Cisco NX-OS トラブルシューティング ガイド Release 4.0

July 8, 2008

Text Part Number: OL-15807-01-J

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

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

Cisco NX-OS トラブルシューティング ガイド Release 4.0

CONTENTS

はじめに

このマニュアルでは、Cisco NX-OS の使用時に発生する可能性のある問題のトラブルシューティングに役立つ情報を提供します。具体的には、問題の認識、原因の特定、および可能な解決方法を見つけるためのツールおよび方法を紹介しています。

対象読者

このマニュアルは、NX-OS の設定および保守の経験が豊富なネットワーク管理者を対象としています。

マニュアルの構成

このマニュアルは、次の章で構成されています。

章	説明
第 1 章「トラブルシューティングの概要」	トラブルシューティングの基本的な概念、方法、およびツールについて説明しています。
第 2 章「インストール、アップグレード、および再起動のトラブルシューティング」	Cisco NX-OS のインストール、アップグレード、または再起動中に発生する可能性のある問題を識別して解決する方法について説明しています。
第 3 章「ライセンスのトラブルシューティング」	ライセンスの問題に関するトラブルシューティングの手順について説明しています。
第 4 章「VDC のトラブルシューティング」	Virtual Device Context（VDC; 仮想デバイス コンテキスト）の使用中に発生する可能性のある問題を識別して解決する方法について説明しています。
第 5 章「ポートのトラブルシューティング」	ポートで発生する可能性のある問題を識別して解決する方法について説明しています。
第 6 章「VLAN のトラブルシューティング」	VLAN に関するトラブルシューティングの手順について説明しています。
第 7 章「STP のトラブルシューティング」	スパニング ツリーに関するトラブルシューティングの手順について説明しています。
第 8 章「ルーティングのトラブルシューティング」	ルーティングに関するトラブルシューティングの手順について説明しています。
付録 A「テクニカル サポートへ問い合わせる前の準備」	Cisco NX-OS デバイスのテクニカル サポートに問い合わせる前に実行する手順について説明しています。
付録 B「トラブルシューティングのツールおよび方法」	Cisco NX-OS で使用できるトラブルシューティングのツールおよび方法について説明しています。

表記法

コマンドの説明では、次の表記法を使用しています。

表記	説明
太字	コマンドおよびキーワードは**太字**で示しています。
イタリック体	ユーザが値を指定する引数は、*イタリック体*で示しています。
[ ]	角カッコの中の要素は、省略可能です。
[x|y|z]	どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
ストリング	引用符を付けない一組の文字。ストリングの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてストリングとみなされます。

出力例では、次の表記法を使用しています。

screen フォント	スイッチに表示される端末セッションおよび情報は、screen フォントで示しています。
太字の **screen** フォント	ユーザが入力しなければならない情報は、**太字**の **screen** フォントで示しています。
*イタリック体*の *screen* フォント	ユーザが値を指定する引数は、*イタリック体*の *screen* フォントで示しています。
< >	パスワードのように出力されない文字は、かぎカッコ（< >）で囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

このマニュアルでは、次の表記法を使用しています。

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

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

関連資料

Cisco NX-OS のマニュアルには、次の URL からアクセスできます。

http://www.cisco.com/en/US/products/ps9372/tsd_products_support_series_home.html

Cisco NX-OS のマニュアル セットには、次の資料が含まれます。

リリース ノート

『*Cisco NX-OS Release Notes, Release 4.0*』

NS-OS コンフィギュレーション ガイド

『*Cisco NX-OS Getting Started with Virtual Device Contexts, Release 4.0*』

『*Cisco NX-OS Fundamentals Configuration Guide, Release 4.0*』

『*Cisco NX-OS Interfaces Configuration Guide, Release 4.0*』

『*Cisco NX-OS Layer 2 Switching Configuration Guide, Release 4.0*』

『*Cisco NX-OS Quality of Service Configuration Guide, Release 4.0*』

『*Cisco NX-OS Unicast Routing Configuration Guide, Release 4.0*』

『*Cisco NX-OS Multicast Routing Configuration Guide, Release 4.0*』

『*Cisco NX-OS Security Configuration Guide, Release 4.0*』

『*Cisco NX-OS Virtual Device Context Configuration Guide, Release 4.0*』

『*Cisco NX-OS Software Upgrade Guide, Release 4.0*』

『*Cisco NX-OS Licensing Guide, Release 4.0*』

『*Cisco NX-OS High Availability and Redundancy Guide, Release 4.0*』

『*Cisco NX-OS System Management Configuration Guide, Release 4.0*』

『*Cisco NX-OS XML Management Interface User Guide, Release 4.0*』

『*Cisco NX-OS System Messages Reference*』

『*Cisco NX-OS MIB Quick Reference*』

NX-OS コマンド リファレンス

『*Cisco NX-OS Command Reference Master Index, Release 4.0*』

『*Cisco NX-OS Fundamentals Command Reference, Release 4.0*』

『*Cisco NX-OS Interfaces Command Reference, Release 4.0*』

『*Cisco NX-OS Layer 2 Switching Command Reference, Release 4.0*』

『*Cisco NX-OS Quality of Service Command Reference, Release 4.0*』

『*Cisco NX-OS Unicast Routing Command Reference, Release 4.0*』

『*Cisco NX-OS Multicast Routing Command Reference, Release 4.0*』

『*Cisco NX-OS Security Command Reference, Release 4.0*』

『*Cisco NX-OS Virtual Device Context Command Reference, Release 4.0*』

『*Cisco NX-OS High Availability and Redundancy Command Reference, Release 4.0*』

『*Cisco NX-OS System Management Command Reference, Release 4.0*』

その他のソフトウェア マニュアル

『*Cisco NX-OS Troubleshooting Guide, Release 4.0*』

マニュアルの入手方法、テクニカル サポート、およびセキュリティ ガイドライン

マニュアルの入手方法、テクニカル サポート、マニュアルに関するフィードバックの提供、セキュリティ ガイドライン、および推奨エイリアスや一般的なシスコのマニュアルについては、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

シスコのテクニカル サポート

次の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。

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

以下を含むさまざまな作業にこの Web サイトが役立ちます。

- テクニカル サポートを受ける
- ソフトウェアをダウンロードする
- セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける
- ツールおよびリソースへアクセスする
  - Product Alert の受信登録
  - Field Notice の受信登録
  - Bug Toolkit を使用した既知の問題の検索
- Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する
- トレーニング リソースへアクセスする
- TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する

Japan テクニカル サポート Web サイトでは、Technical Support Web サイト（http://www.cisco.com/techsupport）の、利用頻度の高いドキュメントを日本語で提供しています。

Japan テクニカル サポート Web サイトには、次の URL からアクセスしてください。

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

Service Request ツールの使用

Service Request ツールには、次の URL からアクセスできます。

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

日本語版の Service Request ツールは次の URL からアクセスできます。

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

シスコの世界各国の連絡先一覧は、次の URL で参照できます。

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

その他の情報の入手方法

シスコの製品、サービス、テクノロジー、ネットワーキング ソリューションに関する情報について、さまざまな資料をオンラインで入手できます。

- シスコの E メール ニュースレターなどの配信申し込みについては、Cisco Subscription Center にアクセスしてください。

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

- 日本語の月刊 Email ニュースレター「Cisco Customer Bridge」については、下記にアクセスください。

  http://www.cisco.com/web/JP/news/cisco_news_letter/ccb/

- シスコ製品に関する変更やアップデートの情報を受信するには、Product Alert Tool にアクセスし、プロファイルを作成して情報の配信を希望する製品を選択してください。Product Alert Tool には、次の URL からアクセスできます。

  http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

- 『*Cisco Product Quick Reference Guide*』はリファレンス ツールで、パートナーを通じて販売されている多くのシスコ製品に関する製品概要、主な機能、製品番号、および簡単な技術仕様が記載されています。『*Cisco Product Quick Reference Guide*』を発注するには、次の URL にアクセスしてください。

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

- ネットワークの運用面の信頼性を向上させることのできる最新の専門的サービス、高度なサービス、リモート サービスに関する情報については、Cisco Services Web サイトを参照してください。Cisco Services Web サイトには、次の URL からアクセスできます。

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

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

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

- DVD に収録されたシスコの技術マニュアル（Cisco Product Documentation DVD）は、Product Documentation Store で発注できます。Product Documentation Store には、次の URL からアクセスできます。

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

- 日本語マニュアルの DVD は、マニュアルセンターから発注できます。マニュアルセンターには下記よりアクセスください。

  http://www.cisco.com/japanese/warp/public/3/jp/service/manual_j/manual_center/index.shtml

- Cisco Press では、ネットワーク、トレーニング、認定関連の出版物を発行しています。Cisco Press には、次の URL からアクセスできます。

  http://www.ciscopress.com

- 日本語のシスコプレスの情報は以下にアクセスください。

  http://www.seshop.com/se/ciscopress/default.asp

- 『*Internet Protocol Journal*』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコが発行する季刊誌です。『*Internet Protocol Journal*』には、次の URL からアクセスできます。

  http://www.cisco.com/ipj

- 『*What's New in Cisco Product Documentation*』は、シスコ製品の最新マニュアル リリースに関する情報を提供するオンライン資料です。毎月更新されるこの資料は、製品カテゴリ別にまとめられているため、目的の製品マニュアルを見つけることができます。

  http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

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

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

CHAPTER 1

トラブルシューティングの概要

この章では、Cisco NX-OS の設定または使用時に発生する可能性のある問題のトラブルシューティングについて、基本的な概念、方法、および一般的なガイドラインを紹介します。

この章で説明する内容は、次のとおりです。

トラブルシューティング手順の概要

ここでは、Cisco NX-OS デバイスまたは接続デバイスに関する問題のトラブルシューティング方法について説明します。

ネットワークのトラブルシューティング手順は、次のとおりです。

ステップ 1　すべてのデバイスで、同じ Cisco NX-OS リリースが使用されるようにします。

ステップ 2　使用している Cisco NX-OS リリースのリリース ノートを参照して、最新の機能、制限事項、および警告を確認します。Cisco NX-OS リリース ノートには、次の URL からアクセスできます。http://www.cisco.com/en/US/products/ps9372/prod_release_notes_list.html

ステップ 3　システム メッセージ ロギングをイネーブルにします。詳細については、「症状の概要」（p.1-6）を参照してください。

ステップ 4　変更を実装したあとは、新しい設定変更に対してトラブルシューティングを実施します。

ステップ 5　特定の症状に関する情報を収集します。詳細については、「情報の収集」（p.1-4）を参照してください。

ステップ 6　デバイスとエンド　　デバイス間の物理的な接続を確認します。詳細については、「ポートの確認」（p.1-4）を参照してください。

ステップ 7　レイヤ 2 接続を確認します。詳細については、「レイヤ 2 接続の確認」（p.1-5）を参照してください。

ステップ 8　エンドツーエンド接続およびルーティング設定を確認します。詳細については、「レイヤ 3 接続の確認」（p.1-5）を参照してください。

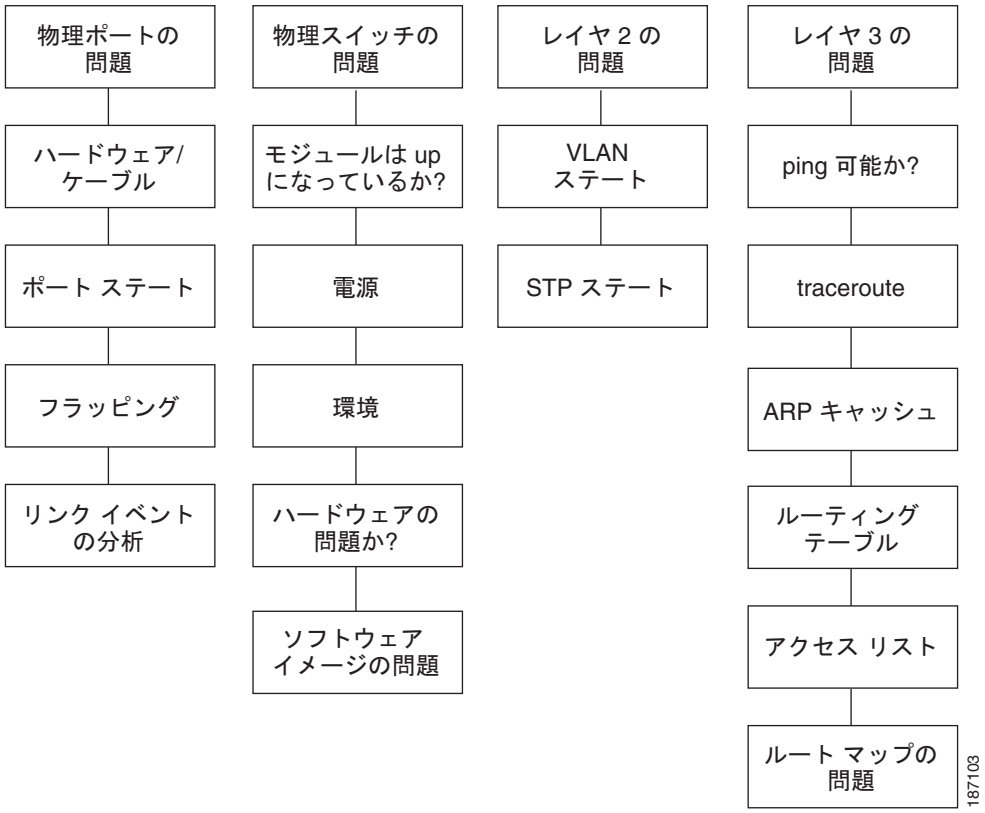
ステップ 9　トラブルシューティングを行っても問題を解決できない場合は、Cisco TAC に連絡するか、テクニカル サポート担当者にお問合せください。

トラブルシューティング手順

次の 4 つの領域のいずれかを選択して 図 1-1 内のその領域の各項目を検証して、問題を絞り込みます。

- 物理ポートの問題
- 物理デバイスの問題
- レイヤ 2 の問題
- レイヤ 3 の問題

図 1-1　トラブルシューティング手順



トラブルシューティングのガイドライン

ここでは、Cisco NX-OS デバイスのトラブルシューティングを行う際のガイドラインを示します。

ここで説明する内容は、次のとおりです。

情報の収集

ここでは、ネットワーク内の問題に関するトラブルシューティングでよく使用されるツールについて説明します。各章には、その章に関連する症状および考えられる問題に個別に対応するツールおよびコマンドが掲載されています。

（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おく必要があります。トポロジの情報については、ネットワーク設計者にお問合せください。

次のコマンドを使用して、デバイスの一般的な情報を収集します。

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

ポートの確認

次の作業を実行して、ポートが適切に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、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。
- ポートの LED がグリーンになっていることを確認します。
- インターフェイスが正しい VDC 内にあることを確認します。

  show vdc membership コマンドを使用して、インターフェースがどの VDC に属しているかを確認します。このコマンドを使用するには、ネットワーク管理者ロールでデバイスにログ インする必要があります。
- インターフェイスが動作していることを確認します。

  show interface brief コマンドを使用します。ステータスが up である必要があります。

ポートのトラブルシューティングの詳細については、第 5 章「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

次のコマンドを使用して、レイヤ 2 接続を確認します。

- **show vlan all-ports** コマンドを使用して、必要なすべてのインターフェイスが同じ VLAN 内にあることを確認します。VLAN のステータスが active である必要があります。
- **show port-channel compatibility-parameters** コマンドを使用して、ポート チャネル内のすべてのポートの速度、デュプレックス、およびトランク モードが同一に設定されていることを確認します。
- **show running-config spanning-tree** コマンドを使用して、ネットワーク内のすべてのデバイスで Spanning Tree Protocol（STP; スパニング ツリー プロトコル）の設定が同一であることを確認します。
- **show processes | include ER** CLI コマンドを使用して、エラー状態にある重要なレイヤ 2 プロセスがないことを確認します。
- **show spanning-tree blockedports** コマンドを使用して、STP によってブロックされているポートを表示します。
- **show mac address-table dynamic vlan** コマンドを使用して、各ノードで学習またはエージングが発生しているかどうかを判別します。

レイヤ 2 に関する問題のトラブルシューティングの詳細については、第 6 章「VLAN のトラブルシューティング」および第 7 章「STP のトラブルシューティング」を参照してください。

レイヤ 3 接続の確認

次の作業を実施して、レイヤ 3 接続を確認します。

- デフォルト ゲートウェイを設定していることを確認します。
- ルーティング ドメイン全体で同一のダイナミック ルーティング プロトコル パラメータを設定していること、またはスタティック ルートを設定していることを確認します。
- 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。

次のコマンドを使用して、ルーティング設定を確認します。

- **show arp**
- **show ip routing**
- **show platform forwarding**

レイヤ 3 接続を確認する方法については、「ping および traceroute」（p.B-4）を参照してください。レイヤ 3 に関する問題のトラブルシューティングの詳細については、第 8 章「ルーティングのトラブルシューティング」を参照してください。

症状の概要

このマニュアルでは、症状ベースのトラブルシューティング方法を使用します。各章で説明する問題の症状とネットワーク内で観察した症状を比較することによって、Cisco NX-OS の問題を診断および解決できます。

このマニュアルで説明する症状とネットワーク内で観察した症状を比較すると、ソフトウェア設定の問題や動作不能のハードウェア コンポーネントを診断して修正することができます。そのため、ネットワークの停止を最小限にしたまま問題の解決を図れます。以下に、問題と対処方法を示します。

- 必要な 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 および RSPAN、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 サポート担当者によって使用されるコア 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 ソフトウェアでは、これらの Syslog（システム）メッセージをコンソール（およびオプションとして別のデバイス上にあるログ収集サーバ）に送信します。ただし、すべてのメッセージがデバイスの問題を表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 ソフトウェアの問題を診断するのに役立つメッセージもあります。

ここで説明する内容は、次のとおりです。

システム メッセージ テキスト

メッセージ テキストは、状態を説明するテキスト文字列です。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。これらの変数フィールドの情報はメッセージごとに変化するので、角括弧（[ ]）で囲まれた短い文字列で表されます。たとえば、10 進数は［dec］と表されます。

```
PORT-3-IF_UNSUPPORTED_TRANSCEIVER: Transceiver for interface [chars] is not supported.
```

この文字列を使用して、『*Cisco NX-OS System Messages Reference*』で一致するシステム メッセージを検索してください。

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。推奨処置は、単純に「対処不要です。」になることがあります。また、推奨処置には、修正、または次の例に示すようにテクニカル サポートへの問い合わせが含まれることもあります。

エラー メッセージ `PORT-3-IF_UNSUPPORTED_TRANSCEIVER: Transceiver for interface [chars] is not supported.`

説明　認定ベンダーのトランシーバ（SFP）ではありません。

推奨処置　**show interface transceiver** CLI コマンドまたは類似の DCNM コマンドを入力して、使用しているトランシーバを調べます。カスタマー サポート担当者に連絡し、トランシーバの認定ベンダーのリストを入手してください。

Syslog サーバの実装

Syslog ファシリティを使用して、Cisco NX-OS 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、ログを長期間にわたって検査する必要がある場合、または Cisco NX-OS デバイスにアクセスできなくなったときに役立ちます。

この例では、Solaris プラットフォームで Syslog ファシリティを使用するための Cisco NX-OS デバイスの設定手順を示します。ここでは Solaris ホストを使用しますが、Syslog の設定はすべての UNIX および Linux システムでほぼ同じです。

Syslog で使用されているファシリティでは、メッセージが Syslog サーバ（この例では Solaris システム）によってどのように処理されるかは、メッセージの重大度によって決まります。異なるメッセージ重大度ごとに、Syslog サーバによるメッセージ処理の方法は変わります。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 サーバで重大度を指定すると、そのレベルまたはそれよりも大きな重大度（小さい数字）を持つすべてのメッセージに、Syslog サーバに設定した処理が適用されるようになります。

（注） シスコ以外の他の Syslog メッセージとの競合を避けるために、Cisco NX-OS のメッセージを標準の Syslog ファイルとは別のファイルに記録するように Syslog サーバを設定する必要があります。ログ メッセージが / ファイル システムに書き込まれるのを防止するため、ログ ファイルは / ファイル システム上に配置しないでください。
Syslog クライアント：switch1
Syslog サーバ：172.22.36.211(Solaris)
Syslog ファシリティ：local1
Syslog 重大度：通知（レベル 5、デフォルト）
Cisco NX-OS メッセージを記録するファイル：/var/adm/nxos_logs

Syslog サーバを設定する手順は、次のとおりです。

ステップ 1　Cisco NX-OS を設定します。

```
switch1# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch1(config)# logging server 192.0.2.1 6 facility local1
```

設定を表示するには、次のように **show logging server** コマンドを入力します。

```
switch1# show logging server
Logging server: enabled
{192.0.2.1}
     server severity: notifications
     server facility: local1
```

ステップ 2　Syslog サーバを次のように設定します。

a. 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、facility.severity と処理の間に少なくとも 1 つのタブが必要です（/var/adm/nxos_logs）。

```
#Below is for the NX-OS logging
local1.notice /var/adm/nxos_logs
```

b. ログ ファイルを作成します。

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

c. 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.
```

d. Syslog プロセスが開始されたことを確認します。

```
# ps -ef |grep syslogd
     root 23508 1 0 11:01:41 ? 0:00 /usr/sbin/syslogd
```

ステップ 3　Cisco NX-OS 上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 ダウンされたあとに再度イネーブルにされ、Syslog サーバ上で次のように一覧表示されます。スイッチの 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] : 2004 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] : 2004 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] : 2004 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表示することで、現在の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。

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

```
switch# show logging ?

console        Show console logging configuration
info           Show logging configuration
internal       syslog syslog internal information
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
pending        server address pending configuration
pending-diff   server address pending configuration diff
server         Show server logging configuration
session        Show logging session status
status         Show logging status
timestamp      Show logging timestamp configuration
|              Pipe command output to filter
```

例 1-1 に、**show logging** コマンドの出力例を示します。

例 1-1　show logging コマンド

```
switch# show logging server
Logging server: enabled
{192.0.1.1}
server severity: critical
server facility: user
```

NVRAM ログの表示

優先度が 0、1、または 2 のシステム メッセージは、スーパーバイザ モジュール上の NVRAM に記録されます。スイッチの再起動後、**show logging nvram** CLI コマンドを使用すると、NVRAM 内のこれらの Syslog メッセージが表示されます。例 1-2 を参照してください。

例 1-2　show logging nvram コマンド

```
switch# show logging nvram
2008 Jun 25 20:10:27 switch %$ VDC-1 %$ %VDC_MGR-2-VDC_ONLINE: vdc 1 has come on
line
2008 Jun 25 20:10:29 switch %$ VDC-1 %$ %PLATFORM-2-PS_OK: Power supply 1 ok (Se
rial number DTH1117T005)
2008 Jun 25 20:10:29 switch %$ VDC-1 %$ %PLATFORM-2-PS_FANOK: Fan in Power suppl
y 1 ok
2008 Jun 25 20:10:29 switch %$ VDC-1 %$ %PLATFORM-2-PS_OK: Power supply 2 ok (Se
rial number DTH1117T009)
2008 Jun 25 20:10:29 switch %$ VDC-1 %$ %PLATFORM-2-PS_FANOK: Fan in Power suppl
y 2 ok
2008 Jun 25 20:10:34 switch %$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 2 powered
up (Serial number JAB104400P0)
2008 Jun 25 20:10:35 switch %$ VDC-1 %$ %CARDCLIENT-2-SSE: MOD:11 FABRIC ONLINE
2008 Jun 25 20:10:48 switch %$ VDC-1 %$ %VDC_MGR-2-VDC_ONLINE: vdc 2 has come on
line
2008 Jun 25 20:10:56 switch %$ VDC-1 %$ %PLATFORM-2-FANMOD_FAN_OK: Fan module 1
(Fan1(sys_fan1) fan) ok
2008 Jun 25 20:10:56 switch %$ VDC-1 %$ %PLATFORM-2-FANMOD_FAN_OK: Fan module 2
(Fan2(sys_fan2) fan) ok
2008 Jun 25 20:10:56 switch %$ VDC-1 %$ %PLATFORM-2-FANMOD_FAN_OK: Fan module 3
(Fan3(fab_fan1) fan) ok
2008 Jun 25 20:10:56 switch %$ VDC-1 %$ %PLATFORM-2-FANMOD_FAN_OK: Fan module 4
(Fan4(fab_fan2) fan) ok
2008 Jun 25 20:16:25 switch %$ VDC-1 %$ %PLATFORM-2-PFM_SYSTEM_RESET: Manual sys
tem restart from Command Line Interface
2008 Jun 25 20:21:42 switch %$ VDC-1 %$ %KERN-2-SYSTEM_MSG: Starting kernel... -
 kernel
2008 Jun 25 20:21:55 switch %$ VDC-1 %$ %CARDCLIENT-2-REG: Sent
2008 Jun 25 20:21:56 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: R2D2: P1 SUP NO GMTL
 FOR P1 SUP  - r2d2
2008 Jun 25 20:21:56 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: R2D2: P1 SUP NO GMTL
 FOR P1 SUP  - r2d2
2008 Jun 25 20:22:00 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: R2D2: P1 SUP: Reset
Tx/Rx during QOS INIT  - r2d2
2008 Jun 25 20:22:08 switch %$ VDC-1 %$ %USER-2-SYSTEM_MSG: no feature-name to a
dd  - clis
2008 Jun 25 20:22:09 switch %$ VDC-1 %$ %CARDCLIENT-2-SSE: LC_READY sent
2008 Jun 25 20:22:10 switch %$ VDC-1 %$ %CARDCLIENT-2-SSE: MOD:6 SUP ONLINE
```

カスタマー サポートへの連絡

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。連絡する前に、サポート担当者が迅速に対応できるように、次の情報を用意しておいてください。

- スイッチの受領日
- シャーシのシリアル番号（シャーシの背面パネル右側のラベルに記載）
- ソフトウェアのタイプとリリース番号
- メンテナンス契約または保証の情報
- 問題の簡単な説明
- 問題を特定し、解決するために行った作業の簡単な説明

これらの情報を収集してから、「マニュアルの入手方法、テクニカル サポート、およびセキュリティ ガイドライン」（p.xi）を参照してください。

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、「テクニカル サポートへ問い合わせる前の準備」（p.A-1）を参照してください。

CHAPTER 2

インストール、アップグレード、および再起動のトラブルシューティング

この章では、Cisco NX-OS のインストール、アップグレード、または再起動時に発生する可能性のある問題を識別して解決する方法について説明します。

この章で説明する内容は、次のとおりです。

概要

Cisco NX-OS は、キックスタート イメージとシステム イメージの 2 つのイメージで構成されます。

インストール、アップグレード、および再起動は、ネットワーク メンテナンス活動の一部分で継続的に実施されます。これらの操作を実稼働環境で実行する際に継続中の動作が中断されるリスクを最小限に抑え、また何らかの問題が発生したときに素早く復旧させる方法を確認しておくことが重要です。

（注） 文書化の目的で、このマニュアルでは「アップグレード」という用語を使用します。ただし、アップグレードは、ユーザのニーズにより、スイッチのアップグレードとダウングレードの両方を意味しています。

ガイドライン

ここでは、Cisco NX-OS ソフトウェアのインストール、イメージのアップグレードとダウングレード、および再起動に関するガイドラインを示します。具体的な内容は、次のとおりです。

インストールのガイドライン

Cisco NX-OS ソフトウェア イメージをインストールする際は、次のガイドラインに従ってください。

- サーバの可用性 — FTP または TFTP サーバが利用できることを確認します。
- 互換性チェック — **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、および新規のロードがハードウェアの互換性に与える影響を確認します。互換性を調べてください。

アップグレードのガイドライン

次のチェックリストを使用して、アップグレードの準備を行ってください。

チェックリスト	確認済み
新しい Cisco NX-OS イメージを、bootflash: または slot0: にあるスーパーバイザ モジュールにコピーします。	❑
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保存します。	❑
コンフィギュレーションのコピーをリモート TFTP サーバにバックアップします。	❑
ネットワークに対するメンテナンスの適切な時間枠の中でアップグレードのスケジュールを確保します。	❑

チェックリストの確認を終了すると、ネットワーク内のスイッチをアップグレードする準備は完了です。

（注） アップグレード中にアクティブ スーパーバイザはスタンバイ スーパーバイザになりますが、これは正常な動作です。

Cisco NX-OS ソフトウェア イメージをアップグレードまたはダウングレードする際は、次のガイドラインに従ってください。

- アップグレードまたはダウングレードするリリースに対応する『*Cisco NX-OS Release Notes*』の内容を確認します。『*Cisco NX-OS Release Notes*』は、次の Web サイトから入手できます。
  http://cisco.com/en/US/products/ps5989/prod_release_notes_list.html
- FTP または TFTP サーバが利用できることを確認します。
- スタートアップ コンフィギュレーションを NVRAM 内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。このステップでは、スタートアップ コンフィギュレーションのコピーをバックアップします（『*Cisco NX-OS System Management Configuration Guide, Release 4.0*』の「Rollback」の章を参照してください）。

- 可能であれば、中断のないアップグレードの実行を選択します。
- 各スーパーバイザ コンソールへの PC シリアル接続を確立して、アップグレードの作業をファイルに記録します。このシリアル接続で、起動時のすべてのエラー メッセージまたは問題を受け取ります。
- **install all** [{| **kickstart** | **system**} *URL*] コマンドを使用して、完了スクリプトの実行、イメージのテスト、およびハードウェアの互換性の確認を行います。詳細については、「Cisco NX-OS ソフトウェアのインストール」（p.2-7）を参照してください。**install all** コマンドを使用すると、次の利点があります。
  - 1 つのコマンドを使用するだけで、中断を最小限に抑えた手順を実行し、スイッチ全体をアップグレードできます。
  - コマンドを続行する前に、目的のシステム変更に関する説明情報を受け取れます。
  - コマンドを取り消すオプションがあります。コマンドの効果についての説明が表示されたあとに次の質問が表示されるので、続行または取り消しを選択できます（デフォルトは no）。

    ```
    Do you want to continue (y/n) [n] :y
    ```

  - このコマンドの進捗状況は、コンソール、Telnet、および SSH の画面に表示できます。
  - 稼働中のキックスタート イメージおよびシステム イメージを含むイメージの整合性は、自動的にチェックされます。
  - このコマンドでは、プラットフォームの妥当性検査を実行して、不正なイメージが使用されていないことを確認します。たとえば、デバイスのアップグレードに、誤って Cisco NX-OS イメージが使用されていないこと確認します。
  - **install all** コマンドを発行したあとに、シーケンス内でいずれかのステップが失敗すると、コマンドは進行中のステップを完了してから終了します。

再起動のガイドライン

Cisco NX-OS から実行できるシステム再起動には、次の 3 つの異なるタイプがあります。

- 回復可能 — プロセスが再起動し、サービスには影響しません。
- 回復不能 — プロセスの再起動回数が一定時間（秒）内に実行できる再起動の最大数を超えたために、プロセスの再起動を再実行できない場合に使用します。
- システム停止またはクラッシュ — システムとの通信が完全にできなくなった場合に使用します。

再起動のスケジュールは、重要な業務時間内にサービスが中断されないように設定してください。

（注） 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 以上（レベル 0、1、および 2）のログ メッセージは、最大 100 個まで NVRAM に保存されます。このログは、**show logging nvram** CLI コマンドを使用していつでも表示できます。

Cisco NX-OS ソフトウェア インストールの確認

show install all status コマンドを使用して、ソフトウェアのインストールの進捗状況を監視できます。

また、**show install all status** CLI コマンドを使用すると、実行中の **install all** コマンドまたは最後に **install all** コマンドが実行されたときのログを、コンソール、SSH、または Telnet セッションから表示できます。

このコマンドでは、コンソール端末に接続していない場合でも、**install all** コマンドの出力がアクティブ スーパーバイザ モジュールおよびスタンバイ スーパーバイザ モジュールの両方に提供されます。ここでは、CLI から発行された **install all** コマンドのステータスだけを表示します。例 2-1 を参照してください。

例 2-1　install all コマンドの出力

```
switch# show install all status
There is an on-going installation... <---------------------- in progress installation
Enter Ctrl-C to go back to the prompt.
Verifying image bootflash:/b-4.0.0.104
-- SUCCESS
Verifying image bootflash:/i-4.0.0.104
-- SUCCESS
Extracting "system" version from image bootflash:/i-4.0.0.104.
-- SUCCESS
Extracting "kickstart" version from image bootflash:/b-4.0.0.104.
-- SUCCESS
Extracting "loader" version from image bootflash:/b-4.0.0.104.
-- SUCCESS
switch# show install all status
This is the log of last installation. <----------------- log of last install
Verifying image bootflash:/b-4.0.0.104
-- SUCCESS
Verifying image bootflash:/i-4.0.0.104
-- SUCCESS
Extracting "system" version from image bootflash:/i-4.0.0.104.
-- SUCCESS
Extracting "kickstart" version from image bootflash:/b-4.0.0.104.
-- SUCCESS
Extracting "loader" version from image bootflash:/b-4.0.0.104.
-- SUCCESS
```

無停止アップグレードの確認

無停止アップグレードが開始されると、Cisco NX-OS はアップグレードが開始されようとしていることをすべてのサービスに通知し、アップグレードを進めることができるかどうかを調べます。アップグレードを続行できない場合、アップグレードは打ち切られます。そのような場合は、**show install all failure-reason** コマンドを入力して、アップグレードを続行できない理由を識別してください。

```
...
Do you want to continue with the installation (y/n)?  [n] y

Install is in progress, please wait.

Notifying services about the upgrade.
[#                    ]   0% -- FAIL. Return code 0x401E0066 (request timed out).

Please issue "show install all failure-reason" to find the cause of the
failure.<---system prompt to enter the show all failure-reason command.

Install has failed. Return code 0x401E0066 (request timed out).
Please identify the cause of the failure, and try 'install all' again.

switch# show install all failure-reason
Service: "cfs" failed to respond within the given time period.
switch#
```

何らかの理由（保存ランタイム状態障害やラインカード アップグレード障害など）で障害がある場合、アップグレードがすでに進行中のときには、変更をロールバックできないため、アップグレードの途中でスイッチが再起動されます。そのような場合、アップグレードは失敗します。**show install all failure-reason** コマンドの入力は求められません。このコマンドを入力しても有益な情報は得られません。

アップグレードに失敗した理由を判別する場合にサポートが必要な場合は、**show tech support** コマンド出力から詳細を収集し、可能であればインストールからコンソール出力を収集します。

ROM モニタ モードの使用

ロードする有効なシステム イメージを検出できない場合、システムは ROM モニタ モードで起動します。ROM モニタ モードには、起動時に起動シーケンスを中断してアクセスすることもできます。ROM モニタ モードでは、デバイスの起動または診断テストを実行できます。

大半のシステムでは、**reload** EXEC コマンドを入力してから、システム起動中の最初の 60 秒間に Break コマンドを発行すると、ROM モニタ モードを開始できます。Break コマンドを発行するには、キーボード上の Break キーを押すか、Break キーの組み合わせを使用します（デフォルトの Break キーの組み合わせは Ctrl+C です）。

Cisco NX-OS 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

ここでは、ソフトウェアのインストレーションへのアップグレードまたはダウングレードが失敗した場合に考えられる原因とその解決方法について説明します。

インストール時のソフトウェアのエラーによる終了

現象　ソフトウェアのインストールが、エラーにより終了する。

表 2-1　ソフトウェアのインストールがエラーにより終了

問題	考えられる原因	解決方法
インストールがエラーにより終了する。	スタンバイ 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格納する十分な領域がない。	**delete** コマンドを使用して、ファイルシステムから不要なファイルを削除します。
	指定されたシステム イメージとキックスタート イメージの間に互換性がない。	インストール プロセスの出力を調べて、非互換性の詳細について確認します。システム イメージをアップデートする前に、キックスタート イメージをアップデートしている可能性があります。
	install all コマンドが、スタンバイ スーパーバイザ モジュール上で発行された。	このコマンドをアクティブ スーパーバイザ モジュールだけで発行するようにします。
	アップグレードの進行中にモジュールが装着された。	インストールを再実行します。詳細については、「Cisco NX-OS ソフトウェアのインストール」（p.2-7）を参照してください。
	アップグレードの進行中にスイッチの電源が停止した。	インストールを再実行します。「Cisco NX-OS ソフトウェアのインストール」（p.2-7）を参照してください。
	ソフトウェア イメージの指定されたパスが正しくない。	リモート ロケーションへのパス全体を正しく指定します。
	別のインストール プロセスがすでに進行中である。	すべてのステージでスイッチの状態を確認し、10 秒間待機してからインストールを再び実行します。10 秒経過する前にインストール プロセスを再実行すると、コマンドは拒否され、インストールが現在進行していることを示すエラー メッセージが表示されます。
	モジュールがアップグレードに失敗した。	インストールを再実行します。詳細については、「Cisco NX-OS ソフトウェアのインストール」（p.2-7）を参照してください。 または、**install module** CLI 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 ソフトウェアのインストール

スイッチ上のソフトウェアの自動アップグレードを CLI から実行する手順は次のとおりです。

ステップ 1　アクティブ スーパーバイザのコンソール、Telnet、または SSH ポートからスイッチにログインします。

ステップ 2　必要であれば、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。

ステップ 3　**install all** コマンドを発行して、アップグレードを実行します。

次の例は、SPC サーバにあるソース イメージを使用して、**install all** コマンドでアップグレードする方法を示しています。

ヒント　**install all** コマンドの互換性チェックの出力内容は、必ず慎重に確認してください。この互換性チェックでは、アップグレードが必要な対象（BIOS、ローダ、ファームウェア）および無停止アップグレードに対応していないモジュールが正確に示されます。出力の結果に対して何らかの疑問や懸念がある場合は、**n** を選択してインストールを停止し、次のレベルのサポートに連絡してください。

```
switch# install all system scp://testuser@tftp-server1/tftpboot/rel/qa/4.0/final/m95
00-sf1ek9-mz.4.0.bin kickstart scp://testuser@tftp-server1/tftpboot/rel/qa/4.0/fin
al/n7000-s1-kickstart-mz.4.0.bin
For scp://testuser@tftp-server1, please enter password:
For scp://testuser@tftp-server1, please enter password:

Copying image from scp://testuser@pal/tftpboot/rel/qa/4.0/final/n7000-s1
-kickstart-mz.4.0.bin to bootflash:///n7000-s1-kickstart-mz.4.0.bin.
[####################] 100% -- SUCCESS

Copying image from scp://testuser@pal/tftpboot/rel/qa/4.0/final/n7000-s1
-mz.4.0.bin to bootflash:///n7000-s1-mz.4.0.bin.
[####################] 100% -- SUCCESS

Verifying image bootflash:///n7000-s1-kickstart-mz.4.0.bin
[####################] 100% -- SUCCESS

Verifying image bootflash:///n7000-s1-mz.4.0.bin
[####################] 100% -- SUCCESS

Extracting "slc" version from image bootflash:///n7000-s1-mz.4.0.bin.
[####################] 100% -- SUCCESS

Extracting "ips" version from image bootflash:///n7000-s1-mz.4.0.bin.
[####################] 100% -- SUCCESS

Extracting "svclc" version from image bootflash:///n7000-s1-mz.4.0.bin.
[####################] 100% -- SUCCESS

Extracting "system" version from image bootflash:///n7000-s1-mz.4.0.bin.
[####################] 100% -- SUCCESS

Extracting "kickstart" version from image bootflash:///n7000-s1-kickstart-mz
.4.0.bin.
[####################] 100% -- SUCCESS

Extracting "loader" version from image bootflash:///n7000-s1-kickstart-mz.2.
1.1a.bin.
[####################] 100% -- SUCCESS
```

```
Compatibility check is done:
Module  bootable          Impact  Install-type  Reason
------  --------  --------------  ------------  ------
     1       yes  non-disruptive       rolling
     2       yes  non-disruptive       rolling
     3       yes      disruptive       rolling  Hitless upgrade is not supported
     4       yes      disruptive       rolling  Hitless upgrade is not supported
     5       yes  non-disruptive         reset
     6       yes  non-disruptive         reset


Images will be upgraded according to following table:
Module       Image       Running-Version           New-Version  Upg-Required
------  ----------  --------------------  --------------------  ------------
     1         slc               2.0(2b)               2.1(1a)           yes
     1        bios      v1.1.0(10/24/03)      v1.1.0(10/24/03)            no
     2         slc               2.0(2b)               2.1(1a)           yes
     2        bios      v1.1.0(10/24/03)      v1.1.0(10/24/03)            no
     3         ips               2.0(2b)               2.1(1a)           yes
     3        bios      v1.1.0(10/24/03)      v1.1.0(10/24/03)            no
     4       svclc               2.0(2b)               2.1(1a)           yes
     4       svcsb               1.3(5m)               1.3(5m)            no
     4       svcsb               1.3(5m)               1.3(5m)            no
     4        bios      v1.1.0(10/24/03)      v1.1.0(10/24/03)            no
     5      system               2.0(2b)               2.1(1a)           yes
     5   kickstart               2.0(2b)               2.1(1a)           yes
     5        bios      v1.1.0(10/24/03)      v1.1.0(10/24/03)            no
     5      loader                1.2(2)                1.2(2)            no
     6      system               2.0(2b)               2.1(1a)           yes
     6   kickstart               2.0(2b)               2.1(1a)           yes
     6        bios      v1.1.0(10/24/03)      v1.1.0(10/24/03)            no
     6      loader                1.2(2)                1.2(2)            no

Do you want to continue with the installation (y/n)?  [n] y

Install is in progress, please wait.

Syncing image bootflash:///n7000-s1-kickstart-mz.4.0.bin to standby.
[####################] 100% -- SUCCESS

Syncing image bootflash:///n7000-s1-mz.4.0.bin to standby.
[####################] 100% -- SUCCESS

Setting boot variables.
[####################] 100% -- SUCCESS

Performing configuration copy.
[####################] 100% -- SUCCESS

Module 5: Waiting for module online.
2005 May 20 15:46:03 ca-9506 %KERN-2-SYSTEM_MSG: mts: HA communication with standby
terminated. Please check the standby supervisor.
 -- SUCCESS

"Switching over onto standby".
```

ステップ 4　スイッチのコンソールを終了し、新規のターミナル セッションを開き、**show module** コマンドを使用し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。

install all コマンドが発行されたときに、コンフィギュレーションがすべてのガイドラインに適合していれば、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。

Cisco NX-OS ソフトウェア システム再起動のトラブルシューティング

ここでは、ソフトウェアの再起動で発生する可能性のある問題とその解決方法について説明します。具体的な内容は、次のとおりです。

電源投入時または再起動時におけるスイッチのハングアップ

現象　電源投入時または再起動時にスイッチがハングアップする。

表 2-2　電源投入時または再起動時におけるスイッチのハングアップ

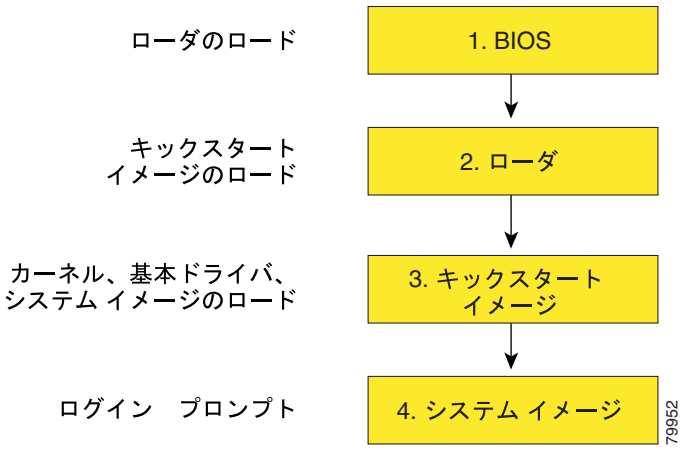
問題	考えられる原因	解決方法
デュアル スーパーバイザ構成で、電源投入時または再起動時にスイッチがハングアップする。	ブートフラッシュが破損している。	詳細については、「デュアル スーパーバイザ モジュール搭載スイッチの復旧」（p.2-16）を参照してください。
シングル スーパーバイザ構成で、電源投入時または再起動時にスイッチがハングアップする。	BIOS が破損している。	このモジュールを交換します。カスタマー サポート担当者に連絡して、故障したモジュールを返却してください。
	キックスタート イメージが破損している。	>loader プロンプトで、起動プロセスを中断します。キックスタート イメージをアップデートします。詳細については、「スーパーバイザ モジュールの loader> プロンプトからの復旧」（p.2-12）を参照してください。
	起動パラメータが不正である。	起動パラメータを確認して修正し、スイッチを再起動します。
	システム イメージが破損している。	switch#boot プロンプトで、起動プロセスを中断します。システム イメージをアップデートします。詳細については、「switch(boot)# プロンプトからの復旧」（p.2-14）を参照してください。

破損したブートフラッシュの復旧

すべてのスイッチ コンフィギュレーションは、内蔵ブートフラッシュに格納されています。内蔵ブートフラッシュが破損すると、場合によってはコンフィギュレーションが失われることがあります。コンフィギュレーション ファイルを、定期的に保存およびバックアップしてください。通常、スイッチの起動は、次のシーケンスで行われます（図 2-1 を参照）。

1. BIOS によって、ローダがロードされます。
2. ローダでは、キックスタート イメージを RAM にロードして起動します。
3. キックスタート イメージでは、システム イメージをロードして起動します。
4. システム イメージでは、スタートアップ コンフィギュレーション ファイルを読み込みます。

図 2-1　通常の起動シーケンス



スイッチ上のイメージが破損しているために先に進めない場合は（エラー状態）、スイッチの起動シーケンスを中断して次の項で説明されている BIOS 設定ユーティリティに入ることにより、イメージを復旧できます。このユーティリティには、破損した内蔵ディスクを復旧する必要がある場合にだけアクセスしてください。

注意　ここで説明されている BIOS 設定の変更は、破損したブートフラッシュを復旧する場合にだけ必要になります。

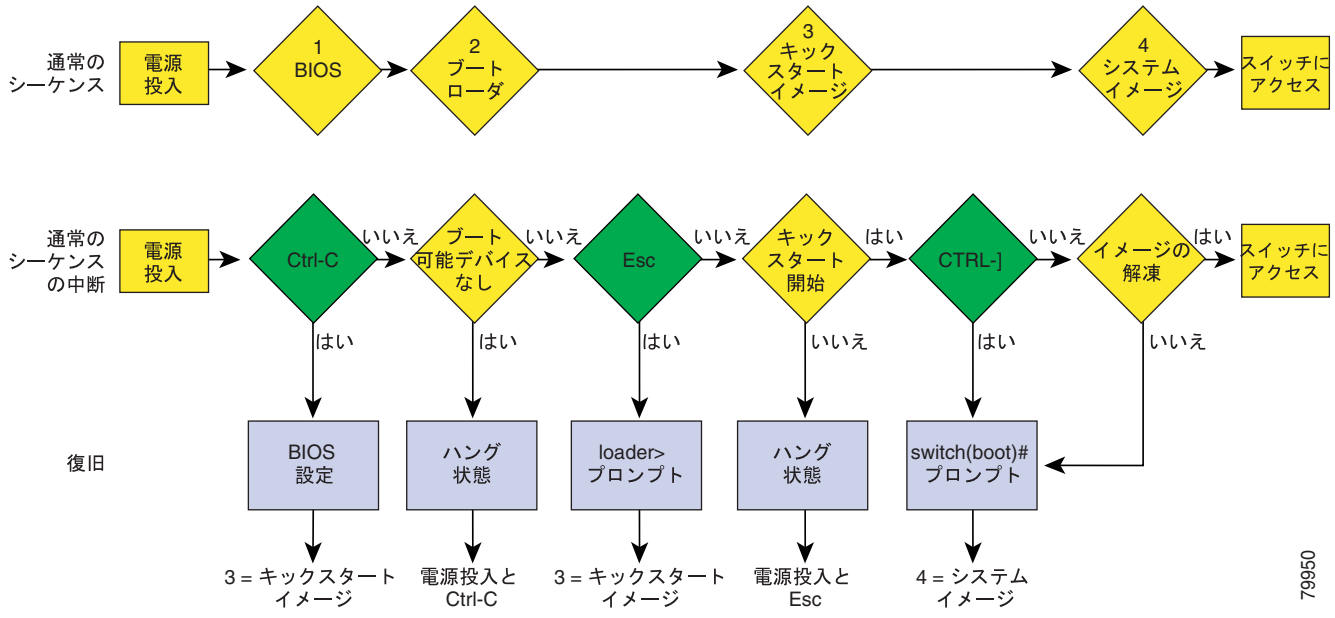
復旧の手順では、通常のシーケンスを中断する必要があります。スイッチの内部シーケンスでは、スイッチの電源を投入してから端末に switch プロンプトが表示されるまでの間に、BIOS、ブートローダ、キックスタート、およびシステムの 4 つのフェーズがあります（表 2-3 および図 2-2 を参照）。

表 2-3　復旧の割り込み

フェーズ	通常のプロンプト[1]	復旧用のプロンプト[2]	説明
BIOS	`loader>`	`No bootable device`	BIOS によって、電源投入時自己診断テスト、メモリ テスト、および他のオペレーティング システム アプリケーションが開始されます。BIOS 設定ユーティリティでネットブート オプションを使用するには、テストの進行中に **Ctrl+C** キーを押します。
ブート ローダ	`Starting kickstart`	`loader>`	ブート ローダでは、ロードされたソフトウェアの圧縮を解除し、そのファイル名を参照先として使用することでイメージを起動します。これらのイメージは、ブートフラッシュから起動できます。メモリ テストが完了したあとは、**Esc** キーを押してブート ローダのプロンプトを開始します。
Kickstart	`Uncompressing system`	`switch(boot)#`	ブート ローダのフェーズが完了したあとは、**Ctrl+]**[3] キーを押して（Ctrl キーと右角カッコ キーを同時に押す）、`switch(boot)#` プロンプトを表示します。破損が原因でコンソールをこのプロンプトで停止させる場合は、システム イメージをコピーしてからスイッチを再起動します。
System	`Login:`	—	システム イメージでは、最後に保存された実行コンフィギュレーションのコンフィギュレーション ファイルをロードし、スイッチのログイン プロンプトに戻ります。

1. このプロンプトまたはメッセージは、各フェーズの最後に表示されます。
2. このプロンプトまたはメッセージは、スイッチが次のフェーズに進めないときに表示されます。
3. 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ことがあるので、その場合はキーの割り当てを変更する必要があります。詳細については、Telnet クライアントに付属のマニュアルを参照してください。

図 2-2　通常および復旧のシーケンス



スーパーバイザ モジュールの loader> プロンプトからの復旧

注意　この手順では、**init system** コマンドを使用しており、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おいてください。

（注）　loader> プロンプトは、通常の switch# プロンプトとは異なります。このプロンプトでは、CLI のコマンド補完機能は機能せず、不要なエラーの原因になることがあります。コマンドは、その全体を正確に入力する必要があります。

ヒント　loader> プロンプトで使用できるコマンドのリストを表示したり、そのリストにある特定のコマンドに関する詳細な情報を取得したりするには、このプロンプトで **help** コマンドを実行してください。

シングル スーパーバイザ モジュール搭載スイッチで、破損したキックスタート イメージ（システム エラー状態）を復旧する手順は、次のとおりです。

ステップ 1　loader> プロンプトでスイッチのローカル IP アドレスを入力し、**Enter** キーを押します。

```
loader> net --ip=172.16.1.2
```

ステップ 2　サブネット マスクを指定します。

```
loader> net --nm= 255.255.255.0
```

ステップ 3　デフォルト ゲートウェイの IP アドレスを指定します。

```
loader> net --gw=172.16.1.1
```

ステップ 4　目的のサーバからキックスタート イメージ ファイルを起動します。

```
loader> boot tftp://172.16.10.100/n7000-s1-kickstart-4.0.bin
```

この例では、172.16.10.100 が TFTP サーバの IP アドレスで、n7000-s1-kickstart-3.0.bin がそのサーバに存在するキックスタート イメージ ファイル名です。

switch(boot)# プロンプトは、使用可能なキックスタート イメージがあることを示すものです。

ステップ 5　switch(boot)# プロンプトで、**init system** コマンドを発行します。

```
switch(boot)# init system
```

注意　このコマンドを発行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おいてください。

ステップ 6　「switch(boot)# プロンプトからの復旧」（p.2-14）で指示されている手順を実行します。

loader> プロンプトからの復旧

注意　この手順では、**init system** コマンドを使用しており、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おいてください。

（注）　loader> プロンプトは、通常の switch# プロンプトまたは switch(boot)# プロンプトとは異なります。このプロンプトでは、CLI のコマンド補完機能は機能せず、不要なエラーの原因になることがあります。コマンドは、その全体を正確に入力する必要があります。

ヒント　loader> プロンプトで使用できるコマンドのリストを表示したり、そのリストにある特定のコマンドに関する詳細な情報を取得したりするには、このプロンプトで **help** コマンドを実行してください。

シングル スーパーバイザ モジュール搭載スイッチで、破損したキックスタート イメージ（システム エラー状態）を復旧する手順は、次のとおりです。

ステップ 1　loader> プロンプトでスイッチの IP アドレスおよびサブネット マスクを入力し、**Enter** キーを押します。

```
loader> ip address 172.16.1.2 255.255.255.0
Found Intel EtherExpressPro100 82559ER at 0xe800, ROM address 0xc000
Probing...[Intel EtherExpressPro100 82559ER]Ethernet addr: 00:05:30:00:52:27
Address: 172.16.1.2
Netmask: 255.255.255.0
Server: 0.0.0.0
Gateway: 0.0.0.0
```

ステップ 2　デフォルト ゲートウェイの IP アドレスを指定します。

```
loader> ip default-gateway 172.16.1.1
Address: 172.16.1.2
Netmask: 255.255.255.0
Server: 0.0.0.0
Gateway: 172.16.1.1
```

ステップ 3　目的のサーバからキックスタート イメージ ファイルを起動します。

```
loader> boot tftp://172.16.10.100/kickstart-image1
Address: 172.16.1.2
Netmask: 255.255.255.0
Server: 172.16.10.100
Gateway: 172.16.1.1
Booting: /kick-282 console=ttyS0,9600n8nn quiet loader_ver= "2.1(2)"....
.....................................Image verification OK
Starting kernel...
INIT: version 2.78 booting
Checking all filesystems..... done.
Loading system software
INIT: Sending processes the TERM signal
Sending all processes the TERM signal... done.
Sending all processes the KILL signal... done.
Entering single-user mode...
INIT: Going single user
INIT: Sending processes the TERM signal
switch(boot)#
```

`switch(boot)#` プロンプトは、使用可能なキックスタート イメージがあることを示すものです。

ステップ 4　`switch(boot)#` プロンプトで、**init system** コマンドを発行します。

```
switch(boot)# init system
```

注意　このコマンドを発行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おいてください。

ステップ 5　「switch(boot)# プロンプトからの復旧」（p.2-14）で指示されている手順を実行します。

switch(boot)# プロンプトからの復旧

シングル スーパーバイザ モジュール搭載スイッチで、キックスタート イメージを使用してシステム イメージを復旧する手順は次のとおりです。

ステップ 1　設定モードへ移行し、mgmt0 インターフェイスの IP アドレスを設定します。

```
switch(boot)# config t
switch(boot)(config)# interface mgmt0
```

ステップ 2　**init system** コマンドを入力した場合は、このステップの手順に従います。それ以外の場合は、ステップ 3 に進みます。

a. **ip address** コマンドを入力して、スイッチのローカル IP アドレスおよびサブネット マスクを設定します。

```
switch(boot)(config-mgmt0)# ip address 172.16.1.2 255.255.255.0
```

b. **ip default-gateway** コマンドを入力して、デフォルト ゲートウェイの IP アドレスを設定します。

```
switch(boot)(config-mgmt0)# ip default-gateway 172.16.1.1
```

ステップ 3　**no shutdown** コマンドを入力して、スイッチ上の mgmt0 インターフェイスをイネーブルにします。

```
switch(boot)(config-mgmt0)# no shutdown
```

ステップ 4　**end** と入力して、EXEC モードに移行します。

```
switch(boot)(config-mgmt0)# end
```

ステップ 5　ファイル システムに問題があると考えられる場合は、**init system check-filesystem** コマンドを入力します。このコマンドは、すべての内部ファイル システムを調べて、発見されたエラーをすべて修復します。処理が完了するまで長時間を要します。

```
switch(boot)# init system check-filesytem
```

ステップ 6　目的の TFTP サーバからシステム イメージをコピーします。

```
switch(boot)# copy tftp://172.16.10.100/system-image1 bootflash:system-image1
```

ステップ 7　目的の TFTP サーバからキックスタート イメージをコピーします。

```
switch(boot)# copy tftp://172.16.10.100/kickstart-image1 bootflash:kickstart-image1
```

ステップ 8　システム イメージ ファイルおよびキックスタート イメージ ファイルが bootflash: ファイル システムにコピーされたことを確認します。

```
switch(boot)# dir bootflash:
12456448     Jul 30 23:05:28 1980  kickstart-image1
12288        Jun 23 14:58:44 1980  lost+found/
27602159     Jul 30 23:05:16 1980  system-image1

Usage for bootflash://sup-local
  135404544 bytes used
   49155072 bytes free
  184559616 bytes total
```

ステップ 9　システム イメージを bootflash: ファイル システムからロードします。

```
switch(boot)# load bootflash:system-image1
Uncompressing system image: bootflash:/system-image1
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC

Would you like to enter the initial configuration mode? (yes/no): yes
```

（注）　**no** を入力した場合は、switch# ログイン プロンプトに戻るので、スイッチを手動で設定する必要があります。

デュアル スーパーバイザ モジュール搭載スイッチの復旧

ここでは、デュアル スーパーバイザ モジュール搭載スイッチの 1 つ または両方のスーパーバイザ モジュールでブートフラッシュが破損した場合の復旧手順について説明します。

1 つのスーパーバイザ モジュールでブートフラッシュが破損した場合の復旧

1 つのスーパーバイザ モジュールではブートフラッシュが機能し、またもう 1 つのスーパーバイザ モジュールではブートフラッシュが破損している場合の復旧手順は、次のとおりです。

ステップ 1　機能しているスーパーバイザ モジュールを起動し、スイッチにログインします。

ステップ 2　起動したスーパーバイザ モジュールの `switch#` プロンプトで、**reload module** *slot* **force-dnld** コマンドを発行します。*slot* は、破損したブートフラッシュがあるスーパーバイザ モジュールのスロット番号です。

破損したブートフラッシュがあるスーパーバイザ モジュールでは、ネットブートを実行し、ブートフラッシュの破損をチェックします。起動スクリプトによってブートフラッシュの破損が検出されると、スクリプトは、破損したブートフラッシュを修復する **init system** コマンドを生成します。スーパーバイザ モジュールは、HA Standby 状態で起動します。

注意　システムでアクティブ スーパーバイザ モジュールが正常に稼働している場合は、内蔵 bootflash: が破損するのを防止するために、スタンバイ スーパーバイザ モジュール上で **init system** コマンドを発行する前に、アクティブ スーパーバイザ モジュール上で **system standby manual-boot** コマンドを EXEC モードで発行する必要があります。スタンバイ スーパーバイザ モジュール上で **init system** コマンドが完了したあとは、アクティブ スーパーバイザ モジュール上で **system no standby manual-boot** コマンドを EXEC モードで発行します。

両方のスーパーバイザ モジュールでブートフラッシュが破損した場合の復旧

両方のスーパーバイザ モジュールでブートフラッシュが破損した場合の復旧手順は、次のとおりです。

ステップ 1　両方のスイッチを起動し、BIOS メモリ テストの完了後に **Esc** キーを押して、ブート ローダを中断します。

（注）　次のメッセージが表示されたら、すぐに **Esc** キーを押してください。

```
00000589K Low Memory Passed
00000000K Ext Memory Passed
Hit ^C if you want to run SETUP....
Wait.....
```

待機時間が長くなるようであれば、ブート ローダ フェーズを省略してキックスタート フェーズに入ります。

loader> プロンプトが表示されます。

注意　loader> プロンプトは、通常の switch# プロンプトまたは switch(boot)# プロンプトとは異なります。このプロンプトでは、CLI のコマンド補完機能は機能せず、不要なエラーの原因になることがあります。コマンドは、その全体を正確に入力する必要があります。

ヒント　loader> プロンプトで使用できるコマンドのリストを表示したり、そのリストにある特定のコマンドに関する詳細な情報を取得したりするには、このプロンプトで **help** コマンドを実行してください。

ステップ 2　スイッチのローカル IP アドレスおよびサブネット マスクを指定します。

```
loader> ip address 172.16.1.2 255.255.255.0
Found Intel EtherExpressPro100 82559ER at 0xe800, ROM address 0xc000
Probing...[Intel EtherExpressPro100 82559ER]Ethernet addr: 00:05:30:00:52:27
Address: 172.16.1.2
Netmask: 255.255.255.0
Server: 0.0.0.0
Gateway: 0.0.0.0
```

ステップ 3　デフォルト ゲートウェイの IP アドレスを指定します。

```
loader> ip default-gateway 172.16.1.1
Address: 172.16.1.2
Netmask: 255.255.255.0
Server: 0.0.0.0
Gateway: 172.16.1.1
```

ステップ 4　目的のサーバからキックスタート イメージ ファイルを起動します。

```
loader> boot tftp://172.16.10.100/kickstart-latest
Address: 172.16.1.2
Netmask: 255.255.255.0
Server: 172.16.10.100
Gateway: 172.16.1.1
Booting: /kick-282 console=ttyS0,9600n8nn quiet loader_ver= "2.1(2)"....
.........................................Image verification OK
Starting kernel...
INIT: version 2.78 booting
Checking all filesystems..... done.
Loading system software
INIT: Sending processes the TERM signal
Sending all processes the TERM signal... done.
Sending all processes the KILL signal... done.
Entering single-user mode...
INIT: Going single user
INIT: Sending processes the TERM signal
switch(boot)#
```

switch(boot)# プロンプトは、使用可能なキックスタート イメージがあることを示すものです。

ステップ 5　**init system** コマンドを発行し、ブートフラッシュのパーティションを再作成してフォーマットします。

ステップ 6　「switch(boot)# プロンプトからの復旧」（p.2-14）で指示されている手順を実行します。

ステップ 7　「1 つのスーパーバイザ モジュールでブートフラッシュが破損した場合の復旧」（p.2-16）で指示されている手順を実行して、もう 1 つのスーパーバイザ モジュールを復旧します。

（注）　起動が失敗したときに **reload module** コマンドを発行しなかった場合、失敗後の 3 ～ 6 分以内に、スーパーバイザ モジュールはスタンバイ スーパーバイザ モジュールを自動的にリロードします。

スイッチまたはプロセスのリセット

回復可能または回復不可能なエラーが発生すると、スイッチまたはスイッチ上のプロセスはリセットされることがあります。

現象　スイッチまたはスイッチ上のプロセスがリセットされる。

表 2-4　スイッチまたはプロセスのリセット

問題	考えられる原因	解決方法
スイッチまたはスイッチ上のプロセスがリセットされる。	システムまたはシステム内のプロセスで、回復可能なエラーが発生した。	Cisco NX-OS では、このエラーから自動的に回復します。「回復可能なシステムの再起動」（p.2-19）および「スイッチまたはプロセスのリセット」（p.2-18）を参照してください。
	システム上で回復不可能なエラーが発生した。	Cisco NX-OS では、このエラーから自動的に回復することはできません。原因の判別については、「回復不能なシステムの再起動」（p.2-23）を確認してください。
	クロック モジュールが故障している。	クロック モジュールが故障しているかどうかを確認します。次のメンテナンス ウィンドウ内で、故障したクロック モジュールを交換します。

回復可能なシステムの再起動

プロセスが再起動すると、常に Syslog メッセージおよび 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していない場合でも、以後の再起動によってサービスが中断される可能性があるので、ただちに状態を確認して解決してください。

回復可能なシステムの再起動時には、次の手順で対応してください。

ステップ 1　次のコマンドを入力して Syslog ファイルを調べ、再起動したプロセスとその原因を確認します。

```
switch# show log logfile | include error
```

各メッセージの内容の詳細については、『*Cisco NX-OS Family System Messages Reference*』を参照してください。

次に、システムの出力例を示します。

```
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 o
r not-connected)
Jan 28 00:58:06 88 % LOG_ZONE-2-ZS_MERGE_FAILED: Zone merge failure, Isolating p
ort fc1/1 (VSAN 100)
Jan 28 00:58:44 88 % LOG_ZONE-2-ZS_MERGE_FAILED: Zone merge failure, Isolating p
ort fc1/1 (VSAN 100)
Jan 28 03:26:38 88 % LOG_ZONE-2-ZS_MERGE_FAILED: Zone merge failure, Isolating p
ort fc1/1 (VSAN 100)
Jan 29 19:01:34 88 % LOG_PORT-5-IF_DOWN: Interface fc1/1 is down (Link failure o
r not-connected)
switch#
```

ステップ 2　次のコマンドを入力して、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します。

```
switch# show processes
```

システム出力では、各状態（プロセス状態）が次のコードで示されます。

- 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 = 追跡または停止
- Z = 存在しない（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） ER は通常、再起動回数が多すぎたためにシステムにより障害とみなされ、ディセーブルにされたプロセスの状態です。

次に、システムの出力例を示します（出力は簡略化するために短縮されています）。

```
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
```

ステップ 3　次のコマンドを入力して、異常終了したプロセスを表示し、スタックトレースまたはコア ダンプが実行されているかどうかを確認します。

```
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
```

ステップ 4　次のコマンドを入力して、再起動した特定プロセスの詳細情報を表示します。

```
switch# show processes log pid 898
Service: idehsd
Description: ide hotswap handler Daemon
Started at Mon Sep 16 14:56:04 2002 (390923 us)
Stopped at Thu Sep 19 14:18:42 2002 (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　次のコマンドを入力して、再起動の発生時刻を確認します。

```
switch# show system uptime
Start Time: Fri Sep 13 12:38:39 2002
Up Time:    0 days, 1 hours, 16 minutes, 22 seconds
```

各再起動のタイムスタンプとシステムのアップタイムの長さを比較して、再起動が繰り返し行われているのか、または 1 回限りなのかを判別してください。

ステップ 6　次のコマンドを入力して、コア ファイルを表示します。

```
switch# show cores
Module-num      Process-name      PID    Core-create-time
----------      ------------      ---    ----------------
5               fspf              1524    Jan 9 03:11
6               fcc               919     Jan 9 03:09
8               acltcam           285     Jan 9 03:09
8               fib               283     Jan 9 03:08
```

この出力には、アクティブ スーパーバイザから現在アップロードできるすべてのコアが表示されます。module-num カラムは、コアが生成されたスロットの番号を示しています。前記の例では、スロット 5 のアクティブ スーパーバイザ モジュールで FSPF コアが生成され、スロット 6 のスタンバイ スーパーバイザ モジュールで FCC コアが生成されています。また、スロット 8 のラインカードで、ACLTCAM および FIB を含むコア ダンプが生成されています。

この例の FSPF コア ダンプを IP アドレスが 1.1.1.1 の TFTP サーバにコピーするには、次のコマンドを入力します。

```
switch# copy core://5/1524 tftp::/1.1.1.1/abcd
```

次のコマンドでは、log ディレクトリにある zone_server_log.889 という名前のファイルが表示されます。

```
switch# show pro log pid 1473
====================================================
Service: ips
Description: IPS Manager

Started at Tue Jan  8 17:07:42 1980 (757583 us)
Stopped at Thu Jan 10 06:16:45 1980 (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

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 .
(テキスト出力は省略)
Stack: 128 bytes. ESP 7FFFF830, TOP 7FFFFCD0
```

ステップ 7　次のコマンドを入力し、スイッチから TFTP を使用して、TFTP サーバにコア ダンプを送信します。

system cores tftp:[*//servername*][*/path*]

このコマンドにより、スイッチに TFTP サーバへのコア ファイルの自動コピーが設定されます。たとえば、IP アドレスが 10.1.1.1 の TFTP サーバにコア ファイルを送信するには、次のコマンドを使用します。

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

次の条件が適用されます。

- コア ファイルは 4 分ごとにコピーされます。この間隔は変更できません。
- TFTP サーバへの特定のコア ファイルのコピーは手動でトリガーすることが可能です。次のコマンドを使用します。**copy core://***module#/pid#* **tftp://***tftp_ip_address/file_name*
- プロセス再起動回数の最大値は、プロセスの HA ポリシーに含まれています（このパラメータは変更できません）。プロセスが最大値を超えて再起動されると、古いコア ファイルが上書きされます。
- プロセスで保存可能な最大コア ファイル数は、プロセスの HA ポリシーに含まれています（このパラメータは変更できず、3 に設定されています）。

ステップ 8　カスタマー サポート 担当者に連絡してコア ダンプの検査を依頼し、再起動の原因と解決方法を判別します。

回復不能なシステムの再起動

回復不能なシステムの再起動は、次の条件で発生することがあります。

- 重要なプロセスが失敗したために、再起動ができない場合
- プロセス再起動がシステム設定で許可されているよりも多く行われている場合
- プロセス再起動の回数がシステム設定の最大値を超えている場合

プロセス再起動の影響は、各プロセスに設定されたポリシーによって異なります。回復不能な再起動は、機能の喪失、アクティブ スーパーバイザの再起動、スーパーバイザのスイッチオーバー、またはスイッチの再起動の原因になります。

回復不能な再起動への対応については、「Cisco NX-OS ソフトウェア システム再起動のトラブルシューティング」（p.2-9）を参照してください。

show system reset-reason CLI コマンドを使用すると、次の情報が表示されます。

- スーパーバイザ モジュールに対して直近の 4 つのリセット原因コードが表示されます。いずれかのスロットにスーパーバイザ モジュールが装着されていない場合は、そのモジュールに対応するリセット原因コードは表示されません。
- **show system reset-reason module** *number* コマンドを使用すると、指定したスロットにある特定のモジュールに対して、直近の 4 つのリセット原因コードが表示されます。スロットにスーパーバイザ モジュールが装着されていない場合、モジュールのリセット原因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されないリロードが発生した時期と理由の履歴をすべて検索します。
- 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が表示されます。
- モジュールのリセットまたはリロードの理由が表示されます。
- リセットまたはリロードの原因になったサービスが表示されます（表示されない場合もあります）。
- リセットまたはリロードが発生したときに稼働していたソフトウェアのバージョンが表示されます。

例 2-2　show system reason-reset コマンドの出力

```
switch# show system reset-reason module 5
----- reset reason for module 5 -----
1) At 224801 usecs after Fri Jan 21 16:36:40 2005
Reason: Reset Requested by CLI command reload
Service:
Version: 2.1(2)
2) At 922828 usecs after Fri Jan 21 16:02:48 2005
Reason: Reset Requested by CLI command reload
Service:
Version: 2.1(2)
3) At 318034 usecs after Fri Jan 21 14:03:36 2005
Reason: Reset Requested by CLI command reload
Service:
Version:2.1(2)
4) At 255842 usecs after Wed Jan 19 00:07:49 2005
Reason: Reset Requested by CLI command reload
Service:
Version: 2.1(2)
```

管理パスワードの回復

管理パスワードを忘れてしまった場合は、表 2-5 の説明に従ってスイッチにアクセスすることができます。

現象　スイッチにアクセスするための管理パスワードを忘れた。

表 2-5　管理者パスワードの回復

問題	解決方法
Cisco NX-OS にアクセスするための管理パスワードを忘れた。	パスワードは、ローカル コンソール接続を使用して回復できます。 詳細については、次の URL を参照してください。 http://www.cisco.com/en/US/products/hw/ps4159/ps4358/prod_password_recoveries_list.html

CHAPTER 3

ライセンスのトラブルシューティング

Cisco NX-OS では、ライセンス機能を使用することができます。このメカニズムでは、デバイスの特定のプレミアム機能に対応するライセンスをインストールすると、その機能へのアクセスが可能になります。

この章では、次の内容について説明します。

ライセンスの概要

Cisco NX-OS では、Enterprise および Advanced の機能を利用するためのライセンスが必要です。ライセンスをインストールすると、スイッチ上でこれらの機能を利用できるようになります。ライセンス付与された機能を有効にするスイッチごとに、1 ライセンスを購入する必要があります。

（注） Cisco NX-OS では、ライセンスをインストールしなくても、機能を有効にできます。猶予期間中は、ライセンスを購入せずに試用することができます。

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発注した場合、そのライセンスは他のスイッチでは使用できません。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ます。

エラー メッセージ　LICMGR-3-LOG_LIC_INVALID_HOSTID: Invalid license hostid VDH=[chars] for feature [chars].

説明　この機能には、無効なライセンス ホスト ID を持ったライセンスがあります。この状況は、特定のスイッチ用のライセンス機能を含むスーパーバイザ モジュールを、別のスイッチに取り付けた場合に発生することがあります。

推奨処置　スーパーバイザが取り付けられているシャーシ用の正しいライセンスを再インストールします。

猶予期間

ライセンスの必要な機能を、ライセンスをインストールせずに使用している場合は、機能を評価するための 120 日の猶予期間が付与されます。猶予期間が終了する前、または猶予期間の終了時に Cisco NX-OS によって機能がディセーブルにされる前に、必要な数のライセンスを購入およびインストールする必要があります。ライセンス付与されていない機能を使用しようとすると、次のシステム メッセージが表示されます。

エラー メッセージ　LICMGR-2-LOG_LIC_GRACE_EXPIRED: Grace period expired for feature [chars].

説明　ライセンスのない機能の猶予期間が過ぎました。この機能を使用しているアプリケーションは、ただちにシャットダウンされます。

推奨処置　機能を引き続き使用する場合は、ライセンス ファイルをインストールしてください。

エラー メッセージ　LICMGR-3-LOG_LICAPP_NO_LIC: Application [chars] running without [chars] license, shutdown in [dec] days.

説明　アプリケーション［chars1］には、ライセンスがありません。アプリケーションは猶予期間の［dec］日間は動作しますが、機能のライセンス ファイルをインストールしないかぎり、その日数を過ぎるとシャットダウンされます。

推奨処置　機能を引き続き使用する場合は、ライセンスをインストールしてください。

エラー メッセージ　LICMGR-3-LOG_LIC_LICENSE_EXPIRED: Evaluation license expired for feature [chars].

説明　機能の評価期間が過ぎました。猶予期間が過ぎると、機能はシャットダウンされます。

推奨処置　機能を引き続き使用する場合は、ライセンスをインストールしてください。

エラー メッセージ　LICMGR-3-LOG_LIC_NO_LIC: No license(s) present for feature [chars]. Application(s) shutdown in [dec] days.

説明　機能にはライセンスがありません。この機能は猶予期間中は有効ですが、その日数が過ぎると、この機能を使用するアプリケーションはシャットダウンされます。

推奨処置　機能を引き続き使用する場合は、ライセンスをインストールしてください。

エラー メッセージ　LICMGR-6-LOG_LICAPP_EXPIRY_WARNING: Application [chars] evaluation license [chars] expiry in [dec] days.

説明　表示されている評価期間の日数が過ぎた場合、機能の永久ライセンスをインストールしない限り、アプリケーションはシャットダウンされます。

推奨処置　機能を引き続き使用する場合は、ライセンス ファイルをインストールしてください。

ライセンス パッケージには、複数の機能が含まれる場合があります。猶予期間中にライセンス パッケージ内の 1 つの機能をディセーブルにしても、その他の機能はイネーブルのままなので、そのライセンス パッケージに対するカウントダウンのクロックは停止しません。ライセンス機能の猶予期間のカウントダウンを中断するには、そのライセンス パッケージに含まれる機能をすべてディセーブルにする必要があります。ライセンス パッケージに含まれる機能でイネーブルになっているものを判別するには、**show license usage** CLI コマンドを使用します。

ガイドライン

ここでは、Cisco NX-OS のライセンスを管理する際のガイドラインを示します。

- 猶予期間の期限切れ警告を無視しないでください。猶予期間の期限が切れるまでの 60 日の間に新しいライセンスの発注、配送、およびインストールを行うことができます。
- ライセンスを必要とする機能を確認し、購入する必要のあるライセンスを慎重に決定してください。
- ライセンスの発注は、次の手順で正確に行ってください。
  - スイッチに付属の Proof of Purchase 文書（購入証明書）に記載されている Product Authorization Key（PAK）を入力します。
  - ライセンスを発注する際は、正しいシャーシ シリアル番号を入力します。このシリアル番号は、ライセンスのインストール先になるシャーシのシリアル番号でなければなりません。**show license host-id** CLI コマンドを使用します。
  - シリアル番号を正確に入力します。シリアル番号に数字のゼロは含まれますが、文字の「O」が含まれることはありません。
  - 使用するシャーシに合ったライセンスを発注します。
- ライセンス ファイルを、遠隔の安全な場所にバックアップしてください。ライセンス ファイルをアーカイブしておけば、スイッチの障害によるライセンス ファイルの消失を防止できます。
- スイッチのシリアル番号に基づいて発注されたライセンスを使用して、各スイッチに正しいライセンスをインストールしてください。ライセンスには、シリアル番号に基づくものと、プラットフォームのタイプに基づくものの 2 種類があります。
- **show license usage** CLI コマンドを使用して、ライセンスがインストールされたことを確認します。
- ライセンス ファイルは絶対に変更しないでください。また、ライセンスの発注対象ではないスイッチには使用しないでください。シャーシの RMA を行う場合は、テクニカル サポート担当者に連絡して新しいシャーシ用の交換ライセンスを発注してください。

トラブルシューティングの初期チェックリスト

ライセンスに関する問題のトラブルシューティングを開始するときは、最初に、次の事項について確認します。

チェックリスト	確認済み
発注したすべてのライセンスで、対応するシャーシ シリアル番号を確認します。	❑
発注したすべてのライセンスで、対応するプラットフォームまたはモジュールのタイプを確認します。	❑
ライセンスの発注に使用した PAK が、シャーシ シリアル番号の取得元のシャーシに付属している PAK と同じものであることを確認します。	❑
機能をイネーブルにするためのライセンスを必要としているすべてのスイッチに、すべてのライセンスがインストールされたことを確認します。	❑

CLI によるライセンス情報の表示

show license コマンドを使用すると、スイッチに設定されているすべてのライセンスの情報を表示できます（例 3-1 ～ 例 3-3 を参照）。

例 3-1　現在のライセンス使用状況に関する情報を表示

```
switch(config)# show license usage
Feature                      Ins  Lic   Status Expiry Date Comments
                                Count
--------------------------------------------------------------------------------
LAN_ADVANCED_SERVICES_PKG     No    -   In use             Grace 102D 0H
LAN_ENTERPRISE_SERVICES_PKG   No    -   In use             Grace 103D 22H
--------------------------------------------------------------------------------
----
```

例 3-2　特定のパッケージに含まれる機能のリストを表示

```
switch(config)# show license usage LAN_ENTERPRISE_SERVICES_PKG
Application
-----------
pbr
Tunnel
-----------
```

例 3-3　ライセンスのホスト ID を表示

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

（注） コロン（:）記号のあとに表示される ID の全体を使用してください。VHD は Vendor Host ID です。

例 3-4　インストールされたライセンス キー ファイルとその内容をすべて表示

```
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>N7K-LAN1K9=</SKU> \
        HOSTID=VDH=TBC10412106 \
        NOTICE="<LicFileID>20071025133322456</LicFileID><LicLineID>1</LicLineID>
 \
```

ライセンスのインストールに関する問題

通常、ライセンスの一般的な問題は、ライセンス ファイルの誤発注、不正なスイッチへのライセンス ファイルのインストール、またはファブリック用のライセンスの数に関係した誤発注が原因で発生します。

ここで説明する内容は、次のとおりです。

シリアル番号の問題

ライセンスに関する一般的な問題のいくつかは、ライセンスの発注時に間違ったシャーシ シリアル番号を使用したことが原因になっています。

CLI で **show license host-id** CLI コマンドを使用して、スイッチの正しいシャーシ シリアル番号を取得します。

ライセンスの発注処理中にシャーシ シリアル番号を入力する際は、シリアル番号に含まれるゼロの代わりに文字の「O」を使用しないように注意してください。

RMA シャーシ エラーまたはスイッチ間におけるライセンスの移動

ライセンスは発行されたスイッチに対して固有のものであり、その他のスイッチでは無効です。ライセンスをスイッチ間で移動する場合は、購入した代理店にお問い合わせください。

ライセンスのインストール後も猶予期間警告が発生

ライセンスが正しくインストールされていない場合、またはまだインストールしていないライセンス パッケージに含まれる機能を使用している場合は、猶予期間警告を引き続き受け取ることになります。

現象　ライセンスのインストール後も猶予期間警告が発生する。

表 3-1　ライセンスのインストール後も猶予期間警告が発生

現象	考えられる原因	解決方法
ライセンスのインストール後も猶予期間警告が発生する。	ライセンス ファイルはコピーされているが、インストールされていない。	**license install** CLI コマンドを使用して、ライセンスをインストールします。
	ライセンスのインストールが失敗した。	ログを参照して、失敗したライセンスのインストールに関するシステム メッセージを調べます。**show license usage** CLI コマンドを使用して、ライセンスなしで使用されている機能を判別します。

猶予期間中のアラート

Cisco NX-OS では、120 日間の猶予期間が与えられます。まだライセンスをインストールしていない機能を評価するときに、この猶予期間のカウントダウンが開始または継続されます。

評価中の機能をディセーブルにすると猶予期間のカウントダウンは中断しますが、有効なライセンスなしでその機能を再びイネーブルにすると、残りの猶予期間に対するカウントダウンが継続されます。

ライセンス パッケージに含まれるすべての機能が、この猶予期間の対象になります。ライセンス パッケージには、複数の機能が含まれる場合があります。猶予期間中にライセンス パッケージ内の 1 つの機能をディセーブルにしても、その他の機能はイネーブルのままなので、そのライセンス パッケージに対するカウントダウンは停止しません。ライセンス パッケージの猶予期間のカウントダウンを中断するには、ライセンス パッケージ内のすべての機能をディセーブルにする必要があります。

スイッチ上のすべてのライセンスは、Cisco NX-OS ライセンス カウンタによって追跡されます。機能の評価および猶予期間が開始されると、コンソール メッセージ、SNMP（簡易ネットワーク管理プロトコル）トラップ、システム メッセージ、および Call Home メッセージを毎日受け取ります。

さらに、猶予期間の最後の 7 日間は、これらのメッセージの頻度が 1 時間ごとになります。次の例では、VDC 機能を使用します。1 月 30 日に、120 日の猶予期間を使用して VDC 機能をイネーブルにしました。この場合、猶予期間の終了まで、次のようにメッセージを受け取ります。

- 1 月 30 日～ 5 月 21 日まで、毎日メッセージを受け取ります。
- 5 月 22 日～ 30 日まで、1 時間ごとにメッセージを受け取ります。

5 月 31 日に猶予期間が終了し、VDC 機能は自動的にディセーブルにされます。有効なライセンスを購入するまで、複数の VDC の使用は許可されません。

（注） 猶予期間中のメッセージの頻度は変更できません。

注意 猶予期間の最後の 7 日間が過ぎると機能が停止し、ネットワーク トラフィックが中断する場合があります。今後のアップグレードでは、ライセンス要求および 120 日間の猶予期間を実施します。

show license usage コマンドを使用して、スイッチの猶予期間情報を表示します。

```
switch(config)# show license usage
Feature                      Ins  Lic   Status Expiry Date Comments
                                Count
--------------------------------------------------------------------------------
LAN_ADVANCED_SERVICES_PKG     No    -   In use             Grace 102D 0H
LAN_ENTERPRISE_SERVICES_PKG   No    -   In use             Grace 103D 22H
--------------------------------------------------------------------------------
----
```

ライセンスが存在しないと表示される

ライセンスが正しくインストールされて機能している場合でも、システム ハードウェアの変更または bootflash: に関する問題の発生が原因で、ライセンスが存在しないと表示されることがあります。

現象　ライセンスが存在しないと表示される。

表 3-2　ライセンスが存在しないと表示される

現象	考えられる原因	解決方法
ライセンスが存在しないと表示される。	ライセンスのインストール後に、スーパーバイザ モジュールが交換された。	ライセンスを再インストールします。
	スーパーバイザの bootflash: が破損している。	破損した bootflash: の復旧については、「破損したブートフラッシュの復旧」（p.2-10）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。

CHAPTER 4

VDC のトラブルシューティング

この章では、Virtual Device Context（VDC; 仮想デバイス コンテキスト）のトラブルシューティング方法について説明します。

この章で説明する内容は、次のとおりです。

VDC のトラブルシューティングについて

Cisco NX-OS では、物理的な NX-OS デバイスを複数の仮想デバイスに分割する場合に使用する VDC がサポートされています。接続ユーザは、各 VDC を 1 つのデバイスのように扱うことができます。VDC は、物理的な NX-OS デバイス内の独立した論理エンティティとして実行され、独自のソフトウェア プロセス セットを実行し、独自の構成を備え、個別の管理者による管理が可能です。

VDC の問題は、VDC の管理とは直接関連していない場合があります。問題に応じたトラブルシューティングの説明を読み、VDC に関連する他の問題を見つけてください。たとえば、VDC テンプレートを設定して特定の VDC のポート チャネル数を制限した場合、この VDC テンプレートに設定された制限を超えるポート チャネルを作成しようとすると問題が発生します。

VDC テンプレートでは、次の機能の制限を設定します。

- ポート チャネル
- SPAN セッション
- IPv4 ルート マップ メモリ
- VLAN
- Virtual routing and forwarding（VRF; 仮想ルーティングおよびフォワーディング）インスタンス

最小リソース値は、その機能で保証されるリソースの下限を設定します。最大リソース値は、その機能で上限となるリソース量を示し、先着順での利用が可能です。

（注） VDC にインターフェイスを割り当てると、Cisco NX-OS はそのインターフェイスのすべての設定を削除します。

VDC の詳細、またはこの章で推奨する VDC 設定変更の詳細については、『*Cisco NX-OS Virtual Device Context Configuration Guide, Release 4.0*』を参照してください。

トラブルシューティングの初期チェックリスト

VDC に関する問題のトラブルシューティングを開始する際には、まず、次の事項について確認します。

チェックリスト	確認済み
VDC を作成または修正する場合は、network-admin としてデバイスにログインしていることを確認します。	❑
正しい VDC に位置していることを確認します。VDC を設定するには、デフォルト VDC に位置する必要があります。	❑
VDC を設定するために、Advanced Services ライセンスをインストール済みであることを確認します。	❑
作成しようとしている VDC の数が 3 つを超えていないことを確認します。	❑

次のコマンドを使用して、VDC 情報を表示します。

- **show vdc membership**
- **show vdc resource**

VDC の問題

VDC の問題は通常、正しくない VDC へのログインまたは VDC への不適切なリソースの割り当てが原因で発生します。

ここで説明する内容は、次のとおりです。

VDC を作成できない

VDC 作成に関連する問題が発生すると、次のいずれかのシステム メッセージが表示されます。

エラー メッセージ　`VDC_MGR-2-VDC_BAD: vdc_mgr: There has been a failure at res_mgr`

説明　テンプレートに設定されたリソースが不足しています。テンプレートが使用されていないときは、デフォルト テンプレートが適用されます。

推奨処置　**show vdc resources** [**detail**] または **show vdc resource template** CLI コマンドを使用して、この VDC の作成に必要なリソースが十分であることを確認します。この VDC の作成に使用するテンプレートを修正するか、現在利用可能なリソースを下限として新しいテンプレートを作成します。

エラー メッセージ　`VDC_MGR-2-VDC_BAD: vdc_mgr: : There has been a failure at sys_mgr`

説明　リソース テンプレートを使用して予約できるリソース以外のシステム リソースが不足しているため、サービスのクラッシュまたは障害が発生しました。これらのリソースは、システム使用率に基づくダイナミック リソースであるため、新しい VDC のサポートには使用できない可能性があります。

推奨処置　**show system internal sysmgr service running** CLI コマンドを使用して、障害の原因を判別します。

表 4-1 に、考えられる原因および解決方法を示します。

現象　VDC を作成できない。

表 4-1　VDC を作成できない

現象	考えられる原因	解決方法
VDC を作成できない。	network-admin としてログインしていない。	ネットワーク管理者権限を持つアカウントでデバイスにログインします。
	デフォルト VDC にログインしていない。	**switchto** CLI コマンドを使用してデフォルト VDC に移動して、リソース割り当てを行います。
	リソースが不足している。	**show vdc resources** [**detail**] または **show vdc resource template** CLI コマンドを使用して、利用可能なリソースを確認します。VDC 設定モードで **limit-resource** CLI コマンドを使用して、テンプレートを修正するか、少ないリソースを使用する VDC を作成します。

デバイスにログインできない

デバイスにログインするときに、問題が発生することがあります。表 4-2 に、考えられる原因および解決方法を示します。

現象　デバイスにログインできない。

表 4-2　デバイスにログインできない

現象	考えられる原因	解決方法
デバイスにログインできない。	VDC のアカウント情報が存在しない。	ネットワーク管理者としてデバイスにログインし、**switchto** CLI コマンドを使用して当該の VDC に移動してから、この VDC のパスワードおよびネットワーク接続を設定します。
	正しくない VDC ユーザ名を使用している。	この VDC 用に作成されたアカウントでデバイスにログインします。

VDC に移動できない

他の VDC に移動するときに、問題が発生することがあります。表 4-3 に、考えられる原因および解決方法を示します。

現象　VDC に移動できない。

表 4-3　VDC に移動できない

現象	考えられる原因	解決方法
VDC に移動できない。	ネットワーク管理者またはネットワーク オペレータとしてログインしていない。	適切な権限を持つアカウントでデバイスにログインします。

VDC を削除できない

VDC 削除に関連する問題が発生すると、次のいずれかのシステム メッセージが表示されます。

エラー メッセージ　`VDC_MGR-2-VDC_UNGRACEFUL: vdc_mgr: Ungraceful cleanup request received for vdc [dec], restart count for this vdc is [dec]`

説明　Vdc_mgr が VDC のアングレースフル クリーンアップを開始しました。

推奨処置　対処不要です。

エラー メッセージ　`VDC_MGR-2-VDC_OFFLINE: vdc [dec] is now offline`

説明　Vdc_mgr が VDC の削除を終了しました。

推奨処置　対処不要です。

表 4-4 に、考えられる原因および解決方法を示します。

現象　VDC を削除できない。

表 4-4　VDC を削除できない

現象	考えられる原因	解決方法
VDC を削除できない。	デフォルト VDC を削除しようとした。	デフォルト VDC は削除できません。
	VDC の削除中に、不明のエラーが発生した。	**show tech-support VDC** CLI コマンドを使用して、詳細を収集します。

VDC にインターフェイスを割り当てられない

VDC 作成に関連する問題が発生すると、次のシステム メッセージが表示されます。

エラー メッセージ　`VDC_MGR-2-VDC_BAD: vdc_mgr: There has been a failure at gim (port_affected_list).`

説明　インターフェイスの割り当てに失敗しました。

推奨処置　**show vdc membership status** または **show interface brief** CLI コマンドを使用して、詳しい情報を収集します。

表 4-5 に、考えられる原因および解決方法を示します。

現象　VDC にインターフェイスを割り当てられない。

表 4-5　VDC にインターフェイスを割り当てられない

現象	考えられる原因	解決方法
VDC にインターフェイスを割り当てられない。	ネットワーク管理者としてログインしていない。	適切な権限を持つアカウントでデバイスにログインします。
	正しい VDC にログインしていない。	リソース割り当てを行うために、**switchto** CLI コマンドを使用してデフォルト VDC に移動します。
	インターフェイスが専用ポート グループの一部である。	**show interface capabilities** CLI コマンドを使用して、ポートが専用グループの一部かどうかを調べます。専用ポート グループのすべてのポートは、同じ VDC に割り当てる必要があります。
	Cisco Nexus 7000 シリーズ 32 ポート 10 Gbps イーサネット モジュール（N7K-M132XP-12）上のインターフェイスである。	このモジュールでは、1 つのポートグループに含まれるすべてのポートを同じ VDC に割り当てる必要があります。ポート番号とポート グループのマッピングについては、表 4-6 を参照してください。
	VDC の割り当てに失敗した。	**show vdc membership** [**status**] または **show interface brief** CLI コマンドを使用して、詳しい情報を収集します。

表 4-6 に、Cisco Nexus 7000 シリーズ 32 ポート 10 Gbps イーサネット モジュール（N7K-M132XP-12）のポート割り当ての要件を示します。

表 4-6　Cisco Nexus 7000 シリーズ 32 ポート 10 Gbps イーサネット モジュールのポート番号

ポート グループ	ポート番号
1	1、3、5、7
2	2、4、6、8
3	9、11、13、15
4	10、12、14、16
5	17、19、21、23
6	18、20、22、24
7	25、27、29、31
8	26、28、30、32

VDC にリソース テンプレートの変更が反映されない

リソース テンプレートを更新するときに、問題が発生することがあります。表 4-7 に、考えられる原因および解決方法を示します。

現象　VDC にリソース テンプレートの変更が反映されない。

表 4-7　VDC にリソース テンプレートの変更が反映されない

現象	考えられる原因	解決方法
VDC にリソース テンプレートの変更が反映されない。	テンプレート変更後に、テンプレートが VDC に再度適用されていない。	**show vdc resource template** CLI コマンドを使用して、テンプレートを確認します。**template** CLI コマンドを使用して、テンプレートを VDC に再度適用します。新しいリソース制限を有効にするには、**reload** CLI コマンドを使用してデバイスを再起動するか、ステートフル スイッチオーバーを実行する必要があります。

VDC が障害状態のままである

VDC に障害が発生したときに、問題が発生することがあります。VDC の作成時に、VDC のスイッチオーバー ポリシーおよび High Availability（HA）ポリシーを設定します。これのポリシーによって、VDC の障害発生時、またはスタンバイ スーパーバイザへのステートフル スイッチオーバーの発生時の動作が決定します。

表 4-8 に、考えられる原因および解決方法を示します。

現象　VDC が障害状態のままである。

表 4-8　VDC が障害状態のままである

現象	考えられる原因	解決方法
VDC が障害状態のままである。	VDC に障害が発生し、この VDC の HA ポリシーが bring down に設定されている。	**show vdc detail** CLI コマンドを使用して、この VDC の HA ポリシーを確認します。VDC 設定モードで **ha-policy** CLI コマンドを使用して、HA ポリシーを変更します。
	スーパーバイザ スイッチオーバが発生し、この VDC のスイッチオーバ ポリシーが bring down に設定されている。	**no vdc** コマンドを使用して、障害が発生した VDC を削除します。VDC を再度作成し、**sw-policy** キーワードを使用して異なるスイッチオーバ ポリシーを設定します。

VDC のスタートアップ コンフィギュレーションに実行コンフィギュレーションをコピーできない

VDC にコンフィギュレーションを保存しようとするときに、問題が発生することがあります。表 4-9 に、考えられる原因および解決方法を示します。

現象　VDC のスタートアップ コンフィギュレーションに実行コンフィギュレーションをコピーできない。

表 4-9　VDC のスタートアップ コンフィギュレーションに実行コンフィギュレーションをコピーできない

現象	考えられる原因	解決方法
VDC のスタートアップ コンフィギュレーションに実行コンフィギュレーションをコピーできない。	デフォルト VDC にリソース割り当てが保存されていない。	デフォルト以外の VDC にコンフィギュレーションを保存する前に、デフォルト VDC にリソース割り当てを保存する必要があります。デフォルト VDC にログインし、**copy running-config startup-config** CLI コマンドを使用してリソース割り当てを保存します。デフォルト以外の VDC にログインしてコンフィギュレーションを保存するか、デフォルト VDC で **copy running-config startup-config vdc-all** CLI コマンドを使用してすべての VDC にコンフィギュレーションを保存します。

CHAPTER 5

ポートのトラブルシューティング

この章では、Cisco NX-OS のポートで発生する可能性のある問題を識別して解決する方法について説明します。具体的な内容は、次のとおりです。

ポートのトラブルシューティングについて

スイッチで 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。設定するインターフェイスは、イーサネット インターフェイス、管理インターフェイス（mgmt0）、または VLAN インターフェイス（SVI）になります。

各インターフェイスには、次のような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、修正を加えないかぎり変更されません。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。
- 動作ステータスでは、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。このステータスは読み取り専用なので、変更することはできません。インターフェイスがダウンしているときは、値の一部が有効にならない場合があります（動作速度など）。

ポート モード、管理ステート、および動作ステートの詳細については、『*Cisco NX-OS Interfaces Configuration Guide, Release 4.0*』を参照してください。

ポートのガイドライン

ポート インターフェイスを設定する際は、次のガイドラインに従ってください。

- スイッチの設定を開始する前に、シャーシ内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。設定を続行する前に、**show module** CLI コマンドを使用して、モジュールが OK またはアクティブであることを確認してください。
- ポート グループに含まれる専用ポートを設定する際には、次のポート モードのガイドラインに従ってください。
  - 専用モードでは、4 ポートで構成される各グループの 1 つのポートのみを設定できます。他の 3 つのポートは使用不能になり、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、専用モードではもう 1 つのポートを設定することはできません。他の 3 つのポートは、引き続きイネーブルのままになります。

ライセンスの要件

Cisco NX-OS でのポートの設定には、ライセンスは必要ありません。

トラブルシューティングの初期チェックリスト

ポート設定に関するトラブルシューティングを開始するときは、次の事項について確認します。

チェックリスト	確認済み
物理メディアを点検して、損傷部分がないことをチェックします。	❑
使用中の Small Form Factor Pluggable（SFP; 着脱可能小型フォーム ファクタ）デバイスが、シスコによって認定されているデバイスであり、故障していないことを確認します。	❑
no shutdown CLI コマンドを使用して、ポートをイネーブルにしたことを確認します。	❑
show interface CLI コマンドを使用して、インターフェイスのステートを確認します。ポートの動作ステートが down になる原因については、『*Cisco Cisco NX-OS Interfaces Configuration Guide, Release 4.0*』を参照してください。	❑
1 つのポートを専用ポートとして設定したこと、およびポート 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 コマンドを使用すると、ポート カウンタを表示できます。通常、カウンタは、トラブルシューティングを行っているときにしか確認しませんが、事前にカウンタをクリアして、基準を設定することが必要です。特定のカウンタで大きな値が出た場合でも、長時間アクティブになっているポートでは意味を持たないことがあります。カウンタをクリアしておくと、トラブルシューティングを行うリンクの動作について、より正確な情報を得ることができます。

次のいずれかのコマンドを使用して、すべてのポート カウンタまたは指定されたインターフェイスのカウンタをクリアします。

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

カウンタを使用すると、表示される受信フレーム数と送信フレーム数の差が非常に大きい場合は、同期の問題があることを識別できます。

次のコマンドを使用して、ポートに関する詳細を収集します。

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

CLI によるポート ステート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。ポートのステートに加えて、このコマンドでは次の情報も表示されます。

- 速度
- 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、および不正なフレームなど）

例 5-1 に、**show interface** コマンドの出力例を示します。

例 5-1　show interface コマンドの出力

```
switch(config)# 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

ここで説明する内容は、次のとおりです。

インターフェイスを確認できない

VDD 設定が原因でデバイス上にインターフェイスを確認できない場合、問題が発生していることがあります。表 5-1 に、考えられる原因および解決方法を示します。

現象　インターフェイスを確認できない。

表 5-1　インターフェイスを確認できない

現象	考えられる原因	解決方法
インターフェイスを確認できない。	インターフェイスが別の VDC に割り当てられている。	network admin としてログインし、**show vdc membership** CLI コマンドを使用してインターフェイスが属している VDC を調べます。

インターフェイス設定が消えた

インターフェイス設定が消えた場合、問題が発生していることがあります。

表 5-2 に、考えられる原因および解決方法を示します。

現象　インターフェイス設定が消えた。

表 5-2　インターフェイス設定が消えた

現象	考えられる原因	解決方法
インターフェイス設定が消えた。	インターフェイスが別の VDC に再割り当てされた。	Cisco NX-OS では、インターフェイスが別の VDC に再割り当てられると、インターフェイス設定が削除されます。インターフェイスを再度設定する必要があります。
	インターフェイス モードがスイッチポート モードに、またはスイッチポート モードから切り替えられた。	Cisco NX-OS では、レイヤ 2 および レイヤ 3 ポート モード間の切り替えを行うと、インターフェイス設定が削除されます。インターフェイスを再度設定する必要があります。

インターフェイスをイネーブルにできない

インターフェイスをイネーブルにするときに、問題が発生することがあります。

表 5-3 に、考えられる原因および解決方法を示します。

現象　インターフェイスをイネーブルにできない。

表 5-3　インターフェイスをイネーブルにできない

現象	考えられる原因	解決方法
インターフェイスをイネーブルにできない。	インターフェイスが専用ポート グループの一部である。	ポート グループの 1 つのポートを専用ポートとしている場合、他の 3 つのポートはイネーブルにできません。**show running-config interface** 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がリモートポートと異なる。	両方のポートで **show interface capabilities** CLI コマンドを使用し、両方のポートが同じ機能を持っているかどうかを調べます。必要に応じて設定を変更し、両ポートの設定を同じにします。
	レイヤ 2 ポートが 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る。	**show interface brief** CLI コマンドを使用して、インターフェイスが VLAN 内に設定さているかどうかを調べます。**show vlan brief** CLI コマンドを使用して、VLAN のステータスを調べます。VLAN 設定モードで **state active** CLI コマンドを使用し、VLAN のステートをアクティブに設定します。
	正しくない SFP がポートに接続された。	**show interface brief** CLI コマンドを使用して、正しくないトランシーバを使用しているかどうかを調べます。シスコがサポートする SFP を使用します。

専用ポートを設定できない

ポートを専用ポートとして設定しようとするときに、問題が発生することがあります。

表 5-4 に、考えられる原因および解決方法を示します。

現象　専用ポートを設定できない。

表 5-4　専用ポートを設定できない

現象	考えられる原因	解決方法
専用ポートを設定できない。	ポート グループの他の 3 つのポートがシャットダウンされていない。	インターフェイス設定モードで **shutdown** CLI コマンドを使用して、ポート グループ内の他の 3 つのポートをディセーブルにします。
	ポート グループ内の他の 3 つのポートのうち 1 つまたは 2 つのポートが、同一の VDC 内に設定されていない。	**show vdc membership** CLI コマンドを使用して、異なる VDC 内に設定されているポートを見つけます。
	ポートがポート グループの最初のポートではない。	専用モードには、ポート グループの最初のポートのみを設定できます。

ポートが Link failure or not-connected ステートのままになる

ポートまたはリンクが動作を開始するときに、問題が発生することがあります。

表 5-5 に、考えられる原因および解決方法を示します。

現象　ポートが Link failure ステートのままになる。

表 5-5　ポートが Link-failure ステートのままになる

現象	考えられる原因	解決方法
ポートが Link failure ステートのままになる。	ポート接続が不良である。	**show port internal info** CLI コマンドを使用して、ポートのステータスが Link- failure になっていることを確認します。 使用しているメディアのタイプを確認します。銅線または光ファイバ、シングルモード（SM）またはマルチモード（MM）のいずれかです。 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。スイッチ上の LED がグリーンになっていることを確認します。 **shut** CLI コマンドの後に **no shut** コマンドを使用して、ポートをいったんディセーブルにしてからイネーブルにします。これで問題が解決しない場合は、接続を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移動してください。
	Small Form-Factor Pluggable（SFP）での中継障害または SFP の故障が原因で信号がない。	この問題が発生すると、ポートは中継ポート状態のままになり、信号は確認できません。また、MAC レベルでの同期も存在しません。この問題には、ポートの速度設定または自動ネゴシエーションが関係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てください。SFP を正しく取り付けても問題が解決しない場合には、SFP を交換するか、スイッチの他のポートを試してみてください。
	リンクが初期化状態で停止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** CLI コマンドを使用して、「**Link Failure, Not Connected system**」メッセージを確認します。 **shut** CLI コマンドの後に **no shut** コマンドを使用して、ポートをいったんディセーブルにしてからイネーブルにします。これで問題が解決しない場合は、接続を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移動してください。

予期しないリンク フラップの発生

ポートでフラップが発生している場合、次の順番でステートの変化が周期的に繰り返されます。

1. Initializing — リンクが初期化される。
2. Offline — ポートがオフラインになる。
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ない。

予期しないリンクフラップのトラブルシューティングでは、次の情報を把握する必要があります。

- リンク フラップを開始した管理者
- リンク ダウンの実際の原因

表 5-6 に、考えられる原因および解決方法を示します。

現象　予期しないリンク フラップが発生する。

表 5-6　予期しないリンク フラップの発生

現象	考えられる原因	解決方法
予期しないリンク フラップが発生する。	ビット レートがしきい値を超えたために、ポートが errDisabled ステートになっている。	**shutdown** CLI コマンドの後に **no shutdown** コマンドを使用して、ポートを通常の状態に戻します。
	システムの問題によって、エンド デバイスによりリンク フラップの動作が開始される。原因の一部は、次のとおりです。 • ハードウェア障害またはクロスバーの同期ずれなどの間欠的なハードウェア エラーのいずれかが発生したため、スイッチでパケットが廃棄された。 • ソフトウェア エラーによってパケットが廃棄された。 • 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 フラップの原因を確認します。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。そのような場合、リンクを再初期化する具体的な方法はデバイスによって異なります。

ポートが ErrDisabled ステートになる

ErrDisabled ステートでは、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ています。ポートがこのステートになるのは、メディアに障害がある可能性を示すポートのフラッピングまたは大量の破損フレーム（CRC エラー）が発生した場合です。

表 5-7 に、考えられる原因および解決方法を示します。

現象　ポートが ErrDisabled ステートになる。

表 5-7　ポートが ErrDisabled ステートになる

現象	考えられる原因	解決方法
ポートが ErrDisabled ステートになる。	ポートでフラップが発生している。	詳細については、「CLI による ErrDisabled ステートの確認」（p.5-9）を参照してください。SFP、ケーブル、および接続を確認します。
	デバイスによって、メディアに障害がある可能性を示す大量の破損フレーム（CRC エラー）が検出された。	

CLI による ErrDisabled ステートの確認

CLI を使用して ErrDisable ステートを確認する手順は、次のとおりです。

ステップ 1　**show interface** コマンドを使用して、スイッチが問題を検出してポートをディセーブルにしたことを確認します。

```
switch# show interface e1/14
e1/7 is down (errDisabled)
```

ステップ 2　ケーブル、SFP、および光ファイバを確認します。

ステップ 3　ポート内部のステート遷移に関する情報を表示します。

```
switch# show port internal event-history interface e1/7
>>>>FSM: <e1/7> has 86 logged transitions<<<<<
1) FSM:<e1/7> Transition at 647054 usecs after Tue Jan  1 22:44..
    Previous state: [PI_FSM_ST_IF_NOT_INIT]
    Triggered event: [PI_FSM_EV_MODULE_INIT_DONE]
    Next state: [PI_FSM_ST_IF_INIT_EVAL]
2) FSM:<e1/7> Transition at 647114 usecs after Tue Jan  1 22:43..
    Previous state: [PI_FSM_ST_IF_INIT_EVAL]
    Triggered event: [PI_FSM_EV_IE_ERR_DISABLED_CAP_MISMATCH]
    Next state: [PI_FSM_ST_IF_DOWN_STATE]
```

この例では、機能のミスマッチまたは「CAP MISMATCH」が原因で、ポート イーサネット 1/7 が ErrDisabled ステートになっています。

ステップ 4　スイッチのログ ファイルを表示し、ポート ステートの変化をリストで確認します。

```
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
```

この例では、ある管理者がポート 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。ポートはポートチャネル 7 と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。

CHAPTER 6

VLAN のトラブルシューティング

この章では、VLAN に関するトラブルシューティング方法について説明します。

この章で説明する内容は、次のとおりです。

VLAN のトラブルシューティングについて

VLAN（仮想 LAN）では、物理的には同じネットワークに接続されていても、論理的には相互に認識する必要のない、論理的に異なる LAN 内に位置するとみなされるデバイスを分離します。

VLAN 名では、次の文字のみを使用する必要があります。

- a ～ z または A ～ Z
- 0 ～ 9
- -（ハイフン）または _（下線）

VLAN を設定する際は、次のガイドラインに従ってください。

- ユーザ トラフィックを管理 VLAN から切り離し、管理 VLAN をユーザ データから分離します。
- プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN には、別々の Quality of Service（QoS）を適用できます。
- すべての発信プライベート VLAN トラフィックに出力 VACL を適用するには、プライマリ VLAN のレイヤ 3 VLAN インターフェイスにセカンダリ VLAN をマッピングしてから、プライマリ VLAN の SVI 上に VACL を設定します。
- プライマリ VLAN のレイヤ 3 VLAN インターフェイスに適用する VACL は、関連付けられた独立 VLAN およびコミュニティ VLAN に自動的に適用されます。
- プライマリ VLAN のレイヤ 3 VLAN インターフェイスにセカンダリ VLAN をマッピングしない場合、プライマリ VLAN とセカンダリ VLAN に異なる VACL が設定される可能性があります。
- プライベート VLAN のトラフィックは、異なる VLAN では異なる方向に伝送されるので、入力トラフィック用と出力トラフィック用にそれぞれ異なる VACL を設定できます。

（注） プライベート VLAN 内のプライマリ VLAN とすべてのセカンダリ VLAN では、同じ VACL を保持することを推奨します。

- DHCP スヌーピングはプライベート VLAN 上でイネーブルにできます。プライマリ VLAN 上で DHCP スヌーピングをイネーブルにすると、DHCP 設定がセカンダリ VLAN に伝播されます。セカンダリ VLAN 上に DHCP を設定しても、プライマリ VLAN 上で DHCP がすでに設定されている場合、セカンダリ VLAN 上での設定は有効になりません。

（注） プライベート VLAN を設定する場合、スティッキ Address Resolution Protocol（ARP; アドレス解決プロトコル）をイネーブルにすることを推奨します。レイヤ 3 プライベート VLAN インターフェイス、または SVI で学習される ARP エントリは、スティッキ ARP エントリになります。セキュリティ上の理由から、プライベート VLAN ポートのスティッキ ARP エントリに期限切れはありません。

- プライベート VLAN ポートには、IEEE 802.1x ポートベース認証を設定できますが、802.1x はポート セキュリティまたはユーザ単位 ACL と共にプライベート VLAN ポートに設定しないでください。
- 802.1x はプライベート VLAN と併用できますが、802.1x ダイナミック VLAN 割り当てまたはゲスト VLAN 割り当てと併用することはできません。
- IGMP は、プライマリ VLAN 上でのみ実行され、すべてのセカンダリ VLAN にプライマリ VLAN の設定が使用されます。

- セカンダリ VLAN 内の IGMP 加入要求は、プライマリ VLAN で受信されたものとして処理されます。
- プライベート VLAN は、次の Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）機能をサポートします。
  - プライベート VLAN ポートを SPAN 送信元ポートとして設定できます。
  - プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN 上で VLAN-based SPAN（VSPAN）を使用したり、単一の VLAN 上で SPAN を使用したりして、出力トラフィックまたは入力トラフィックを個別に監視することができます。
- Remote SPAN（RSPAN）VLAN を、プライベート VLAN のプライマリ VLAN またはセカンダリ VLAN として設定しないでください。
- プライベート VLAN ホストまたはプロミスキャス ポートは、SPAN 宛先ポートにはできません。SPAN 宛先ポートをプライベート VLAN ポートとして設定した場合、ポートは非アクティブとなります。
- 宛先 SPAN ポートは、独立ポートにしないでください（ただし、送信元 SPAN ポートは独立ポートにできます）。
- VSPAN は、プライマリ VLAN またはセカンダリ VLAN の両方にまたがるように設定できます。またはユーザが入力トラフィックか出力トラフィックにのみ関係する場合は、いずれか 1 つを補うように設定できます。
- セカンダリ VLAN で学習された MAC アドレスは、プライマリ VLAN の共有テーブルに追加されます。セカンダリ VLAN がプライマリ VLAN に関連付けられると、セカンダリ VLAN の MAC アドレス テーブルは単一の共有 MAC テーブルにマージされます。

トラブルシューティングの初期チェックリスト

VLAN 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。VLAN に関する問題のトラブルシューティングを開始する際は、まず、次の事項について確認します。

チェックリスト	確認済み
問題のあるポートまたは VLAN の物理接続を確認します。	❑
両方のエンド デバイスが同じ VLAN にあることを確認します。	❑

次の CLI コマンドを使用して、VLAN 情報を表示します。

- **show vlan** *vlan-id*
- **show vlan private-vlan**
- **show vlan all-ports**
- **show vlan private-vlan**
- **show vlan private-vlan type**
- **show interface vlan** *vlan-id* **private-vlan mapping**
- **show tech-support vlan**

VLAN の問題

ここで説明する内容は、次のとおりです。

VLAN を作成できない

VLAN を作成するときに、問題が発生することがあります。

表 6-1 に、考えられる原因および解決方法を示します。

現象　VLAN を作成できない。

表 6-1　VLAN を作成できない

現象	考えられる原因	解決方法
VLAN を作成できない。	Virtual Device Context（VDC; 仮想デバイス コンテキスト）に十分なリソースがない。	**show vdc resource vlan** CLI コマンドを使用して、設定可能な未使用の VLAN 数を調べます。値が 0 の場合、network admin としてログインし、VDC 設定モードで **limit-resource** CLI コマンドを使用して、この VDC に VLAN リソースを追加します。
	予約されている VLAN ID を使用している。	VLAN 3968 ～ 4047 および 4094 は、各 VDC の内部使用のために予約されています。予約されたこれらの VLAN を使用または変更することはできません。

PVLAN を作成できない

プライベート VLAN（PVLAN）を作成するときに、問題が発生することがあります。

表 6-2 に、考えられる原因および解決方法を示します。

現象　PVLAN を作成できない。

表 6-2　PVLAN を作成できない

現象	考えられる原因	解決方法
PVLAN を作成できない。	PVLAN 機能がイネーブルにされていない。	**feature pvlan** CLI コマンドを使用して、PVLAN 機能をイネーブルにします。

VLAN インターフェイスがダウンしている

VLAN インターフェイスの問題が発生することがあります。

表 6-3 に、考えられる原因および解決方法を示します。

現象　VLAN インターフェイスがダウンしている。

表 6-3　VLAN インターフェイスがダウンしている

現象	考えられる原因	解決方法
VLAN インターフェイスがダウンしている。	VLAN が存在しない。	**show vlan** CLI コマンドを使用して、VLAN が存在しているかどうかを調べます。**vlan** CLI コマンドを使用して、VLAN を作成します。
	VLAN 上に STP 転送ステートに設定されたインターフェイスがない。	**show vlan internal vlan-info** CLI コマンドを使用して、Spanning Tree Protocol（STP; スパニング ツリー プロトコル）の動作ステータスをチェックします。少なくとも 1 つのインターフェイスが STP 転送ステートになるように STP を設定します。
	1 つ以上のサービスが原因で VLAN インターフェイスを確認できない。	**show vlan internal vlan-info** CLI コマンドを使用して、VLAN インターフェイスのステートを調べます。ステートが oper-es の場合、**show tech-support interface vlan** CLI コマンドを使用して、詳細情報を収集します。
	VLAN がセカンダリ VLAN である。	**show vlan internal vlan-info** CLI コマンドを使用して、VLAN インターフェイスのステートを調べます。VLAN をプライマリ VLAN またはユーザ VLAN に変更します。
	インターフェイスが正しくない VRF 上にある。	**show vrf interface** CLI コマンドを使用して、VLAN インターフェイスが割り当てられているインターフェイスを調べます。

CHAPTER 7

STP のトラブルシューティング

この章では、Spanning Tree Protocol（STP; スパニング ツリー プロトコル）の実装時に発生する可能性がある問題を識別して解決する方法について説明します。

この章で説明する内容は、次のとおりです。

STP のトラブルシューティングについて

STP は、レイヤ 2 レベルで、ループフリー（ループが発生しない）ネットワークを実現します。レイヤ 2 LAN ポートは、一定の間隔で 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。詳細については、『*Cisco NX-OS Layer 2 Switching Configuration Guide, Release 4.0*』を参照してください。

STP を設定する際は、次のガイドラインに従ってください。

- Multiple STP（MST）とともにプライベート VLAN を使用する場合は、すべてのセカンダリ VLAN がプライマリ VLAN と同じ MST インスタンスに属していることを確認します。
- ネットワーク上のすべての VLAN のスパニング ツリーをディセーブルにせずに、802.1Q トランクのネイティブ VLAN のスパニング ツリーをディセーブルにすると、スパニング ツリー ループが発生することがあります。802.1Q トランクのネイティブ VLAN 上のスパニング ツリーは、イネーブルのままにしておく必要があります。そうできない場合は、ネットワークのすべての VLAN のスパニング ツリーをディセーブルにする必要があります。スパニング ツリーをディセーブルにする前に、ネットワークで物理ループが発生しないことを確認してください。
- 802.1Q トランクを使用して 2 台のシスコ製スイッチを接続する場合、トランク上で許容されている VLAN ごとにスパニング ツリー Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）が交換されます。トランクのネイティブ VLAN 上の BPDU は、タグなしで予約 IEEE 802.1D スパニング ツリー マルチキャスト MAC（メディア アクセス制御）アドレス（01-80-C2-00-00-00）に送信されます。トランクの他のすべての VLAN 上の BPDU は、タグ付きで予約 Cisco Shared Spanning Tree（SSTP）マルチキャスト MAC アドレス（01-00-0c-cc-cc-cd）に送信されます。
- STP では、ポートチャネル バンドルはシングル ポートと見なされます。この場合のポート コストは、そのチャネルに割り当てられているすべての設定済みポート コストの合計です。
- セカンダリ VLAN がプライマリ VLAN に関連付けられている場合、ブリッジ プライオリティなどの 0 プライマリ VLAN の STP パラメータは、セカンダリ VLAN に伝播されます。ただし、他のデバイスに STP パラメータを伝播する必要はありません。VLAN が同一の転送データベースを適切に共有できるように、プライマリ、独立、およびコミュニティ VLAN のスパニング ツリー トポロジが厳密に一致していることを確認するには、STP 設定を手動で検証する必要があります。
- 通常のトランク ポート：
  - プライベート VLAN 内の各 VLAN には、個別に STP インスタンスが存在します。
  - プライマリ VLAN およびすべてのセカンダリ VLAN の STP パラメータは、一致する必要があります。
  - プライマリ VLAN および関連するすべてのセカンダリ VLAN は、同一の MST インスタンスに設定する必要があります。
  - トラフィックが多い状況での衝突を防止するために、リンクの両側のデュプレックス設定を full に設定する必要があります。
- 非トランク ポート：
  - STP は、プライベート VLAN ホスト ポートのプライマリ VLAN のみを認識します。STP は、ホスト ポートのセカンダリ VLAN 上では実行されません。
- プライベート VLAN 上の Rapid PVST+：
  - トランク ポートでは、プライマリおよび セカンダリ プライベート VLAN は 2 つの異なる論理ポートであり、同一の STP トポロジを持つ必要があります。
  - アクセス ポートでは、STP はプライマリ VLAN のみを認識します。

（注） 一部のケースでは、エラー　メッセージが表示されずに設定が許可されても、コマンドは無効である場合があります。

トラブルシューティングの初期チェックリスト

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 に関する問題のトラブルシューティングを開始する際は、まず、次の事項について確認します。

チェックリスト	確認済み
LAN 内のすべてのポートに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。	❑
ネットワーク トポロジ（相互接続されたすべてのポートとスイッチを含む）を確認します。	❑
show spanning-tree summary totals コマンドを使用して、Active ステートの論理インターフェイスの合計数が、許可されている最大数よりも少ないことを確認します。これらの制限の詳細については、『*Cisco NX-OS Layer 2 Switching Configuration Guide, Release 4.0*』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、設定されているシスコの拡張機能を確認します。	❑
ポートがブロックされている場合、隣接デバイスとデュプレックス設定が同じであることを確認します。	❑
トランク設定が、リンクの両側で一致していることを確認します。	❑

次のコマンドを使用して、STP 設定および動作の詳細を表示します。

- **show running-config spanning-tree**
- **show spanning-tree summary**
- **show spanning-tree detail**
- **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**

show spanning-tree blockedports コマンドを使用して、STP にブロックされているポートを表示します。

show mac address-table dynamic vlan コマンドを使用して、各ノードで学習やエージングが発生しているかを判別します。

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 ネットワークでは一般的な問題です。データ ループが発生すると、次のような症状が現れます。

- リンクの使用率が高くなる（最大 100%）
- CPU の使用率、およびバックプレーンのトラフィックの使用率が高くなる
- MAC アドレスの再学習とフラッピングが絶えず発生する
- インターフェイス上で多くの出力が廃棄される

STP ループのトラブルシューティングを行う手順は、次のとおりです。

ステップ 1　リンクの使用率が高いインターフェイスを探し、ループに関連しているポートを特定します。

```
switch# show interface ethernet 2/1 | include rate
  5 minute input rate 9976523 bytes/sec, 25912 packets/sec
  5 minute output rate 985644 bytes/sec, 32456 packets/sec
```

ステップ 2　影響を受けているポートをシャットダウンするか、接続解除します。

```
switch(config)# interface ethernet 2/1
switch(config-if)# shutdown
```

ステップ 3　ネットワーク トポロジ図を使用して、冗長パス上のすべてのスイッチを見つけます。

ステップ 4　このスイッチが、影響を受けていない他のスイッチと同じ STP ルート ブリッジを表示することを確認します。

```
switch# show spanning-tree vlan 9

VLAN0009
  Spanning tree enabled protocol rstp
  Root ID     Priority    32777
              Address     0018.bad7.db15
              Cost        4
...
```

ステップ 5　ルート ポートが、ルート ブリッジへのコストが最小となるポートとして正しく識別されていることを確認します。

```
switch# show spanning-tree vlan 9

VLAN0009
  Spanning tree enabled protocol rstp
  Root ID     Priority    32777
              Address     0018.bad7.db15
              Cost        4
              Port        385 (Ethernet3/1)
              Hello Time  2  sec  Max Age 20 sec  Forward Delay 15 sec
```

ステップ 6　ルート ポートおよび代替ポートで、BPDU が定期的に受信されていることを確認します。

```
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
```

ステップ 7　受信 BPDU カウンタが増加していない場合、内部パケット マネージャが BPDU を受信しているかどうかをチェックします。

```
switch# show system internal pktmgr interface ethernet 3/1
Ethernet3/1, ordinal: 36
  SUP-traffic statistics: (sent/received)
    Packets: 120210 / 15812
    Bytes: 8166401 / 1083056
    Instant packet rate: 5 pps / 5 pps
    Average packet rates(1min/5min/15min/EWMA):
    Packet statistics:
      Tx: Unicast 0, Multicast 120210
          Broadcast 0
      Rx: Unicast 0, Multicast 15812
          Broadcast 0

switch# show system internal pktmgr client 303
Client uuid: 303, 2 filters
  Filter 0: EthType 0x4242,  Dmac 0180.c200.0000
  Filter 0: EthType 0x010b, Snap 267, Dmac 0100.0ccc.cccd

  Options: TO 0, Flags 0x1, AppId 0, Epid 0
  Ctrl SAP: 171, Data SAP 177 (1)
  Rx: 28356632, Drop: 0, Tx: 35498365, Drop: 0
```

ステップ 8　パケット マネージャが BPDU を受信していない場合、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。

```
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
```

ステップ 9　指定ポートが定期的に BPDU を送信していることをチェックします。

```
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
```

ステップ 10　BPDU 送信カウンタが増加している場合、パケット マネージャが BPDU を送信しているかどうかをチェックします。

```
switch# show system internal pktmgr interface ethernet 3/1
Ethernet3/1, ordinal: 36
  SUP-traffic statistics: (sent/received)
    Packets: 120210 / 15812
    Bytes: 8166401 / 1083056
    Instant packet rate: 5 pps / 5 pps
    Average packet rates(1min/5min/15min/EWMA):
    Packet statistics:
     Tx: Unicast 0, Multicast 120210
         Broadcast 0
     Rx: Unicast 0, Multicast 15812
         Broadcast 0

switch# show pktmgr client 303
Client uuid: 303, 2 filters
  Filter 0: EthType 0x4242,  Dmac 0180.c200.0000
  Filter 0: EthType 0x010b, Snap 267, Dmac 0100.0ccc.cccd

  Options: TO 0, Flags 0x1, AppId 0, Epid 0
  Ctrl SAP: 171, Data SAP 177 (1)
  Rx: 28356632, Drop: 0, Tx: 35498365, Drop: 0
```

ステップ 11　パケット マネージャの BPDU 送信カウンタが増加している場合、ハードウェア パケット統計情報カウンタで、BPDU エラー ドロップの可能性をチェックします。

```
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
```

過度のパケット フラディングのトラブルシューティング

STP トポロジの不安定な変更によって、STP ネットワークで過度のパケット フラッディングが発生することがあります。Rapid STP または Multiple STP（MST）では、ポートの状態が forwarding に変更されたときだけでなく、役割が designated から root に変更された場合にもトポロジの変更が発生します。Rapid STP では、レイヤ 2 転送テーブルが即座にフラッシュされます。802.1D では、エージング タイムが短縮されます。転送テーブルが即座にフラッシュされると、接続はより早く復元されますが、フラッディングは増加します。

安定したトポロジでは、1 度のトポロジの変更によって過度のフラッディングが発生することはありません。トポロジはリンク フラップによって変更されるため、リンク フラップが絶え間なく発生するとトポロジ変更が繰り返され、フラッディングが引き起こされる場合があります。フラッディングにより、ネットワーク パフォーマンスが低下し、インターフェイスのパケット ドロップが発生することがあります。

過度なフラッディングのトラブルシューティングを行う手順は、次のとおりです。

ステップ 1　過度なトポロジ変更の発生元を判別します。

```
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
...
```

ステップ 2　トポロジ変更が発生したインターフェイスを判別します。

```
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
...
```

ステップ 3　トポロジ変更を引き起こしていたデバイスを絞り込めるまで、このインターフェイスに接続されているデバイスでステップ 2 を繰り返します。

ステップ 4　このデバイスのインターフェイスのリンク フラップをチェックします。

コンバージェンス時間に関する問題のトラブルシューティング

STP コンバージェンスでは、予想以上に時間がかかる場合や、最終的なネットワーク トポロジが予測とは異なってしまうことがあります。

コンバージェンスに関連する問題のトラブルシューティングを開始するときは、最初に、次の事項について確認します。

- 記録されたネットワーク トポロジ図の誤り
- 設定の誤り — タイマー、直径、シスコの拡張機能（ブリッジ保証、ルート ガード、BPDU ガードなど）の設定に誤りがないことをチェックします。
- コンバージェンス中に、推奨する論理ポート（port-vlan）の制限を越える過大な負荷がスイッチの CPU にかかっている

（注） 推奨されるスケーラビリティの制限は、VDC 単位ではなく、システム全体での制限です。

- STP に影響を与える、ソフトウェアの欠陥

フォワーディング ループからのネットワークの保護

STP によって特定の障害が正しく対処できないという問題に取り組むため、シスコでは多数の機能および拡張機能を開発し、ネットワークをフォワーディング ループから保護しています。

STP のトラブルシューティングは、特定の障害の原因の絞り込みや発見に役立ちますが、ネットワークをフォワーディング ループから保護するには、このような拡張機能を実装することが唯一の手段となります。

ネットワークをフォワーディング ループから保護する手順は、次のとおりです。

ステップ 1　すべてのスイッチ間リンクで、シスコ独自の UniDirectional Link Detection（UDLD; 単一方向リンク検出）プロトコルをイネーブルにします。詳細については、『*Cisco NX-OS Interfaces Configuration Guide, Release 4.0*』の UDLD のセクションを参照してください。

ステップ 2　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 タイプとして設定することで、ブリッジ保証機能をイネーブルにします。

（注）　ブリッジ保証機能は、リンクの両側でイネーブルにする必要があります。そのように設定しない場合、Cisco NX-OS はブリッジ保証の不整合のためにポートを blocked 状態に移行させます。

ステップ 3　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。

Topology Change（TC; トポロジ変更）通知およびそのあとに発生するフラッディングは、ネットワークのパフォーマンスに影響を与える可能性があるため、STP エッジ ポートを設定して量を制限する必要があります。このコマンドは、エンド ステーションと接続されているポートでのみ使用してください。それ以外のポートで使用すると、トポロジで偶発的にループが発生したときに、データパケットのループが発生し、デバイスおよびネットワークの動作が中断することがあります。

ステップ 4　ポートチャネルの設定の誤りの問題を回避するために、ポート チャネルに対して Link Aggregation Control Protocol（LACP）をイネーブルにします。詳細については、『*Cisco NX-OS Interfaces Configuration Guide, Release 4.0*』の LACP のセクションを参照してください。

スイッチ間リンクの自動ネゴシエーションは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、リモートの障害情報を最も早く伝達することができます。リモート側で障害が検出された場合、リンクがパルス受信を続けていても、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ときは、細心の注意を払ってください。STP タイマーは相互に依存しているため、タイマーの変更がネットワーク全体に影響を与えることがあります。

ステップ 5　（任意）**spanning-tree loopguard default** コマンドを使用して、DoS 攻撃（サービス拒絶攻撃）を防止し、ルート ガードによってネットワーク STP 境界を保護します。ルート ガードと BPDU ガードによって、外部の影響から STP を保護できます。

ステップ 6　**spanning-tree bpduguard enable** コマンドを使用して BPDU ガードおよび STP エッジ ポートをイネーブルにし、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 ルータなど）による STP への影響を防止します。

ルート ガードにより、STP は外部の影響から保護されています。BPDU ガードをイネーブルにすると、（優良な BPDU だけでなく）すべての BPDU を受信しているポートがシャットダウンされます。

（注）　2 つの STP エッジ ポートが直接、またはハブを経由して接続されている場合、短時間のループは、ルート ガードまたは BPDU ガードでは防ぐことはできません。

ステップ 7　**vlan** コマンドを使用して独立した VLAN を設定し、管理 VLAN 上でのユーザ トラフィックを防ぎます。管理 VLAN は、ネットワーク全体でなく、1 つのビルディング ブロックに限定します。

ステップ 8　**spanning-tree vlan** *vlan-range* **root primary** コマンドを使用して、予測可能な STP ルートを設定します。

ステップ 9　**spanning-tree vlan** *vlan-range* **root secondary** コマンドを使用して、予測可能なバックアップ STP ルート配置を設定します。

STP ルートとバックアップ STP ルートを設定することで、コンバージェンスが予測どおりに発生し、常に最適のトポロジが構築されるようにする必要があります。STP の優先順位をデフォルト値のままにしないでください。

CHAPTER 8

ルーティングのトラブルシューティング

この章では、仮想デバイス コンテキスト（ルーティング）のトラブルシューティング手順について説明します。

この章では、次の内容について説明します。

ルーティングの概要

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交換の 2 つの基本的な動作が含まれます。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、およびロード バランシングや代替パスの探索などのその他の考慮事項によって異なります。

Cisco NX-OS では、Virtual Device Context（VDC; 仮想デバイス コンテキスト）が採用されており、VDC およびソフトウェア障害ごとに別の管理ドメインを提供します。各 VDC は、複数の Virtual Routing and Forwarding Instances（VRF; 仮想ルーティング / 転送インスタンス）と複数の Routing Information Base（RIB）をサポートしているため、複数のアドレス ドメインを使用できます。

各 VRF は RIB と関連付けられ、この情報が Forwarding Information Base（FIB; 転送情報ベース）によって収集されます。

ルーティングの詳細については、『*Cisco NX-OS Unicast Routing Configuration Guide*』および『*Cisco NX-OS Multicast Routing Configuration Guide for*』を参照してください。

トラブルシューティングの初期チェックリスト

ルーティング に関する問題のトラブルシューティングを開始する際は、まず、次の事項について確認します。

チェックリスト	確認済み
ルーティング プロトコルがイネーブルになっていることを確認します。	❑
必要に応じて、アドレス ファミリーが設定されていることを確認します。	❑
ルーティング プロトコルに対して正しい VRF を設定したことを確認します。	❑

次のコマンドを使用して、ルーティング情報を表示します。

- **show ip arp**
- **show ip traffic**
- **show tcp statistics udp4**
- **show ip client**
- **show tcp client**
- **show ip fib**
- **show ip process**
- **show ip route**
- **show pktmgr interface**
- **show frame traffic**
- **show platform fib**
- **show platform forwarding**
- **show platform ip**
- **show vrf**
- **show vrf interface**

ルーティングのトラブルシューティング

基本的なルーティングの問題のトラブルシューティングを行う手順は、次のとおりです。

ステップ 1　ルーティング プロトコルがイネーブルにされていることを確認します。

```
switch(config)# show ospf
                     ^
% invalid command detected at '^' marker.
```

この機能がイネーブルになっていない場合、Cisco NX-OS によってこのコマンドが無効であることが報告されます。**feature** コマンドを使用して、ルーティング プロトコルをイネーブルにします。

ステップ 2　このルーティング プロトコルの設定を確認します。

```
switch# show running-config eigrp all
version 4.0(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
```

ステップ 3　このルーティング プロトコルの VRF 設定を確認します。

```
switch# show running-config eigrp
version 4.0(1)
feature eigrp
router eigrp 99
  address-family ipv4 unicast
    router-id 192.0.2.1
  vrf red
    stub
```

ステップ 4　このルーティング プロトコルのメモリ利用率をチェックします。

```
switch# show processes memory | include isis
 8913   9293824  bffff1d0/bffff0d0  isis
32243   8609792  bfffe0c0/bfffdfc0  isis
```

ステップ 5　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。

```
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
```

ステップ 6　ルーティング プロトコルがインターフェイス上でイネーブルになっていることを確認します。

```
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
  ...
```

ステップ 7　インターフェイスが正しい VRF 上にあることを確認します。

```
switch(config)# show vrf interface loopback 99
Interface                  VRF-Name                        VRF-ID
loopback99                 default                              1
```

ステップ 8　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。

```
switch(config)# 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:

...
```

ステップ 9　RIB がフォワーディング プレーンとやりとりしていることを確認します。

```
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
m6rib        3          /procket/shm/m6rib-mfdm
```

APPENDIX A

テクニカル サポートへ問い合わせる前の準備

この付録では、Cisco NX-OS のテクニカル サポートへ問い合わせる前に実行する手順について説明します。この付録には、次の内容が記載されています。

TAC へ問い合わせる前に実行する手順

何らかの追加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。ここでは、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問い合わせる前に実行する手順の概要について説明します。

（注） 少なくとも下記のステップ 1 が完了するまでは、モジュールまたはシステムをリロードしないでください。一部のログとカウンタは揮発性ストレージに保持されているので、リロードを実行すると消去されてしまいます。

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作業の手順は、次のとおりです。

ステップ 1　システムの情報とコンフィギュレーションを収集します。この作業は、問題解決の前と後で行う必要があります。次の 3 つのいずれかの方法を使用して、この情報を収集します。

- Telnet または 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** CLI コマンドを実行し、続いて **show tech-support details** CLI コマンドを実行します。
- **tac-pac** *filename* CLI コマンドを使用して、**show tech-support details** CLI コマンドの出力をファイルにリダイレクトし、ファイルを gzip で圧縮します。

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

- ファイル名が指定されなった場合、作成されるファイル名は volatile:show_tech_out.gz になります。「Cisco NX-OS との間でのファイルのコピー」（p.A-4）で説明されている手順を使用して、このファイルをデバイスからコピーします。

ステップ 2　DCNM でエラーが発生する場合は、エラーが表示されている画面のスナップショットをキャプチャします。Windows では、**Alt+PrintScreen** キーを押してアクティブ ウィンドウをキャプチャするか、**PrintScreen** キーだけを押してデスクトップ全体をキャプチャします。このスクリーンショットを Microsoft ペイント（類似のプログラム）の新しいセッションに貼り付けて、ファイルに保存します。

ステップ 3　DCNM または CLI のいずれかで、メッセージ ログに表示される正確なエラー コードを取り込みます。

a. DCNM で **Event Browser** を選択し、生成されたメッセージの最近のリストを表示します。

b. メッセージ ログからエラーをコピーします。このログは、**show logging log** CLI コマンドを使用して表示でき、また **show logging last** *number* コマンドを使用するとログの最後の部分にある行を表示できます。

ステップ 4　テクニカル サポートに問い合わせる前に、次の質問に回答します。

- どのスイッチまたはポートで問題が発生しているか。
- ファブリックで、どの Cisco NX-OS ソフトウェア、ドライバのバージョン、オペレーティング システムのバージョン、およびストレージ デバイスのファームウェアが使用されているか。
- 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** を選択します）。
- このイベントの発生前または発生時に、環境にどのような変更（VLAN、モジュールの追加、アップグレード）が加えられたか。
- 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（どのスイッチ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

ステップ 5　問題がソフトウェアをアップグレードしようとしたことに関係しているかどうかを確認します。

- 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て、テクニカル サポート担当者宛に送付してください。
  - **show install all status**
  - **show system internal log install**
  - **show system internal log install details**
  - **show log nvram**

Cisco NX-OS との間でのファイルのコピー

デバイスとの間でファイルのコピーを行うことが必要になる場合があります。ログ ファイル、コンフィギュレーション ファイル、またはファームウェア ファイルが、これに該当します。

Cisco NX-OS では、スイッチとの間でファイルをコピーする際に使用されるさまざまなプロトコルを提供しています。デバイスは常にクライアントとして動作し、ftp、scp、tftp セッションでは常に Cisco NX-OS が基点になるため、ファイルは外部システムにプッシュされるか、または外部システムからプルされることになります。

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

copy CLI コマンドでは、ftp、scp、sftp、tftp 転送プロトコル、および 12 の異なるコピー ファイルのソースをサポートしています。

```
switch# copy ?
    bootflash: Select source filesystem
    core: Select source filesystem
    debug: Select source filesystem
    ftp: Select source filesystem
    licenses Backup license files
    log: Select source filesystem
    modflash: Select source filesystem
    nvram: Select source filesystem
    running-config Copy running configuration to destination
    scp: Select source filesystem
    sftp: Select source filesystem
    slot0: Select source filesystem
    startup-config Copy startup configuration to destination
    system: Select source filesystem
    tftp: Select source filesystem
    volatile: Select source filesystem
```

転送メカニズムとして、Secure Copy（scp）を使用する場合は、次の構文を使用します。

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

ユーザ user1 を使用して 172.22.36.10 にある /etc/hosts を宛先の hosts.txt へコピーする例を示します。

```
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
```

スタートアップ コンフィギュレーションを stfp 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#
```

ヒント　スタートアップ コンフィギュレーションのサーバへのバックアップは、毎日および変更を行う前に実施する必要があります。コンフィギュレーション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。このスクリプトでは、**copy running-configuration startup-configuration** および **copy startup-configuration tftp:***//server/name* の 2 つのコマンドを使用する必要があります。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。

コア ダンプの使用

コア ダンプには、クラッシュする前のシステムおよびソフトウェアのステータスに関する詳細な情報が含まれています。コア ダンプは、未知の問題が存在する状況で使用できます。コア ダンプは、TFTP サーバまたはローカル システムの slot0: にあるフラッシュ カードに送信できます。コア ダンプを生成するようにシステムを設定する場合は、テクニカル サポート担当者の指導の下で設定を行う必要があります。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。

コア ダンプを TFTP サーバに送信するように設定すると、コア ダンプをテクニカル サポート担当者に E メールで直接送信することができます。

コア ダンプの CLI による設定

システム上でコア ダンプの設定を行うには、次のように **system cores** CLI コマンドを使用します。

```
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（この例ではファイル名が jsmith_cores）は、TFTP サーバのディレクトリに存在している必要があります。

APPENDIX B

トラブルシューティングのツールおよび方法

この付録では、Cisco NX-OS で使用可能なトラブルシューティングのツールおよび方法について説明します。この章で説明する内容は、次のとおりです。

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

Command-Line Interface（CLI; コマンドライン インターフェイス）では、ローカル コンソールを使用するか、またはリモートから Telnet や Secure Shell（SSH; セキュア シェル）セッションを使用して、Cisco NX-OS の設定および監視を実行できます。CLI のコマンド構造は Cisco IOS ソフトウェアと似ており、コンテキスト ヘルプ、**show** コマンド、マルチユーザ サポート、ロールベースのアクセス制御を使用できます。

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、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。エラー コードに関する詳細を確認するには、**show system error-id** コマンドを使用します。

```
switch# copy running-config startup-config
[########################################] 100%
2008 Jan 16 09:59:29 zoom %$ VDC-1 %$ %BOOTVAR-2-AUTOCOPY_FAILED: Autocopy of file
/bootflash/n7000-s1-dk9.4.0.0.837.bin.S8 to standby failed, error=0x401e0008

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

- **show platform —** ルート転送、Quality of Service（QoS）、Access Control List（ACL; アクセス制御リスト）情報を含むプラットフォーム別の情報を提供します。

コンフィギュレーション ファイル

コンフィギュレーション ファイルには、Cisco NX-OS デバイスで機能を設定するための Cisco NX-OS コマンドが含まれています。Cisco NX-OS には、実行コンフィギュレーションとスタートアップ コンフィギュレーションという 2 つのタイプのコンフィギュレーション ファイルがあります。デバイスは、デバイスの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われた現在の変更が保存されます。コンフィギュレーションを変更する前に、コンフィギュレーション ファイルのバックアップ バージョンを作成する必要があります。コンフィギュレーション ファイルをリモート サーバにバックアップすることも（『*Cisco NX-OS Fundamentals Configuration Guide, Release 4.0*』のコンフィギュレーション ファイルの情報を参照）、問題発生時のロールバック用のコンフィギュレーション ファイルのチェックポイント コピーを作成することも（『*Cisco NX-OS System Management Configuration Guide, Release 4.0*』のロールバック機能を参照）できます。

Cisco NX-OS の機能は、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できます。まれにですが、これらのロックを解除できないこともあります。スタートアップ コンフィギュレーション ファイルにロックが残っているかどうかを判別するには、**show system internal sysmgr startup-config locks** コマンドを使用します。これらのロックを解除するには、**system startup-config unlock** コマンドを使用します。

CLI によるデバッグ

Cisco NX-OS では、ネットワークのトラブルシューティングを行うための多数のデバッグ機能セットがサポートされています。CLI を使用して、各機能のデバッグ モードをイネーブルにすると、制御プロトコル交換のリアルタイム更新動作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付加され、発生時刻順に表示されます。デバッグ機能へのアクセスは、CLI のロール機構を使用して制限し、ロール単位でアクセスを分割できます。**debug** コマンドでは、リアルタイムの情報が表示されますが、**show** コマンドを使用すると、リアルタイム情報とともに履歴情報も表示できます。

注意　一部の **debug** コマンドはネットワークのパフォーマンスに影響を与える可能性があるため、**debug** コマンドはシスコ テクニカル サポート担当者の指示に従って使用してください。

（注）　デバッグ メッセージは、特殊なログ ファイルに記録できます。ログ ファイルに記録した方が、デバッグ出力をコンソールに送信するよりも安全で、処理も簡単です。

? オプションを使用すると、各機能で利用できるオプションを表示できます。各コマンド入力には、実デバッグ出力のほかにログ 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動作のタイムスタンプ付きアカウントが表示されます。

デバッグ機能を使用すると、イベント、内部メッセージ、およびプロトコル エラーをトラッキングできます。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には注意が必要です。オプションによっては、コンソールへの出力メッセージが大量に生成されるためにデバイスにアクセスできなくなったり、また CPU に大きな負荷がかかるイベントが生成されてパフォーマンスが著しく低下したりすることがあります。

（注）　**debug-filter** CLI コマンドを使用すると、不要なデバッグ情報をフィルタリングして取り除くことができます。

（注）　**debug** コマンドを入力する前に 2 番めの Telnat または SSH セッションを開くことを推奨します。デバッグ セッションの現在の出力ウィンドウに対する表示が速すぎて停止できない場合、2 番めのセッションを使用して **undebug all** コマンドを入力すれば、デバッグ メッセージの出力を停止できます。

ping および traceroute

（注）

ping および traceroute 機能は、接続およびパス選択に関する問題のトラブルシューティングに使用します。これらの機能を、パフォーマンスの問題の識別または解決には使用しないでください。

TCP/IP ネットワーキングに関する問題のトラブルシューティングを行う場合、最も効果的な 2 つのツールが、ping および traceroute 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 ユーティリティの動作も似ていますが、さらに、フレームが経由した宛先までの特定パスをホップ単位で判別できます。

ここで説明する内容は、次のとおりです。

ping の使用

ping コマンドを使用すると、IPv4 ルーティング型ネットワーク内の特定の宛先に対する接続および遅延を確認できます。

ping6 コマンドを使用すると、IPv6 ルーティング型ネットワーク内の特定の宛先に対する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 デバイスに短い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と、ターゲットの宛先に一連のフレームが送信されます。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。

traceroute の使用

traceroute は、次の目的で使用します。

- 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、双方向のパスがホップ単位で識別され、ホップごとにタイムスタンプが付加されます。traceroute を使用すると、発信スイッチと宛先に最も近いスイッチ間のパスに沿って、ポートの接続をテストできます。

IPv4 ネットワークでは **traceroute** コマンドを使用し、IPv6 ネットワークでは **traceroute6** コマンドを使用します。

宛先に到達できない場合には、パス検出が開始され、障害ポイントまでのパスがトラッキングされます。

プロセスおよび CPU のモニタリング

ここで説明する内容は、次のとおりです。

show processes CLI コマンドの使用

show processes コマンドを使用すると、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（例 B-1 を参照）。このコマンドの出力には、次の情報が表示されます。

- 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された回数（または再開）
- 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、次のように示されます。

- 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 = 存在しない（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 ステートは、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。

例 B-1　show processes コマンド

```
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   Process
-----  -----  --------  -----------  ----  -------------
    1      S  b7f9e468            1     -  init
    2      S         0            1     -  migration/0
    3      S         0            1     -  ksoftirqd/0
    4      S         0            1     -  desched/0
    5      S         0            1     -  migration/1
    6      S         0            1     -  ksoftirqd/1
    7      S         0            1     -  desched/1
    8      S         0            1     -  events/0
    9      S         0            1     -  events/1
   10      S         0            1     -  khelper
   15      S         0            1     -  kthread
   24      S         0            1     -  kacpid
  101      S         0            1     -  kblockd/0
  102      S         0            1     -  kblockd/1
  115      S         0            1     -  khubd
  191      S         0            1     -  pdflush
  192      S         0            1     -  pdflushn
...
```

show processes cpu CLI コマンドの使用

show processes cpu コマンドを使用すると、CPU 使用率を表示できます（例 B-2 を参照）。このコマンドの出力には、次の情報が表示されます。

- 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 = 開始された各プロセスの CPU 時間の平均（ミリ秒単位）
- 1Sec = 最近の 1 秒間における CPU 使用率（パーセント表示）

例 B-2　show processes cpu コマンド

```
switch# show processes cpu

PID    Runtime(ms)  Invoked   uSecs  1Sec   Process
-----  -----------  --------  -----  -----  -----------
    1          922  4294967295      0      0  init
    2          580    377810      1      0  migration/0
    3          889   3156260      0      0  ksoftirqd/0
    4         1648    532020      3      0  desched/0
    5          400    150060      2      0  migration/1
    6         1929   2882820      0      0  ksoftirqd/1
    7         1269    183010      6      0  desched/1
    8         2520  47589180      0      0  events/0
    9         1730   2874470      0      0  events/1
   10           64    158960      0      0  khelper
   15            0    106970      0      0  kthread
   24            0     12870      0      0  kacpid
  101           62   3737520      0      0  kblockd/0
  102           82   3806840      0      0  kblockd/1
  115            0     67290      0      0  khubd
  191            0      5810      0      0  pdflush
  192          983   4141020      0      0  pdflush
  194            0      5700      0      0  aio/0
  193            0      8890      0      0  kswapd0
  195            0      5750      0      0  aio/1
...
```

show system resource CLI コマンドの使用

show system resources コマンドを使用すると、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（例 B-3 を参照）。このコマンドの出力には、次の情報が表示されます。

- Load は、実行中プロセスの数として定義されます。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の数、およびコマンドの実行時に実際に稼働していたプロセスの数が表示されます。
- 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 KB 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。

例 B-3　show system resources コマンド

```
switch# show system resources
Load average:   1 minute: 0.30   5 minutes: 0.34   15 minutes: 0.28
Processes   :   606 total, 2 running
CPU states  :   0.0% user,   0.0% kernel,   100.0% idle
Memory usage:   2063268K total,   1725944K used,    337324K free
                   2420K buffers,  857644K cache
```

オンボード障害ログ機能の使用

Cisco NX-OS には、障害データを永続的ストレージ上のログに記録する機能があります。このデータは、分析の目的で取得して表示できます。この Onboard Failure Logging（OBFL; オンボード障害ログ）機能では、障害情報および環境情報をモジュール上の不揮発性メモリに保管します。この情報は、故障したモジュールの分析に役立ちます。

OBFL 機能によって記録されるデータは、次のとおりです。

- 初期電源投入の時間
- シャーシ内にあるカードのスロット番号
- カードの初期温度
- ファームウェア、BIOS、FPGA 、および ASIC のバージョン
- カードのシリアル番号
- クラッシュに対するスタック 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 限定の履歴情報
- ASIC 割り込みおよびエラー統計情報の履歴
- ASIC レジスタのダンプ

OBFL の設定の詳細については、『*Cisco NX-OS System Management Configuration Guide, Release 4.0*』を参照してください。

GOLD 診断の使用

Generic Online Diagnostics（GOLD; 汎用オンライン診断）は、シスコの全プラットフォームの診断処理に共通のフレームワークを定義します。GOLD により、ハードウェア コンポーネントがチェックされ、システムのデータ プレーンとコントロール プレーンが正常に動作しているかどうかが確認されます。テストによっては、システムの起動時に実施されたり、システム稼働中に実施されたりします。

ブート モジュールは一連のチェックを受けてからオンラインになります。これにより、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でき、障害のあるモジュールが稼働中のネットワークに入り込むことを防止できます。

障害の診断は、システムの稼働中（ランタイム）にも実施されます。一連の診断チェックを設定すると、オンライン システムの状態を判別できます。ただし、ディスラプティブ（中断を伴う）テストと、ノンディスラプティブ（中断を伴わない）テストを区別して実行する必要があります。ノンディスラプティブ テストはバックグラウンドで実行されるため、システム データやコントロール プレーンに影響を与えませんが、ディスラプティブ テストは稼働中のパケット フローに影響を及ぼします。ディスラプティブ テストは、特別にメンテナンス時間枠を設けて計画的に実施する必要があります。**show diagnostic content module** CLI コマンドの出力には、ディスラプティブ テスト、ノンディスラプティブ テストなど、テストの属性が表示されます。

ランタイム診断チェックは、特定の時間に実行、または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、ノンディスラプティブ テストで、システムの稼働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、稼働中のネットワーク環境でハードウェア障害をプロアクティブに検出し、管理者に障害を通知することです。

GOLD では、すべてのテストの診断結果と詳細な統計情報（最後の実行時刻、最初と最後のテストパス時刻、最初と最後のテスト失敗時刻、総実行回数、総失敗回数、失敗連続回数、およびエラーコード）が収集されます。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特定するのに役立ちます。**show diagnostic result** コマンドを使用すると、診断結果を表示できます。

GOLD の設定の詳細については、『*Cisco NX-OS System Management Configuration Guide, Release 4.0*』を参照してください。

EEM の使用

Embedded Event Manager（EEM; 組み込みイベント マネージャ）は、重要なシステム イベントを監視し、ポリシー セットを通じてこれらのイベントに対処できるようにするポリシーベースのフレームワークです。ポリシーは事前にプログラミングされたスクリプトです。発生したイベントに応じて呼び出す処理をこのスクリプトに定義し、ロードすることができます。スクリプトでは、カスタム Syslog または SNMP トラップの生成、CLI コマンド呼び出し、フェールオーバーの強制をはじめ、さまざまな処理を生成できます。

EEM の設定の詳細については、『*Cisco NX-OS System Management Configuration Guide, Release 4.0*』を参照してください。

Ethanalyzer の使用

Ethanalyzer は、Wireshark（旧称 Ethereal）オープン ソース コードに基づく Cisco NX-OS プロトコル アナライザ ツールです。Ethanalyzer は、パケットのキャプチャとデコード用の Wireshark のコマンド ライン バージョンです。Ethanalyzer は、ネットワークのトラブルシューティングおよびコントロール プレーン トラフィックを分析する場合に使用します。

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	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、詳細なプロトコル情報を提供します。
ethanalyzer local interface brief	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、プロトコル情報の概要を提供します。
ethanalyzer local interface limit-captured-frames	キャプチャするフレーム数を制限します。
ethanalyzer local interface limit-frame-size	キャプチャするフレームの長さを制限します。
ethanalyzer local interface capture-filter	キャプチャするパケットのタイプをフィルタします。
ethanalyzer local interface display-filter	表示するキャプチャ済みパケットのタイプをフィルタします。
ethanalyzer local interface decode-internal	Cisco NX-OS の内部フレーム ヘッダをデコードします。 **（注）** NX-OS Ethanalyzer の代わりに Wireshark を使用してデータを分析するときは、このオプションを使用しないでください。
ethanalyzer local interface write	キャプチャしたデータをファイルに保存します。
ethanalyzer local interface read	キャプチャしたデータのファイルを開き、分析します。

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。詳細については、次の URL を参照してください。

http://www.tcpdump.org/tcpdump_man.html

表示フィルタの構文の詳細については、次の URL を参照してください。

http://wiki.wireshark.org/DisplayFilters

管理インターフェイス上に、キャプチャしたデータ（4 パケットに制限）を表示する例を示します。

```
switch(config)# ethanalyzer local interface mgmt brief limit-captured-frames 4
Capturing on eth1
2008-02-18 13:21:21.841182 172.28.230.2 -> 224.0.0.2    HSRP Hello (state Stand
y)
2008-02-18 13:21:21.842190 10.86.249.17 -> 172.28.231.193 TCP 4261 > telnet [AC
] Seq=0 Ack=0 Win=64475 Len=0
2008-02-18 13:21:21.843039 172.28.231.193 -> 10.86.249.17 TELNET Telnet Data ..
2008-02-18 13:21:21.850463 00:13:5f:1c:ee:80 -> ab:00:00:02:00:00 0x6002 DEC DN
 Remote Console
4 packets captured
```

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する例を示します。

```
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: Feb 18, 2008 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/broadca
st)
        .... ..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: 0
    Authentication Data: Default (cisco)
    Virtual IP Address: 172.28.230.1 (172.28.230.1)

1 packets captured
```

表示フィルタを利用して、アクティブな HSRP ステートを持つ HSRP パケットのみを表示する例を示します。

```
switch(config)# ethanalyzer local interface mgmt brief display-filter "hsrp.stat
e==Active" limit-captured-frames 2
Capturing on eth1
2008-02-18 14:35:41.443118 172.28.230.3 -> 224.0.0.2    HSRP Hello (state Active
)
2008-02-18 14:35:44.326892 172.28.230.3 -> 224.0.0.2    HSRP Hello (state Active
)
2 packets captured
```

Wireshark の詳細については、次の URL を参照してください。

http://www.wireshark.org/docs/

DCNM ツール

Cisco DCNM は、サポートされている各機能に関するイベントと統計情報を収集します。

DCNM の詳細については、『*Cisco DCNM Fundamentals Configuration Guide, Release 4.0*』を参照してください。

SNMP および RMON のサポート

Cisco NX-OS は、Management Information Base（MIB）および通知（トラップおよびインフォーム）を含む、SNMP v1、v2、および v3 を包括的にサポートしています。

SNMP 標準により、異なる MIB をサポートしているサードパーティ製のアプリケーションを使用して、Cisco NX-OS の管理および監視を行うことができます。

SNMP v3 は、拡張セキュリティを提供します。各デバイスでは、SNMP サービスを選択的にイネーブルまたはディセーブルに設定できます。また、各デバイスを SNMP v1 および v2 要求の処理方式で設定できます。

Cisco NX-OS では、Remote Monitoring（RMON; リモート モニタリング）アラームおよびイベントもサポートしています。RMON アラームおよびイベントは、しきい値の設定や、ネットワーク動作の変更に基づく通知の送信などのメカニズムを提供します。

AlarmGroup では、アラームを設定することができます。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 使用率のレベルを指定して、RMON アラームを設定できます。*EventGroup* では、アラーム条件に基づいて実行される動作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あります。

SNMP および RMON の設定の詳細については、『*Cisco NX-OS System Management Configuration Guide, Release 4.0*』を参照してください。

RADIUS の使用

RADIUS 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、アトリビュートまたは証明書を交換するためのプロトコルです。これらのアトリビュートは、次の 3 つの Class of Service（CoS; サービス クラス）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共に、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識別します。

アカウンティングは、スイッチ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、（RADIUS を使用して）ローカルまたはリモートで実行できます。

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 Dec 15 04:02:27 2007:start:/dev/pts/0_1039924947:admin
Sun Dec 15 04:02:28 2007:stop:/dev/pts/0_1039924947:admin:vsh exited normally
Sun Dec 15 04:02:33 2007:start:/dev/pts/0_1039924953:admin
Sun Dec 15 04:02:34 2007:stop:/dev/pts/0_1039924953:admin:vsh exited normally
Sun Dec 15 05:02:08 2007:start:snmp_1039928528_172.22.95.167:public
Sun Dec 15 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（開始時と終了時）のみを表示します。

Syslog の使用

システム メッセージ ロギング ソフトウェアでは、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。

- モニタおよびトラブルシューティングのためのログ情報を記録
- 取り込まれるログ情報のタイプを選択
- 取り込まれるログ情報の宛先を選択

Syslog を使用すると、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することができます。すぐに使用する場合には、Syslog メッセージをコンソールに出力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、デバッグからクリティカル イベントまで、7 つのカテゴリに分類されます。デバイス内の特定サービスについて、レポートする重大度レベルを制限できます。たとえば、OSPF サービスについてはデバッグ イベントだけをレポートし、BGP サービスについてはすべての重大度レベルのイベントを記録するといった設定ができます。

ログ メッセージは、システム再起動の全体にわたって保存されるものではありません。ただし、重大度が critical 以上（レベル 0、1、および 2）のログ メッセージは、最大 100 個まで NVRAM に保存されます。このログは、**show logging nvram** コマンドを使用していつでも表示できます。

ここで説明する内容は、次のとおりです。

- ログ レベル（p.B-14）
- Telnet または SSH へのロギングのイネーブル化（p.B-15）

ログ レベル

Cisco NX-OS では、次のログ 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、標準的かつ重要なシステム メッセージがログ ファイルに記録され、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機能を強化するために、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。

ユーザは、コンソールへのロギングをディセーブルにすること、または特定の Telnet や SSH セッションへのロギングをイネーブルにすることができます。

- コンソールへのロギングをディセーブルにするには、設定モードで **no logging console** コマンドを使用します。
- Telnet または SSH へのロギングをイネーブルにするには、EXEC モードで **terminal monitor** コマンドを使用します。

（注） 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、そのステートが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、ステートは維持されます。ただし、Telnet または SSH 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、そのステート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、そのステートは維持されません。

no logging console コマンド（例 B-4 を参照）は、コンソールへのロギングをディセーブルにします。デフォルト設定はイネーブルです。

例 B-4　no logging console コマンド

```
switch(config)# no logging console
```

terminal monitor コマンド（例 B-5 を参照）は、Telnet または SSH へのロギングをイネーブルにします。デフォルト設定はディセーブルです。

例 B-5　terminal monitor コマンド

```
switch# terminal monitor
```

Syslog の設定の詳細については、『*Cisco NX-OS System Management Configuration Guide, Release 4.0*』を参照してください。

SPAN の使用

Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）ユーティリティを使用すると、詳細なトラブルシューティングを実行すること、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をサンプリングして予防的なモニタリングおよび分析を実行できます。

デバイスのコンフィギュレーションを修正しても ネットワークの問題を解決できない場合には、通常、プロトコル レベルを調べる必要があります。エンド ノードとスイッチ間の制御トラフィックは、**debug** コマンドによって確認できます。ただし、ホストまたはディスクなどの特定のエンド ノードが送信または受信しているすべてのトラフィックを調べる必要がある場合には、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できます。

プロトコル アナライザを使用するには、分析対象デバイスの回線内にアナライザを挿入し、デバイスの入出力に割り込む必要があります。

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することによって、この問題を解決できます。SPAN では、すべてのトラフィックをコピーして、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、どの接続デバイスにも割り込まず、CPU に不要な負荷がかからないようにハードウェアで実行されます。

SPAN では、デバイス内で最大 16 の個別の SPAN セッションを作成できます。各セッションに、最大 4 つの個別の送信元と、1 つの宛先ポートを設定します。また、フィルタを適用することにより、受信トラフィックまたは送信トラフィックだけをキャプチャできます。特定の VLAN からのトラフィックをキャプチャすることもできます。

SPAN ユーティリティを起動するには、**span session** *session_num* コマンドを使用し、*session_num* に各 SPAN セッションの識別番号を指定します。このコマンドを入力すると、宛先インターフェイスおよび送信元の VLAN またはインターフェイスを設定できるサブメニューが表示されます。

```
switch2# config terminal
switch2(config)# span session 1 <<=== Create a span session

switch2(config-span)# source interface e1/8 <<=== Specify the port to be spanned

switch2(config-span)# destination interface e1/3 <<==== Specify the span destination
port

switch2(config-span)# end

switch2# show span session 1
Session 1 (active)
   Destination is e1/3
   No session filters configured
   Ingress (rx) sources are
     e1/8,
   Egress (tx) sources are
     fe1/8,
```

SPAN の設定の詳細については、『*Cisco NX-OS System Management Configuration Guide, Release 4.0*』を参照してください。

Blue Beacon 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。ローカルの管理者が、トラブルシューティングや交換を行うハードウェアをすぐに識別できるように、ハードウェア コンポーネントの LED を点滅させておくと便利です。

ハードウェアの 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	シャーシの LED を点滅させます。
blink fan *number*	ファンの LED 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*	電源の LED を点滅させます。
blink xbar *number*	クロスバー モジュールの LED の 1 つを点滅させます。

モジュールのシングル ポート LED を点滅させるには、インターフェイス設定モードで次のコマンドを使用します。

コマンド	目的
beacon	インターフェイスの LED を点滅させます。

INDEX

く

こ

し

す

そ

て

と

ふ

へ

ほ

ま

ゆ

ら