



## **Catalyst 6500 シリーズ スイッチ MSFC コマンド リファレンス**

Cisco IOS Release 12.2 SX

Text Part Number: OL-5081-03-J



**【注意】シスコ製品をご使用になる前に、安全上の注意  
([www.cisco.com/jp/go/safety\\_warning/](http://www.cisco.com/jp/go/safety_warning/))をご確認ください。**

**本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。  
米国サイト掲載ドキュメントとの差異が生じる場合があるため、正式な内容については米国サイトのドキュメントを参照ください。  
また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。**

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

シスコシステムズが採用している TCP ヘッダー圧縮機能は、UNIX オペレーティングシステムの UCB (University of California, Berkeley) パブリックドメイン バージョンの一部として、UCB が開発したプログラムを最適化したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコシステムズおよびこれら各社は、商品性や特定の目的への準拠性、権利を侵害しないことに関する、または取り扱い、使用、または取引によって発生する、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコシステムズおよびその代理店は、このマニュアルの使用またはこのマニュアルを使用できないことによって起こる制約、利益の損失、データの損傷など間接的で偶発的に起こる特殊な損害のあらゆる可能性がシスコシステムズまたは代理店に知らされていても、それらに対する責任を一切負いかねます。

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

*Catalyst 6500 シリーズスイッチ MSFC コマンド リファレンス*  
Copyright © 2001-2005, Cisco Systems, Inc.  
All rights reserved.

Copyright © 2008, シスコシステムズ合同会社 .  
All rights reserved.



<b>はじめに</b>	<b>vii</b>
対象読者	vii
マニュアルの構成	vii
関連資料	viii
表記法	ix
マニュアルの入手方法	x
Cisco.com	x
Product Documentation DVD	x
マニュアルの発注方法	x
シスコ製品のセキュリティ	xi
シスコ製品のセキュリティ問題の報告	xi
Product Alert および Field Notice	xii
テクニカル サポート	xiii
Cisco Technical Support & Documentation Web サイト	xiii
Japan TAC Web サイト	xiv
Service Request ツールの使用	xiv
問題の重大度の定義	xiv
その他の資料および情報の入手方法	xv

---

**CHAPTER 1**

<b>CLI</b>	<b>1-1</b>
ヘルプの利用方法	1-1
コマンド オプションの検索	1-2
コマンドの no 形式および default 形式の使用	1-5
CLI スtring検索の使用	1-6
正規表現	1-6
単一文字パターン	1-6
複数文字パターン	1-7
繰り返し指定	1-8
選択	1-9
位置指定	1-9
リコール機能用カッコ	1-10

alt キーワードの使用方法	1-10
設定変更の保存	1-11
MSFC CLI	1-12
スーパーバイザ エンジン CLI から MSFC CLI へのアクセス	1-12
コンソール ポートから MSFC CLI へのアクセス	1-12
Telnet セッションから MSFC CLI へのアクセス	1-13
Cisco IOS コマンド モード	1-13
Cisco IOS コマンド リストおよび構文の表示	1-14
Cisco IOS コマンドライン インターフェイス	1-15
Cisco IOS コンフィギュレーション モードへのアクセス	1-15
Cisco IOS コンフィギュレーションの表示および保存	1-16
MSFC インターフェイスの復帰	1-16

CHAPTER 2

**Catalyst 6500 シリーズ スイッチ MSFC コマンド 2-1**

clear ip auth-proxy watch-list	2-2
config-register	2-3
config-sync	2-4
define interface-range	2-5
high-availability	2-6
interface range	2-8
ip address	2-10
ip auth-proxy max-login-attempts	2-12
ip auth-proxy watch-list	2-13
ip local-proxy-arp	2-14
ip multicast rpf backoff	2-15
ip multicast rpf interval	2-16
ip verify unicast source reachable-via	2-17
ip wccp accelerated	2-19
ip wccp	2-21
ip wccp group-listen	2-23
ip wccp redirect	2-24
ip wccp redirect exclude	2-26
ipx network	2-28
maximum-paths	2-32
mls aclmerge algorithm	2-33
mls ip	2-34
mls ip cef load-sharing	2-35
mls ip cef rate-limit	2-37
mls ip cef rpf interface-group	2-38

mls ip cef rpf multipath	2-39
mls ip delete-threshold	2-40
mls ip inspect	2-41
mls ip install-threshold	2-42
mls ip multicast consistency-check	2-43
mls ip multicast stub	2-45
mls rate-limit all	2-46
mls rate-limit multicast ipv4	2-47
mls rate-limit multicast ipv6	2-49
mls rate-limit unicast acl	2-51
mls rate-limit unicast cef	2-53
mls rate-limit unicast ip	2-54
mode	2-56
mtu	2-58
redundancy	2-59
route-converge-delay	2-60
set traffic-index	2-61
show fm features	2-62
show fm inband-counters	2-64
show fm insp	2-65
show fm interface	2-66
show fm reflexive	2-68
show fm summary	2-68
show fm vlan	2-69
show ip auth-proxy watch-list	2-70
show ip pim interface	2-71
show ip pim neighbor	2-73
show l3-mgr	2-74
show microcode	2-76
show mls cef ip	2-77
show mls cef ip multicast	2-78
show msfc2 rom-monitor	2-85
show redundancy	2-86
show scp	2-87
show slot0:	2-89
show standby delay	2-92
snmp-server enable traps	2-93
standby delay minimum reload	2-95

standby ip	2-97
standby track	2-99
upgrade rom-monitor	2-101

---

APPENDIX A

**略語** A-1

---

APPENDIX B

**オープンソースソフトウェアについて** B-1

---

INDEX

**索引**



# はじめに

---

ここでは、このマニュアルの対象読者、構成、および表記法、そして関連資料の入手方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 MSFC 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

このマニュアルは、次の章で構成されています。

章	タイトル	説明
第 1 章	<a href="#">CLI</a>	MSFC コマンドライン インターフェイスを説明します。
第 2 章	<a href="#">Catalyst 6500 シリーズ スイッチ MSFC コマンド</a>	アルファベット順に、MSFC 特有のコマンドの詳細情報を説明します。
付録 A	<a href="#">略語</a>	このマニュアルで使用されている略語の定義を説明します。

## 関連資料

Catalyst 6500 シリーズ スイッチの MSFC の Cisco IOS マニュアルには次のものがあります。

- 『 *Catalyst 6500 Series Switch Module Installation Guide* 』
- 『 *Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide* 』
- 『 *Catalyst 6500 Series Switch Cisco IOS System Message Guide* 』
- 『 *Release Notes for Cisco IOS Release 12.2SX on the Catalyst 6500 and Cisco 7600 Supervisor Engine 720 and Supervisor Engine 2* 』

Cisco IOS マニュアルには他に次のものがあります。

- 『 *Configuration Fundamentals Configuration Guide* 』
- 『 *Command Reference* 』

Management Information Base (MIB; 管理情報ベース) の詳細については、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

このマニュアルは、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。波カッコは、たとえば <code>{interface interface type}</code> のように、キーワードや引数を囲むのにも使われます。
[ 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。
シングルクォーテーション	引用符を付けない一組の文字。シングルクォーテーション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シングルクォーテーションとみなされます。
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。
^	^ 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。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符 (!) またはポンド記号 (#) がある場合には、コメント行であることを示します。

(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 で入手できます。ここでは、シスコが提供する製品マニュアルのリソース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](http://www.cisco.com/public/countries_languages.shtml)

### Product Documentation DVD

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ライブラリです。この DVD を使用すると、シスコのハードウェア製品のインストール、ソフトウェア製品のインストール、設定、およびコマンドに関するガイドにアクセスできます。DVD を使用することで、次の URL にあるシスコの Web サイトに収録されている、HTML 形式のマニュアルおよび一部の PDF ファイルにアクセスできます。

<http://www.cisco.com/univercd/home/home.htm>

Product Documentation DVD は定期的に作成され、リリースされています。DVD は、単独または購読契約で入手できます。Cisco.com に登録されている場合、次の URL にある Cisco Marketplace の Product Documentation Store から Product Documentation DVD ( Customer Order Number DOC-DOCDVD= または DOC-DOCDVD=SUB ) を発注できます。

<http://www.cisco.com/go/marketplace/docstore>

### マニュアルの発注方法

Cisco Marketplace にアクセスするには、Cisco.com にユーザ登録されている必要があります。登録されている場合、次の URL にある Product Documentation Store からシスコ製品のマニュアルを発注できます。

<http://www.cisco.com/go/marketplace/docstore>

ログイン ID またはパスワードを取得されていない場合は、次の URL で登録手続きをしてください。

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

## 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](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

このサイトから、次の各内容に関する情報を入手できます。

- 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、セキュリティ上の注意事項、およびセキュリティ応答のリストが以下の URL で確認できます。

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

セキュリティ勧告、セキュリティ上の注意事項、およびセキュリティ応答の更新をリアルタイムで確認するには、Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) フィードに登録します。PSIRT RSS フィードの加入に関する詳細については、次の URL にアクセスしてください。

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](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](mailto:security-alert@cisco.com)  
緊急度の高い問題とは、システムが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](mailto: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 (GnuPG など) 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 ~ 9.x で暗号化された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 への連絡時には、次の URL にある Security Vulnerability Policy ページの Contact Summary セクションにリンクされている有効な公開鍵を使用してください。:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

このページのリンクに、現在使用されている PGP 鍵の ID があります。

PGP を所有または使用していない場合は、機密情報を送信する前に PSIRT に連絡し、他のデータ暗号化方法についてご確認ください。

## Product Alert および Field Notice

シスコ製品に関する変更やアップデートは、Cisco Product Alert および Cisco Field Notice で発表されます。Cisco Product Alert および Cisco Field Notice を受信するには、Cisco.com で Product Alert Tool を使用してください。このツールでプロフィールを作成し、情報の配信を希望する製品を選択できます。

Product Alert Tool にアクセスするには、Cisco.com にユーザ登録されている必要があります。(Cisco.com にユーザ登録するには、次の URL にアクセスしてください。

<http://tools.cisco.com/RPF/register/register.do>)。登録ユーザは、次の URL からこのツールにアクセスできます。<http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en>

## 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。Cisco Technical Support & Documentation 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 サポートにオンラインまたは電話でお問い合わせいただく前に、**Cisco Product Identification Tool** を使用して、製品のシリアル番号をご確認ください。このツールにアクセスするには、Cisco Technical Support & Documentation Web サイトの **Tools & Resources** リンク、**All Tools (A-Z)** タブをクリックし、アルファベット順の一覧から **Cisco Product Identification Tool** を選択します。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。



ヒント

Cisco.com での表示と検索

ブラウザで Web ページが更新されていないと思われる場合は、Ctrl キーを押しながら F5 キーを押して、Web ページを強制的に更新してください。

技術情報を検索する場合は、Cisco.com Web サイト全体ではなく、技術マニュアルに限定して検索してください。具体的には、Cisco.com ホームページで、Search ボックスの下にある **Advanced Search** リンクをクリックし、次に **Technical Support & Documentation** オプション ボタンをクリックします。

Cisco.com の Web サイトまたは特定のマニュアルに関するフィードバックを提供するには、Cisco.com のすべての Web ページの上部にある **Contacts & Feedback** をクリックします。

## 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 )。TAC Service Request ツールに状況を入力すると、推奨される解決方法が提示されます。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できます。

- Cisco Online Subscription Center は、シスコの各種 E メール ニュースレターなどの配信を申し込むことができる Web サイトです。プロフィールを作成し、配信を希望する内容を選択します。Cisco Online Subscription Center には、次の URL からアクセスしてください。

<http://www.cisco.com/offer/subscribe>

- 『Cisco Product Quick Reference Guide』は、手軽に使えるコンパクトなリファレンス ツールで、チャネル パートナーを通じて販売されている多くのシスコ製品に関する製品概要、主な機能、製品番号、および簡単な技術仕様が記載されています。年に 2 回更新され、シスコの最新のチャネル製品が掲載されています。『Cisco Product Quick Reference Guide』の発注および詳細については、次の URL にアクセスしてください。

<http://www.cisco.com/go/guide>

- 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、および認定に関連する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>

- 『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 にアクセスしてください。

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

- Networking Professionals Connection は、ネットワークの専門家がネットワーク製品やネットワーク技術に関する質問、提案、情報をシスコの専門家および他のネットワーク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>

- 『What's New in Cisco Documentation』は、シスコ製品の最新マニュアル リリースに関する情報を提供するオンライン資料です。毎月更新されるこの資料は、製品カテゴリ別にまとめられているため、目的の製品マニュアルを簡単に見つけることができます。最新の『What's New in Cisco Documentation』には、次の URL からアクセスしてください。

<http://www.cisco.com/univercd/cc/td/doc/abtnucd/136957.htm>

- 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>





# CLI

この章では、Catalyst 6500 シリーズスイッチ Cisco IOS ソフトウェアの MSFC の設定に使用する CLI (コマンドライン インターフェイス) を説明します。この章で説明する内容は、次のとおりです。

- [ヘルプの利用方法 \(p.1-1\)](#)
- [コマンド オプションの検索 \(p.1-2\)](#)
- [MSFC CLI \(p.1-12\)](#)

Catalyst 6500 シリーズスイッチ CiscoIOS ソフトウェア コンフィギュレーションの概要については、『*Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide*』を参照してください。

## ヘルプの利用方法

システム プロンプトに疑問符 (?) を入力すると、各コマンド モードで使用できるコマンドのリストが表示されます。コンテキスト ヘルプ機能により、各コマンドの関連キーワードおよび引数のリストも表示できます。

表 1-1 に、コマンド モード、コマンド、キーワード、または引数に対して特定のヘルプ情報を表示できるコマンドの一覧を表示します。

表 1-1 ヘルプの利用方法

コマンド	説明
<code>abbreviated-command-entry?</code>	指定した文字ストリングで始まるコマンドのリストが表示されます (コマンドと疑問符の間にスペースを入れないでください)。
<code>abbreviated-command-entry&lt;Tab&gt;</code>	指定したコマンド省略形から、完全なコマンド名が表示されます。
<code>?</code>	特定のコマンド モードで使用できるすべてのコマンドが一覧表示されます。
<code>command ?</code>	コマンドの関連キーワードが一覧表示されます。コマンドと疑問符の間にスペースを入れてください。
<code>command keyword ?</code>	キーワードの関連引数が一覧表示されます。キーワードと疑問符の間にスペースを入れてください。

## コマンド オプションの検索

ここでは、コマンド構文を表示する例を示します。コマンド構文には、任意または必須のキーワードが含まれています。コマンドのキーワードを表示するには、コンフィギュレーション プロンプトで、またはコマンドの一部とスペースを入力したあとで、疑問符(?)を入力します。Catalyst 6500 シリーズ スイッチソフトウェアにより、使用できるキーワードのリストと、キーワードの簡単な説明が表示されます。たとえば、グローバル コンフィギュレーション モードで **arap** コマンドの全キーワードを調べたい場合には、**arap ?** と入力します。

表 1-2 では、次のコマンド入力を例にして、コマンド入力の際の疑問符(?)の使用法を示します。

- **interface gigabitethernet 1/1**
- **channel-group 1 mode auto**

表 1-2 コマンド オプションの検索

コマンド	コメント
<pre>Router&gt; enable Password: &lt;password&gt; Router#</pre>	<p><b>enable</b> コマンドおよびパスワードを入力して、特権 EXEC コマンドを開始します。</p> <p>特権 EXEC モードが開始されると、プロンプトが Router# に変わります。</p>
<pre>Router# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#</pre>	<p>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。</p> <p>グローバル コンフィギュレーション モードが開始されると、プロンプトが Router(config)# に変わります。</p>
<pre>Router(config)# interface gigabitethernet ? &lt;1-9&gt; GigabitEthernet interface number Router(config)# interface gigabitethernet 1/1 Router(config-if)#</pre>	<p><b>interface gigabitethernet</b> グローバル コンフィギュレーション コマンドを入力し、設定するギガビットイーサネット インターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。</p> <p>? を入力し、コマンドラインに次に入力する内容を調べます。この例では、<i>module-number/port-number</i> のフォーマットで 1 ~ 9 のインターフェイス番号を入力する必要があります。</p> <p>インターフェイス コンフィギュレーション モードが開始されると、プロンプトが Router(config-if)# に変わります。</p>

表 1-2 コマンド オプションの検索 (続き)

コマンド	コメント
<pre>Router(config-if)#? Interface configuration commands:   access-expression Build a bridge boolean access expression   apollo             Apollo interface subcommands   appletalk          Appletalk interface subcommands   arp                Set arp type (arpa, probe, snap) or timeout   backup            Modify backup parameters   bandwidth          Set bandwidth informational parameter   bgp-policy         Apply policy propogated by bgp community string   bridge-group      Transparent bridging interface parameters   carrier-delay     Specify delay for interface transitions   cdp                CDP interface subcommands   channel-group      Etherchannel/port bundling configuration   clns              CLNS interface subcommands   cmns              OSI CMNS   custom-queue-list Assign a custom queue list to an interface   decnet            Interface DECnet config commands   default           Set a command to its defaults   delay             Specify interface throughput delay   description        Interface specific description   dlsw              DLSw interface subcommands   dspu              Down Stream PU   exit              Exit from interface configuration mode   fair-queue        Enable Fair Queuing on an Interface   flowcontrol        Configure flow operation.   fras              DLC Switch Interface Command   help              Description of the interactive help system   hold-queue        Set hold queue depth   ip                Interface Internet Protocol config commands   ipx               Novell/IPX interface subcommands   isis              IS-IS commands   iso-igrp          ISO-IGRP interface subcommands . . .</pre>	<p>? を入力し、ギガビットイーサネットインターフェイスに対して使用できるすべてのインターフェイス コンフィギュレーション コマンドのリストを表示します。</p>
<pre>Router(config-if)# channel-group ? group channel-group of the interface  Router(config-if)#channel-group</pre>	<p>コントローラを設定するコマンドを入力します。この例では、<b>channel-group</b> コマンドを入力します。</p> <p>? を入力し、コマンドラインに次に入力する内容を調べます。この例では、<b>group</b> キーワードを入力する必要があります。</p> <p>&lt;cr&gt; が表示されていないので、コマンドを完成するにはさらに多くの情報を入力する必要があります。</p>

## ■ コマンド オプションの検索

表 1-2 コマンド オプションの検索 (続き)

コマンド	コメント
<pre>Router(config-if)# channel-group ? &lt;1-256&gt; Channel group number  Router(config-if)#channel-group</pre>	<p><b>group</b> キーワードを入力してから、?を入力して、コマンドラインに次に入力する内容を調べます。この例では、チャンネルグループ番号 1 ~ 256 を入力する必要があります。</p> <p>&lt;cr&gt; が表示されていないので、コマンドを完成するにはさらに多くの情報を入力する必要があります。</p>
<pre>Router(config-if)# channel-group 1 ? mode Etherchannel Mode of the interface  Router(config-if)#</pre>	<p>チャンネルグループ番号を入力してから、?を入力して、コマンドラインに次に入力する内容を調べます。この例では、<b>mode</b> キーワードを入力する必要があります。</p> <p>&lt;cr&gt; が表示されていないので、コマンドを完成するにはさらに多くの情報を入力する必要があります。</p>
<pre>Router(config-if)# channel-group 1 mode ? auto Enable PAgP only if a PAgP device is detected desirable Enable PAgP unconditionally on Enable Etherchannel only  Router(config-if)#</pre>	<p><b>mode</b> キーワードを入力してから、?を入力して、コマンドラインに次に入力する内容を調べます。この例では、<b>auto</b>、<b>desirable</b>、または <b>on</b> キーワードを入力する必要があります。</p> <p>&lt;cr&gt; が表示されていないので、コマンドを完成するにはさらに多くの情報を入力する必要があります。</p>
<pre>Router(config-if)# channel-group 1 mode auto ? &lt;cr&gt;  Router(config-if)#</pre>	<p>この例では、<b>auto</b> キーワードを使用します。<b>auto</b> キーワードを入力してから、?を入力して、コマンドラインに次に入力する内容を調べます。</p> <p>&lt;cr&gt; が表示されたので、Return を押せばコマンドを完成できます。さらにキーワードを一覧表示する場合は、キーワードを追加して Return を押し、コマンドを完成させます。</p>
<pre>Router(config-if)# channel-group 1 mode auto Router(config-if)#</pre>	<p>この例では、Return を押して、コマンドを完成します。</p>

## コマンドの no 形式および default 形式の使用法

ほとんどすべてのコンフィギュレーション コマンドに **no** 形式があります。通常、コマンドの機能をディセーブルにする場合に **no** 形式のコマンドを指定します。ディセーブルにした機能を再びイネーブルにしたり、デフォルトでディセーブルに設定されている機能をイネーブルにしたりするには、**no** キーワードを付けないコマンドを使用します。たとえば、IP ルーティングはデフォルトでイネーブルに設定されています。IP ルーティングをディセーブルにするには、**no ip routing** コマンドを指定します。IP ルーティングを再びイネーブルにするには、**ip routing** コマンドを指定します。このマニュアルでは、コンフィギュレーション コマンドの完全な構文およびコマンドの **no** 形式について説明します。

コンフィギュレーション コマンドには **default** 形式もあります。**default** 形式のコマンドは、コマンドの機能をデフォルト設定に戻します。ほとんどのコマンドはデフォルトでディセーブルに設定されているので、**default** 形式は **no** 形式と同じ結果になります。ただし、一部のコマンドはデフォルトでイネーブルに設定され、変数にデフォルト値が割り当てられています。このようなコマンドを **default** 形式で実行すると、コマンドの変数にデフォルト値が再設定されます。このマニュアルでは、コマンドが **no** 形式と異なる場合のコマンドの **default** 形式について説明します。

## CLI スtring検索の使用

コマンド出力のパターンをStringと呼びます。CLI String検索機能を使用すれば、`show` または `more` コマンド出力の検索およびフィルタリングを行うことができます。また、`--More--` プロンプトで検索およびフィルタリングを行うことができます。この機能は、大量の出力をソートする必要のある場合や、出力から不要な情報を除外する場合に役立ちます。

検索機能を使用すれば、フィルタリングされていない出力で、指定された正規表現を含むものを最初の行から始めることができます。コマンド1つあたり、最大1つのフィルタを指定できます。または `--More--` プロンプトから新しい検索を開始できます。

正規表現とは、`show` または `more` コマンド出力のマッチングを行うためにソフトウェアが用いるパターン（句、番号、またはより複雑なパターン）です。正規表現は、大文字と小文字を区別し、複雑な一致要件を可能にします。単純な正規表現の例は、`Serial`、`misses`、`138` などです。複合正規表現の例は、`00210...`、`( is )`、`[Oo]utput` などです。

次の3種類のフィルタリングを行うことができます。

- 指定した正規表現を含む行で出力を始めるには、`begin` キーワードを使用します。
- 指定した正規表現を含む出力行を含めるには、`include` キーワードを使用します。
- 指定した正規表現を含む出力行を除外するには、`exclude` キーワードを使用します。

次に、このフィルタリングされた出力を `--More--` プロンプトで検索できます。



(注)

CLI String検索機能を使用しても、以前の出力へ逆方向に検索またはフィルタリングすることはできません。フィルタリングは、CLI への HTTP アクセスで指定することはできません。

## 正規表現

正規表現は、コマンド出力内の同じ1つの文字に一致する1つの文字でもかまいませんし、コマンド出力内の同じ複数の文字に一致する複数の文字でもかまいません。このセクションでは、単一文字パターンおよび複数文字パターンを作成する方法と、繰り返し指定、選択、位置指定、およびカッコを用いたより複雑な正規表現を作成する方法について説明します。

## 単一文字パターン

最も単純な正規表現は、コマンド出力の同じ1つの文字と一致する単一文字です。単一文字パターンとしては任意の文字（A-Z、a-z）または数字（0-9）を使用できます。他のキーボード文字（! や ~ など）も単一文字パターンとして使用できますが、あるキーボード文字は、正規表現として用いられた場合に特別な意味を持ちます。表 1-3 に特別な意味を持つキーボード文字を一覧表示します。

表 1-3 特別な意味を持つ文字

文字	特別な意味
.	スペースを含む任意の単一文字と一致します。
*	0 個以上のパターンのシーケンスに一致します。
+	1 個以上のパターンのシーケンスに一致します。
?	0 または 1 回のパターンと一致します。
^	Stringの最初と一致します。
\$	Stringの最後と一致します。
_ (アンダースコア)	カンマ (,)、左波カッコ ({)、右波カッコ (})、左カッコ ( (、右カッコ ( ) )、Stringの最初、Stringの最後、またはスペースと一致します。

これらの特殊文字を単一文字パターンとして入力する場合は、各文字の前にバックスラッシュ (\) を置いて特別な意味を持たせないようにしてください。次の例は、それぞれドル記号、アンダースコア、プラス記号に一致する単一文字パターンです。

```
\$ \_ +
```

一連の単一文字パターンを指定して、コマンド出力とのマッチングを行うことができます。たとえば、a、e、i、o、またはuのうちの1つを含むStringに一致する正規表現を作成できます。パターンマッチングが成功するためには、これらの文字のうちの1つだけがStringに存在しなくてはなりません。一連の単一文字パターンを指定するには、単一文字パターンを角カッコ ([ ]) で囲みます。次に例を示します。

```
[aeiou]
```

小文字アルファベットの5つの母音のうちの任意の1文字と一致します。

```
[abcdABCD]
```

小文字または大文字アルファベットの最初の4つの文字のうちの任意の1文字と一致します。

ダッシュ (-) で区切って範囲の終点だけを入力することにより範囲を簡略化できます。上記の範囲は次のように簡略化できます。

```
[a-dA-D]
```

範囲に単一文字パターンとしてダッシュを追加する場合は、もう1つダッシュを追加して、その前にバックスラッシュを置きます。

```
[a-dA-D\ -]
```

範囲に単一文字パターンとして右角カッコ (]) を含めることもできます。次のように記述してください。

```
[a-dA-D\ -])]
```

上記の例は、大文字または小文字のアルファベットの最初の4文字のうちの任意の1文字、ダッシュ、または右角カッコに一致します。

範囲の最初にカレット (^) を含めることにより、範囲の一致を逆にすることができます。次の例では、列挙された文字以外の任意の文字に一致します。

```
[^a-dqsv]
```

次の例では、右角カッコ (]) またはdという文字以外の任意の文字に一致します。

```
[^\])d]
```

## 複数文字パターン

正規表現を作成する場合、複数の文字を含むパターンを指定することもできます。文字、数字、または特別な意味を持たないキーボード文字を組み合わせることで複数文字パターン正規表現を作成できます。たとえば、a4% は複数文字正規表現です。特別な意味を持つキーボード文字からその特別な意味をなくしたい場合には、キーボード文字の前にバックスラッシュを置きます。

複数文字パターンでは、順序が大切です。正規表現 a4% は、a という文字のあとに4が続き、そのあとに % 記号が続く文字と一致します。そのStringに a4% という文字がその順序で含まれていない場合、パターンマッチングは失敗します。この複数文字正規表現では、

```
a.
```

は、ピリオド文字の特別な意味を使用し、a という文字のあとに任意の文字が1つ来るStringと一致します。この例では、ab、a!、またはa2 というStringはすべてこの正規表現での有効な一致となります。

ピリオド文字の前にバックスラッシュを置くことにより、ピリオド文字の特別な意味をなくすことができます。次の表現では、

a\.

a. というStringのみが、この正規表現に一致します。

すべての文字、すべての数字、すべてのキーボード文字、または文字、数字、および他のキーボード文字の組み合わせを含む複数文字正規表現を作成できます。次の例はすべて有効な正規表現です。

telebit 3107 v32bis

## 繰り返し指定

ある特殊文字を単一および複数文字パターンとともに使用することにより、指定された正規表現の繰り返しに一致するより複雑な正規表現を作成できます。表 1-4 に正規表現の「繰り返し」を指定する特殊文字を一覧表示します。

表 1-4 繰り返し指定として使用される特殊文字

文字	説明
*	0 個以上の単一または複数文字パターンに一致します。
+	1 個以上の単一または複数文字パターンに一致します。
?	単一または複数文字パターンの 0 または 1 回の繰り返しに一致します。

次の例は、a という文字の任意の回数 (0 を含む) に一致します。

a\*

このパターンでは、String内で最低 1 つの a という文字が一致している必要があります。

a+

このパターンでは、String bb または bab に一致します。

ba?b

このStringでは、任意の数のアスタリスク (\*) に一致します。

\\*\*

複数文字パターンで繰り返し指定を使用する場合は、パターンをカッコで囲みます。次の例では、パターンは任意の数の複数文字String ab に一致します。

(ab)\*

より複雑な例として、次のパターンは、1 つまたは複数の英数字ペアに一致します (ただし、0、すなわち空Stringには一致しません)。

([A-Za-z][0-9])+

繰り返し指定 (\*、+、または ?) を使用している一致の記述順序では、最も長い構造が最初にマッチします。ネ스팅された構造でのマッチングは外側から内側へ行われます。連結構造では、構造の左側からマッチングされます。したがって、この正規表現は番号の前に文字が指定されるため、A9b3 には一致しますが、9Ab3 には一致しません。

## 選択

選択を使用すると、Stringとのマッチングに選択パターンを指定できます。選択パターンは、縦棒(|)で分離します。選択肢のうちの1つだけが、Stringと一致します。たとえば、正規表現

```
codex | telebit
```

は、codex または telebit というStringと一致しますが、codex と telebit の両方と一致しません。

## 位置指定

Stringの最初または最後に対して正規表現パターンのマッチングを行います。つまり、Stringの最初または最後に固有のパターンが含まれるよう指定します。表 1-5 に示す特殊文字を用いたStringの一部に対して、これらの正規表現の「位置指定」を行います。

表 1-5 位置指定に用いられる特殊文字

文字	説明
^	Stringの最初と一致します。
\$	Stringの最後と一致します。

次の正規表現がStringと一致するのは、Stringがabcdで始まるときだけです。

```
^abcd
```

対照的に、次の表現は、a、b、c、またはdという文字以外のすべての単一文字に一致します。

```
[^abcd]
```

次の例では、正規表現は.12で終わるStringと一致します。

```
$.12
```

これらの位置指定文字を特殊文字アンダースコア(\_)と対比させてください。アンダースコアは、Stringの始め(^)、Stringの終わり(\$)、カッコ(\)、スペース( )、波カッコ({)、カンマ(,) またはアンダースコア(\_)と一致します。アンダースコア文字を使用した場合、パターンはStringのどこに存在していてもかまいません。

たとえば、

```
_1300_
```

は、String内のどこかに1300が含まれるStringに一致します。Stringの1300の前後にスペース、波カッコ、カンマ、またはアンダースコアを置くことができます。たとえば、

```
{1300_
```

は、正規表現に一致しますが、21300 および 13000 は一致しません。

アンダースコア文字を用いれば、

```
^1300$ ^1300(space) (space)1300 {1300, ,1300, {1300} ,1300, (1300
```

のような長い正規表現リストを以下に置き換えることができます。

```
_1300_
```

## リコール機能用カッコ

「[繰り返し指定](#)」(p.1-8) に示すように、カッコを複数文字正規表現とともに使用して、パターンを繰り返すことができます。また、単一文字パターンまたは複数文字パターンを囲むカッコを使用して、正規表現の他の場所で使用するパターンを記憶させることができます。

以前のパターンをリコールする正規表現を作成するには、リコールする特定のパターンを示すカッコ、バックスラッシュ (\)、整数という順序で記述します。これにより、記憶されたパターンを再び使用できます。整数は、正規表現パターン内のカッコの繰り返し数を示します。正規表現内に複数のリコールパターンがある場合、\1 は最初のリコールパターン、\2 は2番めのリコールパターン、というようになります。

次の正規表現は、リコール機能用カッコを使用します。

```
a(.)bc(.)\1\2
```

この正規表現は、a のあとに任意の文字が来て (文字 1 と呼ぶ) その次に bc が来て、その次に任意の文字 (文字 2 と呼ぶ) が来て、その次に再び文字 1 が来て、その次に再び文字 2 が来るストリングと一致します。この正規表現は aZbcTZT と一致します。文字 1 が Z、文字 2 が T であることがソフトウェアに記憶されており、あとの正規表現でも再び Z と T が使用されます。

## alt キーワードの使用方法

ハイアベイラビリティ冗長性をイネーブルにすると、メインの Multilayer Switch Feature Card (MSFC; マルチレイヤ スイッチ フィーチャ カード) で実行するすべてのコンフィギュレーション コマンドは、非メインの MSFC にも送信されます。また、メインとなる MSFC で `copy source running-config` コマンドを入力した場合も、実行コンフィギュレーションの同期更新が行われます。

コンフィギュレーションの同期には、次の 2 つの状態があります。

- Config Sync AdminStatus この機能に対し、そのときにユーザが設定した内容であることを示します。
- Config Sync RuntimeStatus 次に該当する場合に限りイネーブルになります。
  - Config Sync AdminStatus が、メイン MSFC および非メイン MSFC の両方でイネーブルにされた場合。
  - メイン MSFC および非メイン MSFC が互換性のあるイメージを実行している場合。

単一のコンソールから両方の MSFC を設定するには、alt キーワードを入力し、代替コンフィギュレーション指定します。代替コンフィギュレーションを指定した場合、alt キーワードの前で指定したコンフィギュレーションは、スイッチのスロット 1 に搭載されたスーパーバイザ エンジンの 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 に搭載されたスーパーバイザ エンジンの MSFC に適用されます。



(注) Config Sync AdminStatus をイネーブルにするには、alt キーワードを入力する必要があります。

Config Sync RuntimeStatus をイネーブルにした場合、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。どちらの MSFC のコンフィギュレーションも、メイン MSFC のコンソールまたは Telnet セッションから実行します。
- alt キーワードが使用可能です。また、必要にもなります (alt キーワードの詳細は、「[alt キーワードの使用方法](#)」 [p.1-10] 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 をディセーブルにした場合、次の状態になります。

- 両方の MSFC の CLI 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 (任意)。
- 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。

表 1-6 では、**alt** キーワードを含む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 コマンドを示しています。

表 1-6 alt キーワードを含む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
<ul style="list-style-type: none"> <li>• <b>[no] standby</b> [<i>group_number</i>] <b>ip</b> [<i>ip_address</i> [<b>secondary</b>]] <b>alt</b> <b>[no] standby</b> [<i>group_number</i>] <b>ip</b> [<i>ip_address</i> [<b>secondary</b>]]</li> <li>• <b>[no] standby</b> [<i>group_number</i>] <b>priority</b> <i>priority</i> [<b>preempt</b> [<i>delay delay</i>]] <b>alt</b> <b>[no] standby</b> [<i>group_number</i>] <b>priority</b> <i>priority</i> [<b>preempt</b> [<i>delay delay</i>]]</li> <li>• <b>[no] ip address</b> <i>ip_address mask</i> [<b>secondary</b>] <b>alt</b> <b>[no] ip address</b> <i>ip_address mask</i> [<b>secondary</b>]</li> <li>• <b>[no] ipx network</b> <i>network</i> [<b>encapsulation encapsulation_type</b> [<b>secondary</b>]] [<b>alt</b> <b>[no] ipx network</b> <i>network</i> [<b>encapsulation encapsulation_type</b> [<b>secondary</b>]]]</li> </ul>	<ul style="list-style-type: none"> <li>• <b>[no] hostname</b> <i>hostname alt hostname</i> <i>hostname</i></li> <li>• <b>[no] ip default-gateway</b> <i>ip_address alt <b>[no] ip default-gateway</b> <i>ip_address</i></i></li> <li>• <b>router bgp</b> <i>autonomous_system</i> <b>bgp router-id</b> <i>ip_address</i> [<b>alt</b> <i>ip_address</i>]</li> <li>• <b>router ospf</b> <i>process_id</i> <b>router-id</b> <i>ip_address</i> [<b>alt</b> <i>ip_address</i>]</li> </ul>

次の例では、**ip address** コマンドを入力した際に使用される **alt** キーワードを示しています。

```
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
```

## 設定変更の保存

設定変更をスタートアップ コンフィギュレーションに保存して、システムのリロードまたは停電時に設定変更が失われないようにするには、次のコマンドを入力します。

```
Router# copy system:running-config nvram:startup-config
Building configuration...
```

設定を保存するには 1 ~ 2 分かかります。設定が保存されたあと、次の出力が表示されます。

```
[OK]
Router#
```

ほとんどのプラットフォームでは、この手順により設定が NVRAM (不揮発性 RAM) に保存されます。クラス A フラッシュ ファイル システム プラットフォームでは、この手順により設定が CONFIG\_FILE 環境変数によって指定された場所に保存されます。CONFIG\_FILE 環境変数のデフォルトは NVRAM です。

## MSFC CLI

スーパーバイザエンジンの CLI からコマンドを入力することで、MSFC の CLI にアクセスできます。次の項で、MSFC の CLI を説明します。

- [スーパーバイザエンジン CLI から MSFC CLI へのアクセス \(p.1-12\)](#)
- [Cisco IOS コマンド モード \(p.1-13\)](#)
- [Cisco IOS コマンドライン インターフェイス \(p.1-15\)](#)

### スーパーバイザエンジン CLI から MSFC CLI へのアクセス

次の項で、直接接続されたコンソールまたは Telnet セッションから MSFC CLI にアクセスする方法を説明します。

- [コンソールポートから MSFC CLI へのアクセス \(p.1-12\)](#)
- [Telnet セッションから MSFC CLI へのアクセス \(p.1-13\)](#)

### コンソールポートから MSFC CLI へのアクセス

`switch console` コマンドを入力し、コンソールポートに直接接続しているスーパーバイザエンジン CLI から MSFC CLI にアクセスすることができます。MSFC CLI を終了してスーパーバイザ CLI に戻る場合、Router> プロンプトで `^C^C^C` を入力します。

スーパーバイザエンジン CLI から MSFC CLI へのアクセスには、次の作業を実行します。

作業	コマンド
スーパーバイザエンジン CLI から MSFC CLI へのアクセス	<code>switch console [mod]<sup>1</sup></code>

1. `mod` 変数は MSFC のモジュール番号を指定します。番号は 15 (MSFC をスロット 1 のスーパーバイザエンジンに搭載する場合) または 16 (MSFC をスロット 2 のスーパーバイザエンジンに搭載する場合) を使用します。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なスーパーバイザエンジンに搭載されている MSFC に切り替わります。



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

次に、アクティブなスーパーバイザエンジン CLI からアクティブな MSFC CLI にアクセスする例、および MSFC CLI を終了してスーパーバイザエンジン 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 CLI へのアクセス

`session mod` コマンドを入力すると、Telnet セッションを使用しているスーパーバイザ エンジン CLI から MSFC CLI にアクセスできます。MSFC CLI を終了してスーパーバイザ CLI に戻る場合、Router> プロンプトで `exit` コマンドを入力します。



(注) スーパーバイザ エンジンのソフトウェアは MSFC をモジュール 15 (スロット 1 のスーパーバイザ エンジンに搭載した場合) またはモジュール 16 (スロット 2 のスーパーバイザ エンジンに搭載した場合) と認識しています。

次の例では、スーパーバイザ エンジン CLI から MSFC CLI にアクセスする方法、また、MSFC CLI を終了してスーパーバイザ エンジン CLI に戻る方法を示しています。

```
Console> (enable) session 15
Router> exit
Console> (enable)
```



(注) 「スーパーバイザ エンジン CLI から MSFC CLI へのアクセス」(p.1-12) で説明した方法以外に、Telnet から MSFC への直接アクセスをサポートするように Cisco IOS ソフトウェアを設定することもできます。『Cisco IOS Security Configuration Guide』の「Configuring Authentication」を参照してください。URL は次のとおりです。

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgr/secr\\_c/scprt1/scdathen.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgr/secr_c/scprt1/scdathen.htm)

## Cisco IOS コマンド モード

Cisco IOS ユーザ インターフェイスは、多くの異なるモードに分けられます。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。特定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 リストおよび構文の表示」(p.1-14) を参照してください。

スーパーバイザ エンジン上でセッションを開始するには、ユーザ モード (別名ユーザ EXEC モード) から始めます。EXEC モードで使用できるのは、限定的なコマンド サブセットです。すべてのコマンドにアクセスするには、特権 EXEC モードを開始する必要があります。特権 EXEC モードにアクセスするには、通常、パスワードを入力する必要があります。特権 EXEC モードからは、任意の EXEC コマンドを実行できるほか、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。ほとんどの EXEC コマンドは、現在の設定状況を表示する `show` コマンドや、カウンタまたはインターフェイスをクリアする `clear` コマンドといった 1 回限りのコマンドです。スーパーバイザ エンジン を再起動したときに、EXEC コマンドは保存されません。

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を変更できます。変更したコンフィギュレーションを保存しておけば、スーパーバイザ エンジンの再起動後も、コマンドが保存されます。グローバル コンフィギュレーション モードで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、スーパーバイザ エンジンを正常に起動できない場合に使用される独立したモードです。スーパーバイザ エンジンの起動時に有効なシステム イメージが検出されない場合、またはスタートアップ時にコンフィギュレーション ファイルが破壊されている場合、ROM モニタ モードが開始されることがあります。詳細情報については、『*Catalyst 6500 Series IOS Command Reference*』を参照してください。

表 1-7 では、使用される最も一般的な Cisco IOS モードを説明しています。

表 1-7 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>
特権 EXEC	動作パラメータの設定。特権コマンドセットには、 <b>configure</b> コマンドの他にユーザ EXEC モードの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、 <b>enable</b> 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	システム全体に作用する機能の設定。	特権 EXEC モードで、 <b>configure terminal</b> 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 コマンドを実行すると、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がイネーブルになるか、または変更されます。	グローバル コンフィギュレーション モードで、 <b>interface type location</b> 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、 <b>line console 0</b> コマンドを入力します。	Router (config-line)#

ユーザが入力するコマンドは、Cisco IOS コマンド インタープリタ (別名 EXEC) によって認識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して、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** に省略できます。

**exit** と入力すると、MSFC 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特権 EXEC モードに戻るには、**Ctrl-Z** キーを押します。

## Cisco IOS コマンド リストおよび構文の表示

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、その後に疑問符 (?) を入力します。スペースは含めません。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 ヘルプといえます。

```
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えます。

```
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** を押します。上矢印キーを続けて押すことにより、直前に入力したコマンドを20個まで表示できます。



#### ヒント

コマンドの入力にお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** を押すと、ただちに特権 EXEC モードに戻ります。1つ前のモードに戻るには、**exit** を入力します。

## Cisco IOS コマンドライン インターフェイス

次のセクションでは、ルーティングの設定をする前に理解する必要がある、Cisco IOS コンフィギュレーションの基本的な作業を説明しています。

- [Cisco IOS コンフィギュレーション モードへのアクセス \(p.1-15\)](#)
- [Cisco IOS コンフィギュレーションの表示および保存 \(p.1-16\)](#)
- [MSFC インターフェイスの復帰 \(p.1-16\)](#)

## 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には、次の作業を行います。



#### (注)

スーパーバイザ エンジンのコンソール ポートに直接接続されている場合、**switch console** コマンドを入力し、スーパーバイザ エンジン CLI から MSFC CLI にアクセスします。Telnet セッションから MSFC にアクセスするには、「[Telnet セッションから MSFC CLI へのアクセス](#)」(p.1-13) を参照してください。

	作業	コマンド
ステップ 1	スーパーバイザ エンジン CLI にいる場合、MSFC CLI を入力します。	Console> <b>switch console</b> [mod_num]
ステップ 2	EXEC プロンプトで、イネーブル モードを入力します。	Router> <b>enable</b>
ステップ 3	特権 EXEC プロンプトで、グローバル コンフィギュレーション モードを入力します。	Router# <b>configure terminal</b>
ステップ 4	ルーティングを設定するコマンドを入力します。	(『 <i>Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide</i> 』で、適切なコンフィギュレーション作業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)# <b>Ctrl-Z</b>

### Cisco IOS コンフィギュレーションの表示および保存

設定を変更したあと、それを表示および保存するには、次の作業を行います。

	作業	コマンド
ステップ 1	特権 EXEC プロンプトで現在稼働している設定を表示します。	Router# <b>show running-config</b>
ステップ 2	NVRAM の設定を表示します。	Router# <b>show startup-config</b>
ステップ 3	現在の設定を NVRAM に保存します。	Router# <b>copy running-config startup-config</b>

### MSFC インターフェイスの復帰

場合によっては、MSFC インターフェイスの管理上のシャット ダウンが実行される可能性があります。show interface コマンドを使用し、インターフェイスの状態を確認できます。



(注)

冗長スーパーバイザ エンジンの構成では、MSFC 上のインターフェイスがシャット ダウンした場合、冗長 MSFC で一致する VLAN (仮想 LAN) のインターフェイスはパケットの転送を停止します。そのため、冗長 MSFC で一致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 ダウンが実行された MSFC インターフェイスを復帰するには、次の作業を特権モードで実行します。

	作業	コマンド
ステップ 1	復帰させるインターフェイスを指定します。	Router(config)# <b>interface</b> interface_type interface_number
ステップ 2	インターフェイスを復帰させます。	Router(config-if)# <b>no shutdown</b>
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)# <b>Ctrl-Z</b>



# Catalyst 6500 シリーズ スイッチ MSFC コマンド

---

この章では、Cisco IOS ソフトウェアをサポートする Multilayer Switching Feature Card (MSFC; マルチレイヤ スイッチ フィーチャ カード) コマンドがアルファベット順に記載されています。

このマニュアルでは、MSFC 固有のコマンドのみを説明しています。このマニュアルに記載されていない Cisco IOS コマンドの詳細については、次の最新の Cisco IOS 資料を参照してください。

- 『*Cisco IOS Release 12.2 Configuration Fundamentals Configuration Guide*』
- 『*Catalyst 6500 Series Switch Cisco IOS Command Reference*』

# clear ip auth-proxy watch-list

1 つのウォッチ リストのエントリまたはすべてのウォッチ リストのエントリを削除するには、`clear ip auth-proxy watch-list` コマンドを使用します。

```
clear ip auth-proxy watch-list {ip-addr|*}
```

## シンタックスの説明

<i>ip-addr</i>	ウォッチ リストから削除する IP アドレス。
*	ウォッチ リストからすべてのウォッチリスト エントリを削除します。

## デフォルト

このコマンドにはデフォルト設定がありません。

## コマンドモード

特権 EXEC

## コマンド履歴

リリース	変更内容
12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

## 使用上のガイドライン

無効と思われるウォッチ リストのエントリがある場合、`clear ip auth-proxy watch-list` コマンドを入力することで、ウォッチ リストの期限切れを待たずに手動でクリアできます。

## 例

次に、ウォッチリストのエントリを 1 つ削除する例を示します。

```
Router# clear ip auth-proxy watch-list 12.0.0.2
Router#
```

次に、すべてのウォッチリストのエントリを削除する例を示します。

```
Router# clear ip auth-proxy watch-list *
Router#
```

## 関連コマンド

[ip auth-proxy max-login-attempts](#)  
[ip auth-proxy watch-list](#)  
[show ip auth-proxy watch-list](#)

# config-register

コンフィギュレーションレジスタの設定を変更するには、**config-register** コマンドを使用します。

**config-register** *value*

## シンタックスの説明

<i>value</i>	16 進数または 10 進数の値 ( 次のルータの再起動で使用する 16 ビットのコンフィギュレーションレジスタの値 )。有効な値は 0x0 ~ 0xFFFF ( 10 進数では 0 ~ 65535 )
--------------	---

## デフォルト

デフォルトのコンフィギュレーションレジスタの値については、ご使用のプラットフォームのマニュアルを参照してください。新しいプラットフォームの多くはデフォルトを 0x2102 としています。これにより、ルータはフラッシュメモリから起動し、Break キーは無視されます。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

リリース	変更内容
12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

## 使用上のガイドライン

このコマンドはソフトウェア コンフィギュレーションレジスタが使用されるプラットフォームに対してのみ適用されます。

コンフィギュレーションレジスタの最下位の 4 ビット ( ビットの 3、2、1、0 ) は、ブートフィールドを形成します。ブートフィールドは、手動によるルータの起動元 ( ROM、フラッシュメモリ、ネットワーク ) を決定します。

ブートフィールドの値を変更し、残りのビットをデフォルト値のままに設定するには、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レジスタのブートフィールドの値を 0x0 に設定した場合、**boot** コマンドを使用してオペレーティングシステムを手動で起動する必要があります。
- コンフィギュレーションレジスタのブートフィールドの値を 0x1 に設定した場合、ルータはデフォルトの ROM を使用して起動します。
- コンフィギュレーションレジスタのブートフィールドに 0x2 ~ 0xF の値を設定した場合、ルータはブートフィールドを使用し、ネットワークサーバから起動するためのデフォルトのファイル名を形成します。

コンフィギュレーションレジスタのビットの設定およびデフォルトのファイル名の詳細については、適切なルータのハードウェアインストールガイドを参照してください。

## 例

次に、コンフィギュレーションレジスタを設定し、フラッシュメモリからシステムイメージを起動する例を示します。

```
Router(config)# config-register 0x2102
Router(config)#
```

## config-sync

コンフィギュレーションの同期化をイネーブルにするには、**config-sync** コマンドを使用します。コンフィギュレーションの同期化をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
config-sync
```

```
no config-sync
```

**シンタックスの説明** このコマンドには、引数またはキーワードはありません。

**デフォルト** このコマンドにはデフォルト設定がありません。

**コマンドモード** ハイアベイラビリティ冗長サブモード

コマンド履歴	リリース	変更内容
	12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

**例** 次に、コンフィギュレーションの同期化をイネーブルにする例を示します。

```
Router(config)# redundancy
Router(config-r)# high-availability
Router(config-r-ha)# config-sync
Router(config-r-ha)#
```

次に、コンフィギュレーションの同期化をディセーブルにする例を示します。

```
Router(config)# redundancy
Router(config-r)# high-availability
Router(config-r-ha)# no config-sync
Router(config-r-ha)#
```

# define interface-range

インターフェイス レンジ マクロを作成するには、**define interface-range** コマンドを使用します。

```
define interface-range macro-name interface-range
```

## シンタックスの説明

<i>macro-name</i>	インターフェイス レンジ マクロ名。32 文字まで指定できます。
<i>interface-range</i>	インターフェイス レンジ。インターフェイス レンジの有効値のリストについては、「使用上の注意事項」を参照してください。

## デフォルト

このコマンドにはデフォルト設定がありません。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

リリース	変更内容
12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

## 使用上のガイドライン

マクロ名は 32 文字までの文字ストリングです。

マクロには最大 5 つまでのレンジを含むことができます。インターフェイス レンジはスロットをまたがることはできません。 *interface-range* を入力する場合、次のフォーマットを使用できます。

- *card-type* {*slot*}/{*first-interface*} - {*last-interface*}
- *card-type* {*slot*}/{*first-interface*} - {*last-interface*}

*card-type* の有効値は次のとおりです。

- **ge-wan**
- **pos**
- **vlan** *vlan-id* (有効値は、1 ~ 4094)

## 例

次に、複数インターフェイスのマクロを作成する例を示します。

```
Router(config)# define interface-range macrol vlan 223, pos 6/1
Router(config)#
```

## 関連コマンド

[interface range](#)

# high-availability

ハイアベイラビリティ冗長性をイネーブルにし、ハイアベイラビリティ冗長サブモードを開始するには、**high-availability** コマンドを使用します。

**high-availability**

**シンタックスの説明** このコマンドには、引数またはキーワードはありません。

**デフォルト** このコマンドにはデフォルト設定がありません。

**コマンドモード** 冗長コンフィギュレーション サブモード

コマンド履歴	リリース	変更内容
	12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

**使用上のガイドライン** ハイアベイラビリティ冗長コンフィギュレーション サブモードを開始すると、次のオプションが使用できます。

- **[no] config-sync** 自動スタートアップおよび実行コンフィギュレーションの同期化をイネーブルにします。自動スタートアップおよび実行コンフィギュレーションの同期化をディセーブルにするには、このコマンドの **no** 形式を使用します。

Config Sync RuntimeStatus をイネーブルにした場合、次の状態になります。

- 非メイン Multilayer Switch Feature Card (MSFC; マルチレイヤ スイッチ フィーチャカード) の CLI (コマンドライン インターフェイス) 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** キーワードが使用可能です。また、必要にもなります (**alt** キーワードの詳細は、「[alt キーワードの使用方法](#)」(p.1-10) 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 をディセーブルにした場合、次の状態になります。

- 両方の MSFC の CLI 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せん (任意)。
- 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。

- **exit** ハイアベイラビリティ コンフィギュレーション モードを終了します。
- **no** コマンドを無効にするか、またはデフォルトを設定します。
- **[no] single-router-mode** 単一ルータ モードを開始します。単一ルータ モードを終了するには、このコマンドの **no** 形式を使用します。単一ルータ モードを開始すると、次のキーワードが使用できます。
  - **failover table-update-delay time** スイッチオーバー検出とハードウェア Forwarding Information Base (FIB; 転送情報ベース) のリロード間の遅延を秒数で設定できます。time に指定できる値は 0 ~ 4294967295 秒です。

ハイアベイラビリティ冗長性をイネーブルにした場合、メイン MSFC で実行するすべてのコンフィギュレーション コマンドは、非メイン MSFC にも送信されます。さらに、メイン MSFC で **copy source running-config** コマンドを入力した場合も、実行コンフィギュレーションの同期更新が行われます。

ハイアベイラビリティ冗長性をイネーブルにした場合、非メイン MSFC 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ます。EXEC モードのみ使用可能になります。たとえば次の例では、Router-16 は非 MSFC です。ハイアベイラビリティ冗長性およびコンフィギュレーションの同期化がイネーブルになります。

```
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  
Router-16>
```

Supervisor Engine 720 上で、SRM はデフォルトでイネーブルに設定されています。SRM が正常に動作するように、スタートアップ コンフィギュレーションが同一、または非メイン ルートのプロセッサでスタートアップ コンフィギュレーションが存在していないことを確認してください。

**例** 次に、ハイアベイラビリティ冗長性をイネーブルにし、ハイアベイラビリティ冗長サブモードを開始する例を示します。

```
Router(config)# redundancy  
Router(config-r)# high-availability  
Router(config-r-ha)#
```

#### 関連コマンド

[redundancy](#)

**show redundancy** (『*Catalyst 6500 Series Switch Cisco IOS Command Reference*』を参照)

# interface range

コマンドを複数のポートで同時に実行するには、**interface range** コマンドを使用します。

```
interface range {port-range | macro name}
```

## シンタックスの説明

<i>port-range</i>	ポート範囲。 <i>port-range</i> の指定できる値のリストについては、「使用上の注意事項」を参照してください。
<i>macro name</i>	マクロ名を指定します。

## デフォルト

このコマンドにはデフォルト設定がありません。

## コマンドモード

グローバルまたはインターフェイス コンフィギュレーション

## コマンド履歴

リリース	変更内容
12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

## 使用上のガイドライン

**interface range** コマンドは、既存の VLAN (仮想 LAN) Switched Virtual Interface (SVI) 上でのみ使用できます。VLAN SVI を表示するには、**show running config** コマンドを入力します。表示されない VLAN は、**interface range** コマンドで使用することはできません。

**interface range** コマンドとともに入力される値は、すべての既存の VLAN SVI に適用されます。

マクロを使用する前に、**define interface-range** コマンドで範囲を定義する必要があります。

ポート範囲に対して行われるすべての設定変更は NVRAM (不揮発性 RAM) に保存されますが、**interface range** コマンドで作成されたポート範囲は NVRAM には保存されません。

ポート範囲は次の 2 つの方法で入力できます。

- 最大 5 つのポート範囲を指定
- 以前定義したマクロを指定

ポートまたはポート範囲マクロ名のいずれかを指定できます。ポート範囲は同じポート タイプで構成します。範囲内のポートは、スロットをまたぐことはできません。

1 つのコマンドで最大 5 つのポート範囲を定義できます。それぞれの範囲はカンマで区切ってください。

範囲を定義する場合は、最初のポートとハイフン (-) の間にスペースを挿入する必要があります。

範囲を定義する場合は、最初のポートとハイフン (-) の前後にスペースを挿入します。

```
interface range pos 7/1 - 7, pos9/5 - 408
```

*port-range* を入力する場合、次のフォーマットを使用できます。

- *card-type* {slot}/{first-port} - {last-port}
- *card-type* {slot}/{first-port} - {last-port}

*card-type* の有効値は次のとおりです。

- **ge-wan**
- **pos**

- **vlan** *vlan-id*

同じコマンドでマクロとインターフェイス範囲の両方を指定することはできません。マクロを作成したあと、CLI (コマンドライン インターフェイス) でさらに範囲を入力することはできません。すでにインターフェイス範囲を入力している場合は、CLI でマクロを入力することはできません。

*port-range* に 1 つのインターフェイスを指定することもできます。

## 例

次に、2 つのポート範囲でコマンドを実行する例を示します。

```
Router(config)# interface range pos 7/1 - 7, pos 9/5 - 408  
Router(config-if)#
```

次に、ポート範囲マクロを実行する例を示します。

```
Router(config)# interface range macro macrol  
Router(config-if)#
```

## 関連コマンド

[define interface-range](#)

# ip address

プライマリまたはセカンダリの IP アドレスをインターフェイスに設定するには、**ip address** コマンドを使用します。IP アドレスを削除、または IP のプロセスをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
ip address ip_address mask [secondary]
```

```
no ip address ip_address mask [secondary]
```

## シンタックスの説明

<i>ip-address</i>	IP のアドレス
<i>mask</i>	関連した IP サブネットのマスク
<i>secondary</i>	(任意)設定されたアドレスをセカンダリ IP アドレスに指定します。このキーワードが省略された場合、設定されたアドレスはプライマリ IP アドレスになります。

## デフォルト

インターフェイスに IP アドレスは定義されていません。

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

リリース	変更内容
12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

## 使用上のガイドライン

**alt** キーワードを使用することで、代替コンフィギュレーションを指定できます。次のように使用されます。

```
[no] ip address ip-address mask [secondary] alt [no] ip address ip-address mask [secondary]
```

インターフェイスには、1 つのプライマリ IP アドレスおよび複数のセカンダリ IP アドレスを設定できます。Cisco IOS ソフトウェアで生成されたパケットは、常にプライマリ IP アドレスを使用します。そのため、セグメント上のすべてのルータおよびアクセス サーバは、同一のプライマリ ネットワーク番号を共有する必要があります。

Internet Control Message Protocol (ICMP) Mask Request メッセージを使用することで、ホストはサブネット マスクを判断できます。ルータは、ICMP Mask Reply メッセージでこの要求に応答します。

**no ip address** コマンドで IP アドレスを削除し、特定のインターフェイス上の IP のプロセスをディセーブルにできます。他のホストが削除する IP アドレスを使用していることをソフトウェアが検出した場合、コンソール上にエラー メッセージが表示されます。

**secondary** オプションのキーワードを使用して、セカンダリ アドレスの番号を制限なく指定できます。セカンダリ アドレスはプライマリ アドレスと同様に処理されます。ただし、システムは、セカンダリの送信元アドレスのルーティング更新以外のデータグラムを生成することはありません。IP ルーティング テーブル内にインターフェイスのルートがある場合、IP ブロードキャストおよび Address Resolution Protocol (ARP) 要求は正常に処理されます。

セカンダリ IP アドレスはさまざまな状況で使用できます。次に、最も一般的な想定例を挙げます。

- 特定のネットワーク セグメントに十分なホスト アドレスがない場合。たとえば、サブネットワーク化で、論理サブネットごとに 254 までのホストを許可したが、1 つの物理的なサブネットに 300 のホスト アドレスが必要になる場合。ルータまたはアクセス サーバ上でセカンダリ IP アドレスを使用することで、2 つの論理サブネットを 1 つの物理サブネット上で許可できます。

- 多数の古いネットワークがレベル2のブリッジで構築されている場合。セカンダリアドレスを使用することで、サブネット化されたルータベースのネットワークへ移行が可能となります。古いブリッジによるセグメント上のルータは、そのセグメント上の他のサブネットを学習できません。
- 1つのネットワークの2つのサブネットが、他のネットワークによる別の方法で分割される可能性がある場合。この状態は、サブネットが使用中であれば発生しません。この場合、最初のネットワークが拡張されるか、セカンダリアドレスによりセカンダリネットワーク上にレイヤ化されます。

**(注)**

ネットワークセグメント上のルータのいずれかがセカンダリアドレスを使用している場合、同一のセグメント上にある他のすべてのデバイスも、同一のネットワークまたはサブネットのセカンダリアドレスを使用する必要があります。ネットワークセグメント上のセカンダリアドレスの非整合性はルーティングのループを発生させる原因になります。

**(注)**

Open Shortest Path First (OSPF) プロトコルを使用している場合、インターフェイスのすべてのセカンダリアドレスが、プライマリアドレスとして同一の OSPF 領域にあることを確認してください。

インターフェイス上の IP をトランスペアレントにブリッジする場合、次の2つのことを実行する必要があります。

- IP ルーティングをディセーブルにします (*no ip routing* コマンドを入力)。
- ブリッジグループにそのインターフェイスを追加します (*bridge-group* コマンドを参照)。

インターフェイス上の IP を同時にルーティングし、トランスペアレントにブリッジする場合、*bridge crb* コマンドを参照してください。

**例**

次に、131.108.1.27 がインターフェイス Ethernet 0 のプライマリアドレスとして表示する例を示します。192.31.7.17 および 192.31.8.17 がインターフェイス Ethernet 0 のセカンダリアドレスとして表示されています。

```
interface ethernet 0
 ip address 131.108.1.27 255.255.255.0
 ip address 192.31.7.17 255.255.255.0 secondary
 ip address 192.31.8.17 255.255.255.0 secondary
```

**関連コマンド**

*bridge crb* (Cisco IOS のマニュアルを参照)

*bridge-group* (Cisco IOS のマニュアルを参照)

# ip auth-proxy max-login-attempts

ファイアウォール インターフェイスでのログイン 試行回数を制限するには、**ip auth-proxy max-login-attempts** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
ip auth-proxy max-login-attempts 1-maxint
```

```
no ip auth-proxy max-login-attempts
```

<b>シンタックスの説明</b>	<i>1-maxint</i>	最大ログイン試行回数。有効な試行回数の値は 1 ~ 2147483647 です。
------------------	-----------------	--

<b>デフォルト</b>	<i>1-maxint</i> は 5 に設定されています。
--------------	--------------------------------

<b>コマンドモード</b>	インターフェイス コンフィギュレーション
----------------	----------------------

<b>コマンド履歴</b>	リリース	変更内容
	12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

<b>使用上のガイドライン</b>	このコマンドがサポートされるのは、ファイアウォール インターフェイス上のみです。
-------------------	--

最大ログイン試行回数の機能は、ウォッチリストとは独立しています。ウォッチリスト(**ip access-list hardware permit fragments** コマンドを使用)を設定しておらず、最大ログイン試行回数の機能を設定している場合、既存の認証プロキシが実行されますが、再試行回数の指定が新しい数になっています。ウォッチリストを設定した場合、設定した試行回数に到達するとその IP アドレスがウォッチリストに加えられます。

<b>例</b>	次の例では、ファイアウォールでのログイン試行回数を制限する例を示します。
----------	--------------------------------------

```
Router(config-if)# ip auth-proxy max-login-attempts 4
Router(config-if)#
```

<b>関連コマンド</b>	<p><b>clear ip auth-proxy watch-list</b></p> <p><b>ip access-list hardware permit fragments</b> (『<i>Catalyst 6500 Series Switch Cisco IOS Command Reference</i>』を参照)</p> <p><b>ip auth-proxy watch-list</b></p> <p><b>show ip auth-proxy watch-list</b></p>
---------------	--

## ip auth-proxy watch-list

認証プロキシのウォッチ リストをイネーブルにして設定するには、`ip auth-proxy watch-list` コマンドを使用します。このコマンドの `no` 形式の使用法については、「使用上の注意事項」を参照してください。

```
ip auth-proxy watch-list {{add-item ip-addr} | enable | {expiry-time minutes}}
```

```
no ip auth-proxy watch-list [add-item ip-addr] | expiry-time]
```

### シンタックスの説明

<code>add-item ip-addr</code>	ウォッチ リストに IP アドレスを追加します。
<code>enable</code>	ウォッチ リストをイネーブルにします。
<code>expiry-time minutes</code>	エントリがウォッチ リストに存在する期間を指定します。有効値については、「使用上の注意事項」を参照してください。

### デフォルト

デフォルト設定は次のとおりです。

- `minutes` は 30 分です。
- ウォッチリスト機能はディセーブルです。

### コマンドモード

インターフェイス コンフィギュレーション

### コマンド履歴

リリース	変更内容
12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

### 使用上のガイドライン

分に使用できる値は、0 から最大 32 ビットの正の数字 (0x7FFFFFFF または 10 進数で 2147483647) です。`minutes` に 0 を設定することで、エントリをリスト内に永続的に存在させることができます。

このコマンドがサポートされるのは、ファイアウォール インターフェイス上のみです。

このコマンドの `no` 形式は、次の場合に使用します。

- `no ip auth-proxy watch-list` ウォッチ リストをディセーブルにします。
- `no ip auth-proxy watch-list add-item ip-addr` IP アドレスをウォッチ リストから削除します。
- `no ip auth-proxy watch-list expiry-time` デフォルトの設定に戻ります。

ウォッチリストのエントリは、`expiry-time minutes` で指定された時間ウォッチ リストに存在します。

ウォッチ リストをディセーブルにした場合、ウォッチ リストにエントリが追加されなくなり、セッションは `SERVICE_DENIED` 状態になります。セッションは、タイマーで 2 分が過ぎると削除されます。

### 例

次に、認証プロキシのウォッチ リストをイネーブルにする例を示します。

```
Router(config-if)# ip auth-proxy watch-list enable
Router(config-if)#
```

次に、認証プロキシのウォッチ リストをディセーブルにする例を示します。

```
Router(config-if)# no ip auth-proxy watch-list
Router(config-if)#
```

次に、ウォッチ リストに IP アドレスを追加する例を示します。

```
Router(config-if)# ip auth-proxy watch-list add-item 12.0.0.2
Router(config-if)#
```

次に、ウォッチ リストのエントリの継続時間を設定する例を示します。

```
Router(config-if)# ip auth-proxy watch-list expiry-time 29
Router(config-if)#
```

#### 関連コマンド

```
clear ip auth-proxy watch-list
ip auth-proxy max-login-attempts
show ip auth-proxy watch-list
```

## ip local-proxy-arp

ローカルのプロキシ Address Resolution Protocol (ARP) をイネーブルにするには、**ip local-proxy-arp** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
ip local-proxy-arp
no ip local-proxy-arp
```

**シンタックスの説明** このコマンドには、引数またはキーワードはありません。

**デフォルト** ディセーブル

**コマンドモード** インターフェイス コンフィギュレーション

コマンド履歴	リリース	変更内容
	12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

**使用上のガイドライン** ローカル プロキシ ARP 機能により、Multilayer Switch Feature Card (MSFC; マルチレイヤ スイッチ フィーチャ カード) 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 がイネーブルにされている場合、MSFC はサブ ネット内で 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、ホストが接続されている Catalyst 6500 シリーズ スイッチに直接通信することが意図的に禁止されているサブネット上でのみ使用されます。

Internet Control Message Protocol (ICMP) リダイレクトは、ローカル プロキシ ARP がイネーブルの インターフェイスでディセーブルです。

**例** 次に、ローカル プロキシ ARP をイネーブルにする例を示します。

```
Router(config-if)# ip local-proxy-arp
Router(config-if)#
```

# ip multicast rpf backoff

Protocol Independent Multicast (PIM) の待機時間を設定するには、**ip multicast rpf backoff** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
ip multicast rpf backoff {{min max} | disable}
```

```
no ip multicast rpf backoff
```

## シンタックスの説明

<i>min</i>	初期 RPF 延長待機時間(ミリ秒単位)。指定できる値は、1 ~ 65535 ミリ秒です。
<i>max</i>	最大 RPF 延長待機時間(ミリ秒単位)。指定できる値は、1 ~ 65535 ミリ秒です。
<b>disable</b>	起動型 RPF チェックをディセーブルにします。

## デフォルト

起動型 RPF チェックをイネーブルにした場合、デフォルトは次のとおりです。

- *min* は 50 ミリ秒です。
- *max* は 5000 ミリ秒です。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

リリース	変更内容
12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

## 使用上のガイドライン

起動型 Reverse Path Forwarding (RPF) チェックをイネーブルにしない場合、PIM が定期的にルーティング テーブルに変化がないかポーリングします (**ip multicast rpf interval** コマンドを使用して設定します)。起動型 RPF チェックをイネーブルにした場合、ルーティング テーブルが変更されたときに PIM がルーティング テーブルをポーリングします。*min* 引数は、初期待機時間を設定します。一度起動されると、PIM はさらにルーティング テーブルが変更されるのを待ちます。ルーティング テーブルの変更がさらに行われず *min* 時間が切れると、PIM はルーティング変更をスキャンします。待機時間内にさらにルーティング変更が行われた場合、PIM は待機時間を 2 倍に延長します。*max* 引数で、2 倍にした待機時間に対して最大時間を設定できます。

次のような場合、このコマンドを使用します。

- ルータでルート変更が頻繁に行われる場合 (たとえば、ダイヤルイン ルータなど)
- 最大 RPF チェック間隔を短くする場合 (新しく確立したルート上で IP マルチキャストの Availability を高速にするため)
- RPF チェック間隔を伸ばす場合 (RPF チェック導入による CPU の負荷を下げるため)

## 例

次に、PIM 待機時間をミリ秒単位で設定する例を示します。

```
Router(config)# ip multicast rpf backoff 100
Router(config)#
```

## 関連コマンド

**ip multicast rpf interval**

**show ip rpf events** (Cisco IOS のマニュアルを参照)

# ip multicast rpf interval

Reverse Path Forwarding (RPF) の整合性チェック間隔を設定するには、**ip multicast rpf interval** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
ip multicast rpf interval interval
```

```
no ip multicast rpf interval
```

<b>シンタックスの説明</b>	<i>interval</i>	RPF チェックの間隔 (秒単位)。有効値は、1 ~ 10 秒です。
------------------	-----------------	------------------------------------

<b>デフォルト</b>	10 秒
--------------	------

<b>コマンドモード</b>	グローバル コンフィギュレーション
----------------	-------------------

<b>コマンド履歴</b>	リリース	変更内容
	12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

<b>使用上のガイドライン</b>	<b>ip multicast rpf interval</b> コマンドは、Protocol Independent Multicast (PIM) 間隔を設定し、ルーティング テーブルに変化がないかポーリングします。
-------------------	--

<b>例</b>	次に、RPF 整合性チェック間隔を秒単位で設定する例を示します。
----------	----------------------------------

```
Router(config)# ip multicast rpf interval 5
Router(config)#
```

<b>関連コマンド</b>	<b>ip multicast rpf backoff</b>
---------------	---------------------------------

## ip verify unicast source reachable-via

Reverse Path Forwarding (RPF) チェックをイネーブルにして設定するには、`ip verify unicast source reachable-via` コマンドを使用します。RPF をディセーブルにするには、このコマンドの `no` 形式を使用します。

```
ip verify unicast source reachable-via {rx | any} [allow-default] [allow-self-ping] [list]
```

```
no ip verify unicast source reachable-via
```

### シンタックスの説明

<code>rx</code>	送信元アドレスがパケットが受信されたインターフェイスに到達可能かチェックします。
<code>any</code>	任意のパスで送信元アドレスが到達可能かチェックします。
<code>allow-default</code>	(任意) デフォルトのルートが送信元アドレスに一致するかチェックします。
<code>allow-self-ping</code>	(任意) ルータの self-ping を許可します。
<code>list</code>	(任意) アクセス リスト番号。標準 IP アクセス リスト番号の場合、有効値は 1 ~ 199 で、標準 IP 拡張アクセス リスト番号の有効値は、1300 ~ 2699 です。

### デフォルト

ユニキャスト RPF はディセーブルです。

### コマンドモード

インターフェイス コンフィギュレーション

### コマンド履歴

リリース	変更内容
12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

### 使用上のガイドライン

ユニキャスト RPF は、次に示す 3 つの基本モードを提供します。

- `exists-only` モード 送信元アドレスが Forwarding Information Base (FIB; 転送情報ベース) に存在すること、「本物の」インターフェイスから到達可能なことだけが必要とされます。これは、`ip verify unicast source reachable-via any allow-default` コマンドに対しても同様です。`exists-only` モードでは、逆引きで取得され、到達可能な送信元アドレスが FIB テーブルにあることが必須です。送信元アドレスは、設定されたインターフェイスから到達可能である必要があります。
- `any` モード 送信元が、任意のパスで到達可能である必要があります。たとえば、送信元には宛先別ロードバランスが備えられています。
- `Rx` モード 送信元アドレスは、到達したインターフェイスに到達可能である必要があります。たとえば、送信元はロードバランスなしで到達可能である必要があります。



(注)

ユニキャスト RPF は入力機能であり、接続のアップストリーム側になるルータの入力インターフェイスだけに適用されます。

ユニキャスト RPF を使用するには、ルータで Cisco Express Forwarding (CEF) スイッチングまたは distributed Cisco Express Forwarding (dCEF) スイッチングをイネーブルにする必要があります。CEF スイッチングに対して入力インターフェイスを設定する必要はありません。ルータが CEF で実行されている限り、他のスイッチング モードを個々のインターフェイスに設定できます。



(注) ユニキャスト RPF は、CEF なしで動作しません。

ユニキャスト RPF を内部ネットワーク インターフェイスで使用しないでください。内部インターフェイスでは、ルーティングが非対称であることが多く、パケットの送信元に複数のルートがあります。ユニキャスト RPF を適用するのは、対称性が存在する場合、または設定される場合だけです。

#### 例

次に、ユニキャスト RPF exist-only チェック モードをイネーブルにする例を示します。

```
Router(config-if)# ip verify unicast source reachable-via any
Router(config-if)#
```

#### 関連コマンド

ip cef (Cisco IOS マニュアルを参照)

## ip wccp accelerated

キャッシュ エンジン サービス グループの Web Cache Communication Protocol (WCCP) をイネーブルにするには、`ip wccp accelerated` コマンドを使用します。サービス グループのサポートを制御するルータの機能を削除するには、このコマンドの `no` 形式を使用します。

```
ip wccp {web-cache | service-number} accelerated {[group-address groupaddress] [redirect-list
access-list] [group-list access-list] [password password [0 | 7]]}
```

```
no ip wccp web-cache accelerated
```

### シンタックスの説明

<code>web-cache</code>	Web キャッシュ サービスをイネーブルにします。
<code>service-number</code>	WCCP サービス番号。有効な値は 0 ~ 99 です。
<code>group-address groupaddress</code>	(任意) WCCP サービス グループと通信するために、指定したマルチキャスト IP アドレスを使用するようにルータに指示します。詳細については「使用上の注意事項」を参照してください。
<code>redirect-list access-list</code>	(任意) このサービス グループにリダイレクトされるトラフィックを制御するために、アクセス リストを使用するようにルータに指示します。詳細については「使用上の注意事項」を参照してください。
<code>group-list access-list</code>	(任意) サービス グループへの参加が許可されているキャッシュ エンジンを判別するために、アクセス リストを使用するようにルータに指示します。詳細については「使用上の注意事項」を参照してください。
<code>password password</code>	(任意) サービス名で指定されたサービス グループから受信したメッセージに MD5 認証を適用するように、ルータに指示する文字列を指定します。詳細については「使用上の注意事項」を参照してください。

### デフォルト

ディセーブル

### コマンド モード

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更内容
12.2(18)SXF	このコマンドは、Supervisor Engine 720 をサポートするように変更されました。

### 使用上のガイドライン

このコマンドは、キャッシュ エンジンのソフトウェア リリース ACNS 4.2.1 以降のソフトウェア リリースでサポートされています。

WCCP サービスは、0 ~ 99 の数字で特定します。サービス グループで Cisco キャッシュ エンジンを使用している場合は、reverse-proxy サービスは 99 の値で示されます。

`group-address groupaddress` キーワードおよび引数にはマルチキャスト アドレスが必要です。ルータはこれを使用して、リダイレクトされたメッセージを受信するキャッシュ エンジンを判別します。このオプションは、このグループ アドレスで受信した「Here I Am」メッセージに対する「I See You」応答を結合するために、指定したマルチキャスト IP アドレスを使用するようにルータに指示します。この応答は、グループ アドレスにも送信されます。デフォルトでは、`group-address` は設定されていないため、すべての「Here I Am」メッセージにユニキャスト応答が返されます。

*redirect-list access-list* キーワードおよび引数は、サービス名で指定されたサービス グループの キャッシュ エンジンにリダイレクトされるトラフィックを制御するために、アクセス リストを使用するようにルータに指示します。*access-list* 引数では、1 ~ 99 の数値を指定して標準または拡張 アクセス リスト番号を表すか、または名前を指定して名前付きの標準または拡張アクセス リストを表します。アクセス リストは、リダイレクトを許可されるトラフィックを指定します。デフォルトでは、*redirect-list* は設定されていません (すべてのトラフィックがリダイレクトされます)。

*group-list access-list* キーワードおよび引数は、指定されたサービス グループへの参加が許可される キャッシュ エンジンを制御するために、アクセス リストを使用するようにルータに指示します。*access-list* 引数では、1 ~ 99 の数値を指定して標準アクセス リスト番号を表すか、または名前を指定して名前付きの標準アクセス リストを表します。アクセス リストは、サービス グループへの参加が許可されるキャッシュ エンジンを指定します。デフォルトでは、*group-list* は設定されていないため、すべてのキャッシュ エンジンがサービス グループに参加する可能性があります。

*password password* キーワードおよび引数は最大 7 文字まで指定できます。パスワードを指定すると、認証で受け入れられないメッセージは廃棄されます。パスワード名は HMAC MD5 値と結合され、ルータとキャッシュ エンジン間の接続にセキュリティを確立します。

**例** 次に、WCCP バージョン 1 のハードウェア アクセラレーションをイネーブルにする例を示します。

```
Router(config)# ip wccp web-cache accelerated
Router(config)#
```

**関連コマンド** `ip wccp version` (『*Catalyst 6500 Series Switch Cisco IOS Command Reference*』を参照)

## ip wccp

キャッシュ エンジン サービス グループのサポートをイネーブルにするには、**ip wccp** コマンドを使用します。サービス グループのサポートを制御するルータの機能を削除するには、このコマンドの **no** 形式を使用します。

```
ip wccp {web-cache | {service-number | service-name}} [redirect-list access-list]
[group-list access-list] [password password [0 | 7]]
```

```
no ip wccp {web-cache | service-number} [redirect-list access-list] [group-list access-list] [password
password [0 | 7]]
```

### シンタックスの説明

<i>web-cache</i>	Web キャッシュ サービスをイネーブルにします。
<i>service-number</i>	WCCP サービス番号。有効な値は 0 ~ 99 です。
<i>service-name</i>	WCCP サービス名。有効な値は <b>web-cache</b> です。
<i>redirect-list access-list</i>	(任意) このサービス グループにリダイレクトされるトラフィックを制御するために、アクセス リストを使用するようにルータに指示します。
<i>group-list access-list</i>	(任意) サービス グループへの参加が許可されているキャッシュ エンジン を判別するために、アクセス リストを使用するようにルータに指示します。
<i>password password</i>	(任意) サービス グループから受信したメッセージに MD5 認証を適用するように、ルータに指示します。

### デフォルト

WCCP サービスはイネーブルではありません。

### コマンドモード

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更内容
12.2(18)SXF	このコマンドのサポートが MSFC に追加されました。

### 使用上のガイドライン



(注)

**ip wccp {web-cache | service-number} group-list** コマンドの構文は、**ip wccp {web-cache | service-number} group-listen** コマンドの構文に似ていますが、これらは完全に別個のコマンドです。**ip wccp group-listen** コマンドはインターフェイス コンフィギュレーション コマンドであり、キャッシュ クラスタからのマルチキャスト通知を待ち受けるようインターフェイスを設定するのに使用されることに注意してください。詳細については、**ip wccp group-listen** コマンドを参照してください。

*service-number* は、提供された標準キーワード定義の 1 つ、またはダイナミックに定義されるキャッシュ エンジン定義を表す番号のどちらかです。サービスがイネーブルになると、ルータはサービス グループの確立に参加できます。

*service-number* を指定する場合に、サービス グループで Cisco キャッシュ エンジンを使用している場合は、99 の値を入力することで *reverse-proxy* サービスを示すことができます。

*access-list* 引数には、アクセス リストを指定する文字列を 64 文字 (名前または数字) 以内で指定できます。

認証で受け入れられないメッセージは廃棄されます。 *password* は最大 7 文字まで指定できます。

ファスト (CEF) スイッチングがイネーブルになっている場合は、WCCP 透過キャッシングは NAT をバイパスします。このような場合は、次の手順を実行して NAT がバイパスされないようにします。

- 
- ステップ 1** WCCP 透過キャッシングを発信方向に設定します。
  - ステップ 2** Content Engine インターフェイスでファスト / CEF スイッチングをイネーブルにします。
  - ステップ 3** `ip wccp web-cache redirect out` コマンドを入力します。
- 

`ip wccp redirect exclude in` コマンドをキャッシュ方向のルータ インターフェイスで指定することで、WCCP をインターフェイス内部で着信方向に設定できます。こうすることで、このインターフェイスに到着するパケットのリダイレクションが行われないようにします。

また、サービス グループの設定時にリダイレクト リストを指定できます。指定したリダイレクト リストにより、NAT (送信元) IP アドレスを持つパケットを拒否してリダイレクションが行われないようにします。

`ip wccp` コマンドを入力すると、ルータはスペースを割り当てて、サービス グループに参加するために指定された WCCP サービスのサポートをイネーブルにします。

`no ip wccp` コマンドを入力するときに、サービスが設定されているインターフェイスがない場合は、サービス グループへの参加が停止され、スペースの割当てが解除されます。そして、他のサービスが設定されていない場合は WCCP タスクが停止されます。

サービス名の後のキーワードはオプションであり、任意の順序で指定できますが、指定できるのは 1 度だけです。ここでは、このコマンドの各オプション形式の特定の使用方法について説明します。

---

**例** 次に、マルチキャスト アドレス 224.1.1.1 を使用して WCCP 逆プロキシ サービスを実行する例を示します。

```
Router# configure terminal
Router(config)# ip wccp 99 group-address 224.1.1.1
Router(config)# interface ethernet 0
Router(config-if)# ip wccp web-cache group-list
```

次に、宛先が 192.168.196.51 ではない Web 関連パケットをキャッシュ エンジンにリダイレクトする例を示します。

```
Router# configure terminal
Router(config)# access-list 100 deny ip any host 192.168.196.51
Router(config)# access-list 100 permit ip any any
Router(config)# ip wccp redirect-list 100
Router(config)# interface Ethernet 0
Router(config-if)# ip web-cache redirect-list
Router(config-if)# end
Router#
```

---

**関連コマンド** `ip wccp version`

# ip wccp group-listen

Web Cache Communication Protocol (WCCP) 機能向けの IP マルチキャストパケットの受信をイネーブルにするには、**ip wccp group-listen** コマンド モードを使用します。WCCP 機能向けの IP マルチキャストパケットの受信をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
ip wccp {web-cache | {service-number | service-name}} group-listen
```

```
no ip wccp {web-cache | {service-number | service-name}} group-listen
```

シンタックスの説明	web-cache	Web キャッシュ サービスにパケットを送信するようにルータに指示します。
	service-number	WCCP サービス番号。有効な値は 0 ~ 99 です。
	service-name	WCCP サービス名。有効な値は <b>web-cache</b> です。

**デフォルト**      ディセーブル

**コマンドモード**      インターフェイス コンフィギュレーション

コマンド履歴	リリース	変更内容
	12.2(18)SXF	このコマンドのサポートが MSFC に追加されました。

**使用上のガイドライン** *service-number* は、提供された標準キーワード定義の 1 つ、またはダイナミックに定義されるキャッシュ エンジン定義を表す番号のどちらかです。サービスがイネーブルになると、ルータはサービスグループの確立に参加できます。

ルータが IP マルチキャストの使用時にサービス グループのメンバとなる場合は、次の設定が必要です。

- WCCP サービス グループが使用する IP マルチキャスト アドレスを設定する必要があります。
- IP マルチキャスト アドレスを受信する必要があるルータのインターフェイス上で、**ip wccp {web-cache | service-number} group-listen** インターフェイス コンフィギュレーション コマンドを設定する必要があります。

**例**      次に、224.1.1.100 のマルチキャストアドレスを持つ Web キャッシュのマルチキャスト パケットをイネーブルにする例を示します。

```
router# configure terminal
router(config)# ip wccp web-cache group-address 244.1.1.100
router(config)# interface ethernet 0
router(config-if)# ip wccp web-cache group listen
```

**関連コマンド**      [ip wccp](#)  
[ip wccp redirect exclude](#)

# ip wccp redirect

Web Cache Communication Protocol (WCCP) を使用して発信または着信インターフェイス上でのパケットリダイレクションをイネーブルにするには、**ip wccp redirect** コマンドを使用します。WCCP リダイレクションをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
ip wccp service redirect {out | in}
```

```
no ip wccp service redirect {out | in}
```

シンタックスの説明	service	サービス グループ。有効な値は <i>web-cache</i> 、またはサービスの ID 番号 (0 ~ 99) です。
	out	発信インターフェイス上でのパケットリダイレクションを指定します。
	in	着信インターフェイス上でのパケットリダイレクションを指定します。

**デフォルト** WCCP のリダイレクトはディセーブルです。

**コマンドモード** インターフェイス コンフィギュレーション

コマンド履歴	リリース	変更内容
	12.2(18)SXF	このコマンドのサポートが MSFC に追加されました。

**使用上のガイドライン** 着信ネットワーク トラフィックを受信するインターフェイス上に WCCP リダイレクションを設定するには、**ip wccp service redirect in** コマンドを使用します。このコマンドがインターフェイスに適用されると、インターフェイスに到着するすべてのパケットは、指定された WCCP サービスが定義した基準と比較されます。基準に一致したパケットは、リダイレクトされます。

発信インターフェイス上で WCCP リダイレクション チェックを設定するには、**ip wccp service redirect out** コマンドを使用します。



## 注意

**ip wccp service redirect {out | in}** インターフェイス コンフィギュレーション コマンドと、**ip wccp redirect exclude in** インターフェイス コンフィギュレーション コマンドを混同しないよう気をつけてください。



## 注意

このコマンドは、**ip wccp redirect exclude in** コマンドに影響する可能性があります。(これらのコマンドは逆の機能を持ちます)。インターフェイス上に **ip wccp redirect exclude in** を設定し、さらに **ip wccp service redirect in** コマンドを設定すると、**ip wccp redirect exclude in** コマンドが無効にされます。その逆も同様です。**ip wccp redirect exclude in** コマンドを設定することで、**ip wccp service redirect in** コマンドは無効にされます。

**例** 次に、インターフェイス Ethernet 0 上の逆プロキシ パケットがリダイレクション チェックされ、Cisco キャッシュ エンジンへリダイレクトされるコンフィギュレーション セッションの例を示します。

```
Router# configure terminal
Router(config)# ip wccp 99
Router(config)# interface ethernet 0
Router(config-if)# ip wccp 99 redirect ?
    in  Redirect to a Cache Engine appropriate inbound packets
    out Redirect to a Cache Engine appropriate outbound packets
Router(config-if)# ip wccp 99 redirect out
```

次に、インターフェイス Ethernet 0/1 に到着する HTTP トラフィックが、Cisco キャッシュ エンジンへリダイレクトされるセッションを設定する例を示します。

```
Router# configure terminal
Router(config)# ip wccp web-cache
Router(config)# interface ethernet 0/1
Router(config-if)# ip wccp web-cache redirect in
```

**関連コマンド** `ip wccp redirect exclude in` (Cisco IOS のマニュアルを参照)

## ip wccp redirect exclude

Web Cache Communication Protocol (WCCP) を使用して発信または着信インターフェイス上でのパケット リダイレクションをイネーブルにするには、`ip wccp redirect exclude` コマンドを使用します。WCCP リダイレクションをディセーブルにするには、このコマンドの `no` 形式を使用します。

```
ip wccp {web-cache | service-number} redirect exclude in
```

```
no ip wccp {web-cache | service-number} redirect exclude in
```

### シンタックスの説明

<code>web-cache</code>	Web キャッシュ サービスをイネーブルにします。
<code>service-number</code>	ルータが制御するキャッシュ エンジン サービス グループの ID。有効な値は 0 ~ 99 です。
<code>redirect</code>	発信または着信インターフェイス上でのパケット リダイレクション チェックをイネーブルにします。
<code>exclude out</code>	発信インターフェイス上でのパケット リダイレクションを指定します。
<code>exclude in</code>	着信インターフェイス上でのパケット リダイレクションを指定します。

### デフォルト

ディセーブル

### コマンド モード

インターフェイス コンフィギュレーション

### コマンド履歴

リリース	変更内容
12.2(18)SXF	このコマンドのサポートが MSFC に追加されました。

### 使用上のガイドライン

このコマンドは、Supervisor Engine 720 で構成された Catalyst 6500 シリーズ スイッチ上ではサポートされません。

シスコのキャッシュ エンジンがキャッシュ クラスタで使用されている場合、`reverse proxy` サービスは 99 の `service-number` 値で示されます。

着信ネットワーク トラフィックを受信するインターフェイス上に WCCP リダイレクションを設定するには、`ip wccp redirect exclude in` コマンドを使用します。このコマンドがインターフェイスに適用されると、インターフェイスに到着するすべてのパケットは、指定された WCCP サービスが定義した基準と比較されます。基準に一致したパケットは、リダイレクトされます。

発信インターフェイス上で WCCP リダイレクション チェックを設定するには、`ip wccp redirect exclude out` コマンドを使用します。



(注)

このコマンドは、`ip wccp redirect in` コマンドに影響する可能性があります。インターフェイス上に `ip wccp redirect exclude in` コマンドを設定し、さらに `ip wccp redirect in` コマンドを設定すると、`ip wccp redirect exclude in` コマンドが無効にされます。その逆も同様です。`ip wccp redirect exclude in` コマンドを設定することで、`ip wccp redirect in` コマンドは無効にされます。

Release 12.0 以降に変更されたコマンドのリストを含む WCCP 設定コマンドの詳細な説明については、『Cisco IOS Configuration Fundamentals Command Reference』Release 12.1 の一部である『Cisco IOS System Management Commands』の「WCCP Commands」の章を参照してください。

**例** 次に、インターフェイス Ethernet 0 上の逆プロキシ パケットがリダイレクション チェックされ、Cisco キャッシュ エンジンへリダイレクトされるコンフィギュレーション セッションの例を示します。

```
Router# configure terminal
Router(config)# ip wccp 99
Router(config)# interface ethernet 0
Router(config-if)# ip wccp 99 redirect exclude out
```

次に、インターフェイス Ethernet 0/1 に到着する HTTP トラフィックが、Cisco キャッシュ エンジンへリダイレクトされるセッションを設定する例を示します。

```
Router# configure terminal
Router(config)# ip wccp web-cache
Router(config)# interface ethernet 0/1
Router(config-if)# ip wccp web-cache redirect exclude in
```

#### 関連コマンド

**ip wccp redirect exclude in** (『*Catalyst 6500 Series Switch Cisco IOS Command Reference*』を参照)

**show ip interface** (『*Catalyst 6500 Series Switch Cisco IOS Command Reference*』を参照)

**show ip wccp** (『*Catalyst 6500 Series Switch Cisco IOS Command Reference*』を参照)

## ipx network

特定のインターフェイス上で Internetwork Packet Exchange (IPX) ルーティングをイネーブルにし、任意でカプセル化 (フレーム化) の形式を選択するには、**ipx network** コマンドを使用します。IPX ルーティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
ipx network network [encapsulation encapsulation-type [secondary]]
```

```
no ipx network network [encapsulation encapsulation-type]
```

### シンタックスの説明

<i>network</i>	ネットワーク番号。
<i>encapsulation encapsulation-type</i>	(任意)カプセル化(フレーム化)形式。使用可能なカプセル化形式のリストは、 <a href="#">表 2-1</a> を参照してください。
<i>secondary</i>	(任意)最初の(プライマリ)ネットワークのあとに構成される、追加の(セカンダリ)ネットワークを指定します。

### デフォルト

デフォルト設定は次のとおりです。

- IPX ルーティングはディセーブルです。
- カプセル化形式は次のとおりです。
  - イーサネット : **novell-ether**
  - トークンリング : **sap**
  - FDDI : **snap**
  - シリアル : **hdlc**

NetWare のバージョン 4.0 およびイーサネットを使用している場合、デフォルト設定のカプセル化形式を、*novell-ether* から *sap* に変更する必要があります。

### コマンドモード

インターフェイス コンフィギュレーション

### コマンド履歴

リリース	変更内容
12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

### 使用上のガイドライン

*network* には、ネットワーク ケーブルによるセグメントを一意に識別する 8 桁の番号 (16 進数) が使用されます。使用可能な範囲は 1 ~ FFFFFFFD です。*network* 番号に 0 から始まる数字を指定する必要はありません。たとえば、ネットワーク番号 000000AA に対し、AA を入力できます。

**alt** キーワードを使用することで、代替コンフィギュレーションを指定できます。次のように使用されます。

```
[no] ipx network network [encapsulation encapsulation-type [secondary]] [alt [no] ipx network network [encapsulation encapsulation-type [secondary]]]
```

[表 2-1](#) には、指定のインターフェイスで使用できるカプセル化形式を示しています。

表 2-1 カプセル化形式

カプセル化形式	説明
arpa	イーサネット インターフェイス専用 Novell の Ethernet_II カプセル化を使用します。このカプセル化は、TCP/IP および IPX トラフィックの両方を処理するネットワークを扱う場合に推奨します。
hdlc	シリアル インターフェイス専用 High-Level Data Link Control ( HDLC; ハイレベル データリンク コントロール ) のカプセル化を使用します。
novell-ether	イーサネット インターフェイス専用 Novell の Ethernet_802.3 カプセル化を使用します。このカプセル化は、チェックサム FFFF の IPX ヘッダーに続く、標準 802.3 Media Access Control ( MAC; メディア アクセス制御 ) ヘッダーで構成されています。novell-ether は、すべての NetWare バージョンで使用される ( バージョン 3.11 ~ 現在まで ) カプセル化のデフォルト設定です。
novell-fddi	FDDI インターフェイス専用 Novell の FDDI_RAW カプセル化を使用します。このカプセル化は、チェックサム 0xFFFF の IPX ヘッダーに直接続く、標準 Fiber Distributed Data Interface ( FDDI ) MAC ヘッダーで構成されています。
sap	<ul style="list-style-type: none"> <li>イーサネット インターフェイス用 Novell の Ethernet_802.2 カプセル化を使用します。このカプセル化は、802.2 Logical Link Control ( LLC; 論理リンク制御 ) ヘッダーに続く、標準 802.3 MAC ヘッダーで構成されています。sap は、NetWare バージョン 3.12 および 4.0 で使用されるデフォルトのカプセル化です。</li> <li>トークンリング インターフェイス用 このカプセル化は、802.2 LLC ヘッダーに続く、標準 802.5 MAC ヘッダーで構成されています。</li> <li>FDDI インターフェイス用 このカプセル化は、802.2 LLC ヘッダーに続く、標準 FDDI MAC ヘッダーで構成されています。</li> </ul>
snap	<ul style="list-style-type: none"> <li>イーサネット インターフェイス専用 Novell Ethernet_Snap カプセル化を使用します。このカプセル化は、802.2 Subnetwork Access Protocol ( SNAP ) LLC ヘッダーに続く、標準 802.3 MAC ヘッダーで構成されています。</li> <li>トークンリングおよび FDDI インターフェイス用 このカプセル化は、802.2 SNAP LLC ヘッダーに続く、標準 802.5 または FDDI MAC ヘッダーで構成されています。</li> </ul>

ipx network コマンドを使用することで、1つの物理ネットワークに1つの論理ネットワーク、または同一の物理ネットワーク ( ネットワーク ケーブル セグメント ) に複数の論理ネットワークを設定できます。指定のインターフェイス上の各ネットワークは異なるカプセル化形式を使用する必要があります。



(注)

ipx network コマンドを使用して、ルータ上に 200 IPX インターフェイスより多く設定することはできません。

インターフェイス上に設定する最初のネットワークは、プライマリ ネットワークとみなされます。追加のネットワークはいずれもセカンダリ ネットワークとみなされます。追加のネットワークには、secondary キーワードが含まれている必要があります。



(注)

Cisco IOS ソフトウェアのリリースで、将来的にプライマリおよびセカンダリ ネットワークがサポートされることはありません。

Network Link Service Protocol (NLSP) はセカンダリ ネットワークをサポートしません。NLSP で複数のカプセル化を使用するためには、サブインターフェイスを使う必要があります。



(注)

NLSP をイネーブルにし、同一の物理 LAN インターフェイス上に複数のカプセル化を設定する場合、サブインターフェイスを使用する必要があります。セカンダリ ネットワークを使用することはできません。

すべてのネットワークが、カプセル化形式の区別されている同一の物理インターフェイス上にある限り、サポートされるインターフェイス上で IPX ネットワークを設定できます。たとえば、イーサネットは4つのカプセル化形式をサポートするため、1つのイーサネット ケーブル上に4つの IPX ネットワークまで設定できます。

インターフェイスは、正常にカプセル化された、正常なネットワーク番号を持つパケットのみ処理します。他のカプセル化を使用する IPX ネットワークが、物理ネットワーク上に存在することも可能です。ルータに発生する唯一の影響は、パケットのカプセル化が正常に行われているか判断するために、ある程度の処理時間が必要になることです。

インターフェイス上のすべての論理ネットワークは、同一の設定パラメータ セットを共有します。たとえば、インターフェイス上の IPX の Routing Information Protocol (RIP) 更新時間を変更する場合、そのインターフェイスのすべてのネットワークの値が変更されます。

同一の物理ネットワーク上で、複数の論理ネットワークを定義した場合、IPX は異なる物理ネットワークにカプセルがあるかのように各カプセルを処理します。たとえば、各論理ネットワークに IPX は RIP 更新および Service Advertisement Protocol (SAP) 更新を送信することになります。

あるカプセル化形式を他の形式に移行する場合、`ipx network` コマンドを利用できます。この目的でコマンドを使用する場合、プライマリ ネットワークに新しいカプセル化を定義する必要があります。

インターフェイス上のすべてのネットワークを削除するには、次のコマンドを使用します。

```
no ipx network
```

次のコマンドでプライマリ ネットワークを削除した場合も、インターフェイス上のすべてのネットワークを削除することになります。引数の *number* は、プライマリ ネットワークの番号です。

```
no ipx network number
```

インターフェイス上のセカンダリ ネットワークを削除するには、次のコマンドを使用します。引数の *number* は、セカンダリ ネットワークの番号です。

```
no ipx network number
```

```
no ipx network number encapsulation encapsulation-type
```

Novell の FDDI\_RAW カプセル化は、FDDI バックボーンを通じてイーサネットベースの Novell の 終端ホストに接続されたブリッジまたはスイッチの環境で共通です。FDDI\_RAW カプセル化のパケットは Novell パケットとして分類され、ブリッジングおよび IPX ルーティングをイネーブルにしている場合でも、自動的にブリッジされません。さらに、IPX を独立して設定した、または Silicon Switching Engine (SSE; シリコン スイッチング エンジン) スイッチングを設定したインターフェイス上で FDDI\_RAW カプセル化を設定することはできません。同様に、FDDI\_RAW カプセル化が設定されたインターフェイス上で、独立した IPX、または SSE スイッチングをイネーブルにすることはできません。

FDDI\_RAW カプセル化により、CBUS アーキテクチャを使用しないプラットフォームは、高速スイッチングをサポートします。CBUS アーキテクチャを使用するプラットフォームは、FDDI インターフェイスで受信した *novell-fddi* パケットのスイッチング処理のみをサポートします。

---

**例**

次に、サブインターフェイスを使用し、インターフェイス Ethernet 0 に、4 つの論理ネットワークを作成する例を示します。各サブインターフェイスは異なるカプセル化方式を使用しています。各サブインターフェイス上で指定するすべてのインターフェイスの設定パラメータは、そのサブインターフェイスのみに適用されます。

```
ipx routing
interface ethernet 0
  ipx network 1 encapsulation novell-ether

interface ethernet 0.1
  ipx network 2 encapsulation snap

interface ethernet 0.2
  ipx network 3 encapsulation arpa

interface ethernet 0
  ipx network 4 encapsulation sap
```

次に、プライマリおよびセカンダリ ネットワークを使用し、前に示したネットワークと同一の4つの論理ネットワークを作成する例を示します。このインターフェイス上で指定するすべてのインターフェイスの設定パラメータは、すべての論理ネットワークに適用されます。たとえば、ルーティング更新タイマーを 120 秒に設定した場合、この値は4つすべてのネットワーク上で使用されます。

```
ipx routing
ipx network 1 encapsulation novell-ether
ipx network 2 encapsulation snap secondary
ipx network 3 encapsulation arpa secondary
ipx network 4 encapsulation sap secondary
```

次に、インターフェイス FDDI 0.2 および 0.3 の IPX ルーティングをイネーブルにする例を示します。インターフェイス FDDI 0.2 上のカプセル化形式は SNAP です。インターフェイス FDDI 0.3 上のカプセル化形式は Novell の FDDI\_RAW です。

```
ipx routing

interface fddi 0.2 enc sde 2
  ipx network f02 encapsulation snap

interface fddi 0.3 enc sde 3
  ipx network f03 encapsulation novell-fddi
```

---

**関連コマンド**

**ipx routing** (Cisco IOS マニュアルを参照)

# maximum-paths

IP ルーティング プロトコルがサポートできる最大パラレル ルート数を制御するには、**maximum-paths** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

**maximum-paths** *maximum*

**no maximum-paths**

<b>シンタックスの説明</b>	<i>maximum</i>	IP ルーティング プロトコルがルーティング テーブルにインストールする最大パラレル ルート数。指定できる値は、1 ~ 8 です。
------------------	----------------	---

**デフォルト** デフォルト設定は次のとおりです。

- Border Gateway Protocol (BGP) に 1 つのパスがあります。
- 他のすべての IP ルーティング プロトコルには 4 つのパスがあります。

**コマンドモード** ルーティング プロトコル コンフィギュレーション

<b>コマンド履歴</b>	<b>リリース</b>	<b>変更内容</b>
	12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

**例** 次に、宛先に最大 2 つのパスを許可する例を示します。

```
Router (config) # maximum-paths 2
Router (config) #
```

# mls aclmerge algorithm

使用する Access Control List (ACL; アクセス コントロール リスト) マージのタイプを選択するには、`mls aclmerge algorithm` コマンドを使用します。

```
mls aclmerge algorithm {bdd | odm}
```

シンタックスの説明	bdd	BDD ベースの ACL マージ関数を指定します。
	odm	ODM ベースの ACL マージ関数を指定します。

デフォルト `bdd`

コマンドモード グローバル コンフィギュレーション

コマンド履歴	リリース	変更内容
	12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

**使用上のガイドライン** ブーリアン演算法を使用してエントリを縮約し、マージされた単一 Ternary CAM (TCAM) エントリ リストにするには、Binary Decision Diagram (BDD) ベースの ACL マージ関数を使用します。そのあと、TCAM エントリ リストから TCAM がプログラムされます。

Order-Dependent Merge (ODM) アルゴリズムを使用して、TCAM にプログラムできるエントリを処理するには、ODM ベースの ACL マージ関数を使用します。



**(注)** Cisco IOS Release 12.2(14)SX では、`bdd` キーワードは、Supervisor Engine 2 で構成されたシステム上でサポートされません。`bdd` キーワードは、Supervisor Engine 720 で構成されたシステム上ではサポートされません。



**(注)** Cisco IOS Release 12.1(12c)E1 より前のリリースでは、ODM ベースの ACL マージ関数はセキュリティ ACL のみをサポートし、Quality of Service (QoS; サービス品質) フィルタリングが使用されている ACL には適用されません。Cisco IOS Release 12.1(12c)E1 以上のリリースでは、ODM ベースの ACL マージ関数はセキュリティ ACL および QoS フィルタリングが使用されている ACL をサポートします。

アルゴリズム方式を変更すると、その変更は以前のものに適用されません。たとえば、マージがすでに適用された ACL には作用しません。マージの変更は、将来のマージに対してのみ適用します。

現在のマージ方式のステータスを参照するには、`show fm summary` コマンドを使用します。

**例** 次に、BDD ベースの ACL マージを選択して、ACL を処理する例を示します。

```
Router(config)# mls aclmerge algorithm bdd
The algorithm chosen will take effect for new ACLs which are being applied, not
for already applied ACLs.
Router(config)
```

次に、ODM ベースの ACL マージを選択して、ACL を処理する例を示します。

```
Router(config)# mls aclmerge algorithm odm
The algorithm chosen will take effect for new ACLs which are being applied, not
for already applied ACLs.
Router(config)#
```

**関連コマンド** [show fm summary](#)

## mls ip

インターフェイスの内部ルータの Multilayer Switching (MLS; マルチレイヤ スイッチング) IP をイネーブルにするには、`mls ip` コマンドを使用します。インターフェイス上で MLS IP をディセーブルにするには、このコマンドの `no` 形式を使用します。

```
mls ip
no mls ip
```

**シンタックスの説明** このコマンドには、引数またはキーワードはありません。

**デフォルト** マルチキャストはディセーブルです。

**コマンドモード** インターフェイス コンフィギュレーション

リリース	変更内容
12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

**例** 次に、MLS IP ショートカットをイネーブルにする例を示します。

```
Router(config-if)# mls ip
Router(config-if)#
```

**関連コマンド** `mls rp ip` (インターフェイス コンフィギュレーション モード) ([『Catalyst 6500 Series Switch Cisco IOS Command Reference』](#) を参照)  
`show mls ip multicast` ([『Catalyst 6500 Series Switch Cisco IOS Command Reference』](#) を参照)

# mls ip cef load-sharing

CEF ロード バランシングを設定するには、`mls ip cef load-sharing` コマンドを使用します。デフォルト設定に戻すには、このコマンドの `no` 形式を使用します。

```
mls ip cef load-sharing [full [exclude-port {destination | source}]] [simple]
```

```
no mls ip cef load-sharing
```

シンタックスの説明	full	(任意)送信元および宛先レイヤ 4 ポートと送信元および宛先 IP アドレス(レイヤ 3)を含めるように CEF ロード バランシングを設定します。
	<code>exclude-port destination</code>	(任意)宛先レイヤ 4 ポートと送信元および宛先 IP アドレス(レイヤ 3)をロード バランシング アルゴリズムから除外します。
	<code>exclude-port source</code>	(任意)送信元レイヤ 4 ポートと送信元および宛先 IP アドレス(レイヤ 3)をロード バランシング アルゴリズムから除外します。
	<code>simple</code>	(任意)シングルステージのロード シェアリングの CEF ロード バランシングを設定します。

**デフォルト** 送信元 IP アドレスおよび汎用 ID です。

**コマンド モード** グローバル コンフィギュレーション

コマンド履歴	リリース	変更内容
	12.2(17a)SXA	Supervisor Engine 2 でのこのコマンドのサポートが 12.2 SX リリースにも拡張されました。
	12.2(18)SXE	このコマンドは、Supervisor Engine 720 上でのみ <code>exclude-port</code> 、 <code>destination</code> 、および <code>source</code> キーワードを含むように変更されました。
	12.2(18)SXF6	このコマンドは、次のように変更されました。 <ul style="list-style-type: none"> <li>• <code>simple</code> キーワードが追加されました。</li> <li>• このコマンドのサポートが PFC3 に追加されました。</li> </ul>

**使用上のガイドライン** `mls ip cef load-sharing` コマンドは、IPv4、IPv6、および MPLS 転送に影響を与えます。

`mls ip cef load-sharing` コマンドの構造は次のとおりです。

- `mls ip cef load-sharing full` 複数の隣接関係を持つレイヤ 3 およびレイヤ 4 情報を使用します。
- `mls ip cef load-sharing full simple` 複数の隣接関係を持たないレイヤ 3 およびレイヤ 4 情報を使用します
- `mls ip cef load-sharing simple` 複数の隣接関係を持たないレイヤ 3 情報を使用します

その他の注意事項については、『*Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide*』を参照してください。

**例** 次に、複数の隣接関係を持つレイヤ 3 およびレイヤ 4 ポートを含めるようにロード バランシングを設定する例を示します。

```
Router(config)# mls ip cef load-sharing full
Router(config)#
```

## ■ mls ip cef load-sharing

次に、宛先レイヤ 4 ポートと送信元および宛先 IP アドレス (レイヤ 3) をロード バランシング アルゴリズムから除外するようにロード バランシングを設定する例を示します。

```
Router(config)# mls ip cef load-sharing full exclude-port destination
Router(config)#
```

次に、送信元レイヤ 4 ポートと送信元および宛先 IP アドレス (レイヤ 3) をロード バランシング アルゴリズムから除外するようにロード バランシングを設定する例を示します。

```
Router(config)# mls ip cef load-sharing full exclude-port source
Router(config)#
```

次に、デフォルト設定に戻す例を示します。

```
Router(config)# no mls ip cef load-sharing
Router(config)#
```

## 関連コマンド

コマンド	説明
show running-config	『Catalyst 6500 Series Switch Cisco IOS Command Reference』を参照してください。

## mls ip cef rate-limit

Cisco Express Forwarding (CEF) によりパントされたデータ パケットをレート制限するには、**mls ip cef rate-limit** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
mls ip cef rate-limit pps
```

```
no mls ip cef rate-limit
```

### シンタックスの説明

*pps* データ パケットの番号。有効値は 0 ~ 1000000 です。

### デフォルト

レート制限は設定されていません。

### コマンド モード

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更内容
12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

### 使用上のガイドライン

**mls ip cef rate-limit** コマンドは、Supervisor Engine 2 のみで構成されているシステム上でサポートされます。

特定の Denial-of-Service (DoS) 攻撃は、ルータのルート処理エンジンをターゲットにしています。PFC2 で転送できない特定のパケットは、MSFC2 に転送されて処理されます。DoS 攻撃が発生すると、ルータ処理エンジンは過負荷になり、動的なルーティング プロトコルの稼働時にはルーティングが不安定になることがあります。MSFC2 に送信されるトラフィック量を制限し、ルート処理エンジンへのサービス妨害攻撃を防ぐには、**mls ip cef rate-limit** コマンドを使用します。

このコマンドは、次のパケットを含めて、CEF によりパントされたすべてのデータ パケットのレートを制限します。

- ローカル インターフェイス IP アドレス宛のデータパケット
- Address Resolution Protocol (ARP) を必要とするデータパケット

低いレートを設定すると、ローカル インターフェイスの IP アドレス宛のパケット、および ARP を必要とするパケットの処理に影響が及びます。

このコマンドは、これらのパケットを通常の標準レートに制限して、異常な着信レートを回避する場合に使用してください。

その他の注意事項については、『*Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide*』を参照してください。

### 例

次に、レート制限機能をイネーブルにして、設定する例を示します。

```
Router(config)# mls ip cef rate-limit 50000
Router(config)#
```

### 関連コマンド

**set mls rate** (『*Catalyst 6500 Series Switch Command Reference*』を参照)

## mls ip cef rpf interface-group

RPF\_VLAN テーブルのインターフェイス グループを定義するには、**mls ip cef rpf interface-group** コマンドを使用します。インターフェイス グループを削除するには、このコマンドの **no** 形式を使用します。

```
mls ip cef rpf interface-group group-number interface1 interface2 interface3 [...]
```

```
no mls ip cef rpf interface-group group-number interface1 interface2 interface3 [...]
```

### シンタックスの説明

<i>group-number</i>	インターフェイス グループ番号。指定できる値は 1 ~ 4 です。
<i>interface</i>	インターフェイス番号。フォーマットの注意事項については、「使用上の注意事項」を参照してください。
...	追加のインターフェイス番号。詳細については、「使用上の注意事項」を参照してください。

### デフォルト

グループは設定されていません。

### コマンドモード

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更内容
12.2(17a)SXA	このコマンドのサポートが MSFC3 に追加されました。

### 使用上のガイドライン

このコマンドをサポートするのは、MSFC3 のみです。

1 つのインターフェイス グループには、3 ~ 6 個のインターフェイスが含まれています。最大 4 つのインターフェイス グループを設定できます。各インターフェイス グループには、最初の 4 つのエントリがハードウェアの RPF\_VLAN テーブルに設定されます。

*interface* は、次のように入力します。

```
interface-typemod/port
```

スペースで各インターフェイスのエントリを区切ります。*interface-type* と *mod/port* の引数の間にはスペースを含める必要はありません。「例」でサンプルを参照してください。

### 例

次に、インターフェイス グループを定義する例を示します。

```
Router(config)# mls ip cef rpf interface-group 0 F2/1 F2/2 F2/3 F2/4 F2/5 F2/6
Router(config)#
```

### 関連コマンド

[show mls cef ip](#)

# mls ip cef rpf multipath

Reverse Path Forwarding (RPF) モードを設定するには、**mls ip cef rpf multipath** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

```
mls ip cef rpf multipath {interface-group | punt | pass}
```

シンタックスの説明		
<b>interface-group</b>	複数のパス ルートから着信するパケットの RPF チェックをディセーブルにします。詳細については、「使用上の注意事項」を参照してください。	
<b>punt</b>	RPF が失敗したパケットを複数パスのプレフィクスをサポートする RP にリダイレクトします。	
<b>pass</b>	複数のパス ルートから着信するパケットの RPF チェックをディセーブルにします。	

**デフォルト** punt

**コマンドモード** グローバル コンフィギュレーション

コマンド履歴	リリース	変更内容
	12.2(17a)SXA	このコマンドのサポートが MSFC3 に追加されました。

**使用上のガイドライン** このコマンドをサポートするのは、MSFC3 のみです。

**interface-group** モードは **pass** モードと類似していますが、RPF チェックの RPF\_VLAN グローバル テーブルを使用します。他の複数のパス プレフィクスからのパケットは常に RPF チェックを通過します。

RPF\_VLAN テーブルのインターフェイス グループを定義するには、**mls ip cef rpf multipath interface-group** コマンドを入力します。1 つのインターフェイス グループには、3 ~ 6 のインターフェイスが含まれており、最大 4 つのインターフェイス グループを設定できます。各インターフェイス グループには、最初の 4 つのエントリがハードウェアの RPF\_VLAN テーブルに設定されます。4 つ以上の複数のパスを持ち、さらに 2 つ以外のすべてのパスがそのインターフェイス グループに属している各プレフィクスに対して、プレフィクスの Forwarding Information Base (FIB; 転送情報ベース) エントリはこの RPF\_VLAN エントリを使用します。

**例** 次に、RPF が失敗したパケットを複数パスのプレフィクスをサポートする RP にリダイレクトする例を示します。

```
Router(config)# mls ip cef rpf multipath interface-group
Router(config)#
```

**関連コマンド** [show mls cef ip](#)

# mls ip delete-threshold

設定した ACL しきい値を削除するには、**mls ip delete-threshold** コマンドを使用します。

```
mls ip delete-threshold acl-num
```

<b>シンタックスの説明</b>	<i>acl-num</i> 再帰 ACL 番号。有効値は 1 ~ 10000 です。
------------------	---

<b>デフォルト</b>	このコマンドにはデフォルト設定がありません。
--------------	------------------------

<b>コマンドモード</b>	グローバル コンフィギュレーション
----------------	-------------------

<b>コマンド履歴</b>	<b>リリース</b>	<b>変更内容</b>
	12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

<b>使用上のガイドライン</b>	<b>mls ip delete-threshold</b> コマンドは、 <b>mls ip reflexive ndr-entry tcam</b> コマンドをイネーブルにした場合のみ、アクティブになります。
-------------------	--

<b>例</b>	次に、Access Control List (ACL; アクセス コントロール リスト) しきい値を削除する例を示します。
----------	--

```
Router(config)# mls ip delete-threshold 223
Router(config)#
```

<b>関連コマンド</b>	<a href="#">mls ip install-threshold</a> <b>mls ip reflexive ndr-entry tcam</b> (『 <i>Catalyst 6500 Series Switch Cisco IOS Command Reference</i> 』を参照)
---------------	--

## mls ip inspect

他のインターフェイスのトラフィックを拒否する Access Control List (ACL; アクセスコントロールリスト) のトラフィックを許可するには、**mls ip inspect** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
mls ip inspect acl-name
```

```
no mls ip inspect acl-name
```

### シンタックスの説明

<i>acl-name</i>	ACL 名
-----------------	-------

### デフォルト

トラフィックの許可はディセーブルです。

### コマンドモード

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更内容
12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

### 使用上のガイドライン

Catalyst 6500 シリーズスイッチでは、インターフェイスがトラフィックを拒否する設定の場合、**ip inspect** コマンドで設定されたインターフェイスを通じてのみ、Context-Based Access Control (CBAC; コンテキストベースのアクセス制御) はトラフィックの双方向の通過を許可します。

### 例

次に、特定の ACL (`deny_ftp_c` という名前) を通じてトラフィックを許可する例を示します。

```
Router(config)# mls ip inspect deny_ftp_c
Router(config)#
```

### 関連コマンド

**ip inspect** (Cisco IOS マニュアルを参照)

# mls ip install-threshold

設定した Access Control List (ACL; アクセス コントロール リスト) スレッショールドを導入するには、**mls ip install-threshold** コマンドを使用します。

```
mls ip install-threshold acl-num
```

<b>シンタックスの説明</b>	<i>acl-num</i> 再帰 ACL 番号。有効値は 1 ~ 10000 です。
------------------	---

<b>デフォルト</b>	このコマンドにはデフォルト設定がありません。
--------------	------------------------

<b>コマンドモード</b>	グローバル コンフィギュレーション
----------------	-------------------

コマンド履歴	リリース	変更内容
	12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

<b>使用上のガイドライン</b>	<b>mls ip install-threshold</b> コマンドは、 <b>mls ip reflexive ndr-entry tcam</b> コマンドをイネーブルにした場合のみ、アクティブになります。
-------------------	---

<b>例</b>	次に、ACL しきい値を導入する例を示します。
----------	-------------------------

```
Router(config)# mls ip install-threshold 123
Router(config)#
```

<b>関連コマンド</b>	<b>mls ip delete-threshold</b> <b>mls ip reflexive ndr-entry tcam</b> (『 <i>Catalyst 6500 Series Switch Cisco IOS Command Reference</i> 』を参照)
---------------	--

## mls ip multicast consistency-check

ハードウェアによるショートカットの整合性チェッカーをイネーブルにして設定するには、**mls ip multicast consistency-check** コマンドを使用します。整合性チェッカーをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
mls ip multicast consistency-check [{settle-time seconds} | {type scan-mroute [count count-number]
| {period seconds}}]
```

```
no mls ip multicast consistency-check
```

### シンタックスの説明

<b>settle-time seconds</b>	(任意) 整合性チェッカーの entry/oif の整合時間を指定します。有効値は 2 ~ 3600 秒です。
<b>type scan-mroute</b>	(任意) mroute テーブルのスキャン チェックとして、整合性チェックのタイプを指定します。
<b>count count-number</b>	(任意) 各スキャンでチェックする最大プレフィクス数を指定します。有効値は 2 ~ 500 です。
<b>period seconds</b>	スキャン間隔を指定します。有効値は 2 ~ 3600 秒です。

### デフォルト

デフォルト設定は次のとおりです。

- 整合性チェックはイネーブルです。
- **count count-number** は 20 秒です。
- **period seconds** は 2 秒です。
- **settle-time seconds** は 60 秒です。

### コマンドモード

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更内容
12.2(18)SXF	このコマンドのサポートが MSFC に追加されました。

### 使用上のガイドライン

*oif* は、マルチキャスト {\*,G} または {source, group} フローの出力インターフェイスです。

整合性チェッカーは mroute テーブルをスキャンし、マルチキャスト ハードウェアのエントリが mroute テーブルと整合性があるか確認します。不整合が検出された場合は、常に自動的に修正されます。

不整合エラーを表示するには、**show mls ip multicast consistency-check** コマンドを使用します。

### 例

次に、ハードウェアによるショートカット整合性チェッカーをイネーブルにする例を示します。

```
Router (config)# mls ip multicast consistency-check
Router (config)#
```

次に、ハードウェアによるショートカット整合性チェッカーをイネーブルにし、mroute テーブルのスキャン チェックを設定する例を示します。

```
Router (config)# mls ip multicast consistency-check type scan-mroute count 20 period 35
Router (config)#
```

## ■ mls ip multicast consistency-check

次に、ハードウェアによるショートカット整合性チェッカーをイネーブルにし、スキャン間隔を指定する例を示します。

```
Router (config)# mls ip multicast consistency-check type scan-mroute period 35
Router (config)#
```

## 関連コマンド

**show mls ip multicast consistency-check** (『*Catalyst 6500 Series Switch Cisco IOS Command Reference*』を参照)

## mls ip multicast stub

Protocol Independent Multicast (PIM) sparse (疎) モードのスタブ ネットワークに対して非 Reverse Path Forwarding (RPF) トラフィック廃棄のサポートをイネーブルにするには、**mls ip multicast stub** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
mls ip multicast stub
```

```
no mls ip stub
```

**シンタックスの説明** このコマンドには、引数またはキーワードはありません。

**デフォルト** ディセーブル

**コマンドモード** インターフェイス コンフィギュレーション

### コマンド履歴

リリース	変更内容
12.2(14)SX	このコマンドのサポートが MSFC に追加されました。

### 使用上のガイドライン

冗長ルータ上で **mls ip multicast stub** コマンドを入力して、Access Control List (ACL; アクセスコントロール リスト) ベースの RPF 障害フィルタリング方式をイネーブルにすると、次の ACL が自動的に Policy Feature Card (PFC; ポリシー フィーチャ カード) にダウンロードされ、指定したインターフェイスに適用されます。

- access-list 100 permit ip A.B.C.0 0.0.0.255 any
- access-list 100 permit ip A.B.D.0 0.0.0.255 any
- access-list 100 permit ip any 224.0.0.0 0.0.0.255
- access-list 100 permit ip any 224.0.1.0 0.0.0.255
- access-list 100 deny ip any 224.0.0.0 15.255.255.255

これらの ACL によって、ハードウェアで RPF 障害がフィルタおよび廃棄され、ルータに転送されなくなります。

ACL ベースの RPF 障害フィルタリング方式は、ダウンストリーム ルータの存在しない、sparse モードのスタブ ネットワークに限って使用してください。dense (密) モード グループの場合に、PIM アサート メカニズムを正常に動作させるには、ルータ上で RPF 障害パケットが認識されなければなりません。dense モードのネットワーク、および sparse モードの中継ネットワークでは、Cisco Express Forwarding (CEF) または NetFlow ベースのレート制限を使用して、RPF 障害のレートを制限してください。

**例** 次に、PIM sparse モードのスタブ ネットワークに対して、非 RPF トラフィック廃棄のサポートをイネーブルにする例を示します。

```
Router(config-if)# mls ip multicast stub
Router(config-if)#
```

**関連コマンド** **show mls ip multicast** (『Catalyst 6500 Series Switch Cisco IOS Command Reference』を参照)

## mls rate-limit all

ユニキャストおよびマルチキャスト パケットに共通のレート リミッタをイネーブルにして設定するには、`mls rate-limit all` コマンドを使用します。レート リミッタをディセーブルにするには、このコマンドの `no` 形式を使用します。

```
mls rate-limit all { mtu-failure | ttl-failure } pps [packets-in-burst]
```

```
no mls rate-limit all { mtu-failure | ttl-failure }
```

### シンタックスの説明

<code>all</code>	ユニキャストおよびマルチキャスト パケットを制限するレートを指定しません。
<code>mtu-failure</code>	MTU (最大伝送ユニット) が失敗したパケットのレート リミッタをイネーブルにして設定します。
<code>ttl-failure</code>	TTL (存続可能時間) が失敗したパケットのレート リミッタをイネーブルにして設定します。
<code>pps</code>	パケット / 秒。有効な値は 10 ~ 1000000 pps です。
<code>packets-in-burst</code>	(任意) バースト状態のパケット。有効な値は 1 ~ 255 です。

### デフォルト

レイヤ 2 のレート リミッタは、デフォルトでオフです。レート リミッタをイネーブルにして設定すると、`packets-in-burst` はデフォルトで 10 になります。

### コマンドモード

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更内容
12.2(17d)SXB	このコマンドのサポートが MSFC に追加されました。

### 使用上のガイドライン

このコマンドは、Supervisor Engine 2 で構成された Catalyst 6500 シリーズ スイッチ上ではサポートされません。

レート リミッタは、ハードウェアのデータ パスからソフトウェアのデータ パスにバントされたパケットのレートを制限できます。レート リミッタは、設定したレートを超えるトラフィックを廃棄して、ソフトウェアの制御パスで輻輳が発生するのを防ぎます。



(注)

PFC3A を使用して構成された Catalyst 6500 シリーズ スイッチで、レイヤ 2 のレート リミッタをイネーブルにすると、マルチキャスト トラフィックに対する悪影響があります。このような悪影響は、PFC3BXL を使用して構成された Catalyst 6500 シリーズ スイッチ では発生しません。

### 例

次に、ユニキャストおよびマルチキャスト パケットに TTL 障害リミッタを設定する例を示します。

```
Router(config)# mls rate-limit all ttl-failure 15
Router(config)#
```

### 関連コマンド

`show mls rate-limit`

## mls rate-limit multicast ipv4

IPv4 マルチキャスト パケットのレート リミッタをイネーブルにして設定するには、**mls rate-limit multicast ipv4** コマンドを使用します。レート リミッタをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
mls rate-limit multicast ipv4 { connected | fib-miss | igmp | ip-option | partial | non-rpf } pps
    [packets-in-burst]

no mls rate-limit multicast ipv4 { connected | fib-miss | igmp | ip-option | partial | non-rpf }
```

### シンタックスの説明

<b>connected</b>	直接接続されている送信元からのマルチキャスト パケットのレート リミッタをイネーブルにして設定します。
<b>fib-miss</b>	FIB (転送情報ベース) 不一致 マルチキャスト パケットのレート リミッタをイネーブルにして設定します。
<b>igmp</b>	IGMP パケットのレート リミッタをイネーブルにして設定します。
<b>ip-option</b>	IP オプションを持つマルチキャスト パケットのレート リミッタをイネーブルにして設定します。
<b>partial</b>	部分 SC 状態時にマルチキャスト パケットのレート リミッタをイネーブルにして設定します。
<b>non-rpf</b>	RPF チェックに失敗したマルチキャスト パケットのレート リミッタをイネーブルにして設定します。
<i>pps</i>	パケット / 秒。有効な値は 10 ~ 1000000 pps です。
<i>packets-in-burst</i>	(任意) バースト状態のパケット。有効な値は 1 ~ 255 です。

### デフォルト

デフォルト設定は次のとおりです。

- *packets-in-burst* を設定しないと、マルチキャストの場合はデフォルトの **100** がプログラムされます。
- **fib-miss** イネーブル (**100000 pps**) で、*packet-in-burst* は **100** に設定されています。
- **ip-option** ディセーブルです。
- **partial** イネーブル (**100000 pps**) で、*packet-in-burst* は **100** に設定されています。

### コマンドモード

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更内容
12.2(17d)SXB	このコマンドのサポートが MSFC に追加されました。

### 使用上のガイドライン

このコマンドは、Supervisor Engine 2 で構成された Catalyst 6500 シリーズ スイッチ上ではサポートされません。

グローバル スイッチング モードが Truncated モードの場合は、IPv4 レート リミッタを設定できません。

レート リミッタは、ハードウェアのデータ パスからソフトウェアのデータ パスにパントされたパケットのレートを制限できます。レート リミッタは、ソフトウェアの制御パスでの輻輳を防ぎ、設定したレートを超えるトラフィックを廃棄します。

**ip-option** キーワードは、PFC3BXL または PFC3B モードでのみサポートされます。

## ■ mls rate-limit multicast ipv4

**例** 次に、RPF チェックに失敗したマルチキャスト パケットのレート リミッタを設定する例を示します。

```
Router(config)# mls rate-limit multicast ipv4 non-rpf 100
Router(config)#
```

次に、部分 SC 状態時にマルチキャスト パケットのレート リミッタを設定する例を示します。

```
Router(config)# mls rate-limit multicast ipv4 partial 250
Router(config)#
```

次に、FIB 不一致マルチキャスト パケットのレート リミッタを設定する例を示します。

```
Router(config)# mls rate-limit multicast ipv4 fib-miss 15
Router(config)#
```

**関連コマンド**

`show mls rate-limit`

## mls rate-limit multicast ipv6

IPv6 マルチキャスト レート リミッタを設定するには、`mls rate-limit multicast ipv6` コマンドを使用します。レート リミッタをディセーブルにするには、このコマンドの `no` 形式を使用します。

```
mls rate-limit multicast ipv6 {connected pps [packets-in-burst]} | {rate-limiter-name {share {auto | target-rate-limiter}}}
```

```
no mls rate-limit multicast ipv6 {connected | rate-limiter-type}
```

### シンタックスの説明

<code>connected pps</code>	直接接続されている送信元からの IPv6 マルチキャスト パケットのレート リミッタをイネーブルにして設定します。有効な値は 10 ~ 1000000 pps です。
<code>packets-in-burst</code>	(任意) バースト状態のパケット。有効な値は 1 ~ 255 です。
<code>rate-limiter-name</code>	レート リミッタ名。有効な値は <code>default-drop</code> 、 <code>route-ctrl</code> 、 <code>secondary-drop</code> 、 <code>sg</code> 、 <code>starg-bridge</code> 、および <code>starg-m-bridge</code> です。詳細については「使用上の注意事項」を参照してください。
<code>share</code>	IPv6 レート リミッタのシェアリング ポリシーを指定します。詳細については、「使用上の注意事項」を参照してください。
<code>auto</code>	シェアリング ポリシーを自動的に決定します。
<code>target-rate-limiter</code>	グループに対してハードウェアに最初にプログラムされているレート リミッタ名。有効な値は <code>default-drop</code> 、 <code>route-ctrl</code> 、 <code>secondary-drop</code> 、 <code>sg</code> 、 <code>starg-bridge</code> 、および <code>starg-m-bridge</code> です。詳細については「使用上の注意事項」を参照してください。

### デフォルト

`burst` を設定しないと、マルチキャストの場合はデフォルトの 100 がプログラムされます。

### コマンド モード

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更内容
12.2(18)SXD	このコマンドのサポートが MSFC に追加されました。

### 使用上のガイドライン

このコマンドは、Supervisor Engine 2 で構成された Catalyst 6500 シリーズ スイッチ上ではサポートされません。

`rate-limiter-name` 引数には、現在プログラムされていないレート リミッタを指定してください。

`target-rate-limiter` 引数には、ハードウェアにプログラムされていて、グループに対して最初にプログラムされているレート リミッタを指定してください。

表 2-2 に、IPv6 レート リミッタおよび各レート リミッタが処理を行うトラフィックのクラスを示します。

表 2-2 IPv6 レート リミッタ

レート リミッタ ID	レート制限するトラフィック クラス
Connected	直接接続されている送信元トラフィック
Default-drop	* (*, G/m)SSM * (*, G/m)SSM non-rpf
Route-control	* (*, FF02::X/128)

表 2-2 IPv6 レート リミッタ (続き)

レート リミッタ ID	レート制限するトラフィック クラス
Secondary-drop	* (*, G/128) SPT しきい値は無限
SG	* (S, G) RP-RPF ポスト スイッチオーバー * (*, FFx2/16)
Starg-bridge	* (*, G/128) SM (*, G) が存在する場合の * SM 非 rpf トラフィック
Starg-M-bridge	* (*, G/m) SM * (*, FF/8) (*, G) が存在しない場合の * SM 非 rpf トラフィック

IPv6 マルチキャスト トラフィックのレート リミッタを設定するには、次のいずれかの方法を使用できます。

- レート リミッタをトラフィック クラスに直接関連付け レートを選択して、レート リミッタと関連付けます。次に、1000 pps および 20 パースト パケットを選択して、デフォルト廃棄 (default-drop) レート リミッタと関連付ける例を示します。

```
Router(config)# mls rate-limit multicast ipv6 default-drop 1000 20
```

- レート リミッタを、設定済みの別のレート リミッタとスタティックに共有 隣接関係に基づくレート リミッタが十分に確保できない場合は、すでに設定されたレート リミッタ(ターゲット レート リミッタ)と共有できます。次に、ルート制御 (route-cntl) レート リミッタを、デフォルト廃棄 (default-drop) ターゲット レート リミッタと共有します。

```
Router(config)# mls rate-limit multicast ipv6 route-cntl share default-drop
```

ターゲット レート リミッタが未設定の場合は、ターゲット レート リミッタを別のレート リミッタと共有するには、ターゲット レート リミッタが設定されている必要があることを通知するメッセージが表示されます。

- レート リミッタをダイナミックに共有 どのレート リミッタを共有すべきか判断しにくい場合は、share auto キーワードを使用して、ダイナミック共有をイネーブルにします。ダイナミック共有をイネーブルにすると、事前設定されたレート リミッタが選択され、このレート リミッタが指定のレート リミッタと共有されます。次に、ルート制御 (route-cntrl) レート リミッタに対してダイナミック共有を選択する例を示します。

```
Router(config)# mls rate-limit multicast ipv6 route-cntl share auto
```

**例** 次に、直接接続されている送信元からの IPv6 マルチキャスト パケットのレート制限を設定する例を示します。

```
Router(config)# mls rate-limit multicast ipv6 connected 1500 20
Router(config)#
```

次に、レート リミッタをトラフィック クラスに直接関連付ける設定を行う例を示します。

```
Router(config)# mls rate-limit multicast ipv6 default-drop 1000 20
Router(config)#
```

次に、事前設定された別のレート リミッタとレート リミッタをスタティックに共有する例を示します。

```
Router(config)# mls rate-limit multicast ipv6 route-cntl share default-drop
Router(config)#
```

次に、ルート制御 (`route-cntrl`) レート リミッタに対してダイナミック共有をイネーブルにする例を示します。

```
Router(config)# mls rate-limit multicast ipv6 route-cntrl share auto
Router(config)#
```

### 関連コマンド

`show mls rate-limit`

## mls rate-limit unicast acl

ACL ブリッジド レート リミッタを設定するには、`mls rate-limit unicast acl` コマンドを使用します。レート リミッタをディセーブルにするには、このコマンドの `no` 形式を使用します。

```
mls rate-limit unicast acl {input | output | vacl-log} {pps [packets-in-burst]}
```

### シンタックスの説明

<code>input</code>	入力 ACL ブリッジド ユニキャスト パケットのレート リミッタを指定します。
<code>output</code>	出力 ACL ブリッジド ユニキャスト パケットのレート リミッタを指定します。
<code>vacl-log</code>	VACL ログの場合のレート リミッタを指定します。
<code>pps</code>	パケット / 秒。有効値については、「使用上の注意事項」を参照してください。
<code>packets-in-burst</code>	(任意) バースト状態のパケット。有効な値は 1 ~ 255 です。

### デフォルト

デフォルト設定は次のとおりです。

- `input` ディセーブルです。
- `output` ディセーブルです。
- `vacl-log` イネーブル (2000 *pps*) で、`packet-in-burst` は 1 に設定されています。
- `packets-in-burst` を設定しないと、ユニキャストの場合は 10 がプログラムされます。

### コマンドモード

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更内容
12.2(17d)SXB	このコマンドのサポートが MSFC に追加されました。

### 使用上のガイドライン

`input` および `output` キーワードは、Supervisor Engine 2 で構成された Catalyst 6500 シリーズ スイッチ上ではサポートされません。

レート リミッタは、ハードウェアのデータ パスからソフトウェアのデータ パスにパントされたパケットのレートを制限できません。レート リミッタは、ソフトウェアの制御パスでの輻輳を防ぎ、設定したレートを越えるトラフィックを廃棄します。

`pps` を設定する場合に、有効な値は次のとおりです。

- ACL 入力および出力の場合 10 ~ 1000000 *pps*
- VACL ログの場合 10 ~ 5000 *pps*

`vacl-log packets-in-burst` キーワードおよび引数を変更することはできず、デフォルトで 1 に設定されます。

同じハードウェアレジスタが共有される場合もあります。これは次の 2 つのグループに分けられます。

- グループ 1 :
  - 出力 ACL ブリッジド パケット
  - 入力 ACL ブリッジド パケット
- グループ 2 :
  - RPF 障害
  - ACL 廃棄に対する ICMP 到達不能
  - ルートなしに対する ICMP 到達不能
  - IP エラー

各グループのすべてのコンポーネントは、同じハードウェアレジスタを使用または共有します。たとえば、ACL ブリッジド入出力パケットはレジスタ A を使用し、ICMP 到達不能、ルートなし、および RPF 障害はレジスタ B を使用します。

ほとんどの場合、グループのコンポーネントを変更すると、最初のコンポーネントが変更されたように、グループ内のコンポーネントはすべて同じハードウェアレジスタを使用するように上書きされます。上書きが行われるたびに、警告メッセージが出力されますが、これはサービス内部モードをイネーブルにした場合だけです。次の場合には、上書きは行われません。

- 特別な場合で、`pps` の値が 0 (ゼロ) に設定されている場合
- 入出力 ACL ブリッジド パケットがディセーブルの場合、これらを再度イネーブルにするまで上書きは行われません。一方がディセーブルの場合、もう一方はイネーブルであるかぎり影響を受けません。たとえば、入力 ACL ブリッジド パケットのレートを 100 pps に設定したあとに、出力 ACL ブリッジド パケットのレートを 200 pps に設定すると、入力 ACL ブリッジド パケットの値は 200 pps に上書きされ、入出力 ACL ブリッジド パケットは両方とも 200 pps になります。

**例** 次に、ユニキャスト パケットに対する入力 ACL ブリッジド パケット リミッタを設定する例を示します。

```
Router(config)# mls rate-limit unicast acl ingress 100
Router(config)#
```

**関連コマンド** `show mls rate-limit`

## mls rate-limit unicast cef

CEF レートリミッタをイネーブルにして設定するには、`mls rate-limit unicast cef` コマンドを使用します。レートリミッタをディセーブルにするには、このコマンドの `no` 形式を使用します。

```
mls rate-limit unicast cef {receive | glean} pps [packets-in-burst]
```

シンタックスの説明	
<code>receive</code>	受信パケットに対するレートリミッタをイネーブルにして設定します。
<code>glean</code>	ARP(アドレス解決プロトコル)解決パケットに対するレートリミッタをイネーブルにして設定します。
<code>pps</code>	パケット/秒。有効な値は 10 ~ 1000000 pps です。
<code>packets-in-burst</code>	(任意) バースト状態のパケット。有効な値は 1 ~ 255 です。

**デフォルト** デフォルト設定は次のとおりです。

- `receive` ディセーブル
- `glean` ディセーブル

**コマンドモード** グローバル コンフィギュレーション

コマンド履歴	リリース	変更内容
	12.2(17d)SXB	このコマンドのサポートが MSFC に追加されました。

**使用上のガイドライン** CEF レートリミッタ機能をイネーブルにする場合、次の状況が発生します(これらの状況が望ましくない場合は、CEF レートリミッタをディセーブルにしてください)。

- パケットが `glean/receive` 隣接関係にヒットする場合、パケットはソフトウェアに送信されず、廃棄される可能性があります(入力 VLAN [仮想 LAN] に出力 ACL [アクセスコントロールリスト] があり、一致したエントリの結果が `deny` [拒否] である場合)。
- 一致した ACL エントリの結果が `bridge` (ブリッジ) である場合、パケットは `glean/receive` レート制限ではなく、出力 ACL ブリッジ レート制限 (オンの場合) の制約を受けます。
- `glean/receive` 隣接レート制限は、出力 ACL 検索の結果が `permit` (許可)、または入力 VLAN に出力 ACL がない場合にのみ適用されます。

**例** 次に、ユニキャストパケットに対する CEF の `glean` リミッタを設定する例を示します。

```
Router(config)# mls rate-limit unicast cef glean 5000
Router(config)#
```

**関連コマンド** `show mls rate-limit`

## mls rate-limit unicast ip

ユニキャスト パケットのレート リミッタをイネーブルにして設定するには、`mls rate-limit unicast ip` コマンドを使用します。レート リミッタをディセーブルにするには、このコマンドの `no` 形式を使用します。

```
mls rate-limit unicast ip {errors | features | options | rpf-failure} pps [packets-in-burst]
```

```
mls rate-limit unicast ip icmp {redirect | unreachable {acl-drop pps} | no-route pps}
[packets-in-burst]
```

```
no mls rate-limit unicast ip {errors | features | {icmp {redirect | unreachable {acl-drop | no-route}}}}
| options | rpf-failure} pps [packets-in-burst]
```

### シンタックスの説明

<code>errors</code>	IP チェックサム エラーおよび IP 長エラーのユニキャスト パケットのレート制限を指定します。
<code>features</code>	レイヤ 3 のソフトウェア セキュリティ機能（認証プロキシ、IPSec、検査など）を使用したユニキャスト パケットのレート制限を指定します。
<code>options</code>	オプションを持つユニキャスト IPv4 パケットのレート制限を指定します。
<code>rpf-failure</code>	RPF 障害が発生したユニキャスト パケットのレート制限を指定します。
<code>pps</code>	パケット / 秒。有効値については、「使用上の注意事項」を参照してください。
<code>packets-in-burst</code>	（任意）バースト状態のパケット。有効な値は 1 ~ 255 です。
<code>icmp redirect</code>	ICMP リダイレクトを必要とするユニキャスト パケットのレート制限を指定します。
<code>icmp unreachable acl-drop pps</code>	ACL（アクセス コントロール リスト）廃棄パケットに対する ICMP 到達不能のレート リミッタのイネーブル化および設定を行います。
<code>icmp unreachable no-route pps</code>	FIB（転送情報ベース）不一致パケットに対する ICMP 到達不能のレート リミッタのイネーブル化および設定を行います。

### デフォルト

デフォルト設定は次のとおりです。

- `packets-in-burst` を設定しないと、ユニキャストのバーストとしてデフォルトの **10** がプログラムされます。
- `errors` イネーブル（**500 pps**）で、`packet-in-burst` は **10** に設定されています。
- `rpf-failure` イネーブル（**500 pps**）で、`packet-in-burst` は **10** に設定されています。
- `icmp unreachable acl-drop` イネーブル（**500 pps**）で、`packet-in-burst` は **10** に設定されています。
- `icmp unreachable no-route` イネーブル（**500 pps**）で、`packet-in-burst` は **10** に設定されています。
- `icmp redirect` ディセーブルです。

### コマンドモード

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更内容
12.2(17d)SXB	このコマンドのサポートが MSFC に追加されました。

### 使用上のガイドライン

このコマンドは、Supervisor Engine 2 で構成された Catalyst 6500 シリーズ スイッチ上ではサポートされません。

拒否されたパケットに対して OAL サポートを提供するには、`mls rate-limit unicast ip icmp unreachable acl-drop 0` コマンドを入力します。

OAL キャプチャと VACL キャプチャには、互換性がありません。スイッチに両方の機能を設定しないでください。OAL を設定した場合は、SPAN (スイッチドポートアナライザ) を使用してトラフィックをキャプチャします。

レートリミッタは、ハードウェアのデータパスからソフトウェアのデータパスにパントされたパケットのレートを制限できます。レートリミッタは、ソフトウェアの制御パスでの輻輳を防ぎ、設定したレートを超えるトラフィックを廃棄します。



(注)

ICMP レートリミッタを設定して ICMP リダイレクトが発生する場合、既存のデータトラフィックが廃棄されますが、同じインターフェイス上の残りのトラフィックは転送されます。

*pps* を設定する場合、有効値は 0 および 10 ~ 1000000 です。*pps* をグローバルに 0 に設定すると、ルートプロセッサへのパケットのリダイレクションがディセーブルになります。0 の値は、次のレートリミッタでサポートされます。

- ICMP unreachable ACL-drop
- ICMP unreachable no-route
- ICMP redirect
- IP rpf failure

同じハードウェアレジスタが共有される場合もあります。これは次の 2 つのグループに分けられます。

- グループ 1 :
  - 出力 ACL ブリッジドパケット
  - 入力 ACL ブリッジドパケット
- グループ 2 :
  - RPF 障害
  - ACL 廃棄に対する ICMP 到達不能
  - ルートなしに対する ICMP 到達不能
  - IP エラー

各グループのすべてのコンポーネントは、同じハードウェアレジスタを使用または共有します。たとえば、ACL ブリッジド入出力パケットはレジスタ A を使用し、ICMP 到達不能、ルートなし、および RPF 障害はレジスタ B を使用します。

ほとんどの場合、グループのコンポーネントを変更すると、最初のコンポーネントが変更されたように、グループ内のコンポーネントはすべて同じハードウェアレジスタを使用するように上書きされます。上書きが行われるたびに、警告メッセージが出力されますが、これはサービス内部モードをイネーブルにした場合だけです。次の場合には、上書きは行われません。

- 特別な場合で、*pps* の値が 0 (ゼロ) に設定されている場合
- 入出力 ACL ブリッジドパケットがディセーブルの場合、これらを再度イネーブルにするまで上書きは行われません。一方がディセーブルの場合、もう一方はイネーブルであるかぎり影響を受けません。たとえば、入力 ACL ブリッジドパケットのレートを 100 pps に設定したあとに、出力 ACL ブリッジドパケットのレートを 200 pps に設定すると、入力 ACL ブリッジドパケットの値は 200 pps に上書きされ、入出力 ACL ブリッジドパケットは両方とも 200 pps になります。

**例** 次に、ユニキャスト パケットに対する ICMP リダイレクトのリミッタを設定する例を示します。

```
Router(config)# mls rate-limit unicast ip icmp redirect 250
Router(config)#
```

**関連コマンド** show mls rate-limit

## mode

冗長モードを設定するには、mode コマンドを使用します。

```
mode {rpr | rpr-plus | sso}
```

### シンタックスの説明

rpr	RPR モードを指定します。
rpr-plus	RPR+ モードを指定します。
sso	SSO モードを指定します。

### デフォルト

デフォルト設定は次のとおりです。

- アクティブなスーパーバイザ エンジンとスタンバイ スーパーバイザ エンジンが同じイメージを持つ場合は RPR+ モード。
- 異なるバージョンがインストールされている場合は RPR モード。
- システムにハイ アベイラビリティが設定され、アクティブなスーパーバイザ エンジンとスタンバイ スーパーバイザ エンジンが同じイメージを持つ場合は SSO モード。

### コマンドモード

冗長コンフィギュレーション

### コマンド履歴

リリース	変更内容
12.2(14)SX	このコマンドのサポートが MSFC に追加されました。
12.2(17a)SXA	このコマンドは、SSO モードをサポートするように変更されました。

### 使用上のガイドライン

冗長コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **redundancy** コマンドを入力します。冗長コンフィギュレーション モード内で **mode** コマンドを入力できます。

システムを RPR+ モードに設定するには、次の注意事項に従ってください。

- RPR+ モードをサポートするには、アクティブおよびスタンバイ スーパーバイザ エンジンに互換性のあるイメージをインストールする必要があります。
- 両方のスーパーバイザ エンジンで同じリリースの Cisco IOS ソフトウェアを実行する必要があります。
- スイッチオーバー時にオンラインになっていないモジュールはリセットされ、スイッチオーバー時にリロードされます。
- FIB テーブルは、スイッチオーバー時にクリアされます。その結果、ルーティングされたトラフィックは、ルート テーブルが再収束するまで中断されます。

スタンバイ スーパバイザ エンジン は、モードの変更時にリロードされ、現在のモードで作業を開始します。

**例**

次に、冗長モードを RPR+ に設定する例を示します。

```
Router(config)# redundancy  
Router(config-red)# mode rpr-plus  
Router(config-red)#
```

次に、冗長モードを SSO に設定する例を示します。

```
Router(config)# redundancy  
Router(config-red)# mode sso  
Router(config-red)#
```

**関連コマンド**

[redundancy](#)

## mtu

最大パケット サイズまたは Maximum Transmission Unit ( MTU; 最大伝送ユニット ) サイズを調整するには、**mtu** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

**mtu bytes**

**no mtu**

### シンタックスの説明

<i>bytes</i>	バイト サイズ。有効値は、Switched Virtual Interface ( SVI ) ポートでは 64 ~ 9216、その他のすべてのポートでは 1500 ~ 9216 です。
--------------	---

### デフォルト

表 2-3 に、ジャンボ フレームのサポートがディセーブルの場合のデフォルトの MTU 値を示します。

表 2-3 デフォルトの MTU 値

メディア タイプ	デフォルトの MTU ( バイト )
イーサネット	1500
シリアル	1500
トークンリング	4464
ATM	4470
FDDI	4470
HSSI ( HSA )	4470

ジャンボ フレームのサポートがイネーブルの場合、デフォルトは、SVI ポートでは 64、その他のすべてのポートでは 9216 です。ジャンボ フレームのサポートは、デフォルトでディセーブルです。

### コマンド モード

インターフェイス コンフィギュレーション

### コマンド履歴

リリース	変更内容
12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

### 使用上のガイドライン

スイッチ ポートの場合、グローバルに使用できるのは、デフォルト値よりも大きい 1 つの MTU のみです。レイヤ 3 ポート ( ルータ ポートや VLAN [ 仮想 LAN ] を含む ) の場合、インターフェイスごとにデフォルト以外の MTU 値を設定できます。

ジャンボ フレームをサポートしていないモジュールのリストについては、『*Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide*』を参照してください。

**mtu** コマンドで MTU 値を設定すると、プロトコル固有バージョンのコマンドの値に影響が及ぶことがあります ( **ip mtu** コマンドなど )。 **ip mtu** コマンドで指定された値が **mtu** コマンドで指定された値と同じである場合に、**mtu** コマンドの値を変更すると、**ip mtu** 値は、新しい **mtu** コマンドの値と一致するように自動的に調整されます。ただし、**ip mtu** コマンドの値を変更しても、**mtu** コマンドの値には影響しません。

**例** 次に、1800 バイトの MTU を指定する例を示します。

```
Router(config)# interface fastethernet 5/1
Router(config-if)# mtu 1800
```

**関連コマンド** `ip mtu` (『Cisco IOS Release 12.2 Command Reference』を参照)

## redundancy

`redundancy` コマンドは、冗長性をイネーブルにし、冗長コンフィギュレーション モードを開始します。

```
redundancy
```

**シンタックスの説明** このコマンドには、引数またはキーワードはありません。

**デフォルト** このコマンドにはデフォルト設定がありません。

**コマンドモード** グローバル コンフィギュレーション

コマンド履歴	リリース	変更内容
	12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

**使用上のガイドライン** 冗長コンフィギュレーション モードを開始すると、次のオプションが使用できます。

- `exit` 冗長コンフィギュレーション モードを終了します。
- `high-availability` ハイアベイラビリティ冗長コンフィギュレーション モードを開始します。詳細情報に関しては [high-availability](#) コマンドを参照してください。
- `no` コマンドを無効にするか、またはデフォルトを設定します。

**例** 次に、冗長性をイネーブルにし、冗長コンフィギュレーション サブモードを開始する例を示します。

```
Router(config)# redundancy
Router(config-r)#
```

**関連コマンド** [high-availability](#)  
[show redundancy](#)

## route-converge-delay

古い FIB ( 転送情報ベース ) エントリが削除されるまでのタイム インターバルを設定するには、**route-converge-delay** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**route-converge-delay** *seconds*

### シンタックスの説明

<i>seconds</i>	古い FIB エントリが削除されるまでのタイム インターバル。有効値は 60 ~ 3600 秒です。
----------------	--

### デフォルト

*seconds* は 120 秒 ( 2 分 ) です。

### コマンドモード

メイン CPU サブモード

### コマンド履歴

リリース	変更内容
12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

### 使用上のガイドライン

スイッチオーバー時にルーティング プロトコルを再開するルート コンバージ時間をシミュレートするには、ルート コンバージ デレイ タイム インターバルが必要です。

### 例

次に、ルート コンバージ デレイ タイム インターバルを設定する例を示します。

```
Router(config)# redundancy
Router(config-red)# main-cpu
Router(config-red-main)# route-converge-delay 90
Router(config-red-main)#
```

次に、デフォルトのルート コンバージ デレイ タイム インターバルに戻す例を示します。

```
Router(config)# redundancy
Router(config-red)# main-cpu
Router(config-red-main)# no route-converge-delay
Router(config-red-main)#
```

### 関連コマンド

[redundancy](#)

## set traffic-index

アカウントिंगに対し Border Gateway Protocol ( BGP ) トラフィックの分類番号を作成するには、`set traffic-index` コマンドを使用します。

```
set traffic-index num
```

### シンタックスの説明

<i>num</i>	パケットの数。有効値は 1 ~ 7 です。
------------	-----------------------

### デフォルト

このコマンドにはデフォルト設定がありません。

### コマンドモード

ルーティング マップ コンフィギュレーション

### コマンド履歴

リリース	変更内容
12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

### 使用上のガイドライン

着信および発信トラフィックシェーピングは、Destination Sensitive Traffic Shaping ( DSTS ) と呼ばれる宛先トラフィックインデックスに基づいています。宛先の区別では、パケットおよびバイトのカウンタ ( 着信インターフェイスごとに 7 セット ) が提供されます。これが宛先ネットワークがカウントする IP パケットを表しています。宛先の区別にはルートマップを使用し、トラフィックを 7 つのインデックス ( トラフィック分類を示す ) で使用可能なものに分類します。

### 例

次に、BGP トラフィックインデックスを作成する例を示します。

```
Router (config-route-map) # set traffic-index 3
Router (config-route-map)
```

# show fm features

機能マネージャに関する情報を表示するには、**show fm features** コマンドを使用します。

**show fm features**

**シンタックスの説明** このコマンドには、キーワードまたは引数はありません。

**デフォルト** このコマンドにはデフォルト設定がありません。

**コマンドモード** EXEC

コマンド履歴	リリース	変更内容
	12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

**例** 次に、機能マネージャに関する情報を表示する例を示します。

```
Router> show fm features
Designated MSFC:1 Non-designated MSFC:1

Redundancy Status:designated
Interface:FastEthernet2/10 IP is enabled
  hw[EGRESS] = 1, hw[INGRESS] = 1
  hw_force_default[EGRESS] = 0, hw_force_default[INGRESS] = 0
  mcast = 0
  priority = 2
  reflexive = 0
  inbound label:1
    protocol:ip
    feature #:1
    feature id:FM_IP_ACCESS
    ACL:106
  outbound label:2
    protocol:ip
    feature #:1
    feature id:FM_IP_ACCESS
    ACL:106
Interface:FastEthernet2/26 IP is enabled
  hw[EGRESS] = 1, hw[INGRESS] = 0
  hw_force_default[EGRESS] = 0, hw_force_default[INGRESS] = 1
  mcast = 0
  priority = 2
  reflexive = 0
  inbound label:24
    protocol:ip
    feature #:1
    feature id:FM_IP_ACCESS
    ACL:113
  outbound label:3
    protocol:ip
    feature #:1
    feature id:FM_IP_WCCP
    Service ID:0
    Service Type:0
```

```
Interface:Vlan55 IP is enabled
  hw[EGRESS] = 1, hw[INGRESS] = 1
  hw_force_default[EGRESS] = 0, hw_force_default[INGRESS] = 0
  mcast = 0
  priority = 2
  reflexive = 0
  inbound label:4
    protocol:ip
      feature #:1
      feature id:FM_IP_ACCESS
      ACL:111
Interface:Vlan101 IP is enabled
  hw[EGRESS] = 1, hw[INGRESS] = 1
  hw_force_default[EGRESS] = 0, hw_force_default[INGRESS] = 0
  mcast = 0
  priority = 2
  reflexive = 0
  inbound label:5
    protocol:ip
      feature #:1
      feature id:FM_IP_ACCESS
      ACL:101
  outbound label:6
    protocol:ip
      feature #:1
      feature id:FM_IP_ACCESS
      ACL:101
Router>
```

次に、先頭行が Redundancy で始まる機能マネージャを表示する例を示します。

```
Router> show fm features | begin Redundancy
Redundancy Status: designated
Router>
```

# show fm inband-counters

Server Load Balancing (SLB) の Multilayer Switch Feature Card (MSFC; マルチレイヤ スイッチ フィーチャカード) から送信された帯域内のパケット数を表示するには、`show fm inband-counters` コマンドを使用します。

```
show fm inband-counters
```

**シンタックスの説明** このコマンドには、キーワードまたは引数はありません。

**デフォルト** このコマンドにはデフォルト設定がありません。

**コマンドモード** EXEC

コマンド履歴	リリース	変更内容
	12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

**使用上のガイドライン** `show fm inband-counters` コマンドの出力には、送信された SLB 帯域内パケット数が含まれます。Context-Based Access Control (CBAC; コンテキストベース アクセス コントロール) が設定されている場合、出力には CBAC の送信パケット数が含まれます。

**例** 次に、送信された SLB 帯域内パケット数を表示する例を示します。

```
Router# show fm inband-counters
      Inband Packets Sent
Slot  WCCP      SLB
 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
Router#
```

# show fm insp

Context-Based Access Control (CBAC; コンテキストベース アクセス コントロール) が設定された Access Control List (ACL; アクセス コントロール リスト) とポートのリストおよびステータスを表示するには、**show fm insp** コマンドを使用します。

```
show fm insp [detail]
```

## シンタックスの説明

<b>detail</b>	(任意) すべてのフロー情報を表示します。
---------------	-----------------------

## デフォルト

このコマンドにはデフォルト設定がありません。

## コマンドモード

EXEC

## コマンド履歴

リリース	変更内容
12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

## 使用上のガイドライン

CBAC を設定する前にポートに VACL が設定されている場合は、ステータス INACTIVE が表示されます。それ以外の場合はステータス ACTIVE が表示されます。Policy Feature Card (PFC; ポリシーフィーチャカード) リソースが枯渇している場合にこのコマンドを実行すると、BRIDGE が表示され、そのあとに、処理のために Multilayer Switch Feature Card (MSFC; マルチレイヤスイッチフィーチャカード) に送信された、現在アクティブな、失敗した NetFlow 要求の数が表示されます。

**show fm insp** コマンドの出力には、次の情報が含まれます。

- interface IP 検査機能がイネーブルであるインターフェイス
- (方向) IP 検査機能がイネーブルである方向 (IN または OUT)
- acl name 検査されるパケットの識別に使用される名前。
- status (ACTIVE または INACTIVE) このインターフェイスと方向の組がハードウェアでサポートされているかどうか (ハードウェアでサポートされている場合は ACTIVE は、それ以外は INACTIVE)

**detail** キーワードを指定すると、指定されたインターフェイス方向の IP 検査に使用される ACL 内の Access Control Entry (ACE; アクセス コントロール エントリ) も表示されます。

## 例

次に、CBAC が設定された ACL およびポートのリストおよびステータスを表示する例を示します。

```
Router> show fm insp
interface:Vlan305(in) status :ACTIVE
acl name:deny
interfaces:
  Vlan305(out):status ACTIVE
```

## show fm interface

インターフェイスごとに機能マネージャに関する詳細情報を表示するには、`show fm interface` コマンドを使用します。

```
show fm interface {{interface interface-number} | {null interface-number} | {port-channel number} |
                  {vlan vlan-id}}
```

### シンタックスの説明

<i>interface</i>	インターフェイス タイプ。使用できる値は <code>pos</code> 、 <code>atm</code> および <code>ge-wan</code> です。
<i>interface-number</i>	モジュールおよびポート番号。有効値については、「使用上の注意事項」を参照してください。
<code>null interface-number</code>	ヌル インターフェイスを指定します。有効値は <code>0</code> です。
<code>port-channel number</code>	ポートチャネル番号を指定します。有効値は 1 ~ 282 です。
<code>vlan vlan-id</code>	VLAN を指定します。 <i>vlan-id</i> の有効値は 1 ~ 4094 です。

### デフォルト

このコマンドにはデフォルト設定がありません。

### コマンド モード

EXEC

### コマンド履歴

リリース	変更内容
12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

### 使用上のガイドライン

モジュールおよびポート番号を指定するには、*interface-number* 引数を使用します。*interface-number* の有効値は、指定したインターフェイス タイプおよび使用されているシャーシおよびモジュールによって決まります。たとえば、ギガビットイーサネット インターフェイスを指定し、Catalyst 6513 シャーシに搭載された 48 ポート 10/100BASE-T イーサネット モジュールを使用する場合、モジュール番号の有効値は 2 ~ 13 で、ポート番号の有効値は 1 ~ 48 です。

例 次に、指定されたインターフェイスの機能マネージャに関する詳細情報を表示する例を示します。

```
Router> show fm interface fastethernet 2/26
Interface:FastEthernet2/26 IP is enabled
  hw[EGRESS] = 1, hw[INGRESS] = 0
  hw_force_default[EGRESS] = 0, hw_force_default[INGRESS] = 1
  mcast = 0
  priority = 2
  reflexive = 0
  inbound label:24
    protocol:ip
      feature #:1
      feature id:FM_IP_ACCESS
      ACL:113
        vmr IP value #1:0, 0, 0, 0, 0, 0, 0, 0, 6 - 1
        vmr IP mask #1:0, 0, FFFF, FFFF, 0, 0, 0, FF
        vmr IP value #2:642D4122, 0, 0, 0, 1, 0, 0, 6 - 1
        vmr IP mask #2:FFFFFFFF, 0, 0, 0, 1, 0, 0, FF
        vmr IP value #3:0, 64020302, 0, 0, 6, 0, 0, 6 - 1
        vmr IP mask #3:0, FFFFFFFF, 0, 0, 6, 0, 0, FF
        vmr IP value #4:0, 64020302, 0, 0, A, 0, 0, 6 - 1
        vmr IP mask #4:0, FFFFFFFF, 0, 0, A, 0, 0, FF
        vmr IP value #5:0, 64020302, 0, 0, 12, 0, 0, 6 - 1
        vmr IP mask #5:0, FFFFFFFF, 0, 0, 12, 0, 0, FF
        vmr IP value #6:0, 0, 0, 0, 0, 0, 0, 0 - 2
        vmr IP mask #6:0, 0, 0, 0, 0, 0, 0, 0
      outbound label:3
        protocol:ip
          feature #:1
          feature id:FM_IP_WCCP
          Service ID:0
          Service Type:0
Router>
```

## show fm reflexive

ダイナミックな機能マネージャの再帰エントリに関する情報を表示するには、`show fm reflexive` コマンドを使用します。

```
show fm reflexive
```

**シンタックスの説明** このコマンドには、キーワードまたは引数はありません。

**デフォルト** このコマンドにはデフォルト設定がありません。

**コマンドモード** EXEC

コマンド履歴	リリース	変更内容
	12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

**例** 次に、機能マネージャのダイナミック再帰エントリに関する情報を表示する例を示します。

```
Router# show fm reflexive
Reflexive hash table:
  Vlan613:refacl, OUT-REF, 64060E0A, 64060D0A, 0, 0, 7, 783, 6
Router#
```

## show fm summary

機能マネージャに関する情報の概要を表示するには、`show fm summary` コマンドを使用します。

```
show fm summary
```

**シンタックスの説明** このコマンドには、キーワードまたは引数はありません。

**デフォルト** このコマンドにはデフォルト設定がありません。

**コマンドモード** EXEC

コマンド履歴	リリース	変更内容
	12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

**例** 次に、機能マネージャ情報の概要を表示する例を示します。

```
Router# show fm summary
Current global ACL merge algorithm:BDD
Router#
```

# show fm vlan

VLAN (仮想 LAN) 単位の機能マネージャに関する情報を表示するには、**show fm vlan** コマンドを使用します。

```
show fm vlan vlan-id
```

## シンタックスの説明

<i>vlan-id</i>	VLAN 番号。 <i>vlan-id</i> の有効値は 1 ~ 4094 です。
----------------	--

## デフォルト

このコマンドにはデフォルト設定がありません。

## コマンドモード

EXEC

## コマンド履歴

リリース	変更内容
12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

## 例

次に、機能マネージャに関する情報を VLAN 単位で表示する例を示します。

```
Router# show fm vlan 1
hw[EGRESS] = 1, hw[INGRESS] = 1
hw_force_default[EGRESS] = 0, hw_force_default[INGRESS] = 0
mcast = 0
priority = 2
reflexive = 0
vacc_map : map1
inbound label: 5
merge_err: 0
protocol: ip
feature #: 1
feature id: FM_VACL
map_name: map1
seq #: 10
(only for IP_PROT) DestAddr SrcAddr Dpt Spt L4OP TOS Est prot Rslt
vmr IP value # 1: 0.0.0.0 0.0.0.0 0 0 0 0 0 6 permit
vmr IP mask # 1: 0.0.0.0 0.0.0.0 0 0 0 0 0 FF
vmr IP value # 2: 0.0.0.0 0.0.0.0 0 0 0 0 0 11 permit
vmr IP mask # 2: 0.0.0.0 0.0.0.0 0 0 0 0 0 FF
vmr IP value # 3: 0.0.0.0 0.0.0.0 0 0 0 0 0 0 deny
vmr IP mask # 3: 0.0.0.0 0.0.0.0 0 0 0 0 0 0
seq #: 65536
(only for IP_PROT) DestAddr SrcAddr Dpt Spt L4OP TOS Est prot Rslt
vmr IP value # 1: 0.0.0.0 0.0.0.0 0 0 0 0 0 0 permit
vmr IP mask # 1: 0.0.0.0 0.0.0.0 0 0 0 0 0 0
outbound label: 6
merge_err: 0
protocol: ip
feature #: 1
feature id: FM_VACL
map_name: map1
seq #: 10
(only for IP_PROT) DestAddr SrcAddr Dpt Spt L4OP TOS Est prot Rslt
vmr IP value # 1: 0.0.0.0 0.0.0.0 0 0 0 0 0 6 permit
vmr IP mask # 1: 0.0.0.0 0.0.0.0 0 0 0 0 0 FF
vmr IP value # 2: 0.0.0.0 0.0.0.0 0 0 0 0 0 11 permit
vmr IP mask # 2: 0.0.0.0 0.0.0.0 0 0 0 0 0 FF
vmr IP value # 3: 0.0.0.0 0.0.0.0 0 0 0 0 0 0 deny
vmr IP mask # 3: 0.0.0.0 0.0.0.0 0 0 0 0 0 0
seq #: 65536
(only for IP_PROT) DestAddr SrcAddr Dpt Spt L4OP TOS Est prot Rslt
vmr IP value # 1: 0.0.0.0 0.0.0.0 0 0 0 0 0 0 permit
vmr IP mask # 1: 0.0.0.0 0.0.0.0 0 0 0 0 0 0
```

# show ip auth-proxy watch-list

認証プロキシのウォッチ リストを表示するには、`show ip auth-proxy watch-list` コマンドを使用します。

```
show ip auth-proxy watch-list
```

**シンタックスの説明** このコマンドには、引数またはキーワードはありません。

**デフォルト** このコマンドにはデフォルト設定がありません。

**コマンドモード** EXEC

コマンド履歴	リリース	変更内容
	12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

**例** 次に、認証プロキシのウォッチ リストに関する情報を表示する例を示します。

```
Router# show ip auth-proxy watch-list
Authentication Proxy Watch-list is enabled
Watch-list expiry timeout is 2 minutes
Total number of watch-list entries: 3

Source IP      Type           Violation-count
12.0.0.2      MAX_RETRY     MAX_LIMIT
12.0.0.3      TCP_NO_DATA   MAX_LIMIT
1.2.3.4       CFGED         N/A

Total number of watch-listed users: 3
Router#
```

**関連コマンド**

- [clear ip auth-proxy watch-list](#)
- [ip auth-proxy max-login-attempts](#)
- [ip auth-proxy watch-list](#)

# show ip pim interface

発見された PIM ネイバーのリストを表示するには、`show ip pim neighbor` コマンドを使用します。

```
show ip pim [vrf vrf-name] interface [count | detail | {vlan num} | {tunnel num}]
```

シンタックスの説明	
<code>vrf vrf-name</code>	(任意) マルチキャスト VPN Routing/Forwarding instance (VRF; VPN ルーティング/転送インスタンス) に割り当てられた名前を指定します。
<code>count</code>	(任意) インターフェイス マルチキャスト パケット数を表示します。
<code>detail</code>	(任意) PIM の詳細情報を表示します。
<code>vlan num</code>	(任意) VLAN (仮想 LAN) 番号を指定します。有効値は 1 ~ 4094 です。
<code>tunnel num</code>	(任意) トンネル番号を指定します。有効値は 0 ~ 214748364 です。

**デフォルト** このコマンドにはデフォルト設定がありません。

**コマンドモード** EXEC

コマンド履歴	リリース	変更内容
	12.2(18)SXF	このコマンドのサポートが Supervisor Engine 720 に追加されました。

**使用上のガイドライン** このコマンドは、Supervisor Engine 2 で構成された Catalyst 6500 シリーズ スイッチ上ではサポートされません。

このコマンドは、PIM 用に設定されているインターフェイス上でサポートされます。

**例** 次に、`show ip pim interface` コマンドの出力例を示します。

```
Router# show ip pim interface
Address          Interface      Mode   Neighbor  Query   DR
                Count         Interval
198.92.37.6     Ethernet0     Dense  2         30      198.92.37.33
198.92.36.129   Ethernet1     Dense  2         30      198.92.36.131
10.1.37.2       Tunnel0       Dense  1         30      0.0.0.0
Router#
```

次に、インターフェイス マルチキャスト パケット数を表示する例を示します。

```
Router# show ip pim interface count
Address          Interface      FS   Mpackets In/Out
171.69.121.35   Ethernet0     *   548305239/13744856
171.69.121.35   Serial0.33    *   8256/67052912
198.92.12.73    Serial0.1719  *   219444/862191
Router#
```

表 2-4 に、`show ip pim interface` コマンドの出力フィールドの説明を示します。

表 2-4 show ip pim interface のフィールドの説明

フィールド	説明
Address	ネクストホップ ルータの IP アドレス。
Interface	PIM を実行するために設定したインターフェイス タイプおよび番号。
Mode	Cisco IOS ソフトウェアが動作しているマルチキャスト モード。dense(密)モードまたは sparse(疎)モードがあります。DVMRP は、DVMRP トンネルが設定されていることを示します。
Neighbor Count	このインターフェイス全体で発見された PIM ネイバーの数。DVMRP トンネルの Neighbor Count が 1 である場合、ネイバーはアクティブです(プロブおよびレポートを受信します)。
Query Interval	PIM ルータ クエリ メッセージの頻度(秒)、ip pim query-interval インターフェイス コンフィギュレーション コマンドによって設定されます。
DR	LAN 上の指定ルータの IP アドレス。シリアル回線には指定ルータはありません。そのため、IP アドレスは 0.0.0.0 と表示されます。
FS	ファスト スイッチング。この列にアスタリスク(*)が表示されている場合は、ファスト スイッチングがイネーブルであることを示します。
Mpackets In/Out	電源の投入後にインターフェイスを出入りするパケット数。

# show ip pim neighbor

発見された PIM ネイバーのリストを表示するには、`show ip pim neighbor` コマンドを使用します。

```
show ip pim [vrf vrf-name] neighbor [{vlan num} | {tunnel num}]
```

シンタックスの説明	
<i>vrf vrf-name</i>	(任意) マルチキャスト VPN Routing/Forwarding instance (VRF; VPN ルーティング/転送インスタンス) に割り当てられた名前を指定します。
<i>rp-addr</i>	(任意) 指定フォワーダのホスト名または IP アドレス。
<i>vlan num</i>	(任意) VLAN (仮想 LAN) 番号を指定します。有効値は 1 ~ 4094 です。
<i>tunnel num</i>	(任意) トンネル番号を指定します。有効値は 0 ~ 214748364 です。

**デフォルト** このコマンドにはデフォルト設定がありません。

**コマンドモード** EXEC

コマンド履歴	リリース	変更内容
	12.2(18)SXF	このコマンドのサポートが Supervisor Engine 720 に追加されました。

**使用上のガイドライン** このコマンドは、Supervisor Engine 2 で構成された Catalyst 6500 シリーズスイッチ上ではサポートされません。

このコマンドは、PIM 用に設定されているインターフェイス上でサポートされます。

このコマンドを使用して、PIM 用に設定されている LAN 上のルータを判別します。

**例** 次に、発見された PIM ネイバーのリストを表示する例を示します。

```
Router# show ip pim neighbor
```

```
PIM Neighbor Table
Neighbor Address  Interface          Uptime    Expires    Mode
192.168.37.2      Ethernet0          17:38:16  0:01:25    Dense
192.168.37.33     Ethernet0          17:33:20  0:01:05    Dense (DR)
192.168.36.131    Ethernet1          17:33:20  0:01:08    Dense (DR)
192.168.36.130    Ethernet1          18:56:06  0:01:04    Dense
10.1.22.9         Tunnel0            19:14:59  0:01:09    Dense
```

表 2-5 に、出力に示されるフィールドの説明を示します。

表 2-5 show ip pim neighbor のフィールドの説明

フィールド	説明
Neighbor Address	PIM ネイバーの IP アドレス。
Interface	到達可能なネイバーのインターフェイス タイプおよび番号。
Uptime	PIM ネイバー テーブルにエントリが存在する時間 (時、分、秒)。
Expires	エントリが IP マルチキャスト ルーティング テーブルから削除されるまでの時間 (時、分、秒)。
Mode	インターフェイスが動作しているモード。
(DR)	このネイバーが LAN 上の指定ルータかどうかのステータス。

# show l3-mgr

レイヤ 3 マネージャの情報を表示するには、`show l3-mgr` コマンドを使用します。

```
show l3-mgr status
```

```
show l3-mgr {interface {{interface interface-number} | {null interface-number} |
{port-channel number} | {vlan vlan-id} | status}}
```

## シンタックスの説明

<code>status</code>	グローバル引数情報を表示します。
<code>interface</code>	インターフェイスの詳細なレイヤ 3 マネージャを表示します。
<code>interface</code>	インターフェイス タイプ。使用できる値は <code>pos</code> 、 <code>atm</code> 、および <code>ge-wan</code> です。
<code>interface-number</code>	モジュールおよびポート番号。有効値については、「使用上の注意事項」を参照してください。
<code>null interface-number</code>	ヌル インターフェイスを指定します。有効値は 0 です。
<code>port-channel number</code>	ポートチャネル番号を指定します。有効値は 1 ~ 282 です。
<code>vlan vlan-id</code>	VLAN を指定します。vlan-id の有効値は 1 ~ 4094 です。
<code>status</code>	レイヤ 3 マネージャのステータス情報を表示します。

## デフォルト

このコマンドにはデフォルト設定がありません。

## コマンドモード

EXEC

## コマンド履歴

リリース	変更内容
12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

## 使用上のガイドライン

このコマンドはデバッグに使用できます。出力は Cisco TAC および技術上の目的にのみ使用します。

モジュールおよびポート番号を指定するには、`interface-number` 引数を使用します。`interface-number` の有効値は、指定したインターフェイス タイプおよび使用されているシャーシおよびモジュールによって決まります。たとえば、ギガビットイーサネット インターフェイスを指定し、Catalyst 6513 シャーシに搭載された 48 ポート 10/100BASE-T イーサネット モジュールを使用する場合、モジュール番号の有効値は 2 ~ 13 で、ポート番号の有効値は 1 ~ 48 です。

## 例

次に、レイヤ 3 マネージャのステータス情報を表示する例を示します。

```
Router# show l3-mgr status
l3_mgr_state:          2
l3_mgr_req_q.count:   0
l3_mgr_req_q.head:    0
l3_mgr_req_q.tail:    0
l3_mgr_max_queue_count: 1060
l3_mgr_shrunk_count:  0
l3_mgr_req_q.ip_inv_count: 303
l3_mgr_req_q.ipx_inv_count: 0
l3_mgr_outpak_count:  18871
l3_mgr_inpak_count:   18871

l3_mgr_max_pending_pak: 4
l3_mgr_pending_pak_count: 0

nde enable statue:    0
current nde addr:     0.0.0.0

Router#
```

次に、特定のインターフェイスのレイヤ 3 マネージャ情報を表示する例を示します。

```
Router# show l3-mgr interface ge-wan 5/40
vlan:          0
ip_enabled:    1
ipx_enabled:   1
bg_state:      0 0 0 0
hsrp_enabled:  0
hsrp_mac:      0000.0000.0000
state:         0
up:           0

Router#
```

# show microcode

すべてがバンドルされたランタイム スーパーバイザ エンジンの MCP および Link Control Protocol (LCP) イメージのバージョンを表示するには、**show microcode** コマンドを使用します。

**show microcode**

**シンタックスの説明** このコマンドには、引数またはキーワードはありません。

**デフォルト** このコマンドにはデフォルト設定がありません。

**コマンドモード** EXEC

コマンド履歴	リリース	変更内容
	12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

**例** 次に、マイクロコードのバージョンを表示する例を示します。

Console> (enable) **show microcode**

Bundled Images	Version	Size	Built
LCP SLCP	6.2(0.92)	330918	02/16/01 01:26:27
LCP LX1000	6.2(0.92)	312782	02/16/01 01:27:59
LCP LX10100	6.2(0.92)	364846	02/16/01 01:26:47
LCP AX10100	6.2(0.92)	380296	02/16/01 01:27:10
LCP AX1000	6.2(0.92)	338672	02/16/01 01:28:19
LCP VX10100	6.2(0.92)	378532	02/16/01 01:27:35
LCP CPSLCP	6.2(0.92)	585234	02/16/01 00:59:19
LCP CPFAB	6.2(0.92)	251186	02/16/01 01:02:58
LCP CPGBIT	6.2(0.92)	579282	02/16/01 01:00:49
LCP CP10G	6.2(0.92)	477778	02/16/01 01:02:17
LCP CPMBIT2	6.2(0.92)	777922	02/16/01 01:05:20

Console> (enable) show

## show mls cef ip

Multilayer Switching (MLS; マルチレイヤ スイッチング) ハードウェア レイヤ 3 スイッチング テーブル内の IP エントリを表示するには、**show mls cef ip** コマンドを使用します。

```
show mls cef ip [{prefix [mask | module number]} | {module number} | {multicast [{prefix [mask | module num]}]}]
```

### シンタックスの説明

<i>prefix</i>	(任意) A.B.C.D のフォーマットでプレフィクスを入力します。
<i>mask</i>	(任意) A.B.C.D のフォーマットでプレフィクス マスクを入力します。
<i>module number</i>	(任意) 特定のモジュールのエントリを表示します。
<i>multicast</i>	(任意) IP マルチキャスト エントリを表示します。

### デフォルト

このコマンドにはデフォルト設定がありません。

### コマンドモード

EXEC

### コマンド履歴

リリース	変更内容
12.2(17a)SXA	このコマンドのサポートが MSFC3 に追加されました。

### 使用上のガイドライン

**show mls cef ip** コマンド出力の情報は、**show mls ip** コマンドの出力にも表示されます。

### 例

次に、MLS ハードウェア レイヤ 3 スイッチング テーブル内の IP エントリを表示する例を示します。

```
Router# show mls cef ip
Codes: G-GRE encap, W-WCCP encap, M-MPLS encap
       I-IP encap, + - Push Label
Index  Prefix                               Out i/f           Tunnel i/f
-----  -----                               -
192    127.0.0.22/32                          punt
193    127.0.0.0/32                            punt
194    127.255.255.255/32                     punt
195    0.0.0.0/32                              punt
196    255.255.255.255/32                     punt
197    200.2.5.3/32                            punt
Router#
```

### 関連コマンド

[mls ip cef rate-limit](#)  
[mls ip cef rpf interface-group](#)  
[mls ip cef rpf multipath](#)  
[show mls cef ip multicast](#)

## show mls cef ip multicast

スイッチ プロセッサ上の Multilayer Switching (MLS; マルチレイヤ スイッチング) ハードウェア レイヤ 3 スイッチング テーブル内の IP エントリを表示するには、**show mls cef ip multicast** コマンドを使用します。

```
show mls cef ip multicast {bidir | grp-only | source source-ip} [detail | group group-id | vlan rpf-vlanid]
```

```
show mls cef ip multicast control [detail | prefix prefix | vlan rpf-vlanid]
```

```
show mls cef ip multicast group group-id [detail | vlan rpf-vlanid]
```

```
show mls cef ip multicast src-grp [detail | group group-ip | source | vlan rpf-vlanid]
```

```
show mls cef ip multicast subnet [detail | prefix prefix | vlan rpf-vlanid]
```

```
show mls cef ip multicast summary [vpn-num]
```

```
show mls cef ip multicast tcam [prefix [mask-length]] [detail] [module num] [vrf src-ip {src-port | dst-ip} {dst-port | module num}]
```

```
show mls cef ip multicast {grp-mask | vlan rpf-vlanid | vpn vpn-id} [detail]
```

### シンタックスの説明

<b>bidir</b>	Bidir 情報を表示します。
<b>grp-only</b>	(*,G) ショートカットに基づいたハードウェア エントリ情報を表示します。詳細については「使用上の注意事項」を参照してください。
<b>source source-ip</b>	指定の送信元 IP アドレスに基づいたハードウェア エントリ情報を表示します。
<b>detail</b>	(任意) ハードウェア エントリの詳細情報を表示します。
<b>group group-id</b>	(任意) 指定のグループ IP アドレスに基づいたハードウェア エントリ情報を表示します。
<b>vlan rpf-vlanid</b>	(任意) 特定の Reverse Path Forwarding (RPF) VLAN (仮想 LAN) ID に関する情報を表示します。有効値は 0 ~ 4095 です。
<b>control</b>	(*,G/m) エントリに基づいたハードウェア エントリ情報を表示します。詳細については「使用上の注意事項」を参照してください。
<b>prefix prefix</b>	(任意) IP サブネット プレフィクスに基づいたハードウェア エントリ情報を表示します。
<b>src-grp</b>	(S,G) ショートカットに基づいたハードウェア エントリ情報を表示します。詳細については「使用上の注意事項」を参照してください。
<b>subnet</b>	(S/m,*) ショートカットに基づいたハードウェア エントリ情報を表示します。詳細については「使用上の注意事項」を参照してください。
<b>summary</b>	設置されたハードウェア ショートカットの概要を表示します。
<b>tcam</b>	コンパクト フォーマットの Cisco Express Forwarding (CEF) テーブル情報を表示します。
<b>mask-length</b>	(任意) サブネット マスクを指定します。
<b>module num</b>	(任意) 特定のモジュールのエントリを表示します。
<b>vrf src-ip</b>	(任意) 特定の送信元 IP アドレスの数値 VRF ID を表示します。
<b>src-port</b>	(任意) レイヤ 4 送信元ポート。有効値は 0 ~ 65535 です。
<b>dst-ip</b>	(任意) 宛先 IP アドレス。
<b>dst-port</b>	(任意) レイヤ 4 宛先ポート。有効値は 0 ~ 65535 です。
<b>grp-mask</b>	Bidir (*,G/m) ショートカットに基づいたハードウェア エントリ情報を表示します。
<b>vpn vpn-id</b>	特定の VPN ID に基づいたハードウェア エントリの情報を表示します。有効値は 0 ~ 4095 です。

**デフォルト** このコマンドにはデフォルト設定がありません。

**コマンドモード** スイッチ プロセッサ EXEC

コマンド履歴	リリース	変更内容
	12.2(17a)SXA	このコマンドのサポートが MSFC3 に追加されました。

**使用上のガイドライン** 入出力の 2 つの Multicast Multilayer Switching( MMLS; マルチキャスト マルチレイヤ スイッチング) モードがあります。表示される出力は各モードによって異なります。

ハードウェア エントリのタイプは次のとおりです。

- {S/m,\*} 直接接続された送信元を検出するのに使用されるインターフェイス / マスク (またはサブネット) のエントリ。
- {\*,G/m} グループ / マスクとしての RP にサービスされるグループ。
- {G,C} G は、IP マルチキャスト アドレスから抽出される宛先 MAC (メディア アクセス制御) アドレスを意味します。C は入力 VLAN を意味します。
- {S,G,C} S は送信元 IP アドレスを意味します。G はマルチキャスト アドレスの宛先 IP アドレスを意味します。C は、通常フローの RPF VLAN である入力 VLAN を意味します。
- {S,G} ソフトウェアによって維持されるマルチキャスト ルーティング テーブルのエントリまたは FIB (転送情報ベース) テーブルに作成されたマルチキャスト転送テーブルのエントリ。
- {\*,G} 送信元アドレスがワイルドカードである以外は {S,G} と同様。

DF インデックス フィールドの範囲は 1 ~ 4 で、承認 (PIM-RP x DF) テーブル内部にあります。承認テーブルは DF 転送で使用され、Virtual Private Network (VPN; バーチャル プライベート ネットワーク) の 4 つの RP ごとの DF インスタンスのセットの識別に使用されます。

**例** 次に、Bidir (\*,G/m) ショートカットに基づいた入力ハードウェア エントリ情報を表示する例を示します。

```
Router# show mls cef ip multicast grp-mask
```

```
Multicast CEF Entries for VPN#0
Flags: R - Control, S - Subnet, B - Bidir, C - Complete, P - Partial,
       c - Central Rewrite, p - Primary Input, r - Recirculation
Source/mask      Destination/mask  RPF/DF  Flags #packets      #bytes
rwindeX  Output Vlans/Info
-----+-----+-----+-----+-----+-----+-----+
*          226.2.2.0/24          Df0    BCp    0          0
-          V150 [1 oifs]
*          225.2.2.0/24          Df1    BCp    0          0
-          V151 [1 oifs]
*          227.2.2.0/24          Df1    BCp    0          0
-          V151 [1 oifs]
Found 3 entries. 3 are mfd entries
Router#
```

## ■ show mls cef ip multicast

次に、Bidir (\*,G/m) ショートカットに基づいた入力ハードウェア エントリ情報の詳細を表示する例を示します。

```
Router# show mls cef ip multicast grp-mask detail
(*, 226.2.2.0/24)
  PI:1 (1) CR:0 (0) Recirc:0 (1)
  DFidx:0 AdjPtr:7,32775,65543,98311 FibRpfNf:0 FibRpfDf:0 FibAddr:0x100
  rwlans:0 rwindex:0x0 adjmac:0006.d606.e240 rdt:0 E:0 CAP1:0
  fmt:mcast 13rwlvd:1 DM:0 mtu:1518 rwtype:L3 met2:0x0 met3:0x5
  packets:000000000000 bytes:000000000000000000
  Starting Offset: 0x0005
  V E C: 50 I:0x00449

(*, 225.2.2.0/24)
  PI:1 (1) CR:0 (0) Recirc:0 (1)
  DFidx:1 AdjPtr:8,32776,65544,98312 FibRpfNf:0 FibRpfDf:0 FibAddr:0x102
  rwlans:0 rwindex:0x0 adjmac:0006.d606.e240 rdt:0 E:0 CAP1:0
  fmt:mcast 13rwlvd:1 DM:0 mtu:1518 rwtype:L3 met2:0x0 met3:0x6
  packets:000000000000 bytes:000000000000000000
  Starting Offset: 0x0006
  V E C: 51 I:0x0044B

(*, 227.2.2.0/24)
  PI:1 (1) CR:0 (0) Recirc:0 (1)
  DFidx:1 AdjPtr:19,32787,65555,98323 FibRpfNf:0 FibRpfDf:0 FibAddr:0x104
  rwlans:0 rwindex:0x0 adjmac:0006.d606.e240 rdt:0 E:0 CAP1:0
  fmt:mcast 13rwlvd:1 DM:0 mtu:1518 rwtype:L3 met2:0x0 met3:0x7
  packets:000000000000 bytes:000000000000000000
  Starting Offset: 0x0007
  V E C: 51 I:0x0044B

Found 3 entries. 3 are mfd entries
Router#
```

次に、Bidir 情報を表示する例を示します。

```
Router# show mls cef ip multicast bidir

Multicast CEF Entries for VPN#0
Flags: R - Control, S - Subnet, B - Bidir, C - Complete, P - Partial,
       c - Central Rewrite, p - Primary Input, r - Recirculation
Source/mask      Destination/mask  RPF/DF  Flags #packets  #bytes
rwindex  Output Vlan/Info
+-----+-----+-----+-----+-----+-----+
--+-+-----+-----+-----+-----+-----+-----+
*          225.2.2.2/32          Df1    BCp    0          0
-          V151,V130 [2 oifs]
*          225.2.2.1/32          Df1    BCp    0          0
-          V151,V130 [2 oifs]
Found 2 entries. 2 are mfd entries
Router#
```

次に、Bidir 情報の詳細を表示する例を示します。

```
Router# show mls cef ip multicast bidir detail

(*, 225.2.2.2)
  PI:1 (1) CR:0 (0) Recirc:0 (1)
  DFidx:1 AdjPtr:10,32778,65546,98314 FibRpfNf:0 FibRpfDf:0 FibAddr:0xE2
  rrvlans:0 rwindex:0x0 adjmac:0006.d606.e240 rdt:0 E:0 CAP1:0
  fmt:mcast l3rvld:1 DM:0 mtu:1518 rwtype:L3 met2:0x0 met3:0xA
  packets:000000000000 bytes:000000000000000000
  Starting Offset: 0x000A
    V C: 51 I:0x004B5 P->19A0
  - V
    V E C: 30 I:0x0049B

(*, 225.2.2.1)
  PI:1 (1) CR:0 (0) Recirc:0 (1)
  DFidx:1 AdjPtr:9,32777,65545,98313 FibRpfNf:0 FibRpfDf:0 FibAddr:0xE0
  rrvlans:0 rwindex:0x0 adjmac:0006.d606.e240 rdt:0 E:0 CAP1:0
  fmt:mcast l3rvld:1 DM:0 mtu:1518 rwtype:L3 met2:0x0 met3:0x8
  packets:000000000000 bytes:000000000000000000
  Starting Offset: 0x0008
    V C: 51 I:0x004B1 P->199C
  - V
    V E C: 30 I:0x00499

Found 2 entries. 2 are mfd entries
Router#
```

次に、Bidir (\*,G/m) ショートカットに基づいた出力ハードウェア エントリ情報を表示する例を示します。

```
Router# show mls cef ip multicast grp-mask

Multicast CEF Entries for VPN#0
Flags: R - Control, S - Subnet, B - Bidir, C - Complete, P - Partial,
       c - Central Rewrite, p - Primary Input, r - Recirculation
Source/mask      Destination/mask  RPF/DF  Flags #packets    #bytes
rwindex  Output Vlans/Info
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
*                225.2.2.0/24      Df0    BCp    0            0
-
*                225.2.2.0/24      -      Bpr    0            0
0x4AE   Vl151 [1 oifs]
*                225.2.2.0/24      -      Br     0            0
0x40E   Vl151 [1 oifs]
*                226.2.2.0/24      Df1    BCp    0            0
-
*                226.2.2.0/24      -      Bpr    0            0
0x4AE   Vl150 [1 oifs]
*                226.2.2.0/24      -      Br     0            0
0x40E   Vl150 [1 oifs]
*                227.2.2.0/24      Df0    BCp    0            0
-
*                227.2.2.0/24      -      Bpr    0            0
0x4AE   Vl151 [1 oifs]
*                227.2.2.0/24      -      Br     0            0
0x40E   Vl151 [1 oifs]
Found 3 entries. 3 are mfd entries
Router#
```

次に、Bidir (\*,G/m) ショートカットに基づいた出力ハードウェア エントリ情報の詳細を表示する例を示します。

```
Router# show mls cef ip multicast grp-mask detail
(*, 225.2.2.0/24)
  PI:1 (1) CR:0 (0) Recirc:0 (1)
  DFidx:0 AdjPtr:7,32775,65543,98311 FibRpfNf:0 FibRpfDf:0 FibAddr:0x120
  rwlans:0 rwinde:0x0 rdt:0 E:0 CAP1:0
  fmt:recir l3rwl:1 DM:0 mtu:1522 rwtype:RECIR
  packets:000000000000 bytes:000000000000000000

  PI:1 (1) CR:0 (0) Recirc:1 (1)
  AdjPtr:8,32776,65544,98312 FibRpfNf:0 FibRpfDf:0 FibAddr:0x122
  rwlans:0 rwinde:0x4AE adjmac:0006.d606.e240 rdt:1 E:1 CAP1:0
  fmt:mcast l3rwl:1 DM:0 mtu:1522 rwtype:L3 met2:0x0 met3:0x5
  packets:000000000000 bytes:000000000000000000
  Starting Offset: 0x0005
  V E C: 51 I:0x0044C

  PI:0 (1) CR:0 (0) Recirc:1 (1)
  AdjPtr:9,32777,65545,98313 FibRpfNf:0 FibRpfDf:0 FibAddr:0x124
  rwlans:0 rwinde:0x40E adjmac:0006.d606.e240 rdt:1 E:0 CAP1:0
  fmt:mcast l3rwl:1 DM:0 mtu:1522 rwtype:L3 met2:0x0 met3:0x5
  packets:000000000000 bytes:000000000000000000
  Starting Offset: 0x0005
  V E C: 51 I:0x0044C

(*, 226.2.2.0/24)
  PI:1 (1) CR:0 (0) Recirc:0 (1)
  DFidx:1 AdjPtr:10,32778,65546,98314 FibRpfNf:0 FibRpfDf:0 FibAddr:0x126
  rwlans:0 rwinde:0x0 rdt:0 E:0 CAP1:0
  fmt:recir l3rwl:1 DM:0 mtu:1522 rwtype:RECIR
  packets:000000000000 bytes:000000000000000000

  PI:1 (1) CR:0 (0) Recirc:1 (1)
  AdjPtr:11,32779,65547,98315 FibRpfNf:0 FibRpfDf:0 FibAddr:0x128
  rwlans:0 rwinde:0x4AE adjmac:0006.d606.e240 rdt:1 E:1 CAP1:0
  fmt:mcast l3rwl:1 DM:0 mtu:1522 rwtype:L3 met2:0x0 met3:0x1C
  packets:000000000000 bytes:000000000000000000
  Starting Offset: 0x001C
  V E C: 50 I:0x00447

  PI:0 (1) CR:0 (0) Recirc:1 (1)
  AdjPtr:12,32780,65548,98316 FibRpfNf:0 FibRpfDf:0 FibAddr:0x12A
  rwlans:0 rwinde:0x40E adjmac:0006.d606.e240 rdt:1 E:0 CAP1:0
  fmt:mcast l3rwl:1 DM:0 mtu:1522 rwtype:L3 met2:0x0 met3:0x1C
  packets:000000000000 bytes:000000000000000000
  Starting Offset: 0x001C
  V E C: 50 I:0x00447

(*, 227.2.2.0/24)
  PI:1 (1) CR:0 (0) Recirc:0 (1)
  DFidx:0 AdjPtr:13,32781,65549,98317 FibRpfNf:0 FibRpfDf:0 FibAddr:0x12C
  rwlans:0 rwinde:0x0 rdt:0 E:0 CAP1:0
  fmt:recir l3rwl:1 DM:0 mtu:1522 rwtype:RECIR
  packets:000000000000 bytes:000000000000000000

  PI:1 (1) CR:0 (0) Recirc:1 (1)
  AdjPtr:14,32782,65550,98318 FibRpfNf:0 FibRpfDf:0 FibAddr:0x12E
  rwlans:0 rwinde:0x4AE adjmac:0006.d606.e240 rdt:1 E:1 CAP1:0
  fmt:mcast l3rwl:1 DM:0 mtu:1522 rwtype:L3 met2:0x0 met3:0x1D
  packets:000000000000 bytes:000000000000000000
  Starting Offset: 0x001D
  V E C: 51 I:0x0044C
```

```

PI:0 (1) CR:0 (0) Recirc:1 (1)
AdjPtr:15,32783,65551,98319 FibRpfNf:0 FibRpfDf:0 FibAddr:0x130
rwvlans:0 rwindex:0x40E adjmac:0006.d606.e240 rdt:1 E:0 CAP1:0
fmt:mcast l3rwvld:1 DM:0 mtu:1522 rwtype:L3 met2:0x0 met3:0x1D
packets:00000000000000 bytes:000000000000000000
Starting Offset: 0x001D
V E C: 51 I:0x0044C

```

```

Found 3 entries. 3 are mfd entries
Router#

```

次の例では、出力 Bidir 情報を表示する方法を示しています。

```
Router# show mls cef ip multicast bidir
```

```

Multicast CEF Entries for VPN#0
Flags: R - Control, S - Subnet, B - Bidir, C - Complete, P - Partial,
       c - Central Rewrite, p - Primary Input, r - Recirculation
Source/mask      Destination/mask  RPF/DF  Flags #packets    #bytes
rwindex  Output Vlans/Info
-----+-----+-----+-----+-----+-----+-----+
*                225.2.2.2/32      Df0     BCp    0              0
-
*                225.2.2.2/32      -       Bpr    0              0
0x4AE   V151,V130 [2 oifs]
*                225.2.2.2/32      -       Br     0              0
0x40E   V151,V130 [2 oifs]
*                225.2.2.1/32      Df0     BCp    0              0
-
*                225.2.2.1/32      -       Bpr    0              0
0x4AE   V151,V130 [2 oifs]
*                225.2.2.1/32      -       Br     0              0
0x40E   V151,V130 [2 oifs]

```

```

Found 2 entries. 2 are mfd entries
Router#

```

次の例では、出力 Bidir 情報の詳細を表示する方法を示しています。

```
Router# show mls cef ip multicast bidir detail

(*, 225.2.2.2)
PI:1 (1) CR:0 (0) Recirc:0 (1)
DFidx:0 AdjPtr:19,32787,65555,98323 FibRpfNf:0 FibRpfDf:0 FibAddr:0xE6
rwlans:0 rwindex:0x0 rdt:0 E:0 CAP1:0
fmt:recir l3rwlvd:1 DM:0 mtu:1522 rwtype:RECIR
packets:000000000000 bytes:000000000000000000

PI:1 (1) CR:0 (0) Recirc:1 (1)
AdjPtr:20,32788,65556,98324 FibRpfNf:0 FibRpfDf:0 FibAddr:0xE8
rwlans:0 rwindex:0x4AE adjmac:0006.d606.e240 rdt:1 E:1 CAP1:0
fmt:mcast l3rwlvd:1 DM:0 mtu:1522 rwtype:L3 met2:0x0 met3:0x22
packets:000000000000 bytes:000000000000000000
Starting Offset: 0x0022
V C: 51 I:0x004B3 P->24
V E C: 30 I:0x004B6

PI:0 (1) CR:0 (0) Recirc:1 (1)
AdjPtr:21,32789,65557,98325 FibRpfNf:0 FibRpfDf:0 FibAddr:0xEA
rwlans:0 rwindex:0x40E adjmac:0006.d606.e240 rdt:1 E:0 CAP1:0
fmt:mcast l3rwlvd:1 DM:0 mtu:1522 rwtype:L3 met2:0x0 met3:0x22
packets:000000000000 bytes:000000000000000000
Starting Offset: 0x0022
V C: 51 I:0x004B3 P->24
V E C: 30 I:0x004B6

(*, 225.2.2.1)
PI:1 (1) CR:0 (0) Recirc:0 (1)
DFidx:0 AdjPtr:16,32784,65552,98320 FibRpfNf:0 FibRpfDf:0 FibAddr:0xE0
rwlans:0 rwindex:0x0 rdt:0 E:0 CAP1:0
fmt:recir l3rwlvd:1 DM:0 mtu:1522 rwtype:RECIR
packets:000000000000 bytes:000000000000000000

PI:1 (1) CR:0 (0) Recirc:1 (1)
AdjPtr:17,32785,65553,98321 FibRpfNf:0 FibRpfDf:0 FibAddr:0xE2
rwlans:0 rwindex:0x4AE adjmac:0006.d606.e240 rdt:1 E:1 CAP1:0
fmt:mcast l3rwlvd:1 DM:0 mtu:1522 rwtype:L3 met2:0x0 met3:0x1E
packets:000000000000 bytes:000000000000000000
Starting Offset: 0x001E
V C: 51 I:0x004AF P->20
V E C: 30 I:0x004B2

PI:0 (1) CR:0 (0) Recirc:1 (1)
AdjPtr:18,32786,65554,98322 FibRpfNf:0 FibRpfDf:0 FibAddr:0xE4
rwlans:0 rwindex:0x40E adjmac:0006.d606.e240 rdt:1 E:0 CAP1:0
fmt:mcast l3rwlvd:1 DM:0 mtu:1522 rwtype:L3 met2:0x0 met3:0x1E
packets:000000000000 bytes:000000000000000000
Starting Offset: 0x001E
V C: 51 I:0x004AF P->20
V E C: 30 I:0x004B2

Found 2 entries. 2 are mfd entries
Router#
```

## 関連コマンド

[mls ip cef rate-limit](#)  
[mls ip cef rpf interface-group](#)  
[mls ip cef rpf multipath](#)  
[show mls cef ip](#)

# show msfc2 rom-monitor

ROM Monitor (ROMMON;ROM モニタ) リージョンのステータスを表示するには、`show msfc2 rom-monitor` コマンドを使用します。

```
show msfc2 rom-monitor
```

**シンタックスの説明** このコマンドには、引数またはキーワードはありません。

**デフォルト** このコマンドにはデフォルト設定がありません。

**コマンドモード** EXEC

コマンド履歴	リリース	変更内容
	12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

**例** 次に、ROMMON 情報を表示する例を示します。

```
Router# show msfc3 rom-monitor

Region region1: APPROVED, preferred
Region region2: INVALID
Currently running ROMMON from region1 region
Router#
```

表 2-6 に、`show msfc2 rom-monitor` コマンド出力に含まれる可能性のあるフィールドについて説明します。

**表 2-6 show msfc2 rom-monitor コマンドの出力フィールド**

フィールド	説明
Region region1 and region2	ROMMON のイメージ状態、および起動に使用するリージョン 1 またはリージョン 2 のイメージの優先順位
First run	実行中の新規イメージのチェックを示す ROMMON イメージの状態
Invalid	新規イメージのチェックが完了し、アップグレードプロセスが開始していることを示す ROMMON イメージの状態
Approved	ROMMON フィールドのアップグレード プロセスが完了していることを示す ROMMON イメージの状態
Currently running	現在実行しているイメージおよびリージョン

**関連コマンド** [upgrade rom-monitor](#)

# show redundancy

冗長ハイアベイラビリティの設定を表示するには、**show redundancy** コマンドを使用します。

**show redundancy**

**シンタックスの説明** このコマンドには、引数またはキーワードはありません。

**デフォルト** このコマンドにはデフォルト設定がありません。

**コマンドモード** EXEC

コマンド履歴	リリース	変更内容
	12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

**例** 次に、Redundancy Facility (RF) クライアントに関する情報を表示する例を示します。

```
Router# show redundancy
Designated Router: 2 Non-designated Router: 0
Redundancy Status: designated
Config Sync AdminStatus : enabled
Config Sync RuntimeStatus: disabled
Single Router Mode AdminStatus : disabled
Single Router Mode RuntimeStatus: disabled
Single Router Mode transition timer : 120 seconds
Router#
```

# show scp

Switch-Module Configuration Protocol (SCP) 情報を表示するには、**show scp** コマンドを使用します。

```
show scp {accounting | counters | {process [id]} | status}
```

## シンタックスの説明

<b>accounting</b>	SCP アカウンティング情報を表示します。
<b>counters</b>	SCP カウンタ情報を表示します。
<b>process <i>id</i></b>	特定のプロセスおよびプロセス ID に関する情報を表示します。
<b>status</b>	ローカル SCP サーバのステータス情報を表示します。

## デフォルト

このコマンドにはデフォルト設定がありません。

## コマンドモード

EXEC

## コマンド履歴

リリース	変更内容
12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

## 使用上のガイドライン

このコマンドはデバッグに使用できます。出力は Cisco TAC および技術上の目的にのみ使用します。

## 例

次に、SCP アカウンティング情報を表示する例を示します。

```
Router> show scp accounting

      Total 11  1D  1E  2C  82  100  105  10F  119  11C  11D  11E  127
-----
Tot: 10F8  FFC1 2   2   3   1   0   1   2   2   1   6   E   110E
      10FB  FFC1 2   2   3   1   2   1   2   3   1   6   E   110E
11:  10F8  FFC1 2   2   3   1   0   1   2   2   1   6   E   110E
      10FA  FFC1 2   2   3   1   1   1   2   3   1   6   E   110E
13:  0     0     0     0     0     0     0     0     0     0     0     0     0     0
      1     0     0     0     0     0     1     0     0     0     0     0     0     0

      12B  157  1FF
-----
Tot: 1     4     2
      1     4     2
11:  1     4     2
      1     4     2
13:  0     0     0
      0     0     0
Router>
```

次に、SCP カウンタ情報を表示する例を示します。

```
Router> show scp counters
received packets      = 69896
transmitted packets  = 69894
retransmitted packets = 0
loop back packets    = 0
transmit failures     = 0
recv pkts not for me = 0
recv pkts to dead process = 0
recv pkts not enqueueable = 0
response has wrong opcode = 0
response has wrong seqnum = 0
response is not an ack = 0
response is too big   = 0
Router>
```

次に、プロセス名および送受信されるメッセージ数を表示する例を示します。

```
Router> show scp process
PID Process           Msgs      Msgs      NMP Tx Q      Msgs      Bufs  Rx Q  Rx Q
                   Sent      Resent    in Overflow Rcvd      Held  Size Oflow
-----
0   Kernel and Idle   2          0          0              0          0     0    0
1   Flash MIB Updat  0          0          0              0          0     0    0
2   SynDiags          1410       0          0             1410       0     4    0
3   SynConfig         2          0          0             3481603    0    64    0
4   Statuspoll       3481589    0          0              0          0     2    0
5   SL_TASK           0          0          0              0          0    24    0
.
.
.
```

次に、ローカル SCP のサーバステータス情報を表示する例を示します。

```
Router> show scp status
Rx 69866, Tx 69864, Sap 6
Id      Channel name           # msgs pending  # peak count
-----
0   SCP async: TCAM MGR Chann      0              5
1   SCP async: l3_mgr scp cha      0              1
2   SCP async: l3_mgr scp cha      0              2
3   SCP async: Draco-NMP          0              1
Router>
```

## show slot0:

スロット 0: ファイル システムの情報を表示するには、**show slot0:** コマンドを使用します。

**show slot0:** [all | chips | filesys]

<b>シンタックスの説明</b>	<b>all</b>	(任意) すべてのフラッシュ情報を表示します。これには、 <b>show slot0:chips</b> および <b>show slot0:filesys</b> コマンドによる出力情報も含まれます。
	<b>chips</b>	(任意) フラッシュ チップに関する情報を表示します。
	<b>filesys</b>	(任意) ファイル システムに関する情報を表示します。

**デフォルト** このコマンドにはデフォルト設定がありません。

**コマンドモード** EXEC

<b>コマンド履歴</b>	<b>リリース</b>	<b>変更内容</b>
	12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

**例** 次に、イメージに関する情報を表示する例を示します。

```
Router> show slot0:
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time----- name
1  .. image    6375DBB7  A4F144    6 10678468 Nov 09 1999 10:50:42 halley

5705404 bytes available (10678596 bytes used)
Router>
```

## ■ show slot0:

次に、フラッシュ チップに関する情報を表示する例を示します。

```
Router> show slot0: chips
***** Intel Series 2+ Status/Register Dump *****

ATTRIBUTE MEMORY REGISTERS:
  Config Option Reg (4000): 2
  Config Status Reg (4002): 0
  Card Status Reg (4100): 1
  Write Protect Reg (4104): 4
  Voltage Cntrl Reg (410C): 0
  Rdy/Busy Mode Reg (4140): 2

COMMON MEMORY REGISTERS: Bank 0
  Intelligent ID Code : 8989A0A0
  Compatible Status Reg: 8080
  Global Status Reg: B0B0
  Block Status Regs:
    0 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
    8 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
   16 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
   24 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0

COMMON MEMORY REGISTERS: Bank 1
  Intelligent ID Code : 8989A0A0
  Compatible Status Reg: 8080
  Global Status Reg: B0B0
  Block Status Regs:
    0 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
    8 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
   16 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
   24 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0

COMMON MEMORY REGISTERS: Bank 2
  Intelligent ID Code : 8989A0A0
  Compatible Status Reg: 8080
  Global Status Reg: B0B0
  Block Status Regs:
    0 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
    8 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
   16 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
   24 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0

COMMON MEMORY REGISTERS: Bank 3
  Intelligent ID Code : 8989A0A0
  Compatible Status Reg: 8080
  Global Status Reg: B0B0
  Block Status Regs:
    0 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
    8 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
   16 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
   24 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0

COMMON MEMORY REGISTERS: Bank 4
  Intelligent ID Code : FFFFFFFF
  IID Not Intel -- assuming bank not populated

Router>
```

次に、ファイルシステムに関する情報を表示する例を示します。

```
Router> show slot0: fileysys

----- F I L E   S Y S T E M   S T A T U S -----
  Device Number = 0
DEVICE INFO BLOCK: slot0
  Magic Number      = 6887635   File System Vers = 10000   (1.0)
  Length            = 1000000   Sector Size      = 20000
  Programming Algorithm = 4     Erased State     = FFFFFFFF
  File System Offset = 20000    Length = FA0000
  MONLIB Offset     = 100       Length = F568
  Bad Sector Map Offset = 1FFF0  Length = 10
  Squeeze Log Offset = FC0000   Length = 20000
  Squeeze Buffer Offset = FE0000  Length = 20000
  Num Spare Sectors = 0
  Spares:
STATUS INFO:
  Writable
  NO File Open for Write
  Complete Stats
  No Unrecovered Errors
  No Squeeze in progress
USAGE INFO:
  Bytes Used      = 9F365C   Bytes Available = 5AC9A4
  Bad Sectors    = 0        Spared Sectors  = 0
  OK Files       = 1        Bytes = 9F35DC
  Deleted Files  = 0        Bytes = 0
  Files w/Errors = 0        Bytes = 0

Router>
```

# show standby delay

Hot Standby Router Protocol (HSRP) 遅延時間に関する情報を表示するには、**show standby delay** コマンドを使用します。

```
show standby delay [type number]
```

<b>シンタックスの説明</b>	<i>type number</i> (任意) 出力を表示するインターフェイスのタイプおよび番号
------------------	--

<b>デフォルト</b>	このコマンドにはデフォルト設定がありません。
--------------	------------------------

<b>コマンドモード</b>	特権 EXEC
----------------	---------

<b>コマンド履歴</b>	<b>リリース</b>	<b>変更内容</b>
	12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

<b>例</b>	次に、 <b>show standby delay</b> コマンドの出力例を示します。
----------	--

```
Router# show standby delay

Interface          Minimum Reload
VLAN100           1             5
Router#
```

<b>関連コマンド</b>	<a href="#">standby delay minimum reload</a>
---------------	--

## snmp-server enable traps

システム上で使用可能な SNMP (簡易ネットワーク管理プロトコル) 通知 (トラップまたは通知) をイネーブルにするには、**snmp-server enable traps** コマンドを使用します。すべての使用可能な SNMP 通知をディセーブルにするには、このコマンドの **no** 形式を使用します。

**snmp-server enable traps** [*notification-type*]

**no snmp-server enable traps** [*notification-type*]

<b>シンタックスの説明</b>	<i>notification-type</i>	(任意) イネーブルまたはディセーブルにする通知 (トラップまたは通知) タイプ。タイプが指定されない場合、デバイス上で使用可能なすべての通知がイネーブルまたはディセーブルになります。有効値については、「使用上の注意事項」を参照してください。
------------------	--------------------------	---

**デフォルト** このコマンドは、デフォルトではディセーブルです。ほとんどの通知タイプがディセーブルです。ただし、一部の通知タイプはこのコマンドで制御することはできません。

*notification-type* を指定せずにこのコマンドを入力した場合、このコマンドで制御されるすべての通知タイプがイネーブルになります。

イネーブルの場合、デフォルト設定は次のとおりです。

- *interval seconds* は 30 です。
- *fail-interval seconds* は 0 です。

**コマンドモード** グローバル コンフィギュレーション

コマンド履歴	リリース	変更内容
	12.1(11b)E	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

**使用上のガイドライン** 通知タイプの詳細については、Cisco IOS のマニュアルを参照してください。

SNMP 通知はトラップまたは通知要求として送信されます。このコマンドは、指定の通知タイプのトラップおよび通知要求の両方をイネーブルにします。通知をトラップまたは通知のどちらで送信するかを指定するには、**snmp-server host** [*traps* | *informs*] コマンドを使用します。

**snmp-server enable traps** コマンドを入力しない場合、このコマンドの制御で送信される通知はありません。ルータを設定し、これらの SNMP 通知を送信するには、最低 1 つの **snmp-server enable traps** コマンドを入力する必要があります。キーワードを指定せずにコマンドを入力した場合、すべての通知タイプはイネーブルになります。キーワードを指定してコマンドを入力した場合、キーワードに関連した通知タイプのみイネーブルになります。複数の通知タイプをイネーブルにするには、各通知タイプおよび通知オプションの **snmp-server enable traps** コマンドを個別に使用します。

**snmp-server enable traps** コマンドは、**snmp-server host** コマンドと使用します。SNMP 通知を受信するホストを指定するには、**snmp-server host** コマンドを使用します。通知を送信するには、最低 1 つの **snmp-server host** コマンドを使用し、設定する必要があります。

*notification-type* の有効値は次のとおりです。

- **atm** Asynchronous Transfer Mode( ATM; 非同期転送モード )PVC 通知をイネーブルにします。  
**atm pvc** を入力すると、さらに *notification-option* の値を指定できます。
- **bgp** Border Gateway Protocol ( BGP ) のステート変更通知をイネーブルにします。
- **config** コンフィギュレーション通知をイネーブルにします。
- **dls** Data Link Switching ( DLSw; データリンク スイッチング ) 通知をイネーブルにします。
- **entity** エンティティ通知をイネーブルにします。
- **frame-relay** フレームリレー通知をイネーブルにします。
- **hsrp** Hot Standby Router Protocol ( HSRP ) 通知をイネーブルにします。
- **isdn** ISDN トラップをイネーブルにします。*isdn* を入力すると、*notification-option* の値を指定できます。
- **rsvp** Resource Reservation Protocol ( RSVP ) フロー変更の通知をイネーブルにします。
- **rtr** Response Time Reporter 通知をイネーブルにします。
- **snmp** SNMP 通知をイネーブルにします。**snmp** を入力すると、さらに *notification-option* の値を指定できます。
- **syslog** エラー メッセージの通知( Cisco syslog MIB[ 管理情報ベース ] )をイネーブルにします。

## 例

次に、すべてのトラップを myhost.cisco.com という名で指定したホスト (パブリックとして定義されたコミュニティ文字列を使用) に送信する例を示します。

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com public
```

## 関連コマンド

**snmp-server enable traps** コマンドの詳細については、Cisco IOS マニュアルを参照してください。

## standby delay minimum reload

Hot Standby Router Protocol (HSRP) グループを初期化するまでの遅延時間を設定するには、**standby delay minimum reload** コマンドを使用します。遅延時間をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
standby delay minimum [min-delay] reload [reload-delay]
```

```
no standby delay minimum [min-delay] reload [reload-delay]
```

### シンタックスの説明

<i>min-delay</i>	(任意) インターフェイスの起動後に HSRP グループの初期化を遅らせる最小時間 (秒数)。有効な値は 0 ~ 10000 です。
<i>reload-delay</i>	(任意) ルータのリロード後の遅延時間 (秒数)。有効な値は 0 ~ 10000 です。

### デフォルト

デフォルト設定は次のとおりです。

- *min-delay* は 1 秒です。
- *reload-delay* は 5 秒です。

### コマンドモード

インターフェイス コンフィギュレーション

### コマンド履歴

リリース	変更内容
12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

### 使用上のガイドライン

この最小遅延期間は、以降のすべてのインターフェイス イベントに適用されます。

この遅延期間は、ルータのリロード後の最初のインターフェイス起動イベントにのみ適用されません。

アクティブ ルータに障害が発生するか、またはネットワークから取り除かれた場合は、スタンバイ ルータが自動的に新規のアクティブ ルータになります。元のアクティブ ルータがオンライン状態に戻った場合は、**standby preempt** コマンドを使用して、このルータにアクティブ ルータとしての機能を引き継がせるかどうかを制御できます。

ただし、**standby preempt** コマンドが設定されていない場合でも、元のアクティブ ルータをリロードしてオンライン状態に戻すと、このルータはアクティブ ルータとしての機能を再開します。HSRP グループの初期化の遅延期間を設定するには、**standby delay minimum reload** コマンドを使用します。このコマンドを使用すると、ルータがアクティブな機能を再開するまで、パケットの通過を許可する期間を設定できます。

**standby timers** コマンドがミリ秒単位で設定されている場合、またはスイッチの特定の VLAN (仮想 LAN) インターフェイスに HSRP が設定されている場合は、**standby delay minimum reload** コマンドの使用を推奨します。

ほとんどの設定では、デフォルト値により、パケットが通過する十分な期間が設定されます。これより長い遅延期間を設定する必要はありません。

HSRP パケットがインターフェイスに着信すると、遅延はキャンセルされます。

## ■ standby delay minimum reload

**例** 次に、最小遅延時間を 30 秒に、最初のリロード後の遅延時間を 120 秒に設定する例を示します。

```
Router(config-if) # standby delay minimum 30 reload 120
Router(config-if) #
```

**関連コマンド**

[show standby delay](#)

**standby delay minimum reload** (Cisco IOS のマニュアルを参照)

**standby preempt** (Cisco IOS のマニュアルを参照)

**standby timers** (Cisco IOS のマニュアルを参照)

# standby ip

Hot Standby Router Protocol (HSRP) をイネーブルにし、仮想 IP アドレスを設定するには、**standby ip** コマンドを使用します。HSRP をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
standby [group-number] ip [ip-addr [secondary]]
```

```
no standby [group-number] ip [ip-addr]
```

## シンタックスの説明

<i>group-number</i>	(任意) HSRP が有効なインターフェイス上のグループ番号。有効な値は 0 ~ 255 です。
<i>ip-addr</i>	(任意) ホットスタンバイのルータインターフェイスの IP アドレス
<i>secondary</i>	(任意) セカンダリの仮想 IP アドレスを指定します。

## デフォルト

デフォルト設定は次のとおりです。

- HSRP はディセーブルです。
- *group-number* *group-number* を指定しない場合、グループ 0 が使用されます。
- *priority* 10
- *delay* 0
- *hellotime* 3 秒
- *holdtime* 10 秒

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

リリース	変更内容
12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

## 使用上のガイドライン

**standby ip** コマンドは設定されたインターフェイス上で HSRP を有効にします。IP アドレスが指定されると、そのアドレスはホットスタンバイグループ用のアドレスとして使用されます。IP アドレスが指定されない場合、指定のアドレスがスタンバイ機能から学習されます。HSRP が指定のルータを選択する場合、配線上に最低 1 つのルータが指定のアドレスで設定されているか、または指定のアドレスを学習している必要があります。アクティブなルータ上で指定のアドレスを設定すると、現在使用している指定のアドレスは常に上書きされます。

**standby ip** コマンドをインターフェイス上でイネーブルにすると、プロキシ Address Resolution Protocol (ARP) 要求の処理が変更されます (プロキシ ARP がディセーブルでない場合)。インターフェイスのホットスタンバイステートがアクティブの場合、ホットスタンバイグループの MAC (メディアアクセス制御) アドレスを使うことでプロキシ ARP 要求に応答します。インターフェイスが異なる状態の場合、プロキシ ARP 応答は抑制されます。

グループ番号 0 が使用されている場合、グループ番号は NVRAM (不揮発性 RAM) に書き込まれずに、逆に互換性のある番号が提供されます。

トラブルシューティングを支援するため、*group-number* を設定し、VLAN (仮想 LAN) 番号を照合します。

HSRP グループで、最低 1 つのインターフェイスの *priority* を上げます。プライオリティの最も高いインターフェイスが HSRP グループ用にアクティブになります。

HSRP グループのすべてのインターフェイスは同一のタイマーの値を使用する必要があります。

HSRP グループのすべてのインターフェイスは同一の認証文字列を使用する必要があります。

**alt** キーワードを使用することで、代替コンフィギュレーションを指定できます。次のように使用されます。

```
[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]]
```

詳細については、「[alt キーワードの使用方法](#)」(p.1-10) を参照してください。

---

**例**

次に、インターフェイス上でグループ 1 の HSRP をイネーブルにする例を示します。ホットスタンバイグループが使用している IP アドレスは、HSRP により学習されます。

```
Router(config-if) # standby 1 ip  
Router(config-if) #
```

## standby track

他のインターフェイスの利用状況に基づいてホットスタンバイのプライオリティが変更されるようにインターフェイスを設定するには、**standby track** コマンドを使用します。グループのすべてのトラッキング設定を削除するには、**no standby group-number track** コマンドを使用します。

```
standby [group-number] track {interface-type interface-number | designated-router}
[priority-decrement]
```

```
no standby group-number track
```

シンタックスの説明	
<i>group</i>	(任意)トラッキングが適用されるインターフェイス上のグループ番号。有効な値は 0 ~ 255 です。
<i>interface-type</i> <i>interface-number</i>	トラッキングするインターフェイス タイプおよび番号。
<b>designated-router</b>	指定のルータを取りやめ、Hot Standby Router Protocol ( HSRP ) ルータを指定のルータにするかを指定します。
<i>priority-decrement</i>	(任意)インターフェイスがダウン(アップ)した場合に上げたり下げたりする、ルータのホットスタンバイのプライオリティ。有効な値は 1 ~ 255 です。

### デフォルト

デフォルト設定は次のとおりです。

- *group* は 0 です。
- *priority-decrement* は 10 です。
- **designated-router** オプションはディセーブルです。

### コマンドモード

インターフェイス コンフィギュレーション

### コマンド履歴

リリース	変更内容
12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

### 使用上のガイドライン

**designated-router** キーワードを入力する前に、新しい指定のルータが引き継ぐ現行のルータより高い HSRP のプライオリティを保有しているかを確認します。

トラッキングされたインターフェイスがダウンしている場合、ホットスタンバイのプライオリティは *priority-decrement* 引数で指定された数だけ下がります。インターフェイスがトラッキングされていなければ、ステートが変化した場合でもホットスタンバイのプライオリティに影響することはありません。ホットスタンバイとして設定された各インターフェイスには、トラックするインターフェイスのリストを別々に設定できます。

トラッキングされたインターフェイスが複数ダウンした場合、*priority-decrement* で値が設定されているかにかかわらず、プライオリティは下がっていきます。

IP アドレスがインターフェイス上でディセーブルであれば、トラッキングされたインターフェイスはダウンしていると認識されます。

このコマンドの **no** 形式を使用する場合、*group-number* を入力する必要があります。

インターフェイスのトラッキングに HSRP を設定し、そのインターフェイスが活性挿抜 (Online Insertion and Removal; OIR) オペレーションに備えて物理的に外されている場合、HSRP はそのインターフェイスを常にダウンしているとみなします。設定をトラッキングする HSRP インターフェイスを削除することはできません。この状況を回避するには、**no standby track interface-type interface-number** コマンドを使用してから物理的にインターフェイスを取り外してください。

group-number に 0 を入力した場合、グループ番号は NVRAM (不揮発性 RAM) に書き込まれず、逆に互換性のある番号が提供されます。

**例** 次に、インターフェイス上でグループ 1 をトラッキングする HSRP をイネーブルにする例を示します。

```
Router(config-if)# standby 1 track Ethernet0/2  
Router(config-if)#
```

次に、指定のルータを取りやめ、HSRP ルータを指定のルータにする例を示します。

```
Router(config-if)# standby 1 track designated-router 15  
Router(config-if)#
```

**関連コマンド** **show standby** (『*Catalyst 6500 Series Switch Cisco IOS Command Reference*』を参照)

# upgrade rom-monitor

ROM Monitor (ROMMON;ROM モニタ) の実行優先順位を設定するには、**upgrade rom-monitor** コマンドを使用します。

```
upgrade rom-monitor {rp | sp} {invalidate | preference} {region1 | region2}
```

```
upgrade rom-monitor {rp | sp} file {device:filename}
```

## シンタックスの説明

<b>rp</b>	ルート プロセッサを指定します。
<b>sp</b>	Catalyst 6500 シリーズ スイッチ プロセッサを指定します。
<b>invalidate</b>	MAGIC および選択されたリージョンの一連のコードを無効にします。
<b>preference</b>	選択されたリージョンに対する ROMMON の実行優先順位を設定します。
<b>region1</b>	リージョン 1 内の ROMMON を選択します。
<b>region2</b>	リージョン 2 内の ROMMON を選択します。
<b>file</b>	フラッシュ ファイル名を指定します。
<i>device:filename</i>	デバイス名およびフラッシュ ファイルのファイル名

## デフォルト

このコマンドにはデフォルト設定がありません。

## コマンド モード

特権 EXEC

## コマンド履歴

リリース	変更内容
12.2(17a)SXA	このコマンドのサポートが MSFC に追加されました。

## 使用上のガイドライン



### 注意

パラメータを指定しないで **upgrade rom-monitor** コマンドを入力すると、処理が中断されることがあります。



### 注意

コンソール接続の代わりに Telnet セッションから **upgrade rom-monitor** コマンドを入力すると、処理が中断されることがあります。

このコマンドを正常に機能させるには、**slot num** は必須です。

**sp** キーワードはサポートされていません。

リージョン 1 またはリージョン 2 の ROMMON 上に、手動で実行優先順位の設定をするには、**upgrade rom-monitor rp {invalidate | preference} {region1 | region2}** コマンドを入力します。このコマンドは特権 EXEC モードからだけ入力できます。

新しい ROMMON をフラッシュ (リージョン 1 またはリージョン 2) のリージョンにプログラムするには、**upgrade rom-monitor rp file {device:filename}** コマンドを入力します。

## ■ upgrade rom-monitor

**例** 次に、新しい ROMMON を ROMMON フラッシュ ファイルにプログラムする例を示します。

```
Router# upgrade rom-monitor rp file bootflash:FUR_173.srec  
ROMMON image upgrade in progress  
Erasing flash  
Programming flash  
Verifying new image  
ROMMON image upgrade complete, MSFC3 must be reloaded.
```

**関連コマンド** [show msfc2 rom-monitor](#)



## 略語

表 A-1 に、このマニュアルで使用されている略語の定義を示します。

表 A-1 略語リスト

略語	説明
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 : アクセスコントロールリスト
ACNS	Application and Content Networking System
AFI	Authority and Format Identifier
Agport	Aggregation port
ALPS	Airline Protocol Support
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
ATA	Analog Telephone Adaptor
ATM	Asynchronous Transfer Mode : 非同期転送モード
AV	Attribute Value
AVF	active virtual forwarder
AVG	active virtual gateway
BDD	Binary Decision Diagram
BECN	Backward Explicit Congestion Notification
BGP	Border Gateway Protocol
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
BSC	Bisync : バイナリ同期
BSTUN	Block Serial Tunnel
BUS	Broadcast and Unknown Server
BVI	Bridge-group Virtual Interface : ブリッジグループ仮想インターフェイス
CAM	Content-Addressable Memory : 連想メモリ
CAR	Committed Access Rate : 専用アクセスレート
CBAC	Context-Based Access Control : コンテキストベースのアクセス制御

表 A-1 略語リスト (続き)

略語	説明
CCA	Circuit Card Assembly
CDP	Cisco Discovery Protocol
CEF	Cisco Express Forwarding
CHAP	Challenge Handshake Authentication Protocol
CIR	Committed Information Rate : 認定情報速度
CIST	Common and Internal Spanning Tree
CLI	Command-Line Interface : コマンドライン インターフェイス
CLNS	Connection-Less Network Service
CMNS	Connection-Mode Network Service : コネクション モード ネットワーク サービス
COPS	Common Open Policy Server
COPS-DS	Common Open Policy Server Differentiated Services
CoS	Class of Service : サービス クラス
CPLD	Complex Programmable Logic Device
CRC	Cyclic Redundancy Check : 巡回冗長検査
CRF	Concentrator Relay Function : コンセントレータ リレー機能
CST	Common Spanning Tree
CUDD	University of Colorado Decision Diagram
DCC	Data Country Code
dCEF	distributed Cisco Express Forwarding
DDR	Dial-on-Demand Routing : ダイアル オンデマンド ルーティング
DE	Discard Eligibility : 廃棄適性
DEC	Digital Equipment Corporation
DFC	Distributed Forwarding Card
DFI	Domain-Specific Part Format Identifier
DFP	Dynamic Feedback Protocol
DISL	Dynamic Inter-Switch Link
DLC	Data Link Control : データ リンク制御
DLSw	Data Link Switching : データ リンク スイッチング
DMP	Data Movement Processor
DNS	Domain Name System : ドメイン ネーム システム
DoD	Department of Defense : 米国国防総省
DoS	Denial of Service : サービス妨害
dot1q	802.1Q
dot1x	802.1X
DRAM	Dynamic RAM
DRiP	Dual Ring Protocol
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DSPU	Downstream SNA Physical Units
DSTS	Destination-Specific Traffic-Shaping
DTP	Dynamic Trunking Protocol

表 A-1 略語リスト (続き)

略語	説明
DTR	Data Terminal Ready : データ端末動作可能
DXI	Data Exchange Interface : データ交換インターフェイス
EAP	Extensible Authentication Protocol
EARL	Enhanced Address Recognition Logic
EEPROM	Electrically Erasable Programmable Read-Only Memory : 電氣的消去再書き込み可能 ROM
EHSA	Enhanced High System Availability
EIA	Electronic Industries Association : 米国電子工業会
ELAN	Emulated Local Area Network : エミュレート LAN
EOBC	Ethernet Out-of-Band Channel
EOF	End of File
EoMPLS	Ethernet over Multiprotocol Label Switching
ESI	End-System Identifier
FAT	File Allocation Table
FECN	Forward Explicit Congestion Notification
FIB	Forwarding Information Base : 転送情報ベース
FM	Feature Manager
FRU	Field-Replaceable Unit
fsck	file system consistency check
FSM	Feasible Successor Metrics
FSU	fast software upgrade
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
GLBP	Gateway Load Balancing Protocol
GMRP	GARP Multicast Registration Protocol
GVRP	GARP VLAN Registration Protocol
HSRP	Hot Standby Router Protocol
ICC	Inter-card Communication または Interface Controller Card
ICD	International Code Designator
ICMP	Internet Control Message Protocol
IDB	Interface Descriptor Block
IDP	Initial Domain Part または Internet Datagram Protocol
IDS	Intrusion Detection System Module
IFS	IOS File System
IGMP	Internet Group Management Protocol
IGRP	Interior Gateway Routing Protocol
ILMI	Integrated Local Management Interface
IP	Internet Protocol
IPC	Interprocessor Communication : プロセッサ間通信
IPX	Internetwork Packet Exchange
IS-IS	Intermediate System-to-Intermediate System Intradomain Routing Protocol

表 A-1 略語リスト ( 続き )

略語	説明
ISL	Inter-Switch Link : スイッチ間リンク
ISL VLAN	Inter-Switch Link VLAN
ISO	International Organization for Standardization : 国際標準化機構
ISR	Integrated SONET Router
LACP	Link Aggregation Control Protocol
LACPDU	Link Aggregation Control Protocol Data Unit
LAN	Local Area Network
LANE	LAN Emulation : LAN エミュレーション
LAPB	Link Access Procedure, Balanced
LCP	Link Control Protocol
LDA	Local Director Acceleration
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
LLC	Logical Link Control : 論理リンク制御
LTL	Local Target Logic
MAC	Media Access Control : メディア アクセス制御
MD5	Message Digest 5
MFD	Multicast Fast Drop
MIB	Management Information Base
MII	Media-Independent Interface : メディア独立型インターフェイス
MLS	Multilayer Switching : マルチレイヤ スイッチング
MLSE	maintenance loop signaling entity
MOP	Maintenance Operation Protocol
MOTD	Message-of-The-Day
MLSE	Maintenance Loop Signaling Entity
MPLS	Multiprotocol Label Switching : マルチプロトコル ラベル スイッチング
MRM	Multicast Routing Monitor
MSDP	Multicast Source Discovery Protocol
MSFC	Multilayer Switching 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 ( 802.1s )
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
NBP	Name Binding Protocol
NCIA	Native Client Interface Architecture
NDE	NetFlow Data Export : NetFlow データ エクスポート
NET	Network Entity Title

表 A-1 略語リスト ( 続き )

略語	説明
NetBIOS	Network Basic Input/Output System
NFFC	NetFlow Feature Card : NetFlow フィーチャカード
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
NVGEN	Nonvolatile Generation
NVRAM	Nonvolatile RAM : 不揮発性 RAM
OAM	Operation, Administration, and Maintenance
ODM	Order Dependent Merge
OSI	Open Systems Interconnection : 開放型システム間相互接続
OSM	Optical Services Module : オプティカル サービス モジュール
OSPF	Open Shortest Path First
PAE	Port Access Entity
PAgP	Port Aggregation Protocol : ポート集約プロトコル
PBD	Packet Buffer Daughterboard
PC	Personal Computer ( 以前は PCMCIA )
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
PGM	Pragmatic General Multicast
PHY	Physical Sublayer : 物理サブレイヤ
PIB	Policy Information Base
PIM	Protocol Independent Multicast
PPP	Point-to-Point Protocol : ポイントツーポイント プロトコル
PRID	Policy Rule Identifiers
PVLAN	Private VLAN
PVST+	Per VLAN Spanning Tree Plus
QDM	QoS Device Manager
QM	QoS Manager
QM-SP	SP QoS Manager
QoS	Quality of Service
Q-in-Q	802.1Q in 802.1Q
RACL	Router Interface Access Control List
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
RF	Redundancy Facility
RGMP	Router-Ports Group Management Protocol

表 A-1 略語リスト (続き)

略語	説明
RIB	Routing Information Base
RIF	Routing Information Field
RMON	Remote Network Monitor
ROM	Read-Only Memory : 読み出し専用メモリ
ROMMON	ROM Monitor : ROM モニタ
RP	Route Processor : ルート プロセッサ、または Rendezvous Point : ランデブー ポイント
RPC	Remote Procedure Call
RPF	Reverse Path Forwarding
RPR	Route Processor Redundancy
RPR+	Route Processor Redundancy+
RSPAN	Remote SPAN
RST	reset
RSTP	Rapid Spanning-Tree Protocol
RSTP+	Rapid Spanning-Tree Protocol Plus
RSVP	ReSerVation Protocol
SAID	Security Association Identifier
SAP	Service Access Point : サービス アクセス ポイント
SCM	Service Connection Manager
SCP	Switch-Module Configuration Protocol
SDLC	Synchronous Data Link Control
SGBP	Stack Group Bidding Protocol
SIMM	Single In-Line Memory Module
SLB	Server Load Balancing
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
SMDS	Software Management and Delivery Systems
SMF	Software MAC Filter
SMP	Standby Monitor Present
SMRP	Simple Multicast Routing Protocol
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
SREC	S-Record 形式 ( Motorola により定義された ROM 内容の形式 )
SSTP	Cisco Shared Spanning Tree
STP	Spanning-Tree Protocol : スパニングツリー プロトコル
SVC	Switched Virtual Circuit : 相手先選択接続
SVI	Switched Virtual Interface
TACACS+	Terminal Access Controller Access Control System Plus
TARP	Target Identifier Address Resolution Protocol

表 A-1 略語リスト (続き)

略語	説明
TCAM	Ternary Content Addressable Memory
TCL	Table Contention Level
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
TIA	Telecommunications Industry Association : 米国電気通信工業会
TopN	ユーザがレポートを使用してポートトラフィックを分析するためのユーティリティ
ToS	Type of Service : タイプオブサービス
TLV	Type-Length-Value
TTL	Time To Live
TVX	valid transmission
UDLD	UniDirectional Link Detection Protocol : 単一方向リンク検出
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 Circuit : 仮想チャネル回線
VCI	Virtual Circuit Identifier
VCR	Virtual Configuration Register : 仮想コンフィギュレーションレジスタ
VINES	Virtual Network System
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
VPN	Virtual Private Network : バーチャルプライベートネットワーク
VRF	VPN Routing and Forwarding
VTP	VLAN Trunk Protocol : VLAN トランク プロトコル
VVID	Voice VLAN ID
WAN	Wide Area Network
WFQ	Weighted Fair Queueing : 均等化キューイング
WRED	Weighted Random Early Detection : 重み付けランダム早期検出
WRR	Weighted Round-Robin : 重み付けラウンドロビン
XNS	Xerox Network System





# オープンソースソフトウェアについて

Catalyst 6500 シリーズ スイッチ ソフトウェアにおける Cisco IOS ソフトウェアの pipe コマンドは、Henry Spencer の正規表現ライブラリ (regex) を使用しています。

regex は、Henry Spencer 作成の正規表現ライブラリです (Copyright 1992, 1993, 1994, 1997 Henry Spencer. All rights reserved. このソフトウェアは、American Telephone and Telegraph Company または Regents of the University of California のライセンスの対象ではありません。

このソフトウェアは、すべての人が任意の目的で、任意のコンピュータシステム上で使用できます。このソフトウェアの変更および再配布については、次の制限が適用されます。

1. 作成者はこのソフトウェアの使用の結果に責任を負いません。これは、その損害の程度にかかわらず、このソフトウェア内の欠陥により発生した場合でも同様です。
2. このソフトウェアの製造元は、故意または過失を問わず、不正確に記載してはいけません。ソースを読むユーザはほとんどいないため、クレジットはマニュアルに記載する必要があります。
3. 変更バージョンはそのとおり明確にマークする必要があり、オリジナルソフトウェアと偽って記載してはいけません。ソースを読むユーザはほとんどいないため、クレジットはマニュアルに記載する必要があります。
4. この通知を削除または改変することはできません。

Catalyst 6500 シリーズ スイッチ上の Cisco IOS ソフトウェアのソフトウェア パイプ コマンドは、Softfloat を使用します。

Softfloat は、John R. Hauser によって作成されました。この製品は、International Computer Science Institute (所在地: Suite 600, 1947 Center Street, Berkeley, California 94704) の協力を得て実現しました。資金の一部は、助成金 MIP-9311980 に基づいて米国科学財団から提供されました。このコードのオリジナルバージョンは、カリフォルニア大学バークレー校との協力により、Nelson Morgan および John Wawrzynek 両教授の指導の下で、固定小数点ベクトル プロセッサを構築するプロジェクトの一環として作成されました。詳細については、次の Web ページを参照してください。  
<http://www.cs.berkeley.edu/~jhauser/arithmic/SoftFloat.html>

本ソフトウェアは、現状のまま、無償で配布されます。それを避けるべく、妥当な努力が払われましたが、このソフトウェアには時として正しくない動作をもたらす欠陥が含まれている可能性があります。このソフトウェアの使用は、ソフトウェアが原因で被るあらゆる損失、代償、またはその他の問題について全責任を取る能力と意思があり、さらに、ソフトウェアが原因で顧客およびクライアントが被ったあらゆる損失、代償、またはその他の問題に対して John Hauser と International Computer Science Institute を (おそらくは同様の法的警告により) 効果的に保護する個人および団体に制限されます。

Softfloat の派生的製品は、商業目的においても受容されます。ただし、(1) 派生製品のソースコードに、その製品が派生物であることを示す注意書きが目につく形で含まれていること、(2) ソースコードに、このコードの中で保持されている該当部分に対して上記の 4 項を含む注意書きが目につく形で含まれていることが条件となります。



## Symbols

- ?
  - 完全なコマンド 1-14
  - 使用可能コマンドのリスト 1-14
- ? command 1-1

## Numerics

- 802.1X
  - dot1x を参照
- 802.3ad
  - LACP を参照

## A

- ACL
  - 選択
    - BDD ベース マージ関数 2-33
    - ODM ベース マージ関数 2-33
  - 統合
    - 現行方式の表示 2-68
- active virtual forwarder
  - AVF を参照
- active virtual gateway
  - AVG を参照
- Address Resolution Protocol
  - ARP を参照

## B

- BDD
  - ACL マージ関数を選択 2-33
- BGP
  - 最大パラレル ルート数の設定 2-32
  - トラフィックの分類の作成 2-61

## Binary Decision Diagram

- BDD を参照
- Border Gateway Protocol
  - BGP を参照
- bridge crb コマンド 2-11
- bridge-group コマンド 2-11

## C

- CEF
  - イネーブル化
    - レート制限 2-37
  - 設定
    - レート制限 2-37
    - ロード バランシング 2-35
  - ディセーブル化
    - レート制限 2-37
- Cisco Express Forwarding
  - CEF を参照
- CLI
  - 1 レベル前に戻る 1-14
  - MSFC CLI
    - アクセス 1-12
    - アクセス レベル 1-13
    - インターフェイス コンフィギュレーション モード (IOS) 1-14
    - グローバル コンフィギュレーション モード 1-14
    - コマンドのリスト表示 1-14
    - コンソール コンフィギュレーション モード 1-14
    - コンフィギュレーション モード 1-13
    - ストリング検索
      - 位置指定 1-9
      - 繰り返し指定 1-8
      - 検索出力 1-6
      - 使用 1-6
      - 選択 1-9

- 単一文字パターン 1-6
- 表現 1-6
- フィルタリング 1-6
- 複数文字パターン 1-7
- リコール機能用カッコ 1-10
- ソフトウェアの基本事項 1-13
- 特権 EXEC モード 1-14
- Command-Line Interface
  - コマンドライン インターフェイス
    - CLI を参照
- D
- Distributed Forwarding Card
  - DFC を参照
- DoS 保護
  - 設定
    - IPv4 マルチキャスト レート リミッタ 2-47
    - IPv6 マルチキャスト レート リミッタ 2-49
  - ディセーブル化
    - IPv4 マルチキャスト レート リミッタ 2-47
    - IPv6 マルチキャスト レート リミッタ 2-49
  - レート リミッタ
    - ACL ブリッジド レート リミッタのディセーブル化 2-51
    - ACL ブリッジド レート リミッタのイネーブル化 2-51
    - ACL ブリッジド レート リミッタの設定 2-51
    - CEF レート リミッタのイネーブル化 2-53
    - CEF レート リミッタの設定 2-53
    - CEF レート リミッタのディセーブル化 2-53
    - イネーブル化 2-46
    - ディセーブル化 2-46
    - ユニキャスト パケットのイネーブル化 2-54
    - ユニキャスト パケットの設定 2-54
    - ユニキャスト パケットのディセーブル化 2-54
- dot1q
  - 802.1Q トンネリングを参照
- dot1x
  - 802.1X を参照
- E
- Enhanced Address Recognition Logic
  - EARL を参照
- Ethernet over Multiprotocol Label Switching
  - EoMPLS を参照
- F
- Fast Software Upgrade
  - FSU を参照
- FDDI
  - raw、IPX、カプセル化 2-29
- Field-Replaceable Unit
  - FRU を参照
- file system consistency check
  - fsck を参照
- FM
  - FM を参照
- G
- Gateway Load Balancing Protocol
  - GLBP を参照
- H
- Hot Standby Router Protocol
  - HSRP を参照
- HSRP
  - 設定
    - 初期化の遅延 2-95
    - トラッキング 2-99
    - 遅延時間情報の表示 2-92
    - 遅延時間のディセーブル化 2-95
- I
- ICMP サブネット マスク 2-10
- Inter-Card Communication
  - ICC を参照
- Intermediate System-to-Intermediate System
  - IS-IS を参照
- Internet Control Message Protocol ( ICMP )
  - ICMP を参照

- Internet Group Management Protocol
  - IGMP を参照
- Internetwork Packet Exchange
  - IPX を参照
- Inter-Switch Link VLAN
  - ISL VLAN を参照
- IOS
  - インターフェイスの復帰 1-16
  - 設定の表示および保存 1-16
- IP
  - アドレス
    - セカンダリ 2-10
    - プライマリ 2-10
  - セカンダリ アドレス、指定 2-10
  - プライマリ アドレス、設定 2-10
- IP WCCP
  - イネーブル化
    - インターフェイス上でのパケット リダイレクション 2-24
  - ディセーブル化
    - インターフェイス上でのパケット リダイレクション 2-24
- IP マルチキャスト ルーティング
  - PIM
    - ネイバー、表示 2-71, 2-73
- IP ルーティング プロトコル
  - 最大パラレル ルート数の設定 2-32
- IPv4
  - 設定
    - マルチキャスト レート リミッタ 2-47
  - ディセーブル化
    - マルチキャスト レート リミッタ 2-47
- IPv6
  - 設定
    - マルチキャスト レート リミッタ 2-49
  - ディセーブル化
    - マルチキャスト レート リミッタ 2-49
- IPX
  - カプセル化 2-28
    - ARPA 2-29
    - Ethernet\_802.2 2-29
    - Ethernet\_802.3 2-29
    - Ethernet\_II 2-29
    - Ethernet\_Snap 2-29
    - FDDI raw 2-29
    - HDLC 2-29
    - Novell-Ether 2-29
    - SAP 2-29
    - SNAP 2-29
  - サブインターフェイス 2-30
    - コンフィギュレーション (例) 2-31
  - セカンダリ ネットワーク 2-28
  - 複数の論理ネットワーク 2-29
  - フレーム化
    - IPX、カプセル化を参照
  - ルーティング
    - イネーブル化 2-28
    - ディセーブル化 2-28
    - 複数ネットワークのイネーブル化(例) 2-31
- L
- LCP
  - バンドル イメージの表示 2-76
- Link Aggregation Control Protocol
  - LACP を参照
- M
- Maintenance Loop Signaling Entity
  - MLSE を参照
- MCP
  - バンドル イメージの表示 2-76
- Message Digest 5
  - MD5 を参照
- Message-of-The-Day
  - MOTD を参照
- MLS
  - ACL マージ関数を選択 2-33
  - MSFC コマンド
    - トラフィックの許可 2-41
  - 表示
    - ACL 統合方式 2-68
  - レート リミッタ
    - ACL ブリッジド レート リミッタのイネーブル化 2-51
    - ACL ブリッジド レート リミッタの設定 2-51
    - CEF レート リミッタのイネーブル化 2-53
    - CEF レート リミッタの設定 2-53
    - イネーブル化 2-54
    - 設定 2-46
    - ユニキャスト パケットの設定 2-54

- ユニキャストおよびマルチキャスト パケット  
のイネーブル化 2-46
- MLS IP
  - インストール
    - ACL しきい値 2-42
  - インターフェイス
    - 内部ルータのイネーブル化 2-34
    - 内部ルータのディセーブル化 2-34
    - 非 RPF マルチキャスト高速廃棄のイネーブル  
化 2-45
  - グローバル
    - 整合性チェッカーのイネーブル化 2-43
    - 整合性チェッカーのディセーブル化 2-43
  - 削除
    - ACL しきい値 2-40
- more コマンド
  - 検索 1-6
  - フィルタ 1-6
- More-- プロンプト
  - 検索 1-6
  - フィルタ 1-6
- MSFC
  - コンフィギュレーション モード 1-15
  - 実行優先順位の設定 2-101
  - スーパーバイザ エンジンからのアクセス
    - Telnet セッション 1-13
    - コンソール ポート 1-12
  - スーパーバイザ エンジンのコンソール コマンド  
1-12
  - セッション コマンド 1-13
  - フラッシュへの新規 ROMMON のプログラミング  
2-101
- MSFC CLI
  - アクセス 1-12
- MSFC コマンド
  - interface range 2-8
  - mls ip inspect 2-41
  - set traffic-index 2-61
  - show microcode 2-76
  - show msfc2 rom-monitor 2-85
  - show scp 2-87
  - upgrade rom-monitor 2-101
- MSFC へのアクセス
  - Telnet セッション 1-13
  - コンソール ポート 1-12
- MTU
  - 最大サイズの設定 2-58
  - 最大パケット サイズの設定 2-58
  - デフォルト値 2-58
  - デフォルト値の復元 2-58
- Multiple Spanning Tree
  - MST を参照
- N
  - NetFlow データ エクスポート
    - NDE を参照
  - Network Entity Title
    - NET を参照
  - NLSP
    - サブインターフェイス 2-30
    - コンフィギュレーション (例) 2-31
- O
  - ODM
    - ACL マージ関数を選択 2-33
  - ODM アルゴリズム
    - ODD を参照
- P
  - Per VLAN Spanning Tree
    - PVST+ を参照
  - PIM
    - 起動型 RPF チェックのディセーブル化 2-15
    - 起動型チェック間隔の設定 2-15
    - 待機時間の設定 2-15
    - チェック間隔の設定 2-16
    - 表示
      - ネイバー情報 2-71, 2-73
  - port-range
    - 実行 2-8
  - Protocol Independent Multicast
    - PIM を参照
- Q
  - Q-in-Q
    - 802.1Q in 802.1Q
    - 802.1Q トンネリングを参照

- QoS Device Manager
  - QDM を参照
  
- R
  
- Rapid Spanning-Tree Protocol
  - RSTP を参照
- Rapid Spanning-Tree Protocol+
  - RSTP+ を参照
- regex
  - 正規表現ライブラリを参照
- Remote Procedure Call
  - RPC を参照
- Remote SPAN
  - RSPAN を参照
- Reverse Path Forwarding
  - RPF を参照
- ROMMON
  - 実行優先順位の設定 2-101
  - ステータスの表示 2-85
  - フラッシュへの新規 ROMMON のプログラミング 2-101
- Route Processor Redundancy
  - RPR を参照
- Route Processor Redundancy+
  - RPR+ を参照
- RPF
  - exists-only チェックのイネーブル化 2-17
  - exists-only チェックのディセーブル化 2-17
  - PIM 待機時間の設定 2-15
  - 起動型チェック間隔の設定 2-15
  - 起動型チェックのディセーブル化 2-15
  - チェック間隔の設定 2-16
- RPR+
  - 冗長モードの設定 2-56
  
- S
  
- SCP
  - 情報の表示 2-87
- Server Load Balancing
  - SLB を参照
- show コマンド
  - 検索 1-6
  - フィルタ 1-6
  
- SLB
  - 帯域内パケット数の表示 2-64
- slot0
  - 情報の表示 2-89
- SNMP
  - 通知
    - イネーブル化 2-93
    - ディセーブル化 2-93
  - トラップ
    - イネーブル化 2-93
    - ディセーブル化 2-93
- Softfloat
  - オープンソースソフトウェアについて B-1
- SP QoS Manager
  - QM-SP を参照
- SSO
  - 冗長モードの設定 2-56
  - 設定
    - ルート コンバージ ディレイ タイム インターバル 2-60
- SSO 付き SRM
  - 設定
    - 冗長モード 2-56
- Switch-Module Configuration Protocol
  - SCP を参照
  
- T
  
- Tab キー
  - 完全なコマンド 1-1
- Table Contention Level
  - TCL を参照
- Telnet、MSFC へのアクセス 1-13
  
- V
  
- Private VLAN
  - PVLAN を参照
- VLAN Access Control List
  - VACL を参照
  
- W
  
- WCCP
  - イネーブル化
    - IP マルチキャスト パケット受信 2-23

- キャッシュ エンジン サービス グループ 2-19
- パケットリダイレクション 2-26
- ディセーブル化
  - IP マルチキャストパケット受信 2-23
  - サービス グループのサポートの制御 2-19
  - パケットリダイレクション 2-26
- 表示
  - 帯域内パケット数 2-64
- あ
- アクセス コントロール リスト
  - ACL を参照
- アドレス
  - セカンダリ IP 2-10
  - プライマリ IP 2-10
- い
- イネーブル モード 1-15
- インターフェイス
  - アドレス、セカンダリ 2-10
- インターフェイス コンフィギュレーション モード
  - アクセス 1-14
  - 説明 1-14
  - プロンプト 1-14
- インターフェイス レンジ マクロ
  - 作成 2-5
- う
- ウォッチ リスト
  - IP アドレスの追加 2-13
  - イネーブル化 2-13
  - エントリのクリア 2-2
  - 設定 2-13
    - 最大ログイン試行回数 2-12
  - ディセーブル化 2-13
  - 表示 2-70
- お
- オープン ソース ソフトウェアについて
  - Softfloat B-1
- 正規表現ライブラリ B-1
- 重み付けラウンドロビン
  - WRR を参照
- 重み付けランダム早期検出
  - WRED を参照
- か
- 拡張ネットワーク
  - セカンダリ アドレス、IP、使用 2-11
- カプセル化
  - IPX 2-28
- 関連資料 viii
- き
- 起動レジスタ 2-3
- 機能マネージャ
  - 表示
    - CBAC が設定された ACL リストおよびポート 2-65
    - VLAN 単位の情報 2-69
    - 一般情報 2-62
    - インターフェイス単位の情報 2-66
    - 概要 2-68
    - 帯域内パケット数 2-64
    - ダイナミック再帰エントリ 2-68
- 疑問符コマンド 1-1
- く
- グローバル コンフィギュレーション モード
  - アクセス 1-14
  - 説明 1-14
  - プロンプト 1-14
- こ
- コマンドの default 形式、使用 1-5
- コマンドの no 形式、使用 1-5
- コマンドの実行
  - 複数のインターフェイスを同時に 2-8
- コマンドの省略 1-14
- コンテキスト ヘルプ 1-1

- コマンドライン インターフェイス
  - CLI を参照
- コマンド、リスト表示 1-14
- コンソール コンフィギュレーション モード 1-14
  - アクセス 1-14
  - 説明 1-14
  - プロンプト 1-14
- コンソール ポート
  - MSFC へのアクセス 1-12
- コンフィギュレーション モード 1-13
  
- さ
- 最大伝送ユニット
  - MTU を参照
- サブインターフェイス
  - IPX 2-30
  - NLSP 2-30
    - コンフィギュレーション (例) 2-31
- サブネット マスク、ICMP 使用 2-10
  
- し
- ジャンボ フレーム
  - MTU サイズの設定 2-58
  - 最大パケット サイズの設定 2-58
  - デフォルト値 2-58
  - デフォルト値の復元 2-58
- 冗長性
  - 表示
    - 設定情報 2-86
    - モードの設定 2-56
  
- す
- スーパバイザ エンジンのイメージ
  - バンドル イメージの表示 2-76
- スタブ
  - 非 RPF マルチキャスト高速廃棄のイネーブル化 2-45
  
- せ
- 正規表現ライブラリ
  - オープン ソース ソフトウェアについて B-1
- 整合性チェッカー
  - イネーブル化 2-43
  - 設定 2-43
  - ディセーブル化 2-43
- セカンダリ アドレス、IP、使用 2-10
- セカンダリ ネットワーク、IPX 2-28
- セッション コマンド、MSFC 1-13
- 設定変更の保存 1-11
- 設定、保存 1-11
  
- そ
- ソフトウェア コンフィギュレーションの起動レジスタ 2-3
  
- た
- 対象読者 vii
- 単一文字パターン
  - 特殊文字
    - 単一文字パターン、表 1-6
  
- つ
- 通知、イネーブル化 2-93
  
- と
- 特殊文字
  - 位置指定、表 1-9
- 特権 EXEC モード
  - アクセス 1-14
  - 説明 1-14
  - プロンプト 1-14
- トラッキング
  - 設定
    - 指定ルータ 2-99
- トラップ、イネーブル化 2-93
  
- に
- 認証プロキシ
  - ウォッチ リスト
    - IP アドレスの追加 2-13
    - イネーブル化 2-13

エントリのクリア 2-2  
 最大ログイン試行回数の設定 2-12  
 設定 2-13  
 デイセーブル化 2-13  
 表示 2-70  
 認定情報速度  
 CIR を参照

## は

ハードウェア スイッチング  
 整合性チェッカーのイネーブル化 2-43  
 整合性チェッカーのデイセーブル化 2-43  
 設定  
 整合性チェッカー 2-43  
 表示  
 (\*,G/m) エントリに基づいた情報 2-78  
 (\*,G) ショートカット 2-78  
 Bidir 情報 2-78  
 Bidir (\*,G/m) ショートカットに基づいた情報 2-78  
 IP サブネットのプレフィクスに基づいた情報 2-78  
 RPF VLAN ID に基づいた情報 2-78  
 (S,G) ショートカットに基づいた情報 2-78  
 グループ アドレスに基づいた情報 2-78  
 コンパクト フォーマットの CEF テーブル情報 2-78  
 送信元の IP に基づいた情報 2-78  
 ハードウェア レイヤ 3 スイッチング  
 表示  
 IP エントリ情報 2-77  
 パラレル ルータ 2-11  
 バンドル イメージ  
 表示 2-76

## ひ

非 RPF マルチキャスト高速廃棄  
 イネーブル化 2-45  
 表  
 位置指定に用いられる特殊文字 1-9  
 特別な意味を持つ文字 1-6  
 表 : show ip pim neighbor のフィールドの説明 2-73  
 表 : デフォルトの MTU 値 2-58

表 : 特殊文字  
 繰り返し指定 1-8  
 表現  
 選択パターンの指定 1-9  
 単一文字パターン 1-6  
 パターンの繰り返し 1-10  
 複数表現の繰り返しに一致 1-8  
 複数文字パターン 1-7

## ふ

ブート  
 システム ソフトウェア、コンフィギュレーション レジスタ 2-3  
 ブート フィールド  
 デフォルト値、変更 2-3  
 複数のインターフェイスでコマンドを実行 2-8  
 複数パスユニキャスト RPF チェック  
 RPF モード  
 インターフェイス グループ 2-39  
 通過 2-39  
 パント 2-39  
 インターフェイス グループ  
 削除 2-38  
 作成 2-38  
 定義 2-38  
 削除  
 インターフェイス グループ 2-38  
 作成  
 インターフェイス グループ 2-38  
 設定  
 モード 2-39  
 複数文字パターン 1-7  
 プライマリ アドレス  
 IP、設定 2-10  
 ブリッジ プロトコル データ ユニット  
 BPDU を参照  
 フレーム化  
 IPX  
 IPX、カプセル化を参照  
 プロセッサ間通信  
 IPC を参照

- へ
- ページング プロンプト  
--More-- プロンプトを参照
- ま
- マクロ  
インターフェイス レンジ マクロの作成 2-5
- マニュアルの構成 vii
- マニュアルの表記法 ix
- マルチプロトコル ラベル スイッチング  
MPLS を参照
- マルチレイヤ スイッチ フィーチャ カード  
MSFC を参照
- マルチレイヤ スイッチング  
MLS を参照
- み
- 3 つ一組のコンテンツ アドレス可能メモリ  
TCAM を参照
- め
- メディア アクセス制御  
MAC アドレス テーブルを参照
- ゆ
- ユーザ EXEC モード  
アクセス 1-14  
説明 1-14  
プロンプト 1-14
- り
- 略語、リスト A-1
- れ
- レート リミッタ  
ACL ブリッジド レート リミッタのディセーブル化  
2-51
- レイヤ 3 マネージャ  
情報の表示 2-74
- レート リミッタ  
ACL ブリッジド レート リミッタのイネーブル化  
2-51  
ACL ブリッジド レート リミッタの設定 2-51  
CEF レート リミッタの設定 2-53  
設定  
IPv4 マルチキャスト レート リミッタ 2-47  
IPv6 マルチキャスト レート リミッタ 2-49
- ディセーブル化  
CEF レート リミッタ 2-53  
IPv4 マルチキャスト レート リミッタ 2-47  
IPv6 マルチキャスト レート リミッタ 2-49
- ユニキャスト パケットのイネーブル化 2-54  
ユニキャスト パケットの設定 2-46, 2-54  
ユニキャスト パケットのディセーブル化 2-54  
ユニキャストおよびマルチキャスト パケットのイ  
ネーブル化 2-46  
ユニキャストおよびマルチキャスト パケットの  
ディセーブル化 2-46
- ろ
- ロード バランシング  
選択  
Catalyst 6500 シリーズ スイッチのロード バラ  
ンシング アルゴリズム 2-35  
Cisco IOS のロード バランシング アルゴリズム  
2-35