Cisco Nexus 9000 シリーズ NX-OS トラブルシューティング ガイド、リリース 10.1（x）

初版：2021 年 2 月 16 日

最終更新：2022 年 3 月 31 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【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/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、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。

目 次

はじめに：

はじめに xi

対象読者 xi

表記法 xi

Cisco Nexus 9000 シリーズ スイッチの関連資料 xii

マニュアルに関するフィードバック xii

通信、サービス、およびその他の情報 xiii

第 1 章

新機能および変更された機能に関する情報 1

新機能および変更された機能に関する情報 1

第 2 章

概要 3

ソフトウェア イメージ 3

サポートされるプラットフォーム 3

トラブルシューティング プロセスについて 3

ポートの確認 4

レイヤ 2 接続の確認 5

レイヤ 3 接続の確認 5

Symptoms 6

システムメッセージ 6

Syslog サーバの実装 7

ログによるトラブルシューティング 8

モジュールのトラブルシューティング 9

NVRAM ログの表示 9

カスタマー サポートへの問い合わせ 10

第 3 章 インストール、アップグレード、リブートのトラブルシューティング 11
アップグレードとリブートについて 11
アップグレードとリブートのチェックリスト 11
ソフトウェア アップグレードの確認 12
ソフトウェアのアップグレードとダウングレードのトラブルシューティング 13
ソフトウェア アップグレードがエラーで終了する 13
Cisco NX-OS ソフトウェアのアップグレード 14
ソフトウェア システムのリブートのトラブルシューティング 15
電源投入またはスイッチのリブートがハングする 15
破損したブートフラッシュの回復 15
ローダーからの回復 > プロンプト 17
システムまたはプロセスの再起動 20
システムの再起動の回復 20
回復不能なシステムの再起動 25
スタンバイ スーパーバイザが起動に失敗する 26
管理者パスワードの回復 27
ネットワーク管理者権限でのCLIの使用による管理者パスワードの回復 27
管理者パスワードを回復するためのデバイスの電源再投入 28
管理者パスワードを回復するためのデバイスのリロード 32
管理者パスワードの変更 34
管理者パスワードの変更に関するガイドラインと制限事項 34

第 4 章 ライセンスの問題のトラブルシューティング 37
ライセンスの問題のトラブルシューティングに関する情報 37
ライセンスの注意事項および制約事項 37
ライセンスのトラブルシューティングの初期チェックリスト 38
CLI を使用したライセンス情報の表示 39
ライセンスのインストールの問題 40
シリアル番号の問題 40
システム間の RMA シャーシ エラーまたはライセンス転送 40

欠落しているとリストされたライセンス 41

第 5 章 ポートのトラブルシューティング 43

ポートのトラブルシューティングについて 43

ポートのトラブルシューティングの注意事項と制約事項 43

ポートのトラブルシューティングの初期チェックリスト 44

ポート情報の表示 44

CLI からのポート統計情報のトラブルシューティング 45

ポート インターフェイスの問題のトラブルシューティング 46

インターフェイス設定が消えました 46

インターフェイスを有効にできない 46

専用ポートを設定できない 47

ポートがリンク障害または接続されていない状態のままになっている 48

予期しないリンク フラッピングが発生する 49

ポートが ErrDisable 状態にある 50

CLI を使用した ErrDisable 状態の確認 51

第 6 章 vPC のトラブルシューティング 53

vPC のトラブルシューティングに関する詳細 53

vPC の初期トラブルシューティングのチェックリスト 53

CLI を使用した vPC の確認 54

受信したタイプ 1 設定要素の不一致 56

vPC 機能を有効にできない 56

ブロッキング状態の vPC 57

中断状態に移行した vPC 上の VLAN 57

HSRP ゲートウェイを持つホストが VLAN を超えてアクセスできない 57

第 7 章 VLAN のトラブルシューティング 59

VXLAN の問題のトラブルシューティング 59

マルチキャスト カプセル化パスでドロップされたパケット 60

マルチキャスト カプセル化解除パスでドロップされたパケット 61

ユニキャスト カプセル化パスでドロップされたパケット 63
単一のネクスト ホップで VTEP に到達でいる場合にドロップユニキャスト パケット 63
VTEP が ECMP パスを介して到達可能な場合にドロップされるユニキャスト パケット 65
ユニキャスト カプセル化解除パスでドロップされたパケット 67
Broadcom シェル テーブルについて 69
MPLS エントリ テーブル 69
MAC アドレス ラーニング 70
入力 DVP テーブル 70
入力レイヤ 3 ネクスト ホップ 71
VLAN 変換テーブル 71
EGR ポートから NHI へのマッピング 72
VLAN フラッド インデックス テーブル 72
GPORTと前面パネルのポート番号マッピングの取得 73
入力ポートのためにどのインターフェイス トラフィックが使用されるかを特定する 74
VLAN のフラッド リストの検索 74
カプセル化ポートがフラッド リストの一部であるかどうかの判別 74

第 8 章 STP のトラブルシューティング 75
STP のトラブルシューティング 75
STP の初期トラブルシューティングのチェックリスト 75
STP データ ループのトラブルシューティング 76
過剰なパケット フラッディングのトラブルシューティング 79
コンバージェンス時間の問題のトラブルシューティング 80
フォワーディング ループに対するネットワークの保護 81

第 9 章 ルーティングのトラブルシューティング 85
ルーティングの問題のトラブルシューティングについて 85
トラブルシューティング ルートの初期チェックリスト 85
ルーティングのトラブルシューティング 86
ポリシーベース ルーティングのトラブルシューティング 89

第 10 章 メモリのトラブルシューティング 91
メモリのトラブルシューティングに関する詳細情報 91
プラットフォーム メモリ使用率の一般/高レベルの評価 92
ユーザ プロセス 93
大量のメモリを使用しているプロセスの特定 93
組み込みプラットフォームのメモリモニタリング 93
メモリしきい値 94

第 11 章 パケット フローの問題のトラブルシューティング 95
パケットフローの問題 95
レート制限によってドロップされたパケット 95
CoPP のためにドロップされたパケット 95

第 12 章 PowerOn 自動プロビジョニングのトラブルシューティング 97
POAP が完了するはずの時間内にスイッチが起動しない 97
POAP が失敗する 97

第 13 章 Python API のトラブルシューティング 101
Python API エラーの受信 101

第 14 章 NX-API のトラブルシューティング 105
NX-API のガイドライン 105
NX-API が応答しない 105
設定が失敗します 106
Bash に対する許可が拒否される 106
ブラウザ サンドボックスから出力を取得できない 106
CLI コマンド エラーが表示される 107
エラーメッセージが表示される 107
一時ファイルが消える 107
コマンド出力のチャンクが配信されない 107

第 15 章 サーバ障害のトラブルシューティング 109
プロセスのメモリ割り当ての特定 109
プロセスの CPU 使用率の特定 110
モニタリング プロセスのコア ファイル 111
クラッシュ コア ファイルの処理 111
コアのクリア 112
コア ファイルの自動コピーのイネーブル化 112

第 16 章 テクニカル サポートへ問い合わせる前の準備 113
TAC に連絡する前に実行する手順 113
Cisco NX-OS から/へのファイルのコピー 115
コア ダンプの使用 117

第 17 章 トラブルシューティングのツールと方法論 119
コマンドライン インターフェイスのトラブルシューティング コマンド 119
整合性チェッカー コマンド 120
マルチキャスト整合性チェッカー 137
マルチキャスト整合性チェッカ コマンドの出力例 140
輻輳検出および回避 141
ACL 整合性チェッカ 142
設定ファイル 144
CLI デバッグ 144
デバッグ フィルタ 145
Pingおよび Traceroute 146
ping の使用 146
トレースルートの使用 147
プロセスおよび CPU のモニタリング 148
show processes cpu コマンドの使用 149
show system resources コマンドの使用 150
オンボード障害ロギングの使用 151

OBFL エラー ステータス コマンドの使用 151
診断の使用 152
組み込まれている Event Manager の使用 153
Ethanalyzer の使用 153
SNMP および RMON のサポート 171
PCAP SNMP パーサーの使用 171
RADIUS を利用 173
syslog の使用 174
ログ レベル 174
Telnet または SSH へのロギングのイネーブル化 175
SPAN の使用 175
Using sFlow 176
sFlow 整合性チェッカー 176
ブルー ビーコン機能の使用 177
watch コマンドの使用 177
トラブルシューティングのツールと方法論の追加参照 178

はじめに

この前書きは、次の項で構成されています。

- 対象読者 （xi ページ）
- 表記法 （xi ページ）
- Cisco Nexus 9000 シリーズ スイッチの関連資料 （xii ページ）
- マニュアルに関するフィードバック （xii ページ）
- 通信、サービス、およびその他の情報 （xiii ページ）

対象読者

このマニュアルは、Cisco Nexus スイッチの設置、設定、および維持に携わるネットワーク管理者を対象としています。

表記法

コマンドの説明には、次のような表記法が使用されます。

表記法	説明
bold	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
italic	イタリック体の文字は、ユーザが値を指定する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角かっこで囲んで示しています。
[x | y]	いずれか1つを選択できる省略可能なキーワードや引数は、角かっこで囲み、縦棒で区切って示しています。
{x | y}	必ずいずれか1つを選択しなければならない必須キーワードや引数は、波かっこで囲み、縦棒で区切って示しています。

表記法	説明
[x {y | z}]	角かっこまたは波かっこが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角かっこ内の波かっこと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
`variable`	ユーザが値を入力する変数であることを表します。イタリック体が使用できない場合に使用されます。
string	引用符を付けない一組の文字。string の前後には引用符を使用しないでください。引用符を使用すると、その引用符も含めて string と見なされます。

例では、次の表記法を使用しています。

表記法	説明
`screen フォント`	スイッチが表示する端末セッションおよび情報は、スクリーン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。
<>	パスワードのように出力されない文字は、山カッコ（<>）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。

Cisco Nexus 9000 シリーズ スイッチの関連資料

Cisco Nexus 9000 シリーズ スイッチ全体のマニュアル セットは、次の URL にあります。

http://www.cisco.com/en/US/products/ps13386/tsd_products_support_series_home.html

マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、HTML ドキュメント内のフィードバック フォームよりご連絡ください。ご協力をよろしくお願いいたします。

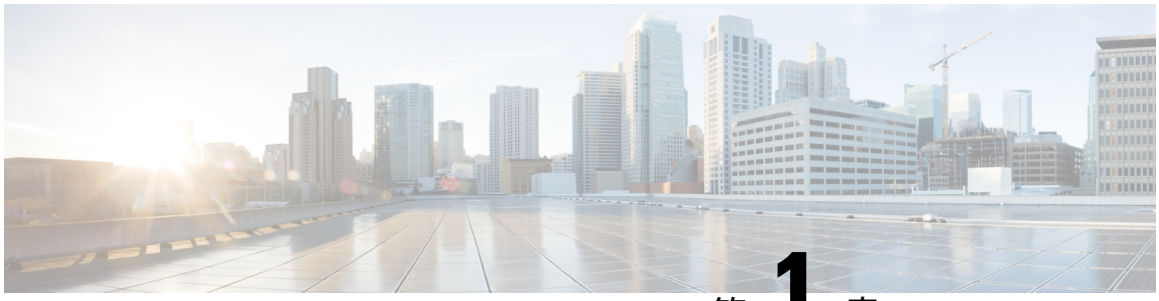
通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、 Cisco Profile Manager でサインアップしてください。
- 重要なテクノロジーによりビジネスに必要な影響を与えるには、シスコサービスにアクセスしてください。
- サービスリクエストを送信するには、 シスコ サポートにアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、 Cisco Marketplace にアクセスしてください。。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、 Cisco Pressにアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、 Cisco Warranty Finder にアクセスしてください。

Cisco バグ検索ツール

Cisco バグ検索ツール （BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。

通信、サービス、およびその他の情報



第 1 章

新機能および変更された機能に関する情報

この章では、「*Cisco Nexus 9000* シリーズ *NX-OS* トラブルシューティング ガイド、リリース *10.1*（*x*）」に記載されている新機能および変更された機能に関するリリース固有の情報について説明します。

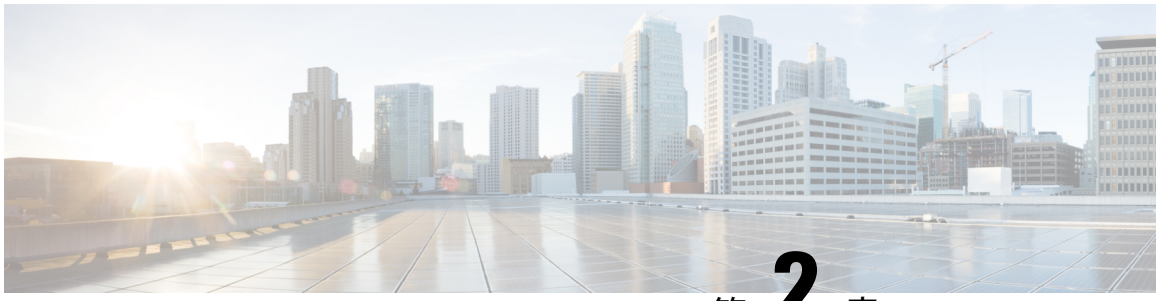
- 新機能および変更された機能に関する情報 （1 ページ）

新機能および変更された機能に関する情報

表 *1*：リリース *10.1*（*x*）の新機能および変更された機能

特長	説明	変更が行われたリリース	参照先
Ethanalyzer バックグラウンド キャプチャ プロセスおよびインバンドパケットの自動収集	Ethanalyzer バックグラウンド キャプチャ プロセスおよびインバンドパケットの自動収集の追加のサポート	10.1(2)	Ethanalyzer の使用 （153 ページ）
マルチキャスト整合性チェッカー	IPv6 L2、IPv6L3、マルチキャスト NLB と マルチキャスト GRE 整合性チェッカーの追加サポート。	10.1(1)	マルチキャスト整合性チェッカー （137 ページ）

新機能および変更された機能に関する情報



第 2 章

概要

- ソフトウェア イメージ （3 ページ）
- サポートされるプラットフォーム （3 ページ）
- トラブルシューティング プロセスについて （3 ページ）
- Symptoms （6 ページ）
- ログによるトラブルシューティング （8 ページ）
- モジュールのトラブルシューティング （9 ページ）
- NVRAM ログの表示 （9 ページ）
- カスタマー サポートへの問い合わせ （10 ページ）

ソフトウェア イメージ

Cisco NX-OS ソフトウェアは、1 つの NXOS ソフトウェア イメージで構成されています。このイメージは、すべての Cisco Nexus 3400 シリーズ スイッチで実行されます。

サポートされるプラットフォーム

Cisco NX-OS リリース 7.0(3)I7(1) 以降、「Nexus スイッチ プラットフォーム サポート マトリクス」を使用して、選択した機能をサポートするさまざまな Cisco Nexus 9000 および 3000 スイッチのリリース元である Cisco NX-OS を知ることができます。

トラブルシューティング プロセスについて

ネットワークに関するトラブルシューティングの一般的な手順は、次のとおりです。

- すべてのデバイスで、Cisco NX-OS リリースの一貫性を保持します。
- Cisco NX-OS リリースの Cisco NX-OS リリース ノートを参照して、最新の機能、制限事項、および注意事項を確認します。
- システム メッセージ ロギングをイネーブルにします。

- 変更を実装したら、新しい設定変更のトラブルシューティングを実施します。
- 特定の現象に関する情報を収集します。
- デバイスとエンド デバイス間の物理接続を確認します。
- レイヤ 2 接続を確認します。
- エンドツーエンドの接続とルーティング設定を確認します。
- トラブルシューティングを行っても問題を解決できなかった場合は、Cisco TAC またはテクニカル サポート担当者にお問い合わせください。

ここでは、ネットワークにおける問題のトラブルシューティングで一般的に使用されるツールについて説明します。

（注） 問題領域を絞り込むためには、ネットワークの正確なトポロジを把握している必要もあります。この情報については、ネットワーク アーキテクトにお問い合わせください。デバイスの一般情報を収集するには、次のコマンドを使用します。

- **show module**
- **show version**
- **show running-config**
- **show logging log**
- **show interfaces brief**
- **show vlan**
- **show spanning-tree**
- **show {ip | ipv6} route**
- **show processes | include ER**
- **show accounting log**

ポートの確認

次の質問に答えて、ポートが正しく接続され、動作していることを確認します。

- 正しいメディア（銅線、光、ファイバ タイプ）を使用していることを確認します。
- メディアが故障または破損していないことを確認します。
- モジュールのポート LED はグリーンですか。
- なぜインターフェイスは動作していないのでしょうか。

ポートのトラブルシューティングのヒントについては、「ポートのトラブルシューティング」を参照してください。

レイヤ 2 接続の確認

レイヤ 2 接続を確認するには、次の質問に回答します。

- **show vlan all-ports** コマンドを使用し、 必要なすべてのインターフェイスが同じ VLAN にあることを確認します。VLANのステータスがアクティブになっている必要があります。
- **show port-channel compatibility-parameters** コマンドを使用し、 コマンドを使用して、速度、デュプレックス、トランクの各モードについて、ポートチャネル内のすべてのポートの設定が同じであることを確認します。
- **show running-config spanning-tree** コマンドを使用し、 コマンドを使用して、スパニングツリープロトコル（STP）がネットワーク内のすべてのデバイスで同じように設定されていることを確認します。
- **show processes | include ER** を使用します。 必須ではないレイヤ 2 プロセスがエラー状態であることを確認します。
- **show mac address-table dynamic vlan** コマンドを使用し、 コマンドを使用して、学習またはエージングが各ノードで発生しているかどうかを判断します。

レイヤ 3 接続の確認

レイヤ 3 接続を確認するには、次の点をチェックします。

- デフォルト ゲートウェイを設定したか。
- ルーティング ドメイン全体で同じダイナミック ルーティング プロトコル パラメータを設定したか、またはスタティック ルートを設定したか。
- IP アクセス リスト、フィルタ、ルート マップによって、ルート アップデートがブロックされていないことを確認します。

ルーティング設定を確認するには、次のコマンドを使用します。

- **show ip arp**
- **show** {**ip** | **ipv6**}
- **show ipv6 neighbor**

Symptoms

このドキュメントでは、ネットワークで観察された症状と各章に記載されている症状を比較することで、Cisco NX-OS の問題を診断して解決できる症状ベースのトラブルシューティングアプローチを使用します。

資料の症状を自分のネットワークで観察した症状と比較することにより、最小限のネットワークの中断で問題を解決するには、ソフトウェアの設定の問題や操作不可能なハードウェア コンポーネントを診断して修正できることが重要です。次に、問題と対処方法を示します。

- 主要な Cisco NX-OS トラブルシューティング ツールを特定します。
- CLI で SPAN または Ethanalyzer を使用し、プロトコル トレースを取得して分析します。
- 物理ポートの問題を識別または除外します。
- スイッチ モジュールの問題を識別または除外します。
- レイヤ 2 の問題を診断および修正します。
- レイヤ 3 の問題を診断および修正します。
- スイッチをアップグレードの障害から復旧します。
- Cisco TAC またはカスタマー サポート担当者が使用するコア ダンプおよびその他の診断データを取得します。

システムメッセージ

システム メッセージは、システム ソフトウェアからコンソール（および任意で別のシステムのロギング サーバ）に送信されます。すべてのメッセージがデバイスの問題を示しているわけではありません。一部のメッセージは単に情報を示すだけですが、リンク、内蔵ハードウェア、またはデバイス ソフトウェアに関する問題の診断に役立つメッセージもあります。

システム メッセージ テキストは、状況を説明する文字列です。メッセージのこの部分には、イベントについての詳細な情報が含まれている場合があります。含まれる情報は、端末ポート番号、ネットワーク アドレス、またはシステム メモリのアドレス空間内での位置に対応するアドレスです。この可変フィールドの情報はメッセージごとに異なるので、ここでは角カッコ（[ ]）で囲んだ短い文字列で示します。たとえば 10 進数は [dec] などで表します。

PORT-3-IF_UNSUPPORTED_TRANSCEIVER：インターフェイス [chars] のトランシーバはサポートされていません。

各システム メッセージのあとには、説明と推奨処置が記載されています。アクションは「アクションは必要ありません（No action is required）」のような簡単なものであることもあります。次の例のように、修正方法に関するものやテクニカル サポートへの連絡を推奨するものもあります。

Error Message PORT-3-IF_UNSUPPORTED_TRANSCEIVER：インターフェイス [chars] のトランシーバはサポートされていません。

Explanation トランシーバ（SFP）が認定ベンダーのものではありません。

Recommended Action を入力します。**show interface transceiver** 使用されているトランシーバを判別する CLI コマンドまたは同様の DCNM コマンド。認定トランシーバ ベンダーのリストについては、カスタマー サポート担当者にお問い合わせください。

Syslog サーバの実装

Syslog ファシリティを使用して、デバイスからメッセージ ログのコピーをホストに送信すると、ログ用により多くの永続的ストレージを確保できます。この機能は、長期間にわたってログを調べたり、デバイスにアクセスできない場合に使用できます。

次に、Solaris プラットフォーム上で Syslog ファシリティを使用するようにデバイスを設定する例を示します。ここでは Solaris ホストを使用しますが、すべての UNIX および Linux システムにおける Syslog の設定は非常によく似ています。

Syslog では、ファシリティを使用して、Syslog サーバ上でのメッセージの処理方法とメッセージの重大度が決定されます。Syslog サーバでは、異なるメッセージの重大度を異なる方法で処理できます。たとえば、メッセージを別々のファイルに記録することや、特定のユーザに電子メールで送信することもできます。syslog サーバでの重大度レベルを指定すると、syslog サーバで設定できるため、そのレベル以上の重大度（より低い数値）のすべてのメッセージに対して処置が行われます。

（注） syslog サーバを設定する必要があります。Cisco NX-OS メッセージは、他社の Syslog メッセージと競合しないように、標準Syslogファイルとは別のファイルに記録される必要があります。/file システムでログ ファイルを見つけないでください。ログ メッセージで/ファイル システムがいっぱいになるのは望ましくありません。この例では、次の値を使用します。

- syslog client: switch1
- syslog server: 172.22.36.211
- (Solaris) syslog facility: local1
- syslog severity: notifications (level 5, the default)
- Cisco NX-OS メッセージを記録するログ ファイル：/var/adm/nxos_logs

Cisco NX-OS で syslog 機能を設定するには、これらの手順に従います。

1. switch# **config terminal**
2. switch(config)# **logging server 192.0.2.1 6 facility local1**

show logging server コマンドを使用し、 コマンドを使用して、syslog 設定を確認します。

```
switch1# show logging server
Logging server:                 enabled
{172.22.36.211}
        server severity:        notifications
        server facility:        local1
        server VRF:             management
```

Syslog サーバを設定するには、次の手順に従います。

1. local1 のメッセージを処理するように、/etc/syslog.conf を変更します。Solaris の場合は、facility.severity と処置（/var/adm/nxos_logs）の間に少なくとも 1 つのタブが必要です。

   ```
   local1.notice /var/adm/nxos_logs
   ```

2. ログ ファイルを作成します。

   ```
   touch /var/adm/nxos_logs
   ```

3. syslog プロセスを再起動します。

   ```
   /etc/init.d/syslog stop
   /etc/init.d/syslog start

   syslog service starting.
   ```

4. syslog プロセスが開始されたことを確認します。

   ```
   ps -ef |grep syslogd
   ```

Cisco NX-OS でイベントを作成して、Syslog サーバをテストします。この場合、ポート e1/2 はシャットダウンおよび再度有効化され、Syslog サーバ上で次のように表示されます。デバイスの IP アドレスは角カッコで囲まれています。

```
tail -f /var/adm/MDS_logs
Sep 17 11:07:41 [172.22.36.142.2.2] : 2013 Sep 17 11:17:29 pacific:
PORT-5-IF_DOWN_INITIALIZING: %$VLAN 1%$ Interface e 1/2 is down (Initializing)

Sep 17 11:07:49 [172.22.36.142.2.2] : 2013 Sep 17 11:17:36 pacific: %PORT-5-IF_UP: %$VLAN
 1%$ Interface e 1/2 is up in mode access

Sep 17 11:07:51 [172.22.36.142.2.2] : 2013 Sep 17 11:17:39 pacific:
%VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from pts/0 (dhcp-171-71-49-125.cisco.com
```

ログによるトラブルシューティング

Cisco NX-OS では、デバイス上でさまざまなタイプのシステム メッセージを生成して、Syslog サーバに送信します。これらのメッセージを確認することにより、現在発生している問題の原因となった可能性のあるイベントを判別できます。

Cisco NX-OS のログにアクセスして表示するには、次のコマンドを使用します。

```
switch# show logging ?
console       Show console logging configuration
info          Show logging configuration
```

```
ip            IP configuration
last          Show last few lines of logfile
level         Show facility logging configuration
logfile       Show contents of logfile
loopback      Show logging loopback configuration
module        Show module logging configuration
monitor       Show monitor logging configuration
nvram         Show NVRAM log
onboard       show logging onboard
server        Show server logging configuration
source-interface  Show logging source-interface configuration
timestamp     Show logging timestamp configuration
```

次は、**show logging server** の出力例を示しています。 コマンドに対して表示されます。

```
switch# show logging server
Logging server:                 enabled
{172.28.254.254}
        server severity:        notifications
        server facility:        local7
        server VRF:             management
```

モジュールのトラブルシューティング

ユーザはモジュールのコンソール ポートに直接接続して、モジュールの起動時の問題をトラブルシューティングすることができます。**attach console module** コマンドを使用し、 して、モジュールのコンソール ポートに接続します。

ブートフラッシュのスペースの問題が原因で、Cisco Nexus End-of-Rack（EoR）スイッチが起動に失敗することがあります。このような場合は、コンソールの bash シェルから空き領域を確認し、不要なファイルを削除して、ブートフラッシュに十分な空きディスク領域を確保します。これにより、EoR スイッチのスムーズな起動が保証されます。

NVRAM ログの表示

プライオリティ0、1、または2のシステムメッセージは、スーパーバイザモジュールのNVRAMに記録されます。スイッチの再起動後、**show logging nvram** を使用して、NVRAM にこれらの syslog メッセージを表示できます。 コマンドに対して表示されます。

```
switch# show logging nvram
2013 Sep 10 15:51:58 switch %$ VDC-1 %$ %SYSMGR-2-NON_VOLATILE_DB_FULL: System n
on-volatile storage usage is unexpectedly high at 99%.
2013 Sep 10 15:52:13 switch %$ VDC-1 %$ %PLATFORM-2-PFM_SYSTEM_RESET: Manual sys
tem restart from Command Line Interface
2013 Sep 10 15:57:49 switch %$ VDC-1 %$ %KERN-2-SYSTEM_MSG: Starting kernel... -
 kernel
2013 Sep 10 15:58:00 switch %$ VDC-1 %$ %CARDCLIENT-2-REG: Sent
2013 Sep 10 15:58:01 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: R2D2: P1 SUP NO GMTL
 FOR P1 SUP  - r2d2
2013 Sep 10 15:58:01 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: R2D2: P1 SUP NO GMTL
 FOR P1 SUP  - r2d2
2013 Sep 10 15:58:05 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: R2D2: P1 SUP: Reset
Tx/Rx during QOS INIT  - r2d2
```

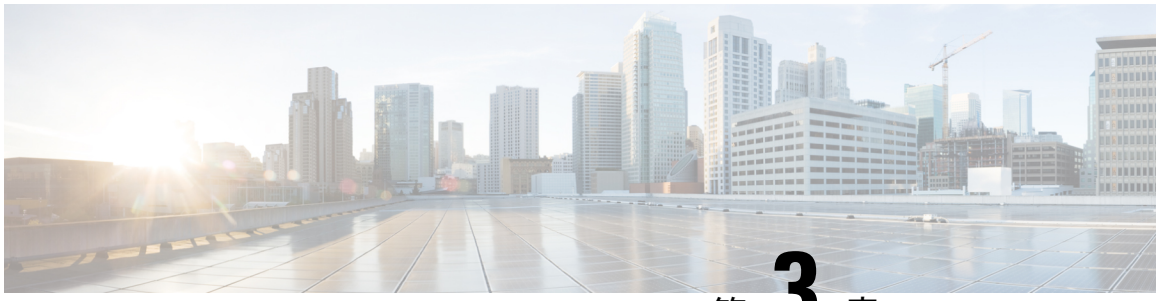
```
2013 Sep 10 15:58:16 switch %$ VDC-1 %$ %USER-2-SYSTEM_MSG: can't dlsym ssnmgr_i
s_session_command: please link this binary with ssnmgr.so! - svi
2013 Sep 10 15:58:16 switch %$ VDC-1 %$ %CARDCLIENT-2-SSE: LC_READY sent
2013 Sep 10 15:58:17 switch %$ VDC-1 %$ snmpd: load_mib_module :Error, while loa
ding the mib module /isan/lib/libpmsnmp_common.so (/isan/lib/libpmsnmp_common.so
: undefined symbol: sme_mib_get_if_info)
2013 Sep 10 15:58:17 switch %$ VDC-1 %$ %CARDCLIENT-2-SSE: MOD:6 SUP ONLINE
```

カスタマー サポートへの問い合わせ

このマニュアルのトラブルシューティング情報を使用しても問題を解決できない場合には、カスタマーサービス担当者に連絡して、支援および詳細な指示を受けてください。担当者ができる限りすばやいサポートを行えるように、連絡する前に次の情報を用意してください。

- 装置の納品日
- シャーシのシリアル番号（シャーシの背面パネルの右側にあるラベルに記載されています）
- ソフトウェアの種類とリリース番号
- メンテナンス契約書または保証情報
- 問題の概要
- 問題を切り分けし解決するために、すでに実行している手順の要約

テクニカル サポートへ問い合わせる前に実施する手順の詳細については、TAC に連絡する前に実行する手順 （113 ページ）を参照してください。



第 3 章

インストール、アップグレード、リブートのトラブルシューティング

- アップグレードとリブートについて （11 ページ）
- アップグレードとリブートのチェックリスト （11 ページ）
- ソフトウェア アップグレードの確認 （12 ページ）
- ソフトウェアのアップグレードとダウングレードのトラブルシューティング （13 ページ）
- ソフトウェア システムのリブートのトラブルシューティング （15 ページ）
- 管理者パスワードの変更 （34 ページ）

アップグレードとリブートについて

アップグレードとリブートは、継続的なネットワーク メンテナンス アクティビティです。実稼働環境でこれらの操作を実行するときは、ネットワークを中断するリスクを最小限に抑え、何か問題が発生したときに迅速に回復する方法を理解する必要があります。

（注） このマニュアルでは、Cisco NX-OS のアップグレードとダウングレードの両方を指すアップグレードという用語を使用します。

アップグレードとリブートのチェックリスト

次のチェックリストを使用して、アップグレードまたはリブートの準備をします。

チェックリスト	Done
アップグレードまたはダウングレードするリリースのリリース ノートを参照してください。	
FTP または TFTP サーバがソフトウェア イメージをダウンロードできることを確認します。	

チェックリスト	Done
bootflash: または slot0: のスーパーバイザ モジュールに新しいイメージをコピーします。	
show install all impact コマンドを使用して、新しいイメージが正常であること、および新しいロードが互換性に関してハードウェアに与える影響を確認します。互換性を確認します。	
startup-config ファイルを NVRAM のスナップショット コンフィギュレーションにコピーします。この手順では、スタートアップ コンフィギュレーション ファイルのバックアップ コピーを作成します。	
Running Configuration を Startup Configuration に保存します。	
設定のコピーをリモート TFTP サーバにバックアップします。	
ネットワークの適切なメンテナンス期間中にアップグレードをスケジュールします。	

チェックリストを完了すると、ネットワーク内のシステムをアップグレードまたはリブートする準備が整います。

（注） アップグレード中にアクティブ スーパーバイザがスタンバイ スーパーバイザになるのは正常な動作です。

（注） 重大度が Critical 以下（レベル 0、1、2）の最大 100 個のログ メッセージが NVRAM に保存されます。このログは、**show logging nvram** コマンドを入力することでいつでも表示できます。

ソフトウェア アップグレードの確認

show install all status コマンドを使用すれば コマンドを使用してソフトウェア アップグレードの進行状況を確認したり、進行中の **install all** コマンドまたは最後にインストールされた **install all** コマンド（コンソール、SSH、または Telnet セッションから）のログをを表示したりします。このコマンドは、コンソール端末に接続していない場合でも、アクティブ スーパーバイザ モジュールとスタンバイ スーパーバイザ モジュールの両方の **install all** 出力を表示します。

ソフトウェアのアップグレードとダウングレードのトラブルシューティング

ソフトウェア アップグレードがエラーで終了する

問題	考えられる原因	ソリューション
アップグレードがエラーで終了する	スタンバイ状態のスーパーバイザ モジュールの bootflash: ファイル システムに、更新されたイメージを入れるだけのスペースがない。	**delete** コマンドを使用し、して、不要なファイルを削除します。
	この項で説明している **install all** コマンドが、スタンバイ状態のスーパーバイザ モジュールで入力された。	コマンドは、アクティブ状態のスーパーバイザ モジュールでのみ入力してください。
	アップグレードの進行中にモジュールが挿入された。	インストールを再開します。
	アップグレードの進行中にシステムの電源が切断された。	インストールを再開します。
	誤ったソフトウェアイメージ パスが指定された。	リモート ロケーションへのパス全体を正確に指定します。
	別のアップグレードがすでに進行中。	すべての段階でシステムの状態を確認し、10 秒後にアップグレードを再開します。10 秒以内にアップグレードを再開すると、コマンドは拒否されます。アップグレードが現在進行中であることを示すエラー メッセージが表示されます。
	モジュールのアップグレードに失敗した。	アップグレードを再起動するか、**install module** コマンドを使用して、失敗したモジュールをアップグレードします。

Cisco NX-OS ソフトウェアのアップグレード

どのシステムでも、CLI で自動ソフトウェア アップグレードを実行できます。

始める前に

アクティブ スーパーバイザのコンソール、Telnet、またはSSHポートを介してスイッチにログインします。

必要に応じて、既存のコンフィギュレーション ファイルのバックアップを作成します。

手順の概要

1. **install all** [**nxos bootflash:***filename*]
2. **show module**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**install all** [**nxos bootflash:***filename*]	アップグレードを実行します。 （注） **install all** コマンドの使用時に設定がすべてのガイドラインを満たしている場合は、すべてのモジュール（スーパーバイザおよびスイッチング）がアップグレードされます。 （注） ファイル名を指定しないで **install all** コマンドを入力した場合は、コマンドにより互換性チェックが実行され、アップグレードされるモジュールが通知されます。さらに、インストールを続行するかどうかの確認が求められます。続行を選択すると、スイッチで現在実行されている NXOS ソフトウェア イメージがインストールされ、必要に応じて、実行中のイメージのさまざまなモジュールのBIOSがアップグレードされます。
ステップ 2	**show module**	システムコンソールを終了し、新しいターミナル セッションを開いて、アップグレードされたスーパーバイザ モジュールを表示します。

ソフトウェア システムのリブートのトラブルシューティング

電源投入またはスイッチのリブートがハングする

問題	考えられる原因	ソリューション
デュアル スーパーバイザ構成で電源投入またはスイッチのリブートがハングする	ブートフラッシュが破損しています。	破損したブートフラッシュの回復 （15 ページ）を参照してください。
	BIOS が破損しています。	このモジュールを交換してください。障害のあるモジュールを返品するために、シスコのカスタマー サポート担当者に連絡してください。
	nx-os イメージが破損しています。	必要に応じてスイッチの電源を再投入し、スイッチに「Loading Boot Loader」メッセージが表示されたら **Ctrl-C** を押して、>ローダ プロンプトでブートプロセスを中断します。
	ブート パラメータが正しくありません。	ブート パラメータを確認して修正し、リブートします。

破損したブートフラッシュの回復

すべてのデバイス設定は、内部ブートフラッシュにあります。内部ファイル システムが壊れると、設定が失われるおそれがあります。設定ファイルは定期的に保存し、バックアップしてください。通常のシステムブートは、次の順序で実行されます。

1. 基本入出力システム（BIOS）がローダをロードします。
2. ローダは nx-os イメージを RAM にロードし、イメージを起動します。
3. nx-os イメージは、スタートアップ設定ファイルを読み取ります。

システムの nx-os イメージが破損しており、続行できない（エラー状態）場合は、次の項で説明する BIOS 設定ユーティリティを入力して、システム ブートシーケンスを中断し、イメージを復旧できます。破損した内部ディスクを復旧する必要がある場合にのみ、このユーティリティにアクセスしてください。

注意 この項で説明する BIOS の変更は、破損したブートフラッシュを復旧する場合にのみ必要なものです。

復旧手順では、通常のシーケンスを中断する必要があります。内部シーケンスは、システムの電源をオンにしてから、システムプロンプトが端末に表示されるまでの3つのフェーズ（BIOS、ブートローダ、および nx-os イメージ）を通過します。次の表に、リカバリ中断プロセスの手順を示します。

表 *2:* リカバリの中断

フェーズ	通常のプロンプト（各フェーズの終了時に表示されます）	リカバリ プロンプト（システムが次のフェーズに進まない場合に表示されます）	説明
BIOS	loader>	ブート可能なデバイスがありません	BIOSは、電源投入時自己診断テスト、メモリ テスト、およびその他のオペレーティングシステムアプリケーションを開始します。テストの進行中に、**Ctrl-C**を押して BIOS設定ユーティリティを起動し、**netboot**オプションを使用します。
ブートローダ	nx-os の開始	loader>	ブートローダは、ロードされたソフトウェアを展開し、そのファイル名を参照として使用してイメージをブートします。イメージはブートフラッシュを介して使用可能になります。メモリテストが終了したら、**Esc** を押してブートローダプロンプトを開始します。

フェーズ	通常のプロンプト（各フェーズの終了時に表示されます）	リカバリ プロンプト（システムが次のフェーズに進まない場合に表示されます）	説明
nx-os イメージ	システムの圧縮解除	switch(boot)#	ブートローダフェーズが終了したら、**Ctrl-]**（Ctrl キーと右ブラケット キー）を押して、switch（boot）# プロンプトを入力します。Telnet クライアントによっては、これらのキーが予約されている場合があり、キーストロークの再マッピングが必要となることがあります。Telnet クライアントが提供するマニュアルを参照してください。破損によってコンソールがこのプロンプトで停止した場合は、nx-os イメージをコピーしてシステムをリブートします。 nx-os イメージは、最後に保存された実行設定の設定ファイルをロードし、スイッチのログインプロンプトを返します。

ローダーからの回復 > プロンプト

help コマンドを使用し、 コマンドを使用して、ローダー > プロンプトでこのプロンプトで使用可能なコマンドのリストを表示するか、そのリスト内の特定のコマンドに関する詳細情報を取得します。

始める前に

この手順では、 **init system** コマンドを使用して、デバイスのファイル システムを再フォーマットします。この手順を開始する前に、コンフィギュレーション ファイルのバックアップを作成してください。

ローダー > プロンプトは、通常の switch # または switch(boot)# プロンプトとは異なります。CLI コマンド補完機能は loader >プロンプトでは機能せず、望ましくないエラーが発生する可能性があります。コマンドを表示するには、コマンドを正確に入力する必要があります。

ローダー > プロンプトから TFTP 経由でブートする場合は、リモート サーバ上のイメージへのフル パスを指定する必要があります。

手順の概要

1. loader> **set ip** *ip-address*
2. loader> **set gw** *gw-address*

3. ローダー **cmdline recoverymode=1**
4. loader> **boot tftp:** *tftp-path*
5. switch(boot)# **init system**
6. switch(boot)# **reload-nxos**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	loader> **set ip** *ip-address* 例： `loader> set ip 172.21.55.213 255.255.255.224`	システムのローカル IP アドレスおよびサブネット マスクを指定します。
ステップ 2	loader> **set gw** *gw-address* 例： `loader> set gw 172.21.55.193`	デフォルト ゲートウェイの IP アドレスを指定します。
ステップ 3	ローダー **cmdline recoverymode=1** 例： `loader> cmdline recoverymode=1`	switch(boot)# プロンプトで、ブート プロセスが停止するように設定します。
ステップ 4	loader> **boot tftp:** *tftp-path* 例： `loader> boot tftp://172.28.255.18/tftpboot/n9000-dk9.6.1.2.I1.1.bin`	必要なサーバから nx-os iイメージ ファイルを起動します。 switch(boot)# プロンプトは、使用可能な nx-os イメージがあることを示します。
ステップ 5	switch(boot)# **init system** 例： `switch(boot)# init system`	nx-os システムを開始します。 **注意** このコマンドを入力する前に、コンフィギュレーション ファイルのバックアップが作成されていることを確認してください。
ステップ 6	switch(boot)# **reload-nxos** 例： `switch(boot)# reload-nxos`	nx-os イメージ ファイルのアップロードを完了します。

例

システムのローカル IP アドレスとサブネット マスクを設定する例を示します。

```
loader> set ip 172.21.55.213 255.255.255.224
set ip 172.21.55.213 255.255.255.224
Correct - ip addr is 172.21.55.213, mask is 255.255.255.224
Found Intel 82546GB [2:9.0] at 0xe040, ROM address 0xf980
Probing...[Intel 82546GB]
```

```
Management interface
Link UP in 1000/full mode
Ethernet addr: 00:1B:54:C1:28:60
Address: 172.21.55.213
Netmask: 255.255.255.224
Server: 0.0.0.0
Gateway: 172.21.55.193
```

次に、デフォルト ゲートウェイの IP アドレスを設定する例を示します。

```
loader> set gw 172.21.55.193
Correct gateway addr 172.21.55.193
Address: 172.21.55.213
Netmask: 255.255.255.224
Server: 0.0.0.0
Gateway: 172.21.55.193
```

次に、サーバから nx-os イメージを起動する例を示します。

```
loader> boot tftp://172.28.255.18/tftpboot/n9000-dk9.6.1.2.I1.1.bin
 Address: 172.21.55.213
 Netmask: 255.255.255.224
 Server: 172.28.255.18
 Gateway: 172.21.55.193
  Filesystem type is tftp, using whole disk
 Booting: /tftpboot/n9000-dk9.6.1.2.I1.1.gbin console=ttyS0,9600n8nn quiet loader
 _ver="3.17.0"....
 ..............................................................................Im
 age verification OK

 Starting kernel...
 INIT: version 2.85 booting
 Checking all filesystems..r.r.r.. done.
 Setting kernel variables: sysctlnet.ipv4.ip_forward = 0
 net.ipv4.ip_default_ttl = 64
 net.ipv4.ip_no_pmtu_disc = 1
 .
 Setting the System Clock using the Hardware Clock as reference...System Clock set. Local
 time: Wed Oct  1
 11:20:11 PST 2013
 WARNING: image sync is going to be disabled after a loader netboot
 Loading system software
 No system image Unexporting directories for NFS kernel daemon...done.
 INIT: Sending processes the KILL signal
 Cisco Nexus Operating System (NX-OS) Software
 TAC support: http://www.cisco.com/tac
 Copyright (c) 2013, Cisco Systems, Inc. All rights reserved.
 The copyrights to certain works contained in this software are
 owned by other third parties and used and distributed under
 license. Certain components of this software are licensed under
 the GNU General Public License (GPL) version 2.0 or the GNU
 Lesser General Public License (LGPL) Version 2.1. A copy of each
 such license is available at
 http://www.opensource.org/licenses/gpl-2.0.php and
 http://www.opensource.org/licenses/lgpl-2.1.php
 switch(boot)#
```

システムまたはプロセスの再起動

回復可能または回復不可能なエラーが発生すると、システムまたはシステム上のプロセスがリセットされることがあります。次の表に、考えられる原因と解決策を示します。

問題	考えられる原因	ソリューション
システムまたはシステム上のプロセスがリセットされた。	システムまたはシステムのプロセスで回復可能なエラーが発生しました。	システムは自動的に問題から回復しました。システムの再起動の回復（20 ページ）を参照してください。
	システムで回復不能なエラーが発生した。	システムは問題から自動的に回復できません。原因を特定するには、システムの再起動の回復 （20 ページ）を参照してください。
	クロックモジュールに障害が発生した。	クロックモジュールに障害が発生していることを確認します。障害が発生したクロック モジュールを次のメンテナンス時間帯に交換します。

システムの再起動の回復

プロセスを再起動するたびに、syslog メッセージと Call Home イベントが生成されます。イベントがサービスに影響を与えない場合でも、今後発生することでサービスの中断が発生する可能性があるため、すぐに状態を特定して解決する必要があります。

（注） 手順を実行した後、テクニカル サポート担当者に連絡し、コア ダンプの確認を依頼することで、再起動状態の原因と解決策を特定します。

始める前に

次の条件が適用されます。

- システムは、4 分ごとにコア ファイルを TFTP サーバに自動的にコピーします。この間隔は設定できません。
- TFTP サーバへの特定のコア ファイルのコピーは、**copy core**:*//module#/pid# tftp://tftp_ip_address/file_name* を使用して手動でトリガできます。 コマンドを使用する必要があります。
- スーパーバイザ フェールオーバーが発生した場合、コアはプライマリ ログフラッシュではなくセカンダリ ログフラッシュにある可能性があります。
- プロセスを再起動できる最大回数は、すべてのプロセスの高可用性（HA）ポリシーの一部です。（このパラメータは設定できません。）プロセスが最大回数を超えて再起動すると、古いコア ファイルが上書きされます。

- 任意のプロセスで保存できるコアファイルの最大数は、任意のプロセスのHAポリシーの一部です。（このパラメータは設定できず、3 に設定されます）。

手順の概要

1. switch# **show log | include error**
2. switch# **show processes**
3. switch# **show process log**
4. switch# **show process log pid** *pid*
5. switch# **show system uptime**
6. switch# **show cores**
7. switch# **copy core:** *core path*
8. switch# **show processes log pid** *pid*
9. switch# **system cores tftp:** *tftp-path*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **show log	include error** 例： `switch# show log logfile	include error` `Sep 10 23:31:31 dot-6 %` `LOG_SYSMGR-3-SERVICE_TERMINATED: Service "sensor"` `(PID 704) has finished with error` `code SYSMGR_EXITCODE_SY.` `switch# show logging logfile	include fail` `Jan 27 04:08:42 88 %LOG_DAEMON-3-SYSTEM_MSG:` `bind() fd 4, family 2, port 123, ad` `dr 0.0.0.0, in_classd=0 flags=1 fails: Address` `already in use` `Jan 27 04:08:42 88 %LOG_DAEMON-3-SYSTEM_MSG:` `bind() fd 4, family 2, port 123, ad` `dr 127.0.0.1, in_classd=0 flags=0 fails: Address` `already in use` `Jan 27 04:08:42 88 %LOG_DAEMON-3-SYSTEM_MSG:` `bind() fd 4, family 2, port 123, ad` `dr 127.1.1.1, in_classd=0 flags=1 fails: Address` `already in use` `Jan 27 04:08:42 88 %LOG_DAEMON-3-SYSTEM_MSG:` `bind() fd 4, family 2, port 123, ad` `dr 172.22.93.88, in_classd=0 flags=1 fails:` `Address already in use` `Jan 27 23:18:59 88 % LOG_PORT-5-IF_DOWN: Interface` `fc1/13 is down (Link failure` `or not-connected)` `Jan 27 23:18:59 88 % LOG_PORT-5-IF_DOWN: Interface` `fc1/14 is down (Link failure` `or not-connected)` `Jan 28 00:55:12 88 % LOG_PORT-5-IF_DOWN: Interface` `fc1/1 is down (Link failure` `or not-connected)` `Jan 28 00:58:06 88 % LOG_ZONE-2-ZS_MERGE_FAILED:` `Zone merge failure, Isolating` `port fc1/1 (VSAN 100)` `Jan 28 00:58:44 88 % LOG_ZONE-2-ZS_MERGE_FAILED:`	syslog ファイルを表示して、再起動したプロセスと再起動した理由を確認できるようにします。

	コマンドまたはアクション	目的
	Zone merge failure, Isolating port fc1/1 (VSAN 100) Jan 28 03:26:38 88 % LOG_ZONE-2-ZS_MERGE_FAILED: Zone merge failure, Isolating port fc1/1 (VSAN 100) Jan 29 19:01:34 88 % LOG_PORT-5-IF_DOWN: Interface fc1/1 is down (Link failure or not-connected) switch#	
ステップ 2	switch# **show processes** **例**： switch# show processes PID State PC Start_cnt TTY Process ----- ----- -------- ----------- ---- ---------- 1 S 2ab8e33e 1 - init 2 S 0 1 - keventd 3 S 0 1 - ksoftirqd_CPU0 4 S 0 1 - kswapd 5 S 0 1 - bdflush 6 S 0 1 - kupdated 71 S 0 1 - kjournald 136 S 0 1 - kjournald 140 S 0 1 - kjournald 431 S 2abe333e 1 - httpd 443 S 2abfd33e 1 - xinetd 446 S 2ac1e33e 1 - sysmgr 452 S 2abe91a2 1 - httpd 453 S 2abe91a2 1 - httpd 456 S 2ac73419 1 S0 vsh 469 S 2abe91a2 1 - httpd 470 S 2abe91a2 1 - httpd	実行中のプロセスと各プロセスのステータスを表示します。 次のコードは、状態（プロセス状態）のシステム出力で使用されます。 • D = 中断なしで休止（通常 I/O） • R = 実行可能（実行キュー上） • S = 休止中 • T = トレースまたは停止 • Z = defunct (「ゾンビ」) プロセス • NR = 実行されていない • ER = 実行されているべきだが、現在は実行されていない （注） ER は通常、何度も再起動され、システムによって障害が検出されて無効にされた場合に、プロセスが開始する状態です。
ステップ 3	switch# **show process log** **例**： switch# show process log Process PID Normal-exit Stack-trace Core Log-create-time ------- --- ----------- ----------- ---- --------------- ntp 919 N N N Jan 27 04:08 snsm 972 N Y N Jan 24 20:50	異常終了したプロセスと、スタックトレースまたはコア ダンプがあるかどうかを表示します。
ステップ 4	switch# **show process log pid** *pid* **例**：	再起動している特定のプロセスの詳細情報を表示します。

	コマンドまたはアクション	目的
	switch# show processes log pid 898 Service: idehsd Description: ide hotswap handler Daemon Started at Mon Sep 16 14:56:04 2013 (390923 us) Stopped at Thu Sep 19 14:18:42 2013 (639239 us) Uptime: 2 days 23 hours 22 minutes 22 seconds Start type: SRV_OPTION_RESTART_STATELESS (23) Death reason: SYSMGR_DEATH_REASON_FAILURE_SIGTERM (3) Exit code: signal 15 (no core) CWD: /var/sysmgr/work Virtual Memory: CODE 08048000 - 0804D660 DATA 0804E660 - 0804E824 BRK 0804E9A0 - 08050000 STACK 7FFFFD10 Register Set: EBX 00000003 ECX 0804E994 EDX 00000008 ESI 00000005 EDI 7FFFFC9C EBP 7FFFFCAC EAX 00000008 XDS 0000002B XES 0000002B EAX 00000003 (orig) EIP 2ABF5EF4 XCS 00000023 EFL 00000246 ESP 7FFFFC5C XSS 0000002B Stack: 128 bytes. ESP 7FFFFC5C, TOP 7FFFFD10 0x7FFFFC5C: 0804F990 0804C416 00000003 0804E994 ..... 0x7FFFFC6C: 00000008 0804BF95 2AC451E0 2AAC24A4 .....Q.*.$.* 0x7FFFFC7C: 7FFFFD14 2AC2C581 0804E6BC 7FFFFCA8 .....*..... 0x7FFFFC8C: 7FFFFC94 00000003 00000001 00000003 ..... 0x7FFFFC9C: 00000001 00000000 00000068 00000000 .....h..... 0x7FFFFCAC: 7FFFFCE8 2AB4F819 00000001 7FFFFD14 .....*..... 0x7FFFFCBC: 7FFFFD1C 0804C470 00000000 7FFFFCE8 ....p..... 0x7FFFFCCC: 2AB4F7E9 2AAC1F00 00000001 08048A2C ...*...*....,... PID: 898 SAP: 0 UUID: 0 switch#	
ステップ 5	switch# **show system uptime** 例： switch# show system uptime Start Time: Fri Sep 13 12:38:39 2013 Up Time: 0 days, 1 hours, 16 minutes, 22 seconds	再起動が最近発生したかどうかを表示します。 再起動が繰り返し発生するのか、1 回だけ発生するのかを判断するには、システムが稼働している時間の長さを各再起動のタイムスタンプと比較します。
ステップ 6	switch# **show cores** 例：	アクティブ スーパーバイザから現在アップロードに使用可能なすべてのコアを表示します。

	コマンドまたはアクション	目的
	switch# show cores Module Instance Process-name PID Date(Year-Month-Day Time) ------ -------- ------------ ---- ------------------------- 28 1 bgp-64551 5179 2013-09-13 23:51:26	
ステップ 7	switch# **copy core:** *core path* 例： switch# copy core://5/1524 tftp::/1.1.1.1/abcd	FSPF コア ダンプを IP アドレスを使用して TFTP サーバにコピーします。
ステップ 8	switch# **show processes log pid** *pid* 例： switch# '''show processes log pid 1473''' ========== Service: ips Description: IPS Manager Started at Tue Jan 8 17:07:42 2013 (757583 us) Stopped at Thu Jan 10 06:16:45 2013 (83451 us) Uptime: 1 days 13 hours 9 minutes 9 seconds Start type: SRV_OPTION_RESTART_STATELESS (23) Death reason: SYSMGR_DEATH_REASON_FAILURE_SIGNAL (2) Exit code: signal 6 (core dumped) CWD: /var/sysmgr/work Virtual Memory: CODE 08048000 - 080FB060 DATA 080FC060 - 080FCBA8 BRK 081795C0 - 081EC000 STACK 7FFFFCF0 TOTAL 20952 KB Register Set: EBX 000005C1 ECX 00000006 EDX 2AD721E0 ESI 2AD701A8 EDI 08109308 EBP 7FFFF2EC EAX 00000000 XDS 0000002B XES 0000002B EAX 00000025 (orig) EIP 2AC8CC71 XCS 00000023 EFL 00000207 ESP 7FFFF2C0 XSS 0000002B	ログ ディレクトリに zone_server_log.889 という名前のファイルを表示します。

	コマンドまたはアクション	目的
	Stack: 2608 bytes. ESP 7FFFF2C0, TOP 7FFFFCF0 0x7FFFF2C0: 2AC8C944 000005C1 00000006 2AC735E2 D..*.....5.* 0x7FFFF2D0: 2AC8C92C 2AD721E0 2AAB76F0 00000000 ,..*.!.*.v.*.... 0x7FFFF2E0: 7FFFF320 2AC8C920 2AC513F8 7FFFF42C ... ..*...*,... 0x7FFFF2F0: 2AC8E0BB 00000006 7FFFF320 00000000 ...*.... ..... 0x7FFFF300: 2AC8DFF8 2AD721E0 08109308 2AC65AFC ...*.!.*.....Z.* 0x7FFFF310: 00000393 2AC6A49C 2AC621CC 2AC513F8 .....*.!.*...* 0x7FFFF320: 00000020 00000000 00000000 00000000 ..... 0x7FFFF330: 00000000 00000000 00000000 00000000 ..... 0x7FFFF340: 00000000 00000000 00000000 00000000 ..... 0x7FFFF350: 00000000 00000000 00000000 00000000 ..... 0x7FFFF360: 00000000 00000000 00000000 00000000 ..... 0x7FFFF370: 00000000 00000000 00000000 00000000 ..... 0x7FFFF380: 00000000 00000000 00000000 00000000 ..... 0x7FFFF390: 00000000 00000000 00000000 00000000 ..... 0x7FFFF3A0: 00000002 7FFFF3F4 2AAB752D 2AC5154C . ... output abbreviated ... Stack: 128 bytes. ESP 7FFFF830, TOP 7FFFFCD0	
ステップ 9	switch# **system cores tftp:** *tftp-path* **例**： `switch(config)# system cores tftp://10.1.1.1/cores`	TFTP サーバを使用してコア ダンプを TFTP サーバに送信するように設定します。 このコマンドにより、システムは TFTP サーバへのコア ファイルの自動コピーを有効にします。

回復不能なシステムの再起動

以下の場合には、回復不能なシステム再起動が発生する可能性があります。

- 重要なプロセスが失敗し、再起動できない。
- プロセスがシステム設定で許可されている回数を超えて再起動した。
- プロセスは、システム設定で許可されているよりも頻繁に再起動した。

プロセス リセットの影響は、プロセスごとに設定されたポリシーによって決まります。回復不能なリセットにより、機能が失われたり、アクティブなスーパーバイザが再起動したり、スーパーバイザがスイッチオーバーしたり、システムが再起動したりすることがあります。

この項で説明している **show system reset-reason** コマンドにより、以下の情報が表示されます。

- 特定のスロット、特定のモジュールでの、最後の4つのリセット理由。モジュールが存在しない場合には、そのモジュールのリセット理由コードは表示されません。
- 予期されたリロードおよび予期しないリロードが発生したタイミングと理由の全体での履歴。
- リセットまたはリロードが発生したときのタイム スタンプ。
- モジュールのリセットまたはリロードの理由。
- リセットまたはリロードの原因となったサービス（常に使用できるわけではない）。
- リセットまたはリロード時に実行されていたソフトウェアのバージョン。

```
switch# show system reset-reason module 27
----- reset reason for Supervisor-module 27 (from Supervisor in slot 27) ---
1) At 281000 usecs after Wed Jun 26 20:16:34 2013
    Reason: Reset Requested by CLI command reload
    Service:
    Version: 6.1(2)I1(1)
2) At 791071 usecs after Wed Jun 26 20:04:50 2013
    Reason: Reset Requested by CLI command reload
    Service:
    Version: 6.1(2)I1(1)
3) At 70980 usecs after Wed Jun 26 19:55:52 2013
    Reason: Reset Requested by CLI command reload
    Service:
    Version: 6.1(2)I1(1)
4) At 891463 usecs after Wed Jun 26 23:44:48 2013
    Reason: Reset Requested by CLI command reload
    Service:
    Version: 6.1(2)I1(1)
```

スタンバイ スーパーバイザが起動に失敗する

スタンバイ スーパーバイザは、アップグレード後に起動しません。次のシステム メッセージが表示されることがあります。

```
SYSMGR-2-STANDBY_BOOT_FAILED
```

このメッセージは、ローダがBIOSによってロードされた後3～6分でスタンバイ スーパーバイザがブート手順を完了できない（ローカル コンソールのログイン プロンプトに到達できない）場合に出力されます。このメッセージは、通常、スタンバイ スーパーバイザに適切に設定されていないブート変数によって発生します。このメッセージは、ローダ プロンプトでユーザが意図的に（Esc キーを押して）起動手順を中止した場合も発生する可能性があります。

スタンバイ スーパーバイザのローカル コンソールに接続します。スーパーバイザがローダ プロンプトにいる場合は、 **boot** コマンドを使用して、ブート手順を続行します。それ以外の場合は、**reload** コマンドをアクティブ スーパーバイザの VSH セッションからスタンバイ スーパーバイザに対して入力します。その際に **force-dnld** オプションを指定します。スタンバイがオンラインになったら、ブート変数を適切に設定して問題を解決します。

症状	考えられる原因	ソリューション
スタンバイ スーパーバイザが起動しません。	TFTPからブートされたアクティブ スーパーバイザ nx-os イメージ。	bootflash: からアクティブ スーパーバイザをリロードします。

管理者パスワードの回復

次のいずれかの方法で、ネットワーク管理者パスワードを回復できます。

- network admin 権限を持つユーザ名で CLI から回復する
- デバイスの電源を再投入する
- デバイスをリロードする

ネットワーク管理者権限でのCLIの使用による管理者パスワードの回復

手順の概要

1. switch# **show user-account**
2. switch# **config terminal**
3. switch(config)# **username admin password** *new-password*
4. switch(config)# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	switch# **show user-account**
	例：
	`switch# show user-account`
	`user:admin`
	`this user account has no expiry date`
	`roles:network-admin`
	`user:dbgusr`
	`this user account has no expiry date`
	`roles:network-admin network-operator`
		ユーザ名に network admin 権限があるかどうかを確認します。

ステップ 2	switch# **config terminal**
	例：
	`switch# config terminal`
	`switch(config)#`
		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。

ステップ 3	switch(config)# **username admin password** *new-password* 例：	ユーザ名に network admin 権限がある場合は、新しいネットワーク管理者パスワードを割り当てます。

	コマンドまたはアクション	目的
	`switch(config)# username admin password egBdf`	（注） new-passwordでは、$文字は使用できません。
ステップ 4	switch(config)# **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

管理者パスワードを回復するためのデバイスの電源再投入

network-admin 権限のあるデバイス上でセッションを開始できない場合は、デバイスの電源を再投入してネットワーク管理者パスワードを回復することができます。

注意 パスワード回復手順を実行すると、デバイス上のすべてのトラフィックが中断されます。デバイスとの接続はすべて 2 ～ 3 分間切断されます。

（注） 管理インターフェイスとの Telnet またはセキュア シェル（SSH）セッションから管理者パスワードを回復することはできません。ローカル コンソール接続を使用できる必要があります。

（注） パスワードの回復によって更新されるのは、ローカル ユーザ データベース内の新しい管理者パスワードのみです。リモート AAA サーバのパスワードは更新されません。新しいパスワードは、ローカル認証がイネーブルの場合にのみ有効になり、リモート認証の場合は有効になりません。パスワードが回復すると、コンソールからのログインに対するローカル認証がイネーブルになり、管理ユーザはコンソールから新しいパスワードでログインできるようになります。

（注） **copy** *configuration-file* **startup-config**の実行時にユーザ名がコンフィギュレーション ファイルで指定されなかったためにパスワードを回復する必要がある場合 **fast-reload** または **reload** コマンドを実行し、ステップ 12 で **write erase** を実行する必要があります。

始める前に

2つのスーパーバイザ モジュールを搭載したデバイスの場合は、回復手順の完了後にアクティブ モジュールになるスーパーバイザ モジュールでパスワード回復手順を実行する必要があり

ます。他方のスーパーバイザモジュールがアクティブにならないようにするには、次の作業のいずれかを実行します。

- 他方のスーパーバイザ モジュールをシャーシから取り外します。
- 回復手順が完了するまで、他方のスーパーバイザ モジュールのコンソール プロンプトを次の 2 つのプロンプトのいずれかに変更します。
  - loader >
  - switch(boot)#

手順

	コマンドまたはアクション	目的
ステップ 1	アクティブなスーパーバイザモジュールのコンソール ポートで端末セッションを確立します。	— （注） US キーマップ以外のキーマップを使用している場合は、ブレイク シーケンスの生成のために必要なキー シーケンスを押しても動作しない可能性があります。この場合、ご使用の端末を US キーマップに設定することを推奨します。キーボード マッピングのため、**Ctrl-C** を **Ctrl-]** の代わりに入力できます。
ステップ 2	SSH または端末エミュレータを使用してコンソール ポートにアクセスする場合は、ステップ 6 に進みます。	—
ステップ 3	Telnet を使用してコンソール ポートにアクセスする場合、**Ctrl-]**（右角カッコ）を押して、Telnet エスケープ シーケンスと競合しないようにします。 **例**： `switch login: Ctrl-]`	— （注） Cisco NX-OS ログイン プロンプトがそのままの状態で、Telnet プロンプトが表示されない場合は、手順 6 に進みます。

ステップ 4	Telnet プロンプトが表示される場合は、Telnet エスケープ シーケンスを Ctrl-]（右角カッコ）以外の文字シーケンスに変更します。
	 例：
	 `telnet> set escape ^\`
	 `Escape Character is 'CTRL+\'`
		次に、Microsoft Telnet で Ctrl+\ をエスケープ キー シーケンスとして設定する例を示します。
		 （注） Cisco NX-OS ログイン プロンプトがそのままの状態で、Telnet プロンプトが表示されない場合は、手順 6 に進みます。

ステップ 5	**Enter** を 1 回または複数回押して Cisco NX-OS ログイン プロンプトに戻ります。 **例**：	—

	コマンドまたはアクション	目的
	telnet> <Enter> switch login:	
ステップ 6	デバイスの電源を一度切ってから再投入します。	—
ステップ 7	**Ctrl-C** を押して、ローダー > プロンプトにアクセスします。 **例：** Ctrl-C loader>	—
ステップ 8	ローダー **cmdline recoverymode=1** **例：** loader> cmdline recoverymode=1	リカバリ モードに切り替えます。
ステップ 9	ローダー> **boot n9000-dk9.x.x.x.bin** **例：** loader> boot n9000-dk9.x.x.x.bin Booting iash Trying diskboot Filesystem type is ext2fs, partition type 0x83 Image valid MD5Sum mismatch INIT: Loading IGB driver ... Signature Envelope.(36)Invalid Tag in Signature Envelope Installing SSE module ... done Creating the sse device node ... done Installing CCTRL driver for card_type 3 ... Checking all filesystems..... Installing SPROM driver ... Installing default sprom values ... done.Configuring network ... Installing psdev ... Installing veobc ... Installing OBFL driver ... Starting portmap daemon... creating NFS state directory: done starting 8 nfsd kernel threads: done starting mountd: done starting statd: done Loading system software No system image is specified INIT: Sending processes the TERM signal INIT: Sending processes the KILL signal Bad terminal type: "linux". Will assume vt100. Cisco Nexus Operating System (NX-OS) Software TAC support: http://www.cisco.com/tac Copyright (c) 2002-2013, Cisco Systems, Inc. All rights reserved. The copyrights to certain works contained in this	スイッチブートプロンプトに到達するには、nx-os イメージだけでデバイスを再起動します。

	コマンドまたはアクション	目的
	software are owned by other third parties and used and distributed under license. Certain components of this software are licensed under the GNU General Public License (GPL) version 2.0 or the GNU Lesser General Public License (LGPL) Version 2.1. A copy of each such license is available at http://www.opensource.org/licenses/gpl-2.0.php and http://www.opensource.org/licenses/lgpl-2.1.php switch(boot)#	
ステップ 10	**Enter** を 1 回または複数回押して Cisco NX-OS ログイン プロンプトに戻ります。 例： telnet> <Enter> switch login:	—
ステップ 11	switch(boot)# **config terminal** 例： switch(boot)# config terminal Enter configuration commands, one per line. End with CNTL/Z. switch(boot)(config)#	ブートコンフィギュレーションモードを開始します。 s
ステップ 12	switch(boot)(config)# **admin-password** *new-password* 例： switch(boot)(config)# admin-password egBdf WARNING! Remote Authentication for login through console has been disabled	ネットワーク管理者パスワードを再設定します。 （注） **copy***configuration-file***startup-config** の実行時にユーザ名がコンフィギュレーション ファイルで指定されなかったためにパスワードを回復する必要がある場合 **fast-reload** または **reload** コマンドを実行し、この手順はスキップし、**write erase** コマンドを入力して、次の手順に進みます。
ステップ 13	switch(boot)(config)# **exit** 例： switch(boot)(config)# exit switch(boot)#	ブート コンフィギュレーション モードを終了します。
ステップ 14	switch(boot)# **load-nxos** 例： switch(boot)# load-nxos	nx-os イメージをロードします。**load-nxos** コマンドは、示されているとおりに入力する必要があります。このコマンドでは、イメージ ファイル名を入力しないでください。

	コマンドまたはアクション	目的

ステップ 15	新しい管理者パスワードを使用してデバイスにログインします。
	例：
	`switch login: admin`
	`Password: egBdf`
		実行コンフィギュレーションにより、コンソールからのログインに対してローカル認証がイネーブルになっていることが示されます。新しいパスワードを今後のログインでも有効にするため、実行コンフィギュレーションは変更しないでください。AAAサーバ上で設定した管理者パスワードを再設定して記憶したら、リモート認証をイネーブルにできます。
		`switch# show running-config aaa`
		`!Command: show running-config aaa`
		`!Time: Fri Jun 7 02:39:23 2013`
		`version 6.1(2)I1(1)`
		`logging level aaa 5`
		`aaa authentication login ascii-authentication`

ステップ 16	switch# **config terminal**
	例：
	`switch# config terminal`
	`switch(config)#`
		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。

ステップ 17	switch(config)# **username admin password** *new-password* 例： `switch(config)# username admin password egBdf`	新しいパスワードを再設定して、簡易ネットワーク管理プロトコル（SNMP）パスワードとしても使用できるようにします。

ステップ 18	switch(config)# **exit**
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 19	必要に応じて、前に取り外したスタンバイ スーパーバイザ モジュールをシャーシに取り付けます。	—
ステップ 20	必要に応じて、スタンバイ スーパーバイザモジュールで nx-os イメージを起動します。	—
ステップ 21	switch(config)# **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

管理者パスワードを回復するためのデバイスのリロード

デバイスの電源を再投入してネットワーク管理者パスワードを再設定できます。

注意 この手順を実行すると、デバイス上のすべてのトラフィックが中断されます。デバイスとの接続はすべて 2 ～ 3 分間切断されます。

（注） 管理インターフェイスとの Telnet またはセキュア シェル（SSH）セッションから管理者パスワードを回復することはできません。ローカル コンソール接続を使用できる必要があります。

（注） パスワードの回復によって更新されるのは、ローカル ユーザ データベース内の新しい管理者パスワードのみです。リモート AAA サーバのパスワードは更新されません。新しいパスワードは、ローカル認証がイネーブルの場合にのみ有効になり、リモート認証の場合は有効になりません。パスワードが回復すると、コンソールからのログインに対するローカル認証がイネーブルになり、管理ユーザはコンソールから新しいパスワードでログインできるようになります。

手順の概要

1. アクティブなスーパーバイザ モジュールのコンソール ポートで端末セッションを確立します。
2. switch# **reload**
3. ローダー> **boot n9000-dk9.x.x.x.bin**
4. 管理者パスワードを回復するためのデバイスの電源再投入 （28 ページ） のステップ 6 ～ 20 を実行して、ネットワーク管理者パスワードを再設定します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	アクティブなスーパーバイザ モジュールのコンソール ポートで端末セッションを確立します。	—

ステップ 2	switch# **reload**
	例：
	`switch# reload`
	`This command will reboot the system. (y/n)?  [n] Y`
	`2013 Jun  7 13:09:56 switch %$ VDC-1 %$`
	`%PLATFORM-2-PFM_SYSTEM_RESET:`
	`Manual system restart from Command Line Interface`
	`writing reset reason 9,`
	`..`
	`..`
	`GNU GRUB  version 0.97`
	`Autobooting bootflash:/n9000-dk9.x.x.x.bin`
	`bootflash:/n...`
		ローダ プロンプトに到達するようにデバイスをリロードします。次のメッセージが表示されたら、**Ctrl-C** を押す必要があります。
		`Booting nx-os image:`
		`bootflash:/n9000-dk9.x.x.x.bin....`

	コマンドまたはアクション	目的
	Filesystem type is ext2fs, partition type 0x83 Booting nx-os image: bootflash:/n9000-dk9.x.x.x.bin....(---->> Press Ctrl + C) ....Aborting Image Boot GNU GRUB version 0.97 Loader Version 3.22.0 loader>	
ステップ 3	ローダー> **boot n9000-dk9.x.x.x.bin** **例**： loader> boot n9000-dk9.x.x.x.bin Filesystem type is ext2fs, partition type 0x83 Booting nx-os image: n9000-dk9.6.1.2.I1.1.gbin.... .....Image verification OK .. .. Lesser General Public License (LGPL) Version 2.1. A copy of each such license is available at http://www.opensource.org/licenses/gpl-2.0.php and http://www.opensource.org/licenses/lgpl-2.1.php switch(boot)#	スイッチ ブート プロンプトに到達するには、nx-os イメージだけでデバイスを再起動します。
ステップ 4	管理者パスワードを回復するためのデバイスの電源再投入 （28 ページ） のステップ 6 ～ 20 を実行して、ネットワーク管理者パスワードを再設定します。	—

管理者パスワードの変更

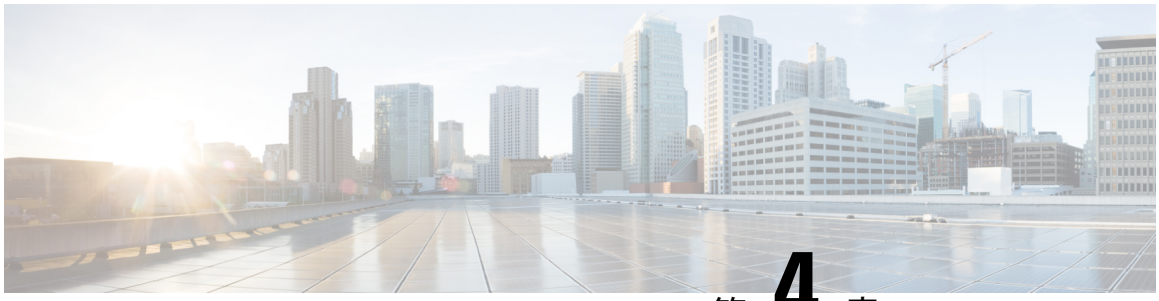
ネットワーク管理者パスワードを変更するには、admin としてログインする必要があります。

管理者パスワードの変更に関するガイドラインと制限事項

管理者パスワードを変更するには、次の注意事項と制約事項に従ってください。

- CLIコマンド no service password-recovery を有効または無効にするには、管理者である必要があります。
- 管理者パスワードを変更するには、管理者としてログインする必要があります。
- 前回のブートで管理者が CLI を無効にした場合、ブート プロンプトから管理者パスワードを変更することはできません。

（注） 管理者としてログインしていない場合は、エラーが表示されます。



第 4 章

ライセンスの問題のトラブルシューティング

- ライセンスの問題のトラブルシューティングに関する情報 （37 ページ）
- ライセンスの注意事項および制約事項 （37 ページ）
- ライセンスのトラブルシューティングの初期チェックリスト （38 ページ）
- CLI を使用したライセンス情報の表示 （39 ページ）
- ライセンスのインストールの問題 （40 ページ）

ライセンスの問題のトラブルシューティングに関する情報

Cisco NX-OS では、一部の機能にライセンスが必要です。ライセンスは、システムでこれらの機能を有効にします。ライセンス機能を有効にするシステムごとにライセンスを購入する必要があります。

シャーシのシリアル番号

ライセンスは、ライセンス ファイルがインストールされるシャーシのシリアル番号を使用して作成されます。シャーシのシリアル番号に基づいてライセンスを注文すると、このライセンスを他のシステムで使用することはできません。

シャーシの交換

ライセンスを含むシャーシを交換する場合は、TAC に連絡して新しいライセンスを生成する必要があります。古いライセンスはシャーシのシリアル番号に基づいており、新しいシャーシでは機能しません。

ライセンスの注意事項および制約事項

Cisco NX-OS のライセンスを扱う場合は、次のガイドラインに従ってください。

- ライセンスが必要な機能に基づいて、必要なライセンスを慎重に決定します。
- 次のように、ライセンスを正確に注文します。
  - システムに付属の購入証明書に記載されている製品認証キーを入力します。
  - ライセンスを注文する際は、正しいシャーシ シリアル番号を入力してください。シリアル番号は、ライセンスをインストールするシャーシと同じである必要があります。**show license host-id** コマンドを使用し、 コマンドを入力して、シャーシのシリアル番号を取得します。
  - シリアル番号を正確に入力します。シリアル番号には、ゼロの代わりに文字「O」を使用しないでください。
  - シャーシに固有のライセンスを注文します。
- ライセンス ファイルをリモートの安全な場所にバックアップします。ライセンス ファイルをアーカイブすると、システムで障害が発生した場合にライセンスが失われることがなくなります。
- システムのシリアル番号を使用して注文したライセンスを使用して、各システムに正しいライセンスをインストールします。ライセンスは、シリアル番号とプラットフォームに固有です。
- **show license usage** を使用 コマンドは、インストールの確認に使用されます。
- ライセンス ファイルを変更したり、注文していないシステムで使用したりしないでください。シャーシを返却する場合は、カスタマーサポート担当者に連絡して、新しいシャーシの交換ライセンスを注文してください。

ライセンスのトラブルシューティングの初期チェックリスト

ライセンスの問題をトラブルシューティングする際は、まず次のことを確認します。

チェックリスト	Done
注文したすべてのライセンスのシャーシ シリアル番号を確認します。	
注文したすべてのライセンスのプラットフォームまたはモジュール タイプを確認します。	
ライセンスの注文に使用した製品認証キーが、シャーシのシリアル番号を取得したのと同じシャーシからのものであることを確認します。	
有効にする機能のライセンスを必要とするすべてのシステムに、すべてのライセンスがインストールされていることを確認します。	

CLI を使用したライセンス情報の表示

手順の概要

1. **show license** [**host-id** | **usage** [*package*]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show license** [**host-id**	**usage** [*package*]] 例： `switch# show license usage LAN_ENTERPRISE_SERVICES_PKG`	このシステムに設定されているライセンス情報を表示します。ライセンスのホストIDを表示するには、**host-id** キーワードを使用します。すべてのライセンス済み機能のリストまたは指定したパッケージ内の機能のリストを表示するには、**usage** キーワードを使用します。

例

次に、インストールされているすべてのライセンス キーファイルと内容を表示する例を示します。

```
switch# show license
entp.lic:
SERVER this_host ANY
VENDOR cisco
INCREMENT LAN_ENTERPRISE_SERVICES_PKG cisco 1.0 permanent uncounted \
        VENDOR_STRING=<LIC_SOURCE>MDS_SWIFT</LIC_SOURCE><SKU>N95-LAN1K9=</SKU> \
        HOSTID=VDH=TBC10412106 \ >
        NOTICE="<LicFileID>20071025133322456</LicFileID>LicLineID>1/LicLineID>
 \
```

この例では、現在のライセンスの使用状況に関する情報を表示します。

```
switch# show license usage
Feature                      Ins   Lic  Status   Expiry Date Comments        Count
--------------------------------------------------------------------------------

LAN_ENTERPRISE_SERVICES_PKG   No    -   In use
--------------------------------------------------------------------------------
```

次に、指定したパッケージの機能のリストを表示する例を示します。

```
switch# show license usage LAN_ENTERPRISE_SERVICES_PKG
Application
-----------
bgp
pim
msdp
ospf
ospfv3
```

```
-----------
```

次に、ライセンスのホスト ID を表示する例を示します。

```
switch# show license host-id
License hostid: VDH=FOX0646S017
```

（注） コロン（:）記号の後に表示される ID 全体を使用します。VHD はベンダー ホスト ID です。

ライセンスのインストールの問題

シリアル番号の問題

ライセンスを注文する際は、正しいシャーシ シリアル番号を使用するようにしてください。**show license host-id** コマンドを使用して、CLI を使用しているシステムの適切なシャーシ シリアル番号を入手します。

別のシャーシ用のライセンスを使用すると、次のシステム メッセージが表示されることがあります。

Error Message: LICMGR-3-LOG_LIC_INVALID_HOSTID: Invalid license hostid VDH=[chars] for feature [chars].

Explanation: The feature has a license with an invalid license Host ID. This can happen if a supervisor module with licensed features for one system is installed on another system.

Recommended Action: Reinstall the correct license for the chassis where the supervisor module is installed.

（注） ライセンスの注文プロセスでシャーシのシリアル番号を入力する場合は、シリアル番号にゼロの代わりに文字「O」を使用しないでください。

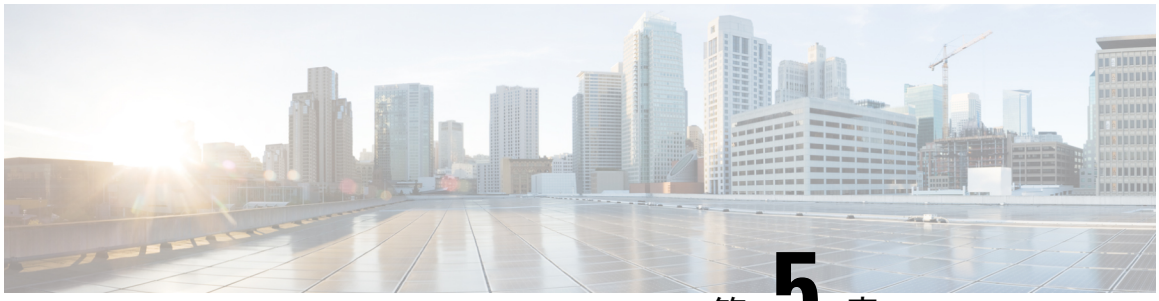
システム間の RMA シャーシ エラーまたはライセンス転送

ライセンスは発行されたシステムに対して固有であり、その他のシステムでは無効です。ライセンスをシステム間で移動する場合は、テクニカル サポートの担当者にお問い合わせください。

欠落しているとリストされたライセンス

ライセンスがインストールされ、正常に動作した後、システム ハードウェアを変更したり、bootflash: の問題が発生したりすると、ライセンスがないとして表示されることがあります。

症状	考えられる原因	対処方法
ライセンスは欠落しているとリストされています。	スーパーバイザ モジュールは、ライセンスのインストール後に交換されました。	破損した bootflash: から回復するには、破損したブートフラッシュの回復 （15 ページ） を参照してください。ライセンスを再インストールします。
	スーパーバイザ bootflash: が破損しています。	



第 5 章

ポートのトラブルシューティング

- ポートのトラブルシューティングについて （43 ページ）
- ポートのトラブルシューティングの注意事項と制約事項 （43 ページ）
- ポートのトラブルシューティングの初期チェックリスト （44 ページ）
- ポート情報の表示 （44 ページ）
- CLI からのポート統計情報のトラブルシューティング （45 ページ）
- ポート インターフェイスの問題のトラブルシューティング （46 ページ）

ポートのトラブルシューティングについて

デバイスで1つのデータ リンクから別のデータ リンクへのフレーム リレーを行うには、フレームが送受信されるインターフェイスの特性を定義する必要があります。設定されているインターフェイスは、イーサネット インターフェイス、VLAN インターフェイス（SVI）、または管理インターフェイス（mgmt0）です。

各インターフェイスには、次のように管理設定と動作ステータスが関連付けられています。

- 管理設定は、修正を加えない限り変更されません。この設定には、管理モードで設定できる各種の属性があります。
- 動作ステータスは、インターフェイス速度のような指定された属性の現在のステータスを表します。このステータスは変更できず、読み取り専用です。インターフェイスがダウンしているときは、一部の値（動作速度など）が有効にならない場合があります。

ポート モード、管理状態、および動作状態の詳細については、『*Cisco Nexus 9000* シリーズ *NX-OS* インターフェイス設定ガイド』を参照してください。

ポートのトラブルシューティングの注意事項と制約事項

ポートインターフェイスを設定する場合は、次のガイドラインに従ってください。

- デバイスの設定を始める前に、シャーシのモジュールが設計どおりに機能していることを確認してください。**show module** コマンドを使用し、して、設定を続行する前にモジュールが正常またはアクティブであることを確認します。
- ポート グループに専用ポートを設定する場合は、次のポート モードの注意事項に従ってください。
  - 専用モードでは、4 ポートグループごと に 1 つのポートのみを設定できます。他の 3 つのポートは使用できず、シャットダウンされたままになります。
  - 他の3つのポートのいずれかがイネーブルの場合、残りのポートを専用モードに設定することはできません。その他の3つのポートは、引き続きイネーブル状態になります。
- Cisco NX-OS のポート設定のライセンス要件はありません。

ポートのトラブルシューティングの初期チェックリスト

トラブルシューティングを始める際は、まず次のことを確認します。

チェックリスト	Done
物理メディアをチェックして、損傷した部分がないことを確認します。	
使用中のSFP（Small Form-Factor Pluggable）デバイスがシスコによって承認されたものであり、故障していないことを確認します。	
ポートが有効になっていることを、**no shutdown** コマンドを使用する必要があります。	
show interface コマンドを使用し、して、インターフェイスの状態を確認します。ポートが動作的なダウン状態になる理由については、『*Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*』を参照してください。	
ポートを専用として設定したこと、ポートグループ内の他の 3 つのポートに接続していないことを確認します。	

ポート情報の表示

show interface counters コマンドを使用すれば ポート カウンタを表示するためのコマンド通常は、アクティブなトラブルシューティング中にのみカウンタを確認します。この場合、まずカウンタをクリアしてベースラインを作成する必要があります。長期間にわたってアクティブになっていたポートの場合、カウンタに格納されている値は意味を持たないことがあります。カウンタをクリアすることにより、現時点での実際のリンクの動作をより正確に把握できます。

すべてのポートカウンタまたは指定したインターフェイスのカウンタをクリアするには、次のいずれかのコマンドを使用します。

- **clear counters interface all**
- **clear counters interface** *range*

カウンタを使用して受信フレーム数と送信フレーム数の有意差を表示することにより、同期の問題を識別できます。

ポートに関する詳細情報を収集するには、次のコマンドを使用します。

- **show interface status**
- **show interface capabilities**
- **show udld**
- **show tech-support udld**

CLI からのポート統計情報のトラブルシューティング

インターフェイスの完全な情報を表示するには、 **show interface** コマンドを使用します。このコマンドは、ポートの状態に加えて、次の情報を表示します。

- Speed
- トランク VLAN のステータス
- 送受信されたフレームの数
- 伝送エラー（破棄、エラー、不正なフレームなど）

```
switch# show interface ethernet 2/45
Ethernet2/45 is down (Administratively down)
  Hardware is 10/100/1000 Ethernet, address is 0019.076c.4dd8 (bia 0019.076c.4dd8)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA
  auto-duplex, auto-speed
  Beacon is turned off
  Auto-Negotiation is turned on
  Input flow-control is off, output flow-control is off
  Auto-mdix is turned on
  Last clearing of "show interface" counters never
  1 minute input rate 0 bytes/sec, 0 packets/sec
  1 minute output rate 0 bytes/sec, 0 packets/sec
  L3 Switched:
    input: 0 pkts, 0 bytes - output: 0 pkts, 0 bytes
  Rx
    0 input packets 0 unicast packets 0 multicast packets
    0 broadcast packets 0 jumbo packets 0 storm suppression packets
    0 bytes
  Tx
    0 output packets 0 multicast packets
    0 broadcast packets 0 jumbo packets
    0 bytes
    0 input error 0 short frame 0 watchdog
    0 no buffer 0 runt 0 CRC 0 ecc
    0 overrun  0 underrun 0 ignored 0 bad etype drop
    0 bad proto drop 0 if down drop 0 input with dribble
```

```
    0 output error 0 collision 0 deferred
    0 late collision 0 lost carrier 0 no carrier
    0 babble
    0 Rx pause 0 Tx pause 0 reset
Receive data field Size is 2112
```

ポートインターフェイスの問題のトラブルシューティング

インターフェイス設定が消えました

インターフェイス設定が消える問題が発生している可能性があります。

Symptoms	考えられる原因	ソリューション
インターフェイス設定が消えました。	インターフェイス モードがスイッチ ポート モードに変更されました。	Cisco NX-OS は、レイヤ 2 ポート モードとレイヤ 3 ポート モードを切り替えるときにインターフェイス設定を削除します。インターフェイスを再設定する必要があります。

インターフェイスを有効にできない

インターフェイスを有効にするときに問題が発生する可能性があります。

問題	考えられる原因	ソリューション
インターフェイスを有効にできません。	インターフェイスは専用ポートグループの一部です。	1 つのポートが専用ポートである場合、ポート グループ内の他の 3 つのポートを有効にすることはできません。**show running-config interface** コマンドを使用し、CLI コマンドを使用して、レートモード設定を確認します。
	インターフェイス設定にリモート ポートとの互換性がありません。	**show interface capabilities** コマンドを使用し、 コマンドを使用して、両方のポートに同じ機能があるかどうかを確認します。必要に応じて設定を変更し、ポートの互換性を確保します。
	レイヤ 2 ポートがアクセス VLAN に関連付けられていない、または VLAN が一時停止状態にあります。	**show interface brief** コマンドを使用し、 コマンドを使用して、VLAN 内でインターフェイスが設定されているかどうかを調べます。**show vlan brief** コマンドを使用し、 コマンドを使用して、VLAN のステータスを調べます。**state active** コマンドを使用し、 コマンドを VLAN コンフィギュレーション モードで使用して、VLAN の状態をアクティブに設定します。
	誤った SFP がポートに接続されています。	**show interface brief** コマンドを使用し、 コマンド を使用して、誤ったトランシーバを使用しているかどうかを確認します。シスコがサポートする SFP と交換します。

専用ポートを設定できない

ポートを専用として設定しようとすると、問題が発生する可能性があります。

問題	考えられる原因	ソリューション
専用ポートを設定できません。	ポート グループ内の他の 3 つのポートはシャットダウンされません。	**shutdown** コマンドを使用し、 コマンドをインターフェイス コンフィギュレーション モードで使用して、ポートグループ内の他の 3 つのポートを無効にします。
	ポートは、ポート グループの最初のポートではありません。	ポート グループの最初のポートのみを専用モードに設定できます。

ポートがリンク障害または接続されていない状態のままになっている

ポートまたはリンクが動作可能にならない問題が発生する可能性があります。

問題	考えられる原因	ソリューション
ポートが link-failure 状態のままになっている。	ポート接続が不良である。	使用中のメディアのタイプを確認します。光、シングルモード（SM）、またはマルチモード（MM）か **shutdown** コマンドを使用し、command followed by the **no shutdown** コマンドを使用して、ポートを無効にしてから有効にします。これで問題が続く場合は、同じモジュールの別のポートまたは他のモジュールのポートに接続を移動してみます。
	Small Form-Factor Pluggable（SFP）の中継障害が原因で信号がないか、SFP に障害がある可能性があります。	この問題が発生すると、ポートはトランジット ポートステートのままになり、信号は表示されません。MAC レベルで同期しない。この問題は、ポート速度の設定または自動ネゴシエーションに関連している可能性があります。インターフェイスに SFP が正しく取り付けられていることを確認します。SFP を取り付け直しても問題が解決しない場合は、SFP を交換するか、スイッチの別のポートを試してください。
	リンクが初期化状態で停止している。または、リンクがポイントツーポイント状態になっている。	**show logging** コマンドを使用し、 して、「Link Failure, Not Connected」システム メッセージが出力されるかどうかを調べます。 **shutdown** コマンドを使用し、command followed by the **no shutdown** コマンドを使用して、ポートを無効にしてから有効にします。これで問題が続く場合は、同じモジュールの別のポートまたは他のモジュールのポートに接続を移動してみます。

予期しないリンク フラッピングが発生する

ポートでフラッピングが発生すると、ポート状態が次の順序で変化し、一巡すると、最初の状態に戻って繰り返します。

1. Initializing：リンクを初期化しています。
2. Offline：ポートはオフライン状態です。

3. Link failure or not connected：物理層リンクが動作不能で、アクティブなデバイス接続がありません。

予期しないリンク フラッピングのトラブルシューティング時には、次の情報を把握することが重要です。

- リンク フラッピングを発生させたユーザ
- 実際のリンク ダウンの理由。

問題	考えられる原因	ソリューション
予期しないリンク フラッピングが発生します。	ビット レートがしきい値を超えたために、ポートが errDisable ステートになっています。	**shutdown** コマンドを使用し、command followed by the **no shutdown** コマンドでポートが通常の状態に戻ります。
	スイッチの問題により、エンドデバイスでリンク フラップ動作が発生しています。原因の一部は次のとおりです。 • ハードウェア障害または断続的なハードウェア エラーにより、スイッチでパケットが廃棄されました。 • ソフトウェア エラーによってパケットが廃棄されました。 • 制御フレームが誤ってデバイスに送信された。	MAC ドライバによって示されるリンク フラップの理由を判別します。エンドデバイス上のデバッグ機能を使用して、問題のトラブルシューティングを行います。外部デバイスでは、エラーが発生すると、リンクの再初期化が選択されることがあります。このような場合、リンクを再初期化する方法はデバイスによって異なります。

ポートが ErrDisable 状態にある

errDisabled状態とは、スイッチがポートの問題を検出して、そのポートをディセーブルにしたことを示します。この状態は、ポートのフラッピングにより生じていて、メディアの問題を示している可能性があります。

問題	考えられる原因	ソリューション
ポートがErrDisable状態にある	ポートがフラッピングしています。	SFP、ケーブル、および接続を確認するには、CLI を使用した ErrDisable 状態の確認 （51 ページ）を参照してください。

CLI を使用した ErrDisable 状態の確認

手順の概要

1. switch# **show interface** *interface slot/port*
2. switch# **show logging logfile**

手順の詳細

	コマンドまたはアクション	目的

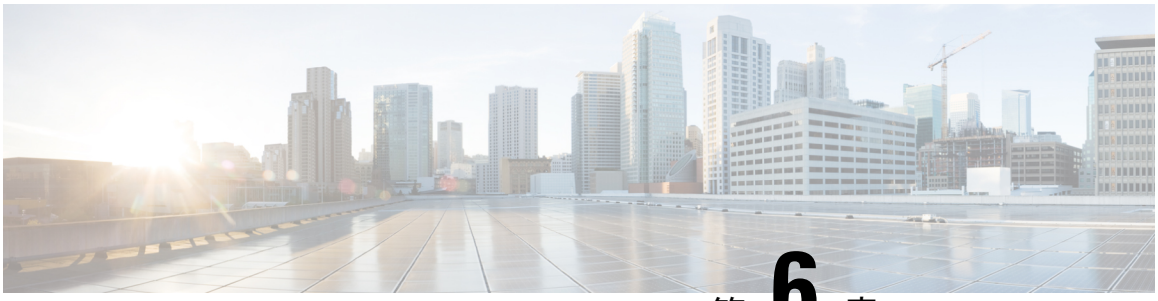
ステップ 1	switch# **show interface** *interface slot/port*
	例：
	`switch# show interface ethernet 1/14`
	`e1/7 is down (errDisabled)`
		デバイスが問題を検出し、ポートをディセーブルにしたことを確認します。
		（注） ポートがディセーブルになっていることを確認したら、ケーブル、SFP、および光ファイバを確認します。

ステップ 2	switch# **show logging logfile** 例： `switch# show logging logfile`	スイッチのログファイルを表示し、ポート状態の変化のリストを確認します。

例

この例は、スイッチのログファイルを表示して、ポート状態変化のリストを確認する方法を示しています。誰かがポート e1/7 をポート チャネル 7 に追加しようとしたときに、エラーが記録されました。このポートがポート チャネル 7 とまったく同じように設定されていなかったため、試行が失敗しました。

```
switch# show logging logfile
 . . .
Jan  4 06:54:04 switch %PORT_CHANNEL-5-CREATED: port-channel 7 created
Jan  4 06:54:24 switch %PORT-5-IF_DOWN_PORT_CHANNEL_MEMBERS_DOWN: Interface
port-channel 7 is down (No operational members)
Jan  4 06:54:40 switch %PORT_CHANNEL-5-PORT_ADDED: e1/8 added to port-channel 7
Jan  4 06:54:56 switch %PORT-5-IF_DOWN_ADMIN_DOWN: Interface e1/7 is down
(Admnistratively down)
Jan  4 06:54:59 switch %PORT_CHANNEL-3-COMPAT_CHECK_FAILURE:
speed is not compatible
Jan 4 06:55:56 switch%PORT_CHANNEL-5-PORT_ADDED: e1/7 added to port-channel 7
```



第 6 章

vPC のトラブルシューティング

- vPC のトラブルシューティングに関する詳細 （53 ページ）
- vPC の初期トラブルシューティングのチェックリスト （53 ページ）
- CLI を使用した vPC の確認 （54 ページ）
- 受信したタイプ 1 設定要素の不一致 （56 ページ）
- vPC 機能を有効にできない （56 ページ）
- ブロッキング状態の vPC （57 ページ）
- 中断状態に移行した vPC 上の VLAN （57 ページ）
- HSRP ゲートウェイを持つホストが VLAN を超えてアクセスできない （57 ページ）

vPC のトラブルシューティングに関する詳細

vPC は、2 つの異なるデバイスに物理的に接続されたリンクを、その他のデバイスから単一のポート チャネルとして見えるようにします。

vPC の初期トラブルシューティングのチェックリスト

vPC の問題をトラブルシューティングする際は、まず次のことを確認します。

チェックリスト	Done
vPC キープアライブリンクは別の VRF にマッピングされますか。そうでない場合は、デフォルトで管理 VRF にマッピングされます。この場合、両方の vPC ピア デバイスの管理ポートに管理スイッチが接続されていますか。	
ピア キープアライブ メッセージに使用される送信元 IP アドレスと宛先 IP アドレスがどちらもその vPC ピアキープアライブ リンクに関連付けられている VRF から到達可能であることを確認してください。	
ピア キープアライブ リンクがアップしていることを確認します。そうしないと、vPC ピア リンクが起動しません。	

チェックリスト	Done
vPC ピア リンクが、vPC VLAN のみを許可するレイヤ 2 ポート チャネル トランクとして設定されていることを確認します。	
vPC ピアデバイスからダウンストリームデバイスに接続するためにポートチャネルに割り当てる vPC 番号は、両方の vPC ピア デバイスで同じである必要があります。	
システム優先順位を手動で設定する場合は、両方の vPC ピア デバイス上で同じプライオリティ値を割り当てていることを確認します。	
show vpc consistency-parameters が設定されており、 コマンドで両方の vPC ピア デバイスに同じタイプ 1 パラメータがあることを確認します。	
プライマリ vPC がプライマリ STP ルートであり、セカンダリ vPC がセカンダリ STP ルートであることを確認します。	

CLI を使用した vPC の確認

CLI を使用して vPC を確認するには、次のいずれかのタスクを実行します。

コマンド	目的
show running-config vpc	vPC 設定の確認
show vpc	vPC のステータスを確認します。
show vpc peer-keepalive	vPC peer-keepalive リンクのステータスを表示します。
show vpc consistency-parameters	vPC ピアに同じタイプ 1 パラメータがあることを確認します。
show tech-support vpc	vPC のテクニカル サポートの詳細情報が表示されます。
show port-channel summary	ポート チャネルのメンバーが vPC にマッピングされていることを確認します。

コマンド	目的
show spanning-tree	STP が有効な場合、次の STP パラメータが同一であることを確認します。 • BPDU フィルタ • BPDU ガード • コスト • リンク タイプ • プライオリティ • VLAN（PVRST+）

次の例は、**show vpc** コマンドのサンプル出力を示しています。 コマンドに対して表示されます。

```
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                     : 1
Peer status                       : peer link is down

vPC keep-alive status             : Suspended (Destination IP not reachable)
Configuration consistency status  : failed
Per-vlan consistency status       : success

Configuration inconsistency reason: Consistency Check Not Performed
Type-2 inconsistency reason       : Consistency Check Not Performed
vPC role                          : none established

Number of vPCs configured         : 2
Peer Gateway                      : Enabled
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Disabled (due to peer configuration)
Auto-recovery status              : Disabled

vPC Peer-link status
---------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ -----------------------------------
1    Po10   down   -


vPC status
----------------------------------------------------
id   Port   Status Consistency Reason                     Active vlans
--   ----   ------ ----------- ------                     ------------
2    Po20   down   failed      Peer-link is down          -



50   Po50   down   failed      Peer-link is down          -
```

受信したタイプ 1 設定要素の不一致

タイプ 1 の設定要素の不一致が原因で vPC リンクを起動できないという問題が発生する場合があります。

症状	考えられる原因	ソリューション
タイプ 1 の設定要素の不一致を受信しました。	vPC ピア ポートまたはメンバーシップ ポートの設定が同一ではありません。	**show vpc consistency-parameters interface** コマンドを使用し、 コマンドを使用して、設定の不一致が発生する場所を特定します。

次に、ポート チャネルの vPC 整合性パラメータを表示する例を示します。

```
switch# show vpc consistency-parameters interface po 10
   Legend:
       Type 1 : vPC will be suspended in case of mismatch
Name                        Type  Local Value            Peer Value
-------------               ----  ---------------------- -----------------------
STP Mode                    1     Rapid-PVST             Rapid-PVST
STP Disabled                1     None                   None
STP MST Region Name         1     ""                     ""
STP MST Region Revision     1     0                      0
STP MST Region Instance to  1
 VLAN Mapping
STP Loopguard               1     Disabled               Disabled
STP Bridge Assurance        1     Enabled                Enabled
STP Port Type               1     Normal                 Normal
STP MST Simulate PVST       1     Enabled                Enabled
Allowed VLANs               -     1-10,15-20,30,37,99    1-10,15-20,30,37,99
```

vPC 機能を有効にできない

vPC 機能を有効にすると、エラーが表示されることがあります。

症状	考えられる原因	ソリューション
vPC 機能を有効にします。	ハードウェアが vPC と互換性がありません。	**show module** コマンドを使用し、コマンドを使用して、各イーサネット モジュールのハードウェア バージョンを確認します。

次に、モジュール ハードウェア バージョンを表示する例を示します。

```
switch# show module
Mod Ports Module-Type                       Model              Status
--- ----- ------------------------------------ ------------------ ----------
22   0    Fabric Module                        N9K-C9508-FM       ok
24   0    Fabric Module                        N9K-C9508-FM       ok
26   0    Fabric Module                        N9K-C9508-FM       ok
27   0    Supervisor Module                    N9K-SUP-A          active *
29   0    System Controller                    N9K-SC-A           active
```

```
30   0    System Controller                  N9K-SC-A           standby

Mod Sw                Hw
--- ----------------- ------
22  6.1(2)I1(1)       0.4040
24  6.1(2)I1(1)       0.4040
26  6.1(2)I1(1)       0.4040
27  6.1(2)I1(1)       0.4080
29  6.1(2)I1(1)       0.2170
30  6.1(2)I1(1)       0.2170
```

ブロッキング状態の vPC

Bridge Assurance（BA）が原因で、vPC がブロッキング状態になることがあります。

症状	考えられる原因	ソリューション
vPC がブロッキング状態。	BPDU は、ポートチャネルの単一リンクでのみ送信します。BA の拮抗が検出されると、vPC 全体がブロッキング状態になります。	vPC では BA を有効にしないでください。

中断状態に移行した vPC 上の VLAN

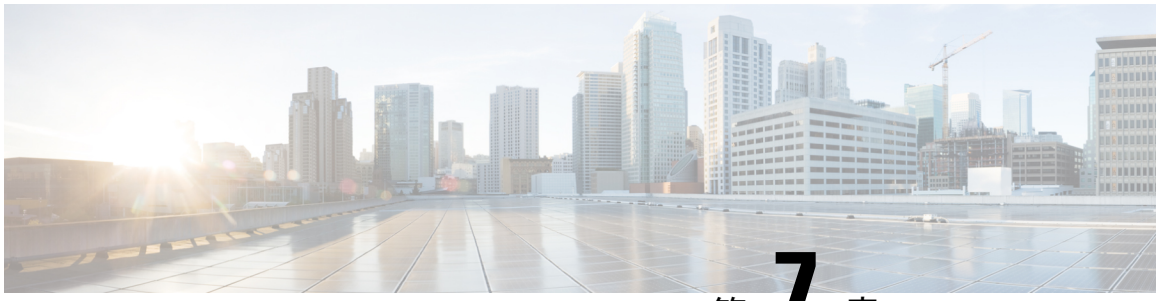
vPC 上の VLAN が中断状態になることがあります。

症状	考えられる原因	ソリューション
vPC 上の VLAN が中断状態に移行した。	vPC で許可されている VLAN が vPC ピア リンクで許可されていない。	vPC で許可されているすべての VLAN は、vPC ピア リンクでも許可される必要があります。また、vPC ピア リンク上では、vPC VLAN のみを許可することを推奨します。

HSRP ゲートウェイを持つホストが VLAN を超えてアクセスできない

VLAN 上の vPC ピア デバイスとその VLAN 上のホストの両方で HSRP が有効になっている場合、それらのデバイスは自身の VLAN の外部に到達できない可能性があります。

症状	考えられる原因	ソリューション
HSRP ゲートウェイを持つホストは、VLAN を超えてアクセスできません。	ホスト ゲートウェイの MAC アドレスが vPC ピア デバイスのいずれかの物理 MAC アドレスにマッピングされている場合、vPC のループ防止メカニズムが原因でパケットがドロップされることがあります。	ホスト ゲートウェイの MAC アドレスを、いずれかの vPC ピアデバイスの物理 MAC アドレスではなく、HSRP MAC アドレスにマッピングします。ピア ゲートウェイは、このシナリオの回避策になります。実装する前に、ピア ゲートウェイの詳細についてコンフィギュレーション ガイドを参照してください。



第 7 章

VLAN のトラブルシューティング

- VXLAN の問題のトラブルシューティング （59 ページ）
- Broadcom シェル テーブルについて （69 ページ）
- GPORTと前面パネルのポート番号マッピングの取得 （73 ページ）
- 入力ポートのためにどのインターフェイス トラフィックが使用されるかを特定する （74 ページ）
- VLAN のフラッド リストの検索 （74 ページ）
- カプセル化ポートがフラッド リストの一部であるかどうかの判別 （74 ページ）

VXLAN の問題のトラブルシューティング

VXLAN データ パスには、次のパスが含まれます。

- マルチキャスト カプセル化パス：ネイティブ レイヤ 2 パケットは、ネットワーク（レイヤ 2 からレイヤ 3）方向へのアクセスで VXLAN にカプセル化されます。
- マルチキャスト カプセル化解除パス：ネイティブ レイヤ 2 パケットはネットワークの VXLAN でカプセル化解除され、（レイヤ 3 からレイヤ 2 へ）方向にアクセスします。
- ユニキャスト カプセル化パス：ネイティブ レイヤ 2 パケットは、ネットワーク（レイヤ 2 からレイヤ 3）方向へのアクセスで VXLAN にカプセル化されます。
- ユニキャスト カプセル化解除パス：ネイティブのレイヤ 2 パケットがネットワークの VXLAN でカプセル化解除され、（レイヤ 3 からレイヤ 2 へ）方向にアクセスします。

これらのデータ パスを理解すると、VXLAN の問題のトラブルシューティングに役立ちます。

注意 VXLAN の問題をトラブルシューティングするには、Broadcom シェル コマンドを実行する必要があります。Broadcom シェル コマンドは、シスコのサポート担当者の直接監督下または要求された場合のみ注意して使用してください。

（注） Cisco Nexus 9300 シリーズ スイッチは、VXLAN をサポートしています。Cisco Nexus 9500 シリーズ スイッチはサポートしていません。

マルチキャスト カプセル化パスでドロップされたパケット

ネットワークにアクセスする方向にデバイスで ARP 要求またはマルチキャスト パケットがドロップされている場合は、次の手順に従います。

手順の概要

1. Broadcom シェルにアクセスします。
2. **stg show** コマンドの出力を調べて、特定の VLAN のポートが STP 転送状態になっているかどうかを確認します。
3. ポートが VLAN の一部であるかどうかを確認します。
4. **mc show** コマンドの出力を調べて、ローカル VLAN ポートとカプセル化ポートがカプセル化フラッド リストに含まれているかどうかを確認します。
5. **mc show** コマンドの出力が正しくない場合は、Broadcom シェル モードを終了し、**showtech-support pixm**、**show tech-support pixm-all**、**show tech-support pixmc-all** コマンドを実行し、出力を表示します。

手順の詳細

ステップ 1 Broadcom シェルにアクセスします。

例：

```
switch# bcm-shell module 1
Warning: BCM shell access should be used with caution
Entering bcm shell on module 1
Available Unit Numbers: 0
```

ステップ 2 **stg show** コマンドの出力を調べて、特定の VLAN のポートが STP 転送状態になっているかどうかを確認します。

例：

```
bcm-shell.0> stg show
STG 6: contains 1 VLAN (3)
  Disable: xe56-xe95
    Block: xe0-xe22,xe24-xe55
  Forward: xe23,hg
```

この例では、VLAN 3 に eth1/24 があり、アップリンク トンネル ポートが eth2/2 であるため、出力に xe23（1/24）と hg が表示されます。

ステップ 3 ポートが VLAN の一部であるかどうかを確認します。

例：

```
bcm-shell.0> vlan show
vlan 3  ports xe23
(0x00000000000000000000000000000000000000000000000000000000100000000), untagged
none (0x00000000000000000000000000000000
00000000000000000000000000000) MCAST_FLOOD_UNKNOWN
```

この例では、xe23 は VLAN 3 の一部である必要があります。

ステップ 4 **mc show** コマンドの出力を調べて、ローカル VLAN ポートとカプセル化ポートがカプセル化フラッド リストに含まれているかどうかを確認します。

a) カプセル化フラッド リストを取得します。

例：

```
bcm-shell.0> d chg vfi 3
Private image version: R
VFI.ipipe0[3]:
<VP_1=0xc01,VP_0=0x1803,UUC_INDEX=0x1803,UMC_INDEX=0x1803,RSVD_VP_0=1,BC_INDEX=0x1803>
```

この例では、0x1803 がカプセル化フラッド リストです。

b) カプセル化フラッド リストを **mc show** コマンドに入力します。

例：

```
bcm-shell.0> mc show 0x1803
Group 0xc001803 (VXLAN)
        port hg7, encap id 400053
        port xe23, encap id 400057
```

この例では、hg7 はアップリンク トンネル ポートで、xe23 は VLAN のローカル ポートです。

アップリンクがポート チャネルの場合、ポート チャネルのすべてのメンバーが出力に表示されます。出力に重複エントリが含まれている場合、対応するパケット レプリケーションがあります。

ステップ 5 **mc show** コマンドの出力が正しくない場合は、Broadcom シェル モードを終了し、**showtech-support pixm**、**show tech-support pixm-all**、**show tech-support pixmc-all** コマンドを実行し、出力を表示します。

例：

```
bcm-shell.0> exit
switch# show tech-support pixm
switch# show tech-support pixm-all
switch# show tech-support pixmc-all
```

マルチキャスト カプセル化解除パスでドロップされたパケット

ネットワークがアクセスする方向にデバイスで ARP 要求またはマルチキャスト パケットがドロップされている場合は、次の手順に従います。

手順の概要

1. パケットがスーパーバイザに送信されたかどうか、およびリモート VXLAN トンネル エンドポイント（VTEP）の検出が行われたかどうかを確認します。
2. ハードウェアに mpls_entry が存在する場合は、vlan_xlate テーブルを確認します。

3. vlan_xlate テーブルにマルチキャスト DIP の正しいエントリがある場合は、VLAN フラッディング リストに正しいメンバー（カプセル化トンネル ポートを除く VLAN のメンバー）が表示されているかどうかを確認します。

手順の詳細

ステップ 1 パケットがスーパーバイザに送信されたかどうか、およびリモート VXLAN トンネル エンドポイント（VTEP）の検出が行われたかどうかを確認します。

a) リモート ピアがソフトウェアで学習されたかどうかを確認します。

例：

```
switch# show nve peers
Interface          Peer-IP           VNI        Up Time
-----------------  ---------------   --------   -----------
nve1               100.100.100.5     10000      00:02:23
```

b) mpls_entry テーブルを確認して、リモート ピアがハードウェアで学習されたかどうかを確認します。

例：

```
switch# bcm-shell module 1
bcm-shell.0> d chg mpls_entry | grep SVP
MPLS_ENTRY.ipipe0[12368]:
<VXLAN_SIP:SVP=0x1751,VXLAN_SIP:SIP=0x66666666,VXLAN_SIP:KEY=0x666666668,VXLAN_SIP:HASH_LSB=0x666
VXLAN_SIP:DATA=0
x1751,VALID=1,KEY_TYPE=8,>
```

c) mpls_entry がなく、送信元仮想ポート（SVP）がない場合は、パケットがスーパーバイザに送信されているかどうかを確認し、IPFIB エラーがないかどうかを確認します。

例：

```
bcm-shell.0> show c cpu0
bcm-shell.0> exit
switch# attach module 1
module-1# show system internal ipfib errors
```

ステップ 2 ハードウェアに mpls_entry が存在する場合は、vlan_xlate テーブルを確認します。

例：

```
module-1# exit
switch# bcm-shell module 1
bcm-shell.0> d chg vlan_xlate | grep 0xe1000003
VLAN_XLATE.ipipe0[8464]:
<VXLAN_DIP:KEY=0x7080000192,VXLAN_DIP:IGNORE_UDP_CHECKSUM=1,VXLAN_DIP:HASH_LSB=3,VXLAN_DIP:DIP=0xe1000003,
XLAN_DIP
:DATA=0x400000,VALID=1,KEY_TYPE=0x12,>
```

vlan_xlate テーブルには、パケットのマルチキャスト宛先 IP アドレス（DIP）のエントリが 1 つ必要です。この例では、マルチキャストパケットが 225.0.0.3 に送信される場合を示しています。

ステップ 3 vlan_xlate テーブルにマルチキャスト DIP の正しいエントリがある場合は、VLAN フラッディング リストに正しいメンバー（カプセル化トンネル ポートを除く VLAN のメンバー）が表示されているかどうかを確認します。

a) VLAN フラッディング リストを確認します。

例：

```
bcm-shell.0> d chg vfi 3
Private image version: R
VFI.ipipe0[3]:
<VP_1=0xc01,VP_0=0x1803,UUC_INDEX=0x1803,UMC_INDEX=0x1803,RSVD_VP_0=1,BC_INDEX=0x1803>
```

0x1803 のカプセル化フラッド リストの場合、対応するカプセル化解除フラッド リストは 0x1c03 になります。

b) ローカル ポートがカプセル化解除フラッド リストに含まれているかどうかを確認します。

例：

```
bcm-shell.0> mc show
Group 0xc001c03 (VXLAN)
        port xe23, encap id 400057
```

xe23 はカプセル化解除フラッド リストの一部である必要があります。

c) ポートがフォワーディング ステートであり、VLAN の一部であることを確認します。

例：

```
bcm-shell.0> stg show
bcm-shell.0> vlan show
```

ユニキャスト カプセル化パスでドロップされたパケット

単一のネクスト ホップで VTEP に到達でいる場合にドロップユニキャスト パケット

アクセスからネットワーク方向のデバイスでユニキャスト パケットがドロップされ、VTEP が ECMP パスを介して到達可能である場合は、次の手順に従います。

手順の概要

1. リモート ピアがハードウェアで検出されたかどうかを確認します。
2. ネクストホップへの送信元仮想ポート（SVP）のマッピングを取得します。
3. ネクストホップ インデックスからポート番号を取得します。
4. ポート番号からチップ上の物理ポートへのマッピングを取得します。
5. 出力ポートからネクストホップ インデックスへのマッピングを取得します。
6. トンネル パラメータをチェックして、EGR IP トンネルの SIP フィールドに正しいローカル VTEP IP アドレスが表示されていることを確認します。

7. トンネル DIP がプログラムされていることを確認します。

手順の詳細

ステップ 1 リモート ピアがハードウェアで検出されたかどうかを確認します。

例：

```
switch# bcm-shell module 1
bcm-shell.0> d chg mpls_entry | grep SVP
MPLS_ENTRY.ipipe0[12368]:
<VXLAN_SIP:SVP=0x1751,VXLAN_SIP:SIP=0x66666666,VXLAN_SIP:KEY=0x666666668,VXLAN_SIP:HASH_LSB=0x666
VXLAN_SIP:DATA=0
x1751,VALID=1,KEY_TYPE=8,>
```

有効な送信元 IP アドレス（SIP）が存在することを確認します。

この例では、102.102.102.102 がリモート VTEP IP アドレスです。

ステップ 2 ネクストホップへの送信元仮想ポート（SVP）のマッピングを取得します。

例：

```
bcm-shell.0> d chg ing_dvp_table 0x1751
Private image version: R
ING_DVP_TABLE.ipipe0[5969]:
<VP_TYPE=3,NEXT_HOP_INDEX=0x18,NETWORK_PORT=1,ECMP_PTR=0x18,DVP_GROUP_PTR=0x18,>
```

この例では、ネクストホップインデックスは 0x18 です。

ステップ 3 ネクストホップ インデックスからポート番号を取得します。

例：

```
bcm-shell.0> d chg ing_l3_next_hop 0x18
Private image version: R
ING_L3_NEXT_HOP.ipipe0[24]:
<VLAN_ID=0xfff,TGID=0x88,PORT_NUM=8,MTU_SIZE=0x3fff,MODULE_ID=1,L3_OIF=0x1fff,ENTRY_TYPE=2
ENTRY_INFO_UPPER=3,DV
P_RES_INFO=0x7f,>
```

この例では、ポート番号は8です。

ステップ 4 ポート番号からチップ上の物理ポートへのマッピングを取得します。

例：

```
bcm-shell.0> phy info
Phy mapping dump:
      port   id0   id1  addr iaddr          name    timeout
  hg0(  1)  600d  8770   1b1   1b1   TSC-A2/31/4     250000
  hg1(  2)  600d  8770    81    81   TSC-A2/00/4     250000
  hg2(  3)  600d  8770   1ad   1ad   TSC-A2/30/4     250000
  hg3(  4)  600d  8770    85    85   TSC-A2/01/4     250000
  hg4(  5)  600d  8770   189   189   TSC-A2/23/4     250000
  hg5(  6)  600d  8770    ad    ad   TSC-A2/08/4     250000
  hg6(  7)  600d  8770   185   185   TSC-A2/22/4     250000
  hg7(  8)  600d  8770    b1    b1   TSC-A2/09/4     250000
  xe0(  9)  600d  84f9     0    89      BCM84848     250000
```

```
  xe1( 10)  600d  84f9     1    8a      BCM84848     250000
  xe2( 11)  600d  84f9     2    8b      BCM84848     250000
  xe3( 12)  600d  84f9     3    8c      BCM84848     250000
```

この例では、ポート番号 8 は hg7 です。

ステップ 5 出力ポートからネクストホップ インデックスへのマッピングを取得します。

例：

```
bcm-shell.0> g chg egr_port_to_nhi_mapping
EGR_PORT_TO_NHI_MAPPING.hg7[2][0x4001808]=0x18: <NEXT_HOP_INDEX=0x18>
```

この例では、ネクストホップ インデックス 0x18 は hg7 を指しています。

ステップ 6 トンネル パラメータをチェックして、EGR IP トンネルの SIP フィールドに正しいローカル VTEP IP アドレスが表示されていることを確認します。

例：

```
bcm-shell.0> d chg egr_ip_tunnel
Private image version: R
EGR_IP_TUNNEL.epipe0[1]:
<TUNNEL_TYPE=0xb,TTL=0xff,SIP=0x65656565,L4_DEST_PORT=0x2118,ENTRY_TYPE=1,DSCP_SEL=1,>
```

この例では、SIP はローカル VTEP IP アドレス（101.101.101.101）で、L4_DEST_PORT は 0x2118（ポート 8472）で、DSCP_SEL = 1 は内部 DSCP パケットが外部 DSCP パケットにコピーされることを意味します。

ステップ 7 トンネル DIP がプログラムされていることを確認します。

例：

```
bcm-shell.0> d chg egr_dvp_attribute 0x1751
Private image version: R
EGR_DVP_ATTRIBUTE.epipe0[5969]:
<VXLAN:TUNNEL_INDEX=1,VXLAN:DVP_IS_NETWORK_PORT=1,VXLAN:DIP=0x66666666,VP_TYPE=2,>
```

VTEP が ECMP パスを介して到達可能な場合にドロップされるユニキャスト パケット

ネットワーク方向にアクセスするデバイスでユニキャスト パケットがドロップされ、VTEP が ECMP パスを介して到達可能である場合は、次の手順に従います。

手順の概要

1. 特定のリモートピア仮想ポート（VP）の ECMP ネクストホップを取得します。
2. ECMP_PTR を 10 進数に変換し、200000 を追加してポート番号を取得します。
3. ECMP ネクストホップ セット内のインターフェイスのリストを取得します。
4. ポート チャネルのメンバーを検索します。
5. 特定のネクストホップ インデックスの物理ネクストホップ インターフェイスを検索します。

手順の詳細

ステップ 1 特定のリモートピア仮想ポート（VP）の ECMP ネクストホップを取得します。

例：

```
bcm-shell.0> d chg ing_dvp_table 0x1751
Private image version: R
ING_DVP_TABLE.ipipe0[5969]:
<VP_TYPE=3,NEXT_HOP_INDEX=0x108,NETWORK_PORT=1,ECMP_PTR=0x108,ECMP=1,DVP_GROUP_PTR=0x108,>
```

この例では、0x1751 は、d chg mpls_entry 出力を使用して取得されたリモート ピア IP アドレスの VP 番号です。

（注） リモート VTEP が ECMP パスを介して到達可能である場合、出力に ECMP=1 が存在する必要があります。

ステップ 2 ECMP_PTR を 10 進数に変換し、200000 を追加してポート番号を取得します。

例：

```
0x108 (264) + 200000 = 200264
```

この例では、ポート番号は 200264 です。

ステップ 3 ECMP ネクストホップ セット内のインターフェイスのリストを取得します。

例：

```
bcm-shell.0> d chg l3 multipath show 200264
Multipath Egress Object 200264
Interfaces: 100606 100607 100608
Reference count: 2
bcm-shell.0> l3 egress show | grep 100606
100606  00:22:bd:f5:1a:60 4095 4101     1t   0        -1   no   no
bcm-shell.0> l3 egress show | grep 100607
100607  00:22:bd:f5:1a:60 4095 4102     2t   0        -1   no   no
bcm-shell.0> l3 egress show | grep 100608
100608  00:22:bd:f5:1a:60 4095 4103     3t   0        -1   no   no
```

この例では、ネクストホップ インターフェイスはポート チャネルである 1t、2t、および 3t です。

ステップ 4 ポート チャネルのメンバーを検索します。

例：

```
bcm-shell.0> trunk show
Device supports 1072 trunk groups:
  1024 front panel trunks (0..1023), 256 ports/trunk
  48 fabric trunks (1024..1071), 64 ports/trunk
trunk 0: (front panel, 0 ports)
trunk 1: (front panel, 1 ports)=hg6 dlf=any mc=any ipmc=any psc=portflow (0x9)
trunk 2: (front panel, 1 ports)=hg4 dlf=any mc=any ipmc=any psc=portflow (0x9)
trunk 3: (front panel, 1 ports)=hg7 dlf=any mc=any ipmc=any psc=portflow (0x9)
```

ステップ 5 特定のネクストホップ インデックスの物理ネクストホップ インターフェイスを検索します。

例：

```
bcm-shell.0> g chg egr_port_to_nhi_mapping
EGR_PORT_TO_NHI_MAPPING.hg4[2][0x4001805]=0x5f7: <NEXT_HOP_INDEX=0x5f7>
EGR_PORT_TO_NHI_MAPPING.hg6[2][0x4001807]=0x9b3: <NEXT_HOP_INDEX=0x9b3>
EGR_PORT_TO_NHI_MAPPING.hg7[2][0x4001808]=0x5f8: <NEXT_HOP_INDEX=0x5f8>
```

この例では、ネクストホップ インデックス 0x5f7 は hg4 を指し、0x9b3 は hg6 を指し、0x5f8 は hg7 を指します。

ユニキャスト カプセル化解除パスでドロップされたパケット

方向にアクセスするために、ネットワーク内のデバイスでユニキャストパケットがドロップされる場合は、次の手順に従います。

手順の概要

1. パケットがスーパーバイザに送信されたかどうか、およびリモート VXLAN トンネル エンドポイント（VTEP）の検出が行われたかどうかを確認します。
2. ハードウェアに mpls_entry が存在する場合は、vlan_xlate テーブルを確認します。
3. ユニキャスト DIP エントリが vlan_xlate テーブルに存在するかどうかを確認します。
4. ユニキャスト DIP エントリが vlan_xlate テーブルに存在するかどうかを確認します。
5. 宛先 MAC アドレスがレイヤ 2 MAC アドレス テーブルに表示されていることを確認します。

手順の詳細

ステップ 1 パケットがスーパーバイザに送信されたかどうか、およびリモート VXLAN トンネル エンドポイント（VTEP）の検出が行われたかどうかを確認します。

a) リモート ピアがソフトウェアで学習されたかどうかを確認します。

例：

```
switch# show nve peers
Interface          Peer-IP           VNI        Up Time
-----------------  ---------------   --------   -----------
nve1               100.100.100.5     10000      00:06:54
```

b) mpls_entry テーブルを確認して、リモート ピアがハードウェアで学習されたかどうかを確認します。

例：

```
switch# bcm-shell module 1
bcm-shell.0> d chg mpls_entry | grep SVP
MPLS_ENTRY.ipipe0[12368]:
<VXLAN_SIP:SVP=0x1751,VXLAN_SIP:SIP=0x66666666,VXLAN_SIP:KEY=0x666666668,VXLAN_SIP:HASH_LSB=0x666
VXLAN_SIP:DATA=0
x1751,VALID=1,KEY_TYPE=8,>
```

c) mpls_entryがなく、送信元仮想ポート（SVP）がない場合は、パケットがスーパーバイザに送信されているかどうかを確認し、IPFIB エラーがないかどうかを確認します。

例：

```
bcm-shell.0> show c cpu0
bcm-shell.0> exit
switch# attach module 1
module-1# show system internal ipfib errors
```

ステップ 2 ハードウェアに mpls_entry が存在する場合は、vlan_xlate テーブルを確認します。

例：

```
module-1# exit
switch# bcm-shell module 1
bcm-shell.0> d chg vlan_xlate | grep 0xe1000003
VLAN_XLATE.ipipe0[8464]:
<VXLAN_DIP:KEY=0x7080000192,VXLAN_DIP:IGNORE_UDP_CHECKSUM=1,VXLAN_DIP:HASH_LSB=3,VXLAN_DIP:DIP=0xe1000003,
XLAN_DIP
:DATA=0x400000,VALID=1,KEY_TYPE=0x12,>
```

vlan_xlate テーブルには、パケットのマルチキャスト宛先 IP アドレス（DIP）のエントリが 1 つ必要です。この例では、マルチキャストパケットが 225.0.0.3 に送信される場合を示しています。

ステップ 3 ユニキャスト DIP エントリが vlan_xlate テーブルに存在するかどうかを確認します。

例：

```
bcm-shell.0> d chg vlan_xlate | grep 0x65656565
VLAN_XLATE.ipipe0[14152]:
<VXLAN_DIP:KEY=0x32b2b2b292,VXLAN_DIP:IGNORE_UDP_CHECKSUM=1,VXLAN_DIP:HASH_LSB=0x565
VXLAN_DIP:DIP=0x65656565,VXLAN_DIP:DATA=0x400000,VALID=1,KEY_TYPE=0x12,>
```

エントリが存在する場合は、カプセル化が解除されます。

ステップ 4 ユニキャスト DIP エントリが vlan_xlate テーブルに存在するかどうかを確認します。

例：

```
bcm-shell.0> d chg vlan_xlate | grep 0x65656565
VLAN_XLATE.ipipe0[14152]:
<VXLAN_DIP:KEY=0x32b2b2b292,VXLAN_DIP:IGNORE_UDP_CHECKSUM=1,VXLAN_DIP:HASH_LSB=0x565
VXLAN_DIP:DIP=0x65656565,VXLAN_DIP:DATA=0x400000,VALID=1,KEY_TYPE=0x12,>
```

エントリが存在する場合は、カプセル化が解除されます。

ステップ 5 宛先 MAC アドレスがレイヤ 2 MAC アドレス テーブルに表示されていることを確認します。

例：

```
bcm-shell.0> l2 show
mac=00:00:bb:01:00:03 vlan=28772 GPORT=0x80000215Unknown GPORT format
mac=00:00:cc:01:00:0a vlan=28772 GPORT=0x80003401Unknown GPORT format
mac=00:00:bb:01:00:05 vlan=28772 GPORT=0x80000215Unknown GPORT format
mac=00:00:aa:01:00:0a vlan=28772 GPORT=0x80003401Unknown GPORT format
mac=00:00:aa:01:00:07 vlan=28772 GPORT=0x80003401Unknown GPORT format
mac=00:00:cc:01:00:01 vlan=28772 GPORT=0x80003401Unknown GPORT format
mac=00:00:bb:01:00:08 vlan=28772 GPORT=0x80000215Unknown GPORT format
mac=00:00:aa:01:00:01 vlan=28772 GPORT=0x80003401Unknown GPORT format
```

```
mac=00:00:cc:01:00:07 vlan=28772 GPORT=0x80003401Unknown GPORT format
mac=00:00:cc:01:00:02 vlan=28772 GPORT=0x80003401Unknown GPORT format
mac=00:00:aa:01:00:04 vlan=28772 GPORT=0x80003401Unknown GPORT format
mac=00:00:cc:01:00:04 vlan=28772 GPORT=0x80003401Unknown GPORT format
mac=00:00:aa:01:00:02 vlan=28772 GPORT=0x80003401Unknown GPORT format
mac=00:00:cc:01:00:09 vlan=28772 GPORT=0x80003401Unknown GPORT format
mac=00:00:aa:01:00:09 vlan=28772 GPORT=0x80003401Unknown GPORT format
mac=00:00:bb:01:00:06 vlan=28772 GPORT=0x80000215Unknown GPORT format
mac=00:00:cc:01:00:06 vlan=28772 GPORT=0x80003401Unknown GPORT format
mac=00:00:aa:01:00:06 vlan=28772 GPORT=0x80003401Unknown GPORT format
mac=00:00:bb:01:00:09 vlan=28772 GPORT=0x80000215Unknown GPORT format
mac=00:00:bb:01:00:04 vlan=28772 GPORT=0x80000215Unknown GPORT format
mac=00:00:bb:01:00:02 vlan=28772 GPORT=0x80000215Unknown GPORT format
mac=00:00:aa:01:00:08 vlan=28772 GPORT=0x80003401Unknown GPORT format
mac=00:00:bb:01:00:07 vlan=28772 GPORT=0x80000215Unknown GPORT format
mac=00:00:cc:01:00:08 vlan=28772 GPORT=0x80003401Unknown GPORT format
mac=00:00:bb:01:00:01 vlan=28772 GPORT=0x80000215Unknown GPORT format
mac=00:00:cc:01:00:05 vlan=28772 GPORT=0x80003401Unknown GPORT format
mac=00:00:aa:01:00:03 vlan=28772 GPORT=0x80003401Unknown GPORT format
mac=00:00:bb:01:00:0a vlan=28772 GPORT=0x80000215Unknown GPORT format
mac=00:00:cc:01:00:03 vlan=28772 GPORT=0x80003401Unknown GPORT format
mac=00:00:aa:01:00:05 vlan=28772 GPORT=0x80003401Unknown GPORT format
```

宛先 MAC アドレスが存在する場合、レイヤ 2 転送が発生します。それ以外の場合、パケットはカプセル化解除フラッディングリストを使用してフラッディングされます。

Broadcom シェル テーブルについて

このセクションでは、VXLAN に関する Broadcom シェル テーブルについて説明します。

MPLS エントリ テーブル

MPLS エントリ（mpls_entry）テーブルには、次の情報が含まれます。

- リモート VTEP（SIP）の IP アドレス
- トンネルカプセル化ポート（SVP）
- VLAN と VNID（VFI、VN_ID）間のマッピング

SIPエントリがmpls_entryテーブルにない場合、パケットはVTEP学習のためにスーパーバイザに送信されます。エントリがハードウェアにインストールされると、パケットはスーパーバイザに送信されなくなります。

（注） 一部のパケットは、ソフトウェア転送が VXLAN パケットに対して実行されないため、学習フェーズ中にドロップされます。

（注） スーパーバイザに送信されるパケットは、class-default CPU キューを使用します。現在、VxLAN 専用の COPP クラスはありません。

次の例は、リモート VTEP IP アドレスが 100.100.100.1 で、VLAN 100 が VNID 10000 にマッピングされるテーブルを示しています。

```
bcm-shell.0> d chg mpls_entry
Private image version: R
MPLS_ENTRY.ipipe0[6816]:
<VXLAN_SIP:SVP=8,VXLAN_SIP:SIP=0x64646401,VXLAN_SIP:KEY=0x646464018
VXLAN_SIP:HASH_LSB=0x401,VXLAN_SIP:DATA=8,VALID=1,KEY_TYPE=8,>
MPLS_ENTRY.ipipe0[8680]:
<VXLAN_VN_ID:VN_ID=0x2710,VXLAN_VN_ID:VFI=0x64,VXLAN_VN_ID:KEY=0x27109
VXLAN_VN_ID:HASH_LSB=0x710,VXLAN_VN_ID:DATA=0x64,VALID=1,KEY_TYPE=9,>
```

出力では、VLAN-VNID マッピングごとに 1 つのエントリが検索されます。この例では、VN_ID = 0x2710 は 16 進表記の VNID、VFI = 0x64 は 16 進表記のマッピング VLAN、0x64 = 100 は 0x2710 VNID 10000 にマッピングされます。

MAC アドレス ラーニング

VXLAN VLAN で学習された MAC アドレスは、内部変換 VLAN で学習されたものとして表示されます（たとえば、VLAN 100 は VLAN 28772 として表示されます）。

GPORT は、MAC アドレスが学習されたポートまたは仮想ポートを参照します。ローカル MAC アドレスの場合、GPORT # と前面パネルの port # の間にマッピングがあります。リモート MAC アドレスは、トンネル ポートを指している SVP に対して学習する必要があります。

このテーブルのミスは、VLAN のローカル ポートおよびトンネル ポートにパケットをフラッディングすることを意味します。このテーブルのヒットは、パケットを対応する GPORT に転送することを意味します。GPORT がトンネル ポートの場合は、パケットを VXLAN にカプセル化する必要があります。GPORT がローカル ポートの場合、通常のレイヤ 2 学習 MAC アドレス転送が発生します。

（注） GPORT と前面パネルのポート番号の間のマッピングを取得するには、GPORTと前面パネルのポート番号マッピングの取得 （73 ページ） セクションを参照してください。

入力 DVP テーブル

入力 DVP テーブルは、仮想ポートをネクストホップ インデックスにマッピングします。これはユニキャスト カプセル化パスで使用され、仮想ポートによってインデックスが作成されます。ECMP の場合は、ECMP = 1 フィールドが必要です。

次の例は、VP 0x1751 のネクストホップ インデックスが0x35であることを示しています。

```
bcm-shell.0> d chg ing_dvp_table 0x1751
Private image version: R
ING_DVP_TABLE.ipipe0[5969]:
<VP_TYPE=3,NEXT_HOP_INDEX=0x35,NETWORK_PORT=1,ECMP_PTR=0x35,DVP_GROUP_PTR=0x35,>
```

入力レイヤ 3 ネクスト ホップ

入力レイヤ 3 ネクスト ホップは、特定のネクストホップ インデックスのポート番号を示します。ユニキャスト カプセル化パスで使用されます。phy_info を使用すれば、ポート番号と実際の前面パネルのポート番号の間のマッピングを取得できます。

```
bcm-shell.0> d chg ing_l3_next_hop
ING_L3_NEXT_HOP.ipipe0[16]:
<VLAN_ID=0xfff,TGID=0x9f,PORT_NUM=0x1f,MTU_SIZE=0x3fff,MODULE_ID=1,L3_OIF=0x1fff,ENTRY_TYPE=2
ENTRY_INFO_UPPER=3,DVP_RES_INFO=0x7f,>
```

VLAN 変換テーブル

VLAN 変換テーブルは、VXLAN マルチキャストとユニキャストの両方のカプセル化解除パスで使用されます。次の 3 種類のエントリが含まれます。

- 外部マルチキャスト グループごとに 1 つのエントリ（マルチキャスト DIP）
- ローカル VTEP（ユニキャスト DIP）の 1 つのエントリ
- ポートごとに VLAN ごとに 1 つのエントリ

次の例は、マルチキャスト DIP エントリを示しています。

```
bcm-shell.0> d chg vlan_xlate | grep 0xe1000003
VLAN_XLATE.ipipe0[8464]:
<VXLAN_DIP:KEY=0x7080000192,VXLAN_DIP:IGNORE_UDP_CHECKSUM=1,VXLAN_DIP:HASH_LSB=3
VXLAN_DIP:DIP=0xe1000003,VXLAN_DIP:DATA=0x400000,VALID=1,KEY_TYPE=0x12,>
```

次の例は、ユニキャスト DIP エントリを示しています。

```
bcm-shell.0> d chg vlan_xlate | grep 0x65656565
VLAN_XLATE.ipipe0[14152]:
<VXLAN_DIP:KEY=0x32b2b2b292,VXLAN_DIP:IGNORE_UDP_CHECKSUM=1,VXLAN_DIP:HASH_LSB=0x565
VXLAN_DIP:DIP=0x65656565,VXLAN_DIP:DATA=0x400000,VALID=1,KEY_TYPE=0x12,>
```

次の例は、VLAN ごと、ポートごとに 1 つのエントリを示しています。

```
bcm-shell.0> d chg vlan_xlate | grep VLAN_ID=3
VLAN_XLATE.ipipe0[3216]:
<XLATE:VLAN_ID=3,XLATE:TGID=0xa0,XLATE:SVP_VALID=1,XLATE:SOURCE_VP=0x201,XLATE:SOURCE_FIELD=0xa0
XLATE:PORT_NUM=0x20,XLATE:OVID=3,XLATE:OTAG=3,XLATE:OLD_VLAN_ID=3,XLATE:MPLS_ACTION=1
XLATE:MODULE_ID=1,XLATE:KEY=0x1805024,XLATE:ITAG=3,XLATE:INCOMING_VIDS=3,XLATE:HASH_LSB=3
XLATE:GLP=0xa0,XLATE:DISABLE_VLAN_CHECKS=1,XLATE:DATA=0x100a000000000000000001,VLAN_ID=3
VALID=1,TGID=0xa0,SVP_VALID=1,SOURCE_VP=0x201,SOURCE_TYPE=1,SOURCE_FIELD=0xa0,PORT_NUM=0x20,OVID=3
OTAG=3,OLD_VLAN_ID=3,MPLS_ACTION=1,MODULE_ID=1,KEY_TYPE=4,KEY=0x1805024,ITAG=3,INCOMING_VIDS=3
HASH_LSB=3,GLP=0xa0,DISABLE_VLAN_CHECKS=1,DATA=0x100a000000000000000001>
```

EGR ポートから NHI へのマッピング

EGR ポートから NHI へのマッピングは、ネクストホップ インデックスを出力ポートにマッピングします。ユニキャスト カプセル化パスで使用されます。

```
bcm-shell.0> g chg egr_port_to_nhi_mapping
EGR_PORT_TO_NHI_MAPPING.hg7[2][0x4001808]=0x36: <NEXT_HOP_INDEX=0x36>
```

VLAN フラッド インデックス テーブル

VLAN フラッドインデックス（VFI）テーブルには、特定の VLAN または VFI の BC/UUC/UMC インデックスが表示されます。**mcshow** コマンドの出力でフラッディング インデックスを使用して、トンネル カプセル化ポートを含む VLAN のメンバーを検索できます。

次の例は、ポート番号を取得する例を示しています。

```
bcm-shell.0> d chg vfi 3
Private image version: R
VFI.ipipe0[3]:
<VP_1=0xc01,VP_0=0x1803,UUC_INDEX=0x1803,UMC_INDEX=0x1803,RSVD_VP_0=1,BC_INDEX=0x1803>
```

次の例は、このポート番号を phy_info に入力して、前面パネルのポート番号を取得する方法を示しています。

```
bcm-shell.0> d chg ing_l3_next_hop
ING_L3_NEXT_HOP.ipipe0[16]:
<VLAN_ID=0xfff,TGID=0x9f,PORT_NUM=0x1f,MTU_SIZE=0x3fff,MODULE_ID=1,L3_OIF=0x1fff,ENTRY_TYPE=2
ENTRY_INFO_UPPER=3,DVP_RES_INFO=0x7f,

bcm-shell.0> phy info
Phy mapping dump:
      port   id0   id1  addr iaddr                  name    timeout
  hg0(  1)  600d  8770   1b1   1b1            TSC-A0/31/4     250000
  hg1(  2)  600d  8770    81    81            TSC-A0/00/4     250000
  hg2(  3)  600d  8770   1ad   1ad            TSC-A0/30/4     250000
  hg3(  4)  600d  8770    85    85            TSC-A0/01/4     250000
  hg4(  5)  600d  8770   1a9   1a9            TSC-A0/29/4     250000
  hg5(  6)  600d  8770    89    89            TSC-A0/02/4     250000
  hg6(  7)  600d  8770   195   195            TSC-A0/26/4     250000
  hg7(  8)  600d  8770    a1    a1            TSC-A0/05/4     250000
  hg8(  9)  600d  8770   191   191            TSC-A0/25/4     250000
```

次の例は、カプセル化解除ルートを示しています。

```
bcm-shell.0> d chg vlan_xlate
Private image version: R
VLAN_XLATE.ipipe0[768]:
<VXLAN_DIP:NETWORK_RECEIVERS_PRESENT=1,VXLAN_DIP:KEY=0x7080000092,VXLAN_DIP:IGNORE_UDP_CHECKSUM=1
VXLAN_DIP:HASH_LSB=1,VXLAN_DIP:DIP=0xe1000001,VXLAN_DIP:DATA=0x400001,VALID=1,KEY_TYPE=0x12,>
VLAN_XLATE.ipipe0[1472]:
<VXLAN_DIP:KEY=0x3232320112,VXLAN_DIP:IGNORE_UDP_CHECKSUM=1,VXLAN_DIP:HASH_LSB=0x402
VXLAN_DIP:DIP=0x64646402,VXLAN_DIP:DATA=0x400000,VALID=1,KEY_TYPE=0x12,>
```

（注） NETWORK_RECEIVERS_PRESENT は 0 に設定する必要があります。

GPORTと前面パネルのポート番号マッピングの取得

次の手順に従って、GPORT から前面パネルのポート番号へのマッピングを取得します。

手順の概要

1. GPORT＃からローカル ターゲット ロジック（LTL）を取得するには、次の式を使用します：LTL＃= 0x10000 - 512 + GPORT＃
2. 対象とする LTL の ifindex を取得します。
3. 前面パネル ポートの ifindex を取得します。
4. GPORT から前面パネル ポート番号へのマッピングを表示します。

手順の詳細

ステップ 1 GPORT＃からローカルターゲットロジック（LTL）を取得するには、次の式を使用します：LTL＃=0x10000 - 512 + GPORT＃

GPORT が 0x201 の場合、LTL は 0x10000 + 0x201 (513) - 0x200 (512) = 0x10001です。

ステップ 2 対象とする LTL の ifindex を取得します。

例：

```
switch# attach module 1
module-1# show system internal pixmc info sdb ltl 0x10001
```

ステップ 3 前面パネル ポートの ifindex を取得します。

例：

```
module-1# exit
switch# show int snmp-ifindex | grep 0x1a002e00
Eth1/24    436219392  (0x1a002e00)
```

ステップ 4 GPORT から前面パネル ポート番号へのマッピングを表示します。

例：

```
switch# bcm-shell module 1
bcm-shell.0> l2 show
mac=00:00:00:00:00:00 vlan=0 GPORT=0xc000000 Trunk=0^M
mac=00:00:bb:01:00:03 vlan=28772 GPORT=0x80001751Unknown GPORT format ^M
mac=00:00:cc:01:00:0a vlan=28772 GPORT=0x80000201Unknown GPORT format ^M
mac=00:00:bb:01:00:05 vlan=28772 GPORT=0x80001751Unknown GPORT format ^M
mac=00:00:aa:01:00:0a vlan=28772 GPORT=0x80000202Unknown GPORT format ^M
```

この例では、MAC アドレス 00:00:bb:01:00:05 はトンネルを通して学習されるので、GPORT 0x1751 はトンネル SVP に対応します。MAC アドレス 00:00:aa:01:00:0a はローカルに学習されるので、GPORT 0x202 は前面パネル ポートに対応します。

入力ポートのためにどのインターフェイス トラフィックが使用されるかを特定する

次に、特定の出力ポートでトラフィックが使用するインターフェイスを検索する例を示します。

```
switch# show system internal ethpm info interface ethernet 2/3 | grep ns_pid
  IF_STATIC_INFO:
port_name=Ethernet2/3,if_index:0x1a006400,ltl=2543,slot=0,nxos_port=50,dmod=1,dpid=9,unit=0
queue=2064,xbar_unitbmp=0x0
ns_pid=8

- dpid=9 is higig8

switch# bcm-shell module 1
bcm-shell.0> g chg egr_port_to_nhi_mapping
EGR_PORT_TO_NHI_MAPPING.hg7[2][0x4001808]=0x36: <NEXT_HOP_INDEX=0x36>
bcm-shell.0> d chg egr_l3_next_hop 0x36
Private image version: R
EGR_L3_NEXT_HOP.epipe0[54]:
<OVID=0x65,MAC_ADDRESS=0x60735cde6e41,L3MC:VNTAG_P=1,L3MC:VNTAG_FORCE_L=1,L3MC:VNTAG_DST_VIF=0x18
L3MC:RSVD_DVP=1,L3MC:INTF_NUM=0x1065,L3MC:FLEX_CTR_POOL_NUMBER=3,L3MC:FLEX_CTR_OFFSET_MODE=3
L3MC:FLEX_CTR_BASE_COUNTER_IDX=0xe41,L3MC:ETAG_PCP_DE_SOURCE=3,L3MC:ETAG_PCP=1
L3MC:ETAG_DOT1P_MAPPING_PTR=1,L3MC:DVP=0x2b9b,L3:OVID=0x65,L3:MAC_ADDRESS=0x60735cde6e41
L3:IVID=0xc83,L3:INTF_NUM=0x1065,IVID=0xc83,INTF_NUM=0x1065,>
```

VLAN のフラッド リストの検索

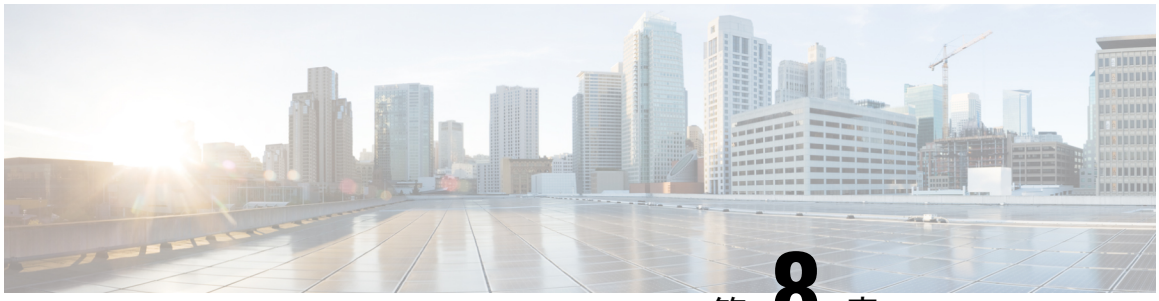
次に、特定の VLAN のフラッド リストを検索する例を示します。

```
bcm-shell.0> d chg vfi 3
Private image version: R
VFI.ipipe0[3]:
<VP_1=0xc01,VP_0=0x1803,UUC_INDEX=0x1803,UMC_INDEX=0x1803,RSVD_VP_0=1,BC_INDEX=0x1803>
```

カプセル化ポートがフラッドリストの一部であるかどうかの判別

次に、ネットワーク方向へのアクセスにおいて、カプセル化ポートがフラッドリストの一部であるかどうかを確認する例を示します。

```
bcm-shell.0> mc show 0x1803
Group 0xc001803 (VXLAN)
        port hg7, encap id 400053
        port xe23, encap id 400057
```



第 8 章

STP のトラブルシューティング

•

• STP のトラブルシューティング （75 ページ）
• STP の初期トラブルシューティングのチェックリスト （75 ページ）
• STP データ ループのトラブルシューティング （76 ページ）
• 過剰なパケット フラッディングのトラブルシューティング （79 ページ）
• コンバージェンス時間の問題のトラブルシューティング （80 ページ）
• フォワーディング ループに対するネットワークの保護 （81 ページ）

STP のトラブルシューティング

STP は、レイヤ 2 レベルで、ループのないネットワークを実現します。レイヤ 2 LAN ポートは定期的に STP フレームを送受信します。ネットワーク デバイスは、これらのフレームを転送せずに、フレームを使用してループフリーパスを構築します。レイヤ 2 の詳細については、『*Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide*』を参照してください。

STP の初期トラブルシューティングのチェックリスト

STP の問題のトラブルシューティングでは、個々のデバイスおよびネットワーク全体の設定と接続に関する情報を収集する必要があります。

STP の問題をトラブルシューティングする際は、まず次のことを確認します。

チェックリスト	Done
デバイスで設定されているスパニング ツリーのタイプを確認します。	
すべての相互接続ポートとスイッチを含む、ネットワーク トポロジを確認します。ネットワーク上のすべての冗長パスを特定し、冗長パスはブロック状態であることを確認します。	

チェックリスト	Done
show spanning-tree summary totals コマンドを使用し、 して、アクティブ状態の論理インターフェイスの総数が、最大許容数を下回っていることを確認します。これらの限界値の詳細については、『*Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide*』を参照してください。	
プライマリおよびセカンダリ ルート ブリッジと、設定されている Cisco 拡張機能を確認します。	

STP 設定と動作の詳細を表示するには、次のコマンドを使用します。

- **show running-config spanning-tree**
- **show spanning-tree summary**
- **show spanning-tree detail**
- **show spanning-tree bridge**
- **show spanning-tree mst**
- **show spanning-tree mst configuration**
- **show spanning-tree interface** *interface-type slot*/*port* [**detail**]
- **show tech-support stp**
- **show spanning-tree vlan**

STP によってブロックされているポートを表示するには、**show spanning-tree blockedports** コマンドを使用します。

各ノードで学習またはエージングが発生するかどうかを確認するには、**show mac address-table dynamic vlan** コマンドを使用します。

STP データ ループのトラブルシューティング

データ ループは、STP ネットワークでよく見られる問題です。データ ループの症状の一部は次のとおりです。

- 高いリンク使用率、最大 100％
- 高い CPU およびバックプレーン トラフィック使用率
- 一定の MAC アドレスの再学習とフラッピング
- インターフェイスでの過剰な出力ドロップ

l2fm ロギング レベルが 4 以上の場合、スイッチはホスト MAC アドレス フラッピングの発生をログに記録し、STP データ ループの特定に役立ちます。1 秒以内に MAC アドレスの移動が検出され、10 回連続して移動すると、スイッチは MAC アドレスが移動しているポートの 1 つの VLAN で学習を無効にします。学習は 120 秒間無効になり、自動的に再度有効になります。

Syslog は、学習が無効または有効になっている間に生成されます。**logging level l2fm** *log-level* コマンドを使用して、ログ レベルを設定できます。

手順の概要

1. switch# **show interface** *interface-type slot*/*port* **include rate**
2. switch(config)# **interface** *interface-type slot*/*port*
3. switch(config-if)# **shutdown**
4. switch(config-if)# **show spanning-tree vlan** *vlan-id*
5. （任意） switch(config-if)# **show spanning-tree interface** *interface-type slot*/*port* **detail**
6. （任意） switch(config-if)# **show interface counters errors**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	switch# **show interface** *interface-type slot*/*port* **include rate**
	例：
	`switch# show interface ethernet 2/1 include rate`
	`1 minute input rate 19968 bits/sec, 0 packets/sec`
	`1 minute output rate 3952023552 bits/sec, 957312 packets/sec`
		リンク使用率が高いインターフェイスを調べることで、ループに関与するポートを特定します。

ステップ 2	switch(config)# **interface** *interface-type slot*/*port* 例： `switch(config)# interface ethernet 2/1`	インターフェイス タイプと位置を設定します。
ステップ 3	switch(config-if)# **shutdown** 例： `switch(config-if)# shutdown`	影響を受けるポートをシャットダウンまたは切断します。 影響を受けるポートを切断した後、ネットワーク トポロジ図を使用して冗長パス内のすべてのスイッチを特定します。

ステップ 4	switch(config-if)# **show spanning-tree vlan** *vlan-id*
	例：
	`switch(config-if)# show spanning-tree vlan 9`
	`VLAN0009`
	`Spanning tree enabled protocol rstp`
	`Root ID Priority 32777''`
	`Address 0018.bad7.db15''`
	`Cost 4`
	`...`
		スイッチが、影響を受けないその他のスイッチと同じ STP ルート ブリッジをリストすることを確認します。

	コマンドまたはアクション	目的

ステップ 5	（任意） switch(config-if)# **show spanning-tree interface** *interface-type slot*/*port* **detail**
	例：
	`switch(config-if)# show spanning-tree interface ethernet 3/1 detail`
	`Port 385 (Ethernet3/1) of VLAN0001 is root forwarding`
	`Port path cost 4, Port priority 128, Port Identifier 128.385`
	`Designated root has priority 32769, address 0018.bad7.db15`
	`Designated bridge has priority 32769, address 0018.bad7.db15`
	`Designated port id is 128.385, designated path cost 0`
	`Timers: message age 16, forward delay 0, hold 0`
	`Number of transitions to forwarding state: 1`
	`The port type is network by default`
	`Link type is point-to-point by default`
	`BPDU: sent 1265, received 1269`
		ルート ポートおよび代替ポートが BPDU を定期的に受信していることを確認します。

ステップ 6	（任意） switch(config-if)# **show interface counters errors**
	例：
	`switch(config-if)# show interface counters errors`
	`--------------------------------------------------------------------------------`
	`Port Align-Err FCS-Err Xmit-Err Rcv-Err UnderSize OutDiscards`
	`--------------------------------------------------------------------------------`
	`mgmt0 -- -- -- -- -- --`
	`Eth1/1 0 0 0 0 0 0`
	`Eth1/2 0 0 0 0 0 0`
	`Eth1/3 0 0 0 0 0 0`
	`Eth1/4 0 0 0 0 0 0`
	`Eth1/5 0 0 0 0 0 0`
	`Eth1/6 0 0 0 0 0 0`
	`Eth1/7 0 0 0 0 0 0`
	`Eth1/8 0 0 0 0 0 0`
		ハードウェア パケット統計情報（エラー ドロップ）カウンタをチェックします。

例

次に、指定ポートが定期的に BPDU を送信している例を示します。

```
switch# show spanning-tree interface ethernet 3/1 detail
Port 385 (Ethernet3/1) of VLAN0001 is root forwarding
   Port path cost 4, Port priority 128, Port Identifier 128.385
   Designated root has priority 32769, address 0018.bad7.db15
   Designated bridge has priority 32769, address 0018.bad7.db15
   Designated port id is 128.385, designated path cost 0
   Timers: message age 16, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   The port type is network by default
   Link type is point-to-point by default
   BPDU: sent 1265, received 1269
```

次に、ハードウェアパケット統計カウンタでBPDUエラードロップの可能性をチェックする例を示します。

```
switch# show interface counters errors
--------------------------------------------------------------------
Port Align-Err FCS-Err Xmit-Err Rcv-Err UnderSize OutDiscards
--------------------------------------------------------------------
mgmt0  --       --       --       --       --       --
Eth1/1  0        0        0        0        0        0
Eth1/2  0        0        0        0        0        0
Eth1/3  0        0        0        0        0        0
Eth1/4  0        0        0        0        0        0
Eth1/5  0        0        0        0        0        0
Eth1/6  0        0        0        0        0        0
Eth1/7  0        0        0        0        0        0
Eth1/8  0        0        0        0        0        0
```

過剰なパケットフラッディングのトラブルシューティング

STP トポロジが不安定になると、STP ネットワークで過剰なパケットフラッディングが発生する可能性があります。Rapid STP または Multiple STP（MST）では、ポートの状態が転送に変更され、ロールが指定からルートに変更されると、トポロジが変更されることがあります。Rapid STP は、レイヤ 2 転送テーブルをただちにフラッシュします。802.1D はエージング タイムを短縮します。転送テーブルの即時フラッシュにより、接続はより高速に復元されますが、フラッディングが増加します。

安定したトポロジでは、トポロジを変更しても過剰なフラッディングは発生しません。リンクフラップはトポロジの変更を引き起こす可能性があるため、継続的なリンク フラップはトポロジの変更とフラッディングを繰り返す可能性があります。フラッディングはネットワーク パフォーマンスを低下させ、インターフェイスでパケット ドロップを引き起こす可能性があります。

手順の概要

1. switch# **show spanning-tree vlan** *vlan-id* **detail**
2. switch# **show spanning-tree vlan** *vlan-id* **detail**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	switch# **show spanning-tree vlan** *vlan-id* **detail**
	例：
	`switch# show spanning-tree vlan 9 detail`
	`VLAN0009 is executing the rstp compatible Spanning Tree protocol`
	`Bridge Identifier has priority 32768, sysid 9, address 0018.bad8.27ad`
	`Configured hello time 2, max age 20, forward delay 15`
	`Current root has priority 32777, address 0018.bad7.db15`
	`Root port is 385 (Ethernet3/1), cost of root path is 4`
	`Topology change flag not set, detected flag not set`
	`'' Number of topology changes 8 last change occurred 1:32:11 ago''`
	`'' from Ethernet3/1''`
	`Times: hold 1, topology change 35, notification 2`
	`...`
		過剰なトポロジ変更の原因を判別します。

ステップ 2	switch# **show spanning-tree vlan** *vlan-id* **detail**
	例：
	`switch# show spanning-tree vlan 9 detail`
	`VLAN0009 is executing the rstp compatible Spanning Tree protocol`
	`Bridge Identifier has priority 32768, sysid 9, address 0018.bad8.27ad`
	`Configured hello time 2, max age 20, forward delay 15`
	`Current root has priority 32777, address 0018.bad7.db15`
	`Root port is 385 (Ethernet3/1), cost of root path is 4`
	`Topology change flag not set, detected flag not set`
	`Number of topology changes 8 last change occurred 1:32:11 ago`
	`'' from Ethernet3/1''`
	`Times: hold 1, topology change 35, notification 2`
	`...`
		トポロジ変更が発生したインターフェイスを特定します。
		トポロジの変更を開始したデバイスを分離できるようになるまで、インターフェイスに接続されているデバイスでこの手順を繰り返します。
		このデバイスのインターフェイスのリンク フラップを確認します。

コンバージェンス時間の問題のトラブルシューティング

STP のコンバージェンスに予想よりも長い時間がかかるか、予期しない最終的なネットワーク トポロジが発生する可能性があります。

コンバージェンスの問題をトラブルシューティングするには、次の問題を確認します。

- 文書化されたネットワーク トポロジ図のエラー。

- タイマーの設定ミス、直径、ブリッジ保証、ルートガード、BPDUガードなどのシスコ拡張機能など。
- 推奨論理ポート（ポート VLAN）の制限を超えたコンバージェンス中のスイッチ CPU の過負荷。
- STP に影響するソフトウェア障害。

フォワーディング ループに対するネットワークの保護

STPが特定の障害に正しく対処できないことを処理するために、シスコでは、ネットワークを転送ループから保護するための多数の機能と拡張機能を開発しました。

STP のトラブルシューティングは、特定の障害の原因を切り分けて見つけるのに役立ちますが、これらの拡張機能の実装は、ネットワークを転送ループから保護する唯一の方法です。

始める前に

- すべてのスイッチ間リンクでシスコ独自の単方向リンク検出（UDLD）プロトコルを有効にします。詳細については、『*Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*』を参照してください。
- すべてのスイッチ間リンクをスパニング ツリー ネットワーク ポート タイプとして設定して、ブリッジ保証機能を設定します。

（注） リンクの両側でブリッジ保証機能をイネーブルにする必要があります。そうでない場合は、Cisco NX-OS はブリッジ保証の不整合のためにポートがブロック状態になります。

- すべてのエンドステーション ポートをスパニング ツリー エッジポート タイプとして設定します。

  STPエッジポートを設定して、ネットワークのパフォーマンスに影響を与える可能性のあるトポロジ変更通知および後続のフラッディングの量を制限する必要があります。このコマンドは、エンドステーションに接続するポートでのみ使用します。そうしないと、偶発的なトポロジ ループによってデータ パケット ループが発生し、デバイスとネットワークの動作が中断される可能性があります。

- ポート チャネルの Link Aggregation Control Protocol（LACP）をイネーブルにして、ポートチャネルの設定ミスの問題を回避します。詳細については、『*Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*』を参照してください。

  スイッチ間リンクで自動ネゴシエーションをディセーブルにしないでください。自動ネゴシエーション メカニズムは、リモート障害情報を伝達できます。これは、リモート側で障害を検出する最も迅速な方法です。リモート側で障害が検出されると、リンクがまだパルスを受信している場合でも、ローカル側はリンクをダウンさせます。

⚠

注意 STP タイマーを変更する場合は注意してください。STP タイマーは相互に依存しており、変更はネットワーク全体に影響を与える可能性があります。

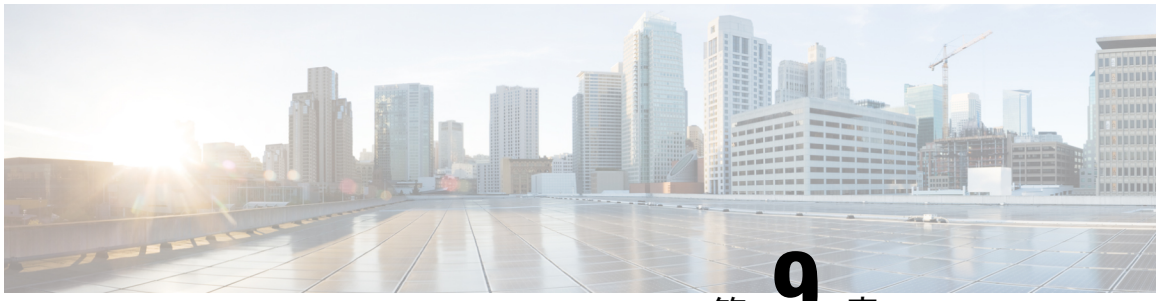
手順の概要

1. （任意） switch(config)# **spanning-tree loopguard default**
2. switch(config)# **spanning-tree bpduguard enable**
3. switch(config)# **vlan** *vlan-range*
4. switch(config)# **spanning-tree vlan** *vlan-range* **root primary**
5. switch(config)# **spanning-tree vlan** *vlan-range* **root secondary**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	（任意） switch(config)# **spanning-tree loopguard default** 例： `switch(config)# spanning-tree loopguard default`	ルート ガードを使用してネットワーク STP 境界を保護します。ルート ガードと BPDU ガードを使用すると、外部からの影響から STP を保護できます。
ステップ 2	switch(config)# **spanning-tree bpduguard enable** 例： `switch(config)# spanning-tree bpduguard enable`	STP エッジポートで BPDU ガードをイネーブルにして、ポートに接続されている不正なネットワーク デバイス（ハブ、スイッチ、ブリッジング ルータなど）の影響を受けないようにします。 ルート ガードは、STP が外部の影響を受けないようにします。BPDU ガードは、BPDU（上位 BPDU だけでなく）を受信しているポートをシャットダウンします。 （注） 2 つの STP エッジ ポートが直接またはハブ経由で接続されている場合、短期間のループはルート ガードまたは BPDU ガードによって防止されません。
ステップ 3	switch(config)# **vlan** *vlan-range* 例： `switch(config)# vlan 9`	個別の VLAN を設定し、管理 VLAN でのユーザ トラフィックを回避します。管理 VLAN は、ネットワーク全体ではなくビルディング ブロックに含まれます。
ステップ 4	switch(config)# **spanning-tree vlan** *vlan-range* **root primary** 例： `switch(config)# spanning-tree vlan 9 root primary`	予測可能な STP ルートを設定します。

	コマンドまたはアクション	目的
ステップ 5	switch(config)# **spanning-tree vlan** *vlan-range* **root secondary** 例： `switch(config)# spanning-tree vlan 12 root secondary`	予測可能なバックアップ STP ルート配置を設定します。 コンバージェンスが予測可能な方法で行われ、すべてのシナリオで最適なトポロジが構築されるように、STP ルートとバックアップ STP ルートを設定する必要があります。STP プライオリティをデフォルト値のままにしないでください。



第 9 章

ルーティングのトラブルシューティング

- ルーティングの問題のトラブルシューティングについて （85 ページ）
- トラブルシューティング ルートの初期チェックリスト （85 ページ）
- ルーティングのトラブルシューティング （86 ページ）
- ポリシーベース ルーティングのトラブルシューティング （89 ページ）

ルーティングの問題のトラブルシューティングについて

レイヤ3ルーティングには、最適なルーティング パスの決定とパケットの交換の決定という、2つの基本的動作があります。ルーティング アルゴリズムを使用すると、ルータから宛先までの最適なパス（経路）を計算できます。この計算方法は、選択したアルゴリズム、ルート メトリック、そしてロード バランシングや代替パスの探索などの考慮事項により異なります。

Cisco NX-OS は、複数の仮想ルーティングおよび転送 (VRF) インスタンス、および複数のルーティング情報ベース (RIB) をサポートしており、複数のアドレス ドメインをサポートします。各 VRF は RIB に関連付けられており、この情報が転送情報ベース（FIB）によって収集されます。

ルーティングの詳細については、以下のドキュメントを参照してください。

- 『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』
- 『*Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide*』

トラブルシューティング ルートの初期チェックリスト

最初に次の項目を確認することで、ルーティングの問題をトラブルシューティングできます。

チェックリスト	Done
ルーティング プロトコルが有効になっていることを確認します。	
必要に応じて、アドレス ファミリが設定されていることを確認します。	
ルーティング プロトコルに適切な VRF が設定されていることを確認します。	

ルーティング情報を表示するには、次のコマンドを使用します。

- **show ip arp**
- **show ip traffic**
- **show ip static-route**
- **show ip client**
- **show ip fib**
- **show ip process**
- **show ip route**
- **show vrf**
- **show vrf interface**

ルーティングのトラブルシューティング

手順の概要

1. switch# **show ospf**
2. switch# **show running-config eigrp all**
3. switch# **show running-config eigrp**
4. switch# **show processes memory** | **include isis**
5. switch# **show ip client pim**
6. switch# **show ip interface** *loopback-interface*
7. switch# **show vrf interface** *loopback -interface*
8. switch# **show routing unicast clients**
9. switch# **show forwarding distribution multicast client**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	switch# **show ospf**
	例：
	`switch# show ospf`
	`                    ^`
	`% invalid command detected at '^' marker.`
		ルーティング プロトコルが有効になっていることを確認します。
		この機能が有効になっていない場合は、Cisco NX-OS によりコマンドが無効であると報告されます。

ステップ 2	switch# **show running-config eigrp all** 例： `switch# show running-config eigrp all`	このルーティング プロトコルの設定を確認します。
ステップ 3	switch# **show running-config eigrp** 例：	このルーティング プロトコルの VRF 設定を確認します。

	コマンドまたはアクション	目的

	`switch# show running-config eigrp`
	`version 6.1(2)I1(1)`
	`feature eigrp`
	`router eigrp 99`
	`  address-family ipv4 unicast`
	`    router-id 192.0.2.1`
	`  vrf red`
	`    stub`	

ステップ 4	switch# **show processes memory | include isis**
	例：
	`switch# show processes memory | include isis`
	` 8913   9293824  bffff1d0/bffff0d0  isis`
	`32243   8609792  bfffe0c0/bfffdfc0  isis`
		このルーティング プロトコルのメモリ使用率をチェックします。

ステップ 5	switch# **show ip client pim**
	例：
	`switch# show ip client pim`
	`  Client: pim, uuid: 284, pid: 3839, extended pid: 3839`
	`  Protocol: 103, client-index: 10, routing VRF id: 255`
	`  Data MTS-SAP: 1519`
	`  Data messages, send successful: 2135, failed: 0`
		ルーティングプロトコルがパケットを受信していることを確認します。

ステップ 6	switch# **show ip interface** *loopback-interface*
	例：
	`switch# show ip interface loopback0`
	`loopback0, Interface status: protocol-up/link-up/admin-up, iod: 36, Context:"default"`
	`  IP address: 1.0.0.1, IP subnet: 1.0.0.0/24`
	`  ...`
	`  IP multicast groups locally joined:`
	`  224.0.0.2  224.0.0.1  224.0.0.13`
	`  ...`
		インターフェイスでルーティング プロトコルが有効になっていることを確認します。

ステップ 7	switch# **show vrf interface** *loopback -interface*
	例：
	`switch# show vrf interface loopback 99`
	`Interface  VRF-Name  VRF-ID`
	`loopback99  default  1`
		インターフェイスが正しいVRFにあることを確認します。

ステップ 8	switch# **show routing unicast clients** **例**： `switch# show routing unicast clients`	ルーティング プロトコルがRIBに登録されていることを確認します。
ステップ 9	switch# **show forwarding distribution multicast client** **例**：	RIB が転送プレーンと通信していることを確認します。

	コマンドまたはアクション	目的
	switch# show forwarding distribution multicast client Number of Clients Registered: 3 Client-name Client-id Shared Memory Name igmp 1 N/A mrib 2 /procket/shm/mrib-mfdm	

例

次に、EIGRP ルーティング プロトコル設定を表示する例を示します。

```
switch# show running-config eigrp all
version 6.1(2)I1(1)
feature eigrp
router eigrp 99
log-neighbor-warnings
  log-neighbor-changes
  log-adjacency-changes
  graceful-restart
  nsf
  timers nsf signal 20
  distance 90 170
  metric weights 0 1 0 1 0 0
  metric maximum-hops 100
  default-metric 100000 100 255 1 1500
  maximum-paths 16
  address-family ipv4 unicast
    log-neighbor-warnings
    log-neighbor-changes
    log-adjacency-changes
    graceful-restart
    router-id 192.0.2.1
    nsf
    timers nsf signal 20
    distance 90 170
    metric weights 0 1 0 1 0 0
    metric maximum-hops 100
    default-metric 100000 100 255 1 1500
    maximum-paths 16
```

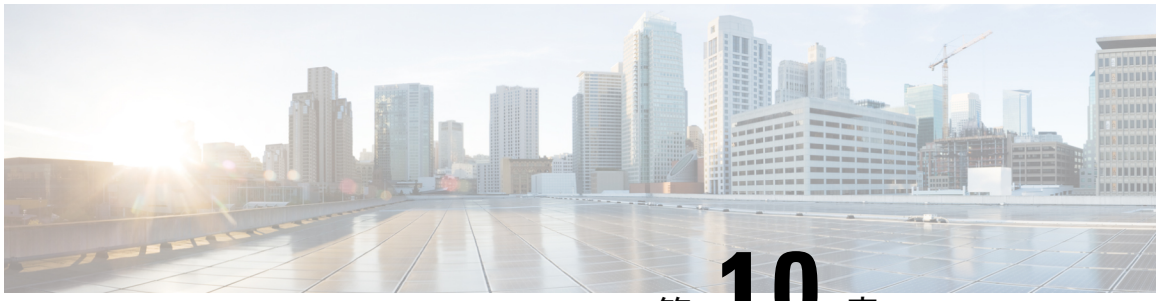
次に、ユニキャスト ルーティング プロトコルが RIB に登録されていることを表示する例を示します。

```
switch# show routing unicast clients
CLIENT: am
 index mask: 0x00000002
 epid: 3908      MTS SAP: 252       MRU cache hits/misses:        2/1
 Routing Instances:
  VRF: management        table: base
 Messages received:
  Register          : 1      Add-route         : 2      Delete-route      : 1
 Messages sent:
  Add-route-ack     : 2      Delete-route-ack  : 1
CLIENT: rpm
 index mask: 0x00000004
```

```
 epid: 4132      MTS SAP: 348       MRU cache hits/misses:        0/0
 Messages received:
  Register          : 1
 Messages sent:
...
CLIENT: eigrp-99
 index mask: 0x00002000
 epid: 3148      MTS SAP: 63775     MRU cache hits/misses:        0/1
 Routing Instances:
  VRF: default           table: base                notifiers: self
 Messages received:
  Register          : 1      Delete-all-routes : 1
 Messages sent:
...
```

ポリシーベースルーティングのトラブルシューティング

- ACL が着信トラフィックと一致することを確認します。
- ルートが使用可能であることを確認します。
  - IP ネットワーク ルートの場合は、**show ip route** を使用します コマンドを使用して、**set ip next-hop** で指定されたネクスト ホップで IP ネットワーク ルートが使用可能であることを確認します コマンドを使用する必要があります。
  - IP ホストルートの場合は、**show ip arp** を使用します コマンドを使用して、**set ip next-hop** で指定されたネクスト ホップで IP ホスト ルートが使用可能であることを確認します コマンドを使用する必要があります。
  - IPv6 ネットワーク ルートの場合は、**show ipv6 route** を使用します コマンドを使用して、**set ipv6 next-hop** で指定されたネクスト ホップで IPv6 ネットワーク ルートが使用可能であることを確認します コマンドを使用する必要があります。
  - IPv6 ホスト ルートの場合は、**show ipv6 neighbor** を使用します コマンドを使用して、**set ipv6 next-hop** で指定されたネクスト ホップで IPv6 ホスト ルートが使用可能であることを確認します コマンドを使用する必要があります。
- ポリシーがシステムでアクティブになっていることを確認します（**show ip policy** を使用 コマンドを通して）。
- エントリの統計情報を確認します（**show route-map** *map-name* **pbr-statistics** を使用 コマンドを通して）。



第 10 章

メモリのトラブルシューティング

- メモリのトラブルシューティングに関する詳細情報 （91 ページ）
- プラットフォーム メモリ使用率の一般/高レベルの評価 （92 ページ）
- ユーザ プロセス （93 ページ）
- 組み込みプラットフォームのメモリモニタリング （93 ページ）

メモリのトラブルシューティングに関する詳細情報

ダイナミック ランダム アクセス メモリ（DRAM）は、すべてのプラットフォームで限られたリソースであり、使用率がチェックされるように制御またはモニタする必要があります。

Cisco NX-OS は、次の 3 つの方法でメモリを使用します。

- **Page cache**：永続ストレージ（CompactFlash）からファイルにアクセスすると、カーネルはデータをページキャッシュに読み取ります。これは、将来データにアクセスするときに、ディスク ストレージに関連する遅いアクセス時間を回避できることを意味します。他のプロセスがメモリを必要とする場合、キャッシュされたページはカーネルによって解放されます。一部のファイル システム（tmpfs）は、純粋にページ キャッシュ内に存在します（たとえば、/dev/sh, /var/sysmgr, /var/tmp）。これは、このデータの永続的なストレージがなく、データが削除されたときを意味します。ページ キャッシュからは復元できません。 tmpfs-cached ファイルは、削除された場合にのみページキャッシュされたページを解放します。

- **Kernel**：カーネルには、独自のテキスト、データ、およびカーネルロード可能モジュール（KLM）を保存するためのメモリが必要です。KLM は、（個別のユーザ プロセスではなく）カーネルにロードされるコードの一部です。カーネル メモリの使用例として、インバンド ポート ドライバがパケットを受信するためにメモリを割り当てる場合があります。

- **User processes**Cisco NX-OS：このメモリは、カーネルに統合されていない Linux プロセス（テキスト、スタック、ヒープなど）によって使用されます。

高いメモリ使用率をトラブルシューティングする場合は、まず使用率の高いタイプ（プロセス、ページキャッシュ、またはカーネル）を判別する必要があります。使用率のタイプを特定したら、追加のトラブルシューティング コマンドを使用して、この動作の原因となっているコンポーネントを特定できます。

プラットフォーム メモリ使用率の一般/高レベルの評価

次の2つの基本的なCLIコマンドを使用して、プラットフォームのメモリ使用率の全体的なレベルを評価できます。 **show system resources**および **show processes memory**.

（注） これらのコマンド出力から、プラットフォームの使用率が通常/予想よりも高いことがわかりますが、どのタイプのメモリ使用率が高いかはわかりません。

（注） *show system resources* コマンドの出力に空きメモリの減少が示されている場合は、Linux カーネルキャッシングが原因である可能性があります。システムがより多くのメモリを必要とするたびに、Linux カーネルはキャッシュされたメモリを解放します。*show system internal kernel meminfo* コマンドは、システムのキャッシュ メモリを表示します。

この項で説明している **show system resources** コマンドは、プラットフォームのメモリ統計情報を表示します。

```
switch# show system resources
Load average:   1 minute: 0.70   5 minutes: 0.89   15 minutes: 0.88
Processes   :   805 total, 1 running
CPU states  :   7.06% user,   5.49% kernel,   87.43% idle
                  CPU0 states  :   9.67% user,   6.45% kernel,   83.87% idle
                  CPU1 states  :   10.41% user,   7.29% kernel,   82.29% idle
                  CPU2 states  :   5.20% user,   4.16% kernel,   90.62% idle
                  CPU3 states  :   5.15% user,   2.06% kernel,   92.78% idle
Memory usage:   16399900K total,   6557936K used,   9841964K free
Kernel vmalloc:   36168240K total,   18446744039385981489K free     >>>>>>>>>>>>
Kernel buffers:   10860132K Used>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>.>>>>>>>
Kernel cached :   120072K Used >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>> seeing these extra
 logs
Current memory status: OK
```

（注） この出力は、/proc/meminfo の Linux メモリ統計情報から取得されます。

- **total**：プラットフォーム上の物理 RAM の量。
- **free**：未使用または使用可能なメモリの量。
- **used**：割り当てられた（永続的な）メモリとキャッシュされた（一時的な）メモリの量。

キャッシュとバッファは、カスタマー モニタリングには関係ありません。

この情報は、プラットフォームの使用率の一般的な表現のみを提供します。メモリ使用率が高い理由をトラブルシューティングするには、より多くの情報が必要です。

show processes memory コマンドは、プロセスごとのメモリ割り当てを表示します。

```
switch# show processes memory
Load average: 1 minute: 0.43 5 minutes: 0.30 15 minutes: 0.28
Processes : 884 total, 1 running
CPU states : 2.0% user, 1.5% kernel, 96.5% idle
PID  MemAlloc MemLimit  MemUsed   StackBase/Ptr     Process
---- -------- --------- --------- ----------------- ----------------
4662 52756480 562929945 150167552 bfffdf00/bfffd970 netstack
```

ユーザ プロセス

ページキャッシュとカーネルの問題が除外されている場合は、一部のユーザプロセスが大量のメモリを使用しているか、実行中のプロセス数が多いため（使用可能な機能の数が多いため）、使用率が高くなっているという可能性があります。

（注） Cisco NX-OS は、ほとんどのプロセスのメモリ制限を定義しています（rlimit）。この rlimit を超えると、sysmgr によってプロセスがクラッシュし、通常はコアファイルが生成されます。rlimit に近いプロセスは、プラットフォームの使用率に大きな影響を与えない可能性がありますが、クラッシュが発生すると問題になる可能性があります。

大量のメモリを使用しているプロセスの特定

次のコマンドは、特定のプロセスが大量のメモリを使用しているかどうかを確認するのに役立ちます。

- The **show process memory** コマンドは、プロセスごとのメモリ割り当てを表示します。

```
switch# show processes memory
PID   MemAlloc MemLimit   MemUsed    StackBase/Ptr     Process
----- -------- ---------- ---------- ----------------- ---------
4662  52756480 562929945  150167552  bfffdf00/bfffd970 netstack
```

（注） **show process memory** の出力 コマンドの出力は、現在の使用率の完全に正確な図を提供しない可能性があります（割り当てられていることを意味しません）。このコマンドは、プロセスが制限に近づいているかどうかを判断するのに役立ちます。

組み込みプラットフォームのメモリモニタリング

Cisco NX-OS には、システムのハング、プロセスのクラッシュ、およびその他の望ましくない動作を回避するために、カーネルによる、メモリ使用量のモニタリング機構が組み込まれてい

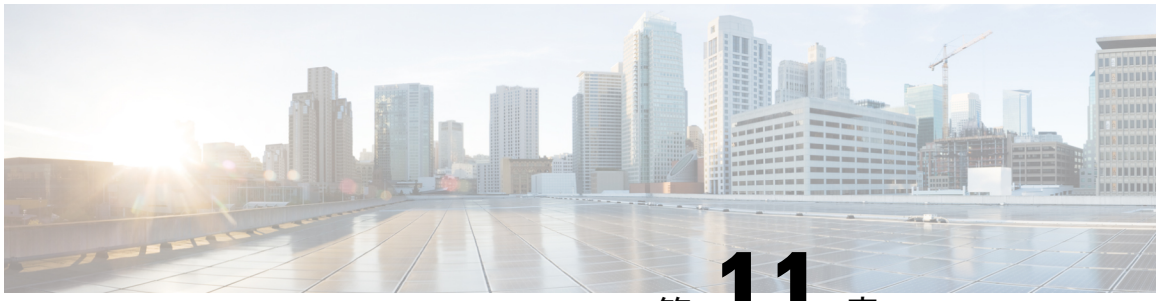
ます。プラットフォームマネージャは、（搭載されているRAMの総量を基準とする）メモリの使用率を定期的にチェックし、使用率が設定されたしきい値を超えると、自動的にアラートイベントを生成します。アラートレベルに達すると、カーネルは不要になったページ（たとえば、アクセスされなくなった永続ファイルのページキャッシュ）を解放することでメモリを解放しようとします。または、クリティカルレベルに達すると、カーネルは、メモリ使用率が最も高いプロセスを強制終了します。Cisco NX-OSの他のコンポーネントには、ボーダーゲートウェイプロトコル（BGP）のグレースフルローメモリハンドリングなどのメモリアラート処理が導入されており、プロセスがそれ自身の動作を調整してメモリの使用率を制御できるようなっています。

メモリしきい値

多くの機能が展開されている場合、ベースラインのメモリでは、次のしきい値が必要です。

- MINOR
- SEVERE
- CRITICAL

デフォルトのしきい値はDRAMサイズに応じて起動時に計算されるため、その値はプラットフォームで使用されているDRAMサイズによって異なります。しきい値は、**system memory-thresholds minor** パーセンテージ **severe** パーセンテージ **critical** パーセンテージを使用して設定できます。 コマンドを使用する必要があります。



第 11 章

パケット フローの問題のトラブルシューティング

- パケットフローの問題 （95 ページ）

パケットフローの問題

パケットは次の理由でドロップされる可能性があります。

- ソフトウェア スイッチのパケットは、コントロール プレーンのポリシー設定（CoPP）が原因でドロップされる可能性があります。
- ハードウェア スイッチのパケットは、帯域幅の制限により、ハードウェアによってドロップされる可能性があります。

レート制限によってドロップされたパケット

show hardware rate-limit コマンドを使用し、 レート制限のためにパケットがドロップされているかどうかを確認します。

```
switch(config)# show hardware rate-limit module 1

Units for Config: packets per second
Allowed, Dropped & Total: aggregated since last clear counters

Rate Limiter Class                          Parameters
-----------------------------------------------------------------
access-list-log                           Config    : 100
                                          Allowed   : 0
                                          Dropped   : 0
                                          Total     : 0
```

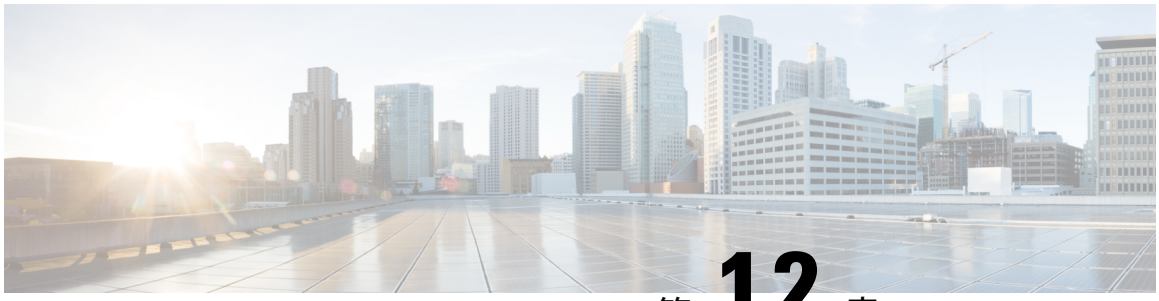
CoPP のためにドロップされたパケット

show policy-map interface control-plane コマンドを使用し、 コマンドを使用して、パケットが CoPP によってドロップされているかどうかを確認します。

```
switch# show policy-map interface control-plane
   class-map copp-system-p-class-exception (match-any)
      match exception ip option
      match exception ip icmp unreachable
      match exception ttl-failure
      match exception ipv6 option
      match exception ipv6 icmp unreachable
      match exception mtu-failure
      set cos 1
      police cir 200 pps , bc 32 packets

      module 27 :
        transmitted 0 packets;
        dropped 0 packets;

      module 28 :
        transmitted 0 packets;
        dropped 0 packets;
```



第 12 章

PowerOn 自動プロビジョニングのトラブルシューティング

- POAP が完了するはずの時間内にスイッチが起動しない （97 ページ）
- POAP が失敗する （97 ページ）

POAP が完了するはずの時間内にスイッチが起動しない

POAP が完了するのに十分な時間が経過してもスイッチが起動しない場合は、シリアル回線を介してスイッチに接続し、次のプロンプトの箇所で停止してしまっているか確認します。

```
Waiting for system online status before starting POAP ...
Waiting for system online status before starting POAP ...
Waiting for system online status before starting POAP ...

System is not fully online. Skip POAP? (yes/no)[n]:
```

プロンプトで **no** と入力すると、POAPを続行できます。そのようにしても 2 回目の試行で POAP が正常に起動しない場合は、復帰時にプロンプトで**yes** と入力して、通常のセットアップを続行します。

POAP が失敗する

PowerOn Auto Provisioning（POAP）が何らかの理由で失敗した場合は、次のアクションを実行します。

- 通常のスイッチの起動手順を続行するには、POAP プロセスを停止します。POAP が完全に停止するまでに数分かかることがありますので、しばらくお待ちください。

```
2013 Oct 29 22:24:59 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: Assigned IP address:
172.23.40.221
2013 Oct 29 22:24:59 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: Netmask: 255.255.255.0
2013 Oct 29 22:24:59 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: DNS Server: 172.21.157.5
2013 Oct 29 22:24:59 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: Default Gateway: 172.23.40.1
2013 Oct 29 22:24:59 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: Script Server: 172.23.40.6
2013 Oct 29 22:24:59 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: Script Name: /pxelinux.0
2013 Oct 29 22:25:09 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: The POAP Script download
```

```
 has started
2013 Oct 29 22:25:09 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: The POAP Script is being
 downloaded from [copy tftp://172.23.40.6//pxelinux.0 bootflash:scripts/script.sh
vrf management ]
2013 Oct 29 22:25:10 switch %$ VDC-1 %$ %POAP-2-POAP_FAILURE: POAP boot file download
 failed.
2013 Oct 29 22:25:10 switch %$ VDC-1 %$ %POAP-2-POAP_FAILURE: POAP DHCP discover
phase failed
2013 Oct 29 22:25:12 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: Abort Power On Auto
Provisioning and continue with normal setup ?(yes/no)[n]:
2013 Oct 29 22:25:46 switch %$ VDC-1 %$ %POAP-2-POAP_DHCP_DISCOVER_START: POAP DHCP
 Discover phase started
2013 Oct 29 22:25:46 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: Abort Power On Auto
Provisioning and continue with normal setup ?(yes/no)[n]:

Abort Auto Provisioning and continue with normal setup ?(yes/no)[n]: yes
```

- ログファイルで失敗の理由を確認します。2つのPOAPログファイルがブートフラッシュに保存されます。POAPプロセスからのログは、次に示すように、poap_*pid*_init.logで終わるファイルに保存されます。失敗の理由は、このファイルの末尾に表示されます。

```
bash-4.2# tail 20131029_222312_poap_5367_init.log -n 3
Tue Oct 29 22:27:41 2013:poap_net_rx_pkt: Droppping the pakcet due to Ethernet
hdrparsing error on if_index - 5000000
Tue Oct 29 22:27:41 2013:DEST IP is not Broadcast
Tue Oct 29 22:27:41 2013:poap_net_rx_pkt: Droppping the pakcet due to Ethernet
hdrparsing error on if_index - 5000000
```

- DHCP または TFTP サーバからダウンロードされた POAP スクリプト ファイルが実行プロセスで失敗するかどうかを確認します。障害の段階に応じて、デバイスは通常のセットアップまたはリブートを続行できます。

```
2013 Oct 29 22:42:34 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: Assigned IP address:
172.23.40.181
2013 Oct 29 22:42:34 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: Netmask: 255.255.255.0
2013 Oct 29 22:42:34 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: DNS Server: 172.21.157.5
2013 Oct 29 22:42:34 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: Default Gateway: 172.23.40.1
2013 Oct 29 22:42:34 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: Script Server: 172.23.40.6
2013 Oct 29 22:42:34 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: Script Name: poap.py
2013 Oct 29 22:42:45 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: The POAP Script download
 has started
2013 Oct 29 22:42:45 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: The POAP Script is being
 downloaded from [copy tftp://172.23.40.6/poap.py bootflash:scripts/script.sh vrf
management ]
2013 Oct 29 22:42:46 switch %$ VDC-1 %$ %POAP-2-POAP_SCRIPT_DOWNLOADED: Successfully
 downloaded POAP script file
2013 Oct 29 22:42:46 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: Script file size 21965,
MD5 checksum 1bd4b86892439c5785a20a3e3ac2b0de
2013 Oct 29 22:42:46 switch %$ VDC-1 %$ %POAP-2-POAP_SCRIPT_STARTED_MD5_NOT_VALIDATED:
 POAP script execution started(MD5 not validated)
2013 Oct 29 22:47:57 switch %$ VDC-1 %$ %POAP-2-POAP_FAILURE: POAP script execution
 aborted
```

- POAPスクリプトファイルのログは、ブートラッシュ方式でファイルに書き込まれます。ファイル名は poap.log で始まります。複数のファイル ログがある場合は、最新のタイムスタンプを持つログを調べてエラーがないか確認します。

```
bash-4.2# tail poap.log.22_42_46
CLI : show file volatile:poap.cfg.md5.poap_md5 | grep -v '^#' | head lines 1 | sed
```

```
's/ .*$//'
INFO: md5sum 46684d8f8b7c5ffac3b37ac8560928e5 (.md5 file)
CLI : show file volatile:poap.cfg md5sum
INFO: md5sum 46684d8f8b7c5ffac3b37ac8560928e5 (recalculated)

CLI : config terminal ; boot nxos bootflash:poap/system.img
CLI : copy running-config startup-config
CLI : copy volatile:poap.cfg scheduled-config
INFO: Configuration successful
```

第 13 章

Python API のトラブルシューティング

• Python API エラーの受信 （101 ページ）

Python API エラーの受信

次のいずれかの Python API エラーが表示された場合は、次のアクションを実行します。

症状	解決方法	例

Python cli API は NameError をスローします。	グローバル名前空間に cli モジュールをインポートします。	`>>> cli('show clock')`
		`Traceback (most recent call last):`
		`  File "<stdin>", line 1, in <module>`
		`NameError: name 'cli' is not defined`
		
		`>>> from cli import *`
		`>>> cli('show clock')`
		`'20:23:33.967 UTC Fri Nov 01 2013\n'`

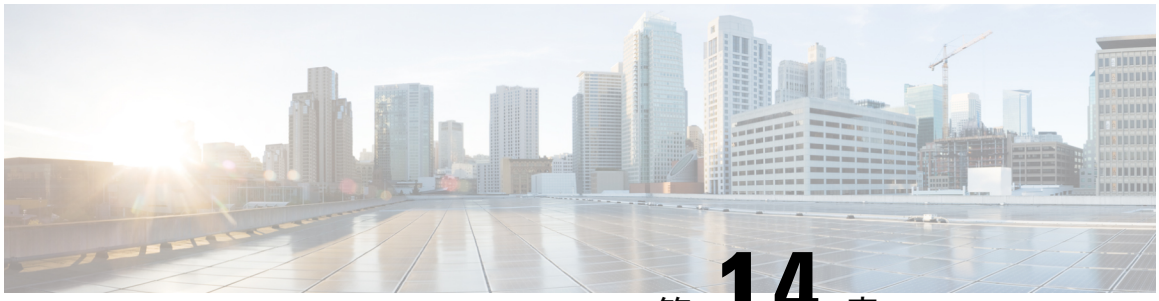
Python clid API は、structured_output_not_supported_error をスローします。	CLI またはクリップ API を使用します。clid API は、構造化データ出力をサポートするコマンドでのみ動作します。	`>>> clid('show clock')`
		`Traceback (most recent call last):`
		`  File "<stdin>", line 1, in <module>`
		`  File "/isan/python/scripts/cli.py", line 45, in clid`
		`  raise structured_output_not_supported_error(cmd)`
		`errors.structured_output_not_supported_error: 'show clock'`

症状	解決方法	例

CLI API および Cisco オブジェクトは、Permission denied エラーをスローします。	ログインIDに、コマンドまたはリソースにアクセスするための十分な権限があることを確認します。必要に応じて、ネットワーク管理者に権限を追加してもらいます。	`>>> from cli import *`
		`>>> cli('clear counters')`
		`Traceback (most recent call last):`
		`  File "<stdin>", line 1, in <module>`
		`  File "/isan/python/scripts/cli.py", line 20, in cli`
		`  raise cmd_exec_error(msg)`
		`errors.cmd_exec_error: '% Permission denied for the role\n\nCmd exec error.\n'`
		`>>> from cisco.interface import *`
		`>>> i=Interface('Ethernet3/2')`
		`Traceback (most recent call last):`
		`  File "<stdin>", line 1, in <module>`
		`  File "/isan/python/scripts/cisco/interface.py", line 75, in __new__`
		`  cls._Interfaces[name].config(True)`
		`  File "/isan/python/scripts/cisco/interface.py", line 91, in config`
		`  s, o = nxcli('show runn interface %s' % self.name)`
		`  File "/isan/python/scripts/cisco/nxcli.py", line 46, in nxcli`
		`  raise SyntaxError, 'Error status %d\n%s' % (status, output)`
		`SyntaxError: Error status 30`
		`% Permission denied for the role`
		
		`Cmd exec error.`
		
		`>>> import os`
		`>>> os.system('whoami')`
		`test`

症状	解決方法	例

urllib2 またはソケット接続は処理されません。	正しい仮想ルーティングコンテキストを使用していることを確認します。そうでない場合は、正しいものに切り替えます。	>>> import urllib2
		>>>
		u=urllib2('http://172.23.40.211:8000/welcome.html')
		Traceback (most recent call last):
		File "<stdin>", line 1, in <module>
		TypeError: 'module' object is not callable
		>>>
		u=urllib2.urlopen('http://172.23.40.211:8000/welcome.html')
		Traceback (most recent call last):
		File "<stdin>", line 1, in <module>
		File "/isan/python/python2.7/urllib2.py", line 127, in urlopen
		return _opener.open(url, data, timeout)
		File "/isan/python/python2.7/urllib2.py", line 404, in open
		response = self._open(req, data)
		File "/isan/python/python2.7/urllib2.py", line 422, in _open
		'_open', req)
		File "/isan/python/python2.7/urllib2.py", line 382, in _call_chain
		result = func(*args)
		File "/isan/python/python2.7/urllib2.py", line 1214, in http_open
		return
		self.do_open(httplib.HTTPConnection, req)
		File "/isan/python/python2.7/urllib2.py", line 1184, in do_open
		raise URLError(err)
		urllib2.URLError: <urlopen error [Errno 113]
		No route to host>
		>>> from cisco.vrf import *
		>>> VRF.get_vrf_name_by_id(get_global_vrf())
		'default'



第 14 章

NX-API のトラブルシューティング

- NX-API のガイドライン （105 ページ）
- NX-API が応答しない （105 ページ）
- 設定が失敗します （106 ページ）
- Bash に対する許可が拒否される （106 ページ）
- ブラウザ サンドボックスから出力を取得できない （106 ページ）
- CLI コマンド エラーが表示される （107 ページ）
- エラーメッセージが表示される （107 ページ）
- 一時ファイルが消える （107 ページ）
- コマンド出力のチャンクが配信されない （107 ページ）

NX-API のガイドライン

NX-API は、スイッチ上の Programmable Authentication Module（PAM）を使用して認証を行います。cookie を使用して PAM の認証数を減らし、PAM の負荷を減らします。

NX-API が応答しない

NX-API が応答しない場合は、次のアクションを実行します。

- **show feature | grep nxapi** コマンドを使用して、NX-API が有効になっていることを確認します。
- **show nxapi** コマンドを使用して、HTTP または HTTPs が有効になっていることを確認します。
- **show nxapi** コマンドを使用して、NX-API が予期されるポートでリッスンしていることを確認します。
- 長時間実行されているコマンドを確認します。現在、NX-API は単一のワーカー プロセスで実行され、シングル スレッドです。1 つのコマンドの完了に時間がかかると、他のコマンドがブロックされます。NX-API は要求をキャッシュします。現在の要求が完了すると、他の要求が処理されます。

- Bash を有効にします。手順詳細については、『*Cisco Nexus 9000 Series NX-OS Programmability Guide*』を参照してください。
- /var/sysmgr_nxapi/logs/error.log でエラーがないか確認します。
- NX-API がまだ応答しない場合は、**no feature nxapi** を入力します および **feature nxapi** NX-API を再起動します。NX-API はステートレスであり、再起動しても安全です。

設定が失敗します

ユーザがコンフィギュレーション コマンドを実行できない場合は、次のアクションを実行します。

- ユーザにコマンドを実行するための正しい権限があることを確認します。

Bash に対する許可が拒否される

ユーザが Bash の「許可が拒否される（Permission Denied）」メッセージを受信した場合は、次のアクションを実行します。

- **show feature | grep bash** を使用して Bash が有効になっていることを確認します コマンドを実行してください。
- 現在のユーザが Bash にアクセスするための正しい権限を持っていることを確認します。
- Bash の詳細については、『*Cisco Nexus 9000 Series NX-OS Programmability Guide*』を参照してください。

ブラウザ サンドボックスから出力を取得できない

ブラウザ サンドボックスから出力を取得できない場合は、次のアクションを実行します。

- 出力が大きい場合やコマンドの実行に時間がかかる場合は、ブラウザがロードを処理できず、タイムアウトする可能性があります。Python クライアントを使用して NX-API にアクセスしてみてください。手順詳細については、『*Cisco Nexus 9000 Series NX-OS Programmability Guide*』を参照してください。

（注） 推奨されるブラウザは Mozilla Firefox です。

CLI コマンド エラーが表示される

ユーザが複数のコマンドを実行したときにCLI コマンドエラーが表示される場合は、次のアクションを実行します。

- 複数のコマンドがどのように区切られているかを確認します。show コマンドと configure コマンドは [スペース] で区切る必要があります。Bash コマンドはセミコロン（;）で区切る必要があります。

エラーメッセージが表示される

エラーメッセージが出力に表示される場合は、次のアクションを実行します。

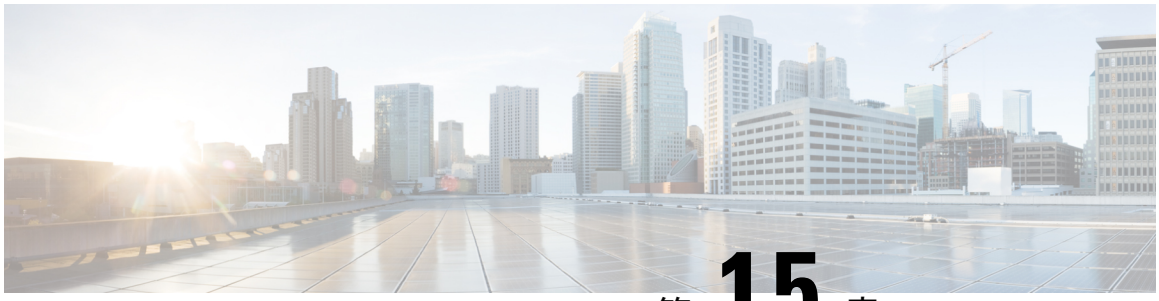
- エラー メッセージの手順に従ってください。
- Bash コマンドが実行されない場合は、Bash が有効になっているか確認するために、**show feature | grep bash** コマンドを実行してください。Bash の詳細については、『*Cisco Nexus 9000 Series NX-OS Programmability Guide*』を参照してください。
- ユーザにコマンドを実行するための正しい権限があることを確認します。
- NX-API が応答しない （105 ページ）の指示に従って操作します。

一時ファイルが消える

リクエストごとに、一時ファイルが /volatile に作成され、クライアントに返されるコマンド出力が保存されます。要求のチャンク パラメータが 0 の場合、コマンド出力がクライアントに送り返される直前にファイルは削除されます。要求のチャンクが 1 の場合、チャンクを抽出してクライアントに送信できるようにファイルは保持されます。そのファイルは定期的にクリーンアップされます。現在、このクリーンアップは 100 リクエストごとに実行されるように設定されています。ファイルは、作成後 60 秒以内にアクセスされなかった場合、または 600 秒以内に変更されなかった、またはステータスが更新されなかった場合にクリーンアップされます。

コマンド出力のチャンクが配信されない

チャンク =1 の要求では、sid が同じ値に設定されている場合、コマンド出力の同じチャンクが取得されます。この機能は、クライアントが特定のチャンクを要求し、ネットワーク内のどこかでドロップまたはブロックされたために、タイムリーに受信しない状況に対応します。クライアントは同じチャンクを再度要求でき、一時ファイルがクリーンアップされていない限り、正しいデータを受信します（一時ファイルが消える （107 ページ） を参照）。



第 15 章

サーバ障害のトラブルシューティング

- プロセスのメモリ割り当ての特定 （109 ページ）
- プロセスの CPU 使用率の特定 （110 ページ）
- モニタリング プロセスのコア ファイル （111 ページ）
- クラッシュ コア ファイルの処理 （111 ページ）
- コアのクリア （112 ページ）
- コア ファイルの自動コピーのイネーブル化 （112 ページ）

プロセスのメモリ割り当ての特定

メモリ内の各プロセスの割り当て、制限、メモリ割り当て、および使用状況を特定できます。次は **show processes memory** コマンドからの出力例です。この出力は、例を簡潔にするために省略されています。

```
switch# show processes memory
 PID  MemAlloc MemLimit    MemUsed     StackBase/Ptr      Process
 ---- -------- --------    -------     -----------------  -----------
   1    159744  0           2027520     ff808d30/ffffffff  init
   2         0  0                 0                 0/0  kthreadd
   3         0  0                 0                 0/0  migration/0
   4         0  0                 0                 0/0  ksoftirqd/0
   5         0  0                 0                 0/0  watchdog/0
   6         0  0                 0                 0/0  migration/1
   7         0  0                 0                 0/0  ksoftirqd/1
   8         0  0                 0                 0/0  watchdog/1
   9         0  0                 0                 0/0  migration/2
  10         0  0                 0                 0/0  ksoftirqd/2
  11         0  0                 0                 0/0  watchdog/2
  12         0  0                 0                 0/0  migration/3
  13         0  0                 0                 0/0  ksoftirqd/3
  14         0  0                 0                 0/0  watchdog/3
  15         0  0                 0                 0/0  migration/4
  16         0  0                 0                 0/0  ksoftirqd/4
  17         0  0                 0                 0/0  watchdog/4
  18         0  0                 0                 0/0  migration/5
  19         0  0                 0                 0/0  ksoftirqd/5
  20         0  0                 0                 0/0  watchdog/5
  21         0  0                 0                 0/0  migration/6
  22         0  0                 0                 0/0  ksoftirqd/6
  23         0  0                 0                 0/0  watchdog/6
  24         0  0                 0                 0/0  migration/7
```

```
  25         0  0                0                0/0  ksoftirqd/7
  26         0  0                0                0/0  watchdog/7
  27         0  0                0                0/0  events/0
  28         0  0                0                0/0  events/1
  29         0  0                0                0/0  events/2
  30         0  0                0                0/0  events/3
  31         0  0                0                0/0  events/4
  32         0  0                0                0/0  events/5
  33         0  0                0                0/0  events/6
  34         0  0                0                0/0  events/7
  35         0  0                0                0/0  khelper
  36         0  0                0                0/0  netns
  37         0  0                0                0/0  kblockd/0
```

この項で説明している **show processes memory** コマンドには、次のキーワードが含まれます。

キーワード	説明
>	出力をファイルにリダイレクトします。
>>	出力が既存のファイルに追加されます。
shared	共有メモリ情報を表示します。

プロセスの CPU 使用率の特定

メモリ内で実行中のプロセスの CPU 使用率を特定できます。次は **show processes cpu** コマンドからの出力例です。この出力は、例を簡潔にするために省略されています。

```
switch# show processes cpu

CPU utilization for five seconds: 0%/0%; one minute: 1%; five minutes: 2%

   PID    Runtime(ms) Invoked   uSecs 5Sec    1Min   5Min    TTY  Process
   ---    ------------------   ----- -----   -----  -----   ---  -----------
   1        28660     405831     70   0.00%   0.00%  0.00%   -    init
   2           21       1185     18   0.00%   0.00%  0.00%   -    kthreadd
   3          468      36439     12   0.00%   0.00%  0.00%   -    migration/0
   4        79725    8804385      9   0.00%   0.00%  0.00%   -    ksoftirqd/0
   5            0          4     65   0.00%   0.00%  0.00%   -    watchdog/0
   6          472      35942     13   0.00%   0.00%  0.00%   -    migration/1
   7        33967     953376     35   0.00%   0.00%  0.00%   -    ksoftirqd/1
   8            0         11      3   0.00%   0.00%  0.00%   -    watchdog/1
   9          424      35558     11   0.00%   0.00%  0.00%   -    migration/2
  10        58084    7683251      7   0.00%   0.00%  0.00%   -    ksoftirqd/2
  11            0          3      1   0.00%   0.00%  0.00%   -    watchdog/2
  12          381      29760     12   0.00%   0.00%  0.00%   -    migration/3
  13        17258     265884     64   0.00%   0.00%  0.00%   -    ksoftirqd/3
  14            0          2      0   0.00%   0.00%  0.00%   -    watchdog/3
  15        46558    1300598     35   0.00%   0.00%  0.00%   -    migration/4
  16      1332913    4354439    306   0.00%   0.00%  0.00%   -    ksoftirqd/4
  17            0          6      2   0.00%   0.00%  0.00%   -    watchdog/4
  18        45808    1283581     35   0.00%   0.00%  0.00%   -    migration/5
  19       981030    1973423    497   0.00%   0.00%  0.00%   -    ksoftirqd/5
  20            0         16      3   0.00%   0.00%  0.00%   -    watchdog/5
  21        48019    1334683     35   0.00%   0.00%  0.00%   -    migration/6
```

```
  22      1084448   2520990    430   0.00%   0.00%  0.00%   -    ksoftirqd/6
  23            0        31      3   0.00%   0.00%  0.00%   -    watchdog/6
  24        46490   1306203     35   0.00%   0.00%  0.00%   -    migration/7
  25      1187547   2867126    414   0.00%   0.00%  0.00%   -    ksoftirqd/7
  26            0        16      3   0.00%   0.00%  0.00%   -    watchdog/7
  27        21249   2024626     10   0.00%   0.00%  0.00%   -    events/0
  28         8503   1990090      4   0.00%   0.00%  0.00%   -    events/1
  29        11675   1993684      5   0.00%   0.00%  0.00%   -    events/2
  30         9090   1973913      4   0.00%   0.00%  0.00%   -    events/3
  31        74118   2956999     25   0.00%   0.00%  0.00%   -    events/4
  32        76281   2837641     26   0.00%   0.00%  0.00%   -    events/5
  33       129651   3874436     33   0.00%   0.00%  0.00%   -    events/6
  34         8864   2077714      4   0.00%   0.00%  0.00%   -    events/7
  35            0         8     23   0.00%   0.00%  0.00%   -    khelper
  36          234        34   6884   0.00%   0.00%  0.00%   -    netns
```

show processes cpu コマンドには、次のキーワードが含まれています。

キーワード	説明
>	出力をファイルにリダイレクトします。
>>	出力が既存のファイルに追加されます。
history	CPU の使用状況に関する情報を表示します。
sort	メモリ使用量に基づいてリストをソートします。

モニタリング プロセスのコア ファイル

show cores を使用してプロセス コア ファイルをモニタできます。 コマンドを使用する必要があります。

```
switch# show cores
Module  Instance  Process-name     PID       Date(Year-Month-Day Time)
------  --------  ---------------  --------  -------------------------
28      1         bgp-64551        5179      2013-11-08 23:51:26
```

出力には、現在アクティブなスーパーバイザからアップロードできるすべてのコアが表示されます。

クラッシュ コア ファイルの処理

クラッシュ コア ファイルを処理するには、**show processes log** コマンドを使用します。

```
switch# show process log
  Process            PID     Normal-exit  Stack-trace  Core     Log-create-time
  -----------------  ------  -----------  -----------  -------  ---------------
  ntp                919               N            N        N  Jun 27 04:08
  snsm               972               N            Y        N  Jun 24 20:50
```

コアのクリア

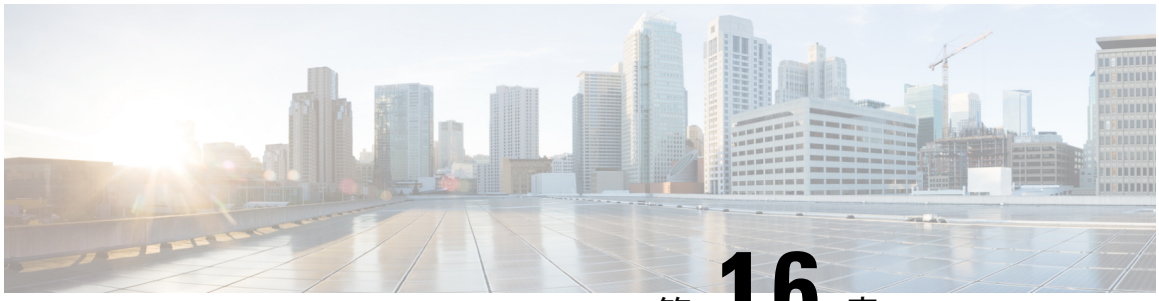
clear cores を使用してコアをクリアできます。 コマンドを使用します。

```
switch# clear cores
```

コア ファイルの自動コピーのイネーブル化

システム コアを入力できます。 コマンドを使用して、TFTP サーバ、フラッシュ ドライブ、またはファイルへのコア ファイルの自動コピーを有効にします。

```
switch(config)# system cores tftp://10.1.1.1/cores
```



第 16 章

テクニカル サポートへ問い合わせる前の準備

- TAC に連絡する前に実行する手順 （113 ページ）
- Cisco NX-OS から/へのファイルのコピー （115 ページ）
- コア ダンプの使用 （117 ページ）

TAC に連絡する前に実行する手順

追加の支援を受けるために、テクニカルサポート担当者または Cisco TAC への問い合わせが必要になることがあります。この項では、問題の解決にかかる時間を短縮するために、次のレベルのサポートに連絡する前に実行する必要がある手順について概説します。

テクニカル サポート担当者に問い合わせる前に必要な準備を行うには、次の手順に従います。

1. システム情報と設定を収集します。この情報は、問題の解決の前と後に収集する必要があります。この情報を収集するには、次の 3 つの方法のいずれかを実施します。
   - Telnet またはセキュア シェル（SSH）アプリケーションを設定して、画面出力をテキスト ファイルに記録します。**terminal length 0** コマンドを使用し、 それから **show tech-support details** コマンド を使用します。

（注） 特定の **show tech** コマンドが大量のデータを生成し、多くのディスク領域を占有する場合は、圧縮形式で保存できます。次の例を参照してください。

```
bash-4.2# time vsh -c " show tech-support platform-sdk" | gzip
 > /bootflash/pltfm-tech.gz
```

（注） SSH のタイムアウト時間は、tac-pac の生成時間よりも長くする必要があります。そうでないと、VSH ログに % VSHD-2-VSHD_SYSLOG_EOL_ERR エラーが記録されることがあります。理想的には、tac-pac または showtech を収集する前に 0（無限）に設定します。

- Cisco NX-OS Release 9.3(1) 以降では、**show tech-support details** [**space-optimized** | **time-optimized**] コマンドを使用できます。マルチスレッド仮想シェルは、最大 16 のスレッドを同時に実行し、同時に監視できます。space-optimized パラメータは、重複する入力コマンドを削除し、出力を圧縮してメモリ使用率を最適化します。

（注） このコマンドは、RAM が 4 GB 未満のデバイスではサポートされません。

- **tac-pac** *filename* コマンドを使用して、**show tech-support details** コマンドの出力をファイルにリダイレクトし、そのファイルを gzip で圧縮します。

```
switch# tac-pac bootflash://showtech.switch1
```

- ファイル名を指定しなかった場合、volatile:show_tech_out.gz というファイルが Cisco NX-OS により作成されます。Cisco NX-OS から/へのファイルのコピー （115 ページ）の手順を使用して、デバイスからファイルをコピーします。

2. DCNM でエラーが発生した場合は、エラーのスクリーン ショットを撮ります。Windows では、アクティブなウィンドウをキャプチャするには **Alt+PrintScreen** を、デスクトップ全体をキャプチャするには **PrintScreen** を押します。スクリーンショットを新しい Microsoft のペイント（または同様のプログラム）セッションに貼り付けて、ファイルを保存します。
3. メッセージ ログ内で確認したのと全く同じエラー コードを DCNM または CLI からキャプチャするようにします。
   - 最近生成されたメッセージのリストを表示するには、DCNM で **Event Browser** を選択します。
   - メッセージログからエラーをコピーします。これは **show logging logfile** または **show logging last** *number* コマンドを使用し、ログの最後の数行を表示して確認できます。
4. テクニカルサポート担当者に連絡する前に、次の質問に回答してください。
   - どのスイッチまたはポートで問題が発生しているか。
   - ネットワーク内にあるのはどの Cisco NX-OS ソフトウェア、ドライバ バージョン、オペレーティング システム バージョン、ストレージ デバイスのファームウェアか。

- どのようなネットワーク トポロジが使用されているか。（DCNM で **Topology > Save layout** を選択）。
- このイベントの発生前または発生時に環境に変更を加えたか（VLAN、アップグレード、またはモジュールの追加）。
- 同様の設定がされた他のデバイスで、この問題が発生したか。
- 問題の発生したデバイスの接続先はどこか（どのデバイスまたはインターフェイスか）。
- この問題が最初に発生したのはいつか。
- この問題が最後に発生したのはいつか。
- この問題の発生頻度はどの程度か。
- 何台のデバイスでこの問題が発生していたか。
- 問題発生時にキャプチャした出力のトレースまたはデバッグを行ったか。どのようなトラブルシューティングの手順を試みたか。次のどのツールを使用したか（使用した場合）。
  - Ethanalyzer、ローカルまたはリモート SPAN
  - CLI デバッグ コマンド
  - traceroute、ping
  - DCNM ツール

5. 問題がソフトウェアアップグレードの試行に関連している場合は、次の質問に回答してください。
   - Cisco NX-OS の元のバージョンは何であったか。
   - Cisco NX-OS の新しいバージョンは何か。
   - 次のコマンドの出力を収集し、カスタマー サポートの担当者に転送します。
     - **show install all status**
     - **show log nvram**

Cisco NX-OS から/へのファイルのコピー

デバイスとの間でファイルを移動する必要がある場合があります。このようなファイルには、ログ ファイル、設定ファイル、ファームウェア ファイルなどがあります。

Cisco NX-OS は、デバイスとの間のコピーに使用するプロトコルを提供します。デバイスは、常にクライアントとして動作します。つまり、FTP、SCP、TFTP セッションは常に Cisco NX-OS で発生し、ファイルは外部システムにプッシュされるか、外部システムからプルされます。

```
File Server: 172.22.36.10
File to be copied to the switch: /etc/hosts
```

この項で説明している **copy** コマンドは、FTP、SCP、SFTP、および TFTP 転送プロトコルと、ファイルをコピーするためのさまざまなソースをサポートします。

```
switch# copy ?
 bootflash:      Select source filesystem
 core:           Select source filesystem
 debug:          Select source filesystem
 ftp:            Select source filesystem
 http:           Select source filesystem

 licenses        Backup license files
 log:            Select source filesystem
 logflash:       Select source filesystem
 nvram:          Select source filesystem
 running-config  Copy running configuration to destination
 scp:            Select source filesystem
 sftp:           Select source filesystem
 startup-config  Copy startup configuration to destination
 system:         Select source filesystem
 tftp:           Select source filesystem
 usb1:           Select source filesystem
 usb2:           Select source filesystem
 volatile:       Select source filesystem
```

次のように、転送メカニズムとしてセキュア コピー（SCP）を使用できます。

```
scp:[//[username@]server][/path]
```

この例では、ユーザ user1 の /etc/hosts を 172.22.36.10 から hosts.txt にコピーします。

```
switch# copy scp://user1@172.22.36.10/etc/hosts bootflash:hosts.txt
user1@172.22.36.10's password:
hosts 100% |***************************| 2035 00:00
```

次に、スタートアップ設定を SFTP サーバにバックアップする例を示します。

```
switch# copy startup-config sftp://user1@172.22.36.10/test/startup configuration.bak1
Connecting to 172.22.36.10...
User1@172.22.36.10's password:
switch#
```

（注） サーバへのスタートアップ設定のバックアップは、毎日および変更を行う前に実施する必要があります。設定の保存およびバックアップを行う短いスクリプトを記述して、Cisco NX-OS 上で実行することもできます。スクリプトには、**copy running-configuration startup-configuration** および **copy startup-configuration tftp:***//server/name* の 2 つのコマンドを含める必要があります。. スクリプトを実行するには、**run-script** *filename* コマンドを使用します。 コマンドを使用します。

コア ダンプの使用

コア ダンプには、クラッシュ前のシステムとソフトウェアのステータスに関する詳細情報が含まれています。不明な問題が存在する状況では、コア ダンプを使用します。コア ダンプは、TFTP サーバまたはローカル システムの slot0: のフラッシュ カードに送信できます。テクニカル サポート担当者の指示に従って、コア ダンプを生成するようにシステムを設定する必要があります。コア ダンプは、テクニカル サポート エンジニアによってデコードされます。

これらのコア ダンプをテクニカル サポート担当者に直接電子メールで送信できるように、コア ダンプを設定し、TFTP サーバに移動します。

system cores コマンドを使用し、 コマンドを使用して、次のようにシステムにコア ダンプを設定します。

```
switch# system cores tftp://10.91.51.200/jsmith_cores
switch# show system cores
Cores are transferred to tftp://10.91.51.200/jsmith_cores
```

（注） ファイル名（この例では jsmith_cores）が TFTP サーバのディレクトリ内に存在する必要があります。

第 17 章

トラブルシューティングのツールと方法論

- コマンドライン インターフェイスのトラブルシューティング コマンド （119 ページ）
- ACL 整合性チェッカ （142 ページ）
- 設定ファイル （144 ページ）
- CLI デバッグ （144 ページ）
- Pingおよび Traceroute （146 ページ）
- プロセスおよび CPU のモニタリング （148 ページ）
- オンボード障害ロギングの使用 （151 ページ）
- 診断の使用 （152 ページ）
- 組み込まれている Event Manager の使用 （153 ページ）
- Ethanalyzer の使用 （153 ページ）
- SNMP および RMON のサポート （171 ページ）
- PCAP SNMP パーサーの使用 （171 ページ）
- RADIUS を利用 （173 ページ）
- syslog の使用 （174 ページ）
- SPAN の使用 （175 ページ）
- Using sFlow, on page 176
- sFlow 整合性チェッカー （176 ページ）
- ブルー ビーコン機能の使用 （177 ページ）
- watch コマンドの使用 （177 ページ）
- トラブルシューティングのツールと方法論の追加参照 （178 ページ）

コマンドラインインターフェイスのトラブルシューティング コマンド

コマンドライン インターフェイス（CLI）を使用すると、ローカルコンソールを使用して、または Telnet またはセキュアシェル（SSH）セッションを使用してリモートで設定およびモニタできます。Cisco NX-OSCLI には、Cisco IOS ソフトウェアに似たコマンド構造があり、状況依存ヘルプ、**show** コマンド、マルチユーザ サポート、およびロールベースのアクセス制御が備わっています。

各機能には、機能の設定、ステータス、パフォーマンスに関する情報を提供する **show** コマンドが用意されています。また、次のコマンドを使用すると、さらに詳しい情報を確認することができます。

- **show system** コア、エラー、および例外を含むシステムレベルのコンポーネントに関する情報を提供します。**show system error-id** コマンドを使用し、 コマンドにより、エラーコードの詳細を検索できます。

```
switch# copy running-config startup-config
[########################################] 100%
2013 May 16 09:59:29 zoom %$ VDC-1 %$ %BOOTVAR-2-AUTOCOPY_FAILED: Autocopy of file
/bootflash/n9000-dk9.6.1.2.I1.1.bin to standby

switch# show system error-id 0x401e0008
Error Facility:     sysmgr
Error Description:  request was aborted, standby disk may be full
```

整合性チェッカー コマンド

Cisco NX-OS には、ソフトウェア状態とハードウェア状態を検証する整合性チェッカー コマンドが用意されています。整合性チェッカーの結果は、PASSED または FAILED として記録されます。

```
2019 May 1 16:31:39 switch vshd: CC_LINK_STATE:
Consistency Check: PASSED
```

整合性チェッカーは、次の機能を実行するツールです。

- システムの整合性を確認する
- 根本原因分析と障害分離の実行を支援する
- ソフトウェア テーブルとハードウェア テーブル間の整合性をチェックする

Cisco NX-OS は、次の整合性チェッカーをサポートします。

表 *3:* 整合性チェッカー コマンド

コマンド	説明	サポートされるプラットフォーム
show consistency-checker copp	CoPP プログラミングを確認します。	Cisco Nexus 34180YC、9200、9300-EX、および 9300-FX プラットフォーム スイッチ、および -EX、-FX、-R ラインカードを備えた Cisco Nexus 9500 プラットフォーム スイッチ

コマンド	説明	サポートされるプラットフォーム
show consistency-checker dme interfaces	DMEインターフェイスを確認します。	Cisco Nexus 34180YC、9200、9300-EX、および 9300-FX プラットフォーム スイッチ、および -EX、-FX ライン カードを備えた Cisco Nexus 9500 プラットフォーム スイッチ
show consistency-checker egress-xlate private-vlan	ハードウェアのプライベート VLAN egress-xlate を確認します。	Cisco Nexus 9200、9300-EX、および 9300-FX プラットフォーム スイッチ、および -EX、-FX、-R ライン カードを備えた Cisco Nexus 9500 プラットフォーム スイッチ
show consistency-checker fex-interfaces {**fex** *fex-id* | **interface ethernet** *fex-id/fex-slot/fex-port*} [**brief** | **detail**]	FEX インターフェイスのソフトウェアとハードウェアの状態を比較します。 （注） *fex-slot* は常に 1 です。	Cisco Nexus 9200、9300-EX、および 9300-FX プラットフォーム スイッチ、および -EX、-FX ライン カードを備えた Cisco Nexus 9500 プラットフォーム スイッチ
test consistency-checker forwarding {**ipv4** | **ipv6**} [**vrf** *vrf-name* | **all**] [**module** *module-number* | **all**]	レイヤ 3 整合性チェッカーを開始します。	Cisco Nexus 9000 シリーズ スイッチ
show consistency-checker forwarding {**ipv4** | **ipv6**} [**vrf** *vrf-name* | **all**] [**module** *module-number* | **all**]	レイヤ 3 整合性チェッカー テスト結果を表示します。	すべての Cisco Nexus 9000 シリーズ スイッチ

コマンド	説明	サポートされるプラットフォーム
show consistency-checker forwarding single-route {**ipv4** | **ipv6**} *ip-address* **vrf** *vrf-name*} [**brief** | **detail**]	特定のルートのレイヤ 3 ルートの整合性をチェックします。ECMP グループ テーブルの枯渇が原因で単一ルートが失敗したときに警告します。	Cisco Nexus 34180YC、9200、9300-EX、および 9300-FX プラットフォーム スイッチ、および -EX、-FX、-R ライン カードを備えた Cisco Nexus 9500 プラットフォーム スイッチ （注） Cisco Nexus 34180YC プラットフォーム スイッチでは、**ipv4** コマンドのみをサポートしています。
show consistency-checker gwmacdb	ゲートウェイ MAC アドレス データベースのハードウェアとソフトウェアの一貫性をチェックします。 （注） このコマンドは、4 ウェイ HSRP に対して誤った結果を表示する場合があります。	すべての Cisco Nexus 9000 シリーズ スイッチ
show consistency-checker kim interface {**ethernet** *slot/port* | **port-channel** *number* | **vlan** *vlan-id*} [**brief** | **detail**]	スーパーバイザとライン カード間の内部接続を確認します。	Cisco Nexus 34180YC、9200、9300-EX、および 9300-FX プラットフォーム スイッチ、および -EX、-FX、-R ライン カードを備えた Cisco Nexus 9500 プラットフォーム スイッチ
show consistency-checker l2 module *module-number*	学習した MAC アドレスがソフトウェアとハードウェア間で一貫していることを確認します。また、ハードウェアに存在するがソフトウェアには存在しない追加エントリと、ハードウェアに存在しないエントリも表示されます。	Cisco Nexus 34180YC、9200、9300-EX、および 9300-FX プラットフォーム スイッチ、および -EX、-FX、-R ライン カードを備えた Cisco Nexus 9500 プラットフォーム スイッチ

コマンド	説明	サポートされるプラットフォーム
show consistency-checker l2 multicast group *ip-address* **source** *ip-address* **vlan** *vlan-id* [**brief** | **detail**]	レイヤ2マルチキャスト グループとの不整合をチェックします。	Cisco Nexus 9200、9300-EX、9300-FX、および9300-GX プラットフォーム スイッチおよび Cisco Nexus 9500 プラットフォーム スイッチ-EX および -FXライン カード N9K-X9432C-S、N9K-X9536PQ ライン カード搭載の Cisco Nexus 9500 シリーズ スイッチ N9K-X9432C-FM-S、N9K-C9508-FMX-S、N9K-C9508-FM-S ファブリック モジュールを搭載した Cisco Nexus 9500 シリーズ スイッチ。 Cisco Nexus N3K-C3232C、N3K-C3264Q、N3K-C31108TC-V、N3K-C3132Q-40GX、N3K-C3132Q-V、N3K-C31108PC-V、N3K-C3172PQ、N3K-C3172TQ、N3K-C3164Q、および N3K-C3164Q -10GE スイッチ。 Cisco Nexus N9K-C9372TX、N9K-C9372TX-E、N9K-C93120TX、N9K-X9432C-S、N9K-C9332PQ、N9K-C9372PX、および N9K-C9372PX-E スイッチ。
show consistency-checker l2 switchport interface {**ethernet** *slot/port* | **port-channel** *number* }[**brief** | **detail** | **all**]	スイッチポートインターフェイスとの不整合をチェックします。	Cisco Nexus 9200、9300-EX、および 9300-FX プラットフォーム スイッチ、および -EX、-FX ライン カードを備えた Cisco Nexus 9500 プラットフォーム スイッチ

コマンド	説明	サポートされるプラットフォーム
show consistency-checker l3-interface interface ethernet *slot/port* [**brief** | **detail**]	ハードウェアのインターフェイスのレイヤ 3 設定と、ハードウェアの L3VLAN、CMLフラグ、IPv4イネーブル、VPN IDの設定を確認します。このコマンドは、物理インターフェイスおよびポートチャネルの一部であるインターフェイスに対して機能します。サブインターフェイスまたはFEXインターフェイスは検証されません。 Cisco NX-OS リリース 9.3(5) 以降、このコマンドは SI および SVI インターフェイスのレイヤ 3 設定をチェックします。サポートは Cisco Nexus 9300-GX プラットフォーム スイッチにも拡張されます。	Cisco Nexus 34180YC、9200、9300-EX、および9300-FX プラットフォーム スイッチ、および -EX、-FX、-R ラインカードを備えた Cisco Nexus 9500 プラットフォーム スイッチ Cisco Nexus N9K-C9316D-GX、N9K-C93600CD-GX、N9K-C9364C-GX デバイス。
show consistency-checker l3-interface module *module-number* [**brief** | **detail**]	モジュール内のすべてのインターフェイスのレイヤ 3 設定と、ハードウェアの L3VLAN、CML フラグ、IPv4 イネーブル、VPN ID の設定を確認します。このコマンドは、物理インターフェイスおよびポートチャネルの一部であるインターフェイスに対して機能します。サブインターフェイスは検証されません。	Cisco Nexus 34180YC、9200、9300-EX、および9300-FX プラットフォーム スイッチ、および -EX、-FX、-R ラインカードを備えた Cisco Nexus 9500 プラットフォーム スイッチ

コマンド	説明	サポートされるプラットフォーム
show consistency-checker l3 multicast group *ip-address* **source** *ip-address* **vrf** *vrf-name* [**brief** | **detail**]	レイヤ 3 マルチキャスト グループとの不整合をチェックします。	Cisco Nexus 9200、9300-EX、9300-FX、および9300-GX プラットフォーム スイッチおよび Cisco Nexus 9500 プラットフォーム スイッチ-EX および -FXライン カード N9K-X9432C-S、N9K-X9536PQ ライン カードを搭載した Cisco Nexus 9500 シリーズスイッチ、および N9K-X9432C-FM-S、N9K-C9508-FMX-S、および N9K-C9508-FM-S ファブリック モジュール。 Cisco Nexus N3K-C3048TP、N3K-C3064-TC、N3K-C3232C、N3K-C3264Q、N3K-C31108TC-V、N3K-C3132Q-40GX、N3K-C3132Q-V、N3K-C31108PC-V、N3K-C3172PQ、C3172TQ、N3K-C3164Q、および N3K-C31128PQ-10GE スイッチ。 Cisco Nexus N9K-C9372TX、N9K-C9372TX-E、N9K-C93120TX、N9K-X9432C-S、N9K-C9332PQ、N9K-C9372PX、および N9K-C9372PX-E スイッチ。
show consistency-checker link-state fabric-ieth [**module** *module-number*] [**brief** | **detail**]	内部ファブリック ポートのリンク状態ステータスについて、ソフトウェアとハードウェア間のプログラミングの一貫性を確認します。	Cisco Nexus 9200、9300-EX、および 9300-FX プラットフォーム スイッチ、および -EX、-FX、-R ライン カードを備えた Cisco Nexus 9500 プラットフォーム スイッチ

コマンド	説明	サポートされるプラットフォーム
show consistency-checker link-state interface ethernet *slot/port* [**brief** | **detail**]	インターフェイスのリンク状態ステータスについて、ソフトウェアとハードウェア間のプログラミングの一貫性を確認します。このコマンドは、物理イーサネットインターフェイスおよびポートチャネルの一部である物理イーサネットインターフェイスに対して機能します。サブインターフェイスまたはFEXインターフェイスは検証されません。	Cisco Nexus 34180YC、9200、9300-EX、および9300-FXプラットフォーム スイッチ、および-EX、-FXラインカードを備えたCisco Nexus 9500プラットフォーム スイッチ
show consistency-checker link-state module *module-number* [**brief** | **detail**]	モジュール内のすべてのインターフェイスのソフトウェアリンク状態をハードウェアリンク状態と照合します。このコマンドは、物理イーサネットインターフェイスおよびポートチャネルの一部である物理イーサネットインターフェイスに対して機能します。サブインターフェイスまたはFEXインターフェイスは検証されません。	Cisco Nexus 34180YC、9200、9300-EX、および9300-FXプラットフォーム スイッチ、および-EX、-FX、-Rラインカードを備えたCisco Nexus 9500プラットフォーム スイッチ
show consistency-checker membership port-channels [**interface port-channel** *channel-number*] [**brief** | **detail**]	すべてのモジュールのハードウェアのポート チャネル メンバーシップをチェックし、ソフトウェア状態で検証します。このコマンドは、ポートチャネルごとに実行されます。	Cisco Nexus 34180YC、9200、9300-EX、および9300-FXプラットフォーム スイッチ、および-EX、-FX、-Rラインカードを備えたCisco Nexus 9500プラットフォーム スイッチ
show consistency-checker membership port-channels [**brief** | **detail**]	すべてのモジュールのハードウェアのポート チャネル メンバーシップをチェックし、ソフトウェア状態で検証します。このコマンドは、システム内のすべてのポートチャネルに対して実行されます。	Cisco Nexus 34180YC、9200、9300-EX、および9300-FXプラットフォーム スイッチ、および-EX、-FX、-Rラインカードを備えたCisco Nexus 9500プラットフォーム スイッチ

コマンド	説明	サポートされるプラットフォーム
show consistency-checker membership vlan *vlan-id* {**native-vlan** | **private-vlan interface** {**ethernet** *slot/port* | **port-channel** *number* | **native-vlan**}} [**brief** | **detail** | **interface**]	ソフトウェアのVLANメンバーシップがハードウェアにプログラムされているものと同じであることを判別します。また、STP BLK状態のインターフェイスも無視します。	Cisco Nexus 9200、9300-EX、および9300-FXプラットフォーム スイッチ、および-EX、-FX、-Rライン カードを備えたCisco Nexus 9500プラットフォーム スイッチ （注） **private-vlan** コマンドでの **brief** または **detail** オプションはサポートされていません。 （注） Cisco Nexus 34180YCプラットフォーム スイッチでは、**native-vlan** コマンドのみをサポートしています。
show consistency-checker pacl {**module** *module-number* | **port-channels interface port-channel** *channel-number*}	ハードウェアとソフトウェア間のIPv4、IPv6、およびMAC PACLプログラミングの整合性を検証し、<label, entry-location>ペアはハードウェアとソフトウェアの間で一貫しています。	Cisco Nexus 34180YC、9200、9300-EX、および9300-FXプラットフォーム スイッチ、および-EX、-FXライン カードを備えたCisco Nexus 9500プラットフォーム スイッチ
show consistency-checker pacl extended ingress {**ip** | **ipv6** | **mac**} **interface** {**ethernet** *slot/port* | **port-channel** *number*} [**brief** | **detail**]	入力インターフェイス（FEXインターフェイスを含む）およびポート チャネルのPACLプログラミングを確認します。	Cisco Nexus 34180YC、9200、9300-EX、および9300-FXプラットフォーム スイッチ、および-EX、-FXライン カードを備えたCisco Nexus 9500プラットフォーム スイッチ
show consistency-checker pacl extended ingress {**ip** | **ipv6** | **mac**} **module** *module-number* [**brief** | **detail**]	指定されたモジュールのすべての物理インターフェイス、サブインターフェイス、ブレークアウト ポート、およびFEXインターフェイスでPACLプログラミングを確認します。	Cisco Nexus 34180YC、9200、9300-EX、および9300-FXプラットフォーム スイッチ、および-EX、-FXライン カードを備えたCisco Nexus 9500プラットフォーム スイッチ

コマンド	説明	サポートされるプラットフォーム
show consistency-checker port-state fabric-ieth [**module** *module-number* [**ieth-port** *ieth-port*]] [**brief** | **detail**]	内部ファブリック ポートの状態を確認します。	Cisco Nexus 9200、9300-EX、および 9300-FX プラットフォーム スイッチ、および -EX、-FX、-R ライン カードを備えた Cisco Nexus 9500 プラットフォーム スイッチ
show consistency-checker port-state [**module** *module-number*] [**brief** | **detail**]	指定されたモジュールのポートの状態を確認します。	Cisco Nexus 9200、9300-EX、および 9300-FX プラットフォーム スイッチ、および -EX、-FX、-R ライン カードを備えた Cisco Nexus 9500 プラットフォーム スイッチ

コマンド	説明	サポートされるプラットフォーム
show consistency-checker racl {**module** *module-number* | **port-channels interface port-channel** *channel-number* | **svi interface vlan** *vlan-id*}	ハードウェアとソフトウェア間の IPv4 および IPv6 RACL プログラミングの一貫性を検証し、<label, entry-location> ペアはハードウェアとソフトウェアの間で一貫しています。 • このコマンドは、モジュールごとに呼び出されると、そのモジュールのすべての物理インターフェイスおよびサブインターフェイスの IPv4 および IPv6 ACL の整合性を確認します。 • 特定のポートチャネルでこのコマンドを呼び出すと、すべてのメンバーポートが検証されます。 • すべてのポートチャネルでこのコマンドを呼び出すと、このコマンドはACLが適用されているポートチャネルごとに確認します。 （注） このコマンドは、IPv4 および IPv6 ACL を検証せず、修飾子とアクションが一致するかどうかを検証しません。	Cisco Nexus 34180YC、9200、9300-EX、および 9300-FX プラットフォーム スイッチ、および -EX、-FX ライン カードを備えた Cisco Nexus 9500 プラットフォーム スイッチ
show consistency-checker racl extended ingress {**ip** | **ipv6**} **interface** {**ethernet** *slot* / ポート </g> | port-channelnumber |vlan lan-id</g> } [brief| detail]	入力インターフェイス、サブインターフェイス、ブレークアウトポート、ポートチャネル、または SVI の RACL プログラミングを確認します。	Cisco Nexus 34180YC、9200、9300-EX、および 9300-FX プラットフォーム スイッチ、および -EX、-FX ライン カードを備えた Cisco Nexus 9500 プラットフォーム スイッチ

コマンド	説明	サポートされるプラットフォーム
show consistency-checker racl extended ingress {**ip** | **ipv6**} **module** *module-number* [**brief** | **detail**]	指定されたモジュールの入力インターフェイスの RACL プログラミングを確認します。このコマンドは、そのモジュールのすべての物理インターフェイス、サブインターフェイス、およびブレークアウトポートで実行されます。	Cisco Nexus 34180YC、9200、9300-EX、および 9300-FX プラットフォーム スイッチ、および -EX、-FX ライン カードを備えた Cisco Nexus 9500 プラットフォーム スイッチ
show consistency-checker stp-state vlan *vlan-id* [**brief** | **detail** | **interface**]	ソフトウェアのスパニング ツリーの状態が、ハードウェアでプログラミングされた状態と同じかどうかを判別します。このコマンドは、動作中（アップ）のインターフェイスでのみ実行されます。	Cisco Nexus34180YC、9200、9300-EX、および 9300-FX プラットフォーム スイッチおよび -EX、-FX、および -R ライン カードを搭載した Cisco Nexus 9500 プラットフォーム スイッチ。
show consistency-checker vacl extended ingress {**ip** | **ipv6** | **mac**} **vlan** *vlan-id* [**brief** | **detail**]	VLAN のすべてのメンバーインターフェイスで VACL プログラミングを確認します。	Cisco Nexus 34180YC、9200、9300-EX、および 9300-FX プラットフォーム スイッチ、および -EX、-FX ライン カードを備えた Cisco Nexus 9500 プラットフォーム スイッチ

コマンド	説明	サポートされるプラットフォーム
show consistency-checker vpc [**source-interface**] [**brief** | **detail**]	vPC の不整合をチェックします。	Cisco Nexus 9200、9300-EX、および 9300-FX プラットフォーム スイッチ、および -EX、-FX ライン カードを備えた Cisco Nexus 9500 プラットフォーム スイッチ N9K-X9432C-S、N9K-X9536PQ ライン カードを搭載した Cisco Nexus 9500 シリーズスイッチ、および N9K-X9432C-FM-S、N9K-C9508-FMX-S、および N9K-C9508-FM-S ファブリック モジュール。 Cisco Nexus N3K-C3048TP、N3K-C3064-TC、N3K-C3232C、N3K-C3264Q、N3K-C31108TC-V、N3K-C3132Q-40GX、N3K-C3132Q-V、N3K-C31108PC-V、N3K-C3172PQ、C3172TQ、N3K-C3164Q、および N3K-C31128PQ-10GE スイッチ。 Cisco Nexus N9K-C9372TX、N9K-C9372TX-E、N9K-C93120TX、N9K-X9432C-S、N9K-C9332PQ、N9K-C9372PX、および N9K-C9372PX-E スイッチ。

コマンド	説明	サポートされるプラットフォーム
show consistency-checker vxlan config-check [**verbose-mode**]	スイッチの VXLAN EVPN 設定を確認します。	Cisco Nexus 9200、9300-EX および 9300-FX プラットフォーム スイッチ Cisco Nexus C31108PC-V、C31108TC-V、C3132Q-V、および 3132C-Z スイッチ。 Cisco Nexus C9396TX、C93128TX、C9396PX、X9564PX、X9564TX、および X9536PQ スイッチ。 Cisco Nexus C3132Q-40GE-SUP、C3132Q-40GX-SUP、C3132Q-XL、C31128PQ-10GE、C3264Q-S、C3264C-E スイッチ。
show consistency-checker vxlan infra [**verbose-mode**]	VXLAN トンネル インフラストラクチャとの不整合をチェックします。	Cisco Nexus 9200、9300-EX および 9300-FX プラットフォーム スイッチ Cisco Nexus C31108PC-V、C31108TC-V、C3132Q-V、および 3132C-Z スイッチ。 Cisco Nexus C9396TX、C93128TX、C9396PX、X9564PX、X9564TX、および X9536PQ スイッチ。 Cisco Nexus C3132Q-40GE-SUP、C3132Q-40GX-SUP、C3132Q-XL、C31128PQ-10GE、C3264Q-S、C3264C-E スイッチ。

コマンド	説明	サポートされるプラットフォーム
show consistency-checker vxlan l2 module *module-number*	VXLAN レイヤ 2 ルートとの整合性を確認します。	Cisco Nexus 9200、9300-EX および 9300-FX プラットフォーム スイッチ Cisco Nexus C31108PC-V、C31108TC-V、C3132Q-V、および 3132C-Z スイッチ。 Cisco Nexus C9396TX、C93128TX、C9396PX、X9564PX、X9564TX、および X9536PQ スイッチ。 Cisco Nexus C3132Q-40GE-SUP、C3132Q-40GX-SUP、C3132Q-XL、C31128PQ-10GE、C3264Q-S、C3264C-E スイッチ。
show consistency-checker vxlan l3 vrf [*vrf-name* | **all**] [**start-scan** | **report**]	VXLAN レイヤ 3 ルートとの不一致をチェックします。	Cisco Nexus 9200、9300-EX および 9300-FX プラットフォーム スイッチ Cisco Nexus C31108PC-V、C31108TC-V、C3132Q-V、および 3132C-Z スイッチ。 Cisco Nexus C9396TX、C93128TX、C9396PX、X9564PX、X9564TX、および X9536PQ スイッチ。
show consistency-checker vxlan pv	ソフトウェア間およびハードウェアの異なるテーブル間で VLAN マッピングが一貫してプログラムされているかどうかを確認します。このコマンドを実行するには、少なくとも 1 つのインターフェイスでポート VLANマッピングを有効にする必要があります。	Cisco Nexus 9200、9300-EX および 9300-FX/FX2 および 9500 プラットフォーム スイッチ

コマンド	説明	サポートされるプラットフォーム
show consistency-checker vxlan qinq-qinvni	ソフトウェアおよびハードウェアで一貫しているマルチタグ VLAN リストおよび関連するマルチタグ vn-segment をチェックします。	Cisco Nexus 9300-FX/FX2 プラットフォーム スイッチ
show consistency-checker vxlan selective-qinvni interface {**ethernet** *slot/port* | **port-channel** *channel-number*}	パケット内の内部タグが保持されるように、ポート固有の選択的 Q-in-VNI マッピングがソフトウェアおよびハードウェアで正しくプログラムされているかどうかを検証します。	Cisco Nexus 9300-EX および 9300-FX/FX2 プラットフォーム スイッチ
show consistency-checker vxlan vlan [**all** | *vlan-id*] [**verbose-mode**]	VXLAN VLAN との不一致をチェックします。	Cisco Nexus 9300-EX および 9300-FX/FX2 プラットフォーム スイッチ Cisco Nexus C31108PC-V、C31108TC-V、C3132Q-V、および 3132C-Z スイッチ。 Cisco Nexus C9396TX、C93128TX、C9396PX、X9564PX、X9564TX、および X9536PQ スイッチ。 Cisco Nexus C3132Q-40GE-SUP、C3132Q-40GX-SUP、C3132Q-XL、C31128PQ-10GE、C3264Q-S、C3264C-E スイッチ。
show consistency-checker vxlan xconnect	VXLAN Xconnect VLAN との不一致をチェックします。Xconnect ACL がすべてのユニットとスライスにインストールされ、MAC 学習がすべての Xconnect VLAN で無効になっていることを検証します。	Cisco Nexus 9200、9332C、9364C、9300-EX、および 9300-FX/FX2 プラットフォーム スイッチ。

コマンド	説明	サポートされるプラットフォーム
show consistency-checker vxlan l3 single-route [**ipv4** | **ipv6**] [*vrf*]	VXLAN レイヤ 3 シングル ルート トラフィックとの不整合をチェックします。	Cisco Nexus 9200、9300-EX および 9300-FX プラットフォーム スイッチ。 Cisco Nexus C31108PC-V、C31108TC-V、C3132Q-V、および 3132C-Z スイッチ。 Cisco Nexus C9396TX、C93128TX、C9396PX、X9564PX、X9564TX および X9536PQ スイッチ、Cisco Nexus 9200、9300-EX、および9300-FXプラットフォームスイッチ。
show consistency-checker vxlan l2 [**mac-address**] [*mac-address*] | **module**] [*module*	VXLAN レイヤ 2 との不一致をチェックします。	Cisco Nexus 9200、9300-EX および 9300-FX プラットフォーム スイッチ。 Cisco Nexus C31108PC-V、C31108TC-V、C3132Q-V、および 3132C-Z スイッチ。 Cisco Nexus C9396TX、C93128TX、C9396PX、X9564PX、X9564TX および X9536PQ スイッチ、Cisco Nexus 9200、9300-EX、および9300-FXプラットフォームスイッチ。 Cisco Nexus C3132Q-40GE-SUP、C3132Q-40GX-SUP、C3132Q-XL、C31128PQ-10GE、C3264Q-S、C3264C-E スイッチ。

コマンド	説明	サポートされるプラットフォーム
show consistency-checker storm-control	ストーム制御整合性チェッカ	Cisco Nexus 9200、9300-EX、および 9300-FX プラットフォーム スイッチ、および -EX、-FX、-R ライン カードを備えた Cisco Nexus 9500 プラットフォーム スイッチ Cisco NX-OSリリース9.3(5)以降では、N3K-C3016Q-40GE、N3K-C3048TP-1GE、N3K-C3064PQ-10GE、N3K-C3064PQ-10GX、N3K-C3064T-10GT、N9K-C9504- FM、N9K-C9508-FM、N9K-C9516-FM、N9K-C9508-FM-S、N3K-C31128PQ、N3K-C3164Q-40GE、N3K-C3232C、N3K-C3132Q-V、N3K-C31108PC-V、N3K-C31108P-V C31108TC-V、N3K-C3264C-E、N3K-C3132C-Z、N9K-C93128TX、N9K-C9396PX、N9K-C9372PX、およびN9K-C9332PQ デバイスでサポートされています。
show consistency-checker segment-routing mpls [**ip**] [*ip-address*] | **mask**] [*mask* | **vrf**] [*vrf*	アンダーレイ セグメント ルーティング（ISIS、BGP、OSPF）およびレイヤ 3 VPN およびレイヤ 2 EVPN オーバーレイ ルートのルート整合性をチェックします。	Cisco Nexus 9200、9300-EX、および 9300-FX プラットフォーム スイッチ、および -EX、-FX ライン カードを備えた Cisco Nexus 9500 プラットフォーム スイッチ。 Cisco Nexus N9K-C9316D-GX、N9K-C93600CD-GX、N9K-C9364C-GX デバイス。

コマンド	説明	サポートされるプラットフォーム
show consistency-checker segment-routing mpls label	アンダーレイ セグメント ルーティング（ISIS、BGP、OSPF）およびオーバーレイ ルートのレイヤ 3 VPN、レイヤ 2 EVPN、および ADJ SIDS のラベル整合性をチェックします。	Cisco Nexus 9200、9300-EX、および 9300-FX プラットフォーム スイッチ、および -EX、-FX ライン カードを備えた Cisco Nexus 9500 プラットフォーム スイッチ。 Cisco Nexus N9K-C9316D-GX、N9K-C93600CD-GX、N9K-C9364C-GX デバイス。
show consistency-checker sflow [**brief** | **detail**]	スーパーバイザーとライン カードハードウェア テーブルのプログラムと整合性構成をチェックします。	Cisco Nexus 9300-FX2、9300-FX3、9300-GX および 9300-GX2 プラットフォーム スイッチ

次のコマンドは JSON 出力をサポートしていません。

- **show consistency-checker forwarding** {**ipv4** | **ipv6**} [**vrf** *vrf-name* | **all**] [**module** *module-number* | **all**]
- **show consistency-checker pacl** {**module** *module-number* | **port-channels interface port-channel** *channel-number*}
- **show consistency-checker racl module** *module-number*
- **show consistency-checker racl port-channels interface port-channel** *channel-number*}
- **show consistency-checker racl svi interface vlan** *vlan-id*
- **show consistency-checker vxlan**
- **test consistency-checker forwarding** {**ipv4** | **ipv6**} [**vrf** *vrf-name* | **all**] [**module** *module-number* | **all**]

show consistency-checker vxlan コマンドはモデル化されていません。

マルチキャスト整合性チェッカー

マルチキャスト整合性チェッカーは、マルチキャストルートの状態を確認するためのレイヤ 2 およびレイヤ 3 ルートの単一ルート整合性チェッカーです。マルチキャスト整合性チェッカーは、各コンポーネントで show コマンドを実行し、関連情報を解析し、処理された情報を他のコンポーネントと比較して不整合をチェックします。マルチキャスト整合性チェッカー コマンドは、障害が発生すると終了します。**show consistency-checker l2 multicast group** および **show consistency-checker l3 multicast group** コマンドは、期待値と実際の値の差を返します。

これらのコマンドは、次の出力形式をサポートしています。

- **verbose**：結果をテキスト形式で表示します。
- **detail**：結果を JSON 形式で表示します。
- **brief**：結果を最小限の詳細とともに JSON 形式で表示します。

Cisco NX-OSリリース10.1(1) 以降では、次の整合性チェッカーがサポートされています。

- IPv6 L2 マルチキャスト整合性チェッカー
- IPv6 L3 マルチキャスト整合性チェッカー
- マルチキャスト NLB 整合性チェッカー
  - マルチキャスト MAC ルックアップ モード整合性チェッカー
  - マルチキャスト NLB L3 ユニキャスト設定整合性チェッカー
- マルチキャスト GRE 整合性チェッカー

次の既存の CLI コマンドは、IPv6 L2 マルチキャスト整合性チェッカーの IPv6 送信元およびグループ アドレスを受け入れるように拡張されています。

show consistency-checker l2 multicast group <ipv4/ipv6 group address> source <ipv4/v6 source address> vrf <vrf-id> [brief|detail]

次に、IPv6 L2 マルチキャスト整合性チェッカーの出力例を示します。

```
# show consistency-checker l2 multicast group ?
  A.B.C.D   Group IP address
  A:B::C:D  Group IPv6 address
```

次の既存の CLI コマンドは、IPv6 L3 マルチキャスト整合性チェッカーの IPv6 送信元およびグループ アドレスを受け入れるように拡張されています。

show consistency-checker l3 multicast group <ipv4/ipv6 group address> source <ipv4/v6 source address> vlan <vlan-id> [brief|detail]

次に、IPv6 L3 マルチキャスト整合性チェッカーの出力例を示します。

```
# show consistency-checker l3 multicast group ?
  A.B.C.D   Group IP address
  A:B::C:D  Group IPv6 address
```

マルチキャスト MAC ルックアップ モードの整合性チェッカーをサポートするために、次の新しい CLI コマンドが追加されました。

show consistency-checker l2 multicast mac <mac> vlan <vlan-id>

次に、マルチキャスト MAC ルックアップ モードの整合性チェッカーの出力例を示します。

```
# show consistency-checker l2 multicast mac 0100.1234.1234 vlan 10 ?
  >       Redirect it to a file
  >>      Redirect it to a file in append mode
  brief   Show consistency checker structured output in brief
  detail  Show consistency checker structured output in detail
  |       Pipe command output to filter
```

（注） この CLI は、MAC ルックアップモードの整合性チェッカまたは NLB の L2 モードの整合性チェッカーに使用されます。入力 MACは、ip-mac または non-ip-mac のいずれかです。

マルチキャスト NLB L3 ユニキャスト設定整合性チェッカーをサポートするために、次の新しい CLI コマンドが追加されました。

show consistency-checker multicast nlb cluster-ip <unicast-cluster-ip> vrf <vrf-id>

次に、マルチキャスト NLB L3 ユニキャスト設定整合性チェッカーの出力例を示します。

```
# show consistency-checker multicast nlb cluster-ip <unicast-cluster-ip>
  >       Redirect it to a file
  >>      Redirect it to a file in append mode
  brief   Show consistency checker structured output in brief
  detail  Show consistency checker structured output in detail
  |       Pipe command output to filter
```

次の既存の CLI コマンドは、マルチキャスト GRE 整合性チェッカーに使用されます。

show consistency-checker l3 multicast group <ipv4 group address> source <ipv4 source address> vrf <vrf-id> [brief|detail]

（注） 既存の IPv4 L3 マルチキャスト整合性チェッカー CLI を使用して、マルチキャスト GRE 整合性チェッカーを開始します。

マルチキャスト整合性チェッカーは、次のデバイスをサポートしています。

- Cisco Nexus 92304QC、9272Q、9236C、92300YC、93108TC-EX、93180LC-EX、93180YC-EX、and 9300-GX プラットフォーム スイッチおよび N9K-X9736C-EX、N9K-X97160YC-EX、N9K-X9732C-EX、および N9K-X9732C-EXM ライン カードです。
- N9K-X96136YC-R、N9K-X9636C-R、およびN9K-X9636Q-Rラインカードを搭載したCisco Nexus 9500シリーズスイッチ。

Cisco NX-OS Release 9.3(5) 以降では、マルチキャスト整合性チェッカーは次のデバイスをサポートしています。

- N9K-X9432C-S、N9K-X9536PQ ライン カードを搭載した Cisco Nexus 9500 シリーズスイッチ、および N9K-X9432C-FM-S、N9K-C9508-FMX-S、および N9K-C9508-FM-S ファブリック モジュール。
- Cisco Nexus N3K-C3232C、N3K-C3264Q、N3K-C31108TC-V、N3K-C3132Q-40GX、N3K-C3132Q-V、N3K-C31108PC-V、N3K-C3172PQ、N3K-C3172TQ、N3K-C3164Q、および N3K-C31128PQ-10GE スイッチ。
- Cisco Nexus N9K-C9372TX、N9K-C9372TX-E、N9K-C93120TX、N9K-X9432C-S、N9K-C9332PQ、N9K-C9372PX、および N9K-C9372PX-スイッチ。

Cisco NX-OSリリース10.1(1) 以降では、マルチキャスト整合性チェッカーは次のデバイスをサポートしています。

- Cisco Nexus N9k-C9504 を搭載した N9K-X97160YC-EX、N9k-C9504 を搭載した N9K-X9732C-EX、N9k-C9504 を搭載した N9K-X9732C-FX、N9k-C9504 を搭載した N9K-X9736C-EX、N9k-C9504 を搭載した N9K-X9736C-FX、N9k-C9504 を搭載した N9K-X9736Q-FX、および N9k-C9504 を搭載した N9K-X9788TC-FX。
- Cisco Nexus N9k-C9508 を搭載した N9K-X97160YC-EX、N9k-C9508 を搭載した N9K-X9732C-EX、N9k-C9508 を搭載した N9K-X9732C-FX、N9k-C9508 を搭載した N9K-X9736C-EX、N9k-C9508 を搭載した N9K-X9736C-FX、N9k-C9508 を搭載した N9K-X9736Q-FX、および N9k-C9508 を搭載した N9K-X9788TC-FX。

マルチキャスト整合性チェッカーは、次のレイヤ2コンポーネントのプログラミングの整合性を検証します：

- IGMP スヌーピング
- MFDM
- MFIBPI
- MFIBPD
- ハードウェア テーブル

マルチキャスト整合性チェッカーは、次のレイヤ3コンポーネントのプログラミングの整合性を検証します：

- PIM
- MRIB
- IGMP スヌーピング
- MFDM
- MFIBPI
- MFIBPD
- ハードウェア テーブル

マルチキャスト整合性チェッカ コマンドの出力例

次に、IGMP スヌーピングの出力例を示します。

```
switch# show ip igmp snooping groups 225.12.12.28 225.12.12.28 vlan 222
Type: S - Static, D - Dynamic, R - Router port, F - Fabricpath core port
Vlan  Group Address      Ver  Type  Port list
222   225.12.12.28       v3   D     Eth1/2 Eth1/3 Po12 Po100 Po18
```

次に、MFDM の出力例を示します。

```
switch# show forwarding distribution l2 multicast vlan 222 group 225.12.12.28 source
225.12.12.28
Vlan: 222, Group: 225.12.12.28, Source: 225.12.12.28
  Outgoing Interface List Index: 4
  Reference Count: 204
  Num L3 usages: 4
  Platform Index: 0xa00004
  Vpc peer link exclude flag set
  Number of Outgoing Interfaces: 5
    Ethernet1/2
    Ethernet1/3
    port-channel12
    port-channel18
    port-channel100
```

次に、IGMP スヌーピングと MFDM を比較する例（成功）を示します。

```
**********************************************************************
Comparing IGMP Snooping with MFDM
**********************************************************************
L2 Eth Receivers :
IGMP Snooping: 1/2, 1/3
MFDM: 1/2, 1/3

L2 PC Receivers :
IGMP Snooping: 100, 12, 18
MFDM: 12, 100, 18

CC between IGMP Snooping and MFDM PASSED
```

次に、IGMP スヌーピングと MFDM を比較する例（失敗）を示します。

```
**********************************************************************
Comparing IGMP Snooping with MFDM
**********************************************************************
L2 Eth Receivers:
IGMP Snooping: 1/2, 1/3
MFDM: 1/2,  1/3

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
L2 PC Receivers:
IGMP Snooping: 100, 12, 18
MFDM: 12, 100, 16
Consistency check failed!!!
Missing elements are: 18
Additional elements are: 16
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

輻輳検出および回避

Cisco NX-OS リリース 9.3(3) 以降、Cisco Nexus 9000 シリーズ スイッチは、輻輳の問題をトラブルシューティングするための **show tech-support slowdrain** コマンドをサポートしています。**show tech-support slowdrain** コマンドには、輻輳検出表示、カウンタ、およびログ メッセージの一部と、スイッチ、Cisco NX-OS バージョン、およびトポロジを理解できるその他のコマンドが含まれています。

輻輳は1つのスイッチから別のスイッチに伝播する可能性があるため、輻輳のトリガーと伝播をより適切に評価するために、すべてのスイッチから同時に **show tech-support slowdrain** コマンドの出力を収集する必要があります。

ACL 整合性チェッカ

Cisco NX-OS Release 9.3(3) 以降、ACL 整合性チェッカは次のデバイスをサポートします。

N9K-C9372PX、N9K-C9372PX-E、N9K-C9372TX、N9K-C9372TX-E、N9K-C9332PQ、N9K-C93128TX、N9K-C9396PX、N9K-C9396TX、N9K-C9508-FM-S、N9K-C9508-FM2、N9K-C9504-FM-S、N9K-X9632PC-QSFP100、N9K-X9432C-S

Cisco NX-OSリリース9.3(5) 以降、ACL 整合性チェッカは Cisco Nexus N9K-C9316D-GX、N9K-C93600CD-GX、N9K-C9364C-GX、N9K-C93240YC-FX2、N9K-C93180YC-EX、N3K-C3636C-R、N3K-C36180YC-Rと、 N9K-X9636Q-R、N9K-X9636C-R、N9K-X9636C-RX および N9K-X96136YC-R ライン カードを搭載した Cisco Nexus 9500 シリーズ スイッチでサポートされています。

次のエンティティは、ACLの整合性チェックの一部として検証されます：

アクション、プロトコル、SIP、DIP、送信元ポート、宛先ポート、送信元MAC、宛先MAC、Ethertype、COS、DSCP、VLAN および UDF です。

Cisco NX-OS は、次の PACL、RACL、および VACL 整合性チェッカ コマンドをサポートしています。

コマンド	説明
show consistency-checker pacl extended ingress ip module <module-id> [brief | detail]	指定した IP モジュールの入力インターフェイスおよびポートチャネルのPACL整合性チェックを実施します。
show consistency-checker pacl extended ingress ipv6 module <module-id> [brief | detail]	指定した IPv6 モジュールの入力インターフェイスおよびポートチャネルの PACL 整合性チェックを実施します。
show consistency-checker pacl extended ingress mac module <module-id> [brief | detail]	指定された MAC モジュールの入力インターフェイスおよびポートチャネルの MAC PACL 整合性チェックを実施します。
show consistency-checker pacl extended ingress ip interface {<int-id> | <ch-id> [brief | detail]	指定された 入力 インターフェイスの PACL 整合性チェックを実施します。
show consistency-checker pacl extended ingress ipv6 interface {<int-id> | <ch-id> [brief | detail]	指定されたIPv6入力インターフェイスのPACL整合性チェックを実施します。
show consistency-checker pacl extended ingress mac interface {<int-id> | <ch-id> [brief | detail]	指定された入力 MAC インターフェイスの PACL 整合性チェックを実施します。

コマンド	説明
show consistency-checker racl extended ingress ip module <module-id> [brief | detail]	指定した IP モジュールの入力インターフェイスおよびポートチャネルの RACL 整合性チェックを実施します。
show consistency-checker racl extended ingress ipv6 module <module-id> [brief | detail]	指定された IPv6 モジュールの入力インターフェイスおよびポートチャネルの RACL 整合性チェックを実施します。
show consistency-checker racl extended ingress ip interface {<int-id> | <ch-id> | <vlan-id>} [brief | detail]	指定された入力インターフェイスの RACL 整合性チェックを実施します。
show consistency-checker racl extended ingress ipv6 interface {<int-id> | <ch-id> | <vlan-id>} [brief | detail]	指定した入力 IPv6 インターフェイスの RACL 整合性チェックを実施します。
show consistency-checker vacl extended ingress ip vlan <vlan-id> [brief | detail]	指定された IP VLAN の VACL 整合性チェックを実施します。
show consistency-checker vacl extended ingress ipv6 vlan <vlan-id> [brief | detail]	指定された IPv6 VLAN の VACL 整合性チェックを実施します。
show consistency-checker vacl extended ingress mac vlan <vlan-id> [brief | detail]	指定された入力 MAC VLAN の VACL 整合性チェックを実施します。

ACL 整合性チェッカ コマンドの出力例

次に、RACL 整合性チェックの結果の例を示します。

```
switch# show consistency-checker racl extended ingress ip module 1 Consistency checker
passed for Eth1/3 (ingress, ip, ip-list)
switch#
switch#
switch# show consistency-checker racl extended ingress ip module 1 brief
{
   "result": {
   "status": "CC_STATUS_OK",
   "checkers": [
     {
       "version": 1,
       "type": "CC_TYPE_IF_RACL",
       "status": "CC_STATUS_OK",
        "platformDetails": {
        "classType": "CC_PLTFM_NXOS_BCM"
      },
      "recoveryActions": [],
      "failedEntities": []
      }
    ]
   }
}
switch#
switch # show consistency-checker racl extended ingress ip interface ethernet 3/5
Consistency checker passed for Ethernet3/5 (ingress, ip, ip-list)
```

```
switch#
switch# show consistency-checker racl extended ingress ip interface ethernet 3/5 brief
{
   "result": {
   "status": "CC_STATUS_OK",
    "checkers": [
      {
       "version": 1,
       "type": "CC_TYPE_IF_RACL",
       "status": "CC_STATUS_OK",
       "platformDetails": {
       "classType": "CC_PLTFM_NXOS_BCM"
      },
       "recoveryActions": [],
       "failedEntities": []
     }
    ]
  }
}
```

設定ファイル

構成ファイルには、Cisco NX-OS デバイス上の機能を構成するために使用される Cisco NX-OS コマンドが保存されます。Cisco NX-OS には、実行構成とスタートアップ構成の 2 種類があります。デバイスは、起動時にスタートアップ コンフィギュレーション（startup-config）を使用して、ソフトウェア機能を設定します。実行コンフィギュレーション（running-config）には、スタートアップコンフィギュレーションファイルに対して行った現在の変更が保存されます。設定を変更する前に、設定ファイルのバックアップを作成してください。コンフィギュレーション ファイルはリモート サーバにバックアップできます。コンフィギュレーション ファイルの詳細については、『*Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide*』を参照してください。また、設定ファイルのチェックポイントコピーを作成すれば、問題が発生した場合にロールバックすることもできます。ロールバック機能については、『*Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*』を参照してください。

Cisco NX-OS 機能は、スタートアップコンフィギュレーションファイルに内部ロックを作成することがあります。まれに、機能により作成されたロックが削除されずに残っていることがあります。**system startup-config unlock** コマンドを使用し、 して、これらのロックを削除してください。

CLI デバッグ

Cisco NX-OS は、ネットワークをアクティブにトラブルシューティングするための広範なデバッグ機能セットをサポートしています。CLI を使用して、各機能のデバッグモードを有効にし、リアルタイムで更新された制御プロトコル交換のアクティビティ ログを表示できます。各ログ エントリにはタイムスタンプがあり、時間順にリストされます。CLI ロール メカニズムを使用してデバッグ機能へのアクセスを制限し、ロール単位でアクセスを分割できます。**debug** コマンドはリアルタイム情報を表示するのに対し、**show** コマンドは、履歴情報とリアルタイム情報を一覧表示するために使用します。

注意 **debug** コマンドを使用し、 できるのは、シスコのテクニカル サポート担当者の指示があった場合に限られます。一部の **debug** コマンドはネットワーク パフォーマンスに影響を与える可能性があるからです。

（注） デバッグ メッセージは、特別なログ ファイルに記録できます。ログ ファイルは、デバッグ出力をコンソールに送信するよりも安全で、処理が容易です。

?オプションを使用すると、任意の機能で使用可能なオプションを表示できます。実際のデバッグ出力に加えて、入力されたコマンドごとにログ エントリが作成されます。デバッグ出力には、ローカルデバイスと他の隣接デバイス間で発生したアクティビティのタイムスタンプ付きアカウントが記録されます。

デバッグ機能を使用して、イベント、内部メッセージ、およびプロトコルエラーを追跡できます。ただし、実稼働環境でデバッグユーティリティを使用する場合は注意が必要です。一部のオプションは、コンソールに大量のメッセージを出力したり、ネットワーク パフォーマンスに重大な影響を与える可能性がある CPU 集約イベントを作成したりすることで、デバイスへのアクセスを妨げる可能性があります。

（注） **debug** コマンドを入力する前に、2番目の Telnet または SSH セッションを開くことを推奨します。デバッグ セッションが現在の出力ウィンドウの妨げとなる場合は、2番目のセッションを使用して **undebug all** を入力し、 デバッグ メッセージの出力を停止します。

デバッグ フィルタ

debug-filter を使用して、不要なデバッグ情報を除外できます。 コマンドを使用する必要があります。この **debug-filter** コマンドを使用すると、関連する **debug** コマンドによって生成されるデバッグ情報を制限できます。

次に、EIGRP hello パケットのデバッグ情報をイーサネット インターフェイス 2/1 に制限する例を示します。

```
switch# debug-filter ip eigrp interface ethernet 2/1
switch# debug eigrp packets hello
```

Pingおよび Traceroute

（注） ping および traceroute 機能を使用して、接続およびパスの選択に関する問題をトラブルシューティングします。これらの機能を使用して、ネットワーク パフォーマンスの問題を特定または解決しないでください。

この項で説明している **ping** および **traceroute** コマンドは、TCP/IP ネットワーキングの問題のトラブルシューティングにもっとも役立つツールの 2 つです。ping ユーティリティは、TCP/IP インターネットワークを経由する宛先に対して、一連のエコーパケットを生成します。エコーパケットは、宛先に到達すると、再ルーティングされて送信元に戻されます。

traceroute ユーティリティも同様の方法で動作しますが、ホップバイホップ ベースで宛先までの特定のパスを決定することもできます。

ping の使用

ping コマンドを使用し、 コマンドを使用すると、IPv4 ルーティング ネットワーク経由で特定の宛先への接続および遅延を確認できます。

ping6 コマンドを使用し、 コマンドを使用すると、IPv6 ルーティング ネットワーク経由で特定の宛先への接続および遅延を確認できます。

ping ユーティリティを使用すると、ポートまたはエンドデバイスにショートメッセージを送信できます。IPv4 または IPv6 アドレスを指定することにより、宛先に一連のフレームが送信できます。これらのフレームは、ターゲットデバイスに到達し、タイムスタンプが付加されて、送信元にループバックされます。

（注） Ping ユーティリティを使用して、 Nexus スイッチに構成された IP アドレスでネットワーク パフォーマンスをテストすることは推奨されません。スイッチの IP アドレス宛ての ICMP（Ping）トラフィックは、CoPP（コントロール プレーン ポリシング）の対象となり、ドロップされる可能性があります。

```
switch# ping 172.28.230.1 vrf management
PING 172.28.230.1 (172.28.230.1): 56 data bytes
64 bytes from 172.28.230.1: icmp_seq=0 ttl=254 time=1.095 ms
64 bytes from 172.28.230.1: icmp_seq=1 ttl=254 time=1.083 ms
64 bytes from 172.28.230.1: icmp_seq=2 ttl=254 time=1.101 ms
64 bytes from 172.28.230.1: icmp_seq=3 ttl=254 time=1.093 ms
64 bytes from 172.28.230.1: icmp_seq=4 ttl=254 time=1.237 ms

--- 172.28.230.1 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 1.083/1.121/1.237 ms
```

トレースルートの使用

traceroute は、次の操作のために使用します。

- データ トラフィックが経由したルートを追跡します。
- スイッチ間（ホップ単位）の遅延を計算します。

traceroute ユーティリティでは、ホップごとに使用されるパスが識別され、双方向で各ホップにタイムスタンプが付けられます。traceroute を使用すると、発信元のデバイスと送信先に最も近いデバイスの間のパスに沿ってポート接続をテストできます。

traceroute {*dest-ipv4-addr* | *hostname*} [**vrf** *vrf-name*] コマンドは IPv4 ネットワーク用に、**traceroute6** {*dest-ipv6-addr* | *hostname*} [**vrf** *vrf-name*] コマンドは IPv6 ネットワーク用に使用します。送信先に到達できない場合は、パス検出によってパスが障害ポイントまで追跡されます。

```
switch# traceroute 172.28.254.254 vrf management
traceroute to 172.28.254.254 (172.28.254.254), 30 hops max, 40 byte packets
 1  172.28.230.1 (172.28.230.1)  0.941 ms  0.676 ms  0.585 ms
 2  172.24.114.213 (172.24.114.213)  0.733 ms  0.7 ms  0.69 ms
 3  172.20.147.46 (172.20.147.46)  0.671 ms  0.619 ms  0.615 ms
 4  172.28.254.254 (172.28.254.254)  0.613 ms  0.628 ms  0.61 ms
```

実行中の traceroute を終了するには、**Ctrl-C** を押します。

次のコマンドを使用して、traceroute の送信元インターフェイスを指定できます。

コマンド	目的
traceroute {*dest-ipv4-addr* | *hostname*} [**source** {*dest-ipv4-addr* | *hostname* | *interface*}] [**vrf** *vrf-name*] **例**： `switch# traceroute 112.112.112.1 source vlan 10`	指定した IP アドレス、ホスト名、またはインターフェイスからの、traceroute パケットの送信元 IPv4 アドレスを指定します。
traceroute6 {*dest-ipv6-addr* | *hostname*} [**source** {*dest-ipv6-addr* | *hostname* | *interface*}] [**vrf** *vrf-name*] **例**： `switch# traceroute6 2010:11:22:0:1000::1 source ethernet 2/2`	指定した IP アドレス、ホスト名、またはインターフェイスからの、traceroute6 パケットの送信元 IPv6 アドレスを指定します。
[**no**] **ip traceroute source-interface** *interface* [**vrf** *vrf-name*] **例**： `switch(config)# ip traceroute source-interface loopback 1`	設定されたインターフェイスから送信元 IP アドレスを持つ traceroute または traceroute6 パケットを生成します。

コマンド	目的

show ip traceroute source-interface [**vrf** *vrf-name*]
例：
`switch# show ip traceroute source-interface vrf all`
`VRF Name Interface`
`default loopback1`
	traceroute のために設定された送信元インターフェイスを表示します。

ip icmp-errors source-interface *interface*
例 1：
`switch(config)# ip icmp-errors source-interface loopback 1`
例 2：
`switch(config)# vrf context vrf-blue`
`switch(config-vrf)# ip icmp-errors source-interface loopback 2`
	設定されたインターフェイスから送信元 IPv4 または IPv6 アドレスを持つ ICMP エラー パケットを生成します。
	また、Virtual Routing and Forwarding（VRF）インスタンス内のスタティック ルートでの BFD を設定することもできます。

プロセスおよび CPU のモニタリング

show processes コマンドを使用し、すれば、実行中のプロセスおよび各プロセスのステータスを確認できます。コマンド出力には次が含まれます。

- PID = プロセス ID
- State = プロセスの状態
- PC = 現在のプログラム カウンタ（16 進形式）
- Start_cnt = プロセスがこれまでに開始（または再開）された回数
- TTY = プロセスを制御している端末通常、「-」（ハイフン）は、特定の TTY 上で実行されていないデーモンを表します。
- Process = プロセスの名前

プロセスの状態は次のとおりです。

- D = 中断なしで休止（通常 I/O）
- R = 実行可能（実行キュー上）
- S = 休止中
- T = トレースまたは停止

- Z = 機能していない (「ゾンビ」) プロセス
- NR = 実行されていない
- ER = 実行されているべきだが、現在は実行されていない

（注） 一般に、ER 状態は、プロセスの再起動回数が多すぎるために、システムが障害発生と判断してそのプロセスをディセーブルにしたことを示しています。

```
switch# show processes ?
cpu      Show processes CPU Info
log      Show information about process logs
memory   Show processes Memory Info

switch# show processes
PID    State  PC        Start_cnt    TTY   Type  Process
-----  -----  --------  -----------  ----  ----  -------------
    1      S  b7f9e468            1     -     O  init
    2      S         0            1     -     O  migration/0
    3      S         0            1     -     O  ksoftirqd/0
    4      S         0            1     -     O  desched/0
    5      S         0            1     -     O  migration/1
    6      S         0            1     -     O  ksoftirqd/1
    7      S         0            1     -     O  desched/1
    8      S         0            1     -     O  events/0
    9      S         0            1     -     O  events/1
   10      S         0            1     -     O  khelper
   15      S         0            1     -     O  kthread
   24      S         0            1     -     O  kacpid
  103      S         0            1     -     O  kblockd/0
  104      S         0            1     -     O  kblockd/1
  117      S         0            1     -     O  khubd
  184      S         0            1     -     O  pdflush
  185      S         0            1     -     O  pdflush
  187      S         0            1     -     O  aio/0
  188      S         0            1     -     O  aio/1
  189      S         0            1     -     O  SerrLogKthread

...
```

show processes cpu コマンドの使用

show processes cpu コマンドを使用し、 コマンドを使用して、CPU 利用率を表示します。コマンド出力には次が含まれます。

- Runtime(ms) = プロセスが使用した CPU 時間（ミリ秒単位）
- Invoked = プロセスがこれまでに開始された回数
- uSecs = プロセスの呼び出しごとの平均 CPU 時間（ミリ秒単位）
- 1Sec = 最近の 1 秒間における CPU 使用率（パーセント単位）

```
switch# show processes cpu
PID    Runtime(ms)  Invoked   uSecs  1Sec   Process
-----  -----------  --------  -----  -----  -----------
    1         2264    108252     20      0  init
    2          950    211341      4      0  migration/0
    3         1154  32833341      0      0  ksoftirqd/0
    4          609    419568      1      0  desched/0
    5          758    214253      3      0  migration/1
    6         2462  155309355     0      0  ksoftirqd/1
    7         2496    392083      6      0  desched/1
    8          443    282990      1      0  events/0
    9          578    260184      2      0  events/1
   10           56      2681     21      0  khelper
   15            0        30     25      0  kthread
   24            0         2      5      0  kacpid
  103           81        89    914      0  kblockd/0
  104           56       265    213      0  kblockd/1
  117            0         5     17      0  khubd
  184            0         3      3      0  pdflush
  185         1796    104798     17      0  pdflush
  187            0         2      3      0  aio/0
  188            0         2      3      0  aio/1
  189            0         1      3      0  SerrLogKthread
...
```

show system resources コマンドの使用

show system resources コマンドを使用し、すれば、システム関連の CPU およびメモリの統計情報を表示できます。このコマンドの出力には、次の情報が表示されます。

- 実行中プロセスの平均数として定義された負荷。Load average には、過去 1 分間、5 分間、および 15 分間のシステム負荷が表示されます。
- Processes には、システム内のプロセス数、およびコマンド発行時に実際に実行されていたプロセス数が表示されます。
- CPU states には、直前の 1 秒間における CPU のユーザ モードとカーネル モードでの使用率およびアイドル時間がパーセントで表示されます。
- Memory usage には、合計メモリ、使用中メモリ、空きメモリ、バッファに使用されているメモリ、およびキャッシュに使用されているメモリがキロバイト単位で表示されます。また、buffers および cache の値には、使用中メモリの統計情報も含まれます。

```
switch# show system resources
Load average:   1 minute: 0.00   5 minutes: 0.02   15 minutes: 0.05
Processes   :   355 total, 1 running
CPU states  :   0.0% user,   0.2% kernel,   99.8% idle
        CPU0 states  :   0.0% user,   1.0% kernel,   99.0% idle
        CPU1 states  :   0.0% user,   0.0% kernel,   100.0% idle
        CPU2 states  :   0.0% user,   0.0% kernel,   100.0% idle
        CPU3 states  :   0.0% user,   0.0% kernel,   100.0% idle
Memory usage:   16402560K total,   2664308K used,   13738252K free
Current memory status: OK
```

オンボード障害ロギングの使用

Cisco NX-OS では、障害データを永続的ストレージに記録する機能が提供されます。この記録は、分析用に取得したり、表示したりできます。このOBFL機能は、障害および環境情報をモジュールの不揮発性メモリに保管します。この情報は、障害モジュールの分析に役立ちます。

OBFL 機能によって保存されるデータは、次のとおりです。

- 初期電源オンの時間
- モジュールのシャーシ スロット番号
- モジュールの初期温度
- ファームウェア、BIOS、FPGA、および ASIC のバージョン
- モジュールのシリアル番号
- クラッシュのスタック トレース
- CPU hog 情報
- メモリ リーク情報
- ソフトウェア エラー メッセージ
- ハードウェア例外ログ
- 環境履歴
- OBFL 固有の履歴情報
- ASIC 割り込みおよびエラー統計の履歴
- ASIC レジスタ ダンプ

OBFL の設定の詳細については、『*Cisco Nexus 9000 Series NX-OS* システム管理設定』を参照してください。

OBFL エラー ステータス コマンドの使用

Cisco NX-OS リリース 9.3(3) 以降、Cisco Nexus 9000 シリーズ スイッチはさまざまなカウンタをサポートし、ファイバ チャネル インターフェイスをモニタし記録します。カウンタは、FCMAC レベルでの問題の特定とトラブルシューティングに役立ちます。

show logging onboard error-stats コマンドを使用し、 コマンドはオンボード エラー統計情報を表示します。出力には、次のカウンタが含まれます。

- FCP_CNTR_MAC_RX_BAD_WORDS_FROM_DECODER
- FCP_CNTR_MAC_RX_EOFA
- FCP_CNTR_MAC_RX_CRC

- FCP_CNTR_MAC_RX_MAX_FRAME_TRUNCATE
- FCP_CNTR_MAC_RX_MIN_FRAME_PAD
- FCP_CNTR_CREDIT_LOSS
- FCP_CNTR_TX_WT_AVG_B2B_ZERO

次に、この **show logging onboard error-stats** コマンドの出力例を示します。

```
switch# show logging onboard error-stats
----------------------------
    Module:  1
----------------------------


-------------------------------------------------------------------------------------------------
ERROR STATISTICS INFORMATION FOR DEVICE: FCMAC
-------------------------------------------------------------------------------------------------
Interface Range    |                                          |          |Time Stamp
                   |            Error Stat Counter Name       |  Count   |MM/DD/YY HH:MM:SS

                   |                                          |          |
-------------------------------------------------------------------------------------------------
fc1/9              |FCP_CNTR_MAC_RX_BAD_WORDS_FROM_DECODER    |4         |11/15/19 09:54:40
fc1/33             |FCP_CNTR_MAC_RX_BAD_WORDS_FROM_DECODER    |4         |11/15/19 09:37:53
fc1/36             |FCP_CNTR_MAC_RX_BAD_WORDS_FROM_DECODER    |4         |11/15/19 09:05:13
fc1/37             |FCP_CNTR_MAC_RX_BAD_WORDS_FROM_DECODER    |4         |11/15/19 08:42:56
fc1/37             |FCP_CNTR_MAC_RX_BAD_WORDS_FROM_DECODER    |4         |11/15/19 08:21:19
fc1/28             |FCP_CNTR_MAC_RX_BAD_WORDS_FROM_DECODER    |4         |11/15/19 08:20:59
fc1/9              |FCP_CNTR_MAC_RX_BAD_WORDS_FROM_DECODER    |5996      |11/14/19 10:25:45
fc1/9              |FCP_CNTR_MAC_RX_BAD_WORDS_FROM_DECODER    |5992      |11/14/19 06:19:04
fc1/36             |FCP_CNTR_MAC_RX_BAD_WORDS_FROM_DECODER    |22112     |11/14/19 06:19:04
fc1/36             |FCP_CNTR_MAC_RX_BAD_WORDS_FROM_DECODER    |21876     |11/14/19 06:18:44
fc1/36             |FCP_CNTR_MAC_RX_BAD_WORDS_FROM_DECODER    |21368     |11/14/19 06:18:24
fc1/36             |FCP_CNTR_MAC_RX_BAD_WORDS_FROM_DECODER    |20872     |11/14/19 06:18:04
fc1/36             |FCP_CNTR_MAC_RX_BAD_WORDS_FROM_DECODER    |20292     |11/14/19 06:17:44
fc1/36             |FCP_CNTR_MAC_RX_BAD_WORDS_FROM_DECODER    |19720     |11/14/19 06:17:24
fc1/36             |FCP_CNTR_MAC_RX_BAD_WORDS_FROM_DECODER    |19284     |11/14/19 06:17:04
fc1/36             |FCP_CNTR_MAC_RX_BAD_WORDS_FROM_DECODER    |18788     |11/14/19 06:16:44
```

診断の使用

Cisco Generic Online Diagnostics（GOLD）では、複数のシスコ プラットフォームにまたがる診断操作の共通フレームワークを定義しています。GOLD の実装により、ハードウェア コンポーネントの健全性を確認し、システム データおよびコントロール プレーンの動作の適切性を検証できます。テストにはシステムの起動時に有効になるものと、システムの実行中に有効になるものがあります。ブートモジュールは、オンラインになる前に一連のチェックを実行して、システムの起動時にハードウェア コンポーネントの障害を検出し、障害のあるモジュールが稼働中のネットワークに導入されないようにします。

システムの動作時または実行時にも不具合が診断されます。一連の診断チェックを設定して、オンライン システムの状態を確認できます。中断を伴う診断テストと中断を伴わない診断テストを区別する必要があります。中断のないテストはバックグラウンドで実行され、システム データまたはコントロール プレーンには影響しませんが、中断のあるテストはライブ パケット フローに影響します。特別なメンテナンス期間中に中断テストをスケジュールする必要があ

ります。この項で説明している **show diagnostic content module** コマンド出力には、中断を伴うテストや中断を伴わないテストなどのテスト属性が表示されます。

ランタイム診断チェックは、特定の時刻に実行するか、バックグラウンドで継続的に実行するように設定できます。

ヘルスモニタリング診断テストは中断を伴わず、システムの動作中にバックグラウンドで実行されます。オンライン診断ヘルス モニタリングの役割は、ライブ ネットワーク環境でハードウェア障害を予防的に検出し、障害を通知することです。

GOLDは、すべてのテストの診断結果と詳細な統計情報を収集します。これには、最後の実行時間、最初と最後のテスト合格時間、最初と最後のテスト失敗時間、合計実行回数、合計失敗回数、連続失敗回数、およびエラーコードが含まれます。これらのテスト結果は、管理者がシステムの状態を判断し、システム障害の原因を理解するのに役立ちます。**show diagnostic result** コマンドを使用し、 コマンドを使用して、診断結果を表示します。

GOLD の設定の詳細については、『*Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*』を参照してください。

組み込まれている Event Manager の使用

Embedded Event Manager（EEM）は、主要なシステム イベントをモニタし、設定されたポリシーを介してそれらのイベントを処理できるポリシーベースのフレームワークです。ポリシーは、設定されたイベントの発生に基づいてデバイスが呼び出すアクションを定義する、ロード可能な事前にプログラムされたスクリプトです。このスクリプトは、カスタム syslog または SNMP トラップの生成、CLI コマンドの呼び出し、フェールオーバーの強制などを含むアクションを生成できます。

EEM の設定の詳細については、「*Cisco Nexus 9000* シリーズ *NX-OS* システム管理設定ガイド」を参照してください。

Ethanalyzer の使用

Ethanalyzer は、Wireshark（旧称 Ethereal）のターミナル バージョンであるオープン ソース ソフトウェア TShark の Cisco NX-OS プロトコル アナライザツール実装です。Ethanalyzer を使用して、すべてのNexusプラットフォームのインバンドおよび管理インターフェイス上のコントロールプレーン トラフィックをキャプチャおよび分析することで、ネットワークのトラブルシューティングを行うことができます。

Ethanalyzer を設定するには、次のコマンドを使用します。

コマンド	目的
ethanalyzer local interface inband	インバンドインターフェイスを介してスーパーバイザによって送受信されたパケットをキャプチャし、キャプチャされたパケットの要約プロトコル情報を表示します。

コマンド	目的
ethanalyzer local interface inband-in	インバンドインターフェイスを介してスーパーバイザが受信したパケットをキャプチャし、キャプチャされたパケットの要約プロトコル情報を表示します。
ethanalyzer local interface inband-out	スーパーバイザからインバンドインターフェイスを介して送信されたパケットをキャプチャし、キャプチャされたパケットのプロトコル情報のサマリーを表示します。
ethanalyzer local interface mgmt	管理インターフェイスを介して送受信されたパケットをキャプチャし、キャプチャされたパケットのプロトコル情報のサマリーが表示されます。
ethanalyzer local interface front-panel	レイヤ3（ルーテッド）前面パネルポートを介してスーパーバイザによって送受信されたパケットがキャプチャされ、キャプチャされたパケットのプロトコル情報のサマリー情報が表示されます。 （注） このコマンドは、レイヤ 2（スイッチポート）前面パネルポートを介してスーパーバイザが送受信するパケットのキャプチャをサポートしません。
ethanalyzer local interface port-channel	スーパーバイザがレイヤ3（ルーテッド）ポートチャネルインターフェイスを介して送受信したパケットをキャプチャし、キャプチャしたパケットのプロトコル情報のサマリーを表示します。 （注） このコマンドは、スーパーバイザがレイヤ 2（スイッチポート）ポートチャネルインターフェイスを介して送受信するパケットのキャプチャをサポートしていません。
ethanalyzer local interface vlan	スーパーバイザがレイヤ 3 スイッチ仮想インターフェイス（SVI）を介して送受信したパケットをキャプチャし、プロトコル情報のサマリーを表示します。

コマンド	目的
ethanalyzer local interface netstack	Netstack ソフトウェアコンポーネントを介してスーパーバイザによって送受信されたパケットをキャプチャし、プロトコル情報のサマリーを表示します。
{|||||| } **ethanalyzer local interfacefrontpanelinbandinbandinbandinbandoutmgmtportchannelvlanlimitcapturedframes**	Ethanalyzer セッション内でキャプチャするフレーム数を制限します。フレーム数には、0〜500,000 の整数値を指定できます。0 を指定すると、Ethanalyzer セッションが自動的に停止する前に最大 500,000 フレームがキャプチャされます。
{|||||| } **ethanalyzer local interfacefrontpanelinbandinbandinbandinbandoutmgmtportchannelvlanlimitframesize**	キャプチャするフレームの長さを制限します。フレームの長さは、192〜65,536 の整数値にすることができます。
{|||||| } **ethanalyzer local interfacefrontpanelinbandinbandinbandinbandoutmgmtportchannelvlancapturefilter**	Berkeley Packet Filter（BPF）構文を使用してキャプチャするパケットのタイプをフィルタリングします。
{|||||| } **ethanalyzer local interfacefrontpanelinbandinbandinbandinbandoutmgmtport-channelvlandisplayfilter**	Wireshark または TShark表示フィルタを使用して、表示するキャプチャされたパケットのタイプをフィルタリングします。
{|||||| } **ethanalyzer local interfacefrontpanelinbandinbandinbandinbandoutmgmtport-channelvlanwrite**	キャプチャしたデータをファイルに保存します。有効なストレージオプションには、スイッチのブート フラッシュ、ログ フラッシュ、USB ストレージデバイス、または揮発性ストレージがあります。
ethanalyzer local read	キャプチャされたデータ ファイルを開いて分析ファイルを。有効なストレージ オプションには、スイッチのブート フラッシュ、ログ フラッシュ、USB ストレージデバイス、または揮発性ストレージがあります。
{|||||| } **ethanalyzer local interfacefrontpanelinbandinbandinbandinbandoutmgmtport-channelvlanautostop**	Ethanalyzer セッションを自動的に停止する条件を指定します。セッションの継続時間（秒）、**write** キーワードを使用してキャプチャパケットをファイルに書き込むときにキャプチャするファイル数、および **write** キーワードを使用してキャプチャパケットをファイルに書き込むときにファイルサイズを指定できます。

コマンド	目的
{| | | | | | } **ethanalyzer local interface** **front-panel** **inband** **inband-in** **inband-out** **mgmt** **port-channel** **vlan** **capture** **ring-buffer**	Ethanalyzer のキャプチャリング バッファ オプションを指定します。このオプションは、write キーワードと組み合わせて使用すると、リング バッファ内の 1 つ以上のファイルに継続的に書き込まれます。新しいファイルに書き込む前に Ethanalyzer が待機する時間（秒単位）、リング バッファの一部として保持するファイルの数、およびリングバッファ内の個々のファイルのファイルサイズを指定できます。
{| | | | | | } **ethanalyzer local interface** **front-panel** **inband** **inband-in** **inband-out** **mgmt** **port-channel** **vlan** **detail**	キャプチャしたパケットの詳細なプロトコル情報を表示します。
{| | | | | | } **ethanalyzer local interface** **front-panel** **inband** **inband-in** **inband-out** **mgmt** **port-channel** **vlan** **raw**	キャプチャされたパケットを 16進数形式で表示します。
{| | | | | | } **ethanalyzer local interface** **front-panel** **inband** **inband-in** **inband-out** **mgmt** **port-channel** **vlan** **vrf**	レイヤ 3 インターフェイスがデフォルト以外の VRF にある場合に、レイヤ 3 インターフェイスがメンバーである VRF を指定します。

ガイドラインと制約事項

- レイヤ 3 インターフェイスがデフォルト以外の VRF のメンバーであり、Ethanalyzer セッションで指定されている場合（たとえば、**ethanalyzer local interface front-panel ethernet1/1** または **ethanalyzer local interface port-channel1** コマンドを使用）、**vrf** キーワードを使用して、レイヤ 3 インターフェイスが Ethanalyzer セッション内のメンバーである VRF を指定する必要があります。たとえば、スーパーバイザが VRF「red」のレイヤ 3 前面パネルポート Ethernet1/1 を介して受信または送信したパケットをキャプチャするには、**ethanalyzer local interface front-panel ethernet1/1 vrf red** コマンドを使用します。
- ファイルへの書き込み時に、Ethanalyzer セッションが 500,000 パケットをキャプチャした場合、またはファイルのサイズが 11 MB に達した場合、Ethanalyzer は自動的に停止します。

例

```
switch(config)# ethanalyzer local interface inband
<CR>
> Redirect it to a file
>> Redirect it to a file in append mode
autostop Capture autostop condition
capture-filter Filter on ethanalyzer capture capture-ring-buffer Capture ring buffer
option
decode-internal Include internal system header decoding detail Display detailed protocol
 information
display-filter Display filter on frames captured
limit-captured-frames Maximum number of frames to be captured (default is 10)
limit-frame-size Capture only a subset of a frame
mirror Filter mirrored packets
```

```
raw Hex/Ascii dump the packet with possibly one line summary
write Filename to save capture to
| Pipe command output to filter

switch(config)# ethanalyzer local interface inband Capturing on 'ps-inb'

1 2021-07-26 09:36:36.395756813 00:22:bd:cf:b9:01 → 00:22:bd:cf:b9:00 0x3737 64 PRI:
7 DEI: 0 ID: 4033
2 2021-07-26 09:36:36.395874466 00:22:bd:cf:b9:01 → 00:22:bd:cf:b9:00 0x3737 205 PRI:
7 DEI: 0 ID: 4033
4 3 2021-07-26 09:36:36.395923840 00:22:bd:cf:b9:01 → 00:22:bd:cf:b9:00 0x3737 806 PRI:
7 DEI: 0 ID: 4033
4 2021-07-26 09:36:36.395984384 00:22:bd:cf:b9:01 → 00:22:bd:cf:b9:00 0x3737 1307 PRI:
7 DEI: 0 ID: 4033
5 2021-07-26 09:37:36.406020552 00:22:bd:cf:b9:01 → 00:22:bd:cf:b9:00 0x3737 64 PRI:
7 DEI: 0 ID: 4033
6 2021-07-26 09:37:36.406155603 00:22:bd:cf:b9:01 → 00:22:bd:cf:b9:00 0x3737 205 PRI:
7 DEI: 0 ID: 4033
7 2021-07-26 09:37:36.406220547 00:22:bd:cf:b9:01 → 00:22:bd:cf:b9:00 0x3737 806 PRI:
7 DEI: 0 ID: 4033
8 8 2021-07-26 09:37:36.406297734 00:22:bd:cf:b9:01 → 00:22:bd:cf:b9:00 0x3737 1307
PRI: 7 DEI: 0 ID: 4033
9 2021-07-26 09:38:36.408983263 00:22:bd:cf:b9:01 → 00:22:bd:cf:b9:00 0x3737 64 PRI:
7 DEI: 0 ID: 4033
10 10 2021-07-26 09:38:36.409101470 00:22:bd:cf:b9:01 → 00:22:bd:cf:b9:00 0x3737 205
PRI: 7 DEI: 0 ID: 4033
```

詳細なプロトコル情報を表示するには、「**detail** オプションを使用します必要に応じて、キャプチャの途中で Ctrl + C を使用して中止し、スイッチプロンプトを戻すことができます。

```
switch(config)# ethanalyzer local interface inband detail
Capturing on 'ps-inb'
Frame 1: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface ps-inb,
 id 0
Interface id: 0 (ps-inb) Interface name: ps-inb
Encapsulation type: Ethernet (1)
Arrival Time: Jul 26, 2021 11:54:37.155791496 UTC
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1627300477.155791496 seconds
[Time delta from previous captured frame: 0.000000000 seconds] [Time delta from previous
 displayed frame: 0.000000000 seconds] [Time since reference or first frame: 0.000000000
 seconds] Frame Number: 1
Frame Length: 64 bytes (512 bits)
Capture Length: 64 bytes (512 bits) [Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:vlan:ethertype:data] Ethernet II, Src:
00:22:bd:cf:b9:01, Dst: 00:22:bd:cf:b9:00
Destination: 00:22:bd:cf:b9:00 Address: 00:22:bd:cf:b9:00
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast) Source:
00:22:bd:cf:b9:01
Address: 00:22:bd:cf:b9:01
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast) Type: 802.1Q Virtual
 LAN (0x8100)
802.1Q Virtual LAN, PRI: 7, DEI: 0, ID: 4033
111. .... .... .... = Priority: Network Control (7) 4 ...0 .... .... .... = DEI: Ineligible
.... 1111 1100 0001 = ID: 4033
Type: Unknown (0x3737) Data (46 bytes)

0000 a9 04 00 00 7d a2 fe 60 47 4f 4c 44 00 0b 0b 0b ....}..`GOLD....
0010 0b 0b 0b 0b 0b 0b 0b 0b 0b 0b 0b 0b 0b 0b 0b 0b ................
```

```
0020 0b 0b 0b 0b 0b 0b 0b 0b 0b 0b 0b 0b 0b 0b ..............
Data: a90400007da2fe60474f4c44000b0b0b0b0b0b0b0b0b0b0b… [Length: 46]
```

キャプチャ中に表示するか、あるいはディスクに保存するパケットを選択するには、「**capture-filter**オプションを使用します。キャプチャ フィルタは、フィルタ処理中に高率のキャプチャを維持します。パケットの完全な分析は行われていないので、フィルタ フィールドはあらかじめ決められており、限定されています。

キャプチャ ファイルのビューを変更するには、**display-filter**オプションを使用します。ディスプレイ フィルタでは、完全に分割されたパケットを使用するため、ネットワーク トレース ファイルを分析する際に非常に複雑かつ高度なフィルタリングを実行できます。Ethanalyzer は、キャプチャしたデータを他のファイルに書き込むように指示されていない場合、キャプチャしたデータを一時ファイルに書き込みます。この一時ファイルは、**capture-filter** オプションに一致するすべてのパケットが一時ファイルに書き込まれますが、**display-filter** オプションに一致するパケットのみが表示されるため、ユーザの知らない間に表示フィルタが使用されるとすぐにいっぱいになります。

この例では、**limit-captured-frames** が 5 に設定されています。**capture-filter** オプションを使用すると、Ethanalyzer では、フィルタ **host 10.10.10.2** に一致する 5 つのパケットを表示します。「**display-filter**オプションを使用すると、Ethanalyzer では、まず 5 つのパケットをキャプチャし、フィルタ「**ip.addr==10.10.10.2**」に一致するパケットのみを表示します。

```
switch(config)# ethanalyzer local interface inband capture-filter "host 10.10.10.2"
limit-captured-frames 5
Capturing on inband
2013-02-10 12:51:52.150404 10.10.10.1 -> 10.10.10.2 UDP Source port: 3200 Destination
port:
3200
2013-02-10 12:51:52.150480 10.10.10.2 -> 10.10.10.1 UDP Source port: 3200 Destination
port:
3200
2013-02-10 12:51:52.496447 10.10.10.2 -> 10.10.10.1 UDP Source port: 3200 Destination
port:
3200
2013-02-10 12:51:52.497201 10.10.10.1 -> 10.10.10.2 UDP Source port: 3200 Destination
port:
3200
2013-02-10 12:51:53.149831 10.10.10.1 -> 10.10.10.2 UDP Source port: 3200 Destination
port:
3200
5 packets captured
switch(config)# ethanalyzer local interface inband display-filter "ip.addr==10.10.10.2"
 limit-captured-frame 5
Capturing on inband
2013-02-10 12:53:54.217462 10.10.10.1 -> 10.10.10.2 UDP Source port: 3200 Destination
port:
3200
2013-02-10 12:53:54.217819 10.10.10.2 -> 10.10.10.1 UDP Source port: 3200 Destination
port:
3200
2 packets captured
```

write オプションを使用して、後で分析するために Cisco Nexus 9000 シリーズ スイッチ上のストレージデバイスの 1 つ（boothflash、logflash など）にあるファイルにキャプチャ データを書き込むことができます。キャプチャ ファイルのサイズは、10 MB に制限されます。

「**write**」オプションを使用した Ethanalyzer のコマンド例は、**ethanalyzer local interface inband writebootflash:***capture_file_name* です。次は **capture-filter** を使用した **write** オプションの例と **first-capture** の出力ファイル名を示します。

```
switch(config)# ethanalyzer local interface inband capture-filter "host 10.10.10.2"
limit-captured-frame 5 write ?
bootflash: Filename logflash: Filename slot0:     Filename
usb1:      Filename
usb2: Filename volatile: Filename
switch(config)# ethanalyzer local interface inband capture-filter "host 10.10.10.2"
limit-captured-frame 5 write bootflash:first-capture
```

キャプチャ データがファイルに保存されるとき、デフォルトでは、キャプチャされたパケットはターミナル ウィンドウに表示されません。「**display** オプションを使用すると、Cisco NX-OS では、キャプチャ データをファイルに保存しながら、パケットを表示します。

capture-ring-buffer オプションを使用すると、指定した秒数、指定したファイル数、または指定したファイルのサイズの後に複数のファイルが作成されます次に、これらのオプションの定義を示します。

```
switch(config)# ethanalyzer local interface inband capture-ring-buffer ?
duration Stop writing to the file or switch to the next file after value seconds have
elapsed
files Stop writing to capture files after value number of files were written or begin
again with the first file after value number of files were
written (form a ring buffer)
filesize Stop writing to a capture file or switch to the next file after it reaches a
size of value kilobytes
```

read オプションを使用すると、デバイス自体に保存されたファイルを読み取ることができます。

```
switch(config)# ethanalyzer local read bootflash:first-capture
2013-02-10 12:51:52.150404 10.10.10.1 -> 10.10.10.2 UDP Source port: 3200 Destination
port:
3200
2013-02-10 12:51:52.150480 10.10.10.2 -> 10.10.10.1 UDP Source port: 3200 Destination
port:
3200
2013-02-10 12:51:52.496447 10.10.10.2 -> 10.10.10.1 UDP Source port: 3200 Destination
port:
3200
2013-02-10 12:51:52.497201 10.10.10.1 -> 10.10.10.2 UDP Source port: 3200 Destination
port:
3200
2013-02-10 12:51:53.149831 10.10.10.1 -> 10.10.10.2 UDP Source port: 3200 Destination
port:
3200

switch(config)# ethanalyzer local read bootflash:first-capture detail Frame 1 (110 bytes
 on wire, 78 bytes captured)
------------------------------SNIP-----------------------------------------------
[Frame is marked: False]
[Protocols in frame: eth:ip:udp:data]
Ethernet II Src: 00:24:98:6f:ba:c4 (00:24:98:6f:ba:c4), Dst: 00:26:51:ce:0f:44
(00:26:51:ce:0f:44)
Destination: 00:26:51:ce:0f:44 (00:26:51:ce:0f:44) Address: 00:26:51:ce:0f:44
(00:26:51:ce:0f:44)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default) Source:
 00:24:98:ce:6f:ba:c4 (00:24:98:6f:ba:c4)
Address: 00:24:98:6f:ba:c4 (00:24:98:6f:ba:c4)
```

```
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default) Type:
 IP (0x0800)
Internet Protocol, Src: 10.10.10.1 (10.10.10.1), Dst: 10.10.10.2 (10.10.10.2)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0xc0 (DSC) 0x30: Class Selector 6; ECN: 0x00)
------------------------------SNIP-----------------------------------------------
```

サーバまたは PC にファイルを転送し、ファイル。cap ファイルまたは 。pcap ファイルを読み取ることができる Wireshark や他のアプリケーションでそのファイル形式を読み取ることもできます。

```
switch(config)# copy bootflash:first-capture tftp:
Enter vrf (If no input, current vrf 'default' is considered): management
Enter hostname for the tftp server: 192.168.21.22
Trying to connect to tftp server......
Connection to Server Established. TFTP put operation was successful
Copy complete.
```

decode-internal オプションは、Nexus 9000 のパケット転送方法に関する内部情報を報告します。この情報は、CPU を通過するパケットのフローを理解し、トラブルシューティングするのに役立ちます。

```
switch(config)# ethanalyzer local interface inband decode-internal capture-filter "host
 10.10.10.2" limit-captured-frame 5 detail
Capturing on inband NXOS Protocol
NXOS VLAN: 0==================->VLAN in decimal=0=L3 interface
NXOS SOURCE INDEX: 1024 ==================->PIXN LTL source index in decimal=400=SUP
inband
NXOS DEST INDEX: 2569==================-> PIXN LTL destination index in
decimal=0xa09=e1/25 Frame 1: (70 bytes on wire, 70 bytes captured)
Arrival Time: Feb 10, 2013 22:40:02.216492000
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1627300477.155791496 seconds
[Time delta from previous captured frame: 0.000000000 seconds] [Time delta from previous
 displayed frame: 0.000000000 seconds] [Time since reference or first frame: 0.000000000
 seconds] Frame Number: 1
Frame Length: 70 bytes Capture Length: 70 bytes [Frame is marked: False]
[Protocols in frame: eth:ip:udp:data]
Ethernet II, Src: 00:26:51:ce:0f:43 (00:26:51:ce:0f:43), Dst: 00:24:98:6f:ba:c3
(00:24:98:6f:ba:c3)
Destination: 00:24:98:6f:ba:c3 (00:24:98:6f:ba:c3) Address: 00:24:98:6f:ba:c3
(00:24:98:6f:ba:c3)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default) Source:
 00:26:51:ce:0f:43 (00:26:51:ce:0f:43)
------------------------------SNIP-----------------------------------------------
```

NX-OS インデックスを 16 進数に変換してから、Local Target Logic（LTL）インデックスを物理または論理インターフェイスにマップするために **show system internal pixm info ltl {index}** コマンドを使用します。

1 つの IP ホストとの間でやり取りされるトラフィックのキャプチャ

```
host 1.1.1.1
```

IP アドレスの範囲との間でやり取りされるトラフィックのキャプチャ

```
net 172.16.7.0/24
```

net 172.16.7.0 mask 255.255.255.0

IP アドレスの範囲からのトラフィックのキャプチャ

```
src net 172.16.7.0/24
```

srcnet 172.16.7.0 mask 255.255.255.0

IP アドレスの範囲へのトラフィックのキャプチャ

```
dst net 172.16.7.0/24
```

dst net 172.16.7.0 mask 255.255.255.0

UDLD、VTP、CDP のトラフィックのキャプチャ

UDLD は 単方向リンク検出、VTP は VLAN Trunking Protocol、CDP は Cisco Discovery Protocol です。

ether host 01□00□0c□cc□cc□cc

MAC アドレスとの間でやり取りされるトラフィックのキャプチャ

ether host 00□01□02□03□04□05

（注） and = &&

or = ||

Not = !

MAC address format : xx:xx:xx:xx:xx:xx

一般的なコントロール プレーン プロトコル

- UDLD: Destination Media Access Controller (DMAC) = 01-00-0C-CC-CC-CC and EthType = 0x0111
- LACP: DMAC = 01:80:C2:00:00:02 and EthType = 0x8809. LACP stands for Link Aggregation Control Protocol
- STP: DMAC = 01:80:C2:00:00:00 and EthType = 0x4242 - or - DMAC = 01:00:0C:CC:CC:CD and EthType = 0x010B
- CDP: DMAC = 01-00-0C-CC-CC-CC and EthType = 0x2000
- LLDP: DMAC = 01:80:C2:00:00:0E or 01:80:C2:00:00:03 or 01:80:C2:00:00:00 and EthType = 0x88CC
- DOT1X: DMAC = 01:80:C2:00:00:03 and EthType = 0x888E. DOT1X stands for IEEE 802.1x
- IPv6: EthType = 0x86DD

- UDP と TCP のポート番号のリスト

Ethanalyzer は、Cisco NX-OS がハードウェアで転送するデータ トラフィックはキャプチャしません。

Ethanalyzer は、**tcpdump** と同じキャプチャ フィルタ構文を使用します。 および Wireshark表示フィルタ構文を使用します。

次の例では、キャプチャされたデータ（4 パケットに限定された）を管理インターフェイス上に表示します。

```
switch(config)# ethanalyzer local interface mgmt limit-captured-frames 4
Capturing on eth1

2013-05-18 13:21:21.841182 172.28.230.2 -> 224.0.0.2 BGP Hello (state Standy)
2013-05-18 13:21:21.842190 10.86.249.17 -> 172.28.231.193 TCP 4261 > telnet [AC] Seq=0
Ack=0 Win=64475 Len=0
2013-05-18 13:21:21.843039 172.28.231.193 -> 10.86.249.17 TELNET Telnet Data ..
2013-05-18 13:21:21.850463 00:13:5f:1c:ee:80 -> ab:00:00:02:00:00 0x6002 DEC DN

Remote Console
4 packets captured
```

次の例では、1 つの HSRP パケットについてキャプチャしたデータの詳細を表示します。

```
switch(config)# ethanalyzer local interface mgmt capture-filter "udp port 1985"
limit-captured-frames 1
Capturing on eth1
Frame 1 (62 bytes on wire, 62 bytes captured)
Arrival Time: May 18, 2013 13:29:19.961280000
[Time delta from previous captured frame: 1203341359.961280000 seconds]
[Time delta from previous displayed frame: 1203341359.961280000 seconds]
[Time since reference or first frame: 1203341359.961280000 seconds]
Frame Number: 1
Frame Length: 62 bytes
Capture Length: 62 bytes
[Frame is marked: False]
[Protocols in frame: eth:ip:udp:hsrp]

Ethernet II, Src: 00:00:0c:07:ac:01 (00:00:0c:07:ac:01), Dst: 01:00:5e:00:00:02
(01:00:5e:00:00:02)
Destination: 01:00:5e:00:00:02 (01:00:5e:00:00:02)
Address: 01:00:5e:00:00:02 (01:00:5e:00:00:02)
.... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
Source: 00:00:0c:07:ac:01 (00:00:0c:07:ac:01)
Address: 00:00:0c:07:ac:01 (00:00:0c:07:ac:01)

.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)

Type: IP (0x0800)
Internet Protocol, Src: 172.28.230.3 (172.28.230.3), Dst: 224.0.0.2 (224.0.0.2)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0xc0 (DSCP 0x30: Class Selector 6; ECN: 0x00)
1100 00.. = Differentiated Services Codepoint: Class Selector 6 (0x30)
.... ..0. = ECN-Capable Transport (ECT): 0
```

```
.... ...0 = ECN-CE: 0

Total Length: 48
Identification: 0x0000 (0)
Flags: 0x00
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 1
Protocol: UDP (0x11)
Header checksum: 0x46db [correct]
[Good: True]
[Bad : False]

Source: 172.28.230.3 (172.28.230.3)
Destination: 224.0.0.2 (224.0.0.2)
User Datagram Protocol, Src Port: 1985 (1985), Dst Port: 1985 (1985)
Source port: 1985 (1985)
Destination port: 1985 (1985)
Length: 28
Checksum: 0x8ab9 [correct]
[Good Checksum: True]
[Bad Checksum: False]

Cisco Hot Standby Router Protocol
Version: 0
Op Code: Hello (0)
State: Active (16)
Hellotime: Default (3)
Holdtime: Default (10)
Priority: 105
Group: 1
Reserved: 0Authentication Data: Default (cisco)
Virtual IP Address: 172.28.230.1 (172.28.230.1)

1 packets captured
```

次の例では、表示フィルタを使用して、アクティブな HSRP 状態の HSRP パケットのみを表示します。

```
switch(config)# ethanalyzer local interface mgmt display-filter "hsrp.state==Active"
limit-captured-frames 2
Capturing on eth1

2013-05-18 14:35:41.443118 172.28.230.3 -> 224.0.0.2 HSRP Hello (state Active)
2013-05-18 14:35:44.326892 172.28.230.3 -> 224.0.0.2 HSRP Hello (state Active)
2 packets captured
```

Ethanalyzer バックグラウンド キャプチャ プロセスおよびインバンド パケットの自動収集

Ethanalyzer は、インバンド パケットをキャプチャするバックグラウンド タスクとして実行できます。インバンド パケット データは PCAP ファイルの RAM メモリに保持されます。設定可能な制限された量の PCAP データ（設定可能なファイル サイズで設定可能な数のファイル）をいつでも使用できます。制限に達すると、最も古いファイルが周期的に現在のキャプチャで上書きされます。

Ethanalyzer のバックグラウンドタスクによってキャプチャされたデータは RAM 内にあり、ブートフラッシュ領域を占有せずに周期的に上書きされます。ユーザがデータを確認できるようにするには、スナップショットを取得する必要があります。 RAM から表示のための不揮発性ストレージ（ブートフラッシュ）への PCAP 形式のバックグラウンドプロセスにより取得されるパケットキャプチャ情報をコピーします。スナップショットを作成する場合は、使用可能なブートフラッシュ領域を考慮する必要があります。

スナップショットは、CLI を介してユーザが手動でトリガーできます。EEM ポリシーは、特定のイベントでスナップショットをトリガーするためにも使用できます。トリガーの使用例として、インバンド レートが定義されたしきい値を超えた場合、CoPP ドロップがしきい値を超えた場合などがあります。スナップショットは、イベントの発生時点までにどのパケットがインバンドにヒットしていたかを示します。

レートをモニタする場合、ユーザが通常予想するレートまたは許容レートを超えるしきい値を設定する必要があります。これは、問題以外のアラートの超過を回避するために設定する必要があります。以下の自動収集 EEM ポリシーで最大トリガーを増やす場合は、注意が必要です。これらのプラクティスに従わないと、無関係な PCAP データが大量にスナップショット化され、ブートフラッシュがいっぱいになる可能性があります。

Ethanalyzer は、バックグラウンド セッションの有効化と設定、セッションの開始と停止、Ethanalyzer 情報のスナップショット、およびバックグラウンド セッション ステータスを確認するための show コマンドを追加するための CLI を追加しました。すべての CLI は有効から実行します。

表 *4 : Ethanalyzer CLI*

CLI	説明
ethanalyzer background-session config <filename|filesize|numfiles|session>	循環バッファのキャプチャ パケットの Ethanalyzer バックグラウンド プロセス/セッションのパラメータを設定します。 • Filename: Ethanalyzer バックグラウンド キャプチャ プロセスによって保存されたバックグラウンド パケット キャプチャ ファイル名。 • Filesize: 一時バッファ内の個々のキャプチャ ファイルのサイズ。値の範囲は 1ー65536 KB です。 • Numfiles: 一時バッファに保存される最大 pcap ファイルの数。値の範囲は 2ー16 です。 • Session: Ethanalyzer バックグラウンド キャプチャ セッションを有効または無効にします。

CLI	説明
ethanalyzer background-session restart	Ethanalyzer バックグラウンド キャプチャ セッションを開始/再起動します。
ethanalyzer background-session stop	Ethanalyzer バックグラウンド キャプチャ セッションを停止します。
show ethanalyzer background-session processes	Ethanalyzer バックグラウンド キャプチャ セッションの詳細を表示します。
show ethanalyzer background-session config	Ethanalyzer バックグラウンド キャプチャ セッション設定ファイルを出力します。
ethanalyzer copy-background-snapshot	一時バッファにキャプチャされたファイルをブートフラッシュにコピーします。ファイルは pcap 形式です。
ethanalyzer copy-compressed-background-snapshot	一時バッファにキャプチャされたファイルを tar し、tar ファイルをブートフラッシュにコピーします。 （注） この CLI を複数回発行すると、古い tar ファイルが削除されます。古い tar ファイルがブートフラッシュに存在する場合は、コピーすることを推奨します。

Cisco NX-OS リリース 10.1(2) Ethanalyzer Autocollection CLI は、すべての Cisco Nexus 9000 シリーズ プラットフォームでサポートされます。

Ethanalyzer Autocollection CLI 警告

Ethnalyzer Autocollection CLI の警告は次のとおりです。

- バックグラウンド プロセスに変更が加えられるたびに、Ethanalyzer バックグラウンド プロセスを再起動/開始する必要があります。設定が変更されると、次の警告メッセージがユーザに表示されます。

  「設定の変更を有効にするには、Ethanalyzer バックグラウンドプロセスを再起動してください。（Please restart the Ethanalyzer background process for any config change to take effect.）」

- スーパーバイザの冗長性がサポートされているプラットフォームでは、アクティブなスーパーバイザのスイッチオーバーによって、Ethanalyzer のバックグラウンドキャプチャプロセスが自動的に開始されないことがあります。ユーザは、Ethanalyzer バックグラウンドプロセスを手動で再起動する必要があります。スイッチオーバー後に Ethanalyzer バックグラウンド プロセスを自動的に開始する場合は、アクティブ スーパーバイザでセッション イネーブルを設定し、スイッチをリロードして有効にする必要があります。この後、スイッ

チオーバーが発生した場合でも、新しくアクティブになったスーパーバイザでEthanalyzer バックグラウンド キャプチャ プロセスが自動的に開始されます。

CLI の例

CLI 出力の例：すべてのコマンドはイネーブル モードから実行されます。

ステップ 1：バックグラウンドで実行されている Ethanalyzer セッションを有効にします。

```
switch# ethanalyzer background-session config session enable
```

```
switch# dir bootflash: | include dump
       1087    Jan 29 13:55:46 2021  dumpcap_bg_session_configuration.xml
switch# show ethanalyzer background-session config
<?xml version="1.0"?>
<!-- This document contains configuration settings for background packet -->
<!-- capture session to execute in ring buffer mode. Please modify the settings
based on system resources -->
<!-- path:         background packet capture directory where ring buffer files w
ill be saved -->
<!-- filename:     background packet capture file name saved by dumpcap. Files w
ill be generated as filename_number_date format -->
<!-- filesize:     Size of individual ring buffer file in kB. Note that the file
size is limited to a maximum value of 65536 kB-->
<!-- num_of_files: value begin again with the first file after value number of f
iles were written (form a ring buffer). The maximum value should be equal to 16
-->
<!-- session:      Enable/disable background packet capture session process. App
licable for both boot-up as well as session restart -->
<ethanalyzer_config>
    <filepath>/tmp/dumpcap_bg_session_files/</filepath>
    <filename>capture</filename>
    <filesize>2048</filesize>
    <numfiles>2</numfiles>
    <session>enable</session>
</ethanalyzer_config>
```

次に、CLI の出力を示します。

```
switch# ethanalyzer background-session restart
root     30038     1  0 13:58 ttyS0    00:00:00 /usr/bin/dumpcap -n -b filesize:
2048 -b files:2 -i ps-inb -Z none -w /tmp/dumpcap_bg_session_files/capture.pcap
```

ステップ 2：バックグラウンド セッション設定パラメータの確認

```
switch# show ethanalyzer background-session process
```

ステップ 3：バックグラウンド Ethanalyzer プロセスの開始

```
switch# ethanalyzer background-session restart
```

ステップ 4：Ethanalyzer バックグラウンド キャプチャ セッションの実行の確認

```
switch# ethanalyzer background-session processes
Background session of packet analyzer:
root 17216 1 4 12:43 ttyS0 00:00:00 /usr/bin/dumpcap -n -b filesize:2048 -b files:2 -i
ps-inb -Z none -w /tmp/dumpcap_bg_session_files/capture.pcap
switch#
```

使用例：CLI を実行してスナップショットをキャプチャして表示する

```
switch# ethanalyzer copy-background-snapshot
```

```
Copy packet analyzer captured frames to bootflash...
Copied snapshot files :
     72 -rw-rw-rw-  1 root  root               65844 Jan 21 00:21
CAPTURE_00001_20210121001903.pcap

switch# ethanalyzer copy-compressed-background-snapshot

Copy packet analyzer captured compressed frames to bootflash...
Copied snapshot files :
     28 -rw-r--r--  1 root  root               27181 Jan 21 00:22 CAPTURE.tar.gz
```

使用例：Ethanalyzer スナップショットの自動収集のトリガーとしてインバンド レート モニタリングを使用する。

表 *5*：インバンド レート モニタリング *CLI* オプション

CLI	説明
設定モード	system inband cpu-mac log threshold rx rx_pps tx tx_pps throttle secondsrx_pps, tx_pps: 0-1500000 Inband rx/tx pps rate that needs to be logged when exceededseconds: log throttle interval (maximum 1 exceed log per defined interval)
有効モード（Enable Mode）	show system inband cpu-mac log threshold" to display settings
デフォルト	off（PPS 値 0）、スロットル間隔 120 秒。

前のセクションで説明したように、Ethanalyzer バックグラウンド プロセス機能が設定され、実行されていることが前提となります。この使用例にはデモまたはサンプル目的のサンプル レートがありますが、ユーザはロギングに値すると考えられる現実的なレートを使用する必要があります。ユーザの要件を超えるしきい値は、非問題のアラートの超過を回避するために通知する必要があります。

（注） 以下の自動収集 EEM ポリシーで最大トリガーを増やす場合は注意が必要です。これらの方法に従わないと、大量の PCAP データがスナップショット化され、ブートフラッシュがいっぱいになる可能性があります。

max-triggers パラメータは、アクティブなスーパーバイザのブートフラッシュ（bootflash:eem_snapshots）の eem_snapshots ディレクトリに永続的に保存されているスナップショットファイルの量に対してチェックされます。スーパーバイザスイッチオーバーの場合、新しくアクティブになったスーパーバイザの収集数は、以前にアクティブだったスーパーバイザの収集数とは異なる場合があり、その結果、自動収集が再開されるかどうかが決まります。自動収集の再開は、新しくアクティブになったスーパーバイザのブートフラッシュに存在するスナップショット バンドルによって異なります。

指定されたディレクトリ内のファイルの量が max-triggers と一致すると、自動収集は停止します。再度開始するには、ユーザがディレクトリからスナップショットファイルを削除して、ファイル数を max-triggers よりも少ない「値」にし、別の量（max-triggers から「value」を引いた数）の自動収集を許可する必要があります。詳細については、「トリガーベースのイベントログの自動収集」の項を「Embedded Event Manager の設定」の章で参照してください。

ステップ 1：インバンド レート モニタリングを有効にする

```
switch(config)# system inband cpu-mac log threshold rx 400 tx 4000 throttle 60
switch# show system inband cpu-mac log threshold
Thresholds Rx: 400 PPS, Tx; 4000 PPS
Log throttle interval: 60 seconds
```

「トリガーベースのイベントログの自動収集」の項を「Embedded Event Manager の設定」の章で説明されているように、トリガーベースのログファイルの自動収集を利用して、ディレクトリを作成します（次の例では、ディレクトリの名前は「auto_collect」です）。 EEM ポリシーを作成または有効にすると、イベント ログと ethanalyzer pcap の組み込みスナップショット収集が有効になります。

ステップ 2：ディレクトリを作成する

```
create auto_collect directory
switch# pwd
bootflash:
switch# cd scripts
switch# mkdir auto_collect
```

ステップ 3：イベント マネージャ ポリシーを有効にする

```
switch(config)# event manager applet syslog_trigger override __syslog_trigger_default
switch(config-applet)# action 1.0 collect auto_collect rate-limit 60 max-triggers 3
$_syslog_msg
```

これにより、60 秒あたり最大 1x の自動収集が有効になり、同じトリガーに対して合計で最大 3 回、同じ syslog トリガーに対して最大 max-triggers x num_files pcap ファイルを保存します（例：3 x 2 = 6 ファイル）。

上記の使用例：大量の ICMP 要求を起動するホスト 20.1.1.100 の誤動作を特定します。

```
switch#
2021 Jan 29 15:15:27 switch %KERN-1-SYSTEM_MSG: [17181.984601] Inband Rx threshold 400
```

```
PPS reached. - kernel
2021 Jan 29 15:15:28 switch %KERN-1-SYSTEM_MSG: [17182.997911] Inband Rx threshold 400
PPS reached. - kernel
switch# show system internal event-logs auto-collect history
DateTime              Snapshot ID  Syslog
Status/Secs/Logsize(Bytes)
2021-Jan-29 15:15:30  620969861    KERN-1-SYSTEM_MSG
PROCESSED:1:7118865
2021-Jan-29 15:15:30  201962781    KERN-1-SYSTEM_MSG
DROPPED-LASTACTIONINPROG
2021-Jan-29 15:15:29  620969861    KERN-1-SYSTEM_MSG                          PROCESSING
...
switch# dir bootflash: | include capture
    2048040    Jan 29 15:15:29 2021  capture_00004_20210129150732.pcap
     169288    Jan 29 15:15:29 2021  capture_00005_20210129151528.pcap
 ...
```

バックグラウンドプロセスでキャプチャされたファイルをデコードするには、シスコ TAC チームにお問い合わせください。

使用例：カスタム（非組み込みの自動コレクション YAML）トリガーの使用（CoPP ドロップしきい値超過）

前提条件は次のとおりです。

1. 前述のように、Ethanalyzerバックグラウンドプロセス機能が設定され、実行されています。

2. 前の使用例のステップ 2 とステップ 3 が完了しています。

ドロップが発生する理由を学習するクラスの CoPP しきい値ロギングを有効にします。詳細については、CoPP設定ガイド（参照）を参照してください。

この例では、ARP を含むクラス copp-class-normal の場合、しきい値は 1000000 に設定され、ロギング レベルは 1（autocollect に対応できる十分な高さ）に設定されます。

```
class copp-class-normal
    logging drop threshold 1000000 level 1
```

前の使用例で使用したものと同じディレクトリ（bootflash:scripts/auto_collect）で、ファイル copp.yaml を次のように追加します（copp = コンポーネント名）。

```
#*********************************************************************
#
# File:   comp specific yaml
# Author:
#
# Description: Module Makefile
#
#
# Copyright (c) 2019 by cisco Systems, Inc.
# All rights reserved.
#
#
# $Id: comp specific yaml $
# $Source:  $
# $Author:  $
#
#*********************************************************************
version: 1
components:
    copp:
            default:
            copp_drops1:
```

```
            serviceCOPP:
              match: CoPP drops exceed threshold
              commands: ethanalyzer copy-background-snapshot
```

上記の使用例：クラスで CoPP ドロップを引き起こす大量の ARP 要求を特定します。

```
switch#
2021 Jan 29 15:49:47 switch %COPP-1-COPP_DROPS1: CoPP drops exceed threshold in class:
copp-class-normal-log,
check show policy-map interface control-plane for more info.
switch# show policy-map interface control-plane class copp-class-normal-log
Control Plane

  Service-policy  input: copp-policy-strict-log

    class-map copp-class-normal-log (match-any)
      match access-group name copp-acl-mac-dot1x-log
      match protocol arp
      set cos 1
      threshold: 1000000, level: 1
      police cir 1400 kbps , bc 32000 bytes
      module 1 :
        transmitted 25690204 bytes;
        5-minute offered rate 168761 bytes/sec
        conformed 194394 peak-rate bytes/sec
          at Fri Jan 29 15:49:56 2021

        dropped 92058020 bytes;
        5-min violate rate 615169 byte/sec
        violated 698977 peak-rate byte/sec        at Fri Jan 29 15:49:56 2021

switch#
switch# show system internal event-logs auto-collect history
DateTime              Snapshot ID  Syslog
Status/Secs/Logsize(Bytes)
2021-Jan-29 15:49:57  1232244872   COPP-1-COPP_DROPS1                          RATELIMITED
2021-Jan-29 15:49:50  522271686    COPP-1-COPP_DROPS1
PROCESSED:1:11182862
2021-Jan-29 15:49:48  522271686    COPP-1-COPP_DROPS1                          PROCESSING
...
switch# dir bootflash: | include capture
    2048192    Jan 29 15:49:49 2021  capture_00038_20210129154942.pcap
    1788016    Jan 29 15:49:49 2021  capture_00039_20210129154946.pcap
....
```

SSO の動作

スタンバイ スーパーバイザ がバックグラウンドプロセス設定 session = disable で起動した場合、ユーザはこの スーパーバイザ がアクティブになったときにプロセスを再起動する必要があります。

参考資料

- Wireshark：CaptureFilters
- Wireshark：DisplayFilters
- 『Cisco Nexus 9000 シリーズ NX-OS Layer 2 スイッチング設定ガイド』
- 『Cisco Nexus 9000 シリーズ NX-OS VXLAN 設定ガイド』

- 『Cisco Nexus 9000 NX-OS インターフェイス設定ガイド』
- 『Cisco Nexus 9000 シリーズ NX-OS ユニキャスト ルーティング設定ガイド』

SNMP および RMON のサポート

Cisco NX-OS は、管理情報ベース（MIB）と通知（トラップと情報）を含む広範な SNMPv1、v2、および v3 のサポートを提供します。

SNMP 標準では、Cisco NX-OS を管理しモニタリングする各 MIB をサポートするサードパーティ製アプリケーションを使用できます。

SNMPv3 はさらに広範なセキュリティ機能を提供します。各デバイスで SNMP サービスを有効または無効にするように選択できます。また、各デバイスで SNMP v1 および v2 要求の処理方法を設定できます。

Cisco NX-OS は、リモート モニタリング（RMON）アラームおよびイベントもサポートします。RMON アラームとイベントは、ネットワーク動作の変化に基づいて、しきい値の設定や通知の送信のメカニズムを提供します。

*[*アラーム グループ（*Alarm Group*）*]* では、アラームを設定できます。アラームは、デバイス内の 1 つまたは複数のパラメータに設定できます。たとえば、デバイスの CPU 使用率の特定のレベルに対して RMON アラームを設定できます。*EventGroup* を使用すると、アラーム条件に基づいて実行するアクションであるイベントを設定できます。サポートされるイベントのタイプには、ロギング、SNMP トラップ、およびログアンドトラップが含まれます。

SNMP および RMON の設定の詳細については、「*Cisco Nexus 9000* シリーズ *NX-OS* システム管理設定ガイド」を参照してください。

PCAP SNMP パーサーの使用

PCAP SNMP パーサーは、.pcap 形式でキャプチャされた SNMP パケットを分析するツールです。スイッチ上で動作し、スイッチに送信されるすべての SNMP get、getnext、getbulk、set、trap、および response 要求の統計情報レポートを生成します。

PCAP SNMP パーサーを使用するには、次のいずれかのコマンドを使用します。

- **debug packet-analysis snmp** [**mgmt0** | **inband**] **duration** *seconds* [*output-file*] [**keep-pcap**]—Tshark を使用して指定の秒数間のパケットをキャプチャし、一時 .pcap ファイルに保存します。次に、その .pcap ファイルに基づいてパケットを分析します。

  結果は出力ファイルに保存されます。出力ファイルが指定されていない場合は、コンソールに出力されます。**keep-pcap** オプションを使用する場合を除き、一時 .pcap ファイルはデフォルトで削除されます。パケット キャプチャは、デフォルトの管理インターフェイス（mgmt0）、または帯域内インターフェイスで実行できます。

  例：

```
switch# debug packet-analysis snmp duration 100

switch# debug packet-analysis snmp duration 100 bootflash:snmp_stats.log

switch# debug packet-analysis snmp duration 100 bootflash:snmp_stats.log keep-pcap

switch# debug packet-analysis snmp inband duration 100

switch# debug packet-analysis snmp inband duration 100 bootflash:snmp_stats.log

switch# debug packet-analysis snmp inband duration 100 bootflash:snmp_stats.log
keep-pcap
```

- **debug packet-analysis snmp** *input-pcap-file* [*output-file*]：既存の .pcap ファイルにあるキャプチャしたパケットを分析します。

  例：

```
switch# debug packet-analysis snmp bootflash:snmp.pcap

switch# debug packet-analysis snmp bootflash:snmp.pcap bootflash:snmp_stats.log
```

次に、**debug packet-analysis snmp** [**mgmt0** | **inband**] **duration** コマンドの統計情報レポートの例を示します。：

```
switch# debug packet-analysis snmp duration 10
Capturing on eth0
36
wireshark-cisco-mtc-dissector: ethertype=0xde09, devicetype=0x0
wireshark-broadcom-rcpu-dissector: ethertype=0xde08, devicetype=0x0

Started analyzing. It may take several minutes, please wait!

Statistics Report
----------------------------------------
SNMP Packet Capture Duration: 0 seconds
Total Hosts: 1
Total Requests: 18
Total Responses: 18
Total GET: 0
Total GETNEXT: 0
Total WALK: 1 (NEXT: 18)
Total GETBULK: 0
Total BULKWALK: 0 (BULK: 0)
Total SET: 0
Total TRAP: 0
Total INFORM: 0

Hosts        GET  GETNEXT  WALK(NEXT) GETBULK  BULKWALK(BULK) SET  TRAP  INFORM  RESPONSE
-------------------------------------------------------------------------------------------
10.22.27.244   0     0        1(18)      0         0(0)          0    0      0       18

Sessions
--------
1

MIB Objects GET  GETNEXT  WALK(NEXT) GETBULK(Non_rep/Max_rep) BULKWALK(BULK,
Non_rep/Max_rep)
-------------------------------------------------------------------------------------------
ifName      0       0        1(18)      0                        0
```

```
SET     Hosts
--------------------
0       10.22.27.244
```

RADIUS を利用

RADIUS プロトコルは、ヘッドエンドの RADIUS サーバとクライアント デバイス間で、属性またはクレデンシャルを交換するために使用されるプロトコルです。これらの属性は、次の 3 つのサービス クラス（CoS）に関連しています。

- 認証
- 許可
- アカウンティング

認証は、特定のデバイスにアクセスするユーザの認証を意味しています。RADIUS を使用して、Cisco NX-OS デバイスにアクセスするユーザ アカウントを管理できます。デバイスへのログインを試みると、Cisco NX-OS によって、中央の RADIUS サーバの情報に基づいてユーザ検証が行われます。

許可は、認証されたユーザのアクセス許可範囲を意味しています。ユーザに割り当てたロールは、ユーザにアクセスを許可する実デバイスのリストとともに、RADIUS サーバに保管できます。ユーザが認証されると、デバイスは RADIUS サーバを参照して、ユーザのアクセス範囲を決定します。

アカウンティングは、デバイスの管理セッションごとに保管されるログ情報を意味しています。この情報を使用して、トラブルシューティングおよびユーザアカウンタビリティのレポートを生成できます。アカウンティングは、ローカルまたはリモートで実装できます（RADIUS を使用して）。

次に、アカウンティング ログ エントリを表示する例を示します。

```
switch# show accounting log
Sun May 12 04:02:27 2007:start:/dev/pts/0_1039924947:admin
Sun May 12 04:02:28 2007:stop:/dev/pts/0_1039924947:admin:vsh exited normally
Sun May 12 04:02:33 2007:start:/dev/pts/0_1039924953:admin
Sun May 12 04:02:34 2007:stop:/dev/pts/0_1039924953:admin:vsh exited normally
Sun May 12 05:02:08 2007:start:snmp_1039928528_172.22.95.167:public
Sun May 12 05:02:08 2007:update:snmp_1039928528_172.22.95.167:public:Switchname
```

（注） アカウンティング ログは、各セッションの最初と最後（開始と終了）だけを表示します。

syslog の使用

システム メッセージ ロギング ソフトウェアを使用して、メッセージをログ ファイルに保存するか、または他のデバイスに転送します。この機能では、次のことができます。

- モニタリングおよびトラブルシューティングのためのログ情報の記録
- キャプチャするログ情報のタイプの選択
- キャプチャするログ情報の宛先の選択

syslog を使用してシステム メッセージを時間順にローカルに保存したり、中央の syslog サーバにこの情報を送信したりできます。syslog メッセージをコンソールに送信してすぐに使用することもできます。これらのメッセージの詳細は、選択した設定によって異なります。

syslog メッセージは、重大度に応じて、debug から critical までの 7 つのカテゴリに分類されます。デバイス内の特定のサービスについて、レポートされる重大度を制限できます。たとえば、OSPF サービスのデバッグ イベントのみを報告し、BGP サービスのすべての重大度レベルのイベントを記録することができます。

ログ メッセージは、システム再起動後には消去されています。ただし、重大度が Critical 以下（レベル 0、1、2）の最大 100 個のログ メッセージは NVRAM に保存されます。このログは、**show logging nvram** でいつでも表示できます。 コマンドを使用します。

ログ レベル

Cisco NX-OS では、次のロギング レベルがサポートされています。

- 0-emergency（緊急）
- 1-alert（警報）
- 2-critical（重大）
- 3-error（エラー）
- 4-warning（警告）
- 5-notification（通知）
- 6-informational（情報）
- 7-debugging（デバッグ）

デフォルトでは、デバイスにより、正常だが重要なシステム メッセージがログ ファイルに記録され、それらのメッセージがシステム コンソールに送信されます。ユーザは、ファシリティ タイプおよび重大度に基づいて、保存するシステム メッセージを指定できます。リアルタイムのデバッグおよび管理を強化するために、メッセージにはタイム スタンプが付加されます。

Telnet または SSH へのロギングのイネーブル化

システム ロギング メッセージは、デフォルトまたは設定済みのロギング ファシリティおよび重大度の値に基づいてコンソールに送信されます。

- コンソールのロギングをディセーブルにするには、**no logging console** コマンドをコンフィギュレーション モードで使用します。
- Telnet または SSH のロギングを有効にするには、 **terminal monitor** コマンドを実行します。
- コンソールセッションへのロギングをディセーブルまたはイネーブルにすると、その状態は、それ以後のすべてのコンソールセッションに適用されます。ユーザがセッションを終了して新規のセッションに再びログインした場合、状態は維持されています。ただし、TelnetセッションまたはSSHセッションへのロギングをイネーブルまたはディセーブルにすると、その状態はそのセッションだけに適用されます。ユーザがセッションを終了したあとは、その状態は維持されません。

この項で説明している **no logging console** コマンドは、コンソールロギングをディセーブルにし、デフォルトでイネーブルになっています。

```
switch(config)# no logging console
```

この項で説明している **terminal monitor** コマンドは、Telnet または SSH のロギングを有効にし、デフォルトではディセーブルになっています。

```
switch# terminal monitor
```

syslog の設定の詳細については、『*Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*』を参照してください。

SPAN の使用

スイッチドポートアナライザ（SPAN）ユーティリティを使って、詳細なトラブルシューティングの実行または特定のアプリケーションホストからトラフィックのサンプルを取得し、プロアクティブなモニタリングと分析を行うことができます。

デバイス設定を修正しても解決できない問題がネットワークにある場合は、通常、プロトコルレベルを調べる必要があります。**debug** コマンドを使用すれば、 エンド ノードとデバイス間の制御トラフィックを調べることができます。ただし、特定のエンドノードを発信元または宛先とするすべてのトラフィックに焦点を当てる必要がある場合は、プロトコルアナライザを使用してプロトコル トレースをキャプチャします。

プロトコルアナライザを使用するには、分析対象のデバイスへのラインにアナライザを挿入する必要があります。このとき、デバイスとの入出力（I / O）は中断されます。

イーサネット ネットワークでは、SPANユーティリティを使用してこの問題を解決できます。SPAN を使用すると、すべてのトラフィックのコピーを取得して、デバイス内の別のポートに

転送できます。このプロセスはどの接続デバイスも中断せず、ハードウェア内で実施されるので不要な CPU 負荷を防ぎます。

SPAN を使用すると、デバイス内で独立した SPAN セッションが作成されます。フィルタを適用して、受信したトラフィックまたは送信したトラフィックのみをキャプチャできます。

SPAN の設定の詳細については、『*Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*』を参照してください。

Using sFlow

Sampled flow (sFlow) allows you to monitor real-time traffic in data networks that contain switches and routers. It uses the sampling mechanism in the sFlow agent software on switches and routers to monitor traffic and to forward the sample data to the central data collector. For more information about sFlow, see RFC 3176.

The sFlow agent, which is embedded in the Cisco NX-OS software, periodically samples or polls the interface counters that are associated with a data source of the sampled packets.

For more information about configuring sFlow, see Cisco Nexus 9000 Series NX-OS System Management Configuration Guide.

sFlow 整合性チェッカー

sFlow 整合性チェッカーは、スーパーバイザーとライン カード ハードウェア テーブルのプログラムと整合性構成のチェックを実行します。スイッチで sFlow を構成すると、その状態がソフトウェア、ストレージ、ライン カード、およびハードウェア テーブルにプログラムされます。しかし、Cisco Nexus 9808 スイッチでは、整合性チェッカーは、スーパーバイザーとライン カード ハードウェア 抽象化レイヤーのプログラムと整合性構成のチェックを実行します。スイッチ上で sFlow を構成中、状態が互いに同期していない場合、SPAN セッションは失敗します。sFlow 整合性チェッカーは、即座に修正できる sFlow セッションの不整合を識別するのに役立ちます。

sFlow 整合性チェッカーを使用して、sFlow スーパーバイザプロセスの構成の整合性を検証できます。

（注） sFlow 整合性チェッカーは、sFlow プロセスのデータ送信元に関連する sFlow 構成情報のみを検証します。

次に、sFlow 整合性チェッカーのコマンドを示します。

```
switch(config)# show consistency-checker sflow
```

次に、出力例を示します。

```
switch(config)# show consistency-checker sflow
SFLOW CC validation start:
```

```
passed for interface ethernet 1/15
Consistency checker passed for SFLOW
```

ブルー ビーコン機能の使用

一部のプラットフォームでは、プラットフォームの LED を点滅させることができます。この機能は、ローカル管理者がトラブルシューティングや交換のためにハードウェアを迅速に識別できるように、ハードウェアをマークするのに便利な方法です。

ハードウェア エンティティの LED を点滅させるには、次のコマンドを使用します。

コマンド	目的
blink chassis	シャーシLEDを点滅させます。
blink fan *number*	ファン LED の 1 つを点滅させます。
blink module *slot*	選択したモジュールの LED を点滅させます。
blink powersupply *number*	電源 LED の 1 つを点滅させます。

watch コマンドの使用

watch コマンドを使用すると、Cisco NX-OS CLI コマンド出力または UNIX コマンド出力を更新し、監視することを許可します（**run bash** コマンド コマンドを通して）。

次のコマンドを使用します。

watch [**differences**] [**interval** *seconds*] *command*watch

- **differences**：コマンド出力の違いを強調表示します。
- **interval** *seconds*：コマンド出力を更新する頻度を指定します。範囲は 0 ～ 2147483647 秒です。
- *command*：監視するコマンドを指定します。

次に、**watch** コマンドを使用して **show interface eth1/15 counters** コマンドの出力を毎秒更新し、相違点を強調表示する例を示します。

```
switch# watch differences interval 1 show interface eth1/15 counters

Every 1.0s:  vsh -c "show interface eth1/15 counters"      Mon Aug 31 15:52:53 2015


--------------------------------------------------------------------------------
Port                                InOctets                      InUcastPkts
--------------------------------------------------------------------------------
Eth1/15                               583736                                0

--------------------------------------------------------------------------------
Port                              InMcastPkts                      InBcastPkts
--------------------------------------------------------------------------------
Eth1/15                                2433                                0
```

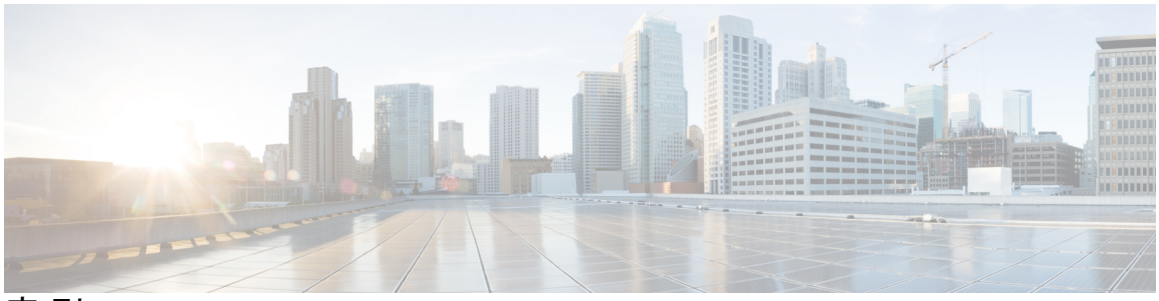
```
--------------------------------------------------------------------------------
Port                                OutOctets                    OutUcastPkts
--------------------------------------------------------------------------------
Eth1/15                               5247672                               0

--------------------------------------------------------------------------------
Port                              OutMcastPkts                    OutBcastPkts
--------------------------------------------------------------------------------
Eth1/15                                 75307                               0
```

トラブルシューティングのツールと方法論の追加参照

関連資料

関連項目	マニュアル タイトル
システム管理ツール	『*Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*』
MIB	『*Cisco Nexus 7000 Series and 9000 Series NX-OS MIB Quick Reference*』



索 引

A

admin-password 31
attach console module 9

B

blink chassis 177
blink fan 177
blink module 177
blink powersupply 177
boot tftp: 18

C

clear cores 112
clear counters interface all 45
clear counters interface 45
cmdline recoverymode = 1 18, 30
copy 28, 31, 116
copy core 20
copy core: 21, 24
copy startup-configuration tftp: 116

D

debug 145, 175
debug packet-analysis snmp 171–172

E

ethanalyzer local interface {inband | mgmt} autostop 155
ethanalyzer local interface {inband | mgmt} capture-filter 155
ethanalyzer local interface {inband | mgmt} capture-ring-buffer 156
ethanalyzer local interface {inband | mgmt} detail 156
ethanalyzer local interface {inband | mgmt} display-filter 155
ethanalyzer local interface {inband | mgmt} limit-captured-frames 155
ethanalyzer local interface {inband | mgmt} limit-frame-size 155
ethanalyzer local interface {inband | mgmt} raw 156
ethanalyzer local interface {inband | mgmt} vrf 156
ethanalyzer local interface {inband | mgmt} write 155
ethanalyzer local interface front-panel 154
ethanalyzer local interface inband 153
ethanalyzer local interface inband-in 154
ethanalyzer local interface inband-out 154
ethanalyzer local interface mgmt 154
ethanalyzer local interface port-channel 154
ethanalyzer local interface vlan 154–155
ethanalyzer local read 155

F

feature nxapi 106

I

init system 17–18
install module 13
install all 12–14
ip icmp-errors source-interface 148
ip traceroute source-interface 147

L

load-nxos 18, 31
logging level l2fm 77
logging server 7

N

no feature nxapi 106
no logging console 175
no shutdown 44, 49–50

P

ping 146
ping6 146

R

reload 26, 33
run bash 177
run-script 116

S

set gw 17–18
set ip 17–18
set ip next-hop 89
set ipv6 next-hop 89
show 119, 144
show {ip | ipv6} 4
show consistency-checker copp 120
show consistency-checker dme interfaces 121
show consistency-checker egress-xlate private-vlan 121
show consistency-checker fex-interfaces 121
show consistency-checker forwarding single-route 122
show consistency-checker forwarding 121
show consistency-checker gwmacdb 122
show consistency-checker kim 122
show consistency-checker l2 module 122
show consistency-checker l2 multicast group 123
show consistency-checker l2 switchport interface 123
show consistency-checker l3 multicast group 125
show consistency-checker l3-interface interface 124
show consistency-checker l3-interface module 124
show consistency-checker link-state fabric-ieth module 125
show consistency-checker link-state interface 126
show consistency-checker link-state module 126
show consistency-checker membership port-channels 126
show consistency-checker membership vlan 127
show consistency-checker pacl extended ingress 127
show consistency-checker pacl 127
show consistency-checker port-state fabric-ieth module 128
show consistency-checker port-state module 128
show consistency-checker racl extended ingress 129–130
show consistency-checker racl 129
show consistency-checker segment-routing mpls label 137
show consistency-checker segment-routing mpls 136
show consistency-checker sflow 137
show consistency-checker storm-contro 136
show consistency-checker stp-state vlan 130
show consistency-checker vacl 130
show consistency-checker vpc 131
show consistency-checker vxlan config-check 132
show consistency-checker vxlan infra 132
show consistency-checker vxlan l2 module 133
show consistency-checker vxlan l2 135
show consistency-checker vxlan l3 single-route 135
show consistency-checker vxlan l3 vrf 133
show consistency-checker vxlan pv 133
show consistency-checker vxlan qinq-qinvni 134
show consistency-checker vxlan selective-qinvni 134
show consistency-checker vxlan vlan 134
show consistency-checker vxlan xconnect 134
show diagnostic content module 153
show diagnostic result 153
show feature | grep bash 106–107
show forwarding distribution multicast client 86–87
show hardware rate-limit 95
show install all status 12, 115
show interface 44–45, 51, 77
show interface brief 47
show interface capabilities 45, 47
show interface counters 44
show interface counters errors 77–78
show interface status 45
show interface transceiver 7
show interfaces brief 4
show ip arp 5, 86, 89
show ip client pim 86–87
show ip client 86
show ip fib 86
show ip interface 86–87
show ip policy 89
show ip process 86
show ip route 86, 89
show ip routing 5
show ip traceroute source-interface 148
show ip traffic 86
show ipv6 neighbor 5, 89
show ipv6 route 89
show license 39
show license host-id 38–39
show license usage 38–39
show log | include error 21
show log nvram 115
show logging nvram 9, 174
show logging logfile 51, 114
show logging log 4
show logging onboard error stats 151
show mac address-table dynamic vlan 5
show ospf 86
show policy-map interface control-plane 95
show port-channel compatibility-parameters 5
show port-channel summary 54
show process log pid 21–22
show process log 21–22
show processes memory 86–87, 92, 109–110
show processes cpu 110, 149
show processes log pid 21, 24
show process memory 93
show processes 4–5, 21–22, 92, 148
show route-map 89
show running-config 4
show running-config eigrp all 86
show running-config interface 47
show running-config spanning-tree 5
show running-config vpc 54
show running-config eigrp 86
show spanning-tree interface 77–78
show spanning-tree summary totals 76
show spanning-tree vlan 77, 79–80
show spanning-tree 4, 55
show system 120
show system error-id 120

show system reset-reason 26
show system resources 92, 150
show system uptime 21, 23
show tech-support details 113–114
show tech-support udld 45
show tech-support vpc 54
show udld 45
show user-account 27
show version 4
show vlan all-ports 5
show vlan brief 47
show vlan 4
show vpc consistency-parameters interface 56
show vpc consistency-parameters 54
show vpc peer-keepalive 54
show vpc 54–55
show vrf interface 86–87
show vrf 86
show cores 21, 23, 111
show ip static-route 86
show logging 49
show logging last 114
show logging server 7, 9
show module 4, 14, 44, 56
show processes log 111
shutdown 48–50, 77
spanning-tree bpduguard enable 82
spanning-tree loopguard default 82
spanning-tree vlan 82
state active 47
system cores tftp: 21, 25
system cores 112, 117
system memory-thresholds minor 94
system startup-config unlock 144

T

tac-pac 114
tcpdump 162
terminal length 0 113
terminal monitor 175
test consistency-checker forwarding 121
traceroute 146–147
traceroute6 147

U

undebug all 145
username admin password 27, 32

V

vlan 82
VXLAN 59–61, 63, 65, 67
　トラブルシューティング 59
　マルチキャスト カプセル化解除パスでドロップされたパケット 61
　マルチキャストカプセル化パスでドロップされたパケット 60
　マルチキャストカプセル化解除パスでドロップされたARP要求 61
　マルチキャストカプセル化解除パスでドロップされたARP要求 60
　ユニキャストカプセル化解除パスでドロップされたパケット 67
　ユニキャストカプセル化パスでドロップされたパケット 63, 65

あ

アカウンティング ログの表示 4

さ

delete 13

て

debug-filter 145

と

ドロップされたパケット 60–61, 63, 65, 67

ふ

ブート 26, 30

へ

ヘルプ 17

ま

マルチキャスト カプセル化解除パス 61
マルチキャスト カプセル化パス 60

ゆ

ユニキャスト カプセル化解除パス 67
ユニキャストカプセル化パス 63, 65

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、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。