
- プロトコル パケットを暗号化する鍵
- TACACS+ サーバ デーモンを常駐させるサーバ
- ログインの最大試行回数
- サーバ デーモンの応答に関するタイムアウト インターバル
- directed request（指定要求）オプションのイネーブル化およびディセーブル化

TACACS+ 認証は、ディセーブルがデフォルトの設定です。TACACS+ 認証とローカル認証の両方を同時にイネーブルに設定できます。

ローカル認証がディセーブルのときに、その他すべての認証方式をディセーブルにすると、ローカル認証が自動的に再度イネーブルになります。

RADIUS 認証の機能

RADIUS は、ネットワーク装置への接続を試みるユーザを認証する際に、NAS が使用するクライアント / サーバ認証および許可アクセス プロトコルです。NAS はクライアントとして動作するとき、1 つまたは複数の RADIUS サーバにユーザ情報を引き渡します。NAS は、1 つまたは複数の RADIUS サーバから受信した応答に基づいて、ユーザに対してネットワーク アクセスを許可または拒否します。RADIUS では、RADIUS クライアントとサーバ間の伝送に UDP を使用します。

クライアントおよびサーバ上で RADIUS 鍵を設定できます。クライアント上でこの鍵を設定する場合、RADIUS サーバ上で設定されている鍵と一致させなければなりません。RADIUS クライアントおよびサーバは、鍵を使用して、転送された RADIUS パケットをすべて暗号化します。RADIUS 鍵を設定しないと、パケットは暗号化されません。鍵自体がネットワーク上を転送されることはありません。

(注)　RADIUS プロトコルの詳細説明については、RFC 2138「Remote Authentication Dial In User Service（RADIUS）」を参照してください。

スイッチ上で設定できる RADIUS パラメータは次のとおりです。

- ログイン アクセスを制御するための RADIUS 認証のイネーブル化およびディセーブル化
- イネーブル アクセスを制御するための RADIUS 認証のイネーブル化およびディセーブル化
- RADIUS サーバの IP アドレスおよび UDP ポートの指定
- RADIUS パケットの暗号化に使用する RADIUS 鍵の指定
- RADIUS サーバのタイムアウト インターバルの指定
- RADIUS 再送信カウントの指定
- RADIUS サーバの待機時間の長さの指定

RADIUS 認証のデフォルト設定は、ディセーブルです。RADIUS 認証とその他の認証方式は同時にイネーブルにできます。最初に使用する方式は、**primary** キーワードを使用して指定できます。

ローカル認証がディセーブルのときに、その他すべての認証方式をディセーブルにすると、ローカル認証が自動的に再度イネーブルになります。

Kerberos 認証の機能

Kerberos は、クライアント / サーバ ベースの秘密鍵ネットワーク認証方式で、信頼できる Kerberos サーバを使用して、サービスとユーザの両方に対するセキュア アクセスを確認します。Kerberos では、この信頼できるサーバを Key Distribution Center（KDC; 鍵発行局）といいます。KDC はユーザおよびサービスを検証するためにチケットを発行します。チケットは、特定のサービスに関してクライアントのアイデンティティを確認するための一時的な一連の電子信用情報です。

このチケットには有効期限があり、サービスがチケットの発行元である Kerberos サーバを信頼している場合、標準のパスワード ペアによる認証メカニズムの代わりにチケットを使用できます。標準のユーザ パスワード方式を使用する場合は、Kerberos がユーザのパスワードを暗号化してチケットに組み込み、パスワードがネットワーク上をクリア テキストとして流れないようにします。Kerberos を使用した場合、パスワードは、Kerberos サーバ以外の装置上で保存されるのは数秒以下です。Kerberos を使用すると、暗号化されたチケットをネットワークから盗もうとする侵入者に対しても防御できます。

表 38-1 に、Kerberos の用語を定義します。

表 38-1　Kerberos の用語

用語	定義
Kerberos 対応	Kerberos 証明書の基盤をサポートするように変更されたアプリケーションおよびサービス。
Kerberos 証明書	Ticket Granting Ticket（TGT; 身分証明書）などの認証チケット、およびサービス証明書のこと。Kerberos 証明書で、ユーザまたはサービスのチケットを検証します。ネットワーク サービスがチケットを発行した Kerberos サーバを信頼することにした場合、ユーザ名およびパスワードを再度入力する代わりに Kerberos 証明書を使用できます。証明書の有効期限は、8 時間がデフォルトの設定です。
Kerberos アイデンティティ	（Kerberos プリンシパルを参照）
Kerberos プリンシパル	Kerberos プリンシパルは、Kerberos サーバに基づき、ユーザが誰であるか、サービスが何であるかを表します。Kerberos アイデンティティともいいます。
Kerberos レルム	Kerberos サーバに登録されたユーザ、ホスト、およびネットワーク サービスで構成されるドメイン。Kerberos サーバを信頼して、ユーザまたはネットワーク サービスに対する別のユーザまたはネットワーク サービスのアイデンティティ検証が行われます。Kerberos レルムは、常に大文字にする必要があります。
Kerberos サーバ	ネットワーク ホスト上で稼働しているデーモン。ユーザおよびネットワーク サービスは、それぞれのアイデンティティを Kerberos サーバに登録します。ネットワーク サービスは Kerberos サーバにクエリを出して、他のネットワーク サービスを認証します。
KDC	ネットワーク ホスト上で稼働している Kerberos サーバおよびデータベース プログラム。さまざまなユーザまたはネットワーク サービスに Kerberos 証明書を割り当てます。
サービス証明書	ネットワーク サービスに関する証明書。KDC から発行されるこの証明書は、ネットワーク サービスと KDC 間で共通のパスワード、およびユーザの TGT と一緒に暗号化されます。
SRVTAB	ネットワーク サービスが KDC と共有するパスワード。ネットワーク サービスは、SRVTAB（別名 KEYTAB）を使用することにより、暗号化されたサービス証明書を認証して解読します。
TGT	KDC が認証済みユーザに発行する証明書。TGT を受け取ったユーザは、KDC が表した Kerberos レルム内のネットワーク サービスに関して、認証を得ることができます。

Catalyst 6500 シリーズ スイッチでは、コンソール ポートおよび帯域内管理ポートの両方で、Telnet クライアントおよびサーバを Kerberos 対応にすることができます。

（注） 認証メカニズムとして TACACS+ を使用している場合、Kerberos 認証は機能しません。

（注） モデムまたは端末サーバからコンソールにログインする場合は、Kerberos 対応のログイン手順を使用できません。

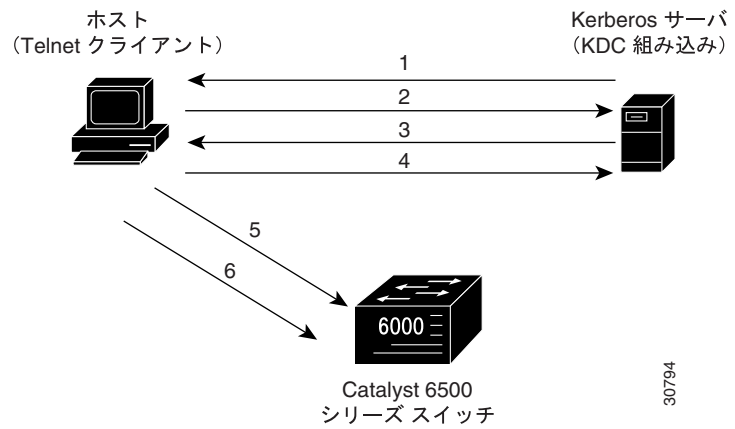
Kerberos 対応のログイン手順を使用する場合

帯域内管理ポートからログインする場合は、Kerberos 対応の Telnet セッションを使用できます。Telnet クライアントおよびサービスが Kerberos 対応になっている場合、ユーザは次の手順でスイッチに Telnet でアクセスします。

1. Telnet クライアントはユーザ名を要求し、Kerberos サーバ上の KDC に TGT 要求を出します。
2. KDC が TGT を作成します。TGT にはユーザのアイデンティティ、KDC のアイデンティティ、TGT の有効期限が指定されます。KDC はさらに、ユーザのパスワードとともに TGT を暗号化し、その TGT をクライアントに送信します。
3. 暗号化された TGT を受け取った Telnet クライアントは、パスワードを要求します。Telnet クライアントが入力されたパスワードを使用して TGT を解読できた場合、KDC の認証が正常に得られます。クライアントはその後、サービス証明書要求を作成して KDC に送信します。この要求には、ユーザのアイデンティティ、およびスイッチに Telnet で接続することを伝えるメッセージが含まれます。この要求は TGT を使用して暗号化されます。
4. KDC がクライアントに発行した TGT を使用してサービス証明書要求を正しく解読できた場合、スイッチへのサービスが用意されます。サービス証明書にはクライアントのアイデンティティ、および所定の Telnet サーバのアイデンティティが指定されます。KDC はさらに、スイッチの Telnet サーバと共通のパスワードを使用して証明書を暗号化し、生成されたパケットを Telnet クライアントの TGT で暗号化して、クライアントにパケットを送信します。
5. Telnet クライアントはまず、自身の TGT を使用してパケットを解読します。暗号化に問題がなければ、クライアントからスイッチの Telnet サーバへ、生成されたパケットを送信します。この時点では、パケットはまだ、スイッチの Telnet サーバと KDC が共有するパスワードで暗号化された状態です。
6. Telnet クライアントは指示された場合、TGT をスイッチに転送します。その結果、別の TGT を取得しなくても、スイッチの別のネットワーク サービスを使用できます。

図 38-1 に、Kerberos 対応 Telnet の接続プロセスを示します。

図 38-1　Kerberos 対応の Telnet 接続



Kerberos 非対応のログイン手順を使用する場合

Kerberos 非対応のログイン手順を使用してスイッチにログインする場合、スイッチがログイン クライアントの代わりに、KDC に対する認証を処理します。ただし、ユーザ パスワードはクリア テキストの状態でログイン クライアントからスイッチに転送されます。

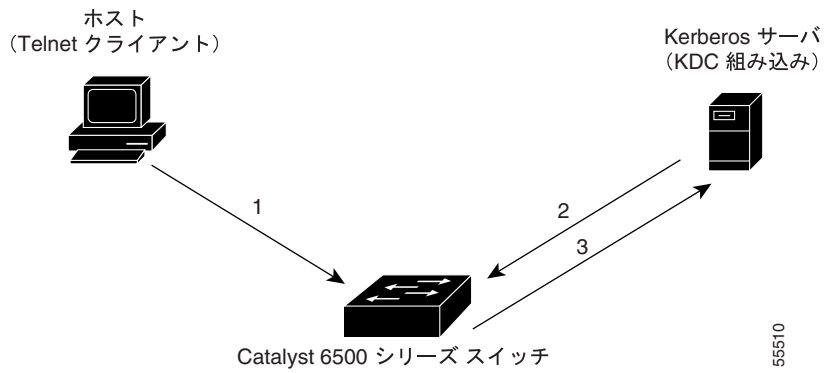
(注)　Kerberos 非対応のログインは、モデムまたは端末サーバから、帯域内管理ポートを使用して実行できます。Telnet は、Kerberos 非対応のログインをサポートしていません。

Kerberos 非対応のログインを開始した場合、手順は次のようになります。

1. ユーザ名およびパスワードを入力するように要求されます。
2. スイッチから KDC に TGT を要求します。その結果、ユーザはスイッチの認証を受けることができます。
3. KDC がスイッチに暗号化された TGT を送信します。TGT にはユーザのアイデンティティ、KDC のアイデンティティ、TGT の有効期限が指定されます。
4. スイッチはユーザが入力したパスワードを使用して、TGT を解読します。解読が正常に完了した場合、ユーザはスイッチの認証が得られます。
5. 他のネットワーク サービスにアクセスする場合は、KDC に直接アクセスして認証を受ける必要があります。TGT を取得するには、Kerberos パッケージに付属しているクライアント ソフトウェア プログラム [kinit] を使用します。

図 38-2 に、Kerberos 非対応のログイン プロセスを示します。

図 38-2　Kerberos 非対応の Telnet 接続



スイッチ上での認証の設定

ここでは、さまざまな認証方式を設定する手順について説明します。

認証のデフォルト設定

表 38-2 に、認証のデフォルト設定を示します。

表 38-2　認証のデフォルト設定

機能	デフォルト値
ログイン認証（コンソールおよび Telnet）	イネーブル
ローカル認証（コンソールおよび Telnet）	イネーブル
ローカル ユーザ認証	ディセーブル
TACACS+ ログイン認証（コンソールおよび Telnet）	ディセーブル
TACACS+ イネーブル認証（コンソールおよび Telnet）	ディセーブル
TACACS+ 鍵	指定なし
TACACS+ ログイン試行回数	3
TACACS+ サーバ タイムアウト	5 秒
TACACS+ 指定要求	ディセーブル
RADIUS ログイン認証（コンソールおよび Telnet）	ディセーブル
RADIUS イネーブル認証（コンソールおよび Telnet）	ディセーブル
RADIUS サーバ IP アドレス	指定なし
RADIUS サーバ UDP 認証ポート	ポート 1812
RADIUS 鍵	指定なし
RADIUS サーバ タイムアウト	5 秒
RADIUS サーバ待機時間	0（サーバは待機状態としてマークされていません）
RADIUS 再送信試行回数	2 回
Kerberos ログイン認証（コンソールおよび Telnet）	ディセーブル
Kerberos イネーブル認証（コンソールおよび Telnet）	ディセーブル
Kerberos サーバ IP アドレス	指定なし
Kerberos DES 鍵	指定なし
Kerberos サーバ認証ポート	ポート 750
Kerberos ローカル レルム名	ヌル ストリング
Kerberos 証明書転送	ディセーブル

表 38-2　認証のデフォルト設定（続き）

機能	デフォルト値
Kerberos クライアント必須	必須ではない
Kerberos 事前認証	ディセーブル

認証設定時の注意事項

ここでは、スイッチでの認証設定時の注意事項について説明します。

- **console** キーワードまたは **telnet** キーワードを使用して、接続タイプ別に使用する認証方式を指定しないかぎり、認証の設定はコンソール接続と Telnet 接続の両方に適用されます。
- スイッチ上で RADIUS または TACACS+ 鍵を設定した場合は、同じ鍵を RADIUS または TACACS+ サーバ上で設定しなければなりません。
- スイッチ上で RADIUS または TACACS+ をイネーブルにする前に、RADIUS サーバまたは TACACS+ サーバを指定する必要があります。
- 複数の RADIUS サーバまたは TACACS+ サーバを設定する場合は、最初に設定するサーバがプライマリ サーバになり、認証要求はそのサーバに最初に送信されます。特定のサーバをプライマリとして指定する場合は、**primary** キーワードを使用します。
- RADIUS および TACACS+ は、1 つのイネーブル モードだけをサポートします（レベル 1）。
- 認証メカニズムとして TACACS+ も使用している場合、Kerberos 認証は機能しません。
- ローカル ユーザ認証をイネーブルにするには、先に少なくとも 1 つのユーザ名を定義します。
- ローカル ユーザ アカウントおよびパスワードは 64 文字以内で、英数字を使用できます。ただし、ローカル ユーザ アカウントには少なくとも 1 文字は英字を使用します。

ログイン認証の設定

ここでは、スイッチ上でログイン認証を設定する手順について説明します。

- スイッチ上でのログイン認証の試行回数の設定（p.38-10）
- イネーブル モードのログイン認証試行回数の設定（p.38-11）

スイッチ上でのログイン認証の試行回数の設定

スイッチ上でログイン認証を設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチ上でログイン試行回数制限をイネーブルにします。コンソール ポート接続または Telnet 接続に限ってログイン認証をイネーブルにする場合は、**console** または **telnet** キーワードを指定します。	**set authentication login attempt** {*count*} [**console** | **telnet**]
ステップ 2	スイッチ上でログイン ロックアウト時間をイネーブルにします。コンソール ポート接続または Telnet 接続に限ってログイン認証をイネーブルにする場合は、**console** または **telnet** キーワードを指定します。	**set authentication login lockout** {*time*} [**console** | **telnet**]
ステップ 3	ローカル認証の設定を確認します。	**show authentication**

次に、ログイン試行回数を 5 回に制限し、コンソール接続と Telnet 接続の両方についてロックアウト時間を 50 秒に設定し、その設定を確認する例を示します。

```
Console> (enable) set authentication login attempt 5
Login authentication attempts for console and telnet logins set to 5.
Console> (enable) set authentication login lockout 50
Login lockout time for console and telnet logins set to 50.
Console> (enable) show authentication

Login Authentication:  Console Session   Telnet Session    Http Session
---------------------  ----------------  ----------------  ----------------
tacacs                 disabled          disabled          disabled
radius                 disabled          disabled          disabled
kerberos               disabled          disabled          disabled
local                  enabled(primary)  enabled(primary)  enabled(primary)
attempt limit          5                 5                 -
lockout timeout (sec)  50                50                -

Enable Authentication: Console Session   Telnet Session    Http Session
---------------------- ----------------- ----------------  ----------------
tacacs                 disabled          disabled          disabled
radius                 disabled          disabled          disabled
kerberos               disabled          disabled          disabled
local                  enabled(primary)  enabled(primary)  enabled(primary)
attempt limit          3                 3                 -
lockout timeout (sec)  disabled          disabled          -
Console> (enable)
```

イネーブル モードのログイン認証試行回数の設定

イネーブル モードのログイン認証を設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	イネーブル モードのログイン試行回数制限をイネーブルにします。コンソール ポート接続または Telnet 接続に限ってログイン認証をイネーブルにする場合は、**console** または **telnet** キーワードを指定します。	**set authentication enable attempt** {*count*} [**console** | **telnet**]
ステップ 2	イネーブル モードのログイン ロックアウト時間をイネーブルにします。コンソール ポート接続または Telnet 接続に限ってログイン認証をイネーブルにする場合は、**console** または **telnet** キーワードを指定します。	**set authentication enable lockout** {*time*} [**console** | **telnet**]
ステップ 3	ローカル認証の設定を確認します。	**show authentication**

次に、イネーブル モードのログイン試行回数を 5 回に制限し、コンソール接続と Telnet 接続の両方でイネーブル モード ロックアウト時間を 50 秒に設定し、その設定を確認する例を示します。

```
Console> (enable) set authentication enable attempt 5
Enable mode authentication attempts for console and telnet logins set to 5.
Console> (enable) set authentication enable lockout 50
Enable mode lockout time for console and telnet logins set to 50.
Console> (enable) show authentication

Login Authentication:  Console Session   Telnet Session    Http Session
---------------------  ----------------  ----------------  ----------------
tacacs                 disabled          disabled          disabled
radius                 disabled          disabled          disabled
kerberos               disabled          disabled          disabled
local                  enabled(primary)  enabled(primary)  enabled(primary)
attempt limit          5                 5                 -
lockout timeout (sec)  50                50                -

Enable Authentication: Console Session   Telnet Session    Http Session
---------------------- ----------------  ----------------  ----------------
tacacs                 disabled          disabled          disabled
radius                 disabled          disabled          disabled
kerberos               disabled          disabled          disabled
local                  enabled(primary)  enabled(primary)  enabled(primary)
attempt limit          5                 5                 -
lockout timeout (sec)  50                50                -
Console> (enable)
```

ローカル認証の設定

ここでは、スイッチ上でローカル認証を設定する手順について説明します。

ローカル認証のイネーブル化

（注） ローカル ログイン認証およびイネーブル認証は、デフォルトの設定として、コンソール接続と Telnet 接続の両方でイネーブルです。デフォルト設定を変更する場合、またはローカル認証をディセーブルにしている場合を除き、次の作業は不要です。

スイッチ上でローカル認証をイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチ上でローカル ログイン認証をイネーブルにします。コンソール ポート接続または Telnet 接続に限ってローカル認証をイネーブルにする場合は、**console** キーワードまたは **telnet** キーワードを指定します。	**set authentication login local enable** [**all** | **console** | **http** | **telnet**]

	作業	コマンド
ステップ 2	スイッチ上でローカル イネーブル認証をイネーブルにします。コンソール ポート接続または Telnet 接続に限ってローカル認証をイネーブルにする場合は、**console** キーワードまたは **telnet** キーワードを指定します。	**set authentication enable local enable** [**all** | **console** | **http** | **telnet**]
ステップ 3	ローカル認証の設定を確認します。	**show authentication**

次に、ローカル ログインをイネーブルに設定し、コンソール接続と Telnet 接続の両方で認証をイネーブルにして、その設定を確認する例を示します。

```
Console> (enable) set authentication login local enable
local login authentication set to enable for console and telnet session.
Console> (enable) set authentication enable local enable
local enable authentication set to enable for console and telnet session.
Console> (enable) show authentication

Login Authentication:  Console Session   Telnet Session
---------------------  ----------------  ----------------
tacacs                 disabled          disabled
radius                 disabled          disabled
kerberos               disabled          disabled
local                  enabled(primary)  enabled(primary)

Enable Authentication: Console Session   Telnet Session
---------------------- ----------------- ----------------
tacacs                 disabled          disabled
radius                 disabled          disabled
kerberos               disabled          disabled
local                  enabled(primary)  enabled(primary)
Console> (enable)
```

ログイン パスワードの設定

ログイン パスワードによって、ユーザ モードの CLI へのアクセスを制御します。パスワードには大文字と小文字の区別があり、任意の印刷可能な文字をスペースも含めて 19 文字まで使用できます。

（注） Release 5.4 より前のソフトウェア リリースのバージョンで設定したパスワードには、大文字と小文字の区別がありません。Release 5.4 をインストール後に、大文字と小文字の区別があるパスワードに再度設定する必要があります。

ローカル認証用にログイン パスワードを設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
アクセスのためのログイン パスワードを設定します。以前のパスワードを入力し（パスワードが設定されていない場合には **Return** キーを押し）、新しいパスワードを入力して、さらにもう一度、新しいパスワードを入力します。	**set password**

次に、スイッチ上でログイン パスワードを設定する例を示します。

```
Console> (enable) set password
Enter old password: <old_password>
Enter new password: <new_password>
Retype new password: <new_password>
Password changed.
Console> (enable)
```

イネーブル パスワードの設定

ログイン パスワードによって、ユーザ モードの CLI へのアクセスを制御します。パスワードには大文字と小文字の区別があり、任意の印刷可能な文字をスペースも含めて 19 文字まで使用できます。

（注） Release 5.4 より前のソフトウェア リリースのバージョンで設定したパスワードには、大文字と小文字の区別がありません。Release 5.4 をインストール後に、大文字と小文字の区別があるパスワードに再度設定する必要があります。

ローカル認証用にイネーブル パスワードを設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
イネーブル モードのパスワードを設定します。以前のパスワードを入力し（パスワードが設定されていない場合には **Return** キーを押し）、新しいパスワードを入力して、さらにもう一度、新しいパスワードを入力します。	**set enablepass**

次に、スイッチ上でイネーブル パスワードを設定する例を示します。

```
Console> (enable) set enablepass
Enter old password: <old_password>
Enter new password: <new_password>
Retype new password: <new_password>
Password changed.
Console> (enable)
```

ローカル認証のディセーブル化

注意 ローカル ログインまたはイネーブル認証をディセーブルにする前に、RADIUS または TACACS+ 認証が正しく設定され、機能しているかどうかを確認します。ローカル認証をディセーブルにした際に、RADIUS や TACACS+ が正しく設定されていなかった場合、または RADIUS サーバや TACACS+ サーバがオンラインでなかった場合、スイッチにログインできない可能性があります。

スイッチ上でローカル認証をディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチ上でローカル ログイン認証をディセーブルにします。コンソール ポート接続または Telnet 接続に限ってローカル認証をディセーブルにする場合は、**console** キーワードまたは **telnet** キーワードを指定します。	**set authentication login local disable** [**all** | **console** | **http** | **telnet**]
ステップ 2	スイッチ上でローカル イネーブル認証をディセーブルにします。コンソール ポート接続または Telnet 接続に限ってローカル認証をディセーブルにする場合は、**console** キーワードまたは **telnet** キーワードを指定します。	**set authentication enable local disable** [**all** | **console** | **http** | **telnet**]
ステップ 3	ローカル認証の設定を確認します。	**show authentication**

(注) RADIUS または TACACS+ 認証をイネーブルにしてから、ローカル認証をディセーブルにします。

次に、ローカル ログイン認証をディセーブルに設定し、コンソール接続と Telnet 接続の両方で認証をイネーブルにして、その設定を確認する例を示します。

```
Console> (enable) set authentication login local disable
local login authentication set to disable for console and telnet session.
Console> (enable) set authentication enable local disable
local enable authentication set to disable for console and telnet session.
Console> (enable) show authentication

Login Authentication:  Console Session   Telnet Session
---------------------  ----------------  ----------------
tacacs                 disabled          disabled
radius                 enabled(primary)  enabled(primary)
kerberos               disabled          disabled
local                  disabled          disabled

Enable Authentication: Console Session   Telnet Session
---------------------- ----------------- ----------------
tacacs                 disabled          disabled
radius                 enabled(primary)  enabled(primary)
kerberos               disabled          disabled
local                  disabled          disabled
Console> (enable)
```

パスワードの回復

ローカル認証パスワードを回復するには、次の手順に従います。ステップ 3 ～ 7 は、いったん電源を切ってから再投入したあと、30 秒以内に行う必要があります。そうでない場合は、パスワードの回復に失敗します。ログイン パスワードとイネーブル パスワードを両方とも忘れた場合には、パスワードごとに手順を繰り返してください。

パスワードを回復するには、イネーブル モードで次の作業を行います。

ステップ 1　スーパバイザ エンジンのコンソール ポートからスイッチに接続します。Telnet 接続の場合はパスワードを回復することはできません。

ステップ 2　**reset system** コマンドを入力してスイッチを再起動します。

ステップ 3　[Enter Password] のプロンプトで **Return** キーを押します（コンソール ポートに接続してから 30 秒間、ログイン パスワードは空白です）。

ステップ 4　**enable** コマンドを使用してイネーブル モードを開始します。

ステップ 5　[Enter Password] のプロンプトで **Return** キーを押します（コンソール ポートに接続してから 30 秒間、イネーブル パスワードは空白です）。

ステップ 6　**set password** コマンドまたは **set enablepass** コマンドを入力します。

ステップ 7　以前のパスワードを要求するプロンプトに対して、**Return** キーを押します。

ステップ 8　新しいパスワードを入力して確認します。

ローカル ユーザ認証の設定

ここでは、スイッチ上でローカル ユーザ認証を設定する手順について説明します。

ローカル ユーザ アカウントの作成

ローカル ユーザ アカウントおよびパスワードは 64 文字以内で、英数字を使用できます。ただし、ローカル ユーザ アカウントには、少なくとも 1 文字は英字を使用します。

スイッチ上でローカル ユーザ アカウントを作成するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	新規のローカル ユーザ アカウントを作成します。	**set localuser user** *username* **password** *pwd* **privilege** *privilege_level*
ステップ 2	ローカル ユーザ アカウントを確認します。	**show localusers**

次に、ローカル ユーザ アカウントとパスワードを作成して権限レベルを設定し、その設定を確認する例を示します。

```
Console> (enable) set localuser user picard password captain privilege 15
Added local user picard.
Console> (enable) show localusers
Local User Authentication: disabled
Username                         Privilege Level
---------                         -------------
picard                              15
Console> (enable)
```

ローカル ユーザ認証のイネーブル化

スイッチ上でローカル ユーザ認証をイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ローカル ユーザ認証をイネーブルにします。	**set localuser authentication enable**
ステップ 2	ローカル ユーザ認証の設定を確認します。	**show authentication**

次に、ローカル ユーザ アカウントを作成してローカル ユーザ認証をイネーブルにし、その設定を確認する例を示します。

```
Console> (enable) set localuser authentication enable
Local User Authentication enabled.
Console> (enable) show authentication
Login Authentication:  Console Session   Telnet Session    Http Session
---------------------  ----------------  ----------------  ----------------
tacacs                 disabled          disabled          disabled
radius                 disabled          disabled          disabled
kerberos               disabled          disabled          disabled
local  *               enabled(primary)  enabled(primary)  enabled(primary)
attempt limit          3                 3                 -
lockout timeout (sec)  disabled          disabled          -

Enable Authentication: Console Session   Telnet Session    Http Session
---------------------- ----------------  ----------------  ----------------
tacacs                 disabled          disabled          disabled
radius                 disabled          disabled          disabled
kerberos               disabled          disabled          disabled
local  *               enabled(primary)  enabled(primary)  enabled(primary)
attempt limit          3                 3                 -
lockout timeout (sec)  disabled          disabled          -
* Local User Authentication enabled.
Console> (enable)
```

ローカル ユーザ認証のディセーブル化

スイッチ上でローカル ユーザ認証をディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ローカル ユーザ認証をディセーブルにします。	**set localuser authentication disable**
ステップ 2	ローカル認証の設定を確認します。	**show authentication**

次に、スイッチのローカル ユーザ認証をディセーブルにし、設定を確認する例を示します。

```
Console> (enable) set localuser authentication disable
local user authentication set to disable.
Console> (enable) show authentication
Login Authentication:  Console Session   Telnet Session    Http Session
---------------------  ----------------  ----------------  ----------------
tacacs                 disabled          disabled          disabled
radius                 disabled          disabled          disabled
kerberos               disabled          disabled          disabled
local  *               enabled(primary)  enabled(primary)  enabled(primary)
attempt limit          3                 3                 -
lockout timeout (sec)  disabled          disabled          -

Enable Authentication: Console Session   Telnet Session    Http Session
---------------------- ----------------- ----------------  ----------------
tacacs                 disabled          disabled          disabled
radius                 disabled          disabled          disabled
kerberos               disabled          disabled          disabled
local  *               enabled(primary)  enabled(primary)  enabled(primary)
attempt limit          3                 3                 -
lockout timeout (sec)  disabled          disabled          -
* Local User Authentication disabled.
Console> (enable)
```

ローカル ユーザ アカウントの削除

スイッチ上でローカル ユーザ アカウントを削除するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ローカル ユーザ アカウントを削除します。	**clear localuser picard**
ステップ 2	ローカル ユーザ アカウントが削除されたことを確認します。	**show localusers**

次に、スイッチのローカル ユーザ認証を削除し、設定を確認する例を示します。

```
Console> (enable) clear localuser number1
Local user cleared.
Console> (enable) show localusers
Local User Authentication: enabled
Username                        Privilege Level
---------                        -------------
picard                             15
number1                            0
worf                               15
troy                               0
Console> (enable)
```

TACACS+ 認証の設定

ここでは、スイッチ上で TACACS+ 認証を設定する手順について説明します。

TACACS+ サーバの指定

1 つまたは複数の TACACS+ サーバを指定してから、スイッチ上で TACACS+ 認証をイネーブルにします。**primary** キーワードでプライマリにするサーバを明示的に指定しないかぎり、最初に指定したサーバがプライマリ サーバになります。

1 つまたは複数の TACACS+ サーバを指定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	1 つまたは複数の TACACS+ サーバの IP アドレスを指定します。	**set tacacs server** *ip_addr* [**primary**]
ステップ 2	TACACS+ の設定を確認します。	**show tacacs**

次に、TACACS+ サーバを指定し、設定を確認する例を示します。

```
Console> (enable) set tacacs server 172.20.52.3
172.20.52.3 added to TACACS server table as primary server.
Console> (enable) set tacacs server 172.20.52.2 primary
172.20.52.2 added to TACACS server table as primary server.
Console> (enable) set tacacs server 172.20.52.10
172.20.52.10 added to TACACS server table as backup server.
Console> (enable)
Console> (enable) show tacacs

Login Authentication:  Console Session   Telnet Session
---------------------  ----------------  ----------------
tacacs                 disabled          disabled
radius                 disabled          disabled
local                  enabled(primary)  enabled(primary)

Enable Authentication: Console Session   Telnet Session
---------------------- ----------------- ----------------
tacacs                 disabled          disabled
radius                 disabled          disabled
local                  enabled(primary)  enabled(primary)
Tacacs key:
Tacacs login attempts: 3
Tacacs timeout: 5 seconds
Tacacs direct request: disabled
Tacacs-Server                             Status
----------------------------------------  -------
172.20.52.3
172.20.52.2                               primary
172.20.52.10
Console> (enable)
```

TACACS+ 認証のイネーブル化

（注） 少なくとも 1 つの TACACS+ サーバを指定してから、スイッチ上で TACACS+ 認証をイネーブルにします。TACACS+ サーバの指定方法については、「TACACS+ サーバの指定」（p.38-19）を参照してください。

スイッチに対するログイン アクセスおよびイネーブル アクセスに関して、TACACS+ 認証をイネーブルに設定できます。状況に応じて、**console** キーワードまたは **telnet** キーワードを指定すると、コンソール接続、または Telnet 接続に限って TACACS+ 認証を使用できます。RADIUS と TACACS+ の両方を使用する場合は、**primary** キーワードを使用して、スイッチに最初に TACACS+ 認証を試行させることができます。

TACACS+ 認証をイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ユーザ ログイン モードについて、TACACS+ 認証をイネーブルにします。コンソール ポート接続または Telnet 接続に限って TACACS+ 認証をイネーブルにする場合は、**console** キーワードまたは **telnet** キーワードを指定します。	**set authentication login tacacs enable** [**all** | **console** | **http** | **telnet**] [**primary**]
ステップ 2	イネーブル モードについて、TACACS+ 認証をイネーブルにします。コンソール ポート接続または Telnet 接続に限って TACACS+ 認証をイネーブルにする場合は、**console** キーワードまたは **telnet** キーワードを指定します。	**set authentication enable tacacs enable** [**all** | **console** | **http** | **telnet**] [**primary**]
ステップ 3	TACACS+ の設定を確認します。	**show authentication**

次に、コンソール接続と Telnet 接続の両方で TACACS+ 認証をイネーブルにして、設定を確認する例を示します。

```
Console> (enable) set authentication login tacacs enable
tacacs login authentication set to enable for console and telnet session.
Console> (enable) set authentication enable tacacs enable
tacacs enable authentication set to enable for console and telnet session.
Console> (enable) show authentication

Login Authentication:  Console Session   Telnet Session
---------------------  ----------------  ----------------
tacacs                 enabled(primary)  enabled(primary)
radius                 disabled          disabled
local                  enabled           enabled

Enable Authentication: Console Session   Telnet Session
---------------------- ----------------- ----------------
tacacs                 enabled(primary)  enabled(primary)
radius                 disabled          disabled
local                  enabled           enabled
Console> (enable)
```

TACACS+ 鍵の指定

（注） クライアント上で TACACS+ 鍵を設定する場合、TACACS+ サーバ上で設定されている鍵と一致させなければなりません。

TACACS+ 鍵を指定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	パケットを暗号化する鍵を指定します。	**set tacacs key** *key*
ステップ 2	TACACS+ の設定を確認します。	**show tacacs**

次に、TACACS+ 鍵を指定し、設定を確認する例を示します。

```
Console> (enable) set tacacs key Secret_TACACS_key
The tacacs key has been set to Secret_TACACS_key.
Console> (enable) show tacacs
Tacacs key: Secret_TACACS_key
Tacacs login attempts: 3
Tacacs timeout: 5 seconds
Tacacs direct request: disabled

Tacacs-Server                              Status
-----------------------------------------  -------
172.20.52.3
172.20.52.2                                primary
172.20.52.10
Console> (enable)
```

TACACS+ タイムアウト インターバルの指定

TACACS+ サーバに再送信するまでのタイムアウト インターバルを指定できます。デフォルトのタイムアウト値は 5 秒です。

TACACS+ タイムアウト インターバルを指定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	TACACS+ タイムアウト インターバルを指定します。	**set tacacs timeout** *seconds*
ステップ 2	TACACS+ の設定を確認します。	**show tacacs**

次に、サーバ タイムアウト インターバルを設定し、設定を確認する例を示します。

```
Console> (enable) set tacacs timeout 30
Tacacs timeout set to 30 seconds.
Console> (enable) show tacacs
Tacacs key: Secret_TACACS_key
Tacacs login attempts: 3
Tacacs timeout: 30 seconds
Tacacs direct request: disabled

Tacacs-Server                              Status
-----------------------------------------  -------
172.20.52.3
172.20.52.2                                primary
172.20.52.10
Console> (enable)
```

TACACS+ ログイン試行回数の指定

ログインの最大試行回数を指定できます。

ログインの最大試行回数を指定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ログインの最大試行回数を指定します。	**set tacacs attempts** *number*
ステップ 2	TACACS+ の設定を確認します。	**show tacacs**

次に、ログイン最大試行回数を指定し、設定を確認する例を示します。

```
Console> (enable) set tacacs attempts 5
Tacacs number of attempts set to 5.
Console> (enable) show tacacs
Tacacs key: Secret_TACACS_key
Tacacs login attempts: 5
Tacacs timeout: 30 seconds
Tacacs direct request: disabled
Tacacs-Server                              Status
-----------------------------------------  -------
172.20.52.3
172.20.52.2                                primary
172.20.52.10
Console> (enable)
```

TACACS+ 指定要求のイネーブル化

TACACS+ 指定要求がイネーブルの場合、設定されている TACACS+ サーバのホスト名をオプションとして指定することにより、その特定の TACACS+ サーバに TACACS+ 認証要求を渡すことができます。スイッチが通信するサーバに、ログインを試行しているユーザに対するアカウントがない場合、認証は失敗します。

TACACS+ 指定要求をイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチ上で TACACS+ 指定要求をイネーブルにします。	**set tacacs directedrequest enable**
ステップ 2	TACACS+ の設定を確認します。	**show tacacs**

次に、TACACS+ 指定要求をイネーブルにして、設定を確認する例を示します。

```
Console> (enable) set tacacs directedrequest enable
Tacacs direct request has been enabled.
Console> (enable) show tacacs
Tacacs key: Secret_TACACS_key
Tacacs login attempts: 5
Tacacs timeout: 30 seconds
Tacacs direct request: enabled

Tacacs-Server                              Status
-----------------------------------------  -------
172.20.52.3
172.20.52.2                                primary
172.20.52.10
Console> (enable)
```

TACACS+ 指定要求のディセーブル化

TACACS+ 指定要求をディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチ上で TACACS+ 指定要求をディセーブルにします。	**set tacacs directedrequest disable**
ステップ 2	TACACS+ の設定を確認します。	**show tacacs**

次に、TACACS+ 指定要求をディセーブルにする例を示します。

```
Console> (enable) set tacacs directedrequest disable
Tacacs direct request has been disabled.
Console> (enable)
```

TACACS+ サーバの消去

1 つまたは複数の TACACS+ サーバを消去するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	設定から消去する TACACS+ サーバの IP アドレスを指定します。設定からサーバをすべて消去するには、**all** キーワードを使用します。	**clear tacacs server** [*ip_addr* | **all**]
ステップ 2	TACACS+ サーバの設定を確認します。	**show tacacs**

次に、設定から特定の TACACS+ サーバを消去する例を示します。

```
Console> (enable) clear tacacs server 172.20.52.3
172.20.52.3 cleared from TACACS table
Console> (enable)
```

次に、設定からすべての TACACS+ サーバを消去する例を示します。

```
Console> (enable) clear tacacs server all
All TACACS servers cleared
Console> (enable)
```

TACACS+ 鍵の消去

TACACS+ 鍵を消去するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	TACACS+ 鍵を消去します。	**clear tacacs key**
ステップ 2	TACACS+ の設定を確認します。	**show tacacs**

次に、TACACS+ 鍵を消去する例を示します。

```
Console> (enable) clear tacacs key
TACACS server key cleared.
Console> (enable)
```

TACACS+ 認証のディセーブル化

ローカル認証がディセーブルで、TACACS+ 認証*だけが*イネーブルのときに、TACACS+ 認証をディセーブルにすると、ローカル認証が再び自動的にイネーブルになります。

TACACS+ 認証をディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ユーザ ログイン モードについて、TACACS+ 認証をディセーブルにします。コンソール ポート接続または Telnet 接続に限って TACACS+ 認証をディセーブルにする場合は、**console** キーワードまたは **telnet** キーワードを指定します。	**set authentication login tacacs disable** [**all** | **console** | **http** | **telnet**]
ステップ 2	イネーブル モードについて、TACACS+ 認証をディセーブルにします。コンソール ポート接続または Telnet 接続に限って TACACS+ 認証をディセーブルにする場合は、**console** キーワードまたは **telnet** キーワードを指定します。	**set authentication enable tacacs disable** [**all** | **console** | **http** | **telnet**]
ステップ 3	TACACS+ の設定を確認します。	**show authentication**

次に、コンソール接続と Telnet 接続の両方で TACACS+ 認証をディセーブルにして、設定を確認する例を示します。

```
Console> (enable) set authentication login tacacs disable
tacacs login authentication set to disable for console and telnet session.
Console> (enable) set authentication enable tacacs disable
tacacs enable authentication set to disable for console and telnet session.
Console> (enable) show authentication

Login Authentication:  Console Session   Telnet Session
---------------------  ----------------  ----------------
tacacs                 disabled          disabled
radius                 disabled          disabled
local                  enabled(primary)  enabled(primary)

Enable Authentication: Console Session   Telnet Session
---------------------- ----------------- ----------------
tacacs                 disabled          disabled
radius                 disabled          disabled
local                  enabled(primary)  enabled(primary)
Console> (enable)
```

RADIUS 認証の設定

ここでは、スイッチ上で RADIUS 認証を設定する手順について説明します。

RADIUS サーバの指定

1 つまたは複数の RADIUS サーバを指定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	3 つまでの RADIUS サーバの IP アドレスを指定します。**primary** キーワードを使用して、プライマリ サーバを指定します。さらにオプションとして、サーバ上で使用する宛先 UDP ポートを指定します。	**set radius server** *ip_addr* [**auth-port** *port*] [**primary**]
ステップ 2	RADIUS サーバの設定を確認します。	**show radius**

次に、RADIUS サーバを指定し、設定を確認する例を示します。

```
Console> (enable) set radius server 172.20.52.3
172.20.52.3 with auth-port 1812 added to radius server table as primary server.
Console> (enable) show radius

Login Authentication:  Console Session   Telnet Session
---------------------  ----------------  ----------------
tacacs                 disabled          disabled
radius                 disabled          disabled
local                  enabled(primary)  enabled(primary)
Enable Authentication: Console Session   Telnet Session
---------------------- ----------------- ----------------
tacacs                 disabled          disabled
radius                 disabled          disabled
local                  enabled(primary)  enabled(primary)

Radius Deadtime:              0 minutes
Radius Key:
Radius Retransmit:            2
Radius Timeout:               5 seconds

Radius-Server                 Status   Auth-port
----------------------------- -------  ------------
172.20.52.3                   primary  1812
Console> (enable)
```

RADIUS 鍵の指定

(注) クライアント上で RADIUS 鍵を指定する場合は、必ず RADIUS サーバ上で指定されている鍵と同じものにします。

RADIUS クライアントとサーバとの間のすべての通信を暗号化し、認証するために、RADIUS 鍵が使用されます。クライアントと RADIUS サーバ上では、同じ鍵を設定しなければなりません。

鍵の長さは 65 文字に制限されています。タブ以外の印字可能な任意の ASCII 文字を使用できます。

RADIUS 鍵を指定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	RADIUS サーバに送信するパケットの暗号化に使用する RADIUS 鍵を指定します。	**set radius key** *key*
ステップ 2	RADIUS の設定を確認します。	**show radius**

次に、RADIUS 鍵を指定し、設定を確認する例を示します（ユーザ モードの場合、RADIUS 鍵値は表示されません）。

```
Console> (enable) set radius key Secret_RADIUS_key
Radius key set to Secret_RADIUS_key
Console> (enable) show radius
Login Authentication:  Console Session   Telnet Session
---------------------  ----------------  ----------------
tacacs                 disabled          disabled
radius                 enabled(primary)  enabled(primary)
local                  enabled           enabled

Enable Authentication: Console Session   Telnet Session
---------------------- ----------------- ----------------
tacacs                 disabled          disabled
radius                 enabled(primary)  enabled(primary)
local                  enabled           enabled

Radius Deadtime:              0 minutes
Radius Key:                   Secret_RADIUS_key
Radius Retransmit:            2
Radius Timeout:               5 seconds

Radius-Server                 Status   Auth-port
----------------------------- -------  ------------
172.20.52.3                   primary  1812
Console> (enable)
```

RADIUS 認証のイネーブル化

（注） スイッチ上で RADIUS 認証をイネーブルにする前に、少なくとも 1 つの RADIUS サーバを指定します。RADIUS サーバの指定手順については、「RADIUS サーバの指定」（p.38-25）を参照してください。

スイッチへのログイン アクセスおよびイネーブル アクセスについて、RADIUS 認証をイネーブルにできます。必要な場合は、**console** キーワードまたは **telnet** キーワードを使用して、RADIUS 認証をコンソール接続、または Telnet 接続だけに使用するように設定できます。RADIUS と TACACS+ の両方を使用する場合は、**primary** キーワードを使用して、スイッチに最初に RADIUS 認証を試行させることができます。

RADIUS ユーザ名を設定して、RADIUS 認証をイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ユーザ ログイン モードについて、RADIUS 認証をイネーブルにします。コンソール ポート接続または Telnet 接続による試行に限って RADIUS をイネーブルにする場合は、**console** キーワードまたは **telnet** キーワードを入力します。	**set authentication login radius enable** [**all** | **console** | **http** | **telnet**] [**primary**]
ステップ 2	イネーブル モードについて、RADIUS 認証をイネーブルに設定します。コンソール ポート接続または Telnet 接続による試行に限って RADIUS をイネーブルにする場合は、**console** キーワードまたは **telnet** キーワードを入力します。	**set authentication enable radius enable** [**all** | **console** | **http** | **telnet**] [**primary**]
ステップ 3	RADIUS サーバ上で $enab15$ を作成し、このユーザにパスワードを割り当てます。	詳細については、以下の（注）を参照してください。
ステップ 4	RADIUS の設定を確認します。	**show authentication**

（注） イネーブル モードの RADIUS 認証を使用するには、RADIUS サーバ上にユーザ $enab15$ を作成し、そのユーザにパスワードを割り当てる必要があります。RADIUS サーバにユーザ名とパスワード（たとえば、ユーザ名 john、パスワード hello）を割り当てるだけでなく、このユーザも作成する必要があります。割り当てられたユーザ名およびパスワード（john/hello）を使用して Catalyst 6500 シリーズ スイッチにログインしたら、$enab15$ ユーザに割り当てられたパスワードを使用してイネーブル モードを開始できます。

RADIUS サーバが $enab15$ ユーザ名をサポートしていない場合は、RADIUS ユーザの Service-Type 属性（属性 6）を Administrative（値 6）に設定すると、個別にイネーブル パスワードを要求されることなく、直接イネーブル モードを起動できます。

次に、RADIUS 認証をイネーブルにして、設定を確認する例を示します。

```
Console> (enable) set authentication login radius enable
radius login authentication set to enable for console and telnet session.
Console> (enable) set authentication enable radius enable
radius enable authentication set to enable for console and telnet session.
Console> (enable) show authentication

Login Authentication:  Console Session   Telnet Session
---------------------  ----------------  ----------------
tacacs                 disabled          disabled
radius                 enabled(primary)  enabled(primary)
local                  enabled           enabled

Enable Authentication: Console Session   Telnet Session
---------------------- ----------------- ----------------
tacacs                 disabled          disabled
radius                 enabled(primary)  enabled(primary)
local                  enabled           enabled
Console> (enable)
```

RADIUS タイムアウト インターバルの指定

RADIUS サーバに再送信するまでのタイムアウト インターバルを指定できます。デフォルトのタイムアウト値は 5 秒です。

RADIUS のタイムアウト インターバルを指定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	RADIUS タイムアウト インターバルを指定します。	**set radius timeout** *seconds*
ステップ 2	RADIUS の設定を確認します。	**show radius**

次に、RADIUS タイムアウト インターバルを設定し、設定を確認する例を示します。

```
Console> (enable) set radius timeout 10
Radius timeout set to 10 seconds.
Console> (enable) show radius

Login Authentication:  Console Session   Telnet Session
---------------------  ----------------  ----------------
tacacs                 disabled          disabled
radius                 enabled(primary)  enabled(primary)
local                  enabled           enabled

Enable Authentication: Console Session   Telnet Session
---------------------- ----------------- ----------------
tacacs                 disabled          disabled
radius                 enabled(primary)  enabled(primary)
local                  enabled           enabled

Radius Deadtime:              0 minutes
Radius Key:                   Secret_RADIUS_key
Radius Retransmit:            2
Radius Timeout:               10 seconds

Radius-Server                 Status   Auth-port
----------------------------- -------  ------------
172.20.52.3                   primary  1812
Console> (enable)
```

RADIUS 再送信試行回数の指定

スイッチが RADIUS サーバとの接続を試行する最大回数を指定できます。この回数を超えると、設定済みの次のサーバとの接続が試行されます。デフォルトの設定では、各 RADIUS サーバとの接続は 2 回試行されます。

RADIUS の再送信試行回数を指定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	RADIUS サーバ再送信試行回数を指定します。	**set radius retransmit** *count*
ステップ 2	RADIUS の設定を確認します。	**show radius**

次に、RADIUS 再送信試行回数を指定し、設定を確認する例を示します。

```
Console> (enable) set radius retransmit 4
Radius retransmit count set to 4.
Console> (enable) show radius

Login Authentication:  Console Session   Telnet Session
---------------------  ----------------  ----------------
tacacs                 disabled          disabled
radius                 enabled(primary)  enabled(primary)
local                  enabled           enabled
Enable Authentication: Console Session   Telnet Session
---------------------- ----------------- ----------------
tacacs                 disabled          disabled
radius                 enabled(primary)  enabled(primary)
local                  enabled           enabled

Radius Deadtime:              0 minutes
Radius Key:                   Secret_RADIUS_key
Radius Retransmit:            4
Radius Timeout:               10 seconds

Radius-Server                 Status   Auth-port
----------------------------- -------  ------------
172.20.52.3                   primary  1812
Console> (enable)
```

RADIUS 待機時間の指定

RADIUS サーバが認証要求に応答しなかった場合、待機時間によって指定された期間は待機状態であるというマークをそのサーバに付けるように、スイッチを設定できます。待機時間内に受信された認証要求はいずれも（そのスイッチへのログインを試行している他のユーザなど）、待機状態とマークされた RADIUS サーバには送信されません。待機時間を設定しておけば、待機状態の RADIUS サーバへの再送信やタイムアウトを省くことができるため、認証プロセスを高速化できます。

1 つの RADIUS サーバだけを設定した場合、または設定されたサーバがすべて待機状態とマークされている場合、使用可能な代替サーバがないため、待機時間は無視されます。

RADIUS 待機時間を設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	RADIUS サーバの待機時間を指定します。	**set radius deadtime** *minutes*
ステップ 2	RADIUS の設定を確認します。	**show radius**

次に、RADIUS 待機時間を設定し、設定を確認する例を示します。

```
Console> (enable) set radius deadtime 5
Radius deadtime set to 5 minute(s)
Console> (enable) show radius

Login Authentication:  Console Session   Telnet Session
---------------------  ----------------  ----------------
tacacs                 disabled          disabled
radius                 enabled(primary)  enabled(primary)
local                  enabled           enabled

Enable Authentication: Console Session   Telnet Session
---------------------- ----------------- ----------------
tacacs                 disabled          disabled
radius                 enabled(primary)  enabled(primary)
local                  enabled           enabled

Radius Deadtime:              5 minutes
Radius Key:                   Secret_RADIUS_key
Radius Retransmit:            4
Radius Timeout:               10 seconds

Radius-Server                 Status   Auth-port
----------------------------- -------  ------------
172.20.52.3                   primary  1812
172.20.52.2                            1812
Console> (enable)
```

RADIUS サーバのオプションの属性の指定

RADIUS ACCESS_REQUEST パケットにオプションの属性を指定できます。**set radius attribute** コマンドによって、Framed-IP address、NAS-Port、Called-Station-Id、Calling-Station-Id などの特定の属性オプションの伝送を指定できます。属性の伝送の設定は、属性番号または属性名で行えます。属性の伝送は、デフォルトでディセーブルに設定されています。

（注） Release 7.5(1) では、Framed-IP address（属性 8）だけをサポートしています。

RADIUS サーバのオプション属性を指定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	RADIUS サーバのオプション属性を指定します。	**set radius attribute** [*number* | *name*] **include-in-access-req** [**enable** | **disable**]
ステップ 2	RADIUS の設定を確認します。	**show radius**

次に、Framed-IP address 属性を番号で指定してイネーブルにし、設定を確認する例を示します。

```
Console> (enable) set radius attribute 8 include-in-access-req enable
Transmission of Framed-ip address in access-request packet is enabled.
Console> (enable) show radius
RADIUS Deadtime:              0 minutes
RADIUS Key:                   123456
RADIUS Retransmit:            2
RADIUS Timeout:               5 seconds
Framed-Ip Address Transmit:   Enabled

RADIUS-Server                 Status   Auth-port     Acct-port
----------------------------- -------  ------------  ------------
10.6.140.230                  primary  1812          1813
Console> (enable)
```

次に、Framed-IP address 属性を名前で指定してディセーブルにする例を示します。

```
Console> (enable) set radius attribute framed-ip-address include-in-access-req disable
Transmission of Framed-ip address in access-request packet is disabled.
Console> (enable)
```

RADIUS サーバの消去

1 つまたは複数の RADIUS サーバを消去するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	設定から消去する RADIUS サーバの IP アドレスを指定します。設定からサーバをすべて消去するには、**all** キーワードを使用します。	**clear radius server** [*ip_addr* | **all**]
ステップ 2	RADIUS サーバの設定を確認します。	**show radius**

次に、設定から単一の RADIUS サーバを消去する例を示します。

```
Console> (enable) clear radius server 172.20.52.3
172.20.52.3 cleared from radius server table.
Console> (enable)
```

次に、設定からすべての RADIUS サーバを消去する例を示します。

```
Console> (enable) clear radius server all
All radius servers cleared from radius server table.
Console> (enable)
```

RADIUS 鍵の消去

RADIUS 鍵を消去するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	RADIUS 鍵を消去します。	**clear radius key**
ステップ 2	RADIUS の設定を確認します。	**show radius**

次に、RADIUS 鍵を消去し、設定を確認する例を示します。

```
Console> (enable) clear radius key
Radius key cleared.
Console> (enable) show radius

Login Authentication:  Console Session   Telnet Session
---------------------  ----------------  ----------------
tacacs                 disabled          disabled
radius                 disabled          disabled
local                  enabled(primary)  enabled(primary)

Enable Authentication: Console Session   Telnet Session
---------------------- ----------------- ----------------
tacacs                 disabled          disabled
radius                 disabled          disabled
local                  enabled(primary)  enabled(primary)

Radius Deadtime:              0 minutes
Radius Key:
Radius Retransmit:            2
Radius Timeout:               5 seconds

Radius-Server                 Status   Auth-port
----------------------------- -------  ------------
172.20.52.3                   primary  1812
Console> (enable)
```

RADIUS 認証のディセーブル化

ローカル認証がディセーブルで、RADIUS 認証*だけが*イネーブルのときに、RADIUS 認証をディセーブルにすると、ローカル認証が自動的に再びイネーブルになります。

RADIUS 認証をディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ログイン モードについて、RADIUS 認証をディセーブルにします。	**set authentication login radius disable** [**all** | **console** | **http** | **telnet**]
ステップ 2	イネーブル モードについて、RADIUS 認証をディセーブルにします。	**set authentication enable radius disable** [**all** | **console** | **http** | **telnet**]
ステップ 3	RADIUS の設定を確認します。	**show authentication**

次に、RADIUS 認証をディセーブルにして、設定を確認する例を示します。

```
Console> (enable) set authentication login radius disable
radius login authentication set to disable for console and telnet session.
Console> (enable) set authentication enable radius disable
radius enable authentication set to disable for console and telnet session.
Console> (enable) show authentication

Login Authentication:  Console Session   Telnet Session
---------------------  ----------------  ----------------
tacacs                 disabled          disabled
radius                 disabled          disabled
local                  enabled(primary)  enabled(primary)

Enable Authentication: Console Session   Telnet Session
---------------------- ----------------- ----------------
tacacs                 disabled          disabled
radius                 disabled          disabled
local                  enabled(primary)  enabled(primary)
Console> (enable)
```

Kerberos 認証の設定

ここでは、スイッチ上で Kerberos 認証を設定する手順について説明します。

Kerberos サーバの設定

スイッチ上の認証方式として Kerberos を使用するには、先に Kerberos サーバを設定する必要があります。KDC 用のデータベースを作成し、そのデータベースにスイッチを追加してください。

（注） Kerberos 認証を使用するには、Network Time Protocol（NTP）がイネーブルになっている必要があります。また、Domain Name System（DNS; ドメイン ネーム システム）をイネーブルにすることも推奨します。

Kerberos サーバを設定するには、次の手順を実行します。

ステップ 1　Kerberos サーバの鍵テーブルにスイッチを入力する前に、KDC が使用するためのデータベースを作成しなければなりません。次の例では、CISCO.EDU というデータベースを作成します。

```
/usr/local/sbin/kdb5_util create -r CISCO.EDU -s
```

ステップ 2　データベースにスイッチを追加します。次の例では、Cat6509 というスイッチを CISCO.EDU データベースに追加します。

```
ank host/Cat6509.cisco.edu@CISCO.EDU
```

ステップ 3　次のようにユーザ名を追加します。

```
ank user1@CISCO.EDU
```

ステップ 4　次のように管理プリンシパルを追加します。

```
ank user1/admin@CISCO.EDU
```

ステップ 5　次のように **admin.local ktadd** コマンドを使用して、データベースにスイッチ用のエントリを作成します。

```
ktadd host/Cat6509.cisco.edu@CISCO.EDU
```

ステップ 6　スイッチがアクセスできる場所に KEYTAB ファイルを移します。

ステップ 7　次のように KDC サーバを起動します。

```
/usr/local/sbin/krb5kdc
    /usr/local/sbin/kadmind
```

Kerberos のイネーブル化

Kerberos 認証をイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	認証方式として Kerberos を指定します。	**set authentication login kerberos enable** [**all** | **console** | **http** | **telnet**] [**primary**]
ステップ 2	設定を確認します。	**show authentication**

次に、Telnet ログイン認証方式として Kerberos をイネーブルにし、設定を確認する例を示します。

```
kerberos> (enable) set authentication login kerberos enable telnet
kerberos login authentication set to enable for telnet session.
kerberos> (enable) show authentication

Login Authentication: Console Session   Telnet Session
---------------------  ----------------  ----------------
tacacs                 disabled          disabled
radius                 disabled          disabled
kerberos               disabled          enabled(primary)
local                  enabled(primary)  enabled

Enable Authentication:Console Session   Telnet Session
---------------------- ----------------- ----------------
tacacs                 disabled          disabled
radius                 disabled          disabled
kerberos               disabled          enabled(primary)
local                  enabled(primary)  enabled
kerberos> (enable)
```

次に、コンソールのログイン認証方式として Kerberos をイネーブルにし、設定を確認する例を示します。

```
kerberos> (enable) set authentication login kerberos enable console
kerberos login authentication set to enable for console session.
kerberos> (enable) show authentication

Login Authentication: Console Session   Telnet Session
--------------------  ----------------  ----------------
tacacs                disabled          disabled
radius                disabled          disabled
kerberos              enabled(primary)  enabled(primary)
local                 enabled           enabled

Enable Authentication:Console Session   Telnet Session
--------------------- ----------------- ----------------
tacacs                disabled          disabled
radius                disabled          disabled
kerberos              enabled(primary)  enabled(primary)
local                 enabled           enabled
kerberos> (enable)
```

Kerberos ローカル レルムの定義

Kerberos レルムは、Kerberos サーバに登録されたユーザ、ホスト、およびネットワーク サービスで構成されるドメインです。Kerberos データベースで定義されたユーザを認証するために、スイッチは KDC が稼働しているホストのホスト名または IP アドレス、および Kerberos レルム名を認識している必要があります。

スイッチが特定の Kerberos レルムで KDC の認証を受けるように設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
スイッチのデフォルト レルムを定義します。	**set kerberos local-realm** *kerberos_realm*

（注） レルムは必ず大文字で入力してください。レルムを小文字で入力すると、Kerberos はユーザを認証しません。

次に、ローカル レルムを定義し、設定を確認する例を示します。

```
kerberos> (enable) set kerberos local-realm CISCO.COM
Kerberos local realm for this switch set to CISCO.COM.
kerberos> (enable) show kerberos
Kerberos Local Realm:CISCO.COM
Kerberos server entries:
Realm:CISCO.COM,  Server:187.0.2.1,  Port:750

Kerberos Domain<->Realm entries:
Domain:cisco.com,  Realm:CISCO.COM

Kerberos Clients NOT Mandatory
Kerberos Credentials Forwarding Enabled
Kerberos Pre Authentication Method set to None
Kerberos config key:
Kerberos SRVTAB Entries
Srvtab Entry 1:host/niners.cisco.com@CISCO.COM 0 932423923 1 1 8 01;;8>00>50;0=0=0
kerberos> (enable)
```

Kerberos サーバの指定

特定の Kerberos レルムで使用する KDC をスイッチに対して指定できます。任意で、KDC にモニタさせるポート番号も指定できます。入力した Kerberos サーバ情報は、1 つの Kerberos レルムに対して 1 エントリとして、テーブルで維持されます。テーブルの最大エントリ数は 100 です。

Kerberos サーバを指定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	特定の Kerberos レルムで使用する KDC を指定します。任意で、KDC にモニタさせるポート番号を入力します(デフォルトのポート番号は 750 です)。	**set kerberos server** *kerberos_realm* {*hostname* | *ip_address*} [*port*]
ステップ 2	Kerberos サーバ エントリを消去します。	**clear kerberos server** *kerberos_realm* {*hostname* | *ip_address*} [*port*]

次に、特定の Kerberos レルムで KDC として動作する Kerberos サーバを指定し、エントリを消去する例を示します。

```
kerberos> (enable) set kerberos server CISCO.COM 187.0.2.1 750
Kerberos Realm-Server-Port entry set to:CISCO.COM - 187.0.2.1 - 750
kerberos> (enable)

Console> (enable) clear kerberos server CISCO.COM 187.0.2.1 750
Kerberos Realm-Server-Port entry CISCO.COM-187.0.2.1-750  deleted
Console> (enable)
```

Kerberos レルムとホスト名または DNS ドメインのマッピング

任意で、ホスト名または DNS ドメインと Kerberos レルムをマッピングすることができます。

Kerberos レルムをホスト名または DNS ドメインにマッピングするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	(任意) ホスト名または DNS ドメインと Kerberos レルムをマッピングします。	**set kerberos realm** {*dns_domain* | *host*} *kerberos_realm*
ステップ 2	Kerberos レルムとドメインまたはホストとのマッピング エントリを消去します。	**clear kerberos realm** {*dns_domain* | *host*} *kerberos_realm*

次に、Kerberos レルムを DNS ドメインにマッピングし、エントリを消去する例を示します。

```
Console> (enable) set kerberos realm CISCO CISCO.COM
Kerberos DnsDomain-Realm entry set to CISCO - CISCO.COM
Console> (enable)

Console> (enable) clear kerberos realm CISCO CISCO.COM
Kerberos DnsDomain-Realm entry CISCO - CISCO.COM deleted
Console> (enable)
```

SRVTAB ファイルのコピー

リモート ユーザが Kerberos の証明書を使用して、スイッチの認証を受けることができるようにするには、スイッチと KDC 間で秘密鍵を共有しなければなりません。そのためには、KDC に保存されているファイルの鍵のコピーをスイッチに与える必要があります。このファイルをスイッチでは SRVTAB ファイル、サーバでは KEYTAB ファイルといいます。

Kerberos レルム内のホストに SRVTAB ファイルをコピーする方法としては、ファイルを物理メディアにコピーして、各ホストを回り、手動でシステムにファイルをコピーするのが最も安全です。物理メディア ドライブを備えていないスイッチに SRVTAB ファイルをコピーするには、Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）を使用し、ネットワークを介してファイルを転送する必要があります。

スイッチから KDC に SRVTAB ファイルをコピーする場合、スイッチがファイル内の情報を解析し、Kerberos SRVTAB エントリ フォーマットで実行コンフィギュレーションに保存します。スイッチに SRVTAB を直接入力する場合は、スイッチ上の Kerberos プリンシパル（サービス）ごとに 1 つずつエントリを作成します。エントリは SRVTAB テーブルで維持されます。テーブルの最大サイズは 20 エントリです。

KDC からスイッチが SRVTAB ファイルを取得するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	KDC から特定の SRVTAB ファイルを取得します。	**set kerberos srvtab remote** {*hostname* | *ip_address*} *filename*
ステップ 2	（任意）スイッチに SRVTAB を直接入力します。	**set kerberos srvtab entry** *kerberos_principal principal_type timestamp key_version number key_type key_length encrypted_keytab*

次に、KDC から SRVTAB ファイルを取得し、スイッチに SRVTAB を直接入力し、設定を確認する例を示します。

```
kerberos> (enable) set kerberos srvtab remote 187.20.32.10
/users/jdoe/krb5/ninerskeytab
kerberos> (enable)

kerberos> (enable) set kerberos srvtab entry host/niners.cisco.com@CISCO.COM 0
932423923 1 1 8 03;;5>00>50;0=0=0
Kerberos SRVTAB entry set to
Principal:host/niners.cisco.com@CISCO.COM
Principal Type:0
Timestamp:932423923
Key version number:1
Key type:1
Key length:8
Encrypted key tab:03;;5>00>50;0=0=0

kerberos> (enable) show kerberos
Kerberos Local Realm:CISCO.COM
Kerberos server entries:
Realm:CISCO.COM,  Server:187.0.2.1,  Port:750
Realm:CISCO.COM,  Server:187.20.2.1,  Port:750

Kerberos Domain<->Realm entries:
Domain:cisco.com,  Realm:CISCO.COM

Kerberos Clients NOT Mandatory
Kerberos Credentials Forwarding Enabled
Kerberos Pre Authentication Method set to None
Kerberos config key:
Kerberos SRVTAB Entries
Srvtab Entry 1:host/niners.cisco.com@CISCO.COM 0 932423923 1 1 8 03;;5>00>50;0=0=0
Srvtab Entry 2:host/niners.cisco.edu@CISCO.EDU 0 933974942 1 1 8 00?58:127:223=:;9
Console> (enable)
```

SRVTAB エントリの削除

SRVTAB エントリを削除にするには、イネーブル モードで次の作業を行います。

作業	コマンド
特定の Kerberos プリンシパルに対する SRVTAB エントリを削除します。	**clear kerberos srvtab entry** *kerberos_principal principal_type*

次に、SRVTAB エントリを削除する例を示します。

```
kerberos> (enable) clear kerberos srvtab entry host/niners.cisco.com@CISCO.COM 0
kerberos> (enable)
```

証明書転送のイネーブル化

Kerberos 対応スイッチの認証を受けたユーザは、TGT が与えられ、その TGT を使用してネットワーク上のホストの認証を受けることができます。ただし、転送が禁止されている場合、ユーザがホストの認証を受けたあとで証明書を表示しようとすると、Kerberos の証明書が存在しないことを示す出力になります。

証明書を転送できるようにするには、ユーザがスイッチの認証を受けたあとで、Kerberos 対応 Telnet を使用して、スイッチから Kerberos 対応リモート ホストへ、ユーザの TGT を転送するようにスイッチを設定します。

セキュリティを強化する手段として、ユーザがスイッチの認証を受けたあとで、Kerberos 対応のクライアントを使用しなければ、そのユーザがネットワーク上の他のサービスに対して認証を得られないようにスイッチを設定できます。Kerberos 認証を必須にしなかった場合、Kerberos 認証が得られないと、アプリケーションはそのネットワーク サービスでデフォルトの認証方式を使用して、ユーザを認証しようとします。たとえば、Telnet の場合はパスワードを要求します。

クライアントが Kerberos レルム内の他のホストに接続するときに、ユーザの証明書を転送するように設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	Kerberos 認証に成功した場合に、すべてのクライアントがユーザ証明書を転送できるようにします。	**set kerberos credentials forward**
ステップ 2	（任意）リモート サーバに対してクライアントが認証を受けられなかった場合に、Telnet が失敗するように設定します。	**set kerberos clients mandatory**

次に、ユーザの証明書を転送するようにクライアントを設定し、その設定を確認する例を示します。

```
kerberos> (enable) set kerberos credentials forward
Kerberos credentials forwarding enabled
kerberos> (enable) show kerberos
Kerberos Local Realm:CISCO.COM
Kerberos server entries:
Realm:CISCO.COM,  Server:187.0.2.1,  Port:750
Realm:CISCO.COM,  Server:187.20.2.1, Port:750

Kerberos Domain<->Realm entries:
Domain:cisco.com,  Realm:CISCO.COM

Kerberos Clients NOT Mandatory
Kerberos Credentials Forwarding Enabled
Kerberos Pre Authentication Method set to None
Kerberos config key:
Kerberos SRVTAB Entries
Srvtab Entry 1:host/aspen-niners.cisco.edu@CISCO.EDU 0 933974942 1 1 8
00?91:107:423=:;9
kerberos> (enable)
```

次に、他のネットワーク サービスの認証を受けるユーザに Kerberos クライアントが必須となるように、スイッチを設定する例を示します。

```
Console> (enable) set kerberos clients mandatory
Kerberos clients set to mandatory
Console> (enable)
```

証明書転送のディセーブル化

証明書転送をディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
証明書転送の設定をディセーブルにします。	**clear kerberos credentials forward**

次に、証明書転送の設定をディセーブルにし、設定を確認する例を示します。

```
Console> (enable) clear kerberos credentials forward
Kerberos credentials forwarding disabled
Console> (enable) show kerberos
Kerberos Local Realm not configured
Kerberos server entries:

Kerberos Domain<->Realm entries:

Kerberos Clients NOT Mandatory
Kerberos Credentials Forwarding Disabled
Kerberos Pre Authentication Method set to None
Kerberos config key:
Kerberos SRVTAB Entries
Console> (enable)
```

Kerberos クライアント必須の設定を消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
Kerberos クライアント必須の設定を消去します。	**clear kerberos clients mandatory**

次に、クライアント必須の設定を消去し、設定を確認する例を示します。

```
Console> (enable) clear kerberos clients mandatory
Kerberos clients mandatory cleared
Console> (enable) show kerberos
Kerberos Local Realm not configured
Kerberos server entries:

Kerberos Domain<->Realm entries:

Kerberos Clients NOT Mandatory
Kerberos Credentials Forwarding Disabled
Kerberos Pre Authentication Method set to None
Kerberos config key:
Kerberos SRVTAB Entries
Console> (enable)
Kerberos server entries:

Kerberos Domain<->Realm entries:

Kerberos Clients Mandatory
Kerberos Credentials Forwarding Disabled
Kerberos Pre Authentication Method set to Encrypted Unix Time Stamp
Kerberos config key:
Kerberos SRVTAB Entries
Console> (enable)
```

プライベート DES 鍵の定義および消去

スイッチ用のプライベート DES 鍵を定義できます。プライベート DES 鍵を使用すると、スイッチが KDC と共有する秘密鍵が暗号化され、**show kerberos** コマンドの実行時に、秘密鍵がクリア テキストで表示されなくなります。鍵の長さは 8 文字以下にしなければなりません。

DES 鍵を定義するには、イネーブル モードで次の作業を行います。

作業	コマンド
スイッチ用の DES 鍵を定義します。	**set key config-key** *string*

次に、DES 鍵を定義し、設定を確認する例を示します。

```
kerberos> (enable) set key config-key abcd
Kerberos config key set to abcd
kerberos> (enable) show kerberos
Kerberos Local Realm:CISCO.COM
Kerberos server entries:
Realm:CISCO.COM,  Server:170.20.2.1,  Port:750
Realm:CISCO.COM,  Server:172.20.2.1,  Port:750

Kerberos Domain<->Realm entries:
Domain:cisco.com,  Realm:CISCO.COM

Kerberos Clients Mandatory
Kerberos Credentials Forwarding Disabled
Kerberos Pre Authentication Method set to Encrypted Unix Time Stamp
Kerberos config key:abcd
Kerberos SRVTAB Entries
Srvtab Entry 1:host/aspen-niners.cisco.edu@CISCO.EDU 0 933974942 1 1 8
12151><88?=>>3>11
kerberos> (enable)
```

DES 鍵を消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
スイッチから DES 鍵を消去します。	**clear key config-key** *string*

次に、DES 鍵を消去する例を示します。

```
Console> (enable) clear key config-key
Kerberos config key cleared
Console> (enable)
```

Telnet セッションの暗号化

Kerberos を使用してスイッチの認証を受けたユーザが、別のスイッチまたはホストに Telnet でアクセスする場合に、それが Kerberos 対応の Telnet になるかどうかは、Telnet サーバで使用している認証方式によって決まります。Telnet サーバが認証に Kerberos を使用している場合は、Telnet セッションが続いている間、あらゆるアプリケーション データ パケットを暗号化することを選択できます。Telnet セッションを暗号化するには、**telnet** コマンドで **encrypt kerberos** オプションを選択します。

Telnet セッションを暗号化するには、次の作業を行います。

作業	コマンド
Telnet セッションを暗号化します。	**telnet encrypt kerberos** *host*

次に、Kerberos 認証および暗号化対応として Telnet セッションを設定する例を示します。

```
Console> (enable) telnet encrypt kerberos
```

Kerberos 設定の表示および消去

次のコマンドを使用すると、スイッチの Kerberos 設定を表示または消去することができます。

- **show kerberos**
- **show kerberos creds**
- **clear kerberos creds**

Kerberos 設定を表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
Kerberos 設定を表示します。	**show kerberos**

次に、Kerberos 設定を表示する例を示します。

```
kerberos> (enable) show kerberos
Kerberos Local Realm:CISCO.COM
Kerberos server entries:
Realm:CISCO.COM,  Server:187.0.2.1,  Port:750
Realm:CISCO.COM,  Server:187.20.2.1,  Port:750

Kerberos Domain<->Realm entries:
Domain:cisco.com,  Realm:CISCO.COM
Kerberos Clients NOT Mandatory
Kerberos Credentials Forwarding Enabled
Kerberos Pre Authentication Method set to None
Kerberos config key:
Kerberos SRVTAB Entries
Srvtab Entry 1:host/niners.cisco.com@CISCO.COM 0 932423923 1 1 8 03;;5>00>50;0=0=0
Srvtab Entry 2:host/niners.cisco.edu@CISCO.EDU 0 933974942 1 1 8 00?58:127:223=:;9
kerberos> (enable)
```

Kerberos 証明書を表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
Kerberos 証明書を表示します。	**show kerberos creds**

次に、Kerberos 証明書を表示する例を示します。

```
Console> (enable) show kerberos creds
No Kerberos credentials.
Console> (enable)
```

すべての Kerberos 証明書を消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
すべての証明書を消去します。	**clear kerberos creds**

次に、スイッチからすべての Kerberos 証明書を消去する例を示します。

```
Console> (enable) clear kerberos creds
Console> (enable)
```

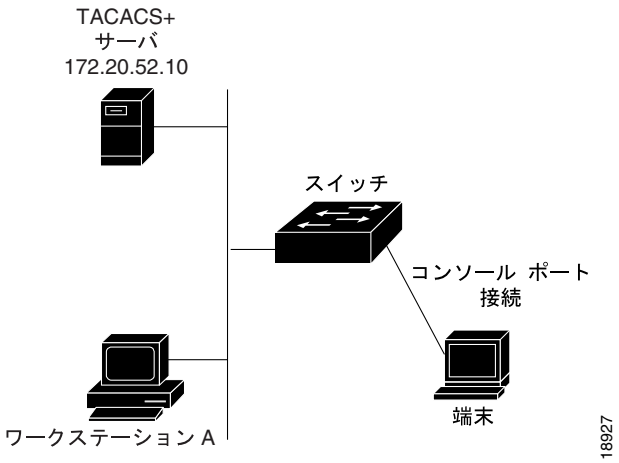
認証の例

図 38-3 に、TACACS+ を使用した単純なネットワーク トポロジーを示します。

この例では、すべての Telnet 接続において、スイッチへのログイン アクセスとイネーブル アクセスの両方について、TACACS+ 認証がイネーブルに設定され、ローカル認証がディセーブルに設定されています。ワークステーション A がスイッチに接続する場合、ユーザは TACACS+ ユーザ名およびパスワードを入力するように要求されます。

ただし、コンソール ポート上では、ログイン アクセスとイネーブル アクセスの両方について、ローカル認証だけがイネーブルに設定されます。直接接続されているターミナルにアクセスできるユーザは、ログインおよびイネーブル パスワードを使用してスイッチにアクセスできます。

図 38-3　TACACS+ ネットワーク トポロジー例



次に、Telnet 接続について TACACS+ 認証がイネーブルにされ、コンソール接続についてローカル認証がイネーブルにされ、TACACS+ 暗号化鍵が指定されるように、スイッチを設定する例を示します。

```
Console> (enable) show tacacs
Tacacs key:
Tacacs login attempts: 3
Tacacs timeout: 5 seconds
Tacacs direct request: disabled

Tacacs-Server                                Status
-------------------------------------------  -------
Console> (enable) set tacacs server 172.20.52.10
172.20.52.10 added to TACACS server table as primary server.
Console> (enable) set tacacs key tintin_et_milou
The tacacs key has been set to tintin_et_milou.
Console> (enable) set authentication login tacacs enable telnet
tacacs login authentication set to enable for telnet session.
Console> (enable) set authentication enable tacacs enable telnet
tacacs enable authentication set to enable for telnet session.
Console> (enable) set authentication login local disable telnet
local login authentication set to disable for telnet session.
Console> (enable) set authentication enable local disable telnet
local enable authentication set to disable for telnet session.
Console> (enable) show tacacs
Tacacs key: tintin_et_milou
Tacacs login attempts: 3
Tacacs timeout: 5 seconds
Tacacs direct request: disabled

Tacacs-Server                                Status
-------------------------------------------  -------
172.20.52.10                                 primary
Console> (enable)
```

許可の機能

ここでは、許可の機能について説明します。

許可の概要

Catalyst 6500 シリーズ スイッチは、TACACS+ および RADIUS 許可をサポートしています。許可機能では、ユーザ名 / パスワードのペアに基づくアクセス リスト（またはユーザ プロファイル）を動的に適用することにより、アクセスを特定のユーザに制限します。アクセス リストは、TACACS+ サーバまたは RADIUS サーバが稼働するホスト上に存在します。サーバは、アクセス リスト番号でユーザ パスワード情報に応答し、それによって特定のリストが適用されます。

許可イベント

次の内容について、許可をイネーブルにすることができます。

- コマンド — コマンドに対する許可をイネーブルに設定した場合、ユーザは特定のコマンドを実行するために有効なユーザ名 / パスワードのペアを入力しなければなりません。すべてのコマンドに許可を設定することも、コンフィギュレーション（イネーブル モード）コマンドだけに許可を設定することもできます。ユーザがコマンドを発行すると、許可サーバはそのコマンドとユーザ情報を受信し、アクセス リストと照合します。ユーザにそのコマンドを発行する権限があれば、コマンドが実行されます。そうでない場合、コマンドは実行されません。
- EXEC モード（ユーザ ログイン）— EXEC モードに対する許可をイネーブルに設定した場合、ユーザは EXEC モードにアクセスするために有効なユーザ名 / パスワードのペアを入力しなければなりません。許可機能をイネーブルに設定した場合に限り、許可が必須になります。
- イネーブル モード（イネーブル ログイン）— イネーブル モードに対する許可をイネーブルに設定した場合、ユーザはイネーブル モードにアクセスするために有効なユーザ名 / パスワードのペアを入力しなければなりません。イネーブル モードに対する許可をイネーブルに設定した場合に限り、許可が必須になります。

TACACS+ プライマリ オプションおよび代替オプション

許可プロセスで使用するプライマリ オプションと代替オプションを指定できます。使用できるオプションおよび代替オプションは、次のとおりです。

- **tacacs+** — ユーザがすでに認証されており、TACACS+ サーバから応答がない場合、許可はただちに成功します。
- **deny** — deny は常に代替オプションです。TACACS+ サーバが応答しない場合、許可は失敗します。これがデフォルトの動作です。
- **if-authenticated** — ユーザがすでに認証されており、TACACS+ サーバから応答がない場合、許可はただちに成功します。
- **none** — TACACS+ サーバが応答しない場合、許可は成功します。

TACACS+ コマンドの許可

すべてのコマンドに許可を設定することも、コンフィギュレーション（イネーブル モード）コマンドだけに許可を設定することもできます。コンフィギュレーション コマンドは、次のとおりです。

- **copy**
- **clear**
- **commit**
- **configure**
- **delete**
- **download**
- **format**
- **reload**
- **rollback**
- **session**
- **set**
- **squeeze**
- **switch**
- **undelete**

入力するすべてのコマンドについて、次に示す TACACS+ 許可プロセスが行われます。

- コマンド許可機能をディセーブルに設定すると、TACACS+ サーバはスイッチ上でのすべてのコマンド実行を許可します。
- コンフィギュレーション コマンドだけについて許可機能をイネーブルにすると、スイッチは引数として入力された文字列がここに記載したいずれかのコマンドに一致するかどうかを確認します。一致するコマンドがない場合、スイッチはそのコマンドを実行します。一致するコマンドがある場合、スイッチはそのコマンドを NAS に転送して許可を求めます。
- すべてのコマンドについて許可機能をイネーブルに設定した場合、スイッチはコマンドを NAS に転送して許可を求めます。

RADIUS 許可

RADIUS の許可機能は限られています。この認証プロトコルには、許可情報を提供する Service-Type という属性があります。この属性は、ユーザ プロファイルの一部分です。

Administrative/Shell (6) Service-Type アクセス権のないユーザが RADIUS 認証を使用してログインすると、NAS がそのユーザの認証を行い、認証が成功すれば EXEC モードにログインさせます。Administrative/Shell (6) Service-Type アクセス権のあるユーザの場合は、NAS はそのユーザの認証を行い、イネーブル モードにログインさせます。

スイッチ上での許可の設定

ここでは、許可を設定する手順について説明します。

TACACS+ 許可のデフォルト設定

表 38-3 に、TACACS+ 許可のデフォルト設定を示します。

表 38-3　許可のデフォルト設定

機能	デフォルト値
TACACS+ ログイン許可（コンソールおよび Telnet）	ディセーブル
TACACS+ EXEC 許可（コンソールおよび Telnet）	ディセーブル
TACACS+ イネーブル許可（コンソールおよび Telnet）	ディセーブル
TACACS+ コマンド許可（コンソールおよび Telnet）	ディセーブル

TACACS+ 許可の設定時の注意事項

ここでは、スイッチ上での TACACS+ 許可の設定時の注意事項について説明します。

- TACACS+ 許可は、ディセーブルがデフォルトの設定です。
- 許可の設定は、コンソール接続、Telnet 接続、または両方のタイプの接続に適用されます。
- 許可をイネーブルにするときは、モード、オプション、代替オプション、および接続タイプを指定する必要があります。
- 許可をイネーブルにする前に、RADIUS サーバおよび TACACS+ サーバの設定を行います。サーバの設定の詳細については、「TACACS+ サーバの指定」（p.38-19）または「RADIUS サーバの指定」（p.38-25）を参照してください。
- 許可をイネーブルにする前に、プロトコル パケット暗号化のための RADIUS 鍵および TACACS+ 鍵を設定します。鍵設定の詳細については、「TACACS+ 鍵の指定」（p.38-21）または「RADIUS 鍵の指定」（p.38-26）を参照してください。

TACACS+ 許可の設定

ここでは、スイッチ上で TACACS+ 許可を設定する手順について説明します。

TACACS+ 許可のイネーブル化

スイッチ上で TACACS+ 許可をイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ユーザ モードの許可をイネーブルにします。コンソール ポート接続または Telnet 接続に限って許可をイネーブルにする場合は、**console** キーワードまたは **telnet** キーワードを指定します。コンソール ポート接続および Telnet 接続の両方について許可をイネーブルにする場合は、**both** キーワードを指定します。	**set authorization exec enable** {*option*}{*fallbackoption*} [**console** | **telnet** | **both**]
ステップ 2	イネーブル モードの許可をイネーブルにします。コンソール ポート接続または Telnet 接続に限って許可をイネーブルにする場合は、**console** キーワードまたは **telnet** キーワードを指定します。コンソール ポート接続および Telnet 接続の両方について許可をイネーブルにする場合は、**both** キーワードを指定します。	**set authorization enable enable** {*option*} {*fallbackoption*} [**console** | **telnet** | **both**]
ステップ 3	コンフィギュレーション コマンドの許可をイネーブルにします。コンソール ポート接続または Telnet 接続に限って許可をイネーブルにする場合は、**console** キーワードまたは **telnet** キーワードを指定します。コンソール ポート接続および Telnet 接続の両方について許可をイネーブルにする場合は、**both** キーワードを指定します。	**set authorization commands enable** {**config** | **all**} {*option*}{*fallbackoption*} [**console** | **telnet** | **both**]
ステップ 4	TACACS+ 許可の設定を確認します。	**show authorization**

次に、コンソール ポート接続および Telnet 接続の両方で、TACACS+ による EXEC モードの許可をイネーブルにする例を示します。**tacacs+** オプションを使用して許可を設定します。代替オプションは **deny** です。

```
Console> (enable) set authorization exec enable tacacs+ deny both
Successfully enabled enable authorization.
Console>
```

次に、コンソール ポート接続および Telnet 接続の両方で、TACACS+ によるイネーブル モードの許可をイネーブルにする例を示します。**tacacs+** オプションを使用して許可を設定します。代替オプションは **deny** です。

```
Console> (enable) set authorization enable enable tacacs+ deny both
Successfully enabled enable authorization.
Console>
```

次に、コンソール ポート接続および Telnet 接続の両方で、TACACS+ コマンドの許可をイネーブルにする例を示します。**tacacs+** オプションを使用して許可を設定します。代替オプションは **deny** です。

```
Console> (enable) set authorization commands enable config tacacs+ deny both
Successfully enabled commands authorization.
Console> (enable)
```

次に、設定を確認する例を示します。

```
Console> (enable) show authorization
Telnet:
-------
            Primary   Fallback
            -------   --------
exec:       tacacs+    deny
enable:     tacacs+    deny
commands:
 config:    tacacs+    deny
 all:       -          -

Console:
--------
            Primary   Fallback
            -------   --------
exec:       tacacs+    deny
enable:     tacacs+    deny
commands:
 config:    tacacs+    deny
 all:       -          -
Console> (enable)
```

TACACS+ 許可のディセーブル化

スイッチ上で TACACS+ 許可をディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ユーザ モードの許可をディセーブルにします。コンソール ポート接続または Telnet 接続に限って許可をディセーブルにする場合は、**console** キーワードまたは **telnet** キーワードを指定します。コンソール ポート接続および Telnet 接続の両方について許可をディセーブルにする場合は、**both** キーワードを指定します。	**set authorization exec disable** [**console** | **telnet** | **both**]
ステップ 2	イネーブル モードの許可をディセーブルにします。コンソール ポート接続または Telnet 接続に限って許可をディセーブルにする場合は、**console** キーワードまたは **telnet** キーワードを指定します。コンソール ポート接続および Telnet 接続の両方について許可をディセーブルにする場合は、**both** キーワードを指定します。	**set authorization enable disable** [**console** | **telnet** | **both**]
ステップ 3	コンフィギュレーション コマンドの許可をディセーブルにします。コンソール ポート接続または Telnet 接続に限って許可をディセーブルにする場合は、**console** キーワードまたは **telnet** キーワードを指定します。コンソール ポート接続および Telnet 接続の両方について許可をディセーブルにする場合は、**both** キーワードを指定します。	**set authorization commands disable** [**console** | **telnet** | **both**]
ステップ 4	TACACS+ 許可の設定を確認します。	**show authorization**

次に、コンソール ポート接続および Telnet 接続の両方で、TACACS+ による EXEC モードの許可をディセーブルにして、設定を確認する例を示します。

```
Console> (enable) set authorization exec disable both
Successfully disabled enable authorization.
Console> (enable)
```

次に、コンソール ポート接続および Telnet 接続の両方で、TACACS+ によるイネーブル モードの許可をディセーブルにして、設定を確認する例を示します。

```
Console> (enable) set authorization enable disable both
Successfully disabled enable authorization.
Console> (enable)
```

次に、コンソール ポート接続および Telnet 接続の両方で、TACACS+ によるコマンドの許可をディセーブルにして、設定を確認する例を示します。

```
Console> (enable) set authorization commands disable both
Successfully disabled commands authorization.
Console> (enable)
```

次に、設定を確認する例を示します。

```
Console> (enable) show authorization

Telnet:
-------
            Primary   Fallback
            -------   --------
exec:       tacacs+    deny
enable:     tacacs+    deny
commands:
 config:    tacacs+    deny
 all:       -         -

Console:
--------
            Primary   Fallback
            -------   --------
exec:       tacacs+    deny
enable:     tacacs+    deny
commands:
 config:    tacacs+    deny
 all:       -         -
Console> (enable)
```

RADIUS 許可の設定

ここでは、スイッチ上で RADIUS 許可を設定する手順について説明します。

- RADIUS 許可のイネーブル化（p.38-50）
- RADIUS 許可のディセーブル化（p.38-50）

RADIUS 許可のイネーブル化

スイッチ上で RADIUS の許可と認証をイネーブルにするには、イネーブル モードで次の作業を行います。

ステップ 1　イネーブル モードで **set authentication login radius enable** コマンドを入力します。このコマンドによって、RADIUS の認証と許可が両方イネーブルになります。

ステップ 2　ユーザが RADIUS サーバでイネーブル モードを開始できるようにするため、RADIUS サーバのそのユーザの Service-Type（RADIUS 属性 6）を Administrative（値 6）に設定します。Service-Type を 6 の Administrative 以外に設定した場合（たとえば、1 の login、7 の shell、または 2 の framed）は、イネーブル プロンプトではなく、そのスイッチの EXEC プロンプトが与えられます。

RADIUS 許可のディセーブル化

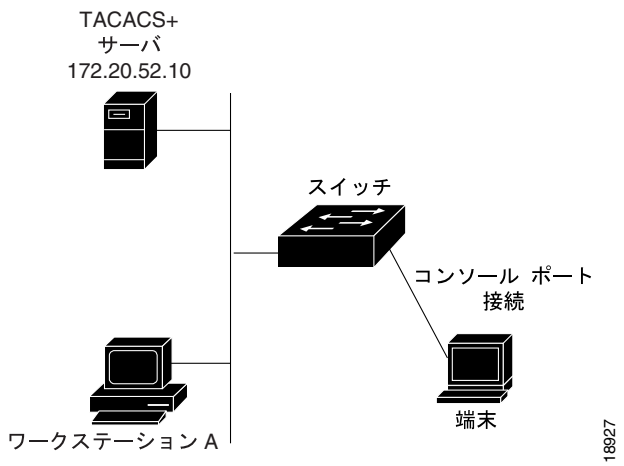
RADIUS 許可をディセーブルにするには、イネーブル モードで **set authentication login radius disable** コマンドを入力します。

許可の例

図 38-4 に、TACACS+ を使用した単純なネットワーク トポロジーを示します。

ワークステーション A がスイッチ上でコマンドの実行を試みると、スイッチはその要求を TACACS+ デーモンに登録します。TACACS+ デーモンは、そのユーザがその機能の使用を許可されているかどうかを判別し、コマンドを実行するか、またはアクセス拒否の応答を送信します。

図 38-4　TACACS+ ネットワーク トポロジー例



この例では、Telnet 接続およびコンソール ポート接続で、スイッチへのイネーブル モード アクセスと、コンフィギュレーション コマンドの入力について TACACS+ 許可をイネーブルにします。

```
Console> (enable) set authorization enable enable tacacs+ deny both
Successfully enabled enable authorization.
Console> (enable) set authorization commands enable config tacacs+ deny both
Successfully enabled commands authorization.
Console> (enable) show authorization
Telnet:
-------
            Primary   Fallback
            -------   --------
exec:       tacacs+    deny
enable:     tacacs+    deny
commands:
 config:    tacacs+    deny
 all:       -          -

Console:
--------
            Primary   Fallback
            -------   --------
exec:       tacacs+    deny
enable:     tacacs+    deny
commands:
 config:    tacacs+    deny
 all:       -          -
Console> (enable)
```

アカウンティングの機能

ここでは、各アカウンティング方式の機能について説明します。

アカウンティングの概要

スイッチへのアクセスをモニタするために、次のアカウンティング方式を設定できます。

- TACACS+ アカウンティング
- RADIUS アカウンティング

アカウンティング機能を利用して、特定のホストに対するユーザ アクティビティ、ネットワーク上での不審な接続の試み、および NAS の設定の不当な変更を追跡することができます。アカウンティング情報はアカウンティング サーバに送られ、レコードとして保存されます。アカウンティング情報には一般に、ユーザのアクション、およびアクションの継続時間が含まれます。アカウンティングは、セキュリティ、課金、およびリソース配分の目的で使用できます。

アカウンティング プロトコルは、転送プロトコルとして TCP を使用し、クライアント / サーバ モデルで動作します。NAS がクライアント、アカウンティング サーバがデーモンとして動作します。NAS はサーバにアカウンティング情報を送信します。サーバはその情報を正常に処理すると、NAS に要求の確認応答を送信します。NAS とサーバ間で行われるすべてのトランザクションは、鍵による認証が行われます。

アカウンティングをイネーブルに設定した場合、システム上でアカウンティングの対象となるイベントが発生すると、アカウンティング情報がメモリに動的に収集されます。イベントが終了すると、アカウンティング レコードが作成され、NAS に送信されます。その後、メモリからレコードが削除されます。NAS がアカウンティングのために使用するメモリの量は、並行して発生するアカウンティング対象イベントの数によって異なります。

アカウンティング イベント

次のイベント タイプのアカウンティングを設定できます。

- EXEC モード アカウンティング — NAS 上でのユーザの EXEC セッション（ユーザ ログイン セッション）に関する情報を提供します（EXEC セッションの接続時間は含まれますが、トラフィック統計情報は含まれません）。
- 接続アカウンティング — NAS からのすべての発信コネクション（Telnet、rlogin など）についての情報を提供します。

（注） ログインしてただちに接続が確立し、接続が打ち切られた場合は、EXEC　イベントと connect イベントがオーバーラップするため、イベントの開始時刻と終了時刻がほぼ同じになります。

- システム アカウンティング ― ユーザには無関係のシステム イベントに関する情報（システム リセット、システム ブート、アカウンティングのユーザ設定など）を提供します。
- コマンド アカウンティング ― ユーザが発行するコマンドごとに 1 つのレコードを送信します。この機能によって監査情報を収集できます。

アカウンティング レコードを作成する場合の指定

アカウンティング情報を収集してレコードを作成するようにスイッチを設定できます。（**set accounting** コマンドを使用して）アカウンティングを設定すると、スイッチは次の 2 種類のレコードを生成できるようになります。

- start レコード ― イベントについての部分的な情報（イベントの開始時刻、サービス タイプ、およびトラフィック統計情報）が含まれます。
- stop レコード ― イベントについての完全な情報（イベントの開始時刻、継続時間、サービス タイプ、およびトラフィック統計情報）が含まれます。

次の 2 つのイベントで、アカウンティング レコードが作成されてサーバに送信されます。

- start-stop ― アクションに継続時間がある場合、その開始時および終了時の両方でレコードが送信されます。NAS がアクションの開始時にアカウンティング レコードを送信できなかった場合にも、ユーザはアクションを続行できます。
- stop-only ― イベントの終了時にだけ、レコードが送信されます。コマンド アカウンティングの場合、各コマンドの継続時間はゼロとみなされるので、stop レコードだけが作成されます。システム イベントにはユーザは対応付けられません。したがって、**set accounting system** コマンドの **start-stop** オプションは、システム イベントについては無視されます。

（注） stop レコードには、イベントについての完全な情報（イベントの開始時刻、継続時間、およびトラフィック統計情報）が含まれます。ただし、冗長性のある設定を行う場合は、NAS 上で発生するイベントの start および stop レコードの両方をモニタすることもできます。

RADIUS サーバの指定

1 つまたは複数の RADIUS サーバを指定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	3 つまでの RADIUS サーバの IP アドレスを指定します。**primary** キーワードを使用して、プライマリ サーバを指定します。さらにオプションとして、サーバ上で使用する宛先 UDP ポートを指定します。	**set radius server** *ip_addr* [**acct-port** *port*] [**primary**]
ステップ 2	RADIUS サーバの設定を確認します。	**show radius**

次に、RADIUS サーバを指定し、設定を確認する例を示します。

```
Console> (enable) set radius server 172.20.52.3
172.20.52.3 with auth-port 1812 added to radius server table as primary server.
Console> (enable) show radius

Login Authentication:  Console Session   Telnet Session
---------------------  ----------------  ----------------
tacacs                 disabled          disabled
radius                 disabled          disabled
local                  enabled(primary)  enabled(primary)

Enable Authentication: Console Session   Telnet Session
---------------------- ----------------- ----------------
tacacs                 disabled          disabled
radius                 disabled          disabled
local                  enabled(primary)  enabled(primary)

Radius Deadtime:              0 minutes
Radius Key:
Radius Retransmit:            2
Radius Timeout:               5 seconds

Radius-Server                 Status   Auth-port
----------------------------- -------  ------------
172.20.52.3                   primary  1812
Console> (enable)
```

サーバのアップデート

スイッチが TACACS+ サーバにアカウンティング情報を送信するように設定することができます。次の 2 つのオプションがあります。

- newinfo ― 新しいアカウンティング情報が発生したときにだけ、アカウンティング情報をサーバに送信します。
- periodic ― アカウンティングのアップデート レコードを定期的にサーバに送信します。このオプションを使用すれば、NAS が再起動され、最初の start 時刻のデータが消失した場合にも、接続およびセッションについての情報が常に最新の状態に保たれます。定期的アップデートの間隔を指定する必要があります。有効な間隔は、1 ～ 71,582 分です。

アカウンティングの抑制

set accounting suppress null-username enable コマンドを使用して、ユーザ名を持たない未知のユーザがスイッチにアクセスした場合にアカウンティングを抑制するように設定することができます。

（注） RADIUS アカウンティングと TACACS+ アカウンティングはほぼ同じです。ただし、RADIUS ではコマンド アカウンティング、定期アップデート、または null-username 抑制は実行できません。

スイッチ上でのアカウンティングの設定

ここでは、TACACS+ および RADIUS でアカウンティングを設定する手順を説明します。

アカウンティングのデフォルト設定

表 38-4 に、アカウンティングのデフォルト設定を示します。

表 38-4　アカウンティングのデフォルト設定

機能	デフォルト値
アカウンティング	ディセーブル
アカウンティング イベント （EXEC、system、commands、および connect）	ディセーブル
アカウンティング レコード	stop-only

アカウンティング設定時の注意事項

ここでは、スイッチ上でのアカウンティング設定時の注意事項について説明します。

- アカウンティングをイネーブルにする前に、RADIUS サーバおよび TACACS+ サーバの設定を行います。サーバの設定の詳細については、「TACACS+ サーバの指定」（p.38-19）または「RADIUS サーバの指定」（p.38-25）を参照してください。
- アカウンティングをイネーブルにする前に、プロトコル パケット暗号化のための RADIUS 鍵および TACACS+ 鍵を設定します。鍵設定の詳細については、「TACACS+ 鍵の指定」（p.38-21）または「RADIUS 鍵の指定」（p.38-26）を参照してください。

（注）　1 つのアカウンティング イベントに割り当てられる DRAM スペースは、約 500 バイトです。アカウンティングが使用する DRAM の総スペースは、システムで*並行して発生する*アカウンティング対象イベントの数によって異なります。

アカウンティングの設定

ここでは、スイッチ上で RADIUS および TACACS+ アカウンティングを設定する手順を説明します。

アカウンティングのイネーブル化

スイッチ上でアカウンティングをイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	接続イベントについてのアカウンティングをイネーブルにします。	**set accounting connect enable** {**start-stop** | **stop-only**} {**tacacs+** | **radius**}
ステップ 2	EXEC モードについてのアカウンティングをディセーブルにします。	**set accounting exec enable** {**start-stop** | **stop-only**} {**tacacs+** | **radius**}
ステップ 3	システム イベントについてのアカウンティングをイネーブルにします。	**set accounting system enable** {**start-stop** | **stop-only**} {**tacacs+** | **radius**}
ステップ 4	コンフィギュレーション コマンドのアカウンティングをイネーブルにします。	**set accounting commands enable** {**config** | **all**} {**stop-only**} **tacacs+**
ステップ 5	未知のユーザについての情報の抑制をイネーブルにします。	**set accounting suppress null-username enable**
ステップ 6	新しい情報が発生するたびにアカウンティングをアップデートするように設定します。	**set accounting update** {**new-info** | {**periodic** [*interval*]}}
ステップ 7	アカウンティングの設定を確認します。	**show accounting**

次に、stop-only の TACACS+ アカウンティングをイネーブルにする例を示します。

```
Console> (enable) set accounting connect enable stop-only tacacs+
Accounting set to enable for connect events in stop-only mode.
Console> (enable)

Console> (enable) set accounting exec enable stop-only tacacs+
Accounting set to enable for exec events in stop-only mode.
Console> (enable)

Console> (enable) set accounting system enable stop-only tacacs+
Accounting set to enable for system events in stop-only mode.
Console> (enable)

Console> (enable) set accounting commands enable all stop-only tacacs+
Accounting set to enable for commands-all events in stop-only mode.
Console> (enable)
```

次に、未知のユーザのアカウンティングを抑制する例を示します。

```
Console> (enable) set accounting suppress null-username enable
Accounting will be suppressed for user with no username.
Console> (enable)
```

次に、サーバを定期的にアップデートする例を示します。

```
Console> (enable) set accounting update periodic 120
Accounting updates will be periodic at 120 minute intervals.
Console> (enable)
```

次に、設定を確認する例を示します。

```
Console> (enable) show accounting
Event     Method  Mode
-----     ------- ----
exec:     tacacs+ stop-only
connect:  tacacs+ stop-only
system:   tacacs+ stop-only
commands:
config:   -       -
all:      tacacs+ stop-only
TACACS+ Suppress for no username: enabled
Update Frequency: periodic, Interval = 120

Accounting information:
-----------------------
Active Accounted actions on tty0, User (null) Priv 0
Active Accounted actions on tty288091924, User (null) Priv 0
Overall Accounting Traffic:
          Starts   Stops  Active
          -----    -----  ------
Exec           0       0       0
Connect        0       0       0
Command        0       0       0
System         1       0       0
Console> (enable)
```

アカウンティングのディセーブル化

スイッチ上で RADIUS アカウンティングをディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	接続イベントについてのアカウンティングをディセーブルにします。	**set accounting connect disable**
ステップ 2	EXEC モードについてのアカウンティングをディセーブルにします。	**set accounting exec disable**
ステップ 3	システム イベントについてのアカウンティングをディセーブルにします。	**set accounting system disable**
ステップ 4	コンフィギュレーション コマンドのアカウンティングをディセーブルにします。	**set accounting commands disable**
ステップ 5	未知のユーザについての情報の抑制をディセーブルにします。	**set accounting suppress null-username disable**
ステップ 6	アカウンティングの設定を確認します。	**show accounting**

次に、stop-only のアカウンティングをディセーブルにする例を示します。

```
Console> (enable) set accounting connect disable
Accounting set to disable for connect events.
Console> (enable)

Console> (enable) set accounting exec disable
Accounting set to disable for exec events.
Console> (enable)

Console> (enable) set accounting system disable
Accounting set to disable for system events.
Console> (enable)

Console> (enable) set accounting commands disable
Accounting set to disable for commands-all events.
Console> (enable)
```

次に、未知のユーザのアカウンティングの抑制をディセーブルにする例を示します。

```
Console> (enable) set accounting suppress null-username disable
Accounting will be not be suppressed for user with no username.
Console> (enable)
```

次に、設定を確認する例を示します。

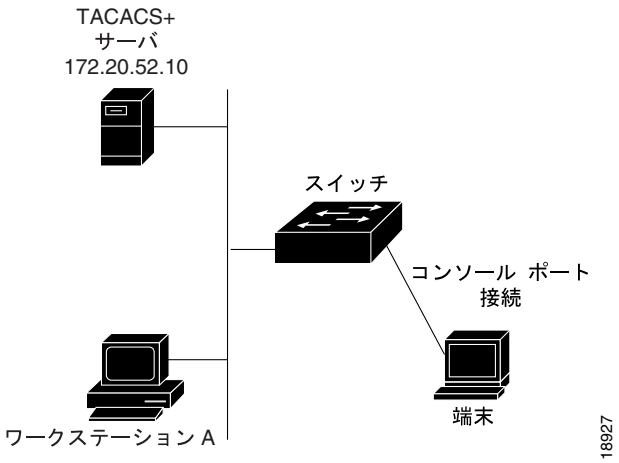
```
Console> (enable) show accounting
Event     Method  Mode
-----     ------- ----
exec:     -       -
connect:  -       -
system:   -       -
commands:
config:   -       -
all:      -       -

TACACS+ Suppress for no username: disabled
Update Frequency: new-info

Accounting information:
-----------------------
Active Accounted actions on tty0, User (null) Priv 0
Active Accounted actions on tty288091924, User (null) Priv 0
Overall Accounting Traffic:
          Starts   Stops  Active
          -----    -----  ------
Exec           0       0       0
Connect        0       0       0
Command        0       0       0
System         1       2       0
Console> (enable)
```

アカウンティングの例

図 38-5 に、TACACS+ を使用した単純なネットワーク トポロジーを示します。

ワークステーション A がスイッチ上でアカウンティング対象のイベントを開始すると、スイッチはイベント情報を収集し、イベントの終了時にその情報をサーバに転送します。イベントの終了時にアカウンティング情報が収集されます。未知のユーザについてはアカウンティングを抑制し、120 分ごとにシステムをアップデートします。

図 38-5　TACACS+ ネットワーク トポロジー例



この例では、接続アカウンティング、EXEC モード アカウンティング、システム アカウンティング、およびすべてのコマンド アカウンティングについて、TACACS+ アカウンティングをイネーブルに設定しています。

```
Console> (enable) set accounting connect enable stop-only tacacs+
Accounting set to enable for connect events in stop-only mode.
Console> (enable) set accounting exec enable stop-only tacacs+
Accounting set to enable for exec events in stop-only mode.
Console> (enable) set accounting commands enable all stop-only tacacs+
Accounting set to enable for commands-all events in stop-only mode.
Console> (enable) set accounting update periodic 120
Accounting updates will be periodic at 120 minute intervals.
Console> (enable) show accounting
Event     Method  Mode
-----     ------- ----
exec:     tacacs+ stop-only
connect:  tacacs+ stop-only
system:   tacacs+ stop-only
commands:
config:   -       -
all:      tacacs+ stop-only

TACACS+ Suppress for no username: enabled
Update Frequency: periodic, Interval = 120

Accounting information:
-----------------------
Active Accounted actions on tty0, User (null) Priv 0
Active Accounted actions on tty288091924, User (null) Priv 0
Overall Accounting Traffic:
          Starts   Stops  Active
          -----    -----  ------
Exec           0       0       0
Connect        0       0       0
Command        0       0       0
System         1       0       0
Console> (enable)
```

CHAPTER 39

802.1X 認証の設定

この章では、Catalyst 6500 シリーズ スイッチ上で IEEE 802.1X 認証を設定する方法について説明します。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

(注) MAC（メディア アクセス制御）アドレス認証バイパスの設定については、第 40 章「MAC 認証バイパスの設定」を参照してください。

(注) イーサネット、ファスト イーサネット、またはギガビット イーサネット ポートへのアクセスを試みたステーションの MAC アドレスが、そのポートに指定されている MAC アドレスと異なる場合に、ポート セキュリティ機能を使用してポートへのアクセスをブロックする手順については、第 37 章「ポート セキュリティの設定」を参照してください。また、ホスト MAC アドレスに基づく指定ホストに送信、または指定ホストから受信したトラフィックをフィルタリングする場合に、ポート セキュリティ機能を使用する手順についても説明します。

(注) Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）を設定して、Catalyst 6500 シリーズ スイッチの CLI（コマンドライン インターフェイス）へのアクセスをモニタおよび制御する方法については、第 38 章「AAA によるスイッチ アクセスの設定」を参照してください。

(注) Network Admission Control（NAC）の設定については、第 42 章「NAC の設定」を参照してください。

この章で説明する内容は、次のとおりです。

802.1X 認証の機能

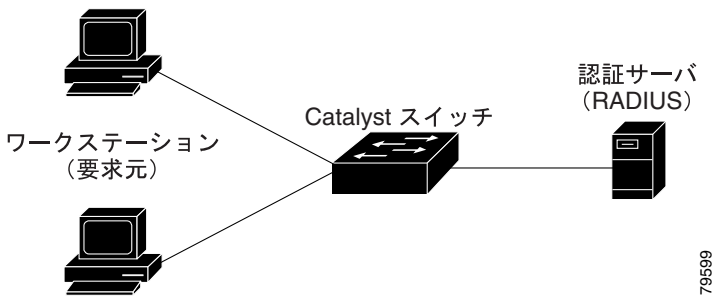
802.1X 規格では、クライアント / サーバベースのアクセス制御および認証プロトコルを定義しています。このプロトコルは、無許可の装置が公的にアクセス可能なポートから LAN にアクセスするのを制限します。802.1X は、ポートごとに 2 つの個別の仮想アクセス ポイントを作成してネットワーク アクセスを制御します。一方のアクセス ポイントが未制御のポートで、もう一方は制御ポートです。1 つのポートを通過するトラフィックはすべて、両方のアクセス ポイントで利用できます。802.1X は、スイッチまたは LAN が提供するサービスを利用できるようにする前に、スイッチのポートに接続されている各ユーザ デバイスを認証し、そのポートを VLAN（仮想 LAN）に割り当てます。802.1X アクセス制御によりデバイスが認証されるまでは、Extensible Authentication Protocol over LAN（EAPOL）トラフィックだけしか、そのデバイスの接続ポートを通過できません。認証に成功すると、通常のトラフィックがポートを通過できるようになります。双方向のトラフィックまたは着信トラフィックのみを制限できます。

ここでは、次の内容について説明します。

デバイスの役割

802.1X ポートベース認証を使用すると、ネットワーク内のデバイスには特定の役割が割り当てられます（図 39-1 を参照）。

図 39-1　802.1X デバイスの役割



- *要求元* ― LAN およびスイッチ サービスへのアクセスを要求し、スイッチの要求に応答します。ワークステーションは、802.1X 準拠のソフトウェアを実行している必要があります。

(注) 802.1X では、*クライアント*または*ホスト*に対して*要求元*という用語を使用します。Catalyst 6500 シリーズ CLI の構文では*ホスト*が使用されるので、このマニュアルでは、*要求元*ではなく*ホスト*を使用します。

- *認証サーバ* ― 実際にホストの認証を行います。認証サーバは、ホストの ID を確認し、LAN およびスイッチ サービスへのホストのアクセスを許可するかどうかをスイッチに通知します。スイッチはプロキシとして機能するので、認証サービスはホストにトランスペアレントです。このリリースでは、Extensible Authentication Protocol（EAP）拡張機能搭載の Remote Authentication Dial-In User Service（RADIUS）セキュリティ システムが唯一のサポート対象認証サーバです。Cisco Secure Access Control Server バージョン 3.0 で利用できます。RADIUS は、RADIUS サーバと 1 つまたは複数の RADIUS クライアント間で安全な認証情報が交換されるクライアント / サーバ モデルで動作します。
- *スイッチ* ― ホストの認証ステータスに基づいてネットワークへの物理的なアクセスを制御します。スイッチは、ホストと認証サーバとの間の媒介（プロキシ）として機能し、ホストに ID 情報を要求し、その情報を認証サーバで確認し、ホストに応答をリレーします。スイッチは RADIUS クライアントと対話します。RADIUS クライアントは EAP フレームのカプセル化およびカプセル化解除を行い、認証サーバと対話します。

  スイッチが EAPOL フレームを受信して認証サーバにリレーすると、イーサネット ヘッダーが取り除かれ、残りの EAP フレームが RADIUS 形式で再度カプセル化されます。EAP フレームはカプセル化の間は変更や検査が行われず、認証サーバはネイティブのフレーム形式内で EAP をサポートする必要があります。スイッチが認証サーバからフレームを受信すると、サーバのフレーム ヘッダーが削除され、EAP フレームが残ります。これがイーサネット用にカプセル化されてホストに送信されます。

認証の開始とメッセージ交換

スイッチまたはホストは、認証を開始できます。**set port dot1x** *mod/port* **port-control auto** コマンドを使用してポート上で認証をイネーブルにする場合、スイッチは、ポートのリンク ステートがダウンからアップに移行したことを確認したときに、認証を開始する必要があります。スイッチは、EAP-Request/Identity フレームをホストに送信して ID を要求します（一般に、スイッチは最初の ID/要求フレームを送信して、そのあとで 1 つまたは複数の認証情報の要求を送信します）。ホストは、フレームを受信すると EAP-Response/Identity フレームを送信します。

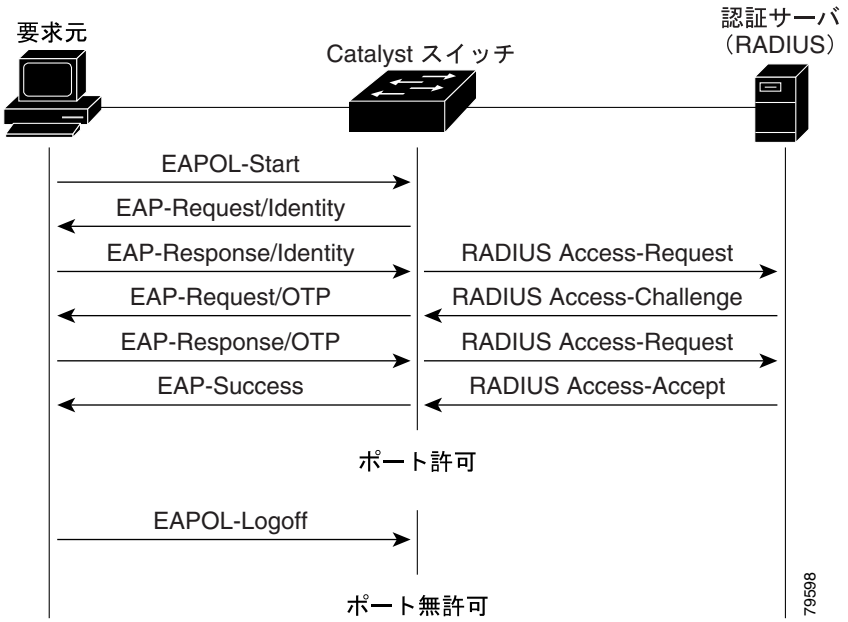
起動中に、ホストがスイッチから EAP-Request/Identity フレームを受信しない場合は、ホストは EAPOL-Start フレームを送信して認証を開始できます。これにより、スイッチはホストの ID を要求するようになります。

(注) ネットワーク アクセス装置で 802.1X がイネーブルになっていないかサポートされていない場合は、ホストからの EAPOL フレームは廃棄されます。認証の開始を 3 回試行してもホストが EAP-Request/Identity フレームを受信しない場合は、ホストはポートが許可ステートにあるかのようにフレームを送信します。許可ステートにあるポートは、ホストが正常に認証されたということです。詳細については、「許可および無許可ステートのポート」（p.39-4）を参照してください。

ホストが ID を供給すると、スイッチは媒介として動作し、認証が成功または失敗するまでホストと認証サーバとの間で EAP フレームを受け渡します。認証が成功すると、スイッチのポートは許可された状態になります。詳細については、「許可および無許可ステートのポート」（p.39-4）を参照してください。

特定の EAP フレーム交換は、使用される認証方式に左右されます。図 39-2 に、RADIUS サーバで One Time Password（OTP; ワンタイム パスワード）認証方式を使用するホストによって開始されるメッセージ交換を示します。

図 39-2　メッセージ交換



許可および無許可ステートのポート

スイッチ ポートのステートによって、ホストがネットワーク アクセスを許可されているかどうかがわかります。ポートは、*無許可*ステートで開始します。このステートでは、ポートは、802.1X プロトコル パケットを除いてすべての入力トラフィックおよび出力トラフィックを許可していません。ホストが正常に認証されると、ポートは*許可*ステートに移行し、そのホストへのすべてのトラフィックは通常のフローが許可されます。

802.1X をサポートしていないホストが無許可の 802.1X ポートに接続している場合は、スイッチはホストに ID を要求します。この場合、ホストは要求に応答できないので、ポートは無許可ステートのままで、ホストはネットワーク アクセスが許可されません。

802.1X 対応ホストが 802.1X プロトコルを実行していないポートに接続している場合、ホストは EAPOL-Start フレームを送信して認証プロセスを開始します。応答が得られなかった場合、ホストは要求を固定回数だけ送信します。応答が得られないので、ホストはポートが許可ステートにあるかのようにフレームの送信を開始します。

ポートの許可ステートを制御するには、**set port dot1x** *mod/port* **port-control** コマンドと以下のキーワードを使用します。

- **force-authorized** ― 802.1X 認証をディセーブルにして、認証交換なしでポートを許可ステートに移行させます。ポートは、ホストの 802.1X ベースの認証なしで通常のトラフィックを送受信します。これがデフォルト設定です。
- **force-unauthorized** ― ポートを無許可ステートのままにし、ホストが認証を試みてもすべて無視します。スイッチは、インターフェイスを介してホストに認証サービスを提供できません。
- **auto** ― 802.1X 認証をイネーブルにして、ポートに無許可ステートを開始させ、EAPOL フレームだけがポートを通じて送受信できるようにします。ポートのリンク ステートがダウンからアップに移行するか、EAPOL-Start フレームを受信すると、認証プロセスが開始されます。スイッチは、ホストの ID を要求し、ホストと認証サーバ間で認証メッセージのリレーを開始します。ネットワークにアクセスしようとする各ホストは、ホストの MAC アドレスを使用して一意に識別されます。

ホストが正常に認証されると（認証サーバから Accept フレームを受信する）、ポート ステートが許可に切り替わり、認証されたホストのフレームはすべてそのポートを通じて許可されます。認証が失敗した場合は、ポートは無許可ステートのままですが、認証を再試行できます。スイッチは、認証サーバにアクセスできない場合、要求を再送信できます。指定された試行回数のあとでもサーバから応答が得られない場合は、認証が失敗し、ネットワーク アクセスは許可されません。

ホストがログオフすると、サーバは EAPOL-Logoff メッセージを送信し、スイッチ ポートを無許可ステートに移行させます。

ポートのリンク ステートがアップからダウンに移行した場合、または EAPOL-Logoff メッセージを受信した場合は、ポートは無許可ステートに戻ります。

表 39-1 に、802.1X の用語の説明を示します。

表 39-1　802.1X の用語

用語	定義
認証者 PAE[1]	ポイントツーポイント LAN セグメントの一端のエンティティで、ホストの認証を実行します（「認証者」エンティティともいいます）。認証者は実際の認証方式からは独立しており、認証交換のパススルーとしてのみ機能します。認証者はホストと対話し、ホストからの情報を認証サーバに引き渡し、認証サーバから指示されればホストを認証します。
認証サーバ	認証者 PAE に対して認証サービスを提供するエンティティ。ホスト PAE の証明書を確認してから、ホスト PAE が LAN/ スイッチ サービスへのアクセスを許可するかどうかを、クライアントである認証者 PAE に通知します。
許可ステート	ホスト PAE が許可されたあとのポートのステータス
両方	未許可のスイッチ ポートでの着信および発信の双方向のフロー制御
制御ポート	セキュリティ保護されているアクセス ポイント
EAP	Extensible Authentication Protocol
EAPOL[2]	LAN MAC サービスで直接処理できる、カプセル化された EAP メッセージ
In	未許可スイッチ ポートでの着信フレームに限ったフロー制御
ポート	LAN インフラストラクチャへの単一ポイント接続（MAC ブリッジ ポートなど）
PAE	特定のシステム ポートに対応するポート アクセス エンティティ プロトコル オブジェクト
PDU	プロトコル データ ユニット
RADIUS	Remote Access Dial-In User Service
要求元[3] PAE	LAN/ スイッチ サービスへのアクセスを要求し、認証者からの情報要求に応答するエンティティ
未許可ステート	認証要求元 PAE が許可される前のポートのステータス
未制御ポート	セキュリティ保護されていないアクセス ポイントであり、制御されていない PDU の交換を許可します。

1. PAE = Port Access Entity（ポート アクセス エンティティ）
2. EAPOL = Extensible Authorization Protocol over LAN
3. 802.1X では、*クライアント*または*ホスト*に対して*要求元*という用語を使用します。Catalyst 6500 シリーズ CLI の構文では*ホスト*が使用されるので、このマニュアルでは、*要求元*ではなく*ホスト*を使用します。

認証サーバ

認証者と認証サーバとの間で交換されたフレームは、認証メカニズムによって異なるので、802.1X 規格では定義されていません。他のプロトコルを使用できますが、特に認証サーバがリモートに配置されているときは認証には RADIUS の使用を推奨します。RADIUS には、内蔵の EAP フレームのカプセル化をサポートする拡張機能が搭載されているためです。

スイッチに設定可能な 802.1X パラメータ

スイッチ上で設定できる 802.1X パラメータは、次のとおりです。

- Force-Authorized、Force-Unauthorized、または自動 802.1X ポート制御を指定
- 単一認証、複数認証、および複数ホスト認証を指定
- システム認証制御のイネーブル化およびディセーブル化
- 待機時間の指定
- 認証者からホストへの再送信時間の指定
- バックエンド認証者からホストへの再送信時間の指定
- バックエンド認証者から認証サーバへの再送信時間の指定
- バックエンド認証者からホストに再送信されるフレーム数の指定
- ホストの自動的な再認証時間の指定
- セキュリティ違反後のポート シャットダウン タイムアウト時間の指定
- ホストの自動的な再認証のイネーブル化およびディセーブル化

RADIUS サーバを使用した 802.1X VLAN 割り当ての概要

Release 7.2(2) より前のスーパバイザ エンジン ソフトウェア リリースでは、802.1X クライアントが認証されると、そのクライアントは NVRAM（不揮発性 RAM）に設定された VLAN に加入します。Release 7.2(2) 以降のソフトウェア リリースでは、認証後に 802.1X ホストはその VLAN 割り当てを RADIUS サーバから受信できます。

この VLAN 割り当て機能によって、特定の VLAN に対するユーザ アクセスを制限できます。たとえば、ゲスト ユーザはネットワークへのアクセスが制限された VLAN に割り当てることが可能です。

802.1X 認証を受けたポートは、そのポートに接続されているホストのユーザ名に基づいて、VLAN に割り当てられます。この機能は、ユーザ名と VLAN のマッピングが保存されている RADIUS サーバと連動します。

あるポートの 802.1X 認証が完了すると、RADIUS サーバから VLAN が送信され、ユーザはその VLAN へのアクセス権を与えられます。VLAN 割り当て機能に関連した 802.1X ポートの動作は以下のとおりです。

- リンク確立時、802.1X ポートは NVRAM に設定されている元の VLAN に配置されています。
- リンク確立後、RADIUS が提供する VLAN が有効であり、管理ドメイン内でアクティブな状態であれば、ポートは RADIUS 提供の VLAN に割り当てられます。
- ポートが別の VLAN に属している場合、そのポートは RADIUS が提供する VLAN に移動します。
- RADIUS が提供する VLAN が管理ドメイン内でアクティブな状態でない場合、そのポートは非アクティブ ステートになります。
- RADIUS 提供の VLAN が無効であるか、またはポートのハードウェアに問題がある場合、そのポートは 802.1X 未許可ステートになります。

- 1 つの 802.1X ポートに対して複数ホスト オプションをイネーブルにした場合は、最初の認証済みユーザが受信した RADIUS 提供 VLAN と同じ VLAN にすべてのホストが入ります。
- 802.1X 設定モジュールがダウン状態の場合は、802.1X ポートのすべての Enhanced Address Recognition Logic（EARL）エントリが消去されます。
- 802.1X 設定モジュールがアップ状態に戻ると、すべての 802.1X ポートが NVRAM に設定されている VLAN に割り当てられます。
- 802.1X 設定モジュールのコンフィギュレーションが消去された場合、すべての 802.1X ポートが NVRAM 設定 VLAN に移動し、802.1X ポートの EARL エントリはすべて消去されます。
- 802.1X ポートが許可ステートから未許可ステートに移行すると、そのポートは NVRAM に設定された VLAN に移動します。

「RADIUS サーバを使用した 802.1X VLAN の割り当て」の機能を正常に完了させるには、RADIUS サーバによって以下の 3 つの RFC 2868 属性を認証者（認証ホストと接続しているシスコ製スイッチ）に戻す必要があります。

- [64] Tunnel-Type = VLAN
- [65] Tunnel-Medium-Type = 802
- [81] Tunnel-Private-Group-Id = VLAN NAME

属性 [64] には、[VLAN] 値（タイプ 13）が含まれる必要があります。属性 [65] には、[802] 値（タイプ 6）が含まれる必要があります。属性 [81] では、正常に認証された 802.1X 認証ホストを割り当てた VLAN 名を指定します。

（注） VLAN は、番号ではなく名前で指定する必要があります。

DHCP での 802.1X 認証の機能

802.1X 認証は Dynamic Host Configuration Protocol（DHCP）をサポートしており、認証済みユーザの ID を DHCP 検出プロセスに付加することによって、DHCP サーバが異なるエンド ユーザのクラスに IP アドレスを割り当てることを可能にします。これを利用すれば、エンド ユーザに付与された IP アドレスをアカウンティングのために保護したり、レイヤ 3 の基準に準拠したサービスを提供したりできます。RADIUS サーバが要求元を認証すると、DHCP サーバは IP アドレスのリースに関連付けられた認証済みユーザの ID を保持します。この認証済みユーザの ID は、DHCP 検出プロセスに付加されます。それにより、異なるユーザのクラスごとに異なるアドレスを割り当てることができます。

要求元と RADIUS サーバとの間で 802.1X 認証が成功すると、スイッチはポートをフォワーディング ステートに設定し、RADIUS サーバから受信した属性を格納します。この属性は、DHCP サーバ内のアドレス プールへのマッピングに使用されます。スイッチは DHCP リレー エージェントとして機能できるため、DHCP メッセージを受け取り、そのメッセージを他のインターフェイスで伝送するために再生成できます。要求元が（認証後に）DHCP を検出すると、スーパバイザ エンジン上の DHCP リレー エージェントがパケットを受信し、RADIUS サーバから受信して格納した属性を DHCP 発見パケットに付加し、再びブロードキャストします。ユーザと IP アドレスは、1 対 1、1 対多、多対多でマッピングできます。1 対多のマッピングを使用すれば、同じユーザが複数のポートの 802.1X ホストを通じて認証できます。

補助 VLAN トラフィック用に設定されたポート上での 802.1X 認証の概要

Multiple VLAN Access Port（MVAP）の 802.1X をイネーブルにできます。また、802.1X ポートの補助 VLAN ID をイネーブルにできます。

802.1X 認証および補助 VLAN 用に設定されたポートを単一ホスト認証モードにして、IP Phone からの補助 VLAN タグ付きパケットを転送する必要があります。IP Phone にはホスト PAE 機能が装備されていないので、802.1X 認証用に設定されたポート上で IP Phone からの補助 VLAN タグ付きパケットを受信したときは、パケットは許可トラフィックとして転送されます。

IP Phone の先に接続されているホスト PAE は認証されます。IP Phone の先のホスト PAE からのトラフィックだけが認証後に転送されます。

（注）　802.1X 対応 VLAN ポートに接続した IP Phone にホスト PAE を接続した場合は、古いホストを取り外したあとで新しいホスト PAE が認証されます。新しいホスト PAE からのトラフィックだけが認証後に転送されます。

ゲスト VLAN に対する 802.1X 認証の概要

ここでは、ゲスト VLAN に対する 802.1X 認証について説明します。

ゲスト VLAN 機能によって、802.1X 非対応ホストは 802.1X 認証を使用するネットワークにアクセスできます。802.1X 認証をサポートするようにシステムをアップグレードしているときに、ゲスト VLAN を使用できます。

802.1X ゲスト VLAN として VLAN を設定すると、802.1X 非対応ホストはすべてこの VLAN に入れられます。どのような VLAN（プライベート VLAN と RSPAN VLAN を除く）もゲスト VLAN として設定できます。ポートがすでにゲスト VLAN で転送を行っているときに、そのホストのネットワーク インターフェイス上での 802.1X サポートをイネーブルにすると、ポートはただちにゲスト VLAN から除外され、認証者は認証発生待ちとなります。

ポート上での 802.1X 認証をイネーブルにすると、802.1X プロトコルが実行されます。ホストが一定時間内に認証者からのパケットに応答できない場合、認証者はそのホストをゲスト VLAN に入れます。

ゲスト VLAN は、単一認証と複数ホスト モードの両方でサポートされています。

（注）　ゲスト VLAN 機能を認証失敗 VLAN 機能と対比させてください。従来型の 802.1X ポートでは、スイッチはポートに接続された要求元の ID 情報が認証サーバで検証されて認証されるまで、ネットワークへのアクセスを提供しません。認証失敗 VLAN 機能を使用すれば、ポート単位で認証失敗 VLAN を設定できます。要求元による 802.1X 認証が 3 回失敗すると、ポートは要求元からのネットワーク アクセスが可能な認証失敗 VLAN に移動されます。

認証失敗 VLAN は、ゲスト VLAN とは無関係です。ただし、ゲスト VLAN と認証失敗 VLAN を同じ VLAN にすることができます。802.1X 非対応ホストと認証失敗ホストを区別しない場合は、両方を同じ VLAN（ゲスト VLAN または認証失敗 VLAN）に設定できます。

詳細については、「認証失敗 VLAN の設定」（p.39-37）を参照してください。

Windows XP ホストでのゲスト VLAN に対する 802.1X 認証の際の使用上の注意事項

ここでは、Windows XP ホストでのゲスト VLAN に対する 802.1X 認証を設定する際の注意事項について説明します。

- ゲスト VLAN がポートでイネーブルの場合、そのポートは単一方向のポートとして設定できません。また、その逆に単一方向ポートをゲスト VLAN に設定できません。
- ホストが認証者に応答できない場合、ポートは 180 秒間接続されたままです。180 秒が経過すると、ログイン / パスワード ウィンドウはホストに表示されません。解決策はユーザに接続を解除させ、ネットワーク インターフェイス ケーブルを再接続することです。
- 不正なログイン / パスワードにより応答するホストは、認証を失敗し、ゲスト VLAN に割り当てられません。ホストが初めて認証に失敗すると、待機時間タイマーが始動し、稼働している間はアクティビティが一切発生しません。待機時間タイマーが満了すると、ホストにログイン / パスワード ウィンドウが表示されます。ホストが 2 度めも認証に失敗すると、待機時間タイマーが再度始動し、稼働している間はアクティビティが一切発生しません。ホストに 3 度めのログイン / パスワード ウィンドウが表示されます。3 度めも失敗すると、ポートは接続しているが未許可ステートに入れられます。この問題の解決策はユーザに接続を解除させ、ネットワーク インターフェイス ケーブルを再接続することです。
- ホストが認証者 PAE からのユーザ名およびパスワード認証要求に応答しない場合、それはゲスト VLAN に配置されます。

（注） ゲスト VLAN はローカル スイッチに限定され、VTP を通じて伝播されることはありません。

ポート セキュリティでの 802.1X 認証の機能

802.1X 認証はポート セキュリティ機能と互換性があります（詳細については、第 37 章「ポート セキュリティの設定」を参照）。特定ポートの 1 つだけの MAC アドレスのポート セキュリティをイネーブルにした場合は、その MAC アドレスだけが RADIUS サーバを介して認証されます。それ以外の MAC アドレスを通じて接続しているユーザはすべて、アクセスが拒否されます。複数の MAC アドレスのポート セキュリティをイネーブルにしている場合は、各アドレスは 802.1X RADIUS サーバを介して認証が必要です。

（注） 警告 CSCin25663 のため、ポート セキュリティ用に設定する MAC アドレスから logoff メッセージを受信した場合、またはその特定の MAC アドレスの再認証に失敗した場合、その MAC アドレスは削除されます。この問題は今後のソフトウェア リリースで解決されます。

（注） 802.1X 認証とポート セキュリティが任意の 802.1X ポート上でイネーブルになっているときは、ポート上では 802.1X 認証がポート セキュリティに優先されます。まずホストが認証され、それからポート セキュリティによって保護されます。

802.1X モード（単一認証モード、複数ホスト モード、または複数認証モード）に対してポート セキュリティをイネーブルにできます。1 つのポート上で一度にイネーブルにできるのは 1 つのモードだけです。デフォルトのポート モードは単一認証モードです。

単一認証モードおよび複数ホスト モードのポート セキュリティをディセーブルにできます。ただし、複数認証モードのポート セキュリティはディセーブルにできません。

MAC アドレス ベースのポート セキュリティについてイネーブルに設定されているポートで、802.1X 認証もイネーブルにすると、最大許容数の MAC アドレスを設定していないかぎりは、ポート上で 802.1X 認証は発生しません。802.1X 単一ホスト モード認証もイネーブルに設定されているポートに対して、最大許容数未満の MAC アドレスを設定すると、設定済みの MAC アドレスを削除するかどうかを尋ねるシステム メッセージが表示されます。このメッセージに [yes] と応答すると、MAC アドレス ベースのポート セキュリティに対して設定された MAC アドレスは削除され、ポートは 802.1X 認証を使用して認証されます。その他のモードに対して 802.1X 認証がイネーブルに設定されている場合は、メッセージは表示されず、MAC アドレスは保持されます。

複数認証モードでは、すべての接続ホストは 802.1X を使用して認証され、ポート セキュリティを使用して保護されています。802.1X は、MAC アドレスを認証してから MAC アドレスにポート セキュリティを施して保護します。MAC アドレスが EAPOL-Logoff パケットを送信すると、ポート セキュリティ テーブルから MAC アドレスが削除されます。

ARP トラフィック検査での 802.1X 認証の機能

（注） この機能を使用できるのは、PFC2 搭載の Supervisor Engine 2、PFC3A/PFC3B/PFC3BXL 搭載の Supervisor Engine 720、および PFC3B/PFC3BXL 搭載の Supervisor Engine 32 だけです。

（注） ARP トラフィック検査と 802.1X の設定は相互に排他的な関係にあります。

ARP トラフィック検査によって、セキュリティ ACL（VACL）フレームワーク内に順序依存型の一連のルールを設定して ARP テーブルへの攻撃を防止できます。ARP トラフィック検査は 802.1X ポート認証プロトコルを補完するもので、認証されたクライアントの MAC アドレスをポートにバインドしてから、IP/MAC アドレスのバインドを追加することで追加のスプーフ検査に対する MAC アドレスのスプーフィングの可能性を排除します。

ARP トラフィック検査を 802.1X 認証と併用することにより、悪意のあるユーザ / ホストが他のホストの ARP テーブルを破壊する可能性を排除し、ポートおよびユーザのセキュリティを強化できます。要求元の 802.1X 認証が成功したあと、ARP トラフィック検査（要求元の IP アドレスおよび MAC アドレスをバインドします）が実行され、スプーフィングの可能性を排除します。

ARP は認証メカニズムを備えていない簡易プロトコルで、ARP 要求および応答が正しいかどうかを確認する方法がありません。認証メカニズムがなければ、悪意のあるユーザ / ホストによってレイヤ 2 ネットワークまたはブリッジ ドメインにある同じ VLAN 上の他のホストの ARP テーブルが破壊される可能性があります。

たとえば、ユーザ / ホスト A（悪意のあるユーザ）が、デフォルト ルータの IP アドレスとホスト A の MAC アドレスで、非送信請求 ARP 応答（不必要な ARP パケット）をサブネット上の他のホストに送信することがあります。従来の OS（オペレーティング システム）では、デフォルト ルータのスタティック ARP エントリがホストにすでにある場合でも、ホスト A からの新たにアドバタイズされたバインディングが学習されます。ホスト A が IP 転送をイネーブルにし、すべてのパケットを「スプーフィングされた」ホストとルータ間でやり取りする場合、ホスト A は（たとえば dsniff プログラムを使用して）man-in-the-middle 攻撃を実行できます。スプーフィングされたホストでは、そのトラフィックのすべてにスニッフィングが行われていることを認識しません。

また、ARP 検査を実行することで、（イーサネット ヘッダーにある）送信元イーサネット MAC アドレスが ARP ヘッダーの送信元 MAC アドレスと異なるパケットを廃棄できます。**set security acl arp-inspection match-mac** {**enable** [**drop** [**log**]] | **disable**} コマンドを CLI から入力することで、この機能をイネーブル（またはディセーブル）にできます。

ARP トラフィック検査の設定については、「ARP トラフィックの検査」（p.15-30）を参照してください。

認証のデフォルト設定

表 39-2 に、802.1X 認証のデフォルト設定を示します。

表 39-2　802.1X 認証のデフォルト設定

機能	デフォルト値
PAE 機能	認証者のみ
プロトコル バージョン	1
802.1X ポート制御	Force-Authorized
802.1X 複数ホスト	ディセーブル
802.1X システム認証制御	イネーブル
802.1X 待機時間	60 秒
802.1X 認証者からホストへの再送信時間	30 秒
802.1X バックエンド認証者からホストへの再送信時間	30 秒
802.1X バックエンド認証者から認証サーバへの再送信時間	30 秒
バックエンド認証者からホストに再送信される 802.1X フレーム数	2
802.1X ホストの自動再認証時間	3600 秒
802.1X 認証者によるホストの自動再認証	ディセーブル
802.1X シャットダウン タイムアウト時間	300 秒
802.1X RADIUS アカウンティング	ディセーブル
802.1X RADIUS VLAN 割り当て	イネーブル
802.1X RADIUS キープアライブ ステート	イネーブル

認証設定時の注意事項

ここでは、スイッチ上で 802.1X 認証を設定する際の注意事項について説明します。

- 802.1X は他のプロトコルでも機能しますが、リモートに配置された認証サーバでは RADIUS を使用することを推奨します。
- 802.1X はイーサネット ポート上でのみサポートされています。
- Release 7.5(1) では、2 つの帯域内管理インターフェイスの sc0 と sc1 をサポートしています。802.1X 認証は、RADIUS サーバと通信するときは、常に認証者の ID として sc0 インターフェイスを使用します。sc1 インターフェイスでは 802.1X 認証はサポートされていません。
- 802.1X をトランク ポート上でイネーブルに設定するには、そのポートのトランキングをオフにする必要があります。802.1X ポート上でトランキングをイネーブルに設定することはできません。
- 802.1X をダイナミック ポート上でイネーブルに設定するには、そのポートのダイナミック VLAN をオフにする必要があります。802.1X ポート上でダイナミック VLAN をイネーブルに設定することはできません。
- 802.1X をチャネリング ポート上でイネーブルに設定するには、そのポートのチャネリングをオフにする必要があります。802.1X ポート上でチャネリングをイネーブルに設定することはできません。
- Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）宛先ポート上では 802.1X をイネーブルに設定することはできません。また、802.1X ポート上で SPAN 宛先を設定することはできません。ただし、802.1X ポートを SPAN 送信元ポートとして設定することはできます。
- 補助 VLAN を **dot1p** または **untagged** に設定できません。また、補助 VLAN は 802.1X 対応ポート上のネイティブ VLAN と同じにしてはなりません。
- 802.1X 対応補助 VLAN ポート上では、複数認証オプションをイネーブルにできません。802.1X 対応 AUX ポート上で複数ホスト オプションをイネーブルにすることは推奨できません。
- 802.1X 対応補助 VLAN ポートは、ポート上の補助 VLAN がゲスト VLAN と同じ場合は、ゲスト VLAN に入れられないので、補助 VLAN と同じゲスト VLAN を割り当てないでください。
- 802.1X 対応ポートでは、管理上設定された VLAN は補助 VLAN と同じにすることはできません。
- プライベート VLAN および 802.1X の設定は相互に排他的な関係にあります。
- PFC3A/PFC3B/PFC3BXL を使用することにより、**set rate-limit l2port-security** コマンドを使用してスイッチ上で 802.1X ポート セキュリティ レート リミッタをグローバルにイネーブル、ディセーブル、または設定できます。レート制限設定の詳細については、「スイッチ上でのレイヤ 2 PDU レート制限の設定」（p.8-65）を参照してください。

スイッチ上での 802.1X 認証の設定

ここでは、スイッチ上で 802.1X 認証を設定する手順について説明します。

(注)　VLAN 割り当てに関する RADIUS サーバの使用については、「RADIUS サーバを使用した 802.1X VLAN 割り当ての概要」（p.39-6）を参照してください。

802.1X 認証のグローバルなイネーブル化

各ポートに対して 802.1X 認証を設定するには、先にシステム全体でイネーブルに設定する必要があります。802.1X 認証をグローバルにイネーブルにすると、802.1X 認証の要求する特定の要件を各ポートが満たしていれば、各ポートに 802.1X 認証を設定できます。各ポートに 802.1X 認証を設定する手順については、「各ポートに対する 802.1X 認証のイネーブル化」（p.39-14）を参照してください。

802.1X 認証をグローバルにイネーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
802.1X 認証をグローバルにイネーブルにします。	**set dot1x system-auth-control enable**

次に、802.1X 認証をグローバルにイネーブルにする例を示します。

```
Console> (enable) set dot1x system-auth-control enable
dot1x system-auth-control enabled.
```

802.1X 認証のグローバルなディセーブル化

802.1X 認証をシステム全体に対してイネーブルに設定しているときは、これをグローバルにディセーブルにできます。802.1X 認証をグローバルにディセーブルにすると、（それまで 802.1X 認証を設定していたポートを含め）、どのポートでも 802.1X 認証を利用できなくなります。

802.1X 認証をグローバルにディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
802.1X 認証をグローバルにディセーブルにします。	**set dot1x system-auth-control disable**

次に、802.1X 認証をグローバルにディセーブルにする例を示します。

```
Console> (enable) set dot1x system-auth-control disable
dot1x system-auth-control disabled.
```

各ポートに対する 802.1X 認証のイネーブル化

802.1X 認証をグローバルにイネーブルにすると、コンソールから各ポートに対して 802.1X 認証をイネーブルにする必要があります。802.1X 認証をグローバルにイネーブルに設定する手順については、「802.1X 認証のグローバルなイネーブル化」（p.39-14）を参照してください。

（注） スイッチ上で 802.1X 認証をイネーブルにする前に、少なくとも 1 つの RADIUS サーバを指定する必要があります。詳細については、第 21 章「AAA によるスイッチ アクセスの設定」を参照してください。

スイッチへのアクセスに 802.1X 認証をイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	特定のポート上で 802.1X 制御をイネーブルにします。	**set port dot1x** *mod/port* **port-control auto**
ステップ 2	802.1X の設定を確認します。	**show port dot1x** *mod/port*

次に、モジュール 3 のポート 1 上で 802.1X 認証をイネーブルにし、設定を確認する例を示します。

```
Console> (enable) set port dot1x 3/1 port-control auto
Port 3/1 dot1x port-control is set to auto.
Trunking disabled for port 3/1 due to Dot1x feature.
Spantree port fast start option enabled for port 3/1.
Console> (enable) show port dot1x 3/1
Port  Auth-State          BEnd-State Port-Control        Port-Status
----- ------------------- ---------- ------------------- -------------
 3/1  connecting          idle       auto                unauthorized

Port  Port-Mode     Re-authentication   Shutdown-timeout   Control-Mode
                                                           admin   oper
----- ------------- -----------------   ----------------   ---------------
 3/1  SingleAuth    disabled            disabled           Both    Both
Console> (enable)
```

(注) 新しい認証のために現状のマシンを消去するには、**set port dot1x** *mod/port* **initialize** コマンドを入力します。

アクセス不可能認証バイパスでの 802.1X のイネーブル化

802.1X アクセス不可能認証バイパスをポート単位でイネーブルにできます。この機能により、ポートをクリティカルとして指定できます。ポートがクリティカルとして指定された場合、802.1X は通常の方法でこのポートを認証しようとします。認証サーバに到達できないポートでも、管理上設定された VLAN またはポートのネイティブ VLAN 内のネットワークにアクセスできます。ポートが単一認証モードの場合に限り、ポートをクリティカルとして設定できます。

クリティカル ポートがネットワークへのアクセス権を取得して、認証サーバが使用可能になると、クリティカル ポートは無許可ステートに戻り、通常の認証プロセスが再開します。クリティカル ポートが認証されると、RADIUS サーバが指定した VLAN に移行します。この時点で、**set port dot1x** *mod/port* **initialize** コマンドを使用して、ポートを手動で初期化する必要があります。

ホストが通常の認証プロセスにより認証されたあとで認証サーバがダウンした場合、スイッチはこのポートがクリティカル ポートかどうかを確認します。スイッチがこのポートをクリティカル ポートと判断した場合、このポートに対する通常の再認証プロセスは一時的にディセーブルになります。ポートは、認証サーバがアクティブになり認証プロセスを再開するまで、ネットワークへのアクセス権が与えられます。

ポートをクリティカル ポートとして指定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポートをクリティカル ポートとして指定します。	**set port dot1x** *mod/port* **critical** {**enable** | **disable**}
ステップ 2	802.1X の設定を確認します。	**show port dot1x** *mod/port*

次に、クリティカル ポートとしてポートを指定する例を示します。

```
Console> (enable) set port dot1x 5/48 critical enable
Port 5/48 critical-port option is enabled
Console> (enable)
```

次に、802.1X の設定を確認する例を示します。

```
Console> (enable) show port dot1x 5/48
Port  Auth-State          BEnd-State Port-Control        Port-Status
----- ------------------- ---------- ------------------- -------------
 5/48 -                   -          force-authorized    -

Port  Port-Mode     Re-authentication   Shutdown-timeout   Control-Mode
                                                          admin   oper
----- ------------- -----------------   ----------------   ---------------
 5/48 SingleAuth    disabled            disabled           Both    -

Port  Posture-Token Critical Termination action Session-timeout
----- ------------- -------- ------------------ ---------------
 5/48 -             YES      -                  -
Console> (enable)
```

複数 802.1X 認証のイネーブル化

複数のホストが 802.1X ポートにアクセスできるように、複数認証を指定できます。シスコ独自の複数認証では、1 つのポート上で複数の dot1x ホストの認証が可能で、すべてのホストが別個に認証されます。複数 802.1X 認証をイネーブルにする際は次の注意事項に従ってください。

- 複数の認証済みポートの非 802.1X ホストからのトラフィックはブロックされます。
- ゲスト VLAN は、複数の認証済みポート上でイネーブルにできません。
- MVAP 上では複数認証はイネーブルにできません。
- 複数の認証済みポートはポート VLAN になり、RADIUS 指定の VLAN にはなりません。
- ポート上で複数認証をイネーブルにするには、先にポート セキュリティをポート上でイネーブルにする必要があります。
- 複数の認証済みポート上では、ポート セキュリティをディセーブルにできません。
- ポート セキュリティ タイマーは、複数の認証済みポートで使用します。再認証タイマーは、複数の認証済みポートでは使用しません。

複数 802.1X 認証をイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	特定のポート上で複数 802.1X 認証をイネーブルにします。	**set port dot1x** *mod/port* **multiple-authentication** {**enable** | **disable**}
ステップ 2	802.1X の設定を確認します。	**show port dot1x** *mod/port*

次に、モジュール 3 のポート 1 上で複数 802.1X 認証をイネーブルにし、設定を確認する例を示します。

```
Console> (enable) set port dot1x 3/1 multiple-authentication enable
PortSecurity should be enabled on port 3/1, before enabling Multiple-authentication
Port Security not enabled on 3/1.
Console> (enable) set port security 3/1 enable
Port 3/1 security enabled.
Console> (enable) set port dot1x 3/1 multiple-authentication enable
Port 3/1 Multiple-authentication option enabled
Console> (enable) show port dot1x 3/1
Port  Auth-State          BEnd-State Port-Control        Port-Status
----- ------------------- ---------- ------------------- -------------
 3/1  connecting          idle       auto                unauthorized

Port  Port-Mode     Re-authentication   Shutdown-timeout   Control-Mode
                                                          admin    oper
----- ------------ -----------------   ----------------   ---------------
 3/1  MultiAuth     disabled            disabled           Both     Both
Console> (enable)
```

ホストの自動再認証の設定およびイネーブル化

802.1X ホストの自動再認証をイネーブルに設定する前であれば、802.1X 認証がホストを再認証する頻度を指定できます。ホストの自動再認証をイネーブルに設定する前に期間を指定しない場合は、802.1X は 3600 秒をデフォルト設定とします（有効な値は 1 ～ 65,535 秒です）。

特定ポートに接続したホストの 802.1X ホスト自動再認証をイネーブルにできます。特定ポートに接続したホストを手動で再認証する手順については、「手動でのホストの再認証」（p.39-18）を参照してください。

802.1X 認証がホストを再認証する頻度を設定し、802.1X 自動再認証をイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ホストの再認証の時間定数を設定します。	**set dot1x re-authperiod** *seconds*
ステップ 2	再認証をイネーブルにします。	**set port dot1x** *mod/port* **re-authentication enable**
ステップ 3	802.1X の設定を確認します。	**show port dot1x** *mod/port*

次に、自動再認証を 7,200 秒に設定し、ポート 3/1 で 802.1X 再認証をイネーブルにし、設定を確認する例を示します。

```
Console> (enable) set dot1x re-authperiod 7200
dot1x re-authperiod set to 7200 seconds
Console> (enable) set port dot1x 3/1 re-authentication enable
Port 3/1 Dot1x re-authentication enabled.
Console> (enable) show port dot1x 3/1
Port  Auth-State          BEnd-State Port-Control        Port-Status
----- ------------------- ---------- ------------------- -------------
 3/1  connecting          idle       auto                unauthorized

Port  Port-Mode     Re-authentication   Shutdown-timeout   Control-Mode
                                                          admin    oper
----- ------------ -----------------   ----------------   ---------------
 3/1  MultiAuth     enabled             disabled           Both     Both
Console> (enable)
```

手動でのホストの再認証

特定のポートに接続したホストは、いつでも手動で再認証できます。802.1X ホストに自動再認証の設定をする場合は、「ホストの自動再認証の設定およびイネーブル化」（p.39-17）を参照してください。

特定のポートに接続したホストを手動で再認証するには、イネーブル モードで次の作業を行います。

作業	コマンド
特定のポートに接続したホストを手動で再認証します。	**set port dot1x** *mod/port* **re-authenticate**

次に、モジュール 3 のポート 1 に接続したホストを手動で再認証する例を示します。

```
Console> (enable) set port dot1x 3/1 re-authenticate
Port 3/1 re-authenticating...
dot1x re-authentication successful...
dot1x port 3/1 authorized.
Console> (enable)
```

複数ホストのイネーブル化

特定ポートをイネーブルにして複数ユーザのアクセスを可能にします。ポートが複数のユーザに対してイネーブルで、そのポートに接続したホストが正常に許可されているとき、MAC アドレスを持つホストはすべて、そのポートに対してトラフィックを送受信することができます。そのあとでハブを介して複数のホストをそのポートに接続すると、そのポートのセキュリティ レベルを低くすることができます。

特定のポート上で複数ホストのアクセスをイネーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
特定のポート上で複数ホストをイネーブルにします。	**set port dot1x** *mod/port* **multiple-host enable**

次に、モジュール 3 のポート 1 上で複数ホストのアクセスをイネーブルにする例を示します。

```
Console> (enable) set port dot1x 3/1 multiple-host enable
Port 3/1 Multiple-host option enabled.
Console> (enable)
```

複数ホストのディセーブル化

イネーブルに設定されているポート上で複数ユーザのアクセスをディセーブルに設定できます。

特定のポート上で複数ホストのアクセスをディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
特定のポート上で複数ホストをディセーブルにします。	**set port dot1x** *mod/port* **multiple-host disable**

次に、モジュール 3 のポート 1 上で複数ホストのアクセスをディセーブルにする例を示します。

```
Console> (enable) set port dot1x 3/1 multiple-host disable
Port 3/1 Multiple-host option disabled.
Console> (enable)
```

待機時間の設定

認証者がホストを認証できないときは、一定時間のアイドル状態を経て再試行します。アイドル時間は、quiet-period の値によって決まります（デフォルトの設定は 60 秒です）。この値は、0 ～ 65,535 秒の範囲で設定できます。

待機時間の値を設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
待機時間の値を設定します。	**set dot1x quiet-period** *seconds*

次に、待機時間を 45 秒に設定する例を示します。

```
Console> (enable) set dot1x quiet-period 45
dot1x quiet-period set to 45 seconds.
Console> (enable)
```

シャットダウン タイムアウト時間の設定

セキュリティ違反のためにポートがシャットダウンした場合、手動で再度イネーブルにするか、シャットダウン タイムアウト時間を設定してポートが再びイネーブルになるようにする必要があります。

セキュリティ違反のあとにポートがディセーブルになる期間を設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
シャットダウン タイムアウト時間を設定します。	**set dot1x shutdown-timeout** *1 – 65535 seconds*

次に、シャットダウン タイムアウト時間を設定する例を示します。

```
Console> (enable) set dot1x shutdown-timeout 300
dot1x shutdown-timeout set to 300 seconds.
Console> (enable)
```

認証者からホストへの EAP-Request/Identity フレーム再送信時間の設定

ホストは、EAP-Request/Identity フレームを受信したことを認証者に通知します。認証者は、この通知を受信しないときは、一定時間待機してから、フレームを再送信します。認証者が通知を待つ時間を 1 ～ 65,535 秒の範囲で設定できます（デフォルトの設定は 30 秒です）。

認証者からホストへの EAP-Request/Identity フレームの再送信時間を設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
認証者からホストへの EAP-Request/Identity フレームの再送信時間を設定します。	**set dot1x tx-period** *seconds*

次に、認証者からホストへの EAP-Request/Identity フレームの再送信時間を 15 秒に設定する例を示します。

```
Console> (enable) set dot1x tx-period 15
dot1x tx-period set to 15 seconds.
Console> (enable)
```

バックエンド認証者からホストへの EAP-Request フレーム再送信時間の設定

ホストは、EAP-Request フレームを受信したことをバックエンド認証者に通知します。バックエンド認証者は、この通知を受信しないときは、一定時間待機してから、フレームを再送信します。バックエンド認証者が通知を待つ時間を 1 ～ 65,535 秒の範囲で設定できます（デフォルトの設定は 30 秒です）。

バックエンド認証者からホストへの EAP-Request フレーム再送信時間を設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
バックエンド認証者からホストへの EAP-Request フレーム再送信時間を設定します。	**set dot1x supp-timeout** *seconds*

次に、バックエンド認証者からホストへの EAP-Request フレーム再送信時間を 15 秒に設定する例を示します。

```
Console> (enable) set dot1x supp-timeout 15
dot1x supp-timeout set to 15 seconds.
Console> (enable)
```

バックエンド認証者から認証サーバへのトランスポート レイヤ パケット再送信時間の設定

認証サーバは、トランスポート レイヤ パケットを受信するたびにバックエンド認証者に通知します。バックエンド認証者は、パケットの送信後この通知を受信しないときは、一定時間待機してから、パケットを再送信します。バックエンド認証者が通知を待つ時間を 1 ～ 65,535 秒の範囲で設定できます（デフォルトの設定は 30 秒です）。

バックエンド認証者から認証サーバへのトランスポート レイヤ パケットの再送信時間の値を設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
バックエンド認証者から認証サーバへの、トランスポート レイヤ パケットの再送信時間を設定します。	**set dot1x server-timeout** *seconds*

次に、バックエンド認証者から認証サーバへの、トランスポート レイヤ パケットの再送信時間を 15 秒に設定する例を示します。

```
Console> (enable) set dot1x server-timeout 15
dot1x server-timeout set to 15 seconds.
Console> (enable)
```

バックエンド認証者からホストへの再送信フレーム数の設定

認証サーバは、一定数のフレームを受信するたびにバックエンド認証者に通知します。バックエンド認証者は、フレーム送信後にこの通知を受信しないときは、一定時間待機してから、そのフレームを再送信します。バックエンド認証者が再送信するフレーム数を 1 ～ 10 の範囲（デフォルトは 2）で設定できます。

バックエンド認証者からホストに再送信されるフレーム数を設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
バックエンド認証者からホストへの再送信フレーム数を設定します。	**set dot1x max-req** *count*

次に、バックエンド認証者からホストに再送信されるフレーム数を 4 に設定する例を示します。

```
Console> (enable) set dot1x max-req 4
dot1x max-req set to 4.
Console> (enable)
```

802.1X コンフィギュレーション パラメータのデフォルト値へのリセット

1 つのコマンドで、802.1X コンフィギュレーション パラメータをデフォルト値に戻すことができます。これは 802.1X をグローバルにディセーブルにすることにもなります。

802.1X コンフィギュレーション パラメータをデフォルト値に戻すには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	802.1X コンフィギュレーション パラメータをデフォルト値に戻し、802.1X をグローバルにディセーブルにします。	**clear dot1x config**
ステップ 2	802.1X の設定を確認します。	**show dot1x**

次に、802.1X コンフィギュレーション パラメータをデフォルト値に戻し、設定を確認する例を示します。

```
Console> (enable) clear dot1x config
This command will disable dot1x on all ports and take dot1x parameter values back to
factory defaults.
Do you want to continue (y/n) [n]?
Console> (enable) show dot1x
PAE Capability              Authenticator Only
Protocol Version            1
system-auth-control         enabled
max-req                     2
quiet-period                45 seconds
radius-accounting           disabled
radius-vlan-assignment      enabled
radius-keepalive state      enabled
re-authperiod               7200 seconds
server-timeout              30 seconds
shutdown-timeout            300 seconds
supp-timeout                30 seconds
tx-period                   30 seconds

Console> (enable)
```

DHCP リレー エージェントでの 802.1X 認証のイネーブル化

DHCP リレー エージェントが特定の VLAN の 802.1X パラメータを DHCP サーバに送信できるようにするには、イネーブル モードで次の作業を行います。

（注） 管理 VLAN（sc0 または sc1 インターフェイスで設定されている VLAN）を、dot1x-dhcp Access Control Entry（ACE; アクセス制御エントリ）のある Access Control List（ACL; アクセス制御リスト）にマッピングできません。VLAN 1 または VLAN 2 が dot1x-dhcp ACE のある ACL にマッピングされる際に、**clear config interface** コマンドを使用できません。

	作業	コマンド
ステップ 1	DHCP リレー エージェントの 802.1X 認証をイネーブルにします。 **（注）** このコマンドは、指定された ACL 名で ACE エントリを生成します。この ACL は他の ACE エントリを持つこともできますが、DHCP の ACE エントリが優先されます。	**set security acl ip** *acl_name* **permit dot1x-dhcp**
ステップ 2	802.1X の設定を確認します。	**show dot1x**

次に、802.1X の DHCP リレー トラフィック用の ACL エントリを作成する例を示します。

```
Console> (enable) set security acl ip dhcp_relay permit dot1x_dhcp
Successfully configured Dot1x Dhcp ACL for dhcp_relay. Use 'commit' command to save
changes
```

次に、既存の ACL エントリ上で DHCP 以外のトラフィックを許可するように ACL を設定する例を示します。

```
Console> (enable) set security acl ip dhcp_relay permit any
dhcp_relay editbuffer modified. Use 'commit' command to apply changes.
console> (enable)
```

次に、ACE を NVRAM にコミットする例を示します。

```
Console> (enable) commit security acl dhcp_relay
Commit operation in progress
ACL 'dhcp_relay' successfully committed.
```

次に、dhcp-relay-acl に適用する VLAN をマッピングする例を示します。

```
Console> (enable) set security acl map dhcp_relay 1-3,20
Mapping in progress...
ACL dhcp_relay successfully mapped to VLAN 1.
ACL dhcp_relay successfully mapped to VLAN 2.
ACL dhcp_relay successfully mapped to VLAN 3.
ACL dhcp_relay successfully mapped to VLAN 20.
```

クライアントからサーバに転送される DHCP パケットには、DHCP リレー エージェント情報フィールドが追加されます。[dhcp-relay-acl] にマッピングされていない VLAN とすべての DHCP パケットは変更なく従来どおりスイッチされます。

DHCP リレー エージェントでの 802.1X 認証のディセーブル化

DHCP リレー エージェントが特定の VLAN の 802.1X パラメータを DHCP サーバに送信しないようにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	DHCP リレー エージェントの 802.1X 認証をディセーブルにします。	**clear security acl map dhcp_relay** *vlan_ID*
ステップ 2	802.1X の設定を確認します。	**show dot1x**

次に、VLAN1 ～ 3 および 20 の 802.1X 認証パラメータを送信しないように DHCP リレー エージェントを設定し、設定を確認する例を示します。

```
Console> (enable) clear security acl map dhcp_relay 1-3,20
Successfully cleared mapping between ACL dhcp_relay and VLAN 1.
Successfully cleared mapping between ACL dhcp_relay and VLAN 2.
Successfully cleared mapping between ACL dhcp_relay and VLAN 3.
Successfully cleared mapping between ACL dhcp_relay and VLAN 20.
```

802.1X ゲスト VLAN へのホストの追加

一般的に、ゲスト VLAN は最小限のサービスをサポートし、最小限のネットワーク アクセスを行います。ホストは、**set port dot1x** *mod/port* **port-control auto** コマンド オプションが使用された場合にだけ、ゲスト VLAN に追加されます。**set port dot1x** *mod/port* **port-control** コマンド オプションを **auto** から **force-authorized** または **force-unauthorized** に変更すると、ホストはゲスト VLAN から削除され、ポート VLAN に戻されます。

ポートを 802.1X ゲスト VLAN に追加するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	アクティブ VLAN を 802.1X ゲスト VLAN として設定します。	**set port dot1x** *mod/port* **guest-vlan** {*vlan* | **none**}
ステップ 2	ポートごとに 802.1X ゲスト VLAN 設定を確認します。	**show port dot1x guest-vlan**

次に、ポート 3/1 を 802.1X ゲスト VLAN 200 に追加する例を示します。

```
Console> (enable) set port dot1x 3/1 guest-vlan 200
Port 3/1 is Multiple-authentication enabled, guest-vlan can not be enabled
Console> (enable) set port dot1x 3/1 multiple-authentication disable
Port 3/1 Multiple-authentication option disabled
Console> (enable) set port dot1x 3/1 guest-vlan 200
Port 3/1 Guest Vlan is set to 200
Console> (enable) show port dot1x guest-vlan
Guest-Vlan    Status   Mod/Ports
------------- -------- ------------------
200           active   3/1
none          none     2/1-2,3/2-48,8/1-8
Console> (enable)
```

次に、ポートをゲスト VLAN から削除する例を示します。

```
Console> (enable) set port dot1x 3/1 guest-vlan none
Port 3/1 Guest Vlan is cleared
Console> (enable)
```

802.1X 単一方向制御ポートの設定

802.1X により、スイッチに接続されているホストにおける無人システムのバックアップまたはソフトウェア アップグレードを実行するために、ウェイクオン LAN テクノロジー（リモート ウェイクアップともいう）を使用できます。

単一方向制御ポートが設定されている場合、ホスト認証の前にポートは発信方向のみのトラフィックを許可します。この動作により、管理ステーションは選択されたホストへウェイクオン LAN フレームを送信できます。このフレームは、ホストに対して電源投入とブート、認証、およびその後の無人操作を実行するトリガとなります。

（注） ウェイクオン LAN テクノロジーではホストに特定のハードウェアが必要ですが、これはこのマニュアルの範囲ではありません。

Release 8.3(1) より前のソフトウェア リリースでは、デフォルトで 802.1X ブリッジ ポートが双方向ステートに設定されています。このステートでは制御は無許可のポートで双方向のプロトコル交換に影響します。単一方向制御ポート機能により、**set port dot1x** *mod/port* **port-control-direction** コマンドを使用して、802.1X 対応ポートを単一方向（**in** キーワード）または双方向（**both** キーワード）ステートに設定できます。

単一方向ステート

ポートを単一方向ポート（**in** キーワード）として設定して **set port dot1x** *mod/port* **port-control auto** コマンドを使用してポートを **auto** に設定する場合、ブリッジ ポートはスパニングツリー フォワーディング ステートに移行します。この場合、ポートに向かうすべてのトラフィックがスーパバイザ

エンジンに転送されて処理されます。ウェイクオン LAN 機能により、接続ホストがスリープ モードまたは電源切断ステートの場合、ホストはネットワークの他のデバイスとトラフィックを交換しません。単一方向ポートと接続されたホストはトラフィックをネットワーク外に送信できず、ネットワーク内の他のデバイスからのトラフィックのみを受信できます。単一方向ポートが何らかの入力トラフィックを認識した場合、ポートは双方向ステート（デフォルト）に戻ってスパニング ツリー ステートがブロッキング モードに移行し、入出力トラフィックが廃棄されます。ポートの認証者システムが初期化ステートに移行し、EAPOL パケット交換以外のトラフィックは許可されません。ポートが双方向ステートに戻る際、5 分タイマーが起動してタイマーが切れるまでにポートが認証されなかった場合、ポートは単一方向ステートに戻ります。

双方向ステート

ポートを双方向ポート（**both** キーワード）として設定して **set port dot1x** *mod/port* **port-control auto** コマンドを使用してポートを **auto** に設定する場合、ポートは双方向でアクセス制御されます。このステートは、ポートでの入力パケットの受信および出力パケットの伝送をディセーブルにします。ポートが双方向ポートとして設定される場合、Release 8.3(1) より前のソフトウェア リリースのように動作し、ポートはスパニング ツリー ブロッキング ステートになり通常の認証プロセスに従います。

設定時の注意事項

ここでは、802.1X 単一方向ポートを設定する上での注意事項を説明します。

- 補助 VLAN ― ポートを単一方向ポートとして設定する際にポートで補助 VLAN をサポートするには、接続された IP Phone が確実に即座に動作するよう補助 VLAN がスパニング ツリー フォワーディング ステートに移行します。入力トラフィックの障害を避けるために、まずポート VLAN もスパニング ツリー フォワーディング ステートに移行し、トラフィックがポート VLAN で確認されたら、ポートはすべての追加トラフィックを廃棄するためにスパニング ツリー ブロッキング ステートに移行します。そこで接続ホストはトラフィックの送信許可を得るように要求されます。
- ゲスト VLAN ― ゲスト VLAN は、双方向ポートとして設定されているポートでのみサポートされます。ゲスト VLAN がポートでイネーブルの場合、そのポートは単一方向のポートとして設定できません。また、その逆に単一方向ポートをゲスト VLAN に設定できません。
- ポート モード ― 単一方向ポートとして設定されているポートのポート モード（単一認証モード、複数ホストモード、または複数認証モード）は単一認証モード（デフォルトのポート モード）でなければなりません。

CLI を使用した 802.1X 単一方向または双方向ポートの設定

in キーワードを指定する場合、すべての入力トラフィックは廃棄されて出力トラフィックは許可されます。**both** キーワード（デフォルト）を指定した場合、ポート上のすべての受信トラフィックおよび送信トラフィックが廃棄されます。ポートを 802.1X 単一方向ポートまたは双方向ポートとして設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
ポートを 802.1X 単一方向ポートまたは双方向ポートとして設定します。	**set port dot1x** *mod/port* **port-control-direction** [**both** | **in**]

次に、ポートを単一方向または双方向ステートに設定して設定を変更する例を示します。

```
Console> (enable) set port dot1x 3/1 port-control-direction both
Port 3/1 Port Control Direction set to Both.
Console> (enable) set port dot1x 3/1 port-control-direction in
Port 3/1 Port Control Direction set to In.
Console> (enable) show port dot1x 3/1
Port  Auth-State          BEnd-State Port-Control        Port-Status
----- ------------------- ---------- ------------------- -------------
 3/1  connecting          idle       auto                unauthorized

Port  Port-Mode     Re-authentication   Shutdown-timeout   Control-Mode
                                                           admin   oper
----- ------------- -----------------   ----------------   ---------------
 3/1  SingleAuth    enabled             disabled           In      Both
Console> (enable)
```

ACL 割り当てでの 802.1X の設定

ここでは、ACL 割り当てでの 802.1X を設定する手順について説明します。

概要

ACL 割り当てで 802.1X を設定する場合、ユーザの 802.1X 認証に基づいてアクセス制御ポリシーをインターフェイスに動的に割り当てるのに ID ベースの ACL が使用されます。この機能は、ユーザを特定のネットワーク セグメントに限定し、機密性の高いサーバへのアクセスを制限し、使用可能なプロトコルとアプリケーションを制限します。また、この機能を使用すると、ユーザの移動性に支障が出たり、管理上のオーバーヘッドが大幅に増加したりすることなく、ごく特定の ID ベースのセキュリティを提供できます。

ACL 割り当てで 802.1X を設定する場合、ユーザが物理的な位置を変更するたびに発生する、IP アドレスまたは MAC アドレスに基づいたアクセス制御ポリシーの作成、変更、削除における問題を解消できます。この機能によって、VLAN-based Policy（VACL; VLAN ベース ポリシー）や Port-based Policy（PACL; ポートベース ポリシー）の代わりに ID ベースのセキュリティ アクセス ポリシーを作成する際に、ユーザの移動性を損なうことなくポリシーを作成できます。この機能を使用することで、ユーザの物理的な位置を変更したり、ネットワーク接続を変更したりするたびに、ユーザはアクセス ポリシーの変更についてネットワーク管理者に依存する必要はありません。

新しい **group** *group_name* キーワードは、ポリシーをグループとして分類するのに使用します。グループとは、ポリシーを適用するユーザ（IP アドレス）のセットです。この機能を実行する前に、ユーザ セットへの IP アクセスを許可したい場合、ACL ACE に各ユーザの IP アドレスを指定する必要があります。ACE ごとに設定可能な IP アドレスは 1 つだけです。この新しい機能を使用する場合、**set security acl ip** *grpacl* **permit ip group** *ip-permit-group* **any** のように、ACE に *group_name* を指定します。*ip-permit-group* はグループで、そのグループ内のすべてのユーザは認証されます。ユーザ認証が成功してユーザの IP アドレスが取得されたら、ユーザがグループに属している場合、ユーザの IP アドレスがグループに追加され、新しい ACE が作成されてハードウェア（PFC）にインストールされます。ACL はユーザ認証およびログオフにより動的に伸縮します。すなわち ACL は動的で、ポリシーは認証済みで有効なユーザに対してのみインストールされます。

ACL 割り当てで 802.1X を設定する場合、ユーザが認証されるたびに自動的に Quality of Service（QoS; サービス品質）ACL および VACL をユーザに設定できます。RADIUS サーバは、認証成功パケットとともに QoS VLAN ベース ACL、QoS ポートベース ACL、または VACL ポリシー名を送信します。ポリシー名に関連付けられたポリシーは、すでに CLI を使用してスイッチに設定されています。ポリシーは ACE のセットに変換されて、スイッチにインストールされます。

IP アドレスに ACL を適用できます。802.1X 認証がユーザ名で実行され MAC アドレスと結びついているものの IP アドレスは認証時には認識されていないため（認証に成功したあとでのみ DHCP がホストで開始されます）、ACE のインストールが実行されるのは、DHCP スヌーピングまたはダイナミック ARP 検査を通じて IP アドレスが認識されたあとになります。

ACL 割り当てで 802.1X を設定する場合、主に次の 2 種類の設定作業があります。

- RADIUS サーバ内にあるユーザのグループ名の関連付けと設定
- スイッチの CLI を使用したスイッチ上のグループの設定、コミット、ACL のマッピング

802.1X ACL 割り当てが設定されると、スイッチは次の作業を実行します。

- ユーザの認証
- DHCP スヌーピングまたはダイナミック ARP 検査を使用したユーザの IP アドレスの取得
- IP アドレスを使用した ACL の拡張と PFC のプログラミング

ACL 割り当てでの 802.1X 設定時の注意事項

ここでは、ACL 割り当てで 802.1X を設定する上での注意事項を説明します。

- ACL 割り当てでの 802.1X に設定されているポートのポート モード（単一認証モード、複数ホストモード、または複数認証モード）は単一認証モード（デフォルトのポート モード）でなければなりません。
- （DHCP スヌーピングまたはダイナミック ARP 検査を通じて取得した）動的に学習された IP アドレスは、グループ名を拡張するのに使用します。ACL 割り当てでの 802.1X は、スタティック IP アドレスでもサポートされています（スタティック IP アドレスが RADIUS サーバにも設定されている必要があります）。
- グループはポリシー グループです。ポリシー グループの例としては、IP アドレスのセットに対する「http アクセスの拒否」などのポリシーです。
- ユーザは永続的にグループと結びついているわけではなく、ユーザは同時に複数のポリシー グループに属することができます。複数のポリシーを定義したい場合、たとえば、「http アクセスの拒否」と「FTP アクセスの拒否」の両方を定義したい場合、2 つのポリシー グループ（1 つは「http アクセスの拒否」を定義したグループ、もう 1 つは「FTP アクセスの拒否」を定義したグループ）を定義できます。
- RADIUS サーバは、認証成功パケット内の特定のユーザに適用されなければならないすべてのポリシーを送信でき、ユーザはこれらのグループをすべてスイッチに追加できます。RADIUS サーバが送信したポリシー グループはスイッチに設定されていませんが、ポリシーは無視されるか、ポートが無許可ステートになります。RADIUS サーバがスイッチの ACL 内に存在しないグループ ID を送信すると、認証が失敗します。
- Release 8.3(1) 以降のソフトウェア リリースでは、1 つのグループ名に設定されている 802.1X 認証済みユーザを VLAN 間で均一に分散することにより、負荷を分散できます。詳細については、「802.1X ユーザ分散の設定」（p.39-32）を参照してください。

CLI を使用した ACL 割り当てでの 802.1X の設定

(注) ここでは、ACL 割り当てでの 802.1X の設定に使用する、Release 8.3(1) で導入された CLI について説明します。ACL 設定の詳細については、第 15 章「アクセス制御の設定」を参照してください。

ACL 割り当てで 802.1X をイネーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
ACL 割り当てで 802.1X を設定します。	**set security acl ip** {*acl_name*} {**permit** | **deny** | **redirect** {*mod_num/port_num*}} [**ip**] {*src_ip_spec* | [**group** {*group_name*}} {*dest_ip_spec* | [**group**} [**precedence** {*precedence*}] [**tos** {*tos*}] [**fragment**] [**capture**] [**log**] [**before** {*editbuffer_index*} | **modify** {*editbuffer_index*}]

次に、802.1X グループのグループ名を指定してグループが設定済みであることを確認する例を示します。

```
Console> (enable) set security acl ip grpacl permit ip group ip-permit-group any
grpacl editbuffer modified. Use 'commit' command to apply changes.
Console> (enable) commit security acl grpacl
ACL commit in progress.

ACL 'grpacl' successfully committed.
Console> (enable)

Console> (enable) show dot1x group all
Group Manager Info

Current Group Count = 1

------------------------------------------------------------
Info of Group ip-permit-group
User Count  = 0
Console> (enable)
```

QoS ACL での 802.1X の設定

ここでは、QoS ACL で 802.1X を設定する手順について説明します。

- QoS ACL での 802.1X 設定時の注意事項（p.39-29）
- QoS ACL での 802.1X 設定例（p.39-29）
- RADIUS サーバの設定（p.39-31）

RADIUS サーバは、ポリシー名を 802.1X クライアントに送信します。ポリシーはすでにスイッチに定義されていてコミットされています。ユーザは、QoS ポリシーを設定する際にすべての既存の QoS 機能を完全に利用できます。802.1X クライアントは、QoS サブシステムと対話して認証が行われたあとにインターフェイスにポリシーを適用します。ポリシーは、認証済みクライアントがインターフェイスから脱退する際に削除されます。802.1X がインターフェイスにポリシーを付加した場合でも、スイッチの CLI から直接ポリシーのマッピングを解除できます。

QoS ACL での 802.1X 設定時の注意事項

ここでは、QoS ACL で 802.1X を設定する上での注意事項を説明します。

- QoS ポリシーの設定に誤りがあり 802.1X がインターフェイスでユーザを認証しようとした場合、認証が失敗します。
- 802.1X がインターフェイスで適切に認証されたあとに QoS ポリシーを誤って設定した場合、同じ QoS ポリシーを使用してインターフェイスで再認証が行われる際に、認証が失敗します。
- 複数の QoS ポリシー（入力および出力ポリシー）が同時に適用される場合、QoS ポリシーが失敗すると、認証も失敗します。
- ポートベース ポリシーおよび VLAN ベース ポリシーを同じインターフェイスに適用すると、認証が失敗します。
- 802.1X ユーザがログインする際にのみ、802.1X セキュリティおよび QoS ポリシーが適用されます。スイッチまたは RADIUS サーバで 802.1X セキュリティ ポリシーと QoS ポリシーの一方または両方を変更する場合、802.1X ユーザが再認証されるまで変更は適用されません。再認証がイネーブル（デフォルトでない）の場合、ポリシーは通常 1 時間以内に有効になります。再認証がディセーブル（デフォルト）の場合、各 802.1X ユーザがログアウトし、再びログインするまでポリシー変更は有効になりません。
- 既存の QoS コマンドは、QoS ポリシー情報の作成と表示に使用されます。コマンドは **set qos enable**、**set qos acl**、および **commit qos acl** ですが、これに限定されません。スケジューリング コマンドおよびポートベース QoS コマンドもダイナミック QoS ポリシーの作成に使用できます。
- QoS ポリシーをスイッチに定義したあとは、（**set qos acl map** コマンドを使用して）ポリシーを VLAN またはポートにマッピングし、さらにポリシー マッピングが成功したことを確認する必要があります。確認後、ACL マッピングを消去して 802.1X をインターフェイスに設定します。

（注） QoS ACL の名前付けには注意してください。QoS ACL 名は、RADIUS サーバに指定されているポリシー名と一致する必要があります。

QoS ACL での 802.1X 設定例

次の例では、QoS がイネーブルで [Dot1xDscp5Policy] という 802.1X QoS ポリシーが作成されます。その後、ポリシーはコミットされます。さらに、同じポリシー名（Dot1xDscp5Policy）が RADIUS サーバに作成されます。一定期間が経過したあと、802.1X がクライアントを認証してポリシーが適用されたあとでそのポリシーがポート 3/1 に適用されたことが確認できます。ポリシー マッピングがマッピング コマンドのコンフィギュレーション（config）画面に表示されないことを確認できます。これは、実行コンフィギュレーションでのみ表示されます。

RADIUS サーバの AV ペアには [qos:inpacl=Dot1xDscp5Policy] という入力が必要です。ポート 3/1 の要求元認証を実行後、ポート 3/1 に対する QoS ランタイム マッピングが実行されます。

AV ペアに対する他のオプションは、qos:invacl=<policy-name> および qos:outpacl=<policy-name> です。

AV ペアのポリシー名がスイッチのポリシー名と一致しない場合、要求元は認証されません。

```
Console> (enable) set qos enable
QoS is enabled.
Console> (enable) set qos acl ip Dot1xDscp5Policy dscp 5 any
Dot1xDscp5Policy editbuffer modified. Use 'commit' command to apply changes.
Console> (enable) commit qos acl all

QoS ACL 'Dot1xDscp5Policy' successfully committed.
Console> (enable) show qos acl map config Dot1xDscp5Policy
QoS ACL mappings on input side:
ACL name                        Type Vlans
------------------------------- ---- --------------------------------
Dot1xDscp5Policy                  IP
ACL name                        Type Ports
------------------------------- ---- --------------------------------
Dot1xDscp5Policy                  IP
QoS ACL mappings on output side:
ACL name                        Type Vlans
------------------------------- ---- --------------------------------
Dot1xDscp5Policy                  IP
Console> (enable)

<<< Dot1x Authenticates a client on 3/1 and applies Dot1xDscp5Policy >>>

Console> (enable) show qos acl map runtime Dot1xDscp5Policy
QoS ACL mappings on input side:
ACL name                        Type Vlans
------------------------------- ---- --------------------------------
Dot1xDscp5Policy                  IP
ACL name                        Type Ports
------------------------------- ---- --------------------------------
Dot1xDscp5Policy                  IP 3/1
QoS ACL mappings on output side:
ACL name                        Type Vlans
------------------------------- ---- --------------------------------
Dot1xDscp5Policy                  IP
Console> (enable) show qos acl map config Dot1xDscp5Policy
QoS ACL mappings on input side:
ACL name                        Type Vlans
------------------------------- ---- --------------------------------
Dot1xDscp5Policy                  IP
ACL name                        Type Ports
------------------------------- ---- --------------------------------
Dot1xDscp5Policy                  IP
QoS ACL mappings on output side:
ACL name                        Type Vlans
------------------------------- ---- --------------------------------
Dot1xDscp5Policy                  IP
Console> (enable)
```

次の例では、**show qos acl map** コマンドを使用してダイナミック QoS ポリシー情報が表示されます。**runtime** キーワードを使用すると、どのダイナミック ポリシーがどのインターフェイスに適用されるかを確認できます。**config** キーワードではダイナミック QoS ポリシー マッピングを表示できません。

```
Console> (enable) show qos acl map config Dot1xDscp5Policy
QoS ACL mappings on input side:
ACL name                         Type Vlans
-------------------------------- ---- --------------------------------
Dot1xDscp5Policy                   IP
ACL name                         Type Ports
-------------------------------- ---- --------------------------------
Dot1xDscp5Policy                   IP
QoS ACL mappings on output side:
ACL name                         Type Vlans
-------------------------------- ---- --------------------------------
Dot1xDscp5Policy                   IP
Console> (enable) show qos acl map runtime Dot1xDscp5Policy
QoS ACL mappings on input side:
ACL name                         Type Vlans
-------------------------------- ---- --------------------------------
Dot1xDscp5Policy                   IP
ACL name                         Type Ports
-------------------------------- ---- --------------------------------
Dot1xDscp5Policy                   IP 3/1
QoS ACL mappings on output side:
ACL name                         Type Vlans
-------------------------------- ---- --------------------------------
Dot1xDscp5Policy                   IP
Console> (enable)
```

RADIUS サーバの設定

Cisco Secure Access Control Server（ASC）3.x 以降を使用する場合、認証済みクライアントと関連付けられる QoS ポリシー名を設定する必要があります。RADIUS サーバを設定するには、ACS のホームページから次の手順を実行します。

ステップ 1　**network configuration** を選択します。

ステップ 2　NAS IP をクリックして、属性の RADIUS IOS/PIX スタイルをオンにします。Authenticate Using（認証使用）フィールドが表示されます。

ステップ 3　**IOS/PIX** オプションを選択して実行します。

ステップ 4　**interface config** を選択します。

ステップ 5　**RADIUS (IOS/PIX)** を選択します。

ステップ 6　AV ペア オプションの前にある両方のチェック ボックスをオンにします。最初のオプションは AV ペアです。

AV ペア ボックスがすべてのユーザに表示されます。チェック ボックスをオンにして AV ペア文字列をウィンドウに入力します。この場合の文字列は、各ユーザに関連付ける QoS ポリシー名を表します。複数の AV ペア文字列を送信する場合、各 AV ペアを別の 26/9/1 属性として送信できるように別の行に分ける必要があります。

802.1X ユーザ分散の設定

802.1X ユーザ分散を設定することにより、同じグループ名を持つユーザを複数の VLAN に分散できます。Release 8.3(1) より前のソフトウェア リリースでは、802.1X でサポートされていた RADIUS VLAN 割り当て機能は RADIUS サーバから取得した VLAN 番号を使用し、すべてのユーザをその VLAN に追加しました。Release 8.3(1) 以降のソフトウェア リリースでは、1 つのグループ名に設定されている 802.1X 認証済みユーザを VLAN 間で均一に分散することにより、負荷を分散できます。

これらの 2 つの方法は、異なる VLAN でユーザのロード バランシングを実現するために使用します。VLAN は RADIUS サーバから提供されるか、スイッチの CLI を通じて VLAN グループ名に設定されます。

- ユーザに対して複数の VLAN 名を送信するように RADIUS サーバを設定します。ユーザへの応答の一部として複数の VLAN 名を送信できます。802.1X ユーザ分散では、特定の VLAN 内にあるすべてのユーザを追跡し、許可済みユーザをユーザが最も少ない VLAN に移動することでロード バランシングを実現しています。
- ユーザに VLAN グループ名を送信するように RADIUS サーバを設定します。ユーザへの応答の一部として VLAN グループ名を送信できます。選択された VLAN グループ名は、Catalyst CLI を使用して設定された VLAN グループ名の中から検索されたものです（「CLI を使用した 802.1X ユーザ分散の設定」[p.39-33] を参照）。VLAN グループ名が見つかると、この VLAN グループ名の下に設定された対応する VLAN が検索されてユーザの割り当てが最も少ない VLAN を探し、対応する許可済みユーザをその VLAN に移動することでロード バランシングを実現します。

802.1X ユーザ分散の設定の注意事項

ここでは、802.1X ユーザ分散機能を設定する際の注意事項について説明します。

- 少なくとも 1 つの VLAN が VLAN グループにマッピングされていることを確認します。
- 複数の VLAN を VLAN グループにマッピングできます。
- VLAN グループは VLAN を追加または削除することで変更できます。
- VLAN グループ名から既存の VLAN を削除する場合、VLAN に認証されたポートは消去されませんが、マッピングは既存の VLAN から削除されます。
- VLAN グループ名から最後の VLAN を消去すると、VLAN グループが削除されます。
- アクティブ VLAN がグループにマッピングされていても VLAN グループを消去できます。VLAN グループを消去する際、グループ内のいずれかの VLAN にある認証ステートのポートまたはユーザは消去されませんが、VLAN グループへの VLAN マッピングは消去されます。
- **set dot1x radius-vlan-assignment disable** コマンドを入力すると、RADIUS サーバから送信された VLAN 情報は無視されて、ポートは NVRAM 設定 VLAN のままになります。このコマンドは、VLAN 割り当て機能をグローバルにイネーブルまたはディセーブルにするのに使用します。このコマンドがイネーブルの場合、スイッチはトンネル属性を使用して RADIUS アクセス受入れメッセージ内の VLAN 名を抽出します。このコマンドは、デフォルトではイネーブルです。

CLI を使用した 802.1X ユーザ分散の設定

VLAN グループを設定してそれに VLAN をマッピングするには、イネーブル モードで次の作業を行います。

作業	コマンド
VLAN グループを設定して単一 VLAN または VLAN の範囲をそれにマッピングします。	**set dot1x vlan-group** {*vlan-group-name*} {*vlans*}
設定を確認します。	**show dot1x vlan-group** [**all** | {*vlan-group-name*}]
VLAN グループ設定または VLAN グループのエレメントを消去します。	**clear dot1x vlan-group** [**all** {*vlan-group-name*} [{*vlans*}]]

次に、VLAN グループを設定し、VLAN をグループにマッピングし、VLAN グループが設定されていて特定の VLAN にマッピングされていることを確認する例を示します。

```
Console> (enable) set dot1x vlan-group eng-dept 10
Vlan group name eng-dept is successfully configured and mapped to vlan 10
Console> (enable) set dot1x vlan-group hr-dept 20
Vlan group name hr-dept is successfully configured and mapped to vlan 20
Console> (enable) show dot1x vlan-group eng-dept
Group Name                      Vlans Mapped
-------------                   --------------
eng-dept                        10
Console> (enable) show dot1x vlan-group all
Group Name                      Vlans Mapped
-------------                   --------------
eng-dept                        10
hr-dept                         20
Console> (enable)
```

次に、VLAN を既存の VLAN グループに追加して、VLAN が追加されたことを確認する例を示します。

```
Console> (enable) set dot1x vlan-group eng-dept 30
Vlan 30 is successfully mapped to vlan group eng-dept.
Console> (enable) show dot1x vlan-group eng-dept
Group Name                      Vlans Mapped
-------------                   --------------
eng-dept                        10,30
Console> (enable)
```

次に、VLAN を VLAN グループから消去する例を示します。

```
Console> (enable) clear dot1x vlan-group eng-dept 10
Vlan 10 is successfully cleared from vlan group eng-dept.
Console> (enable)
```

次に、すべての VLAN が VLAN グループから消去された場合に VLAN グループが消去される例を示します。

```
Console> (enable) clear dot1x vlan-group eng-dept 30
Vlan 30 is successfully cleared from vlan group eng-dept.
Warning: No more vlans mapped to this group, vlan group is cleared.
Console> (enable) show dot1x vlan-group eng-dept
Vlan group eng-dept doesn't exist, can not display.
Console> (enable)
```

次に、すべての既存の VLAN グループを消去する例を示します。

```
Console> (enable) clear dot1x vlan-group all
Console> (enable) show dot1x vlan-group all
No vlan groups are present for display.
Console> (enable)
```

802.1X RADIUS アカウンティングとトラッキングのイネーブル化およびディセーブル化

802.1X RADIUS アカウンティングおよびトラッキングを使用して、802.1X ユーザ アカウンティング情報を RADIUS サーバに送信できます。この機能は UDP ポート番号 1813 を使用します。

802.1X アカウンティング パケットは、次の情報を RADIUS サーバに提供できます。

- ユーザが正常に認証した時
- ユーザがログオフした時
- リンクが 802.1X ポートでダウンした時
- 再認証が成功した時
- 再認証が失敗した時

アカウンティング パケットの属性は次のとおりです（オプションの属性もあります）。

- 属性 [1] USERNAME ― 認証されようとしているユーザ名
- 属性 [4] NAS-IP ― 認証およびアカウント セッションを開始するスイッチの IP アドレス（通常、sc0 インターフェイス IP アドレス）
- 属性 [40] ACCT-STATUS-TYPE ― START/STOP/INTERIM
  - ― 認証が成功してポートが許可ステートに移行する際に START が送信されます。
  - ― ユーザが logoff を送信するか、リンクがダウンするか、再認証が失敗した場合に STOP が送信されます。
  - ― 再認証が成功すると、INTERIM が送信されます。
- 属性 [44] ACCT-SESSION-ID ― すべてのアカウンティング セッションに関連付けられた固有のセッション IDT

アカウンティング パケット フォーマットは次のとおりです。

```
<NAS-IP> <user-id> <date> <time> <random16bit#>
```

アカウンティング パケット フォーマットの例は次のとおりです。

```
9.9.150.140 rameshp 31/07/2003 12:40:00 12345
```

上記に挙げた属性は、（START/STOP/INTERIM の）ACCT-STATUS-TYPE の属性に関係なく、共通です。

INTERIM アップデートに固有の属性は次のとおりです。

- 属性 [8] FRAMED-IP-ADDRESS ― ユーザに割り当てられた IP アドレス（このアドレスはスタティック割り当てまたは DHCP を通じて取得可能）
- 属性 [81] TUNNEL-PRIVATE-GROUP-ID ― RADIUS サーバが送信する実際の VLAN 名

  [Interim Accounting Request] 内の上記の属性とともに送信される CISCO-AV-PAIRS は次のとおりです。
  - ― AAA:ip-addr-method ― IP 割り当てが DHCP を通じたものか静的に設定されるかを送信します。
  - ― AAA:vlan-assign-method ― ローカル デバイスまたは RADIUS による割り当て

RADIUS サーバが VLAN を送信しない場合のタイプは「ローカル デバイス」になります。この場合、管理上設定されたポート VLAN はユーザの VLAN です。RADIUS サーバが VLAN を送信した場合、タイプは「RADIUS による割り当て」になります。

STOP パケットに固有の属性は次のとおりです。

- 属性 [49] ACCT-TERMINATION-CAUSE ― 原因はユーザのログオフ、ポートのダウン、再認証失敗などが考えられます。
- CISCO-AV-PAIRS
  - Cisco:Input-Octets ― ポートで受信される入力トラフィックのバイト数を指定する 64 バイトの整数
  - Cisco:Output-Octet ― ポートから転送された出力トラフィックのバイト数を指定する 64 バイトの整数

CLI を使用した 802.1X RADIUS アカウンティングおよびトラッキングのイネーブル化およびディセーブル化

802.1X RADIUS アカウンティングおよびトラッキングをグローバルにイネーブルまたはディセーブルにするには、イネーブル モードで次の作業を行います（デフォルトはディセーブル）。

作業	コマンド
802.1X RADIUS アカウンティングとトラッキングをグローバルにイネーブルまたはディセーブルにします。	**set dot1x radius-accounting** {**enable** | **disable**}

次に、802.1X RADIUS アカウンティングとトラッキングをグローバルにイネーブルまたはディセーブルにする例を示します。

```
Console> (enable) set dot1x radius-accounting enable
dot1x radius-accounting enabled.
Console> (enable) set dot1x radius-accounting disable
dot1x radius-accounting disabled.
Console> (enable)
```

認証済み ID とポート説明のマッピングの設定

認証済み ID とポート説明のマッピングを使用して、RADIUS サーバから受信した情報に基づいてポート名を 802.1X ポートに割り当てることができます。この機能は AV ペア「要求元名」を使用して一意に認証済みユーザのポート名を割り当てます。現在サポートされているのは、認証サーバから送信されるシスコのサポートする AV ペアのみで、他のベンダー固有の AV ペアは無視されます。

RADIUS サーバから受信されるポート名を表示するには、**show port** コマンドを入力します。スイッチが 20 文字以上の認証済みポート名を受信する場合、名前は 19 文字に切り捨てられて # 記号が名前に付加されます（合計で 20 文字が許可され、**set port name** コマンドと互換性があります）。**set port name** コマンドを入力する場合、最終結果は、認証済み ID とポート説明のマッピング機能を使用した場合と同じですが、この機能は 802.1X 認証で動的に名前を割り当てるところが異なっています。動的に割り当てられたポート名の例は次のとおりです。

```
Console> (enable) show port 4/1
* = Configured MAC Address

# = 802.1X Authenticated Port Name.

Port  Name                 Status     Vlan       Duplex Speed       Type
----- -------------------- ---------- ---------- ------ ----------- ------------
 4/1  rmanam-test-supplic# connected  1          a-full       a-100 10/100BaseTX

Port  AuxiliaryVlan AuxVlan-Status
----- ------------- --------------
 4/1  none          none

.
.
.
Console> (enable)
```

RADIUS サーバ設定の DNS レゾリューションの設定

RADIUS サーバ用の Domain Name System（DNS; ドメイン ネーム システム）レゾリューションを設定する場合、IP アドレスに加えて DNS 名を使用して RADIUS サーバを設定できます。DNS 名と IP アドレスを関連付けるのに設定された DNS サーバを使用して、スイッチが自動的に DNS 名を解決します。設定済みの DNS 名は、プライマリまたはセカンダリとして設定された他の IP アドレスと共存できます。DNS 名は NVRAM に保存されます。DNS レゾリューションが機能するために、RADIUS キープアライブ機能をイネーブルにする必要があります。DNS レゾリューション機能により、スイッチの知識なしに RADIUS サーバの IP アドレスを透過的に変更できます。次に、スイッチは修正された IP アドレスを使用して DNS 名を解決します。

スイッチは、DNS 名の初期設定時、802.1X がディセーブルまたはイネーブルになるとき、802.1X ポート認証中、または RADIUS サーバへの要求がタイムアウトの場合に、IP アドレスに対する DNS 名のレゾリューションを再び実行します（2 回めの解決）。このレゾリューションは、DNS 名と IP アドレスのマッピングが DNS サーバ側で変更されていないかをチェックします。

DNS 名が RADIUS サーバの IP アドレスの代わりに設定されている場合に、**show config** または **show radius** コマンドを入力して DNS 名を表示します。最大 3 つの RADIUS サーバを設定できます。設定済みの RADIUS サーバ パラメータを表示するには、次のように **show radius** コマンドを入力します。

```
Console> (enable) show radius
RADIUS Deadtime:              0 minutes
RADIUS Key:                   cisco
RADIUS Retransmit:            2
RADIUS Timeout:               5 seconds
Framed-Ip Address Transmit:   Disabled

RADIUS-Server                      Status  Auth-port Acct-port Resolved IP Address
---------------------------------- ------- --------- --------- -------------------
9.9.150.16                         primary 1812      1813
cat6k-sup2                                 1812      1813      9.9.150.20
cat6k-sup3                                 1812      1813      9.9.150.21
Console> (enable)
```

認証失敗 VLAN の設定

従来型の 802.1X ポートでは、スイッチはポートに接続された要求元の ID 情報が認証サーバで検証されて認証されるまで、ネットワークへのアクセスを提供しません。認証失敗 VLAN 機能を使用すれば、ポート単位で認証失敗 VLAN を設定できます。要求元による 802.1X 認証が 3 回失敗すると、ポートは要求元からのネットワーク アクセスが可能な認証失敗 VLAN に移動されます。

（注） 認証失敗 VLAN 機能をゲスト VLAN 機能と対比させてください。ゲスト VLAN 機能によって、802.1X 非対応ホストは 802.1X 認証を使用するネットワークにアクセスできます。802.1X 認証をサポートするようにシステムをアップグレードしているときに、ゲスト VLAN を使用できます。一般的に、ゲスト VLAN は最小限のサービスをサポートし、最小限のネットワーク アクセスを行います。

認証失敗 VLAN は、ゲスト VLAN とは無関係です。ただし、ゲスト VLAN と認証失敗 VLAN を同じ VLAN にすることができます。802.1X 非対応ホストと認証失敗ホストを区別しない場合は、両方を同じ VLAN（ゲスト VLAN または認証失敗 VLAN）に設定できます。

詳細については、「ゲスト VLAN に対する 802.1X 認証の概要」（p.39-8）を参照してください。

認証失敗 VLAN 設定時の注意事項および制限事項

ここでは、認証失敗 VLAN の設定時の注意事項および制限事項について説明します。

- 要求元による 802.1X 認証が 3 回失敗すると、ポートは要求元からのネットワーク アクセスが可能な認証失敗 VLAN に移動されます。3 回の試行では、ポートが認証失敗 VLAN でイネーブルにされ、EAP 成功パケットが要求元に送信されるまで 3 分間の遅延が生じます（失敗したあとにデフォルト待機時間の 60 秒に基づいて、それぞれの失敗で 1 分間の遅延が生じます）。
- 失敗した 802.1X 認証の回数は、リンク確立後からポートが認証失敗 VLAN に移動するまで数えられます。ポートが認証失敗 VLAN に移動すると、失敗回数カウンタがリセットされます。
- 認証に失敗したユーザだけが認証失敗 VLAN に移動されます。
- 認証失敗 VLAN は、単一認証モード（デフォルト ポート モード）でのみサポートされています。
- 認証失敗 VLAN は、単一方向ポートとして設定されたポートではサポートされていません。
- 要求元の MAC アドレスが CAM テーブルに追加され、この MAC アドレスだけが認証失敗 VLAN ポートで許可されます。ポートに新たに現れる MAC アドレスは、セキュリティ違反として扱われます。
- 認証失敗 VLAN ポートを RSPAN VLAN またはプライベート VLAN の一部にすることはできません。
- Multiple VLAN Access Port（MVAP）では、認証失敗 VLAN と補助 VLAN を同じにすることはできません。
- 認証失敗 VLAN およびポート セキュリティ機能は、相互に競合しません。さらに、Dynamic ARP Inspection（DAI）、DHCP スヌーピング、および IP ソース ガードなどの他のセキュリティ機能を認証失敗 VLAN で個別にイネーブルまたはディセーブルにできます。
- 認証失敗 VLAN は、ゲスト VLAN とは無関係です。ただし、ゲスト VLAN と認証失敗 VLAN を同じ VLAN にすることができます。802.1X 非対応ホストと認証失敗ホストを区別しない場合は、両方を同じ VLAN（ゲスト VLAN または認証失敗 VLAN）に設定できます。
- 認証失敗 VLAN では、ハイ アベイラビリティがサポートされています。

認証失敗 VLAN の作成および 802.1X ポートの追加

認証失敗 VLAN を作成し、VLAN に 802.1X ポートを追加するには、イネーブル モードで次の作業を行います。

作業	コマンド
認証失敗 VLAN を作成し、VLAN に 802.1X ポートを追加します。	**set port dot1x** *mod/ports* **auth-fail-vlan** {**none** | *vlan*}

次に、認証失敗 VLAN（VLAN 81）を作成し、ポート 3/33 を追加する例を示します。

```
Console> (enable) set port dot1x 3/33 auth-fail-vlan 81
Port 3/33 Auth Fail Vlan is set to 81
Console> (enable)
```

次に、認証失敗 VLAN の設定を表示する例を示します。

```
Console> (enable) show port dot1x auth-fail-vlan
Auth-Fail-Vlan Status   Mod/Ports
-------------- -------- ------------------
81             active   3/33
none           none     1/1-2,2/1-2,3/1-32,3/34-48
Console> (enable)
```

次に、認証失敗 VLAN からポートを消去する例を示します。

```
Console> (enable) set port dot1x 3/33 auth-fail-vlan none
Port 3/33 Auth Fail Vlan is cleared
Console> (enable)
```

次に、認証失敗 VLAN のアクティブ ユーザおよびポートを表示する例を示します。

```
Console> (enable) show dot1x auth-fail-users
Username       Mod/Port   Auth-Fail-Vlan
--------       --------   --------------
testuser       3/33       81
Console> (enable)
```

RADIUS サーバ フェールオーバーの設定

Release 8.4(1) より前のソフトウェア リリースでは、アクティブ RADIUS サーバがダウンまたは到達不能になった場合に、バックアップ RADIUS サーバがアクティブになる前に 802.1X 認証がタイムアウトしていました。Release 8.4(1) およびこれ以降のソフトウェア リリースでは、一部の RADIUS サーバ タイマー値を設定することが可能で、**show radius** コマンドはアクティブ RADIUS サーバを表示するように拡張されました。

RADIUS サーバ フェールオーバーを回避するには、次のコマンドを入力します。

- **set dot1x max-req** ― ステート マシンが認証セッションをタイムアウトするまでに、ステート マシンが要求元に EAP-Request フレームを再送信する最大回数を指定します。有効な値は、1 ～ 10 です。デフォルトは 2 です。次に例を示します。

  ```
  Console> (enable) set dot1x max-req 8
  dot1x max-req set to 8.
  Console> (enable)
  ```

- **set dot1x server-timeout** ― バックエンド認証者から認証サーバへのパケット再送信の時間定数を指定します。有効な値は、1 ～ 65535 秒です。認証サーバがバックエンド認証者に特定のパケットを受信したことを通知しない場合、バックエンド認証者は一定期間（**server-timeout** *seconds* パラメータを入力して設定）待機してから、パケットを再送信します。デフォルトは 30 です。次に例を示します。

```
Console> (enable) set dot1x server-timeout 100
dot1x server-timeout set to 100 seconds.
Console> (enable)
```

次に、**show radius** コマンドを入力して、RADIUS サーバ コンフィギュレーションを表示し、アクティブな RADIUS サーバを確認する例を示します。

```
Console> (enable) show radius
Active RADIUS Server:        81.81.81.20
RADIUS Deadtime:             1 minutes
RADIUS Key:                  cisco
RADIUS Retransmit:           2
RADIUS Timeout:              5 seconds
Framed-Ip Address Transmit:  Disabled

RADIUS-Server                    Status  Auth-port Acct-port Resolved IP Address
-------------------------------- ------- --------- --------- -------------------
81.81.81.20                      primary 1812      1813
10.6.89.200                              1812      1813
10.6.98.35                               1812      1813
Console> (enable)
```

show コマンドの使用方法

802.1X 認証とその設定に関する情報を表示するには、**show** コマンドを使用します。

- **show port dot1x ?**
- **show port dot1x**
- **show port dot1x statistics**
- **show dot1x**
- **show cam static**

show port dot1x コマンドの使用方法のオプションを表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
show port dot1x コマンドの使用方法のオプションを表示します。	**show port dot1x ?**

次に、**show port dot1x** コマンドの使用方法のオプションを表示する例を示します。

```
Console> (enable) show port dot1x ?
  guest-vlan                Show Port guest vlan information
  statistics                Show statistic information
  <mod>                     Module number
  <mod/port>                Module number and Port number(s)
  |                         Output modifiers
  <cr>
```

特定モジュールの特定ポート上での認証者 PAE およびバックエンド認証者に関するすべてのパラメータの値を表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
特定モジュールの特定ポート上での、認証者 PAE およびバックエンド認証者に関するすべての設定可能なパラメータ値および現在のステート パラメータ値を表示します。	**show port dot1x** *mod/port*

次に、モジュール 3 のポート 1 上での認証者 PAE およびバックエンド認証者に関するすべてのパラメータ値を表示する例を示します。

```
Console> (enable) show port dot1x 3/1
Port  Auth-State          BEnd-State Port-Control        Port-Status
----- ------------------- ---------- ------------------- -------------
 3/1  connecting          idle       auto                unauthorized

Port  Port-Mode     Re-authentication   Shutdown-timeout   Control-Mode
                                                           admin   oper
----- ------------ -----------------   ----------------   ---------------
 3/1  SingleAuth    enabled             disabled           In      Both
Console> (enable)
```

特定モジュールの特定ポート上で認証者によって送受信される EAP フレーム別の統計情報を表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
特定モジュールの特定ポート上で認証者によって送受信される EAP フレーム別の統計情報を表示します。	**show port dot1x statistics** *mod/port*

次に、モジュール 3 のポート 1 上で認証者によって送受信される EAP フレーム別の統計情報を表示する例を示します。

```
Console> (enable) show port dot1x statistics 3/1
Port   Tx_Req/Id Tx_Req Tx_Total Rx_Start Rx_Logoff Rx_Resp/Id Rx_Resp
-----  --------- ------ -------- -------- --------- ---------- -------
 3/1   43        0      43       0        0         0          0

Port   Rx_Invalid Rx_Len_Err Rx_Total Last_Rx_Frm_Ver Last_Rx_Frm_Src_Mac
-----  ---------- ---------- -------- --------------- -------------------
 3/1   2          0          2        0               00-00-00-00-00-00
Console> (enable)
```

グローバル 802.1X パラメータを表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
PAE 機能、プロトコルのバージョン、system-auth-control、およびその他のグローバル dotlx パラメータを表示します。	**show dot1x**

次に、グローバル 802.1X パラメータを表示する例を示します。

```
Console> (enable) show dot1x
PAE Capability              Authenticator Only
Protocol Version            1
system-auth-control         enabled
max-req                     2
quiet-period                60 seconds
radius-accounting           disabled
radius-vlan-assignment      enabled
radius-keepalive state      enabled
re-authperiod               7200 seconds
server-timeout              30 seconds
shutdown-timeout            300 seconds
supp-timeout                30 seconds
tx-period                   30 seconds

Console> (enable)
```

802.1X 認証 MAC アドレスを表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
802.1X 認証 MAC アドレスを表示します。	**show cam static**

次に、802.1X 認証 MAC アドレスを表示する例を示します。この例では、802.1X とポート セキュリティの両方がイネーブルに設定されています。

```
Console> (enable) show cam static 8/17
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry $ = Dot1x Security Entry

VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs / [Protocol Type]
----  ------------------    -----  ------------------------------------------
12    00-40-ca-13-ae-bf  $          8/17
17    00-30-94-c2-c3-c1  X          8/17
Total Matching CAM Entries Displayed  =2
Console> (enable)
```

CHAPTER 40

MAC 認証バイパスの設定

この章では、Catalyst 6500 シリーズ スイッチ上で MAC（メディア アクセス制御）認証バイパスを設定する手順について説明します。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

(注) IEEE 802.1X 認証の設定については、第 39 章「802.1X 認証の設定」を参照してください。

(注) イーサネット、ファスト イーサネット、またはギガビット イーサネット ポートへのアクセスを試みたステーションの MAC アドレスが、そのポートに指定されている MAC アドレスと異なる場合に、ポート セキュリティ機能を使用してポートへのアクセスをブロックする手順については、第 37 章「ポート セキュリティの設定」を参照してください。また、ホスト MAC アドレスに基づく指定ホストに送信、または指定ホストから受信したトラフィックをフィルタリングする場合に、ポート セキュリティ機能を使用する手順についても説明します。

(注) Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）を設定して、Catalyst 6500 シリーズ スイッチの CLI（コマンドライン インターフェイス）へのアクセスをモニタおよび制御する方法については、第 38 章「AAA によるスイッチ アクセスの設定」を参照してください。

この章で説明する内容は、次のとおりです。

MAC 認証バイパス機能の概要

ここでは、Catalyst 6500 シリーズ スイッチの MAC 認証バイパス機能について説明します。

概要

MAC 認証バイパスは、802.1X の要求元機能を持たない装置（プリンタおよび IP Phone など）へのネットワーク アクセスを可能にする 802.1 X に代わるものです。MAC 認証バイパスは、接続装置の MAC アドレスを使用してネットワーク アクセスを許可または拒否します。

MAC 認証バイパスをサポートするために、RADIUS 認証サーバでは、ネットワークへのアクセスが必要な装置の　MAC　アドレスのデータベースを維持します。MAC　認証バイパスは、Calling-Station-ID（属性 31）として MAC アドレスおよび値が 10 の Service-Type（属性 6）を含む RADIUS 要求を生成します。

装置の MAC アドレスを入手するには、スイッチ ポートを VLAN（仮想 LAN）内でフォワーディング ステートにする必要があります。ポートが VLAN でフォワーディング ステートでなければ、スイッチ上でユニキャスト トラフィックを受信または送信できません。スイッチ ポートは、ポート上でラーニングがディセーブルなネイティブ VLAN で起動するため、パケットはスーパバイザ エンジンにリダイレクトされます。スーパバイザ エンジンが新しい MAC アドレスを確認すると、CAM（連想メモリ）エントリおよびトラップ ビットを挿入します。トラップ ビットは、MAC アドレスからの不必要なフラッディングからスーパバイザ エンジンを保護するよう設定されています。スーパバイザ エンジンは、MAC 認証が終了するまで、それ以上のパケットをリダイレクトしません。認証が成功すると、RADIUS サーバが VLAN を送信し、ポートはこの VLAN に移行します。認証成功後、トラップ エントリは削除されます。RADIUS サーバ指定の VLAN に移行したポートは、他のスイッチ ポートと同様に動作します。MAC 認証が失敗した場合、ポートは認証失敗 VLAN（設定されている場合）に移行します（認証失敗 VLAN については、「認証失敗 VLAN の設定」[p.39-37]を参照）。

MAC アドレス再認証の概要

再認証モードでは、ポートは RADIUS サーバ指定の VLAN のままで自身を再認証しようとします。再認証が成功した場合、ポートは RADIUS サーバ指定の VLAN のままです。再認証が失敗した場合、ポートは認証失敗 VLAN（設定されている場合）に移行されるか、または既存の VLAN から管理上設定された VLAN に移行されます。失敗したポートには、定期的に再認証が試されます。以前認証された VLAN 上の失敗ポートの MAC アドレス CAM エントリは削除され、ポートは初期化プロセスにより、自動的に管理上設定された VLAN に移行し、ポート自身への再認証を試行します。再認証が成功した場合、ポートは RADIUS サーバ指定の VLAN に移行されます。

また、RADIUS サーバ指定のタイマーも再認証をトリガーします。RADIUS サーバの属性 27 および 29 は、再認証動作を制御します。属性 27（セッション タイムアウト）では、認証が再試行されるまでの時間を指定し、属性 29（ターミネーション アクション）では、再認証動作が次のいずれになるかを指定します。

- 初期化 ― 既存のセッションは、再認証結果が確認できるまで、中断されます。
- 再認証 ― 再認証試行中は、既存のセッションは中断されません。

MAC 認証バイパス ステートの概要

ここでは、次の MAC 認証バイパス ステートについて説明します。

- 待機 ― 待機ステートの場合、スイッチは認証される必要がある MAC アドレスの受信を待機します。ラーニングはディセーブルで、アイドル タイマーが開始します。ポートは、フォワーディング ステートでユニキャスト トラフィックを受信し、ポート上のすべてのレイヤ 2 エントリは消去されます。他に機能が設定されている場合は、ポートは認証結果を待ってから（結果が成功でも失敗でも）他のステートに移行します。トラフィックが確認されなければ、ポートは待機ステートのままです。
- 認証 ― スイッチがリダイレクトされたパケットからポートの MAC アドレスを学習すると、MAC 認証バイパス ステート マシンは認証に移行します。このステートでは、RADIUS 要求が作成され、RADIUS サーバに送信されます。スイッチは、RADIUS サーバ応答を待機します。認証が成功すると、ポートは認証済みステートに移行します。このステートでは、ポート上で RADIUS サーバ指定の VLAN が設定され、スタティック CAM エントリが RADIUS サーバ指定の VLAN に挿入され、古い VLAN 上のトラップ エントリは削除されます。認証に失敗すると、ポートは認証失敗ステートに移行します。RADIUS タイムアウトまたは初期化が発生した場合、ポートは再度待機ステートに移行します。
- 認証済み ― 認証済みステートでは、RADIUS が受信したポリシー（VLAN）がポート上で設定されます。初期化がある場合、ポートは待機ステートに移行し、再認証イベントを受信すると、認証ステートに移行します。認証済みステートでは、ポート上のトラップ エントリが古い VLAN から削除され、スタティック CAM エントリが新しい VLAN に挿入されます。
- 認証失敗 ― 認証失敗ステートでは、他の機能が設定されていなければ、ポートは待機ステートに移行するまで [auth-fail-timeout]（秒）待機します。フォールバック機能（Web ベースのプロキシ認証、802.1X、または認証失敗 VLAN など）が設定されている場合、ポートはこれらのステートに移行します。トラップは認証失敗ステートのまま存在するため、MAC アドレスは [auth-fail-timeout]（秒）間自身を再認証できません。ポートが認証失敗ステートから待機ステートに移行すると、トラップ エントリは消去され、ポートは認証プロセスを再開します。
- 終了 ― MAC 認証バイパスがホストの認証に失敗すると、アクセスを許可する可能性がある他の機能（Web ベースのプロキシ認証、802.1X、または認証失敗 VLAN）がポートに設定されていない場合は、終了ステートになります。終了ステートでは、ポートの許可 / アップ、およびほかの機能で必要とされる任意のポリシーの付加が行われます。たとえば、ゲスト VLAN が設定されている場合、ポートはゲスト VLAN に追加されます。Web ベースのプロキシ認証が設定されている場合は、HTTP リダイレクションなどで Dynamic Host Configuration Protocol（DHCP）、Domain Name System（DNS; ドメイン ネーム システム）、Access Control Entry（ACE; アクセス制御エントリ）を許可するためにポリシーが付加されます。他の機能が設定されていない場合は、認証が失敗すると、ポートは待機、認証、認証失敗、および待機ステートを移動するか、またはトラフィックを確認するまで待機ステートのままです。

MAC 認証バイパス ステート イベントの概要

ここでは、次の MAC 認証バイパス イベントについて説明します。

- AuthenticateMac ― このイベントは、コンポーネントを処理するリダイレクトされたパケットがポート上で MAC アドレスを確認すると、通知されます。このイベントは、MAC 認証バイパス ステート マシンが待機ステートの場合に通知されます。
- Initialize ― このイベントは CLI によりトリガーされ、どのステートでも受信されます。このイベントを受信すると、ポートは待機ステートに移行し、クリーンアップ（ポートの拒否、任意のスタティック エントリまたはトラップ CAM エントリのクリーンアップなど）が必要な場合は、実行します。
- Reauthenticate ― このイベントは、セッションタイムアウトの時間切れか、または CLI トリガー（CLI から入力された実行コマンド）が原因で受信されます。このイベントは、ポートが認証済みステートである場合にのみ受け入れられます。それ以外の場合、無視されます。CLI により発生したイベントでは、CLI はポートが認証済みステートの場合にのみ受け入れられることを通知します。

- Authentication success ― このイベントは、RADIUS サーバからの認証が成功した場合に、通知されます。このイベントは、ポートが認証ステートの場合にのみ受け入れられ、ポートを認証済みステートに移行させます。
- Authentication failure ― このイベントは、RADIUS サーバからの認証失敗を受信した場合に、通知されます。このイベントは、ポートが認証ステートの場合にのみ受け入れられ、このポートを認証失敗ステートに移行させます。
- RADIUS timeout ― このイベントは、RADIUS サーバが応答しない場合に受信されます。このイベントはポートが認証ステートの場合にのみ受け入れられ、最大再試行回数の満了後、RADIUS サーバが応答しなければ、ポートを待機ステートに移行させます。
- AuthFail timeout ― このイベントは、ポートが RADIUS サーバの認証失敗による認証失敗ステートにあり、ポートをアップにするその他の潜在的機能が設定されていない場合に、受信されます。このイベントにより、ポートは待機ステートに移行し、認証プロセスを再開します。
- Security violation ― このイベントは、待機ステート以外のすべてのステートで受信されます。このイベントは、ポート上で 2 つめの MAC アドレスが確認された場合に通知されます。セキュリティ違反の場合に行う措置は、MAC アドレスの制限またはポートのシャット ダウンのいずれかで、設定されたグローバル違反モードによって異なります。

MAC 認証バイパスの設定時の注意事項および制限事項

ここでは、MAC 認証バイパスの設定時の注意事項および制限事項について説明します。

- セキュリティ違反 — MAC 認証バイパスでは、ポートごとに 1 つのホストのみがサポートされます。ポート上に複数のホストが表示された場合、セキュリティ違反となりポートはシャットダウンします。補助 VLAN ポートの場合、ポートごとに 1 つのホストの制限はデータ VLAN 上のホストにのみ適用されます。つまり、補助（音声）VLAN ではホスト数の制限はありません。
- ポリシーの適用 — MAC 認証バイパスでは、802.1X でサポートされるすべてのポリシー適用メカニズムがサポートされます。
- DHCP スヌーピング — MAC 認証バイパスは、DHCP スヌーピングとは無関係です。MAC アドレスが認証に成功するまでは、MAC アドレスからのトラフィックは許可されず（トラップ エントリのため）、MAC 認証のトリガーとなるトラフィックは DHCP など任意のタイプのトラフィックとなります。
- 802.1X — MAC 認証バイパスは独立した機能ですが、802.1X と組み合わせて使用する場合は、MAC アドレス認証の代替として機能します。ポート上で MAC 認証バイパスと 802.1X の両方が設定されている場合、ポートは 802.1X を使用して認証しようとします。ホストが EAPOL 要求に応答しない場合、認証試行を継続せずに、802.1X ポートが MAC 認証バイパス ステートに移行され、MAC 認証バイパスを使用して認証が試行されます。
- 認証失敗 VLAN — 802.1X 認証が失敗すると、MAC 認証バイパスが設定されているかどうかに関わらず、認証失敗 VLAN が設定されている場合は、ポートは認証失敗 VLAN に移行されます。この認証失敗 VLAN は、802.1X 認証失敗ユーザ専用で、MAC 認証バイパス用の汎用認証失敗 VLAN ではありません。認証失敗 VLAN については、「認証失敗 VLAN の設定」（p.39-37）を参照してください。
- ゲスト VLAN — 802.1X ゲスト VLAN および MAC 認証バイパスは、既存のゲスト VLAN 動作に対する一部の変更点を除いて、連動します。MAC 認証バイパスおよび ゲスト VLAN が設定されていて、ポートで Extensible Authentication Protocol over LAN （EAPOL）パケットが受信されない場合、802.1X ステート マシンは MAC 認証バイパス ステートに移行され、ポートをネイティブ VLAN でフォワーディングに設定し、ラーニングをディセーブルにします。ゲスト VLAN が設定されていない場合、ポートは MAC 認証バイパス ステートのままでポート上の MAC アドレスを待機します。ゲスト VLAN の詳細については、「ゲスト VLAN に対する 802.1X 認証の概要」（p.39-8）を参照してください。
- ポート セキュリティ — 新しくリダイレクトされた MAC アドレスは、ポート セキュリティより先に MAC 認証バイパス機能により確認されます。MAC アドレスが認証に成功すると、新しく学習された MAC アドレスがポート セキュリティ機能に通知されます。着信パスでは、MAC 認証バイパス機能はどのポート セキュリティ機能よりも先に開始します。
- 補助 VLAN — MAC 認証バイパスは、補助（音声）VLAN でサポートされます。MAC 認証バイパスは、ポート VLAN 上でのみ表示される MAC アドレスに制限されます。Cisco Discovery Protocol（CDP）を介して学習されるすべての IP Phone MAC アドレスは、補助 VLAN 上で許可されます。
- Dynamic ARP Inspection（DAI）— MAC 認証バイパスと連動します。
- VLAN Management Policy Server（VMPS; VLAN マネジメント ポリシー サーバ）— MAC 認証バイパスおよび VMPS を同時に使用することはできません。CLI により、同時に両方の機能を設定できないようにされます。
- LAN ポート IP — MAC 認証バイパスと LAN ポート IP の両方を設定する場合、先に MAC 認証バイパスが実行されます。認証後、MAC 認証バイパス機能が LAN ポート IP 機能のトリガーとなります。LAN ポート IP 例外リスト内のホストは、MAC 認証バイパス（設定されている場合）による認証後、アクセスできるようになります。
- Web ベース プロキシ認証 — インターフェイスで MAC 認証バイパスと Web ベース プロキシ認証の両方が設定されている場合、MAC 認証バイパスはレイヤ 2 の機能であるため、Web ベース プロキシ認証より先に MAC 認証バイパスが開始します。レイヤ 2 の機能は常に、レイヤ 3 の機能よりも先に試行されます。
- RADIUS アカウンティング — RADIUS アカウンティングがサポートされます。

- SNMP（簡易ネットワーク管理プロトコル）― 必要な Set および Get 要求はすべて、SNMP にエクスポートされます。MAC 認証バイパスに対する SNMP サポートは、今後のソフトウェア リリースで対応する予定です。
- ハイ アベイラビリティ ― ハイ アベイラビリティがサポートされます。ポートの MAC 認証バイパス の開始ステートと終了ステート（許可および無許可）は、スタンバイ スーパバイザ エンジンに同期化されます。中間ステートは、同期化されません。

MAC 認証バイパスの設定

ここでは、MAC 認証バイパスを設定する手順について説明します。

MAC 認証バイパスのグローバルなイネーブル化およびディセーブル化

デフォルトの設定はディセーブルです。MAC 認証バイパスをグローバルにイネーブルまたはディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
MAC 認証バイパスをグローバルにイネーブルまたはディセーブルにします。	**set mac-auth-bypass {disable | enable}**

次に、MAC 認証バイパスをグローバルにイネーブルにする例を示します。

```
Console> (enable) set mac-auth-bypass enable
Mac-Auth-Bypass enabled globally.
Console> (enable)
```

ポート上での MAC 認証バイパスのイネーブル化およびディセーブル化

ポート上で MAC 認証バイパスをイネーブルまたはディセーブルにする場合、同じポート上の PortFast も自動的にイネーブルまたはディセーブルになります。デフォルトでは、イネーブルです。

ポートで MAC 認証バイパスをイネーブルまたはディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
ポート上で MAC 認証バイパスをイネーブルまたはディセーブルにします。	**set port mac-auth-bypass** *mod/port* {**disable** | **enable**}

次に、ポートで MAC 認証バイパスをイネーブルにする例を示します。

```
Console> (enable) set port mac-auth-bypass 3/1 enable
MAC-Auth-Bypass successfully enabled on 3/1.
Console> (enable)
```

ポートの MAC 認証バイパス ステートの初期化

ポートの MAC 認証バイパス ステートを初期化して、ポートが再度認証を行えるようにするには、イネーブル モードで次の作業を実行します。

作業	コマンド
ポートの MAC 認証バイパス ステートを初期化して、ポートが再度認証を行えるようにします。	**set port mac-auth-bypass** *mod/port* **initialize**

次に、ポートの MAC 認証バイパス ステートを初期化して、ポートが再度認証を行えるようにする例を示します。

```
Console> (enable) set port mac-auth-bypass 3/1 initialize
Mac-Auth-Bypass successfully Initialized 3/1.
Console> (enable)
```

ポートの MAC アドレスの再認証

ポートの MAC アドレスを再認証するには、イネーブル モードで次の作業を行います。

作業	コマンド
ポートの MAC アドレスを再認証します。	**set port mac-auth-bypass** *mod/port* **reauthenticate**

次に、ポートの MAC アドレスを再認証する例を示します。

```
Console> (enable) set port mac-auth-bypass 3/1 reauthenticate
Reauthenticating MAC address 00-00-00-00-00-01 on port 3/1 using Mac-Auth-Bypass.
Console> (enable)
```

シャットダウン タイムアウト時間の指定

ポート上でセキュリティ違反があった場合、ポートはシャット ダウンされます。ポートが自動的に再イネーブル化されるまでのシャット ダウン時間（秒）を指定するには、グローバルな **set mac-auth-bypass shutdown-timeout** *seconds* コマンドを使用します。範囲は、30 ～ 65535 秒です。デフォルトは 60 秒です。シャットダウン タイムアウト時間を 0 秒に指定すると、自動ポート イネーブル機能がディセーブルとなり、手動でポートを再イネーブル化する必要があります。

シャットダウン タイムアウト時間を指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
シャットダウン タイムアウト時間を指定します。	**set mac-auth-bypass shutdown-timeout** *seconds*

次に、シャットダウン タイムアウト時間を指定する例を示します。

```
Console> (enable) set mac-auth-bypass shutdown-timeout 40
Shutdown Timeout set to 40 seconds.
Console> (enable)
```

認証失敗タイムアウト時間の指定

グローバルな **set mac-auth-bypass auth-fail-timeout** *seconds* コマンドにより、ポートが再認証を試行するまで認証失敗（AuthFail）ステートで待機する時間（秒）を指定できます。範囲は、5 ～ 65535 秒です。デフォルトの設定は 60 秒です。

認証失敗タイムアウト時間を指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
認証失敗タイムアウト時間を指定します。	**set mac-auth-bypass auth-fail-timeout** *seconds*

次に、認証失敗タイムアウト時間を指定する例を示します。

```
Console> (enable) set mac-auth-bypass auth-fail-timeout 60
Authfail Timeout set to 60 seconds.
Console> (enable)
```

再認証タイムアウト時間の指定

グローバルな **set mac-auth-bypass reauth-timeout** *seconds* コマンドにより、グローバルな再認証がイネーブルとなってから、再認証がトリガーされるまでの時間（秒）を指定できます。範囲は、300 ～ 65535 秒です。デフォルトの設定は 3600 秒です。

再認証タイムアウト時間を指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
再認証タイムアウト時間を指定します。	**set mac-auth-bypass reauth-timeout** *seconds*

次に、再認証タイムアウト時間を指定する例を示します。

```
Console> (enable) set mac-auth-bypass reauth-timeout 400
Reauth Timeout set to 400 seconds.
Console> (enable)
```

再認証のイネーブル化またはディセーブル化

グローバルな **set mac-auth-bypass re-authentication** コマンドをイネーブルにすると、すべての MAC 認証バイパス値がデフォルトに戻ります。デフォルトの設定はディセーブルです。

MAC 認証バイパス再認証をグローバルにイネーブルまたはディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
MAC 認証バイパス再認証をグローバルにイネーブルまたはディセーブルにします。	**set mac-auth-bypass reauthentication** {**disable** | **enable**}

次に、MAC 認証バイパス再認証をグローバルにイネーブルにする例を示します。

```
Console> (enable) set mac-auth-bypass reauthentication enable
Global reauthentication mode enabled.
Console> (enable)
```

セキュリティ違反モードの指定

ポート上でセキュリティ違反が発生すると、ポートは制限モードになるか、またはシャット ダウンされます。制限モードでは、セキュリティ違反の原因となる MAC アドレスが、トラップ エントリとしてフォワーディング テーブルに追加されます。デフォルトの設定はシャットダウンです。

セキュリティ違反モードをグローバルに指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
セキュリティ違反モードをグローバルに指定します。	**set mac-auth-bypass violation** {**restrict** | **shutdown**}

次に、セキュリティ違反モードで [restricted] を指定する例を示します。

```
Console> (enable) set mac-auth-bypass violation restrict
Mac-Auth-Bypass security violation mode set to restrict.
Console> (enable)
```

MAC 認証バイパス RADIUS アカウンティングのイネーブル化またはディセーブル化

デフォルトの設定はディセーブルです。MAC 認証バイパス RADIUS アカウンティングをイネーブルまたはディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
MAC 認証バイパス RADIUS アカウンティングをイネーブルまたはディセーブルにします。	**set mac-auth-bypass radius-accounting** {**disable** | **enable**}
MAC 認証バイパス RADIUS アカウンティング ステートを確認します。	**show mac-auth-bypass config**

次に、MAC 認証バイパス RADIUS アカウンティングをイネーブルにする例を示します。

```
Console> (enable) set mac-auth-bypass radius-accounting enable
Radius Accounting for MacAuth enabled.
Console> (enable)
```

次に、MAC 認証バイパス RADIUS アカウンティング ステートを確認する例を示します。

```
Console> (enable) show mac-auth-bypass config
Mac-Auth-Bypass Global Config
-----------------------------
Mac-Auth-Bypass Status      = Enabled
AuthFail Timeout            = 60
RadiusAccounting            = Enabled
Reauthentication            = Disabled
Reauth Timeout              = 3600
Shutdown Timeout            = 60
Violation mode              = Shutdown
Console> (enable)
```

MAC 認証バイパス情報の表示

show port mac-auth-bypass {*mod/port*} コマンドにより、ポート ステート（認証、認証済み、送信元 MAC アドレス学習の待機など）、およびポートの RADIUS サーバ指定の VLAN が表示されます。

MAC 認証バイパス情報を表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
MAC 認証バイパスがイネーブルなスイッチ上のすべてのポートまたは単一のポートの MAC 認証バイパス情報を表示します。	**show port mac-auth-bypass** [*mod/port*]
MAC 認証バイパスがイネーブルなスイッチ上のすべてのポートまたは指定の MAC アドレスを持つポートの MAC 認証バイパス情報を表示します。	**show mac-auth-bypass** {**all** | **config** | *mac_address*}

次に、ポート 5/1 の MAC 認証バイパス情報を表示する例を示します。

```
Console> (enable) show port mac-auth-bypass 5/1
Port  Mac-Auth-Bypass State MAC Address       Auth-State     Vlan
----- --------------------- ----------------- -------------- -----
 5/1  Disabled              -                 -              1

Port  Termination action Session Timeout Shutdown/Time-Left
----- ------------------ --------------- ------------------
 5/1  -                  3600            -        -
Console> (enable)
```

次に、MAC 認証バイパスがイネーブルなスイッチ上のすべてのポートの MAC 認証バイパス情報を表示する例を示します。

```
Console> (enable) show mac-auth-bypass all

Port  Mac-Auth-Bypass State MAC Address       Auth-State     Vlan
----- --------------------- ----------------- -------------- -----
 5/1  Disabled              -                 -              1
 5/2  Enabled               00-00-00-00-00-00 waiting        1
 5/3  Enabled               00-00-00-00-00-00 waiting        1
 5/4  Enabled               00-00-00-00-00-00 waiting        1
 5/5  Enabled               00-00-00-00-00-00 waiting        1
 5/6  Enabled               00-00-00-00-00-00 waiting        1
 5/7  Enabled               00-00-00-00-00-00 waiting        1
 5/8  Enabled               00-00-00-00-00-00 waiting        1
.
.
.
Port  Termination action Session Timeout Shutdown/Time-Left
----- ------------------ --------------- ------------------
 5/1  -                  3600            -        -
 5/2  reauthenticate     3600            NO       -
 5/3  reauthenticate     3600            NO       -
 5/4  reauthenticate     3600            NO       -
 5/5  reauthenticate     3600            NO       -
 5/6  reauthenticate     3600            NO       -
 5/7  reauthenticate     3600            NO       -
 5/8  reauthenticate     3600            NO       -
.
.
.
Console> (enable)
```

MAC 認証バイパスのグローバル設定の表示

show mac-auth-bypass config コマンドにより、MAC 認証バイパスのグローバルな設定値（タイマー値、違反モード、グローバル再認証モードなど）が表示されます。

MAC 認証バイパスのグローバルな設定値を表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
MAC 認証バイパスのグローバルな設定値を表示します。	**show mac-auth-bypass** {**all** | **config** | *mac_address*}

次に、MAC 認証バイパスのグローバルな設定値を表示する例を示します。

```
Console> (enable) show mac-auth-bypass config
Mac-Auth-Bypass Global Config
-----------------------------
Mac-Auth-Bypass Status      = Enabled
AuthFail Timeout            = 60
RadiusAccounting            = Enabled
Reauthentication            = Disabled
Reauth Timeout              = 3600
Shutdown Timeout            = 60
Violation mode              = Shutdown
Console> (enable)
```

CHAPTER 41

Web ベース プロキシ認証の設定

この章では、Catalyst 6500 シリーズ スイッチ上で Web ベース プロキシ認証を設定する手順について説明します。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

(注) IEEE 802.1X 認証の設定については、第 39 章「802.1X 認証の設定」を参照してください。

(注) MAC（メディア アクセス制御）アドレス認証バイパスの設定については、第 40 章「MAC 認証バイパスの設定」を参照してください。

(注) イーサネット、ファスト イーサネット、またはギガビット イーサネット ポートへのアクセスを試みたステーションの MAC アドレスが、そのポートに指定されている MAC アドレスと異なる場合に、ポート セキュリティ機能を使用してポートへのアクセスをブロックする手順については、第 37 章「ポート セキュリティの設定」を参照してください。また、ホスト MAC アドレスに基づく指定ホストに送信、または指定ホストから受信したトラフィックをフィルタリングする場合に、ポート セキュリティ機能を使用する手順についても説明します。

(注) Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）を設定して、Catalyst 6500 シリーズ スイッチの CLI（コマンドライン インターフェイス）へのアクセスをモニタおよび制御する方法については、第 38 章「AAA によるスイッチ アクセスの設定」を参照してください。

この章で説明する内容は、次のとおりです。

Web ベース プロキシ認証の機能概要

Catalyst 6500 シリーズ スイッチは、ネットワーク クライアントが IEEE 802.1X ホストをサポートしない場合、Web ベース プロキシ認証を行います。Web ベース プロキシ認証では、フロントエンド システムの標準 Web ベース インターフェイス（HTTP/HTTPS）を介して、クライアント ID および証明書入力の認証を行います。

802.1X ポートベース認証では、LAN およびスイッチのサービスにアクセスし、スイッチからの要求に応答するために、*要求元*が必要です。

（注） 802.1X では、*クライアント*または*ホスト*に対して*要求元*という用語を使用します。Catalyst 6500 シリーズ CLI の構文では*ホスト*が使用されるので、このマニュアルでは、*要求元*ではなく*ホスト*を使用します。

Web ベース プロキシ認証では、すべての 802.1X 認証をサポートし、ホスト非対応クライアントのサポートを提供します。

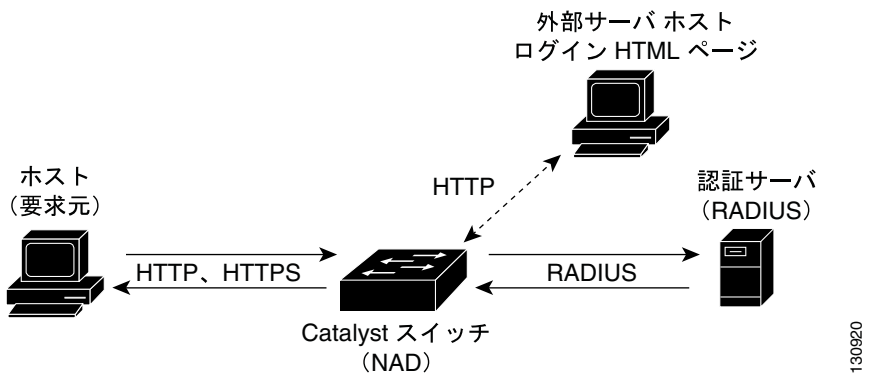
802.1X 認証については、「802.1X 認証の設定」の章を参照してください。

ここでは、Web ベース プロキシ認証機能について説明します。

デバイスの役割

Web ベース プロキシ認証は、標準の Web ベース インターフェイスを介して認証を行います（図 41-1 を参照）。

図 41-1　デバイス統合 Web ベース プロキシ認証



ホスト（要求元）— Web ベース プロキシ認証をイネーブルにすると、ホストは LAN およびスイッチ サービスへのアクセスを要求し、スイッチからの要求に応答できるようになります。

スイッチ — ホストが Web ベース プロキシ認証がイネーブルなスイッチ ポートに接続している場合、Network Access Device（NAD）または Catalyst 6500 シリーズ スイッチは、すべての HTML ページをホスティングします。ログイン Web ページは、ローカル ファイル システムまたは外部 Web サーバでホスティングされます。ホストが IP アドレスを受信すると、Web ブラウザが開かれます。HTTP パケットが代行受信されると、Catalyst 6500 シリーズ スイッチはホストとの TCP 接続を確立し、ログイン Web ページを送信するか（ログイン Web ページがスイッチ上でローカルに保管されている場合）、または URL が外部ログイン Web ページの URL のロケーションにクライアントをリダイレクトします。外部 Web サーバから直接ログイン ページをダウンロードできます。

証明書（ユーザ名、パスワード、およびその他のオプションを含む）は、ホストで入力されます。次に、ホストはそのページを提出します。Catalyst 6500 シリーズ スイッチは、この HTTP POST 要求を代行受信して、接続を確立し、POST 要求を取り込みます。Catalyst 6500 シリーズ スイッチは POST 要求を取り込むと、Web ページを処理して証明書を抽出します。

認証サーバ — サーバはホストの ID を確認し、このホストが LAN およびスイッチ サービスへのアクセスを許可されているかどうかをスイッチに通知します。スイッチはプロキシとして機能するので、認証サービスはホストにトランスペアレントです。Extensible Authentication Protocol（EAP）拡張機能搭載の Remote Authentication Dial-In User Service（RADIUS）セキュリティ システムが唯一のサポート対象認証サーバです。Cisco Secure Access Control Server バージョン 3.0 で利用できます。RADIUS は、RADIUS サーバと 1 つまたは複数の RADIUS クライアント間で安全な認証情報が交換されるクライアント / サーバ モデルで動作します。

認証の開始とメッセージ交換

ホストは、Web 認証を実行する必要があるスイッチ ポートと接続されます。ホストが IP アドレスを受信すると、Web ブラウザが開かれます。HTTP パケットが代行受信されると、NAD はホストとの TCP 接続を確立し、ログイン Web ページを送信するか（ログイン Web ページがスイッチ上でローカルに保管されている場合）、または URL が外部ログイン Web ページの URL のロケーションにクライアントをリダイレクトして、クライアントが外部 Web サーバから直接ログイン ページをダウンロードできるようにします。

証明書（ユーザ名、パスワード、およびその他のオプションを含む）は、ホストから入力および提出できます。NAD はこの情報を代行受信して、接続を確立し、要求を取り込みます。次に、NAD は Web ページ情報を処理して、外部 Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）サーバ（RADIUS）により認証される証明書を抽出します。次のように、NAD は認証結果に基づいて、クライアントに認証成功または認証失敗のページを送信します。

- 認証が成功した場合、NAD はこのホストの RADIUS から受信した新しいポリシー グループにより Policy-based ACL（PBACL）を更新します。URL は、クライアントが最初にアクセスしようとした URL にクライアントをリダイレクトします。
- 認証が失敗した場合、NAD はホストにログイン失敗 Web ページを送信します。ここでは、ログイン失敗フィールドおよび入力フィールドが示されます。外部のログイン失敗ページが指定される場合、NAD URL はログイン失敗ページのロケーションにクライアントをリダイレクトします。

ログインまたはログイン失敗ページが外部の Web サーバを示す場合、ホストが認証される前でも、デフォルト ポリシーによりこの Web サーバへの HTTP アクセスが許可されます。

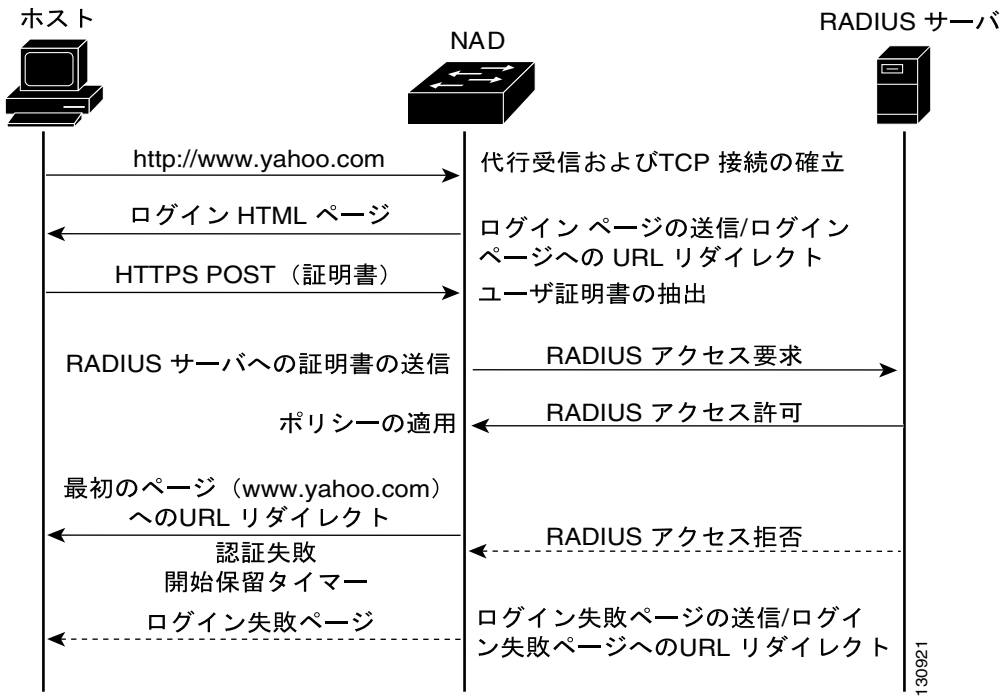
（注） デフォルト ポリシーが HTTP アクセスおよび外部ページを許可しない場合は、クライアントはこれらの Web ページをダウンロードできず、Web ベース プロキシ認証は機能しません。

ログイン / ログイン失敗ページには、NAD が処理するようプログラミングされているユーザ名、パスワード、およびその他のフィールドと同じ変数名と変数タイプが含まれます。デフォルト ページは、NAD 上でログイン ファイルが設定されていない場合に使用されます。

最初のログイン ページは、HTTP および HTTPS を使用して送信され、Catalyst 6500 シリーズ スイッチにユーザ証明書を提出するのに使用されます。HTTPS 機能が完全に動作可能となるまで、証明書転送には HTTP が使用されます。

認証開始およびメッセージ交換の一連のイベントに関しては、図 41-2 を参照してください。

図 41-2　認証の開始とメッセージ交換



ホスト検出および HTTP トラフィックの代行受信

Address Resolution Protocol（ARP; アドレス解決プロトコル）検査は、割り当てられたスタティックな IP アドレスによりホストのアドレスを指定するのに使用されます。ARP 検査が Web 認証ポート上で任意の ARP 要求を受信すると、Web ベース プロキシ認証がホスト IP アドレス用にトリガーされます。Web ベース プロキシ認証が動作可能なポート上でイネーブルの場合、Web ベース プロキシ認証が Dynamic Host Configuration Protocol（DHCP）スヌーピング テーブル内のすべての IP アドレスで開始されます。DHCP スヌーピング エントリが存在しない場合、DHCP スヌーピング エントリが作成されるか、または ARP 要求が受信されるまで、Web ベース プロキシ認証はトリガーされません。

ホストが検出されると、ホストからの HTTP トラフィックは代行受信され、スーパバイザ エンジンにリダイレクトされます。このプロセスは、URL リダイレクションともいいます。URL リダイレクションを設定するには、**permit url-redirect** コマンドを入力して、Access Control List（ACL; アクセス制御リスト）を設定し、スーパバイザ エンジンにすべての TCP ポート 80 およびポート 8080 の着信トラフィックをリダイレクトする必要があります。**permit url-redirect** コマンドにより、すべての TCP ポート 80 およびポート 8080 のトラフィックがスーパバイザ エンジンにリダイレクトされます。

この Access Control Entry（ACE; アクセス制御エントリ）によりポート / ポート VLAN にマッピングされる任意の ACL は、ACE 基準に一致するすべての HTTP/HTTPS プロトコル パケットをスーパバイザ エンジンにリダイレクトします。

この ACE を設定せずに、Web ベース プロキシ認証をイネーブルにすると、HTTP/HTTPS パケットは代行受信されず、認証は開始されません。この場合、ホスト トラフィックはポート /VLAN 上に設定されたデフォルト ポリシーにより制御されます。

Web ベース プロキシ認証では、新しいホストが検出されると、ソフトウェアを介して URL リダイレクションを通知し、代行受信された HTTP パケットにコールバック機能を提供します。

アクセス制御

アクセス制御は、PBACL により提供されます。PBACL を使用して、代行受信、デフォルト、およびホスト固有の ACL を設定できます。

PBACL は、VLAN にマッピングされます。VLAN 内のすべてのポートは、PBACL よってのみデフォルト アクセスが指定されています。

（注） VLAN 内のすべてのポート上で、Web ベース プロキシ認証をイネーブルにすることを推奨します。

Web ベース プロキシ認証でサポートされる HTML ページ

ここでは、Web ベース プロキシ認証をサポートするのに必要な次の HTML ページについて説明します。

- ログイン ページ（p.41-5）
- 成功ページ（p.41-6）
- ログイン失敗ページ（p.41-6）

ログイン ページ

ログイン ページは、クライアント側で最初の URL 代行受信への応答として表示されます。Web ベース プロキシ認証は、カスタマイズされたログイン ページをサポートします。カスタマイズされたログイン ページには、ログイン ページの URL（HTTP のみ）が必要です。ログイン ページには、次のフィールドが含まれます。

- ユーザ名 ― 文字列
- パスワード ― 文字列
- 次のオプション付きオプション ボタン
  - I have a registered account（登録済みアカウントがある）
  - I have a Guest account（ゲスト アカウントがある）
  - I don’t have an account（アカウントがない）

（注） スイッチが HTTPS プロトコルをサポートしている場合、ログイン ページの送信ボタンは HTTPS URL を示します。スイッチが HTTPS をサポートしていない場合、ログイン ページは HTTP URL を示します。

カスタマイズされたログイン ページが指定されない場合、デフォルトのログイン ページが送信されます。

成功ページ

成功ページは、認証成功後に表示されます。成功ページは、最初にアクセスを試みた URL にクライアント ブラウザを自動的にリダイレクトする自動リダイレクション ページです。

ログイン失敗ページ

ログイン失敗ページには、認証失敗についての情報が含まれます。ここでは、認証失敗の場合に証明書を再入力できます。ログイン失敗ページには、ログイン ページのすべてのフィールドおよび認証失敗についての情報が含まれます。

（注） 誤ったユーザ名 / パスワードを入力したり、[I don’t have an account] オプションを選択したり、スイッチでこのオプションのデフォルト ポリシーが設定されていない場合、認証失敗が発生する可能性があります。

カスタマイズされたログイン失敗ページが指定されない場合、デフォルトのログイン失敗ページが表示されます。

ポートごとに複数のホスト

Web ベース プロキシ認証では、ポート上で確認されるすべてのホスト（IP アドレス）を認証します。ポート上でサポートされるホストの最大数は、32 です。

ポート上で確認されたすべての新しいホストには、新しい Web ベース プロキシ認証ステートが作成されます。複数の DHCP バインディングがすでに作成されているポート上で、Web ベース プロキシ認証をイネーブルにした場合、すべての IP アドレスに対して Web ベース プロキシ認証が初期化されます。

ハイ アベイラビリティ

Web ベース プロキシ認証はハイ アベイラビリティをサポートします。認証済みホストからの情報だけが、スタンバイ スーパバイザ エンジンに同期化されます。スイッチオーバー時は、すべての認証済みホストは認証されたままです。認証されないホストまたは認証実行中のホストからの通知は、同期化されません。Web ベース プロキシ認証では、スイッチオーバー時にこれらのホストを初期化するため、認証が再起動します。

たとえば、証明書を入力し、ログイン ページを提出し、スイッチが RADIUS に 証明書を送信して応答を待機している場合に、スイッチオーバーが発生すると、入力した証明書は失われ、任意の URL にアクセスを試みた際にログイン ページがホストに再送されます。証明書を再入力する必要があります。

ホスト ステート

ホストのステートによって、ホストがネットワーク アクセスを許可されているかどうかがわかります。ホスト ステートは、次のとおりです。

- 初期化 — このホストの IP アドレスが、ホストからスーパバイザ エンジンへ任意の HTTP パケットをリダイレクトする URL リダイレクションに登録されている場合に発生します。最初の HTTP パケットを代行受信すると、ホスト ステートは接続ステートに変更されます。

- 接続 ― ログイン ページがクライアントに表示され、クライアントからの応答を待機する際に発生します。ホストが HTTP POST 応答を受信すると、ホスト ステートは認証ステートに変更されます。
- 認証 ― ホストの応答（HTTP POST メッセージ）が処理され、証明書を抽出できる場合に発生します。証明書は外部 RADIUS サーバにより、次のように認証されます。
  - HTTP 応答が失敗した場合、ステートは解析エラー ステートに変更されます。たとえば、指定の外部ログイン ページが、スイッチが処理するようプログラミングされている変数 / フィールド名に適合しなければ、このステートは発生します。
  - 認証が成功した場合、ステートは認証済みステートに変更されます。認証が失敗して、再試行カウントが最大設定値より少ない場合、ステートは認証失敗ステートまたは保留ステートに変更されます。
  - 認証済み ― 認証成功時に発生します。認証済みステートでは、RADIUS 属性が処理され、ポリシーはホストに適用され、戻されます。HTTP パケットは代行受信されず、スーパバイザ エンジンにリダイレクトされません。セッション タイマーが満了すると、ステートはセッションタイムアウト ステートに変更されます。
  - 認証失敗 ― RADIUS が許可 / 拒否ページまたはログイン失敗ページに認証失敗情報を組み込んで送信すると、発生します。
  - 解析エラー ― HTTP POST メッセージからユーザ証明書を抽出できない場合に発生します。NAD 内部に保存されている標準のログイン ページが、クライアントに送信されます。ホストが HTTP POST 応答を受信すると、ステートは認証ステートに変更されます。
  - セッションタイムアウト ― セッション タイマーの満了時に発生します。ユーザ ポリシーは削除され、ステートは初期化ステートに変更されます。
  - 保留 ― 認証再試行カウントが、設定された最大再試行数を超過した場合に発生します。HTTP パケットは、代行受信されません。ポートの初期化および DHCP バインディングの取り消しにより、保留ステートの指示は解除されます。

他の機能との相互作用

Web ベース プロキシ認証は、次の機能と相互作用します。

- DHCP スヌーピング ― 同じポート /VLAN 上で、Web ベース プロキシ認証と DHCP スヌーピングをイネーブルにできます。Web ベース プロキシ認証用のデフォルト ACL には、DHCP スヌーピングを許可する ACE が含まれます。DHCP スヌーピング バインディングを作成すると、Web ベース プロキシ認証がトリガーされます。
- Dynamic ARP Inspection（DAI）― 同じポート /VLAN 上で、Web ベース プロキシ認証と DAI をイネーブルにできます。デフォルトの ACL では、ARP 検査を許可する ACE が必要です。ホストには、スタティックな IP アドレスが設定されています。ARP 検査により、Web ベース プロキシ認証がトリガーされます。
- IP Souce Guard（IPSG）― 同じポート上で、Web ベース プロキシ認証と IPSG をイネーブルにできます。IPSG はアクセス ポリシーに PACL を使用します。一方、Web ベース プロキシ認証はアクセス ポリシーに PBACL を使用します。IPSG を Web ベース プロキシ認証と連動させるには、ポート ACL をマージ モードにする必要があります。
- 802.1X ― Web ベース プロキシ認証と 802.1X は独立した ID 認証プロトコルで、レイヤ 2 で 802.1X を、レイヤ 3 で Web ベース認証を行います。Web ベース プロキシ認証を 802.1X と同時にイネーブルにできます。ポート上に Web ベース プロキシ認証および 802.1X を設定すると、ポートは 802.1X を使用して認証しようとします。認証の成功後、RADIUS からポリシーを受け取ります。ポリシーがすべての Web（HTTP/HTTPS）トラフィックを許可する場合、Web ベース プロキシ認証は実行されません。802.1X ポリシーが Web トラフィックを許可する場合、ホストは認証されません。802.1X ポリシーが Web トラフィックを許可しない場合に、ホストがポリシーで許可されていない最初の HTTP/HTTPS パケットを送信すると、Web ベース プロキシ認証が実行されます。パケットは、URL リダイレクト ACE により代行受信されます。
- MAC 認証バイパス ― MAC 認証バイパスは、MAC アドレスを使用するレイヤ 2 認証です。MAC 認証バイパスでは、実際の認証は行われません。MAC 認証バイパスが設定されたインターフェイス上で、Web ベース プロキシ認証を設定すると、MAC 認証バイパスの完了後、Web ベース プロキシ認証が実行されます。MAC 認証バイパスは、VLAN にポートを追加し、DHCP により IP アドレスを取得します。これにより、Web ベース プロキシ認証がトリガーされます。
- ポート セキュリティ ― ポート上で、ポート セキュリティおよび Web ベース プロキシ認証をイネーブルにすると、ポート セキュリティにより保護されたホストが Web 認証されます。
- Voice VLAN ID（VVID）― Web ベース プロキシ認証および VVID のサポートは、ポート VLAN ホストに制限されます。
- ゲスト VLAN ― 802.1X 認証または MAC 認証バイパスが終了すると、ポートは 802.1X または MAC 認証バイパスの認証結果に基づいて、ゲスト VLAN に追加されます。ポートは、ゲスト VLAN 内の DHCP を使用して IP アドレスを受け取ります。IP アドレス受信後、Web ベース プロキシ認証が実行されます。
- 認証失敗 VLAN ― Web ベース プロキシ認証および認証失敗 VLAN を同じポート /VLAN 上でイネーブルにできます。
- Network Admission Control（NAC）― 同じポート /VLAN 上で、Web ベース プロキシ認証と NAC をイネーブルにできます。両方の機能をイネーブルにすると、まず Web ベース プロキシ認証が実行されてから、NAC がトリガーされます。Web ベース プロキシ認証で、認証の再開が決定されると、NAC のホスト ステートが初期化されます。

Web ベース プロキシ認証のデフォルト設定

表 41-1 に、Web ベース プロキシ認証のデフォルト設定値を示します。

表 41-1　Web ベース プロキシ認証のデフォルト設定

機能	デフォルト値
Port Access Entity（PAE）機能	認証者のみ
Web ベース プロキシ認証 — グローバル	ディセーブル
Web ベース プロキシ認証 — ポート単位	ディセーブル
グローバルなセッションタイムアウト	3600 秒
待機タイムアウト	60 秒
ログイン試行	3 回

Web ベース認証時の注意事項および制限事項

ここでは、Web ベース プロキシ認証の設定時の注意事項および制限事項について説明します。

- Web ベース認証は、トランク インターフェイスまたはポートチャネル インターフェイス上でサポートされません。
- PBACL は VLAN にマッピングされるため、VLAN 内のすべてのポートは、PBACL デフォルト ポリシーによりデフォルト アクセスが指定されています。VLAN 内のすべてのポート上で、Web ベース認証をイネーブルにすることを推奨します。
- ポート上で Web ベース プロキシ認証をイネーブルにする前に、次の ACE を使用して VLAN に PBACL をマッピングする必要があります。
  - DHCP snooping
  - ARP inspection
  - Allow DNS
  - Policy config
  - URL Redirect
  - Default policy
- ポート上で Web ベース プロキシ認証をイネーブルにする前に、スタティック IP ホストの ARP 検査をイネーブルにして、スタティック ARP 検査のルールを設定する必要があります。

次に、これらの ACE を使用して一般的な ACL を設定する例を示します。

```
permit dhcp-snooping
permit arp-inspection <ip_addr> <hwaddr>
permit udp any eq dns any                    [permit DNS]
permit tcp any eq domain any                 [permit DNS w/TCP]
<Policy configuration>
permit ip group Exception ExpServers
permit ip group Engineer EngServers
permit ip group Manager MgrServers
permit ip group Admin any
permit url-redirect                          [permit URL redirection]
deny ip any any                              [Default policy]
```

最初にホストがアップされた際、ホスト IP およびすべてのホスト トラフィックにはポリシーが設定されていません。ただし、デフォルト ポリシーによって制御され、PBACL で設定される HTTP トラフィックは除きます。HTTP トラフィックは、スーパバイザ エンジンにリダイレクトされます。Web ベース プロキシ認証では、DHCP または ARP からのトリガーを受信すると、URL リダイレクションにこの IP を登録します。スーパバイザ エンジン上の URL リダイレクション モジュールはパケットを受信し、これを Web ベース プロキシ認証に伝送します。

認証の成功後、Web ベース プロキシ認証は RADIUS から受信したグループにホスト IP を追加し、PBACL を拡張して、Ternary CAM（TCAM）を更新します。ホスト トラフィックは、ポリシー設定により制御されます。HTTP リダイレクションの ACE は最後なので、ホスト ポリシーがある場合でも、影響されません。ホスト ポリシーが削除されると（セッション タイムアウトを超過したあと）、ホスト トラフィックは再度デフォルト ポリシーにより処理され、HTTP トラフィックはスーパバイザ エンジンにリダイレクトされます。

Web ベース プロキシ認証の設定

ここでは、Web ベース プロキシ認証を設定する手順について説明します。

Web ベース プロキシ認証のグローバルなイネーブル化またはディセーブル化

Web ベース プロキシ認証を各ポートで設定する前に、システム全体でイネーブルにする必要があります。Web ベース プロキシ認証をグローバルにイネーブルにしたあとで、各ポートに Web ベース プロキシ認証を設定できます。各ポートで Web ベース プロキシ認証をイネーブルにするには、「ポート上での Web ベース プロキシ認証のイネーブル化またはディセーブル化」（p.41-12）を参照してください。

Web ベース プロキシ認証をグローバルにイネーブルまたはディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
Web ベース プロキシ認証をグローバルにイネーブルにします。	**set web-auth enable**
Web ベース プロキシ認証をグローバルにディセーブルにします。	**set web-auth disable**

次に、Web ベース プロキシ認証をグローバルにイネーブルにする例を示します。

```
Console> (enable) set web-auth enable
web-authentication successfully enabled on globally.
Console> (enable)
```

次に、Web ベース プロキシ認証をグローバルにディセーブルにする例を示します。

```
Console> (enable) set web-auth disable
web-authentication successfully disabled on globally.
Console> (enable)
```

ポート上での Web ベース プロキシ認証のイネーブル化またはディセーブル化

Web ベース プロキシ認証をグローバルにイネーブルにしたあと、各ポートで Web ベース プロキシ認証をイネーブルにできます。Web ベース プロキシ認証をグローバルにイネーブルにするには、「Web ベース プロキシ認証のグローバルなイネーブル化またはディセーブル化」（p.41-11）を参照してください。

（注） Web ベース プロキシ認証をグローバルにディセーブルにした場合、ポート上で Web ベース プロキシ認証は開始されませんが、設定には保存されます。

ポート上で Web ベース プロキシ認証をイネーブルまたはディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
ポート上で Web ベース プロキシ認証をイネーブルにします。	**set port web-auth** *mod/port* **enable**
ポート上で Web ベース プロキシ認証をディセーブルにします。	**set port web-auth** *mod/port* **disable**

次に、ポート上で Web ベース プロキシ認証をイネーブルにする例を示します。

```
Console> (enable) set port web-auth 1/1 enable
web-authentication successfully enabled on Interface 1/1.
Console> (enable)
```

次に、ポート上で Web ベース プロキシ認証をディセーブルにする例を示します。

```
Console> (enable) set port web-auth 1/1 disable
web-authentication successfully disabled on Interface 1/1.
Console> (enable)
```

ポート上での Web ベース プロキシ認証の初期化

set port web-auth initialize コマンドを使用して、ポートを初期化すると、ポートは最初のステートに戻ります。このステートでは、ホストの IP アドレスが、ホストからスーパバイザ エンジンへ任意の HTTP パケットをリダイレクトする URL リダイレクションに登録されます。

ip_addr 引数を指定する場合、Web ベース プロキシ認証はこのホストに対してのみ初期化されます。*ip_addr* 引数を指定しない場合、Web ベース プロキシ認証はすべてのホストに対して初期化されます。

認証用の Web ベース プロキシ認証ポートを再度初期化する前に、Web ベース プロキシ認証をグローバルおよび各ポートでイネーブルにする必要があります。

認証用の Web ベース プロキシ認証ポートを再度初期化するには、イネーブル モードで次の作業を実行します。

作業	コマンド
認証用の Web ベース プロキシ認証ポートを再度初期化します。	**set port web-auth** *mod/port* **initialize** [*ip_addr*]

次に、ポート上のすべてのホストで Web ベース プロキシ認証を再度初期化する例を示します。

```
Console> (enable) set port web-auth 2/1 initialize
Initialized web-authentication for all hosts on port 2/1.
Console> (enable)
```

次に、特定ホストで Web ベース プロキシ認証を再度初期化する例を示します。

```
Console> (enable) set port web-auth 2/1 initialize 10.1.1.1
Initialized web-authentication for host 10.1.1.1 on port 2/1.
Console> (enable)
```

ログイン ページ URL の設定

URL を入力する場合、url = **http://***string* を使用します。

ログイン ページに URL を設定するには、イネーブル モードで次の作業を実行します。

作業	コマンド
ログイン ページに URL を設定します。	**set web-auth login-page url** *url*

次に、ログイン ページの URL を設定する例を示します。

```
Console> (enable) set web-auth login-page url http://proxyauth.cisco.com/login.html
web-auth login-page configured.
Console> (enable)
```

ログイン失敗ページ URL の設定

URL を入力する場合、フォーマット、url = **http://***string* を使用します。

ログイン失敗ページに URL を設定するには、イネーブル モードで次の作業を実行します。

作業	コマンド
ログイン失敗ページに URL を設定します。	**set web-auth login-fail-page url** *url*

次に、ログイン失敗ページの URL を設定する例を示します。

```
Console> (enable) set web-auth login-fail-page url
http://proxyauth.cisco.com/login.html
web-auth login fail page configured.
Console> (enable)
```

セッション タイムアウト時間の指定

このセッションが有効である時間（長さ）を指定できます。この時間を超過すると、Web 認証されたセッションは終了します。RADIUS が提供するセッション タイムアウトは、ローカルに設定された値よりも優先されます。

グローバルな Web ベース プロキシ認証セッションのタイムアウト時間を指定するには、イネーブル モードで次の作業を実行します。

作業	コマンド
グローバルな Web ベース プロキシ認証セッションのタイムアウト時間を指定します。	**set web-auth session-timeout** *seconds*

次に、グローバルな Web ベース プロキシ認証セッションのタイムアウト時間を指定する例を示します。

```
Console> (enable) set web-auth session-timeout 20
web-authentication session-timeout set to 20 seconds.
Console> (enable)
```

待機時間の指定

認証者がホストを認証できないときは、一定時間のアイドル状態を経て再試行します。アイドル時間は、quiet-period の値によって決まります。デフォルトは 60 秒です。設定できる *seconds* 値は、0 ～ 65535 秒です。

待機時間の長さを指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
待機時間を指定します。	**set web-auth quiet-timeout** *seconds*

次に、待機時間を指定する例を示します。

```
Console> (enable) set web-auth quiet-timeout 20
web-authentication quiet-timeout set to 20 seconds.
Console> (enable)
```

ログインの最大試行回数の指定

ユーザがブロックされるまでの、失敗ログインの最大試行回数を指定できます。

ログインの最大試行回数を指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
ログインの最大試行回数を指定します。	**set web-auth login-attempts** *count*

次に、ログインの最大試行回数を指定する例を示します。

```
Console> (enable) set web-auth login-attempts
web-authentication max retry count set to <count>
Console> (enable)
```

Web ベース プロキシ認証情報の表示

ここでは、次の Web ベース プロキシ認証情報を表示する手順について説明します。

- セッション情報の要約の表示（p.41-14）
- ポート単位の情報の表示（p.41-16）

セッション情報の要約の表示

vlan *vlan_id* キーワードおよび引数を指定すると、指定 VLAN の情報の要約が表示されます。

コマンド出力では、以下が適用されます。

- * は、RADIUS が割り当てた値を示します。
- State フィールドには、所定のホストの現在の Web 認証ステートが表示されます。

Web ベース プロキシ認証セッションの情報の要約を表示するには、ユーザ モードで次の作業を実行します。

作業	コマンド
Web ベース プロキシ認証セッションの情報の要約を表示します。	**show web-auth summary** [**vlan** *vlan_id*]

次に、Web ベース プロキシ認証セッションの情報の要約を表示する例を示します。

```
Console> (enable) show web-auth summary
Web-authentication enabled globally
Login-page location url http://proxyauth.cisco.com/login.html
Login-fail-page location url http://proxyauth.cisco.com/loginfail.html
session-timeout : 3600 secs
quiet timeout : 60 secs
Max Login attempt count: 3
-------------------------------------------------------------------------------------------
-----------------------------------
IP Address                  Interface       Web Auth State
     Session-Timeout   Leftover-Session-Time       VLAN
-------------------------------------------------------------------------------------------
-------------------------------------------------
9.9.150. 1                      1/1             Authenticated
              * 7200                          200                               100
9.9.150.2                  1/2           Authenticating            3600                      -
                               100
9.9.150.3                       1/3             Authentication-fai
         3600                             -                                 100
9.9.160.10                     1/4             Held
               3600                             -                                  200
9.9.170.15                     1/5
            Connecting                      3600                              -
                   300
Console> (enable)
```

次に、特定 VLAN の Web ベース プロキシ認証セッションの情報の要約を表示する例を示します。

```
Console> (enable) show web-auth summary vlan 100
-------------------------------------------------------------------------------------------
-----------------------------------
IP Address                  Interface       Web Auth State
     Session-Timeout   Leftover-Session-Time
-------------------------------------------------------------------------------------------
-----------------------------------
9.9.150. 1                      1/1             Authenticated
             * 7200                          200
9.9.150.2                  1/2           Authenticating            3600                      -

9.9.150.3                       1/3             Held
                               3600                             -
Console> (enable)
```

ポート単位の情報の表示

show port web-auth コマンドを使用すると、次の情報が表示されます。

- ホストの IP アドレス
- 現在のステート
- セッションタイムアウト。表示される時間は、RADIUS から提供されない場合に設定されたタイムアウトです。
- 残りのセッション タイムアウト値

Web ベース プロキシ認証ポートの情報を表示するには、ユーザ モードで次の作業を実行します。

作業	コマンド
Web ベース プロキシ認証ポートの情報を表示します。	**show port web-auth** *mod/port*

次に、Web ベース プロキシ認証ポートを表示する例を示します。

```
Console> (enable) show port web-auth 2/1
Web Authentication Information for port 2/1
-------------------------------------------------------------------------------------------
---------
IP Address    Web Auth State      Session-Timeout   Leftover-Session-Time
-------------------------------------------------------------------------------------------
---------
9.9.150. 1        Authenticated               7200                       200
9.9.150.4         URL-Redirected            3600                        -
9.9.150.10       Connecting                  3600                          -
Console> (enable)
```

CHAPTER 42

NAC の設定

この章では、Catalyst 6500 シリーズ スイッチ上で Network Admission Control（NAC）を設定する手順について説明します。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

(注) IEEE 802.1X 認証の設定については、第 39 章「802.1X 認証の設定」を参照してください。

(注) MAC（メディア アクセス制御）認証バイパスの設定については、第 40 章「MAC 認証バイパスの設定」を参照してください。

(注) イーサネット、ファスト イーサネット、またはギガビット イーサネット ポートへのアクセスを試みたステーションの MAC アドレスが、そのポートに指定されている MAC アドレスと異なる場合、ポート セキュリティ機能を使用してポートへのアクセスをブロックする手順については、第 37 章「ポート セキュリティの設定」を参照してください。また、ホスト MAC アドレスに基づく指定ホストに送信、または指定ホストから受信したトラフィックをフィルタリングする場合に、ポート セキュリティを使用する場合に、ポート セキュリティを使用する手順についても説明します。

(注) Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）を設定して、Catalyst 6500 シリーズ スイッチの CLI（コマンドライン インターフェイス）へのアクセスをモニタおよび制御する方法については、第 38 章「AAA によるスイッチ アクセスの設定」を参照してください。

この章で説明する内容は、次のとおりです。

LAN ポート IP による NAC の設定

ここでは、LAN ポート IP による NAC の設定手順について説明します。

LAN ポート IP による NAC の機能概要

ここでは、LAN ポート IP の概要について説明します。

概要

NAC 機能は、ネットワーク化された企業に対して増加するワームおよびウイルスの脅威および影響に対処します。この機能は、ユーザがセキュリティの脅威を識別、防御、および適合するのに役立つ Cisco Self-Defending Network Initiative の一部です。

NAC はその初期段階で、スイッチおよびルータがネットワークに接続しようとしているエンドポイントのアクセス権を制限できるようにします。アクセスは、現在のアンチウイルス ステート（アンチウイルス ソフトウェアのバージョン、ウイルス定義、およびスキャン エンジンのバージョン）などのエンドポイント デバイスの情報に基づいて行われます。

NAC システムにより、非準拠のデバイスに対するアクセスの拒否、検疫エリアへの配置、またはコンピューティング リソースへの制限付きアクセスの許可が可能になり、非セキュアなノードがネットワークに悪影響を及ぼさないようにします。

シスコの NAC プログラムの主要コンポーネントは Cisco Trust Agent で、エンドポイント システムに常駐して、ネットワーク上のシスコ製スイッチおよびルータと通信します。Cisco Trust Agent は、使用されているアンチウイルス ソフトウェアが何であるかなどのセキュリティ ステートの情報を収集して、シスコ製スイッチおよびルータにこの情報を送信します。次に、この情報は Cisco Secure Access Control Server（ACS）にリレーされて、アクセス制御が決定されます。ACS は、シスコ製スイッチまたはルータにエンドポイントに対する処理の実行を指示します。

ウイルス感染およびネットワークへの影響

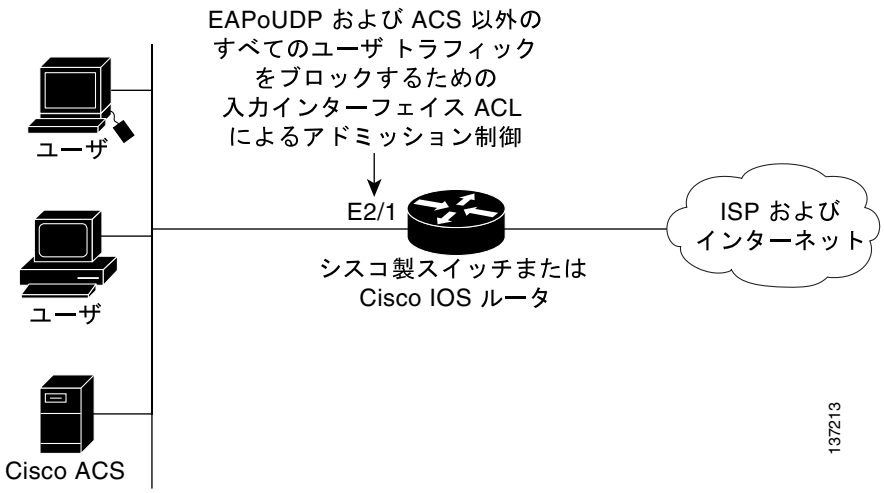
ウイルス感染は、ネットワークに対する重大なセキュリティ違反において単独では最大の原因で、多大な経済的損失をもたらすことが少なくありません。ウイルス感染の原因は、非セキュアなエンドポイント（PC、ラップトップ、およびサーバなど）にあります。エンドポイントにアンチウイルス ソフトウェアがインストールされている場合でも、このソフトウェアがディセーブルである場合がよくあります。ソフトウェアがイネーブルであっても、エンドポイントに最新のウイルス定義およびスキャン エンジンがない場合もあります。また、アンチウイルス ソフトウェアがインストールされていない機器によって、より一層のセキュリティ上のリスクが発生します。現在のアンチウイルス ベンダーはアンチウイルス ソフトウェアのディセーブル化をより困難にしていますが、最新ではないウイルス定義およびスキャン エンジンのリスクには対処していません。

NAC の機能概要

エンドポイント システムまたはクライアントは、通常 PC、ラップトップ、ワークステーション、およびサーバなどネットワーク上のホストとなっています。エンドポイント システムは潜在的なウイルス感染源であるため、これらのアンチウイルス ステートはネットワーク アクセスが許可される前に検証される必要があります。エンドポイントが、アップストリームのシスコ製ネットワーク アクセス デバイス（シスコ製スイッチまたはルータ）を介してネットワークに IP 接続しようとすると、ネットワーク アクセス デバイスはエンドポイントにアンチウイルス ステートを要求します。エンドポイント システムは、Cisco Trust Agent というクライアントを実行して、エンド デバイスから収集したアンチウイルス ステート情報をネットワーク アクセス デバイスに転送します。次に、この情報は Cisco Secure ACS に送信されます。ACS では、エンドポイントのアンチウイルス ステートを検証し、アクセス制御を決定して、ネットワーク アクセス デバイスに戻します。ネットワーク デバイスでは、エンド デバイスの許可、拒否、または検疫が行われます。Cisco Secure ACS は、バックエンドのアンチウイルス ベンダー固有のサーバを順々に使用して、エンドポイントのアンチウイルス ステートを評価する場合もあります。

図 42-1 に、Cisco NAC の機能を示します。

図 42-1　Cisco IOS NAC システム



NAD

通常、Network Access Device（NAD）はシスコ製スイッチまたはルータ（レイヤ 3 Extensible Authentication Protocol over UDP [EAPoUDP] アクセス ポイント）で、インターネットまたはリモートの企業ネットワークなどの外部ネットワークと接続しています。

Cisco Trust Agent

Cisco Trust Agent は、エンドポイント システムで稼働する専門ソフトウェアです。Cisco Trust Agent は、スイッチまたはルータからのエンドポイント システムのアンチウイルス ステートに関する要求に応答します。NAD（スイッチまたはルータ）は、Cisco Trust Agent が稼働していないエンドポイント システムを「クライアントレス」として分類します。

Cisco Secure ACS

Cisco Secre ACS は、業界標準の RADIUS 認証プロトコルを使用して NAC に AAA サービスを提供します。Cisco Secre ACS は、エンドポイント システムのアンチウイルス証明に基づいて、NAD にアクセス制御の決定を戻します。

Cisco Secre ACS 上で次のアトリビュート / 値ペア（AV ペア）を設定するには、RADIUS cisco_av_pair Vendor-Specific Attiribute（VSA）を使用します。これらの AV ペアは、NAD に他のアクセス制御アトリビュートと同時に送信されます。

- url-redirect ― AAA クライアントが HTTP 要求を代行受信し、新しい URL にリダイレクトできるようにします。このリダイレクションは、ポスチャ確認の結果、修復 Web サーバ上で利用可能な更新またはパッチがネットワーク アクセス制御エンドポイントで必要となる場合に特に役立ちます。たとえば、新しいウイルスの Directory Administration Tool（DAT）ファイルまたはオペレーティング システムのパッチをダウンロードして適用するのに、修復 Web サーバにユーザをリダイレクトできます。次の例を参照してください。

  ```
  url-redirect=http://10.1.1.1
  ```

  （注） **監査サポートへの URL リダイレクト：**監査機能は、Cisco Trust Agent（CTA）がイネーブルでないホスト用です。監査機能は、NAD がクライアントレス認証を実行する際に監査で必要なポリシーを送信するすると、ACS によりトリガーされます。監査機能は、監査サーバの URL を ホストの URL リダイレクト ポリシーとして送信することで達成されます。ホストからの HTTP トラフィックが確認されると、監査サーバの URL が提供されます。Policy-Based ACL（PBACL）により設定されたポリシーは、監査サーバとホスト間の通信を許可します。通常、セッション タイムアウトは監査が完了するには短く、このタイムアウトが満了すると、再確認が実行されます。NAD は ACS に事前に受信したステート アトリビュートを送信して、新しいポリシーを伝達します。このセッション タイムアウト間に監査が終了しない場合、ACS は別の短いセッション タイムアウトを送信し、監査のポスチャ トークンが受信されるまでこのプロセスを継続します。このプロセスが完了しないか、または時間がかかる場合、監査サーバは ACS に「エラー」のポスチャ トークンを戻します。

- posture-token ― Cisco Secure ACS が、ポスチャ確認で取得した System Posture Token（SPT）のテキスト バージョンを送信できるようにします。SPT は常に数値形式で送信されます。posture-token AV ペアを使用することにより、ポスチャ確認要求の結果が AAA クライアント上で読み取りやすくなります。次の例を参照してください。

  ```
  posture-token=Healthy
  ```

有効な SPT は、最良のものから順に次のとおりです。

- Healthy
- Checkup
- Quarantine
- Infected
- Unknown

- status-query-timeout　—　AAA　クライアントのステータスクエリのデフォルト値を指定した値（秒）で上書きします。次の例を参照してください。

```
status-query-timeout=150
```

シスコのソフトウェアでサポートされる AV ペアの詳細については、ご使用の AAA クライアントに実装されているソフトウェア リリースのマニュアルを参照してください。

修復

NAC は、エンドポイント デバイスからの任意の HTTP 要求を指定のリダイレクト アドレスへリダイレクトする HTTP リダイレクションをサポートします。このサポート メカニズムにより、送信元からのすべての HTTP 要求が指定の Web ページ（URL）にリダイレクトされ、そこで最新のアンチウイルス ファイルがダウンロードされます。HTTP リダイレクションが機能するには、ACS 上で [url-redirect] VSA の値を設定し、それに相応してエンドポイント システムのアクセスを許可するダウンロード可能な Access Control List（ACL; アクセス制御リスト）内の Access Control Entry（ACE; アクセス制御エントリ）をリダイレクト URL アドレスに関連付ける必要があります。

LAN ポート IP ポスチャ確認の要約

LAN ポート IP は、エンドユーザ デバイスのポスチャを確認し、そのポスチャに基づいてネットワークのアクセス権を与えるメカニズムです。ポスチャ確認後、エンドユーザ デバイスは 5 つのステート（healthy、checkup、quarantine、infected、または unknown）のいずれかに分類されます。デバイスのポスチャ ステートにより、ネットワークのアクセス権が与えられます。

LAN ポート IP の実行メカニズムには、URL リダイレクションおよび監査が含まれます。ネットワーク アクセスの実行には、PBACL が使用されます。

ポスチャ確認の基本的手順は、次のとおりです。

1. NAD は、Address Resolution Protocol（ARP; アドレス解決プロトコル）検査および（または）Dynamic Host Configuration Protocol（DHCP）スヌーピングを使用して、MAC および IP アドレス バインディングを学習します。
2. NAD は、ホストに EOU hello 要求を送信します。
3. CTA が稼働しているホストは、hello 応答により返答します。
4. NAD は、EOU 確認アイデンティティ要求を送信します。
5. CTA は、EOU 確認応答により返答します。
6. NAD は、EOU から抽出した EAP パケットを RADIUS アクセス要求に組み込んで、認証サーバ（ACS など）に送信します。
7. ACS はアクセス確認を返し、CTA には EOU 確認パケットの形式で転送されます。
8. ACS がポスチャ確認セッションに対して成功または失敗応答を送信するまで、手順 6 および手順 7 は継続されます。
9. 成功した場合、ACS は PBACL グループ、セッション タイムアウト、ステータス クエリ タイムアウト、認証済みユーザ名などが含まれるポスチャに関連付けられたポリシー、およびポスチャ トークン VSA を送信します。

ホストが NAD から送信された EOU hello 要求に応答しない場合、NAD（事前に設定された試行回数のあと）はホストにクライアントレス（CTA なし）を宣告します。NAD はホストの代わりに擬似認証を実行して、ポリシーを伝達します。監査などほかのポスチャ確認メカニズムがトリガーされます。

クライアントレス モードでは、NAD は 3 つの EOU hello メッセージ（デフォルト）を送信してから、ホストに CTA がないことを宣告します。クライアントレス認証の実行およびそのポリシーのインストールを行うこのプロセスでは、約 90 秒（30 秒が 3 回）かかります。CTA を持たないことが明らかなポート上でのこの遅延を避けるには、ポート単位の CLI を使用してポート モードをバイパスに設定します（**set port eou** *mod*/*port* **bypass**）。これを実行すると、ポートは新しい IP アドレスを学習した場合、直ちにクライアントレス認証を行います。

ポスチャ確認非対応のためポスチャ確認を試行しないホストは例外です。例外と指定されたホストが検出された場合、事前設定済みのポリシーがインストールされます。

LAN ポート IP のハードウェアおよびソフトウェア要件

LAN ポート IP を設定する場合は、次のハードウェアおよびソフトウェア要件に従ってください。

- Catalyst 6500 シリーズ スイッチ上では、Release 8.5(1) 以降のソフトウェア リリースが稼働している必要があります。
- エンドポイント デバイス（PC、およびラップトップなど）上に CTA がインストールされている必要があります。
- AAA 用の Cisco Secure ACS が必要です。

LAN ポート IP 設定時の注意事項および制限事項

LAN ポート IP を設定する場合、次の設定時の注意事項および制限事項に従ってください。

- ACL および PBACL の設定に精通している必要があります。
- AAA の設定に精通している必要があります。
- LAN ポート IP は、802.1X、MAC 認証バイパス、および Web ベース プロキシ認証など他のセキュリティ機能と連動します。次のように、802.1X ポートに適用される制限事項は LAN ポート IP にも適用されます。
  - LAN ポート IP は、アクセス ポート上でのみ設定可能です。トランク ポート上では、設定できません。
  - LAN ポート IP ポートを、EtherChannel の一部にすることはできません。
  - ダイナミック ポートでは、LAN ポート IP をイネーブルにできません。
  - LAN ポート IP は、イーサネット ポート上でのみイネーブルにできます。
  - LAN ポート IP ポートは、SPAN 宛先ポートにできません。
  - LAN ポート IP ポートを、プライベート VLAN の一部にすることはできません。
- LAN ポート IP は、802.1X または MAC 認証バイパスなどの認証機能がイネーブルの場合、認証の終了後にのみ初期化されます。
- 802.1X ― 802.1X 認証では、VLAN 割り当てなどのレイヤ 2 ポリシーを適用し、ポートに PBACL などのレイヤ 3 ポリシー アトリビュートも適用できます。LAN ポート IP ポリシーは、RADIUS サーバからダウンロードされたポリシーグループのメンバーシップでのみ構成されます。802.1X のディセーブルおよびイネーブルは、LAN ポート IP に影響しません。
- マルチホストおよびマルチ認証モードは、サポートされません ― LAN ポート IP での 802.1X は、単一ホスト モードでのみサポートされます。
- 補助 VLAN ― LAN ポート IP は、マルチ VLAN アクセス ポート上でのみサポートされます。

- ゲスト VLAN および認証失敗 VLAN ― LAN ポート IP でこれら 2 つの機能が設定されている場合、LAN ポート IP の動作は、ポスチャ確認のためにゲスト VLAN または認証失敗 VLAN から IP アドレスを取得するという点のみが異なります。
- DHCP スヌーピングおよび（または）ARP 検査 ― IP ラーニングは、ARP 検査または DHCP スヌーピングにより行われます。LAN ポート IP を機能させるには、少なくともいずれかの機能がイネーブルである必要があります。これらの機能は、LAN ポート IP をトリガーするのに必要です（これらの機能の ACE を含む PBACL を LAN ポート IP が格納された VLAN にマッピングする必要があります）。これらの機能がいずれもイネーブルでない場合、レイヤ 2 スイッチはポート上に表示される新しい IP アドレスを学習できません。

（注）　Supervisor Engine 1 は、ARP 検査をサポートしません。Supervisor Engine 1 を搭載している場合は、DHCP スヌーピングをイネーブルにする必要があります。

- ポート セキュリティ ― LAN ポート IP は、ポート セキュリティと組み合わさって機能します。ポート セキュリティで確認された MAC アドレスのみが、ポスチャ確認を通過できます。ポート セキュリティ違反が発生し、ポートがシャットダウンした場合、ポートの LAN ポート IP ステートも消去されます。認証機能を設定すると、認証機能が MAC アドレスをポート セキュリティに提供し、MAC アドレスが認証に成功したことが保証され、LAN ポート IP が初期化されます。
- セキュリティ ACL（VACL）― セキュリティ ACL は PBACL として使用され、PBACL は VACL モードで LAN ポート IP でのみサポートされます。
- MAC 認証バイパス ― LAN ポート IP は、MAC 認証バイパス、802.1X、または Web ベース プロキシ認証を使用した認証に成功した場合にのみ初期化されます。これらの認証機能のイネーブル化またはディセーブル化は、LAN ポート IP に影響しません。
- Web ベース プロキシ認証 ― LAN ポート IP は、Web ベース プロキシ認証でアイデンティティ証明書の確認が完了した場合にのみ初期化されます。Web ベース プロキシ認証ステートでは、ポートは認証の完了を無期限に待機し、この段階で通過を許可されるのは、DHCP または Domain Name System（DNS; ドメイン ネーム システム）のみです。インターフェイス上で設定された ACL は、HTTP トラフィックのリダイレクションを処理します。インターフェイス上で設定された PBACL は、その他のトラフィックが許可されていないことを保証します。

LAN ポート IP の設定

ここでは、LAN ポート IP を設定する手順について説明します。

（注）　LAN ポート IP の設定情報を表示して、LAN ポート IP の設定要素を消去するには、「LAN ポート IP の CLI コマンド例」（p.42-10）を参照してください。PBACL を設定するには、「PBACL の設定」（p.42-21）を参照してください。

（注）　次の設定手順の詳細については、「LAN ポート IP の設定例」（p.42-23）を参照してください。

LAN ポート IP を設定するには、次の手順を実行します。

ステップ 1　次のように、**set eou** {**enable | disable**} コマンドを使用して、スイッチ上で LAN ポート IP をグローバルにイネーブルにします（デフォルトはディセーブル）。

```
Console> (enable) set eou enable
EoU globally enabled.
Console> (enable)
```

ステップ 2　次のように、**set port eou** *mod/port* {**bypass | auto | disable | initialize | revalidate**} コマンドを使用して、ポート単位で LAN ポート IP をイネーブルにします。

```
Console> (enable) set port eou 7/1 auto
EoU enabled on 7/1
Console> (enable)
```

ステップ 3　次のコマンドを使用して、RADIUS サーバおよび RADIUS 鍵を定義します。

set radius server *ip_addr* [**auth-port** *port*] [**acct-port** *port*] [**primary**]

set radius key *key*

次に、RADIUS サーバを定義する例を示します。

```
Console> (enable) set radius server 10.76.39.93 auth-port 1812 primary
10.76.39.93 with auth-port 1812 acct-port 1813 added to radius server table as primary
server.
Console> (enable)
```

次に、RADIUS 鍵を定義する例を示します。

```
Console> (enable) set radius key cisco
Radius key set to cisco
Console> (enable)
```

ステップ 4　次のように、PBACL を定義して VLAN にマッピングします。

a. DHCP スヌーピングおよび（または）ARP 検査をイネーブルにします。

set security acl ip *acl-name* **permit dhcp-snooping**

set security acl ip *acl-name* **permit arp-inspection**

b. EAPoUDP リダイレクションをイネーブルにします。

set security acl ip *acl-name* **permit eapoudp**

c. 各種 LAN ポート IP ステートに対応するポリシー グループを使用して、他のポリシー ステートメントを定義します。例：

set security acl ip NACACL permit ip group healthy_hosts any

set security acl ip NACACL deny ip group infected_hosts any

set security acl ip NACACL permit ip group exception_hosts any

set security acl ip NACACL permit ip group clientless_hosts host 10.76.39.100

d. URL リダイレクションでは、次の ACE を適所で適用します。

set security acl ip NACACL permit url-redirect

ステップ 5　次のように、クライアントレス Non-Responsive Host（NRH ホスト）では、クライアントレス機能をイネーブルにします。

set eou allow clientless enable

ステップ 6　また、NRH ホストのポリシーを定義することもできます。上記の手順で定義された ACL には、指定されたグループが存在する必要があります。

set policy name *exception_policy* **group** *exception_hosts*

ステップ 7　次のように、例外ホストを指定して、ポリシーを割り当てます。

set eou authorize ip 77.0.0.90 policy exception_policy

ステップ 8　RADIUS サーバを設定します。RADIUS サーバ設定の詳細については、次の URL で『*Implementing Network Admission Control Phase One Configuration and Deployment*』を参照してください。

http://www.cisco.com/application/pdf/en/us/guest/netsol/ns466/c654/cdccont_0900aecd80217e26.pdf

ACL で使用されるポリシー グループが、ポスチャトークン VSA（26/9/1 sec:pg=healthy_hosts など）により設定されていることを確認します。

ACS のポリシー グループは定義されているが、VLAN にマッピングされた VACL がそのグループを参照しない場合、ポリシーのインストールが失敗するためポスチャ確認は失敗します。

ステップ 9　次のように、sc0 インターフェイスで適切な IP アドレスが設定されていることを確認します。

set interface {**sc0** | **sl0** | **sc1**} {**up** | **down**}

set interface sc0 [**vlan**] [*ip_addr*/*netmask* [*broadcast*]]

ステップ 10　ホストが接続されている VLAN にデフォルト ルータが存在することを確認します。デフォルト ルータがない場合は、sc0 の IP アドレス用にホスト上のスタティックな ARP が必要です。

ステップ 11　ホストおよび管理インターフェイス（sc0）が同じ VLAN にあり、この VLAN に VACL が設定されている場合、スイッチの IP アドレスから RADIUS サーバへのトラフィックを許可する ACE を設定する必要があります。

LAN ポート IP の CLI コマンド例

ここでは、次の LAN ポート IP の CLI コマンド例を紹介します。

LAN ポート IP のグローバルなイネーブル化またはディセーブル化

スイッチ上で LAN ポート IP をイネーブルまたはディセーブルにするには、イネーブル モードで次の作業を行います（デフォルトはディセーブルです）。

作業	コマンド
スイッチ上で LAN ポート IP をグローバルにイネーブルまたはディセーブルにします。	**set eou** {**enable** | **disable**}

次に、スイッチ上で LAN ポート IP をグローバルにイネーブルにする例を示します。

```
Console> (enable) set eou enable
EoU globally enabled.
Console> (enable)
```

クライアントレス ホストおよび例外ホストに対する LAN ポート IP ポスチャ確認のバイパスのイネーブル化またはディセーブル化

クライアントレス ホストおよび例外ホストに対する LAN ポート IP ポスチャ確認のバイパスをグローバルにイネーブルまたはディセーブルにするには、イネーブル モードで次の作業を実行します（デフォルトはディセーブル）。

作業	コマンド
クライアントレス ホストおよび例外ホストに対する LAN ポート IP ポスチャ確認のバイパスをイネーブルにします。	**set eou allow clientless** {**enable** | **disable**}

次に、クライアントレス ホストおよび例外ホストに対する LAN ポート IP ポスチャ確認のバイパスをイネーブルする例を示します。

```
Console> (enable) set eou allow clientless enable
EoU Clientless hosts will be allowed
Console> (enable)
```

例外ホスト デバイスとしての IP アドレスのスタティックな許可およびデバイスへのポリシーの適用

これにより、特定の IP アドレスが例外ホストとして処理され、このホストが検出されると、ポリシー名により指定されたポリシーがダイナミックにインストールされます。

（注） ポリシー テンプレートが存在しない場合は、次のコマンドを実行して、ポリシー テンプレートを作成します。

IP デバイスをスタティックに許可して、関連するポリシーをデバイスに適用するには、イネーブル モードで次の作業を実行します。

作業	コマンド
IP デバイスをスタティックに許可して、関連するポリシーをデバイスに適用します。	**set eou authorize ip** *ip_addr* **policy** *policy_name* **set eou authorize ip** *ip_addr ip_mask* **policy** *policy_name*

次に、IP デバイスをスタティックに許可して、関連するポリシーをデバイスに適用する例を示します。

```
Console> (enable) set eou authorize ip 172.20.52.19 255.255.255.224 policy poll
Mapped IP address 172.20.52.0 IP mask 255.255.255.224 to policy name poll
Console> (enable)
```

例外ホスト デバイスとしての MAC アドレスのスタティックな許可およびデバイスへのポリシーの適用

これにより、特定の MAC アドレスが例外ホストとして処理され、このホストが検出されると、ポリシー名により指定されたポリシーがダイナミックにインストールされます。

(注)　ポリシー テンプレートが存在しない場合は、**set eou authorize** コマンドを実行して、テンプレートを作成します。

デバイスの MAC アドレスを使用してデバイスをスタティックに許可し、関連するポリシーをデバイスに適用するには、イネーブル モードで次の作業を実行します。

作業	コマンド
デバイスの MAC アドレスを使用してデバイスをスタティックに許可し、関連するポリシーをデバイスに適用します。	**set eou authorize mac-address** *mac_address* **policy** *policy_name* **set eou authorize mac-address** *mac_address mac_mask* **policy** *policy_name*

次に、デバイスの MAC アドレスを使用してデバイスをスタティックに許可し、関連するポリシーをデバイスに適用する例を示します。

```
Console> (enable) set eou authorize mac-address 03-56-B7-45-65-56 policy poll
Mapped MAC 03-56-b7-45-65-56 to policy name poll.
Console> (enable)
```

ホストのステート マシンの再起動

ホストのステート マシンを再起動するには、イネーブル モードで次の作業を行います。

作業	コマンド
ホストのステート マシンを再起動します。	**set eou initialize all** **set eou initialize authentication** {**clientless** | **eap** | **static**} **set eou initialize ip** *ip-address* **set eou initialize mac** *mac-address* **set eou initialize posture-token** *posture-token*

次に、IP アドレスを使用してホストのステート マシンを再起動する例を示します。

```
Console> (enable) set eou initialize ip 172.20.52.19
Initializing Eou for ipAddress 172.20.52.19
Console> (enable)
```

CTA パケットの再送信回数の指定

CTA が反応なしと宣告されるまでにパケットが CTA に再送信される回数を指定するには、イネーブル モードで次の作業を実行します（デフォルトは 3 で、1 ～ 10 の範囲です）。

作業	コマンド
CTA が反応なしと宣告されるまでにパケットが CTA に再送信される回数を指定します。	**set eou max-retry** *max-retry*

次に、CTA が反応なしと宣告されるまでにパケットが CTA に再送信される回数を 6 に指定する例を示します。

```
Console> (enable) set eou max-retry 6
eou max-retry set to 6.
Console> (enable)
```

ホストの再確認

ホストを再確認するには、イネーブル モードで次の作業を行います。

作業	コマンド
ホストを再確認します。	**set eou revalidate all** **set eou revalidate authentication** {**clientless** | **eap** | **static**} **set eou revalidate ip** *ip-address* **set eou revalidate mac** *mac-address* **set eou revalidate posture-token** *posture-token*

次に、すべてのクライアントレス ホストを再確認する例を示します。

```
Console> (enable) set eou revalidate authentication clientless
Revalidate all clientless hosts
Console> (enable)
```

LAN ポート IP イベントの EOU ロギングのイネーブル化またはディセーブル化

LAN ポート IP イベントの EOU ロギングをイネーブルまたはディセーブルにするには、イネーブル モードで次の作業を行います（デフォルトはディセーブル）。

作業	コマンド
LAN ポート IP イベントの EOU ロギングをイネーブルまたはディセーブルにします。	**set eou logging** {**enable** | **disable**}

次に、LAN ポート IP イベントの EOU ロギングをイネーブルにする例を示します。

```
Console> (enable) set eou logging enable
EoU Logging enabled
Console> (enable)
```

EAPOUDP 関連タイマーの設定

EAPOUDP 関連タイマーを設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
EAPOUDP 関連タイマーを設定します。	**set eou timeout aaa** *aaa-timeout* **set eou timeout hold-period** *hold-timeout* **set eou timeout retransmit** *retransmit-timeout* **set eou timeout revalidation** *revalidation-timeout* **set eou timeout status-query** *status-query-timeout*

タイマーのデフォルトおよび範囲は、次のとおりです。

- aaa ― デフォルトは 60 秒で、範囲は 1 ～ 60 秒です。
- hold-period ― デフォルトは 180 秒で、範囲は 60 ～ 86400 秒です。
- retransmit ― デフォルトは 30 秒で、範囲は 1 ～ 60 秒です。
- revalidation ― デフォルトは 3600 秒で、範囲は 5 ～ 86400 秒です。
- status-query ― デフォルトは 300 秒で、範囲は 30 ～ 1800 秒です。

次に、再確認タイマーを 200 秒に設定する例を示します。

```
Console> (enable) set eou timeout revalidation 200
Console> (enable)
```

EOU レート制限の設定

EOU レート制限（デフォルトは 0 で、範囲は 10 ～ 200）を設定するには、イネーブル モードで次の作業を実行します。

作業	コマンド
EOU レート制限を設定します。	**set eou rate-limit** *ratelimit*

次に、EOU レート制限を 40 に設定する例を示します。

```
Console> (enable) set eou rate-limit 40
eou ratelimit set to 40.
Console> (enable)
```

EOU RADIUS アカウンティングのイネーブル化またはディセーブル化

EOU RADIUS アカウンティングをイネーブルまたはディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
EOU RADIUS アカウンティングをイネーブルまたはディセーブルにします。	**set eou radius-accounting** {**enable** | **disable**}

次に、EOU RADIUS アカウンティングをイネーブルにする例を示します。

```
Console> (enable) set eou radius-accounting enable
Radius Accounting for Eou Enabled.
Console> (enable)
```

ポート単位での LAN ポート IP のバイパス、ディセーブル化、またはイネーブル化

LAN ポート IP をポート単位でバイパス、ディセーブル化、またはイネーブル化できます。**auto** モードを指定すると、クライアントが検出された場合に LAN ポート IP が自動的にイネーブルになります。

ポート単位で、LAN ポート IP のバイパス、ディセーブル化、または auto モードを指定するには、イネーブル モードで次の作業を実行します。

作業	コマンド
ポート単位で LAN ポート IP のバイパス、ディセーブル化、または auto モードを指定します。	**set port eou** *mod*/*port* {**auto** | **bypass** | **disable** | **initialize** | **revalidate**}

次に、ポート 5/1 で LAN ポート IP をイネーブルにする例を示します。

```
Console> (enable) set port eou 5/1 auto
EoU enabled on 5/1
Console> (enable)
```

次に、ポート 7/1 を bypass モードに設定する例を示します。

```
Console> (enable) set port eou 7/1 bypass

Eou Bypass enabled on 7/1
Console> (enable)
```

ポート単位での LAN ポート IP の初期化

ポート単位で LAN ポート IP を初期化するには、イネーブル モードで次の作業を行います。

作業	コマンド
ポート単位で LAN ポート IP を初期化します。	**set port eou** *mod*/*port* **initialize**

次に、ポート 7/1 で LAN ポート IP を初期化する例を示します。

```
Console> (enable) set port eou 7/1 initialize
Initializing EoU for all hosts on port 7/1
Console> (enable)
```

ポート単位での LAN ポート IP の再確認

ポート単位で LAN ポート IP を再確認するには、イネーブル モードで次の作業を行います。

作業	コマンド
ポート単位で LAN ポート IP を再確認します。	**set port eou** *mod*/*port* **revalidate**

次に、ポート 7/1 で LAN ポート IP を再確認する例を示します。

```
Console> (enable) set port eou 7/1 revalidate
Re-validating EoU for all hosts on port 7/1
Console> (enable)
```

スーパバイザ エンジンへの LAN ポート IP 制御パケットのリダイレクション

スーパバイザ エンジンにすべての LAN ポート IP 制御パケット（EAP over UDP パケット）をリダイレクトするには、イネーブル モードで次の作業を実行します。

作業	コマンド
スーパバイザ エンジンにすべての LAN ポート IP 制御パケット（EAP over UDP パケット）をリダイレクトします。	**set security acl ip** *acl_name* **permit eapoudp** *ip_mask* [**before** | **modify**] *ace_insert_position*

次に、スーパバイザ エンジンにすべての LAN ポート IP 制御パケット（EAP over UDP パケット）をリダイレクトする例を示します。

提供される予定です。

グローバルな EOU 設定の表示

グローバルな EOU 設定を表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
グローバルな EOU 設定を表示します。	**show eou config**

次に、グローバルな EOU 設定を表示する例を示します。

```
Console> (enable) show eou config
Eou Protocol Version : 1
Eou Global Config
-----------------
Eou Global Enable         : Enabled
Eou Clientless            : Disabled
Eou Logging               : Enabled
Eou Radius Accounting     : Enabled
Eou MaxRetry              : 3
Eou AAA timeout           : 60
Eou Hold timeout          : 180
Eou Retransmit timeout    : 30
Eou Revalidation timeout  : 3600
Eou Status Query timeout  : 300
Eou Rate Limit            : 40
Eou Udp Port              : 21862

Ip Exception List and Policies
--------------------------------------
0.0.0.18         255.255.255.224  TEST

Console> (enable)
```

すべての LAN ポート IP 対応ポート上の LAN ポート IP ステートの要約の表示

すべての LAN ポート IP 対応ポート上の LAN ポート IP ステートの要約を表示するには、ユーザ モードで次の作業を実行します。

作業	コマンド
すべての LAN ポート IP 対応ポート上の LAN ポート IP ステートの要約を表示します。	**show eou all**

次に、すべての LAN ポート IP 対応ポート上の LAN ポート IP ステートの要約を表示する例を示します。

```
Console> (enable) show eou all
Eou Summary
-----------
Eou Global State = enabled

Currently Validating EOU Sessions = 0
mNo/pNo   Host Ip            Nac_Token   Host_Fsm_State   Username
-------   ----------------   ---------   --------------   --------
Console> (enable)
```

ポート単位の LAN ポート IP ステートの要約の表示

LAN ポート IP 対応ポートのポート単位の LAN ポート IP ステートの要約を表示するには、ユーザ モードで次の作業を実行します。

作業	コマンド
LAN ポート IP 対応ポートのポート単位の LAN ポート IP ステートの要約を表示します。	**show port eou** *mod/port*

次に、ポート 7/1 上の LAN ポート IP ステートの要約を表示する例を示します。

```
Console> (enable) show port eou 7/1
Port     EOU-State IP Address      MAC Address
-------- --------- --------------- -----------------
 7/1     bypass    -               -

Port     FSM State     Auth Type   SQ-Timeout Session Timeout
-------- ------------- ----------- ---------- ---------------
 7/1      -             -           -          -

Port     Posture      URL Redirect
-------- ------------ --------------------
 7/1      -            -

Port     Termination action Session id
-------- ------------------ --------------------------------
 7/1      -                  -
Console> (enable)
```

ホスト固有の情報の表示

ホスト固有の情報を表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
ホスト固有の情報を表示します。	**show eou host** {**ip** | **mac**} *value* **show eou host mac_address** *mac_address*

次に、ホスト固有の情報を表示する例を示します。

```
Console> (enable) show eou host 9.6.2.15
HostIP          HostMac           Port   Posture-token
--------------- ----------------- ------ --------------------
9.6.2.15        00-11-85-8d-bf-ab 2/5    Healthy
IP Address      Eou State     AuthType SQTimeout SessTimeout
--------------- ------------- -------- --------- -----------
9.6.2.15        authenticated eap      301       3600
Console> (enable)
```

EOU 認証関連情報の表示

次の認証関連情報を表示するには、ユーザ モードで次の作業を行います。

- **clientless** ― すべてのクライアントレス ポートを表示します。
- **eap** ― EAP 認証をするすべてのポートを表示します。
- **static** ― 例外リストのすべてのホストを表示します。

作業	コマンド
認証関連情報を表示します。	**show eou authentication** {**clientless** | **eap** | **static**}

次に、認証関連情報を表示する例を示します。

```
Console> (enable) show eou authentication eap
Host IP         HostMac            Port    Posture-token
--------------- ------------------ ------- --------------------
9.6.2.15        00-11-85-8d-bf-ab  2/5     Healthy
IP Address      Eou State     AuthType  SQTimeout SessTimeout
--------------- ------------- --------- --------- -----------
9.6.2.15        authenticated eap       301       3600

Console> (enable)
```

EOU ログの表示

EOU ログを表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
EOU ログを表示します。	**show eou log**

次に、EOU ログを表示する例を示します。

```
Console> (enable) show eou log
LPIP-EVENT : New ip on port 3/12 9.9.150.21 from Arp-inspection
LPIP-ERROR : Failure to get host information for 9.9.143.20
LPIP-EVENT : Host 9.9.150.34 moved to EAPOUDP_TX_HELLO state
Console> (enable)
```

ポスチャトークン単位の EOU 結果の表示

ポスチャトークン単位の EOU 結果を表示するには、ユーザ モードで次の作業を実行します。

作業	コマンド
ポスチャトークン単位の EOU 結果を表示します。	**show eou posture-token** *posture_token*

LAN ポート IP 設定の消去

LAN ポート IP 設定を消去して、デフォルト値に戻すには、イネーブル モードで次の作業を実行します。

作業	コマンド
LAN ポート IP 設定を消去して、デフォルト値に戻します。	**clear eou config**

次に、LAN ポート IP 設定を消去して、デフォルト値に戻す例を示します。

```
Console> (enable) clear eou config
This command will disable EoU on all ports and take EoU parameter values back to
defaults.
Do you want to continue (y/n) [n]? y
Console> (enable)
```

すべての LAN ポート IP パラメータの消去

このコマンドにより、すべてのポートで学習されたホストの EOU セッションすべてが消去されます。EOU 設定は消去されません。すべての LAN ポート IP パラメータを消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
すべての LAN ポート IP パラメータを消去します。	**clear eou all**

次に、すべての LAN ポート IP パラメータを消去する例を示します。

```
Console> (enable) clear eou all
Console> (enable)
```

特定のホストの LAN ポート IP セッションの消去

MAC アドレスまたは IP アドレスにより特定のホストの LAN ポート IP セッションを消去するには、イネーブル モードで次の作業を実行します。

作業	コマンド
MAC アドレスまたは IP アドレスにより特定のホストの LAN ポート IP セッションを消去します。	**clear eou host** {*ip-address* | *mac-address*}

次に、指定の IP アドレスのホストの EOU セッションを消去する例を示します。

```
Console> (enable) clear eou host 9.9.10.10
EOU session of host with IP 9.9.10.10 cleared.
Console> (enable)
```

例外グループからの IP アドレスの消去または例外グループの消去

例外グループから IP アドレスを消去するか、または例外グループを消去するには、イネーブル モードで次の作業を実行します。

作業	コマンド
例外グループから IP アドレスを消去するか、または例外グループを消去します。	**clear eou authorize ip** *ip-address* **policy** *policy_name* **clear eou authorize ip** *ip-address ip_mask* **policy** *policy_name* **clear eou authorize mac-address** *mac_address* **policy** *policy_name* **clear eou authorize mac-address** *mac_address mac_mask* **policy** *policy_name*

次に、例外グループから IP アドレスを消去する例を示します。

```
Console> (enable) clear eou authorize ip 10.1.1.1 255.255.255.240 policy pol1
Cleared host 10.1.1.1 255.255.255.240 from exception group and removed its policy
mapping.
Console> (enable)
```

EAPOUDP 関連タイマーのデフォルト値へのクリア

EAPOUDP 関連タイマーをデフォルト値にクリアするには、イネーブル モードで次の作業を行います。

作業	コマンド
EAPOUDP 関連タイマーをデフォルト値にクリアします。	**clear eou timeout** [**aaa** | **hold-period** | **restransmit** | **revalidation** | **status-query**]

次に、保留期間タイマーをデフォルト値にクリアする例を示します。

```
Console> (enable) clear eou timeout hold-period
Console> (enable)
```

CTA パケットの再送信回数の消去

グローバルな CTA パケットの再送信回数を消去するには、イネーブル モードで次の作業を実行します（このコマンドにより、再送信回数がデフォルト値の 3 に戻されます）。

作業	コマンド
グローバルな CTA パケット再送信回数を消去します。	**clear eou max-retry**

次に、グローバルな CTA パケットの再送信回数を消去する例を示します。

```
Console> (enable) clear eou max-retry
Eou max-retry set to 3
Console> (enable)
```

PBACL の設定

ここでは、PBACL を設定する手順について説明します。

既存のポリシー グループへの IP アドレスの追加

このコマンドにより、既存のポリシー グループに IP アドレスを追加できるようになります。グループ データベースにグループ名が存在しない場合、このコマンドは失敗します。

既存のポリシー グループに IP アドレスを追加するには、イネーブル モードで次の作業を実行します。

作業	コマンド
既存のポリシー グループに IP アドレスを追加します。	**set policy group** *group-name* **ip-address** *ip-address*

次に、既存のポリシー グループに IP アドレスを追加する例を示します。

```
Console> (enable) set policy group grp1 ip-address 100.1.1.1 255.255.255.255
Added IP 100.1.1.1/255.255.255.255 to policy group grp1.
Console> (enable)
```

ポリシー テンプレートへのポリシー グループの追加

ポリシー テンプレートにポリシー グループを追加できます。ポリシー テンプレートが存在しない場合は、作成されます。同様に、グループ名が存在しない場合も作成されます。

ポリシー テンプレートにポリシー グループを追加するには、イネーブル モードで次の作業を実行します。

作業	コマンド
ポリシー テンプレートにポリシー グループを追加します。	**set policy name** *policy-name* **group** *group-name*

次に、ポリシー テンプレートにポリシー グループを追加する例を示します。

```
Console> (enable) set policy name pol1 group grp1
Added group grp1 to policy template pol1.
Console> (enable)
```

ポリシー グループからの IP アドレスの消去

ポリシー グループから IP アドレスを消去するには、イネーブル モードで次の作業を実行します。

作業	コマンド
ポリシー グループから IP アドレスを消去します。	**clear policy group** *group-name* **ip-address** *ip-address*

次に、ポリシー グループから IP アドレスを消去する例を示します。

```
Console> (enable) clear policy group grp1 ip-address 100.1.1.1
Cleared IP 100.1.1.1 from policy group grp1.
Console> (enable)
```

ポリシー テンプレートからのポリシー グループの消去

ポリシー テンプレートからポリシー グループを消去するには、イネーブル モードで次の作業を実行します。

作業	コマンド
ポリシー テンプレートからポリシー グループを消去します。	**clear policy name** *policy-name* **group** *group-name*

次に、ポリシー テンプレートからポリシー グループを消去する例を示します。

```
Console> (enable) clear policy name pol1 group grp1
Cleared group grp1 from policy template pol1.
Console> (enable)
```

ポリシー グループ情報の表示

ポリシー グループ情報を表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
ポリシー グループ情報を表示します。	**show policy group** {**all** | *group-name*}

次に、ポリシー グループ情報を表示する例を示します。

```
Console> (enable) show policy group all
Group Name            = grp1
Group Id                  = 1
No.of IP Addresses = 3
Src Type                  = ACL CLI
     List of Hosts in group.
     ----------------------
     Interface      = 0/0
     IpAddress    =  100.1.1.1
     Src type       = CONFIG

     Interface      = 0/0
     IpAddress    = 100.1.1.2
     Src type       = CONFIG

-------------------------------------------------
Group Name             = grp2
Group Id                   = 2
No.of IP Addresses  = 0
Src Type                  = ACL CLI
Console> (enable)
```

ポリシー テンプレートおよび関連するポリシー グループの表示

ポリシー テンプレートおよび関連するポリシー グループを表示するには、イネーブル モードで次の作業を実行します。

作業	コマンド
ポリシー テンプレートおよび関連するポリシー グループを表示します。	**show policy name** {**all** | *policy-name*}

次に、ポリシー テンプレートおよび関連するポリシー グループを表示する例を示します。

```
Console> (enable) show policy name all
Policy Template pol1
Security Policy Groups :grp1 grp2
Console> (enable)
```

LAN ポート IP の設定例

LAN ポート IP を設定する場合、次の設定例を使用します。

- ポート 8/14 が RADIUS サーバに接続
- ポート 8/13 が CTA を持つホストに接続
- ポート 8/24 が CTA を持たないホストに接続

```
begin
!
# ***** NON-DEFAULT CONFIGURATION *****
!
!
#time: Fri Mar 4 2005, 17:11:20
!
#version 8.5(0.44)JAC
!
!
#Nac
set eou enable
set eou allow clientless enable
set policy name exception_policy group exception_hosts
set eou authorize ip 77.0.0.90 policy exception_policy
!
#radius
set radius server 10.76.39.93 auth-port 1812 primary
set radius key cisco
!
#vtp
set vtp mode transparent vlan
set vlan 12 name RADIUS_CONNECTIVIY type ethernet mtu 1500 said 100012 state active
set vlan 77 name ALL_HOSTS type ethernet mtu 1500 said 100077 state active
set vlan 1,3
!
#ip
set interface sc0 12 9.6.3.3/255.255.255.0 9.6.3.255
set interface sl0 down
set interface sc1 77 77.0.0.2/255.255.255.0 77.0.0.255
set ip route 10.0.0.0/255.0.0.0 9.6.3.1
!
!
#security ACLs
clear security acl all
#NACACL
set security acl ip NACACL permit arp
set security acl ip NACACL permit arp-inspection any any
set security acl ip NACACL permit dhcp-snooping
```

```
set security acl ip NACACL permit udp any eq 21862 host 9.6.3.3 eq 53000
set security acl ip NACACL permit ip group Healthy_hosts any
set security acl ip NACACL deny ip group infected_hosts any
set security acl ip NACACL permit ip group exception_hosts any
set security acl ip NACACL permit ip group clientless_hosts host 10.76.39.100
#
commit security acl all #
# map the ACL to VLAN 77
set security acl map NACACL 77
!
#module 8 : 48-port 10/100BaseTX Ethernet
set vlan 12 8/14
set vlan 77 8/13,8/24
set port name 8/13 HOSTS
set port name 8/14 RADIUS
set port name 8/24 HOSTS
set port eou 8/13 enable
set port eou 8/24 bypass
set port dhcp-snooping 8/14 trust enable
!
#module 9 empty
!
#module 15 : 1-port Multilayer Switch Feature Card
!
#module 16 empty
!
#switch port analyzer
set span permit-list disable
set span permit-list include
end
sup2> (enable)
```

Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）の設定（デフォルト ルータ）は、次のとおりです。

```
Router# show run
Building configuration...
Current configuration : 509 bytes
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
!
ip subnet-zero
!
!
!
ip multicast-routing
ip dhcp-server 10.76.39.93
redundancy
 high-availability
 single-router-mode
!
!
!
interface Vlan12
 ip address 9.6.3.6 255.255.255.0
!
interface Vlan77
 ip address 77.0.0.76 255.255.255.0
 ip helper-address 10.76.39.93
!
ip classless
ip route 10.76.0.0 255.255.0.0 Vlan12
no ip http server
!
!
!
line con 0
line vty 0 4
 login
!
!
end
```

LAN ポート 802.1X による NAC の設定

(注) LAN ポート 802.1X 固有の CLI コマンドはありません。ポスチャ確認および認証は、標準の 802.1X 認証を通じて単一の EAP トンネル内でシームレスに行われます。IEEE 802.1X 認証の設定については、第 39 章「802.1X 認証の設定」を参照してください。

(注) LAN ポート IP に適用される制限事項は、LAN ポート 802.1X にも適用されます。LAN ポート IP の制限事項については、「LAN ポート IP 設定時の注意事項および制限事項」（p.42-6）を参照してください。

LAN ポート 802.1X は標準の 802.1X 認証と組み合わさって、レイヤ 2 ネットワーク エッジでの統合型認証およびポスチャ確認メカニズムを提供します。LAN ポート 802.1X は、ネットワーク内で LAN ポート IP と同じポイントで動作しますが、ポスチャ確認の開始、ホストと認証サーバ間の通信、および生成されるアクセス制限の適用には、異なるメカニズムを使用します。

LAN ポート 802.1X ポスチャ確認は、標準の 802.1X メカニズム（要求元が NAD に EAPOL-Start メッセージを送信するか、または NAD が EAP-Request/Identity メッセージにより要求元をプローブする）によりトリガーされます。ポスチャ情報はバックエンド サーバにより確認されるため、ユーザ ID 証明書とともに送信されます。要求元と NAD 間の認証交換は、EAPOL 上で行われます。ポリシーの適用は、指定された VLAN に認証済みポートを割り当ててセグメンテーションを提供したり、ポスチャが不十分なホストを検疫することにより、レイヤ 2 で行われます。

(注) LAN ポート IP とは異なり、LAN ポート 802.1X ではポスチャが適切でないホストからの非 IP バージョン 4 トラフィックを制限するため、このような制限を必要とする配置での使用が推奨されます。

LAN ポート 802.1X のポリシー適用は、次のとおりです（標準 802.1X 認証ではサポートされています）。

- VLAN 割り当て — 通常のネイティブ VLAN 割り当て（LAN ポート 802.1X では、プライベート VLAN 割り当てはサポートされません）
- セキュリティ ACL 割り当て — RADIUS サーバから送信される PBACL 名は、ポート インターフェイスに割り当てられ、PACL または VACL となります。
- ポリシー グループ — PBACL ポリシー グループは、ACS サーバから送信されます。

LAN ポート 802.1X では、ポリシー適用に VLAN と PBACL の組み合わせが使用され、LAN ポート IP では PBACL のみが使用されます。

再認証は、標準の 802.1X 認証と同様に機能し、RADIUS サーバが送信したセッション タイムアウトおよびターミネーション アクション アトリビュート、またはローカルの CLI で設定したアトリビュートを使用します。これらのアトリビュートは、RADIUS サーバからの Access-Accept メッセージの一部として受信されません。

LAN ポート 802.1X では、ホストは次のカテゴリのいずれかに分類されます。

- 拡張 CTA — この CTA は、単一の EAP トンネル内の認証 Type-Length-Value（TLV）とポスチャ TLV の両方を送信でき、RADIUS サーバからのポリシー適用には、VLAN 割り当てと PBACL グループの両方が含まれます。
- レガシー要求元およびレガシー CTA — これらのホストには、拡張 CTA がありません。CTA に接続できない標準 802.1X 要求元はあります。また、EAPoUDP を使用してポスチャ確認できるレガシー CTA もあります。これらのホストでは、LAN ポート 802.1X が完了すると、スイッチがポスチャ確認の結果を確認します。ポスチャ結果が受信されなければ、ホストに拡張 CTA がないとみなされます。ポート上で設定されている LAN ポート IP は、ポスチャ確認を行うようトリガーされます。このカテゴリは、LAN ポート IP と 802.1X 認証の組み合わせです。
- レガシー 要求元および CTA なし — これらの 802.1X 対応ホストには、CTA がありません。802.1X 認証の完了後、スイッチはポスチャ確認が実行されていないことを認識し、ポート上で LAN ポート IP がイネーブルの場合は、スイッチは LAN ポート IP でポスチャ確認を実行するよう指示します。LAN ポート IP が実行されると、ホストが EoU パケットに応答していないことを認識し、ホストに「クライアントレス」ポスチャ ポリシーをダウンロードします。対照的に、802.1X 認証では認証結果に基づいてポリシーを適用します。
- 要求元なしおよびレガシー CTA — ホストに 802.1X 対応の要求元がない場合、802.1X のタイムアウトが発生し、ポートはゲスト VLAN に移行されます。または MAC 認証バイパスが設定されている場合は、ホストの MAC アドレスを認証するのに MAC 認証バイパスが要求されます。ポートの許可後（MAC 認証バイパスまたはゲスト VLAN により）、LAN ポート IP が設定されている場合は、LAN ポート IP がポスチャ確認を行い、ポスチャ ポリシーを取得します。
- 要求元なしおよび CTA なし — ダム ホストが 802.1X 対応でなく、CTA もインストールされていないスイッチ ポートに接続されている場合、スイッチは最初、EAPOL 交換を行い、応答がない場合は、ポートをゲスト VLAN ステートに移行するか、または MAC アドレス バイパス（設定されている場合）が MAC アドレスを認証するよう要求します。ポートがこれらいずれかの機能により許可されると、スイッチは LAN ポート IP（設定されている場合）がポスチャ確認を行うよう要求します。LAN ポート IP では、hello メッセージに応答がないことを認識し、クライアントレス認証を行って、反応がないホスト用にポスチャ ポリシーを取得します。

CHAPTER 43

ユニキャスト フラッディング ブロックの設定

この章では、Catalyst 6500 シリーズ スイッチ上でユニキャスト フラッディング ブロックを設定する方法について説明します。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

この章で説明する内容は、次のとおりです。

ユニキャスト フラッディング ブロックの機能

ポート単位で任意のイーサネット ポート上でのユニキャスト フラッディング ブロックをイネーブルにできます。ユニキャスト フラッディング ブロックによって、ホストが 1 つしかポートに接続していないイーサネットポート上のユニキャスト フラッディング パケットを廃棄できます。スイッチのすべてのイーサネット ポートはユニキャスト フラッディングを許可するよう設定されていますが、ユニキャスト フラッディング ブロックを使用することで、ユニキャスト フラッディング パケットがポートに到達する前に廃棄できます。

注意　ユニキャスト フラッディング ブロックをイネーブルにするには、先にイーサネット ポートに対応付けられたスタティック CAM（連想メモリ）エントリが存在していなければなりません。ポートに対応付けられたスタティック CAM エントリがない場合は、ユニキャスト フラッディング ブロックをイネーブルにするとネットワークとの接続が切断されます。**show cam static** コマンドを入力すると、スタティック CAM エントリがあるかどうかが確認できます。

（注）　セキュア ポート上にユニキャスト フラッディング ブロックを設定する場合は、第 37 章「ポート セキュリティの設定」を参照してください。

ユニキャスト フラッディング ブロック設定時の注意事項

ここでは、ユニキャスト フラッディング ブロック設定時の注意事項について説明します。

- イーサネット ポートだけがユニキャスト フラッディング トラフィックをブロックできます。
- イーサネット ポートが Internetwork Packet Exchange（IPX）ネットワークに組み込まれている場合は、CAM テーブルにスタティック CAM エントリを手動で入力してから、ポートのユニキャスト フラッディング ブロックをディセーブルにする必要があります。
- SPAN 宛先ポート上では、ユニキャスト フラッディング ブロックを設定できません。
- ユニキャスト フラッディング ブロック ポート上では、SPAN 宛先を設定できません。
- トランク ポート上では、ユニキャスト フラッディング ブロックを設定できません。トランク ポート上では、ユニキャスト フラッディング ブロックを設定しようとすると、エラー メッセージが表示されます。
- ポート チャネル上では、ユニキャスト フラッディング ブロックを設定できません。
- ユニキャスト フラッディング ブロック ポート上では、ポート チャネルを設定できません。
- ユニキャスト フラッディング ブロックと GARP VLAN Registration Protocol（GVRP）は、一緒に使用できません。ユニキャスト フラッディング パケットをブロックして、同時に GVRP スイッチと VLAN（仮想 LAN）設定情報を交換することはできません。

スイッチ上でのユニキャスト フラッディング ブロックの設定

ここでは、ユニキャスト フラッディング ブロックの設定手順について説明します。

（注）　ユニキャスト フラッディング ブロックを設定するときは、ユニキャスト フラッディング ブロックはプロトコル フィルタリングなどのその他の機能に優先されるので注意してください。

ユニキャスト フラッディング ブロックのイネーブル化

ポート上でユニキャスト フラッディング パケットを廃棄するようにスイッチを設定するには、ユニキャスト フラッディング ブロックをイネーブルにする必要があります。

（注）　MAC（メディア アクセス制御）アドレスの限度に達すると、ポートはユニキャスト フラッディングをディセーブルにします。

ユニキャスト フラッディング ブロックをイネーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
必要なイーサネット ポート上でユニキャスト フラッディング ブロックをイネーブルにし、ユニキャスト フラッディングをディセーブルにします。	**set port unicast-flood** *mod/port* **disable**

次に、ポート上でユニキャスト フラッディング ブロックをディセーブルにする例を示します。

```
Console> (enable) set port unicast-flood 4/1 disable
WARNING: Trunking & Channelling will be disabled on the port.
Unicast Flooding is successfully disabled on the port 4/1.
Console> (enable)
```

ユニキャスト フラッディング ブロックのディセーブル化

ポート上でユニキャスト フラッディング パケットを受信するようスイッチを設定するには、ユニキャスト フラッディング ブロックをディセーブルにする必要があります。

ユニキャスト フラッディング ブロックをディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
必要なイーサネット ポート上でユニキャスト フラッディング ブロックをディセーブルにし、ユニキャスト フラッディングをイネーブルにします。	**set port unicast-flood** *mod/port* **enable**

次に、ポート上でユニキャスト フラッディング ブロックをディセーブルにする例を示します。

```
Console> (enable) set port unicast-flood 4/1 enable
Unicast Flooding is successfully enabled on the port 4/1.
Console> (enable)
```

ユニキャスト フラッディング ブロックの表示

ユニキャスト フラッディング ブロック情報を表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
ポートごとの、ユニキャスト フラッディング ブロック情報を表示します。	**show port unicast-flood** *mod/port*

次に、モジュール 4 のポート 1 のユニキャスト フラッディング ブロック情報を表示する例を示します。

```
Console> (enable) show port unicast-flood 4/1
Port      Unicast Flooding
----      ----------------
4/1       Disabled
Console> (enable)
```

CHAPTER 44

SNMP の設定

この章では、Catalyst 6500 シリーズ スイッチ上で SNMP（簡易ネットワーク管理プロトコル）を設定する方法について説明します。

この章で説明する内容は、次のとおりです。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

SNMP の用語

表 44-1 に、SNMP で使用する用語を定義します。

表 44-1　SNMP の用語

用語	定義
認証	データ整合性、データ オリジン認証など、メッセージ整合性およびメッセージ再送に対する保護を行うプロセス
信頼できる SNMP エンジン	ネットワーク通信に使用される SNMP の 1 つが、メッセージの再送、遅延、転送に対して保護する許容 SNMP エンジンに指定されます。SNMPv3 パケットの認証および暗号化に使用されるセキュリティ キーは、信頼できる SNMP エンジンの ID およびユーザ パスワードと同等の機能を持ちます。応答を返す SNMP メッセージ（たとえば、get exact、get next、set request）の場合、このメッセージの*受信側*が信頼できる相手となります。応答を返さない SNMP メッセージの場合、*送信側*が信頼できる相手となります。
コミュニティ ストリング	管理ステーションと SNMPv1 または SNMPv2c エンジンとの間でメッセージの認証に使用する文字列
データ整合性	不正な方法でメッセージ パケットが変更または破壊されていないデータの状態（ステート）
データ オリジン認証	メッセージの送信先と思われるユーザの ID を確認する能力。この能力により、別の SNMP エンジンによるメッセージ取り込みと再送からユーザを保護します。また、誤ったパスワードまたはセキュリティ レベルを使用する特定のユーザとのパケット送受信からも保護します。
暗号化	SNMP パケットの内容をスクランブルして不正なユーザからデータを隠す方法
グループ	特定のセキュリティ モデルに属すユーザの集合。グループは、そこに属するすべてのユーザのアクセス権を定義します。アクセス権は、読み取り、書き込み、作成ができる SNMP オブジェクトを定義します。また、グループはユーザが受け取りを許可される通知も定義します。
通知ホスト	通知（トラップおよび通知）の送信先となる SNMP エンティティ
通知ビュー	各グループのビューの名前（最大 64 文字）。ビュー名は、グループ内の各ユーザに送信できる通知リストを定義します。
プライバシ	SNMP パケットの内容の暗号化されたステート。このステートでは、内容はネットワーク上で公開されないようになっています。暗号化は、CBC-DES（DES-56）と呼ばれるアルゴリズムで実行されます。
読み取りビュー	各グループのビューの名前（最大 64 文字）。ビュー名は、グループ内の各ユーザが読み取りできる Object Identifier（OID; オブジェクト識別子）リストを定義します。

表 44-1　SNMP の用語（続き）

用語	定義
セキュリティ レベル	各 SNMP パケット上で実行されるセキュリティ アルゴリズムのタイプ。noauth、auth、および priv の 3 つのレベルがあります。noauth レベルは、ユーザ名のストリング照合によってパケットを認証します。auth レベルは、HMAC MD5 または SHA アルゴリズムを使用してパケットを認証します。priv レベルは、HMAC MD5 または SHA アルゴリズムを使用してパケットを認証し、CBC-DES（DES-56）アルゴリズムでパケットを暗号化します。
セキュリティ モデル	SNMP エージェントが使用するセキュリティ戦略。現在、Cisco IOS ソフトウェアは SNMPv1、SNMPv2c、および SNMPv3 という 3 種類のセキュリティ モデルをサポートしています。
SNMP	ネットワーク装置をモニタおよび制御し、設定、統計情報収集、パフォーマンス、およびセキュリティを管理する手段を備えたネットワーク管理プロトコル
SNMPv2c	SNMP の 2 番めのバージョン。中央集中および分散型ネットワーク管理計画をサポートし、SMI、プロトコル動作、管理アーキテクチャ、およびセキュリティ機能が強化されています。
SNMP エンジン	ローカルまたはリモート装置に常駐できる SNMP
SNMP エンティティ	SNMPv1 や SNMPv2c と異なり、SNMPv3 では、SNMP エージェントや SNMP マネージャなどの用語は廃止されています。これらの概念を統合して SNMP エンティティと呼びます。SNMP エンティティは、SNMP エンジンと SNMP アプリケーションで構成されます。
SNMP グループ	アクセス ポリシーを定義する共通 SNMP リストに属する SNMP ユーザの集合で、ここでは OID 番号は読み取りアクセスも書き込みアクセスもともに可能です。特定の SNMP グループに属するユーザは、そのグループによって定義されたこれらの属性をすべて継承します。
SNMP ユーザ	SNMP 管理操作のサービス対象者。ユーザとは情報を受信するリモート SNMP エンジン上にいる人のことです。
SNMP ビュー	SNMP オブジェクトとそのオブジェクトが利用できるアクセス権との間のマッピング。オブジェクトは、それぞれのビューにさまざまなアクセス権を持っています。アクセス権は、コミュニティ ストリングまたはユーザがオブジェクトにアクセス可能かどうかを示します。
書き込みビュー	各グループのビューの名前（最大 64 文字）。ビュー名は、グループ内の各ユーザが作成または変更できる OID リストを定義します。

SNMP の機能

SNMP はアプリケーションレイヤ プロトコルで、ネットワーク装置間の管理情報の交換を容易にします。SNMP を使用することにより、ネットワーク管理者はネットワーク パフォーマンスの管理、ネットワーク障害の発見と解決、ネットワーク拡大の計画立案ができます。

SNMP には次の 3 つのバージョンがあります。

- バージョン 1（SNMPv1）— SNMP の初期の実装です。機能の詳細については、RFC 1157 を参照してください。SNMPv1 の詳細については、「SNMPv1 および SNMPv2c の機能」（p.44-6）を参照してください。
- バージョン 2（SNMPv2c）— SNMP の 2 番めのリリースで、RFC 1902 に規定されており、データ型、カウンタ サイズ、およびプロトコルの動作について、機能の追加および拡張が施されています。SNMPv2c の詳細については、「SNMPv1 および SNMPv2c の機能」（p.44-6）を参照してください。
- バージョン 3（SNMPv3）— SNMP の最新バージョンで、詳細は RFC 2571、RFC 2572、RFC 2573、RFC 2574、RFC 2575 に規定されています。SNMPv1 および SNMPv2c 対応の Catalyst エンタープライズ LAN スイッチでの SNMP 機能は変わりませんが、管理およびセキュリティについては大幅に機能が強化されています。SNMPv3 の詳細については、「SNMPv3 の機能」（p.44-8）を参照してください。

セキュリティ モデルおよびセキュリティ レベル

セキュリティ モデルは、ユーザと、ユーザが属するグループに対して設定された認証戦略です。セキュリティ レベルとは、セキュリティ モデル内のセキュリティの許可されたレベルです。セキュリティ モデルとセキュリティ レベルの組み合わせによって、SNMP パケットの処理の際に採用されるセキュリティ メカニズムが決まります。SNMPv1、SNMPv2c、および SNMPv3 の 3 つのセキュリティ モデルがあります。表 44-2 に、セキュリティ モデルとセキュリティ レベルの組み合わせを示します。

表 44-2　SNMP セキュリティ レベル

モデル	レベル	認証	暗号化	処理
v1	noAuthNoPriv	コミュニティ ストリング	なし	認証にコミュニティ ストリングの照合を使用します。
v2c	noAuthNoPriv	コミュニティ ストリング	なし	認証にコミュニティ ストリングの照合を使用します。
v3	noAuthNoPriv	ユーザ名	なし	認証にユーザ名の照合を使用します。
v3	authNoPriv	MD5 または SHA	なし	HMAC-MD5 または HMAC-SHA アルゴリズムに基づいて認証を行います。
v3	authPriv	MD5 または SHA	DES	HMAC-MD5 または HMAC-SHA アルゴリズムに基づいて認証を行います。認証の他に、CBC-DES（DES-56）に基づく DES 56 ビット暗号化を行います。

SNMPv3 オブジェクトについて次の事項に注意してください。

- 各ユーザは 1 つのグループに属します。
- グループは、ユーザの集合に対するアクセス ポリシーを定義します。

- SNMP オブジェクトは、読み取り、書き込み、および作成のアクセス ポリシーを参照します。
- グループによって、ユーザが受信できる通知リストが決まります。
- グループは、そのユーザのセキュリティ モデルおよびセキュリティ レベルも定義します。

SNMP ifindex 持続機能

SNMP ifIndex 持続機能は常にイネーブルです。ifIndex 持続機能により、次に示す処理が発生したあとも、ポートおよび VLAN の ifIndex 値は常に保持および使用されます。

- スイッチの再起動
- ハイアベイラビリティ スイッチオーバー
- ソフトウェア アップグレード
- モジュールのリセット
- モジュールの取り外し、および同じタイプのモジュールの取り付け

Fast EtherChannel および Gigabit EtherChannel インターフェイスの場合、ifIndex 値が保持および使用されるのは、ハイアベイラビリティ スイッチオーバーが発生したあとのみです。

SNMPv1 および SNMPv2c の機能

SNMPv1 および SNMPv2c ネットワーク管理で使用するコンポーネントは、次の 3 つのカテゴリに分類されます。

- 管理対象装置（スイッチなど）
- 管理対象装置で実行される SNMP エージェントおよび MIB（管理情報ベース）（Remote Monitoring [RMON] MIB など）
- エージェントと通信して管理対象装置から統計情報およびアラートを入手する、CiscoWorks2000 などの SNMP ネットワーク管理アプリケーション。CiscoWorks2000 の詳細については、「CiscoWorks2000 の使用方法」（p.44-7）を参照してください。

（注） SNMP　管理アプリケーションおよび　SNMP　管理アプリケーションを実行するコンピュータを Network Management System（NMS; ネットワーク管理システム）といいます。

管理対象装置の使用方法

Catalyst 6500 シリーズ スイッチは、次の機能を使用した SNMP ネットワーク管理をサポートする管理対象装置です。

- SNMP トラップ（「CLI での SNMPv1 および SNMPv2c の設定」[p.44-12] を参照）
- スーパバイザ エンジン ソフトウェアの RMON（第 45 章「RMON の設定」を参照）
- 外部 SwitchProbe 装置の RMON および RMON2

SNMP エージェントおよび MIB の使用方法

SNMP ネットワーク管理では、次の SNMP エージェント機能を使用します。

- MIB 変数へのアクセス ― この機能は、NMS からの要求への応答として、SNMP エージェントによって実行されます。SNMP エージェントは要求された MIB 変数の値を検索し、NMS にこれらの値を戻します。
- MIB 変数の設定 ― この機能もまた、NMS からのメッセージへの応答として、SNMP エージェントにより実行されます。SNMP エージェントは、MIB 変数の値を NMS から要求された値に変更します。

（注） MIB の詳細については、http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml を参照してください。

- SNMP トラップ ― この機能は、エージェントで重大イベントが発生したことを NMS に通知するために使用されます。次のいずれかのトラップ イベントが発生すると、SNMP エージェントはトラップ レシーバーとして指定された NMS に対して、SNMP トラップ メッセージを送信します。
  - ― ポートまたはモジュールがアップまたはダウンした場合
  - ― 温度が制限値を超えた場合
  - ― スパニングツリー トポロジーが変更された場合
  - ― 認証に失敗した場合
  - ― 電源障害が発生した場合

- SNMP コミュニティ ストリング ― SNMP コミュニティ ストリングは、MIB オブジェクトへのアクセスを認証する組み込みパスワードです。
  - ― read-only ― コミュニティ ストリング以外のすべての MIB オブジェクトへの読み取りアクセスを許可しますが、書き込みアクセスは許可しません。
  - ― read-write ― すべての MIB オブジェクトへの読み書きアクセスを許可しますが、コミュニティ ストリングへのアクセスは許可しません。
  - ― read-write-all ― コミュニティ ストリングを含むすべての MIB オブジェクトへの読み書きアクセスを許可します。

（注） NMS のコミュニティ ストリング定義は、スイッチの 3 つのコミュニティ ストリング定義の少なくとも 1 つと一致している必要があります。

CiscoWorks2000 の使用方法

CiscoWorks2000 は、シスコのエンタープライズ系ネットワークおよび装置を管理する、管理プラットフォームに依存しない Web ベース製品ファミリーの 1 つです。CiscoWorks2000 には、スイッチド インターネットワークの配置、設定、モニタ、管理、およびトラブルシューティングを実行できる Resource Manager Essentials および CWSI Campus が統合されています。詳細については、次のマニュアルを参照してください。

- 『*Getting Started With Resource Manager Essentials*』
- 『*Getting Started With CWSI Campus*』

SNMPv3 の機能

SNMPv3 には SNMPv1 および SNMPv2c の機能がすべて搭載されているだけでなく、管理とセキュリティについて機能が大幅に強化されています。SNMPv3 は相互運用が可能な標準ベースのプロトコルであり、ネットワーク上でパケットを認証および暗号化して装置に安全にアクセスできるようにします。SNMPv3 に搭載されているセキュリティ機能には、次のものがあります。

- メッセージ整合性 — 不正変更または破壊することなくデータを安全に収集します。
- 認証 — メッセージが有効な送信元からのものかどうかを判別します。
- 暗号化 — パケットの内容をスクランブルして許可されていない送信元から見えないようにします。

SNMP エンティティ

SNMPv1 や SNMPv2c と異なり、SNMPv3 では、*SNMP エージェント*や *SNMP マネージャ*などの概念は廃止されています。これらの概念は *SNMP エンティティ*として統合されています。SNMP エンティティは、SNMP エンジンと SNMP アプリケーションで構成されます。SNMP エンジンは、次の 4 つのコンポーネントで構成されます。

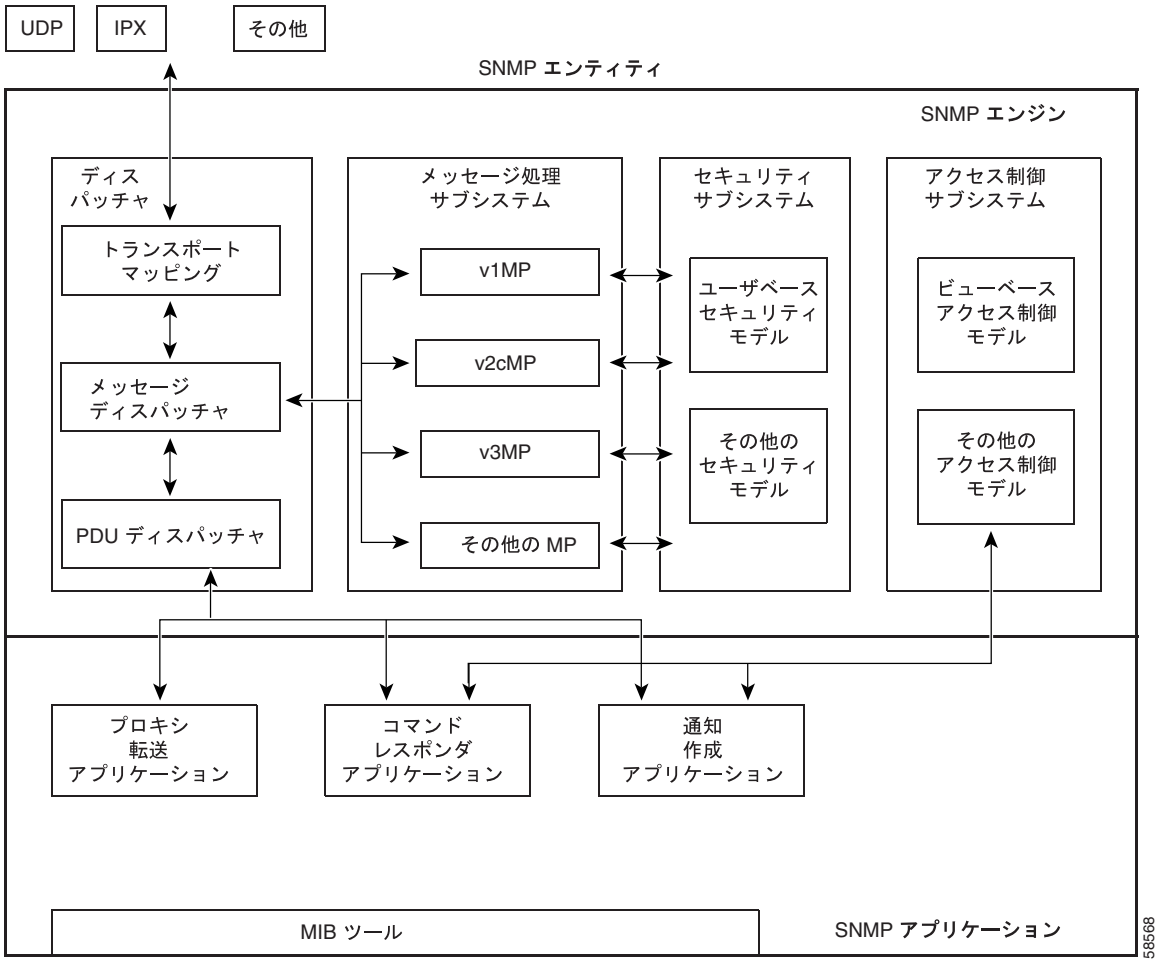
- ディスパッチャ
- メッセージ処理サブシステム
- セキュリティ サブシステム
- アクセス制御サブシステム

図 44-1 に、SNMP エンティティを示します。

ディスパッチャ

ディスパッチャは、メッセージを送受信するトラフィック マネージャです。メッセージの受信後、ディスパッチャは、メッセージのバージョン番号を調べてからそのメッセージを該当するメッセージ処理モデルに渡します。ディスパッチャには、アプリケーションに Protocol Data Unit（PDU; プロトコル データ ユニット）をディスパッチし、メッセージ送信用のトランスポートを選択する役割もあります。

図 44-1　従来の SNMP エージェントに対する SNMP エンティティ



メッセージ処理サブシステム

メッセージ処理サブシステムは、ディスパッチャからの発信 PDU を受け入れ、メッセージ ヘッダーでラップしてディスパッチャに戻すことで伝送の準備をします。また、ディスパッチャからの着信メッセージも受け入れ、各メッセージ ヘッダーを処理し、同封された PDU をディスパッチャに戻します。メッセージ処理サブシステムを実装すると、SNMP（SNMPv1、SNMPv2c、SNMPv3）の 1 つのバージョンに対応する 1 つのメッセージ形式をサポートするか、それぞれが異なるバージョンの SNMP をサポートしている多数のモジュールを装備することになります。

セキュリティ サブシステム

セキュリティ サブシステムは、メッセージを認証して暗号化します。各発信メッセージは、メッセージ処理サブシステムからセキュリティ サブシステムに渡されます。セキュリティ サブシステムは、必要なサービスに応じて同封された PDU とメッセージ ヘッダーの一部のフィールドを暗号化します。また、認証コードを生成してメッセージ ヘッダーに挿入します。メッセージは、暗号化のあと、メッセージ処理サブシステムに戻されます。

各着信メッセージは、メッセージ処理サブシステムからセキュリティ サブシステムに渡されます。セキュリティ サブシステムは、必要に応じて認証コードをチェックし、復号化を実行します。処理されたメッセージは、メッセージ処理サブシステムに戻されます。セキュリティ サブシステムを実装すると、1 つまたは複数の個別のセキュリティ モデルをサポートします。現在、唯一定義されているセキュリティ モデルは SNMPv3 対応の User-based Security Model（USM）で、RFC 2274 に規定されています。

USM は、以下のセキュリティ上の潜在的な脅威から SNMPv3 メッセージを保護します。

- 未許可の SNMP エンティティによって送信中に変更されたメッセージを送信する許可ユーザ
- 許可ユーザになりすます不正ユーザ
- メッセージ ストリームを変更するユーザ
- メッセージを傍受する不正ユーザ

USM は現在、認証プロトコルとして HMAC-MD5-96 および HMAC-SHA-96、プライバシ プロトコルとして CBC-DES を定義しています。

SNMPv1 および SNMPv2c セキュリティ モデルはコミュニティ名の認証しか備えておらず、プライバシは備えていません。

アクセス制御サブシステム

アクセス制御サブシステムは、管理対象オブジェクトへのアクセスを許可するかどうかを決定します。View-based Access Control Model（VACM）を使用することで、どのユーザのどの操作がどの管理対象オブジェクトにアクセスできるかを制御できます。

アプリケーション

SNMPv3 アプリケーションとは、SNMP エンティティ内の内部アプリケーションを指します。この内部アプリケーションでは、次の処理を行います。

- SNMP メッセージの生成
- 受信した SNMP メッセージへの応答
- 通知の生成および受信
- SNMP エンティティ間のメッセージの転送

現在、5 種類のアプリケーションがあります。

- コマンド ジェネレータ ― SNMP コマンドを生成して管理データを収集または設定します。
- コマンド レスポンダ ― 管理データにアクセスします。たとえば、コマンド レスポンダ アプリケーションでは、**processing get**、**get-next**、**get-bulk**、および **set pdus** が使用されます。
- 通知作成 ― トラップまたは情報メッセージを起動します。
- 通知受信 ― トラップまたは情報メッセージを受信し処理します。
- プロキシ転送 ― SNMP エンティティでメッセージを転送します。

SNMP 処理のイネーブル化およびディセーブル化

ここでは、**set snmp enable** | **disable** コマンドを使用して、スイッチに対する SNMP 要求とスイッチからの SNMP トラップの処理をイネーブルまたはディセーブルに設定する手順を説明します。

SNMP をイネーブル モードに設定した場合、そのスイッチに対する他の SNMP 設定と競合しなければ、スイッチへの SNMP 要求が処理されて、SNMP トラップが送出されます。

SNMP をディセーブル モードに設定した場合、そのスイッチに対する他の SNMP 設定とは関係なく、SNMP 要求は無視され、SNMP トラップは送出されません。

いずれの SNMP モードでも（イネーブルまたはディセーブル）、他の SNMP 設定を変更できます。RMON 関連の処理は、いずれのモードにも影響しません。

CLI（コマンド ライン インターフェイス）を使用して SNMP 処理をイネーブルにするには、イネーブル モードで次の作業を行います（SNMP 処理はイネーブル モードがデフォルトです）。

	作業	コマンド
ステップ 1	SNMP 処理をイネーブルにします。	**set snmp enable** | **disable**
ステップ 2	SNMP 処理がイネーブルに設定されたことを確認します。	**show snmp**

次に、SNMP 処理をイネーブルにする例を示します。

```
Console> (enable) set snmp enable
SNMP enabled.
Console> (enable)
```

次に、SNMP 処理をディセーブルにする例を示します。

```
Console> (enable) set snmp disable
SNMP disabled.
Console> (enable)
```

次に、SNMP の設定を確認する例を示します。

```
Console> (enable) show snmp
SNMP:                       Disabled
RMON:                       Disabled
Extended RMON Netflow Enabled : None.
Memory usage limit for new RMON entries: 85 percent
Traps Enabled:
None
Port Traps Enabled: None

Community-Access     Community-String
----------------     --------------------
read-only            public
read-write           private
read-write-all       secret

Trap-Rec-Address Trap-Rec-Community Trap-Rec-Port Trap-Rec-Owner Trap-Rec-Index
---------------- ------------------ ------------- -------------- --------------
Console> (enable)
```

スイッチ上での SNMPv1 および SNMPv2c の設定

ここでは、SNMPv1 および SNMPv2c の基本設定について説明します。Catalyst 6500 シリーズ スイッチによってサポートされる SNMP コマンドの詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

SNMPv1 および SNMPv2c のデフォルト設定

ここに記載されている各コマンドの SNMP デフォルト設定については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

NMS での SNMPv1 および SNMPv2c の設定

NMS での SNMP の設定手順については、NMS のマニュアルを参照してください（「CiscoWorks2000 の使用方法」[p.44-7] を参照）。

スイッチは、RMON2 トラップ宛先テーブルに指定された 20 までのトラップ レシーバーをサポートしています。RMON2 トラップ宛先テーブルは、NMS を使用して設定します。

CLI での SNMPv1 および SNMPv2c の設定

(注)　Release 7.5(1) の拡張 SNMP 機能については、「Release 7.5(1) の SNMPv1 および SNMPv2c 拡張機能」（p.44-14）を参照してください。

CLI を使用して SNMP を設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	各アクセス タイプについて SNMP コミュニティ ストリングを定義します。	**set snmp community read-only** *community_string* **set snmp community read-write** *community_string* **set snmp community read-write-all** *community_string*
ステップ 2	トラップ レシーバーおよびコミュニティを指定します。最大 10 のトラップ レシーバーを指定できます。	**set snmp trap** *rcvr_address rcvr_community*
ステップ 3	トラップ レシーバーに送信する SNMP トラップを指定します。	**set snmp trap enable** [**all** | **auth** | **bridge** | **chassis** | **config** | **entity** | **entityfru** | **envfan** | **envpower** | **envshutdown** | **envtemp** | **flashinsert** | **flashremove** | **ippermit** | **module** | **stpx** | **syslog** | **system** | **vlancreate** | **vlandelete** | **vmps** | **vtp**]
ステップ 4	SNMP の設定を確認します。	**show snmp**

次に、コミュニティ ストリングを定義し、トラップ レシーバーを割り当て、トラップ レシーバーに送信するトラップを指定する例を示します。

```
Console> (enable) set snmp community read-only Everyone
SNMP read-only community string set to 'Everyone'.
Console> (enable) set snmp community read-write Administrators
SNMP read-write community string set to 'Administrators'.
Console> (enable) set snmp community read-write-all Root
SNMP read-write-all community string set to 'Root'.
Console> (enable) set snmp trap 172.16.10.10 read-write
SNMP trap receiver added.
Console> (enable) set snmp trap 172.16.10.20 read-write-all
SNMP trap receiver added.
Console> (enable) set snmp trap enable all
All SNMP traps enabled.
Console> (enable) show snmp
RMON:                          Disabled
Extended RMON:                 Extended RMON module is not present
Traps Enabled:
Port,Module,Chassis,Bridge,Repeater,Vtp,Auth,ippermit,Vmps,config,entity,stpx
Port Traps Enabled: 1/1-2,4/1-48,5/1
Community-Access     Community-String
----------------     --------------------
read-only            Everyone
read-write           Administrators
read-write-all       Root
Trap-Rec-Address                            Trap-Rec-Community
------------------------------------------  --------------------
172.16.10.10                                read-write
172.16.10.20                                read-write-all
Console> (enable)
```

(注)　SNMP コミュニティへのアクセスをディセーブルにするには、そのコミュニティのコミュニティ ストリングを空白にします（コミュニティ ストリングには値を入力しないでください）。

Release 7.5(1) の SNMPv1 および SNMPv2c 拡張機能

ここでは、Release 7.5(1) に追加された拡張機能について説明します。

複数の SNMP コミュニティ ストリングの設定

community-ext キーワードを使用すると、複数の SNMP コミュニティ ストリングを設定できます。**community-ext** キーワードを使用して定義したコミュニティ ストリングは、既存のコミュニティ ストリングの複製にはできません。**community-ext** キーワードを使用して新しいコミュニティ ストリングを追加すると、vacmAccessTable（ビューを指定した場合）、snmpCommunityTable、および vacmSecurityToGroup のテーブルに該当するエントリが作成されます。

CLI を使用して複数の SNMP コミュニティ ストリングを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	複数の SNMP コミュニティ ストリングを設定します。	**set snmp community-ext** *community_string* {**read-only** | **read-write** | **read-write-all**} [**view** *view_oid*] [**access** *access_number*]
ステップ 2	SNMP の設定を確認します。	**show snmp**

次に、追加 SNMP コミュニティ ストリングを設定する例を示します。

```
Console> (enable) set snmp community-ext public1 read-only

Community string public1 is created with access type as read-only
Console> (enable)
```

次に、コミュニティ ストリングをアクセス番号に制限する例を示します。

```
Console> (enable) set snmp community-ext private1 read-write access 2

Community string private1 is created with access type as read-write access number 2
Console> (enable)
```

次に、コミュニティ ストリングのアクセス番号を変更する例を示します。

```
Console> (enable) set snmp community-ext private1 read-write access 3

Community string private1 is updated with access type as read-write access
number 3
Console> (enable)
```

次に、SNMP 設定を表示する例を示します。

```
Console> (enable) show snmp

SNMP:Enabled
RMON:Disabled
Extended RMON Netflow Enabled :None.
Memory usage limit for new RMON entries:85 percent
Traps Enabled:None
Port Traps Enabled:None

Community-Access Community-String
---------------- --------------------
read-only        public
read-write       private
read-write-all   secret

Additional-                          Access-
Community-String     Access-Type     Number  View
-------------------- --------------- ------- ----------------------------------
public1              read-only
public2              read-only       1
private1             read-write      2       1.3.6
secret1              read-write-all  500     1.3.6.1.4.1.9.9

Trap-Rec-Address Trap-Rec-Community Trap-Rec-Port Trap-Rec-Owner Trap-Rec-Index
---------------- ------------------ ------------- -------------- --------------
Console> (enable)
```

SNMP コミュニティ ストリングの消去

コミュニティ ストリングは、**clear snmp community-ext** *community-string* コマンドを使用すると消去できます。このコマンドを使用してコミュニティ ストリングを消去すると、vacmAccessTable および vacmSecurityToGroup テーブルの対応するエントリも削除されます。

CLI を使用して SNMP コミュニティ ストリングを消去するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	SNMP コミュニティ ストリングを消去します。	**clear snmp community-ext** *community-string*
ステップ 2	SNMP の設定を確認します。	**show snmp**

次に、SNMP コミュニティ ストリングを消去する例を示します。

```
Console> (enable) clear snmp community-ext public1
Community string public1 has been removed
Console> (enable)
```

ホストのアクセス番号の指定

1 つまたは複数のホストに対応付けられたアクセス番号のリストを指定して、特定のコミュニティ ストリングを使用してシステムにアクセスできるホストを制限できます。各 IP アドレスをスペースで区切って、アクセス番号に対応付けられた複数の IP アドレスを指定できます。既存のアクセス番号が使用されている場合は、新しい IP アドレスはリストに追加されます。

CLI を使用してホストのアクセス番号を指定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ホストのアクセス番号を指定します。	**set snmp access-list** *access_number IP_address* [**ipmask** *maskaddr*]
ステップ 2	SNMP の設定を確認します。	**show snmp access-list**

次に、ホストのアクセス番号を指定する例を示します。

```
Console> (enable) set snmp access-list 1 172.20.60.100
Access number 1 has been created with new IP Address 172.20.60.100

Console> (enable) set snmp access-list 2 172.20.60.100 mask 255.0.0.0
Access number 2 has been created with new IP Address 172.20.60.100 mask 255.0.0.0

Console> (enable) set snmp access-list 2 172.20.60.7
Access number 2 has been updated with new IP Address 172.20.60.7

Console> (enable) set snmp access-list 2 172.20.60.7 mask 255.255.255.0
Access number 2 has been updated with existing IP Address 172.20.60.7 mask
255.255.255.0
Console> (enable)
```

次に、SNMP 設定を表示する例を示します。

```
Console> (enable) show snmp access-list
Access-Number   IP-Addresses/IP-Mask
-------------   ------------------------
1               172.20.60.100/255.0.0.0
                1.1.1.1/-
2               172.20.60.7/-
                2.2.2.2/-
3               2.2.2.2/155.0.0.0
4               1.1.1.1/2.1.2.4
                2.2.2.2/-
                2.2.2.5/-
Console> (enable)
```

アクセス番号に対応付けられた IP アドレスの消去

CLI を使用してアクセス番号に対応付けられた IP アドレスを消去するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	アクセス番号に対応付けられた IP アドレスを消去します。	**clear snmp access-list** *access_number IP_address* [[*IP_address*] ...]
ステップ 2	SNMP の設定を確認します。	**show snmp access-list**

次に、アクセス番号に対応付けられた IP アドレスを消去する例を示します。

```
Console> (enable) clear snmp access-list 101
All IP addresses associated with access-number 101 have been cleared.
Console> (enable)

Console> (enable) clear snmp access-list 2 172.20.60.8
Access number 2 no longer associated with 172.20.60.8
Console> (enable)
```

インターフェイス エイリアスの指定、表示、および消去

インターフェイス エイリアスの指定、表示、および消去ができます。エイリアスには最大 64 文字まで使用できます。

（注） バイナリ コンフィギュレーション モードでは、**set snmp ifalias** コマンドを使用できません。このコマンドを入力する場合、または ifalias が NVRAM（不揮発性 RAM）に保存されてない場合は、テキスト ファイル コンフィギュレーション モードを使用する必要があります。

インターフェイス エイリアスの指定、表示、および消去を行うには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	インターフェイス エイリアスを指定します。	**set snmp ifalias** {*ifIndex*} [*ifAlias*]
ステップ 2	インターフェイス エイリアスを表示します。	**show snmp ifalias** [*ifIndex*]
ステップ 3	インターフェイス エイリアスを消去します。	**clear snmp ifalias** {*ifIndex*} **all**

次に、インターフェイス エイリアスを指定、表示、および消去する例を示します。

```
Console> (enable) set snmp ifalias 1 Inband port

ifIndex 1 alias set
Console> (enable)

Console> (enable) show snmp ifalias 1
ifIndex    ifName               ifAlias
---------- -------------------- --------------------------------
1          sc0                  Inband port
Console> (enable)

Console> (enable) clear snmp ifalias all
Console> (enable)
```

スイッチ上での SNMPv3 の設定

ここでは、SNMPv3 の基本設定について説明します。Catalyst 6500 シリーズ スイッチによってサポートされる SNMP コマンドの詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

SNMPv3 のデフォルト設定

ここに記載されている各コマンドの SNMP デフォルト設定については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

NMS での SNMPv3 の設定

NMS での SNMP の設定手順については、NMS のマニュアルを参照してください（「CiscoWorks2000 の使用方法」[p.44-7] を参照）。

スイッチは、RMON2 トラップ宛先テーブルに指定された 20 までのトラップ レシーバーをサポートしています。RMON2 トラップ宛先テーブルは、NMS を使用して設定します。

CLI での SNMPv3 の設定

CLI を使用して SNMPv3 を設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ローカル SNMP エンジンに対して SNMP サーバエンジン ID 名を設定します。	**set snmp engineid** *engineid*
ステップ 2	MIB ビューを設定します。	**set snmp view** [**-hex**] {*viewname*} {*subtree*} [*mask*] [***included*** | ***excluded***] [***volatile*** | ***nonvolatile***]
ステップ 3	各種のセキュリティ レベルで 1 つの特定のセキュリティ モデルを持つグループのアクセス権を設定します。	***set snmp access*** [***-hex***] {*groupname*} {***security-model v3***} {***noauthentication*** | ***authentication*** | ***privacy***} [**read** [***-hex***] {*readview*}] [***write*** [***-hex***] {*writeview*}] [***notify*** [***-hex***] {*notifyview*}] [***context*** [***-hex***] {*contextname*} [***exact*** | ***prefix***]] [***volatile*** | ***nonvolatile***]
ステップ 4	通知用のターゲット アドレスを指定します。	***set snmp notify*** [***-hex***] {**notifyname**} ***tag*** [***-hex***] {*notifytag*} [***trap*** | ***inform***] [***volatile*** | ***nonvolatile***]
ステップ 5	ターゲット アドレス テーブルに snmpTargetAddrEntry を設定します。	***set snmp targetaddr*** [***-hex***] {*addrname*} ***param*** [***-hex***] {*paramsname*} {*ipaddr*} [***udpport*** {*port*}] [***timeout*** {**value**}] [***retries*** {**value**}] [***volatile*** | ***nonvolatile***] [***taglist*** {[***-hex***] *tag*} [[***-hex***] *tag*]]
ステップ 6	ターゲットへのメッセージ生成に使用する SNMP パラメータを設定します。	***set snmp targetparams*** [***-hex***] {*paramsname*} ***user*** [***-hex***] {*username*} {***security-model v3***} {***message-processing v3***} {***noauthentication*** | ***authentication*** | ***privacy***} [***volatile*** | ***nonvolatile***]
ステップ 7	新しいユーザを設定します。	***set snmp user*** [***-hex***] {*username*} [**remote** {*engineid*}] [{***authentication*** [***md5*** | *sha*] {*authpassword*}] [***privacy*** {*privpassword*}] [***volatile*** | ***nonvolatile***]
ステップ 8	指定されたセキュリティ モデルでユーザをグループに関連付けます。	***set snmp group*** [***-hex***] {*groupname*} ***user*** [***-hex***] {*username*} {***security-model v1*** | ***v2*** | ***v3***} [***volatile*** | ***nonvolatile***]

	作業	コマンド
ステップ 9	システムのデフォルト部分用のコミュニティ テーブルを設定します。これは、SNMP の旧バージョンのコミュニティ ストリングを SNMPv3 にマッピングします。	***set snmp community*** {***read-only*** | ***read-write*** | ***read-write-all***} [*community_string*]
ステップ 10	各種コミュニティ ストリングとフル アクセス権を備えたセキュリティ モデルとの間のマッピング用のコミュニティ テーブルを設定します。	***set snmp community index*** {*index_name*} ***name*** [*community_string*] ***security*** {*security_name*} ***context*** {*context_name*} ***transporttag*** {*tag_value*} [***volatile*** | ***nonvolatile***]
ステップ 11	SNMP の設定を確認します。	***show snmp***

次に、interfacesMibView に MIB ビューを設定する例を示します。

```
Console> (enable) set snmp view interfacesMibView 1.3.6.1.2.1.2 included
Snmp view name was set to interfacesMibView with subtree 1.3.6.1.2.1.2 included,
nonvolatile.
```

次に、guestgroup というグループに SNMPv3 認証読み取りモードに対するアクセス権を設定する例を示します。

```
Console> (enable) set snmp access guestgroup security-model v3 authentication read
interfacesMibView
Snmp access group was set to guestgroup version v3 level authentication,
readview interfacesMibView, context match:exact, nonvolatile.
```

次に、ターゲット アドレスを指定する例を示します。

```
Console> (enable) set snmp notify notifytable1 tag routers trap
Snmp notify name was set to notifytable1 with tag routers notifyType trap, and
storageType nonvolatile.
```

次に、ターゲット アドレス テーブルに snmpTargetAddrEntry を設定する例を示します。

```
Console> (enable) set snmp targetaddr router_1 param p1 172.20.21.1
Snmp targetaddr name was set to router_1 with param p1
ipAddr 172.20.21.1, udpport 162, timeout 1500, retries 3, storageType nonvolatile.

Console> (enable) set snmp targetaddr router_2 param p2 172.20.30.1
Snmp targetaddr name was set to router_2 with param p2
ipAddr 172.20.30.1, udpport 162, timeout 1500, retries 3, storageType nonvolatile.
```

次に、SNMP ターゲット パラメータの設定例を示します。

```
Console> (enable) set snmp targetparams p1 user guestuser1 security-model v3
message-processing v3 authentication
Snmp target params was set to p1 v3 authentication, message-processing v3,
user guestuser1 nonvolatile.

Console> (enable) set snmp targetparams p2 user guestuser2 security-model v3
message-processing v3 privacy
Snmp target params was set to p2 v3 privacy, message-processing v3,
user guestuser2 nonvolatile.
```

次に、ユーザとして guestuser1 および guestuser2 を設定する例を示します。

```
Console> (enable) set snmp user guestuser1 authentication md5 guestuser1password
privacy privacypasswd1
Snmp user was set to guestuser1 authProt md5 authPasswd guestuser1password privProt
des privPasswd
privacypasswd1 with engineid 00:00:00:09:00:10:7b:f2:82:00:00:00 nonvolatile.

Console> (enable) set snmp user guestuser2 authentication sha guestuser2password
Snmp user was set to guestuser2 authProt sha authPasswd guestuser2password privProt
no-priv with engineid
00:00:00:09:00:10:7b:f2:82:00:00:00 nonvolatile.
```

次に、グループ guestgroup および mygroup のメンバーとして guestuser1 および guestuser2 を設定する例を示します。

```
Console> (enable) set snmp group guestgroup user guestuser1 security-model v3
Snmp group was set to guestgroup user guestuser1 and version v3, nonvolatile.

Console> (enable) set snmp group mygroup user guestuser1 security-model v3
Snmp group was set to mygroup user guestuser1 and version v3, nonvolatile.

Console> (enable) set snmp group mygroup user guestuser2 security-model v3
Snmp group was set to mygroup user guestuser2 and version v3, nonvolatile.
```

次に、ワークステーションで guestuser1 に対する SNMPv3 セットアップを確認する例を示します。

```
workstation% getnext -v3 10.6.4.201 guestuser1 ifDescr.0
Enter Authentication password :guestuser1password
Enter Privacy password        :privacypasswd1
ifDescr.1 = sc0
```

次に、ワークステーションで snmpEngineID MIB の guestgroup に対する SNMPv3 セットアップを確認する例を示します。

```
workstation% getnext -v3 10.6.4.201 guestuser1 snmpEngineID
Enter Authentication password :guestuser1pasword
Enter Privacy password        :privacypasswd1
snmpEngineID = END_OF_MIB_VIEW_EXCEPTION
```

次に、ワークステーションで公開アクセスに対する SNMPv2c セットアップを確認する例を示します。

```
workstation% getnext -v2c 10.6.4.201 public snmpEngineID
snmpEngineID.0 =
00 00  00 09   00 10  7b f2    82 00  00 00
```

次に、guestgroup のアクセス権を引き上げて、snmpEngineMibView の読み取り権限を設定する例を示します。

```
Console> (enable) set snmp view snmpEngineMibView 1.3.6.1.6.3.10.2.1 included
Snmp view name was set to snmpEngineMibView with subtree 1.3.6.1.6.3.10.2.1 included,
nonvolatile

Console> (enable) set snmp access guestgroup security-model v3 authentication read
snmpEngineMibView
Snmp access group was set to guestgroup version v3 level authentication,
readview snmpEngineMibView, nonvolatile.
```

次に、ワークステーションで guestuser1 に対する SNMPv3 アクセス権を確認する例を示します。

```
workstation% getnext -v3 10.6.4.201 guestuser1 snmpEngineID
Enter Authentication password :guestuser1password
Enter Privacy password        :privacypasswd1
snmpEngineID.0 =
00 00  00 09   00 10  7b f2    82 00  00 00
```

次に、guestgroup のアクセス権を削除する例を示します。

```
Console> (enable) clear snmp acc guestgroup security-model v3 authentication
Cleared snmp access guestgroup version v3 level authentication.
```

次に、ワークステーションで guestuser1 のアクセス権が削除されたことを確認する例を示します。

```
workstation% getnext -v3 10.6.4.201 guestuser1 ifDescr.1
Enter Authentication password :guestuser1password
Enter Privacy password        :privacypasswd1
Error code set in packet - AUTHORIZATION_ERROR:1.
```

次に、ワークステーションで guestuser2 のアクセス権を確認する例を示します。

```
workstation% getnext -v3 10.6.4.201 guestuser2 ifDescr.1
Enter Authentication password :guestuser2password
Enter Privacy password        :privacypasswd2
REPORT received, cannot recover:
usmStatsUnsupportedSecLevels.0 = 1
```

CHAPTER 45

RMON の設定

この章では、Catalyst 6500 シリーズ スイッチ上で Remote Monitoring（RMON）を設定する方法について説明します。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

この章で説明する内容は、次のとおりです。

RMON の機能

RMON は、さまざまなネットワーク エージェントおよびコンソール システムでネットワーク モニタ データを交換することができる Internet Engineering Task Force（IETF）標準モニタ仕様です。スーパバイザ エンジン ソフトウェアには、次の RMON 仕様コンポーネントのサポートが組み込まれています（詳細については「サポートされる RMON および RMON2 MIB オブジェクト」[p.45-4] を参照）。

- RFC 1757 に定義されている RMON グループ
  - イーサネット、ファスト イーサネット、Fast EtherChannel、およびギガビット イーサネット スイッチ ポートの統計情報（RMON グループ 1、各ポートにつきスーパバイザ エンジンの RAM を 140 バイト使用）
  - イーサネット、ファスト イーサネット、Fast EtherChannel、およびギガビット イーサネット スイッチ ポートのヒストリ（RMON グループ 2、最初の 50 バケットにスーパバイザ エンジンの RAM を 3 KB 使用、以後はバケットが 1 つ追加されるたびに 56 バイト使用）
  - アラーム（RMON グループ 3、設定した各アラームにつきスーパバイザ エンジンの RAM を 1.3 KB 使用）
  - イベント（RMON グループ 9、設定した各イベントにつきスーパバイザ エンジンの RAM を 1.3 KB 使用）
- RFC 2021 に定義されている RMON2 グループ
  - UsrHistory（RMON2 グループ 18）
  - ProbeConfig（RMON2 グループ 19）

組み込み RMON エージェントにより、スイッチで専用モニタリング プローブまたはネットワーク アナライザを使用しなくても、レイヤ 2 ですべてのポートのネットワーク トラフィックを同時にモニタできます。

スイッチ上での RMON のイネーブル化

（注）　RMON は、デフォルトではディセーブルに設定されています。

RMON をイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチ上で RMON をイネーブルにします。	**set snmp rmon enable**
ステップ 2	RMON がイネーブルに設定されたことを確認します。	**show snmp**

次に、スイッチ上で RMON をイネーブルにし、RMON がイネーブルに設定されたことを確認する例を示します。

```
Console> (enable) set snmp rmon enable
SNMP RMON support enabled.
Console> (enable) show snmp
RMON:                          Enabled
Extended RMON:                 Extended RMON module is not present
Traps Enabled:
Port,Module,Chassis,Bridge,Repeater,Vtp,Auth,ippermit,Vmps,config,entity,stpx
Port Traps Enabled: 1/1-2,4/1-48,5/1
Community-Access     Community-String
----------------     --------------------
read-only            Everyone
read-write           Administrators
read-write-all       Root
Trap-Rec-Address                            Trap-Rec-Community
------------------------------------------  --------------------
172.16.10.10                                read-write
172.16.10.20                                read-write-all
Console> (enable)
```

RMON データの表示

RMON データにアクセスできるのは、RFC 1757 および RFC 2021 をサポートしている Network Management System（NMS; ネットワーク管理システム）からだけです（「CiscoWorks2000 の使用方法」[p.44-7] を参照）。スイッチの CLI（コマンドライン インターフェイス）から RMON データにアクセスすることはできませんが、CLI の **show** コマンドにより同様の情報が得られます。

サポートされる RMON および RMON2 MIB オブジェクト

表 45-1 に、スーパバイザ エンジン ソフトウェアがサポートしている RMON および RMON2 MIB オブジェクトを示します。

表 45-1　スーパバイザ エンジンの RMON および RMON2 サポート

Object Identifier（OID; オブジェクト識別子）および説明	送信元
...mib-2（1）.rmon（16）.statistics（1）.etherStatsTable（1）	RFC 1757（RMON-MIB）
パケット、オクテット、ブロードキャスト、エラーなどのカウンタ	
...mib-2(1).rmon(16).history(2).historyControlTable(1) ...mib-2(1).rmon(16).history(2).etherHistoryTable(2)	RFC 1757 (RMON-MIB) RFC 1757 (RMON-MIB)
あとから検索できるように、統計グループ カウンタを定期的に収集して保存します。	
...mib-2（1）.rmon（16）.alarm（3）	RFC 1757（RMON-MIB）
ネットワーク管理上、重要な RMON 変数に設定できるスレッシュホールド	
...mib-2（1）.rmon（16）.event（9）	RFC 1757（RMON-MIB）
アラーム グループのスレッシュホールドを超過したときに SNMP（簡易ネットワーク管理プロトコル）トラップを生成し、イベントをログに保存します。	
...mib-2（1）.rmon（16）.usrHistory（18）	RFC 2021（RMON2-MIB）
RMON1 リンク レイヤ統計情報のヒストリ拡張情報で、RMON、RMON2、MIB-I、または MIB-II 統計情報が含まれます。	
...mib-2（1）.rmon（16）.probeConfig（19）	RFC 2021（RMON2-MIB）
エージェント機能および設定のリストを表示します。	

CHAPTER 46

SPAN および RSPAN の設定

この章では、Catalyst 6500 シリーズ スイッチ上で Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）および Remote SPAN（RSPAN）を設定する方法について説明します。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

この章で説明する内容は、次のとおりです。

(注) Network Management Station（NMS; ネットワーク管理ステーション）で SPAN または RSPAN を設定する方法については、NMS のマニュアルを参照してください（「CiscoWorks2000 の使用方法」[p.44-7] を参照）。

SPAN および RSPAN の機能

ここでは、SPAN および RSPAN の設定に関連した概念および用語について説明します。

SPAN セッション

SPAN セッションとは、複数の宛先ポートと 1 組の送信元ポートとのアソシエーションです。モニタ対象のネットワーク トラフィックを指定するパラメータによって設定されます。スイッチド ネットワーク内で複数の SPAN セッションを設定できます。SPAN セッションは、スイッチの通常の動作を妨げません。SPAN セッションのイネーブル化またはディセーブル化は、CLI（コマンド ライン インターフェイス）または SNMP（簡易ネットワーク管理プロトコル）コマンドで設定できます。イネーブルの場合、SPAN セッションはさまざまなイベントまたはアクションに基づいて、アクティブになったり非アクティブになったりします。その状況は Syslog メッセージによって示されます。**show span** および **show rspan** コマンドの [Status] フィールドに、SPAN または RSPAN セッションの動作状態が示されます。

SPAN または RSPAN 宛先セッションは、システムの電源投入後、宛先ポートが動作可能になるまで非アクティブのままです。RSPAN 送信元セッションは、いずれかの送信元ポートが動作可能になるか、または RSPAN VLAN（仮想 LAN）がアクティブになるまで、非アクティブのままです。

宛先ポート

宛先ポート（別名 *モニタ ポート*）は、SPAN が解析のためにパケットを送信するスイッチ ポートです。アクティブ宛先ポートになったポートは、SPAN セッションに必要なトラフィック以外は転送しません。デフォルトの設定では、アクティブ宛先ポートは、特にそのポートをイネーブルにしないかぎり、（ネットワークからスイッチング バスまでの）着信トラフィックを禁止します。宛先ポートに対して着信トラフィックが許可される場合、宛先ポートのネイティブ VLAN 内でスイッチングされます。SPAN セッションがアクティブなとき、宛先ポートはスパニングツリーに加わりません。ネットワーク トポロジーにループが発生しないようにする方法については、「CLI での SPAN の設定」（p.46-8）の注意を参照してください。

複数の宛先ポートを各ローカル SPAN セッションに指定できますが、単一の宛先ポートを複数の SPAN セッションの宛先ポートにすることができません。宛先ポートとして設定されたスイッチ ポートは、送信元ポートとして設定することはできません。EtherChannel ポートは、SPAN 宛先ポートにできません。

SPAN セッションの設定時に SPAN 宛先ポートのトランキング モードを [on] または [nonegotiate] にした場合、宛先ポートが転送する SPAN パケットは、トランク タイプで指定されたカプセル化が行われます。ただし、この宛先ポートはトランキングを中止します。**show trunk** コマンドに、SPAN セッションを設定する前のポートのトランキング ステータスが反映されます。

送信元ポート

送信元ポートは、ネットワーク トラフィックを解析するためにモニタされるスイッチ ポートです。送信元ポートを通過するトラフィックは、入力、出力、またはその両方として分類できます。すべての送信元ポートに適用可能なトラフィック タイプ（入力、出力、または両方）をユーザが指定することにより、1 つの SPAN セッションで 1 つまたは複数の送信元ポートをモニタできます。

送信元ポートは任意の VLAN で設定できます。VLAN を送信元ポートとして設定できます（*src_vlans*）。その場合、指定した VLAN 内のすべてのポートが、SPAN セッションの送信元ポートになります。

送信元ポートは管理用（*Admin Source*）、動作用（*Oper Source*）、またはその両方です。管理用送信元ポートは、SPAN セッションの設定時に指定した送信元ポートまたは送信元 VLAN です。動作用送信元ポートは、宛先ポートがモニタする送信元ポートです。たとえば、送信元 VLAN を管理用送信元として使用する場合、動作用送信元は指定されたすべての VLAN のすべてのポートです。

動作用送信元は、常にアクティブ ポートです。ポートがスパニングツリーに含まれていない場合、動作用送信元ではありません。EtherChannel 送信元内のすべての物理ポートは、論理ポートがスパニングツリーに含まれている場合、動作用送信元に含まれます。

管理用送信元 VLAN に属している宛先ポートは、動作用送信元から除外されます。

複数のアクティブ SPAN セッションで 1 つのポートを送信元ポートとして設定できますが、アクティブ送信元ポートを SPAN セッションの宛先ポートとして設定することはできません。

SPAN セッションが非アクティブの場合、セッションがアクティブになるまで、[oper source] フィールドはアップデートされません。

トランク ポートは送信元ポートとして設定できます。また、非トランク送信元ポートと混在させることができます。ただし、宛先ポートが転送するパケットのカプセル化は、SPAN セッションの設定時に宛先ポートのトランク設定値によって決定されます。

入力 SPAN

入力 SPAN は、送信元ポートが受信したネットワーク トラフィックを、宛先ポートで解析するためにコピーします。

出力 SPAN

出力 SPAN は、送信元ポートが送信したネットワーク トラフィックを、宛先ポートで解析するためにコピーします。

VSPAN

VLAN-based SPAN（VSPAN）は、1 つまたは複数の VLAN のネットワーク トラフィックを解析します。VSPAN は入力 SPAN、出力 SPAN、またはその両方として設定できます。送信元 VLAN 内のすべてのポートが VSPAN セッションの動作用送信元ポートになります。管理用送信元 VLAN に属している宛先ポートは、動作用送信元から除外されます。管理用送信元 VLAN に対してポートの追加または削除を行うと、それに応じて動作用送信元が変更されます。

VSPAN セッションでは、次の注意事項に従ってください。

- トランク ポートは VSPAN セッションの送信元ポートとして組み込まれますが、管理用送信元リストに指定されていて、かつトランクに対してアクティブな VLAN だけがモニタ対象になります。

- 入力と出力の両方の SPAN が設定された VSPAN セッションの場合、システムは使用しているスーパバイザ エンジンのタイプに基づいて、次のように動作します。
  - WS-X6K-SUP1A-PFC、WS-X6K-SUP1A-MSFC、WS-X6K-S1A-MSFC2、WS-X6K-S2-PFC2、WS-X6K-S1A-MSFC2、WS-SUP720、WS-SUP32-GE-3B ― 2 つのパケットが同じ VLAN でスイッチングされる場合、それらは SPAN 宛先ポートにより転送されます。
  - WS-X6K-SUP1-2GE、WS-X6K-SUP1A-2GE ― 1 つのパケットだけが SPAN 宛先ポートによって転送されます。
- 帯域内ポートは、VSPAN セッションの動作用送信元として組み込まれません。
- VLAN が消去されると、VSPAN セッションの送信元リストから削除されます。
- 管理用送信元 VLAN リストが空の場合、VSPAN セッションは使用できません。
- 非アクティブの VLAN を VSPAN の設定に使用することはできません。
- 送信元 VLAN のいずれかが RSPAN VLAN になると、VSPAN セッションが非アクティブになります。

トランク VLAN フィルタリング

トランク VLAN フィルタリングとは、トランク送信元ポート上で選択された 1 組の VLAN 上で、ネットワーク トラフィックを解析することです。トランク VLAN フィルタリングを、選択した VLAN のどれかに含まれる他の送信元ポートと組み合わせることができます。また、RSPAN にトランク VLAN フィルタリングを使用することもできます。SPAN は、トラフィック タイプ（入力、出力、またはその両方）に基づいて、選択された VLAN 内のネットワーク トラフィックのコピーを宛先ポートに送信します。

トランク VLAN フィルタリングは、トランク送信元ポートだけで使用します。トランク VLAN フィルタリングを、選択されたフィルタ VLAN のリスト外の VLAN に所属する他の送信元ポートと組み合わせた場合、SPAN には、動作用送信元内の選択された VLAN の 1 つまたは複数に所属するポートだけが含まれます。

VLAN が消去されると、VLAN フィルタ リストから削除されます。VLAN フィルタ リストが空の場合、SPAN セッションは使用できません。

トランク VLAN フィルタリングは、VSPAN セッションには適用できません。

SPAN トラフィック

マルチキャストおよび Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）パケットを含むすべてのネットワーク トラフィックは、SPAN を使用してモニタできます（RSPAN は BPDU パケットまたは Cisco Discovery Protocol [CDP]、Dynamic Trunking Protocol［DTP; ダイナミック トランキング プロトコル］、および VLAN Trunking Protocol［VTP;VLAN トランキング プロトコル］などのレイヤ 2 プロトコル パケットのモニタをサポートしていません）。マルチキャスト パケットのモニタは、イネーブルがデフォルトの設定です。

SPAN の設定によっては、同じ送信元パケットに対して複数のコピーが SPAN 宛先ポートに送信されます。たとえば、双方向（入力と出力の両方）SPAN セッションが送信元 a1 と a2 から宛先ポート d1 まで設定されているとします。パケットが a1 からスイッチに入り、a2 にスイッチングされた場合、着信と発信の両方のパケットが宛先ポート d1 に送信されます。パケットは両方とも同じです（レイヤ 3 のリライトが行われた場合にはパケットは異なります）。複数のスイッチに送信元が分散されている RSPAN セッションの場合も、宛先ポートが同じパケットのコピーを複数転送する場合があります。

SPAN/RSPAN のセッション限度

Catalyst 6500 シリーズ スイッチでは、最大 30 の SPAN セッションを設定（および NVRAM [不揮発性 RAM] に保存）できます。使用できる SPAN/RSPAN セッションの組み合わせについては、表 46-1 を参照してください。各セッションの送信元として、複数のポートまたは VLAN を設定できます。

表 46-1　SPAN/RSPAN のセッション限度

SPAN/RSPAN セッション	Catalyst 6500 シリーズ スイッチ[1]
rx または **both** SPAN セッション	2
tx SPAN セッション	4
tx、**rx**、または **both** RSPAN 送信元セッション	1[2]
RSPAN 宛先	24
SPAN セッションの合計	30[3]

1. RSPAN 送信元セッションを設定すると、**rx** または **both** SPAN セッションの限度数が 1 つ少なくなります。
2. Supervisor Engine 720 では、2 つの RSPAN 送信元セッションをサポートします。
3. 2 **rx** または **both** SPAN セッション + 4 **tx** SPAN セッション + 24 RSPAN 宛先セッション = 合計 30 SPAN セッション

スイッチ上での SPAN の設定

ここでは、SPAN を設定する手順について説明します。

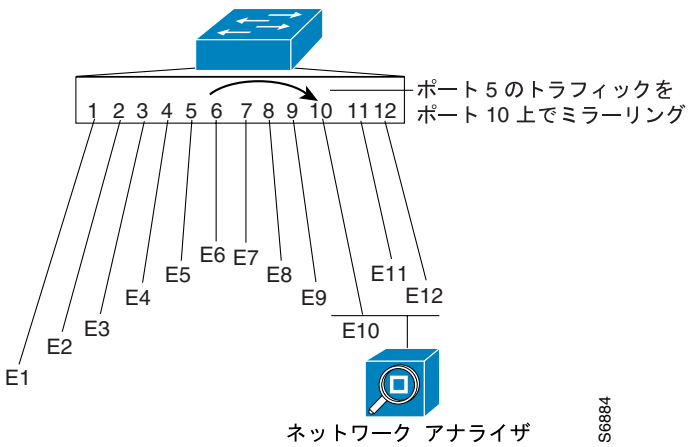
SPAN のハードウェア要件

すべての Catalyst 6500 シリーズ スイッチのスーパバイザ エンジンが SPAN をサポートしています。

SPAN の機能

SPAN は、SwitchProbe 装置または他の Remote Monitoring（RMON）プローブなどのネットワーク アナライザによる解析のためにネットワーク トラフィックを選択します。SPAN は、VLAN 上の 1 つあるいは複数の送信元ポートから、1 つあるいは複数の VLAN から、または sc0 コンソール インターフェイスから、宛先ポートへのトラフィック解析のためにミラーリングします（図 46-1 を参照）。図 46-1 では、イーサネット ポート 5（送信元ポート）のすべてのトラフィックがイーサネット ポート 10 にミラーリングされています。イーサネット ポート 10 のネットワーク アナライザは、イーサネット ポート 5 に物理的に接続していなくても、このポートからすべてのネットワーク トラフィックを受信します。

図 46-1　SPAN の設定例



SPAN の設定では、送信元ポートと宛先ポートが同じスイッチ上になければなりません。

SPAN は、送信元ポート上のネットワーク トラフィックのスイッチングに影響を与えません。送信元ポートが送受信したパケットのコピーが宛先ポートに送信されます。

SPAN 設定時の注意事項

ここでは、SPAN 設定時の注意事項について説明します。

- ポートのモニタにはネットワーク アナライザを使用します。
- SPAN 送信元ポートについて、Asynchronous Transfer Mode（ATM; 非同期転送モード）ポートで SPAN はサポートされません。SPAN はイーサネット 10/100/1000 Mbps ポートおよび 10 Gbps ポートで動作します。
- SPAN がイネーブルの場合、SPAN は入力済みの設定を使用します。コンフィギュレーション コマンドを入力していない場合は、デフォルトのパラメータが使用されます。
- 複数の SPAN 送信元ポートを指定する場合、ポートがそれぞれ異なる VLAN に所属していてもかまいません。
- 「SPAN/RSPAN のセッション限度」（p.46-5）を参照してください。
- RSPAN セッションは、SPAN/RSPAN の限度内であれば、SPAN セッションと共存させることができます。「SPAN/RSPAN のセッション限度」（p.46-5）を参照してください。
- オプションの **inpkts** キーワードはディセーブルがデフォルトの設定です。**inpkts** キーワードとオプションの **enable** キーワードを組み合わせて指定すると、SPAN 宛先ポートで通常の着信トラフィックを受信できるようになります。SPAN 宛先ポートで通常の着信トラフィックを受信しないようにする場合は、オプションの **disable** キーワードを入力します。
- オプションの **inpkts** キーワードをイネーブルにすると、宛先ポートが Spanning-Tree Protocol（STP; スパニングツリー プロトコル）をサポートしないので、これが原因でループが発生する可能性があることを通知する警告メッセージが表示されます。
- ラーニングはイネーブルがデフォルトの設定です。**inpkts** キーワードとオプションの **learning** キーワードを組み合わせて指定すると、特定のポートでラーニングがイネーブルまたはディセーブルになります。
- SPAN 送信元ポートとして、Multilayer Switch Module（MSM）を指定できます。ただし、MSM ポートを SPAN 宛先ポートとして指定することはできません。
- 複数の SPAN セッションを設定する場合、個々の SPAN セッションのインデックスとして、宛先モジュール番号 / ポート番号を明示する必要があります。
- **set span** コマンドで **create** キーワードを指定せず、かつセッションが 1 つだけの場合、そのセッションが上書きされます。対応する宛先ポートが存在している場合、（**create** キーワードの指定にかかわらず）そのセッションが上書きされます。**create** キーワードを指定し、対応する宛先ポートがない場合、セッションが作成されます。
- SPAN 送信元ポート（1 つまたは複数）上の VLAN がスパニングツリーによってブロックされた場合、実際には送信元ポート（1 つまたは複数）から送信されていない余分なパケットが、宛先ポートに送信されたように見えることがあります。余分なパケットはスイッチ ファブリックを通じて送信元ポートに送信され、送信元ポートでスパニングツリーによってブロックされます。

CLI での SPAN の設定

SPAN を設定するには、送信元、宛先ポート、宛先ポートにミラーリングする送信元をトラフィックが通過する方向、さらに宛先ポートでパケットを受信できるかどうかを指定します。

SPAN ポートを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	SPAN の送信元ポートと宛先ポートを設定します。	**set span** {*src_mod/src_ports* | *src_vlans* | **sc0**} {*dest_mod/dest_port*} [**rx** | **tx** | **both**] [**session** *session_number*] [**inpkts** {**enable** | **disable**}] [**learning** {**enable** | **disable**}] [**multicast** {**enable** | **disable**}] [**filter** *vlans...*] [**create**]
ステップ 2	SPAN の設定を確認します。	**show span**

注意

SPAN 宛先ポートを他の装置に接続し、（**inpkts enable** キーワードを使用して）着信パケットの受信をイネーブルにすると、SPAN 宛先ポートは、SPAN 宛先ポートが設定されたすべての VLAN のトラフィックを受信します。ただし、SPAN 宛先ポートは、その VLAN のスパニングツリーに*参加しません*。**inpkts** キーワードを使用して、SPAN 宛先ポートでネットワーク ループが発生しないようにする場合、または SPAN 宛先ポートを未使用の VLAN に割り当てる場合は、注意してください。

次に、ポート 1/1（SPAN 送信元）の送信および受信トラフィックの両方をポート 2/1（SPAN 宛先）にミラーリングする SPAN の設定例を示します。

```
Console> (enable) set span 1/1 2/1

Destination     : Port 2/1
Admin Source    : Port 1/1
Oper Source     : Port 1/1
Direction       : transmit/receive
Incoming Packets: disabled
Learning        : enabled
Multicast       : enabled
Filter          : -
```

次に、VLAN 522 を SPAN 送信元、ポート 2/1 を SPAN 宛先に設定する例を示します。

```
Console> (enable) set span 522 2/1

Destination     : Port 2/1
Admin Source    : VLAN 522
Oper Source     : Port 3/1-2
Direction       : transmit/receive
Incoming Packets: disabled
Learning        : enabled
Multicast       : enabled
Filter          : -
Console> (enable)
```

次に、VLAN 522 を SPAN 送信元、ポート 2/12 を SPAN 宛先に設定する例を示します。送信トラフィックだけをモニタします。SPAN 宛先ポートでは、正常な着信パケットを受信します。

```
Console> (enable) set span 522 2/12 tx inpkts enable

Destination     : Port 2/12
Admin Source    : VLAN 522
Oper Source     : Port 2/1-2
Direction       : transmit
Incoming Packets: enabled
Learning        : enabled
Multicast       : enabled
Filter          : -
Console> (enable)
```

次に、ポート 3/2 を SPAN 送信元、ポート 2/2 を SPAN 宛先に設定する例を示します。

```
Console> (enable) set span 3/2 2/2 tx create

Destination     : Port 2/1
Admin Source    : port 3/1
Oper Source     : Port 3/1
Direction       : transmit/receive
Incoming Packets: disabled

Destination     : Port 2/2
Admin Source    : port 3/2
Oper Source     : Port 3/2
Direction       : transmit
Incoming Packets: disabled
Learning        : enabled
Multicast       : enabled
Filter          : -
Console> (enable)
```

SPAN をディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
スイッチ上で SPAN をディセーブルにします。	**set span disable** [*dest_mod*/*dest_port* | *all*]

次に、スイッチ上で SPAN をディセーブルにする例を示します。

```
Console> (enable) set span disable 2/1
This command will disable your span session.
Do you want to continue (y/n) [n]?y
Disabled port 2/1 to monitor transmit traffic of VLAN 522
Console> (enable)
```

スイッチ上での RSPAN の設定

ここでは、RSPAN を設定する手順について説明します。

RSPAN のハードウェア要件

RSPAN スーパバイザ エンジンの要件は、次のとおりです。

- 送信元スイッチの場合 ― 次のいずれかを搭載した Catalyst 6500 シリーズ スイッチ
  - ― Supervisor Engine 1A および Policy Feature Card（PFC; ポリシー フィーチャ カード）：WS-X6K-SUP1A-PFC
  - ― Supervisor Engine 1A、PFC、および Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）：WS-X6K-SUP1A-MSFC
  - ― Supervisor Engine 1A、PFC、および MSFC2：WS-X6K-S1A-MSFC2
  - ― Supervisor Engine 2 および PFC2：WS-X6K-S2-PFC2
  - ― Supervisor Engine 1A、PFC、および MSFC2：WS-X6K-S1A-MSFC2
  - ― Supervisor Engine 720、およびオンボード コンポーネントである Policy Feature Card 3A（PFC3A; ポリシー フィーチャ カード 3A）、PFC3B、または PFC3BXL、Multilayer Switch Feature Card 3（MSFC3; マルチレイヤ スイッチ フィーチャ カード 3）、720 Gbps 統合スイッチ ファブリック：WS-SUP720
  - ― PFC3B/PFC3BXL、MSFC2A、および Supervisor Engine 32：WS-SUP32-GE-3B
- 宛先または中間スイッチの場合 ― RSPAN VLAN をサポートする任意のシスコ製スイッチ

RSPAN トラフィックのエンドツーエンド パスに、他社製のスイッチまたは他のシスコ製スイッチを配置することはできません。

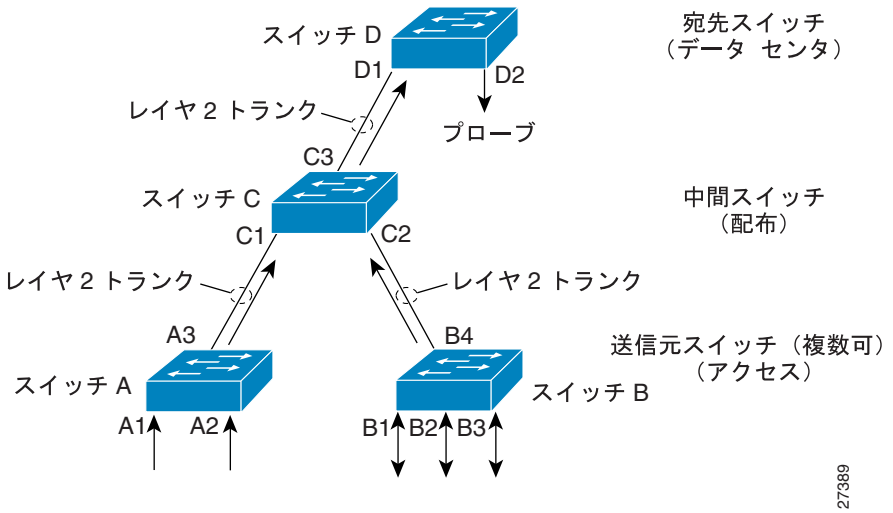
RSPAN の機能

（注）　SPAN と RSPAN の両方の設定に関連する概念と用語については、「SPAN および RSPAN の機能」（p.46-2）を参照してください。

RSPAN は、SPAN のすべての機能（「SPAN の機能」[p.46-6] を参照）に加えて、複数のスイッチに分散された送信元ポートおよび宛先ポートに対するサポートを備えています。これにより、ネットワーク上の複数のスイッチをリモート モニタできます（図 46-2 を参照）。

各 RSPAN セッションのトラフィックは、ユーザが指定した RSPAN VLAN 上で伝送されます。この RSPAN VLAN は、参加しているすべてのスイッチで RSPAN セッション専用です。送信元は RSPAN VLAN に含めることができないので、送信元からの SPAN トラフィックは RSPAN VLAN にスイッチングされてから、RSPAN VLAN 内で設定された宛先ポートに転送されます。RSPAN セッションにおける送信元のトラフィック タイプ（入力、出力、またはその両方）は、送信元スイッチごとに異なっていてかまいませんが、1 つの RSPAN セッションでは、各送信元スイッチのすべての送信元で同じです。RSPAN トラフィックを伝送するために選択したポート以外は、RSPAN VLAN 内でポートを設定しないでください。RSPAN VLAN では、ラーニングはディセーブルです。

図 46-2　RSPAN の設定例



RSPAN 設定時の注意事項

ここでは、RSPAN 設定時の注意事項について説明します。

ヒント　RSPAN VLAN には特殊なプロパティがあるので、ネットワーク上に RSPAN VLAN として使用する VLAN をいくつか確保しておき、これらの VLAN には、アクセス ポートを割り当てないでください。

ヒント　出力 Access Control List（ACL; アクセス制御リスト）を RSPAN トラフィックに適用し、特定のフローを選択してフィルタリングすることができます。これらの ACL は、RSPAN 送信元スイッチ内の RSPAN VLAN 上で指定します。

- RSPAN には、「SPAN 設定時の注意事項」（p.46-7）のすべての項目が当てはまります。
- RSPAN セッションは、SPAN/RSPAN の限度内であれば、SPAN セッションと共存させることができます。「SPAN/RSPAN のセッション限度」（p.46-5）を参照してください。
- RSPAN の設定では、送信元ポートと宛先ポートを複数のスイッチに分散させることができます。
- RSPAN では、ある VLAN（たとえば VLAN2）のすべての送信元ポートに送信元スイッチがあり、それが VLAN2 内のアップリンク ポートを介して宛先スイッチに接続している場合は、トランキングが必要です。RSPAN を使用すると、トラフィックは RSPAN VLAN のリモート スイッチに転送されます。RSPAN VLAN はトランク ポート専用に設定されており、アクセス ポートに対しては設定されていません。
- ラーニング オプションが適用されるのは、RSPAN 宛先ポートだけです。
- RSPAN は、BPDU パケットまたは CDP、DTP、および VTP などのレイヤ 2 プロトコル パケットのモニタをサポートしていません。
- 接続しているリンクでの帯域使用率を最適化する目的で、参加している送信元スイッチ、中間スイッチ、または宛先スイッチのそれぞれで、RSPAN VLAN に Quality of Service（QoS; サービス品質）パラメータを設定できます。
- 1 台の Catalyst 6500 シリーズ スイッチが送信元となることのできる RSPAN セッション（入力、出力、またはその両方）は 1 つだけです。送信元スイッチでリモートの入力または双方向 SPAN セッションを設定した場合、ローカルの入力または双方向 SPAN セッションの限度が 1 になります。RSPAN セッション限度には、ネットワーク上で伝送できる RSPAN セッションの数に対する制限はありません（「SPAN/RSPAN のセッション限度」[p.46-5] を参照）。

- 送信元トランク ポートにアクティブ RSPAN VLAN が設定されている場合、ポートベース RSPAN セッションの送信元として RSPAN VLAN を組み込むことはできません。RSPAN VLAN を VSPAN セッションの送信元にすることもできません。
- 次の条件を満たす場合、任意の VLAN を RSPAN VLAN として設定できます。
  - すべてのスイッチで、RSPAN セッションに同じ RSPAN VLAN を使用する。
  - 参加しているすべてのスイッチが適切なハードウェアとソフトウェアを備えている。
  - RSPAN VLAN にアクセス ポート（sc0 インターフェイスを含む）を設定していない。
- VTP および VTP プルーニングがイネーブルの場合、RSPAN トラフィックはトランクでプルーニングが実行され、ネットワーク上で RSPAN トラフィックの不要なフラッディングを防ぎます。
- GARP VLAN Registration Protocol（GVRP）がイネーブルになっていて、GVRP 要求が既存の RSPAN VLAN と競合する場合、RSPAN セッションで不要なトラフィックが発生する場合があります。
- RSPAN VLAN は ISL（スイッチ間リンク）/dot1q マッピングに使用できます。ただし、これらの VLAN で不要なトラフィックが発生しないようにするために、すべてのスイッチで RSPAN VLAN の特殊なプロパティがサポートされていなければなりません。

RSPAN の設定

RSPAN セッションを設定する場合、最初に、RSPAN に参加するスイッチのいずれにも*存在しない* RSPAN VLAN を、RSPAN セッション用として選択します。ネットワークで VTP がイネーブルになっている場合、1 つのスイッチで RSPAN VLAN を作成し、VTP がその RSPAN VLAN を VTP ドメイン内の他のスイッチに伝播するようにできます。

VTP プルーニングを使用して、RSPAN トラフィックのフローを効率化するか、または RSPAN トラフィックを伝送する必要のないすべてのトランクから、RSPAN VLAN を手動で削除してください。

RSPAN VLAN を作成したあとで、**set rspan** コマンドを入力して、送信元スイッチと宛先スイッチを設定します。

RSPAN VLAN を設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	RSPAN VLAN を設定します。	**set vlan** *vlan* [**rspan**]
ステップ 2	RSPAN VLAN の設定を確認します。	**show vlan**

次に、RSPAN VLAN として VLAN 500 を設定し、設定を確認する例を示します。

```
Console> (enable) set vlan 500 rspan
vlan 500 configuration successful
Console> (enable)
Console> (enable) show vlan
.
(テキスト出力は省略)
.
VLAN DynCreated  RSPAN
---- ---------- --------
1    static     disabled
2    static     disabled
3    static     disabled
99   static     disabled
500  static     enabled
Console> (enable)
```

RSPAN 送信元ポートを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	RSPAN 送信元ポートを設定します。RSPAN に参加している各送信元スイッチで、このコマンドを使用します。	**set rspan source** {*src_mod/src_ports...*| *vlans...*	**sc0**} {*rspan_vlan*} [**rx**	**tx**	**both**] **session** *session_number* [**multicast** {**enable**	**disable**}] [**filter** *vlans...*] [**create**]
ステップ 2	RSPAN の設定を確認します。	**show rspan**

次に、RSPAN VLAN 500 の入力側送信元ポートとして、ポート 4/1 および 4/2 を指定する例を示します。

```
Console> (enable) set rspan source 4/1-2 500 rx
Rspan Type      : Source
Destination     : -
Rspan Vlan      : 500
Admin Source    : Port 4/1-2
Oper Source     : None
Direction       : receive
Incoming Packets: -
Learning        : -
Multicast       : enabled
Filter          : -
Console> (enable)
```

RSPAN 送信元 VLAN を設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	RSPAN 送信元 VLAN を設定します。送信元 VLAN 内のすべてのポートが動作用送信元ポートになります。	**set rspan source** {*src_mod/src_ports...*| *vlans...*	**sc0**} {*rspan_vlan*} [**rx**	**tx**	**both**] **session** *session_number* [**multicast** {**enable**	**disable**}] [**filter** *vlans...*] [**create**]
ステップ 2	RSPAN の設定を確認します。	**show rspan**

次に、RSPAN VLAN 500 の送信元 VLAN として、VLAN 200 を指定する例を示します（オプションで **rx** キーワードを選択すると、VLAN 内のすべてのポートが入力ポートになります）。

```
Console> (enable) set rspan source 200 500 rx
Rspan Type      : Source
Destination     : -
Rspan Vlan      : 500
Admin Source    : VLAN 200
Oper Source     : None
Direction       : receive
Incoming Packets: -
Learning        : -
Multicast       : enabled
Filter          : -
Console> (enable)
```

RSPAN 宛先ポートを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	RSPAN 宛先ポートを設定します。RSPAN に参加している各宛先スイッチで、このコマンドを使用します。	**set rspan destination** *mod/port* {*rspan_vlan*} **session** *session_number* [**inpkts** {**enable** | **disable**}] [**learning** {**enable** | **disable**}] [**create**]
ステップ 2	RSPAN の設定を確認します。	**show rspan**

```
Console> (enable) set rspan destination 3/1 500
Rspan Type      : Destination
Destination     : Port 3/1
Rspan Vlan      : 500
Admin Source    : -
Oper Source     : -
Direction       : -
Incoming Packets: disabled
Learning        : enabled
Multicast       : -
Filter          : -
Console> (enable)
```

RSPAN をディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
スイッチ上で RSPAN をディセーブルにします。	**set rspan disable source** [*rspan_vlan* | **all**] **set rspan disable destination** [*mod*/*port* | **all**]

次に、イネーブルになっている送信元セッションをすべてディセーブルにする例を示します。

```
Console> (enable) set rspan disable source all
This command will disable all remote span source session(s).
Do you want to continue (y/n) [n]? y
Disabled monitoring of all source(s) on the switch for remote span.
Console> (enable)
```

次に、*rspan_vlan* 番号を使用して、1 つの送信元セッションをディセーブルにする例を示します。

```
Console> (enable) set rspan disable source 903
Disabled monitoring of all source(s) on the switch for rspan_vlan 903.
Console> (enable)
```

次に、イネーブルになっている宛先セッションをすべてディセーブルにする例を示します。

```
Console> (enable) set rspan disable destination all
This command will disable all remote span destination session(s).
Do you want to continue (y/n) [n]? y
Disabled monitoring of remote span traffic for all rspan destination ports.
Console> (enable)
```

次に、*mod*/*port* を使用して、1 つの宛先セッションをディセーブルにする例を示します。

```
Console> (enable) set rspan disable destination 4/1
Disabled monitoring of remote span traffic on port 4/1.
Console> (enable)
```

RSPAN の設定例

ここでは、RSPAN を設定する手順について説明します。

単一 RSPAN セッションの設定

次に、単一 RSPAN セッションを設定する例を示します。図 46-3 に、RSPAN の設定例を示します。この RSPAN セッションを設定するコマンドについては、表 46-2 を参照してください。表 46-2 では、**set vlan** *vlan* **rspan** コマンドを使用して、すべてのスイッチ上でこのセッションに対応する RSPAN VLAN 901 をすでに設定していることを前提としています。ネットワークで VTP がイネーブルになっている場合、1 つのスイッチで RSPAN VLAN を作成し、VTP がその RSPAN VLAN を VTP ドメイン内の他のスイッチに伝播するようにできます。表 46-2 の設定例では、スイッチ C またはスイッチ D の設定を変更しなくても、スイッチ A、スイッチ B、またはその両方で RSPAN セッションをディセーブルにできます。

図 46-3　単一 RSPAN セッション

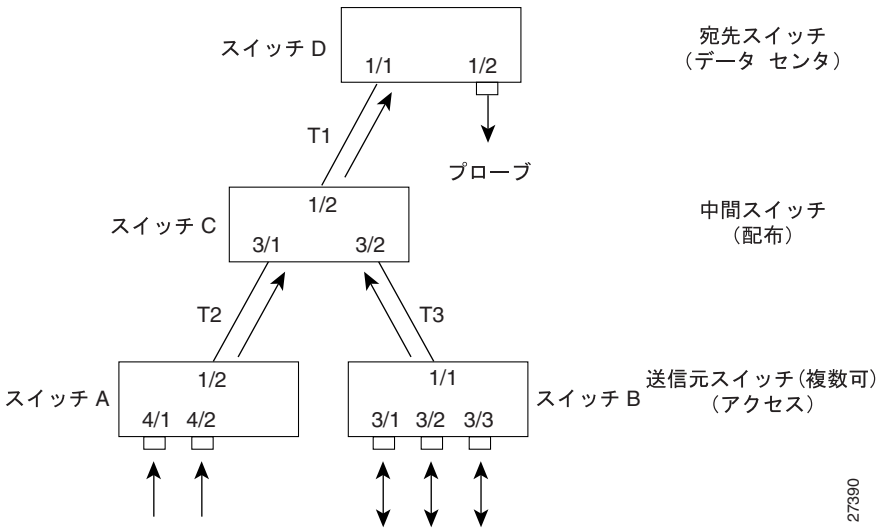


表 46-2　単一 RSPAN セッションの設定

スイッチ	ポート	RSPAN VLAN	方向	RSPAN CLI コマンド
A（送信元）	4/1、4/2	901	入力	**set rspan source 4/1-2 901 rx**
B（送信元）	3/1、3/2、3/3	901	双方向	**set rspan source 3/1-3 901**
C（中間）	–	901	–	RSPAN CLI コマンドは不要
D（宛先）	1/2	901	–	**set rspan destination 1/2 901**

アクティブ RSPAN セッションの変更

次に、アクティブ RSPAN セッションを変更する例を示します。図 46-3 を参照してください。RSPAN セッションをディセーブルにするコマンド、および RSPAN セッションから送信元ポートを追加または削除するコマンドについては、表 46-3 を参照してください。

表 46-3　アクティブ RSPAN セッションの変更

スイッチ	アクション	RSPAN CLI コマンド
A（送信元）	RSPAN セッションをディセーブル化	**set rspan disable source 901**
B（送信元）	RSPAN セッションから送信元ポート 3/2 を削除	**set rspan source 3/1, 3/3 901**
B（送信元）	RSPAN セッションに送信元ポート 3/2 を戻す	**set rspan source 3/1-3 901**

中間スイッチでの RSPAN 送信元ポートの追加

次に、中間スイッチで RSPAN 送信元ポートを追加する例を示します。図 46-4 に RSPAN の設定例を示します。この RSPAN セッションを設定するコマンドについては、表 46-4 を参照してください。スイッチ C のポート 2/1 ～ 2 は、同じ RSPAN セッションに対して設定できます。

図 46-4　中間スイッチでの RSPAN 送信元ポートの追加

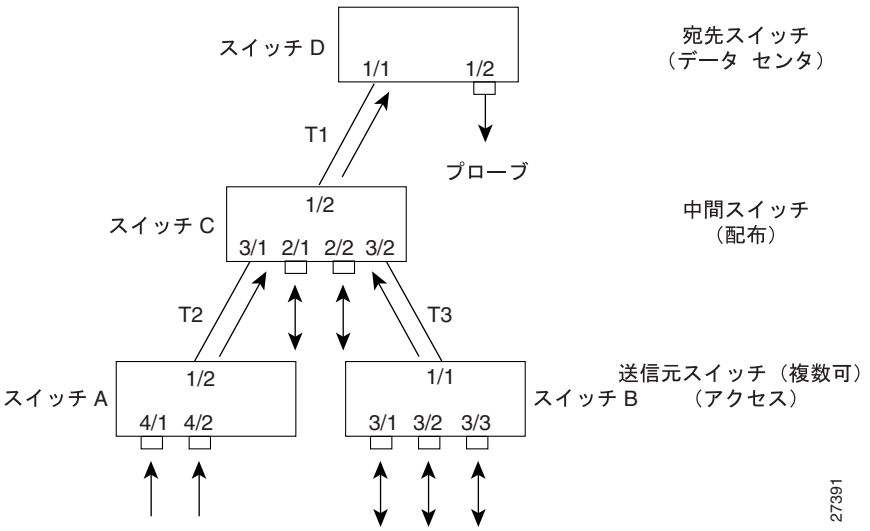


表 46-4　中間スイッチでの RSPAN 送信元ポートの追加

スイッチ	ポート	RSPAN VLAN	方向	RSPAN CLI コマンド
A（送信元）	4/1、4/2	901	入力	**set rspan source 4/1-2 901 rx**
B（送信元）	3/1、3/2、3/3	901	双方向	**set rspan source 3/1-3 901**
C（中間）	–	901	–	RSPAN CLI コマンドは不要
C（送信元）	2/1、2/2	901	双方向	**set rspan source 2/1-2 901**
D（宛先）	1/2	901	–	**set rspan destination 1/2 901**

複数の RSPAN セッションの設定

次に、複数の RSPAN セッションを設定する例を示します。図 46-5 に RSPAN の設定例を示します。この RSPAN セッションを設定するコマンドについては、表 46-5 を参照してください。この例は、モニタ プローブがデータ センタに、送信元ポートがアクセス スイッチにある場合の一般的な事例です（任意のスイッチの他のポートも RSPAN 用に設定できます）。SPAN トラフィックのルート変更がない場合、宛先スイッチと中間スイッチは 1 回の設定だけですみます。

図 46-5 では、RSPAN VLAN 901（プローブ 1）および RSPAN VLAN 902（プローブ 2）で 2 つの RSPAN セッションを使用します。わかりやすくするために、トランク T1 ～ T6 でトラフィックが流れる方向を示していますが、トランクの方向は、RSPAN VLAN のトランクの STP ステートによって決まります。個々の RSPAN セッションに対応するスイッチのそれぞれで、RSPAN VLAN を設定する必要があります。ネットワークで VTP がイネーブルになっている場合、1 つのスイッチで RSPAN VLAN を作成し、VTP がその RSPAN VLAN を VTP ドメイン内の他のスイッチに伝播するようにできます。VTP がディセーブルの場合は、各スイッチで RSPAN VLAN を作成します。

図 46-5　複数の RSPAN セッションの設定

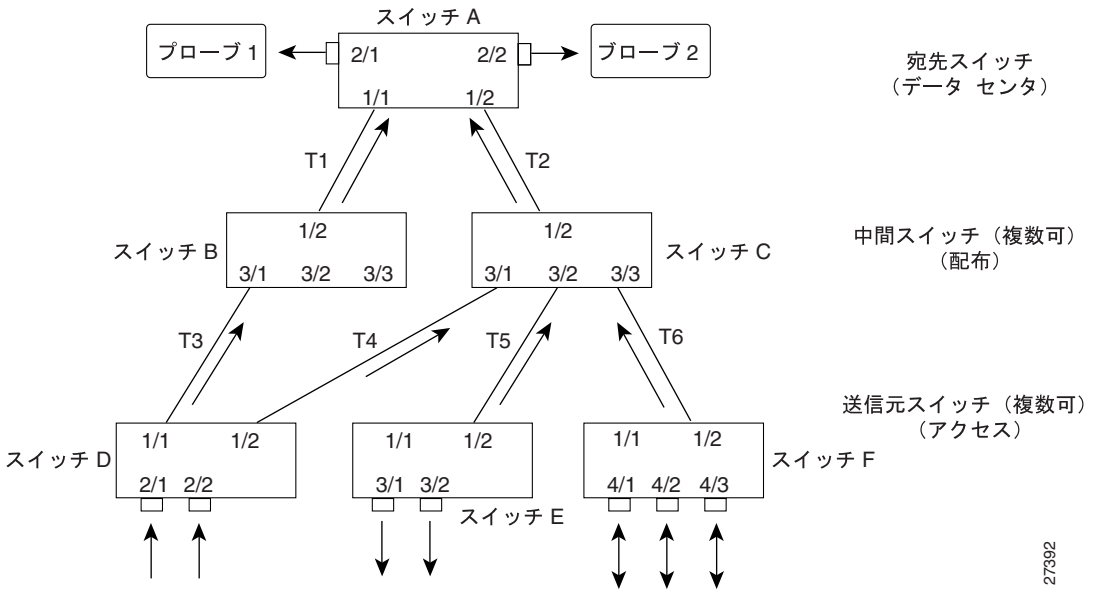


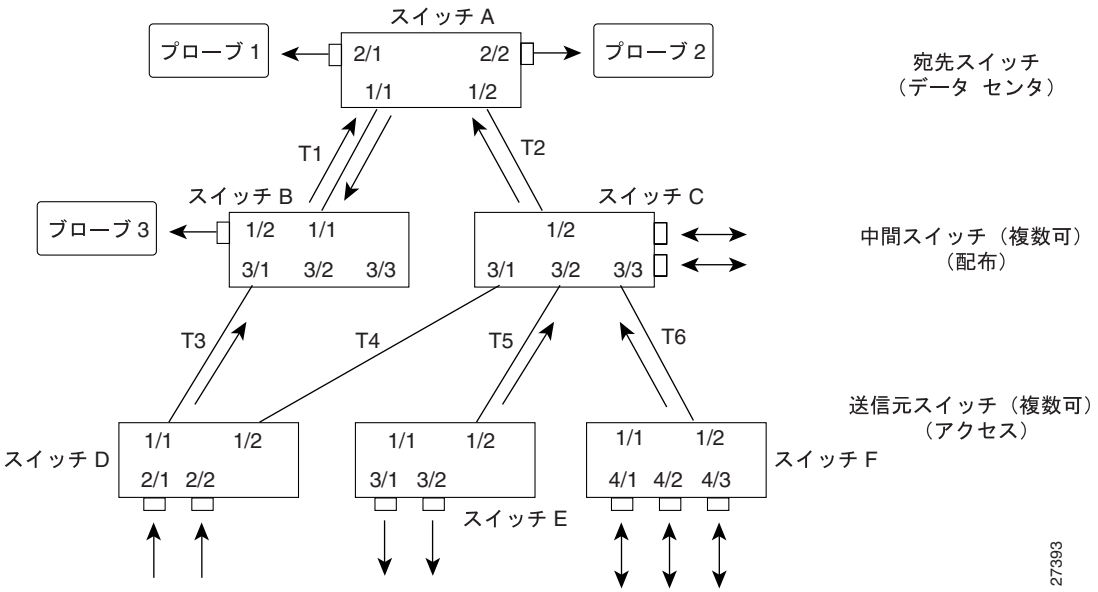
表 46-5　複数の RSPAN セッションの設定

スイッチ	ポート	RSPAN VLAN	方向	RSPAN CLI コマンド
A（宛先）	2/1	901	–	**set rspan destination 2/1,901**
A（宛先）	2/2	902	–	**set rspan destination 2/2,902**
B（中間）	–	901、902	–	RSPAN CLI コマンドは不要
C（中間）	–	901、902	–	RSPAN CLI コマンドは不要
D（送信元）	2/1-2	901	入力	**set rspan source 2/1-2 901 rx**
E（送信元）	3/1-2	901	出力	**set rspan source 3/1-2 901 tx**
F（送信元）	4/1-3	901	両方	**set rspan source 4/1-3 902**

1 つの RSPAN セッションに対する複数のネットワーク アナライザの追加

同じ RSPAN セッションに複数のネットワーク アナライザ（プローブ）を接続できます。たとえば、図 46-6 では、**set rspan destination 1/2 901** コマンドを使用することにより、スイッチ B にプローブ 3 を追加して、RSPAN VLAN 901 をモニタできます。同様に、スイッチ C に送信元ポートを追加できます。

図 46-6　RSPAN セッションへの複数のプローブの追加



CHAPTER 47

スイッチ TopN レポートの使用方法

この章では、Catalyst 6500 シリーズ スイッチ上でスイッチ TopN レポート ユーティリティを使用する方法について説明します。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

この章で説明する内容は、次のとおりです。

スイッチ TopN レポート ユーティリティの機能

ここでは、スイッチ TopN レポート ユーティリティの機能について説明します。

TopN レポートの概要

スイッチ TopN レポート ユーティリティを使用して、スイッチ上の各物理ポートのデータを収集し、解析することができます。

（注） スイッチ TopN レポート ユーティリティを使用して、Multilayer Switch Module（MSM）ポートまたは Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）、MSFC2、MSFC2A、および MSFC3 ポートに関するレポートを生成することはできません。

（注） ポートの使用率を計算する場合、スイッチ TopN レポート ユーティリティは Tx および Rx ラインを同一のカウンタにバンドルし、また、使用率の割合を計算する場合は全二重通信の帯域幅も確認します。たとえば、ギガビット イーサネット ポートは 2000 Mbps の全二重通信です。

スイッチ TopN レポート ユーティリティは、各物理ポートについて、次のデータを収集します。

- ポート使用率（**util**）
- 入力 / 出力バイト数（**bytes**）
- 入力 / 出力パケット数（**pkts**）
- 入力 / 出力ブロードキャスト パケット数（**bcst**）
- 入力 / 出力マルチキャスト パケット数（**mcst**）
- 入力エラー数（**in-errors**）
- バッファ オーバーフロー エラー数（**buf-ovflw**）

スイッチ TopN レポート ユーティリティは、起動後に対応するハードウェア カウンタからデータを収集し、ユーザが指定した期間だけスリープ モードになります。スリープ モードが終了すると、同じハードウェア カウンタから現在のデータを収集し、旧データと比較して、差分を保存します。各ポートのデータは、表 47-1 に示す値からユーザが指定したメトリックに基づいてソートされます。

表 47-1　スイッチ TopN レポートの有効メトリック値

メトリック値	定義
util	ポート使用率
bytes	入力 / 出力バイト
pkts	入力 / 出力パケット
bcst	入力 / 出力ブロードキャスト パケット
mcst	入力 / 出力マルチキャスト パケット
errors	入力エラー
overflow	バッファ オーバーフロー

background キーワードを指定しないでスイッチ TopN レポートを実行する場合

show top コマンドの入力時に **background** キーワードを指定しないと、処理は開始されますが、画面上にシステム プロンプトが再表示されません。そのため、レポート生成中、他のコマンドを入力できなくなります。

スイッチ TopN レポートの生成プロセスを中断するには、同じコンソールまたは Telnet セッションで **Ctrl-C** を押すか、または別のコンソールか Telnet セッションを使用して **clear top** [*report_num*] コマンドを入力します。スイッチ TopN レポート ユーティリティによるデータ処理が終了すると、データが画面上にただちに出力されます。ただし、この出力内容は保存されません。

background キーワードを指定してスイッチ TopN レポートを実行する場合

show top コマンドの入力時に **background** キーワードを指定すると、処理が開始されたあと、システム プロンプトがただちに再表示されます。処理の終了後、レポートのデータは画面上にすぐには表示されませんが、あとから表示できるよう保存されます。

レポート処理が完了すると、その通知として画面上に Syslog メッセージが表示されます。処理が完了したレポートを表示するには、**show top report** [*report_num*] コマンドを入力します。完成しているレポートだけが表示されます。完成していないレポートについては、スイッチ TopN プロセスの要約が表示されます。

background キーワードを指定したスイッチ TopN プロセスを中断できるのは、**clear top** [*report_num*] コマンドを入力した場合だけです。**Ctrl-C** を押しても、プロセスは中断されません。完成したレポートは、**clear top**{**all** | *report_num*} コマンドを入力して削除しないかぎりいつでも利用できます。

スイッチ TopN レポートの実行および表示

スイッチ TopN レポート ユーティリティをバックグラウンドで起動し、結果を表示するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチ TopN レポート ユーティリティをバックグラウンドで実行します。	**show top** [*N*] [*metric*] [**interval** *interval*] [*port_type*] **background**
ステップ 2	処理終了後、生成されたレポートを表示します。	**show top report** [*report_num*]

(注) **show top report** コマンドを使用して完成したレポートを表示するには、スイッチ TopN レポート ユーティリティの実行時に **background** キーワードを指定する必要があります。background キーワードを指定しないと、処理終了後にレポートがただちに出力され、レポート内容は保存されません。

show top report コマンドで *report_num* を指定すると、関連するレポートが表示されます。各プロセスに固有のレポート番号が割り当てられています。

report_num 変数を指定しないと、すべてのアクティブなスイッチ TopN プロセスと、そのスイッチのすべての関連スイッチ TopN レポートが表示されます。（**background** キーワードの指定に関係なく）すべてのスイッチ TopN プロセスがリストに表示されます。

background キーワードを指定してスイッチ TopN レポート ユーティリティを実行する例を示します。

```
Console> (enable) show top 5 pkts background
Console> (enable) 06/16/1998,17:21:08:MGMT-5:TopN report 4 started by Console//.
Console> (enable) 06/16/1998,17:21:39:MGMT-5:TopN report 4 available.
Console> (enable) show top report 4
Start Time:     06/16/1998,17:21:08
End Time:       06/16/1998,17:21:39
PortType:       all
Metric:         pkts (Tx + Rx)
Port  Band- Uti Bytes               Pkts       Bcst       Mcst       Error Over
      width  %  (Tx + Rx)           (Tx + Rx)  (Tx + Rx)  (Tx + Rx)  (Rx)  flow
----- ----- --- -------------------- ---------- ---------- ---------- ----- ----
 1/1    100   0                7950         81          0         81     0    0
 2/1    100   0                2244         29          0         23     0    0
 1/2    100   0                1548         12          0         12     0    0
 2/10   100   0                   0          0          0          0     0    0
 2/9    100   0                   0          0          0          0     0    0
Console> (enable)
```

スイッチ TopN レポート ユーティリティをフォアグラウンドで実行し、結果をただちに表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
スイッチ TopN レポート ユーティリティをフォアグラウンドで実行します。	**show top** [*N*] [*metric*] [**interval** *interval*] [*port_type*]

次に、スイッチ TopN レポート ユーティリティをフォアグラウンドで実行する例を示します。

```
Console> (enable) show top 5 pkts
Start Time:     06/16/1998,17:26:38
End Time:       06/16/1998,17:27:09
PortType:       all
Metric:         pkts (Tx + Rx)
Port  Band- Uti Bytes               Pkts       Bcst       Mcst       Error Over
      width  %  (Tx + Rx)           (Tx + Rx)  (Tx + Rx)  (Tx + Rx)  (Rx)  flow
----- ----- --- -------------------- ---------- ---------- ---------- ----- ----
 2/1    100   0                10838         94          2         26     0    0
 1/1    100   0                 7504         79          0         79     0    0
 1/2    100   0                 2622         21          0         21     0    0
 2/10   100   0                    0          0          0          0     0    0
 2/9    100   0                    0          0          0          0     0    0
Console> (enable)
```

保存されているレポートまたは保留状態のレポートを表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
レポートを表示します。	**show top report** [*report_num*]

(注) *report_num* を指定しなければ、すべての保存および保留状態のレポートが表示されます。

次に、特定のレポートを表示する例と、すべての保存および保留状態のレポートを表示する例を示します。

```
Console> (enable) show top report 5
Start Time:     06/16/1998,17:29:40
End Time:       06/16/1998,17:30:11
PortType:       all
Metric:         overflow
Port  Band- Uti Bytes               Pkts       Bcst       Mcst       Error Over
      width  %  (Tx + Rx)           (Tx + Rx)  (Tx + Rx)  (Tx + Rx)  (Rx)  flow
----- ----- --- -------------------- ---------- ---------- ---------- ----- ----
 1/1    100   0                 7880         83          0         83     0    0
 2/12   100   0                    0          0          0          0     0    0
 2/11   100   0                    0          0          0          0     0    0
 2/10   100   0                    0          0          0          0     0    0
 2/9    100   0                    0          0          0          0     0    0
Console> (enable) show top report
Rpt  Start time          Int N   Metric     Status   Owner (type/machine/user)
---  ------------------- --- --- ---------- -------- -------------------------
  1  06/16/1998,17:05:00 30  20  Util       done     telnet/172.16.52.3/
  2  06/16/1998,17:05:59 30  5   Util       done     telnet/172.16.52.3/
  3  06/16/1998,17:08:06 30  5   Pkts       done     telnet/172.16.52.3/
  4  06/16/1998,17:21:08 30  5   Pkts       done     Console//
  5  06/16/1998,17:29:40 30  5   Overflow   pending  Console//
Console> (enable)
```

保存されているレポートを削除するには、イネーブル モードで次の作業を行います。

作業	コマンド
レポートを削除します。	**clear top** {**all** | *report_num*}

(注) すべての完成しているレポートを削除するには、**all** キーワードを指定します。**clear top all** コマンドでは、保留状態のレポートは消去されません。すでに完成しているレポートだけが消去されます

次に、特定のレポートを削除する例と、すべての保存レポートを削除する例を示します。

```
Console> (enable) clear top 4
Console> (enable) 06/16/1998,17:36:45:MGMT-5:TopN report 4 killed by Console//.
Console> (enable) clear top all
06/16/1998,17:36:52:MGMT-5:TopN report 1 killed by Console//.
06/16/1998,17:36:52:MGMT-5:TopN report 2 killed by Console//.
Console> (enable) 06/16/1998,17:36:52:MGMT-5:TopN report 3 killed by Console//.
06/16/1998,17:36:52:MGMT-5:TopN report 5 killed by Console//.
Console> (enable)
```

CHAPTER 48

マルチキャスト サービスの設定

この章では、Catalyst 6500 シリーズ スイッチ上で Internet Group Management Protocol（IGMP）スヌーピング、GARP Multicast Registration Protocol（GMRP）、および Router-Port Group Management Protocol（RGMP）、双方向 Protocol Independent Multicast（PIM）を設定する方法について説明します。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

この章で説明する内容は、次のとおりです。

マルチキャスティングの機能

ここでは、Catalyst 6500 シリーズ スイッチのマルチキャスティング機能について説明します。

マルチキャスティングおよびマルチキャスト サービスの概要

IGMP スヌーピングは、IP マルチキャスト トラフィックのスイッチングを制御することにより、スイッチのマルチキャスト トラフィックを管理します。GMRP はプロトコルに依存せず、IP マルチキャスト トラフィックとレイヤ 2 マルチキャスト トラフィックの両方を管理できます。

スイッチは、IGMP スヌーピングまたは GMRP を使用してスイッチ ポートを動的に設定し、IP マルチキャスト ホストに関連付けられたポートだけに IP マルチキャスト トラフィックを転送します。IGMP ソフトウェア コンポーネントは、シスコ製ルータおよびスイッチの両方で稼働します。

（注） IP マルチキャストおよび IGMP の詳細については、RFC 1112 を参照してください。GMRP については、IEEE 802.1p を参照してください。

set cam static コマンドを入力して、マルチキャスト グループをスタティックに設定することができます。IGMP スヌーピングによって学習されるマルチキャスト グループは動的です。マルチキャスト グループ アドレスにグループ メンバーシップを指定すると、スタティックな設定が IGMP スヌーピングまたは GMRP による自動処理よりも優先されます。マルチキャスト グループ メンバーシップのリストは、ユーザが定義した設定値と、IGMP スヌーピングまたは GMRP によって学習された設定値の両方で構成できます。

IGMP スヌーピングの機能

（注） スイッチ上で GMRP がすでにイネーブルになっている場合は、IGMP スヌーピングをイネーブルに設定できません。

（注） どの Catalyst 6500 シリーズ スーパバイザ エンジン モデル（Supervisor Engine 1、Supervisor Engine 1A、Supervisor Engine 2、Supervisor Engine 720、および Supervisor Engine 32）でも IGMP スヌーピングを実行できます。IGMP スヌーピングをイネーブルにするのに PFC（ポリシー フィーチャ カード）は必要ではありません。Cisco Group Management Protocol（CGMP）は、Catalyst 6500 シリーズ スイッチではサポートされていません。ただし、CGMP サーバは MSFC（マルチレイヤ スイッチ フィーチャ カード）上でサポートされています。CGMP クライアント装置をサポートするには、CGMP サーバとして MSFC を設定します。

（注）　IGMP バージョン 3 スヌーピングは、Supervisor Engine 1 または Supervisor Engine 1A を搭載したシステムでサポートされません。

IGMP スヌーピングは、IP マルチキャスト トラフィックを振り分けてスイッチングできるようにすることによって、Catalyst 6500 シリーズ スイッチ上でレイヤ 2 マルチキャスト トラフィックを管理します。

スイッチは、IGMP スヌーピングを使用してレイヤ 2 インターフェイスを動的に設定し、IGMP Join およびレポート メッセージを通じて特定の IP マルチキャスト トラフィック ストリームの受信に関心を示しているインターフェイスだけに IP マルチキャスト トラフィックが転送されるようにします。

Catalyst 6500 シリーズ スイッチは、IGMP 制御トラフィックとマルチキャスト データ トラフィックを区別できます。スイッチ上で IGMP がイネーブルになっている場合、IGMP 制御トラフィックは CPU に転送されて処理されます。このプロセスは特殊な ASIC（特定用途向け IC）によってハードウェアで実行されるので、スイッチはパフォーマンスを低下させることなく、IGMP 制御トラフィックのスヌーピングを行うことができます。

ルータは定期的に汎用クエリをすべての VLAN（仮想 LAN）に送信します。マルチキャストのレシーバーはそのルータのクエリに応答し、その応答をスイッチが代行受信します。ルータに転送されるのは、各 VLAN、または各 IP マルチキャスト グループの最初の IGMP Join（レポート）だけです。同一 VLAN およびグループに対する以後のレポートは抑制されます。スイッチ プロセッサは、IGMP Join 要求の送信元となる各 MAC（メディア アクセス制御）グループのレイヤ 2 転送テーブルに、VLAN ごとにエントリを 1 つずつ作成します。このマルチキャスト トラフィックに関心のあるすべてのホストが Join 要求を送信し、この転送テーブル エントリのポート リストに加えられます。ポートがディセーブルになると、そのポートはすべてのマルチキャスト グループ エントリから削除されます。

IGMP バージョン 3 は、送信元ベースのフィルタリングを使用し、ホストが Source Specific Multicast（SSM）でチャネル加入を信号通知する業界指定の標準プロトコルになっています。送信元ベースのフィルタリングによって、ホストとルータは特定のマルチキャスト グループに対してどの送信元アドレスを許可またはブロックするかを指定できます。Catalyst 6500 シリーズ スイッチで IGMP バージョン 3 スヌーピングをイネーブルにすると、スイッチは、グループ単位、VLAN 単位でポートから受信 IGMP バージョン 3 のレポートに基づいて IGMP バージョン 3 ステートを維持します。また、スイッチは、受信する IGMP バージョン 3 メッセージのタイプに基づいてそのポート上で送信元トラフィックを許可またはブロックします。スイッチが SSM の IGMP バージョン 2 スヌーピング レポートを受信する場合、レポートは MSFC2 に転送されてシステム エラー メッセージが生成されます。

（注）　IGMP バージョン 3 スヌーピングでは、MSFC2 上で Cisco IOS Release 12.1(11b)E1 以降のリリースを使用します。

IGMP バージョン 3 スヌーピングの制限事項

次の制限事項が IGMP バージョン 3 スヌーピングに適用されます。

- Release 8.3(1) では、MMLS（マルチキャスト マルチレイヤ スイッチング）で IGMP バージョン 3 スヌーピングを使用する場合、Cisco IOS Release 12.2(17d)SXB1 を実行する必要があります。
- IGMP バージョン 3 スヌーピングは、PIM-SSM でのみ使用する必要があります。非 SSM モードで受信された IGMP バージョン 3 レポートに対しては、IGMP バージョン 2 スヌーピングが実行されます。
- IGMP バージョン 3 スヌーピングは、INCLUDE モードでのみサポートされています。EXCLUDE モードではサポートされていません。EXCLUDE モードに対応する IGMP バージョン 3 レポートは処理されず、ただ VLAN 上にフラッディングされます。
- Release 8.3(1) 以降のソフトウェア リリースでは、IGMP バージョン 3 スヌーピングは、Multicast OSPF（MOSPF）または Distance Vector Multicast Routing Protocol（DVMRP）を稼働しているルータを検出しません。
- SPAN（スイッチド ポート アナライザ）、RSPAN（Remote SPAN）、プライベート VLAN、および RGMP は IGMP バージョン 3 スヌーピングでサポートされていません。
- IGMP バージョン 3 スヌーピングは、Single-Router Mode（SRM; 単一ルータ モード）のみでサポートされています。Supervisor Engine 2 で Dual-Router Mode（DRM; デュアル ルータ モード）がサポートされていても、バージョン 3 スヌーピングは DRM をサポートしません。
- IGMP バージョン 3 スヌーピングは、Supervisor Engine 1 または Supervisor Engine 1A を搭載したシステムでサポートされません。
- SSM フローの *, G/m ハードウェア スイッチングは許可動作のみがある ACE（アクセス制御エントリ）でサポートされます。拒否動作は SSM で使用されません。SSM が使用される際に拒否動作を含む ACE を設定すると、通常の PIM sparse（疎）モードで動作している IGMP バージョン 2 スヌーピング ホストのデータが消失する可能性があります。
- レイヤ 2 スイッチング用に設定されているシステムのみが約 700 の ACL（アクセス制御リスト）をサポートしています。

マルチキャスト グループへの加入

IGMP バージョン 2 では、IP マルチキャスト グループに加入するホストは、ルータのクエリに応答するか、または加入する IP マルチキャスト グループを指定して（たとえば、グループ 224.1.2.3）、IGMP Join（別名、Join メッセージ）を送信します。スイッチ ハードウェアは、パケットが IGMP レポートであることを認識して、スイッチの CPU に転送します。スイッチは 01-00-5e-01-02-03 に対応する新しいグループ エントリを組み込み、そのエントリにホスト ポートおよびルータ ポートを追加します。スイッチはさらに、ホストからの Join をすべてのマルチキャスト ルータ ポートにリレーします。セグメントに対応する指定マルチキャスト ルータがグループの Outgoing Interface List（OIL; 発信インターフェイス リスト）に Outgoing Interface（OIF）を追加し、224.1.2.3 のマルチキャスト トラフィックをこのセグメントに転送し始めます。

この VLAN の 2 番めのホストがグループ 244.1.2.3 に加わる場合は、ホストからこのグループへの IGMP Join を送信します。スイッチ ハードウェアは、このパケットが IGMP 制御パケットであることを認識して、スイッチの CPU に転送します。スイッチにはこの VLAN の 01-00-5e-01-02-03 に対応するグループ エントリがすでにあるので、2 番めのホスト ポートをエントリに追加するだけです。初めてグループに加入するホストではないので、スイッチはレポートを抑制します（スイッチはレポートをルータに送りません）。

IGMP バージョン 3 レポートは、ホストによってアドレス 224.0.0.22 に送信されます。マルチキャスト ルータは、インターフェイスの各グループについてステート レコードを維持し、スイッチは VLAN 単位で各グループのステート レコードを維持します。ステート レコードに含まれているのは、マルチキャスト IP アドレス、グループ タイマー、送信元タイマー、およびホストによって指定されたフィルタ モードです。ホストは次のいずれかのフィルタ モードを指定できます。

- INCLUDE モード — このモードでは、ホストはマルチキャスト グループにメンバーシップを知らせ、トラフィックを受信する送信元 IP アドレスのリスト（INCLUDE リスト）を提供します。
- EXCLUDE モード — このモードでは、ホストはマルチキャスト グループにメンバーシップを知らせ、トラフィックを受信しない送信元 IP アドレスのリスト（EXCLUDE リスト）を提供します。このモードは、ホストが IP アドレスが EXCLUDE リストに記載されていない送信元からだけトラフィックを受信するということです。すべての送信元のトラフィックを受信するには、ホストは空の EXCLUDE リストで EXCLUDE モードのメンバーシップを表明します。

（注） IP MMLS がディセーブルの場合、IGMP 互換性モードは、VLAN 上のグループ（その VLAN 上のその特定グループについてバージョン 3 ステートが以前存在していた）についてバージョン 1 またはバージョン 2 メッセージを受け取るとすぐに、バージョン 1 またはバージョン 2 に変わります。

マルチキャスト トラフィックの抑制

ホストがグループにマルチキャスト トラフィックを送信した場合、スイッチ ハードウェアはそのストリームを IGMP 制御パケットとして認識しないので、パケットはスイッチの CPU にリダイレクトされません。代わりに、マルチキャスト トラフィックは MAC グループ エントリに転送され、スイッチはそのグループ エントリに追加されているポートだけにトラフィックを限定します。

ルータは IGMP 汎用クエリを送信します。スイッチは VLAN 内のすべてのポートにこれらのクエリをフラッディングし、マルチキャスト グループに関心のあるホストが、関心のある各グループに対する IGMP Join で応答します。

スイッチはこの IGMP Join を代行受信し、VLAN ごとに、また IP マルチキャスト グループごとに最初の Join だけをマルチキャスト ルータ ポートに転送します。同一 VLAN およびグループに対する以後のレポートは抑制されます（ルータに送られません）。スイッチの IGMP バージョン 3 スヌーピングをイネーブルにすると、すべての Join がルータ ポートに転送されます。

（注） ネットワークに CGMP スイッチが含まれている場合、Join および Leave メッセージの抑制は行われません。IGMP バージョン 2 スイッチと CGMP スイッチの両方が含まれているネットワークでは、ルータが CGMP Join および Leave メッセージを生成できるように、すべての Join および Leave メッセージがマルチキャスト ルータに転送されます。

マルチキャスト グループからの脱退

IGMP バージョン 1 または 2 が稼働しているネットワークでは、マルチキャスト トラフィックを受信するホストが VLAN に少なくとも 1 つあるかぎり、セグメントの指定マルチキャスト ルータは、その VLAN へのマルチキャスト トラフィックの転送を継続します。ホストがマルチキャスト グループから脱退する場合、マルチキャスト ルータから定期的に送られる汎用クエリを無視する（IGMP バージョン 1 ホストの動作）か、または IGMP Leave を送信する（IGMP バージョン 2 ホストの動作）ことができます。Supervisor Engine 1 または 2 を搭載したシステムでは、Leave メッセージを受け取ったスイッチは、Leave メッセージが届いたポートに MAC ベースの汎用クエリを送り、そのポートの接続装置が特定のマルチキャスト グループに対するトラフィックに関心があるかどうかを調べます。そのポートが VLAN で最後のポートだった場合、スイッチは VLAN 内のすべてのポートに MAC ベースの汎用クエリを送ります。MAC ベースの汎用クエリは、受け取った IGMP Leave メッセージの対象であるレイヤ 2 Group Destination Address（GDA）MAC アドレスが宛先になります。レイヤ 3 では、MAC ベースの汎用クエリの宛先は 244.0.0.1（すべてのホスト）になり、IGMP ヘッダーでグループ アドレス フィールドが 0.0.0.0 に設定されます。

MAC マルチキャスト グループ アドレスに対応付けられた IP マルチキャスト グループを宛先とする IGMP Join を受信しなかった場合、そのポートはマルチキャスト転送エントリから削除されます。ポートがエントリで最後に残った非マルチキャスト ルータ ポートでないかぎり、スイッチは IGMP Leave を抑制します（ルータに送信されません）。ポートがエントリで最後の非マルチキャスト ルータ ポートだった場合は、IGMP Leave はマルチキャスト ルータ ポートに転送され、MAC グループ転送エントリが削除されます。

IGMP Leave を受信したルータは、複数の IGMP グループ特定クエリを送信します。クエリへの応答として Join メッセージが届かず、そのインターフェイス経由で接続されたダウンストリーム ルータがない場合、ルータはマルチキャスト ルーティング テーブルで、その IP マルチキャスト グループ エントリに対応する OIL からインターフェイスを削除します。

IGMP 高速脱退処理

IGMP スヌーピング高速脱退処理を使用すると、スイッチ プロセッサは最初に MAC ベースの汎用クエリをポートに送らなくても、転送テーブル エントリのポート リストからインターフェイスを削除できます。ポートに IGMP Leave が届くと、そのポートはマルチキャスト転送エントリからただちに削除されます（またはエントリ全体が削除されます）。

IGMP 高速ブロック処理

IGMP バージョン 3 は、高速ブロック処理をサポートしています。スイッチ上で高速ブロック処理をイネーブルにすると、スイッチはポートに接続したホストから Block（ブロック）または Exclude（除外）メッセージを受け取ると、ただちにそのポートへのマルチキャスト パケットの転送を中止します。

（注） 各ポートに複数のホストが接続している場合は、高速脱退処理機能は使用しないでください。各ポートに複数のホストが接続しているときに高速脱退をイネーブルにすると、一部のホストが削除されることがあります。高速脱退は、IGMP バージョン 2 を搭載したホストでだけサポートされています。

GMRP の機能

GMRP は、IGMP スヌーピングと同様、制約付きマルチキャスト フラッディング機能を提供する Generic Attribute Registration Protocol（GARP）アプリケーションです。GMRP および GARP は、IEEE によって定義された標準プロトコルです。プロトコル動作の詳細は、802.1p を参照してください。

GMRP ソフトウェア コンポーネントは、スイッチとホストの両方で稼働します（GMRP ホスト ソフトウェアは別途必要です）。IP マルチキャスト環境では、ホスト上で IGMP と GMRP を組み合わせて使用する必要があります。ホストの GMRP ソフトウェアで、ホストのレイヤ 3 IGMP 制御パケットのレイヤ 2 GMRP バージョンを生成するためです。スイッチはホストから、レイヤ 2 GMRP トラフィックとレイヤ 3 IGMP トラフィックの両方を受信します。スイッチはルータにレイヤ 3 IGMP 制御パケットを転送し、受信した GMRP トラフィックを使用して、ホストの VLAN 内のマルチキャストをレイヤ 2 で制限します。

ホストが IP マルチキャスト グループに加入する場合、ホストから IGMP Join を送信します。その結果、GMRP Join が生成されます。スイッチは、GMRP Join メッセージを受信すると、Join の受信に使用したポートを該当するマルチキャスト グループに追加します。スイッチは、この GMRP Join を VLAN 内の他のすべてのホストに伝播します。通常、そのうちの 1 つがマルチキャスト送信元です。送信元からグループにマルチキャストを行う場合、スイッチはグループへの Join メッセージを受信したポートに限定してマルチキャストを転送します。

スイッチは定期的に GMRP クエリを送信します。ホストはマルチキャスト グループにとどまる場合、そのクエリに応答し、スイッチは何も実行しません。マルチキャスト グループにとどまる予定がないホストは、Leave メッセージを送信するか、またはスイッチからの定期クエリを無視することができます。Leave メッセージを受信したスイッチ、または **leaveall** タイマーが満了するまでの間にホストから応答を受信しなかったスイッチは、そのホストをマルチキャスト グループから削除します。

（注） ルーティング環境で GMRP を使用するには、ルータを接続するすべてのポート上で GMRP **forwardall** オプションをイネーブルにする必要があります（「スイッチ ポート上の GMRP forward-all オプションのイネーブル化」[p.48-24] を参照）。

RGMP の機能

RGMP を使用しなかった場合、すべてのマルチキャスト ルータがスイッチに入ってきたすべてのマルチキャスト データ トラフィックを受信することになります。RGMP を利用すると、マルチキャスト ルータは、そのルータにマルチキャスト トラフィックのダウンストリーム レシーバーがない場合に、マルチキャスト トラフィックを受信しないことを要求できます。Catalyst 6500 シリーズ スイッチは、RGMP をサポートしています。RGMP を使用すると、受信ルータとして設定したルータだけにマルチキャスト データ トラフィックが転送されるので、ネットワークの輻輳が軽減されます。

（注） RGMP を使用するには、スイッチ上で IGMP スヌーピングを、ルータ上で PIM をイネーブルにする必要があります。現在サポートされているのは、PIM sparse（疎）モードだけです。

ネットワーク上のすべてのルータが RGMP 対応でなければなりません。RGMP 対応ルータは、スイッチに RGMP Hello メッセージを定期的に送信します。RGMP Hello メッセージはスイッチに対して、ルータからスイッチに RGMP Join も送信された場合に限り、そのルータにマルチキャスト データを送信するように指示します。RGMP Join が送信されると、ルータはマルチキャスト データを受信できるようになります。RGMP データを受信できるようにルータを設定する方法については、「RGMP 関連の CLI コマンド」（p.48-37）を参照してください。

マルチキャスト データの受信を中止する場合、ルータからスイッチへ、RGMP Leave メッセージを送信する必要があります。ルータ上で RGMP をディセーブルにするには、ルータからスイッチへ、RGMP Bye メッセージを送信しなければなりません。

表 48-1 に、RGMP メッセージ タイプの概要を示します。

表 48-1　RGMP メッセージ タイプ

説明	アクション
Hello	ルータ上で RGMP がイネーブルになっている場合、スイッチがルータにマルチキャスト データ トラフィックを送信するのは、グループに対して RGMP Join が送信された場合に限られます。
Bye	ルータ上で RGMP がディセーブルになっている場合、スイッチはルータにすべてのマルチキャスト データ トラフィックを送信します。
Join	マルチキャスト MAC アドレス宛のマルチキャスト データ トラフィックが、レイヤ 3 グループ アドレス G からルータへ送信されます。これらのパケットは、RGMP パケットの Group Address フィールドにグループ G が指定されています。
Leave	グループ G 宛のマルチキャスト データ トラフィックは、ルータに送信されません。これらのパケットは、RGMP パケットの Group Address フィールドにグループ G が指定されています。

マルチキャスト トラフィックの抑制

ギガビット イーサネット ポートでは、マルチキャスト トラフィックに使用する帯域幅の範囲を制限できます。ギガビット イーサネット ポート上でマルチキャスト トラフィックに使用する帯域幅全体に対する割合を指定するには、**set port broadcast** コマンドを入力します。

RPF 失敗トラフィックのレート制限

複数のルータが同じ LAN セグメントに接続する冗長構成では、送信元から発信インターフェイスのレシーバーにマルチキャスト トラフィックを転送するルータは 1 つだけです。この種のトポロジーでは、Protocol Independent Multicast Designated Forwarder（PIM-DF）だけが共通 VLAN のデータを転送し、非 PIM-DF は転送されたマルチキャスト トラフィックを受信します。冗長ルータ（非 PIM-DF）はこのトラフィックを廃棄する必要があります。誤ったインターフェイスに着信しており、Reverse Path Forwarding（RPF）チェックに失敗するためです。RPF チェックに失敗するトラフィックを非 RPF トラフィックといいます。

マルチキャスト プロトコル仕様に従って、ルータは PIM アサート メカニズムが正しく機能するように非 RPF パケットを受信する必要があるので、すべての非 RPF パケットをハードウェア内で廃棄することはできません。

PFC3A では、非 RPF パケットのレート制限のハードウェア サポートが強化されています。非 RPF パケットの受信では、マッチするエントリがまだ存在しない場合、PFC3A は非 RPF エントリ（送信元、グループ、および入力インターフェイス情報を含む）を NetFlow テーブル内に作成したあと、着信 VLAN の非 RPF パケットをブリッジングし、MSFC3 に送ります。マッチする NetFlow エントリをすでに持つ非 RPF パケットは、着信 VLAN でブリッジングされるだけで、MSFC3 には送信されません。

NetFlow テーブル内の非 RPF エントリは定期的に期限切れになり、非 RPF パケットが MSFC3 にリークして PIM アサート メカニズムが正しく機能するようにします。

RPF 失敗のレート制限はデフォルトでイネーブルです。

直接接続サブネット インストールのイネーブル化

PIM sparse モードでは、インターフェイスの Designated Router（DR; 指定ルータ）である第 1 ホップ ルータは、PIM レジスタ メッセージ内に送信元トラフィックをカプセル化し、Rendezvous Point（RP; ランデブー ポイント）にユニキャストすることが必要な場合があります。グループの新しい発信元がルーティング テーブル内で学習されないように、（*,G）フローは完全にハードウェア スイッチング フローのままである必要があります。ハードウェア Forwarding Information Base（FIB; 転送情報ベース）に組み込まれている（サブネット / マスク、224/4）エントリにより、（*,G）フローが完全にハードウェア スイッチング フローのままであることも、新しい直接接続発信元を完全に学習することもできます。直接接続サブネットのインストールは、デフォルトでグローバルにイネーブルです。PIM 対応インターフェイスごとに 1 つずつ（サブネット / マスク、224/4）がインストールされます。

FIB エントリを表示するには、**show mls ip multicast connected** コマンドを入力します。

直接接続サブネットのインストールをイネーブルにするには、次の作業を行います。

作業	コマンド
直接接続サブネットのインストールをイネーブルにします。	Router(config) # **mls ip multicast connected**

次に、直接接続サブネットのインストールをイネーブルにする例を示します。

```
Router(config)# mls ip multicast connected
Router(config)#
```

IGMP クエリアの概要

IGMP クエリアを使用すると、PIM および IGMP が設定されていない VLAN 内で IGMP スヌーピングを行うことができます。マルチキャスト トラフィックはルーティングが不要なためです。

(注)　マルチキャスト ルータのない VLAN で IGMP スヌーピングを正しく機能させるには、IGMP クエリア機能をイネーブルにする必要があります。

VLAN に IGMP クエリア機能を設定すると、スイッチは 125 秒間隔で IGMP 汎用クエリ メッセージを送信し、他のスイッチからの汎用クエリ メッセージを待ち受けます。スイッチが汎用クエリを受信すると、クエリ送信元の選定が開始されます。スイッチ間でのクエリ送信元選定は、IP アドレスまたは MAC アドレスのどちらかに基づいて行われます。着信クエリで、送信元 IP アドレスがゼロ以外の場合、IP アドレスに基づいて選定が行われ、送信元 IP アドレスの小さいスイッチがクエリ送信元になります。着信クエリで、送信元 IP アドレスがゼロの場合は、送信元 MAC アドレスに基づいて選定が行われ、送信元 MAC アドレスの小さいスイッチが選定されてクエリ送信元になります。クエリ送信元に選定されなかったスイッチは、「他のクエリ送信元インターバル」タイマーを維持します。このタイマーが満了すると、そのスイッチはクエリ送信元として自己選定します。

IGMP クエリア機能をイネーブルにする手順については、「IGMP クエリア機能のイネーブル化」（p.48-16）を参照してください。

スイッチ上での IGMP スヌーピングの設定

IGMP スヌーピングにより、スイッチで IGMP パケットを確認し、パケットの内容に基づいて転送先を決定することができます。

(注)　IGMP スヌーピングがイネーブルの場合、Quality of Service（QoS; サービス品質）は IGMP トラフィックをサポートしません。

ここでは、IGMP スヌーピングを設定する手順について説明します。

IGMP スヌーピングのデフォルト設定

表 48-2 に、IGMP スヌーピングのデフォルト設定を示します。

(注)　IGMP スヌーピングは、7.*x* および 8.*x* リリース トレインのすべてのスーパバイザ エンジン ソフトウェア リリースにおいて、デフォルトでイネーブルです。また、5.*x* リリース トレインの Release 5.5(9) 以降のソフトウェア リリースおよび 6.*x* リリース トレインの Release 6.3(1) 以降のソフトウェア リリースにおいて、デフォルトでイネーブルです。

表 48-2　IGMP スヌーピングのデフォルト設定

機能	デフォルト値
IGMP スヌーピング	イネーブル
マルチキャスト ルータ	設定なし

IGMP スヌーピングの設定時の注意事項

ここでは IGMP スヌーピング設定時の注意事項について説明します。

- IGMP バージョン 3 スヌーピングでは、プロキシ レポートのサポートはありません。IGMP バージョン 2 スヌーピングでは、最初の Join と最後の Leave だけがルータに転送されます。ルータによって開始された Group Specific（GS）クエリの場合、少なくとも 1 つのポートがグループに存在していれば、スイッチはレポートで応答します。IGMP バージョン 3 スヌーピングでは、すべてのレポートはルータに転送され、GS および Group and Source-Specific（GSS）クエリは VLAN にフラッディングされ、メンバーシップを更新します。
- IGMP バージョン 3 スヌーピングが機能するには、少なくとも 1 台のバージョン 3 ルータが VLAN になければなりません。
- IGMP バージョン 2 スヌーピングとは異なり、IGMP バージョン 3 スヌーピングでは、再起動のあとも保持される永続的なエントリは追加できません。
- IGMP バージョン 2 スヌーピング レポートはキャプチャされ、スーパバイザ エンジンに送信されます。IGMP バージョン 3 スヌーピング レポートは、アドレス 224.0.0.22 に送信されます。この範囲ではスヌーピングがサポートされていないため、レポートはフラッディング以外にスーパバイザ エンジン用にキャプチャされます。
- このリリースの IGMP バージョン 3 スヌーピングでは、RGMP、SPAN、および RSPAN の相互作用はイネーブルになっていません。
- IGMP クエリアは、IGMP バージョン 2 スヌーピングとだけ相互作用します。IGMP バージョン 3 スヌーピングをイネーブルにする前に、IGMP クエリアをディセーブルにする必要があります。

IGMP スヌーピングのイネーブル化

（注） GMRP がイネーブルの場合は、IGMP スヌーピングをイネーブルにできません。

IGMP スヌーピングをイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	IGMP スヌーピングをイネーブルにします。	**set igmp enable**
ステップ 2	IGMP スヌーピングがイネーブルに設定されていることを確認します。	**show igmp statistics** [*vlan*]

次に、IGMP スヌーピングをイネーブルにし、設定を確認する例を示します。

```
Console> (enable) set igmp enable
IGMP Snooping is enabled.
Console> (enable) show igmp statistics
IGMP enabled

IGMP statistics for vlan 1:
     Transmit:
                     General Queries: 0
               Group Specific Queries: 0
                              Reports: 0
                               Leaves: 0

     Receive:
                     General Queries: 1056
               Group Specific Queries: 0
   Group and Source Specific Queries: 2
                              Reports: 60379
                               Leaves: 0
                    Total Valid pkts: 63552
                  Total Invalid pkts: 0
                         Other pkts: 2115
           MAC-Based General Queries: 0
         Failures to add GDA to EARL: 0
              Topology Notifications: 0
                IGMP packets dropped: 0
         IGMP Leave msgs in the list: 0
              IGMP V3 IS_IN messages: 13
              IGMP V3 IS_EX messages: 5
              IGMP V3 TO_IN messages: 0
              IGMP V3 TO_EX messages: 1
              IGMP V3 ALLOW messages: 0
              IGMP V3 BLOCK messages: 1
Console> (enable)
```

IGMP フラッディングのイネーブル化

IGMP フラッディングがディセーブルの場合、送信元トラフィックが VLAN でフラッディングすることはなく、ルータ ポートにのみ送信されます。IGMP フラッディングはデフォルトでイネーブルです。

IGMP フラッディングをイネーブルまたはディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	IGMP フラッディングをイネーブルまたはディセーブルにします。	**set igmp flooding** {**enable** | **disable**}
ステップ 2	IGMP フラッディング ステートを表示します。	**show igmp flooding**

次に、IGMP フラッディングをイネーブルおよびディセーブルにする例を示します。

```
Console> (enable) set igmp flooding enable
IGMP Flooding enabled (default)
Console> (enable) set igmp flooding disable
IGMP Flooding disabled
Console> (enable)
Console> (enable) show igmp flooding
Mcast flooding disabled
Console> (enable)
```

IGMP スヌーピング モードの指定

IGMP スヌーピングは、IGMP-only モードまたは IGMP-CGMP モードで動作します。スイッチは、ネットワーク上に存在するトラフィックに応じて、動的に IGMP-only モードまたは IGMP-CGMP モードのいずれかを選択します。IGMP-only モードは、CGMP デバイスがまったく存在しないネットワークで使用します。IGMP-CGMP モードは、IGMP デバイスと CGMP デバイスの両方が存在するネットワークで使用します。auto モードは、モードの動的スイッチングを無効にします。

IGMP スヌーピング モードを指定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	IGMP スヌーピング モードを指定します。	**set igmp mode** {**igmp-only** | **igmp-cgmp** | **auto**}
ステップ 2	IGMP スヌーピング モードを表示します。	**show igmp mode**

次に、IGMP モードを IGMP-only に指定し、設定を確認する例を示します。

```
Console> (enable) set igmp mode igmp-only
IGMP mode set to igmp-only
Console> (enable) show igmp mode
IGMP Mode:                  igmp-only
IGMP Operational Mode:      igmp-only
IGMP Address Aliasing Mode: normal
Console> (enable)
```

IGMP Leave クエリ タイプの指定

ポートが Leave メッセージをホストから受信する場合、IGMP Leave クエリ タイプを使用するように指定できます。MAC ベースの汎用クエリを指定した場合、Leave クエリが正確な GDA について送信され、その GDA を使用するグループに少なくとも 1 つのメンバーシップを持つバージョン 1 または 2 のホストが応答します。汎用クエリを指定すると、すべてのグループのすべてのバージョン 1 および 2 のホストからのレポートが登録されます。Auto モードを指定することもできます。Auto モードを指定した場合、ネットワーク内にバージョン 1 のホストが存在しなければ、グループ固有クエリが送信され、バージョン 1 のホストが存在すれば汎用クエリが送信されます。グループ固有クエリは、ネットワーク コンバージェンスを高速化します。

デフォルトでは、ポートが Leave メッセージを受信すると MAC ベースの汎用クエリが送信されます。

Leave クエリ タイプを指定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	IGMP Leave クエリ タイプを指定します。	**set igmp leave-query-type auto-mode** | **general-query** | **mac-gen-query**
ステップ 2	IGMP Leave クエリ タイプを表示します。	**show igmp leave-query-type**

次に、IGMP Leave クエリ タイプをグループ固有クエリに設定する例を示します。

```
Console> (enable) set igmp leave-query-type auto-mode
IGMP Leave Query Type set to auto-mode
Console> (enable) show igmp leave-query-type
IGMP Leave Query Type : Group-Specific Query
Console> (enable)
```

IGMP 高速脱退処理のイネーブル化

IGMP 高速脱退処理をイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチ上で IGMP 高速脱退処理をイネーブルにします。	**set igmp fastleave enable**
ステップ 2	IGMP 高速脱退処理がイネーブルに設定されていることを確認します。	**show multicast protocols status**

次に、IGMP 高速脱退処理をイネーブルにし、設定を確認する例を示します。

```
Console> (enable) set igmp fastleave enable
IGMP fastleave set to enable.
Warning:Can cause disconnectivity if there are more than one host joining the
         same group per access port.
console> (enable) show multicast protocols status
IGMP disabled
IGMP fastleave enabled
IGMP V3 processing disabled
IGMP V3 fastblock feature disabled
RGMP enabled
GMRP disabled
Console> (enable)
```

IGMP バージョン 3 スヌーピングのイネーブル化

IGMP バージョン 3 スヌーピングをイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	IGMP バージョン 3 スヌーピングをイネーブルにします。	**set igmp v3-processing enable**
ステップ 2	IGMP バージョン 3 スヌーピング情報を表示します。	**show multicast v3-group** **show multicast router**

次に、IGMP スヌーピングをイネーブルにし、設定を確認する例を示します。

```
Console> (enable) set igmp v3-processing enable
IGMP V3 processing enabled
Console> (enable) show multicast v3-group
Displaying V3 group information for all vlans
-------------------------------------------
(G,C): (227.1.1.1,2),  V3 state: INC
V1/V2 Compatibility mode: none (V3)
Include list: 2.2.2.6, Src timer 125 sec, Ports: 6/29 15/1
              2.2.2.5, Src timer 125 sec, Ports: 6/29 15/1
Exclude list: NULL

(G,C): (227.1.1.1,60),  V3 state: INC
V1/V2 Compatibility mode: none (V3)
Include list: 2.2.2.7, Src timer 115 sec, Ports: 13/30 15/1
              2.2.2.5, Src timer 115 sec, Ports: 13/30 15/1
              2.2.2.8, Src timer 115 sec, Ports: 13/30 15/1
Exclude list: NULL

Console> (enable) show multicast v3-group 2 227.1.1.1
 ----IGMP V3 information----
(G,C): (227.1.1.1,2),  V3 state: INC
V1/V2 Compatibility mode: none (V3)
Include list: 2.2.2.6, Src timer 125 sec, Ports: 6/29 15/1
              2.2.2.5, Src timer 125 sec, Ports: 6/29 15/1
Exclude list: NULL

Console> (enable) show multicast v3-group
Displaying V3 group information for all vlans
-------------------------------------------
(G,C): (227.1.1.1,2),  V3 state: EX
V1/V2 Compatibility mode: none (V3) Group timer: 125 sec
Include list: NULL
Exclude list: 2.2.2.6, Excluded Ports: 6/29
              2.2.2.5, Excluded Ports: 6/29

Console> (enable) show multicast router
Port           Vlan
-------------- ----------------
15/1           $  2,60

Total Number of Entries = 1
'*' - Configured
'+' - RGMP-capable
'#' - Channeled Port
'$' - IGMP-V3 Router
Console> (enable)
```

IGMP バージョン 3 高速ブロック処理のイネーブル化

IGMP バージョン 3 高速ブロック処理をイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	IGMP 高速ブロック処理をイネーブルします。	**set igmp fastblock enable**
ステップ 2	IGMP 高速ブロック処理がイネーブルに設定されていることを確認します。	**show multicast protocols status**

次に、IGMP 高速ブロック処理をイネーブルにし、設定を確認する例を示します。

```
Console> (enable) set igmp fastblock enable
IGMP V3 fastblock enabled

Console> (enable) show multicast protocols status
IGMP enabled
IGMP fastleave disabled
IGMP V3 processing enabled
IGMP V3 fastblock feature enabled
RGMP disabled
GMRP disabled
Console> (enable)
```

IGMP レート制限のイネーブル化

マルチキャスト パケットのレート制限を行うには、**set multicast ratelimit** コマンドを入力します。マルチキャスト パケットのレート制限は、デフォルトでディセーブルで、デフォルトのレート制限は秒あたり 0 パケットです。

マルチキャスト レート制限をイネーブルにしてレート制限を指定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	マルチキャスト レート制限をイネーブルにしてレート制限を指定します。	**set multicast ratelimit** {**disable** | **enable**} **set multicast ratelimit rate** *rate*
ステップ 2	マルチキャスト レート制限情報を表示します。	**show multicast ratelimit-info**

次に、マルチキャスト レート制限をイネーブルにしてレート制限を指定する例を示します。

```
Console> (enable) set multicast ratelimit enable
Enabling Multicast Ratelimiting
Set a non-zero threshold rate to operationally enable multicast ratelimiting
Console> (enable) set multicast ratelimit rate 1000
Multicast ratelimit watermark rate is set to 1000 pps
Console> (enable) show multicast ratelimit-info
Multicast ratelimiting enabled
Ratelimit threshold rate: 1000 pps
VLAN  RateLimited-Since         Ratelimited-for(seconds)
----  ------------------        ------------------------
Console> (enable)
```

IGMP クエリア機能のイネーブル化

IGMP クエリア機能を入力すると、PIM および IGMP が設定されていない VLAN 内で IGMP スヌーピングをサポートできます。マルチキャスト トラフィックはルーティングが不要なためです。

(注) VLAN 内のすべてのスイッチに対して IGMP クエリアをイネーブルに設定することができます。1 台のスイッチがクエリアとして選定されます。

VLAN 内で IGMP クエリア機能をイネーブルにするには、イネーブル モードで次の作業のいずれかを行います。

作業	コマンド
特定の VLAN またはすべての VLAN 上で IGMP クエリア機能をイネーブルにします。	**set igmp querier** {**disable** | **enable**} *vlan*
スイッチが汎用クエリを送信する間隔を指定します。デフォルトは 125 秒です。	**set igmp querier** *vlan* **qi** *val*
汎用クエリが送信されない場合に、クエリ送信元として自己選定するまでにスイッチが待機する時間の長さを指定します。デフォルトは 300 秒です。	**set igmp querier** *vlan* **oqi** *val*
IGMP クエリアの IP アドレスを指定します。IP アドレスを指定しない場合、デフォルトの IP アドレスは、0.0.0.0 です。	**set igmp querier address** *ip_address vlan*
IGMP クエリア情報を表示します。	**show igmp querier information**

次に、IGMP クエリア機能をイネーブルにし、クエリア情報を表示する例を示します。

```
Console> (enable) set igmp querier enable 4001
IGMP querier is enabled for VLAN(s) 4001
Console> (enable) set igmp querier 4001 qi 130
QI for VLAN(s) 4001 set to 130 second(s)
Console> (enable) set igmp querier address 40.1.1.1 4001
Querier Address for vlan 4001 set to 40.1.1.1
Console> (enable) show igmp querier information
VLAN Querier Address Querier State         Query Tx Count QI (sec) OQI (sec)
---- --------------- --------------------- -------------- -------- --------
4001 40.1.1.1        QUERIER               0              130      300
Console> (enable)
```

マルチキャスト ルータ情報の表示

IGMP スヌーピングをイネーブルにすると、スイッチは、マルチキャスト ルータの接続先ポートを自動的に学習します。

動的に学習されたマルチキャスト ルータ情報を表示するには、イネーブル モードで次のいずれかの作業を行います。

作業	コマンド
動的に学習されたマルチキャスト ルータ ポートおよび手動で設定されたマルチキャスト ルータ ポートの情報を表示します。	**show multicast router** [*mod/port*] [*vlan_id*]
IGMP スヌーピングを使用して動的に学習されたマルチキャスト ルータ ポートの情報だけを表示します。	**show multicast router igmp** [*mod/port*] [*vlan_id*]

次に、すべてのマルチキャスト ルータ ポートについて情報を表示する例を示します（ポート 2/1 のマルチキャスト ルータの横にあるアスタリスク [*] は、そのエントリが手動で設定されたことを示しています）。

```
Console> (enable) show multicast router
Port           Vlan
-------------- ----------------
 2/1    *         @  99
 2/2              @  201
16/1     +        @  10,200-201

Total Number of Entries = 3
'*' - Configured
'+' - RGMP-capable
'#' - Channeled Port
'$' - IGMP-V3 Router
'@' - IGMP-Querier Router
Console> (enable)
```

次に、IGMP により動的に学習されたマルチキャスト ルータ ポートだけを表示する例を示します。

```
Console> (enable) show multicast router igmp
IGMP enabled

Port       Vlan
---------  ----------------
 1/1       1
 2/1       2,99,255

Total Number of Entries = 2
'*' - Configured
'*' - Configured
'+' - RGMP-capable
'#' - Channeled Port
'$' - IGMP-V3 Router
'@' - IGMP-Querier Router
Console> (enable)
```

マルチキャスト グループ情報の表示

マルチキャスト グループ情報を表示するには、イネーブル モードで次のいずれかの作業を行います。

作業	コマンド
マルチキャスト グループについての情報を表示します。	**show multicast group** [*mac_addr*] [*vlan_id*]
IGMP により動的に学習されたマルチキャスト グループの情報だけを表示します。	**show multicast group igmp** [*mac_addr*] [*vlan_id*]
各 VLAN に含まれるマルチキャスト アドレス（グループ）の総数を表示します。	**show multicast group count** [*vlan_id*]
各 VLAN で、IGMP によって動的に学習されたマルチキャスト アドレス（グループ）の総数を表示します。	**show multicast group count igmp** [*vlan_id*]

次に、スイッチ上のすべてのマルチキャスト グループについて、情報を表示する例を示します。

```
Console> (enable) show multicast group
IGMP enabled

VLAN  Dest MAC/Route Des  Destination Ports or VCs / [Protocol Type]
----  ------------------  -----------------------------------------------------
1     01-00-11-22-33-44*  2/6-12
1     01-11-22-33-44-55*  2/6-12
1     01-22-33-44-55-66*  2/6-12
1     01-33-44-55-66-77*  2/6-12

Total Number of Entries = 4
Console> (enable)
```

IGMP スヌーピング統計情報の表示

スイッチ上の IGMP スヌーピング統計情報を表示するには、次の作業を行います。

作業	コマンド
IGMP スヌーピング統計情報を表示します。	**show igmp statistics** [*vlan_id*]

次に、IGMP スヌーピング統計情報を表示する例を示します。

```
Console> (enable) show igmp statistics
IGMP enabled

IGMP statistics for vlan 1:
     Transmit:
                      General Queries: 0
                Group Specific Queries: 0
                               Reports: 0
                                Leaves: 0

     Receive:
                      General Queries: 10
                Group Specific Queries: 0
   Group and Source Specific Queries: 0
                               Reports: 0
                                Leaves: 0
                     Total Valid pkts: 20
                   Total Invalid pkts: 0
                            Other pkts: 5
           MAC-Based General Queries: 0
         Failures to add GDA to EARL: 0
              Topology Notifications: 0
              IGMP packets dropped: 0
              IGMP Leave msgs in the list: 0
              IGMP V3 IS_IN messages: 0
              IGMP V3 IS_EX messages: 0
              IGMP V3 TO_IN messages: 0
              IGMP V3 TO_EX messages: 0
              IGMP V3 ALLOW messages: 0
              IGMP V3 BLOCK messages: 0
Console> (enable)
```

IGMP 高速脱退処理のディセーブル化

IGMP 高速脱退処理をディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
IGMP 高速脱退処理をディセーブルにします。	**set igmp fastleave disable**

次に、IGMP 高速脱退処理をディセーブルにする例を示します。

```
Console> (enable) set igmp fastleave disable
IGMP fastleave set to disable.
Console> (enable)
```

IGMP スヌーピングのディセーブル化

IGMP スヌーピングをディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
IGMP スヌーピングをディセーブルにします。	**set igmp disable**

次に、IGMP スヌーピングをディセーブルにする例を示します。

```
Console> (enable) set igmp disable
IGMP feature for IP multicast disabled
Console> (enable)
```

スイッチ上での GMRP の設定

ここでは、GMRP を設定する方法について説明します。

（注） GMRP 動作の概要については、「GMRP の機能」（p.48-6）を参照してください。

GMRP のソフトウェア要件

GMRP を使用するには、Release 5.2 以降のスーパバイザ エンジン ソフトウェア リリースが必要です。

GMRP のデフォルト設定

表 48-3 に、GMRP のデフォルト設定を示します。

表 48-3　GMRP のデフォルト設定

機能	デフォルト値
GMRP イネーブル ステート	ディセーブル
GMRP ポート別イネーブル ステート	ディセーブル
GMRP forward-all（すべて転送）	すべてのポート上でディセーブル
GMRP 登録	すべてのポート上で標準
GARP/GMRP タイマー	• Join 時間：200 ミリ秒 • Leave 時間：600 ミリ秒 • Leaveall 時間：10,000 ミリ秒

GMRP のグローバルなイネーブル化

(注)　IGMP スヌーピングがイネーブルの場合は、GMRP をイネーブルにできません。

GMRP をグローバルにイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	GMRP をグローバルにイネーブルにします。	**set gmrp enable**
ステップ 2	設定を確認します。	**show gmrp configuration**

次に、GMRP をグローバルにイネーブルにし、設定を確認する例を示します。

```
Console> (enable) set gmrp enable
GMRP enabled.
Console> (enable) show gmrp configuration
Global GMRP Configuration:
GMRP Feature is currently enabled on this switch.
GMRP Timers (milliseconds):
Join = 200
Leave = 600
LeaveAll = 10000
Port based GMRP Configuration:
Port                                        GMRP Status Registration ForwardAll
------------------------------------------- ----------- ------------ -----------
1/1-2,3/1,6/1-48,7/1-24                     Enabled     Normal       Disabled
Console> (enable)
```

スイッチ ポート単位での GMRP のイネーブル化

(注)　GMRP がグローバルにイネーブル化されているかどうかに関係なく、ポート単位で GMRP の設定を変更できます。ただし、GMRP をグローバルにイネーブルにするまで、GMRP は個々のポート上で機能しません。GMRP のグローバルな設定については、「GMRP のグローバルなイネーブル化」（p.48-22）を参照してください。

スイッチ ポート単位で GMRP をイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチ ポート単位で GMRP をイネーブルにします。	**set port gmrp enable** *mod/port*
ステップ 2	設定を確認します。	**show gmrp configuration**

次に、ポート 6/12 上で GMRP をイネーブルにし、設定を確認する例を示します。

```
Console> (enable) set port gmrp enable 6/12
GMRP enabled on port 6/12.
Console> (enable) show gmrp configuration
Global GMRP Configuration:
GMRP Feature is currently enabled on this switch.
GMRP Timers (milliseconds):
Join = 200
Leave = 600
LeaveAll = 10000
Port based GMRP Configuration:
Port                                       GMRP Status Registration ForwardAll
------------------------------------------ ----------- ------------ ----------
1/1-2,3/1,6/1-9,6/12,6/15-48,7/1-24        Enabled     Normal       Disabled
6/10-11,6/13-14                            Disabled    Normal       Disabled
Console> (enable)
```

スイッチ ポート単位での GMRP のディセーブル化

(注) GMRP がグローバルにイネーブル化されているかどうかに関係なく、ポート単位で GMRP の設定を変更できます。ただし、GMRP をグローバルにイネーブルにするまで、GMRP は個々のポート上で機能しません。GMRP のグローバルな設定については、「GMRP のグローバルなイネーブル化」（p.48-22）を参照してください。

スイッチ ポート単位で GMRP をディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチ ポート単位で GMRP をディセーブルにします。	**set port gmrp disable** *mod/port*
ステップ 2	設定を確認します。	**show gmrp configuration**

次に、ポート 6/10 ～ 14 上で GMRP をディセーブルにし、設定を確認する例を示します。

```
Console> (enable) set port gmrp disable 6/10-14
GMRP disabled on ports 6/10-14.
Console> (enable) show gmrp configuration
Global GMRP Configuration:
GMRP Feature is currently enabled on this switch.
GMRP Timers (milliseconds):
Join = 200
Leave = 600
LeaveAll = 10000
Port based GMRP Configuration:
Port                                       GMRP Status Registration ForwardAll
------------------------------------------ ----------- ------------ ----------
1/1-2,3/1,6/1-9,6/15-48,7/1-24             Enabled     Normal       Disabled
6/10-14                                    Disabled    Normal       Disabled
Console> (enable)
```

スイッチ ポート上の GMRP forward-all オプションのイネーブル化

ポート上で GMRP forward-all オプションをイネーブルにすると、スイッチで登録されているすべてのマルチキャスト トラフィックのコピーがそのポートに転送されます。マルチキャストを受信しなければならないルータに接続されているすべてのポート上で、forward-all オプションをイネーブルにしてください（ルータは GMRP をサポートしていないので、GMRP Join メッセージを送信できません）。forward-all オプションを使用して、ネットワーク アナライザまたはプローブが接続されたポートに、すべての登録マルチキャスト トラフィックを転送することもできます。

スイッチ ポート上で GMRP forward-all オプションをイネーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
スイッチ ポート上で GMRP forward-all オプションをイネーブルにします。	**set gmrp fwdall enable** *mod/port*

次に、ポート 1/1 上で GMRP forward-all オプションをイネーブルにする例を示します。

```
Console> (enable) set gmrp fwdall enable 1/1
GMRP Forward All groups option enabled on port 1/1.
Console> (enable)
```

スイッチ ポート上の GMRP forward-all オプションのディセーブル化

スイッチ ポート上で GMRP forward-all オプションをディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
スイッチ ポート上で GMRP forward-all オプションをディセーブルにします。	**set gmrp fwdall disable** *mod/port*

次に、ポート 1/1 上で GMRP forward-all オプションをディセーブルにする例を示します。

```
Console> (enable) set gmrp fwdall disable 1/1
GMRP Forward All groups option disabled on port 1/1.
Console> (enable)
```

GMRP 登録の設定

ここでは、スイッチ ポート上で GMRP 登録モードを設定する手順について説明します。

- normal（標準）登録の設定（p.48-24）
- fixed（固定）登録の設定（p.48-25）
- forbidden（禁止）登録の設定（p.48-25）

normal（標準）登録の設定

normal 登録モードでスイッチ ポートを設定すると、そのポート上で動的な GMRP マルチキャストの登録および登録解除ができるようになります。すべてのスイッチ ポート上で normal モードがデフォルトの設定です。

スイッチ ポート上で normal 登録モードを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチ ポート上で normal 登録を設定します。	**set gmrp registration normal** *mod/port*
ステップ 2	設定を確認します。	**show gmrp configuration**

次に、ポート 2/10 上で normal 登録を設定する例を示します。

```
Console> (enable) set gmrp registration normal 2/10
GMRP Registration is set normal on port 2/10.
Console> (enable)
```

fixed（固定）登録の設定

fixed 登録モードでスイッチ ポートを設定すると、その時点ですべてのポート上で登録されているマルチキャスト グループが、すべてそのポート上で登録されます。ただし、それ以後、他のポートで登録または登録解除が行われても無視されます。fixed 登録モードのスイッチ ポートは引き続き、そのポート固有のマルチキャスト グループを登録します。そのポートのマルチキャスト グループの登録を解除するには、ポートを **normal** 登録モードに戻す必要があります。

スイッチ ポート上で fixed 登録モードを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチ ポート上で fixed 登録を設定します。	**set gmrp registration fixed** *mod/port*
ステップ 2	設定を確認します。	**show gmrp configuration**

次に、ポート 2/10 上で fixed 登録を設定し、設定を確認する例を示します。

```
Console> (enable) set gmrp registration fixed 2/10
GMRP Registration is set fixed on port 2/10.
Console> (enable) show gmrp configuration
Global GMRP Configuration:
GMRP Feature is currently enabled on this switch.
GMRP Timers (milliseconds):
Join = 200
Leave = 600
LeaveAll = 10000
Port based GMRP Configuration:
GMRP-Status Registration ForwardAll Port(s)
----------- ------------ ---------- -------------------------------------------
Enabled     Normal       Disabled   1/1-4
                                    2/1-9,2/11-48
                                    3/1-24
                                    5/1
Enabled     Fixed        Disabled   2/10
Console> (enable)
```

forbidden（禁止）登録の設定

forbidden 登録モードでスイッチ ポートを設定すると、すべての GMRP マルチキャストを登録解除し、そのポート上での以降の GMRP マルチキャスト登録を防止することができます。

スイッチ ポート上で forbidden 登録モードを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチ ポート上で forbidden 登録を設定します。	**set gmrp registration forbidden** *mod/port*
ステップ 2	設定を確認します。	**show gmrp configuration**

次に、ポート 2/10 上で forbidden 登録を設定し、設定を確認する例を示します。

```
Console> (enable) set gmrp registration forbidden 2/10
GMRP Registration is set forbidden on port 2/10.
Console> (enable) show gmrp configuration
Global GMRP Configuration:
GMRP Feature is currently enabled on this switch.
GMRP Timers (milliseconds):
Join = 200
Leave = 600
LeaveAll = 10000
Port based GMRP Configuration:
GMRP-Status Registration ForwardAll Port(s)
----------- ------------ ---------- ------------------------------------------
Enabled     Normal       Disabled   1/1-4
                                    2/1-9,2/11-48
                                    3/1-24
                                    5/1
Enabled     Forbidden    Disabled   2/10
Console> (enable)
```

GARP タイマーの設定

（注） **set gmrp timer** および **show gmrp timer** コマンドは、**set garp timer** および **show garp timer** コマンドのエイリアスです。必要に応じてこれらのエイリアスを使用できます。

（注） GARP　タイマーの値を変更すると、GMRP　だけではなく、スイッチ上で実行しているすべての GARP アプリケーションに影響を及ぼします（たとえば、GVRP は同じタイマーを使用します）。

（注） GMRP Leaveall メッセージを送信するポートのみが、以前に GMRP Join メッセージを受信しています。

デフォルトの GARP タイマー値は、スイッチ上で変更できます。

タイマー値を設定する場合には、**leave** の値を **join** の値の 3 倍以上にしなければなりません（**leave** >= **join** × 3）。また、**leaveall** の値は、**leave** の値より大きくなければなりません（**leaveall** > **leave**）。スイッチに登録する属性が多いほど、**leave** 値と **join** 値の差を広げて設定する必要があります。

多数のマルチキャスト グループが登録された状況で、スイッチのパフォーマンスをさらに向上させるには、タイマー値を秒単位まで増やします。

このルールから外れたタイマー値を設定しようとすると、エラーが返されます。たとえば、**leave** タイマーを 600 ミリ秒に設定し、**join** タイマーを 350 ミリ秒に設定しようとすると、エラーになります。この場合、**leave** タイマーを 1050 ミリ秒以上に設定してから、**join** タイマーを 350 ミリ秒に設定してください。

注意 レイヤ 2 で接続されたすべての装置に同じ GARP タイマー値を設定してください。レイヤ 2 で接続された装置間で GARP タイマーが異なっていると、GARP アプリケーション（たとえば、GMRP および GVRP）が正常に動作しません。

GARP タイマーの値を設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	GARP タイマーの値を設定します。	**set garp timer** {**join** | **leave** | **leaveall**} *timer_value*
ステップ 2	設定を確認します。	**show garp timer**

次に、GARP タイマーを設定し、設定を確認する例を示します。

```
Console> (enable) set garp timer leaveall 12000
GMRP/GARP leaveAll timer value is set to 12000 milliseconds.
Console> (enable) set garp timer leave 650
GMRP/GARP leave timer value is set to 650 milliseconds.
Console> (enable) set garp timer join 300
GMRP/GARP join timer value is set to 300 milliseconds.
Console> (enable) show garp timer
Timer     Timer Value (milliseconds)
--------  --------------------------
Join      300
Leave     650
LeaveAll  12000
Console> (enable)
```

GMRP 統計情報の表示

スイッチ上の GMRP 統計情報を表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
GMRP 統計情報を表示します。	**show gmrp statistics** [*vlan_id*]

次に、VLAN 23 の GMRP 統計情報を表示する例を示します。

```
Console> show gmrp statistics 23
GMRP Statistics for vlan <23>:
Total valid GMRP Packets Received:500
Join Empties:200
Join INs:250
Leaves:10
Leave Alls:35
Empties:5
Fwd Alls:0
Fwd Unregistered:0
Total valid GMRP Packets Transmitted:600
Join Empties:200
Join INs:150
Leaves:45
Leave Alls:200
Empties:5
Fwd Alls:0
Fwd Unregistered:0
Total valid GMRP Packets Received:0
Total GMRP packets dropped:0
Total GMRP Registrations Failed:0
Console>
```

GMRP 統計情報の消去

スイッチ上の GMRP 統計情報を消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
GMRP 統計情報を消去します。	**clear gmrp statistics** {*vlan_id* | **all**}

次に、すべての VLAN について、GMRP 統計情報を消去する例を示します。

```
Console> (enable) clear gmrp statistics all
Console> (enable)
```

スイッチ上での GMRP のグローバルなディセーブル化

スイッチ上で GMRP をグローバルにディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
スイッチ上で GMRP をグローバルにディセーブルにします。	**set gmrp disable**

次に、スイッチ上で GMRP をグローバルにディセーブルにする例を示します。

```
Console> (enable) set gmrp disable
GMRP disabled.
Console> (enable)
```

スイッチ上でのマルチキャスト ルータ ポートおよびグループ エントリの設定

ここでは、マルチキャスト ルータ ポートを手動で指定し、マルチキャスト グループ エントリを設定する手順について説明します。

マルチキャスト ルータ ポートの指定

IGMP スヌーピングをイネーブルにすると、スイッチは、マルチキャスト ルータの接続先ポートを自動的に学習します。ただし、マルチキャスト ルータ ポートを手動で指定することもできます。

マルチキャスト ルータ ポートを手動で指定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	マルチキャスト ルータ ポートを手動で指定します。	**set multicast router** *mod/port*
ステップ 2	設定を確認します。	**show multicast router** [**igmp** | **rgmp**][*mod/port*] [*vlan_id*]

次に、マルチキャスト ルータ ポートを手動で指定し、設定を確認する例を示します（ポート 2/2 のマルチキャスト ルータの横にあるアスタリスク [*] は、このエントリが手動で設定されたことを示しています）。

```
Console> (enable) set multicast router 2/2
Port 2/2 added to multicast router port list.
console> (enable) show multicast router
Port           Vlan
-------------- ----------------
 2/2    *            50
 8/48             @  10
16/1              @  200-201

Total Number of Entries = 3
'*' - Configured
'+' - RGMP-capable
'#' - Channeled Port
'$' - IGMP-V3 Router
'@' - IGMP-Querier Router
Console> (enable)
```

マルチキャスト グループの設定

マルチキャスト グループを手動で設定するには、イネーブル モードで次の作業を行います。

（注） Release 7.1(1) 以降のソフトウェア リリースでは、レイヤ 2 マルチキャスト エントリの最大数は 15488 です。

	作業	コマンド
ステップ 1	CAM（連想メモリ）テーブルに 1 つまたは複数のマルチキャスト MAC アドレスを追加します。	**set cam** {**static** | **permanent**} *multicast_mac mod/port* [*vlan*]
ステップ 2	マルチキャスト グループの設定を確認します。	**show multicast group** [*mac_addr*] [*vlan_id*]

次に、マルチキャスト グループを手動で設定し、設定を確認する例を示します（アスタリスク [*] は、このエントリが手動で設定されたことを示しています）。

```
Console> (enable) set cam static 01-00-11-22-33-44 2/6-12
Static multicast entry added to CAM table.
Console> (enable) set cam static 01-11-22-33-44-55 2/6-12
Static multicast entry added to CAM table.
Console> (enable) set cam static 01-22-33-44-55-66 2/6-12
Static multicast entry added to CAM table.
Console> (enable) set cam static 01-33-44-55-66-77 2/6-12
Static multicast entry added to CAM table.
Console> (enable) show multicast group
IGMP disabled

VLAN  Dest MAC/Route Des  Destination Ports or VCs / [Protocol Type]
----  ------------------  -----------------------------------------------------
1     01-00-11-22-33-44*  2/6-12
1     01-11-22-33-44-55*  2/6-12
1     01-22-33-44-55-66*  2/6-12
1     01-33-44-55-66-77*  2/6-12

Total Number of Entries = 4
Console> (enable)
```

マルチキャスト ルータ ポートの消去

手動で設定したマルチキャスト ルータ ポートを消去するには、イネーブル モードで次のいずれかの作業を行います。

作業	コマンド
手動で設定したマルチキャスト ルータ ポートを指定して消去します。	**clear multicast router** *mod/port*
手動で設定したマルチキャスト ルータ ポートをすべて消去します。	**clear multicast router all**

次に、手動で設定したマルチキャスト ルータ ポートを消去する例を示します。

```
Console> (enable) clear multicast router 2/12
Port 2/12 cleared from multicast router port list.
Console> (enable)
```

マルチキャスト グループ エントリの消去

手動で設定したマルチキャスト グループ エントリを CAM テーブルから消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
CAM テーブルからマルチキャスト グループ エントリを消去します。	**clear cam** *mac_addr* [*vlan*]

次に、CAM テーブルからマルチキャスト グループ エントリを消去する例を示します。

```
Console> (enable) clear cam 01-11-22-33-44-55 1
CAM entry cleared.
Console> (enable)
```

RGMP の機能

RGMP は、関心のないマルチキャスト ルータだけに接続しているポートを介してスイッチからマルチキャスト トラフィックが送信されることを抑制します。Catalyst 6500 シリーズ スイッチは、RGMP をサポートしています。RGMP を使用すると、受信ルータとして設定したルータだけにマルチキャスト データ トラフィックが転送されるので、ネットワークの輻輳が軽減されます。

（注） RGMP を使用するには、スイッチ上で IGMP スヌーピングをイネーブルにする必要があります。IGMP スヌーピングは、ホストが接続されているスイッチ ポートからのマルチキャスト トラフィック送信を抑制します。IGMP スヌーピングは、1 つまたは複数のマルチキャスト ルータが接続されているポートからのトラフィックは抑制しません。

（注） RGMP を動作させるすべてのルータおよびスイッチ上で、PIM をイネーブルにする必要があります。現在サポートされているのは、PIM sparse モードだけです。

ネットワーク上のすべてのルータが RGMP 対応でなければなりません。RGMP 対応ルータは、スイッチに RGMP Hello メッセージを定期的に送信します。RGMP Hello メッセージはスイッチに対して、ルータからスイッチに RGMP Join メッセージも送信された場合に限り、そのルータにマルチキャスト データを送信するように指示します。RGMP Join メッセージが送信されると、ルータはマルチキャスト データを受信できるようになります。RGMP データを受信できるようにルータを設定する方法については、「RGMP 関連の CLI コマンド」（p.48-37）を参照してください。

マルチキャスト データの受信を中止する場合、ルータからスイッチへ、RGMP Leave メッセージを送信する必要があります。ルータ上で RGMP をディセーブルにするには、ルータからスイッチへ、RGMP Bye メッセージを送信しなければなりません。

表 48-4 に、RGMP パケット タイプの概要を示します。

表 48-4　RGMP パケット タイプ

説明	アクション
Hello	ルータ上で RGMP がイネーブルになっている場合、スイッチがルータにマルチキャスト データ トラフィックを送信するのは、グループに対して RGMP Join が送信された場合に限られます。
Bye	ルータ上で RGMP がディセーブルになっている場合、スイッチはルータにすべてのマルチキャスト データ トラフィックを送信します。
Join	マルチキャスト MAC アドレス宛のマルチキャスト データ トラフィックが、レイヤ 3 グループ アドレス G からルータへ送信されます。これらのパケットは、RGMP パケットの Group Address フィールドにグループ G が指定されています。
Leave	グループ G 宛のマルチキャスト データ トラフィックは、ルータに送信されません。これらのパケットは、RGMP パケットの Group Address フィールドにグループ G が指定されています。

RGMP を使用する場合の制限事項は、次のとおりです。

- sparse（疎）モードに限定 ― RGMP がサポートしているのは PIM sparse モードだけです。RGMP は、PIM dense（密）モードをサポートしていません。ただし、RGMP では、2 つの AutoRP グループの dense モードがサポートされています。これらのグループへのトラフィックは抑制されず、すべてのルータ ポートにフラッディングされます。そのため、PIM sparse-dense モードを設定する必要があります。AutoRP グループ以外のグループを dense モードに設定すると、これらのトラフィックは、RGMP 対応ルータ ポートからは正しく転送されません。
- RGMP を使用してマルチキャスト トラフィックを効率的に抑制するには、RGMP 対応ルータを、RGMP 対応スイッチ上の個別ポートに接続してください。
- RGMP は、RGMP 対応ルータを検出したポートからのトラフィック送信を抑制するだけです。ポート上で RGMP 非対応ルータが検出されると、そのポートはすべてのマルチキャスト トラフィックを受信します。
- RGMP は、ネットワーク上の直接接続された送信元をサポートしていません。直接接続された送信元のトラフィックは、RGMP または PIM が適用されずにネットワーク上に送信されます。RGMP 対応ルータは、RGMP を介したそのグループからの受信をあらかじめ要求していないかぎり、このトラフィックを受信しません。この制約は、ホストおよびルータのマルチキャスト トラフィック送信機能（**ping** コマンドや **mtrace** コマンドなど、および UDPTN などのマルチキャスト トラフィックを送信するマルチキャスト アプリケーション）に適用されます。
- RGMP　は、ネットワーク内の直接接続されたレシーバーをサポートしています。これらのレシーバーへのトラフィックは、IGMP スヌーピングによって抑制されます。または、レシーバーがルータの場合、PIM および RGMP によって抑制されます。ルータ上で RGMP がイネーブルになっている場合、ネットワーク上の CGMP はサポートされません。ルータ インターフェイス上でイネーブルにできるのは、RGMP または CGMP のどちらか一方だけです。インターフェイス上で RGMP をイネーブルにすると、CGMP は自動的にディセーブルになります。逆の場合も同じです。
- RGMP の次の特性は、IGMP スヌーピングと同じです。
  - RGMP は、送信元の IP アドレスではなく、マルチキャスト グループに基づいてトラフィックを抑制します。
  - ネットワークのスパニング ツリー トポロジーが変更された場合、CGMP と同様に、ステートは反映されません。
  - RGMP は、RGMP 制御ネットワークで PIMv2 Bootstrap Router（BSR）を使用できるマルチキャスト グループ 224.0.0.x（x = 0 ～ 255）のトラフィックは抑制しません。
  - シスコ製スイッチの RGMP は、IP マルチキャスト アドレス上ではなく、MAC アドレス上に適用されます。1 つの MAC アドレスに複数の IP マルチキャスト アドレスをマッピングできるので（RFC 1112 を参照）、RGMP は 1 つの MAC アドレスにマッピングされた複数の IP マルチキャスト グループを識別しません。
  - スイッチのトラフィック抑制機能は、CAM テーブルの容量により制限されます。

スイッチ上での RGMP の設定

ここでは、RGMP の設定コマンドについて説明します。

スーパバイザ エンジン上での RGMP の設定

ここでは、RGMP の設定コマンドについて説明します。

RGMP のデフォルト設定

RGMP はディセーブルがデフォルトの設定です。

RGMP のイネーブル化およびディセーブル化

（注）　RGMP をイネーブルにするには、IGMP スヌーピングがイネーブルに設定されている必要があります。

RGMP をイネーブルまたはディセーブルにするには、イネーブル モードで次のいずれかの作業を行います。

作業	コマンド
RGMP をイネーブルにします。	**set rgmp enable**
RGMP をディセーブルにします。	**set rgmp disable**

次に、RGMP をイネーブルにする例を示します。

```
Console> (enable) set rgmp enable
RGMP enabled.
Console> (enable)
```

次に、RGMP をディセーブルにする例を示します。

```
Console> (enable) set rgmp disable
RGMP disabled.
Console> (enable)
```

RGMP グループ情報の表示

次のコマンドを使用して、1 つまたは複数の RGMP 対応ルータによって加えられたマルチキャスト グループをすべて表示し、さらに、1 つまたは複数の RGMP 対応ルータによって加えられたマルチキャスト グループの数を表示します。

RGMP グループ情報を表示するには、イネーブル モードで次のいずれかの作業を行います。

作業	コマンド
1 つまたは複数の RGMP 対応ルータによって加えられたマルチキャスト グループをすべて表示します。	**show rgmp group** [*mac_addr*] [*vlan_id*]
1 つまたは複数の RGMP 対応ルータによって加えられたマルチキャスト グループの数を表示します。	**show rgmp group count** [*vlan_id*]

次に、RGMP グループ情報を表示する例を示します。

```
Console> (enable) show rgmp group
VlanDest MAC/Route Des  RGMP Joined Router Ports
---------------------------------------------------------------------------------------
-
1   01-00-5e-00-01-28   5/1,5/15
1   01-00-5e-01-01-01   5/1
2   01-00-5e-27-23-70*  3/1, 5/1
Total Number of Entries = 3
'*' - Configured
Console> (enable)

Console> (enable) show rgmp group count 1
Total Number of Entries = 2
```

RGMP VLAN 統計情報の表示

指定された VLAN の RGMP 統計情報を表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
指定された VLAN の RGMP 統計情報を表示します。	**show rgmp statistics** [*vlan*]

次に、指定された VLAN について RGMP 統計情報を表示する例を示します。

```
Console> (enable) show rgmp statistics 23
RGMP enabled
RGMP Statistics for vlan <23>:
Receive:
Valid pkts:    20
Hellos:        10
Joins:         5
Leaves:        5
Byes:          0
Discarded:     0
Transmit:
Total Pkts:    10
Failures:      0
Hellos:        10
Joins:         0
Leaves:        0
Byes:          0
Console> (enable)
```

RGMP 対応ルータ ポートの表示

次のコマンドを使用すると、検出された RGMP 対応ルータ ポートが表示されます。ポートの前にある [+] が、RGMP 対応ルータであることを示しています。

RGMP 対応ルータ ポートを表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
RGMP 対応ルータ ポートを表示します。	**show multicast router** [**igmp** | **rgmp**] [*mod/port*] [*vlan_id*]

次に、RGMP 対応ルータに接続しているポートを表示する例を示します。

```
Console> (enable) show multicast router
Port           Vlan
-------------- ----------------
 2/2     +        @  40
 8/48            @  10
16/1     +        @  200-201

Total Number of Entries = 3
'*' - Configured
'+' - RGMP-capable
'#' - Channeled Port
'$' - IGMP-V3 Router
'@' - IGMP-Querier Router
Console> (enable)
```

次に、RGMP 対応ルータ ポートのみを表示する例を示します。

```
Console> (enable) show multicast router rgmp
Port           Vlan
-------------- ----------------
 2/2     +        @  40
16/1     +        @  200

Total Number of Entries = 2
'*' - Configured
'+' - RGMP-capable
'#' - Channeled Port
'$' - IGMP-V3 Router
'@' - IGMP-Querier Router
Console> (enable)
```

RGMP 統計情報の消去

次のコマンドを使用すると、保存されている RGMP 統計情報が消去されます。

RGMP 統計情報を消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
RGMP 統計情報を消去します。	**clear rgmp statistics**

次に、RGMP 統計情報を消去する例を示します。

```
Console> (enable) clear rgmp statistics
RGMP statistics cleared.
Console> (enable)
```

RGMP 関連の CLI コマンド

このコマンドは、ルータからの RGMP 関連コマンドをイネーブルまたはディセーブルにします。

RGMP をイネーブルまたはディセーブルにするには、コンフィギュレーション モードで次のいずれかの作業を行います。

作業	コマンド
RGMP をイネーブルにします。	Router(config)# **ip rgmp**
RGMP をディセーブルにします。	Router(config)# **no ip rgmp**

このコマンドは、RGMP デバッギングをイネーブルまたはディセーブルにします。

RGMP デバッギングをイネーブルまたはディセーブルにするには、イネーブル モードで次のいずれかの作業を行います。

作業	コマンド
RGMP デバッギングをイネーブルにします。	Router# **debug ip rgmp** [*group-name* | *group-address*]
RGMP デバッギングをディセーブルにします。	Router# **no debug ip rgmp** [*group-name* | *group-address*]

MSFC 上での RGMP の設定

MSFC 上の VLAN インターフェイス上で RGMP を設定するには、次の作業を行います。

	作業	コマンド
ステップ 1	VLAN インターフェイス コンフィギュレーション モードにアクセスします。	Router(config)# **interface vlan** *vlan_ID*
ステップ 2	RGMP をイネーブルにします。	Router(config-if)# **ip rgmp**

debug ip rgmp コマンドを使用して、MSFC 上の RGMP をモニタできます。

マルチキャスト プロトコル ステータスの表示

次のコマンドを使用すると、スイッチ上のレイヤ 2 マルチキャスト プロトコルのステータス（イネーブルまたはディセーブル）が表示されます。

マルチキャスト プロトコル ステータスを表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
マルチキャスト プロトコル ステータスを表示します。	**show multicast protocols status**

次に、マルチキャスト プロトコル ステータスを表示する例を示します。

```
Console> (enable) show multicast protocols status
IGMP enabled
IGMP fastleave disabled
IGMP V3 processing disabled
IGMP V3 fastblock feature disabled
RGMP disabled
GMRP disabled
Console> (enable)
```

双方向 PIM の機能

Supervisor Engine 720 では、双方向 PIM グループのハードウェア フォワーディングをサポートしています。双方向 PIM グループをサポートするために、Supervisor Engine 720 では Designated Forwarder（DF）モードという新しいモードを実装しています。DF は、双方向 PIM グループのセグメントとの間でパケットを転送するために選定されたルータです。DF モードでは、スーパバイザ エンジンが RPF インターフェイスおよび DF インターフェイスからのパケットを受け入れます。

スーパバイザ エンジンが双方向 PIM グループを転送している際、RPF インターフェイスは常に（*,G）エントリの出力インターフェイス リストに含まれていて、DF インターフェイスは IGPM/PIM Join に応じて含まれています。

RP へのルートが使用できなくなった場合、グループは dense モードに変わります。RP への RPF リンクが使用できなくなる場合、双方向フローがハードウェア FIB から削除されます。

スイッチ上での双方向 PIM の設定

ここでは、双方向 PIM の設定方法と、双方向 PIM 設定情報および統計情報の表示方法について説明します。

双方向 PIM の設定

双方向 PIM を設定するには、次の手順を実行します。

ステップ 1　双方向 PIM をグローバルにイネーブルにします。

ステップ 2　双方向グループ用の RP を設定します。

これらの手順については、次で詳しく説明します。

双方向 PIM のグローバルなイネーブル化およびディセーブル化

双方向 PIM をイネーブルまたはディセーブルにするには、次の手順を実行します。

作業	コマンド
スイッチ上で双方向 PIM をグローバルにイネーブルにします。	Router(config)# **ip pim bidir-enable**
スイッチ上で双方向 PIM をグローバルにディセーブルにします。	Router(config)# [**no**] **ip pim bidir-enable**

次に、スイッチ上で双方向 PIM をイネーブルにする例を示します。

```
Router(config)# ip pim bidir-enable
Router(config)#
```

次に、スイッチ上で双方向 PIM をディセーブルにする例を示します。

```
Router(config)# no ip pim bidir-enable
Router(config)#
```

双方向 PIM グループの RP の設定

(注) 双方向 RP に対するグループ マッピングのトラフィック フローは、4 つだけハードウェアで切り換えられます。残りのグループへのトラフィックはソフトウェアで転送されます。

双方向グループ用の RP をスタティックに設定するには、次の作業を行います。

	作業	コマンド
ステップ 1	グループの RP の IP アドレスをスタティックに設定します。**override** キーワードを設定する場合、スタティック RP を使用します。	Router(config)# **ip pim rp-adress** *ip_address access-list* [**override**]
ステップ 2	アクセス リストを設定します。	Router(config)# **access-list** *access-list* **permit** | **deny** *ip_address*
ステップ 3	ルータが RP として機能するグループを設定するために自動 RP を使用するようにシステムを設定します。	Router(config)# **ip pim send-rp-announce** type number **scope** ttl-value [**group-list** access-list] [**interval** seconds] [**bidir**]
ステップ 4	標準 IP アクセス リストを設定します。	Router(config)# **ip access-list standard** *access-list-name* **permit** | **deny** *ip_address*
ステップ 5	MLS IP マルチキャストをイネーブルにします。	Router(config)# **mls ip multicast**

次に、双方向グループに対するスタティック RP を設定する例を示します。

```
Router(config)# ip pim rp-address 10.0.0.1 10 bidir override
Router(config)# access-list 10 permit 224.1.0.0 0.0.255.255
Router(config)# ip pim send-rp-announce Loopback0 scope 16 group-list c21-rp-list-0
bidir
Router(config)# ip access-list standard c21-rp-list-0 permit 230.31.31.1 0.0.255.255
```

双方向 PIM スキャン間隔の設定

双方向 PIM RP RPF スキャンの間隔を指定できます。

双方向 RP RPF スキャン間隔を設定するには、次のいずれかの作業を行います。

作業	コマンド
双方向 RP RPF スキャン間隔を設定します。有効な範囲は 1 ～ 1000 秒です。デフォルトは 10 秒です。	Router(config)# **mls ip multicast bidir gm-scan-interval** *interval*
デフォルトに戻します。	Router(config)# **no mls ip multicast bidir gm-scan-interval**

次に、双方向 RP RPF スキャン間隔を設定する例を示します。

```
Router(config)# mls ip multicast bidir gm-scan-interval 30
Router(config)#
```

次に、デフォルトの双方向 RP RPF スキャン間隔に戻す例を示します。

```
Router(config)# no mls ip multicast bidir gm-scan-interval
Router(config)#
```

双方向 PIM 情報の表示

双方向 PIM 情報を表示するには、次の手順を実行します。

作業	コマンド
PIM グループと RP とのマッピングを表示し、使用中の学習 RP を表示します。	Router# **show ip pim rp mapping** [**in-use**]
PIM グループとアクティブ RP とのマッピングを表示します。	Router# **show mls ip multicast rp-mapping** [*rp-address*]
RP マッピング キャッシュ内のグループおよびマスク範囲に基づいて情報を表示します。	Router# **show mls ip multicast rp-mapping gm-cache**
RP マッピング キャッシュ内の DF リストに基づいて情報を表示します。	Router# **show mls ip multicast rp-mapping df-cache**
双方向 PIM 情報を表示します。	Router# **show mls ip multicast bidir**
マルチキャスト ルーティング テーブルに関する情報を表示します。	Router# **show ip mroute**

次に、PIM グループと RP とのマッピングに関する情報を表示する例を示します。

```
Router# show ip pim rp mapping
PIM Group-to-RP Mappings
This system is an RP (Auto-RP)
This system is an RP-mapping agent
Group(s) 230.31.0.0/16
  RP 60.0.0.60 (?), v2v1, bidir
    Info source:60.0.0.60 (?), elected via Auto-RP
         Uptime:00:03:47, expires:00:02:11
  RP 50.0.0.50 (?), v2v1, bidir
    Info source:50.0.0.50 (?), via Auto-RP
         Uptime:00:03:04, expires:00:02:55
  RP 40.0.0.40 (?), v2v1, bidir
    Info source:40.0.0.40 (?), via Auto-RP
         Uptime:00:04:19, expires:00:02:38
```

次に、双方向 PIM に関連した IP マルチキャスト ルーティング テーブル内の情報を表示する例を示します。

```
Router# show ip mroute bidirectional
    (*, 225.1.3.0), 00:00:02/00:02:57, RP 3.3.3.3, flags:BC
      Bidir-Upstream:GigabitEthernet2/1, RPF nbr 10.53.1.7, RPF-MFD
      Outgoing interface list:
        GigabitEthernet2/1, Bidir-Upstream/Sparse-Dense, 00:00:02/00:00:00,H
        Vlan30, Forward/Sparse-Dense, 00:00:02/00:02:57, H

    (*, 225.1.2.0), 00:00:04/00:02:55, RP 3.3.3.3, flags:BC
      Bidir-Upstream:GigabitEthernet2/1, RPF nbr 10.53.1.7, RPF-MFD
      Outgoing interface list:
        GigabitEthernet2/1, Bidir-Upstream/Sparse-Dense, 00:00:04/00:00:00,H
        Vlan30, Forward/Sparse-Dense, 00:00:04/00:02:55, H

    (*, 225.1.4.1), 00:00:00/00:02:59, RP 3.3.3.3, flags:BC
      Bidir-Upstream:GigabitEthernet2/1, RPF nbr 10.53.1.7, RPF-MFD
      Outgoing interface list:
        GigabitEthernet2/1, Bidir-Upstream/Sparse-Dense, 00:00:00/00:00:00,H
        Vlan30, Forward/Sparse-Dense, 00:00:00/00:02:59, H
```

次に、特定のマルチキャスト ルートに関連する情報を表示する例を示します。

```
Router# show ip mroute 239.1.1.2 4.4.4.4
IP Multicast Routing Table
Flags:D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel
       Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags:H - Hardware switched
 Timers:Uptime/Expires
 Interface state:Interface, Next-Hop or VCD, State/Mode

(4.4.4.4, 239.1.1.2), 1d02h/00:03:20, flags:FTZ
 Incoming interface:Loopback0, RPF nbr 0.0.0.0, Partial-SC
  Outgoing interface list:
    Vlan10, Forward/Sparse-Dense, 1d02h/00:02:39 (ttl-threshold 5)
```

次に、特定のマルチキャスト グループ アドレスのエントリを表示する例を示します。

```
Router# show mls ip multicast group 230.31.31.1
Multicast hardware switched flows:
(*, 230.31.31.1) Incoming interface:Vlan611, Packets switched:1778
Hardware switched outgoing interfaces:Vlan131 Vlan151 Vlan415 Gi4/16 Vlan611
RPF-MFD installed
```

次に、PIM グループとアクティブな RP とのマッピングに関する情報を表示する例を示します。

```
Router# show mls ip multicast rp-mapping
State:H - Hardware Switched, I - Install Pending, D - Delete Pending, Z - Zombie

RP Address      State       RPF            DF-count    GM-count
60.0.0.60       H           Vl611                 4           1
```

次に、RP マッピング キャッシュ内のグループおよびマスク範囲に基づいた情報を表示する例を示します。

```
Router# show mls ip multicast rp-mapping gm-cache
State:H - Hardware Switched, I - Install Pending, D - Delete Pending,
       Z - Zombie

RP Address     State       Group           Mask            State
Packet/Byte-count
60.0.0.60      H           230.31.0.0      255.255.0.0     H             100/6400
```

次に、特定の MLS IP マルチキャスト グループについての情報を表示する例を示します。

```
Router# show mls ip multicast rp-mapping df-cache
State:H - Hardware Switched, I - Install Pending, D - Delete Pending, Z - Zombie

RP Address      State        DF             State
60.0.0.60       H           Vl131           H
60.0.0.60       H           Vl151           H
60.0.0.60       H           Vl415           H
60.0.0.60       H           Gi4/16          H
```

CHAPTER 49

QoS の設定

この章では、Catalyst 6500 シリーズ スイッチ上で Quality of Service（QoS; サービス品質）を設定する方法について説明します。また、Common Open Policy Service（COPS）および Resource Reservation Protocol（RSVP）をサポートするために必要な設定情報についても説明します。

(注)

- この章で使用しているコマンドの完全構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。
- 自動 QoS の使用方法については、第 50 章「自動 QoS の使用」を参照してください。

次のいずれかを使用して、QoS を設定できます。

- SNMP（簡易ネットワーク管理プロトコル）
- COPS プロトコル
- RSVP ヌル サービス テンプレートおよびレシーバー プロキシ機能
- CLI（コマンドライン インターフェイス）

この章で説明する内容は、次のとおりです。

QoS の機能

（注）　このマニュアルおよびその他すべての Catalyst 6500 シリーズ スイッチのマニュアルにおいて、*QoS* という用語は Catalyst 6500 シリーズの QoS 機能を意味します。

ネットワークは通常、*ベストエフォート型*の配信方式で動作します。したがって、すべてのトラフィックに等しいプライオリティが与えられ、正しいタイミングで配信される可能性も同等です。輻輳が発生した場合に廃棄される可能性についても、すべてのトラフィックで同等です。

Catalyst 6500 シリーズ スイッチの QoS は、ネットワーク トラフィックを選択し、相対的な重要度に従ってプライオリティを与え、輻輳回避技法によってプライオリティベースの処理を実行します。QoS によりネットワーク パフォーマンスが予測可能になり、帯域幅をより効率的に利用できるようになります。

QoS は、ネットワーク トラフィック内のレイヤ 2 およびレイヤ 3 の値を、設定値に設定するか、または受信したレイヤ 2 またはレイヤ 3 の値に基づく値に設定します。IP トラフィックは、スイッチから送出されるときにレイヤ 3 値を維持します。

PFC3 では、QoS は入力トラフィックと出力トラフィックの両方で設定可能です。QoS は、入力トラフィックについてはポートまたは VLAN（仮想 LAN）単位で設定できます。出力トラフィックについては VLAN 単位でのみ設定できます。

他のハードウェアでは、QoS は入力トラフィックについてポートまたは VLAN 単位で設定できます。

ここでは、QoS について説明します。

QoS の用語

ここでは、QoS 用語をいくつか定義しておきます。

- *パケット* ― レイヤ 3 でトラフィックを伝送します。
- *フレーム* ― レイヤ 2 でトラフィックを伝送します。レイヤ 2 フレームは、レイヤ 3 パケットを伝送します。
- *ラベル* ― パケットおよびフレームで伝送されるプライオリティ値です。
  - ― レイヤ 2 の Class of Service（CoS; サービス クラス）値。範囲は 0（ロー プライオリティ）～ 7（ハイ プライオリティ）です。

    レイヤ 2 ISL（スイッチ間リンク）フレーム ヘッダーには、下位 3 ビットで IEEE 802.1p CoS 値を伝送する、1 バイトのユーザ フィールドがあります。

レイヤ 2 802.1Q フレーム ヘッダーには、2 バイトのタグ制御情報フィールドがあり、その上位 3 ビット（ユーザ プライオリティ ビット）で CoS 値が伝送されます。

他のフレーム タイプでは CoS 値は伝送されません。

（注）　ISL トランクとして設定されたポート上では、すべてのトラフィックが ISL フレームに収められます。802.1Q トランクとして設定されたポートでは、ネイティブ VLAN のトラフィックを除き、すべてのトラフィックが 802.1Q フレームに収められます。

- レイヤ 3 IP precedence 値 ― IP バージョン 4 の仕様では、1 バイトの Type of Service（ToS; サービス タイプ）フィールドの上位 3 ビットを IP precedence と定めています。IP precedence 値の範囲は、0（ロー プライオリティ）～ 7（ハイ プライオリティ）です。
- レイヤ 3 Differentiated Services Code Point（DSCP）値 ― Internet Engineering Task Force（IETF）は、1 バイトの ToS フィールドのうち上位 6 ビットを DSCP と定めています。どの DSCP 値でどのプライオリティを表すかを設定できます。DSCP 値の範囲は 0 ～ 63 です（詳細については「DSCP 値マッピングの設定」[p.49-71] を参照）。

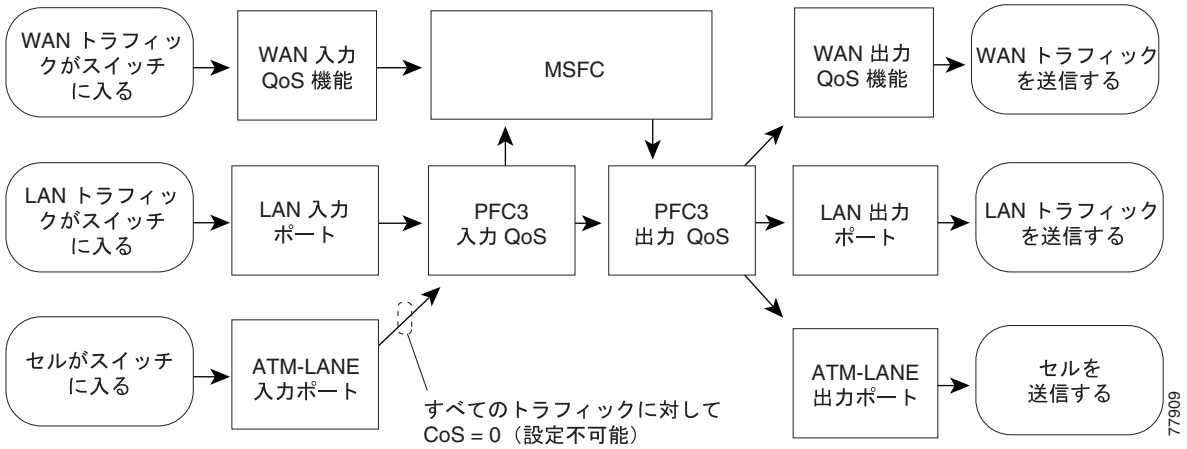
（注）　レイヤ 3 の IP パケットは、IP precedence 値または DSCP 値のどちらでも伝送できます。DSCP 値は IP precedence と同じ値に設定できるので、QoS ではどちらの値でも使用できます。

- *分類* ― トラフィックを選択することです。
- *マーキング* ― RFC 2475 に従い、レイヤ 3 の DSCP 値をパケットに設定する処理です。このマニュアルでは、マーキングの定義を拡大して、レイヤ 2 の CoS 値の設定までを含めています。
- *スケジューリング* ― キューにトラフィックを割り当てることです。QoS は、CoS 値に基づいてトラフィックを割り当てます。
- *輻輳回避* ― プライオリティの高い CoS 値のトラフィック用に入力および出力ポート容量を QoS で確保しておく処理です。QoS では、CoS 値ベースの廃棄スレッシュホールドによって輻輳回避を実現します。廃棄スレッシュホールドは、バッファ利用率であり、この割合に達すると、特定の CoS 値のトラフィックが廃棄され、プライオリティの高い CoS 値のトラフィック用にバッファが残されます。
- *ポリシング* ― トラフィック フローによって消費される帯域幅をスイッチで制限する処理です。ポリシングによって、トラフィックをマーキングするか、または廃棄することができます。
- 特に明記しないかぎり、*レイヤ3 スイッチング エンジン*は、次の両方を表します。
  - Layer 3 Switching Engine II（PFC2）を搭載した Supervisor Engine 2
  - Layer 3 Switching Engine WS-F6K-PFC（PFC）を搭載した Supervisor Engine 1
- Random Early Detection（RED; ランダム早期検出）は、廃棄スレッシュホールド アルゴリズムです。
- Shaped Round Robin（SRR）は、デキューイング アルゴリズムです。
- Weighted Random Early Detection（WRED; 重み付きランダム早期検出）は、廃棄スレッシュホールド アルゴリズムです。
- Weighted Round Robin（WRR; 重み付きラウンドロビン）は、デキューイング アルゴリズムです。
- Deficit Weighted Round Robin（DWRR）は、デキューイング アルゴリズムです。

フローチャート

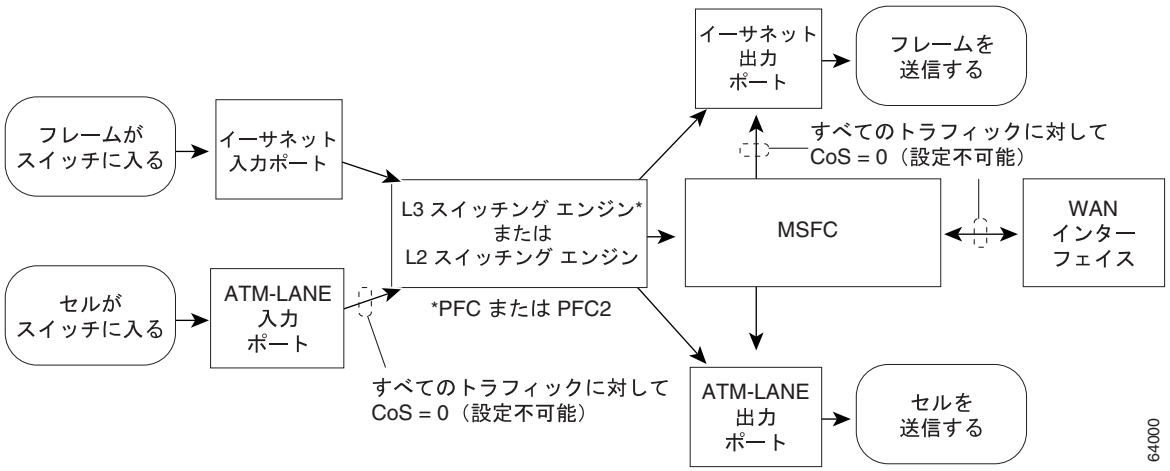
図 49-1 に、QoS 機能を使用したトラフィック フローを示します。図 49-2 ～ 図 49-9 には、QoS 機能を使用したトラフィック フローの詳細を示します。

図 49-1　PFC3 で QoS 機能を使用したトラフィック フロー



（注） PFC3 は WAN トラフィックでレイヤ 3 スイッチングを実現します。PFC3 は、Multilayer Switch Feature Card 3（MSFC3; マルチレイヤ スイッチ フィーチャ カード 3）によりソフトウェアで転送された入力 WAN トラフィックに QoS を提供できます。PFC3 は、LAN ポートからスイッチに入った、または MSFC3 によりソフトウェアで転送された出力 WAN トラフィックに QoS を提供できます。

図 49-2　PFC および PFC2 で QoS 機能を使用したトラフィック フロー



(注)

- PFC または PFC2 は、入力 WAN トラフィックのレイヤ 3 スイッチングを提供できます。
- PFC または PFC2 は、WAN トラフィックには QoS を提供しません。PFC または PFC2 では、PFC QoS は WAN トラフィックの ToS バイトを変更しません。
- レイヤ 3 スイッチングされた入力 LAN トラフィックは MSFC または MSFC2 を通過せず、レイヤ 3 スイッチング エンジンによって割り当てられた CoS 値を維持します。
- **show port capabilities** コマンドを入力すると、ポートのキュー構造が表示されます（詳細については「受信キュー」[p.49-13] および「送信キュー」[p.49-28] を参照）。

図 49-3　イーサネット入力ポートの分類、マーキング、スケジューリング、および輻輳回避

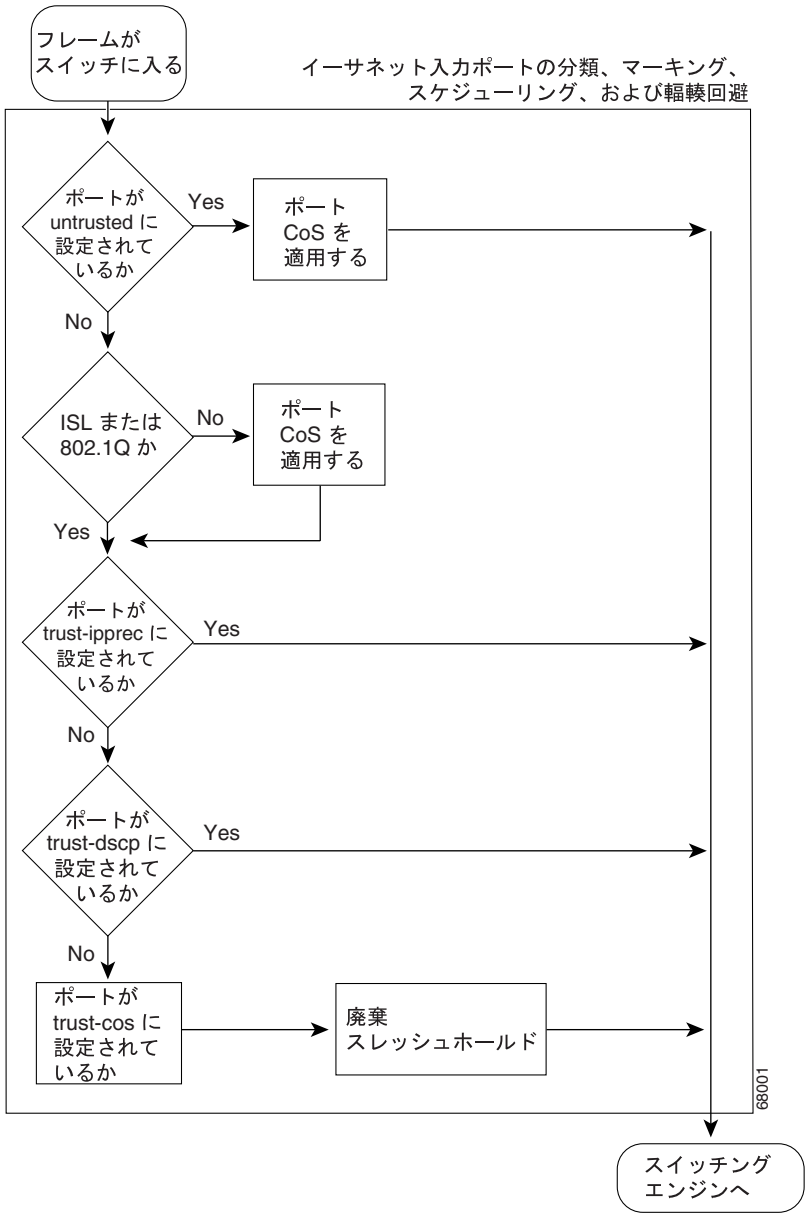


図 49-4　PFC3 の分類、マーキング、およびポリシング

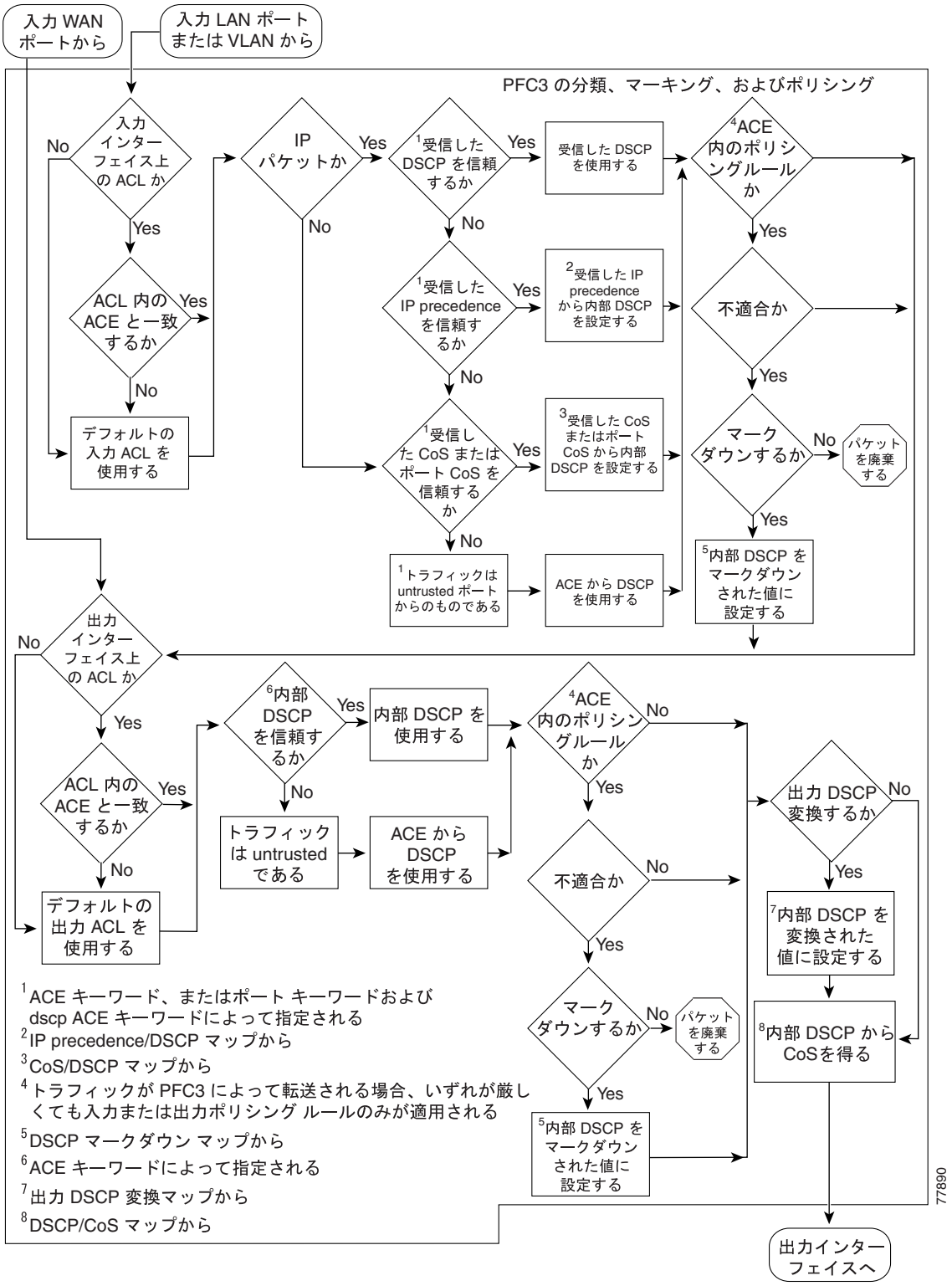
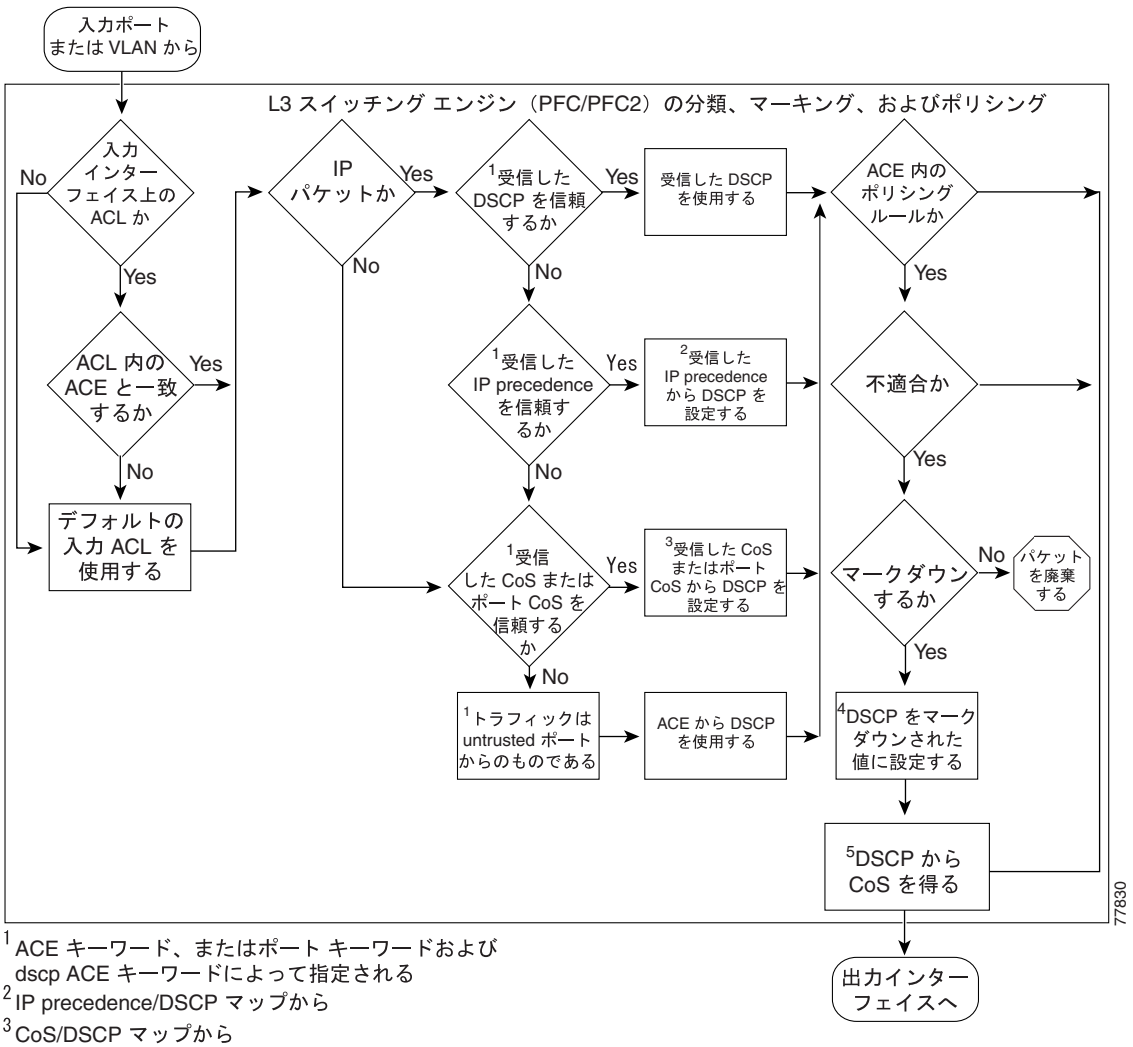


図 49-5　PFC および PFC2 の分類、マーキング、およびポリシング



[1] ACE キーワード、またはポート キーワードおよび dscp ACE キーワードによって指定される
[2] IP precedence/DSCP マップから
[3] CoS/DSCP マップから
[4] DSCP マークダウン マップから
[5] DSCP/CoS マップから

図 49-6　レイヤ 2 スイッチング エンジンの分類およびマーキング

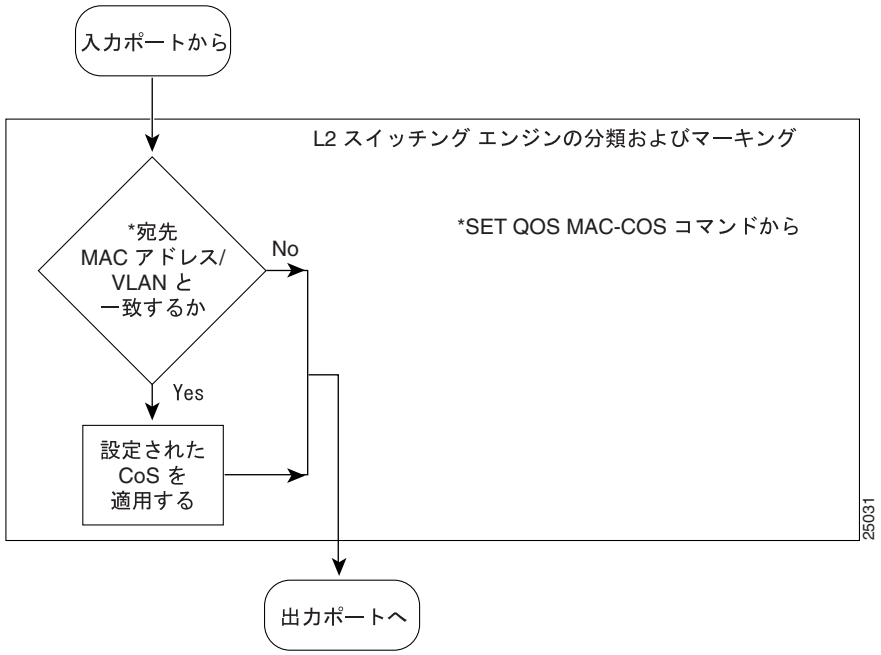


図 49-7　MSFC のマーキング（MSFC および MSFC2）

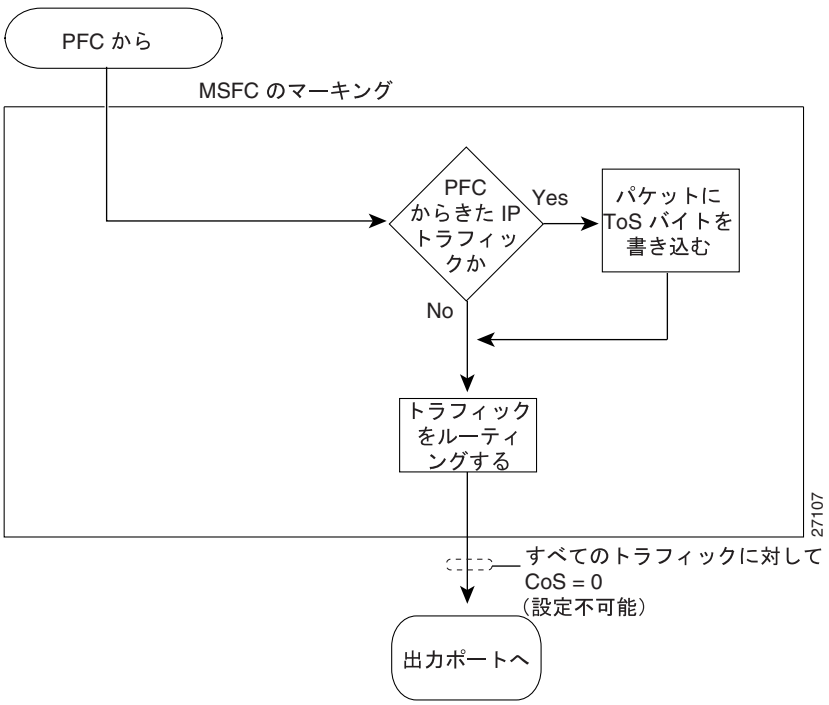


図 49-8　イーサネット出力ポートのスケジューリング、輻輳回避、およびマーキング

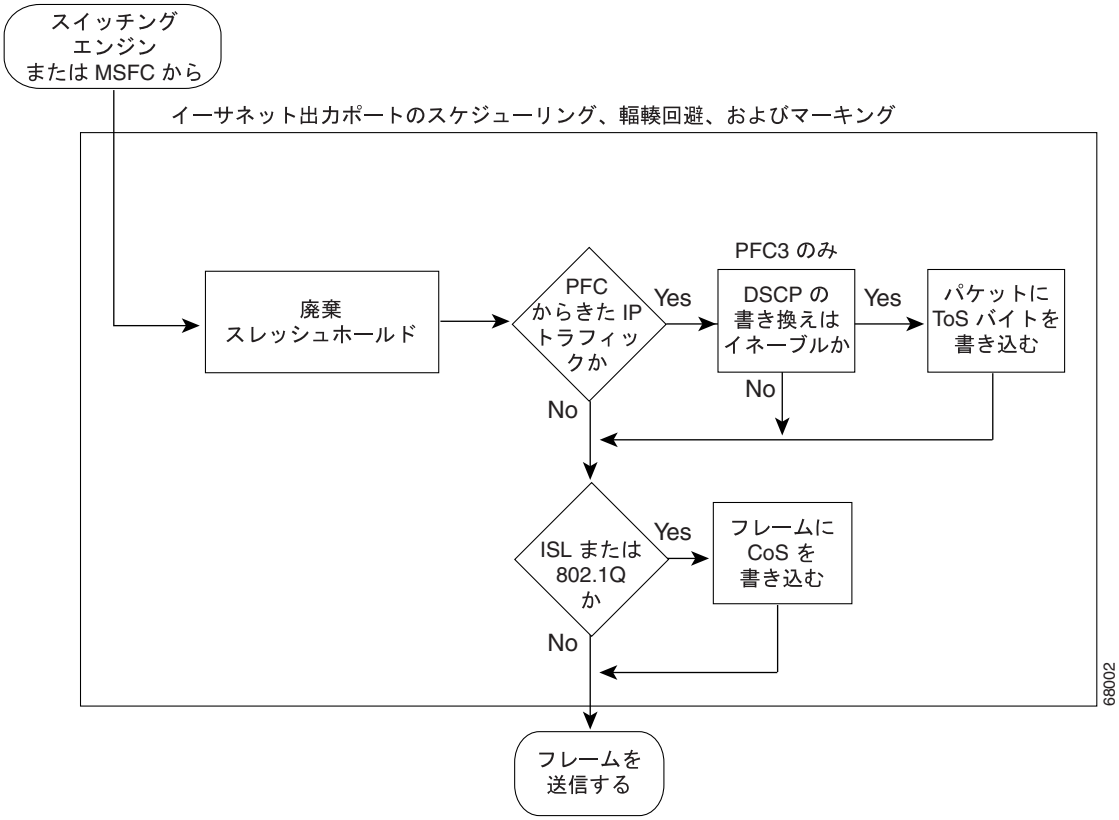
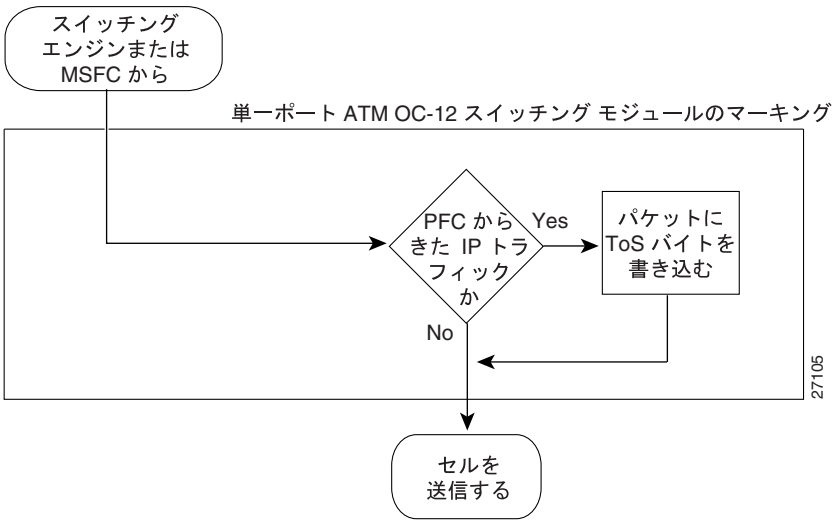


図 49-9　単一ポート ATM OC-12 スイッチング モジュールのマーキング



QoS フィーチャ セットの概要

スイッチ上の QoS フィーチャ セットは、スーパバイザ エンジンに搭載されているスイッチング エンジンによって決まります。スイッチング エンジンの設定を表示するには、スーパバイザ エンジンに対して **show module** コマンドを入力します。出力には、[Sub-Type] として次のいずれかが表示されます。

- PFC3B または PFC3BXL を搭載した Supervisor Engine 32（WS-SUP32-GE-3B）
- PFC3A/PFC3B/PFC3BXL を搭載した Supervisor Engine 720（WS-SUP720）
- Layer 3 Switching Engine II（WS-F6K-PFC2）を搭載した Supervisor Engine 2（WS-X6K-SUP2-2GE）
- 次のいずれかを搭載した Supervisor Engine 1（WS-X6K-SUP1A-2GE または WS-X6K-SUP1-2GE）
  - Layer 3 Switching Engine（WS-F6K-PFC）
  - Layer 2 Switching Engine II（WS-F6020A）
  - Layer 2 Switching Engine I（WS-F6020）

Layer 3 Switching Engine（WS-F6K-PFC）および Layer 3 Switching Engine II（WS-F6K-PFC2）は、同様のフィーチャ セットをサポートしています。2 種類のレイヤ 2 スイッチング エンジンは、同じ QoS フィーチャ セットをサポートしています。

他の 2 つのレイヤ 3 スイッチング エンジンがサポートする機能に加えて、PFC3A は次の機能をサポートしています。

- 出力 QoS
- 出力 DSCP 変換
- オプションの出力 DSCP の書き換え

ここでは、QoS フィーチャ セットについて説明します。

- イーサネット入力ポートの機能（p.49-10）
- レイヤ 3 スイッチング エンジンの機能（p.49-10）
- レイヤ 2 スイッチング エンジンの機能（p.49-11）
- イーサネット出力ポートの機能（p.49-11）
- 単一ポート ATM OC-12 スイッチング モジュールの機能（p.49-11）
- MSFC、MSFC2、または MSFC3（p.49-11）

イーサネット入力ポートの機能

使用するスイッチング エンジンの種類に関係なく、QoS はイーサネット入力ポートでレイヤ 2 の CoS 値を使用して、分類、マーキング、スケジューリング、および輻輳回避をサポートしています。イーサネット入力ポートでの分類、マーキング、スケジューリング、および輻輳回避では、レイヤ 3 の IP precedence 値または DSCP 値は使用されません。また、設定も行われません。レイヤ 3 スイッチング エンジンでは、イーサネット入力ポートの信頼状態を設定できます。レイヤ 3 の IP precedence または DSCP 値、レイヤ 2 の CoS 値を設定するときに、スイッチング エンジンによってこの信頼状態が使用されます。詳細については、「イーサネット入力ポートのマーキング、スケジューリング、輻輳回避、および分類」（p.49-12）を参照してください。

レイヤ 3 スイッチング エンジンの機能

PFC3A/PFC3B/PFC3BXL、PFC2、または PFC では、QoS は Access Control List（ACL; アクセス制御リスト）を使用して分類、マーキング、およびポリシングをサポートしています。

PFC3A/PFC3B/PFC3BXL は、入力トラフィックおよび出力トラフィックの両方で QoS を提供します。PFC2 および PFC は入力トラフィックでのみ QoS を提供します。

PFC3 では、QoS はマップ ベースの出力 DSCP 変換をサポートしています。これを使用すれば、出力トラフィックがポリシング ルールで処理されたあとにそれをリマークできます。さらに出力トラフィック内の受信した DSCP を保全するオプションをサポートしています。

ACL は一連の Access Control Entry（ACE; アクセス制御エントリ）からなり、ACE でレイヤ 2、3、4 の分類基準、マーキング ルール、およびポリサーを指定します。マーキングでは、レイヤ 3 の IP precedence または DSCP 値とレイヤ 2 の CoS 値を、受信した値または設定済みのレイヤ 2 またはレイヤ 3 の値に設定します。ポリシングでは、帯域幅限度を指定して、不適合トラフィックを廃棄、またはマーキングします。詳細については、「レイヤ 3 スイッチング エンジンにおける分類、マーキング、およびポリシング」（p.49-16）を参照してください。

レイヤ 3 スイッチング エンジンは処理中に、非 IP トラフィックを含むすべてのトラフィックに DSCP 値を対応付けます。詳細については、「内部 DSCP 値」（p.49-16）を参照してください。

レイヤ 2 スイッチング エンジンの機能

レイヤ 2 スイッチング エンジンでは、QoS はレイヤ 2 の宛先 MAC（メディア アクセス制御）アドレスおよび VLAN を使用してトラフィックを分類し、レイヤ 2 の CoS 値を使用してマーキングします。レイヤ 2 スイッチング エンジンの分類およびマーキングでは、レイヤ 3 の IP precedence または DSCP 値を使用することも設定することもありません。詳細については、「レイヤ 2 スイッチング エンジン搭載の Supervisor Engine 1 における分類およびマーキング」（p.49-27）を参照してください。

イーサネット出力ポートの機能

使用するスイッチング エンジンの種類に関係なく、QoS はレイヤ 2 の CoS 値を使用して、イーサネット出力ポートでのスケジューリングおよび輻輳回避をサポートしています。イーサネット出力ポートのマーキングでは、レイヤ 2 の CoS 値を設定します。レイヤ 3 スイッチング エンジンでは、レイヤ 3 の DSCP 値を設定します。詳細については、「イーサネット出力ポートのスケジューリング、輻輳回避、およびマーキング」（p.49-28）を参照してください。

単一ポート ATM OC-12 スイッチング モジュールの機能

単一ポート ATM OC-12 スイッチング モジュールからの入力インターフェイスは untrusted（信頼性がない）なので、QoS はそのインターフェイスから受信するすべてのトラフィックで、CoS を 0 に設定します。レイヤ 3 スイッチング エンジンでは、QoS は単一ポート ATM OC-12 スイッチング モジュールに送信される IP トラフィックに、レイヤ 3 の DSCP 値を使用してマーキングできます。

MSFC、MSFC2、または MSFC3

QoS は、MSFC に送信された IP トラフィックにレイヤ 3 の DSCP 値を使用してマーキングします。CoS は、MSFC から出力ポートに送信されるすべてのトラフィックで 0 です。

（注） レイヤ 3 スイッチングされたトラフィックは MSFC を通過せず、レイヤ 3 スイッチング エンジンによって割り当てられた CoS 値を維持します。

イーサネット入力ポートのマーキング、スケジューリング、輻輳回避、および分類

ここでは、イーサネット入力ポートのマーキング、スケジューリング、輻輳回避、および分類について説明します。

概要

イーサネット ポートの信頼状態によって、受信したトラフィックのマーキング、スケジューリング、および分類をどのように行うか、また、輻輳回避を実行するかどうかが決まります。各ポートの信頼状態は、次のキーワードのうちの 1 つで設定できます。

- **untrusted**（デフォルト）
- **trust-ipprec**（レイヤ 3 スイッチング エンジン専用 ― ギガビット イーサネットを除いて **1q4t** ポートではサポートされません）
- **trust-dscp**（レイヤ 3 スイッチング エンジン専用 ― ギガビット イーサネットを除いて **1q4t** ポートではサポートされません）
- **trust-cos**

（注） **1q4t** ポート上では（ギガビット イーサネットを除く）、**trust-cos** ポート キーワードを指定するとエラー メッセージが表示され、受信キューの廃棄スレッシュホールドがアクティブになり、（エラー メッセージで示されるように）トラフィックには **trust-cos** の信頼状態が適用されません。**trust-cos** 信頼状態を適用するには、入力トラフィックに対応する **trust-cos** ACL を設定する必要があります。

詳細については、「ポートの信頼状態の設定」（p.49-40）を参照してください。

上記のポート設定キーワードに加えて、レイヤ 3 スイッチング エンジンでは、QoS は **trust-ipprec**、**trust-dscp**、および **trust-cos** ACE キーワードを使用します。ACE キーワードとポート キーワードを混同しないでください。

untrusted　キーワードを指定して設定されたポートは、「untrusted　ポート」と呼ばれます。**trust-ipprec**、**trust-dscp**、または **trust-cos** キーワードを指定して設定されたポートは、「trusted（信頼性のある）ポート」と呼ばれます。QoS が入力ポートの輻輳回避を実行するのは、**trust-cos** キーワードを指定して設定されたポートだけです。

入力ポートのマーキング、スケジューリング、および輻輳回避では、レイヤ 2 の CoS 値が使用されます。入力ポートでのマーキング、スケジューリング、および輻輳回避では、レイヤ 3 の IP precedence 値または DSCP 値は使用されません。また、設定も行われません。

untrusted ポートでのマーキング

QoS は untrusted ポート経由で受信したすべてのフレームに、ポート CoS 値（デフォルトは 0）をマーキングします。QoS は、untrusted ポートに対して入力ポート輻輳回避を実行しません。トラフィックはそのままスイッチング エンジンに送られます。

trusted ポートでのマーキング

ISL フレームが trusted ポートを経由してスイッチに入ると、QoS がユーザ フィールドの下位 3 ビットを CoS 値として受け入れます。802.1Q フレームが trusted ポートからスイッチに入ると、QoS がユーザ プライオリティ ビットを CoS 値として受け入れます。QoS は他のフレーム タイプで受信したすべてのトラフィックに、ポートの CoS 値を使用してマーキングします。

ポート CoS 値は各イーサネット ポートについて設定できます。詳細については、「ポート CoS 値の設定」（p.49-41）を参照してください。

イーサネット入力ポートのスケジューリングおよび輻輳回避

QoS は、**untrusted**、**trust-ipprec**、または **trust-dscp** キーワードを指定して設定されたポートに対して、入力ポート輻輳回避を実行しません。トラフィックはそのままスイッチング エンジンに送られます。

QoS では、CoS 値に基づく受信キュー廃棄スレッシュホールドを使用して、**trust-cos** キーワードを指定して設定されたポートからスイッチに入るトラフィックの輻輳を回避します（詳細については「ポートの信頼状態の設定」[p.49-40] を参照）。

受信キュー

show port capabilities コマンドを入力すると、ポートのキュー構造が表示されます。コマンドにより、次のいずれかが表示されます。

- **rx-(1q8t)** は、標準キューが 1 つ、設定可能なテール廃棄スレッシュホールドが 8 つという意味です。
- **rx-(1q2t)** は、標準キューが 1 つ、設定可能、および設定不可能なテール廃棄スレッシュホールドが 1 つずつという意味です。
- **rx-(1q4t)** は、標準キューが 1 つ、設定可能なテール廃棄スレッシュホールドが 4 つという意味です。
- **rx-(1p1q4t)** は、完全優先キューが 1 つ、標準キューが 1 つ、設定可能なテール廃棄スレッシュホールドが 4 つという意味です。
- **rx-(1p1q0t)** は、完全優先キューが 1 つ、標準キューが 1 つ、設定不可能なスレッシュホールドが 1 つという意味です。
- **rx-(1p1q8t)** は、完全優先キューが 1 つ、標準キューが 1 つ、設定可能な WRED 廃棄スレッシュホールドが 8 つという意味です（**1p1q8t** ポート上の標準キューには、設定不可能なテール廃棄スレッシュホールドも 1 つあります）。

完全優先キューは、他のキューより優先的に処理されます。QoS は完全優先キュー内のトラフィックを処理してから、標準キューを処理します。QoS が標準キューを処理する場合、パケットの受信後、完全優先キューにトラフィックがあるかどうかを調べます。完全優先キュー内でトラフィックを検出すると、標準キューの処理を中断し、先に完全優先キュー内のすべてのトラフィックを処理してから、標準キューに戻ります。

入力スケジューリング

QoS は CoS 値に基づき、受信キューを利用してトラフィックのスケジューリングを行います。デフォルト設定では、PFC QoS は CoS 5 を持つすべてのトラフィックを（存在する場合）完全優先キューに割り当てます。PFC QoS は他のすべてのトラフィックを標準キューに割り当てます。完全優先キューが存在しない場合、PFC QoS はすべてのトラフィックを標準キューに割り当てます。

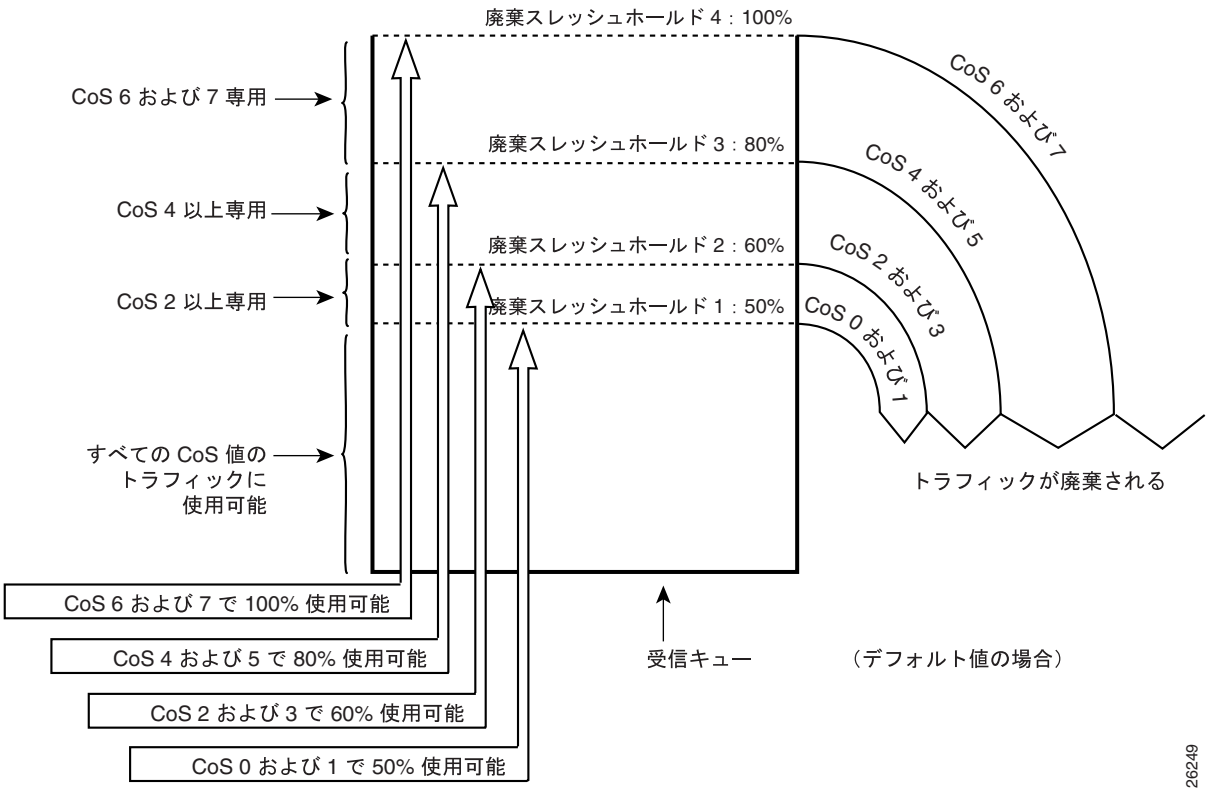
入力輻輳回避

trust-cos キーワードを指定して設定されているポートでは、QoS は CoS 値に基づく受信キュー廃棄スレッシュホールドを適用して、受信トラフィックの輻輳を回避します。デフォルトの CoS/ スレッシュホールド マッピングについては、「QoS のデフォルト設定」（p.49-30）を参照してください。

（注） 一部のポート タイプでは、CoS 値をキューにマッピングするか、またはキューとスレッシュホールドにマッピングして、テール廃棄と WRED 廃棄の両方のスレッシュホールドを使用するように、標準受信キューを設定できます。スイッチは、キューだけにマッピングされた CoS 値を伝送するトラフィックに対して、テール廃棄スレッシュホールドを使用します。WRED 廃棄スレッシュホールドの使用対象となるのは、キューとスレッシュホールドにマッピングされた CoS 値を伝送するトラフィックです。詳細については、「1p1q8t 受信キュー」（p.49-70）を参照してください。

図 49-10 に、**1q4t** ポートの廃棄スレッシュホールドを示します。廃棄スレッシュホールドは他の設定でも同様に機能します。

図 49-10　受信キューの廃棄スレッシュホールド



レイヤ 3 スイッチング エンジンにおけるイーサネット入力ポートの分類

untrusted、**trust-ipprec**、**trust-dscp**、および **trust-cos** ポート キーワードを使用すると、レイヤ 3 スイッチング エンジンによってマーキングされるトラフィックを、ポート単位で分類できます。

trust-ipprec および **trust-dscp** キーワードは、レイヤ 3 スイッチング エンジンでのみサポートされ、ギガビット イーサネットを除く **1q4t** ポート上ではサポートされていません。**1q4t** ポート上では（ギガビット イーサネットを除く）、**trust-cos** ポート キーワードを指定するとエラー メッセージが表示され、受信キューの廃棄スレッシュホールドがアクティブになり、（エラー メッセージで示されるように）トラフィックには **trust-cos** の信頼状態が適用されません。**trust-cos** 信頼状態を適用するには、入力トラフィックに対応する **trust-cos** ACL を設定する必要があります。

ポート単位の分類に加えて、ポートの設定に関係なく、パケット単位でトラフィックを分類する ACE（IP および Internetwork Packet Exchange [IPX] トラフィックの場合、「名前付き IP ACL」[p.49-46] および「名前付き IPX ACL の作成または変更」[p.49-51] を参照）、またはフレーム単位でトラフィックを分類する ACE（その他のトラフィックの場合、「名前付き MAC ACL の作成または変更」[p.49-52] を参照）を作成できます（「マーキング ルール」[p.49-22] を参照）。

ポート単位の分類に基づいてトラフィックをマーキングするには、**dscp** ACE キーワードを指定した ACE とトラフィックが一致しなければなりません（「マーキング ルール」[p.49-22] を参照）。デフォルト ACL 内の ACE のデフォルト設定には、**dscp** ACE キーワードが指定されています。表 49-1 に、ポート単位の分類とそれによって実行されるマーキング ルールを示します。

表 49-1　ポート単位の分類に基づくマーキング

ポート キーワード	ACE キーワード	マーキング ルール
untrusted	**dscp**	ACE で指定された内部 DSCP 値および出力 DSCP 値を設定します。
trust-ipprec	**dscp**	IP トラフィックの場合、受信したレイヤ 3 IP precedence 値に基づいて内部 DSCP 値および出力 DSCP 値を設定します。その他のトラフィックの場合、受信したレイヤ 2 CoS 値またはポートのレイヤ 2 CoS 値に基づいて内部 DSCP 値および出力 DSCP 値を設定します。 （注）― **trust-ipprec** ポート キーワードを指定すると、QoS は IP precedence ビットだけを使用します。DSCP 値を指定されたトラフィックが、**trust-ipprec** ポート キーワードを設定したポートを介してスイッチに入ると、DSCP 値の上位 3 ビットが IP precedence 値として解釈され、残りの DSCP 値は無視されます。
trust-dscp	**dscp**	IP トラフィックの場合、受信したレイヤ 3 DSCP 値に基づいて内部 DSCP 値および出力 DSCP 値を設定します。その他のトラフィックの場合、受信したレイヤ 2 CoS 値またはポートのレイヤ 2 CoS 値に基づいて内部 DSCP 値および出力 DSCP 値を設定します。
trust-cos	**dscp**	受信したレイヤ 2 CoS 値またはポートのレイヤ 2 CoS 値に基づいて内部 DSCP 値および出力 DSCP 値を設定します。

QoS は、設定可能なマッピング テーブルを使用して内部 DSCP および出力 DSCP を設定します。DSCP は、それぞれ 3 ビット値である CoS と IP precedence からなる 6 ビット値です（詳細については「内部 DSCP 値」[p.49-16] および「DSCP 値マッピングの設定」[p.49-71] を参照）。

レイヤ 3 スイッチング エンジンにおける分類、マーキング、およびポリシング

(注)　レイヤ 3 スイッチング エンジンを使用する Catalyst 6500 シリーズ スイッチが QoS を実行するのは、フレーム タイプが Ethernet_II、Ethernet_802.3、Ethernet_802.2、および Ethernet_SNAP の場合に限られます。

ここではレイヤ 3 スイッチング エンジンにおける分類、マーキング、およびポリシングについて説明します。

(注)　レイヤ 3 スイッチング エンジンでの分類には、レイヤ 2、3、および 4 の値が使用されます。レイヤ 3 スイッチング エンジンでのマーキングには、レイヤ 2 の CoS 値およびレイヤ 3 の IP precedence 値または DSCP 値が使用されます。

内部 DSCP 値

ここでは、内部 DSCP 値について説明します。

内部 DSCP の作成元

すべてのトラフィック（非 IP トラフィックを含む）のプライオリティは、処理中、内部 DSCP 値で表されます。QoS は、次のものに基づいて内部 DSCP 値を作成します。

- **trust-cos** トラフィックの場合、受信したレイヤ 2 CoS 値またはポートのレイヤ 2 CoS 値（untrusted ポートからのトラフィックには、ポートの CoS 値が使用されます。untrusted ポートからのトラフィックが **trust-cos** ACL と一致する場合は、QoS はポートの CoS 値から内部 DSCP 値を作成します）
- **trust-ipprec** トラフィックの場合、受信した IP precedence
- **trust-dscp** トラフィックの場合、受信した DSCP 値
- **untrusted** トラフィックの場合、ポートの CoS または設定された DSCP 値

トラフィックの信頼状態は、一致する ACE で特に設定されていないかぎり、入力ポートの信頼状態と同じです。

(注) **trust-cos** ACL は、untrusted ポートからのトラフィックで受信した CoS を復元できません。untrusted ポートからのトラフィックには、常にポート CoS 値が含まれます。

QoS は、設定可能なマッピング テーブルを使用して 6 ビットの内部 DSCP 値を作成します。DSCP は、それぞれ 3 ビット値である CoS または IP precedence からなる 6 ビット値です（詳細については「受信 CoS 値と内部 DSCP 値のマッピング」[p.49-71] または「受信 CoS 値と内部 DSCP 値のマッピング」[p.49-72] を参照）。

出力 DSCP および CoS の作成元

出力 IP トラフィックについては、QoS は内部 DSCP 値（IP precedence の値と同じ値に設定できる）から ToS バイトを作成し、出力ポートに送信します。その ToS バイトが IP パケットに書き込まれます。**trust-dscp** および **untrusted** IP トラフィックの場合、ToS バイトには、受信した ToS バイトの下位 2 ビットが含まれます。

すべての出力トラフィックについて、QoS は、設定可能なマッピング テーブルを使用して、トラフィックと対応付けられた内部 DSCP 値から CoS 値を作成します（「内部 DSCP 値と出力 CoS 値のマッピング」[p.49-73] を参照）。QoS はイーサネット出力ポートに CoS 値を送信し、それがスケジューリングに使用され、ISL フレームと 802.1Q フレームに書き込まれます。

ACL

QoS は、ACE からなる ACL を使用します。ACE は、分類基準、マーキング ルール、およびポリサーを指定します。QoS は受信したトラフィックと ACL 内の ACE を、一致するまで比較します。トラフィックが ACE に指定された分類基準と一致すると、QoS は ACE の指定に従ってパケットのマーキングとポリシングを行い、それ以上は比較を行いません。

ACL には、IP（レイヤ 3 スイッチング エンジンでの場合）、IPX、および MAC の 3 つのタイプがあります。QoS は各タイプ（IP、IPX、および MAC）のトラフィックを対応する ACL タイプとだけ比較します（表 49-2 を参照）。

表 49-2　サポートする Ethertype フィールド値

ACL タイプ	Ethertype フィールド値	プロトコル
IP	0x0800	IP
IPX[1]	0x8137 および 0x8138	IPX
MAC[2]	0x0600 および 0x0601	XNS
	0x0BAD および 0x0BAF	Banyan VINES
	0x6000 ～ 0x6009 および 0x8038 ～ 0x8042	DECnet
	0x809b および 0x80f3	AppleTalk

1. PFC3 は、IPX トラフィックには QoS を提供しません。
2. Ethertype パラメータを含まない QoS MAC ACL は、Ethertype フィールドのどの値を持つトラフィックとも一致します。したがって、IP および IPX を除く任意のトラフィックに、MAC レベルの QoS を適用できます。

QoS は、ユーザが作成した*名前付き* ACL（ACE が順番に並べられたリストで構成されている）、およびユーザ側で設定できる*デフォルト*の ACL（ACE が 1 つだけ指定されている）をサポートしています。

名前付き ACL

新しい ACL 名を指定して ACE を入力すると、名前付き ACL が作成されます。既存の ACL 名を指定して ACE を入力すると、既存の ACL に ACE が追加されます。

名前付き ACL 内の ACE ごとに、分類基準を指定できます。分類基準は、具体的な値にすることも、ワイルドカードを使用することもできます（詳細については「ACL の作成または変更」[p.49-45] を参照）。

ここでは、名前付き ACL に指定できる分類基準について説明します。

- IP ACE レイヤ 3 の分類基準（p.49-18）
- IP ACE レイヤ 4 プロトコルの分類基準（p.49-18）
- IP ACE レイヤ 4 TCP の分類基準（p.49-19）
- IP ACE レイヤ 4 UDP の分類基準（p.49-19）
- IP ACE レイヤ 4 ICMP の分類基準（p.49-20）
- IP ACE レイヤ 4 IGMP の分類基準（p.49-21）
- IPX ACE の分類基準（p.49-21）
- MAC ACE レイヤ 2 の分類基準（p.49-21）

IP ACE レイヤ 3 の分類基準

次のレイヤ 3 パラメータを指定すると、特定のレイヤ 3 値を持つトラフィックと一致する IP ACE を作成できます（「名前付き IP ACL」[p.49-46] を参照）。

- IP 送信元アドレスおよびマスク。具体的な値として入力するか、**any** キーワードを指定するか、または **host** キーワードおよびホスト アドレスを指定します。
- IP 宛先アドレスおよびマスク。具体的な値として入力するか、**any** キーワードを指定するか、または **host** キーワードおよびホスト アドレスを指定します。
- DSCP 値（0 ～ 63）、数値（0 ～ 7）で指定した IP precedence、または次のキーワードで指定した IP precedence
  - **Network**（IP precedence 7）
  - **Internet**（IP precedence 6）
  - **Critical**（IP precedence 5）
  - **Flash-override**（IP precedence 4）
  - **Flash**（IP precedence 3）
  - **Immediate**（IP precedence 2）
  - **Priority**（IP precedence 1）
  - **Routine**（IP precedence 0）

（注） DSCP または IP precedence 値パラメータが指定されていない IP ACE は、すべての DSCP または IP precedence 値と一致します。

IP ACE レイヤ 4 プロトコルの分類基準

レイヤ 4 プロトコル パラメータを指定すると、特定のレイヤ 4 プロトコル トラフィックと一致する IP ACE を作成できます（「その他のレイヤ 4 プロトコル用の IP ACL」[p.49-49] を参照）。プロトコルは、数字（0 ～ 255）または次のキーワードで指定します。**ahp**（51）、**eigrp**（88）、**esp**（50）、**gre**（47）、**igrp**（9）、**icmp**（1）、**igmp**（2）、**igrp**（9）、**ip**（0）、**ipinip**（4）、**nos**（94）、**ospf**（89）、**pcp**（108）、**pim**（103）、**tcp**（6）、**udp**（17）です。

(注)　レイヤ 4 プロトコル パラメータが指定されていない IP ACE、または **ip** キーワードが指定されている IP ACE は、すべての IP トラフィックと一致します。

IP ACE レイヤ 4 TCP の分類基準

TCP の送信元ポート、宛先ポート、またはその両方のパラメータを指定することにより、特定の TCP ポートのトラフィックと一致する TCP ACE を作成できます（詳細については「TCP トラフィック用の IP ACE」[p.49-46] を参照）。

TCP ポート パラメータは数字（0 ～ 65535）または次のキーワードで指定します。

キーワード	ポート		キーワード	ポート		キーワード	ポート		キーワード	ポート
bgp	179		**ftp**	21		**lpd**	515		**telnet**	23
chargen	19		**ftp-data**	20		**nntp**	119		**time**	37
daytime	13		**gopher**	70		**pop2**	109		**uucp**	540
discard	9		**hostname**	101		**pop3**	110		**whois**	43
domain	53		**irc**	194		**smtp**	25		**www**	80
echo	7		**klogin**	543		**sunrpc**	111			
finger	79		**kshell**	544		**tacacs**	49			

(注)　レイヤ 4 TCP ポート パラメータが指定されていない TCP ACE は、すべての TCP トラフィックと一致します。

IP ACE レイヤ 4 UDP の分類基準

UDP ポート パラメータを指定することにより、特定の UDP 送信元ポート、宛先ポート、またはその両方のポートのトラフィックと一致する UDP ACE を作成できます。詳細については、「UDP トラフィック用の IP ACE」（p.49-47）を参照してください。

UDP ポート パラメータは数字（0 ～ 65535）または次のキーワードで指定します。

キーワード	ポート		キーワード	ポート		キーワード	ポート		キーワード	ポート
biff	512		**echo**	7		**rip**	520		**talk**	517
bootpc	68		**mobile-ip**	434		**snmp**	161		**tftp**	69
bootps	67		**nameserver**	42		**snmptrap**	162		**time**	37
discard	9		**netbios-dgm**	138		**sunrpc**	111		**who**	513
dns	53		**netbios-ns**	137		**syslog**	514		**xdmcp**	177
dnsix	195		**ntp**	123		**tacacs**	49			

(注)　レイヤ 4 UDP ポート パラメータが指定されていない UDP ACE は、すべての UDP トラフィックと一致します。

IP ACE レイヤ 4 ICMP の分類基準

Internet Control Management Protocol（ICMP）タイプ、さらに任意で ICMP コードを指定することにより、特定の ICMP メッセージが含まれているトラフィックと一致する ICMP ACE を作成できます。詳細については、「ICMP トラフィック用の IP ACE」（p.49-48）を参照してください。

ICMP タイプとコードは数字（0 ～ 255）または次のキーワードで指定します。

キーワード	タイプ	コード	キーワード	タイプ	コード
administratively-prohibited	3	13	*net-tos-unreachable*	3	11
alternate-address[1]	6	—	*net-unreachable*	3	0
conversion-error	31	0	*network-unknown*	3	6
dod-host-prohibited	3	10	*no-room-for-option*	12	2
dod-net-prohibited	3	9	*option-missing*	12	1
echo	8	0	*packet-too-big*	3	4
echo-reply	0	0	*parameter-problem*	12	0
general-parameter-problem[1]	12	—	*port-unreachable*	3	3
host-isolated	3	8	*precedence-unreachable*	3	15
host-precedence-unreachable	3	14	*protocol-unreachable*	3	2
host-redirect	5	1	*reassembly-timeout*	11	1
host-tos-redirect	5	3	*redirect*[1]	5	—
host-tos-unreachable	3	12	*router-advertisement*	9	0
host-unknown	3	7	*router-solicitation*	10	0
host-unreachable	3	1	*source-quench*	4	0
information-reply	16	0	*source-route-failed*	3	5
information-request	15	0	*time-exceeded*[1]	11	—
mask-reply	18	0	*timestamp-reply*	14	0
mask-request	17	0	*timestamp-request*	13	0
mobile-redirect	32	0	*traceroute*	30	0
net-redirect	5	0	*ttl-exceeded*	11	0
net-tos-redirect	5	2	*unreachable*[1]	3	—

1. すべてのコード値と一致

（注） レイヤ 4 ICMP の*タイプ*パラメータだけを指定した ICMP ACE は、その*タイプ*値に対応するすべての*コード*値と一致します。レイヤ 4 ICMP のタイプおよびコード パラメータが指定されていない ICMP ACE は、すべての ICMP トラフィックと一致します。

IP ACE レイヤ 4 IGMP の分類基準

IGMP のタイプ パラメータを指定すると、特定の IGMP メッセージが含まれているトラフィックと一致する IGMP ACE を作成できます（詳細については「IGMP トラフィック用の IP ACE」[p.49-48] を参照）。プロトコルは、数字（0 ～ 255）または次のキーワードで指定します。**host-query**（1）、**host-report**（2）、**dvmrp**（3）、**pim**（4）、**trace**（5）です。

（注）

- IGMP スヌーピングがイネーブルの場合、QoS はマルチキャスト トラフィックをサポートしています。
- IGMP スヌーピングがイネーブルの場合、QoS は IGMP トラフィックをサポートしていません。
- QoS は、バージョン 1 の 4 ビットの Type フィールドを使用した IGMP 分類をサポートしています。
- レイヤ 4 IGMP タイプ パラメータが指定されていない IGMP ACE は、すべての IGMP トラフィックと一致します。

IPX ACE の分類基準

（注）

PFC3 は、IPX トラフィックには QoS を提供しません。MAC ACL を使用して IPX トラフィックをフィルタリングする方法の詳細については、「MAC ACE レイヤ 2 の分類基準」（p.49-21）を参照してください。

次のパラメータを指定すると、特定の IPX トラフィックと一致する IPX ACE を作成できます（「名前付き IPX ACL の作成または変更」[p.49-51] を参照）。

- IPX 送信元ネットワーク（-1 はすべてのネットワーク番号と一致）
- プロトコル。数字（0 ～ 255）またはキーワードで指定します。**any**、**ncp**（17）、**netbios**（20）、**rip**（1）、**sap**（4）、**spx**（5）です。
- IPX ACE は、次のオプション パラメータをサポートしています。
  - IPX 宛先ネットワーク（-1 はすべてのネットワーク番号と一致）
  - IPX 宛先ネットワークを指定した場合、IPX ACE は次のオプション パラメータをサポートしています。IPX 宛先ネットワーク マスク（-1 はすべてのネットワーク番号と一致）、IPX 宛先ノード、および IPX 宛先ノード マスクです。

MAC ACE レイヤ 2 の分類基準

次のレイヤ 2 パラメータを指定すると、特定のイーサネット トラフィックと一致する MAC ACE を作成できます（「名前付き MAC ACL の作成または変更」[p.49-52] を参照）。

- イーサネット送信元アドレス、宛先アドレス、およびマスク。具体的な値として入力するか、**any** キーワードを指定するか、または **host** キーワードおよびホスト イーサネット アドレスを指定します。
- 任意で次のリストに含まれる Ethertype パラメータ
  - 0x809B（または **ethertalk**）
  - 0x80F3（または **aarp**）
  - 0x6001（または **dec-mop-dump**）
  - 0x6002（または **dec-mop-remote-console**）

- 0x6003（または **dec-phase-iv**）
- 0x6004（または **dec-lat**）
- 0x6005（または **dec-diagnostic-protocol**）
- 0x6007（または **dec-lavc-sca**）
- 0x6008（または **dec-amber**）
- 0x6009（または **dec-mumps**）
- 0x8038（または **dec-lanbridge**）
- 0x8039（または **dec-dsm**）
- 0x8040（または **dec-netbios**）
- 0x8041（または **dec-msdos**）
- 0x8042（キーワードなし）
- 0x0BAD（キーワードなし）
- 0x0baf（または **banyan-vines-echo**）
- 0x0600（または **xerox-ns-idp**）

• PFC3A では、任意で次のリストに含まれる Ethertype パラメータ
- 0x8137（または **ipx-arpa**）
- 非 ARPA IPX では 0xffff

Ethertype パラメータを含まない QoS MAC ACL は、Ethertype フィールドのどの値を持つトラフィックとも一致します。したがって、IP および IPX を除く任意のトラフィックに、MAC レベルの QoS を適用できます。

デフォルトの ACL

IP、さらにレイヤ 3 スイッチング エンジンでは IPX および MAC トラフィックに 1 つずつ、3 種類のデフォルト ACL があります。各 ACL には、設定可能なマーキング ルールと設定可能なポリサーを指定した ACE が 1 つだけあります。デフォルトの ACL には、すべてのトラフィックと一致する分類基準があります。この分類基準を設定することはできません。QoS は、サポート対象の Ethertype フィールド値を持ちながら、名前付き ACL と一致しないトラフィックをデフォルトの ACL と比較します。一致しない IP トラフィックは、デフォルトの IP ACL と一致します。一致しない IPX トラフィックは、デフォルトの IPX ACL と一致します。一致しないイーサネット トラフィックは、デフォルトの MAC ACL と一致します。

（注） デフォルトの ACL がすべてのトラフィックと一致するので、すべてのトラフィックは ACL 内の 1 つの ACE（名前付き ACL 内の ACE またはデフォルト ACL のいずれか）と一致します。

マーキング ルール

（注） PFC2 は、IPX または MAC トラフィックをマーキングできません。PFC3 は、IPX トラフィックに QoS を提供しません。

マーキング ルールでは、トラフィックが ACE のフィルタリング パラメータと一致したときに、QoS がトラフィックをどのようにマーキングするかを指定します（「ACE 名、マーキング ルール、ポリシング、およびフィルタリングの構文」[p.49-45] を参照）。QoS は、4 種類のマーキング ルールをサポートしています。このマーキング ルールは、**trust-dscp**、**trust-ipprec**、**trust-cos**、および **dscp** の 4 つの ACE キーワードで指定されます。各 ACE に、キーワードをどれか 1 つ指定します。

マーキング ルールは次のとおりです。

- **trust-dscp**（IP ACL 専用）― 受信した DSCP 値に基づいて内部 DSCP および出力 DSCP を設定するように、QoS に指示します（詳細については「内部 DSCP 値」[p.49-16] を参照）。
- **trust-ipprec**（IP ACL 専用）― 受信した IP precedence 値に基づいて内部 DSCP および出力 DSCP を設定するように、QoS に指示します。

（注）　**trust-ipprec** ポート キーワードを指定すると、QoS は IP precedence ビットだけを使用します。DSCP 値を指定されたトラフィックが、**trust-ipprec** ポート キーワードを設定したポートを介してスイッチに入ると、DSCP 値の上位 3 ビットが IP precedence 値として解釈され、残りの DSCP 値は無視されます。

- **trust-cos**（PFC2 では IPX および MAC を除くすべての ACL、PFC3 では IPX を除くすべての ACL）― 受信した CoS 値またはポートの CoS 値に基づいて内部 DSCP および出力 DSCP を設定するように、QoS に指示します。**trust-cos** キーワードを使用して設定されたポートからのトラフィックでは、QoS は ISL フレームおよび 802.1Q フレームで受信した CoS 値を使用します。それ以外の場合、QoS はポートで設定されている CoS 値を使用します（デフォルト値は 0）。
- **dscp**（PFC2 では IPX および MAC を除くすべての ACL、PFC3 では IPX を除くすべての ACL）― ポートの trust キーワードの指定に従ってトラフィックをマーキングするように、QoS に指示します。
  - **trust-dscp** ポート キーワードを使用して設定された入力ポートからの IP トラフィックでは、**dscp** ACE キーワードが指定されていることにより、QoS は受信した DSCP 値に基づいて内部 DSCP 値および出力 DSCP 値を設定します。非 IP トラフィックの場合、QoS は受信した CoS 値またはポートの CoS 値に基づいて、DSCP を設定します。
  - **trust-ipprec** ポート キーワードを使用して設定された入力ポートからの IP トラフィックでは、**dscp** ACE キーワードが指定されていることにより、QoS は受信した IP precedence 値に基づいて内部 DSCP 値および出力 DSCP 値を設定します。非 IP トラフィックの場合、QoS は受信した CoS 値またはポートの CoS 値に基づいて DSCP 値を設定します。
  - **trust-cos** ポート キーワードを使用して設定された入力ポートからの IP トラフィックでは、**dscp** ACE キーワードが指定されていることにより、QoS は受信した CoS 値またはポート CoS 値に基づいて内部 DSCP 値および出力 DSCP 値を設定します。
  - **untrusted** ポート キーワードを使用して設定された入力ポートからの IP トラフィックでは、**dscp** ACE キーワードが指定されていることにより、QoS は ACE の DSCP 値に基づいて内部 DSCP 値および出力 DSCP 値を設定します。

（注）　デフォルト ACL 内の ACE のデフォルト設定には、ポート単位のトラフィック分類をサポートしている **dscp** ACE キーワードが指定されています。デフォルト値を使用すると、デフォルト ACL 内の ACE が、**untrusted** ポート キーワードを使用して設定された入力ポートからのトラフィックに、DSCP ゼロを適用します。

QoS は、設定可能なマッピング テーブルを使用して DSCP 値を設定します。DSCP 値は、それぞれ 3 ビット値である CoS と IP precedence からなる 6 ビット値です（詳細については「受信 CoS 値と内部 DSCP 値のマッピング」[p.49-71] および「受信 CoS 値と内部 DSCP 値のマッピング」[p.49-72] を参照）。

ポリサー

名前付きポリサーを作成し、帯域幅利用限度を指定できます。ACE にポリサー名を指定することにより、この限度をトラフィックに適用できます（詳細については「ポリサーの作成」[p.49-42] を参照）。

ポリシングでは、トークン バケット方式が使用されます。パケットが到着したとき、そのパケットのサイズ（バイト単位）がバケット レベルに加算されます。0.25 ミリ秒ごとに、トークン レートに等しい値がバケット レベルから差し引かれます。

帯域幅利用限度は、平均速度および最大バースト サイズで指定します。このような限度を超えるパケットは、「不適合」となります。トラフィックが平均速度で流れ、バースト サイズを超えないかぎりそのトラフィックは適合です。

PFC および PFC2 では、ポリシング レートはレイヤ 3 パケット サイズを使用します。PFC3 では、ポリシング レートはレイヤ 2 フレーム サイズを使用します。

各ポリサーで、不適合パケットを廃棄するのか、それとも新しい DSCP 値を適用するのかを指定します（新しい DSCP 値を適用することを「マークダウン」といいます）。不適合パケットは、元のプライオリティを維持しないので、適合パケットが消費した帯域幅の一部とはみなされません。

QoS はすべてのポリサーで、設定可能なテーブルを使用し、受信した DSCP 値をマークダウンされる DSCP 値にマッピングします（詳細については「DSCP マークダウン値のマッピング」[p.49-73] を参照）。マークダウンが発生すると、QoS はこのテーブルからマークダウンされる DSCP 値を取得します。ユーザが個々のポリサーで、マークダウンされる DSCP 値を指定することはできません。

（注） デフォルトでは、マークダウンが発生しないようにマークダウン　テーブルが設定されます。マークダウン DSCP 値は受信 DSCP 値と同じです。マークダウンを可能にするには、ネットワークに合わせてテーブルを適切に設定します。

ポリサーを作成するときには、ポリサーごとに固有の名前を付け、その名前を使用して、ACE にポリサーを組み込みます。同じポリサーを複数の ACE で使用できます。

次のポリサーを作成できます。

- マイクロフロー（microflow）― QoS は、マイクロフロー ポリサーで指定された帯域幅限度を、そのマイクロフロー ポリサーを使用する ACE と一致するフローごとに個別に適用します。最大 63 のマイクロフロー ポリサーを作成できます。
- 集約（aggregate）― QoS は、集約ポリサーで指定された帯域幅限度を、その集約ポリサーを使用する ACE と一致するすべてのフローに累積方式で適用します。最大 1023 の集約ポリサーを作成できます。
- PFC2 および PFC3A では、標準レートおよび超過レートのデュアル レート集約ポリサーを指定できます。
  - 標準レート ― このレートを超えるパケットがマークダウンされます。
  - 超過レート ― このレートを超えるパケットは、マークダウンされるか、廃棄指示フラグの指定に従って廃棄されます。

（注） 廃棄指示フラグは、超過レート ポリサーに適用され、標準レート ポリサーには設定できません。標準レート集約ポリサーに対する廃棄指示フラグの効果を実現するには、超過レートを標準レートと同じに設定し、廃棄指示フラグを設定します。または、超過レートを指定せずに標準レートを設定すると、廃棄指示フラグが使用可能状態であれば、自動的に超過レートが標準レートと同じに設定されます。

各 ACE にマイクロフロー ポリサーおよび集約ポリサーの両方を含めると、単独の帯域幅使用率と、他のフローと合算された帯域幅使用率の両方に基づいて、フローのポリシングを行うことができます。

たとえば、グループの個々のフローに適した帯域幅限度を設定して、[group_individual] というマイクロフロー ポリサーを作成し、さらにグループ全体として適切な帯域幅限度を設定して、[group_all] という集約ポリサーを作成できます。グループのトラフィックと一致する ACE に、この両方のポリサーを含めます。この組み合わせは、個々のメンバーには個別に作用し、グループには累積方式で作用します。

ACE にマイクロフロー ポリサーおよび集約ポリサーの両方が含まれている場合、QoS はどちらかのポリサーに基づいて不適合ステータスに対応し、ポリサーの指定に従って新しい DSCP 値を適用するか、またはパケットを廃棄します。両方のポリサーから不適合ステータスが返され、かつどちらかのポリサーでパケットの廃棄が指定されている場合、パケットは廃棄されます。それ以外の場合は、新しい DSCP 値が適用されます。

ポリサーの作成時には、次の注意事項に従ってください。

- IP ACE には、マイクロフロー ポリサーを指定できます。マイクロフロー ポリサーは、IPX または MAC の ACE には指定できません。IPX および MAC の ACE がサポートしているのは集約ポリサーだけです。
- デフォルトの設定では、マイクロフロー ポリサーは、ブリッジド トラフィックには影響しません。ブリッジド トラフィックのマイクロフロー ポリシングをイネーブルにするには、**set qos bridged-microflow-policing** コマンドを入力します（詳細については「ブリッジド トラフィックに対するマイクロフロー ポリシングのイネーブル化およびディセーブル化」[p.49-61] を参照）。
- Layer 3 Switching Engine II では、マイクロフロー ポリシングを実行する場合には、ブリッジド トラフィックのマイクロフロー ポリシングをイネーブルにする必要があります。
- MSFC では、QoS は Multilayer Switching（MLS; マルチレイヤ スイッチング）候補フレームに対してマイクロフロー ポリサーを適用しません（MSFC2 は候補フレームおよびイネーブル フレームを使用しません）。
- 結果が矛盾しないように、同じ集約ポリサーを備えている ACE は、すべて同じ ACE キーワードを使用する必要があります。ACE は、**trust-dscp**、**trust-ipprec**、**trust-cos**、および **dscp** の 4 つの ACE キーワードで指定されます。ACE が **dscp** キーワードを使用する場合は、ACE に一致するトラフィックはすべて、同じポート キーワードが設定されたポートを通過する必要があります。ポートは、**trust-dscp**、**trust-ipprec**、**trust-cos**、および **untrusted** の 4 つのポート キーワードで指定されます。ACL を VLAN に付加する場合、VLAN 内のすべてのポートを、同じポート キーワードを使用して設定する必要があります。

PFC2 のポリシング決定

PFC2 では、ポリシング決定は次の 2 レベルからなります。

- 標準ポリシング レベル ― マイクロフロー ポリサーまたは集約標準レート ポリサーで不適合の決定が返される場合に設定
- 超過ポリシング レベル ― 集約超過レート ポリサーで不適合の決定が返される場合に設定

超過レート集約ポリサーで不適合の決定が返され、かつ廃棄指示フラグが設定されている場合、またはマイクロフロー ポリサーで不適合の決定が返され、かつ廃棄指示フラグが設定されている場合には、パケットは廃棄されます。

超過ポリシング レベルを設定すると、超過 DSCP マッピングを使用して、元の DSCP 値がマークダウンされる値に置き換えられます。標準ポリシング レベルだけを設定すると、標準 DSCP マッピングが使用されます。両方のポリシング レベルが設定されている場合には、超過ポリシング レベルのマッピング ルールが優先されます。超過ポリシング レベルは最悪の不適合違反を表すためです。

PFC3 のポリシング決定

PFC2 のポリシング決定に加えて、PFC3 は出力 QoS をサポートしています。ここでは、PFC3 のポリシング決定について説明します。

- ハードウェア転送された LAN トラフィックのポリシング（p.49-26）
- ソフトウェア転送された LAN トラフィックのポリシング（p.49-26）
- ソフトウェア転送された WAN トラフィックのポリシング（p.49-26）

ハードウェア転送された LAN トラフィックのポリシング

ハードウェア転送された LAN トラフィック（PFC3 によって転送されたトラフィック）は、入力と出力の両方のポリシング ルールで処理されます。LAN トラフィックが入力と出力の両方のポリシング ルールで処理される場合、QoS は両ルールを同時に評価し、最も厳しいルールを適用します。ポリシング ルールは同時に評価されるため、入力ポリシング ルールからのマークダウンが出力ポリシングのマークダウンの基礎として使用されることはありません。

ソフトウェア転送された LAN トラフィックのポリシング

ソフトウェア転送された LAN トラフィック（MSFC によりソフトウェアで転送された LAN トラフィック）は、入力と出力の両方のポリシング ルールで処理されます。ソフトウェア転送されたトラフィックが入力と出力の両方のポリシング ルールで処理される場合、QoS はルールを順番に評価します。入力ポリシング ルールからのマークダウンを、出力ポリシングのマークダウンの基礎として使用できます。

ソフトウェア転送された WAN トラフィックのポリシング

PFC3 は、ソフトウェア転送された WAN トラフィックで出力 QoS を提供できます。ソフトウェア転送された WAN トラフィックは出力ポリシング ルールでのみ処理されます。

ACL の付加

各ポートをポートベースの QoS（デフォルト）または VLAN ベースの QoS 対応として設定し（「ポートベースまたは VLAN ベース QoS のイネーブル化」[p.49-40] を参照）、特定のインターフェイスに ACL を付加できます（「インターフェイスへの ACL の付加」[p.49-55] を参照）。各ポートおよび VLAN に各タイプ（IP、IPX、イーサネット）を 1 つずつ、合計 3 つまで名前付き ACL を付加できます。

VLAN ベースの QoS 対応として設定されたポートでは、次のように名前付き ACL をポートの VLAN に付加できます。トランクの場合、次のように、トランクで認められる任意の VLAN に名前付き ACL を付加できます。

- VLAN ベースの QoS 対応として設定されたポートでは、そのポート経由で受信したトラフィックが、そのポートの VLAN に付加されているすべての名前付き ACL と比較されます。ポートの VLAN に名前付き ACL を結合しなかった場合、またはトラフィックが名前付き ACL 内の ACE と一致しなかった場合、QoS はポート経由で受信したトラフィックをデフォルトの ACL と比較します。
- VLAN ベースの QoS 対応として設定されたトランクでは、そのポート経由で受信したトラフィックが、そのトラフィックの VLAN に付加されているすべての名前付き ACL と比較されます。名前付き ACL が付加されていない VLAN のトラフィックの場合、またはトラフィックが名前付き ACL 内の ACE と一致しなかった場合、QoS はトラフィックをデフォルトの ACL と比較します。

ポートベースの QoS 対応として設定されたポートでは、次のように名前付き ACL をポートに付加できます。

- ポートベースの QoS 対応として設定されたポートでは、そのポート経由で受信したトラフィックが、そのポートに付加されているすべての名前付き ACL と比較されます。ポートに名前付き ACL を結合しなかった場合、またはトラフィックが名前付き ACL 内の ACE と一致しなかった場合、QoS はポート経由で受信したトラフィックをデフォルトの ACL と比較します。
- ポートベースの　QoS　対応として設定されたトランクでは、ポート経由で受信したすべての VLAN のトラフィックが、そのポートに付加されているすべての名前付き ACL と比較されます。ポートに名前付き ACL を結合しなかった場合、またはトラフィックが名前付き ACL 内の ACE と一致しなかった場合、QoS はポート経由で受信したトラフィックをデフォルトの ACL と比較します。

PFC3 では、入力および出力 QoS を設定できます。入力 QoS を設定するには、**input** キーワードにより QoS ACL をポートおよび VLAN に付加します。出力 QoS を設定するには、**output** キーワードにより QoS ACL を VLAN に付加します。出力 QoS は、ポート ベースの QoS（デフォルト）または VLAN ベースの QoS 設定を使用しません。

PFC3 の出力 DSCP 変換

PFC3 は、マップ ベースの出力 DSCP 変換をサポートしています。最大 15 個の DSCP/DSCP 変換マップを設定し、そのマップを VLAN に適用できます。QoS は VLAN 内の出力トラフィックで内部 DSCP 値をリマークします。

レイヤ 3 スイッチング エンジンの最終 CoS 値と ToS 値

レイヤ 3 スイッチング エンジンでは、トラフィックと一致する ACE に指定されたマーキング ルールおよびポリサーの指定に従って、QoS が CoS 値および ToS 値をトラフィックに対応付けます（「内部 DSCP 値」[p.49-16] を参照）。対応付けられた CoS および ToS は、イーサネット出力ポートで使用されます（「イーサネット出力ポートのスケジューリング、輻輳回避、およびマーキング」[p.49-28] を参照）。

PFC3A では QoS を設定して、マーキングおよびポリシングにより作成した DSCP の代わりに、出力 ToS バイト内で受信した DSCP 値を使用できます。

レイヤ 2 スイッチング エンジン搭載の Supervisor Engine 1 における分類およびマーキング

レイヤ 2 スイッチング エンジンを搭載した Supervisor Engine 1 の場合、QoS は特定の MAC アドレス /VLAN ペア宛てのトラフィックを分類し、設定された CoS 値を使用してマーキングすることができます（詳細については「QoS の用語」[p.49-2] および「ホスト宛先 MAC アドレス /VLAN ペアへの CoS 値のマッピング」[p.49-60] を参照）。

（注） レイヤ 2 スイッチング エンジンを搭載した Supervisor Engine 1 での分類およびマーキングには、レイヤ 2 の CoS 値が使用されます。レイヤ 2 スイッチング エンジンを搭載した Supervisor Engine 1 の分類およびマーキングでは、レイヤ 3 の IP precedence 値または DSCP 値を使用することも設定することもありません。

イーサネット出力ポートのスケジューリング、輻輳回避、およびマーキング

ここでは、イーサネット出力ポートのスケジューリング、輻輳回避、およびマーキングについて説明します。

概要

QoS は送信キューを使用して、CoS 値に基づいてトラフィックをスケジューリングし、CoS 値に基づく送信キュー廃棄スレッシュホールドを使用して、イーサネット ポートから送信されるトラフィックの輻輳を回避します。

（注）　イーサネット出力ポートのスケジューリングおよび輻輳回避では、レイヤ 2 の CoS 値が使用されます。イーサネット出力ポートのマーキングでは、レイヤ 2 の CoS 値を書き込み、さらに IP トラフィックの場合は、レイヤ 3 の ToS バイトを書き込みます。

送信キュー

show port capabilities コマンドを入力すると、ポートのキュー構造が表示されます。コマンドにより、次のいずれかが表示されます。

- **tx-(2q2t)** は、標準キューが 2 つあり、それぞれに設定可能なテール廃棄スレッシュホールドが 2 つあるという意味です。
- **tx-(1p2q1t)** は、完全優先キューが 1 つ、標準キューが 2 つあり、それぞれに設定可能な WRED 廃棄スレッシュホールドが 1 つあるという意味です（**1p2q1t** ポート上の各標準キューには、設定不可能なテール廃棄スレッシュホールドも 1 つずつあります）。
- **tx-(1p2q2t)** は、完全優先キューが 1 つ、標準キューが 2 つあり、それぞれに設定可能な WRED 廃棄スレッシュホールドが 2 つあるという意味です。
- **tx-(1p3q1t)** は、完全優先キューが 1 つ、標準キューが 3 つあり、それぞれに設定可能な WRED 廃棄スレッシュホールドが 1 つあるという意味です（**1p3q1t** ポート上の各標準キューには、設定不可能なテール廃棄スレッシュホールドも 1 つずつあります）。
- **tx-(1p3q8t)** は、完全優先キューが 1 つ、標準キューが 3 つあり、それぞれに設定可能な WRED 廃棄スレッシュホールドが 8 つあるという意味です（**1p3q8t** ポート上の各標準キューには、設定不可能なテール廃棄スレッシュホールドも 1 つずつあります）。
- **tx-(1p7q8t)** は、完全優先キューが 1 つ、標準キューが 7 つあり、それぞれに設定可能な WRED 廃棄スレッシュホールドが 8 つあるという意味です（**1p7q8t** ポート上の各標準キューには、設定不可能なテール廃棄スレッシュホールドも 1 つずつあります）。

完全優先キューを持つポート タイプでは、スイッチは完全優先送信キュー内のトラフィックを処理してから標準キューを処理します。スイッチが標準キューを処理する場合、パケットの送信後、完全優先キューにトラフィックがあるかどうかを調べます。完全優先キュー内でトラフィックを検出すると、標準キューの処理を中断し、先に完全優先キュー内のすべてのトラフィックを処理してから、標準キューに戻ります。

スケジューリングおよび輻輳回避

QoS は CoS 値ベースの送信キュー廃棄スレッシュホールドを実装し、送信トラフィックにおける輻輳を回避します。デフォルトの CoS/ スレッシュホールド マッピングについては、「QoS のデフォルト設定」（p.49-30）を参照してください。

一部のポート タイプでは、設定不可能な 100% テール廃棄スレッシュホールドと設定可能な WRED 廃棄スレッシュホールドの両方を使用するように、各標準送信キューを設定できます（「1p3q1t 送信キュー」[p.49-69] および 「1p2q1t、1p3q8t、および 1p7q8t 送信キュー」[p.49-70] を参照）。スイッチは、キューだけにマッピングされた CoS 値を伝送するトラフィックに対して、テール廃棄スレッシュホールドを使用します。WRED 廃棄スレッシュホールドの使用対象となるのは、キューとスレッシュホールドにマッピングされた CoS 値を伝送するトラフィックです。

マーキング

スイッチからトラフィックが送信されると、QoS は IP トラフィックに ToS バイトを書き込み（レイヤ 3 スイッチング エンジンの場合のみ）、スケジューリングと輻輳回避に使用された CoS 値を ISL トラフィックまたは 802.1Q トラフィックに書き込みます（詳細については 「レイヤ 3 スイッチング エンジンの最終 CoS 値と ToS 値」[p.49-27] を参照）。

QoS 統計データのエクスポート

QoS 統計データのエクスポート機能は、ポート単位および集約ポリサー単位で利用状況の情報を生成し、この情報を UDP パケットでトラフィックのモニタ、プランニング、またはアカウンティング アプリケーションに転送します。QoS 統計データのエクスポートは、ポート単位および集約ポリサー単位でイネーブルにできます。ポート単位で生成される統計データは、入出力パケット数とバイトで構成されます。集約ポリシング統計情報は、許可されたパケット数およびポリシング レートを超えるパケット数で構成されます。

QoS 統計データの収集は固定されたインターバルで定期的に発生しますが、データをエクスポートするインターバルは設定可能です。QoS 統計データの収集はデフォルトでイネーブルに設定されており、データ エクスポート機能は、すべてのポートと Catalyst 6500 シリーズ スイッチ上で設定されている集約ポリシングに対して、デフォルトでディセーブルに設定されています。

（注）

- ポート単位のカウンタ情報および利用状況の統計情報は、ATM ポートでは使用できません。
- QoS 統計データのエクスポートは、TopN および NetFlow Data Export（NDE;NetFlow データ エクスポート）とは完全に別個のもので、これらの機能と相互作用することはありません。

QoS 統計データ エクスポートの設定手順については、「QoS 統計データ エクスポートの設定」（p.49-86）を参照してください。

QoS のデフォルト設定

表 49-3 に、QoS のデフォルト設定を示します。

表 49-3　QoS のデフォルト設定

機能	デフォルト値
QoS イネーブル ステート	ディセーブル （注）QoS がイネーブルで他のすべての QoS パラメータがデフォルト値の場合、QoS はスイッチから送信されたすべてのトラフィックで、レイヤ 3 の DSCP を 0 に、レイヤ 2 の CoS を 0 に設定します。
DSCP の書き換え	イネーブル
出力 DSCP 変換	ディセーブル
ポートの CoS 値	0
VLAN 内マイクロフロー ポリシング	ディセーブル
CoS/ 内部 DSCP のマッピング （CoS 値に基づく内部 DSCP）	CoS 0 = DSCP　0 CoS 1 = DSCP　8 CoS 2 = DSCP 16 CoS 3 = DSCP 24 CoS 4 = DSCP 32 CoS 5 = DSCP 40 CoS 6 = DSCP 48 CoS 7 = DSCP 56
IP precedence/ 内部 DSCP のマッピング （IP precedence 値に基づく内部 DSCP）	IP precedence 0 = DSCP　0 IP precedence 1 = DSCP　8 IP precedence 2 = DSCP 16 IP precedence 3 = DSCP 24 IP precedence 4 = DSCP 32 IP precedence 5 = DSCP 40 IP precedence 6 = DSCP 48 IP precedence 7 = DSCP 56
内部 DSCP/ 出力 CoS のマッピング （内部 DSCP 値に基づく出力 CoS）	DSCP　0 ～ 7　= CoS 0 DSCP　8 ～ 15 = CoS 1 DSCP 16 ～ 23 = CoS 2 DSCP 24 ～ 31 = CoS 3 DSCP 32 ～ 39 = CoS 4 DSCP 40 ～ 47 = CoS 5 DSCP 48 ～ 55 = CoS 6 DSCP 56 ～ 63 = CoS 7
DSCP マップからの DSCP のマークダウン	マークダウンされる DSCP 値と元の DSCP 値が同じ（マークダウンなし）
ポリサー	なし
名前付き ACL	なし
デフォルトの ACL	ポート単位の分類およびマーキングをサポート、untrusted ポートからのトラフィックで DSCP を 0 に設定、ポリシングなし
COPS[1] サポート	ディセーブル
RSVP サポート	ディセーブル
QoS 統計データのエクスポート	ディセーブル

表 49-3　QoS のデフォルト設定（続き）

機能	デフォルト値
QoS がイネーブルの場合	
Runtime ― ポート ベースまたは VLAN ベース	ポート ベース
Config ― ポート ベースまたは VLAN ベース	ポート ベース
ポートの信頼状態	untrusted
2q2t 送信キュー容量の割合	• ロー プライオリティ：80% • ハイ プライオリティ：20%
1p1q0t 受信キュー容量の割合	• 標準：80% • 完全優先：20%
1p2q2t 送信キュー容量の割合	• ロー プライオリティ：70% • ハイ プライオリティ：15% • 完全優先：15%
1p2q1t 送信キュー容量の割合	• ロー プライオリティ：70% • ハイ プライオリティ：15% • 完全優先：15%
1p3q8t 送信キュー容量の割合	• ロー プライオリティ：65% • ミディアム プライオリティ：15% • ハイ プライオリティ：15% • 完全優先：5%
1p7q8t 送信キュー容量の割合	• 標準キュー 1（最低プライオリティ）：25% • 標準キュー 2：15% • 標準キュー 3：15% • 標準キュー 4：10% • 標準キュー 5：10% • 標準キュー 6：10% • 標準キュー 7（最高プライオリティ）：10% • 完全優先：5%
1p3q8t 標準送信キューのロー/ ミディアム / ハイ プライオリティ帯域幅割り当て比率	20:100:200
1p7q8t 標準送信キューの最低 / 最高プライオリティ帯域幅割り当て比率	10:20:30:40:40:70:70
1p2q1t 標準送信キューのロー / ハイ プライオリティ帯域幅割り当て比率	100:255
2q2t、**1p2q2t**、および **1p2q1t** 標準送信キューのロー / ハイ プライオリティ帯域幅割り当て比率	5:255
1p3q1t 標準送信キューのロー/ ミディアム / ハイ プライオリティ帯域幅割り当て比率	100:150:200

表 49-3　QoS のデフォルト設定（続き）

機能	デフォルト値
1q4t/2q2t 受信キューおよび送信キューの CoS 値 / 廃棄スレッシュホールド マッピング	• 受信キュー 1/ 廃棄スレッシュホールド 1（50%）および 送信キュー 1/ 廃棄スレッシュホールド 1（80%）：CoS 0 および 1 • 受信キュー 1/ 廃棄スレッシュホールド 2（60%）および 送信キュー 1/ 廃棄スレッシュホールド 2（100%）：CoS 2 および 3 • 受信キュー 1/ 廃棄スレッシュホールド 3（80%）および 送信キュー 2/ 廃棄スレッシュホールド 1（80%）：CoS 4 および 5 • 受信キュー 1/ 廃棄スレッシュホールド 4（100%）および 送信キュー 2/ 廃棄スレッシュホールド 2（100%）：CoS 6 および 7
1q2t ポートの受信キューの CoS 値 / 廃棄スレッシュホールド マッピングおよびスレッシュホールドの割合	• 受信キュー 1/ 廃棄スレッシュホールド 1： — CoS 0、1、2、3、および 4 — 廃棄スレッシュホールド：80% • 受信キュー 1/ 廃棄スレッシュホールド 2： — CoS 5、6、および 7 — 廃棄スレッシュホールド：100%（設定不可能） **（注）** **1p2q2t** 送信キューは **1p1q4t/1p2q2t** と同様
1p1q4t/1p2q2t ポートの受信キューおよび送信キューの CoS 値 / 廃棄スレッシュホールド マッピングおよびスレッシュホールドの割合	• 完全優先受信キュー 1 および 完全優先送信キュー 1：CoS 5 • 受信キュー 1/ 廃棄スレッシュホールド 1 および 送信キュー 1/ 廃棄スレッシュホールド 1： — CoS 0 および 1 — 送信キューのローおよびハイ WRED 廃棄スレッシュホールド：40% および 70% • 受信キュー 1/ 廃棄スレッシュホールド 2 および 送信キュー 1/ 廃棄スレッシュホールド 2： — CoS 2 および 3 — 送信キューのローおよびハイ WRED 廃棄スレッシュホールド：70% および 100% • 受信キュー 1/ 廃棄スレッシュホールド 3 および 送信キュー 2/ 廃棄スレッシュホールド 1： — CoS 4 — 送信キューのローおよびハイ WRED 廃棄スレッシュホールド：40% および 70% • 受信キュー 1/ 廃棄スレッシュホールド 4 および 送信キュー 2/ 廃棄スレッシュホールド 2： — CoS 6 および 7 — 送信キューのローおよびハイ WRED 廃棄スレッシュホールド：70% および 100%
1p1q0t 受信キューの CoS 値マッピング	• 受信キュー 1（標準）設定不可能 100% テール廃棄スレッシュホールド：CoS 0、1、2、3、4、6、および 7 • 受信キュー 2（完全優先）：CoS 5

表 49-3　QoS のデフォルト設定（続き）

機能	デフォルト値
1q8t 受信キューの CoS 値 / 廃棄スレッシュホールド マッピング	• スレッシュホールド 1：50%（CoS 0） • スレッシュホールド 2：50% • スレッシュホールド 3：60%（CoS 1、2、3、4） • スレッシュホールド 4：60% • スレッシュホールド 5：80%（CoS 6 および 7） • スレッシュホールド 6：80% • スレッシュホールド 7：100%（CoS 5） • スレッシュホールド 8：100%
1p3q8t 送信キューの CoS 値 / 廃棄スレッシュホールド マッピング	• 標準送信キュー 1（ロー プライオリティ）のローおよびハイ WRED 廃棄スレッシュホールド — スレッシュホールド 1 — 70% および 100%（CoS 0） — スレッシュホールド 2 ～ 8 — 100% および 100% • 標準送信キュー 2（ミディアム プライオリティ）のローおよびハイ WRED 廃棄スレッシュホールド — スレッシュホールド 1 — 70% および 100%（CoS 1 および 2） — スレッシュホールド 2 ～ 8 — 100% および 100% • 標準送信キュー 3（ハイ プライオリティ）のローおよびハイ WRED 廃棄スレッシュホールド — スレッシュホールド 1 および 2 — 40% および 70% — スレッシュホールド 3 および 4 — 50% および 80% — スレッシュホールド 5 — 60% および 90%（CoS 3 および 4） — スレッシュホールド 6 — 60% および 90% — スレッシュホールド 7 — 70% および 100%（CoS 6 および 7） — スレッシュホールド 8 — 70% および 100% • 完全優先送信キュー 4：CoS 5

表 49-3　QoS のデフォルト設定（続き）

機能	デフォルト値
1p7q8t 送信キューの CoS 値 / 廃棄スレッシュホールド マッピング	• 標準送信キュー 1（最低プライオリティ）のローおよびハイ WRED 廃棄スレッシュホールド — スレッシュホールド 1 — 70% および 100%（CoS 0） — スレッシュホールド 2 ～ 8 — 100% および 100% • 標準送信キュー 2 のローおよびハイ WRED 廃棄スレッシュホールド — スレッシュホールド 1 — 70% および 100%（CoS 1） — スレッシュホールド 2 ～ 8 — 100% および 100% • 標準送信キュー 3 のローおよびハイ WRED 廃棄スレッシュホールド — スレッシュホールド 1 — 70% および 100%（CoS 2） — スレッシュホールド 2 ～ 8 — 100% および 100% • 標準送信キュー 4 のローおよびハイ WRED 廃棄スレッシュホールド — スレッシュホールド 1 — 70% および 100%（CoS 3） — スレッシュホールド 2 ～ 8 — 100% および 100% • 標準送信キュー 5 のローおよびハイ WRED 廃棄スレッシュホールド — スレッシュホールド 1 — 70% および 100%（CoS 4） — スレッシュホールド 2 ～ 8 — 100% および 100% • 標準送信キュー 6 のローおよびハイ WRED 廃棄スレッシュホールド — スレッシュホールド 1 — 100% および 100% — スレッシュホールド 2 — 70% および 100%（CoS 6） — スレッシュホールド 3 ～ 8 — 100% および 100% • 標準送信キュー 7 のローおよびハイ WRED 廃棄スレッシュホールド — スレッシュホールド 1 — 100% および 100% — スレッシュホールド 2 — 70% および 100%（CoS 7） — スレッシュホールド 3 ～ 8 — 100% および 100% • 完全優先送信キュー 8：CoS 5
1p3q1t 送信キューの CoS 値 / 廃棄スレッシュホールド マッピング	• 標準送信キュー 1（ロー プライオリティ）のテール廃棄スレッシュホールド： — CoS 0 および 1 — ローおよびハイ WRED 廃棄スレッシュホールド：70% および 100% • 標準送信キュー 2（ミディアム プライオリティ）のテール廃棄スレッシュホールド： — CoS 2、3、および 4 — ローおよびハイ WRED 廃棄スレッシュホールド：70% および 100% • 標準送信キュー 3（ハイ プライオリティ）のテール廃棄スレッシュホールド： — CoS 6 および 7 — ローおよびハイ WRED 廃棄スレッシュホールド：70% および 100% • 標準送信キュー 4（完全優先）：CoS 5

表 49-3　QoS のデフォルト設定（続き）

機能	デフォルト値
1p1q8t 受信キューのポート CoS 値 / 廃棄スレッシュホールド マッピング	• 受信キュー 1（標準）の WRED 廃棄スレッシュホールド：CoS 0、1、2、3、4、6、および 7 — 廃棄スレッシュホールド 1：CoS 0 ロー WRED スレッシュホールド：40% ハイ WRED 廃棄スレッシュホールド：70% — 廃棄スレッシュホールド 2：CoS 1 ロー WRED スレッシュホールド：40% ハイ WRED 廃棄スレッシュホールド：70% — 廃棄スレッシュホールド 3：CoS 2 ロー WRED スレッシュホールド：50% ハイ WRED 廃棄スレッシュホールド：80% — 廃棄スレッシュホールド 4：CoS 3 ロー WRED スレッシュホールド：50% ハイ WRED 廃棄スレッシュホールド：80% — 廃棄スレッシュホールド 5：CoS 4 ロー WRED スレッシュホールド：60% ハイ WRED 廃棄スレッシュホールド：90% — 廃棄スレッシュホールド 6：CoS 6 ロー WRED スレッシュホールド：60% ハイ WRED 廃棄スレッシュホールド：90% — 廃棄スレッシュホールド 6：CoS 7 ロー WRED スレッシュホールド：70% ハイ WRED 廃棄スレッシュホールド：100% • 受信キュー 2（完全優先）：CoS 5
1p2q1t 送信キューのポート CoS 値 / 廃棄スレッシュホールド マッピング	• 標準送信キュー 1（ロー プライオリティ）の WRED 廃棄スレッシュホールド： — CoS 0、1、2、および 3 — ロー WRED スレッシュホールド：70% — ハイ WRED 廃棄スレッシュホールド：100% • 標準送信キュー 2（ハイ プライオリティ）の WRED 廃棄スレッシュホールド： — CoS 4、6、または 7 — ロー WRED スレッシュホールド：70% — ハイ WRED 廃棄スレッシュホールド：100% • 完全優先送信キュー 3：CoS 5

表 49-3　QoS のデフォルト設定（続き）

機能	デフォルト値
QoS がディセーブルの場合	
Runtime ― ポート ベースまたは VLAN ベース	VLAN ベース
Config ― ポート ベースまたは VLAN ベース	ポート ベース
ポートの信頼状態	**trust-cos**（レイヤ 2 スイッチング エンジン） **trust-dscp**（レイヤ 3 スイッチング エンジン）
受信キュー廃棄スレッシュホールドの割合	すべてのスレッシュホールドを 100% に設定
送信キュー廃棄スレッシュホールドの割合	すべてのスレッシュホールドを 100% に設定
送信キューのロー プライオリティ / ハイ プライオリティ帯域幅割り当て比率	255:1
送信キュー容量の比率	• ロー プライオリティ：100% • ハイ プライオリティ：未使用
CoS 値 / 廃棄スレッシュホールドのマッピング	受信廃棄スレッシュホールド 1 および送信キュー 1/ 廃棄スレッシュホールド 1：CoS 0 ～ 7

1. COPS = Common Open Policy Service

QoS 設定時の注意事項および制限事項

QoS は、Committed Information Rate（CIR; 認定情報速度）および Peak Information Rate（PIR; ピーク情報速度）値に次のハードウェア粒度を持ちます。

CIR および PIR rate 値の範囲	粒度
1 ～ 2097152 （2 Mbps）	65536 （64 KB）
2097153 ～ 4194304 （4 Mbps）	131072（128 KB）
4194305 ～ 8388608 （8 Mbps）	262144（256 KB）
8388609 ～ 16777216 （16 Mbps）	524288（512 KB）
16777217 ～ 33554432 （32 Mbps）	1048576 （1 MB）
33554433 ～ 67108864 （64 Mbps）	2097152 （2 MB）
67108865 ～ 134217728（128 Mbps）	4194304 （4 MB）
134217729 ～ 268435456（256 Mbps）	8388608 （8 MB）
268435457 ～ 536870912（512 Mbps）	16777216 （16 MB）
536870913 ～ 1073741824 （1 Gbps）	33554432 （32 MB）
1073741825 ～ 2147483648 （2 Gbps）	67108864 （64 MB）
2147483649 ～ 4294967296 （4 Gbps）	134217728（128 MB）
4294967297 ～ 8000000000 （8 Gbps）	268435456（256 MB）

各範囲内で、PFC QoS は粒度の値の倍数である rate 値で PFC ハードウェアをプログラミングします。

QoS は、CIR および PIR トークン バケット（バースト）サイズに次のハードウェア粒度を持ちます。

CIR および PIR トークン バケット サイズの範囲	粒度
1 ～ 32768 （32 KB）	1024 （1 KB）
32769 ～ 65536 （64 KB）	2048 （2 KB）
65537 ～ 131072（128 KB）	4096 （4 KB）
131073 ～ 262144（256 KB）	8192 （8 KB）
262145 ～ 524288（512 KB）	16384 （16 KB）
524289 ～ 1048576（1 MB）	32768 （32 KB）
1048577 ～ 2097152（2 MB）	65536 （64 KB）
2097153 ～ 4194304（4 MB）	131072（128 KB）
4194305 ～ 8388608（8 MB）	262144（256 KB）
8388609 ～ 16777216（16 MB）	524288（512 KB）
16777217 ～ 33554432（32 MB）	1048576（1 MB）

QoS の設定の注意および制限事項

ここでは、Catalyst 6500 シリーズ スイッチ上で QoS を設定する手順について説明します。

（注） 一部の QoS **show** コマンドでは、**config** および **runtime** キーワードを使用します。**runtime** キーワードは、ハードウェアに現在プログラミングされている QoS 値を表示する場合に使用します。QoS がディセーブルの場合、**runtime** キーワードを使用すると、その出力には [QoS is disabled] と表示されます。**config** キーワードを使用すると、入力はしたもののハードウェアにはプログラミングされていない可能性のある値が表示されます（たとえば、COPS が QoS ポリシー ソースとして選択された結果、現在は使用されていないローカル設定の QoS 値、または QoS がディセーブルのときに設定された QoS 値など）。

QoS のイネーブル化

QoS をイネーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
スイッチ上で QoS をイネーブルにします。	**set qos** {**enable** | **disable**}

次に、QoS をイネーブルにする例を示します。

```
Console> (enable) set qos enable
QoS is enabled.
Console> (enable)
```

DSCP の書き換えのイネーブル化

（注） このコマンドをサポートしているのは PFC3 だけです。

DSCP の書き換えでは、マーキングおよびポリシングからの DSCP 値を出力 DSCP 値として使用します。DSCP の書き換えをイネーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
スイッチ上で DSCP の書き換えをイネーブルにします。	**set qos dscp-rewrite enable**

次に、DSCP の書き換えをイネーブルにする例を示します。

```
Console> (enable) set qos dscp-rewrite enable
DSCP rewrite has been globally enabled.
Console> (enable)
```

DSCP の書き換えのディセーブル化

（注） このコマンドをサポートしているのは PFC3 だけです。

DSCP の書き換えでは、受信した DSCP 値を出力 DSCP 値として使用します。DSCP の書き換えをディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
スイッチ上で DSCP の書き換えをディセーブルにします。	**set qos dscp-rewrite disable**

次に、DSCP の書き換えをディセーブルにする例を示します。

```
Console> (enable) set qos dscp-rewrite disable
DSCP rewrite has been globally disabled.
Console> (enable)
```

ポートベースまたは VLAN ベース QoS のイネーブル化

(注)　レイヤ 2 スイッチング エンジンを搭載した Supervisor Engine 1 は、このコマンドをサポートしていません。

デフォルトの設定では、QoS はポートに付加された ACL を使用します。VLAN に付加された ACL を使用するように、QoS をポート単位で設定できます。ポート上で VLAN ベースの QoS をイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポート上で VLAN ベースの QoS をイネーブルにします。	**set port qos** *mod/port* {**port-based** | **vlan-based**}
ステップ 2	設定を確認します。	**show port qos** *mod/port*

詳細については、「ACL の付加」（p.49-26）を参照してください。

次に、ポート上で VLAN ベースの QoS をイネーブルにする例を示します。

```
Console> (enable) set port qos 1/1-2 vlan-based
Hardware programming in progress...
QoS interface is set to vlan-based for ports 1/1-2.
Console> (enable)
```

ポートベースから VLAN ベースの QoS にポートの設定を変更すると、そのポートからすべての ACL が切り離されます。VLAN に付加された ACL が、ポートにただちに適用されます（詳細については「インターフェイスへの ACL の付加」[p.49-55] を参照）。

ポートの信頼状態の設定

次のコマンドで、ポートの信頼状態を設定します（詳細については「イーサネット入力ポートのマーキング、スケジューリング、輻輳回避、および分類」[p.49-12] を参照）。デフォルトの設定では、すべてのポートが untrusted です。

ポートの信頼状態を設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポートの信頼状態を設定します。	**set port qos trust** {**untrusted** | **trust-cos** | **trust-ipprec** | **trust-dscp**}
ステップ 2	設定を確認します。	**show port qos**

ポートの信頼状態を設定する際は、次の構文に関する注意事項に留意してください。

- **trust-ipprec** および **trust-dscp** キーワードは、レイヤ 3 スイッチング エンジンでのみサポートされています。
- **1q4t** ポート（ギガビット イーサネットを除く）は、**trust-ipprec** および **trust-dscp** のポート キーワードをサポートしていません。**trust-ipprec** または **trust-dscp** 信頼状態を適用するには、入力トラフィックに一致する **trust-ipprec** または **trust-dscp** ACL を設定する必要があります。

- **1q4t** ポート上では（ギガビット イーサネットを除く）、**trust-cos** ポート キーワードを指定するとエラー メッセージが表示され、受信キューの廃棄スレッシュホールドがアクティブになり、（エラー メッセージで示されるように）トラフィックには **trust-cos** の信頼状態が適用されません。**trust-cos** 信頼状態を適用するには、入力トラフィックに一致する **trust-cos** ACL を設定する必要があります。

次に、**trust-cos** キーワードを指定してポート 1/1 を設定する例を示します。

```
Console> (enable) set port qos 1/1 trust trust-cos
Port 1/1 qos set to trust-cos
Console> (enable)
```

（注） CoS 値を伝送するのは、ISL フレームまたは 802.1Q フレームだけです。受信トラフィックが ISL フレームまたは 802.1Q フレームであり、かつそのフレームがネットワーク ポリシーと矛盾しないことがはっきりしている CoS 値を伝送する場合に限って、**trust-cos** キーワードを使用してポートを設定します。

ポート CoS 値の設定

（注） QoS が **set port qos ... cos** コマンドに適用した CoS 値を使用するかどうかは、ポートおよびポートから受信したトラフィックの信頼状態によって決まります。ポートおよびポートから受信したトラフィックの信頼状態の設定は、**set port qos ... cos** コマンドでは行いません。**set port qos ... cos** コマンドに適用した CoS 値を使用するには、入力トラフィックに一致する trust-CoS ACL を設定するか、またはタグ付けされていないトラフィックを受信するポートに trust CoS を設定する必要があります。

trusted に設定されているポートからのマーキングされてないフレーム、および untrusted に設定されているポートからのすべてのフレームには、次のコマンドで指定した CoS 値が割り当てられます。

ポートに CoS 値を設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポートに CoS 値を設定します。	**set port qos cos** *cos_value*
ステップ 2	設定を確認します。	**show port qos**

次に、ポート 1/1 のポート CoS 値を 3 に設定する例を示します。

```
Console> (enable) set port qos 1/1 cos 3
Port 1/1 qos cos set to 3
Console> (enable)
```

デフォルトのポート CoS 値に戻すには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	デフォルトのポート CoS 値に戻します。	**clear port qos cos**
ステップ 2	設定を確認します。	**show port qos**

次に、ポート 1/1 の CoS 値をデフォルト値に戻す例を示します。

```
Console> (enable) clear port qos 1/1 cos
Port 1/1 qos cos setting cleared.
Console> (enable)
```

ポリサーの作成

（注）　レイヤ 2 スイッチング エンジンを搭載した Supervisor Engine 1 は、このコマンドをサポートしていません。

ポリサーを作成するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポリサーを作成します。	**set qos policer microflow** *microflow_name* {**rate** *rate*} {**burst** *burst_value*} {**drop** | **policed-dscp**} PFC または PFC2 の場合： **set qos policer aggregate** *aggregate_name* {**rate** *rate*} {**burst** *burst_value*} {**drop** | **policed-dscp**} PFC2 または PFC3A の場合： **set qos policer aggregate** *aggregate_name* {**rate** *rate*} **policed-dscp** {**erate** *erate_value*} {**drop** | **policed-dscp**} **burst** *burst_value* [**eburst** *eburst_value*]
ステップ 2	設定を確認します。	**show qos policer** {**config** | **runtime**} {**microflow** | **aggregate** | **all**}

詳細については、「ポリサー」（p.49-24）および「PFC2 のポリシング決定」（p.49-25）を参照してください。

policer_name パラメータは大文字と小文字の区別があり、最大 31 文字です。使用できる文字は a ～ z、A ～ Z、0 ～ 9、ダッシュ（-）、下線（_）、およびピリオド（.）です。ポリサーは、（数字ではなく）英字から始め、すべてのマイクロフローおよび集約ポリサー中で一意の名前でなければなりません。コマンド キーワードをポリサー名として使用することはできません。

rate および *erate* パラメータの有効値は、32 Kbps（32 を入力）～ 32 Gbps（32000000 を入力）です。すべてのトラフィックを不適合と分類するには、*rate* パラメータを 0 に設定します。*erate* パラメータは、*rate* パラメータよりも大きい値に設定してください。PFC1 および PFC2 では、rate 値に対するハードウェアの粒度は次のようになっています。

rate 値の範囲	粒度	rate 値の範囲	粒度
1 ～ 1000（1 Mbps）	32768（32 KB）	64001 ～ 128000（128 Mbps）	4194304（4 MB）
1001 ～ 2000（2 Mbps）	65536（64 KB）	128001 ～ 256000（256 Mbps）	8388608（8 MB）
2001 ～ 4000（4 Mbps）	131072（128 KB）	256001 ～ 512000（512 Mbps）	16777216（16 MB）
4001 ～ 8000（8 Mbps）	262144（256 KB）	512001 ～ 1024000（1 Gbps）	33554432（32 MB）
8001 ～ 16000（16 Mbps）	524288（512 KB）	1024001 ～ 2048000（2 Gbps）	67108864（64 MB）
16001 ～ 32000（32 Mbps）	1048576（1 MB）	2048001 ～ 4096000（4 Gbps）	134217728（128 MB）
32001 ～ 64000（64 Mbps）	2097152（2 MB）	4096001 ～ 8192000（8 Gbps）	268435456（256 MB）

各範囲内で、QoS は粒度の値の倍数である rate 値でハードウェアをプログラミングします。

burst パラメータと *eburst* パラメータに使用できる値は、1 KB（1 と入力）～ 256 MB（256000 と入力）です。*burst* と *eburst* のパラメータを設定する際には、次の事項に注意してください。

- **burst** キーワード、*burst_value* パラメータ、オプションの **eburst** キーワード、*eburst_value* パラメータによって、トークン バケット サイズが設定されます。
- トークン バケット サイズは、0.25 ミリ秒あたりに送信できる適合バイトの最大数を定義します。
- 特定のレートを維持するには、最低でもトークン バケット サイズに *rate* を 4000 で割った値を設定します。トークンは 1/4000 秒（0.25 ミリ秒）ごとにバケットから削除され、特定のレートを維持するにはバケットの長さが少なくともバースト サイズでなければならないためです。
- **eburst** キーワードと *eburst_value* パラメータを入力しないと、QoS によって、両方のトークン バケットが **burst** キーワードと *burst_value* パラメータで設定されたサイズになります。
- バースト サイズより大きいパケットは不適合とみなされるので、バースト サイズはポリシングが適用される最大のパケット サイズ以上に設定してください。
- QoS は、入力された値ではなく、32 K の倍数（32,768）を使用してハードウェアをプログラミングします。

drop キーワードを入力して、すべての不適合パケットが廃棄されるようにするか、**policed-dscp** キーワードを入力して、すべての標準レートの不適合パケットが標準マークダウン DSCP マップの指定に従ってマークダウンされるようにします（詳細については「DSCP マークダウン値のマッピング」[p.49-73] を参照）。

次に、不適合のトラフィックのマークダウンが行われるレート制限を 1 Mbps、バースト制限を 10 MB に設定して、マイクロフロー ポリサーを作成する例を示します。

```
Console> (enable) set qos policer microflow my-micro rate 1000 burst 10000
policed-dscp
Hardware programming in progress...
QoS policer for microflow my-micro created successfully.
Console> (enable)
```

次に、PFC2 または PFC3A の場合、64 Kbps のレート制限および 128 KB のバースト制限（これらの値を超過するトラフィックを廃棄）を使用して集約超過レート ポリサーを作成する例を示します。

```
Console> (enable) set qos policer aggregate test rate 64 burst 128 drop
QoS policer for aggregate test created successfully.
Console> (enable) show qos policer config aggregate test
QoS aggregate policers:
QoS aggregate policers:
Aggregate name                 Normal rate (kbps) Burst size (kb) Normal action
------------------------------ ------------------ --------------- -------------
test                                           64             128    policed-dscp
                               Excess rate (kbps) Burst size (kb) Excess action
                               ------------------ --------------- -------------
                                               64             128    drop
                               ACL attached
                               -----------------------------------
Console> (enable)
```

次に、PFC2 または PFC3A の場合、64 Kbps のレート制限および 100 KB のバースト制限（標準マークダウン DSCP マップの指示に従ってすべての不適合パケットをマークダウン）を使用して、集約超過レート ポリサーを作成する例を示します。

```
Console> (enable) set qos policer aggregate test2 rate 64 burst 100 policed-dscp
QoS policer for aggregate test2 created successfully.
Console> (enable) show qos policer config aggregate test2
QoS aggregate policers:
Aggregate name                 Normal rate (kbps)  Burst size (kb) Normal action
------------------------------ ------------------  --------------- -------------
test2                                          64             100  policed-dscp
                               Excess rate (kbps)  Burst size (kb) Excess action
                               ------------------  --------------- ---------------
                                         8000000             100  policed-dscp
                               ACL attached
                               ------------------------------------

Console> (enable)
```

次に、PFC2 または PFC3A の場合、64 Kbps のレート制限および 128 KB のバースト制限（64 Kbps の標準レートおよび 96 KB のバースト サイズを超えるトラフィックが標準のマークダウン DSCP マップの指定に従ってマークダウンされ、128 Kbps および 96 KB のバースト サイズを超えるトラフィックが廃棄される）を使用して集約超過レート ポリサーを作成する例を示します。

```
Console> (enable) set qos policer aggregate test3 rate 64 policed-dscp erate 128 drop
burst 96
QoS policer for aggregate test3 created successfully.
Console> (enable) show qos policer config aggregate test3
QoS aggregate policers:
Aggregate name                 Normal rate (kbps)  Burst size (kb) Normal action
------------------------------ ------------------  --------------- -------------
test3                                          64              96 policed-dscp
                               Excess rate (kbps)  Burst size (kb) Excess action
                               ------------------  --------------- ---------------
                                             128              96 drop
                               ACL attached
                               ------------------------------------

Console> (enable)
```

ポリサーの削除

（注）　削除できるのは、インターフェイスに付加されていないポリサーだけです（詳細については「インターフェイスからの ACL の切り離し」[p.49-56] を参照）。

1 つまたはすべてのポリサーを削除するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	1 つまたはすべてのポリサーを削除します。	**clear qos policer** {**microflow** | **aggregate**} {*policer_name* | **all**}
ステップ 2	設定を確認します。	**show qos policer** {**config** | **runtime**} {**microflow** | **aggregate** | **all**}

次に、my_micro というマイクロフロー ポリサーを削除する例を示します。

```
Console> (enable) clear qos policer microflow my_micro
my_micro QoS microflow policer cleared.
Console> (enable)
```

ACL の作成または変更

(注)　レイヤ 2 スイッチング エンジンを搭載した Supervisor Engine 1 は、このコマンドをサポートしていません。

ここでは、ACL の作成および変更について説明します。

ACL 名

ACL 名は大文字と小文字の区別があり、最大 31 文字です。使用できる文字は a ～ z、A ～ Z、0 ～ 9、ダッシュ（-）、下線（_）、およびピリオド（.）です。ACL 名は英字から始め、すべてのタイプのすべての QoS ACL 中で一意の名前にしなければなりません。コマンド キーワードを ACL 名として使用することはできません。

ACE 名、マーキング ルール、ポリシング、およびフィルタリングの構文

ACE コマンド構文は、次のとおりです。
ACL_command　ACL_type_and_name　marking_rule　policing_rule　filtering

たとえば、IP ACE の場合、コマンド構文は次のようになります。

set qos acl ip *acl_name* {**dscp** *dscp_value* | **trust-cos** | **trust-ipprec** | **trust-dscp**} [**microflow** *microflow_name*] [**aggregate** *aggregate_name*] *src_ip_spec* [**precedence** *precedence* | **dscp-field** *dscp*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

- **set qos acl ip** *acl_name* ― 指定したタイプの名前付き ACL を作成するか、ACL がすでに存在する場合は、その ACL に ACE を追加します。「ACL 名」（p.49-45）を参照してください。
- {**dscp value_** *dscp* | **trust-cos** | **trust-ipprec** | **trust-dscp**} ― マーキング ルールを選択します。「マーキング ルール」（p.49-22）を参照してください。
- [**microflow** *microflow_name*] [**aggregate** *aggregate_name*] ― オプションとして ACE にポリシングを設定します。「ポリサー」（p.49-24）を参照してください。
- *src_ip_spec* [**precedence** *precedence* | **dscp-field** *dscp*] ― 残りのパラメータは、**editbuffer** キーワードを除いて、フィルタリングを設定します。

名前付き IP ACL

ここでは、IP ACL の作成または変更について説明します。

送信元および宛先の IP アドレスとマスク

IP ACE では、*ip_address mask* の形式で、送信元および宛先の IP アドレスおよびマスクを指定します（後述の説明では、それぞれ *src_ip_spec* および *dest_ip_spec* パラメータで表します）。マスクは必須です。ワイルドカードが必要な場合は、1 ビットを使用します。連続させる必要はありません。

アドレスおよびマスクには、次のいずれかの形式を使用します。

- 4 つの部分からなるドット付き 10 進表記の 32 ビット値
- 0.0.0.0 255.255.255.255 というワイルドカード アドレスおよびワイルドカード マスクの省略形としてキーワード **any**
- *ip_address* 0.0.0.0 というアドレスおよびワイルドカード マスクの省略形として **host** *ip_address*

ポート operator パラメータ

IP ACE の *operator* パラメータは次のいずれかです。

- **lt**（未満）
- **gt**（より大きい）
- **eq**（一致）
- **neq**（不一致）
- **range**（ポート パラメータのペアを指定）

QoS ACL に適用される制限事項については、「レイヤ 4 演算設定時の注意事項」（p.15-25）を参照してください。

precedence パラメータ オプション

IP ACE の *precedence* パラメータ キーワード オプションについては、「IP ACE レイヤ 3 の分類基準」（p.49-18）を参照してください。

TCP トラフィック用の IP ACE

TCP トラフィック用の IP ACE を作成または変更するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	TCP トラフィック用の IP ACE を作成または変更します。	**set qos acl ip** {*acl_name*} {{**dscp** *dscp_value*} | **trust-cos** | **trust-ipprec** | **trust-dscp**} [**microflow** *microflow_name*] [**aggregate** *aggregate_name*] **tcp** {*src_ip_spec*} [{*operator*} {*port*} [*port*]] {*dest_ip_spec*} [{*operator*} {*port*} [*port*]] [**established**] [**precedence** *precedence_value* | **dscp-field** *dscp*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]
ステップ 2	設定を確認します。	**show qos acl info** {**acl_name** | **all**} **editbuffer** [*editbuffer_index*]

port パラメータ キーワード オプションについては、「IP ACE レイヤ 4 TCP の分類基準」（p.49-19）を参照してください。

established キーワードを指定すると、ACK（確認応答）または RST（リセット）ビット セットとトラフィックが比較されます。

次に、TCP トラフィック用の IP ACE を作成する例を示します。

```
Console> (enable) set qos acl ip my_IPacl trust-ipprec microflow my-micro
aggregate my-agg tcp any any
my_IPacl editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

UDP トラフィック用の IP ACE

UDP トラフィック用の IP ACE を作成または変更するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	UDP トラフィック用の IP ACE を作成または変更します。	**set qos acl ip** {*acl_name*} {{**dscp** *dscp_value*} | **trust-cos** | **trust-ipprec** | **trust-dscp**} [**microflow** *microflow_name*] [**aggregate** *aggregate_name*] **udp** {*src_ip_spec*} [{*operator*} {*port*} [*port*]] {*dest_ip_spec*} [{*operator*} {*port*} [*port*]] [**precedence** *precedence_value* | **dscp-field** *dscp*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]
ステップ 2	設定を確認します。	**show qos acl info** {**acl_name** | **all**} **editbuffer** [*editbuffer_index*]

port パラメータ キーワード オプションについては、「IP ACE レイヤ 4 UDP の分類基準」（p.49-19）を参照してください。

次に、UDP トラフィック用の IP ACE を作成する例を示します。

```
Console> (enable) set qos acl ip my_IPacl trust-ipprec microflow my-micro
aggregate my-agg udp any any
my_IPacl editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

ICMP トラフィック用の IP ACE

ICMP トラフィック用の IP ACE を作成または変更するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ICMP トラフィック用の IP ACE を作成または変更します。	**set qos acl ip** *acl_name* {**dscp** *dscp* | **trust-cos** | **trust-ipprec** | **trust-dscp**} [**microflow** *microflow_name*] [**aggregate** *aggregate_name*] **icmp** *src_ip_spec dest_ip_spec* [*icmp_type* [*icmp_code*] | *icmp_message*] [**precedence** *precedence* | **dscp-field** *dscp*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]
ステップ 2	設定を確認します。	**show qos acl info** {**acl_name** | **all**} **editbuffer** [*editbuffer_index*]

icmp_code および *icmp_type* パラメータ キーワード オプションについては、「IP ACE レイヤ 4 ICMP の分類基準」（p.49-20）を参照してください。

次に、ICMP *echo* トラフィック用の IP ACE を作成する例を示します。

```
Console> (enable) set qos acl ip my_IPacl trust-ipprec microflow my-micro
aggregate my-agg icmp any any echo
my_IPacl editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

IGMP トラフィック用の IP ACE

（注） IGMP スヌーピングがイネーブルの場合、QoS は IGMP トラフィックをサポートしていません。

IGMP トラフィック用の IP ACE を作成または変更するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	IGMP トラフィック用の IP ACE を作成または変更します。	**set qos acl ip** *acl_name* {**dscp** *dscp_value* | **trust-cos** | **trust-ipprec** | **trust-dscp**} [**microflow** *microflow_name*] [**aggregate** *aggregate_name*] **igmp** *src_ip_spec dest_ip_spec* [*igmp_type*] [**precedence** *precedence_value* | **dscp-field** *dscp*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]
ステップ 2	設定を確認します。	**show qos acl info** {**acl_name** | **all**} **editbuffer** [*editbuffer_index*]

igmp_type パラメータ キーワード オプションについては、「IP ACE レイヤ 4 IGMP の分類基準」（p.49-21）を参照してください。

次に、IGMP Protocol Independent Multicast（PIM）トラフィック用の IP ACE を作成する例を示します。

```
Console> (enable) set qos acl ip my_IPacl trust-ipprec microflow my-micro
aggregate my-agg igmp any any pim
my_IPacl editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

その他のレイヤ 4 プロトコル用の IP ACL

パラメータを追加して、すべてのレイヤ 4 プロトコルと一致する名前付き IP ACL を作成または変更するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	IP ACE を作成または変更します。	**set qos acl ip** *acl_name* {**dscp** *dscp_value* | **trust-cos** | **trust-ipprec** | **trust-dscp**} [**microflow** *microflow_name*] [**aggregate** *aggregate_name*] *protocol src_ip_spec dest_ip_spec* [**precedence** *precedence_value* | **dscp-field** *dscp*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]
ステップ 2	設定を確認します。	**show qos acl info** {**acl_name** | **all**} **editbuffer** [*editbuffer_index*]

(注)　Release 8.3(1) 以降のソフトウェア リリースでは、**output** キーワードを適用した ACL が **trust-cos** および **trust-ipprec** キーワードをサポートします。

protocol パラメータ キーワード オプションについては、「IP ACE レイヤ 4 プロトコルの分類基準」（p.49-18）を参照してください。

次に、IPINIP トラフィック用の IP ACE を作成する例を示します。

```
Console> (enable) set qos acl ip my_IPacl trust-ipprec microflow my-micro
aggregate my-agg ipinip any any
my_IPacl editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

すべての IP トラフィック用の IP ACE

すべての IP トラフィックに一致する IP ACE を作成または変更するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	IP ACE を作成または変更します。	**set qos acl ip** *acl_name* {**dscp** *dscp* | **trust-cos** | **trust-ipprec** | **trust-dscp**} [**microflow** *microflow_name*] [**aggregate** *aggregate_name*] *src_ip_spec* [**precedence** *precedence* | **dscp-field** *dscp*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]
ステップ 2	設定を確認します。	**show qos acl info** {**acl_name** | **all**} **editbuffer** [*editbuffer_index*]

次に、IP ACE を作成する例を示します。

```
Console> (enable) set qos acl ip my_IPacl trust-ipprec microflow my-micro
aggregate my-agg any
my_IPacl editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

デフォルトの IP ACL の変更

ここでは、デフォルトの IP ACL を変更する方法について説明します。

- デフォルトの IP 入力 ACL の変更（p.49-50）
- デフォルトの IP 出力 ACL の変更（p.49-50）

デフォルトの IP 入力 ACL の変更

デフォルトの IP 入力 ACL を変更するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	デフォルトの IP ACL を変更します。	**set qos acl default-action ip** {**dscp** *dscp* | **trust-cos** | **trust-ipprec** | **trust-dscp**} [**microflow** *microflow_name*] [**aggregate** *aggregate_name*] [**input**]
ステップ 2	設定を確認します。	**show qos acl info default-action** {**ip** | **ipx** | **mac** | **all**}

（注）　**input** キーワードをサポートしているのは PFC3 だけです。

詳細については、「デフォルトの ACL」（p.49-22）を参照してください。

次に、デフォルトの IP ACL を変更する例を示します。

```
Console> (enable) set qos acl default-action ip dscp 5 microflow my-micro
aggregate my-agg
QoS default-action for IP ACL is set successfully.
Console> (enable)
```

デフォルトの IP 出力 ACL の変更

（注）　このコマンドをサポートしているのは PFC3 だけです。

デフォルトの IP 出力 ACL を変更するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	デフォルトの IP ACL を変更します。	**set qos acl default-action ip** {**dscp** *dscp* | **trust-dscp**} [**aggregate** *aggregate_name*] **output**
ステップ 2	設定を確認します。	**show qos acl info default-action ip**

（注）　デフォルトの出力 ACL では、**trust-dscp** キーワードにより、ACL は受信した DSCP 値ではなく、内部 DSCP 値を信頼するようになります（「内部 DSCP 値」[p.49-16] を参照）。

詳細については、「デフォルトの ACL」（p.49-22）を参照してください。

次に、デフォルトの IP ACL を変更する例を示します。

```
Console> (enable) set qos acl default-action ip dscp 5 microflow my-micro
aggregate my-agg
QoS default-action for IP ACL is set successfully.
Console> (enable)
```

名前付き IPX ACL の作成または変更

（注） PFC3 は、IPX トラフィックには QoS を提供しません。MAC ACL を使用して IPX トラフィックをフィルタリングする方法の詳細については、「MAC ACE レイヤ 2 の分類基準」（p.49-21）を参照してください。

名前付き IPX ACL を作成または変更するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	名前付き IPX ACL を作成または変更します。	PFC の場合： **set qos acl ipx** *acl_name* {**dscp** *dscp_value* | **trust-cos**} [**aggregate** *aggregate_name*] *protocol src_net* [*dest_net*[*.dest_node*] [[*dest_net_mask*] *.dest_node_mask*]] [**before** *editbuffer_index* | **modify** *editbuffer_index*] PFC2 の場合： **set qos acl ipx** *acl_name* **aggregate** *aggregate_name protocol src_net* [*dest_net*[*.dest_node*] [[*dest_net_mask*] *.dest_node_mask*]] [**before** *editbuffer_index* | **modify** *editbuffer_index*]
ステップ 2	設定を確認します。	**show qos acl info** {**acl_name** | **all**} **editbuffer** [*editbuffer_index*]

protocol パラメータは、数字（0 ～ 255）または次のキーワードで指定します。**any**、**ncp**（17）、**netbios**（20）、**rip**（1）、**sap**（4）、**spx**（5）です。

src_net パラメータおよび *dest_net* パラメータは、IPX ネットワーク番号です。1 ～ FFFFFFFE の範囲（-1 はすべてのネットワーク番号と一致）で最大 8 桁の 16 進数として入力します。先行ゼロは不要です。

IPX 宛先ネットワークを指定した場合、IPX ACE は次のオプション パラメータをサポートしています。

- IPX 宛先ネットワーク マスク。1 ～ FFFFFFFE の範囲（-1 はすべてのネットワーク番号と一致）で最大 8 桁の 16 進数として入力します。ワイルドカードが必要な場合は、1 ビットを使用します。連続させる必要はありません。
- IPX 宛先ノード。12 桁の 16 進数（48 ビット）として入力します。形式はドットで区切った 4 桁の 16 進数が 3 組です（xxxx.xxxx.xxxx）。
- IPX 宛先ノードを指定する場合、IPX ACE は 12 桁の 16 進数（48 ビット）として入力された IPX 宛先ノード マスクをサポートしています。形式はドットで区切った 4 桁の 16 進数が 3 組です（xxxx.xxxx.xxxx）。ワイルドカードが必要な場合は、1 ビットを使用します。連続させる必要はありません。

次に、IPX ACE を作成する例を示します。

```
Console> (enable) set qos acl ipx my_IPXacl trust-cos aggregate my-agg -1
my_IPXacl editbuffer modified. Use ‘commit’ command to apply changes.
Console> (enable)
```

名前付き MAC ACL の作成または変更

名前付き MAC ACL を作成または変更するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	名前付き MAC ACL を作成または変更します。	PFC、PFC2、または PFC3 の場合： **set qos acl mac** *acl_name* {**dscp** *dscp_value* | **trust-cos**} [**aggregate** *aggregate_name*] *src_mac_spec dest_mac_spec* [*ethertype*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]
ステップ 2	設定を確認します。	**show qos acl info** {**acl_name** | **all**} **editbuffer** [*editbuffer_index*]

MAC アドレスおよびマスクとして、*src_mac_spec* および *dest_mac_spec* パラメータを入力します。各パラメータは 12 桁の 16 進数（48 ビット）で、ダッシュで区切られたペアの形式です。ワイルドカードが必要な場合は、1 ビットを使用します。連続させる必要はありません。0-0-0-0-0-0 ff-ff-ff-ff-ff-ff という MAC アドレスおよびマスクには **any** キーワードを使用します。すべてゼロのマスク（*mac_address* 0-0-0-0-0-0）を指定する場合は、MAC アドレスとともに **host** キーワードを使用します。

ethertype パラメータは、**0x** で始まる 4 桁の 16 進数（16 ビット）（たとえば 0x0600）、またはキーワードとして入力します（「MAC ACE レイヤ 2 の分類基準」[p.49-21] を参照）。

次に、MAC ACE を作成する例を示します。

```
Console> (enable) set qos acl mac my_MACacl trust-cos aggregate my-agg any any
my_MACacl editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

（注） Ethertype パラメータを含まない QoS MAC ACL は、Ethertype フィールドのどの値を持つトラフィックとも一致します。したがって、IP および IPX を除く任意のトラフィックに、MAC レベルの QoS を適用できます。

デフォルトの IPX および MAC ACL の作成または変更

（注） PFC3 は、IPX トラフィックには QoS を提供しません。

デフォルトの IPX および MAC ACL を作成または変更するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	デフォルトの IPX ACL または MAC ACL を、作成または変更します。	PFC の場合： **set qos acl default-action** {**ipx** | **mac**} {**dscp** *dscp* | **trust-cos**} [**aggregate** *aggregate_name*] PFC2 の場合： **set qos acl default-action** {**ipx** | **mac**} **aggregate** *aggregate_name* PFC3 の場合： **set qos acl default-action mac aggregate** *aggregate_name*
ステップ 2	設定を確認します。	**show qos acl info default-action** {**ip** | **ipx** | **mac** | **all**}

詳細については、「デフォルトの ACL」（p.49-22）を参照してください。

次に、デフォルトの IPX ACL を変更する例を示します。

```
Console> (enable) set qos acl default-action ipx dscp 5 aggregate my-agg
QoS default-action for IPX ACL is set successfully.
Console> (enable)
```

（注）　IPX および MAC の ACL は、マイクロフロー ポリサーをサポートしていません。

名前付き ACL の削除

名前付き ACL を削除にするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	名前付き ACL を削除します。	**clear qos acl** *acl_name* [*editbuffer_index*]
ステップ 2	設定を確認します。	**show qos acl info** {*acl_name* | **all**}

次に、icmp_acl という名前の ACL を削除する例を示します。

```
Console> (enable) clear qos acl icmp_acl 1
ACL icmp_acl ACE# 1 is deleted.
icmp_acl editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

デフォルト ACL のデフォルト値に戻す場合

デフォルト ACL のデフォルト値に戻すには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	デフォルト ACL のデフォルト値に戻します。	**clear qos acl default-action** {**ip** | **ipx** | **mac**} [**tx**]
ステップ 2	設定を確認します。	**show qos acl info default-action** {**ip** | **ipx** | **mac** | **all**}

次に、デフォルト IP ACL のデフォルト値に戻す例を示します。

```
Console> (enable) clear qos acl default-action ip
Hardware programming in progress...
QoS default-action for IP ACL is restored to default setting.
Console> (enable)
```

コミットされていない ACL の廃棄

コミットされていない新しい ACL、または既存の ACL に対するコミットされていない変更を廃棄するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	コミットされていない ACL を廃棄します。	**rollback qos acl** {*acl_name* | **all**}
ステップ 2	既存の ACL に対する変更を廃棄した場合は、設定を確認します。	**show qos acl info** {*acl_name* | **all**}

次に、まだコミットされていない my_acl という名前の ACL を廃棄する例を示します。

```
Console> (enable) rollback qos acl my_acl
Rollback for QoS ACL my_acl is successful.
Console> (enable)
```

(注)　デフォルト ACL に対する変更はただちに有効になり、廃棄することはできません。

ACL のコミット

名前付き ACL を作成、変更、削除した場合、変更はメモリの編集バッファ内に一時的に格納されます。ACL をコミットして使用できるようにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ACL をコミットします。	**commit qos acl** *acl_name*
ステップ 2	設定を確認します。	**show config qos acl** {*acl_name* | **all**}

次に、my_acl という名前の ACL をコミットする例を示します。

```
Console> (enable) commit qos acl my_acl
Hardware programming in progress...
ACL my_acl is committed to hardware.
Console> (enable)
```

(注)　インターフェイスにすでに付加されている ACL をコミットした場合、新しい値がただちに有効になります。デフォルト ACL に対する変更には、コミットは不要です。

QoS ACL の保存場所については、「VACL および QoS ACL の設定およびフラッシュ メモリへの保存」（p.15-67）を参照してください。

インターフェイスへの ACL の付加

(注)　レイヤ 2 スイッチング エンジンを搭載した Supervisor Engine 1 は、このコマンドをサポートしていません。

以下のことが可能です。

- 入力トラフィックの場合、各タイプ（IP、IPX、MAC レイヤ）の 1 つの ACL を各 VLAN に付加します。
- 入力トラフィックの場合、各タイプ（IP、IPX、MAC レイヤ）の 1 つの ACL を、ポート ベース QoS で設定した各ポートに付加します。VLAN ベースの QoS で設定されたポートには、ACL を付加できません（詳細については「ポートベースまたは VLAN ベース QoS のイネーブル化」[p.49-40] を参照）。
- PFC3 では、出力トラフィックの場合、IP ACL を各 VLAN に付加します。

あるタイプ（IP、IPX、または MAC レイヤ）の ACL がインターフェイスにすでに付加されているときに、同じタイプの別の ACL を付加すると、以前の ACL が切り離されます。

ポートまたは VLAN に ACL を付加するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	インターフェイスに ACL を付加します。	**set qos acl map** *acl_name* {*mod/port* [**input**] | *vlan* [**input** | **output**]}
ステップ 2	設定を確認します。	**show qos acl map** {**config** | **runtime**} {*acl_name* | *mod/port* | *vlan* | **all**}

(注)　**input** および **output** キーワードをサポートしているのは PFC3 だけです。

(注)　Release 8.3(1) 以降のソフトウェア リリースでは、**output** キーワードで VLAN に付加された ACL も **trust-cos** および **trust-ipprec** キーワードをサポートします。

次に、test という名前の ACL を VLAN 1 に付加して入力トラフィックをフィルタリングする例を示します。

```
Console> (enable) set qos acl map test 1
ACL test is successfully mapped to vlan 1 on input side.
Console> (enable)
```

次に、test2 という名前の ACL を VLAN 1 に付加して出力トラフィックをフィルタリングする例を示します。

```
Console> (enable) set qos acl map test2 1 output
ACL test2 is successfully mapped to vlan 1 on output side.
Console> (enable)
```

(注)　デフォルトの ACL は、インターフェイスに付加する必要はありません。

インターフェイスからの ACL の切り離し

（注） レイヤ 2 スイッチング エンジンを搭載した Supervisor Engine 1 は、このコマンドをサポートしていません。

ポートまたは VLAN から ACL を切り離すには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	インターフェイスから ACL を切り離します。	**clear qos acl map** *acl_name* {*mod/port* [**input**] | *vlan* [**input** | **output**] | **all**}
ステップ 2	設定を確認します。	**show qos acl map** {**config** | **runtime**} {*acl_name* | *mod/port* | *vlan* | **all**}

（注） **input** および **output** キーワードをサポートしているのは PFC3 だけです。

次に、ポート 2/1 から my_acl という名前の ACL を切り離す例を示します。

```
Console> (enable) clear qos acl map my_acl 2/1
Hardware programming in progress...
ACL my_acl is detached from port 2/1.
Console> (enable)
```

次に、VLAN 4 から my_acl という名前の ACL を切り離す例を示します。

```
Console> (enable) clear qos acl map my_acl 4
Hardware programming in progress...
ACL my_acl is detached from vlan 4.
Console> (enable)
```

（注） デフォルトの ACL をインターフェイスから切り離すことはできません。

PFC3 出力 DSCP 変換の設定

ここでは、PFC3 出力 DSCP 変換の設定方法について説明します。

- DSCP 変換マップの設定（p.49-57）
- 設定済み DSCP 変換マップの消去（p.49-58）
- VLAN への DSCP 変換マップの適用（p.49-58）
- VLAN への DSCP 変換マップの消去（p.49-58）

DSCP 変換マップの設定

PFC3 は、16 個の DSCP 変換マップをサポートしています。QoS は、デフォルト マッピング用に 1 つの変換マップを使用します。設定できる変換マップは 15 個です。この変換マップでは、内部 DSCP と出力 DSCP との関係を定義します。

DSCP 変換マップを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	DSCP 変換マップを設定します。	**set qos dscp-mutation-map** *map_id* *internal_dscp_list*:*mutated_dscp*...
ステップ 2	設定を確認します。	**show qos maps** {**config** | **runtime**} **dscp-mutation-map** *map_id*

次に、DSCP 変換マップ 1 を設定する例を示します。

```
Console> (enable) set qos dscp-mutation-map 1 30:2
QoS dscp-mutation-map with mutation-table-id 1 has been set correctly.
Console> (enable)
```

次に、DSCP 変換マップ 1 を確認する例を示します。

```
Console> (enable) show qos maps config dscp-mutation-map 1
VLAN ID map:
Map ID  VLANS
------  ----------------------------------------
     1  1,78-1005,1025-4094
DSCP mutation map 1:
DSCP                              Policed DSCP
--------------------------------  ------------
                                0  0
                                1  1
                                2  1
                                3  1
                                4  1
                                5  1
                                6  1
                                7  1
                                8  1
                                9  9
                               10  1
                               11  11
                               12  12
                               13  13
                               14  14
                               15  15
.
.
.
                               59  59
                               60  60
                               61  61
                               62  62
                               63  63
Console> (enable)
```

設定済み DSCP 変換マップの消去

設定済みの DSCP 変換マップを消去するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	設定済みの DSCP 変換マップを消去します。	**clear qos dscp-mutation-map** *vlan_mapped_id* | **all**
ステップ 2	設定を確認します。	**show qos maps** {**config** | **runtime**} **dscp-mutation-map** *map_id*

次に、DSCP 変換マップ 3 を消去する例を示します。

```
Console> (enable) clear qos dscp-mutation-map 3
QoS dscp-mutation-map for mutation-table-id 3 is restored to default.
Console> (enable)
```

VLAN への DSCP 変換マップの適用

DSCP 変換マップを VLAN に適用するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	DSCP 変換マップを VLAN に適用します。	**set qos dscp-mutation-table-map** *map_id vlan_list*
ステップ 2	設定を確認します。	**show qos maps** {**config** | **runtime**} **mutation-table-id** *map_id*

次に、DSCP 変換マップ 1 を VLAN 3 および 20 ～ 30 に適用する例を示します。

```
Console> (enable) set qos dscp-mutation-table-map 1 3,20-30
VLAN(s) 3,20-30 are mapped to mutation-table-id 1.
Console> (enable)
```

次に、VLAN/ 変換マップのマッピングを確認する例を示します。

```
Console> (enable) show qos maps config mutation-table-id 1
VLAN ID map:
Map ID VLANs
------ ----------------------------
1      1,20-30
```

VLAN への DSCP 変換マップの消去

DSCP 変換マップを VLAN から消去するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	DSCP 変換マップを VLAN から消去します。	**clear qos dscp-mutation-table-map** {*map_id* | *vlan_id* | **all**}
ステップ 2	設定を確認します。	**show qos maps** {**config** | **runtime**} **dscp-mutation-map** *map_id*

次に、VLAN と DSCP 変換マップ 2 とのアソシエーションを消去する例を示します。

```
Console> (enable) clear qos dscp-mutation-table-map 2
All VLANS in mutation-table-id 2 are cleared.
```

次に、VLAN 3 ～ 33 と DSCP 変換マップとのアソシエーションを消去する例を示します。

```
Console> (enable) clear qos dscp-mutation-table-map 3-33
VLAN(s) 3-33 are removed from mutation-table-ids.
```

次に、すべての VLAN とすべての DSCP 変換マップとのアソシエーションを消去する例を示します。

```
Console> (enable) clear qos dscp-mutation-table-map all
All VLANs are removed from mutation-table-ids.
```

802.1Q トンネル ポートでの CoS/CoS マッピングの設定

入力 CoS/CoS マッピングは、WS-X6704-10GE、WS-X6724-SFP、WS-X6748-GE-TX スイッチング モジュールの 802.1Q トンネル ポートでサポートされています。802.1Q トンネル ポートとして設定されていないポートでは、CoS/CoS マッピングはディセーブルです。

CoS/CoS マップの定義

CoS/CoS マップを定義するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	CoS/CoS マッピングを定義します。	**set qos cos-cos-map** *CoS_value*
ステップ 2	設定を確認します。	**show qos maps cos-cos-map** [*mod/port*]

次に、CoS/CoS マップを定義する例を示します。

```
Console> (enable) set qos cos-cos-map 3 2 1 4 5 6 7 4
QoS cos-cos-map set successfully.
Console> (enable)
```

ポートでの CoS/CoS マップのイネーブル化

CoS/CoS マップをポートでイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	802.1Q トンネル ポートで CoS/CoS マップをイネーブルにします。	**set port qos** *mod/port* **trust trust-cos**
ステップ 2	ポート QoS の信頼設定を確認します。	**show port qos** *mod/port*

```
Console> (enable) set port qos 1/1 trust trust-cos
Port 1/1 qos set to trust-cos
Console> (enable)
```

（注） 802.1Q トンネル ポートのポート信頼が **trust-cos** でない場合、CoS/CoS マップは自動的にディセーブルになります。

CoS/CoS マップの消去

CoS/CoS マップを消去するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	802.1Q トンネル ポートで CoS/CoS マップを消去します。	**clear qos cos-cos-map**
ステップ 2	QoS 設定を確認します。	**show qos maps cos-cos-map** [*mod/port*]

次に、CoS/CoS マッピングを消去する例を示します。

```
Console> (enable) clear qos cos-cos-map
QoS cos-cos-map setting restored to default.
Console> (enable)
```

ホスト宛先 MAC アドレス /VLAN ペアへの CoS 値のマッピング

(注)　QoS が次のコマンドをサポートしているのはレイヤ 2 スイッチング エンジンを使用する場合に限定されます。

特定のホスト宛先 MAC アドレス /VLAN 番号値のペアを宛先とするすべてのフレームに CoS 値をマッピングするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ホスト宛先 MAC アドレス /VLAN 番号値のペアに CoS 値をマッピングします。	**set qos mac-cos** *dest_mac VLAN cos_value*
ステップ 2	設定を確認します。	**show qos mac-cos** {*dest_mac* [*vlan*] | **all**}

次に、宛先 MAC アドレスおよび VLAN 525 に CoS 2 をマッピングする例を示します。

```
Console> (enable) set qos mac-cos 00-40-0b-30-03-48 525 2
CoS 2 is assigned to 00-40-0b-30-03-48 vlan 525.
Console> (enable)
```

ホスト宛先 MAC アドレス /VLAN ペアに割り当てられた CoS 値の削除

(注)　QoS が次のコマンドをサポートしているのはレイヤ 2 スイッチング エンジンを使用する場合に限定されます。

ホスト宛先 MAC アドレス /VLAN 番号値のペアに割り当てられた CoS を削除するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ホスト宛先 MAC アドレス /VLAN 番号値のペアに割り当てられた CoS 値を削除します。	**clear qos mac-cos** {*dest_mac* [*vlan*] | **all**}
ステップ 2	設定を確認します。	**show qos mac-cos** {*dest_mac* [*vlan*] | **all**}

次に、宛先 MAC アドレス /VLAN に割り当てられたすべての CoS を削除する例を示します。

```
Console> (enable) clear qos mac-cos all
All CoS to Mac/Vlan entries are cleared.
Console> (enable)
```

ブリッジド トラフィックに対するマイクロフロー ポリシングのイネーブル化およびディセーブル化

(注)　レイヤ 2 スイッチング エンジンを搭載した Supervisor Engine 1 は、このコマンドをサポートしていません。

デフォルトでは、マイクロフロー ポリサーはレイヤ 3 スイッチングされるトラフィックだけに影響します。スイッチ上または特定の VLAN 上でブリッジド トラフィックに対してマイクロフロー ポリシングをイネーブルまたはディセーブルにするには、イネーブル モードで次のいずれかの作業を行います。

作業	コマンド
スイッチ上または特定の VLAN 上で、ブリッジド トラフィックに対するマイクロフロー ポリシングをイネーブルにします。	**set qos bridged-microflow-policing** {**enable** | **disable**} *vlan*
スイッチ上または特定の VLAN 上で、ブリッジド トラフィックに対するマイクロフロー ポリシングをディセーブルにします。	**set qos bridged-microflow-policing** {**enable** | **disable**} *vlan*
設定を確認します。	**show qos bridged-microflow-policing runtime** {**config** | **runtime**} *vlan*

(注)　Layer 3 Switching Engine II では、マイクロフロー ポリシングを実行する場合には、ブリッジド トラフィックのマイクロフロー ポリシングをイネーブルにする必要があります。

詳細については、「ポリサー」（p.49-24）を参照してください。

次に、VLAN 1 ～ 20 のトラフィックに対してマイクロフロー ポリシングをイネーブルにする例を示します。

```
Console> (enable) set qos bridged-microflow-policing enable 1-20
QoS microflow policing is enabled for bridged packets on vlans 1-20.
Console> (enable)
```

標準受信キュー テール廃棄スレッシュホールドの設定

スイッチ上で標準受信キュー テール廃棄スレッシュホールドを設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
標準受信キュー テール廃棄スレッシュホールドを設定します。	**set qos drop-threshold** *port_type* **rx queue 1** *thr1 thr2 thr3 thr4*

詳細については、「受信キュー」（p.49-13）を参照してください。

QoS は、**1q2t**、**1q4t**、および **1p1q4t** ポートに関して個別の設定を維持します。このコマンドは標準キューを設定します。キュー 1 を指定します（完全優先キューのスレッシュホールドは、存在する場合は個別に設定できないので、キュー 1 に指定されたスレッシュホールド 4 を使用します）。

スレッシュホールドはすべて割合（1 ～ 100）として指定します。10 という値は、バッファが 10% 満たされている場合のスレッシュホールドを意味します。

次に、標準受信キュー テール廃棄スレッシュホールドを設定する例を示します。

```
Console> (enable) set qos drop-threshold 1q4t rx queue 1 20 40 75 100
Receive drop thresholds for queue 1 set at 20% 40% 75% 100%
Console> (enable)
```

（注） **1p1q0t** 受信キューには、廃棄スレッシュホールドを設定できません。

2q2t ポート標準送信キュー テール廃棄スレッシュホールドの設定

すべての **2q2t** ポート上で標準送信キュー テール廃棄スレッシュホールドを設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
すべての **2q2t** ポート上で標準送信キュー テール廃棄スレッシュホールドを設定します。	**set qos drop-threshold** *port_type* **tx queue** *q# thr1 thr2*

キュー番号 1 はロー プライオリティ送信キュー、キュー番号 2 はハイ プライオリティ キューです。どちらのキューでも、ロー プライオリティ スレッシュホールド番号が 1、ハイ プライオリティ スレッシュホールド番号が 2 です。

スレッシュホールドはすべて割合（1 ～ 100）として指定します。10 という値は、バッファが 10% 満たされている場合のスレッシュホールドを意味します。

次に、ロー プライオリティ送信キューのテール廃棄スレッシュホールドを設定する例を示します。

```
Console> (enable) set qos drop-threshold 2q2t tx queue 1 40 100
Transmit drop thresholds for queue 1 set at 40%  100%
Console> (enable)
```

（注） **1p3q1t** 送信キューには、テール廃棄スレッシュホールドを設定できません。

標準キュー WRED 廃棄スレッシュホールドの設定

1p1q8t ポートは、標準受信キュー内に WRED 廃棄スレッシュホールドが設定されています。

1p2q2t、**1p3q1t**、**1p2q1t**、**1p3q8t**、および **1p7q8t** ポートは、標準送信キュー内に WRED 廃棄スレッシュホールドが設定されています。

(注)　**1p7q8t**（送信）、**1p3q1t**（送信）、**1p2q1t**（送信）、および **1p1q8t**（受信）ポートは、設定不可能なテール廃棄スレッシュホールドも備えています。

各タイプのすべてのポート上で標準キュー WRED 廃棄スレッシュホールドを設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
指定のタイプのすべてのポート上で標準キュー WRED 廃棄スレッシュホールドを設定します。	**set qos wred 1p1q8t rx queue** *q#* [*thr1Lo*:]*thr1Hi* [*thr2Lo*:]*thr2Hi* [*thr_n_Lo*:]*thr_n_Hi*...[*thr8Lo*:]*thr8Hi* **set qos wred 1p7q8t tx queue** *q#* [*thr1Lo*:]*thr1Hi* [*thr2Lo*:]*thr2Hi* [*thr_n_Lo*:]*thr_n_Hi*...[*thr8Lo*:]*thr8Hi* **set qos wred 1p3q8t tx queue** *q#* [*thr1Lo*:]*thr1Hi* [*thr2Lo*:]*thr2Hi* [*thr_n_Lo*:]*thr_n_Hi*...[*thr8Lo*:]*thr8Hi* **set qos wred 1p2q2t tx queue** *q#* [*thr1Lo*:]*thr1Hi* [*thr2Lo*:]*thr2Hi* **set qos wred 1p3q1t tx queue** *q#* [*thr1Lo*:]*thr1Hi* **set qos wred 1p2q1t tx queue** *q#* [*thr1Lo*:]*thr1Hi*

1p1q8t ポートを設定する場合、次の事項に注意してください。

- キュー 1 は単一標準受信キューです。
- 単一標準受信キューを設定する場合は、次の事項に注意してください。
  - 最初に入力した値によって、最下位プライオリティ スレッシュホールドが設定されます。
  - 次に入力した値によって、2 番めに高いプライオリティ スレッシュホールドが設定されます。
  - 8 番めに入力した値によって、最上位のプライオリティ スレッシュホールドが設定されます。

1p7q8t ポートを設定する場合、次の事項に注意してください。

- キュー 1 は最低プライオリティ標準送信キューです。
- キュー 7 は最高プライオリティ標準送信キューです。
- 各標準送信キューを設定する場合は、次の事項に注意してください。
  - 最初に入力した値によって、最下位プライオリティ スレッシュホールドが設定されます。
  - 次に入力した値によって、2 番めに高いプライオリティ スレッシュホールドが設定されます。
  - 8 番めに入力した値によって、最上位のプライオリティ スレッシュホールドが設定されます。

1p3q8t ポートを設定する場合、次の事項に注意してください。

- キュー 1 はロー プライオリティ標準送信キューです。
- キュー 2 はミディアム プライオリティ標準送信キューです。
- キュー 3 はハイ プライオリティ標準送信キューです。
- 各標準送信キューを設定する場合は、次の事項に注意してください。
  - 最初に入力した値によって、最下位プライオリティ スレッシュホールドが設定されます。
  - 次に入力した値によって、2 番めに高いプライオリティ スレッシュホールドが設定されます。
  - 8 番めに入力した値によって、最上位のプライオリティ スレッシュホールドが設定されます。

1p2q2t ポートを設定する場合、次の事項に注意してください。

- キュー 1 はロー プライオリティ標準送信キューです。
- キュー 2 はハイ プライオリティ標準送信キューです。
- 各標準送信キューを設定する場合は、次の事項に注意してください。
  - 最初に入力した値によって、ロー プライオリティ スレッシュホールドが設定されます。
  - 次に入力した値によって、ハイ プライオリティ スレッシュホールドが設定されます。

1p3q1t ポートを設定する場合、次の事項に注意してください。

- キュー 1 はロー プライオリティ標準送信キューです。
- キュー 2 はミディアム プライオリティ標準送信キューです。
- キュー 3 はハイ プライオリティ標準送信キューです。
- 各標準送信キューを設定する場合は、入力した 1 つの値によってスレッシュホールドが設定されます。

1p2q1t ポートを設定する場合、次の事項に注意してください。

- キュー 1 はロー プライオリティ標準送信キューです。
- キュー 2 はハイ プライオリティ標準送信キューです。
- 各標準送信キューを設定する場合は、入力した 1 つの値によってスレッシュホールドが設定されます。

スレッシュホールドを設定する場合、次の事項に注意してください。

- スレッシュホールドはすべて割合（0 ～ 100）として指定します。10 という値は、バッファが 10% 満たされている場合のスレッシュホールドを意味します。
- 下限 WRED スレッシュホールドと上限 WRED スレッシュホールドの両方を設定できます。下限スレッシュホールドは、上限スレッシュホールドよりも低い割合に設定する必要があります。
- 下限 WRED スレッシュホールドは、この値以下のトラフィックは廃棄されないトラフィック レベルです。上限 WRED スレッシュホールドは、この値を超えるトラフィックがすべて廃棄されるトラフィック レベルです。下限と上限の WRED スレッシュホールドの間では、キューにあるトラフィックは、キューがいっぱいになるにつれて廃棄される可能性が高くなります。デフォルトの下限 WRED スレッシュホールドは 0 です（廃棄される可能性がすべてのトラフィックにあります）。

次に、ロー プライオリティ送信キューの WRED 廃棄スレッシュホールドを設定する例を示します。

```
Console> (enable) set qos wred 1p2q2t queue 1 40:70 70:100
WRED thresholds for queue 1 set to 40:70 and 70:100 on all WRED-capable 1p2q2t ports.
Console> (enable)
```

（注） 完全優先キューのスレッシュホールドは設定できません。

標準送信キュー間の帯域幅の割り当て

スイッチはデキューイング アルゴリズムの 1 つを使用して、一度に 1 つの標準キューからフレームを送信します。デキューイング アルゴリズムは重み値を使用して、ラウンドロビン方法で処理されるように相対的な帯域幅を各キューに割り当てます。

- SRR ― Supervisor Engine 32 **1p3q8t** ポート上のオプションとしてサポートされています。SRR をイネーブルにしない場合、DWRR が使用されます。SRR では、キューは重み値が割り当てる特定の帯域幅だけを使用できます。
- DWRR ― **1p3q1t**、**1p2q1t**、**1p3q8t**、および **1p7q8t** ポート上でサポートされています。DWRR は、送信の際にすべてのロー プライオリティ キューを追跡し、次のラウンドを補正します。
- WRR ― 他のすべてのポートでサポートされています。WRR では、他のキューが帯域幅を使用していない場合に、キューは割り当てられている以上の帯域幅（最大でポートの総帯域幅まで）を使用できます。

キューに設定する重みが大きいほど、多くの送信帯域幅がそのキューに割り当てられます。重み値の比率によってキューの総帯域幅が分割されます。たとえば、重み値が 25:25:50 のギガビット イーサネット ポートの 3 つのキューの分配は、次のようになります。

- キュー 1 ― 250 Mbps
- キュー 2 ― 250 Mbps
- キュー 3 ― 500 Mbps

（注） 実際の帯域幅の分配は、ポート　ハードウェアが設定された重み値に適用する粒度によって決まります。

標準送信キュー間で帯域幅を割り当てるには、イネーブル モードで次の作業を行います。

作業	コマンド
標準送信キュー間で帯域幅を割り当てます。	**set qos wrr** *port_type queue1-weight queue2-weight* [*queue3-weight*] [**srr**]

port_type パラメータの有効値は、**2q2t**、**1p2q2t**、**1p3q1t**、**1p2q1t**、**1p3q8t**、および **1p7q8t** です。

QoS では、ポート タイプごとに個別の設定を維持します。このコマンドによって設定されるのは、標準キューだけです。完全優先キューは設定不要です。有効な重み値の範囲は 1 ～ 255 です。

次に、**2q2t** ポートに帯域幅を割り当てる例を示します。

```
Console> (enable) set qos wrr 2q2t 30 70
QoS wrr ratio is set successfully.
Console> (enable)
```

受信キュー容量比の設定

1p1q0t ポートおよび **1p1q8t** ポートの場合、ネットワーク上の標準プライオリティと完全優先トラフィックの配分を推定します（たとえば、標準プライオリティ トラフィックが 85%、完全優先トラフィックが 15% など）。推定した割合を使用して、キューの比率を指定します。1 ～ 99 の範囲で、必ず合計が 100 になるようにしてください。

受信キュー容量比を設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
受信キュー 1（標準プライオリティ）と受信キュー 2（完全優先）間で受信キュー容量比を設定します。	**set qos rxq-ratio** {**1p1q0t** | **1p1q8t**} *queue1-val queue2-val*

次に、受信キュー容量比を設定する例を示します。

```
Console> (enable) set qos rxq-ratio 1p1q0t 80 20
QoS rxq-ratio is set successfully.
Console> (enable)
```

送信キュー容量比の設定

2q2t、**1p2q2t**、**1p2q1t**、**1p3q8t**、および **1p7q8t** ポートの場合、ネットワーク上の各種プライオリティのトラフィックの配分を推定します（たとえば、ロー プライオリティ トラフィックが 75%、ハイ プライオリティ トラフィックが 15%、完全優先トラフィックが 10% など）。推定した割合を使用して、キューの比率を指定します。1 ～ 99 の範囲で、必ず合計が 100 になるようにしてください。

ポート タイプごとに送信キュー容量比を設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
送信キュー容量比を設定します。	**set qos txq-ratio** {**2q2t** | **1p2q2t** | **1p2q1t** | **1p3q8t** | **1p7q8t**} *queue1-val queue2-val* [*queue3-val* [*queue4-val*]]

次に、送信キュー容量比を設定する例を示します。

```
Console> (enable) set qos txq-ratio 2q2t 80 20
QoS txq-ratio is set successfully.
Console> (enable)
```

CoS 値と廃棄スレッシュホールドのマッピング

次のコマンドを使用して、CoS 値と送受信キュー廃棄スレッシュホールドを対応付けます。QoS では、ポート タイプごとに個別の設定を維持します。

ここでは、CoS 値と廃棄スレッシュホールド間のマッピングについて説明します。

- 1q4t/2q2t ポートの対応付け（p.49-67）
- 1q8t、1q2t/1p2q2t、および 1p1q4t/1p2q2t ポートの対応付け（p.49-67）
- 1p1q0t/1p3q1t ポートの対応付け（p.49-69）
- 1p1q8t/1p2q1t、1p3q8t、および 1p7q8t ポートの対応付け（p.49-70）
- デフォルトの CoS マッピングに戻す場合（p.49-71）

1q4t/2q2t ポートの対応付け

1q4t/2q2t ポート上では、受信キューと送信キューを同じコマンドで設定します。

1q4t/2q2t ポート上で CoS 値と廃棄スレッシュホールドを対応付けるには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	CoS 値と廃棄スレッシュホールドを対応付けます。	**set qos map 2q2t tx** *q# thr#* **cos** *coslist*
ステップ 2	設定を確認します。	**show qos info config** {**1q4t rx** | **2q2t tx**}

送受信廃棄スレッシュホールド間の関係は、次のとおりです。

- 受信キュー 1（標準）スレッシュホールド 1 = 送信キュー 1（標準ロー プライオリティ）スレッシュホールド 1
- 受信キュー 1（標準）スレッシュホールド 2 = 送信キュー 1（標準ロー プライオリティ）スレッシュホールド 2
- 受信キュー 1（標準）スレッシュホールド 3 = 送信キュー 2（標準ハイ プライオリティ）スレッシュホールド 1
- 受信キュー 1（標準）スレッシュホールド 4 = 送信キュー 2（標準ハイ プライオリティ）スレッシュホールド 2

このコマンドでは、送信キューと送信キュー廃棄スレッシュホールド値を使用します。次に、CoS 値 0 および 1 を、標準受信キュー 1/ スレッシュホールド 1 および標準送信キュー 1/ スレッシュホールド 1 の両方に対応付ける例を示します。

```
Console> (enable) set qos map 2q2t tx 1 1 cos 0,1
Qos tx priority queue and threshold mapped to cos successfully.
Console> (enable)
```

1q8t、1q2t/1p2q2t、および 1p1q4t/1p2q2t ポートの対応付け

1q8t、**1q2t/1p2q2t**、および **1p1q4t/1p2q2t** ポート上では、受信キューと送信キューを個別に設定します。

1q8t 受信キュー

CoS 値と **1q8t** 受信キュー廃棄スレッシュホールドを対応付けるには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	CoS 値と受信キュー廃棄スレッシュホールドを対応付けます。	**set qos map 1q8t rx 1** *thr#* **cos** *coslist*
ステップ 2	設定を確認します。	**show qos info config 1q2t rx**

スレッシュホールド 1 は最低プライオリティ スレッシュホールドです。プライオリティはスレッシュホールド番号とともに増加します。

次に、CoS 値 3 をスレッシュホールド 2 に対応付ける例を示します。

```
Console> (enable) set qos map 1q8t rx 1 2 cos 3
QoS rx priority queue and threshold mapped to cos successfully.
Console> (enable)
```

1q2t 受信キュー

CoS 値と **1q2t** 受信キュー廃棄スレッシュホールドを対応付けるには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	CoS 値と受信キュー廃棄スレッシュホールドを対応付けます。	**set qos map 1q2t rx 1 1 cos** *coslist*
ステップ 2	設定を確認します。	**show qos info config 1q2t rx**

スレッシュホールド 1 はロー プライオリティ スレッシュホールドです。スレッシュホールド 2 はハイ プライオリティ スレッシュホールドであり、設定不可能です。

次に、CoS 値 3 をスレッシュホールド 1 に対応付ける例を示します。

```
Console> (enable) set qos map 1q2t rx 1 1 cos 3
QoS rx priority queue and threshold mapped to cos successfully.
Console> (enable)
```

1p1q4t 受信キュー

CoS 値と **1p1q4t** 受信キュー廃棄スレッシュホールドを対応付けるには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	CoS 値と受信キュー廃棄スレッシュホールドを対応付けます。	**set qos map 1p1q4t rx** *q# thr#* **cos** *coslist*
ステップ 2	設定を確認します。	**show qos info config 1p1q4t rx**

キュー 1 は標準キューです。キュー 2 は完全優先キューです。

スレッシュホールドの番号の範囲は 1（ロー プライオリティ）～ 4（ハイ プライオリティ）です。

次に、完全優先受信キュー 2/ スレッシュホールド 1 に CoS 値 5 を対応付ける例を示します。

```
Console> (enable) set qos map 1p1q4t rx 2 1 cos 5
Qos rx strict queue and threshold mapped to cos successfully.
Console> (enable)
```

1p2q2t 送信キュー

CoS 値と **1p2q2t** 送信キュー廃棄スレッシュホールドを対応付けるには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	CoS 値と送信キュー廃棄スレッシュホールドを対応付けます。	**set qos map 1p2q2t tx** *q# thr#* **cos** *coslist*
ステップ 2	設定を確認します。	**show qos info config 1p2q2t tx**

キュー 1 は標準ロー プライオリティ、キュー 2 はハイ プライオリティ、キュー 3 は完全優先です。

スレッシュホールド 1 はロー プライオリティ、スレッシュホールド 2 はハイ プライオリティです。

次に、完全優先送信キュー 3/ 廃棄スレッシュホールド 1 に CoS 値 5 を対応付ける例を示します。

```
Console> (enable) set qos map 1p2q2t tx 3 1 cos 5
Qos tx strict queue and threshold mapped to cos successfully.
Console> (enable)
```

1p1q0t/1p3q1t ポートの対応付け

1p1q0t/1p3q1t ポート上では、受信キューと送信キューを個別に設定します。

1p1q0t 受信キュー

CoS 値と **1p1q0t** 受信キューを対応付けるには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	CoS 値と受信キューを対応付けます。	**set qos map 1p1q0t rx** *q#* **cos** *coslist*
ステップ 2	設定を確認します。	**show qos info config 1p1q0t rx**

キュー 1 は標準キューです。キュー 2 は完全優先キューです。

次に、CoS 値 5 を完全優先受信キュー 2 に対応付ける例を示します。

```
Console> (enable) set qos map 1p1q0t rx 2 cos 5
QoS queue mapped to cos successfully.
Console> (enable)
```

1p3q1t 送信キュー

1p3q1t 送信キューでは次のように、CoS 値を設定不可能なテール廃棄スレッシュホールドまたは設定可能な WRED 廃棄スレッシュホールドと対応付けることができます。

- CoS 値をテール廃棄スレッシュホールドと対応付けるには、CoS 値をキューにマッピングします。
- CoS 値を WRED 廃棄スレッシュホールドと対応付けるには、CoS 値をキューおよびスレッシュホールドにマッピングします。

CoS 値と **1p3q1t** 送信キュー廃棄スレッシュホールドを対応付けるには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	CoS 値と送信キュー廃棄スレッシュホールドを対応付けます。	**set qos map 1p3q1t tx** *q#* [*thr#*] **cos** *coslist*
ステップ 2	設定を確認します。	**show qos info config 1p3q1t tx**

キュー 1 は標準ロー プライオリティ、キュー 2 はミディアム プライオリティ、キュー 3 はハイ プライオリティ、キュー 4 は完全優先です。

CoS 値をテール廃棄スレッシュホールドにマッピングするには、スレッシュホールド番号を省略するか **0** を入力します。

WRED 廃棄スレッシュホールド番号は 1 です。

次に、CoS 値 0 を送信キュー 1/ 廃棄スレッシュホールド 1 に対応付ける例を示します。

```
Console> (enable) set qos map 1p3q1t tx 1 1 cos 0
Qos tx strict queue and threshold mapped to cos successfully.
Console> (enable)
```

1p1q8t/1p2q1t、1p3q8t、および 1p7q8t ポートの対応付け

1p1q8t/1p2q1t および **1p3q8t** ポートを設定する場合、次の事項に注意してください。

- 受信キューと送信キューは別々に設定します。
- CoS 値は、設定不可能なテール廃棄スレッシュホールドまたは設定可能な WRED 廃棄スレッシュホールドと対応付けることができます。
  - CoS 値をテール廃棄スレッシュホールドと対応付けるには、CoS 値をキューにマッピングします。
  - CoS 値を WRED 廃棄スレッシュホールドと対応付けるには、CoS 値をキューおよびスレッシュホールドにマッピングします。

1p1q8t 受信キュー

CoS 値と **1p1q8t** 受信キュー廃棄スレッシュホールドを対応付けるには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	CoS 値と受信キューを対応付けます。	**set qos map 1p1q8t rx** *q#* [*thr#*] **cos** *coslist*
ステップ 2	設定を確認します。	**show qos info config 1p1q8t rx**

1p1q8t ポート上では、キュー 1 は標準受信キュー、キュー 2 は完全優先受信キューです。

CoS 値をテール廃棄スレッシュホールドにマッピングするには、スレッシュホールド番号を省略するか **0** を入力します。

次に、CoS 値 5 を完全優先受信キュー 2 に対応付ける例を示します。

```
Console> (enable) set qos map 1p1q8t rx 2 cos 5
QoS queue mapped to cos successfully.
Console> (enable)
```

1p2q1t、1p3q8t、および 1p7q8t 送信キュー

CoS 値と **1p2q1t**、**1p3q8t**、または **1p7q8t** 送信キュー廃棄スレッシュホールドを対応付けるには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	CoS 値と送信キュー廃棄スレッシュホールドを対応付けます。	**set qos map** [**1p2q1t** | **1p3q8t** | **1p7q8t**] **tx** *q#* [*thr#*] **cos** *coslist*
ステップ 2	設定を確認します。	**show qos info config 1p2q1t tx**

1p2q1t ポート上では、キュー 1 はロー プライオリティ標準送信キュー、キュー 2 はハイ プライオリティ標準送信キュー、キュー 3 は完全優先送信キューです。

1p3q8t ポート上では、キュー 1 はロー プライオリティ標準送信キュー、キュー 2 はミディアム プライオリティ標準送信キュー、キュー 3 はハイ プライオリティ標準送信キュー、キュー 4 は完全優先送信キューです。

1p7q8t ポート上では、キュー 1 は最低プライオリティ標準送信キュー、キュー 7 は最高プライオリティ標準送信キュー、キュー 8 は完全優先送信キューです。

CoS 値をテール廃棄スレッシュホールドにマッピングするには、スレッシュホールド番号を省略するか **0** を入力します。

次に、CoS 値 0 を送信キュー 1/ 廃棄スレッシュホールド 1 に対応付ける例を示します。

```
Console> (enable) set qos map 1p2q1t tx 1 1 cos 0
Qos tx strict queue and threshold mapped to cos successfully.
Console> (enable)
```

デフォルトの CoS マッピングに戻す場合

デフォルトの CoS 値 / 廃棄スレッシュホールドのマッピングに戻すには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	QoS マップのデフォルトに戻します。	**clear qos map** {**1p1q4t rx** | **1p1q0t rx** | **1p2q2t tx** | **2q2t tx** | **1p3q1t tx** | **1q8t rx** | **1p3q8t tx** | **1p7q8t tx**}
ステップ 2	設定を確認します。	**show qos info config** {**1q4t rx** | **1p1q4t rx** | **1p1q0t rx** | **1p1q8t rx** | **1p2q2t tx** | **2q2t tx** | **1p3q1t tx** | **1p2q1t tx** | **1q8t rx** | **1p3q8t tx** | **1p7q8t tx**}

次に、デフォルトの QoS マッピングに戻す例を示します。

```
Console> (enable) clear qos map 1p3q1t tx
Qos map setting cleared.
Console> (enable)
```

DSCP 値マッピングの設定

（注） レイヤ 2 スイッチング エンジンを搭載した Supervisor Engine 1 は、このコマンドをサポートしていません。

ここでは、DSCP 値を他の値にマッピングする方法について説明します。

- 受信 CoS 値と内部 DSCP 値のマッピング（p.49-71）
- 受信 CoS 値と内部 DSCP 値のマッピング（p.49-72）
- 内部 DSCP 値と出力 CoS 値のマッピング（p.49-73）
- DSCP マークダウン値のマッピング（p.49-73）

受信 CoS 値と内部 DSCP 値のマッピング

受信 CoS 値を内部 DSCP 値（「内部 DSCP 値」[p.49-16] を参照）にマッピングするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	受信 CoS 値を内部 DSCP 値にマッピングします。	**set qos cos-dscp-map** *dscp1 dscp2 dscp3 dscp4 dscp5 dscp6 dscp7 dscp8*
ステップ 2	設定を確認します。	**show qos maps** {**config** | **runtime**} [**cos-dscp-map** | **ipprec-dscp-map** | **dscp-cos-map** | **policed-dscp-map**]

受信 CoS 値 0 ～ 7 のマッピング先として 8 つの DSCP 値を入力します。次に、受信 CoS 値を内部 DSCP 値にマッピングする例を示します。

```
Console> (enable) set qos cos-dscp-map 20 30 1 43 63 12 13 8
QoS cos-dscp-map set successfully.
Console> (enable)
```

デフォルトの CoS 値 /DSCP 値マッピングに戻すには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	デフォルトの CoS 値/DSCP 値マッピングに戻します。	**clear qos cos-dscp-map**
ステップ 2	設定を確認します。	**show qos maps** {**config** | **runtime**} [**cos-dscp-map** | **ipprec-dscp-map** | **dscp-cos-map** | **policed-dscp-map**]

次に、デフォルトの CoS 値 /DSCP 値マッピングに戻す例を示します。

```
Console> (enable) clear qos cos-dscp-map
QoS cos-dscp-map setting restored to default.
Console> (enable)
```

受信 CoS 値と内部 DSCP 値のマッピング

受信 IP precedence 値を内部 DSCP 値（「内部 DSCP 値」[p.49-16] を参照）にマッピングするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	受信 IP precedence 値を内部 DSCP 値にマッピングします。	**set qos ipprec-dscp-map** *dscp1 dscp2 dscp3 dscp4 dscp5 dscp6 dscp7 dscp8*
ステップ 2	設定を確認します。	**show qos maps** {**config** | **runtime**} [**cos-dscp-map** | **ipprec-dscp-map** | **dscp-cos-map** | **policed-dscp-map**]

受信 IP precedence 値 0 ～ 7 のマッピング先として 8 つの内部 DSCP 値を入力します。次に、受信 IP precedence 値を内部 DSCP 値にマッピングする例を示します。

```
Console> (enable) set qos ipprec-dscp-map 20 30 1 43 63 12 13 8
QoS ipprec-dscp-map set successfully.
Console> (enable)
```

デフォルトの IP precedence 値 /DSCP 値マッピングに戻すには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	デフォルトの IP precedence 値 /DSCP 値マッピングに戻します。	**clear qos ipprec-dscp-map**
ステップ 2	設定を確認します。	**show qos maps** {**config** | **runtime**} [**cos-dscp-map** | **ipprec-dscp-map** | **dscp-cos-map** | **policed-dscp-map**]

次に、デフォルトの QoS マッピングに戻す例を示します。

```
Console> (enable) clear qos ipprec-dscp-map
QoS ipprec-dscp-map setting restored to default.
Console> (enable)
```

内部 DSCP 値と出力 CoS 値のマッピング

内部 DSCP 値を、出力ポートのスケジューリングおよび輻輳回避に使用する出力 CoS 値にマッピングするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	内部 DSCP 値を出力 CoS 値にマッピングします。	**set qos dscp-cos-map** *dscp_list:cos ...*
ステップ 2	設定を確認します。	**show qos maps** {**config** | **runtime**} [**cos-dscp-map** | **ipprec-dscp-map** | **dscp-cos-map** | **policed-dscp-map**]

詳細については、「内部 DSCP 値」（p.49-16）および「イーサネット出力ポートのスケジューリング、輻輳回避、およびマーキング」（p.49-28）を参照してください。

内部 DSCP 値 / 出力 CoS 値のペアを、64 個まで入力します。次に、内部 DSCP 値を出力 CoS 値にマッピングする例を示します。

```
Console> (enable) set qos dscp-cos-map 20-25:7 33-38:3
QoS dscp-cos-map set successfully.
Console> (enable)
```

デフォルトの CoS 値 /DSCP 値マッピングに戻すには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	デフォルトの DSCP 値/CoS 値マッピングに戻します。	**clear qos dscp-cos-map**
ステップ 2	設定を確認します。	**show qos maps** {**config** | **runtime**} [**cos-dscp-map** | **ipprec-dscp-map** | **dscp-cos-map** | **policed-dscp-map**]

次に、デフォルトの CoS 値 /DSCP 値マッピングに戻す例を示します。

```
Console> (enable) clear qos dscp-cos-map
QoS dscp-cos-map setting restored to default.
Console> (enable)
```

DSCP マークダウン値のマッピング

ポリサーで使用する DSCP マークダウン値をマッピングするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	DSCP 値をマークダウン DSCP 値にマッピングします。	**set qos policed-dscp-map** *dscp_list:markdown_dscp ...*
ステップ 2	PFC2 で、DSCP 値をマークダウン DSCP 値にマッピングします。	**set qos policed-dscp-map** [**normal** | **excess**] *in_profile_dscp_list:policed_dscp ...*
ステップ 3	設定を確認します。	**show qos maps** {**config** | **runtime**} [**cos-dscp-map** | **ipprec-dscp-map** | **dscp-cos-map** | **policed-dscp-map**]

詳細については、「ポリサー」（p.49-24）を参照してください。

最大 64 個の DSCP 値リスト /DSCP 値のペアを入力します。

次に、DSCP マークダウン値をマッピングする例を示します。

```
Console> (enable) set qos policed-dscp-map 20-25:7 33-38:3
QoS dscp-dscp-map set successfully.
Console> (enable)
```

次に、超過レートを超えるパケットの DSCP マークダウン値をマッピングする例を示します。

```
Console> (enable) set qos policed-dscp-map 33:30
QoS normal-rate policed-dscp-map set successfully.
Console> (enable) set qos policed-dscp-map excess-rate 33:30
QoS excess-rate policed-dscp-map set successfully.
Console> (enable)
```

（注） マークダウン ペナルティと矛盾しない、CoS 値にマッピングするマークダウン DSCP 値を設定してください（「内部 DSCP 値と出力 CoS 値のマッピング」[p.49-73] を参照）。

デフォルトの DSCP マークダウン値マッピングに戻すには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	デフォルトの DSCP マークダウン マッピングに戻します。	**clear qos policed-dscp-map** [**normal-rate** | **excess-rate**]
ステップ 2	設定を確認します。	**show qos maps** {**config** | **runtime**} [**cos-dscp-map** | **ipprec-dscp-map** | **dscp-cos-map** | **policed-dscp-map**]

次に、デフォルトの DSCP マークダウン マッピングに戻す例を示します。

```
Console> (enable) clear qos policed-dscp-map
QoS dscp-cos-map setting restored to default.
Console> (enable)
```

（注） **normal-rate** または **excess-rate** キーワードを指定しなかった場合、**clear qos policed-dscp-map** コマンドは標準の policed-dscp マップだけを消去します。

QoS 情報の表示

QoS 情報を表示するには、次の作業を行います。

作業	コマンド
QoS 情報を表示します。	**show qos info** [**runtime** | **config**]

次に、ポート 2/1 について、QoS 実行情報を表示する例を示します。

```
Console> show qos info config 2/1
QoS setting in NVRAM:
QoS is enabled
Port 2/1 has 2 transmit queue with 2 drop thresholds (2q2t).
Port 2/1 has 1 receive queue with 4 drop thresholds (1q4t).
Interface type:vlan-based
ACL attached:
The qos trust type is set to untrusted.
Default CoS = 0
Queue and Threshold Mapping:
Queue Threshold CoS
----- --------- ---------------
1     1         0 1
1     2         2 3
2     1         4 5
2     2         6 7
Rx drop thresholds:
Rx drop thresholds are disabled for untrusted ports.
Queue #  Thresholds - percentage (abs values )
-------  ---------------------------------------
1        50% 60% 80% 100%
Tx drop thresholds:
Queue #  Thresholds - percentage (abs values )
-------  ---------------------------------------
1        40% 100%
2        40% 100%
Tx WRED thresholds:
WRED feature is not supported for this port_type.
Queue Sizes:
Queue #  Sizes - percentage (abs values )
-------  ---------------------------------------
1        80%
2        20%
WRR Configuration of ports with speed 1000Mbps:
Queue #  Ratios (abs values )
-------  ---------------------------------------
1        100
2        255
Console> (enable)
```

QoS 統計情報の表示

QoS 統計情報を表示するには、次の作業を行います。

作業	コマンド
QoS 統計情報を表示します。	**show qos statistics** {*mod*[/*port*] | **l3stats** | **aggregate-policer** [*policer_name*]}

次に、ポート 2/1 の QoS 統計情報を表示する例を示します。

```
Console> (enable) show qos statistics 2/1
On Transmit:Port 2/1 has 2 Queue(s) 2 Threshold(s)
Q #  Threshold #:Packets dropped
---  -------------------------------------------
1    1:0 pkts, 2:0 pkts
2    1:0 pkts, 2:0 pkts
On Receive:Port 2/1 has 1 Queue(s) 4 Threshold(s)
Q #  Threshold #:Packets dropped
---  -------------------------------------------
1    1:0 pkts, 2:0 pkts, 3:0 pkts, 4:0 pkts
```

次に、QoS レイヤ 3 統計情報を表示する例を示します。

```
Console> (enable) show qos statistics l3stats
QoS Layer 3 Statistics show statistics since last read.
Packets dropped due to policing: 0
IP packets with ToS changed:     0
IP packets with CoS changed:     26
Non-IP packets with CoS changed: 0
Console>
```

次に、QoS 集約ポリサー（aggregate policer）統計情報を表示する例を示します。

```
Console> (enable) show qos statistics aggregate-policer
QoS aggregate-policer statistics:
Aggregate Policer                Packet Count Packets exceed Packets exceed
                                              normal rate    excess rate
-------------------------------- ------------ -------------- -----------------
test                                     1000             20                 5
```

デフォルトの QoS に戻す場合

（注） デフォルトの設定に戻すと、QoS がディセーブルになります。QoS はディセーブルがデフォルトの設定のためです。

デフォルトの QoS に戻すには、イネーブル モードで次の作業を行います。

作業	コマンド
デフォルトの QoS に戻します。	**clear qos config**

次に、デフォルトの QoS に戻す例を示します。

```
Console> (enable) clear qos config
This command will disable QoS and take values back to factory default.
Do you want to continue (y/n) [n]? y
QoS config cleared.
Console> (enable)
```

QoS のディセーブル化

QoS をディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
スイッチ上で QoS をディセーブルにします。	**set qos** {**enable** | **disable**}

次に、QoS をディセーブルにする例を示します。

```
Console> (enable) set qos disable
QoS is disabled.
Console> (enable)
```

COPS サポートの設定

(注)

- レイヤ 2 スイッチング エンジンを搭載した Supervisor Engine 1 は、このコマンドをサポートしていません。
- COPS で設定できる QoS は、IP トラフィック専用です。他のすべてのトラフィックに対応する QoS を設定する場合は、CLI または SNMP を使用します。
- このマニュアルおよびその他すべての Catalyst 6500 シリーズ スイッチ関連のマニュアルにおいて、*COPS* という用語は、Catalyst 6500 シリーズ スイッチに実装された COPS サポートを意味します。

ここでは、COPS サポートの設定について説明します。

ポート ASIC

一部の COPS サポート機能は、ポート Application Specific Integrated Circuit（ASIC; 特定用途向け IC）によって制御されるすべてのポートが対象です。ここで使用する *ASIC 単位*という用語は、同一ポート ASIC 上のすべてのポートを設定する機能を表します。

- ギガビット イーサネット スイッチング モジュール上のポート ASIC は、1 つのモジュール上で最大 4 ポート（1 ～ 4、5 ～ 8、9 ～ 12、および 13 ～ 16）までを制御します。
- 10 Mbps、10/100 Mbps、および 100 Mbps イーサネット スイッチング モジュールのポート ASIC が、すべてのポートを制御します。
- 10 Mbps、10/100 Mbps、および 100 Mbps イーサネット スイッチング モジュール上では、別のポート ASIC のセットがあり、12 ポートずつ制御します（1 ～ 12、13 ～ 24、25 ～ 36、および 37 ～ 48）が、COPS でこれらを設定することはできません。
- EtherChannel ポートを変更すると、その EtherChannel 内のすべてのポート、および EtherChannel ポートを制御する ASIC（1 つまたは複数）の支配下にあるすべてのポートに変更が適用されます。

QoS ポリシーの概要

*QoS ポリシー*という用語は、ポートの信頼状態、ポートおよび VLAN に適用されている ACL など、有効となっている QoS 値を意味します。

QoS ポリシー ソースとして COPS を選択する場合

QoS は、ローカルに設定された QoS 値をデフォルトの QoS ポリシー ソースとして使用します。QoS ポリシー ソースとして COPS を選択するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	QoS ポリシー ソースとして COPS を選択します。	**set qos policy-source** {**local** | **cops**}
ステップ 2	QoS ポリシー ソースを確認します。	**show qos policy-source**

次に、QoS ポリシー ソースとして COPS を選択する例を示します。

```
Console> (enable) set qos policy-source cops
QoS policy source for the switch set to COPS.
Console> (enable) show qos policy-source
QoS policy source for the switch set to COPS.
Console> (enable)
```

QoS ポリシー ソースとして COPS を選択すると、次の値がローカルに設定された値から受信した COPS 値に切り替わります。

- すべての DSCP マップ
- 名前付き ACL およびデフォルト ACL の定義
- マイクロフローおよび集約ポリサー
- キューへの CoS 割り当て
- スレッシュホールドの設定
- WRR の重みおよびバッファの設定
- デフォルトのポート CoS およびインターフェイスに付加された ACL

ローカルに設定された QoS ポリシーを選択する場合

ローカルに設定された QoS ポリシーを選択するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ローカルに設定された QoS ポリシーを選択します。	**set qos policy-source** {**local** | **cops**}
ステップ 2	QoS ポリシー ソースを確認します。	**show qos policy-source**

次に、ローカルに設定された QoS ポリシーを選択する例を示します。

```
Console> (enable) set qos policy-source local
QoS policy source for the switch set to local.
Console> (enable) show qos policy-source
QoS policy source for the switch set to local.
Console> (enable)
```

ローカルに設定された QoS ポリシーを使用できるようにする場合

イネーブルの場合、COPS はすべてのポートに対してデフォルトの QoS ポリシー ソースです。ASIC 単位で、ローカルに設定された QoS ポリシーを使用できます。ポート ASIC 上でローカルに設定された QoS ポリシーを使用できるようにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ローカルに設定された QoS ポリシーをポート上で使用できるようにします。	**set port qos policy-source** {**local** | **cops**}
ステップ 2	ポートに対応する QoS ポリシー ソースを確認します。	**show port qos**

次に、ローカルに設定された QoS ポリシーを使用できるようにする例を示します。

```
Console> (enable) set port qos 1/1 policy-source local
QoS policy source set to local on port(s) 1/1-2.
Console> (enable)
```

ポート ロールの割り当て

COPS は、ポートの設定にスロット番号、ポート番号といったパラメータを使用しません。COPS は、ユーザが作成してポート ASIC に割り当てた*ロール*を使用します。

ロールとは、ポートの機能を説明する名前です（*access*、*mod2_1-4* など）。QoS は、1 台のスイッチで最大 64 のロールをサポートしています。1 つのポート ASIC に複数のロールを割り当てることができます（*mod2ports1-12* および *access* など）。ただし、ロール名を結合した合計の長さが 255 文字を超える場合は、ポート ASIC に割り当てることができないという制限があります。

ロール名は最大 31 文字です。大文字と小文字は区別されませんが、大文字および小文字を含めることができます。a ～ z、A ～ Z、0 ～ 9、ダッシュ（-）、下線（_）、およびピリオド（.）を使用できます。ロール名の先頭には、下線は使用できません。

ポートに新しいロールを初めて割り当てたときに、ロールが作成されます。

ポート ASIC にロールを割り当てるには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポート ASIC にロールを割り当てます。	**set port cops** {*mod/port*} **roles** *role1* [*role2*] ...
ステップ 2	ポートのロールを確認します。	**show port cops** [*mod*[*/port*]]

次に、ポート 2/1 を制御している ASIC に新しいロールを 2 つ割り当てる例を示します。

```
Console> (enable) set port cops 2/1 roles mod2ports1-12 access
New role 'mod2ports1-12' created.
New role 'access' created.
Roles added for port 2/1-12.
Console> (enable)
```

ポート ASIC からのロールの削除

ポート ASIC からロールを削除するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポート ASIC からロールを削除します。	**clear port cops** {*mod/port*} {**all-roles** | **roles** *role1* [*role2*] ...}
ステップ 2	ポートのロールを確認します。	**show port cops** [*mod*[*/port*]]

次に、ポート ASIC からロールを削除する例を示します。

```
Console> (enable) clear port cops 3/1 roles backbone_port main_port
Roles cleared for port(s) 3/1-4.
Console> (enable)
```

ロールの削除

ロールを削除する（すべてのポートから削除する）には、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ロールを削除します。	**clear cops** {**all-roles** | **roles** *role1* [*role2*] ...}
ステップ 2	ポートのロールを確認します。	**show port cops** [*mod*[*/port*]]

次に、ロールを削除する例を示します。

```
Console> (enable) clear cops roles backbone_port main_port
Roles cleared.
Console> (enable)
```

PDP サーバの設定

（注） COPS と RSVP は、同じ Policy Decision Point（PDP）サーバを使用できます。

COPS は PDP サーバから QoS ポリシーを取得します。プライマリ PDP サーバを設定し、さらに任意でバックアップ PDP サーバを設定します。

PDP サーバを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	PDP サーバを設定します。	**set cops server** *ip_address* [*port*] [**primary**] [**diff-serv** | **rsvp**]
ステップ 2	PDP サーバの設定を確認します。	**show cops info**

ip_address パラメータには、サーバの IP アドレスまたは名前を指定できます。

port 変数は PDP サーバの TCP ポート番号です。

diff-serv キーワードを使用して、COPS 専用のアドレスを設定します。

次に、PDP サーバを設定する例を示します。

```
Console> (enable) set cops server my_server1 primary
my_server1 added to the COPS diff-serv server table as primary server.
my_server1 added to the COPS rsvp server table as primary server.
Console> (enable)
```

PDP サーバの設定削除

PDP サーバの設定を削除するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	PDP サーバの設定を削除します。	**clear cops server** {**all** | *ip_address* [**diff-serv** | **rsvp**]}
ステップ 2	PDP サーバの設定を確認します。	**show cops info**

次に、PDP サーバの設定を削除する例を示します。

```
Console> (enable) clear cops server all
All COPS diff-serv servers cleared.
All COPS rsvp servers cleared.
Console> (enable)
```

COPS ドメイン名の設定

PDP サーバは COPS ドメイン名を使用して、スイッチなどの Policy Enforcement Point（PEP）装置と通信します。スイッチに COPS ドメイン名を設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	COPS ドメイン名を設定します。	**set cops domain-name** *domain_name*
ステップ 2	COPS ドメイン名を確認します。	**show cops info**

次に、COPS ドメイン名を設定する例を示します。

```
Console> (enable) set cops domain-name my_domain
Domain name set to my_domain.
Console> (enable)
```

COPS ドメイン名の削除

COPS ドメイン名を削除するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	COPS ドメイン名を削除します。	**clear cops domain-name**
ステップ 2	設定を確認します。	**show cops info**

次に、COPS ドメイン名を削除する例を示します。

```
Console> (enable) clear cops domain-name
Domain name cleared.
Console> (enable)
```

COPS 通信パラメータの設定

COPS が PDP サーバとの通信に使用するパラメータを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	COPS が PDP サーバとの通信に使用するパラメータを設定します。	**set cops retry-interval** *initial increment maximum*
ステップ 2	設定を確認します。	**show cops info**

秒単位（0 ～ 65535 の範囲）でパラメータを入力します。必ず、*initial* パラメータ値と *increment* パラメータ値の合計が *maximum* パラメータの値を超えないようにしてください。

次に、COPS が PDP サーバとの通信に使用するパラメータを設定する例を示します。

```
Console> (enable) set cops retry-interval 15 1 30
Connection retry intervals set.
Console> (enable)
```

RSVP サポートの設定

（注）

- レイヤ 2 スイッチング エンジンを搭載した Supervisor Engine 1 は、このコマンドをサポートしていません。
- このマニュアルおよび他のすべての Catalyst 6500 シリーズ スイッチ関連のマニュアルで、*RSVP* は、Catalyst 6500 シリーズ スイッチに実装された RSVP ヌル サービス テンプレートおよびレシーバー プロキシ機能サポートを意味します。

ここでは、RSVP ヌル サービス テンプレートおよびレシーバー プロキシ機能サポートの設定について説明します。

- RSVP サポートのイネーブル化（p.49-82）
- RSVP サポートのディセーブル化（p.49-83）
- DSBM 選定への参加のイネーブル化（p.49-83）
- DSBM 選定への参加のディセーブル化（p.49-83）
- PDP サーバの設定（p.49-84）
- PDP サーバの設定削除（p.49-84）
- RSVP ポリシー タイムアウトの設定（p.49-85）
- RSVP にローカル ポリシーを使用させる設定（p.49-85）

RSVP サポートのイネーブル化

RSVP サポートをイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチ上で RSVP サポートをイネーブルにします。	**set qos rsvp** {**enable** | **disable**}
ステップ 2	設定を確認します。	**show qos rsvp info**
ステップ 3	RSVP アクティビティを表示します。	**show qos rsvp flow-info**

次に、RSVP サポートをイネーブルにする例を示します。

```
Console> (enable) set qos rsvp enable
RSVP enabled on the switch.
Console> (enable)
```

RSVP サポートのディセーブル化

RSVP サポートをディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチ上で RSVP サポートをディセーブルにします。	**set qos rsvp** {**enable** | **disable**}
ステップ 2	設定を確認します。	**show qos rsvp info**

次に、RSVP サポートをディセーブルにする例を示します。

```
Console> (enable) set qos rsvp disable
RSVP disabled on the switch.
Console> (enable)
```

DSBM 選定への参加のイネーブル化

Catalyst 6500 シリーズ スイッチは、Designated Subnet Bandwidth Manager（DSBM）として動作できます。ポート単位で、DSBM の選定に参加できるように設定できます。

（注） RSVP 装置がネットワークに追加されても、DSBM は再選定されません。どの装置を DSBM にするかを制御するには、DSBM として選定されるようにする装置を除くすべての装置で選定への参加を禁止します。DSBM の選定後、ネットワーク構成に応じて、他の装置で選定に参加できるように再設定します。

DSBM の選定にポートを参加させるには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	DSBM の選定にポートが参加できるようにします。	**set port rsvp** {*mod/port*} **dsbm-election** {**disable** | **enable** *priority*}
ステップ 2	ポートの設定を確認します。	**show port rsvp** [*mod* | *mod/port*]

priority パラメータの範囲は、128 ～ 255 です。

次に、DSBM の選定にポート 2/1 および 3/2 が参加できるようにする例を示します。

```
Console> (enable) set port rsvp 2/1,3/2 dsbm-election enable 232
DSBM enabled and priority set to 232 for ports 2/1,3/2.
Console> (enable)
```

DSBM 選定への参加のディセーブル化

DSBM の選定にポートが参加できないようにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	DSBM の選定にポートが参加できないようにします。	**set port rsvp** {*mod/port*} **dsbm-election** {**disable** | **enable** *priority*}
ステップ 2	設定を確認します。	**show port rsvp show port rsvp** [*mod*[*/port*]]

次に、DSBM の選定にポート 2/1 が参加できないようにする例を示します。

```
Console> (enable) set port rsvp 2/1 dsbm-election disable
DSBM disabled for port 2/1.
Console> (enable)
```

PDP サーバの設定

（注） COPS および RSVP は、同じ PDP サーバを使用できます。

スイッチが DSBM の場合、RSVP は PDP サーバと通信します。プライマリ PDP サーバを設定し、さらに任意でバックアップ PDP サーバを設定します。

PDP サーバを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	PDP サーバを設定します。	**set cops server** *ip_address* [*port*] [**primary**] [**diff-serv** | **rsvp**]
ステップ 2	PDP サーバの設定を確認します。	**show cops info**

ip_address パラメータには、サーバの IP アドレスまたは名前を指定できます。

port 変数は PDP サーバの TCP ポート番号です。

rsvp キーワードを使用して、RSVP 専用のアドレスを設定します。

次に、PDP サーバを設定する例を示します。

```
Console> (enable) set cops server my_server1 primary rsvp
my_server1 added to the COPS rsvp server table as primary server.
Console> (enable)
```

PDP サーバの設定削除

PDP サーバの設定を削除するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	PDP サーバの設定を削除します。	**clear cops server** {**all** | *ip_address* [**diff-serv** | **rsvp**]}
ステップ 2	PDP サーバの設定を確認します。	**show cops info**

rsvp キーワードを使用して、RSVP アドレスだけを削除します。

次に、PDP サーバの設定を削除する例を示します。

```
Console> (enable) clear cops server all
All COPS diff-serv servers cleared.
All COPS rsvp servers cleared.
Console> (enable)
```

RSVP ポリシー タイムアウトの設定

スイッチが DSBM であるときに、PDP サーバとの通信が切断された場合、スイッチはタイムアウト値として指定された時間だけ、キャッシュの値を使用して、DSBM としての動作を継続します。新規または変更された RSVP ***path*** メッセージに対する動作は、RSVP ローカル ポリシーの設定によって決まります。

タイムアウトの設定時間内に、PDP サーバとの通信が再び確立されなかった場合、スイッチの役割はすべてのポートに対応する Subnet Bandwidth Manager（SBM）クライアントの役割に戻り、セグメント上で新しく選定された DSBM に、RSVP メッセージを転送します。PDP サーバとの通信が行われなかった場合、スイッチは DSBM の選定に参加しません。

PDP サーバとの通信が切断されてから、スイッチが引き続き DSBM として動作する時間の長さを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	RSVP ポリシー タイムアウトを設定します。	**set qos rsvp policy-timeout** *timeout*
ステップ 2	設定を確認します。	**show qos rsvp info**

分単位（0 ～ 65535 の範囲）で *timeout* パラメータを入力します（デフォルト値は 30）。

次に、RSVP ポリシー タイムアウトを設定する例を示します。

```
Console> (enable) set qos rsvp policy-timeout 45
RSVP database policy timeout set to 45 minutes.
Console> (enable)
```

RSVP にローカル ポリシーを使用させる設定

PDP サーバとの通信が切断されたあとの RSVP の動作を設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	PDP サーバとの間で通信が行われない場合の RSVP の動作を設定します。	**set qos rsvp local-policy** {**forward** | **reject**}
ステップ 2	設定を確認します。	**show qos rsvp info**

forward キーワードは、新規または変更された RSVP **path** メッセージをすべて転送するローカル ポリシーを設定します。**reject** キーワードは、新規または変更された RSVP **path** メッセージの転送を拒否するローカル ポリシーを設定します。次に、新規または変更された RSVP **path** メッセージをすべて拒否するように、デフォルトのローカル RSVP ポリシー設定を変更する例を示します。

```
Console> (enable) set qos rsvp local-policy reject
RSVP local policy set to reject.
Console> (enable)
```

（注） RSVP ローカル ポリシーが使用されるのは、PDP との接続が切断されたあと、RSVP ポリシー タイムアウトが満了するまでの間だけです。RSVP ポリシー タイムアウトが満了すると、スイッチは SBM クライアントとして動作します。RSVP ローカル ポリシーの設定とは無関係に、RSVP メッセージはそのままスイッチを通過します。スイッチが PDP との接続を確立することがなければ、RSVP ローカル ポリシー設定は使用されません。

QoS 統計データ エクスポートの設定

ここでは、QoS 統計データ エクスポート機能を設定する手順について説明します。

QoS 統計データ エクスポートのグローバルなイネーブル化

ポートおよび集約ポリサーに対して QoS 統計データをエクスポートするには、最初にこの機能をグローバルに設定する必要があります。

QoS 統計データ エクスポートをグローバルにイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	QoS 統計データのエクスポートをイネーブルにします。	**set qos statistics export enable | disable**
ステップ 2	設定を確認します。	**show qos statistics export info**

次に、QoS 統計データ エクスポートをグローバルにイネーブルにし、設定を確認する例を示します。

```
Console> (enable) set qos statistics export enable
Export is enabled.
Export destination:172.20.52.3 SYSLOG facility LOG_LOCAL6 (176), severity LOG_DE
BUG (7)
Aggregate policer export is not supported
Console> (enable) show qos statistics export info
Statistics export status and configuration information
-----------------------------------------------------
Export status: enabled
Export time interval: 300
Export destination:172.20.52.3 SYSLOG facility LOG_LOCAL6 (176), severity LOG_DE
BUG (7)
Port    Export
------  --------
 1/1    disabled
 1/2    disabled
 3/1    disabled
 3/2    disabled
 5/1    disabled
 5/2    disabled
 5/3    disabled
 5/4    disabled
(テキスト出力は省略)
Console> (enable)
```

ポート単位の QoS 統計データ エクスポートのイネーブル化

ポート単位で QoS 統計データ エクスポートをイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポート単位で QoS 統計データのエクスポートをイネーブルにします。	**set qos statistics export port** *mod/port* **enable** | **disable**
ステップ 2	設定を確認します。	**show qos statistics export info**

(注)　ポート単位での設定を有効にするには、QoS 統計データのエクスポートをグローバルにイネーブルにする必要があります。

次に、ポート単位で QoS 統計データ エクスポートをイネーブルにし、設定を確認する例を示します。

```
Console> (enable) set qos statistics export port 5/1 enable
Port export enabled on 5/1.
Console> (enable) show qos statistics export info
Statistics export status and configuration information
-----------------------------------------------------
Export status: enabled
Export time interval: 300
Export destination:172.20.52.3 SYSLOG facility LOG_LOCAL6 (176), severity LOG_DE
BUG (7)
Port    Export
------  --------
 1/1    disabled
 1/2    disabled
 3/1    disabled
 3/2    disabled
 5/1    enabled
 5/2    disabled
(テキスト出力は省略)
Console> (enable)
```

ポート上でイネーブルにした場合、QoS 統計データ エクスポートには、デリミタ文字で区切られた次の各フィールドが含まれます。

- エクスポート タイプ（ポートは [1]）
- スロット / ポート
- 入力パケット数
- 入力バイト数
- 出力パケット数
- 出力バイト数
- タイム スタンプ

集約ポリサー単位の QoS 統計データ エクスポートのイネーブル化

集約ポリサー単位で QoS 統計データ エクスポートをイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	集約ポリサー単位で QoS 統計データのエクスポートをイネーブルにします。	**set qos statistics export aggregate** *name* {**enable** | **disable**}
ステップ 2	設定を確認します。	**show qos statistics export info**

(注)　集約ポリサー単位での設定を有効にするには、QoS　統計データのエクスポートをグローバルにイネーブルにする必要があります。

次に、特定の集約ポリサーに対する QoS 統計データ エクスポートをイネーブルにし、設定を確認する例を示します。

```
Console> (enable) set qos statistics export aggregate ipagg_3 enable
Statistics data export enabled for aggregate policer ipagg_3
Console> (enable) show qos statistics export info
Statistics export status and configuration information
-----------------------------------------------------
Export status: enabled
Export time interval: 300
Export destination:172.20.52.3 SYSLOG facility LOG_LOCAL6 (176), severity LOG_DE
BUG (7)
Port    Export
------  --------
 1/1    disabled
 1/2    disabled
 3/1    disabled
 3/2    disabled
 5/1    enabled
 5/2    disabled
(テキスト出力は省略)

Aggregate name  Export
--------------  --------
ipagg_3         enabled
Console> (enable)
```

名前付き集約ポリサーに対してイネーブルにした場合、QoS 統計データ エクスポートには、デリミタ文字で区切られた次の各フィールドが含まれます。

- エクスポート タイプ（集約ポリサーは [2]）
- 集約ポリサー名
- 方向（[in]）
- 適合パケット数
- CIR を超えたパケット数
- PIR を超えたパケット数
- タイム スタンプ

集約ポリサー QoS 統計情報の消去

集約ポリサー QoS 統計情報を消去するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	集約ポリサー QoS 統計情報を消去します。	**clear qos statistics aggregate-policer** [*policer_name*]
ステップ 2	設定を確認します。	**show qos statistics export info**

次に、特定の集約ポリサーに関して、集約ポリサー QoS 統計情報を消去する例を示します。

```
Console> (enable) clear qos statistics aggregate-policer aggr_1
Aggregate policer 'aggr_1' statistical counters cleared.
```

集約ポリサーを指定しない場合は、すべての集約ポリサーの統計情報が消去されます。

```
Console> (enable) clear qos statistics aggregate-policer
QoS aggregate policers statistical counters cleared.
```

QoS 統計データ エクスポートの間隔の設定

QoS 統計データがエクスポートされるデフォルトの間隔は 30 秒です。QoS 統計データ エクスポートの間隔を設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	QoS 統計データ エクスポートの間隔を設定します。	**set qos statistics export interval** *interval_seconds*
ステップ 2	設定を確認します。	**show qos statistics export info**

次に、QoS 統計データ エクスポートの間隔を設定し、その設定を確認する例を示します。

```
Console> (enable) set qos statistics export interval 500
Time interval set to 500
Console> (enable) show qos statistics export info
Statistics export status and configuration information
-----------------------------------------------------
Export status: enabled
Export time interval: 500
Export destination:172.20.52.3 SYSLOG facility LOG_LOCAL6 (176), severity LOG_DE
BUG (7)
Port    Export
------  --------
 1/1    disabled
 1/2    disabled
 3/1    disabled
 3/2    disabled
 5/1    enabled
 5/2    disabled
（テキスト出力は省略）

Aggregate name  Export
--------------  --------
ipagg_3         enabled
Console> (enable)
```

QoS 統計データ エクスポートの宛先ホストおよび UDP ポートの設定

QoS 統計データ エクスポートの宛先ホストおよび UDP ポート番号を設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	QoS 統計データ エクスポートの宛先ホストおよび UDP ポート番号を設定します。	**set qos statistics export destination** {*host_name* | *ip_address*} [**syslog** [*facility* | *severity*] *port*]
ステップ 2	設定を確認します。	**show qos statistics export info**

次に、QoS 統計データ エクスポートの宛先ホストおよび UDP ポート番号を設定し、設定を確認する例を示します。

```
Console> (enable) set qos statistics export destination stargate 9996
Statistics data export destination set to stargate port 9996.
Console> (enable) show qos statistics export info
Statistics export status and configuration information
-----------------------------------------------------
Export status: enabled
Export time interval: 500
Export destination:Stargate, UDP port 9996
Port    Export
------  --------
 1/1    disabled
 1/2    disabled
 3/1    disabled
 3/2    disabled
 5/1    enabled
 5/2    disabled
(テキスト出力は省略)

Aggregate name  Export
--------------  --------
ipagg_3         enabled
Console> (enable)
```

QoS 統計情報の表示

集約ポリサー単位のパケットおよびバイト レートに関する QoS 統計情報を表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
集約ポリサー単位のパケットおよびバイト レートの QoS 統計情報を表示します。	**show qos statistics aggregate-policer** [*policer_name*]

次に、集約ポリサー単位のパケットおよびバイト レートに関する QoS 統計情報を表示する例を示します。

```
Console> show qos statistics aggregate-policer
QoS aggregate-policer statistics:
Aggregate Policer                Packet Count Packets exceed Packets exceed
                                              normal rate excess rate
-------------------------------- ------------ -------------- -----------------
test                                     1000             20                 5
Console>
```

CHAPTER 50

自動 QoS の使用

この章では、Catalyst 6500 シリーズ スイッチ上で自動 Quality of Service（QoS; サービス品質）設定機能を使用する方法について説明します。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

(注) 自動 QoS は、Release 8.1(1) の Supervisor Engine 720 上ではサポートされていません。

(注) 自動音声設定の使用方法については、「SmartPort の使用方法」（p.53-41）を参照してください。

この章で説明する内容は、次のとおりです。

自動 QoS の機能

自動 QoS は、Catalyst 6500 シリーズ スイッチ上で QoS 設定を簡略化するマクロで構成されます。自動 QoS マクロは、音声ポート用の推奨 Architecture for Voice, Video, and Integrated Data（AVVID）の実装に必要なすべての QoS 設定タスクを取り扱います。

自動 QoS は、Cisco IP Phone 79xx シリーズと Cisco SoftPhone を使用して構築された音声ネットワークに照準を絞っています。ただし、その他の電話機も自動設定された QoS 設定から同等の恩恵を受けられます。自動 QoS では、**ciscoipphone** や **ciscosoftphone** などのキーワード、または特定ポートで適用する QoS パラメータのタイプを指定可能にする、その他の AVVID タイプを使用します。自動 QoS により、該当するすべての QoS 設定（Internet Engineering Task Force [IETF] 推奨値および実証済みの AVVID 設定）がポートに適用されます。

QoS の概要

ここでは、QoS の概要について説明します。

音声および映像ネットワーク用の一般的な CoS および DSCP 値

IETF では、音声および映像ネットワークにある各種トラフィック タイプに対して複数の値を使用することを推奨しています。自動 QoS は、このような値を使用して Class of Service（CoS; サービス クラス）/ キュー マップ、Differentiated Service Code Point（DSCP）/CoS マップなどの QoS パラメータを設定します。

Catalyst 6500 シリーズ スイッチは、QoS に差別化サービス（DIFFSERV）モデルを使用します。このモデルには、次の 3 種類のトラフィックがあります。

- EF（Expedited Forwarding; 緊急転送型）
- AF（Assured Forwarding; 確認転送型）
- BE（Best Effort; ベストエフォート型）

AF クラス内には 4 つのトラフィック クラスがあります。クラスは AF*XY* で表されます。*X* は、クラス番号、*Y* は廃棄優先順位番号です。*X* はキューに対応し、*Y* はキュー内の廃棄優先順位番号（Weighted Random Early Detection [WRED; 重み付きランダム早期検出] またはテールドロップ）に対応します。EF のプライオリティが最も高く、BE が最低です。AF のプライオリティは、両者の間のどこかです。

表 50-1 に、音声ネットワークおよびその他のトラフィック タイプの推奨 CoS および DSCP 値を示します。表示されている値は、自動 QoS マクロで CoS/ キュー マップおよび他の CoS/DSCP 値依存設定を設定する際に採用されます。

表 50-1　シスコの音声および映像ネットワーク用の一般的な CoS および DSCP 値

CoS 値[1]	DSCP	意味
0	0	デフォルト トラフィック（BE クラス）
3	26（IETF 推奨）	音声 / ビデオ コール制御 / シグナリング（TCP） AF31 クラス
5	46（IETF 推奨）	音声伝達ストリーム（RTP/UDP） EF クラス
4	34（IETF 推奨）	ビデオ伝達ストリーム AF41 クラス
2	18	ミッションクリティカル / トランザクション トラフィック AF21 クラス
1	10	ストリーミング ビデオ（非対話型） AF11
6	48	ルーティング プロトコル（デフォルトで）
7		Spanning-Tree Protocol（STP; スパニングツリー プロトコル）

1. 値の中には、Catalyst ソフトウェアの現在の QoS デフォルト値とは異なるものもあります（CoS/DSCP マップなど）。

これらの CoS/DSCP 値のプライオリティは、次のとおりです。

- CoS 5（音声データ）— 最高のプライオリティ（ある場合はプライオリティ キュー、ない場合はハイ キュー）
- CoS 6、7（ルーティング プロトコル）— プライオリティは 2 番め（ハイ キュー）
- CoS 3、4（コール信号およびビデオ ストリーム）— プライオリティは 3 番め（ハイ キュー）
- CoS 1、2（ストリーミングおよびミッションクリティカル）— プライオリティは 4 番め（ハイ キュー）
- CoS 0 — 低プライオリティ（ロー キュー）

プライオリティ キューを実装していないポートでは、WRED およびテールドロップ メカニズムを使用してキュー内にトラフィックの優先順位付けを達成します。具体的なスケジューリング設定については、「グローバル自動 QoS 詳細設定」（p.50-7）を参照してください。

QoS シナリオ — Cisco IP Phone

通常の設定で、Cisco IP Phone 79xx は、Catalyst スイッチのポートに直接接続できます。必要に応じて PC を電話機に接続し、スイッチのホップとして使用できます。

一般的に電話機から発信されてスイッチに入るトラフィックは、802.1Q/p ヘッダーを使用してタグでマーキングされます。ヘッダーには、VLAN 情報と CoS 3 ビット フィールドが含まれています。CoS によって、そのパケットのプライオリティが決まります。スイッチは、CoS フィールドを使用して PC のトラフィックと電話機のトラフィックを区別します。スイッチは、DSCP フィールドを同じ用途に使用することもできます。

Cisco IP Phone 79xx の通常の設定では、電話機から発信されてスイッチに入るトラフィックは信頼されます。ポートの信頼状態を trust-cos に設定して、音声トラフィックをネットワークのその他のトラフィック タイプより優先させます。

Cisco IP Phone 79xx には内蔵スイッチがあり、PC、電話機およびスイッチ ポートから着信するトラフィックをミックスします。Cisco IP Phone 79xx には設定が必要な信頼機能と分類機能があります。詳細については、「ciscosoftphone に対するポート固有の自動 QoS 設定」（p.50-10）を参照してください。

QoS シナリオ — Cisco SoftPhone

Cisco SoftPhone は標準の PC 上で実行するソフトウェア製品で、IP Phone をエミュレートします。Cisco SoftPhone と Cisco IP Phone 79xx の主な違いは、Cisco SoftPhone は DSCP を介してその音声トラフィックをマーキングするのに対し、Cisco IP Phone 79xx は CoS を介してトラフィックをマーキングする点です。スイッチ上の QoS 設定は、ポートに入るトラフィックのレイヤ 3 マーキングを信頼することで、この動作に対応します。それ以外のすべての動作は Cisco IP Phone 79xx と同じです。

スイッチ上での自動 QoS マクロの使用

ここでは、QoS マクロについて説明します。

自動 QoS の概要

自動 QoS マクロは、次の 2 つの別個のコンポーネントに分けられます。

- グローバル自動 QoS コマンド（**set qos auto**）— すべてのスイッチ全般に関連する QoS 設定で特定のインターフェイス固有ではないものを扱います。このような設定には、CoS/ キュー マップ、CoS/DSCP マップ、特定のポート タイプの WRED 設定、グローバル マッピングなどがあります。
- ポート固有自動 QoS コマンド（**set port qos** *mod/port* **autoqos**）— 特定ポートのすべての着信 QoS パラメータを設定して、必要なトラフィック タイプ（音声、ビデオ、アプリケーション）のパラメータを反映します。

ヒント　自動 QoS が正常に機能するようにするには、両方のコンポーネントを実行する必要があります。

自動 QoS 設定時の注意事項および制限事項

ここでは、自動 QoS の設定時の注意事項および制限事項について説明します。

コンフィギュレーション ファイル

他のコマンドを実装するコマンド（マクロ）を作成すると、コマンドの競合につながることもあります。たとえば、特定の設定で CoS/ キュー マップを設定してから自動 QoS マクロ機能をイネーブルにすると、イネーブルにされたマクロが CoS/ キュー マップを変更します。

コマンドの競合を避けるため、コンフィギュレーション ファイルには、マクロに組み込まれていたレガシー コマンドをすべて組み入れます。実際のマクロ コマンドはコンフィギュレーション ファイルには出現せず、代わりにマクロを実行した結果生じた既存のコンフィギュレーション コマンドがすべてコンフィギュレーション ファイルに組み込まれます。たとえば、**set qos autoqos** コマンドを入力してから **write config** コマンドを入力すると、実際のマクロ コマンド自身を除いて既存の QoS 関連の CLI（コマンドライン インターフェイス）コマンドがすべて表示されます。

サポート対象の電話機

ciscoipphone キーワードを指定して自動 QoS を使用する場合、一部の QoS 設定で、電話機固有の設定（trust-ext、ext-cos）が必要です。この設定は、次の電話機のみでサポートされています。Cisco IP Phone 7910、Cisco IP Phone 7940、Cisco IP Phone 7960、および Cisco IP Phone 7935 です。ただし、**ciscoipphone** キーワードはこれらのモデルに限定されません。どの電話機も、スイッチに設定したその他すべての QoS 設定の恩恵を受けられます。

Cisco SoftPhone は、**ciscoipsoftphone** キーワードによってサポートされています。

CDP の依存関係

Cisco IP Phone に QoS 設定と信頼境界を設定するには、ポート上で CDP のバージョン 2 以降をイネーブルにします。信頼境界機能をイネーブルにすると、CDP がイネーブルになっていないか、CDP のバージョン 1 が稼働している場合は、Syslog の警告メッセージが表示されます。

CDP は、**ciscoipphone** QoS 設定に対してだけイネーブルにする必要があり、CDP は自動 QoS 機能の他のコンポーネントには作用しません。ポート固有の自動 QoS 機能で **ciscoipphone** キーワードを使用すると、ポートで CDP がイネーブルに設定されていない場合は警告が表示されます。「CDP の警告」（p.50-25）を参照してください。

COPS の考慮事項

ポートを、ローカル ポリシーまたは Common Open Policy Service（COPS）ポリシー用に設定できます。この設定によって、ポートが QoS 設定情報をローカル コンフィギュレーションから得るか、COPS サーバから得るかが決まります。COPS をグローバルにイネーブルにするだけでなく、ポート上で COPS をイネーブルにすると、COPS サーバによって指定されたポリシーが適用されます。COPS をディセーブルにしている場合や設定済みのポリシーがローカルである場合は、ローカル コンフィギュレーションの QoS ポリシーが適用されます。

自動 QoS 機能はポートのローカル ポリシーにだけ作用します。設定済みのポリシーが現在 COPS に設定されているポート上で自動 QoS を実行すると、ポリシーはローカル ポリシーに戻ります。グローバル QoS ポリシーが（グローバル自動 QoS コマンドによって）ローカルに戻り、ポートベー

スのポリシーが（ポートベースの自動 QoS コマンドによって）ローカルに戻ります。ポートのポリシーまたはグローバル ポリシーが COPS からローカルに変更された場合は、警告が表示されます。詳細については、「COPS 警告メッセージ」（p.50-24）を参照してください。すでにポートに対応付けられている既存の COPS の役割は変更されません。

RSVP の考慮事項

グローバルおよびポートベース Resource Reservation Protocol（RSVP）関連のすべての設定（RSVP Designated Subnet Bandwidth Manager [DSBM] 選択設定など）は、自動 QoS マクロによっては変更されません。

現在の QoS のデフォルト設定

現在の QoS のすべての設定は、「自動 QoS 設定ステートメントの詳細」（p.50-19）に記載されているように適用されます。このような QoS 設定の一部は、現在の QoS のデフォルト設定を表します。自動 QoS を適用すると、すべての QoS 設定は、デフォルトかどうかに関係なくポート / スイッチに適用されます。

EtherChannel の考慮事項

グローバル自動 QoS コマンドは、チャネリングをサポートしています。すべての発信 QoS は、すべてのチャネリング / 非チャネリング インターフェイスに対して設定されます。チャネリングは、ポート単位の自動 QoS コマンドではサポートされていません。

ビデオ トラフィックの考慮事項

ビデオ トラフィックに対応付けられた CoS および DSCP 値は、グローバル QoS 設定のために優先順位付けされます。詳細については、「音声および映像ネットワーク用の一般的な CoS および DSCP 値」（p.50-2）を参照してください。

QoS 設定の消去

QoS 設定を消去すると、設定がデフォルトの QoS 値にリセットされます。自動 QoS 機能はデフォルト値を変更しません。

PFC/PFC2 のサポート

ciscoipphone および **trust cos** キーワードには、Policy Feature Card（PFC; ポリシー フィーチャ カード）や PFC2 は不要です。一方、**ciscosoftphone** および **trust dscp** キーワードには、PFC や PFC2 が必要です。

1p1q0t/1p3q1t ポートのサポート

すべての 1p1q0t/1p3q1t ポートは、ポートベース モードまたは VLAN ベース モードになければなりません。変更が必要な場合（たとえば、自動 QoS を実行する前にポートが VLAN ベース モードに設定されている場合）、Syslog メッセージが表示されます。メッセージは、インターフェイス タイプの変更が必要であり、その変更はモジュールのすべてのポートが対象であることを示します。詳細については、「必要なすべてのポートでのインターフェイス変更 — 警告レベル」（p.50-26）を参照してください。

グローバル自動 QoS マクロ

ここでは、グローバル自動 QoS マクロについて説明します。

概要

出力側と入力側の両方の QoS を正常に動作するよう設定する必要があります。すべてのトラフィック タイプが指定のポートを出てゆくことができるので、出力側の QoS はグローバル QoS に設定する必要があります。設定は、「音声および映像ネットワーク用の一般的な CoS および DSCP 値」（p.50-2）に記載の考えられるトラフィック タイプを *すべて*考慮しています。出力側の QoS 設定は、スイッチのすべてのポートに適用されます。グローバル QoS 設定は、*入力側*のスケジューリング設定も取り扱います。CoS/ キュー マッピングの粒度が*ポートタイプ*固有であり、ポート固有ではないからです。QoS Access Control List（ACL; アクセス制御リスト）、ポート信頼、デフォルト CoS などのポート固有 QoS 設定は、変更されません。

グローバル自動 QoS 詳細設定

表 50-2 ～表 50-6 に、グローバル自動 QoS コマンドによって設定されるすべての QoS パラメータの値を示します。

（注） 1p1q8t デフォルト WRED 設定は、現在の QoS デフォルトから変更されません。CoS/ スレッシュホールド マップだけが変更されます。

表 50-2　スイッチ全般の設定（グローバル QoS 設定）

QoS パラメータ	設定
CoS/DSCP マップ	0 **10 18 26 34 46** 48 56（太字はデフォルト以外の値を示します）
IP precedence/DSCP マップ	0 **10 18 26 34 46** 48 56（太字はデフォルト以外の値を示します）
DSCP/CoS マップ	{0-7}、{8-15}、{16-23}、{24-31}、{32-39}、{40-47}、{48-55}、{56-63}（デフォルトに準拠）
Policed-DSCP マップ	46：0 と 26：0 のデフォルトに準拠（「グローバル自動 QoS マクロ」[p.50-7] を参照）
Policed-DSCP マップ超過レート	デフォルトに準拠（「グローバル自動 QoS マクロ」[p.50-7] を参照）
デフォルト QoS IP ACL	ip dscp 0（デフォルトに準拠）

表 50-3　スケジューリング固有の設定（グローバル QoS 設定）

フィールド	値
1p1q0t rxq-ratio	80% : 20%（q1：p1）
1p3q1t wrr	20 100 200（q1 q2 q3）
2q2t txq-ratio	80% : 20%（q1：q2）
2q2t wrr	100 255（q1 q2）

表 50-4　CoS/ キュー マップおよびテール /WRED 設定（グローバル QoS 設定）

	2q2t	テール（2q2t）	1q2t	テール（1q2t）	1q4t	テール（1q4t）	1p3q1t	WRED（1p3q1t）	1p1q0t
Q1t1	0	（100%）	0, 1, 2, 3, 4	（80%）	0	（50%）	0	（70% : 100%）	0, 1, 2, 3, 4
Q1t2		（100%）	5, 6, 7	（100%）		（60%）			
Q1t3					1, 2, 3, 4	（80%）			
Q1t4					5, 6, 7	（100%）			
Q2t1	1, 2, 3, 4	（80%）					1, 2	（70% : 100%）	5, 6, 7
Q2t2	5, 6, 7	（100%）							
Q3t1							3, 4	（70% : 90%）	
Q3							6, 7	WRED　のディセーブル化	
Q4t1							5		

表 50-5　スケジューリング固有の設定（グローバル QoS 設定）

フィールド	値
1p2q2t txq-ratio	70% : 15% : 15%（q1 q2 1p）
1p2q2t wrr	50 255（q1 q2）
1p1q8t rxq-ratio	80 20（q1 1p）
1p2q1t txq-ratio	70% : 15% : 15%（q1 q2 1p）
1p2q1t wrr	50 255（q1 q2）

表 50-6　CoS/ キュー マップおよびテール /WRED 設定（グローバル QoS 設定）

	1p2q2t	WRED	1p1q4t	テール	1p2q1t	WRED	1p1q8t	WRED
Q1t1	0	（70% : 100%）	0	（50%）	0	（70% : 100%）	0	（40% : 70%）
Q1t2		（70% : 100%）		（60%）			1, 2	（60% ： 90%）（*スレッシュホールド 5*）
Q1t3			1,2,3,4	（80%）			3, 4	（70% : 100%）（*スレッシュホールド 8*）
Q1t4			6,7	（100%）				
Q2t1	1, 2, 3, 4	（70% : 90%）	5		1, 2, 3, 4	（70% : 90%）	5, 6, 7	
Q2t2	6, 7	（100% : 100%）						
Q2					6, 7	WRED のディセーブル化		
Q3t1	5				5			

ポート固有の自動 QoS マクロ

ポート固有の自動 QoS マクロは、特定のトラフィック タイプ固有のすべての着信 QoS 設定を処理します。**ciscoipphone**、**ciscosoftphone**、および **trust** のサポートが実装されています。対応する CLI コマンドについては、「自動 QoS の CLI インターフェイス」（p.50-13）を参照してください。

QoS 入力ポート固有の設定には、ポート信頼、デフォルト CoS、分類、およびポリシングがありますが、スケジューリングはありません。入力スケジューリングは、グローバル自動 QoS マクロを使用してプログラミングします。グローバル自動 QoS マクロ コマンドとともに、すべての QoS 設定を特定の QoS トラフィック タイプ用に正しく設定します。

ポートにすでに対応付けられている既存の QoS ACL は、ACL マッピングを変更すると削除されます。ACL 名とインスタンスは変更されません。

ここでは、ポート固有の自動 QoS マクロについて説明します。

ciscoipphone に対するポート固有の自動 QoS 設定

ciscoipphone キーワードを使用して、信頼境界機能をイネーブルにするだけでなく、ポートも trust-cos に設定します。グローバル自動 QoS コマンドとの併用により、スイッチに対してすべての設定がなされ、シグナリング、音声伝達、ポートを出入りする PC データを適切に処理します。

グローバル自動 QoS コマンドによって扱われるスイッチ側の QoS 設定以外にも、電話機にはラベリングが正常に発生するように設定が必要な QoS 機能がいくつかあります。QoS 設定情報は、スイッチから CDP を介して電話機に送信されます。設定する必要がある QoS 値は、電話機の「PC ポート」の信頼設定（trust または untrusted）と、ポートが信頼できない場合に電話機がパケットに再マーキングするために使用する CoS 値（ext-cos）です。

AVVID では、untrusted および cos-ext 値を 0 にすることを推奨しています。スイッチに入る PC トラフィックには電話機によって CoS 0 がマーキングされ、電話機によって生成される音声伝達トラフィックには常に CoS 5 とラベリングされ、シグナリングは CoS 3 がラベリングされます。

表 50-7 に、ポート上で自動 QoS **ciscoipphone** マクロを実行すると実装される、ポート固有の設定を示します。詳しい設定例については、「ポート固有の自動 QoS — voip ciscoipphone」（p.50-22）を参照してください。

（注） 信頼境界機能を動作させるには、CDP バージョン 2 をイネーブルにする必要があります。CDP バージョン 2 がイネーブルになっていない場合は、Syslog メッセージが表示されます。「CDP の警告」（p.50-25）を参照してください。

表 50-7　音声用のポート固有の設定（ciscoipphone キーワード）

項目	値
インターフェイス タイプ	port-based
ポリシー ソース ― config	local
ポリシー ソース ― runtime	local（デフォルト準拠）
信頼タイプ ― config	trust-cos
信頼タイプ ― runtime	trust-cos
デフォルト CoS ― config	0（デフォルト準拠）
デフォルト CoS ― runtime	0（デフォルト準拠）
trust-device	ciscoipphone
ポート接続の QoS ACL	trust-cos any（1q4t/2q2t ポートの場合。そうでない場合はなし）
QoS ACL 名	ACL_IP-PHONES（1q4t/2q2t ポートの場合。そうでない場合はなし）[1,2]
trust-ext	untrusted
cos-ext	0

1. IP QoS ACL だけが適用されます（IPX ではありません）。
2. ACL_IP-PHONES 名がすでに使用されている場合は、名前 ACL_IP-PHONES*x*（*x* は 1 ～ 99 の値）が、順次試行されます。この名前がすべて使用されている場合は、Syslog メッセージが表示されます。

ciscosoftphone に対するポート固有の自動 QoS 設定

Cisco SoftPhone に接続したポート上では、QoS 設定は、ポートに入るトラフィックのレイヤ 3 マーキングを信頼するように設定する必要があります。レイヤ 3 マーキングをすべて信頼するのはセキュリティ リスクになります。PC ユーザは DSCP 46 の非優先トラフィックを送信して不正なパフォーマンス向上を獲得する可能性があるからです。すべての着信トラフィックのポリシングによって、悪意のあるユーザがネットワークから無許可の帯域幅を獲得するのを防ぎます。ポリシングは、DSCP 46（EF）着信トラフィックを、Cisco SoftPhone アプリケーションが使用する codec レートにレート制限する（ワーストケース G.722）ことで達成します。このレートを超過するトラフィックは、デフォルトのトラフィック レート（DSCP 0 - BE）にマークダウンされます。シグナリング トラフィック（DSCP 26）も、超過するものが検出された場合はポリシングされ、ゼロにマークダウンされます。その他のすべての着信トラフィック タイプは、デフォルト トラフィック（DSCP 0 - BE）に再分類されます。

注意　Cisco SoftPhone ポートの信頼境界機能をディセーブルにする必要があります。

表 50-8 に、ポート上で自動 QoS **voip ciscoipphone** マクロを実行すると実装される、ポート固有の設定を示します。詳しい設定例については、「ポート固有の自動 QoS ― voip ciscosoftphone」（p.50-22）を参照してください。

表 50-8　音声用のポート固有の設定（ciscosoftphone キーワード）

項目	値
インターフェイス タイプ	port-based
ポリシー ソース ― config	local
ポリシー ソース ― runtime	local
信頼タイプ ― config	untrusted
項目	**値**
信頼タイプ ― runtime	untrusted
デフォルト CoS ― config	0
デフォルト CoS ― runtime	0
trust-device	none
trust-ext	untrusted
cos-ext	0
ポート接続の QoS ACL	trust-dscp aggregate POLICE_SOFTPHONE-DSCP46-x-y any dscp-field 46[1、2] trust-dscp aggregate POLICE_SOFTPHONE-DSCP26-x-y any dscp-field 26 *
QoS ACL 名	ACL_IP-SOFTPHONES-x-y[3、4]
QoS ポリサー	aggregate POLICE_SOFTPHONE-DSCP46-3-1 rate 320 burst 20 policed-dscp aggregate POLICE_SOFTPHONE-DSCP26-3-1 rate 32 burst 8 policed-dscp
QoS ポリサー名	POLICE_SOFTPHONE-DSCP46-x-y POLICE_SOFTPHONE-DSCP26-x-y

1. x = モジュール番号（ポートベース自動 QoS マクロが適用されるインターフェイス）
2. y = ポート番号（範囲が指定されている場合、範囲の最初の数値を使用）
3. IP QoS ACL だけが適用されます（IPX ではありません）。
4. ACL_IP-SOFTPHONES-x-y 名がすでに使用されている場合は、名前 ACL_IP-SOFTPHONES-x-y-z（z は 1 ～ 99 の値）が、順次試行されます。この名前がすべて使用されている場合は、エラー メッセージが表示されます。ポリサー名でも同様な動作が取られます（「ポリサー名の不足」[p.50-25] を参照）。

ciscosoftphone のポリシング設定

ciscosoftphone ポートベース自動 QoS マクロが実行されるインターフェイスには、2 つのレート リミッタが関連付けられています。2 つのレート リミッタによって、Cisco SoftPhone ポートのすべての着信トラフィックに次の特性が確保されます。

1. DSCP 46 のレートは、予期された SoftPhone アプリケーション レート以下（ワーストケース G.722）。
2. DSCP 26 のレートは、予期されたシグナリング レート以下。
3. その他すべてのトラフィックは DSCP 0（デフォルト トラフィック）に再マーキングされる。

アクション 3 はデフォルトの QoS ACL によって達成されます。アクション 1 または 2 を超過するトラフィックはゼロに policed-dscp が行われます（DSCP 0 - BE にマーキングが戻されます）。

DSCP-46 は、バーストが 20 KB の 320 Kbps のレートでポリシングされます。DSCP 26 は、バーストが 8 KB の 32 Kbps でポリシングされます。バーストおよびレートの値は、256 Kbps のワーストケース G.722 codec（256 バイトの最大パケット長）と最大パケット長が 1000 バイトのマイナー シ

グナリングに基づきます。シグナリングは、DSCP 26 と、DSCP 46 の SoftPhone ストリームのベアラ チャネルで伝送されます。

ポートは、すべてのポート タイプで untrusted に設定され、入力 QoS スケジューリングを防ぎます。グローバル自動 QoS マクロは、policed-dscp-map を設定して、DSCP 46 と DSCP 26 がともに DSCP 0 にマークダウンされるようにします。また、グローバル自動 QoS マクロは、その他のすべてのトラフィックを DSCP 0 に再マーキングするのに使用する、デフォルト QoS IP ACL を設定します。

ciscosoftphone の制限事項

Catalyst 6500 シリーズ スイッチ上でサポートされるポリサーと QoS ACL の総数には制限があるので、**ciscosoftphone** 自動 QoS マクロには同様な制限が対応付けられています。最大 1023 の集約ポリサーがサポートされています。また、約 500 の Cisco SoftPhone インターフェイスがサポートされています（その他の QoS ACL およびセキュリティ ACL が設定されている場合は、その数は減ります）。

Cisco SoftPhone インターフェイスが大量にある場合は、起動時間と NVRAM（不揮発性 RAM）スペースの両方に影響が出ます。Cisco SoftPhone インスタンスの数が大量にあると、起動時間が増えます。Cisco SoftPhone インスタンスの数が多いと、NVRAM スペースが不足する可能性があります。NVRAM スペースの不足を回避するには、テキスト設定モードを使用する必要があります。詳細については、「TCAM スペースの不足」（p.50-24）を参照してください。

ポート固有の自動 QoS 設定 ― trust cos

trust cos 自動 QoS キーワードは、「すべてを信頼する」解決策が必要なポートに使用します。このキーワードは、ポートがすべての着信トラフィックのレイヤ 2 でマーキング（CoS）を信頼するので、その他のスイッチ、または既知のサーバに接続するポートでだけ使用します。信頼境界機能はディセーブルであり、このようなタイプのポート上では QoS ポリシングは設定されません。

表 50-9 に、ポート上で自動 QoS 信頼マクロ実行後の設定の詳細について概説します。設定例については、「ポート固有の自動 QoS ― trust cos」（p.50-23）を参照してください。

表 50-9　信頼用のポート固有の設定（trust cos キーワード）

項目	値
インターフェイス タイプ	port-based
ポリシー ソース ― config	local
ポリシー ソース ― runtime	local（デフォルト準拠）
信頼タイプ ― config	trust-cos
信頼タイプ ― runtime	trust-cos
デフォルト CoS ― config	0（デフォルト準拠）
デフォルト CoS ― runtime	0（デフォルト準拠）
trust-device	none
ポート接続の QoS ACL	trust-cos any（1q4t/2q2t ポートの場合。そうでない場合はなし）
QoS ACL 名	ACL_IP-TRUSTCOS（1q4t/2q2t ポートの場合。そうでない場合はなし）[1,2]
trust-ext	untrusted
cos-ext	0

1. IP QoS ACL だけが適用されます（IPX ではありません）。
2. ACL_IP-TRUSTCOS 名がすでに使用されている場合は、名前 ACL_IP-TRUSTCOS*x*（*x* は 1 ～ 99 の値）が、順次試行されます。この名前がすべて使用されている場合は、Syslog メッセージが表示されます。

ポート固有の自動 QoS 設定 — trust dscp

trust dscp 自動 QoS キーワードは、「すべてを信頼する」解決策が必要なポートに使用します。ポートがすべての着信トラフィックのレイヤ 3 でのマーキング（DSCP）を信頼するので、このキーワードはその他のスイッチ、または既知のサーバに接続するポートでだけ使用します。信頼境界機能はディセーブルであり、このようなタイプのポート上では QoS ポリシングは設定されません。

表 50-10 に、ポート上で自動 QoS 信頼マクロ実行後の設定の詳細について概説します。設定例については、「ポート固有の自動 QoS 設定 — trust dscp」（p.50-13）を参照してください。

表 50-10　信頼用のポート固有の設定（trust dscp キーワード）

項目	値
インターフェイス タイプ	port-based
ポリシー ソース — config	local
ポリシー ソース — runtime	local（デフォルト準拠）
信頼タイプ — config	trust-dscp（1q4t/2q2t ポートを除くすべて） untrusted（1q4t/2q2t ポート）
信頼タイプ — runtime	trust-dscp（1q4t/2q2t ポートを除くすべて） untrusted（1q4t/2q2t ポート）
デフォルト CoS — config	0（デフォルト準拠）
デフォルト CoS — runtime	0（デフォルト準拠）
trust-device	none
ポート接続の QoS ACL	trust-dscp any（1q4t/2q2t ポートの場合。そうでない場合はなし）
QoS ACL 名	ACL_IP-TRUSTDSCP（1q4t/2q2t ポートの場合。そうでない場合はなし）[1、2]
trust-ext	untrusted
cos-ext	0

1. IP QoS ACL だけが適用されます（IPX ではありません）。
2. ACL_IP-TRUSTDSCP 名がすでに使用されている場合は、名前 ACL_IP-TRUSTDSCP*x*（*x* は 1 ～ 99 の値）が、順次試行されます。この名前がすべて使用されている場合は、Syslog メッセージが表示されます。

自動 QoS の CLI インターフェイス

ここでは、自動 QoS の CLI インターフェイスについて説明します。

- グローバル自動 QoS マクロ — set qos autoqos（p.50-14）
- ポート固有の自動 QoS マクロ — set port qos autoqos（p.50-14）
- QoS 設定の表示（p.50-15）
- 自動 QoS 設定の消去（p.50-15）
- QoS 設定のトラッキング（p.50-18）

グローバル自動 QoS マクロ — set qos autoqos

グローバル自動 QoS マクロを実行すると、スイッチのすべてのポートにグローバル QoS 設定が適用されます。終了後、プロンプトが表示され、ポートベース自動 QoS コマンドが現在サポートされていることを示します。

```
Console> (enable) set qos autoqos ?
Usage: set qos autoqos
Console> (enable) set qos autoqos
QoS is enabled.
........
All ingress and egress QoS scheduling parameters configured on all ports.
CoS to DSCP, DSCP to COS, IP Precedence to DSCP and policed dscp maps configured.
Global QoS configured, port specific autoqos recommended:
    set port qos <mod/port> autoqos trust <cos|dscp>
    set port qos <mod/port> autoqos voip <ciscoipphone|ciscosoftphone>
Console> (enable)
```

ポート固有の自動 QoS マクロ — set port qos autoqos

ポート固有の自動 QoS マクロは、*mod/port* の組み合わせを受け入れます。また、AVVID タイプのキーワードを指定する必要があります。**ciscoipphone**、**ciscosoftphone**、および **trust** キーワードがサポートされています。

次に、**ciscoipphone** キーワードの使用例を示します。

```
Console> (enable) set port qos 3/1 autoqos help
Usage: set port qos <mod/port> autoqos trust <cos|dscp>
       set port qos <mod/port> autoqos voip <ciscoipphone|ciscosoftphone>
Console> (enable) set port qos 3/1 autoqos voip ciscoipphone
Port 3/1 ingress QoS configured for Cisco IP Phone.
It is recommended to execute the "set qos autoqos" global command if not executed
previously.
Console> (enable)
```

次に、**ciscosoftphone** キーワードの使用例を示します。

```
Console> (enable) set port qos 3/1 autoqos voip ciscosoftphone
Port 3/1 ingress QoS configured for Cisco Softphone.
It is recommended to execute the "set qos autoqos" global command if not executed
previously.
Console> (enable)
```

次に、**trust cos** キーワードの使用例を示します。

```
Console> (enable) set port qos 3/1 autoqos trust cos
Port 3/1 QoS configured to trust all incoming CoS marking.
It is recommended to execute the "set qos autoqos" global command if not executed
previously.
Console> (enable)
```

次に、**trust dscp** キーワードの使用例を示します。

```
Console> (enable) set port qos 3/1 autoqos trust dscp
Port 3/1 QoS configured to trust all incoming DSCP marking.
It is recommended to execute the "set qos autoqos" global command if not executed
previously.
Console> (enable)
```

QoS 設定の表示

QoS 設定を表示するには、既存の QoS **show** コマンドを入力します。これらのコマンドには、**show port qos** および **show qos info runtime** があります。

自動 QoS 設定の消去

ポートベース **clear** コマンドおよびグローバル **clear** コマンドを入力して自動 QoS 設定を消去できます。自動 QoS 設定を消去するには、ポートベース **clear** コマンドで QoS が動作している各インターフェイスを消去し、次で説明しているグローバル **clear** コマンドを入力します。

- 自動 QoS ポートベース設定の消去（p.50-15）
- 自動 QoS グローバル設定の消去（p.50-16）

自動 QoS ポートベース設定の消去

ポートベース自動 QoS コマンドを通じて設定されているすべての自動 QoS 設定は、次のように **clear port qos** *mod/port* **autoqos** コマンドを入力することで出荷時の設定に戻せます。

```
Console> (enable) set port qos 3/1 autoqos voip ciscosoftphone
Port 3/1 ingress QoS configured for Cisco Softphone.
It is recommended to execute the "set qos autoqos" global command if not executed
previously.
Console> (enable) clear port qos ?
  <mod/port>                  Module number and Port number(s)
Console> (enable) clear port qos 3/1 ?
  autoqos                     Clear port based autoqos settings
  cos                         Clear QoS default CoS value on ports
  cos-ext                     Clear QoS default CoS extension on ports
Console> (enable) clear port qos 3/1 autoqos
Port based QoS settings will be restored back to factory defaults for port 3/1.
Do you want to continue (y/n) [n]? y
Port 3/1 autoqos settings have been cleared.
It is recommended to execute the "clear qos autoqos" global command if
not executed previously to clear global autoqos settings.
Console> (enable)
```

ポートベース **clear** コマンドは、ポートベース自動 QoS **set** コマンドに対応するすべてのポートでサポートされています。自動 QoS ポートベース コマンドを通じて設定されたすべての QoS 設定は、出荷時の設定に戻ります（自動 QoS ACL を除く）。QoS ACL が自動 QoS に関連していなくても、ポートにマッピングされたすべての QoS ACL はポートからマッピング解除されます。自動 QoS 用に作成された QoS ACL は、グローバル **clear** コマンドを入力すると消去されます。

自動 QoS グローバル設定の消去

グローバル自動 QoS コマンドを通じて設定されているすべての自動 QoS 設定は、次のように **clear qos autoqos** コマンドを入力することで出荷時の設定に戻せます。

```
Console> (enable) clear qos autoqos
Its highly recommended to execute clear port autoqos commands prior
to the global clear command:
    clear port qos <mod/port> autoqos

Do you want to continue (y/n) [n]? y
.......................
Autoqos ACL 'ACL_IP-SOFTPHONE-3-1' successfully deleted.
Cleared Autoqos policer 'POLICE_SOFTPHONE-DSCP46-3-1'
Cleared Autoqos policer 'POLICE_SOFTPHONE-DSCP26-3-1'

All ingress and egress QoS scheduling parameters set to factory default.
CoS to DSCP, DSCP to COS, IP Precedence to DSCP and policed dscp maps
configured.  Global Autoqos QoS cleared.
Console> (enable)
```

set port autoqos コマンドを通じて作成された QoS ACL はグローバル自動 QoS **clear** コマンドを入力すると消去されます。さらに、自動 QoS ACL で使用されるポリサーも消去されます。

グローバル自動 QoS **clear** コマンドは、自動 QoS ACL 名を検索します。検索アルゴリズムは、次の文字列で開始される名前を探します。

- ACL_IP-PHONES（ciscoipphone の場合）
- ACL_IP-SOFTPHONE（ciscoipphone の場合）
- ACL_IP-TRUSTCOS（trust cos の場合）
- ACL_IP-TRUSTDSCP（trust dscp の場合）

上記の文字列で開始される QoS ACL は自動 QoS ACL とみなされて消去されます。QoS ACL 名が見つかり、QoS ACL がコミットされていて、それがポートや VLAN にマッピングされている場合、自動 QoS ACL が削除されます。

同様に、検索アルゴリズムは名前が次の文字列で始まる集約 QoS ポリサーを検索します。
POLICE_SOFTPHONE-DSCP（ciscosoftphone の場合）

グローバル **clear** コマンドは、POLICE_SOFTPHONE-DSCP で始まる集約ポリサー名を検索します。ポリサーが検出されて、これに関連する QoS ACL がない場合、このポリサーが削除されます。ポリサーが検出されて、これに関連する QoS ACL がある場合、ポリサーが使用中であることを示す警告が表示されます。

グローバル **clear** コマンドを使用する場合、さまざまなエラー状態が発生する可能性があります。グローバル **clear** コマンドを入力する前に適切にポートベース **clear** コマンドを実行した場合、エラー状態が発生することはありません。ただし、グローバル **clear** コマンドを最初に使用したり自動 QoS 設定を変更した場合、エラー状態が発生する場合があります。

- 自動 QoS ACL はまだポートまたは VLAN にマッピングされています。

  グローバル **clear** コマンドは、VLAN やポートにマッピングされている自動 QoS ACL を削除しません。代わりに、コマンドはポートや VLAN にマッピングされている QoS ACL 名を示す警告を表示します。
- 集約ポリサーは使用中です。

  自動 QoS ポリサーが使用中（QoS ACL が参照中）の場合、グローバル **clear** コマンドはこれを削除できません。代わりに、集約ポリサー名を表示します。
- 自動 QoS ACL はコミットされません。

  グローバル **clear** コマンドは、コミットされた自動 QOS ACL のみを削除しますが、コミットされていない自動 QoS ACL は無視します。

次に、これらの各種エラー状態で表示される内容の例を示します。

```
Console> (enable) clear qos autoqos
Its highly recommended to execute clear port autoqos commands prior
to the global clear command:
    clear port qos <mod/port> autoqos

Do you want to continue (y/n) [n]? y
.......................
Autoqos ACL 'ACL_IP-SOFTPHONE-3-2' successfully deleted.
Autoqos ACL 'ACL_IP-SOFTPHONE-3-3' successfully deleted.
Autoqos ACL 'ACL_IP-SOFTPHONE-3-4' still mapped to port or vlan.
Autoqos ACL 'ACL_IP-SOFTPHONE-3-5' still mapped to port or vlan.
Autoqos ACL 'ACL_IP-SOFTPHONE-3-6' still mapped to port or vlan.
Cleared Autoqos policer 'POLICE_SOFTPHONE-DSCP46-3-2'
Cleared Autoqos policer 'POLICE_SOFTPHONE-DSCP26-3-2'
Cleared Autoqos policer 'POLICE_SOFTPHONE-DSCP46-3-3'
Cleared Autoqos policer 'POLICE_SOFTPHONE-DSCP26-3-3'
Could not clear Autoqos policer ''POLICE_SOFTPHONE-DSCP46-3-4', still in use.
QoS is disabled.

All ingress and egress QoS scheduling parameters set to factory default.
CoS to DSCP, DSCP to COS, IP Precedence to DSCP and policed dscp maps
configured.  Global Autoqos QoS cleared.
Console> (enable)
```

QoS 設定のトラッキング

コンフィギュレーション ファイルに表示される「コメント」を確認することで、QoS 設定が従来の QoS と自動 QoS のどちらに基づいているかを判別できます。従来の QoS または自動 QoS コメントは、**set qos autoqos** グローバル コンフィギュレーション コマンドの入力後に作成され、**clear global autoqos** コマンドまたは **clear qos config** コマンドが入力されるまで残ります。次に例を示します。

```
Console> (enable) set qos autoqos
..............
All ingress and egress QoS scheduling parameters configured on all ports.
CoS to DSCP, DSCP to COS, IP Precedence to DSCP and policed dscp maps
configured.  Global QoS configured, port specific autoqos recommended:
    set port qos <mod/port> autoqos trust <cos|dscp>
    set port qos <mod/port> autoqos voip <ciscoipphone|ciscosoftphone>
Console> (enable) show config
This command shows non-default configurations only.
Use 'show config all' to show both default and non-default configurations.
..................


.............................

.........................

..

begin
<snip>
#qos - qos configuration via autoqos
set qos enable
set qos map 2q2t tx 2 1 cos 1
set qos map 2q2t tx 2 1 cos 2
<snip>
Console> (enable) clear qos autoqos
Its highly recommended to execute clear port autoqos commands prior
to the global clear command:
    clear port qos <mod/port> autoqos

Do you want to continue (y/n) [n]? y
.......................

No Autoqos ACLs found.
No Autoqos aggregate policer(s) found.
QoS is disabled.

All ingress and egress QoS scheduling parameters set to factory default.
CoS to DSCP, DSCP to COS, IP Precedence to DSCP and policed dscp maps
configured.  Global Autoqos QoS cleared.
Console> (enable) show config
This command shows non-default configurations only.
Use 'show config all' to show both default and non-default configurations.
..................

<snip>
#qos
<snip>
Console> (enable)
```

自動 QoS 設定ステートメントの詳細

ここでは、自動 QoS 設定ステートメントの詳細を示します。

グローバル自動 QoS マクロ

グローバル自動 QoS コマンドを入力すると、次のような設定になります。

```
set qos autoqos
---------------
set qos enable

set qos policy-source local
set qos ipprec-dscp-map 0 10 18 26 34 46 48 56
set qos cos-dscp-map 0 10 18 26 34 46 48 56
set qos dscp-cos-map 0-7:0 8-15:1 16-23:2 24-31:3 32-39:4 40-47:5 48-55:6 56-63:7
set qos acl default-action ip dscp 0
set qos map 2q2t tx queue 2 2 cos 5,6,7
set qos map 2q2t tx queue 2 1 cos 1,2,3,4
set qos map 2q2t tx queue 1 1 cos 0
set qos drop-threshold 2q2t tx queue 1 100 100
set qos drop-threshold 2q2t tx queue 2 80 100
set qos drop-threshold 1q4t rx queue 1 50 60 80 100
set qos txq-ratio 2q2t 80 20
set qos wrr 2q2t 100 255

set qos map 1p3q1t tx 1 1 cos 0
set qos map 1p3q1t tx 2 1 cos 1,2
set qos map 1p3q1t tx 3 1 cos 3,4
set qos map 1p3q1t tx 3 0 cos 6,7
set qos map 1p3q1t tx 4 cos 5
set qos wrr 1p3q1t 20 100 200
set qos wred 1p3q1t queue 1 70:100
set qos wred 1p3q1t queue 2 70:100
set qos wred 1p3q1t queue 3 70:90
set qos map 1p1q0t rx 1 cos 0,1,2,3,4
set qos map 1p1q0t rx 2 cos 5,6,7
set qos rxq-ratio 1p1q0t 80 20
set qos map 1p2q2t tx 1 2 cos 0
set qos map 1p2q2t tx 2 1 cos 1,2,3,4
set qos map 1p2q2t tx 2 2 cos 6,7
set qos map 1p2q2t tx 3 cos 5
set qos txq-ratio 1p2q2t 75 15 15
set qos wrr 1p2q2t 50 255
set qos wred 1p2q2t queue 1 1 40:70
set qos wred 1p2q2t queue 1 2 70:100
set qos wred 1p2q2t queue 2 1 40:70
set qos wred 1p2q2t queue 2 2 70:100
set qos map 1p1q4t rx 1 1 cos 0
set qos map 1p1q4t rx 1 3 cos 1,2,3,4
set qos map 1p1q4t rx 1 4 cos 6,7
set qos map 1p1q4t rx 2 cos 5
set qos drop-threshold 1p1q4t rx queue 1 50 60 80 100

set qos map 1p2q1t tx 1 1 cos 0
set qos map 1p2q1t tx 2 1 cos 1,2,3,4
set qos map 1p2q1t tx 2 cos 6,7
set qos map 1p2q1t tx 3 cos 5
set qos txq-ratio 1p2q1t 75 15 15
set qos wrr 1p2q1t 50 255
```

```
set qos wred 1p2q1t queue 1 70:100
set qos wred 1p2q1t queue 2 70:100
set qos map 1p1q8t rx 1 1 cos 0
set qos map 1p1q8t rx 1 5 cos 1,2
set qos map 1p1q8t rx 1 8 cos 3,4
set qos map 1p1q8t rx 2 cos 5,6,7
set qos wred 1p1q8t queue 1 1 40:70
set qos wred 1p1q8t queue 1 5 60:90
set qos wred 1p1q8t queue 1 8 70:100
set qos rxq-ratio 1p1q8t 80 20
set qos policed-dscp-map 0:0
set qos policed-dscp-map 1:1
set qos policed-dscp-map 2:2
set qos policed-dscp-map 3:3
set qos policed-dscp-map 4:4
set qos policed-dscp-map 5:5
set qos policed-dscp-map 6:6
set qos policed-dscp-map 7:7
set qos policed-dscp-map 8:8
set qos policed-dscp-map 9:9
set qos policed-dscp-map 10:10
set qos policed-dscp-map 11:11
set qos policed-dscp-map 12:12
set qos policed-dscp-map 13:13
set qos policed-dscp-map 14:14
set qos policed-dscp-map 15:15
set qos policed-dscp-map 16:16
set qos policed-dscp-map 17:17
set qos policed-dscp-map 18:18
set qos policed-dscp-map 19:19
set qos policed-dscp-map 20:20
set qos policed-dscp-map 21:21
set qos policed-dscp-map 22:22
set qos policed-dscp-map 23:23
set qos policed-dscp-map 24:24
set qos policed-dscp-map 25:25
set qos policed-dscp-map 26:0
set qos policed-dscp-map 27:27
set qos policed-dscp-map 28:28
set qos policed-dscp-map 29:29
set qos policed-dscp-map 30:30
set qos policed-dscp-map 31:31
set qos policed-dscp-map 32:32
set qos policed-dscp-map 33:33
set qos policed-dscp-map 34:34
set qos policed-dscp-map 35:35
set qos policed-dscp-map 36:36
set qos policed-dscp-map 37:37
set qos policed-dscp-map 38:38
set qos policed-dscp-map 39:39
set qos policed-dscp-map 40:40
set qos policed-dscp-map 41:41
set qos policed-dscp-map 42:42
set qos policed-dscp-map 43:43
set qos policed-dscp-map 44:44
set qos policed-dscp-map 45:45
set qos policed-dscp-map 46:0
set qos policed-dscp-map 47:47
set qos policed-dscp-map 48:48
set qos policed-dscp-map 49:49
set qos policed-dscp-map 50:50
set qos policed-dscp-map 51:51
set qos policed-dscp-map 52:52
set qos policed-dscp-map 53:53
set qos policed-dscp-map 54:54
set qos policed-dscp-map 55:55
set qos policed-dscp-map 56:56
set qos policed-dscp-map 57:57
set qos policed-dscp-map 58:58
set qos policed-dscp-map 59:59
```

```
set qos policed-dscp-map 60:60
set qos policed-dscp-map 61:61
set qos policed-dscp-map 62:62
set qos policed-dscp-map 63:63
set qos policed-dscp-map excess-rate 0:0
set qos policed-dscp-map excess-rate 1:1
set qos policed-dscp-map excess-rate 2:2
set qos policed-dscp-map excess-rate 3:3
set qos policed-dscp-map excess-rate 4:4
set qos policed-dscp-map excess-rate 5:5
set qos policed-dscp-map excess-rate 6:6
set qos policed-dscp-map excess-rate 7:7
set qos policed-dscp-map excess-rate 8:8
set qos policed-dscp-map excess-rate 9:9
set qos policed-dscp-map excess-rate 10:10
set qos policed-dscp-map excess-rate 11:11
set qos policed-dscp-map excess-rate 12:12
set qos policed-dscp-map excess-rate 13:13
set qos policed-dscp-map excess-rate 14:14
set qos policed-dscp-map excess-rate 15:15
set qos policed-dscp-map excess-rate 16:16
set qos policed-dscp-map excess-rate 17:17
set qos policed-dscp-map excess-rate 18:18
set qos policed-dscp-map excess-rate 19:19
set qos policed-dscp-map excess-rate 20:20
set qos policed-dscp-map excess-rate 21:21
set qos policed-dscp-map excess-rate 22:22
set qos policed-dscp-map excess-rate 23:23
set qos policed-dscp-map excess-rate 24:24
set qos policed-dscp-map excess-rate 25:25
set qos policed-dscp-map excess-rate 26:26
set qos policed-dscp-map excess-rate 27:27
set qos policed-dscp-map excess-rate 28:28
set qos policed-dscp-map excess-rate 29:29
set qos policed-dscp-map excess-rate 30:30
set qos policed-dscp-map excess-rate 31:31
set qos policed-dscp-map excess-rate 32:32
set qos policed-dscp-map excess-rate 33:33
set qos policed-dscp-map excess-rate 34:34
set qos policed-dscp-map excess-rate 35:35
set qos policed-dscp-map excess-rate 36:36
set qos policed-dscp-map excess-rate 37:37
set qos policed-dscp-map excess-rate 38:38
set qos policed-dscp-map excess-rate 39:39
set qos policed-dscp-map excess-rate 40:40
set qos policed-dscp-map excess-rate 41:41
set qos policed-dscp-map excess-rate 42:42
set qos policed-dscp-map excess-rate 43:43
set qos policed-dscp-map excess-rate 44:44
set qos policed-dscp-map excess-rate 45:45
set qos policed-dscp-map excess-rate 46:46
set qos policed-dscp-map excess-rate 47:47
set qos policed-dscp-map excess-rate 48:48
set qos policed-dscp-map excess-rate 49:49
set qos policed-dscp-map excess-rate 50:50
set qos policed-dscp-map excess-rate 51:51
set qos policed-dscp-map excess-rate 52:52
set qos policed-dscp-map excess-rate 53:53
set qos policed-dscp-map excess-rate 54:54
set qos policed-dscp-map excess-rate 55:55
set qos policed-dscp-map excess-rate 56:56
set qos policed-dscp-map excess-rate 57:57
set qos policed-dscp-map excess-rate 58:58
set qos policed-dscp-map excess-rate 59:59
set qos policed-dscp-map excess-rate 60:60
set qos policed-dscp-map excess-rate 61:61
set qos policed-dscp-map excess-rate 62:62
set qos policed-dscp-map excess-rate 63:63
```

ポート固有の自動 QoS ― voip ciscoipphone

ポート固有の自動 QoS コマンドを入力すると、次のような設定になります。

```
set port qos mod/port autoqos voip ciscoipphone
---------------
set port qos mod/port policy-source local
set port qos mod/port port-based
set port qos mod/port cos 0
set port qos mod/port cos-ext 0
set port qos mod/port trust-ext untrusted
set port qos mod/port trust-device ciscoipphone
```

ポート タイプが 1q4t/2q2t の場合、次のような設定になります。

```
set qos acl ip ACL_IP-PHONES trust-cos any
commit qos acl ACL_IP-PHONES
set qos acl map ACL_IP-PHONES mode/port
set port qos mod/port trust trust-cos
```

ポート タイプが別のポート タイプの場合、次のような設定になります。

```
set port qos mod/port trust trust-cos
```

（注） ACL_IP-PHONES 名が使用中の場合、自動 QoS は、既存の ACL が作成しようとしているものと同じかどうか確認します。既存の QoS ACL が同じである場合は、自動 QoS によって再使用されます。既存の QoS ACL が同じでない場合は、自動 QoS は他の名前を試みます。

ポート固有の自動 QoS ― voip ciscosoftphone

ポート固有の自動 QoS コマンドを入力すると、次のような設定になります。

```
set port qos mod/port autoqos voip ciscosoftphone
---------------
set port qos mod/port policy-source local
set port qos mod/port port-based
set port qos mod/port cos 0
set port qos mod/port cos-ext 0
set port qos mod/port trust-ext untrusted
set port qos mod/port trust-device none
set port qos mod/port trust untrusted
set qos policer aggregate POLICE_SOFTPHONE-DSCP46-mod-port rate 320 burst 20
policed-dscp
set qos policer aggregate POLICE_SOFTPHONE-DSCP26-mod-port rate 32  burst 8
policed-dscp
set qos acl ip ACL_IP-SOFTPHONE-mod-port trust-dscp aggregate
POLICE_SOFTPHONE-DSCP46-mod-port any dscp-field 46
set qos acl ip ACL_IP-SOFTPHONE-mod-port trust-dscp aggregate
POLICE_SOFTPHONE-DSCP26-mod-port any dscp-field 26
commit qos acl ACL_IP-SOFTPHONE-mod-port
set qos acl map ACL_IP-SOFTPHONE-mod-port mod/port
```

ポート固有の自動 QoS — trust cos

ポート固有の自動 QoS コマンドを入力すると、次のような設定になります。

```
set port qos mod/port autoqos trust cos
---------------
set port qos mod/port policy-source local
set port qos mod/port port-based
set port qos mod/port cos 0
set port qos mod/port cos-ext 0
set port qos mod/port trust-ext untrusted
set port qos mod/port trust-device none
```

ポート タイプが 1q4t/2q2t の場合、次のような設定になります。

```
set qos acl ip ACL_IP-TRUSTCOS trust-cos any
commit qos acl ACL_IP-TRUSTCOS
set qos acl map ACL_IP-TRUSTCOS mode/port
set port qos mod/port trust trust-cos
```

ポート タイプが別のポート タイプの場合、次のような設定になります。

```
set port qos mod/port trust trust-cos
```

ポート固有の自動 QoS — trust dscp

ポート固有の自動 QoS コマンドを入力すると、次のような設定になります。

```
set port qos mod/port autoqos trust cos
---------------
set port qos mod/port policy-source local
set port qos mod/port port-based
set port qos mod/port cos 0
set port qos mod/port cos-ext 0
set port qos mod/port trust-ext untrusted
set port qos mod/port trust-device none
```

ポート タイプが 1q4t/2q2t の場合、次のような設定になります。

```
set qos acl ip ACL_IP-TRUSTCOS trust-cos any
commit qos acl ACL_IP-TRUSTCOS
set qos acl map ACL_IP-TRUSTCOS mode/port
set port qos mod/port trust trust-cos
```

ポート タイプが別のポート タイプの場合、次のような設定になります。

```
set port qos mod/port trust trust-cos
```

警告とエラー状況

ここでは、自動 QoS の警告とエラー状況について説明します。

ACL 名の不足

1q4t/2q2t タイプのポートに対して QoS ACL を作成して信頼に関する問題を解決する際、次の QoS ACL 名がすでに使用中なので注意してください（x は 1 ～ 99）。

- ACL_IP-PHONESx（**ciscoipphone** の場合）
- ACL_IP-SOFTPHONE-m-p-x（**ciscosoftphone** の場合）
- ACL_IP-TRUSTCOSx（**trust cos** の場合）
- ACL_IP-TRUSTDSCPx（**trust dscp** の場合）

次に、システムの ACL 名がない場合の表示例を示します。

```
Console> (enable) set port qos 4/1 autoqos voip ciscoipphone
ERROR:  IP QoS ACL name in use, could not configure QoS ACL.
Rename existing QoS ACL ACL_IP-PHONES.
Autoqos did not complete.  Settings remain unchanged.
Console> (enable)
```

TCAM スペースの不足

ポートベースの自動 QoS コマンドを使用して ACL を設定する場合、Ternary CAM（TCAM）がいっぱいである可能性があります。このような場合は、エラー メッセージが表示され、ポートベースの自動 QoS コマンドは失敗し、すべての QoS 設定は元のままとなります。

次に、システムに TCAM スペースがない場合の表示例を示します。

```
Console> (enable) set port qos 4/1 autoqos voip ciscoipphone
Error:  Please remove QoS or security ACLs to make space for new QoS ACL.
Autoqos did not complete.  Settings remain unchanged.
Console> (enable)
```

COPS 警告メッセージ

COPS がグローバルにイネーブルになっているか、ポート上でイネーブルになっている場合に、グローバル自動 QoS コマンドまたはポート固有の自動 QoS コマンドを実行すると、ポリシー ソースがローカルに変更され、警告メッセージが表示されます。

次に、ポートベースのコマンドが正常終了した場合に、次のようにポートベースのポリシー設定がローカルに変更される例を示します。

```
Console> (enable) set port qos 4/1 autoqos voip ciscosoftphone
Warning:  QoS policy changed to local for port 4/1.
Port 4/1 ingress QoS configured for ciscosoftphone.
It is recommended to execute the "set qos autoqos" global command if not executed
previously.
```

次の例はグローバル コマンドのもので、グローバル自動 QoS コマンドの実行に先立ってグローバル QoS ポリシーが COPS である場合は、次のように警告メッセージが表示されることを示します。

```
Console> (enable) set qos autoqos
........
Warning: QoS policy source changed to local.
All ingress and egress QoS scheduling parameters configured on all ports.
CoS to DSCP, DSCP to COS and IP Precedence to DSCP maps configured.
Global QoS configured, port specific autoqos recommended:
   set port qos <mod/port> autoqos trust [cos|dscp]
   set port qos <mod/port> autoqos voip [ciscoipphone|ciscosoftphone]
Console> (enable)
```

CDP の警告

ciscoipphone キーワードを指定し、trust オプションを指定しないでポート固有の自動 QoS コマンドを実行すると、trust-device 機能がイネーブルになります。trust-device 機能は CDP に依存します。CDP がイネーブルになっていないか、バージョン 2 が稼働していない場合は、次のように警告メッセージが表示されます。

```
Console> (enable) set port qos 4/1 autoqos voip ciscoipphone
Warning:  CDP is disabled or CDP version 1 is in use.  Ensure that CDP version 2 is
enabled globally, and also ensure that CDP is enabled on the port(s) you wish to
configure autoqos on.
Port 4/1 ingress QoS configured for ciscoipphone.
It is recommended to execute the "set qos autoqos" global command if not executed
previously.
Console> (enable)
```

ポリサー名の不足

ciscosoftphone キーワードを指定してポート固有の自動 QoS コマンドを実行すると、2 つのポリサーインスタンスが作成され、次のストリングで名前が付けられます。

- POLICE_SOFTPHONE-DSCP46-x-y
- POLICE_SOFTPHONE-DSCP26-x-y

この場合は、x はモジュール番号、y はポート番号で、*mod/port* の組み合わせは **ciscosoftphone** キーワードで指定します。

上のポリサー名がすでに使用中の場合、マクロは次の名前を試みます。

- POLICE_SOFTPHONE-DSCP46-x-y-z
- POLICE_SOFTPHONE-DSCP26-x-y-z

この場合、z は 1 ～ 99 で、1 から始まります。両方の名前が同じ z 値で有効になる必要があります。そうしないと、両方の名前が同じ z 値で有効になるまで、マクロは次の z 値を順次試みます。z の値を 99 にして失敗した場合は、次のエラー メッセージが表示され、すべての設定は元のままです。

```
Console> (enable) set port qos 4/1 autoqos voip ciscosoftphone
ERROR:  QoS policer name in use, could not configure QoS policer.
Rename existing QoS policer POLICE_SOFTPHONE-DSCP46-4-1 and/or
POLICE_SOFTPHONE-DSCP26-4-1.
Autoqos did not complete.  Settings remain unchanged.
Console> (enable)
```

ディセーブルになった QoS

QoS がディセーブルになっているインターフェイス上でポートベースの自動 QoS コマンドを実行すると、次のように CLI に通知メッセージが表示されます。

```
Console> (enable) set port qos 4/1 autoqos voip ciscosoftphone
Port 4/1 ingress QoS configured for ciscosoftphone.  Policing configured on 4/1.
QoS is disabled, changes will take effect after QoS is enabled.
It is recommended to execute the "set qos autoqos" global command if not executed
previously.
Console> (enable)
```

Syslog の追加

次のように、QoS ファシリティにスイッチのロギング レベルを 4 または 5 に設定します（**set logging level qos 5**）。

- ログ レベル 4 = 警告
- ログ レベル 5 = 通知

ここでは、自動 QoS 機能に対する Syslog の追加について説明します。

- CDP の警告 — 警告レベル（p.50-26）
- 必要なすべてのポートでのインターフェイス変更 — 警告レベル（p.50-26）

CDP の警告 — 警告レベル

ポート上で CDP がディセーブルになっているか、CDP がグローバルにディセーブルになっている場合、あるいは CDP がバージョン 1 モードで稼働している場合、ポートベースの自動 QoS **voip ciscoipphone** キーワードを実行すると、次のように警告メッセージが表示されます。

```
Console> (enable)
2001 Jun 02 09:20:42 %QOS-4-DEVICE_CDP_DIS:Trust-Device feature enabled with CDP
disabled or running in v1 mode.
Console> (enable)
```

必要なすべてのポートでのインターフェイス変更 — 警告レベル

1p1q0t/1p3q1t ポートの場合、インターフェイス タイプの変更が必要な場合（自動 QoS マクロの実行前に VLAN ベースのモードが設定されているとき）は、次のように Syslog メッセージが表示され、モジュール内のすべてのポートでインターフェイス タイプがポートベースの QoS に変更されたことを示します。

```
Console> (enable)
2001 Jun 02 09:20:42 %QOS-3-INTERFACE-CHANGED:All ports in module 3 have been
configured to port-based QoS.
Console> (enable)
```

その他の関連 Syslog メッセージ

ここでは、自動 QoS 設定に関連するその他の関連 Syslog メッセージについて説明します。

- 装置がポートで検出されない — 通知レベル（信頼境界機能）（p.50-26）
- ポート上で装置が検出された — 通知レベル（p.50-27）
- trust-device 設定で CDP がディセーブルになっている — 警告レベル（p.50-27）

装置がポートで検出されない — 通知レベル（信頼境界機能）

ciscoipphone キーワードを使用してポート上で信頼境界をイネーブルにすると、電話でポートとの接続が解除されていることが検出された場合、次のように Syslog メッセージが表示され、装置の接続が解除され、ポートの信頼状態が変更されたことを示します。

```
Console> (enable)
2001 Jun 02 09:20:42 %QOS-5-DEVICE_LOST:ciscoipphone not detected on port 4/1, port
set to untrusted.
Console> (enable)
```

ポート上で装置が検出された ― 通知レベル

信頼できる装置がポートに接続されると、Syslog メッセージが表示され、ポートの信頼状態が変更されたことを示します。見出しには、設定で指定した新しい信頼のタイプが含まれます。次の例では、設定でポート 4/1 の信頼状態が [trust-cos] に設定されています。

```
Console> (enable)
2001 Jun 02 09:20:42 %QOS-5-DEVICE_DETECTED:ciscoipphone detected on port 4/1, port
set to trust-cos.
Console> (enable)
```

trust-device 設定で CDP がディセーブルになっている ― 警告レベル

ポート上でポートベースの自動 QoS **ciscoipphone** キーワードを実行すると、trust-device が、信頼境界をアクティブにする [ciscoipphone] に設定されます。信頼境界機能をイネーブルにすると、ポート上で CDP がディセーブルになっているか、CDP がバージョン 1 モードで稼働している場合、あるいは CDP がグローバルにディセーブルになっている場合は、次のように Syslog メッセージが表示されます。

```
Console> (enable)
2001 Jun 02 09:20:42 %QOS-4-DEVICE_CDP_DIS:Trust-Device feature enabled with CDP
disabled or running in v1 mode.
Console> (enable)
```

このメッセージは、問題が検出されたときに一度だけ表示されます。問題が解決すると、設定が再度壊された場合にこのメッセージが再び表示されることがあります。誤った設定の検出のための時間は最大 15 秒です。

自動 QoS 機能の要約

ここでは、QoS 機能を要約します。

- グローバル自動 QoS 機能（set qos autoqos）（p.50-27）
- ポートベースの自動 QoS 機能（p.50-27）

グローバル自動 QoS 機能（set qos autoqos）

グローバル自動 QoS 機能は、次のように要約されます。

- 「音声および映像ネットワーク用の一般的な CoS および DSCP 値」（p.50-2）に記載のすべてのトラフィック タイプに対応し、優先順位を付けるようにスイッチ全般の QoS パラメータをすべて設定します。
- 以前に適用された古いまたは誤った設定を上書きします。
- ポートベースの自動 QoS コマンドを操作します。

ポートベースの自動 QoS 機能

ポートベースの自動 QoS 機能は、次のように要約されます。

- voip ciscoipphone
  - ― ポートベースの QoS にポートを変更します。
  - ― 1p1q0t/1p3q1t ポートの場合は、すべてのポートをポートベース モードに変更します。
  - ― trust-cos QoS ACL を、必要とするポートに対して作成します（1q4t/2q2t ポート）。
  - ― trust-cos ACL をポートに適用します（1q4t/2q2t ポート）。

  - ポート上で信頼境界をイネーブルにします。
  - ポートの信頼を trust-cos に設定します。
  - 補助 VLAN 付きまたはなしのポートをサポートしています。
  - 10/100 ポートおよび 10/100/1000 ポート上でのみサポートしています。
  - PFC や PFC2 は不要です（PFC および PFC2 はサポートされています）。
- voip ciscosoftphone
  - ポートベースの QoS にポートを変更します。
  - 信頼を untrusted に変更します。
  - 1p1q0t/1p3q1t ポートの場合は、すべてのポートをポートベース モードに変更します。
  - ポート上で信頼境界をディセーブルにします。
  - 2 つのレート リミッタを適用します。1 つは DSCP 46、もう 1 つは DSCP 26 着信トラフィック用です。着信の DSCP 46 および DSCP 26 トラフィックに限って信頼します。
  - いずれかのレート リミッタの違反のため、トラフィックを DSCP 0 にマークダウンします。
  - その他すべて（DSCP 26 および 46 以外）の着信トラフィックを DSCP 0 に再マーキングします。
  - 補助 VLAN 付きまたはなしのポートをサポートしています。
  - すべてのポート上でサポートされています。
  - PFC または PFC2 が必要です。
- trust cos
  - ポートベースの QoS にポートを変更します。
  - 1p1q0t/1p3q1t ポートの場合は、すべてのポートをポートベース モードに変更します。
  - trust-cos QoS ACL を、必要とするポートに対して作成します（1q4t/2q2t ポート）。
  - trust-cos ACL をポートに適用します（1q4t/2q2t ポート）。
  - ポート上で信頼境界をディセーブルにします。
  - ポートの信頼を trust-cos に設定します。
  - 補助 VLAN 付きまたはなしのポートをサポートしています。
  - すべてのポート上でサポートされています。
  - PFC は不要です（PFC および PFC2 はサポートされています）。
- trust dscp
  - ポートベースの QoS にポートを変更します。
  - 1p1q0t/1p3q1t ポートの場合は、すべてのポートをポートベース モードに変更します。
  - trust-dscp QoS ACL を、必要とするポートに対して作成します（1q4t/2q2t ポート）。
  - trust-dscp ACL をポートに適用します（1q4t/2q2t ポート）。
  - ポート上で信頼境界をディセーブルにします。
  - ポートの信頼を untrusted（1q4t/2q2t ポート）、または trust-dscp（1q4t/2q2t ポート以外）に設定します。
  - 補助 VLAN 付きまたはなしのポートをサポートしています。
  - すべてのポート上でサポートされています。
  - PFC または PFC2 が必要です。

ネットワークでの自動 QoS の使用方法

ヒント　自動 QoS が正常に機能するようにするには、グローバル自動 QoS マクロと、インターフェイスごとにインターフェイス固有自動 QoS マクロを実行する必要があります。

インターフェイスとそのインターフェイスに接続しているデバイスに応じて、さまざまな自動 QoS マクロを実行する必要があります。グローバル自動 QoS マクロと、次にインターフェイスごとに必要なキーワードを指定してインターフェイス固有自動 QoS マクロを実行するには、次の手順を実行します。

ステップ 1　**set qos autoqos** コマンドを実行して QoS をイネーブルにし、すべての発信 QoS 設定を設定します。

ステップ 2　各ポートについて、ポートベースの自動 QoS コマンドを実行します（表 50-11 を参照）。

表 50-11　自動 QoS キーワードの使用方法

キーワード	ポート タイプ
ciscoipphone	Cisco IP Phone 79xx だけに接続するポート
ciscoipphone	Cisco IP Phone 79xx を、79xx に接続した PC に接続するポート
ciscoipphone	Cisco IP Phone 79xx を、Cisco SoftPhone を稼働する 79xx に接続した PC に接続するポート[1]
ciscosoftphone	Cisco IP Phone 79xx なしで Cisco SoftPhone を稼働する PC を接続するポート
trust	すべての自動 QoS トラフィック タイプが存在するネットワークのその他の場所に接続するポート[2]

1. Cisco SoftPhone が稼働している PC に Cisco IP Phone 79xx を接続するポートの場合、Cisco CallManager との CTI 通信を通過する制御トラフィックにはタグが付けられますが、DSCP 0 に再マーキングされます。
2. その他のネットワークまたは Cisco CallManager に接続するポートの場合、**trust** キーワードを使用することを推奨します。現在、Cisco CallManager とゲートウェイは、Skinny、H.323、および MGCP シグナリング トラフィックを正しくマーキングします。ただし、Cisco CallManager の一部のバージョンでは、H.323 および MGCP トラフィックを明示的にマーキングしません。このような場合には QoS ACL を使用することを推奨します。

CHAPTER 51

ASLB の設定

この章では、Catalyst 6500 シリーズ スイッチ上で Accelerated Server Load Balancing（ASLB）を設定する方法について説明します。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

(注) この章で説明する情報および手順は、Policy Feature Card（PFC; ポリシー フィーチャ カード）を搭載した Supervisor Engine 1 にのみ当てはまります。ASLB は、PFC2 搭載の Supervisor Engine 2、PFC3A/PFC3B/PFC3BXL 搭載の Supervisor Engine 720、または PFC3B/PFC3BXL 搭載の Supervisor Engine 32 ではサポートされていません。

この章で説明する内容は、次のとおりです。

ハードウェアおよびソフトウェアの要件

ASLB 設定のハードウェアおよびソフトウェアの要件は、次のとおりです。

- LocalDirector の要件は、次のとおりです。
  - ハードウェア プラットフォーム ― LocalDirector モデル 410、415、416、420、または 430
  - インターフェイス モジュール ― ASLB を設定するには、10/100BASE-X イーサネット インターフェイスが 2 つ、または 1000BASE-X ギガビット イーサネット インターフェイスが 2 つ必要です。

    （注） 1000BASE-X インターフェイスは、LocalDirector 420 および 430 上でのみサポートされています（LocalDirector 410、415、または 416 ではサポートされていません）。

  - ソフトウェア ― シスコ コンフィギュレーション バージョン 3.2.x
- Catalyst 6500 シリーズ スイッチの要件は、次のとおりです。
  - PFC を搭載した Supervisor Engine 1（または 1A）
  - Release 5.3(1)CSX 以降のスーパバイザ エンジン ソフトウェア リリース
- 構成ルータは、次のとおりです。
  - Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）― Release 5.4(1)CSX 以降のスーパバイザ エンジン ソフトウェア リリースでは、ASLB を構成するルータとして Catalyst 6500 シリーズ スイッチ内の MSFC を使用できます。これより古いスーパバイザ エンジン ソフトウェア リリースでは、内部 MSFC は構成ルータとして*使用できません*。
  - 外部 MSFC ― Catalyst 6500 シリーズ スイッチの外付け MSFC は、構成ルータとして使用できます。
  - Multilayer Switch Module（MSM）― ASLB に使用する Catalyst 6500 シリーズ スイッチに MSM が搭載されている場合、その MSM は ASLB の構成ルータとして使用できます。Catalyst 6500 シリーズ スイッチの外付け MSM も、構成ルータとして使用できます。
  - その他のシスコ製ルータも、ASLB の構成ルータとして使用できます。

ASLB の機能

(注)　TCP/IP トラフィックのロードバランシングの概要については、『*Cisco LocalDirector Installation and Configuration Guide*』Version 3.2 を参照してください。

ここでは、ASLB について説明します。

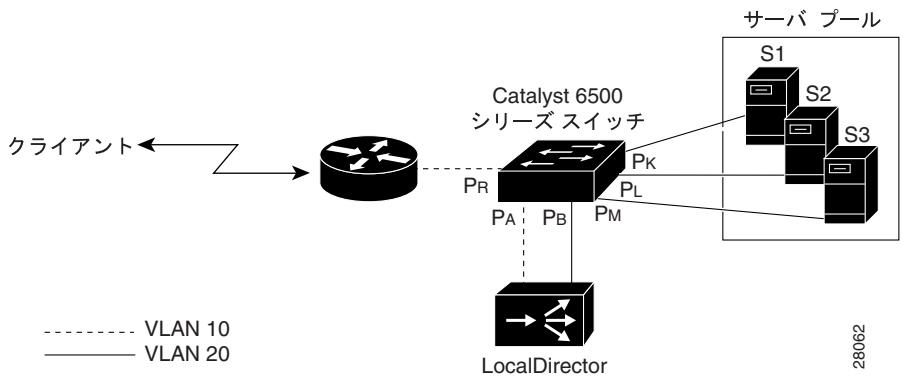
LocalDirector は、機密性に優れたリアルタイムの内蔵 OS（オペレーティング システム）で、複数のサーバ間で TCP/IP トラフィック負荷をインテリジェントに分散します。ASLB によって、Catalyst 6500 シリーズ スイッチは Cisco LocalDirector のロードバランシング フローをキャッシュし、LocalDirector のパフォーマンスを高速化できます。

(注)　LocalDirector のパフォーマンス高速化は、Catalyst 6500 シリーズのレイヤ 3 スイッチング テクノロジーによって達成されます。

図 51-1 に、ASLB 機能を使用した場合のネットワークを示します。スイッチと LocalDirector は、2 つのリンクで接続する必要があります。一方のリンクはルータが存在する VLAN に接続し、もう一方はサーバが存在する VLAN に接続します。図 51-1 では、1 つの LocalDirector リンクが VLAN 10（ルータ VLAN）、もう 1 つのリンクは VLAN 20（サーバ VLAN）に接続されています。

LocalDirector は、directed モードおよび dispatched モードをサポートしています。Catalyst 6500 シリーズ スイッチの ASLB 機能でサポートされているのは、dispatched モードだけです。

図 51-1　ASLB の機能



ASLB のレイヤ 3 動作

サーバの仮想 IP アドレスと TCP ポートのペアを 1024 個まで指定して、スイッチによるトラフィック高速化を行うことができます。SYN、FIN、RST、およびゼロ以外のオフセットを持つフラグメント パケットを除いて、指定した仮想 IP/ ポート間のすべてのトラフィックが高速化されます。このパケットは、（バックアップ LocalDirector が設定されている場合）アクティブ LocalDirector およびスタンバイ LocalDirector の両方にリダイレクトされます。

ASLB のレイヤ 2 動作

Catalyst 6500 シリーズ スイッチの CAM（連想メモリ）テーブルには、ルータ VLAN およびサーバ VLAN のエントリが含まれています。CAM テーブルでは、ルータ VLAN にはポート インデックスに対応付けられた LocalDirector の MAC アドレスのエントリが入っており、サーバ VLAN にはポート インデックスに対応付けられたルータの MAC アドレスのエントリが入っています。このようなポート インデックスでは、ポートは 0/0 として表示されています。**show cam system** コマンドを入力すれば、システムの CAM エントリを表示できます。

表 51-1 に、CAM テーブルのエントリを示します（ASLB 設定は、図 51-1 に示されています）。最初のエントリは、VLAN 10 における LocalDirector の MAC アドレスを表しています。CAM テーブルでは、この MAC アドレスの Xtag 値が 14 であることが示されています。この値は、レイヤ 3 検索が必要であることを示します。2 番めのエントリは、ルータの MAC アドレスであり、これもレイヤ 3 検索が必要です。

表 51-1　レイヤ 2 テーブル エントリ

VLAN	MAC アドレス	インデックス	Xtag[1]
10	LocalDirector MAC	0/0	14
20	ルータ MAC[2]	0/0	14

1. Xtag = レイヤ 2 テーブルで、MAC アドレスが属するルータを表す identifier フィールド
2. ルータの MAC アドレスは、ルータ VLAN（VLAN 10）ではなくサーバ VLAN（VLAN 20）に追加される点に注意してください。

クライアントからサーバへのデータ転送

図 51-2 に、ルータからサーバへのデータ転送を示します。表 51-2 で一連のイベントについて説明し、表 51-3 にレイヤ 3 テーブル エントリを示します。

ここでは、クライアントからサーバへのデータ転送パスについて説明します。

- パス 1（p.51-5）
- パス 2（p.51-5）
- パス 3 — N（p.51-5）
- パス N + 1、N + 2...（p.51-5）

パス 1

ルータからの最初のパケットは、LocalDirector の宛先 MAC アドレスが指定され、VLAN 10 に存在します。この MAC アドレスは、レイヤ 2 テーブルで Xtag 値が 14 になっています。この値はレイヤ 3 検索が必要であることを表し、SYN フラグが設定されているため、フレームはポート P_A に転送されます。

スイッチ ハードウェアはフレームをポート P_A に転送するほか、レイヤ 3 転送テーブルに「候補」エントリを作成します。このエントリはあとの段階で「イネーブラ」フレームによって更新され、完全な ASLB Multilayer Switching（MLS; マルチレイヤ スイッチング）エントリになります。

パス 2

LocalDirector はポート P_A からフレームを受信したあと、標準的なロードバランシング決定を行い、フレームをポート P_B に転送します。LocalDirector は宛先 MAC アドレスを適切なサーバのアドレスに変更します。このフレームはスイッチに入った時点で、「イネーブラ」フレームとみなされます。スイッチ ハードウェアはレイヤ 3 テーブルで検索を行い、前の候補パケット（LocalDirector を通じて転送されたパケット）によって作成されたエントリを検索します。この検索が成功すると、レイヤ 3 テーブルで「ヒット」が成立します。

パス 3 ― N

ASLB MLS エントリが作成済みになっています。パケットに SYN、FIN、RST フラグが設定されている場合、またはパケットがフラグメント化されている場合を除き、ルータからの後続のフレーム（LocalDirector MAC の宛先 MAC アドレスを指定）がレイヤ 3 スイッチングされます。

パス N + 1、N + 2...

接続の最後のフレームで、TCP ヘッダーに FIN または RST フラグのどちらかが設定され、それによってパケットが LocalDirector に転送されます。LocalDirector は、宛先 MAC アドレスを適切なサーバのアドレスに変更したあと、フレームをスイッチに戻さなければなりません。このリダイレクトされたフレームは、フローの最初のフレームと同じパスをたどります。LocalDirector はサーバとの接続終了を示すのに FIN パケットを使用し、ASLB は該当する ASLB MLS エントリを削除します。

図 51-2　ASLB パケット フロー：クライアントからサーバへ

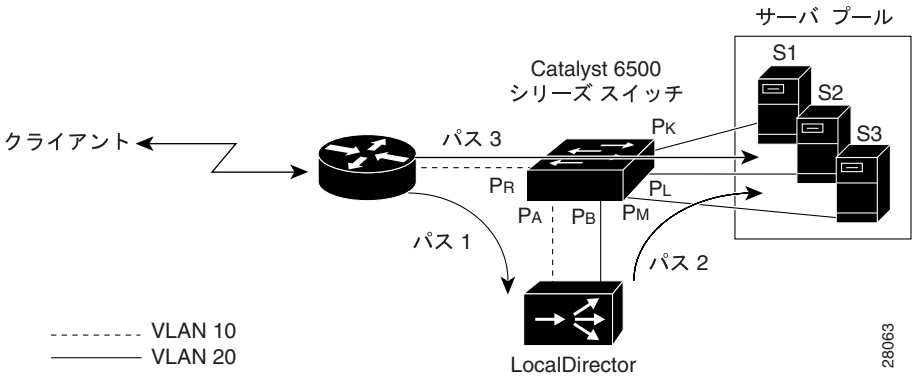


表 51-2　ASLB パケット フロー：クライアントからサーバへ

パス番号	VLAN	MAC 宛先アドレス	MAC 送信元アドレス	IP 宛先アドレス	IP 送信元アドレス	フラグ	アクション
1	10	LocalDirector MAC[1]	ルータ MAC	VIP[2]	CIP[3]	SYN	レイヤ 3 テーブル内の候補エントリ
2	20	サーバ MAC[4]	ルータ MAC[1]	VIP	CIP	–	イネーブラ フレーム
3 ― N	10	LocalDirector MAC[1]	ルータ MAC	VIP	CIP	–	完全な ASLB MLS エントリの作成
N + 1	10	LocalDirector MAC[1]	ルータ MAC	VIP	CIP	FIN/RST	パス 1 リダイレクト
N + 2...	20	サーバ MAC	ルータ MAC[1]	VIP	CIP	FIN/RST	パス 2

1. この MAC アドレスでは、このパケットの VLAN に対応するレイヤ 2 テーブル内の Xtag 値が 14 です。
2. VIP = Virtual IP Address（仮想 IP アドレス）
3. CIP = Client's IP address（クライアントの IP アドレス）
4. LocalDirector が選択したサーバの MAC アドレス

表 51-3　ASLB レイヤ 3 テーブル エントリ：クライアントからサーバへ

IP 宛先アドレス	IP 送信元アドレス	プロトコル	ポート	VLAN	MAC 宛先アドレス	MAC 送信元アドレス
VIP[1]	CIP[2]	TCP	80/YZ	20	サーバ MAC[3]	ルータ MAC

1. VIP = Virtual IP Address（仮想 IP アドレス）
2. CIP = Client's IP address（クライアントの IP アドレス）
3. LocalDirector が選択したサーバの MAC アドレス

サーバからクライアントへのデータ転送

図 51-3 に、サーバからクライアントへのデータ転送を示します。表 51-4 で一連のイベントについて説明し、表 51-5 にレイヤ 3 テーブル エントリを示します。

サーバからルータまたはクライアント装置へのトラフィックは同様に動作しますが、方向は逆となります（「クライアントからサーバへのデータ転送」[p.51-4] の説明を参照）。ただし、LocalDirector は、ルータに向かうすべてのパケットに対して固有の MAC アドレスをパケットの送信元として表します。クライアントからサーバへのトラフィックでは、パケットの送信元 MAC アドレスは書き換えられません。

図 51-3　ASLB パケット フロー：サーバからクライアントへ

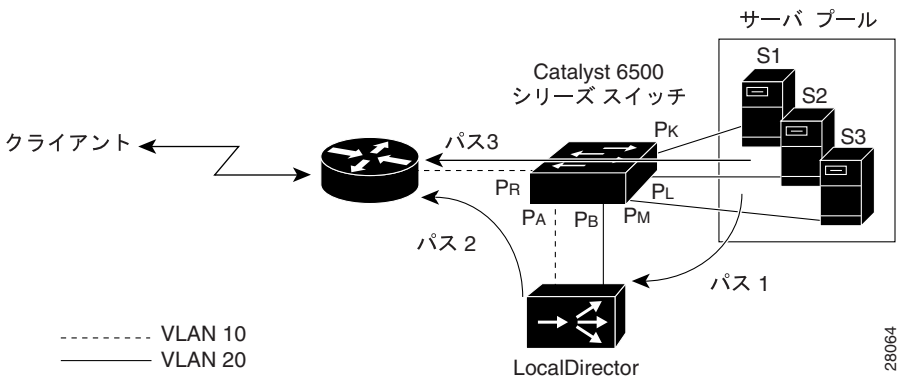


表 51-4　ASLB パケット フロー：サーバからクライアントへ

パス番号	VLAN	MAC 宛先アドレス	MAC 送信元アドレス	IP 宛先アドレス	IP 送信元アドレス	フラグ	アクション
1	20	ルータ MAC[1]	サーバ MAC[2]	CIP[3]	VIP[4]	SYN	レイヤ 3 テーブル内の候補エントリ
2	10	ルータ MAC	LocalDirector MAC[1]	CIP	VIP	–	イネーブラ パケット
3 ― N	20	ルータ MAC[1]	サーバ MAC	CIP	VIP	–	完全な ASLB MLS エントリの作成
N + 1	20	ルータ MAC[1]	サーバ MAC	CIP	VIP	FIN/RST	パス 1 リダイレクト
N +2...	10	ルータ MAC	LocalDirector MAC[1]	CIP	VIP	FIN/RST	パス 2

1. この MAC アドレスでは、このパケットの VLAN に対応するレイヤ 2 テーブル内の Xtag 値が 14 です。
2. LocalDirector が選択したサーバの MAC アドレス
3. CIP = Client’s IP address（クライアントの IP アドレス）
4. VIP = Virtual IP Address（仮想 IP アドレス）

表 51-5　ASLB レイヤ 3 テーブル エントリ：サーバからクライアントへ

IP 宛先アドレス	IP 送信元アドレス	プロトコル	ポート	VLAN	MAC 宛先アドレス	MAC 送信元アドレス
VIP[1]	CIP[2]	TCP	80/YZ	20	サーバ MAC[3]	ルータ MAC
CIP	VIP	TCP	YZ/80	10	ルータ MAC	LocalDirector MAC

1. VIP = Virtual IP Address（仮想 IP アドレス）
2. CIP = Client’s IP address（クライアントの IP アドレス）
3. LocalDirector が選択したサーバの MAC アドレス

ケーブル接続の注意事項

ここでは、ASLB 設定のケーブル接続を行う際の注意事項について説明します。

- スイッチへのサーバ接続を確認してください。各サーバはスイッチに直接接続されているか、またはサーバ VLAN の LocalDirector ポートと同じブリッジング ドメイン内に存在している必要があります。
- カテゴリ 5 Unshielded Twisted-Pair（UTP; シールドなしツイストペア）ケーブル 2 本を使用して、2 つの 10/100 スイッチ ポート、または 2 つの 1000BASE-X スイッチ ポートを、対応する 2 つの LocalDirector インターフェイスに接続します。

注意　Catalyst 6500 シリーズ スイッチに LocalDirector を直接接続します。

LocalDirector インターフェイスの設定手順については、「LocalDirector インターフェイスの設定」（p.51-8）を参照してください。スイッチの設定手順については、「CLI による ASLB の設定」（p.51-11）を参照してください。

スイッチ上での ASLB の設定

ここでは、ASLB の設定作業について紹介します。

LocalDirector インターフェイスの設定

LocalDirector インターフェイスを ASLB 用に設定するための詳しい手順については、『*Cisco LocalDirector Installation and Configuration Guide*』Version 3.2 を参照してください。

ASLB 設定時の注意事項

ここでは、ASLB を設定する際の使用上の注意事項と制限事項を示します。

設定例については、「ASLB の設定例」（p.51-19）を参照してください。設定作業中に問題が生じた場合は、「ASLB 設定のトラブルシューティング」（p.51-26）を参照してください。

ルータ

ルータ設定時の注意事項は次のとおりです。

- ルータはロードバランシングの対象になるサーバのデフォルト　ゲートウェイでなければならず、ルータの MAC アドレスを明確にしておく必要があります。
- 同一のルータ VLAN 上に、複数のルータが存在する必要があります。**set lda mac router** コマンドを入力して、すべての構成ルータの MAC アドレスを指定します。
- ASLB を設定すると、LocalDirector が接続されている 2 つの VLAN 上の TCP トラフィックをリダイレクトするための VACL が作成されます。これらの VLAN には、セキュリティ Cisco IOS Access Control List（ACL; アクセス制御リスト）または VACL は設定できません。

サーバ

サーバ設定時の注意事項は次のとおりです。

- 各サーバはスイッチに直接接続されているか、またはサーバ VLAN の LocalDirector ポートと同じブリッジング ドメイン内に存在している必要があります。
- サーバのデフォルト ルートを、サーバの実際の IP アドレスと同じサブネットに存在するルータのエイリアス アドレスとして設定します。
- サーバが仮想 IP アドレスに関する Address Resolution Protocol（ARP; アドレス解決プロトコル）要求を無視するように設定します。サーバの OS によっては、エイリアス（セカンダリ）IP アドレスに関する ARP 要求への応答をディセーブルに設定できない場合があります。仮想 IP アドレスに関する ARP 要求に応答するサーバの場合、対応策として、ルータ側でスタティック ARP エントリを使用してください。

注意　クライアント / サーバ間トラフィックを高速化するには、サーバが仮想 IP アドレスに関する ARP 要求を無視するように設定する必要があります。この設定をしなかった場合は、トラフィックの高速化が開始されず、LocalDirector に障害があった場合にネットワークでの完全冗長トポロジーの復旧に時間がかかります。

IP アドレス

IP アドレス設定時の注意事項は次のとおりです。

（注）　仮想 IP アドレスには、サーバの IP ネットワーク アドレス以外の IP アドレスを指定できます。

- LocalDirector が各サーバの実際の IP アドレスを ARP 要求できるように、LocalDirector とサーバが同じサブネット上に存在するようにしてください。
- 各ルータが仮想 IP アドレスと同じサブネット上に存在するようにしてください。ルータが仮想 IP アドレスを ARP 要求できるようにするためです。

次のように、ネットワークに ASLB を設定します（この例では、仮想 IP アドレスは 171.1.1.200 です）。

ルータ	LocalDirector	サーバ[1]
171.1.1.1	171.1.1.2	171.1.1.x

1. 各サーバのデフォルト ルータは 171.1.1.1 です。

ASLB 設定で使用するサーバがプライバシのために RFC 1918 に準拠しなければならない場合には、次の例を参考にしてください（この例では、仮想 IP アドレスは 171.1.1.200 です）。

ルータ	LocalDirector	サーバ[1]
171.1.1.1	171.1.1.2	10.1.1.x（実際の IP アドレス）
エイリアス 10.1.1.1	エイリアス 10.1.1.2	エイリアスを 171.1.1.200 にループバック

1. 各サーバのデフォルト ルータは 10.1.1.1 です。

スーパバイザ エンジン

スーパバイザ エンジン設定時の注意事項は次のとおりです。

- 最大 32 のルータ MAC アドレスがサポートされています。
- 最大 1024 の仮想 IP/TCP ポートのペアがサポートされています。

バックアップ LocalDirector の設定（任意）

バックアップ LocalDirector のポートをスイッチに接続し、**set lda server** および **set lda router** コマンドを入力してサーバおよびルータの設定を指定します。アクティブ LocalDirector およびバックアップ LocalDirector を所定のポートに接続しないと、ASLB 機能は作動しません。

MSFC および MLS

MSFC および MLS 設定時の注意事項は次のとおりです。

- Release 5.4(1)CSX 以降のスーパバイザ エンジン ソフトウェア リリースでは、MSFC は ASLB の構成ルータになることができます。

（注） MSFC がクライアントからのトラフィックをルーティングするとき、トラフィックはレイヤ 3 スイッチングされます。このプロセスによって MLS エントリが作成されます。このエントリは同じトラフィックの ASLB MLS エントリとは別個に存在します。

- 終了した ASLB フローを削除するためのエージングにより、MLS の終了したフローも削除されます。ASLB MLS エントリは、MLS ショートカット エントリとレイヤ 3 MLS キャッシュを共用します。

  MLS コマンド（**set mls**、**clear mls**、および **show mls**）は、ASLB（**set lda**、**clear lda**、**show lda**、および **commit lda**）コマンドと相互作用しません。ASLB では、個別のコマンドを使用して LocalDirector MLS エントリを表示します。
- ASLB をイネーブルにすると、full-flow モードのフロー マスク（ip-flow）を 1 つ使用して ASLB MLS エントリが作成されます。

NDE

ASLB をイネーブルにしている場合は、NetFlow Data Export（NDE;NetFlow データ エクスポート）を使用できません。逆に NDE をイネーブルにしている場合は ASLB を使用できません。

VLAN

VLAN 設定時の注意事項は次のとおりです。

- ASLB を設定すると、LocalDirector が接続されている 2 つの VLAN（ルータ VLAN およびサーバ VLAN）上で TCP トラフィックをリダイレクトするための VACL が作成されます。これらの VLAN にセキュリティ Cisco IOS ACL または VACL を設定することはできません。
- ルータ VLAN およびサーバ VLAN は ASLB 専用にしてください。これら 2 つの VLAN には、他のネットワーク装置（エンド ステーション、クライアントなど）を接続しないでください。
- VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）がサーバ モードのとき、ASLB 用に作成した VLAN は VTP によって他のスイッチに伝播されます。ネットワークのすべての VTP スイッチ上で、Spanning-Tree Protocol（STP; スパニングツリー プロトコル）がこれらの ASLB VLAN に作用する結果、ネットワーク全体でオーバーヘッドが増加します。スパニングツリーの伝播遅延を防ぐには、次の方法を使用してください。
  - スイッチを VTP トランスペアレントとして設定し、VLAN を伝播させないようにします。
  - すべてのスイッチ上のすべてのトランクから、ASLB VLAN を削除します（**clear trunk** コマンドを使用します）。

スイッチ ポートの設定

スイッチ ポート設定時の注意事項は次のとおりです。

- LocalDirector（バックアップが設定されている場合は、アクティブ LocalDirector およびスタンバイ LocalDirector の両方）に接続するポート上で、Cisco Discovery Protocol（CDP）をディセーブルにします。
- EtherChannel の一部分であるポートを指定すると、EtherChannel に含まれるすべてのポート間でトラフィックが自動的にリダイレクトされます。

CLI による ASLB の設定

ここでは、Catalyst 6500 シリーズ スイッチの **lda** コマンド セットを使用して ASLB を設定する方法について説明します。

LocalDirector に接続されたスイッチ ポートの設定

LocalDirector に接続された 10/100 イーサネット スイッチ ポートを設定するには、次の作業を行います。

ステップ 1　**set vlan** *vlan_num mod_ports* コマンドを入力して、スイッチ ポートを適正な VLAN（ルータ VLAN およびサーバ VLAN）に追加します。

ステップ 2　すべての 10/100 スイッチ ポートはデフォルトで自動ネゴシエーションを行うように設定されているので、スイッチ ポートの速度およびデュプレックス タイプの設定は不要です。自動ネゴシエーションに問題がある場合には、ポート速度およびデュプレックス タイプを次の方法で設定してください。

set port speed *mod/port* {**10** | **100** | **auto**} コマンドを入力して、ポート速度を設定します。

set port duplex *mod/port* {**full** | **half** | **auto**} コマンドを入力して、デュプレックス タイプを設定します。

ASLB のイネーブル化およびディセーブル化

（注）　ASLB は、デフォルトでディセーブルに設定されています。ASLB がディセーブルになっている状態では、**set lda** コマンドを入力して設定作業を行うことはできません。**set lda** コマンドを入力するには、ASLB をイネーブルにする必要があります。

ASLB をイネーブルまたはディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
ASLB をイネーブルまたはディセーブルにします。	**set lda enable** | **disable**

次に、スイッチ上で ASLB をイネーブルにする例を示します。

```
Console> (enable) set lda enable
Successfully enabled Local Director Accelerator.
Console> (enable)
```

次に、スイッチ上で ASLB をディセーブルにする例を示します。

```
Console> (enable) set lda disable
Successfully disabled Local Director Accelerator.
Console> (enable)
```

高速化するサーバ仮想 IP アドレスおよび TCP ポートの指定

（注）　Catalyst 6500 シリーズ スイッチによる高速化の対象として、仮想 IP アドレスと TCP ポートのペアを 1024 個まで指定できます。新しいペアを指定しても、以前に指定したペアは置き換えられません。以前に入力したペアをキャンセルするには、**clear lda vip** コマンドを使用します。

(注)　*destination_tcp_port* には、ワイルドカードの数値としてゼロ（0）を使用できます。

高速化するサーバ仮想 IP アドレスおよび TCP ポートを指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
高速化するサーバ仮想 IP アドレスおよび TCP ポートを指定します。	**set lda vip** {*server_virtual_ip*} {*destination_tcp_port*} [{*server_virtual_ip*} {*destination_tcp_port*}...]

次に、高速化するサーバ仮想 IP アドレスおよび TCP ポートを指定する例を示します。

```
Console> (enable) set lda vip 10.0.0.8 8
Successfully set server virtual ip and port information.
Use commit lda command to save settings to hardware.
Console> (enable)
```

構成ルータの MAC アドレスの指定

(注)　最大 32 個のルータ MAC アドレスを指定できます。

構成ルータの MAC アドレスを指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
構成ルータの MAC アドレスを指定します。	**set lda mac router** {*mac-address*}...

次に、構成ルータの MAC アドレスを指定する例を示します。

```
Console> (enable) set lda mac router 00-23-45-67-ee-7f
Successfully set mac address.
Use commit lda command to save settings to hardware.
Console> (enable)
```

LocalDirector の MAC アドレスの指定

LocalDirector の MAC アドレスを指定するには、イネーブル モードで次の作業を行います。

:

作業	コマンド
LocalDirector の MAC アドレスを指定します。	**set lda mac ld** {*ld_mac-address*}

次に、LocalDirector の MAC アドレスを指定する例を示します。

```
Console> (enable) set lda mac ld 00-11-22-33-55-66
Successfully set mac address.
Use commit lda command to save settings to hardware.
Console> (enable)
```

ルータ VLAN および VLAN 上の LocalDirector ポートの指定

(注) **set lda router** コマンドを入力したあとで、LocalDirector の接続先スイッチ ポートを変更した場合には、もう一度 **set lda router** コマンドを入力して新しい設定を指定する必要があります。

(注) LocalDirector のフェールオーバー コンフィギュレーションを設定する場合を除き、バックアップ LocalDirector ポートの指定は省略可能です。フェールオーバー コンフィギュレーションを設定する場合は、バックアップ LocalDirector のポートを指定する必要があります。この作業を行わないと、スーパバイザ エンジンはバックアップ LocalDirector にトラフィックを送信しないため、フェールオーバーは機能しません。

ルータ VLAN、およびその VLAN 上の LocalDirector ポートを指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
ルータ VLAN およびその VLAN 上の LocalDirector ポートを指定します。	**set lda router** {*router_vlan*} {*ld_mod/port*} [*backup_ld_mod/port*]

次に、ルータ VLAN およびその VLAN 上の LocalDirector ポートを指定する例を示します。

```
Console> (enable) set lda router 110 4/26
Successfully set router vlan and LD port.
Use commit lda command to save settings to hardware.
Console> (enable)
```

サーバ VLAN および VLAN 上の LocalDirector ポートの指定

(注) **set lda server** コマンドを入力したあとで、LocalDirector の接続先スイッチ ポートを変更した場合には、もう一度 **set lda server** コマンドを入力して新しい設定を指定する必要があります。

(注) LocalDirector のフェールオーバー コンフィギュレーションを設定する場合を除き、バックアップ LocalDirector ポートの指定は省略可能です。フェールオーバー コンフィギュレーションを設定する場合は、バックアップ LocalDirector のポートを指定する必要があります。この作業を行わないと、スーパバイザ エンジンはバックアップ LocalDirector にトラフィックを送信しないため、フェールオーバーは機能しません。

サーバ VLAN、およびその VLAN 上の LocalDirector ポートを指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
サーバ VLAN およびその VLAN 上の LocalDirector ポートを指定します。	**set lda server** {*server_vlan*} {*ld_mod/port*} [*backup_ld_mod/port*]

次に、サーバ VLAN およびその VLAN 上の LocalDirector ポートを指定する例を示します。

```
Console> (enable) set lda server 105 4/40
Successfully set server vlan and LD port.
Use commit lda command to save settings to hardware.
Console> (enable)
```

UDP エージングの設定

UDP エージングを設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
UDP エージングを設定します。	**set lda udpage** *time_in_ms*

エージングは、1 ～ 2024000 ミリ秒（ms）の範囲で設定できます。UDP エージングをディセーブルにするには、0 を入力します。

次に、UDP エージングを 500 ミリ秒に設定する例を示します。

```
Console> (enable) set lda udpage 500
Successfully set LDA UDP aging time to 500ms.
Console> (enable)
```

ASLB 設定のコミット

（注） ASLB の設定値は、一時的に編集バッファに格納されます。これらの設定値は NVRAM に保存されますが、設定値を有効にするには、**commit lda** コマンドを入力する必要があります。このコマンドによって設定値が確認されます。情報が正しく入力されており、かつ整合性検査にパスすれば、設定値がハードウェアにプログラミングされます。ASLB 設定が正常にコミットされると、NVRAM にマッピングが保存され、システムの起動時に復元されます。

ASLB 設定値をコミットするには、イネーブル モードで次の作業を行います。

作業	コマンド
ASLB 設定値をコミットします。	**commit lda**

次に、ASLB 設定値をコミットする例を示します。

```
Console> (enable) commit lda
Commit operation in progress...
Successfully committed Local Director Accelerator.
Console> (enable)
```

ASLB 設定の表示

（注） **show lda** コマンドにキーワード（**committed** | **uncommitted**）を指定しないで入力すると、コミットされた設定値が表示されます。

コミットされた ASLB 設定値、またはまだコミットされていない ASLB 設定値を表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
コミットされた ASLB 設定値、またはまだコミットされていない ASLB 設定値を表示します。	**show lda** [**committed** | **uncommitted**]

次に、コミットされた ASLB 設定値を表示する例を示します。

```
Console> (enable) show lda committed
Status:Committed

Virtual IP addresses:
Local Director Flow:10.0.0.8/ (TCP port 8)

Router MAC:
00-23-45-67-ee-7f


LD MAC:00-11-22-33-55-66

LD Router Side:
---------------
Router and LD are on VLAN 110
LD is connected to switch port 4/26 on VLAN 110

LD Server Side:
---------------
Server(s) and LD are on VLAN 105
LD is connected to switch port 4/40 on VLAN 105
Console> (enable)
```

設定を変更し、その変更をコミットせずに、もう一度 **show lda** コマンドを入力すると、メッセージが表示され、前回のコミット以降に設定が変更されているが、新しい変更については表示せず、コミット済みの変更だけを表示する旨が示されます。新しい変更を表示するには、**show lda uncommitted** コマンドを入力します。

ASLB MLS エントリの表示

（注） **short** | **long** オプションの使用により、出力を通常のフォーマット（1 行が 80 文字）または幅の広いフォーマットで表示できます。

ASLB MLS エントリを表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
ASLB MLS エントリを表示します。	**show lda mls entry** **show lda mls entry** [**destination** *ip_addr_spec*] [**source** *ip_addr_spec*] [**protocol** *protocol*] [**src-port** *port*] [**dst-port** *port*] [**short** | **long**]

次に、すべての ASLB MLS エントリを short フォーマットで表示する例を示します。

```
Console> (enable) show lda mls entry short
Destination-IP  Source-IP       Prot  DstPrt SrcPrt Destination-Mac   Vlan
--------------- --------------- ----- ------ ------ ----------------- ----
EDst ESrc DPort  SPort  Stat-Pkts  Stat-Bytes  Uptime   Age
---- ---- ------ ------ ---------- ----------- -------- --------
10.0.0.8        172.20.20.10    TCP  8      64     00-33-66-99-22-44 105
ARPA ARPA -      4/25   0          0           00:00:02 00:00:05

10.0.0.8        172.20.20.11    TCP  8      64     00-33-66-99-22-44 105
ARPA ARPA -      4/25   0          0           00:00:05 00:00:08
Console> (enable)
```

次に、特定の送信元 IP アドレスについて、ASLB 情報を short フォーマットで表示する例を示します。

```
Console> (enable) show lda mls entry source 172.20.20.11 short
Destination-IP  Source-IP       Prot  DstPrt SrcPrt Destination-Mac   Vlan
--------------- --------------- ----- ------ ------ ----------------- ----
EDst ESrc DPort  SPort  Stat-Pkts  Stat-Bytes  Uptime   Age
---- ---- ------ ------ ---------- ----------- -------- --------
10.0.0.8        172.20.20.11    TCP  8      64     00-33-66-99-22-44 105
ARPA ARPA -      4/25   0          0           00:00:05 00:00:08
Console> (enable)
```

ASLB MLS 統計情報の表示

ASLB MLS 統計情報を表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
ASLB MLS エントリの統計情報を表示します。	**show lda mls statistics entry** **show lda mls statistics count** **show lda mls statistics entry** [**destination** *ip_addr_spec*] [**source** *ip_addr_spec*] [**protocol** *protocol*] [**src-port** *port*] [**dst-port** *port*]

次に、すべての ASLB MLS エントリについて統計情報を表示する例を示します。

```
Console> (enable) show lda mls statistics entry
                                 Last    Used
Destination IP  Source IP       Prot DstPrt SrcPrt Stat-Pkts  Stat-Bytes
--------------- --------------- ---- ------ ------ ---------- ---------------
10.0.0.8        172.20.20.10    TCP  WWW    64     636        29256
10.0.0.8        172.20.22.10    TCP  WWW    64     0          0
Console> (enable)
```

次に、ASLB のアクティブ MLS エントリ数を表示する例を示します。

```
Console> (enable) show lda mls statistics count
LDA active shortcuts: 20
Console> (enable)
```

次に、特定の宛先 IP アドレスについて統計情報を表示する例を示します。

```
Console> (enable) show lda mls statistics entry destination 172.20.22.14
               Last Used          Last    Used
Destination IP  Source IP       Prot DstPrt SrcPrt Stat-Pkts  Stat-Bytes
--------------- --------------- ---- ------ ------ ---------- ---------------
172.20.22.14    172.20.25.10    6    50648  80     3152       347854
Console> (enable)
```

ASLB 設定の消去

注意　**clear lda** コマンドにキーワードを指定しないで入力すると、ハードウェアと NVRAM から ASLB 設定*全体*（MLS エントリを含む）が削除されます。**clear lda mls** コマンドにキーワードを指定しないで入力すると、すべての MLS エントリが消去されます。

ASLB エントリまたはルータの MAC アドレスを消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
ASLB 設定値を消去します。	**clear lda mls** **clear lda mls** [**destination** *ip_addr_spec*] [**source** *ip_addr_spec*] [**protocol** *protocol* **src-port** *src_port* **dst-port** *dst_port*] **clear lda vip** {**all** | *vip* | *vip tcp_port*} **clear lda mac** {**all** | *router_mac_address*}

次に、特定の宛先アドレスについて MLS エントリを消去する例を示します。

```
Console> (enable) clear lda mls destination 172.20.26.22
MLS IP entry cleared.
Console> (enable)
```

次に、仮想 IP アドレスおよびポートのペア（10.0.0.8、ポート 8）を削除する例を示します。

```
Console> (enable) clear lda vip 10.0.0.8 8
Successfully deleted vip/port pairs.
Console> (enable)
```

次に、すべての ASLB ルータ MAC アドレスを消去する例を示します。

```
Console> (enable) clear lda mac all
Successfully cleared Router MAC address.
Console> (enable)
```

次に、特定の ASLB ルータ MAC アドレスを消去する例を示します。

```
Console> (enable) clear lda mac 1-2-3-4-5-6
Successfully cleared Router MAC address.
Console> (enable)
```

ASLB の設定例

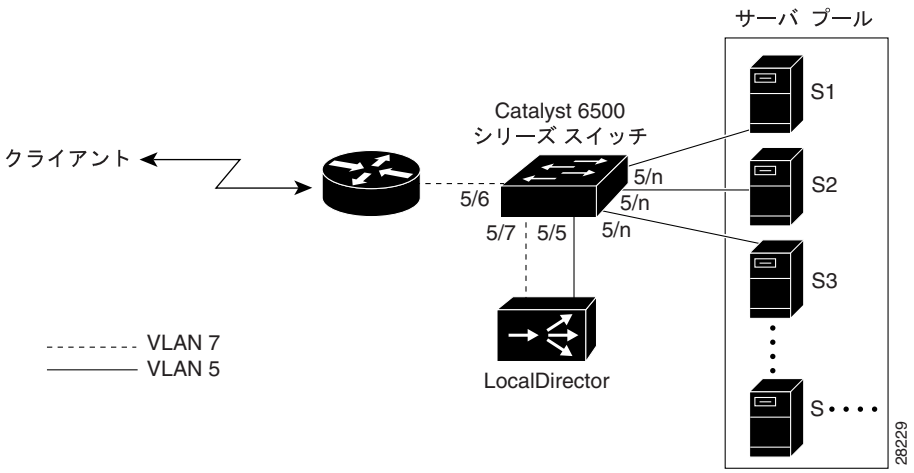
ここでは、一般的な ASLB ネットワークの設定例を示します。図 51-4 はネットワーク例です。設定の仕様は次のとおりです。

- 仮想 IP アドレスは 192.255.201.55 です。
- ルータ インターフェイスの MAC アドレスは 00-d0-bc-e9-fb-47、IP アドレスは 192.255.201.1 です。
- LocalDirector の IP アドレスは 192.255.201.2 です。
- LocalDirector の MAC アドレスは 00-e0-b6-00-4b-04 です。
- サーバ ファームの IP アドレスは、192.255.201.3 ～ 192.255.201.11 です。
- 一連のサーバは、仮想 IP アドレス 192.255.201.55 に関する ARP 要求を無視するように設定されています。

図 51-4 の例では、次の処理が行われています。

- サーバ 192.255.201.3 ～ 192.255.201.10 で、ラウンドロビン シーケンスにより HTTP 接続の負荷を分散
- ポート 8001 への接続をサーバ 192.255.201.11 に転送
- サーバ 192.255.201.3 ～ 192.255.201.8 で、LocalDirector のデフォルトである [leastconns] シーケンスにより、FTP 接続の負荷を分散

図 51-4　ASLB の設定例



ルータの設定は、次のとおりです（この例では MSM を使用しています）。

```
!
interface Port-channel1.7
encapsulation isl 7
ip address 192.255.201.1 255.255.255.0
no ip redirects
no ip directed-broadcast
!
```

Catalyst 6500 シリーズ スイッチの設定は、次のとおりです。

```
Console (enable) show lda
Status:Committed

Virtual IP addresses:
Local Director Flow:192.255.201.55/www (TCP port 80)
Local Director Flow:192.255.201.55/ (TCP port 8001)
Local Director Flow:192.255.201.55/ftp (TCP port 21)

Router MAC:
00-d0-bc-e9-fb-47

LD MAC:  00-e0-b6-00-4b-04

LD Router Side:
---------------
Router and LD are on VLAN 7
LD is connected to switch port 5/7 on VLAN 7

LD Server Side:
---------------
Server(s) and LD are on VLAN 5
LD is connected to switch port 5/5 on VLAN 5
Console (enable)
```

LocalDirector の設定は、次のとおりです。

```
LD430# show configuration
:Saved
:LocalDirector 430 Version 3.1.3.105
syslog output 20.3
no syslog console
hostname LD430
no shutdown ethernet 0
no shutdown ethernet 1
shutdown ethernet 2
shutdown ethernet 3
interface ethernet 0 100full
interface ethernet 1 100full
interface ethernet 2 auto
interface ethernet 3 auto
mtu 0 1500
mtu 1 1500
mtu 2 1500
mtu 3 1500
no multiring all
no secure  0
no secure  1
no secure  2
no secure  3
ping-allow 0
ping-allow 1
no ping-allow 2
no ping-allow 3

ip address 192.255.201.2 255.255.255.0
route 0.0.0.0 0.0.0.0 192.255.201.1 1
no rip passive
rip version 1
failover ip address 0.0.0.0
no failover
snmp-server enable traps
no snmp-server contact
no snmp-server location
virtual 192.255.201.55:80:0:tcp is
virtual 192.255.201.55:8001:0:tcp is
virtual 192.255.201.55:21:0:tcp is
```

```
predictor 192.255.201.55:80:0:tcp roundrobin
redirection 192.255.201.55:80:0:tcp dispatched assisted wildcard-ttl 60
fixed-ttl 60 igmp 224.0.1.2 port 1637
redirection 192.255.201.55:8001:0:tcp dispatched assisted wildcard-ttl 60
fixed-ttl 60 igmp 224.0.1.2 port 1637
redirection 192.255.201.55:21:0:tcp dispatched assisted wildcard-ttl 60
fixed-ttl 60 igmp 224.0.1.2 port 1637
real 192.255.201.5:80:0:tcp is
real 192.255.201.3:80:0:tcp is
real 192.255.201.4:80:0:tcp is
real 192.255.201.6:80:0:tcp is
real 192.255.201.7:80:0:tcp is
real 192.255.201.8:80:0:tcp is
real 192.255.201.9:80:0:tcp oos
real 192.255.201.10:80:0:tcp oos
real 192.255.201.11:8001:0:tcp oos
real 192.255.201.3:21:0:tcp is
real 192.255.201.4:21:0:tcp is
real 192.255.201.5:21:0:tcp is
real 192.255.201.6:21:0:tcp is
real 192.255.201.7:21:0:tcp is
real 192.255.201.8:21:0:tcp is
bind 192.255.201.55:80:0:tcp 192.255.201.3:80:0:tcp
bind 192.255.201.55:80:0:tcp 192.255.201.4:80:0:tcp
bind 192.255.201.55:80:0:tcp 192.255.201.5:80:0:tcp
bind 192.255.201.55:80:0:tcp 192.255.201.6:80:0:tcp
bind 192.255.201.55:80:0:tcp 192.255.201.7:80:0:tcp
bind 192.255.201.55:80:0:tcp 192.255.201.8:80:0:tcp
bind 192.255.201.55:80:0:tcp 192.255.201.9:80:0:tcp
bind 192.255.201.55:80:0:tcp 192.255.201.10:80:0:tcp
bind 192.255.201.55:8001:0:tcp 192.255.201.11:8001:0:tcp
bind 192.255.201.55:21:0:tcp 192.255.201.3:21:0:tcp
bind 192.255.201.55:21:0:tcp 192.255.201.4:21:0:tcp
bind 192.255.201.55:21:0:tcp 192.255.201.5:21:0:tcp
bind 192.255.201.55:21:0:tcp 192.255.201.6:21:0:tcp
bind 192.255.201.55:21:0:tcp 192.255.201.7:21:0:tcp
bind 192.255.201.55:21:0:tcp 192.255.201.8:21:0:tcp
```

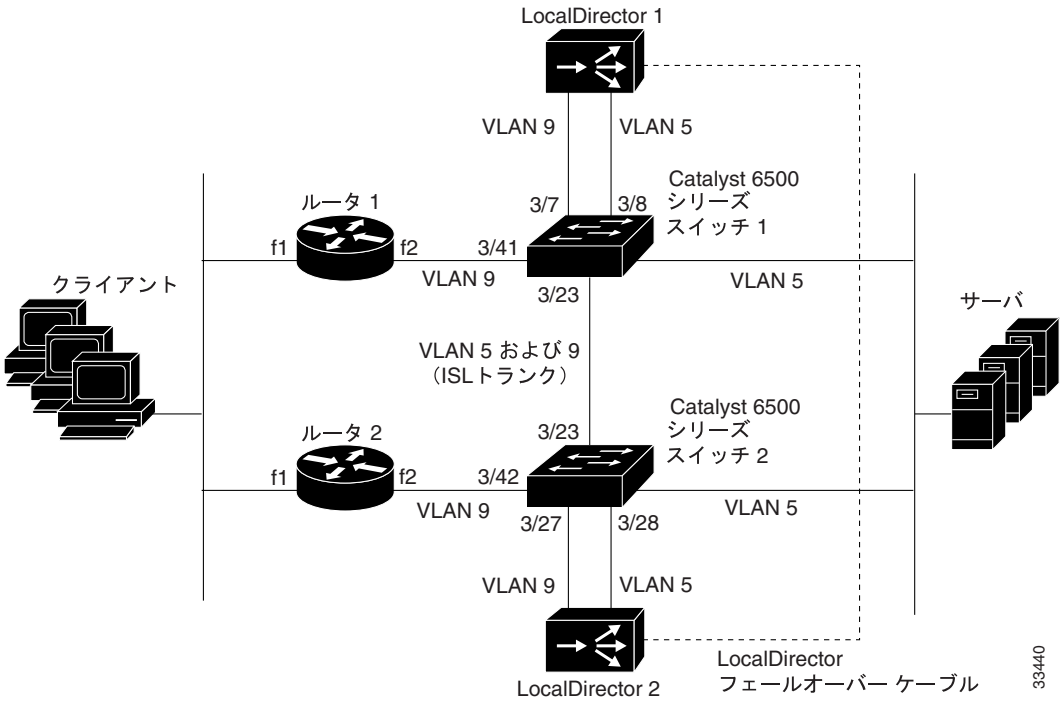
ASLB 冗長構成の例

ここでは、一般的な冗長 ASLB ネットワーク構成例を示します。図 51-5 は冗長ネットワーク例です。サーバ VIP アドレス 13.13.13.13 に対する HTTP および Telnet を高速化するように、LocalDirectors および Catalyst 6500 シリーズ スイッチを設定します。

注意

図 51-5 では、ルータ 1 およびルータ 2 のインターフェイス（f1 および f2）上で Hot Standby Router Protocol（HSRP）が稼働しています。インターフェイス f2 がアクティブになっているルータ上で f1 がアクティブになっている必要があります。アクティブになっていない場合、一方のルータ上のインターフェイス f1 にトラフィックが到達しても、もう一方のルータ上でアクティブになっているインターフェイス f2 に転送されません。HSRP の **track** コマンドを使用して、各ルータの反対側のインターフェイスの状況を追跡します。

図 51-5　ASLB 冗長構成の例



IP アドレス

IP アドレスは、次のとおりです。

- ルータ 1、f1 IP アドレス：7.0.0.100（ネットワーク 7）
- ルータ 2、f1 IP アドレス：7.0.0.101（ネットワーク 7）
- HSRP IP アドレス：ネットワーク 7 で 7.0.0.1
- ルータ 1、f2 IP アドレス：5.0.0.100（ネットワーク 5）
- ルータ 2、f2 IP アドレス：5.0.0.101（ネットワーク 5）
- HSRP IP アドレス：ネットワーク 5 で 5.0.0.2
- LocalDirector IP アドレス：5.0.0.1
- サーバ IP アドレス：5.100.100.100
- サーバの VIP アドレス：13.13.13.13

MAC アドレス

MAC アドレスは、次のとおりです。

- ネットワーク 7 の HSRP MAC アドレス：00-00-0c-07-ac-00
- ネットワーク 5 の HSRP MAC アドレス：00-00-0c-07-ac-01
- ルータ 1、f2 MAC アドレス：00-d0-79-7b-20-88
- ルータ 2、f2 MAC アドレス：00-d0-79-7b-18-88
- LocalDirector MAC アドレス：00-e0-b6-00-47-ec

Catalyst 6500 シリーズ スイッチ 1 の設定

スイッチ 1 の設定は、次のとおりです。

```
set trunk 3/23 on isl 1,5,9
set lda enable
clear lda vip all
set lda vip 13.13.13.13 80 13.13.13.13 23
clear lda mac all
set lda mac router 00-00-0c-07-ac-01
set lda mac router 00-d0-79-7b-20-88
set lda mac router 00-d0-79-7b-18-88
set lda mac ld 00-e0-b6-00-47-ec
set lda router 9 3/7 3/23
set lda server 5 3/8 3/23
commit lda
```

Catalyst 6500 シリーズ スイッチ 2 の設定

スイッチ 2 の設定は、次のとおりです。

```
set trunk 3/23 on isl 1,5,9
set lda enable
clear lda vip all
set lda vip 13.13.13.13 80 13.13.13.13 23
clear lda mac all
set lda mac router 00-00-0c-07-ac-01
set lda mac router 00-d0-79-7b-20-88
set lda mac router 00-d0-79-7b-18-88
set lda mac ld 00-e0-b6-00-47-ec
set lda router 9 3/27 3/23
set lda server 5 3/28 3/23
commit lda
```

ルータ 1 の設定

ルータ 1 の設定は、次のとおりです。

```
interface FastEthernet1
 ip address 7.0.0.100 255.0.0.0
 no ip redirects
 no ip directed-broadcast
 no ip route-cache distributed
 load-interval 30
 no keepalive
 full-duplex
 standby 1 ip 7.0.0.1
 standby 1 track FastEthernet2
!
interface FastEthernet2
 ip address 5.0.0.100 255.0.0.0
 no ip redirects
 no ip directed-broadcast
 no ip route-cache distributed
 no keepalive
 full-duplex
 standby priority 250
 standby 2 ip 5.0.0.2
 standby 2 track FastEthernet1
!
ip route 13.13.13.13 255.255.255.255 5.0.0.1
```

ルータ 2 の設定

ルータ 2 の設定は、次のとおりです。

```
interface FastEthernet1
 ip address 7.0.0.101 255.0.0.0
 no ip redirects
 no ip directed-broadcast
 no ip route-cache distributed
 load-interval 30
 no keepalive
 full-duplex
 standby 1 ip 7.0.0.1
 standby 1 track FastEthernet2
!
interface FastEthernet2
 ip address 5.0.0.101 255.0.0.0
 no ip redirects
 no ip directed-broadcast
 no ip route-cache distributed
 no keepalive
 full-duplex
 standby priority 250
 standby 2 ip 5.0.0.2
 standby 2 track FastEthernet1
!
ip route 13.13.13.13 255.255.255.255 5.0.0.1
```

LocalDirector の設定

LocalDirector 1 および LocalDirector 2 の設定は、次のとおりです（設定は両方の LocalDirector で共通です）。

```
no shutdown ethernet 0
no shutdown ethernet 4
interface ethernet 0 100full
interface ethernet 4 100full
ip address 5.0.0.1 255.0.0.0
failover ip address 5.0.0.5
virtual 13.13.13.13:80:0:tcp is
virtual 13.13.13.13:23:0:tcp is
predictor 13.13.13.13:80:0:tcp roundrobin
predictor 13.13.13.13:23:0:tcp roundrobin
redirection 13.13.13.13:80:0:tcp dispatched assisted
redirection 13.13.13.13:23:0:tcp dispatched assisted
real 5.100.100.100:80:0:tcp is
real 5.100.100.100:23:0:tcp is
bind 13.13.13.13:80:0:tcp 5.100.100.100:80:0:tcp
bind 13.13.13.13:23:0:tcp 5.100.100.100:23:0:tcp
```

ASLB 設定のトラブルシューティング

表 51-6 に、発生する可能性のある問題と、ASLB 設定のトラブルシューティングのために推奨する対処方法を示します。

表 51-6　ASLB 設定のトラブルシューティング

現象	対処方法
LocalDirector がトラフィックを受信しない。	**set lda server** および **set lda router** コマンドを使用して指定したポートに、LocalDirector が接続していることを確認します。
LocalDirector 接続エントリが削除されない。	**set lda vip** コマンドを使用して、すべての仮想 IP/ ポートのペアを設定していることを確認します。
ASLB MLS エントリが単一方向にしか作成されない。	スーパバイザ エンジン（**set lda vip** コマンド）および LocalDirector の両方で、仮想 IP/ ポートのペアをすべて設定していることを確認します。 LocalDirector が [dispatched assisted] モードになっていることを確認します。 「IP アドレス」（p.51-9）に記載されている注意事項に従って、ルータ、LocalDirector、およびサーバの IP アドレスを設定していることを確認します。トラフィックが仮想 IP アドレスに転送されたときに、LocalDirector に到達する方法をルータが認識していることを確認します（仮想 IP アドレスがルータ インターフェイスとは別のサブネットに存在する場合）。 ルータの MAC アドレスが、**set lda mac router** コマンドで指定したアドレスと同じであることを確認します。 LocalDirector の MAC アドレスが、**set lda mac ld** コマンドで指定したアドレスと同じであることを確認します。
バックアップ LocalDirector がトラフィックを受信しない。	**set lda router** および **set lda server** コマンドを使用してバックアップ LocalDirector ポートを設定していることを確認します。たとえば、**set lda router** {*router_vlan*} **3/7 3/9** および **set lda server** {*server_vlan*} **3/8 3/10** コマンドを入力します。
ルータからサーバへの ping は成功するが、データ トラフィックを送信しても ASLB MLS エントリが作成されない。	サーバが仮想 IP アドレスに関する ARP 要求を無視するように設定されていることを確認します。
次のメッセージが表示される。 %CDP-4-NVLANMISMATCH:Native vlan mismatch detected on port ...	LocalDirector に接続されたポート上で CDP[1] をディセーブルにします（**set cdp disable** コマンドを入力します）。
LocalDirector の **set** コマンドが有効にならない。	**set lda** コマンドは、**commit lda** コマンドを入力しないかぎり有効になりません。 どの **set lda** コマンドが有効になっているかを確認するには、**show lda commit** コマンドを使用します。 どの設定済み **set lda** コマンドがコミットされていないか、または現在の **set lda** コマンドをコミットするとどのような変化が起きるかを判別するには、**show lda uncommitted** コマンドを使用します。
Catalyst 6500 シリーズ スイッチ ポートに［collisions］、または［port disabled］と表示される。	LocalDirector とスイッチ間のリンクの両端で、ポート速度およびデュプレックスの設定が一致していることを確認します。たとえば、スイッチ上のポート 3/7 が LocalDirector の interface ethernet 0 に接続されている場合、ポート 3/7 が 100full に設定され、LocalDirector の interface ethernet 0 も 100full に設定されていることを確認します。

1. CDP = Cisco Discovery Protocol

CHAPTER 52

スイッチ ファブリック モジュールの設定

この章では、Catalyst 6500 シリーズ スイッチ上の Supervisor Engine 720 でサポートされる 720 Gbps 統合スイッチ ファブリック、および Supervisor Engine 2 でサポートされる外部スイッチ ファブリック モジュール（WS-C6500-SFM）とスイッチ ファブリック モジュール 2（WS-X6500-SFM 2）について説明します。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

この章では、次の用語を使用します。

- CEF720 — WS-X67*xx-xxx*（WS-X6724-SFP など）に適合する部品番号を持つモジュール。これらのモジュールは、Supervisor Engine 720 上の 720 Gbps 統合スイッチ ファブリックに接続します。
- CEF256 — WS-X65*xx-xxx*（WS-X6548-GE-TX など）、OSM（オプティカル サービス モジュール）、拡張 FlexWAN モジュール、および大部分のサービス モジュール（Firewall Services Module [FWSM]、Secure Socket Layer Services Module [SSLM]、Virtual Private Network Services Module [VPNSM]、Network Analysis Module 1 [NAM-1]、NAM-2、Intrusion Detection System Module [IDSM-2]、Content Services Gateway [CSG]、および Communications Media Module [CMM] など）に適合する部品番号を持つモジュール。これらのモジュールは、Supervisor Engine 720 上の 720 Gbps 統合スイッチ ファブリックまたは Supervisor Engine 2 によってサポートされている 256 Gbps 外部スイッチング ファブリック モジュール、および 32 Gbps スイッチング バスに接続します。
- ファブリック非対応 — CEF720 または CEF256 カテゴリに分類されないモジュール。これらのモジュールにはファブリック接続がなく、32 Gbps スイッチング バスだけに接続します。

この章で説明する内容は、次のとおりです。

(注) WS-C6500-SFM は、Catalyst 6500 シリーズの 6 スロット シャーシおよび 9 スロット シャーシでのみサポートされています。WS-X6500-SFM 2 は、Catalyst 6500 シリーズの 6 スロット、9 スロット、13 スロットのシャーシ、および Catalyst 6509-NEB シャーシでサポートされています。

720 Gbps 統合スイッチ ファブリックの機能の概要

(注)　720 Gbps 統合スイッチ ファブリックは Supervisor Engine 720 でのみサポートされています。

(注)　Release 8.3(1) 以降のソフトウェア リリースでは、冗長システムにおいて、720 Gbps 統合スイッチ ファブリックがスタンバイ スイッチ ファブリックへのハイ アベイラビリティ フェイルオーバーをサポートします。フェイルオーバーを機能させるためには、ハイ アベイラビリティをイネーブルにする必要があります（**set system highavailability enable** コマンドを入力します）。

720 Gbps 統合スイッチ ファブリックは Supervisor Engine 720 に組み込まれ、CEF256 および CEF720 モジュール間に専用接続を確立し、これらのモジュール間で中断のないフレーム伝送を実現します。720 Gbps 統合スイッチ ファブリックが提供する CEF256 および CEF720 モジュール間の直接接続に加えて、これらのモジュールは 32 Gbps スイッチング バスへ直接接続できます。

外部スイッチ ファブリック モジュールの機能の概要

(注)　外部スイッチ ファブリック モジュールは、Catalyst 6500 シリーズ スイッチに搭載された Supervisor Engine 2 でのみサポートされています。

外部スイッチ ファブリック モジュールは、CEF256 モジュール間に専用接続を確立し、これらのモジュール間で中断のないフレーム伝送を実現します。外部スイッチ ファブリック モジュールは、Supervisor Engine 2 で機能しないため、CEF720 モジュールをサポートしません。さらにスイッチ ファブリック モジュールを使用することによって、CEF256 モジュールは 32 Gbps スイッチング バスに接続できます。

表 52-1　モジュール タイプ別のスイッチ ファブリック接続速度

スイッチ ファブリック タイプ	モジュール タイプ[1]	
	CEF256	CEF720
スイッチ ファブリック モジュール（256 Gbps）	1 × 16 Gbps	サポート対象外
スイッチ ファブリック モジュール 2（256 Gbps）	1 × 16 Gbps	サポート対象外
Supervisor Engine 720 上の統合スイッチ ファブリック（720 Gbps）	1 × 16 Gbps	1 × 40 Gbps： WS-X6724-SFP 2 × 40 Gbps： WS-X6748-GE-TX WS-X6748-SFP WS-X6704-10GE

1. 表示されている速度は双方向です。

set system crossbar-fallback bus-mode | none コマンドを入力して、スイッチ ファブリック モジュールが削除されるか、または接続が切断された場合のパケットの処理方法を指定します。**bus-mode** キーワードを指定すると、スイッチングは flow-through モードで実行されます。**none** キーワードを指定すると、スイッチ ポートはディセーブルになり、スイッチングは停止します。詳細については、「代替オプションの設定」（p.52-5）を参照してください。

外部スイッチ ファブリック モジュールにはコンソールはありません。前面パネルにある 2 列の LCD ディスプレイに、ファブリックの利用状況、ソフトウェア リビジョン、および基本的なシステム情報が表示されます。

(注)　*9 スロット スイッチ*の用語は、WS-C6509-NEB および WS-C6509-NEB-A スイッチを意味します。

WS-C6500-SFM は、6 スロットおよび 9 スロット スイッチの、スロット 5 またはスロット 6 のどちらかに搭載します。WS-X6500-SFM 2 は、13 スロット スイッチのスロット 7 またはスロット 8 のどちらか、または 6 スロットおよび 9 スロット スイッチのスロット 5 またはスロット 6 のどちらかに搭載します。最初に取り付けたスイッチ ファブリック モジュールがプライマリ モジュールとして機能します。スタンバイ スイッチ ファブリック モジュールを取り付けて冗長構成にすることができます。

6 スロットまたは 9 スロット シャーシに 2 つのスイッチ ファブリック モジュールを同時に取り付けるときは、プライマリ モジュールはスロット 5 に、バックアップ モジュールはスロット 6 に装着します。スロット 5 のモジュールをリセットすると、スロット 6 のモジュールがアクティブになります。

13 スロット シャーシに 2 つのスイッチ ファブリック モジュールを同時に取り付けるときは、プライマリ モジュールはスロット 7 に、バックアップ モジュールはスロット 8 に装着します。スロット 7 のモジュールをリセットすると、スロット 8 のモジュールがアクティブになります。

転送モード

CEF256/CEF720 モジュールは、中央集中型の転送を使用する場合、次の 3 つのいずれかのモードで動作します。

- compact mode ― システムに搭載されたすべてのモジュールが CEF256 または CEF720 である場合の動作モード（ファブリック非対応モジュールはこのモードになりません）。このモードでは、CEF256/CEF720 モジュールはスイッチング バス上のスーパバイザ エンジンに各フレームの「コンパクト」32 バイト ヘッダーを送信します。転送の決定が行われると、CEF256/CEF720 モジュールはフレーム全体をスイッチ ファブリックを介して出力モジュールに送信します。
- truncated mode ― システムにファブリック非対応モジュールが最低 1 つ存在する場合の動作モード。このモードでは、CEF256/CEF720 モジュールはスイッチング バス上のスーパバイザ エンジンに各フレームの最初の 64 バイトを送信します。転送の決定が行われると、CEF256/CEF720 モジュールはフレーム全体をスイッチ ファブリックを介して出力モジュールに送信します。
- flow-through モード ― スイッチ ファブリックが存在しない場合の CEF256 モジュールの動作モード。このモードでは、CEF256 モジュールはスイッチング バス上のスーパバイザ エンジンにパケット全体を送信します。このモードは CEF720 モジュールには適用できず、スイッチ ファブリックが必要になります。

表 52-2 は、CEF256、CEF720、およびファブリック非対応モジュールが搭載されている場合に使用されるスイッチ モードを示します。

表 52-2　搭載されているスイッチ ファブリック モジュール別のスイッチング モード

搭載されているモジュール タイプ	スイッチング モード
CEF256 または CEF720 モジュール（ファブリック非対応モジュールが搭載されていない場合）	compact
CEF256 および / または CEF720 モジュール（ファブリック非対応モジュールが搭載されている場合）	truncated
CEF256 およびファブリック非対応モジュール	flow-through
ファブリックがイネーブルでないモジュール	flow-through

スイッチ上での統合スイッチ ファブリックおよびスイッチ ファブリック モジュールの設定とモニタ

720 Gbps 統合スイッチ ファブリックおよびスイッチ ファブリック モジュールは、ユーザ側での設定作業を必要としませんが、モニタを行う目的でいくつかの **show** コマンドをサポートしています。完全に自動化された起動シーケンスによってモジュールがオンラインになり、ポート上で接続診断テストが実行されます。

スーパバイザ エンジンからモジュールをリセットするには **reset** *module* コマンド、モジュールをディセーブルおよびイネーブルにするには **set module enable** | **disable** コマンド、モジュールの電源を切断するには **set module powerdown** *module* コマンドを入力します。

ここでは、720 Gbps 統合スイッチ ファブリックおよびスイッチ ファブリック モジュールを設定する方法を説明します。

代替オプションの設定

set system crossbar-fallback {**bus-mode** | **none**} コマンドを使用すると、スイッチ ファブリック モジュールとの接続が切断された場合の代替オプションを設定することができます。

スイッチが compact モードの場合、crossbar-fallback を **none** に設定すると、スイッチは他のスイッチング モードで稼働することができなくなります。スイッチにファブリック非対応モジュールが搭載されていない場合、スイッチング モードは compact になります。次に、crossbar-fallback を **none** に設定し、ファブリック非対応モジュールを挿入した場合、スイッチが compact モードを維持できなくなってしまうため、モジュールは電源投入されません。また、crossbar-fallback を **none** に設定し、最後のスイッチ ファブリック モジュールを取り外した場合、すべてのモジュールのポートがディセーブルになります。ポートがディセーブルにならない場合、このポートのモジュールの電源は切断されます。スイッチ ファブリック モジュールが搭載されていないと、スイッチは compact モードで稼働できず、crossbar-fallback が **none** に設定されているため、スイッチは実質的にディセーブルになります。

スイッチ ファブリック モジュールの代替オプションを設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
スイッチ ファブリック モジュールの代替オプションを設定します。	**set system crossbar-fallback** {**bus-mode**	**none**}

次に、代替オプションを bus-mode に設定する例を示します。

```
Console> (enable) set system crossbar-fallback bus-mode
System crossbar-fallback set to bus-mode.
Console> (enable)
```

スイッチング モードの設定

パフォーマンスを向上させるために、システムが使用するスイッチング モードを手動で設定することができます。シャーシにファブリック非対応モジュールが 1 つまたは複数搭載されている場合は、flow-through モードを使用するようにスイッチを設定します。CEF256 または CEF720 モジュールのみがシャーシに搭載されている場合は、compact モードを使用するようにスイッチを設定します。

（注） ファブリック非対応モジュールは、compact モードをサポートしていません。

（注） スイッチ ファブリック機能を持つ Supervisor Engine 720 と CEF720 モジュールがシャーシ内に混在している場合、**bus-only** 動作は許可されません。システムは truncated モードのままです。

ファブリック非対応モジュールが搭載されている場合に、flow-through モードを使用するようにスイッチを設定するには、次の作業を行います。

作業	コマンド
flow-through モードを使用するようにスイッチを設定します。	**set system switchmode allow bus-only**

次に、flow-through モードを使用するようにスイッチを設定する例を示します。

```
Console> (enable) set system switchmode allow bus-only

Console> (enable)
```

CEF256 および（または）CEF720、およびファブリック非対応モジュールが搭載されている場合に、truncated モードを使用するようにスイッチを設定するには、次の作業を行います。

作業	コマンド
truncated モードを使用するようにスイッチを設定します。	**set system switchmode allow truncated**

次に、truncated モードを使用するようにスイッチを設定する例を示します。

```
Console> (enable) set system switchmode allow truncated

Console> (enable)
```

冗長性

スイッチ ファブリック モジュールを冗長構成にする場合、設定作業は必要ありません。スロット 5 のモジュールがプライマリ モジュールとして動作し、プライマリ モジュールが故障したとき、スロット 6 の冗長スイッチ ファブリック モジュールが自動的に処理を引き継ぎます。Catalyst 6506 および Catalyst 6509 スイッチは、WS-C6500-SFM および WS-X6500-SFM 2 による混合冗長構成をサポートしています。Catalyst 6513 スイッチは、WS-C6500-SFM2 のみによる冗長構成をサポートしています。

720 Gbps 統合スイッチ ファブリックを冗長構成にする場合、設定作業は必要ありません。アクティブな Supervisor Engine 720 内の統合スイッチ ファブリックがプライマリ スイッチ ファブリックとして機能します。スーパバイザ エンジンのスイッチオーバーが起こると、スイッチ ファブリックもスイッチオーバーします。

統合スイッチ ファブリックおよびスイッチ ファブリック モジュールのモニタ

ここでは、統合スイッチ ファブリックおよびスイッチ ファブリック モジュールをモニタする手順について説明します。

（注）　720 Gbps 統合スイッチ ファブリックおよびスイッチ ファブリック モジュールがサポートする **show** コマンドは、すべてスーパバイザ エンジンから実行します。

モジュール情報の表示

モジュール情報を表示するには、次の作業を行います。

作業	コマンド
モジュール情報を表示します。	**show module** *mod*[1]

1. **show module** コマンドは統合スイッチ ファブリックには使用できません。

次に、モジュール情報を表示する例を示します。

```
Console> show module
Mod Slot Ports Module-Type               Model               Sub Status
--- ---- ----- ------------------------- ------------------- --- --------
1   1    2     1000BaseX Supervisor      WS-X6K-SUP2-2GE     yes ok
4   4    24    100BaseFX MM Ethernet     WS-X6224-MM-MT      no  ok
5   5    0     Switch Fabric Module      WS-C6500-SFM        no  ok

Mod Module-Name         Serial-Num
--- ------------------- -----------
1                       Munish
4                       SAD02390156
5                       SAD042818BR

Mod MAC-Address(es)                         Hw     Fw          Sw
--- --------------------------------------- ------ ----------- ------------------
1   00-40-0b-ff-00-00 to 00-40-0b-ff-00-01 0.219  6.1(0.146) 6.2(0.33-Eng)KEY
    00-50-3e-7e-71-56 to 00-50-3e-7e-71-57
    00-01-64-f8-ca-00 to 00-01-64-f8-cd-ff
4   00-10-7b-c2-3a-c0 to 00-10-7b-c2-3a-d7 0.204  4.2(0.24)V 6.2(0.14)KEY
5   00-40-0b-ff-00-00                       0.204  6.1(0.133) 6.2(0.14)KEY

Mod Sub-Type                Sub-Model           Sub-Serial  Sub-Hw
--- ----------------------- ------------------- ----------- ------
1   L3 Switching Engine II  WS-F6K-PFC2         SAD04110B5S 0.305
Console> (enable)
```

ファブリック チャネル カウンタの表示

ファブリック チャネル カウンタを表示するには、次の作業を行います。

作業	コマンド
ファブリック チャネル カウンタを表示します。	**show fabric channel counters** {*mod* | **all**} [**hex**]

次に、ファブリック チャネル カウンタを表示する例を示します。

```
Console> show fabric channel counters 5
Channel 0 counters:
0  rxTotalPkts                      =                    0
1  txTotalPkts                      =                    0
2  rxGoodPkts                       =                    0
3  rxErrors                         =                    0
4  txErrors                         =                    0
5  txDropped                        =                    0
```

ファブリック チャネルのスイッチング モードおよびチャネル ステータスの表示

ファブリック チャネルのスイッチング モードおよびチャネル ステータスを表示するには、次の作業を行います。

作業	コマンド
ファブリック チャネルのスイッチング モードおよびチャネル ステータスを表示します。	**show fabric channel switchmode** [*mod*]

次に、ファブリック チャネルのスイッチング モードおよびチャネル ステータスを表示する例を示します。

```
Console> show fabric channel switchmode
Global switching mode:truncated

Module Num Fab Chan Fab Chan Switch Mode  Channel Status
------ ------------ -------- ------------ --------------
     1             1   0, 0   flow through ok
     4             0 n/a      n/a          n/a
     5            18   0, 0   n/a          ok
     5            18   1, 1   n/a          unused
     5            18   2, 2   n/a          unused
     5            18   3, 3   n/a          unused
     5            18   4, 4   n/a          unused
     5            18   5, 5   n/a          unused
     5            18   6, 6   n/a          unused
     5            18   7, 7   n/a          unused
     5            18   8, 8   n/a          unused
     5            18   9, 9   n/a          unused
     5            18  10, 10  n/a          unused
     5            18  11, 11  n/a          unused
     5            18  12, 12  n/a          unused
     5            18  13, 13  n/a          unused
     5            18  14, 14  n/a          unused
     5            18  15, 15  n/a          unused
     5            18  16, 16  n/a          unused
     5            18  17, 17  n/a          unused
```

show fabric channel switchmode コマンドの出力で、Switch Mode フィールドに表示されるモードは、次のいずれかです。

- flow-through モード
- truncated モード
- compact モード

（注）　各モードの定義については、「外部スイッチ ファブリック モジュールの機能の概要」（p.52-2）を参照してください。

ファブリック チャネル利用率の表示

ファブリック チャネル利用率を表示するには、次の作業を行います。

作業	コマンド
ファブリック チャネル利用率を表示します。	**show fabric channel utilization**

次に、ファブリック チャネル利用率を表示する例を示します。

```
Console> show fabric channel utilization
Fab Chan Input Output
-------- ----- ------
Fab Chan Speed Input Output
-------- ----- ----- ------
       0   n/a    0%     0%
       1   n/a    0%     0%
       2   n/a    0%     0%
       3   n/a    0%     0%
       4   20G    0%     0%
       5   n/a    0%     0%
       6   n/a    0%     0%
       7   20G    0%     0%
       8    8G    0%     0%
       9   n/a    0%     0%
      10   n/a    0%     0%
      11   n/a    0%     0%
      12   n/a    0%     0%
      13   n/a    0%     0%
      14   n/a    0%     0%
      15   n/a    0%     0%
      16   20G    0%     0%
      17   n/a    0%     0%
```

ファブリック エラーの表示

1 つまたはすべてのモジュールのファブリック エラーを表示するには、次の作業を行います。

作業	コマンド
ファブリック エラーを表示します。	**show fabric errors** {*mod* | **all**}

次に、ファブリック エラーを表示する例を示します。

```
Console> (enable) show fabric errors all
Module errors:
Slot  Channel    CRC        Hbeat      Sync       DDR sync
----- ---------- ---------- ---------- ---------- ----------
2     0          0          0          0          0

Fabric errors:
Slot  Channel    Sync       Buffer     Timeout
----- ---------- ---------- ---------- ----------
2     0          0          0          0

Console> (enable)
```

バックプレーン トラフィックおよびファブリック チャネル入出力の表示

バックプレーン トラフィックおよびファブリック チャネルの入出力を表示するには、次のいずれかの作業を行います。

作業	コマンド
バックプレーン トラフィックおよびファブリック チャネルの入出力を含むシステム ステータスを表示します。	**show system**
バックプレーン トラフィックおよびファブリック チャネルの入出力を表示します。	**show traffic**

(注) PFC3A 搭載の Supervisor Engine 720 は、ハードウェア トラフィック メータをサポートしません。このモジュール上で **show system** コマンドおよび **show traffic** コマンドを入力する場合、バックプレーン トラフィック情報を受信しません。

次に、バックプレーン トラフィックおよびファブリック チャネルの入出力を含むシステム ステータスを表示する例を示します。

```
Console> (enable) show system
PS1-Status PS2-Status
---------- ----------
ok         none

Fan-Status Temp-Alarm Sys-Status Uptime d,h:m:s Logout
---------- ---------- ---------- -------------- ---------
ok         off        ok         13,19:01:16    20 min

PS1-Type             PS2-Type
-------------------- --------------------
WS-CAC-1300W         none

Modem   Baud  Backplane-Traffic Peak Peak-Time
------- ----- ----------------- ---- ------------------------
disable  9600   0%                0% Tue Oct 19 2004, 12:04:18

PS1 Capacity: 1153.32 Watts (27.46 Amps @42V)

System Name              System Location          System Contact           CC
------------------------ ------------------------ ------------------------ ---


Slot Channel Fab Chan Input Output
---- ------- -------- ----- ------
   2       0        1    0%     0%

Core Dump                Core File
------------------------ ----------------------------------------
disabled                 slot0:crashdump

Crash Info               Crash Info File
------------------------ ----------------------------------------
enabled                  bootflash:crashinfo

System Information Logging  Host              Interval
--------------------------  ----------------  --------
Disabled                    -                 1440

System Information Log File
------------------------------------------------------------------------
tftp:sysinfo

Index        System Information Logging Commands
-----        ------------------------------------------------------------

Syslog Dump              Syslog File
------------------------ ----------------------------------------
disabled                 bootflash:sysloginfo

No profile is configured for the system
Console> (enable)
```

次に、バックプレーン トラフィックおよびファブリック チャネルの入出力を表示する例を示します。

```
Console> (enable) show traffic
Threshold: 100%

Backplane-Traffic Peak Peak-Time
----------------- ---- -------------------------
  0%                0% Tue Oct 19 2004, 12:04:18

Slot Channel Fab Chan Input Output
---- ------- -------- ----- ------
   2       0        1    0%     0%

Console> (enable)
```

スイッチング モード設定の表示

スイッチング モード設定を表示するには、次の作業を行います。

作業	コマンド
スイッチング モード設定を表示します。	**show system switchmode**

次に、スイッチング モード設定を表示する例を示します。

```
Console> show system switchmode
Switchmode allow:truncated
Switchmode threshold:2
Console> (enable)
```

統合スイッチ ファブリックのステータスの表示

統合スイッチ ファブリックのステータスおよび転送速度を表示するには、次の作業を行います。

作業	コマンド
統合スイッチ ファブリックのステータスと速度を表示します。	**show fabric status**

次に、統合スイッチ ファブリックのステータスと速度を表示する例を示します。

```
Console> show fabric status
Mod Speed  Fabric
           status
--- ----- -------
  5   20G  active
Console> (enable)
```

LCD バナーの設定

スーパバイザ エンジンから **set banner lcd** コマンドを入力して LCD バナーを変更し、次の情報を含めるようにすることができます。

- シャーシのシリアル番号
- スイッチの IP アドレス
- システム名
- スーパバイザ エンジンのバージョン
- アクティブおよびスタンバイ スーパバイザ エンジン上の Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）のバージョン
- システムの連絡先

LCD バナーの内容を変更すると、シャーシに搭載されているスイッチ ファブリック モジュールにこの情報が送信され、LCD に表示されます。

（注） **set banner lcd** コマンドは、統合スイッチ ファブリック搭載のシステムではサポートされていません。

LCD バナーの内容を変更するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	LCD バナーの内容を変更します。	**set banner lcd** *c* [*text*] *c*
ステップ 2	LCD バナーの変更を確認します。	**show banner**

次に、スイッチ ファブリック モジュールの LCD バナーを変更する例を示します。

```
Console> (enable) set banner lcd &HelloWorld!&
LCD banner set
Console> (enable) show banner
MOTD banner:

LCD config:
Hello
World!
```

CHAPTER 53

VoIP ネットワークの設定

この章では、Catalyst 6500 シリーズ スイッチ上で Voice over IP（VoIP）ネットワークを設定する方法について説明します。

(注) VoIP に関連するいくつかのシスコ製ネットワーキング製品も紹介しますが、この章では主に、VoIP ネットワークに Catalyst 6500 シリーズ製品を組み込むための設定について説明します。

(注) この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

この章で説明する内容は、次のとおりです。

ハードウェアおよびソフトウェアの要件

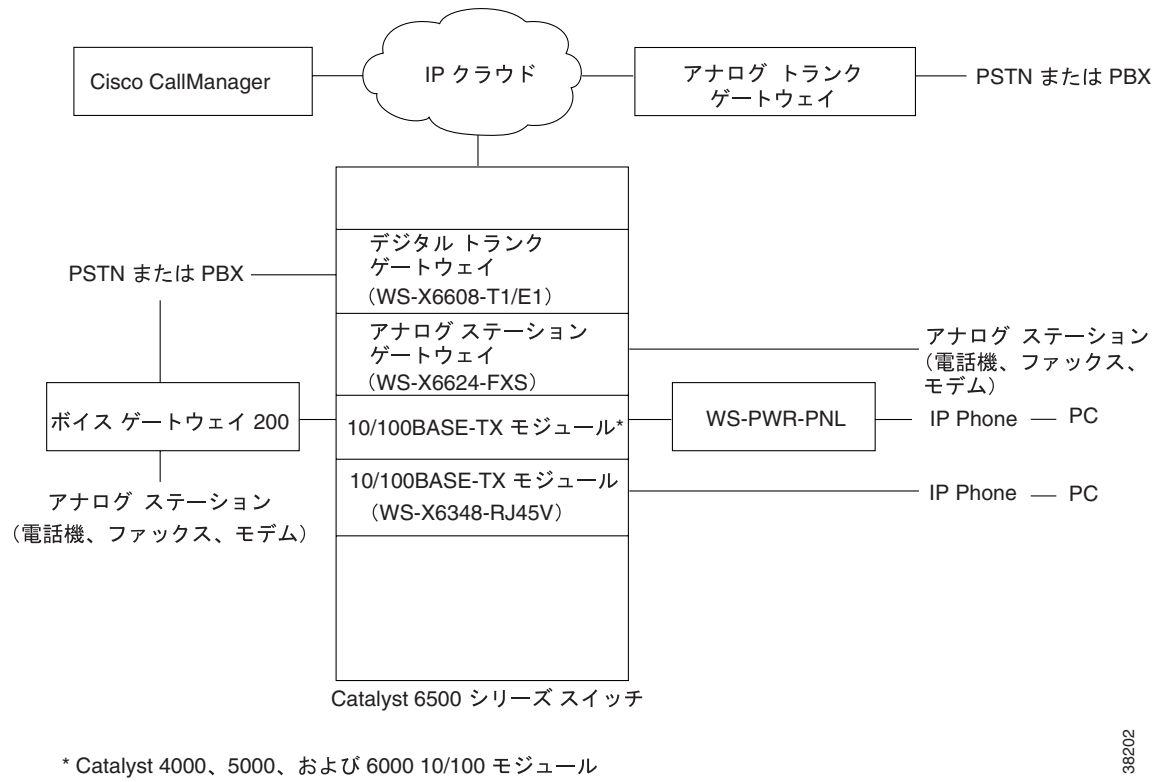
Catalyst 6500 シリーズ スイッチおよび Cisco CallManager のハードウェアおよびソフトウェア要件は、次のとおりです。

- Release 6.1(1) 以降のスーパバイザ エンジン ソフトウェア リリースが稼働する Catalyst 4500 シリーズ、5000 ファミリー、および Catalyst 6500 シリーズ スイッチ
- IEEE 802.3af 準拠の Release 8.2(1) 以降のスーパバイザ エンジン ソフトウェア リリースが稼働する Catalyst 4500 シリーズ、および Catalyst 6500 シリーズ スイッチ
- Cisco CallManager（CCM）Release 3.0 以降のリリース

VoIP ネットワークの機能

従来の回線交換 PBX（構内交換機）ネットワークではなく、IP ネットワークを基盤とするテレフォニー システムを、IP PBX システムといいます（図 53-1 を参照）。ここでは、このシステムのコンポーネントについて説明します。

図 53-1　IP PBX システム



* Catalyst 4000、5000、および 6000 10/100 モジュール

Cisco IP Phone 7960

Cisco IP Phone 7960 は、IP PBX システムへの接続を提供します。IP Phone には、外部装置との接続用の RJ-45 ジャックが 2 つ（LAN/ 電話用ジャック、および PC/ 電話用ジャック）あります。各ジャックは、カテゴリ 3 または 5 の Unshielded Twisted-Pair（UTP; シールドなしツイストペア）ケーブルを使用します。LAN/ 電話機ジャックは、クロス ケーブルを使用して電話機を LAN に接続します。PC/ 電話機ジャックを PC またはワークステーションに接続するには、ストレート ケーブルを使用します。

インライン パワー方式は、カテゴリ 3、カテゴリ 4、カテゴリ 5 以上で、最長 100 m で動作するように設計されていて、さらにインライン パワーは、トークンリング / ファスト イーサネット アダプタ（LanTel Silver Bullet SB-LN/VIP-DATA アダプタ）を使用して 100 m の IBM トークンリング STP ケーブルで動作します。

この IP Phone は Dynamic Host Configuration Protocol（DHCP）対応です。オプションとして、スタティック IP アドレスを電話機にプログラミングすることができます。

IP Phone への電力供給は、次の方法で行うことができます。

- 外部電源 — オプションの変圧器および電源コードを使用して、標準的な壁面コンセントに接続します。
- 音声ドータカードを搭載したイーサネット スイッチング モジュール — IP Phone にインライン パワーを供給します。
- WS-PWR-PNL（インライン パワー パッチ パネル）— IP Phone にインライン パワーを供給します。インライン パワー パッチ パネルを使用して、IP Phone を既存の Catalyst 4500 シリーズ、5000 ファミリー、および 6500 シリーズ 10/100BASE-TX スイッチング モジュールに接続できます。
- WS-F6K-VPWR Inline-Power Field-Upgrade Module または WS-F6K-FE48-AF Inline-Power Field-Upgrade Module 搭載の WS-X6148-RJ-45 10/100 スイッチング モジュール — IP Phone にインライン パワーを供給します。
- WS-F6K-VPWR Inline-Power Field-Upgrade Module または WS-F6K-FE48-AF Inline-Power Field-Upgrade Module 搭載の WS-X6148-RJ-21 10/100 スイッチング モジュール — IP Phone にインライン パワーを供給します。
- WS-F6K-FE96-AF Inline-Power Field-Upgrade Module 搭載の WS-X6148X2-RJ-45 10/100 スイッチング モジュール — IP Phone にインライン パワーを供給します。
- WS-F6K-FE96-AF Inline-Power Field-Upgrade Module 搭載の WS-X6148X2-RJ-21 10/100 スイッチング モジュール — IP Phone にインライン パワーを供給します。
- WS-F6K-VPWR-GE Inline-Power Field-Upgrade Module または WS-F6K-GE48-AF Inline-Power Field-Upgrade Module 搭載の WS-6548-GE-TX ギガビット イーサネット スイッチング モジュール — IP Phone にインライン パワーを供給します。
- WS-F6K-VPWR-GE Inline-Power Field-Upgrade Module または WS-F6K-GE48-AF Inline-Power Field-Upgrade Module 搭載の WS-6148-GE-TX ギガビット イーサネット スイッチング モジュール — IP Phone にインライン パワーを供給します。

図 53-2 に、Cisco IP Phone 7960 および PC を Catalyst 6500 シリーズ スイッチに接続する方法を示します。

図 53-2　Cisco IP Phone 7960 と Catalyst 6500 シリーズ スイッチとの接続

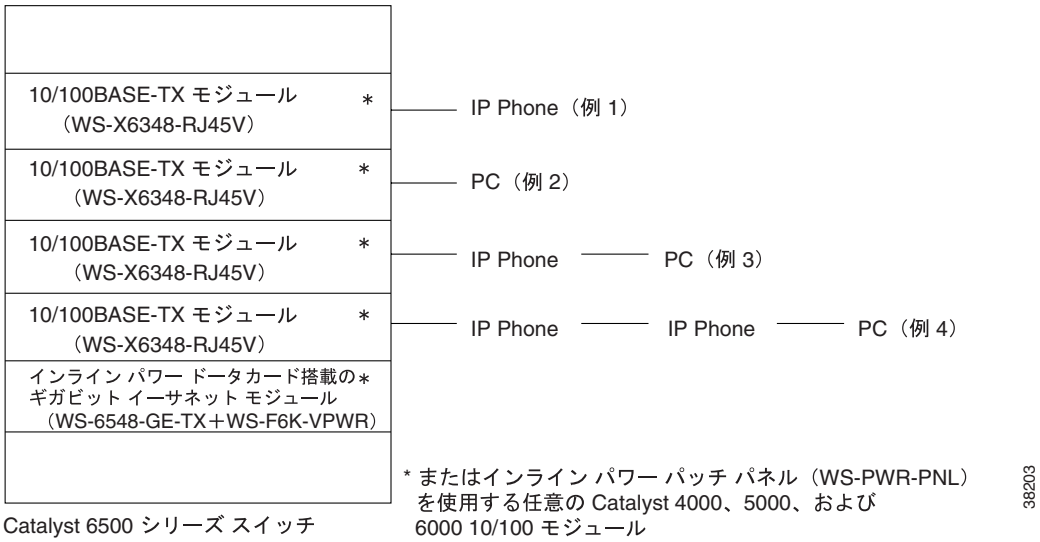


図 53-2 に示した例について説明します。

- 例 1：Cisco IP Phone 7960 1 台

  例 1 では、1 台の IP Phone を Catalyst 6500 シリーズ スイッチの 10/100 ポートに接続しています。IP Phone の PC/ 電話ジャックは使用しません。10/100 ポートまたは壁面コンセントのいずれかで、IP Phone に電力を供給できます。

- 例 2：PC 1 台

  例 2 では、1 台の PC を Catalyst 6500 シリーズ スイッチの 10/100 ポートに接続しています。壁面コンセントから PC に電力を供給します。

- 例 3：1 台の Cisco IP Phone 7960 および 1 台の PC

  例 3 では、1 台の IP Phone を Catalyst 6500 シリーズ スイッチの 10/100 ポートに接続し、IP Phone の PC/ 電話機ジャックに 1 台の PC を接続しています。PC は、Catalyst 6500 シリーズ スイッチの 10/100 ポートに直接接続しているかのように動作します。10/100 ポートまたは壁面コンセントのいずれかで、IP Phone に電力を供給できます。PC は、壁面コンセントから電力を供給する必要があります。

- 例 4：2 台の Cisco IP Phone 7960 および 1 台の PC

  例 4 では、2 台の IP Phone を Catalyst 6500 シリーズ スイッチの 10/100 ポートに接続し、IP Phone の PC/ 電話機ジャックに 1 台の PC を接続しています。PC は、Catalyst 6500 シリーズ スイッチの 10/100 ポートに直接接続しているかのように動作します。1 台めの IP Phone には、10/100 ポートまたは壁面コンセントのいずれかで、電力を供給できます。2 台めの IP Phone および PC は、壁面コンセントから電力を供給する必要があります。

（注） シスコ製 IP Phone とサードパーティ ベンダー製電話機の設定の詳細については、電話機に付属するマニュアルを参照してください。

Cisco CallManager

Cisco CallManager は、オープン性を特色とする業界標準のコール プロセッシング システムです。Windows NT サーバ上で稼働する CallManager ソフトウェアは、電話機間でのコール確立および切断を行い、従来の PBX の機能性を企業 IP ネットワークに統合します。Cisco CallManager は、IP PBX システムのコンポーネント、電話機、アクセス ゲートウェイ、および電話会議やメディア ミックスなどの機能に必要な各種リソースを管理します。各 Cisco CallManager は、その CallManager のゾーン内のデバイスを管理し、他のゾーンを管理する Cisco CallManager と情報を交換して、複数ゾーン間でのコール発信を可能にします。Cisco CallManager を既存の PBX システムと併用して、PSTN（公衆交換電話網）経由でコールをルーティングすることも可能です。

（注） この章で説明する IP 装置と Cisco CallManager を併用するための設定方法については、『*Cisco CallManager Administration Guide*』、『*Configuration Notes for Cisco CallManager*』、および『*Cisco CallManager Remote Serviceability Users Guide*』を参照してください。

アクセス ゲートウェイ

アクセス ゲートウェイは、IP PBX システムと既存の PSTN または PBX システムとの通信を可能にします。アクセス ゲートウェイは、アナログ ステーション ゲートウェイ、アナログ トランク ゲートウェイ、デジタル トランク ゲートウェイ、およびコンバージド ボイス ゲートウェイで構成されています。

ここでは、ゲートウェイについて説明します。

- アナログ ステーション ゲートウェイ（p.53-5）
- アナログ トランク ゲートウェイ（p.53-6）
- デジタル トランク ゲートウェイ（p.53-6）
- コンバージド ボイス ゲートウェイ（p.53-7）

アナログ ステーション ゲートウェイ

Catalyst 6500 シリーズ 24 ポート Foreign Exchange Station（FXS）アナログ インターフェイス モジュールを使用すると、Plain Old Telephone Service（POTS; 加入電話サービス）電話機およびファックス機を IP PBX ネットワークに接続できます。アナログ ステーション ゲートウェイは、POTS 機器の PSTN 側と同様に動作します。このゲートウェイは IP アドレスを必要とし、Cisco CallManager のドメインに登録され、Cisco CallManager によって管理されます。

アナログ ステーション インターフェイスの設定手順については、「スイッチ上での VoIP の設定」（p.53-11）を参照してください。このモジュールの機能は、表 53-1 のとおりです。

表 53-1　24 ポート FXS アナログ インターフェイス モジュールの機能

ポート単位のデジタル信号処理
G.711 および G.729 音声符号化
無音圧縮、音声アクティビティ検出
コンフォート ノイズ生成
リンガー（周波数および音はソフトウェアによりプログラム可能、国別）
DTMF[1] 検出
シグナリング、ループ スタート
回線エコー キャンセレーション（32 ミリ秒）

表 53-1　24 ポート FXS アナログ インターフェイス モジュールの機能（続き）

ポート単位のデジタル信号処理
インピーダンス（600 ohm）
プログラム可能なアナログ ゲイン、シグナリング タイマー
ファックス パススルー
SPAN[2] またはポート ミラーリングのサポート
FXS インターフェイス機能
アドレス シグナリング フォーマット : 帯域内 DTMF
シグナリング フォーマット : ループ スタート
呼び出し音 : プログラム可能
リング電圧 : プログラム可能、国別
リング周波数 : プログラム可能、国別
距離 : 最大ループ 500 ohm

1. DTMF = Dual Tone Multifrequency（デュアル トーン多重周波数）
2. SPAN = Switched Port Analyzer（スイッチド ポート アナライザ）

アナログ トランク ゲートウェイ

シスコ製アクセス アナログ トランク ゲートウェイは、IP PBX から PSTN または PBX への接続を可能にします。このゲートウェイは、PSTN への最大 8 つのトランクをサポートし、PSTN からのトランク回線には電話機のように認識されます。このゲートウェイを使用して、IP PBX は PSTN を通じて IP コールを発信します。アナログ ステーション ゲートウェイと同様に、アナログ トランク ゲートウェイは回線エコー キャンセレーション、および DTMF トーンの生成および検出を行います。アナログ トランク ゲートウェイは、POTS 電話機またはファックス機などの POTS エンド デバイスには接続しないので、リング電圧は提供しません。アナログ トランク ゲートウェイは IP アドレスを必要とし、Cisco CallManager のドメインに登録され、Cisco CallManager によって管理されます。

アナログ トランク ゲートウェイの設定手順については、ゲートウェイに付属するマニュアルを参照してください。

デジタル トランク ゲートウェイ

Catalyst 6500 シリーズ 8 ポート T1/E1 PSTN インターフェイス モジュールは、PSTN へのデジタル T1/E1 接続またはトランスコーディングおよび会議をサポートしています。このモジュールは IP アドレスを必要とし、Cisco CallManager のドメインに登録され、Cisco CallManager によって管理されます。

モジュール ソフトウェアは、TFTP サーバからダウンロードします。ダウンロードしたソフトウェアに応じて、ポートは T1/E1 インターフェイスとして動作することも、トランスコーディングおよび会議をサポートすることもできます。トランスコーディングおよび会議機能は、相互に排他的です。トランスコーディング用にポートを 1 つ使用すると、会議用に使用できるポートが 1 つ減り、また、その逆も同様です。

8 ポート T1/E1 PSTN インターフェイスの設定手順については、「スイッチ上での VoIP の設定」（p.53-11）を参照してください。このモジュールの機能は、表 53-2 のとおりです。

表 53-2　8 ポート T1/E1 PSTN インターフェイス モジュールの機能

T1/E1 ポート単位のデジタル信号処理
G.711 から G.723 および G.729A へのトランスコーディング（トランスコーディングは最大 8 × 32 チャネル）
会議ブリッジング、meet-me および ad-hoc 会議モード（会議は最大 8 × 16 チャネル）
コンフォート ノイズ生成
ファックス パススルー
無音圧縮、音声アクティビティ検出
回線エコー キャンセレーション
共通チャネル信号 T1 の場合：音声トラフィック用に 23 の DS0 チャネル、24 番めのチャネルはシグナリングに使用 E1 の場合：音声トラフィック用に 29 の DS0 チャネル、16 番めのチャネルはシグナリング専用 どのチャネルにも、共通チャネル信号を設定できます。
ISDN PRI（一次群速度インターフェイス）シグナリング : 各インターフェイスは、T1 には 23 チャネル、E1 には 30 チャネルをサポートしています。デフォルト モードでは、T1 の 24 番め、または E1 の 16 番めのチャネルは、シグナリング専用です。ネットワーク側およびユーザ側の両方の動作モードがサポートされています。
T1 Binary 8-Zero Substitution/Alternate Mark Inversion（B8ZS/AMI）伝送符号化、U-law または A-law 符号化 E1 HDB3 伝送符号化
T1 回線のビット レート：1.544 Mbps E1 回線のビット レート：2.048 Mbps
T1 伝送符号：AMI、B8ZS E1 伝送符号：HDB3
フレーミング フォーマット：D4 スーパーフレームおよび拡張スーパーフレーム
リンク管理
FDL[1] は、問題を診断し、T1 回線に関する統計情報を収集するためのリンク管理プロトコルです。

1. FDL = Facilities Data Link

コンバージド ボイス ゲートウェイ

Cisco Voice Gateway 200（VG200）を使用すると、標準的な（ゲートウェイまたは PSTN 上のどこかに直接接続する）POTS 電話機を、Cisco IP または任意の H.323 準拠テレフォニー デバイスに接続できます。Cisco CallManager と併用した場合、VG200 は Media Gateway Control Protocol（MGCP）ゲートウェイとして動作します。Cisco VG200 は、データ ネットワークとの接続用に 10/100BASE-T イーサネット ポートを 1 つ備えています。次のテレフォニー接続も使用可能です。

- セントラル オフィスまたは PBX との接続用に、1 ～ 4 つの Foreign Exchange Office（FXO）ポート
- POTS テレフォニー装置との接続用に、1 ～ 4 つの FXS ポート
- 1 つまたは 2 つの T1 デジタル ポート（次の接続用）
  - FXO エミュレーションによる PSTN
  - FXS エミュレーションによる T1 チャネル バンク
  - Ear and Mouth（E&M）エミュレーションによるトランク（タイ）回線を介した PBX

これらのポートを使用し、VoIP ネットワークを POTS 装置、PBX、または PSTN と統合することができます。

Cisco VG200 の設定手順については、ゲートウェイに付属するマニュアルを参照してください。

コール発信の仕組み

IP Phone は、ハブ ポートまたはスイッチ ポートを通じて LAN に接続します。IP Phone は、DHCP を起動および使用して、IP アドレスおよび TFTP ファイル サーバの IP アドレスを取得します。IP Phone は、IP アドレスを使用して TFTP サーバと通信し、コンフィギュレーション ファイルを取得します。コンフィギュレーション ファイルには、電話機の Cisco CallManager の IP アドレスが含まれています。電話機は次に、Cisco CallManager と通信して、自機を登録します。電話機は起動するたびに、異なる IP アドレスを取得する可能性があります。Cisco CallManager は、電話機の MAC アドレスを使用して、終始一貫したユーザ電話番号と、特定の電話機との対応付けを行います。Cisco CallManager は常に、電話機の MAC アドレスと電話番号をマッピングするテーブルを保持しています。電話機が登録されるたびに、テーブルは新しい IP アドレスで更新されます。Cisco CallManager は、登録時に、電話機のキーパッド テンプレートおよび機能をダウンロードします。さらに、使用すべき実行イメージを電話機に指示します。電話機は TFTP サーバにアクセスして、実行イメージを取得します。各電話機には制御チャネルと呼ばれる Cisco CallManager への専用 TCP 接続があります。キーの押し下げなどの制御情報はすべて、このチャネルを通じて電話機から　Cisco CallManager へ送信されます。リング トーン、ビジー トーンなどを生成する命令は、このチャネルを通じて Cisco CallManager から電話機へ送信されます。

Cisco CallManager では、IP アドレス / 電話番号（およびその逆）のマッピングをテーブルに保存しています。他のユーザへの通話を希望するユーザは、着呼側の電話番号を押します。Cisco CallManager はこの電話番号を IP アドレスに変換し、TCP 接続を通じて、着呼側の IP Phone にリング トーンの IP パケット バージョンを生成します。着呼側の IP Phone がこのパケットを受信すると、リング トーンを生成します。ユーザが受話器を取ると、Cisco CallManager は着呼側の IP Phone に対し、発呼側との通話を開始するように指示し、自らをループから削除します。この時点で、UDP を介して実行される Real-Time Transport Protocol（RTP）により、2 つの IP Phone 間で通話されるようになります。音声パケットは遅延に影響されやすいので、タイムアウトおよび再試行によってパケット間に遅延が生じる TCP は、音声伝送には適していません。通話中にどちらかの電話機での機能キーが押されたり、どちらかのユーザが受話器を置くかフラッシュ ボタンを押すといった変化が発生すると、その情報が制御チャネルを通じて Cisco CallManager に伝えられます。

IP PBX ネットワーク外部の番号にコールが発信された場合、Cisco CallManager はそのコールをアナログまたはデジタル トランク ゲートウェイにルーティングします。アナログまたはデジタル トランク ゲートウェイは、さらに PSTN へコールをルーティングします。

VLAN の機能

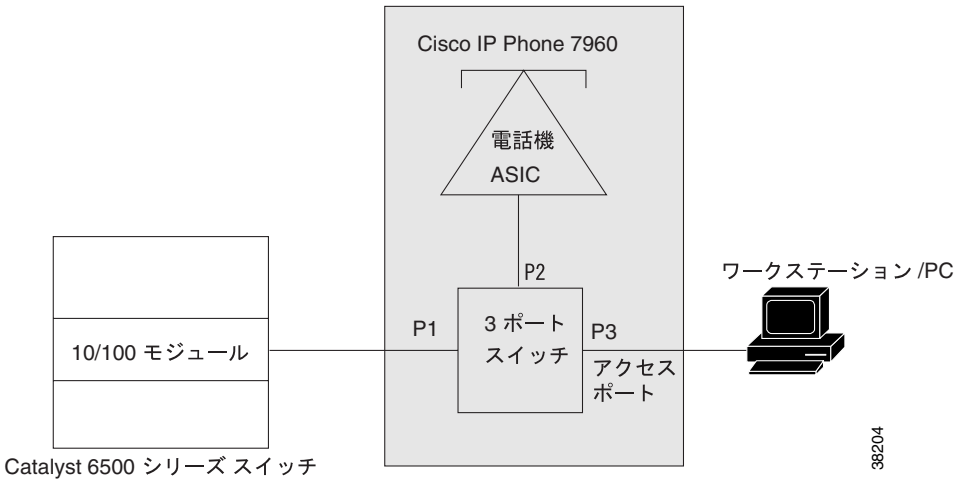
ここでは、ネイティブ VLAN および補助 VLAN について説明します。ここでは、次の用語を使用します。

- 補助 VLAN ― IP Phone 用の個別の VLAN
- ネイティブ VLAN ― データ用の従来の VLAN
- 補助 VLAN ID ― 補助 VLAN の VLAN ID
- ネイティブ VLAN ID ― ネイティブ VLAN の VLAN ID

(注)　VLAN の詳細については、第 11 章「VLAN の設定」を参照してください。

図 53-3 に、Cisco IP Phone 7960 と Catalyst 6500 シリーズ スイッチとの接続方法を示します。

図 53-3　スイッチと電話機の接続



IP Phone を Catalyst 6500 シリーズ スイッチの 10/100 ポートに接続する場合、IP Phone の *アクセス ポート*（PC/ 電話ジャック）を PC 接続に使用できます。

PC と電話機が送受信するパケットは、同じ物理リンクを通り、同じスイッチポートを共用します。「Cisco IP Phone 7960」（p.53-3）に、さまざまな構成が示されています。

既存のスイッチ ベース ネットワークに IP ベースの電話機を導入する場合、次のような問題があります。

- 現在の VLAN が IP サブネット ベースで設定されている場合、電話機を 1 つのポートに割り当て、同じポートに接続する他の装置（PC）と電話機が同じサブネットに属するように、IP アドレスを追加設定することが不可能な場合があります。
- VLAN をサポートする電話機上のデータ トラフィックによって、VoIP トラフィックの品質が低下する可能性があります。

これらの問題は、電話機に接続する各ポート上で、音声トラフィックを個別の VLAN に分離することで解決できます。電話機接続用に設定されたスイッチ ポートには、次のトラフィックを転送するための専用 VLAN を設定します。

- IP Phone との間の音声トラフィック（補助 VLAN）
- IP Phone のアクセス ポートを介してスイッチに接続する PC との間のデータ トラフィック（ネイティブ VLAN）

電話機を個別の補助 VLAN に分離することにより、音声トラフィックの品質を向上させるだけでなく、IP アドレスが不足している既存ネットワークに多数の電話機を追加できます。新しい VLAN とは、新しいサブネットおよび新しい IP アドレスの集合を意味します。

CDP および VoIP の機能

Cisco Discovery Protocol（CDP）は Release 8.1(1) のソフトウェア リリースで機能強化されているため、新しい高消費電力の Cisco IP Phone との下位互換性を実現します。この機能強化した CDP により、Cisco IP Phone はスイッチへの電源要求を CDP パケット内でネゴシエーションします。スイッチはこの情報を使用して、使用可能な電力をオーバーサブスクライブしないようにします。

接続されている IP Phone を適切に検出して電力を供給できるように、スイッチ上で CDP をイネーブルにすることを推奨します。CDP は、Catalyst 6500 シリーズ スイッチ上でイネーブルになっています（デフォルト設定）。ただし、VoIP ネットワークの設定時には、CDP がイネーブルになっていることを確認してください。CDP の詳細については、第 30 章「CDP の設定」を参照してください。

スイッチ上での VoIP の設定

ここでは、Catalyst 6500 シリーズ スイッチに VoIP 動作を設定するための CLI（コマンドライン インターフェイス）コマンドとその手順について説明します。

（注） 自動音声設定の使用方法については、「SmartPort の使用方法」（p.53-41）を参照してください。

（注） 補助 VLAN ID、ポート別の電源管理の詳細、Quality of Service（QoS; サービス品質）設定などの情報を伝達するために、IP Phone に接続する Catalyst 6500 シリーズ スイッチ ポート上で、CDP をイネーブルにする必要があります。

音声関連の CLI コマンド

表 53-3 に、設定手順で使用する CLI コマンドを示します。

表 53-3　音声関連の CLI コマンド モジュールおよびプラットフォーム サポート

CLI コマンド	イーサネット モジュール[1]	WS-X6608-T1/E1[2]	WS-X6624-FXS[3]
インライン パワー関連のコマンド			
set port inlinepower	X[4]		
set inlinepower defaultallocation	これはスイッチ レベルのコマンドであり、個々のモジュールには影響しません。		
show port inlinepower	X		
show environment power	X	X	X

表 53-3　音声関連の CLI コマンド モジュールおよびプラットフォーム サポート（続き）

CLI コマンド	イーサネット モジュール[1]	WS-X6608-T1/E1[2]	WS-X6624-FXS[3]
音声関連のコマンド			
set port auxiliaryvlan	X/X		
show port auxiliaryvlan	X/X		
set port voice interface		X	X
show port voice interface		X	X
show port voice	X	X	X
show port voice fdl		X	
show port voice active	X	X	X
音声関連の QoS コマンド			
set port qos *mod/port* **cos-ext** **set port qos** *mod/port* **trust-ext**	X/X		
show port qos	X/X		

1. イーサネット モジュール = 音声ドータカードを搭載したイーサネット スイッチング モジュール
2. WS-X6608-T1 および WS-X6608-E1 = 8 ポート T1/E1 ISDN PRI モジュール
3. WS-X6624-FXS = 24 ポート FXS アナログ ステーション インターフェイス モジュール
4. X = Catalyst 6500 シリーズ スイッチ上でのみサポートされるコマンド。XX = Catalyst 4500 シリーズ、5000 ファミリー、および 6500 シリーズ スイッチ上でサポートされるコマンド。表 53-3 に示すモジュールは、すべて Catalyst 6500 シリーズ スイッチ上でのみサポートされています。

ポート単位の電源管理の設定

ここでは、ポート単位の電源管理、および IP Phone の電源管理を設定する CLI コマンドについて説明します。

（注） システムのパワー バジェットを超過しないように、「システム ステータス レポートの生成」（p.21-19）を参照して、使用する構成で必要な電力量を判別してください。

（注） ここで説明する内容が当てはまるのは、音声ドータカードを搭載したイーサネット　スイッチング モジュールのみです。それ以外のイーサネット スイッチング モジュールに接続する IP Phone への電力供給については、『*Catalyst Family Inline-Power Patch Panel Installation Note*』を参照してください。

モジュールは、音声ドータカードを搭載したイーサネット スイッチング モジュールに接続する各 IP Phone について、使用可能なシステム電力の一部を割り当て、電話機に電力を供給して稼働させます。ポート単位で個別に電力を供給できます。

1 つのポートで電力を供給できるのは、そのスイッチ ポートに直接接続された 1 台の IP Phone に限られます。スイッチ ポートに接続された電話機から 2 台めの電話機がデイジーチェーン接続されている場合、2 台めの電話機は、スイッチから電力を受けることはできません。

ここでは、次の項目について説明します。

show コマンドによるモジュール タイプおよびバージョン情報の表示

モジュールに音声ドータカードが搭載されているかどうかを判別するには、**show module** コマンドを実行し、[Sub] フィールドを確認します。たとえば、次に示す出力例では、スロット 3 の 10/100BASE-TX モジュールに音声ドータカードが搭載されています。

モジュールのステータスおよび情報を表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
モジュールのステータスおよび情報を表示します。	**show module** [*mod*]

次の例は、サブモジュールに関する情報を表示するサブモジュール フィールドを示します。出力例に示すように、モジュール 3 に搭載されたインライン パワー ドータカードは WS-F6K-SVDB-FE であり、モジュール 6 に搭載されたインライン パワー ドータカードは WS-F6K-VPWR-GE-TX です。

```
Console> (enable) show module
Mod Slot Ports Module-Type               Model               Sub Status
--- ---- ----- ------------------------- ------------------- --- --------
1   1    2     1000BaseX Supervisor      WS-X6K-SUP2-2GE     yes ok
3   3    48    10/100BaseTX Ethernet     WS-X6548-RJ-45      yes ok
4   4    48    10/100BaseTX Ethernet     WS-X6148-RJ45V      no  ok
6   6    48    10/100/1000BaseT Ethernet WS-X6148-GE-TX      yes ok

Mod Module-Name          Serial-Num
--- -------------------- -----------
1                        SAD04460M9G
3                        SAD0447099V
4                        SAD061901FL
6                        SAD0706025A

Mod MAC-Address(es)                         Hw     Fw          Sw
--- --------------------------------------- ------ ----------- ------------------
1   00-d0-c0-d4-04-4e to 00-d0-c0-d4-04-4f 1.1    6.1(2)      7.7(0.82-Eng)
    00-d0-c0-d4-04-4c to 00-d0-c0-d4-04-4d
    00-02-4a-30-88-00 to 00-02-4a-30-8b-ff
3   00-02-b9-ff-eb-70 to 00-02-b9-ff-eb-9f 0.203  6.3(1)      8.2(1)
4   00-00-00-00-00-00 to 00-00-00-00-00-2f 1.3    5.4(2)      7.7(0.81)
6   00-40-0b-ff-00-00 to 00-40-0b-ff-00-2f 0.304  7.2(1)      8.2(1)

Mod Sub-Type                Sub-Model           Sub-Serial  Sub-Hw Sub-Sw
--- ----------------------- ------------------- ----------- ------ ------
1   L3 Switching Engine II  WS-F6K-PFC2         SAD044302EA 1.0
3   IEEE InlinePower Module WS-F6K-FE48-AF      sasdfasdf   0.1    8.1(0)
6   Inline Power Module     WS-F6K-VPWR-GE      SAD070700GV 0.201  8.1(0)
Console> (enable)
```

モジュールおよびサブモジュールのバージョンを表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
モジュールおよびサブモジュールのバージョンを表示します。	**show version** [*mod*]

次に、モジュールおよびサブモジュールのバージョンを表示する例を示します。

```
Console> (enable) show version 6
Mod Port Model               Serial #    Versions
--- ---- ------------------- ----------- --------------------------------------
6   48   WS-X6148-GE-TX      SAD0706025A Hw :0.304
                                         Fw :7.2(1)
                                         Sw :8.1(0)
         WS-F6K-VPWR-GE      SAD070700GV Hw :0.201
                                         Sw :8.1(0)
Console>
```

電源管理モード

各ポートは、CLI、SNMP（簡易ネットワーク管理プロトコル）、またはコンフィギュレーション ファイルにより設定され、次のいずれかのモードになります。CLI コマンドは、**set port inlinepower** *mod/port* {{**auto** | **static** | **limit**} [*wattage*] | **off**} です。

- **auto** ― 検出機能がイネーブルとなり、スーパバイザ エンジンは、スイッチング モジュールが電話機を検出した場合にだけ、ポートに電力供給するように指示します。ポートに許容される最大ワット数を指定できます。ワット数を指定しない場合、スイッチはハードウェアが対応する最大値を超えない範囲で電力を供給します。
- **static** ― 検出機能がイネーブルとなり、スーパバイザ エンジンは、スイッチング モジュールが電話機を検出した場合にだけ、指定したワット数でポートに電力供給するように指示します。ポートに許容される最大ワット数を指定できます。ワット数を指定しない場合、スイッチはハードウェアが対応する最大値の電力供給を許可します。この最大ワット数は、スイッチが決定するか手動で設定するかにかかわらず、ポートに対してあらかじめ割り当てられます。スイッチがこの割り当てを満たすだけの電力を持たない場合、コマンドの実行は失敗します。
- **off** ― 検出機能がディセーブルとなり、ポートが外部装置に電力供給しないようにします。外部装置が壁面コンセントから電力供給され、インライン パワーがオフの場合でもポートのリンクはアップし、ブリッジ グループに加入し、STP フォワーディング ステートになります。
- **limit** ― 検出機能がイネーブルとなります。このモードでは、外部装置に割り当てられる電力を任意で制限できます。**limit** キーワードで指定したワット数が、IEEE 分類で決められた電力より低い場合、電力の供給を拒否することなく、これら 2 つの値の最小値が割り当てられます。装置が設定値よりも多くの電力を消費する場合、ポートはシャット ダウンされ、適切な Syslog メッセージが表示されます。**limit** キーワードは、すべてのモジュールでサポートされるわけではありません。モジュール上で **limit** キーワードがサポートされているかどうかを確認するには、**show environment power** *mod* コマンドを入力します。コマンド出力で、ポート単位の電力モニタリングが表示されていれば、このモードはサポートされています。
- *max-wattage* ―（任意）**auto** モードまたは **static** モードでポートに供給できる最大許容電力。有効値は、4000 ～ 15400 ミリワットです。

また、各ポートは次のステータスのいずれかになります。

- on ― ポートから電力供給されています。
- off ― ポートから電力供給されていません。
- power-deny ― スーパバイザ エンジンがポートに割り当てるだけの電力を持たないか、ポートに割り当てられた電力がポートに必要な電力を下回っています。ポートから電力が供給されていません。

- err-disable ― ポートが、static モードに設定された接続装置に電力を供給できません。
- faulty ― ポートが診断テストに失敗しました。

ここでは、IP Phone の電力所要量と管理について説明します。

電力所要量

IP Phone の電力所要量はそれぞれ異なります。表 53-4 に、IP Phone の電力所要量をクラスごとに示します。スーパバイザ エンジンは、ポートごとの設定、分類（IEEE のみ）、およびデフォルト電力に基づいて、最初に各ポートへの電力割り当てを計算します。正しい電力の総量を Cisco IP Phone の CDP メッセージから判別できれば、スーパバイザ エンジンは auto モードに設定されたポートに対して割り当てられた電力をそれに合わせて増減します。割り当てられた電力は、static モードで設定されたポートのように調節されていません。

たとえば、6.3 W 必要な Cisco IP Phone に 7 W の電力をデフォルトで割り当てます。スーパバイザ エンジンは、Cisco IP Phone にその 7 W を割り当てたあと、起動させます。Cisco IP Phone がいったん動作すれば、実際に必要な電力要件の CDP メッセージがスーパバイザ エンジンに送られます。その後、ポートが auto モードに設定されている場合、スーパバイザ エンジンは割り当てられた電力を実際に必要な量まで減らします。ポートが static モードに設定されている場合、スーパバイザ エンジンは指定どおりの電力を割り当てます。ポートが off に設定されている場合、スーパバイザ エンジンはそのポートに電力を割り当てません。

表 53-4　IP Phone の電力所要量

Phone クラス	所要電力（W）
Cisco	6.3
Cisco + IEEE	7
Cisco ハイ パワー	15.4
クラス 0 IEEE	15.4
クラス 1 IEEE	4
クラス 2 IEEE	7.0
クラス 3	15.4
クラス 4（クラス 0 を参照）	予約済み

使用電力

表 53-5 に、音声ドータ カードの各ポートに供給できる使用電力を示します。

表 53-5　音声ドータ カードの効率

ドータ カード	各ポート（W）の最大電力	効率
WS-F6K-PWR	6.3	100%
WS-F6K-VPWR-GE	6.3	89%
WS-F6K-GE48-AF	15	89%
WS-F6K-FE48-AF	15	89%
WS-F6K-FE96-AF	15	89%

たとえば、6.3 W の電力が必要なデバイスがある場合、効率が 89% のドータカードを使用するポートに割り当てる電力は、6.3/（0.89）= 7 W になります。効率が 100% の音声ドータ カードを使用している場合、割り当てる電力は 6.3 W になります。

壁面コンセントによる電話機への電力供給

スイッチング モジュール ポート上に、壁面コンセントから電力を供給される電話機が存在する場合、スイッチング モジュールはその電話機の存在を検出できません。スーパバイザ エンジンは、ポートとの CDP メッセージングを通じて、このような電話機を検出します。電話機がインライン パワーをサポートし（スーパバイザ エンジンは CDP を通じてこのことを判別します）、かつ auto、static、または off モードに設定されている場合、スーパバイザ エンジンはポートに電力を供給しません。停電が発生し、かつモードが auto に設定されている場合、電話機の電力は失われますが、スイッチング モジュールがこの電話機を検出し、スーパバイザ エンジンに報告することにより、スーパバイザ エンジンは電話機にインライン パワーを供給します。停電が発生し、かつモードが static に設定されている場合、電話機の電力は失われますが、スイッチング モジュールがこの電話機を検出し、あらかじめ割り当てられたインライン パワーを供給します。

電話機の電源切断

スーパバイザ エンジンは、スイッチング モジュールへのメッセージ送信により、特定のポートへの電力供給をオフにすることができます。auto モードでは、ポートに使用されていたその電力は、システムの使用可能な電力に加えられます。static モードでは、ポートに使用されていたその電力は、システムの使用可能な電力には加えられません。このような状況になるのは、CLI または SNMP を通じて電話機の電力を切断する場合だけです。

電話機の取り外し

*電力供給されている*電話機が取り外された場合、スイッチング モジュールは、リンクダウン メッセージを使用してスーパバイザ エンジンに通知します。スーパバイザ エンジンは、そのポートに割り当てていた電力を、使用可能なシステム総電力量に戻します。

さらに、*電力供給されていない*電話機が取り外された場合にも、スイッチング モジュールはスーパバイザ エンジンに通知します。

注意　ポートに電話ケーブルを差し込み、電源をオンにすると、スーパバイザ エンジンは回線上でリンクが起動するまで、4 秒間待機します。この 4 秒のあいだに、電話ケーブルを取り外し、ネットワーク装置を接続すると、装置が損傷することがあります。装置を取り外し、新しい装置を接続する場合は、10 秒以上待機してから行うようにしてください。

ハイ アベイラビリティのサポート

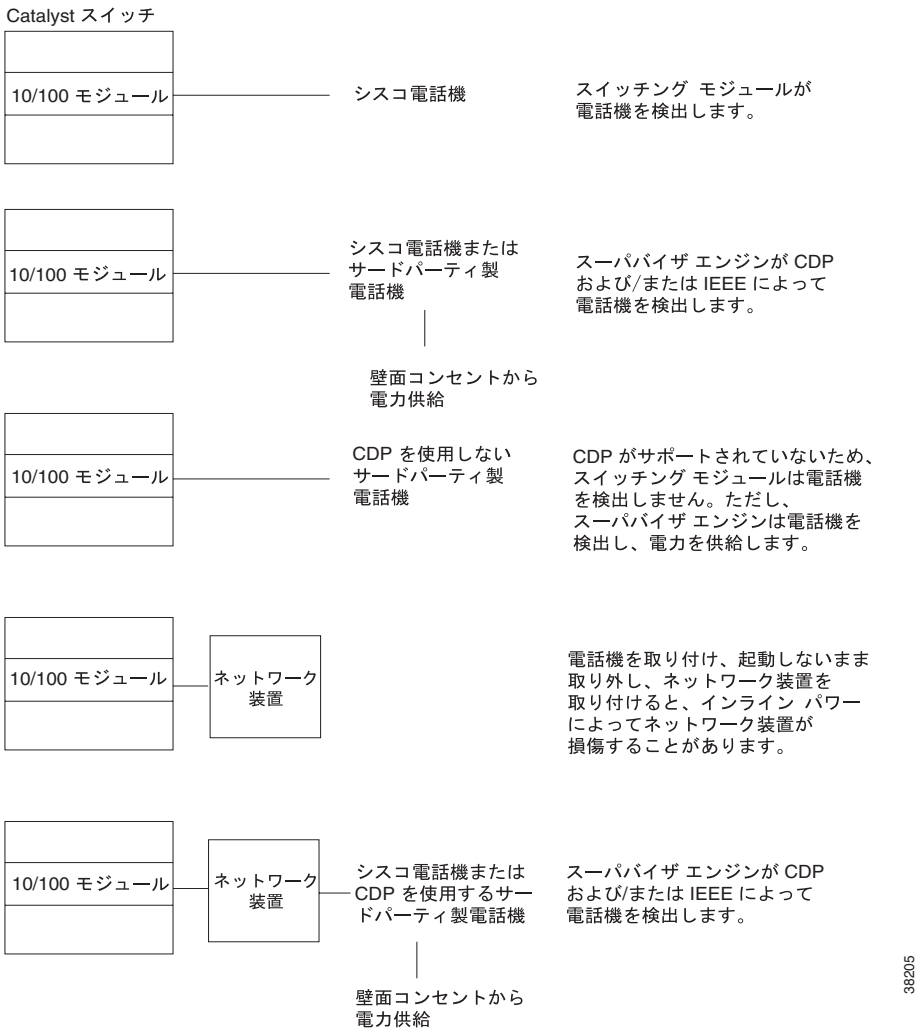
アクティブ スーパバイザ エンジンからスタンバイ スーパバイザ エンジンへのフェールオーバー時にハイ アベイラビリティを維持するため、アクティブとスタンバイ スーパバイザ エンジン間で、ポート単位の電源管理情報および電話機ステータス情報が同期化されます。

（ポート単位で）同期化される情報は、電話機の有無、電話機の電源ステータス（on、off、denied、または faulty）、割り当て電力、装置のクラス、装置のタイプ、装置の最大電力、および装置の検出です。アクティブ スーパバイザ エンジンはこの情報をスタンバイ スーパバイザ エンジンに送信し、スタンバイ スーパバイザ エンジンは内部データ構造を更新します。切り替えが行われると、スタンバイ スーパバイザ エンジンは、使用可能な電力量から各モジュールおよびポートへ、一度に 1 モジュールずつ電力を割り当てます。各モジュールに電力を割り当てたあと、スーパバイザ エンジンは電話機に対し、スロット番号の小さい方から順に電力を割り当て、最終的にインライン パワーを供給されるすべてのポートが、on、off、または denied のいずれかのステータスになります。

電話機検出の概要

図 53-4 に、Catalyst 6500 シリーズ スイッチ ポートに接続された電話機をシステムが検出する方法を示します。

図 53-4　電源検出の概要



ポートまたはポート グループの電源モードの設定

ポートまたはポート グループの電源モードを設定するには、ユーザ モードで次の作業を行います。

作業	コマンド
ポートまたはポート グループの電源モードを設定します。	**set port inlinepower** *mod/port* {[**auto** | **static**] [*max-wattage*] | **off**}

（注） Catalyst 6500 シリーズ スイッチ上で、**set port inlinepower** *mod/port* **static** | **auto** *max-wattage* コマンドにより 500 の倍数で *max-wattage* 値を設定した場合、グローバル割り当てにより供給される電力は、**show environment power** コマンドの Total PWR Allocated to Module フィールドに表示される電力よりもやや小さくなる可能性があります。この不一致は、ワットからアンペアへの、およびその逆の、単位の内部変換により生じます。割り当て総電力とシステムから供給される総電力との間の差異は、+/–0.42 W 以下です。

次に、ポートまたはポート グループの電源モードを設定する例を示します。

```
Console> (enable) set port inlinepower 2/5 off
Inline power for port 2/5 set to off.
Console> (enable) set port inlinepower 2/3-9 auto 800
Inline power for ports 2/3-9 set to auto and max-wattage to 800.
Console> (enable)
```

電力割り当てのデフォルト設定

set inlinepower defaultallocation コマンドはグローバルで、Cisco IP Phone にのみ有効です。インライン パワーの使用量が指定スレッシュホールドを超過すると、インライン パワー スレッシュホールド通知により Syslog メッセージが生成されます。デフォルトの電力割り当てを設定するには、イネーブル モードで次の作業を実行します（デフォルトの割り当て値は、15400 ミリワットです）。

注意 システムに接続されたすべてのインライン パワー装置を起動するのに十分な電力がない場合、**set inlinepower defaultallocation** コマンドを使用すると悪影響が生じる場合があります。小さな値で電力割り当てを設定しても、最初は、接続されたすべてのインライン パワー装置に電源が投入されます。ただし CDP メッセージの受信後は、装置がより多くの電力を消費することを学習するので、一部のポートへの電力供給を拒否します。小さな値を設定すると、しばらくの間、電力が過剰に引き出される原因にもなり、予期せぬ結果（ハードウェア障害および想定外のリセットなど）が生じることがあります。

（注） WS-X6348-RJ21V、WS-X6348-RJ-45V、WS-X6148-RJ-45V、および WS-X6148-RJ21V モジュールでサポートされる最大電力は、7000 ミリワットです。

作業	コマンド
デフォルトの電力割り当てを設定します。	**set inlinepower defaultallocation** *value*

次に、デフォルトの電力割り当てを設定する例を示します。

```
Console> (enable) set inlinepower defaultallocation 9500
Default inline power allocation set to 9500 mWatt per applicable port.
Console> (enable)
```

モジュールのインライン パワー通知スレッシュホールドの設定

インライン パワー使用率のスレッシュホールドを設定するには、**set inlinepower notify-threshold** コマンドを使用します。スレッシュホールドの割合は 1 ～ 99 であり、99% がデフォルトです。スレッシュホールドを超えると、Syslog およびトラップ（設定されている場合）が生成されます。

モジュールのインライン パワー通知スレッシュホールドを設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
モジュールのインライン パワー通知スレッシュホールドを設定します。	**set inlinepower notify-threshold** {*percentage value*} **module** {*mod_num*}

次に、モジュール 4 のインライン パワー通知スレッシュホールドを 50 に設定する例を示します。

```
Console> (enable) set inlinepower notify-threshold 50 mod 4
Module 4 inlinepower notify-threshold is set to 50%.
Console> (enable)
```

モジュールおよび各ポートの電源ステータスの表示（イネーブル モード）

モジュールおよび各ポートの電源ステータスを表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
モジュールおよび各ポートの電源ステータスを表示します。	**show port inlinepower** [*mod*[*/port*]] [**detail**]

次に、モジュールおよび各ポートの電源ステータスを表示する例を示します。

```
Console> show port inlinepower 6/1
Configured Default Inline Power allocation per port: 15.400 Watts (0.36
Amps @42V)
Total inline power drawn by module 4:  33.934 Watts ( 0.807 Amps @42V)

Port  InlinePowered  PowerAllocated   Device     IEEE class
                     From PS   To PD
      Admin  Oper    mWatts    mWatts
----- ------ ------ -------   ------- ---------- ----------
 6/1  auto   on     7079      6300    cisco      none

Port  MaximumPower  ActualConsumption
      mWatts        mWatts
----- ------------  -----------------
 6/1  15400         6300

Console>
```

次に、モジュールおよび各ポートの詳細な電源ステータスを表示する例を示します。

```
Console> show port inlinepower 4/1 detail
Configured Default Inline Power allocation per port: 15.400 Watts (0.36
Amps @42V)
Total inline power drawn by module 4:  33.934 Watts ( 0.807 Amps @42V)

Port      InlinePowered      PowerAllocated  Device     IEEE class DiscoverMode
                             From PS To PD
      Admin  Oper   Detected mWatts  mWatts
----- ------ ------ -------- ------- ------- ---------- ---------- ------------
 4/1  auto   on     yes      7079    6300    cisco      none        cisco

Port  MaximumPower  ActualConsumption  absentCounter  OverCurrent
      mWatts        mWatts
----- ------------  -----------------  -------------  -----------
 4/1  15400         6300               0              0
Console>
```

モジュールのスイッチ電力環境の表示

モジュールのスイッチ電力環境を表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
モジュールのスイッチ電力環境を表示します。	**show environment power** [*mod*]

次に、モジュールのスイッチ電力環境を表示する例を示します。

```
Console> (enable) show environment power 2
Feature not supported on module 2.
Console> (enable)

Console> (enable) show environment power
PS1 Capacity:1153.32 Watts (27.46 Amps @42V)
PS2 Capacity:none
PS Configuration :PS1 and PS2 in Redundant Configuration.
Total Power Available:1153.32 Watts (27.46 Amps @42V)
Total Power Available for Line Card Usage:1153.32 Watts (27.46 Amps @42V)
Total Power Drawn From the System:683.76 Watts (16.28 Amps @42V)
Total Inline Power Drawn From the System: 57.54 Watts ( 1.37 Amps @42V)
Remaining Power in the System:469.56 Watts (11.18 Amps @42V)
Configured Default Inline Power allocation per port:15.400 Watts (0.36 Amps
@42V)

Slot power Requirement/Usage :

Slot Card Type           PowerRequested PowerAllocated CardStatus
                         Watts   A @42V Watts   A @42V
---- ------------------- ------- ------ ------- ------ ----------
1    WS-X6K-SUP2-2GE     128.52   3.06  128.52   3.06  ok
2                          0.00   0.00  128.52   3.06  none
3    WS-X6548-RJ-45      123.06   2.93  123.06   2.93  ok
4    WS-X6148-RJ45V      100.38   2.39  100.38   2.39  ok
6    WS-X6148-GE-TX      145.74   3.47  145.74   3.47  ok

Slot Inline Power Requirement/Usage :

Slot CardType            Total Allocated   Max H/W Supported  Max H/W
Supported
                         To Module (Watts) Per Module (Watts) Per Port (Watts)
---- ------------------- ----------------- ------------------ ----------------
3    WS-X6548-RJ-45      31.08             315.84             15.400
6    WS-X6148-GE-TX      26.46             315.84             7.000
Console> (enable)
```

partial-deny ステータスは、一部のモジュール ポートにはインライン パワーが供給されているが、モジュール上のすべてのポートにインライン パワーが供給されているわけではないことを表します。

Catalyst LAN スイッチ上での補助 VLAN の設定

ここでは、補助 VLAN の設定手順について説明します。

補助 VLAN の概要

CDP パケットを送信するようにスイッチ ポートを設定し、その CDP パケットで、接続された Cisco IP Phone 7960 が次のフレーム タイプで音声トラフィックをスイッチへ転送するように指示することができます。

- 補助 VLAN ID およびレイヤ 2 CoS の設定値 5 を伝送する 802.1Q フレーム（スイッチ ポートは、補助 VLAN ID を伝送する 802.1Q フレーム以外のすべての 802.1Q フレームを廃棄します）。
  - 補助 VLAN ID が変更されたときは、Cisco IP Phone 7960 をリセットします。
  - **set port auxiliaryvlan** *mod*[*/port*] *aux_vlan_id* コマンドを入力します。

（注）　802.1Q フレームおよび個別の VLAN の使用を推奨します。

- VLAN ID 0 およびレイヤ 2 CoS の設定値 5 を伝送する 802.1Q フレームである 802.1p フレーム（**set port auxiliaryvlan** *mod*[*/port*] **dot1p** コマンドを使用）
- VLAN ID およびレイヤ 2 CoS 値を伝送しない、タグなしの 802.3 フレーム（**set port auxiliaryvlan** *mod*[*/port*] **untagged** コマンドを使用）

（注）　Cisco IP Phone 7960 は、音声トラフィックで常にレイヤ 3 の IP precedence を 5 に設定します。

補助 VLAN 設定時の注意事項

ここでは、補助 VLAN 設定時の注意事項について説明します。

- 補助 VLAN ポートは、「通常の」トランク ポートとして扱われていない場合でも、機能上は 1 つのトランクです。補助 VLAN をポートに追加し、**set dot1q-all-tagged** コマンドがイネーブルのとき、**set dot1q-all-tagged** コマンドは、補助 VLAN が設定されるそのポートにネイティブ VLAN をタグ付けします。補助 VLAN が設定されたポートは、802.1Q トランクとして **show trunk** コマンドの出力結果に表示されませんが、**set dot1q-all-tagged** コマンドがイネーブルになると、そのポートは 802.1Q トランクのように機能します。
- 次のいずれかが当てはまる場合、IP Phone およびそれに接続する装置は同じ VLAN に属し、かつ同じ IP サブネットに属する必要があります。
  - 両者が同じフレーム タイプを使用する。
  - 電話機が 802.1p フレームを使用し、装置がタグなしフレームを使用する。

　　— 電話機がタグなしフレームを使用し、装置が 802.1p フレームを使用する。
　　— 電話機が 802.1Q フレームを使用し、補助 VLAN がネイティブ VLAN と同じである。

- IP Phone およびそれに接続する装置が同じ VLAN およびサブネットに属していても、使用するフレーム タイプが異なる場合には、両者は通信できません。同一サブネット内の装置間トラフィックがルーティングされないためです（ルーティングでは、フレーム タイプの相違は認められません）。
- 電話機のアクセス　ポートに接続された装置から受信されるトラフィックで使用するフレーム タイプを、スイッチ コマンドで設定することはできません。
- Release 6.2(1) 以降のソフトウェア リリースでは、ダイナミック ポートはネイティブ VLAN と補助 VLAN の 2 つの VLAN に属することができます。補助 VLAN の設定の詳細については、第 18 章「VMPS によるダイナミック ポート VLAN メンバーシップの設定」を参照してください。

補助 VLAN の設定

補助 VLAN を設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
補助 VLAN を設定します。	**set port auxiliaryvlan** *mod*[*/ports*] {*vlan* | **untagged** | **dot1p** | **none**}

次に、補助 VLAN に音声ポートを追加し、カプセル化タイプを指定し、また VLAN が音声関連の情報を含む CDP メッセージを送受信しないことを指定する例を示します。

```
Console> (enable) set port auxiliaryvlan 2/1-3 222
Auxiliaryvlan 222 configuration successful.
AuxiliaryVlan AuxVlanStatus Mod/Ports
------------- ------------- -------------------------
222           active        1/2,2/1-3
Console> (enable) set port auxiliaryvlan 5/7 untagged
Port 5/7 allows the connected device send and receive untagged packets and without
802.1p priority.
Console> (enable) set port auxiliaryvlan 5/9 dot1p
Port 5/9 allows the connected device send and receive packets with 802.1p priority.
Console> (enable) set port auxiliaryvlan 5/12 none
Port 5/12 will not allow sending CDP packets with Voice VLAN information.
Console> (enable)
```

デフォルトの設定は **none** です。表 53-6 に、**set port auxiliaryvlan** コマンドのキーワードとその意味を説明します。

表 53-6　キーワードの意味

キーワード	アクション
dot1p	電話機が 802.1p プライオリティ 5 でパケットを送信するように指定します。
untagged	電話機がタグなしパケットを送信するように指定します。
none	スイッチがそのポートからは補助 VLAN 情報を含む CDP パケットを送信しないように指定します。

補助 VLAN 設定の確認

補助 VLAN の設定ステータスを確認するには、イネーブル モードで次の作業を行います。

作業	コマンド
補助 VLAN の設定ステータスを確認します。	**show port auxiliaryvlan** {*vlan* | **untagged** | **dot1p** | **none**}

次に、補助 VLAN の設定ステータスを確認する例を示します。

```
Console> show port auxiliaryvlan 123
AuxiliaryVlan AuxVlanStatus Mod/Ports
------------- ------------- ------------------------
222           active        1/2,2/1-3
Console>
```

IP Phone が検出されるまで補助 VLAN をディセーブルにする

Release 8.3(1) 以降のソフトウェア リリースでは、IP Phone が検出されるまで補助 VLAN を確実にディセーブルにすることにより、補助 VLAN に対するセキュリティを実現しています。スイッチが IP Phone の存在を検出すると即座に補助 VLAN がイネーブルになります。

IP Phone の存在は、スイッチと電話の間での CDP パケット交換を通じて判断します。この検出方法は、インライン パワー式の IP Phone と壁面コンセントから電力を供給される IP Phone の両方で使用されます。

（注） 補助 VLAN ID がポート VLAN ID と同じ場合、または補助 VLAN ID が **none**、**dot1p**、または **untagged** と設定されている場合、この機能はポートに適用されません。コマンド エントリで補助 VLAN ID とポート VLAN ID が同じになった場合、この機能はディセーブルになり、「cdpverify feature on port <mod>/<port> is disabled.」という警告メッセージが表示されます。

補助 VLAN IP Phone 検出をイネーブルまたはディセーブルにするには、イネーブル モードで次の作業を行います（デフォルトはディセーブルです）。

作業	コマンド
補助 VLAN IP Phone 検出をイネーブルまたはディセーブルにします。	**set port auxiliaryvlan** *mod*[*/port*] {*vlan* | **untagged** | **dot1p** | **none**} [**cdpverify** {**enable** | **disable**}]

次に、補助 VLAN ID IP Phone 検出をイネーブルまたはディセーブルにする例を示します。

```
Console> (enable) set port auxiliaryvlan 3/1 50 cdpverify enable
AuxiliaryVlan Status   Mod/Ports
------------- -------- ---------------------------------------------------
50            active   3/1
Console> (enable)

Console> (enable) show config
This command shows non-default configurations only.
Use 'show config all' to show both default and non-default configurations.
.
.
.
!
#module 3 : 48-port 10/100BaseTX Ethernet
set port auxiliaryvlan 3/1 50 cdpverify enable
!
Console> (enable)
```

アクセス ゲートウェイの設定

ここでは、次の Catalyst 6500 シリーズ アクセス ゲートウェイ モジュールの設定に使用するコマンドについて説明します。

- アナログ ステーション ゲートウェイ ― 24 ポート FXS アナログ インターフェイス モジュール
- デジタル トランク ゲートウェイ ― 8 ポート T1/E1 PSTN インターフェイス モジュール

ポート音声インターフェイスの設定

ポート上で DHCP がイネーブルに設定されている場合、ポートはその他のすべての設定情報を TFTP サーバから取得します。ポート上で DHCP をディセーブルにするときは、次のように、いくつかの必須パラメータを指定する必要があります。

- Domain Name System（DNS; ドメイン ネーム システム）パラメータを指定しない場合、ソフトウェアはスーパバイザ エンジン上のシステム DNS コンフィギュレーションを使用して、ポートを設定します。
- 8 ポート T1/E1 PSTN インターフェイス モジュールのみの場合、各ポートに一意の IP アドレスが必要なので、一度に 1 つのポートしか指定できません。

DHCP、TFTP、および DNS サーバにポート音声インターフェイスを設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
DHCP、TFTP、および DNS サーバにポート音声インターフェイスを設定します。	**set port voice interface** *mod/port* **dhcp enable** [**vlan** *vlan*] **set port voice interface** *mod/port* **dhcp disable** {*ipaddrspec*} {**tftp** *ipaddr*} [**vlan** *vlan*] [**gateway** *ipaddr*] [**dns** [*ipaddr*] [*domain_name*]]

次に、DHCP、TFTP、および DNS サーバにポート音声インターフェイスを設定する例を示します。

```
Console> (enable) set port voice interface 7/1 dhcp enable
Port 7/1 DHCP enabled.

Console> (enable) set port voice interface 7/3 dhcp disable 171.68.111.41/24 tftp
173.32.43.11 dns 172.20.34.204 cisco.com
Port 7/3 dhcp disabled.
System DNS configurations applied.

Console> (enable) set port voice interface 7/4-6 dhcp enable vlan 3
Vlan 3 configuration successful
Ports 7/4-6 DHCP enabled.
Console> (enable)
```

ポート音声インターフェイスの設定表示

ポート音声インターフェイスの設定を表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
ポート音声インターフェイスの設定を表示します。	**show port voice interface** [*mod*[*/port*]]

次に、ポート音声インターフェイスの設定を表示する例を示します（出力は、24 ポート FXS アナログ インターフェイス モジュールの場合を示しています）。

```
Console> show port voice interface 5
Port     DHCP    MAC-Address       IP-Address      Subnet-Mask
-------- ------- ----------------- --------------- ---------------
 5/1-24  disable 00-10-7b-00-13-ea 10.6.15.158     255.255.255.0

Port     Call-Manager(s)   DHCP-Server     TFTP-Server     Gateway
-------- ----------------- --------------- --------------- ---------------
 5/1-24  10.6.15.155       -               10.6.15.155     -

Port     DNS-Server(s)     Domain
-------- ----------------- --------------------------------------------------
 5/1-24  12.2.2.1*         cisco.cisco.com
         7.7.7.7
(*): Primary
Console> (enable)
```

FDL 統計情報の表示

（注） Facilities Data Link（FDL）は、問題を診断し統計情報を収集するのに使用するリンク管理プロトコルです。

特定のポートの FDL 統計情報を表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
指定されたポートの FDL 統計情報を表示します。	**show port voice fdl** [*mod*[*/port*]]

次に、指定されたポートの FDL 統計情報を表示する例を示します。

```
Console> (enable) show port voice fdl 7/1-3
Port  ErrorEvents       ErroredSecond     SeverlyErroredSecond
      Last 15' Last 24h Last 15' Last 24h Last 15' Last 24h
----- -------- -------- -------- -------- -------- -----------
 7/1  17       18       19       20       21       22
 7/2  17       18       19       20       21       22
 7/3  17       18       19       20       21       22

Port  FailedSignalState FailedSignalSecond
      Last 15' Last 24h Last 15' Last 24h
----- -------- -------- -------- ---------
 7/1  37       38       39       40
 7/2  37       38       39       40
 7/3  37       38       39       40

Port         LES               BES               LCV
      Last 15' Last 24h Last 15' Last 24h Last 15' Last 24h
----- -------- -------- -------- -------- -------- --------
 7/1  41       48       49       50       53       54
 7/2  41       48       49       50       53       54
 7/3  41       48       49       50       53       54
Console> (enable)
```

表 53-7 に、**show port voice fdl** コマンドで（指定したポート タイプに応じて）出力される可能性のあるフィールドを説明します。

表 53-7　FDL フィールドの説明

フィールド	説明
ErrorEvents	エラー イベントのカウント
ErroredSecond	エラーの秒数
SeverelyErroredSecond	重大エラーの秒数
FailedSignalState	信号不良ステート エラーのカウント
FailedSignalSecond	エラー イベントのカウント
LES	検出された回線エラー秒数（Line Errored Seconds）
BES	検出されたバースト エラー秒数（Bursty Errored Seconds）
LCV	検出された伝送符号違反秒数（Line Code Violation）

各ポートの設定の表示

各ポートの設定を表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
各ポートの設定を表示します。	**show port** [*mod*[*/port*]]

ここでは、次のゲートウェイ モジュールに対する **show port** コマンドの出力について説明します。

- 8 ポート T1/E1 PSTN インターフェイス モジュール（p.53-27）
- 8 ポート T1/E1 PSTN インターフェイス モジュールのトランスコーディング / 会議用の設定（p.53-28）
- 24 ポート FXS アナログ インターフェイス モジュール（p.53-30）

8 ポート T1/E1 PSTN インターフェイス モジュール

Status フィールドには、各ポートのレイヤ 2 ステータスが表示されます。表示される可能性のある値は、notconnect、connected、disabled、および faulty です。次の出力例は、T1 モジュールに関するものです。E1 モジュールの場合も、ポート速度が 2.048 になる点を除いて出力内容は同じです。

```
Console> show port 7
Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 7/1                     connected  123        full   1.544 T1
 7/2                     connected  2          full   1.544 T1
 7/3                     disable    1          full   1.544 T1
 7/4                     connected  11         full   1.544 T1
 7/5                     connected  123        full   1.544 T1
 7/6                     connected  1          full   1.544 T1
 7/7                     faulty     2          full   1.544 T1
 7/8                     faulty     2          full   1.544 T1

Port     DHCP    MAC-Address       IP-Address      Subnet-Mask
-------- ------- ----------------- --------------- ---------------
 7/1     enable  00-10-7b-00-0a-58 172.20.34.68    255.255.255.0
 7/2     enable  00-10-7b-00-0a-59 172.20.34.70    255.255.255.0
 7/3     enable  00-10-7b-00-0a-5a 172.20.34.64    255.255.255.0
 7/4     enable  00-10-7b-00-0a-5b 172.20.34.66    255.255.255.0
 7/5     enable  00-10-7b-00-0a-5c 172.20.34.59    255.255.255.0
 7/6     enable  00-10-7b-00-0a-5d 172.20.34.67    255.255.255.0
 7/7     enable  00-10-7b-00-0a-5e (Port host processor not online)
 7/8     enable  00-10-7b-00-0a-5f (Port host processor not online)

Port     Call-Manager(s)   DHCP-Server     TFTP-Sever      Gateway
-------- ----------------- --------------- --------------- ---------------
 7/1     172.20.34.207*    172.20.34.207   172.20.34.207   -
         callm.cisco.com
 7/2     172.20.34.207     172.20.34.207   172.20.34.207   172.20.34.20
 7/3     172.20.34.207     172.20.34.207   172.20.34.207   -
 7/4     172.20.34.207     172.20.34.207   172.20.34.207   -
 7/5     172.20.34.207     172.20.34.207   172.20.34.207   -
 7/6     172.20.34.207     172.20.34.207   172.20.34.207   -
 7/7     (Port host processor not online)
 7/8     (Port host processor not online)

Port     DNS-Server(s)   Domain
-------- --------------- -------------------------------------------------
 7/1     172.20.34.207   cisco.com
 7/2     172.20.34.207*  int.cisco.com
         171.69.45.34
         172.78.111.132
 7/3     172.20.34.207   -
 7/4     172.20.34.207   -
 7/5     172.20.34.207   -
 7/6     172.20.34.207   -
 7/7     (Port host processor not online)
 7/8     (Port host processor not online)

Port     CallManagerState DSP-Type
-------- ---------------- --------
 7/1     registered       C549
 7/2     registered       C549
 7/3     registered       C549
 7/4     registered       C549
 7/5     registered       C549
 7/6     notregistered    C549
 7/7     (Port host processor not online)
 7/8     (Port host processor not online)
```

```
Port  NoiseRegen NonLinearProcessing
----- ---------- -------------------
 7/1  disabled   disabled
 7/2  disabled   disabled
 7/3  disabled   disabled
 7/4  disabled   disabled
 7/5  enabled    disabled
 7/6  disabled   enabled
 7/7  (Port host processor not online)
 7/8  (Port host processor not online)

(*): Primary
Console>
```

8 ポート T1/E1 PSTN インターフェイス モジュールのトランスコーディング / 会議用の設定

MTP（Media Termination Point）および Conf Bridge（Conference Bridge）は、どちらもポートのタイプを表します。MTP ポートを流れるコールに、トランスコーディングが適用されます。

次の例では、トランスコーディング ポートは MTP、会議ポートは Conf Bridge として出力されています。

```
Console> (enable) show port 7
Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 7/1                     notconnect 1            full 1.544 T1
 7/2                     notconnect 1            full 1.544 T1
 7/3                     connected  1            full 1.544 T1
 7/4                     connected  1            full 1.544 T1
 7/5                     connected  1            full 1.544 T1
 7/6                     connected  1            full 1.544 T1
 7/7                     enabled    1            full     - Conf Bridge
 7/8                     enabled    1            full     - MTP

Port     DHCP    MAC-Address       IP-Address      Subnet-Mask
-------- ------- ----------------- --------------- ---------------
 7/1     enable  00-10-7b-00-12-08 10.6.15.165     255.255.255.0
 7/2     enable  00-10-7b-00-12-09 10.6.15.166     255.255.255.0
 7/3     enable  00-10-7b-00-12-0a 10.6.15.167     255.255.255.0
 7/4     enable  00-10-7b-00-12-0b 10.6.15.168     255.255.255.0
 7/5     enable  00-10-7b-00-12-0c 10.6.15.169     255.255.255.0
 7/6     enable  00-10-7b-00-12-0d 10.6.15.170     255.255.255.0
 7/7     enable  00-10-7b-00-12-0e 10.6.15.171     255.255.255.0
 7/8     enable  00-10-7b-00-12-0f 10.6.15.172     255.255.255.0

Port     Call-Manager(s)   DHCP-Server     TFTP-Server     Gateway
-------- ----------------- --------------- --------------- ---------------
 7/1     10.6.15.155       10.6.15.155     10.6.15.155     -
 7/2     10.6.15.155       10.6.15.155     10.6.15.155     -
 7/3     10.6.15.155       10.6.15.155     10.6.15.155     -
 7/4     10.6.15.155       10.6.15.155     10.6.15.155     -
 7/5     10.6.15.155       10.6.15.155     10.6.15.155     -
 7/6     10.6.15.155       10.6.15.155     10.6.15.155     -
 7/7     10.6.15.155       10.6.15.155     10.6.15.155     -
 7/8     10.6.15.155       10.6.15.155     10.6.15.155     -

Port     DNS-Server(s)     Domain
-------- ----------------- ------------------------------------------------
 7/1     -                 -
 7/2     -                 -
 7/3     -                 -
 7/4     -                 -
 7/5     -                 -
 7/6     -                 -
 7/7     -                 -
 7/8     -                 -
```

```
Port     CallManagerState DSP-Type
-------- ---------------- --------
 7/1     registered       C549
 7/2     registered       C549
 7/3     registered       C549
 7/4     registered       C549
 7/5     registered       C549
 7/6     registered       C549
 7/7     registered       C549
 7/8     registered       C549

Port  NoiseRegen NonLinearProcessing
----- ---------- -------------------
 7/1  enabled    enabled
 7/2  enabled    enabled
 7/3  enabled    enabled
 7/4  enabled    enabled
 7/5  enabled    enabled
 7/6  enabled    enabled
 7/7  disabled   disabled
 7/8  disabled   disabled
Console> (enable)
```

24 ポート FXS アナログ インターフェイス モジュール

次の例では、すべてのポートの [Type] フィールドが FXS であり、かつ同一モジュールのすべてのポートが同一 VLAN に属する必要があります。

```
Console> (enable) show port 3
Port  Name                 Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 3/1                     onhook     1            full   64k FXS
 3/2                     onhook     1            full   64k FXS
 3/3                     onhook     1            full   64k FXS
 3/4                     onhook     1            full   64k FXS
 3/5                     onhook     1            full   64k FXS
 3/6                     onhook     1            full   64k FXS
 3/7                     onhook     1            full   64k FXS
 3/8                     offhook    1            full   64k FXS
 3/9                     offhook    1            full   64k FXS
 3/10                    onhook     1            full   64k FXS
 3/11                    onhook     1            full   64k FXS
 3/12                    onhook     1            full   64k FXS
 3/13                    onhook     1            full   64k FXS
 3/14                    onhook     1            full   64k FXS
 3/15                    onhook     1            full   64k FXS
 3/16                    onhook     1            full   64k FXS
 3/17                    onhook     1            full   64k FXS
 3/18                    onhook     1            full   64k FXS
 3/19                    onhook     1            full   64k FXS
 3/20                    onhook     1            full   64k FXS
 3/21                    onhook     1            full   64k FXS
 3/22                    onhook     1            full   64k FXS
 3/23                    onhook     1            full   64k FXS
 3/24                    onhook     1            full   64k FXS

Port     DHCP    MAC-Address       IP-Address      Subnet-Mask
-------- ------- ----------------- --------------- ---------------
 3/1-24  enable  00-10-7b-00-13-e4 172.20.34.50    255.255.255.0

Port     Call-Manager(s)   DHCP-Server     TFTP-Sever      Gateway
-------- ----------------- --------------- --------------- ---------------
 3/1-24  172.20.34.207     172.20.34.207   172.20.34.207   -

Port     DNS-Server(s)     Domain
-------- ----------------- ------------------------------------------------
 3/1-24  172.20.34.207*    cisco.com
         172.34.23.111

Port     CallManagerState DSP-Type
-------- ---------------- --------
 3/1-24  registered       C549

Port     ToneLocal     Impedance InputGain(dB) OutputAtten(dB)
-------- ------------- --------- ------------- ---------------
 3/1-24  northamerica  0         0             0

Port     RingFreq Timing    Timing         Timing    Timing
         (Hz)     Digit(ms) InterDigit(ms) Pulse(ms) PulseDigit(ms)
-------- -------- --------- -------------- --------- --------------
 3/1-24  20       100       100            0         0
(*): Primary
Console> (enable)
```

アクティブ コール情報の表示

ポート上のアクティブ コールに関する情報を表示するには、**show port voice active** コマンドを使用します。8 ポート T1/E1 PSTN インターフェイス モジュールの場合は 1 ポートにつき最大 8 コールありますが、24 ポート FXS アナログ ステーション インターフェイス モジュールの場合は 1 ポートにつき 1 コールだけです。

アクティブ コール情報を表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
アクティブ コール情報を表示します。	**show port voice active** [*mod/port*] [**all** | **call** | **conference** | **transcode**] [*ipaddr*]

パラメータを指定せずに **show port voice active** コマンドを入力すると、システム内のすべてのコール（通常のコール、会議コール、およびトランスコーディング コール）が表示されます。各出力フィールドについて、以下に説明します。

- Type ― [call] という表記は、24 ポート FXS アナログ インターフェイス モジュールおよび 8 ポート PSTN インターフェイス モジュールのコールを表します。

  8 ポート T1/E1 PSTN インターフェイスをトランスコーディングおよび / または会議用に設定している場合、Type フィールドには、会議コールについては [conferencing]、トランスコーディング コールについては [transcoding] が表示されます。
- Conference-ID、Transcoding-ID、および Party-ID は、トランスコーディングおよび / または会議用の 8 ポート T1/E1 PSTN インターフェイスだけに適用されます。

次の例では、システム内のすべてのコールを表示しています。

```
Console> show port voice active
Port  Type         Total Conference-ID/ Party-ID IP-Address
                         Transcoding-ID
----- ------------ ----- -------------- -------- ---------------
 3/1  call         1     -              -        199.22.25.254
 3/2  call         1     -              -        172.225.25.54
 4/5  call         3     -              -        165.34.234.111
                                                 172.32.34.12
                                                 198.96.23.111
 3/8  conferencing 2     1              1        255.255.255.241
                                        2        173.23.13.42
                                        3        198.97.123.98
                                        5        182.34.54.26
                         2              1        199.22.25.25
                                        3        182.34.54.2
                                        6        121.43.23.43
 3/2  call         1     -              -        172.225.25.54
 3/8  transcoding  1     1              1        255.255.255.241
                                        2        183.32.43.3
```

次に、ポートに関する詳細なコール情報を表示する例を示します（この例ではモジュールだけを指定し、そのモジュール上のすべてのポートに関する詳細なコール情報を表示しています）。

```
Console> show port voice active 3/2
Port 3/2:
Channel #1:
  Remote IP address                       : 165.34.234.111
  Remote UDP port                         : 124
  Call state                              : Ringing
  Codec Type                              : G.711
  Coder Type Rate                         : 35243
  Tx duration                             : 438543 sec
  Voice Tx duration                       : 34534 sec
  ACOM Level Current                      : 123213
  ERL Level                               : 123 dB
  Fax Transmit Duration                   : 332433
  Hi Water Playout Delay                  : 23004 ms
  Logical If index                        : 4
  Low water playout delay                 : 234 ms
  Receive delay                           : 23423 ms
  Receive bytes                           : 2342342332423
  Receive packets                         : 23423423402384
  Transmit bytes                          : 23472377
  Transmit packets                        : 94540
Channel #2:
  Remote IP address                       : 165.34.234.112
  Remote UDP port                         : 125
  Call state                              : Ringing
  Codec Type                              : G.711
  Coder Type Rate                         : 35243
  Tx duration                             : 438543 sec
  Voice Tx duration                       : 34534 sec
  ACOM Level Current                      : 123213
  ERL Level                               : 123 dB
  Fax Transmit Duration                   : 332433
  Hi Water Playout Delay                  : 23004 ms
  Logical If index                        : 4
  Low water playout delay                 : 234 ms
  Receive delay                           : 23423 ms
  Receive bytes                           : 2342342332423
  Receive packets                         : 23423423402384
  Transmit bytes                          : 23472377
  Transmit packets                        : 94540
Channel #3:
.
（テキスト出力は省略）
.
Console>
```

次に、指定された IP アドレスにおける特定のコールを表示する例を示します。

```
Console> show port voice active 3/2 171.69.67.91
  Remote IP address                       : 171.69.67.91
  Remote UDP port                         : 125
  Call state                              : Ringing
  Codec Type                              : G.711
  Coder Type Rate                         : 35243
  Tx duration                             : 438543 sec
  Voice Tx duration                       : 34534 sec
  ACOM Level Current                      : 123213
  ERL Level                               : 123 dB
  Fax Transmit Duration                   : 332433
  Hi Water Playout Delay                  : 23004 ms
  Logical If index                        : 4
  Low water playout delay                 : 234 ms
  Receive delay                           : 23423 ms
  Receive bytes                           : 2342342332423
  Receive packets                         : 23423423402384
  Transmit bytes                          : 23472377
  Transmit packets                        : 94540
Console>
```

Cisco IP Phone 7960 における QoS の設定

ここでは、Cisco IP Phone 7960 における QoS について説明します。

- Cisco IP Phone 7960 における QoS の概要（p.53-33）
- Cisco IP Phone 7960 における QoS の設定（p.53-34）

（注）　自動 QoS の使用方法については、第 50 章「自動 QoS の使用」を参照してください。

（注）　自動音声設定の使用方法については、「SmartPort の使用方法」（p.53-41）を参照してください。

Cisco IP Phone 7960 における QoS の概要

（注）　Cisco IP Phone 7960 は、電話機が生成する音声トラフィックに対し、レイヤ 3 IP precedence およびレイヤ 2 CoS を常に 5 に設定します。電話機が生成する音声トラフィックのレイヤ 3 IP precedence およびレイヤ 2 CoS 値は、設定することができません。

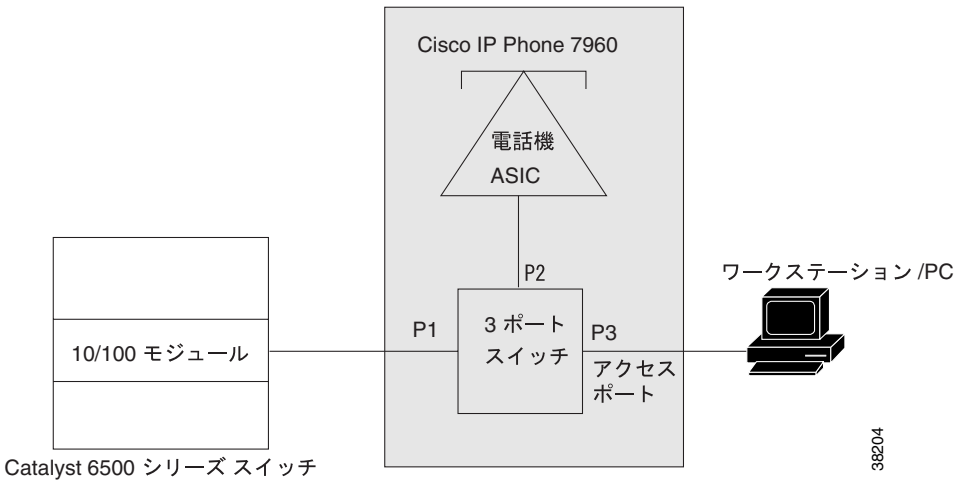
Cisco IP Phone 7960 アクセス ポート（図 53-5 を参照）は、*trusted* または *untrusted* モードのいずれかに設定できます。

untrusted（信頼性がない）モードは、アクセス ポート経由で受信する 802.1Q または 802.1p フレームのすべてのトラフィックが、設定されたレイヤ 2 CoS 値でマークされます。デフォルトのレイヤ 2 CoS 値は 0 です。電話機が Cisco LAN スイッチに接続されている場合は、untrusted モードがデフォルトになります。

trusted（信頼性がある）モードは、アクセス ポート経由で受信するすべてのトラフィックが、そのまま電話機のスイッチを通過します。電話機が Cisco LAN スイッチに接続されていない場合は、trusted モードがデフォルトになります。

802.1Q または 802.1p 以外のフレーム タイプのトラフィックは、アクセス ポートの信頼状態とは無関係に、そのまま電話機のスイッチを通過します。

図 53-5　IP Phone ポート上での QoS の設定



Cisco IP Phone 7960 における QoS の設定

ここでは、Cisco IP Phone 7960 における QoS の設定手順について説明します。

- 電話機アクセス ポートの信頼モードの設定（p.53-34）
- 電話機アクセス ポートの CoS 値の設定（p.53-35）
- 電話機アクセス ポートの QoS 設定の確認（p.53-35）

電話機アクセス ポートの信頼モードの設定

電話機アクセス ポートの信頼モードを設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
電話機アクセス ポートの信頼モードを設定します。	**set port qos** *mod/ports...***trust-ext** {**trusted** | **untrusted**}

次に、電話機のアクセス ポートを trusted モードに設定する例を示します。

```
Console> (enable) set port qos 3/7 trust-ext trusted
Port in the phone device connected to port 3/7 is configured to be trusted.
Console> (enable)
```

次に、電話機のアクセス ポートを untrusted モードに設定する例を示します。

```
Console> (enable) set port qos 3/7 trust-ext untrusted
Port in the phone device connected to port 3/7 is configured to be untrusted.
Console> (enable)
```

電話機アクセス ポートの CoS 値の設定

電話機アクセス ポートの CoS 値を設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
電話機アクセス ポートの CoS 値を設定します。	**set port qos** *mod/ports* **cos-ext** *cos_value*

次に、untrusted モードの電話機アクセス ポートが使用するレイヤ 2 CoS 値を設定する例を示します。

```
Console> (enable) set port qos 2/1 cos-ext 3
Port 2/1 qos cos-ext set to 3.
Console> (enable)
```

電話機アクセス ポートの QoS 設定の確認

電話機アクセス ポートの QoS 設定を確認するには、イネーブル モードで次の作業を行います。

作業	コマンド
電話機アクセス ポートの QoS 設定を確認します。	**show port qos** [*mod*[*/port*]]

次に、電話機アクセス ポートの QoS 設定を確認する例を示します。

```
Console> (enable) show port qos 3/4
(テキスト出力は省略)
Port  Ext-Trust Ext-Cos
----- --------- -------
 3/4  untrusted       0
(テキスト出力は省略)
```

信頼境界の設定によるポート セキュリティの強化

ここでは、信頼境界について説明します。この機能を使用すると、スイッチ ポートの QoS **trust-cos** 設定を使用するために、ユーザがネットワークに接続された Cisco IP Phone から PC を外し、スイッチ ポートに直接 PC を接続しても、セキュリティの問題が発生するのを防ぐことができます。

次の項で信頼境界について説明します。

サポート対象の Cisco IP Phone

信頼境界機能に対応している Cisco IP Phone は、次のとおりです。

- Cisco IP Phone 7910
- Cisco IP Phone 7935
- Cisco IP Phone 7940
- Cisco IP Phone 7960

QoS および Cisco IP Phone の設定

Cisco IP Phone は、Catalyst 6500 シリーズ スイッチのポートに直接接続されます。通常、電話機から発信されてスイッチに入るトラフィックは、802.1Q ヘッダーを使用してタグでマーキングされます。このヘッダーは、VLAN 情報と 3 ビットの CoS フィールドで構成されます。CoS によって、そのパケットのプライオリティが決まります。ほとんどの Cisco IP Phone の設定では、電話機からスイッチに入るトラフィックは信頼され、音声トラフィックがネットワーク内の他のタイプのトラフィックよりも優先されます。電話機が接続されているスイッチ ポートは、**trust-cos** に設定されています。したがって、ポートは、そのポートに到達するすべてのパケットの CoS ラベルを信頼します。

QoS、Cisco IP Phone、PC の設定

Cisco IP Phone は PC またはワークステーションに接続できます。この電話機にはハブが内蔵されており、PC、電話機、スイッチ ポートから着信するトラフィックに対応できます。PC からのトラフィックと電話機からのトラフィックを区別するために、3 ビットの CoS ラベルが使用されます。

適切なラベルが生成されるようにするには、電話機に QoS 機能を設定する必要があります。QoS 設定情報は、スイッチから CDP を使用して電話機に送信されます。QoS の設定によって、電話機の信頼状態と分類情報（Ext-Cos）が決まります。電話機は次の 2 つの信頼状態をサポートしています。

- trusted
- untrusted ― 新しい CoS 値（Ext-Cos）でマーキングされます。

電話機が trusted モードの場合、PC が作成するラベルはすべて、電話機を通じて直接スイッチに送信され、変更されません。電話機が untrusted モードの場合、PC から着信するトラフィックはすべて、Ext-Cos 値でマーキングされてから、スイッチに送信されます。

電話機に接続されている PC またはワークステーションのほとんどはパケットにタグを付けることができません。このような場合、電話機を通じて PC からスイッチに入るトラフィックには、その電話機に設定されている「デフォルトの ext-cos」が付けられます。

パケットにタグを付ける機能を持つ PC もあります。Windows 2000 が稼働している PC は、任意のプライオリティの 802.1Q フレームを送信するように設定できます。この問題を解決するには、電話機を untrusted に設定しなければなりません。これによって、PC から着信するすべてのトラフィックに適切なプライオリティがマーク付けされます。

信頼境界を使用すると、ユーザがネットワークから電話機を外して PC を直接スイッチ ポートに差し込むことによって、スイッチ上の trust-cos 設定値を利用することを防止できます。信頼境界機能は、CDP を使用して、電話機がポートに接続されているかどうかを検出します。電話機がポートに直接接続されていない場合は、この機能によって、ポートは自動的に untrusted に設定されるので、セキュリティの問題は生じません。

信頼境界は、コンフィギュレーション コマンドを使用して新たな信頼タイプを作成することによって実現されます。このコマンドを使用すると、ポートに接続されているデバイスに基づいて、ポートの信頼タイプを設定できます。Cisco IP Phone の場合は、信頼タイプを「**trust-device ciscoipphone**」に設定します。

信頼境界の設定上の注意事項

ここでは、信頼境界を設定する際の注意事項について説明します。

- Common Open Policy Service（COPS）の考慮事項

  COPS は、適用される QoS パラメータに直接影響します。ポートには、ローカル ポリシーまたは COPS ポリシーを適用できます。この設定によって、ポートが QoS 設定情報をローカル コンフィギュレーションから取得するか、COPS サーバから取得するかが決まります。COPS が、あるポートに対してイネーブルに設定され、グローバルにもイネーブルに設定されている場合は、COPS サーバによって指定されたポリシーが適用されます。COPS がディセーブルになっている場合や実行時のポリシーがローカルである場合は、ローカル コンフィギュレーションの QoS ポリシーが適用されます。拡張信頼境界機能を使用すると、ポートに適用される「ローカル」ポリシーが無効になります。

- QoS 設定のサポート

  すべての QoS ポート信頼設定値（**trust-cos**、**trust-ipprec**、**trust-dscp**）がサポートされていますが、Cisco IP Phone ネットワークには、**trust-cos** を使用する必要があります。

- システム ログ メッセージ

  信頼境界は、新たに追加された QoS Syslog を使用して、ポートの信頼状態の変更を通知し、不適切な設定について警告します。これらの Syslog を見るためには、QoS ロギング レベルを 5 に設定します（**set logging level qos 5**）。デフォルトの設定値は 3 です。Syslog については、『*Catalyst 6500 Series System Message Guide*』を参照してください。

- 最終的な実行ポート信頼値

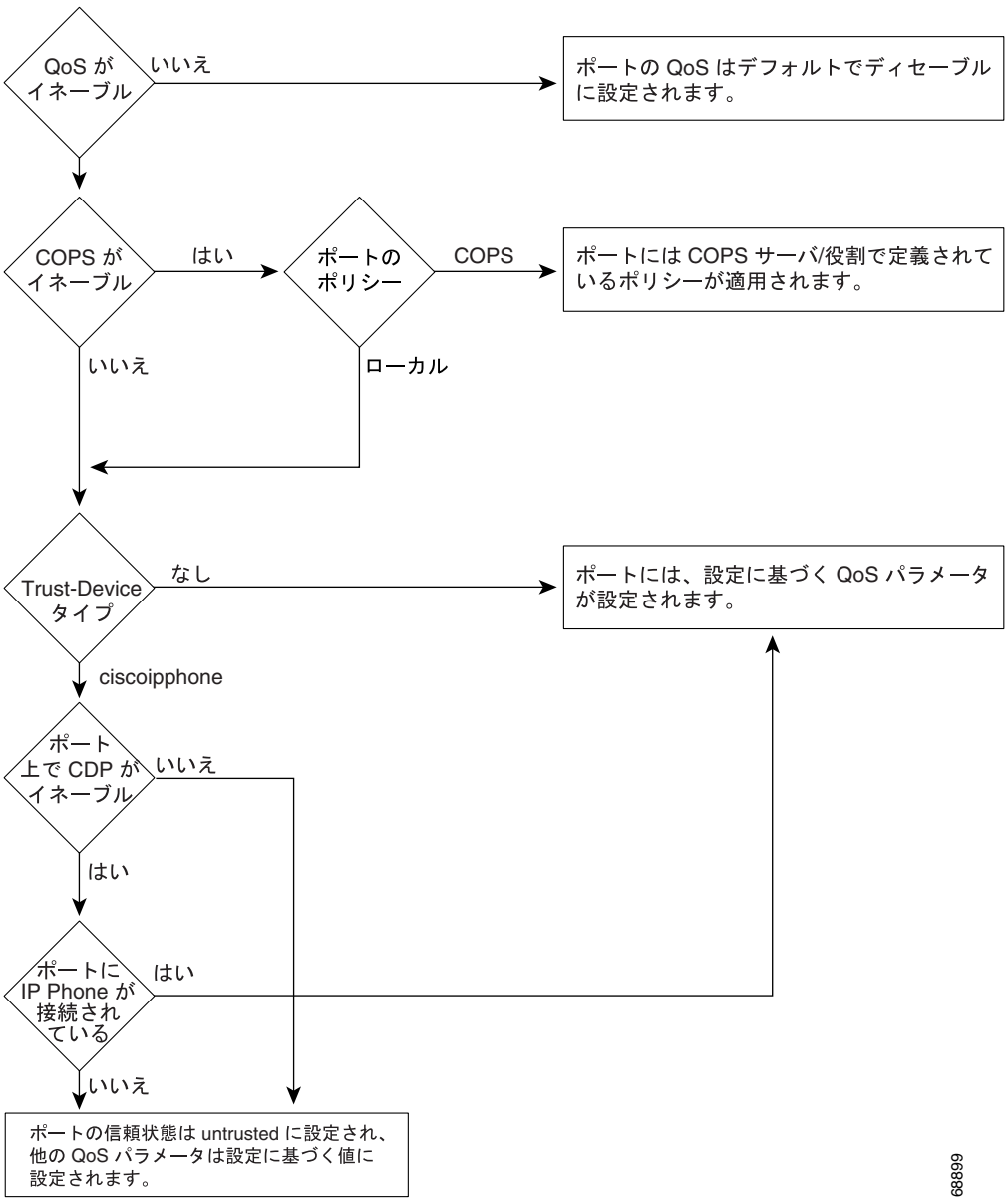
  ポートの最終的な実行信頼値は、次の事項に基づいて決まります。

  - 信頼境界の設定
  - ポートへの電話機の接続
  - QoS の設定
  - COPS の設定

  信頼境界をイネーブルにするには、QoS をイネーブルにするとともに、CDP をグローバルとポート単位の両方でイネーブルに設定し、バージョン 2 モードで稼働する必要があります。また、COPS をローカル ポリシーに設定するか（COPS のデフォルト）、またはディセーブル（COPS のデフォルト）に設定する必要があります。ポート上で **ciscoipphone** が trust-device に設定されていれば、この機能はイネーブルになり、Cisco IP Phone がポートに接続されているかどうかが検出され、トラスト値が設定されます。

  最終的なポート信頼値の判別については、図 53-6 を参照してください。

図 53-6　ポートの最終的な信頼値



信頼境界の設定

ここでは、信頼境界機能の設定手順を説明します。

- デフォルト設定（p.53-38）
- Cisco IP Phone の信頼デバイス指定（p.53-39）
- ポートの trust-device ステートの確認（p.53-39）

デフォルト設定

すべてのポートに対するデフォルト設定値は **trust-device none** です。

Cisco IP Phone の信頼デバイス指定

Cisco IP Phone を信頼デバイスとして指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
Cisco IP Phone を信頼デバイスとして指定します。	**set port qos** *mod/ports...***trust-device** [**ciscoipphone** | **none**]

次に、ポート 4/1 上の Cisco IP Phone だけを信頼デバイスに設定する例を示します。

```
Console> (enable) set port qos 4/1 trust-device ciscoipphone
Port 4/1 set to only trust device of type ciscoIPPhone.
Console> (enable)
```

次に、ポート 4/1 上で信頼デバイスをディセーブルにする例を示します。

```
Console> (enable) set port qos 4/1 trust-device none
Port 4/1 trust device feature disabled.
Console> (enable)
```

ポートの trust-device ステートの確認

ポートの trust-device ステートを確認するには、ユーザ モードで次の作業を行います。

作業	コマンド
ポートの trust-device ステートを確認します。	**show port qos** [*mod*[/*port*]]

信頼境界がアクティブな状態の場合、実行時のポートの信頼状態は電話機が接続されているかどうかによって異なります。

（注） 電話機がスイッチ ポートから外された場合、ポートが untrusted ステートに変更されるのに、わずかなコンバージェンス時間がかかります（最大 15 秒）。

次に、ポート 4/1 上の trust-device ステートおよび trust ステートを確認する例を示します。

```
Console> (enable) show port qos 4/1

（テキスト出力は省略）

Port  TxPort Type  RxPort Type  Trust Type   Trust Type    Def CoS Def CoS
                                 config       runtime       config  runtime
----- ------------ ------------ ------------ ------------- ------- -------
 4/1        1p3q1t       1p1q0t    trust-cos    trust-cos*       0       0

Port  Ext-Trust Ext-Cos Trust-Device

----- --------- ------- ------------

 4/1  untrusted       0 ciscoIPPhone


(*)Runtime trust type set to untrusted.

Config:
Port  ACL name                          Type
----- -------------------------------- ----
No ACL is mapped to port 4/1.

Runtime:
Port  ACL name                          Type
----- -------------------------------- ----
No ACL is mapped to port 4/1.
Console> (enable)
```

SmartPort の使用方法

SmartPort 機能は、Catalyst 6500 シリーズ スイッチ上で音声設定を簡略化する 2 つのマクロで構成されています。SmartPort マクロは、音声ポート用の推奨 Architecture for Voice, Video, and Integrated Data（AVVID）の実装に必要なすべての音声設定タスクを取り扱います。

SmartPort は、Cisco IP Phone 79xx シリーズと Cisco SoftPhone を使用して構築された音声ネットワークに照準を絞っています。SmartPort では、**ciscoipphone** または **ciscosoftphone** キーワードを使用して、特定ポートに必要な音声パラメータのタイプを指定するマクロを起動します。

ここでは、SmartPort について説明します。

SmartPort マクロの概要

ciscoipphone または **ciscosoftphone** キーワードを使用してポート上で SmartPort マクロを実行すると、次の機能が実装されます。

- ポートがイネーブルになります。
- CDP、STP、および VTP についてレイヤ 2 プロトコルがディセーブルになります。
- ポートのメンバーシップが [static] に設定されます。
- ポート上で **set port host** コマンドが実行されます。
- 指定したデータ VLAN がポートと対応付けられます。
- グローバル自動 QoS コマンドが実行されます。

ciscoipphone キーワードをポート上で実行すると、上述の機能以外に、次の機能も実装されます。

- 指定した補助 VLAN がポートと対応付けられます。
- インライン パワーがイネーブルになります。
- CDP がグローバルに、またポート上でイネーブルになります。
- CDP がバージョン v2 に設定されます。
- Cisco IP Phone 用のポートベース自動 QoS コマンドが実行されます。

ciscosoftphone キーワードをポート上で実行すると、上述の機能以外に、次の機能も実装されます。

- ポートの補助 VLAN が [none] に設定されます。
- Cisco SoftPhone 用のポートベース自動 QoS コマンドが実行されます。

SmartPorts ― Cisco IP Phone

通常の設定では、Cisco IP Phone 79xx は、Catalyst スイッチのポートに直接接続します。必要に応じて PC を電話機に接続し、スイッチのホップとして使用できます。

一般的に電話機から発信されてスイッチに入るトラフィックは、802.1Q/p ヘッダーを使用してタグでマーキングされます。ヘッダーには、VLAN 情報と CoS 3 ビット フィールドが含まれています。CoS によって、そのパケットのプライオリティが決まります。スイッチは、CoS フィールドを使用して PC のトラフィックと電話機のトラフィックを区別します。スイッチは、DSCP フィールドを同じ用途に使用することもできます。

Cisco IP Phone 79xx の通常の設定では、電話機から発信されてスイッチに入るトラフィックは信頼されます。ポートの信頼状態を trust-cos に設定して、音声トラフィックをネットワークのその他のトラフィック タイプより適切に優先させます。

Cisco IP Phone 79xx には内蔵スイッチがあり、PC、電話機およびスイッチ ポートから着信するトラフィックをミックスします。Cisco IP Phone 79xx には設定が必要な信頼機能と分類機能があります。

IP Phone を接続するポートは、いくつかの機能をイネーブルまたはディセーブルに設定する必要があります。SmartPort によって、必ず必要な機能がイネーブルに設定されるようになります。このような機能の大部分は、**set port host** コマンドを実行すると実装されます（チャネルのディセーブル化、PortFast のイネーブル化など）。QoS が機能するためには、VLAN と補助 VLAN をポート上に設定する必要があります。インライン パワーはイネーブルに設定する必要があり（使用可能な場合）、信頼境界機能が機能するためには、CDP をイネーブルに設定しなければなりません。QoS 設定は自動 QoS 機能によって処理されます（第 50 章「自動 QoS の使用」を参照）。

SmartPort ― Cisco SoftPhone

Cisco SoftPhone は標準の PC 上で実行するソフトウェア製品で、IP Phone をエミュレートします。Cisco SoftPhone と Cisco IP Phone 79xx の主な違いは、Cisco SoftPhone は DSCP を介してその音声トラフィックをマーキングするのに対し、Cisco IP Phone 79xx は CoS を介してトラフィックをマーキングする点です。スイッチ上の QoS 設定は、ポートに入るトラフィックのレイヤ 3 マーキングを信頼することで、この動作に対応します。それ以外のすべての動作は Cisco IP Phone 79xx と同じです。CDP などの一部の機能は、信頼境界が Cisco SoftPhone をサポートしないので、イネーブルにする必要がありません。

SmartPort 設定時の注意事項および制限事項

ここでは、SmartPort の設定時の注意事項および制限事項について説明します。

- サポート対象の電話機（p.53-43）
- CDP の依存関係（p.53-43）
- EtherChannel の考慮事項（p.53-43）
- PFC/PFC2 のサポート（p.53-43）
- モジュールのサポート（p.53-43）

サポート対象の電話機

ciscoipphone キーワードを指定して SmartPort を使用する場合、一部の QoS 設定で、電話機固有の設定（trust-ext、ext-cos）が必要です。この設定は、次の電話機のみでサポートされています。Cisco IP Phone 7910、Cisco IP Phone 7940、Cisco IP Phone 7960、および Cisco IP Phone 7935 です。ただし、**ciscoipphone** キーワードはこれらのモデルに限定されません。どの電話機も、スイッチに設定したその他すべての QoS 設定の恩恵を受けられます。

Cisco SoftPhone は、**ciscoipsoftphone** キーワードによってサポートされています。

CDP の依存関係

Cisco IP Phone に QoS 設定と信頼境界を設定するには、ポート上で CDP のバージョン 2 以降をイネーブルにします。

CDP は、**ciscoipphone** QoS 設定に対してだけイネーブルにする必要があり、CDP は SmartPhone 機能の他のコンポーネントには作用しません。

EtherChannel の考慮事項

SmartPort コマンドはチャネリングをサポートしていません。

PFC/PFC2 のサポート

ciscoipphone キーワードには、Policy Feature Card（PFC; ポリシー フィーチャ カード）や PFC2 は不要です。**ciscosoftphone** キーワードには、PFC や PFC2 が必要です。

モジュールのサポート

ciscoipphone キーワードは、10/100 および 10/100/1000 イーサネット ポート上でのみサポートされています。

一方、**ciscosoftphone** キーワードは、すべてのイーサネット ポート上でサポートされています。

SmartPort の CLI インターフェイス

ここでは、SmartPort の CLI インターフェイスについて説明します。

コマンドについて

ciscoipphone または **ciscosoftphone** キーワード、およびデータ VLAN を指定する必要があります。補助 VLAN の指定は **ciscoipphone** キーワードのオプションです。Remote SPAN（RSPAN）とプライベート VLAN はサポートされていません。SmartPort のコマンド構文は次のとおりです。

```
Console> (enable) set port macro
Usage: set port macro <mod/ports..> ciscoipphone vlan <vlan> [auxvlan <auxvlan>]
       set port macro <mod/ports..> ciscosoftphone vlan <vlan>
Console> (enable)
```

(注)　**set port macro** *mod/ports...* **ciscoipphone vlan** *vlan* [**auxvlan** *auxvlan*] コマンドは、ポート上の「cdpverify」機能をイネーブルにします。

ciscoipphone コマンドの出力

ciscoipphone キーワードを入力すると、次のような出力が表示されます（補助 VLAN の指定はオプションです）。

```
Console> (enable) set port macro 3/1 ciscoipphone vlan 2 auxvlan 3
Port 3/1 enabled.
Layer 2 protocol tunneling disabled for CDP STP VTP on port(s) 3/1.
Port 3/1 vlan assignment set to static.
Spantree port fast start option set to default for ports 3/1.
Port(s) 3/1 channel mode set to off.

Warning: Connecting Layer 2 devices to a fast start port can cause
temporary spanning tree loops. Use with caution.

Spantree port  3/1 fast start enabled.
Dot1q tunnel feature disabled on port(s)  3/1.
Port(s)  3/1 trunk mode set to off.
VLAN  Mod/Ports
---- ----------------------
2     2/1
      3/1
      16/1
AuxiliaryVlan Status   Mod/Ports
------------- --------
------------------------------------------------------
3             inactive 3/1

Vlan 3 is not active.
Inline power for port 3/1 set to auto.

CDP enabled globally
CDP enabled on port 3/1.
CDP version set to v2
........
All ingress and egress QoS scheduling parameters configured on all ports.
CoS to DSCP, DSCP to COS, IP Precedence to DSCP and policed dscp maps
configured.  Global QoS configured.
Port 3/1 ingress QoS configured for Cisco IP Phone.
Macro completed on port 3/1.
Console> (enable)
```

補助 VLAN を指定しなかった場合は、次の警告メッセージが表示されます。

```
Console> (enable) set port macro 3/1 ciscoipphone vlan 2
Warning:  All inbound QoS tagging information will be lost as no auxiliary
vlan was specified.
Do you want to continue (y/n) [n]?
```

ciscosoftphone コマンドの出力

ciscosoftphone キーワードを入力すると、次のような出力が表示されます

```
Console> (enable) set port macro 3/1 ciscosoftphone vlan 32
Port 3/1 enabled.
Layer 2 protocol tunneling disabled for CDP STP VTP on port(s) 3/1.
Port 3/1 vlan assignment set to static.
Spantree port fast start option set to default for ports 3/1.
Port(s) 3/1 channel mode set to off.

Warning: Connecting Layer 2 devices to a fast start port can cause
temporary spanning tree loops. Use with caution.

Spantree port  3/1 fast start enabled.
Dot1q tunnel feature disabled on port(s)  3/1.
Port(s)  3/1 trunk mode set to off.
Vlan 32 configuration successful
VLAN 32 modified.
VLAN 2 modified.
VLAN  Mod/Ports
---- ----------------------
32    3/1
      16/1
Port 3/1 will not send out CDP packets with AuxiliaryVlan information.
Executing autoqos........
All ingress and egress QoS scheduling parameters configured on all ports.
CoS to DSCP, DSCP to COS, IP Precedence to DSCP and policed dscp maps
configured.  Global QoS configured.
Port 3/1 ingress QoS configured for Cisco Softphone.
Macro completed on port 3/1.
Console>> (enable)
```

SmartPort ステートメントの詳細

ここでは、SmartPort マクロ ステートメントの詳細を示します。

- ciscoipphone マクロ ステートメント（p.53-45）
- ciscosoftphone マクロ ステートメント（p.53-46）

ciscoipphone マクロ ステートメント

ciscoipphone マクロ コマンドを入力すると、次のような設定になります。

```
set port macro mod/port ciscoipphone vlan vlan [auxvlan auxvlan]
-----------------------------------------------------------
set port enable mod/port
set port l2protocol-tunnel mod/port cdp stp vtp disable
set port membership mod/port static
set port host mod/port
set vlan mod/port vlan
set port auxiliaryvlan mod/port auxvlan  (set to none if not specified)
set port inlinepower mod/port auto (if supported by module)
set cdp enable
set cdp enable mod/port
set cdp version v2
set qos autoqos
set port qos mod/port autoqos voip ciscoipphone
```

ciscosoftphone マクロ ステートメント

ciscosoftphone マクロ コマンドを入力すると、次のような設定になります。

```
set port macro mod/port ciscosoftphone vlan vlan
------------------------------------------------------------
set port enable mod/port
set port l2protocol-tunnel mod/port cdp stp vtp disable
set port membership mod/port static
set port host mod/port
set vlan mod/port vlan
set port auxiliaryvlan mod/port none
set qos autoqos
set port qos mod/port autoqos voip ciscosoftphone
```

ネットワークでの SmartPort の使用方法

インターフェイスとそのインターフェイスに接続しているデバイスに応じて、さまざまな自動音声マクロを実行する必要があります。各ポートについて、該当するキーワードを指定してポートベースのマクロ コマンドを実行します（表 53-8 を参照）。

表 53-8　自動音声設定キーワードの使用方法

キーワード	ポート タイプ
ciscoipphone	Cisco IP Phone 79xx だけに接続するポート
ciscoipphone	Cisco IP Phone 79xx を、79xx に接続した PC に接続するポート
ciscoipphone	Cisco IP Phone 79xx を、Cisco SoftPhone を稼働する 79xx に接続した PC に接続するポート[1]
ciscosoftphone	Cisco IP Phone 79xx なしで Cisco SoftPhone を稼働する PC を接続するポート

1. Cisco IP Phone 79xx を Cisco SoftPhone を稼働する PC に接続するポートの場合、Cisco CallManager との CTI 通信を通過する制御トラフィックにはタグが付けられますが、DSCP 0 に再マーキングされます。

Release 8.4(1) における SmartPort の拡張機能

ここでは、Release 8.4(1) における SmartPort の拡張機能について説明します。

ciscorouter SmartPort テンプレート

ciscorouter インターフェイス マクロ コマンドを入力すると、次のような設定になります。

（注） **nativevlan** の指定は必須です。**allowedvlans** の指定は省略可能です。

```
set port macro mod/port ciscorouter nativevlan nativevlan allowedvlans vlans
--------------------------------------------------------------------------------
set port enable mod/port
set vlan nativevlan mod/port
set port auxiliaryvlan mod/port auxvlan none
set port inlinepower mod/port auto
set cdp enable mod/port
set port membership mod/port static
set port l2protocol-tunnel mod/port cdp stp vtp dis
set udld enable mod/port
set spantree portfast mod/port enable trunk
set spantree bpdu-guard mod/port enable
set trunk mod/port nonegotiate dot1q
```

allowedvlans パラメータが指定されない場合は、次の設定が使用されます。

```
set trunk mod/port 1-4094 (if all specified)
```

allowedvlans パラメータが指定される場合は、次の設定が使用されます。

```
set trunk mod/port none
set trunk mod/port vlans (if specified)

set port qos mod/port autoqos trust dscp
```

ciscoswitch SmartPort テンプレート

ciscoswitch インターフェイス マクロ コマンドを入力すると、次のような設定になります。

（注） **nativevlan** の指定は必須です。**allowedvlans** の指定は省略可能です。

```
set port macro mod/port ciscoswitch nativevlan nativevlan allowedvlans vlans
--------------------------------------------------------------------------------
set port enable mod/port
set vlan nativevlan mod/port
set port auxiliaryvlan mod/port auxvlan none
set port inlinepower mod/port auto
set cdp enable mod/port
set port membership mod/port static
set port l2protocol-tunnel mod/port cdp stp vtp dis
set udld enable mod/port
set spantree portfast mod/port disable
set spantree bpdu-guard mod/port disable
set spantree link-type mod/port point-to-point
set trunk mod/port nonegotiate dot1q
```

allowedvlans パラメータが指定されない場合は、次の設定が使用されます。

```
set trunk mod/port 1-4094 (if all specified)
```

allowedvlans パラメータが指定される場合は、次の設定が使用されます。

```
set trunk mod/port none
set trunk mod/port vlans (if specified)

set port qos mod/port autoqos trust dscp
```

ciscodesktop SmartPort テンプレート

ciscodesktop インターフェイス マクロ コマンドを入力すると、次のような設定になります。

（注） **vlan** の指定は必須です。

```
set port macro mod/port ciscodesktop vlan vlan
-----------------------------------------------------
set port enable mod/port
set port host mod/port
      set vlan vlan mod/port
set port auxiliaryvlan mod/port auxvlan none
set port inlinepower mod/port auto
set cdp enable mod/port
set port membership mod/port static
set port l2protocol-tunnel mod/port cdp stp vtp dis
set spantree bpdu-guard mod/port enable
set port security mod/port enable age 2 maximum 1
                   violation restrict
set port qos mod/port autoqos trust dscp
set port qos mod/port trust untrusted
```

ciscoipphone SmartPort テンプレート

ciscoipphone インターフェイス マクロ コマンドを入力すると、次のような設定になります。

（注） **vlan**（*nativevlan*）の指定は必須です。**auxvlan** の指定は省略可能です。IP Phone の MAC アドレスはネイティブおよび補助 VLAN の両方に表示されることがあるため、ポート セキュリティは IP Phone の最大数が 3 に設定されます。

```
set port macro mod/port ciscoipphone vlan nativevlan auxvlan auxvlan
-----------------------------------------------------------------
set port enable mod/port
set port l2protocol-tunnel mod/port cdp stp vtp dis
set port membership mod/port static
set port host mod/port
set spantree bpdu-guard mod/port enable
set vlan nativevlan mod/port
set port auxiliaryvlan mod/port auxvlan  (set to none if not specified)
set port inlinepower mod/port auto (if supported by module)
set cdp enable mod/port
set port security mod/port enable age 2 maximum 3 violation restrict
set port qos mod/port autoqos voip ciscoipphone
```

ciscosoftphone SmartPort テンプレート

ciscosoftphone インターフェイス マクロ コマンドを入力すると、次のような設定になります。

（注）　**vlan**（*nativevlan*）の指定は必須です。

```
set port macro mod/port ciscosoftphone vlan nativevlan
------------------------------------------------------------------
set port enable mod/port
set port l2protocol-tunnel mod/port cdp stp vtp dis
set port membership mod/port static
set port host mod/port >
set spantree bpdu-guard mod/port enable
set vlan nativevlan mod/port
set port auxiliaryvlan mod/port auxvlan  none
set port inlinepower mod/port auto
set cdp enable mod/port
set port security mod/port enable age 2 maximum 1 violation restrict
set port qos mod/port autoqos voip ciscosoftphone
```

グローバル SmartPort テンプレート

ciscosmartports グローバル マクロ コマンドを入力すると、次のような設定になります。

```
set macro ciscosmartports
-----------------------------------------------------
set udld enable
set errdisable-timeout enable udld
set errdisable-timeout enable duplex-mismatch
set errdisable-timeout enable channel-misconfig
set errdisable-timeout enable bpdu-guard
set errdisable-timeout interval 60
set cdp enable
set cdp version v2
set spantree mode rapid-pvst+
set spantree macreduction enable
set spantree portfast bpdu-guard enable
set spantree global-default loop-guard enable
set qos autoqos
```

ユーザ定義可能な SmartPort マクロの設定

ここでは、SmartPort マクロを定義および実装する手順について説明します。

- 概要（p.53-49）
- CLI を使用したユーザ定義可能な SmartPort マクロの設定（p.53-50）

概要

ここでは、ユーザ定義可能な SmartPort マクロについて説明します。

- マクロの作成 — ユーザ定義可能なマクロの機能は、概念の上では **alias** コマンドと同様です。**alias** コマンドは、1 つのコマンドのみに対するエイリアスです。ユーザ定義可能なマクロの機能では、1 つまたは複数のコマンドに対するコマンド セットを作成します。このマクロは、マクロの一部となるコマンド リストを入力したあとで、**set macro name** *name* コマンドを使用して作成されます。

- マクロの変数の作成 — マクロを定義する際、変数で指定しなければならないパラメータが必要なコマンドがあります（イーサネット ポート用の VLAN ID または Access Control List［ACL; アクセス制御リスト］用の IP アドレスなど）。変数は、「keyword-value」のペアで定義されます。ここでは、最初のパラメータには変数の名前を付け、次のパラメータにはその値を入力します。各変数は、ポート単位またはグローバル単位で定義できます。変数の作成には、**set macro variable** *name_of_variable variable_value mod/port* コマンドを使用します。変数とその値は、スイッチのテーブル / データベースに保管されます。定義済みの変数を持つマクロがポートに適用されると、マクロはテーブル/データベースから値を取り、マクロ内のコマンドを実行します。
- マクロおよび変数の定義の表示 — マクロおよびその変数の定義を表示するには、**show macro** *macro-name* コマンドおよび **show macro variable** [**all**] [**name** *name_of_macro*] [*mod/port*] コマンドを入力します。
- マクロの適用 — マクロを作成したら、ポートに適用する必要があります。ポートに適用するマクロに変数が含まれる場合、この変数はテーブル / データベースで事前定義された各値に置き換えられてから、マクロ定義内のコマンドが実行されます。ポートにマクロを適用するには、**set port macro** *mod/port name_of_macro* コマンドを入力します。
- マクロの消去（削除）— 必要でなくなったマクロを消去できます。マクロを消去する場合は、マクロおよびその定義のみがシステムから消去されます。マクロを適用したポート上の設定は消去されません。マクロを消去するには、**clear macro** *name* コマンドを入力します。
- マクロ タイプ — マクロ タイプにはグローバル マクロおよびポートベース マクロの 2 種類があります。

CLI を使用したユーザ定義可能な SmartPort マクロの設定

ここでは、CLI を使用してユーザ定義可能な SmartPort マクロを設定する手順について説明します。

ユーザ定義マクロの作成

マクロを作成（定義）するには、**set macro name** *name* コマンドを使用してコマンドのリスト（1 ラインに 1 コマンド）を入力します。マクロを終わらせて、マクロ モードを終了するには、**@** 区切り文字をタイプしてから Enter を押します。次に例を示します。

```
Console> (enable) set macro name videophone
Enter macro commands one per line. End with character '@'.
set port enable #MODPORT
set vlan $DATAVLAN #MODPORT
set port auxiliaryvlan #MODPORT $AUXVLAN
set qos autoqos
@
Console> (enable)
```

ユーザ定義マクロを作成するには、次の注意事項および制限事項に従ってください。

- マクロ名の最大長は、16 文字です。マクロ内のコマンド ラインの最大数は、64 です。マクロ名にはスタティック マクロ名と同じ名前（ciscoswitch または ciscorouter など）を付けることはできません。
- ユーザ定義マクロまたはスタティック マクロでは、マクロ内にマクロを設定できます。
- マクロ作成時または変更時には、構文確認は行われません。マクロ作成時に不適切なコマンドを入力すると、マクロがポートに適用される際に不適切なコマンドは実行されません。
- 上記の例の場合、マクロの適用先であるポートを指定する変数は #MODPORT です。マクロがポート 3/2 に適用される場合、マクロがポートに適用されるときに、#MODPORT は 3/2 に置き換えられます。
- 上記の例では、$DATAVLAN および $AUXVLAN が変数で、マクロがポートに適用されるときに、適切な値に置き換えられます。
- 定義されたマクロは、NVRAM（不揮発性 RAM）に保存されます。

既存のユーザ定義マクロの変更

既存のユーザ定義マクロを変更するには、**set macro name** *name* コマンドを使用します。マクロを変更する際、新しい定義が古い定義と置き換えられますが、新しい定義は以前適用されていたすべてのポートに自動的に適用されるわけではありません。変更したマクロは明示的に適用する必要があります。次に例を示します。

```
Console> (enable) set macro name fileserver
Enter macro commands one per line. End with the character '@'.
cmd1
cmd2
@
Console> (enable)
```

「fileserver」という名前のマクロは、同名で新しい定義を持つマクロを作成することにより上書きされます。次に例を示します。

```
Console> (enable) set macro name fileserver
Enter macro commands one per line. End with the character '@'.
cmd2
cmd3
@
Warning: The macro fileserver has been modified; Do you want to modify (y/n) y
Console> (enable)
```

変数の定義

変数を定義するには、**set macro variable** *name_of_variable variable_of_value* [*mod/port*] コマンドを使用します。変数は、ポート単位またはグローバル単位で定義できます。ポートにマクロを適用する際、変数は定義された値に置き換えられます。変数名の最大長は、16 文字です。マクロ定義では、1 行で複数の変数を使用できます。ポート単位の変数は、ポート単位で定義されます。ポートごとに異なる値を使用して変数を定義することにより、個々のポートで異なる値を設定できます。変数定義にポート情報が含まれていない場合、グローバル変数として処理されます。グローバル変数定義は、ポート単位の変数が定義されていない場合に使用されます。次に例を示します。

```
Console> (enable) set macro variable $DATAVLAN 3 3/2

Variable DATAVLAN successfully created
Console> (enable) set macro variable $DATAVLAN 5 3/3
Console> (enable) set macro variable $AUXVLAN 4 3/2

Variable AUXVLAN successfully created
Console> (enable)
```

変数定義でポートが指定されていない場合、この変数はグローバル変数とみなされます。次に例を示します。

```
Console> (enable) set macro variable $CDPVER v2

Variable CDPVER successfully created
Console> (enable)

Console> (enable) set macro variable $DATAVLAN 77
Console> (enable)
```

上記の例では、$CDPVER はグローバル変数で、$DATAVLAN および $AUXVLAN はポート単位の変数です。$DATAVLAN も、グローバル変数として定義されています。変数 $DATAVLAN を使用するマクロが、ポート 3/2 または 3/3 以外のポートに適用される場合、このマクロでは、ポートに値 77 を使用します。定義された変数およびその値は、NVRAM に保存されます。

特別な変数の使用

マクロでは事前定義されていない変数を持つ場合もあります。この変数は、マクロの適用時に値を取得します。#MODPORT は、そのような変数の 1 つです。たとえば、マクロで変数 #MODPORT が定義されているとします。このマクロがモジュール / ポートに適用されると、変数 #MODPORT はマクロが適用されるモジュール / ポート（*mod/port*）に置き換えられます。次に例を示します。

```
Console> (enable) set macro name videophone
Enter macro commands one per line. End with character @.
set port enable #MODPORT
set vlan $DATAVLAN #MODPORT
set port auxiliaryvlan #MODPORT $AUXVLAN
@
Console> (enable)
```

上記の例の場合、#MODPORT は、マクロ videophone がポートに適用される際に値を取得する特殊変数です。

（注） #MODPORT は、現在サポートされている唯一の特殊変数です。

ユーザ定義のマクロの適用

作成したマクロは、ポートに適用することができます。マクロがポートに適用されるときに、マクロ定義のコマンドはスイッチで実行されます。マクロ定義のコマンドが任意の変数を使用する場合、この変数が各ユーザ定義の値に置き換わってから、コマンドが実行されます。ポートにマクロを適用するには、**set port macro** *mod/port name_of_macro* コマンドを入力します。

ユーザ定義のマクロを作成および実行するには、次の手順を実行します。

ステップ 1　次のコマンドを入力して、マクロを作成します。

```
Console> (enable) set macro name videophone
Enter macro commands one per line. End with character @.
set port enable #MODPORT
set vlan $DATAVLAN #MODPORT
set port auxiliaryvlan #MODPORT $AUXVLAN
@
Macro videophone successfully created
Console> (enable)
```

ステップ 2　次のコマンドを入力して、マクロ変数を定義します。

```
Console> (enable) set macro variable $DATAVLAN 3 3/2

Variable DATAVLAN successfully created
Console> (enable) set macro variable $DATAVLAN 5 3/3
Console> (enable) set macro variable $AUXVLAN 4 3/2

Variable AUXVLAN successfully created
Console> (enable) set macro variable $AUXVLAN 77 3/7
Console> (enable) set macro variable $DATAVLAN 99
Console> (enable) set macro variable $CDPVER v2

Variable CDPVER successfully created
Console> (enable)
```

ステップ 3　次のコマンドを入力して、ポート 3/2 のマクロを適用します。

```
Console> (enable) set port macro 3/2 videophone
```

マクロが適用される前に、$DATAVLAN および $AUXVLAN 変数はそれぞれ「3」と「4」に置き換えられ、次のコマンドが実行されます。

```
set port enable 3/2
set vlan 3 3/2
set port auxiliaryvlan 3/2 4
set cdp enable
set cdp version v2
set qos autoqos
```

ステップ 4　次のコマンドを入力して、ポート 3/7 のマクロを適用します。

```
Console> (enable) set port macro 3/7 videophone
```

マクロが適用される前に、$AUXVLAN 変数は「77」に置き換えられます。$DATAVLAN はポート 3/7 に定義されていないため、マクロはグローバル変数のリストを検索して $DATAVLAN を検出します。この場合、$DATAVLAN 変数がグローバル定義「99」に置き換えられ、次のコマンドが実行されます。

```
set port enable 3/7
set vlan 99 3/7
set port auxiliaryvlan 3/7 77
set cdp enable
set cdp version v2
set qos autoqos
```

ユーザ定義のマクロを適用する場合は、次の注意事項および制限事項に従ってください。

- マクロをポートに適用するときに、マクロ内で定義されていない変数が使用されている場合、マクロはポートに適用されず、適切なエラー メッセージが表示されます。エラー応答は、マクロの定義には影響しません。
- マクロをポートに適用するときに、マクロ内で有効なコマンドと無効なコマンドの両方が使用されている場合でもマクロはポートに適用され、無効なコマンドの実行時には、適切なエラー メッセージが表示されます。エラー応答は、マクロの定義には影響しません。
- マクロを適用する場合、適用されるマクロの記録はコンフィギュレーション　ファイルまたは NVRAM に保存されません。ただし、各ポートには適用された最新マクロの記録が保存されています。

- ポートに適用されたマクロは、消去できません。ただし、ポート上のマクロを取り消す方法として、ポートの設定を消去する別の新しいマクロを定義して、ポートに適用するやり方があります。

マクロの表示

ここでは、マクロのさまざまな表示方法について説明します。

- 構文は次のとおりです。

  show macro name *name_of_macro*

  show macro all

- 次のように、**show macro name** *name_of_macro* コマンドを入力して、マクロの定義を表示します。

```
Console> (enable) show macro name videophone

The macro definition for videophone is:

set port enable #MODPORT
set vlan $DATAVLAN #MODPORT
set port auxiliaryvlan #MODPORT $AUXVLAN
Console> (enable)
```

- 次のように、**show macro all** コマンドを入力して、スイッチ内のすべてのマクロの名前を表示します。

```
Console> (enable) show macro all
Macro Names
-----------
fileserver
videophone
Console> (enable)
```

マクロ変数の表示

ここでは、マクロ変数のさまざまな表示方法について説明します。

- 構文は次のとおりです。

  show macro variable [**all**] [**name** *name_of_macro*] [*mod/port*]

  show macro variables name *name_of_macro mod/port*

- 次のように、**show macro variable all** コマンドを入力して、スイッチ内のすべてのマクロ変数を表示します。

```
Console> (enable) show macro variable all

Variable                Port            Value           Type
--------                ----            -----           ------
DATAVLAN                3/2              3                Per-port
DATAVLAN                3/3              5                Per-port
DATAVLAN                NA               99               Global
AUXVLAN                 3/2              4                Per-port
AUXVLAN                 3/7              77               Per-port
CDPVER                  NA               v2               Global
Console> (enable)
```

- 次のように、**show macro variable name** *name_of_macro* コマンドを入力して、個々のマクロ変数および適用されるすべてのポートを表示します。

```
Console> (enable) show macro variable name $DATAVLAN

Variable                Port            Value           Type
--------                ----            -----           ------
DATAVLAN                3/2              3                Per-port
DATAVLAN                3/3              5                Per-portGlobal
DATAVLAN                NA               99               Global
Console> (enable)
```

- 次のように、**show macro variable name** *name_of_macro mod/port* コマンドを入力して、個々のマクロ変数および適用される特定のポートを表示します。

```
Console> (enable) show macro variable name $DATAVLAN 3/2

Variable                Port            Value           Type
--------                ----            -----           ------
DATAVLAN                3/2              3                Per-port
Console> (enable)
```

- 次のように、**show macro variables name** *name_of_macro mod/port* コマンドを入力して、マクロ変数をマクロ名で表示します。

```
Console> (enable) show macro variables name videophone 3/2

Variable-Name                   Variable Value          Port
-------------                   --------------          -----
DATAVLAN                        3                       3/2
AUXVLAN                         4                       3/2
Console> (enable)
```

マクロおよびマクロ変数の消去

clear macro name *name_of_macro* コマンドでマクロを消去する場合、マクロからコマンドが消去され、スイッチからマクロが削除されます。消去されたマクロによって適用された設定は、保持されます。消去されたマクロが変数を使用していた場合は、他のマクロでその変数が使用されていなければ、自動的に消去されます。

ここでは、マクロおよびマクロ変数のさまざまな消去方法について説明します。

- 構文は次のとおりです。

  clear macro name *name_of_macro*

  clear macro all

  clear macro variable [**all**] [*name_of_variable*] [*mod/ports*]

- 次のように、**clear macro name** *name_of_macro* コマンドを入力して、個々のマクロおよびその変数を消去します。

```
Console> (enable) clear macro name videophone

Clearing macro videophone....
Cleared Macro videophone ....
Console> (enable)
```

- 次のように、**clear macro all** コマンドを入力して、すべてのマクロおよびその変数を消去します。

```
Console> (enable) clear macro all

Clearing all macros....
All macros are cleared
Console> (enable)
```

- 次のように、**clear macro variable** *name_of_variable* コマンドを入力して、すべてのポートからマクロ変数を個別に消去します。

```
Console> (enable) clear macro variable $DATAVLAN

Clearing variable $DATAVLAN for all mod/ports...

Deleting Variable: DATAVLAN ...
Cleared variable DATAVLAN
Console> (enable)
```

- 次のように、**clear macro variable** *name_of_variable mod/ports* コマンドを入力して、1 つのポートからマクロ変数を個別に消去します。

```
Console> (enable) clear macro variable $AUXVLAN 3/7

Clearing variable $AUXVLAN for mod/port.3/7..
Console> (enable)
```

- 次のように、**clear macro variable all** コマンドを入力して、すべてのポートからすべてのマクロ変数を消去します。

```
Console> (enable) clear macro variable all

Clearing all variables for all mod/ports...

All variables in the switch are cleared
Console> (enable)
```

マクロ ポート マッピングの表示

ここでは、マクロ ポート マッピングのさまざまな表示方法について説明します。

- 構文は次のとおりです。

  show macro map [**all**] [**name** *name_of_macro*] [**port** *mod/port*]

- 次のように、**show macro map all** コマンドを入力して、すべてのマクロ ポート マッピングを表示します。

```
Console> (enable) show macro map all

Port                    Macro
-----                   -----
3/2                       videophone
3/7                       videophone
Console> (enable)
```

- 次のように、**show macro map name** *name_of_macro* コマンドを入力して、特定マクロのマクロ ポート マッピングを表示します。

```
Console> (enable) show macro map name videophone

Port                    Macro
-----                   -----
3/2                       videophone
3/7                       videophone
Console> (enable)
```

- 次のように、**show macro map port** *mod/port* コマンドを入力して、特定ポートのマクロ ポート マッピングを表示します。

```
Console> (enable) show macro map port 3/2

Port                    Macro
-----                   -----
3/2                     videophone
Console> (enable)
```

ユーザ定義可能な SmartPort マクロ設定の表示

NVRAM に保管されているマクロおよび変数の定義は、次のように **show config** コマンドを入力すると、表示できます。

```
Console> (enable) show config
This command shows non-default configurations only.
Use 'show config all' to show both default and non-default configurations.
.
.
.
.....................

begin
!
# ***** NON-DEFAULT CONFIGURATION *****
!
!
#time: Tue Mar 22 2005, 09:39:57
!
#version 8.5(0.52)JAC
!

!
#Macros
set macro name videophone

set port enable #MODPORT
set vlan $DATAVLAN #MODPORT
set port auxiliaryvlan #MODPORT $AUXVLAN
@
!
#Macro-Port mapping
set port macro 3/2 videophone
set port macro 3/7 videophone
!
.
.
.
```

マクロ内のマクロの設定

マクロ定義内にマクロを設定することができます。ルート マクロがポートに適用されると、ルート マクロ内のマクロは定義によって置き換えられ、ルート マクロはポートに適用されます。また、ユーザ定義マクロの定義内にスタティック マクロ（ciscoswitch または ciscorouter など）を含めることもできます。

（注） マクロ定義内にマクロがある場合、およびルート マクロがポートに適用されている場合は、**show macro map** コマンドを入力すると、ルート マクロが表示されます。

APPENDIX A

略語

表 A-1 に、このマニュアルで使用している略語とその意味を示します。

表 A-1　　略語一覧

略語	説明
AAA	Authentication, Authorization, Accounting（認証、許可、アカウンティング）
AAL	ATM Adaptation Layer（ATM アダプテーション レイヤ）
ACE	Access Control Entry（アクセス制御エントリ）
ACL	Access Control List（アクセス制御リスト）
AFI	Authority and Format Identifier
AMP	Active Monitor Present
APaRT	Automated Packet Recognition and Translation（自動パケット認識および変換）
ARP	Address Resolution Protocol（アドレス解決プロトコル）
ASLB	Accelerated Server Load Balancing
ATM	Asynchronous Transfer Mode（非同期転送モード）
BES	Bursty Errored Seconds
BIA	Bottom Interface Adapter
BPDU	Bridge Protocol Data Unit（ブリッジ プロトコル データ ユニット）
BRF	Bridge Relay Function（ブリッジ リレー機能）
BUS	Broadcast and Unknown Server
CAM	Content-Addressable Memory（連想メモリ）
CDP	Cisco Discovery Protocol
CEF	Cisco Express Forwarding
CIR	Committed Information Rate（認定情報速度）
CLI	Command-Line Interface（コマンドライン インターフェイス）
CMM	Communications Media Module
COPS	Common Open Policy Service
COPS-DS	COPS Differentiated Services
COPS-PR	COPS for Provisioning
CoS	Class of Service（サービス クラス）
CPLD	Complex Programmable Logic Device
CRAM	Compression and Reordering of the ACL Masks
CRC	Cyclic Redundancy Check（巡回冗長検査）

表 A-1　略語一覧（続き）

略語	説明
CRF	Concentrator Relay Function（コンセントレータ リレー機能）
CSG	Content Services Gateway
DAI	Dynamic ARP Inspection
DCC	Data Country Code
DEC	Digital Equipment Corporation
DFI	Domain-Specific Part Format Identifier
DHCP	Dynamic Host Configuration Protocol
DISL	Dynamic Inter-Switch Link
DMP	Data Movement Processor
DNS	Domain Name System（ドメイン ネーム システム）
DRAM	Dynamic RAM
DRiP	Dual Ring Protocol
DSAP	Destination Service Access Point
DSBM	Designated Subnet Bandwidth Manager
DSCP	Differentiated Services Code Point
DSP	Digital Signal Processing または Processor（デジタル信号処理またはプロセッサ）
DTP	Dynamic Trunking Protocol（ダイナミック トランキング プロトコル）
EAP	Extensible Authentication Protocol
EARL	Enhanced Address Recognition Logic
EEPROM	Electrically Erasable Programmable Read-Only Memory（電気的消去再書き込み可能 ROM）
ESI	End-System Identifier
FCS	Frame Check Sequence
FEFI	Far End Fault Indication
GARP	General Attribute Registration Protocol
GBIC	Gigabit Interface Converter（ギガビット インターフェイス コンバータ）
GMRP	GARP Multicast Registration Protocol
GSR	Gigabit Switch Router
GVRP	GARP VLAN Registration Protocol
HCRMON	High Capacity RMON
HDD	Hard Disk Drive Driver
HTTP	HyperText Transfer Protocol
ICD	International Code Designator
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IDP	Initial Domain Part
IDSM	Intrusion Detection System Module
IGMP	Internet Group Management Protocol
ILMI	Integrated Local Management Interface
IP	Internet Protocol
IPC	Interprocessor Communication（プロセッサ間通信）

表 A-1　略語一覧（続き）

略語	説明
IPX	Internetwork Packet Exchange
ISL	Inter-Switch Link（スイッチ間リンク）
ISO	International Organization of Standardization（国際標準化機構）
KDC	Key Distribution Center（鍵発行局）
LACP	Link Aggregation Control Protocol
LAN	Local-Area Network
LANE	LAN Emulation（LAN エミュレーション）
LCP	Link Control Protocol（リンク制御プロトコル）
LCV	Line Code Violation Seconds
LD	LocalDirector
LEC	LAN Emulation Client（LANE クライアント）
LECS	LAN Emulation Configuration Server（LANE コンフィギュレーション サーバ）
LEM	Link Error Monitor（リンク エラー モニタ）
LER	Link Error Rate（リンク エラー レート）
LES	LAN Emulation Server（LANE サーバ）または Line Errored Seconds
LLC	Logical Link Control（論理リンク制御）
MAC	Media Access Control（メディア アクセス制御）
MDG	Multiple Default Gateway
MIB	Management Information Base（管理情報ベース）
MII	Media-Independent Interface（メディア独立型インターフェイス）
MISTP	Multi-Instance Spanning-Tree Protocol
MLS	Multilayer Switching（マルチレイヤ スイッチング）
MMLS	Multicast Multilayer Switching（マルチキャスト マルチレイヤ スイッチング）
MOP	Maintenance Operation Protocol
MOTD	Message-of-The-Day（ログイン バナー）
MSFC	Multilayer Switch Feature Card（マルチレイヤ スイッチ フィーチャ カード）
MSM	Multilayer Switch Module
MST	Multiple Spanning Tree
MTP	Media Termination Point
MTU	Maximum Transmission Unit（最大伝送ユニット）
MVAP	Multiple VLAN Access Port
NAM	Network Analysis Module（ネットワーク解析モジュール）
NDE	NetFlow Data Export（NetFlow データ エクスポート）
NMP	Network Management Processor（ネットワーク管理プロセッサ）
NSAP	Network Service Access Point（ネットワーク サービス アクセス ポイント）
NTP	Network Time Protocol
NVRAM	Nonvolatile RAM（不揮発性 RAM）
OAM	Operation, Administration, and Maintenance
OSI	Open System Interconnection（開放型システム間相互接続）
OUI	Organizational Unique Identifier
PAE	Port Access Entity
PAgP	Port Aggregation Protocol（ポート集約プロトコル）

表 A-1　略語一覧（続き）

略語	説明
PBF	Policy-Based Forwarding
PCM	Pulse Code Modulation（パルス符号変調）
PCR	Peak Cell Rate（ピーク セル レート）
PDP	Policy Decision Point
PDU	Protocol Data Unit（プロトコル データ ユニット）
PEP	Policy Enforcement Point
PFC	Policy Feature Card（ポリシー フィーチャ カード）
PHY	Physical Sublayer（物理サブレイヤ）
PIB	Policy Information Base
PPP	Point-to-Point Protocol（ポイントツーポイント プロトコル）
PRID	Policy Rule Identifiers
PROM	Programmable Read-Only Memory
PVID	Port VLAN Identifier（ポート VLAN ID）
PVST+	Per VLAN Spanning-Tree Plus
QoS	Quality of Service（サービス品質）
RADIUS	Remote Access Dial-In User Service
RAM	Random-Access Memory（ランダムアクセス メモリ）
rcp	Remote Copy Protocol
RGMP	Router-Ports Group Management Protocol
RIF	Routing Information Field
RMON	Remote Monitoring
ROM	Read-Only Memory
RSA	Rivest, Shamir, Adleman
RSPAN	Remote SPAN
RST	Reset（リセット）
RSVP	Resource Reservation Protocol
SAID	Security Association Identifier
SAP	Service Access Point（サービス アクセス ポイント）
SIMM	Single In-Line Memory Module
SLCP	Supervisor Line-Card Processor
SLIP	Serial Line Internet Protocol（シリアル ライン インターネット プロトコル）
SMP	Standby Monitor Present
SMT	Station Management（ステーション管理）
SNAP	Subnetwork Access Protocol
SNMP	Simple Network Management Protocol（簡易ネットワーク管理プロトコル）
SPAN	Switched Port Analyzer（スイッチド ポート アナライザ）
SRB	Source-Route Bridge（ソースルート ブリッジ）
SRT	Source-Route Transparent Bridge
SSH	Secure Shell（セキュア シェル）
SSL	Secure Socket Layer
SSLM	Secure Socket Layer Mudule
STE	Spanning Tree Explorer

表 A-1　略語一覧（続き）

略語	説明
STP	Spanning-Tree Protocol（STP; スパニングツリー プロトコル）
SVC	Switched Virtual Circuit（相手先選択接続）
TAC	Technical Assistance Center（Cisco）
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol（簡易ファイル転送プロトコル）
TGT	Ticket Granting Ticket（身分証明書）
TLV	Type-Length-Value
ToS	Type of Service（サービス タイプ）
TrBRF	Token Ring Bridge Relay Function（トークンリング ブリッジ リレー機能）
TrCRF	Token Ring Concentrator Relay Function（トークンリング コンセントレータ リレー機能）
TTL	Time To Live
UART	Universal Asynchronous Receiver/Transmitter
UDLD	UniDirectional Link Detection（単一方向リンク検出）
UDLP	UniDirectional Link Protocol
UDP	User Datagram Protocol
UNI	User-Network Interface
UTC	Coordinated Universal Time（協定世界時）
VACL	VLAN Access Control List
VCC	Virtual Channel Connection（仮想チャネル接続）（ATM 用語）、Virtual Channel Circuit（仮想チャネル回線）
VCI	Virtual Circuit Identifier（仮想回線識別子）
VCR	Virtual Configuration Register（仮想コンフィギュレーション レジスタ）
VID	VLAN ID
VIP	Virtual IP Address
VLAN	Virtual LAN（仮想 LAN）
VMPS	VLAN Membership Policy Server（VLAN メンバーシップ ポリシー サーバ）
VoIP	Voice over IP
VPN	Virtual Private Network（仮想私設網）
VPNSM	Virtual Private Network Services Module
VTP	VLAN Trunking Protocol（VLAN トランキング プロトコル）
VVID	Voice VLAN Identifier
WRED	Weighted Random Early Detection（重み付きランダム早期検出）
WRR	Weighted Round-Robin（重み付きラウンドロビン）

Numerics

A

B

C

D

H

I

K

L

M

N

Q

R

S

T

U

W

X

Y

あ

い

え

お

か

き

し

す

せ

そ

た

ち

て

と

に

ね

は

ほ

ま

め

も

ゆ

よ

り

る

れ

ろ