cisco.



Catalyst 4500 シリーズ スイッチ Cisco IOS ソフトウェア コンフィギュレーション ガイド

Release 12.2(44)SG

Text Part Number: OL-15342-01-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。

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

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

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

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

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

CCDE, CCENT, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0803R)

Catalyst 4500 シリーズスイッチ Cisco IOS ソフトウェア コンフィギュレーション ガイド Copyright © 1999-2007 Cisco Systems, Inc.
All rights reserved.

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



CONTENTS

はじめに xli

対象読者 xli

マニュアルの構成 xlii

関連資料 xlv

ソフトウェア マニュアル xlvi

表記法 xlvii

タスク テーブルのコマンド xlvii

Notices xIviii

OpenSSL/Open SSL Project xlviii

License Issues xIviii

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

Japan TAC Web サイト I

 CHAPTER 1
 製品概要
 1-1

レイヤ2ソフトウェアの機能 1-2

802.1Q およびレイヤ 2 プロトコル トンネリング 1-2

CDP 1-2

EtherChannel バンドル 1-3

ジャンボ フレーム 1-3

LLDP 1-3

Multiple Spanning-Tree 1-3

PVRST+ 1-4

QoS 1-4

Resilient Ethernet Protocol 1-5

STP 1-5

Stateful Switchover 1-5

SVI 自動ステート 1-6

UBRL 1-6

UDLD 1-6

単一方向イーサネット 1-6

VLAN 1-6

レイヤ3ソフトウェアの機能 1-8

```
CEF
        1-8
  HSRP
          1-8
     SSO 認識 HSRP
  IP ルーティング プロトコル
                         1-9
    BGP
           1-9
     EIGRP
            1-9
     GLBP
            1-10
    IGRP
            1-10
    IS-IS
           1-10
    OSPF
            1-11
     RIP
          1-11
     VRRP
            1-11
  マルチキャスト サービス
                       1-12
  NSF/SSO
          1-13
  ISSU
         1-13
  PBR
        1-13
  UDLR
         1-13
  VRF-Lite
           1-14
管理機能
         1-15
  Cisco Network Assistant および組み込み CiscoView
                                          1-15
  DHCP
          1-15
  FAT ファイル管理システム (Supervisor Engine 6-E のみ)
                                              1-16
  強制 10/100 自動ネゴシエーション
                              1-16
  インテリジェントな電源管理
                         1-16
  MAC アドレス通知
                   1-16
  MAC 通知 MIB
              1-16
  NetFlow 統計情報
                  1-16
  SSH
        1-17
  SNMP
         1-17
  SPAN および RSPAN
                     1-17
  VRRP
         1-17
  WCCP
          1-18
セキュリティ機能
               1-19
  802.1X ID ベースのネットワーク セキュリティ
                                    1-19
  DAI
        1-20
  DHCP スヌーピング
                  1-20
  フラッディング ブロック
                      1-20
  ハードウェアベースのコントロール プレーン ポリシング
                                              1-21
```

スタティック ホストのための IPSG 1-21 **IPSG** 1-21 ローカル認証、RADIUS、および TACACS+ 認証 1-22 NAC 1-22 ACL によるネットワーク セキュリティ 1-22 ポート セキュリティ 1-23 ストーム制御 1-23 uRPF ストリクト モード (Supervisor Engine 6-E のみ) 1-23 ユーティリティ 1-24 レイヤ 2 traceroute 1-24 TDR 1-24 デバッグ機能 1-24 Metro の機能 1-25

1-25

CHAPTER 2 CLI 2-1

スイッチ CLI へのアクセス 2-2

Resilient Ethernet Protocol

EIA/TIA-232 コンソール インターフェイスを使用して CLI にアクセスする場合 2-2

Telnet を使用して CLI にアクセスする場合 2-2

コマンドラインの処理 2-4

ヒストリ置換 2-4

Cisco IOS コマンド モードの概要 2-5

コマンド リストおよび構文の取得 2-7

スタンバイ スーパーバイザ エンジンの仮想コンソール 2-7

ROMMON の CLI 2-9

CHAPTER 3 スイッチの初期設定 3-1

デフォルトのスイッチ設定 3-2

DHCP ベースの自動設定の設定 3-2

DHCP ベースの自動設定の概要 3-2

DHCP クライアントの要求プロセス 3-3

DHCP サーバの設定 3-4

TFTP サーバの設定 3-5

DNS サーバの設定 3-5

リレー装置の設定 3-6

コンフィギュレーション ファイルの入手方法 3-6

構成例 3-7

スイッチの設定 3-9

コンフィギュレーション モードによるスイッチの設定 3-9 実行コンフィギュレーション設定の確認 3-10 実行コンフィギュレーション設定値の起動ファイルへの保存 3-10 NVRAM での設定の確認 3-11 デフォルト ゲートウェイの設定 3-11 スタティック ルートの設定 3-12 特権 EXEC コマンドへのアクセス制御 3-14 スタティック イネーブル パスワードの設定または変更 3-14 enable password コマンドおよび enable secret コマンドの使用 3-14 特権パスワードの設定または変更 3-15 TACACS+ によるスイッチ アクセスの制御 3-16 TACACS+ の概要 3-16 TACACS+ の動作 3-18 TACACS+ の設定 3-18 TACACS+ 設定の表示 3-23 パスワードの暗号化 3-23 複数の特権レベルの設定 3-24 コマンドの特権レベルの設定 3-24 回線のデフォルト特権レベルの変更 3-25 特権レベルへのログイン 特権レベルの終了 3-25 パスワード、アクセス レベル、および特権レベルの設定の表示 3-25 イネーブル パスワードを忘れた場合の回復方法 3-26 スーパーバイザ エンジンのスタートアップ コンフィギュレーションの変更 3-27 スーパーバイザ エンジンのブート コンフィギュレーションの概要 3-27 ROM モニタの概要 3-27 ソフトウェア コンフィギュレーション レジスタの設定 3-28 ブート フィールドの変更および boot コマンドの使用 ブート フィールドの変更 3-30 コンフィギュレーション レジスタ設定値の確認 3-31 スタートアップ システム イメージの指定 3-32 フラッシュ メモリの使用 3-32 フラッシュ メモリの機能 3-32 セキュリティ上の注意 3-32 フラッシュ メモリの設定 3-32 環境変数の制御 3-33

スイッチの出荷時のデフォルト設定へのリセット

3-34

CHAPTER 4 スイッチの管理 4-1

システム日時の管理 4-2 システム クロック 4-2 NTP の概要 4-2

NTP の設定 4-4

NTP のデフォルト設定 4-4

NTP 認証の設定 4-4

NTP アソシエーションの設定 4-6

NTP ブロードキャスト サービスの設定 4-7

NTP アクセス制限の設定 4-8

NTP パケット用の送信元 IP アドレスの設定 4-10

NTP 設定の表示 4-11

手動での日時の設定 4-11

システム クロックの設定 4-11

日時設定の表示 4-12

時間帯の設定 4-12

夏時間の設定 4-13

システム名とプロンプトの設定 4-15

デフォルトのシステム名およびプロンプトの設定 4-15

システム名の設定 4-15

DNS の概要 4-15

DNS のデフォルト設定 4-16

DNS の設定 4-16

DNS 設定の表示 4-17

バナーの作成 4-18

バナーのデフォルト設定 4-18

MoTD ログイン バナーの設定 4-18

ログイン バナーの設定 4-19

MAC アドレス テーブルの管理 4-20

アドレス テーブルの作成 4-20

MAC アドレスと VLAN 4-21

MAC アドレス テーブルのデフォルト設定 4-21

アドレス エージング タイムの変更 4-21

ダイナミック アドレス エントリの削除 4-22

MAC 変更通知トラップの設定 4-22

MAC 移動通知トラップの設定 4-25

MAC しきい値通知トラップの設定 4-26

スタティック アドレス エントリの追加および削除 4-27

ユニキャスト MAC アドレス フィルタリングの設定 4-29 アドレス テーブル エントリの表示 4-30

ARP テーブルの管理 4-31

組み込み CiscoView サポートの設定 4-31

組み込み CiscoView の概要 4-31

組み込み CiscoView のインストールおよび設定 4-32

組み込み CiscoView 情報の表示 4-34

CHAPTER 5 CISCO IOS ISSU プロセスの設定 5-1

関連資料 5-1

内容 5-1

ISSU を実行するための前提条件 5-2

ISSU の実行に関する制約事項 5-3

ISSU の実行に関する情報 5-3

SSO の概要 5-3

NSF の概要 5-5

ISSU プロセスの概要 5-6

ISSU をサポートする Cisco IOS ソフトウェアのバージョニング機能 5-11 互換性マトリクス 5-12

ISSU に対する SNMP サポート 5-13

Cisco Feature Navigator を使用した互換性の検証 5-13

ISSU プロセスの実行方法 5-14

ISSU ソフトウェア インストレーションの確認 5-14

ISSU プロセスを開始する前の冗長モードの確認 5-15

ISSU プロセスを開始する前の ISSU ステートの確認 5-17

スタンバイ スーパーバイザ エンジンへの新しい Cisco IOS ソフトウェアの ロード 5-17

スタンバイ スーパーバイザ エンジンへの切り替え 5-20

ISSU ロールバック タイマーの停止(任意) 5-23

新しくスタンバイになったスーパーバイザ エンジンへの新しい Cisco IOS ソ フトウェアのロード 5-24

ISSU プロセス中のソフトウェア アップグレードの中断 5-26

アップグレード問題を回避するためのロールバック タイマーの設定 5-27

ISSU 互換性マトリクス情報の表示 **5-28**

CHAPTER 6 インターフェイスの設定 6-1

インターフェイス設定の概要 6-2

interface コマンドの使用 6-3

インターフェイスの範囲設定 6-5

インターフェイス範囲マクロの定義および使用 6-7

10 ギガビット イーサネット ポートおよびギガビット イーサネット SFP ポートの配置 6-8

10 ギガビット イーサネット ポートまたはギガビット イーサネット ポートの WS-X4606-10GE-E および Supervisor Engine 6-E への配置 **6-10**

ポート番号設定を行う TwinGig コンバータ 6-10

TwinGig コンバータの制限事項 6-11

X2/TwinGig コンバータ モードの選択 6-11

Supervisor Engine 6-E での共有バックプレーン アップリンク モードの起動 6-13

光デジタル モニタ トランシーバのサポート 6-14

オプションのインターフェイス機能の設定 6-15

イーサネット インターフェイス速度およびデュプレックス モードの設定 6-15

速度およびデュプレックス モード設定時の注意事項 6-15

インターフェイス速度の設定 6-15

インターフェイスのデュプレックス モードの設定 6-17

インターフェイス速度およびデュプレックス モードの設定の表示 6-17

インターフェイスに関する記述の追加 6-18

フロー制御の設定 6-18

ジャンボ フレーム サポートの設定 6-22

ジャンボ フレームをサポートするポートおよびモジュール 6-22

ジャンボ フレーム サポートの概要 6-23

MTU サイズの設定 6-25

ベビー ジャイアント機能との対話 6-25

ポート デバウンス タイマーの設定 6-26

ポートでの Auto-MDIX の設定 6-27

インターフェイスの Auto-MDIX 設定の表示 6-28

OIR の概要 6-30

インターフェイスのモニタリングおよびメンテナンス 6-31

インターフェイスとコントローラのステータスのモニタリング 6-31

インターフェイスのクリアとリセット 6-31

インターフェイスのシャットダウンおよび再起動 6-32

インターフェイス リンク ステータス イベントおよびトランク ステータス イベントの設定 6-33

インターフェイスのリンク ステータス イベント通知の設定 6-33

グローバルな設定 6-33

スイッチのグローバル リンク ステータス ロギング イベントの設定 6-34

結果 6-34

デフォルト設定へのインターフェイスのリセット 6-35

CHAPTER 7 ポートのステータスと接続の確認 7-1

モジュール ステータスの確認 7-2

インターフェイスのステータスの確認 7-3

MAC アドレスの表示 7-4

TDR を使用したケーブル ステータスの確認 7-5

概要 7-5

TDR テストの実行 7-5

注意事項 7-6

Telnet の使用 7-7

ログアウト タイマーの変更 7-7

ユーザ セッションのモニタリング 7-8

ping の使用 7-9

ping の機能 7-9

ping の実行 7-9

IP traceroute の使用 7-10

IP traceroute の機能 7-10

IP traceroute の実行 7-10

レイヤ 2 traceroute の使用 7-11

レイヤ 2 traceroute の使用上の注意事項 7-11

レイヤ 2 traceroute の実行 7-12

ICMP の設定 7-13

ICMP Protocol Unreachable メッセージのイネーブル化 7-13

ICMP Redirect メッセージのイネーブル化 7-13

ICMP Mask Reply メッセージのイネーブル化 7-14

CHAPTER 8 RPR および SSO を使用したスーパーパイザ エンジンの冗長設定 8-1

スーパーバイザ エンジンの冗長構成 8-2

概要 8-2

RPR 動作 8-3

SSO 動作 8-3

スーパーバイザ エンジンの冗長構成の同期化 8-5

RPR スーパーバイザ エンジンの設定の同期化 8-5

SSO スーパーバイザ エンジンの設定の同期化 8-5

スーパーバイザ エンジンの冗長構成に関する注意事項および制約事項 8-6

スーパーバイザ エンジンの冗長設定 8-8

冗長構成の設定 8-8

スタンバイ スーパーバイザ エンジンの仮想コンソール 8-10

8-12

```
ソフトウェア アップグレードの実行
                                           8-15
               冗長スーパーバイザ エンジンでの Bootflash 操作
                                                    8-17
             Cisco NSF/SSO スーパーパイザ エンジンの冗長構成の設定
CHAPTER 9
                                                         9-1
               NSF/SSO スーパーバイザ エンジンの冗長構成の概要
                                                       9-2
                  Cisco IOS NSF 認識および NSF 対応サポートの概要
                                                         9-2
                  NSF/SSO スーパーバイザ エンジンの冗長構成の概要
                                                         9-4
                 SSO の動作
                             9-5
                 NSF の動作
                             9-5
                 CEF
                        9-6
                  ルーティング プロトコル
                                      9-6
                    BGP の動作
                               9-7
                    OSPF の動作
                                9-7
                    IS-IS の動作
                               9-8
                    EIGRP の動作
                                 9-9
                 NSF の注意事項と制約事項
                                       9-10
               NSF/SSO スーパーバイザ エンジンの冗長構成の設定
                                                       9-11
                  SSO の設定
                             9-11
                  CEF NSF の設定
                                9-12
                  CEF NSF の確認
                                9-12
                 BGP NSF の設定
                                9-13
                  BGP NSF の確認
                                9-13
                  OSPF NSF の設定
                                 9-14
                  OSPF NSF の確認
                                 9-15
                  IS-IS NSF の設定
                                 9-15
                  IS-IS NSF の確認
                                 9-16
                  EIGRP NSF の設定
                                  9-18
                  EIGRP NSF の確認
                                  9-18
             環境モニタリングおよび電源管理
CHAPTER 10
                                       10-1
               環境モニタリングの概要
                                   10-2
                  CLI コマンドによる環境のモニタリング
                                                10-2
                  環境状態の表示
                               10-2
                    Supervisor Engine II-Plus から V-10GE の状態
                                                       10-2
                    Supervisor Engine 6-E の状態
                                           10-3
                  緊急処理
                           10-3
                  システム アラーム
```

スーパーバイザ エンジンの設定の同期化

8-14

手動による切り替え

10-4

電源管理 10-6

Catalyst 4500 シリーズ スイッチの電源管理 10-6

サポート対象の電源装置 10-7

Catalyst 4500 スイッチの電源管理モード 10-8

電源管理モードの選択 10-8

Catalyst 4500 シリーズ スイッチでの電源管理の制限事項 10-9

Catalyst 4500 シリーズ スイッチの電源装置で利用できる電力 10-13

4200 W AC 電源装置に関する特記事項 10-14

複合モードの電力維持機能 10-15

1400 W DC 電源装置に関する特記事項 10-17

1400 W DC SP トリプル入力電源装置に関する特記事項 10-18

Supervisor Engine II-TS でインライン パワーが不足した場合の処理 10-18

モジュールの電源切断 10-20

Catalyst 4948 スイッチの電源管理 10-21

Catalyst 4948 スイッチの電源管理モード 10-21

CHAPTER 11 POE の設定 11-1

概要 11-2

ハードウェア要件 11-2

雷源管理モード 11-3

インテリジェントな電源管理 11-5

インターフェイス上の受電装置に対する消費電力量の設定 11-6

概要 11-6

PoE およびサポートされているケーブル接続トポロジ 11-8

インターフェイスの動作ステータスの表示 11-9

モジュールで消費される PoE の表示 11-11

E シリーズにおける Enhanced Power PoE のサポート 11-15

CHAPTER 12 Cisco Network Assistant による Catalyst 4500 シリーズ スイッチの設定 12-1

Network Assistant の設定および使用法 12-2

Network Assistant の関連機能およびデフォルト設定 12-2

CLI コマンドの概要 12-3

スイッチでの Network Assistant の設定 12-4

CNA から Catalyst 4500 ヘアクセスするのに必要な最小設定 12-4

コミュニティを使用する必要がある場合の追加設定 12-5

クラスタを使用する必要がある場合の追加設定 12-5

コミュニティを使用したネットワーク管理 12-6

候補およびメンバの特性 12-7

候補およびメンバの自動検出 12-7 コミュニティ名 12-8 ホスト名 12-8 パスワード 12-8 通信プロトコル 12-8 Network Assistant のアクセス モード 12-8 コミュニティ情報 12-9 デバイスの追加 12-9 クラスタのコミュニティへの変換 12-10 クラスタを使用したネットワーク管理 スイッチ クラスタの概要 12-11 CLI を使用したスイッチ クラスタ管理 12-14

コミュニティ モードまたはクラスタ モードでの Network Assistant の設定 12-14

コミュニティ モードのネットワーク スイッチ上での Network Assistant の 設定 12-14

クラスタ モードのネットワーク スイッチ上での Network Assistant の設定 12-18

CHAPTER 13 VLAN、VTP、および VMPS の設定 13-1

VLAN 13-2

VLAN の概要 13-2

VLAN 設定時の注意事項および制約事項 13-4

VLAN 範囲 13-4

標準範囲の VLAN で設定できるパラメータ 13-5

VLAN のデフォルト設定 13-5

VLAN の設定 13-6

グローバル コンフィギュレーション モードでの VLAN の設定 13-6 VLAN へのレイヤ 2 LAN インターフェイスの割り当て 13-8

VTP 13-9

VTP の概要 13-9

VTP ドメインの概要 13-9

VTP モードの概要 13-10

VTP アドバタイズの概要 13-10

VTP バージョン 2 の概要 13-11

VTP プルーニングの概要 13-11

VTP 設定時の注意事項および制約事項 13-13

VTP のデフォルト設定 13-13

VTP の設定 13-14

VTP グローバル パラメータの設定 13-14

Catalyst 4500 シリーズ スイッチ Cisco IOS ソフトウェア コンフィギュレーション ガイド

VTP サーバとしてのスイッチの設定 13-15

VTP クライアントとしてのスイッチの設定 13-16

VTP のディセーブル化 (VTP トランスペアレント モード) 13-17

VTP 統計情報の表示 13-18

VMPS 13-19

VMPS の概要 13-19

VMPS サーバの概要 13-19

VMPS サーバのセキュリティ モード 13-20

代替 VLAN 13-21

不正な VMPS クライアント要求 13-21

VMPS クライアントの概要 13-21

ダイナミック VLAN メンバシップの概要 13-22

デフォルトの VMPS クライアント設定 13-22

VMPS クライアントとしてのスイッチの設定 13-23

VMPS の管理およびモニタリング 13-26

ダイナミック ポート VLAN メンバシップのトラブルシューティング 13-27

ダイナミック ポート VLAN メンバシップの設定例 13-27

VMPS データベース コンフィギュレーション ファイルの例 13-31

CHAPTER 14 IP アンナンバード インターフェイスの設定 14-1

関連資料 14-1

IP アンナンバード サポートの概要 14-2

DHCP サーバとリレー エージェントでの IP アンナンバード インターフェイス サポート 14-2

DHCP オプション 82 14-2

接続ホストのポーリングを行う IP アンナンバード 14-3

DHCP サーバにおける IP アンナンバード インターフェイス サポートの設定 14-4

LAN および VLAN インターフェイスに対する IP アンナンバード インターフェイス サポートの設定 14-4

イーサネット VLAN 範囲に対する IP アンナンバード インターフェイス サポートの設定 14-5

接続ホストのポーリングを行う IP アンナンバード インターフェイス サポートの 設定 14-6

IP アンナンバード インターフェイス設定の表示 14-8

IP アンナンバードのトラブルシューティング 14-9

CHAPTER 15 レイヤ 2 イーサネット インターフェイスの設定 15-1

レイヤ2 イーサネット スイッチングの概要 15-2

レイヤ 2 イーサネット スイッチングの概要 15-2

セグメント間のフレーム スイッチング 15-2

MAC アドレス テーブルの作成 15-3

VLAN トランクの概要 15-3

カプセル化タイプ 15-4

レイヤ2インターフェイス モード 15-4

レイヤ2 イーサネット インターフェイスのデフォルト設定 15-6

レイヤ 2 インターフェイス設定時の注意事項および制約事項 15-6

レイヤ2スイッチング用のイーサネットインターフェイスの設定 15-7

レイヤ 2 トランクとしてのイーサネット インターフェイスの設定 15-7

レイヤ 2 アクセス ポートとしてのインターフェイスの設定 15-10

レイヤ 2 設定のクリア 15-11

CHAPTER 16 SmartPort マクロの設定 16-1

SmartPort マクロの概要 16-2

SmartPort マクロの設定 16-3

マクロに渡されるパラメータ 16-3

マクロ パラメータのヘルプ 16-3

SmartPort マクロのデフォルト設定 16-4

cisco-global 16-4

cisco-desktop 16-5

cisco-phone 16-5

cisco-router 16-6

cisco-switch 16-6

SmartPort マクロの設定時の注意事項 16-6

SmartPort マクロの作成 16-8

SmartPort マクロの適用 16-9

cisco-global 16-10

cisco-desktop 16-11

cisco-phone 16-12

cisco-switch 16-13

cisco-router 16-14

SmartPort マクロの表示 16-15

CHAPTER 17 STP および MST の設定 17-1

STP の概要 17-2

ブリッジ ID の概要 17-2

ブリッジ プライオリティ値 17-2

拡張システム ID 17-3

STP MAC アドレスの割り当て 17-3

BPDU 17-3 ルート ブリッジの選定 17-4 STP タイマー 17-5 STP トポロジの作成 17-5 STP ポート ステート 17-6 MAC アドレスの割り当て 17-6 STP および IEEE 802.1Q トランク 17-6 PVRST+ 17-7 STP のデフォルト設定 17-8 STP の設定 17-9 STP のイネーブル化 17-9 拡張システム ID のイネーブル化 17-10 ルート ブリッジの設定 セカンダリ ルート スイッチの設定 17-13 STP ポート プライオリティの設定 17-15 STP ポート コストの設定 17-17 VLAN のブリッジ プライオリティの設定 17-19 hello タイムの設定 17-20 VLAN の最大エージング タイムの設定 17-20 VLAN の転送遅延時間の設定 STP のディセーブル化 17-22 PVRST+ のイネーブル化 17-22 リンク タイプの指定 17-23 プロトコル移行の再開 17-24 MST の概要 17-25 IEEE 802.1s MST 17-25 IEEE 802.1w RSTP 17-26 RSTP のポートの役割 17-27 RSTP ポート ステート 17-27 MST/SST 間のインターオペラビリティ 17-28 CST 17-29 MSTI 17-29

MST リージョン 17-29

MST リージョンの概要

境界ポート 17-30

IST マスター

エッジ ポート

MST のコンフィギュレーション パラメータ

17-30

17-30

17-30

17-29

リンク タイプ 17-31

メッセージ エージおよびホップ カウント 17-31

MST/PVST+ 間のインターオペラビリティ 17-31

MST 設定時の注意事項および制約事項 17-32

MST の設定 17-33

MST のイネーブル化 17-33

MSTI パラメータの設定 17-35

MSTI ポート パラメータの設定 17-36

プロトコル移行の再開 17-36

MST コンフィギュレーションの表示 17-37

CHAPTER 18 Resilient Ethernet Protocol の設定 18-1

REP の概要 18-2

リンク完全性 18-3

ファスト コンバージェンス 18-4

VLAN ロード バランシング 18-4

スパニング ツリー インタラクション 18-6

REP ポート 18-6

REP の設定 18-7

REP のデフォルト設定 18-7

REP 設定時の注意事項 18-7

REP 管理 VLAN の設定 18-8

REP インターフェイスの設定 18-9

VLAN ロード バランシングの手動によるプリエンプションの設定 18-13

REP の SMMP トラップ設定 18-14

REP のモニタリング 18-15

CHAPTER 19 任意の STP 機能の設定 19-1

ルート ガードの概要 19-2

ルート ガードのイネーブル化 19-3

ループ ガードの概要 19-4

ループ ガードのイネーブル化 19-6

PortFast の概要 19-7

PortFast のイネーブル化 19-8

BPDU ガードの概要 19-9

BPDU ガードのイネーブル化 19-9

PortFast BPDU フィルタリングの概要 19-10

PortFast BPDU フィルタリングのイネーブル化 19-11

UplinkFast の概要 19-13

UplinkFast のイネーブル化 19-14
BackboneFast の概要 19-16
BackboneFast のイネーブル化 19-19

CHAPTER 20

EtherChannel の設定 20-1

EtherChannel の概要 20-2

ポートチャネル インターフェイス 20-2

EtherChannel の設定方法 20-3

EtherChannel 設定の概要 20-3

EtherChannel の手動設定 20-3

PAgP EtherChannel の設定 20-4

IEEE 802.3ad LACP EtherChannel 設定 20-4

ロード バランシング 20-5

EtherChannel 設定時の注意事項および制約事項 20-6

EtherChannel の設定 20-7

レイヤ 3 EtherChannel の設定 20-7

ポートチャネル論理インターフェイスの作成 20-7

物理インターフェイスのレイヤ 3 EtherChannel としての設定 20-8

レイヤ 2 EtherChannel の設定 20-10

LACP システム プライオリティおよびシステム ID の設定 20-13

EtherChannel ロード バランシングの設定 20-14

EtherChannel からのインターフェイスの削除 20-15

EtherChannel の削除 20-15

CHAPTER 21

IGMP スヌーピングとフィルタリングの設定 21-1

IGMP スヌーピングの概要 21-2

即時脱退処理 21-3

IGMP 設定可能な Leave タイマー 21-4

EHT 21-4

IGMP スヌーピングの設定 21-5

IGMP スヌーピングのデフォルト設定 21-5

IGMP スヌーピングのグローバルなイネーブル化 21-5

VLAN 上での IGMP スヌーピングのイネーブル化 21-6

学習方式の設定 21-7

PIM/DVMRP 学習方式の設定 21-7

CGMP 学習方式の設定 21-7

マルチキャスト ルータへの静的な接続の設定 21-8

IGMP 即時脱退処理のイネーブル化 21-8

IGMP Leave タイマーの設定 21-9

EHT の設定 21-10

ホストの静的な設定 21-11

マルチキャスト フラッディングの抑制 21-11

IGMP スヌーピング インターフェイスの設定 21-12

IGMP スヌーピング スイッチの設定 21-13

IGMP スヌーピング情報の表示 21-15

クエリア情報の表示 21-15

IGMP ホスト メンバシップ情報の表示 21-15

グループ情報の表示 21-16

マルチキャスト ルータ インターフェイスの表示 21-18

MAC アドレス マルチキャスト エントリの表示 21-18

VLAN インターフェイス上の IGMP スヌーピング情報の表示 21-19

IGMP フィルタリングの設定 21-20

IGMP フィルタリングのデフォルト設定 21-20

IGMP プロファイルの設定 21-20

IGMP プロファイルの適用 21-22

IGMP グループの最大数の設定 21-23

IGMP フィルタリングの設定の表示 21-25

CHAPTER 22 IPv6 MLD スヌーピングの設定 22-1

MLD スヌーピングの概要 22-2

MLD メッセージ 22-3

MLD クエリー 22-3

マルチキャスト クライアント エージングの堅牢性 22-3

マルチキャスト ルータ検出 22-4

MLD レポート 22-4

MLD Done メッセージおよび即時脱退 22-4

TCN 処理 22-5

IPv6 MLD スヌーピングの設定 22-6

MLD スヌーピングのデフォルト設定 22-6

MLD スヌーピング設定時の注意事項 22-7

MLD スヌーピングのイネーブル化またはディセーブル化 22-7

スタティックなマルチキャスト グループの設定 22-8

マルチキャスト ルータ ポートの設定 22-9

MLD 即時脱退のイネーブル化 22-10

IGMP スヌーピング クエリーの設定 22-10

MLD リスナー メッセージ抑制のディセーブル化 22-12

MLD スヌーピング情報の表示 22-13

CHAPTER 23 802.1Q およびレイヤ 2 プロトコル トンネリングの設定 23-1

802.1Q トンネリングの概要 23-2

802.1Q トンネリングの設定 23-4

802.1Q トンネリングの設定時の注意事項 23-4

ネイティブ VLAN 23-4

システム MTU 23-5

802.1Q トンネリングおよび他の機能 23-5

802.1Q トンネル ポートの設定 23-6

レイヤ2プロトコルトンネリングの概要 23-8

レイヤ2プロトコルトンネリングの設定 23-10

レイヤ 2 プロトコル トンネリングのデフォルト設定 23-11

レイヤ 2 プロトコル トンネリングの設定時の注意事項 23-11

レイヤ2トンネリングの設定 23-12

トンネリング ステータスのモニタリングおよびメンテナンス 23-14

CHAPTER 24 CDP の設定 24-1

CDP の概要 24-2

CDP の設定 24-2

CDP のグローバルなイネーブル化 24-2

CDP のグローバル設定の表示 24-2

インターフェイス上での CDP のイネーブル化 24-3

CDP インターフェイスの設定の表示 24-3

CDP のモニタリングおよびメンテナンス 24-4

CHAPTER 25 LLDP および LLDP-MED の設定 25-1

LLDP および LLDP-MED の概要 25-2

LLDP の概要 25-2

LLDP-MED の概要 25-2

LLDP および LLDP-MED の設定 25-4

デフォルトの LLDP 設定 25-4

LLDP-MED 特性の設定 25-4

LLDP のグローバルなディセーブルにおよびイネーブルに 25-5

インターフェイス上での LLDP のディセーブルおよびイネーブル 25-6

LLDP-MED TLV の設定 25-7

LLDP と LLDP-MED のモニタリングおよびメンテナンス 25-8

CHAPTER 26 UDLD の設定 26-1

UDLD の概要 26-2

UDLD のデフォルト設定 26-3

スイッチ上での UDLD の設定 26-3
UDLD のグローバルなイネーブル化 26-3
インターフェイス上で UDLD をイネーブルにする方法 26-4
光ファイバ以外のインターフェイス上での UDLD のディセーブル化 26-4
光ファイバ インターフェイス上での UDLD のディセーブル化 26-4
ディセーブルになったインターフェイスのリセット 26-4

CHAPTER 27 レイヤ 3 インターフェイスの設定 27-1

レイヤ 3 インターフェイスの概要 27-2 論理レイヤ 3 VLAN インターフェイス 27-2 物理レイヤ 3 インターフェイス 27-3 SVI 自動ステート除外の概要 27-3 レイヤ 3 インターフェイス カウンタの概要 27-4

設定時の注意事項 27-6

IP MTU サイズの設定

論理レイヤ 3 VLAN インターフェイスの設定 27-7 レイヤ 3 インターフェイスとしての VLAN の設定 27-9

SVI 自動ステート除外の設定 27-9

レイヤ 3 インターフェイス カウンタの設定 27-12

27-10

物理レイヤ 3 インターフェイスの設定 27-14

EIGRP スタブ ルーティングの設定 27-15

概要 27-15

EIGRP スタブ ルーティングの設定方法 27-16 デュアルホーム リモート トポロジ 27-17 EIGRP スタブ ルーティングの設定作業リスト 27-20

EIGRP のモニタリングおよびメンテナンス 27-21

EIGRP の設定例 27-21

経路集約の例 27-21

ルート認証の例 27-22

スタブ ルーティングの例 27-22

CHAPTER 28 CEF の設定 28-1

CEF の概要 28-2

CEF の利点 28-2

FIB 28-2

隣接関係テーブル 28-2

隣接関係の検出 28-3

隣接関係の解決 28-3

特殊な処理が必要な隣接関係タイプ 28-3

Catalyst 4500 シリーズ スイッチ Cisco IOS ソフトウェア コンフィギュレーション ガイド

未解決の隣接関係 28-3

Catalyst 4500 シリーズ スイッチでの CEF の実装 28-4

ハードウェアおよびソフトウェアのスイッチング 28-4

ハードウェア スイッチング 28-5

ソフトウェア スイッチング 28-5

ロード バランシング 28-6

ソフトウェア インターフェイス 28-6

CEF 設定の制限事項

CEF の設定 28-7

> CEF のイネーブル化 28-7

CEF のロード バランシングの設定 28-7

宛先別ロード バランシングの設定 28-7

負荷分散型ハッシュ機能の設定 28-8

CEF 情報の表示 28-8

CEF のモニタリングおよびメンテナンス 28-9

IP 統計情報の表示 28-9

ユニキャスト RPF の設定 CHAPTER 29 29-1

章の内容 29-1

ユニキャスト RPF について 29-2

ユニキャスト RPF の概要

ユニキャスト RPF の実装 29-4

> セキュリティ ポリシーとユニキャスト RPF 29-5

29-2

ユニキャスト RPF を使用する場所 29-5

ルーティング テーブルの要件 29-8

ユニキャスト RPF を使用できない場所

BOOTP および DHCP を使用したユニキャスト RPF 29-9

制約事項 29-9

関連機能および技術 29-9

ユニキャスト RPF 設定の前提条件 29-10

ユニキャスト RPF の設定作業リスト 29-11

ユニキャスト RPF の設定 29-11

ユニキャスト RPF の確認 29-12

ユニキャスト RPF のモニタリングおよびメンテナンス 29-13

ユニキャスト RPF の設定例 29-15

専用線集約ルータでのユニキャスト RPF の例 29-15

Cisco AS5800 でのダイヤルアップ ポートを使用したユニキャスト RPF の例 29-15

着信および発信フィルタを使用したユニキャスト RPF の例 29-15

ACL およびロギングを使用したユニキャスト RPF の例 29-16

CHAPTER 30 単一方向イーサネットの設定 30-1

単一方向イーサネットの概要 30-2 単一方向イーサネットの設定 30-2

CHAPTER 31 IP マルチキャストの設定 31-1

IP マルチキャストの概要 31-2

IP マルチキャスト プロトコル 31-3

IGMP 31-3

PIM 31-3

IGMP スヌーピングおよび CGMP 31-4

Catalyst 4500 シリーズ スイッチ上での IP マルチキャスト 31-5

CEF、MFIB、およびレイヤ2フォワーディング 31-6

IP マルチキャスト テーブル 31-8

ハードウェアおよびソフトウェアによる転送 31-9

非 RPF トラフィック 31-10

マルチキャスト高速ドロップ 31-11

MFIB 31-12

S/M,224/4 **31-13**

サポートされない機能 31-13

IP マルチキャスト ルーティングの設定 31-14

IP マルチキャスト ルーティングのデフォルト設定 31-14

IP マルチキャスト ルーティングのイネーブル化 31-15

インターフェイス上での PIM のイネーブル化 31-15

稠密モードのイネーブル化 31-15

希薄モードのイネーブル化 31-16

希薄/稠密モードのイネーブル化 31-16

IP マルチキャスト ルーティングのモニタリングおよびメンテナンス 31-17

システムおよびネットワーク統計情報の表示 31-17

マルチキャスト ルーティング テーブルの表示 31-18

IP MFIB の表示 31-21

IP MFIB 高速ドロップの表示 31-22

PIM 統計情報の表示 31-22

テーブルおよびデータベースの削除 31-23

設定例 31-24

PIM 稠密モードの例 31-24

PIM 希薄モードの例 31-24

BSR の設定例 31-24

CHAPTER 32 PBR の設定 32-1

PBR の概要 32-2

PBR の概要 32-2

PBR フロー スイッチングの概要 32-2

PBR の使用 32-3

PBR の設定作業リスト 32-4

PBR のイネーブル化 32-4

ローカル PBR のイネーブル化 32-5

サポートされない機能 32-5

PBR の設定例 32-6

同等アクセス例 32-6

ネクスト ホップを変更する例 32-7

ACE の拒否例 32-7

CHAPTER 33 VRF-Lite の設定 33-1

VRF-Lite の概要 33-2

VRF-Lite のデフォルト設定 33-4

VRF-Lite 設定時の注意事項 33-4

VRF の設定 33-5

VPN ルーティング セッションの設定 33-6

CE ルーティング セッションへの BGP PE の設定 33-7

VRF-Lite の設定例 33-8

スイッチ S8 の設定 33-8

スイッチ S20 の設定 **33-10**

スイッチ S11 の設定 33-10

PE スイッチ S3 の設定 33-11

VRF-Lite ステータスの表示 33-12

CHAPTER 34 QoS の設定 34-1

Catalyst 4500 シリーズ スイッチでの QoS の概要 34-2

プライオリティ 34-2

QoS の用語 34-4

QoS の基本モデル 34-6

分類 34-7

QoS ACL に基づく分類 34-9

クラス マップおよびポリシー マップに基づく分類 34-10

ポリシングおよびマーキング 34-10

内部 DSCP 值 34-14

マッピング テーブル 34-15

キューイングおよびスケジューリング 34-15

AQM 34-15

送信キュー間のリンク帯域幅の共有 34-16

ストリクト プライオリティ / 低遅延キューイング 34-16

トラフィック シェーピング 34-17

パケットの変更 34-17

PVQoS 34-17

QoS およびソフトウェア処理されるパケット 34-17

Supervisor Engine II-Plus、II+10GE、VI、V、V-10GE、4924、4948、および4948-10GE での Auto-QoS の設定 34-19

生成される Auto-QoS 設定 34-19

Auto-QoS の設定上の影響 34-20

設定時の注意事項 34-21

VoIP 用の Auto-QoS のイネーブル化 34-21

Auto-QoS 情報の表示 34-22

Auto-QoS 設定例 34-22

Supervisor Engine II-Plus、II+10GE、VI、V、V-10GE、4924、4948、および4948-10GE での QoS の設定 34-25

QoS のデフォルト設定 34-26

設定時の注意事項 34-27

QoS のグローバルなイネーブル化 34-27

信頼境界の設定によるポート セキュリティの確保 34-28

DBL のイネーブル化 34-29

DBL のグローバルなイネーブル化 34-30

DBL の選択的イネーブル化 34-30

名前付き集約ポリサーの作成 34-33

QoS ポリシーの設定 34-35

QoS ポリシー設定の概要 34-35

クラス マップの設定(任意) 34-36

ポリシー マップの設定 34-38

インターフェイスへのポリシー マップの付加 34-43

CoS 変換の設定 34-44

UBRL の設定 34-45

例 34-46

階層型ポリサーの設定 34-50

PVQoS のイネーブル化 34-52

インターフェイス上での QoS のイネーブル化またはディセーブル化 34-55 レイヤ 2 インターフェイス上での VLAN ベース QoS の設定 34-55 インターフェイスの信頼状態の設定 34-56 インターフェイスの CoS 値の設定 34-57 インターフェイスの DSCP 値の設定 34-58

送信キューの設定 34-59

DSCP 値から特定の送信キューへのマッピング 34-59

送信キュー間での帯域幅の割り当て 34-60

送信キューのトラフィック シェーピングの設定 34-60

ハイ プライオリティ送信キューの設定 34-61

DSCP マップの設定 34-61

CoS/DSCP マップの設定 34-61

ポリシング済み DSCP マップの設定 34-62

DSCP/CoS マップの設定 34-63

レイヤ 2 制御パケット QoS のイネーブル化 34-64

使用上の注意事項 34-68

機能の相互作用 34-69

Supervisor Engine 6-E での Auto-QoS の設定 34-70

Supervisor Engine 6-E での QoS の設定 34-72

MQC ベースの QoS の設定 34-72

概要 34-72

プラットフォームでサポートされる分類基準および QoS 機能 34-74

プラットフォーム ハードウェアの機能 34-75

QoS サービス ポリシーを適用するための前提条件 34-75

QoS サービス ポリシーの適用に関する制約事項 34-75

分類 34-75

ポリシング 34-76

ポリシングの実装方法 34-77

プラットフォームの制約事項 34-77

ネットワーク トラフィックのマーク付け 34-77

ネットワーク トラフィックのマーク付け 34-77

アクション ドライバのマーク付け 34-80

トラフィック マーキング手順のフローチャート 34-80

ネットワーク トラフィックのマーク付けに関する制約事項 34-81

マルチ属性マーキングのサポート 34-81

マーキング用のハードウェア機能 34-82

ポリシー マップ マーキング アクションの設定 34-82

マーキング統計 34-84

シェーピング、共有(帯域幅) プライオリティ キュー、キュー制限、および DBL 34-84

シェーピング 34-84

共有(帯域幅) 34-86

プライオリティ キューイング 34-89 キュー制限 34-91 DBL を経由した AQM 34-93 伝送キューの統計 34-95 階層型ポリシー 34-95 ポリシーの関連付け 34-97 ソフトウェア QoS 34-98

 CHAPTER 35
 音声インターフェイスの設定
 35-1

音声インターフェイスの概要 35-2

Cisco IP Phone の音声トラフィック 35-2

Cisco IP Phone のデータ トラフィック 35-3

Cisco 7960 IP Phone への接続用のポートの設定 35-4

音声およびデータ トラフィック用の音声ポートの設定 35-5

着信フレームの CoS プライオリティの変更 35-7

電力の設定 35-7

 CHAPTER 36
 PVLAN の設定
 36-1

コマンド リスト 36-2

PVLAN の概要 36-3

定義一覧 36-4

複数のスイッチの PVLAN 36-5

標準トランク ポート 36-5

PVLAN トランク 36-6

PVLAN と他の機能との相互作用 36-8

PVLAN & VLAN ACL/QoS 36-8

PVLAN とユニキャスト、ブロードキャスト、およびマルチキャスト トラフィック 36-8

PVLAN と SVI 36-9

PVLAN の設定 36-10

PVLAN の設定手順 36-10

PVLAN のデフォルト設定 36-11

PVLAN 設定時の注意事項および制約事項 36-11

PVLAN としての VLAN の設定 36-13

セカンダリ VLAN のプライマリ VLAN との関連付け 36-14

レイヤ 2 インターフェイスの PVLAN 混合モード ポートとしての設定 36-15

レイヤ 2 インターフェイスの PVLAN ホスト ポートとしての設定 36-16 レイヤ 2 インターフェイスの PVLAN トランク ポートとしての設定 36-17 レイヤ 2 インターフェイスの PVLAN 混合モード トランク ポートとしての設定 36-19

セカンダリ VLAN 入力トラフィックのルーティングの許可 36-21

CHAPTER 37 802.1X ポートペース認証の設定 37-1

802.1X ポートベース認証の概要 37-2

装置の役割 37-3

802.1X とネットワーク アクセス コントロール 37-4

認証の開始とメッセージ交換 37-4

許可ステートおよび無許可ステートのポート 37-5

802.1X ホストモード 37-7

VLAN 割り当てを使用した 802.1X 認証の利用 37-7

ゲスト VLAN を使用した 802.1X 認証の使用 37-9

ゲスト VLAN を使用した 802.1X 認証の使用上の注意事項 37-9

Windows XP ホスト上でのゲスト VLAN 使用 802.1X 認証の使用上の注意 事項 37-9

MAC 認証バイパスを使用した 802.1X 認証の利用 37-10

機能の相互作用 37-10

アクセス不能認証バイパスを使用した 802.1X 認証の利用 37-12

単方向制御ポートを使用した 802.1X 認証の利用 37-12

単方向ステート 37-13

双方向ステート 37-13

認証失敗 VLAN 割り当てを使用した 802.1X 認証の利用 37-13

認証失敗 VLAN 割り当ての使用上の注意事項 37-14

ポート セキュリティを使用した 802.1X 認証の利用 37-15

RADIUS によるセッション タイムアウトを使用した 802.1X 認証の利用 37-16

RADIUS アカウンティングを使用した 802.1X 認証の利用 37-16

音声 VLAN ポートを使用した 802.1X 認証の利用 37-19

複数ドメイン認証の使用 37-20

サポート対象トポロジ 37-21

802.1X の設定 37-22

802.1X のデフォルト設定 37-23

802.1X 設定時の注意事項 37-23

802.1X 認証のイネーブル化 37-24

スイッチ /RADIUS サーバ通信の設定 37-26

複数ドメイン認証の設定 37-28

RADIUS によるセッション タイムアウトの設定 37-31

802.1X RADIUS アカウンティングのイネーブル化 37-32

ゲスト VLAN を使用した 802.1X 認証の設定 37-33

MAC 認証バイパスを使用した 802.1X 認証の設定 37-36 アクセス不能認証バイパスを使用した 802.1X 認証の設定 37-37 単方向制御ポートを使用した 802.1X 認証の設定 認証失敗 VLAN 割り当てを使用した 802.1X 認証の設定 37-41 音声 VLAN に対する 802.1X 認証の設定 37-43 定期的再認証のイネーブル化 37-44 複数ホストのイネーブル化 37-45 待機時間の変更 37-46 スイッチ / クライアント間の再送信時間の変更 37-47 スイッチ/クライアント間のフレーム再送信回数の設定 37-48 手動によるポート接続クライアントの再認証 37-49 802.1X 認証ステートの初期化 37-50 802.1X クライアント情報の削除 37-50 802.1X 設定をデフォルト値にリセットする方法 37-50 802.1X 統計情報およびステータスの表示

______ ポート セキュリティの設定 38-1

コマンド リスト 38-2

ポート セキュリティの概要 38-4

セキュア MAC アドレス 38-4

セキュア MAC アドレスの最大数 38-5

セキュア MAC アドレスのエージング 38-5

ポートのスティッキ アドレス 38-6

違反処理 38-7

無効なパケット操作 38-7

アクセス ポート上のポート セキュリティ 38-8

アクセス ポート上のポート セキュリティの設定 38-8

例 38-11

例 1:最大セキュア アドレス数の設定 38-12

例 2: 違反モードの設定 38-12

例 3: エージング タイマーの設定 38-12

例 4:エージング タイマーのタイプの設定 38-13

例 5: セキュア MAC アドレスの設定 38-13

例 6: スティッキ ポート セキュリティの設定 38-14

例7:不良パケットに対するレート制限の設定 38-14

例 8: ダイナミック セキュア MAC アドレスの削除 38-15

PVLAN ポートのポート セキュリティ 38-16

独立 プライベート VLAN ホスト ポートでのポート セキュリティの設定 38-16

Catalyst 4500 シリーズ スイッチ Cisco IOS ソフトウェア コンフィギュレーション ガイド

独立 PVLAN ホスト ポートでのポート セキュリティの例 38-17

PVLAN 混合モード ポートでのポート セキュリティの設定 38-18

PVLAN 混合モード ポートでのポート セキュリティの例 38-18

トランク ポートのポート セキュリティ 38-19

トランク ポート セキュリティの設定 38-19

トランク ポート セキュリティの例 38-21

例 1: すべての VLAN での最大セキュア MAC アドレス制限の設定 38-22

例 2: 特定の VLAN での最大セキュア MAC アドレス制限の設定 38-22

例 3: VLAN 範囲でのセキュア MAC アドレスの設定 38-23

トランク ポート セキュリティの注意事項および制約事項 38-23

ポート モードの変更 38-24

音声ポート上のポート セキュリティ 38-25

音声ポート上のポート セキュリティの設定 38-25

音声ポート セキュリティの例 38-27

例 1:音声 VLAN およびデータ VLAN への最大 MAC アドレスの設定 38-28

例 2:音声 VLAN およびデータ VLAN へのスティッキ MAC アドレスの設定 38-29

音声ポート セキュリティの注意事項および制約事項 38-30

ポート セキュリティ設定の表示 38-31

例 38-31

例 1:スイッチ全体のセキュリティ設定の表示 38-32

例 2: インターフェイスのセキュリティ設定の表示 38-32

例 3: スイッチ全体のすべてのセキュア アドレスの表示 38-33

例 4: インターフェイス上の最大 MAC アドレス数の表示 38-33

例 5: VLAN 範囲に対するインターフェイス上のセキュリティ設定の表示 38-33

例 6:インターフェイスのセキュア MAC アドレスおよびエージング情報 の表示 38-34

例 7: インターフェイスの VLAN 範囲でのセキュア MAC アドレスの表示 38-34

他の機能/環境でのポート セキュリティの設定 38-35

DHCP および IP ソース ガード 38-35

802.1X 認証 38-36

ワイヤレス環境でのポート セキュリティの設定 38-36

レイヤ 2 EtherChannel でのポート セキュリティの設定 38-37

ポート セキュリティの注意事項および制約事項 38-38

CHAPTER 39 コントロール プレーン ポリシングの設定 39-1

CoPP 機能の概要 39-2

コントロール プレーン ポリシングの注意事項 39-4

CoPP のデフォルト設定 39-5

CoPP の設定 39-5

コントロール プレーン トラフィックの CoPP を設定 39-5

データ プレーンおよび管理プレーン トラフィックの CoPP の設定 39-6

CoPP 設定時の注意事項および制約事項 39-9

CoPP のモニタリング 39-10

CHAPTER 40 DHCP スヌーピング、IP ソース ガード、およびスタティック ホストの IPSG の設定 40-1

DHCP スヌーピングの概要 40-2

信頼送信元と信頼できない送信元 40-2

DHCP スヌーピング データベース エージェントの概要 40-3

オプション 82 データ挿入 40-4

スイッチ上での DHCP スヌーピングの設定 40-8

DHCP スヌーピングのデフォルト設定 40-8

DHCP スヌーピングのイネーブル化 40-9

集約スイッチ上での DHCP スヌーピングの設定 40-11

DHCP スヌーピングとオプション 82 のイネーブル化 40-11

PVLAN 上での DHCP スヌーピングのイネーブル化 40-13

DHCP スヌーピング データベース エージェントのイネーブル化 40-13

データベース エージェントの設定例 40-14

例 1: データベース エージェントのイネーブル化 40-14

例 2:TFTP ファイルからのバインディング エントリの読み取り

40-15

例 3: DHCP スヌーピング データベースへの情報の追加 40-17

DHCP スヌーピング情報の表示 40-18

バインディング テーブルの表示 40-18

DHCP スヌーピング設定の表示 40-18

IP ソース ガードの概要 40-19

スイッチ上での IP ソース ガードの設定 40-20

PVLAN トでの IP ソース ガードの設定 40-21

IP ソース ガード情報の表示 40-22

IP 送信元バインディング情報の表示 40-24

スタティック ホストの IP ソース ガードの設定 40-25

レイヤ 2 アクセス ポート上のスタティック ホストの IPSG 40-26

PVLAN ホスト ポート上のスタティック ホストの IPSG 40-29

Catalyst 4500 シリーズ スイッチ Cisco IOS ソフトウェア コンフィギュレーション ガイド

CHAPTER 41 DAI の設定 41-1

DAI の概要 41-2

ARP キャッシュのポイズニング 41-2

DAI の目的 41-3

インターフェイスの信頼状態、セキュリティ適用範囲、およびネットワーク の構成 41-3

スタティック バインディング DHCP スヌーピングのエントリの相対的なプライオリティ 41-4

ドロップされたパケットのロギング 41-4

ARP パケットのレート制限 41-5

ポート チャネルとその動作 41-5

DAI の設定 41-6

DHCP 環境での DAI の設定 41-6

スイッチ A 41-8

スイッチ B 41-10

非 DHCP 環境に対する ARP ACL の設定 41-11

ログ バッファの設定 41-15

着信 ARP パケットのレート制限 41-18

確認検査の実行 41-20

CHAPTER 42 ACL によるネットワーク セキュリティの設定 42-1

ACL の概要 42-2

ACL の概要 42-2

ACL を使用するサポート対象機能 42-3

ルータ ACL 42-3

PACL 42-4

VLAN マップ 42-5

ハードウェアおよびソフトウェア ACL のサポート 42-6

TCAM プログラミングと Supervisor Engine II-Plus、Supervisor Engine IV、Supervisor Engine V、および Supervisor Engine V-10GE の ACL 42-7

TCAM プログラミング アルゴリズム 42-8

プログラミング アルゴリズムの変更 42-9

TCAM リージョンのサイズ変更 42-11

ACL による高 CPU のトラブルシューティング 42-12

制御パケットのキャプチャのモード選択 42-13

注意事項および制限事項 42-14

設定 42-14

Supervisor Engine 6-E の TCAM プログラミングと ACL 42-16

ACL のレイヤ 4 演算 42-16

レイヤ 4 演算の制約事項 42-16

レイヤ 4 演算設定時の注意事項 42-17

ACL 処理が CPU に与える影響 42-18

ユニキャスト MAC アドレス フィルタリングの設定 42-20

名前付き MAC 拡張 ACL の設定 42-20

名前付き IPv6 ACL の設定 42-22

レイヤ 3 インターフェイスへの IPv6 ACL の適用 42-23

VLAN マップの設定 42-24

VLAN マップ設定時の注意事項 42-25

VLAN マップの作成および削除 42-25

ACL および VLAN マップの例 42-26

VLAN への VLAN マップの適用 42-28

ネットワークでの VLAN マップの使用方法 42-28

別の VLAN にあるサーバへのアクセスの拒否 42-30

VLAN アクセス マップ情報の表示 42-31

ルータ ACL を VLAN マップと併用する方法 42-32

ルータ ACL を VLAN マップと併用する場合の注意事項 42-32

VLAN に適用されるルータ ACL と VLAN マップの例 42-32

ACL およびスイッチド パケット 42-32

ACL およびルーテッド パケット 42-33

PACL の設定 42-34

PACL の作成 42-34

PACL 設定時の注意事項 42-34

レイヤ 2 インターフェイス上での IP ACL と MAC ACL の設定 42-35

アクセス グループ モードを PACL と併用する方法 42-35

レイヤ 2 インターフェイス上でのアクセス グループ モードの設定 42-36

レイヤ2インターフェイスへの ACL の適用 42-36

レイヤ 2 インターフェイス上の ACL 設定の表示 42-37

VLAN マップおよびルータを PACL と併用する方法 42-38

CHAPTER 43 ポート ユニキャストおよびマルチキャスト フラッディング ブロック 43-1

フラッディング ブロックの概要 43-1

ポート ブロックの設定 43-2

インターフェイス上でのフラッディングするトラフィックのブロック 43-2

ポート上での通常の転送の再開 43-3

CHAPTER 44 ストーム制御の設定 44-1

ストーム制御の概要 44-2

ハードウェアベースのストーム制御実装 44-2 ソフトウェアベースのストーム制御実装 44-3 ブロードキャスト ストーム制御のイネーブル化 44-4 マルチキャスト ストーム制御のイネーブル化 44-6 スーパーバイザ エンジン 6-E でのマルチキャスト抑制 WS-X4516 スーパーバイザ エンジンでのマルチキャスト抑制 44-7 WS-X4515、WS-X4014、および WS-X4013+ スーパーバイザ エンジンでの マルチキャスト抑制 ブロードキャスト ストーム制御のディセーブル化 44-8 マルチキャスト ストーム制御のディセーブル化 ストーム制御の表示 44-10

CHAPTER 45 SPAN と RSPAN の設定 45-1

SPAN と RSPAN の概要 45-2

SPAN と RSPAN の概念と用語 45-3

SPAN セッション 45-3

トラフィック タイプ 45-4

送信元ポート 45-5

宛先ポート 45-5

VSPAN 45-6

SPAN トラフィック 45-6

SPAN と RSPAN のセッション限度 45-6

SPAN と RSPAN のデフォルト設定 45-7

SPAN の設定 45-8

SPAN 設定時の注意事項および制約事項 45-8

SPAN 送信元の設定 45-9

SPAN 宛先の設定 45-10

トランク インターフェイス上の送信元 VLAN のモニタリング 45-10

設定例 45-11

SPAN の設定の確認 45-11

CPU ポートのスニッフィング 45-12

カプセル化の設定 45-14

入力パケット 45-14

アクセス リスト フィルタリング 45-16

ACL 設定時の注意事項 45-16

アクセス リスト フィルタリングの設定 45-17

パケット タイプ フィルタリング 45-18

設定例 45-19

RSPAN の設定 45-20

RSPAN 設定時の注意事項 45-20

RSPAN セッションの作成 45-21

RSPAN 宛先セッションの作成 45-23

RSPAN 宛先セッションの作成および入力トラフィックのイネーブル化 45-24

RSPAN セッションからのポートの削除 45-25

監視する VLAN の指定 45-26

フィルタリングする VLAN の指定 45-28

SPAN および RSPAN ステータスの表示 45-30

CHAPTER 46 システム メッセージ ロギングの設定 46-1

システム メッセージ ロギングの概要 46-2

システム メッセージ ロギングの設定 46-3

システム ログ メッセージの形式 46-3

システム メッセージ ロギングのデフォルト設定 46-4

メッセージ ロギングのディセーブル化 46-4

メッセージ表示先装置の設定 46-5

ログ メッセージの同期化 46-6

ログ メッセージのタイムスタンプのイネーブル化およびディセーブル化 46-8

ログ メッセージのシーケンス番号のイネーブル化およびディセーブル化 46-8

メッセージの重大度の定義 46-9

履歴テーブルおよび SNMP への Syslog メッセージの送信制限 46-10

UNIX Syslog サーバの設定 46-11

UNIX Syslog デーモンへのメッセージ ロギング 46-11

UNIX システム ロギング ファシリティの設定 46-12

ロギング設定の表示 46-13

CHAPTER 47 SNMP の設定 47-1

SNMP の概要 47-2

SNMP のバージョン 47-2

SNMP マネージャの機能 47-4

SNMP エージェントの機能 47-4

SNMP コミュニティ ストリング 47-4

SNMP を使用した MIB 変数へのアクセス 47-5

SNMP 通知 47-5

SNMP の設定 47-6

SNMP のデフォルト設定 47-6

SNMP 設定時の注意事項 47-6

Catalyst 4500 シリーズ スイッチ Cisco IOS ソフトウェア コンフィギュレーション ガイド

SNMP エージェントのディセーブル化 47-7

コミュニティ ストリングの設定 47-7

SNMP グループおよびユーザの設定 47-9

SNMP 通知の設定 47-11

エージェントの連絡先および設置場所の設定 47-15

SNMP で使用する TFTP サーバの限定 47-15

SNMP の例 47-16

SNMP ステータスの表示 47-18

CHAPTER 48 NetFlow の設定 48-1

NetFlow 統計情報収集機能の概要 48-2

NDE バージョン 48-2

ハードウェアから取得する情報 48-4

ソフトウェアから取得する情報 48-4

入力および出力インターフェイス番号と AS 番号の割り当て 48-4

予測フィールドの割り当て 48-4

出力インターフェイスおよび出力関連予測フィールドの割り当て 48-4

入力インターフェイスおよび入力関連予測フィールドの割り当て

UBRL およびマイクロフロー ポリシングと Netflow 統計情報の機能の相互作用 48-5

VLAN の統計情報 48-6

NetFlow 統計情報収集機能の設定 48-7

必要なハードウェアの確認 48-7

NetFlow 統計情報収集機能のイネーブル化 48-8

スイッチド / ブリッジド IP フローの設定 48-8

NetFlow 統計情報のエクスポート 48-10

NetFlow 統計情報収集機能の管理 48-10

集約キャッシュの設定 48-10

集約キャッシュ設定およびデータ エクスポートの確認 48-11

ルータベース集約の NetFlow 最小プレフィクス マスクの設定 48-11

prefix 集約方式の最小マスクの設定 48-12

destination-prefix 集約方式の最小マスクの設定 48-12

source-prefix 集約方式の最小マスクの設定 48-12

集約方式の最小マスクのモニタおよび保守 48-12

NetFlow エージング パラメータの設定 48-13

NetFlow 統計情報収集機能の設定例 48-14

NetFlow の設定例 48-15

NetFlow イネーブル化方式のサンプル 48-15

NetFlow 集約設定のサンプル 48-15

48-5

AS の設定 48-16

宛先プレフィクスの設定 48-16

プレフィクスの設定 48-16

プロトコル ポートの設定 48-16

送信元プレフィクスの設定 48-16

ルータベース集約方式の NetFlow 最小プレフィクス マスクのサンプル 48-17

prefix 集約方式 48-17

destination-prefix 集約方式 48-17

source-prefix 集約方式 48-17

RMON の概要 49-2

RMON の設定 49-4

デフォルトの RMON 設定 49-4

RMON アラームとイベントの設定 49-4

インターフェイス設定する RMON 収集 49-5

RMON ステータスの表示 49-7

_______ **診断の実行** 50-1

オンライン診断 50-1

オンライン診断によるトラブルシューティング 50-2

POST 診断 50-3

概要 50-4

POST 結果のサンプル **50-4**

Supervisor Engine V-10GE の POST 結果 50-9

アクティブ スーパーバイザ エンジン上での POST 50-9

アクティブ スーパーバイザ エンジンの POST 結果のサンプル

スタンバイ スーパーバイザ エンジン上での POST 50-11

スタンバイ スーパーバイザ エンジンの POST 表示のサンプル 50-12

障害の原因およびトラブルシューティング 50-14

CHAPTER 51 WCCP パージョン 2 サービスの設定 51-1

WCCP の概要 51-2

WCCP の概要 51-2

ハードウェア アクセラレーション 51-2

WCCP 構成の概要 51-3

WCCP の機能 51-4

HTTP および非 HTTP サービスのサポート 51-4

50-9

複数ルータのサポート 51-5 MD5 セキュリティ 51-5

ウェブ コンテンツ パケットの返送 51-5

WCCP の制約事項 51-6

WCCP の設定 51-7

WCCP を使用したサービス グループの設定 51-7

Web キャッシュ サービスの指定 51-8

WCCP サービス グループに対するアクセス リストの使用 51-9

ルータおよびキャッシュ エンジンへのパスワードの設定 51-9

WCCP 設定値の確認およびモニタリング 51-10

WCCP の設定例 51-11

一般的な WCCP 設定の実行例 51-11

Web キャッシュ サービスの実行例 51-11

リバース プロキシ サービスの実行例 51-11

アクセス リストの使用例 51-11

スイッチおよびコンテント エンジンへのパスワードの設定例 51-12

WCCP 設定の確認例 51-12

CHAPTER 52 MIB サポートの設定 52-1

Cisco IOS リリースの MIB サポートの判断 52-1

Cisco IOS MIB ツールの使用 52-2

MIB のダウンロードおよびコンパイル 52-3

MIB を扱う際の考慮事項 52-3

MIB のダウンロード 52-4

MIB のコンパイル 52-4

SNMP サポートのイネーブル化 52-5

CHAPTER 53 ROM モニタ 53-1

ROM モニタの設置 53-2

ROM モニタ コマンド 53-2

コマンドの説明 53-3

コンフィギュレーション レジスタ 53-4

コンフィギュレーション レジスタの手動での変更 53-4

コンフィギュレーション レジスタのプロンプトでの変更 53-4

コンソール ダウンロード 53-6

エラー レポート 53-6

デバッグ コマンド 53-7

ROM モニタの終了 53-7

APPENDIX A 略語 A-1

INDEX 索引

Contents



はじめに

ここでは、このマニュアルの対象読者、マニュアルの構成、および手順や情報を記述するための表記法について説明します。また、シスコ製品のマニュアルを入手する方法とテクニカル サポートについても説明します。

対象読者

このマニュアルは、Catalyst 4500 シリーズ スイッチの設定および保守を担当する、経験豊富なネットワーク管理者を対象としています。

OL-15342-01-J

マニュアルの構成

このマニュアルは、次の章から構成されています。

章	タイトル	説明
第1章	製品概要	Catalyst 4500 シリーズ スイッチ向け Cisco IOS ソフトウェアの概要を示します。
第2章	CLI	CLI (コマンドライン インターフェイス)の使い方 を説明します。
第3章	スイッチの初期設定	スイッチの基本設定の手順について説明します。
第4章	スイッチの管理	スイッチを管理する方法について説明します。
第5章	Cisco IOS ISSU プロセスの設定	スイッチに ISSU を設定する方法について説明します。
第6章	インターフェイスの設定	ファスト イーサネット、ギガビット イーサネット、 10 ギガビット イーサネット インターフェイス上で、 特定のレイヤに限定されない機能を設定する方法に ついて説明します。
第7章	ポートのステータスと接続の確 認	モジュールとインターフェイスのステータスを確認 する方法について説明します。
第8章	RPR および SSO を使用したスーパーバイザ エンジンの冗長設定	Catalyst 4507R および 4510R スイッチ上に、Router Processor Redundancy (RPR)と Stateful Switchover (SSO)を設定する方法について説明します。
第9章	Cisco NSF/SSO スーパーバイザ エンジンの冗長構成の設定	SSO を備えた Cisco Nonstop Forwarding (NSF) を使用して、スーパーバイザ エンジンの冗長性を設定する方法について説明します。
第 10 章	環境モニタリングおよび電源管 理	電力管理機能および環境モニタリング機能の設定方法について説明します。
第 11 章	PoE の設定	Power over Ethernet (PoE) の設定方法について説明 します。
第 12 章	Cisco Network Assistant による Catalyst 4500 シリーズ スイッチ の設定	Network Assistant および組み込み CiscoView のインストール方法と設定方法について説明します。
第 13 章	VLAN、VTP、および VMPS の設定	VLAN(仮想 LAN)、VLAN Trunking Protocol(VTP; VLAN トランキング プロトコル)、および VLAN Management Policy Server(VMPS; VLAN マネジメン ト ポリシー サーバ)の設定方法について説明しま す。
第 14 章	IP アンナンバード インターフェ イスの設定	IP Unnumbered サポートを設定する方法について説明します。
第 15 章	レイヤ 2 イーサネット インター フェイスの設定	VLAN トランクなど、レイヤ 2 機能をサポートする ようにインターフェイスを設定する方法について説 明します。
第 16 章	SmartPort マクロの設定	SmartPort マクロを設定する方法について説明します。
第 17 章	STP および MST の設定	Spanning-Tree Protocol (STP; スパニングツリー プロトコル) および Multiple Spanning-Tree (MST) プロトコルの設定方法、これらのスパニングツリーの動作方法について説明します。

章	タイトル	説明
第 18 章	Resilient Ethernet Protocol の設定	Resilient Ethernet Protocol(REP)の設定方法について説明します。
第 19 章	任意の STP 機能の設定	スパニングツリー PortFast、UplinkFast、BackboneFast、およびその他の STP 機能の設定方法について説明します。
第 20 章	EtherChannel の設定	レイヤ 2 およびレイヤ 3 EtherChannel ポート バンドルの設定方法について説明します。
第 21 章	IGMP スヌーピングとフィルタリ ングの設定	Internet Group Management Protocol (IGMP; インターネット グループ管理プロトコル)スヌーピングの設定方法について説明します。
第 22 章	IPv6 MLD スヌーピングの設定	IPv6 MLD スヌーピングの設定方法について説明します。
第 23 章	802.1Q およびレイヤ 2 プロトコルトンネリングの設定	802.1Q およびレイヤ 2 プロトコル トンネリングの 設定方法について説明します。
第 24 章	CDP の設定	Cisco Discovery Protocol (CDP; シスコ検出プロトコル)の設定方法について説明します。
第 25 章	LLDP および LLDP-MED の設定	Link Layer Discovery Protocol (LLDP)の設定方法について説明します。
第 26 章	UDLD の設定	UniDirectional Link Detection(UDLD; 単一方向リンク検出)プロトコルの設定方法について説明します。
第 27 章	レイヤ 3 インターフェイスの設 定	レイヤ 3 機能をサポートするようにインターフェイ スを設定する方法について説明します。
第 28 章	CEF の設定	IP ユニキャスト トラフィック用 Cisco Express Forwarding(CEF; シスコエクスプレス フォワーディ ング)の設定方法について説明します。
第 29 章	ユニキャスト RPF の設定	ユニキャスト Reverse Path Forwarding (RPF)の設定 方法について説明します。
第 30 章	単一方向イーサネットの設定	単一方向イーサネットを設定する方法について説明 します。
第 31 章	IP マルチキャストの設定	IP Multicast Multilayer Switching (MMLS; マルチキャスト マルチレイヤ スイッチング)の設定方法について説明します。
第 32 章	PBR の設定	Policy-Based Routing(PBR; ポリシーベース ルーティング) の設定方法について説明します。
第 33 章	VRF-Lite の設定	Customer Edge (CE; カスタマー エッジ)デバイスに Multiple VPN Routing/Forwarding (Multi-VRF)インス タンスを設定する方法について説明します。
第 34 章	QoS の設定	QoS (Quality Of Service) の設定方法について説明します。
第 35 章	音声インターフェイスの設定	音声インターフェイスを設定する方法について説明 します。
第 36 章	PVLAN の設定	プライベート VLAN を設定および修正する方法に ついて説明します。
第 37 章	802.1X ポートベース認証の設定	802.1X ポートベースの認証の設定方法について説明します。

童	タイトル	説明
第 38 章	ポート セキュリティの設定	ポート セキュリティおよびトランク ポート セキュ リティの設定方法について説明します。
第 39 章	コントロール プレーン ポリシン グの設定	Control Plane Policing (CoPP; コントロール プレーンポリシング)を使用して Catalyst 4500 シリーズ スイッチを保護する方法について説明します。
第 40 章	DHCP スヌーピング、IP ソース ガード、およびスタティック ホス トの IPSG の設定	Dynamic Host Configuration Protocol (DHCP) スヌーピングおよび IP ソース ガードの設定方法について説明します。
第 41 章	DAI の設定	Dynamic ARP Inspection (DAI; ダイナミック ARP インスペクション)を設定する方法について説明します。
第 42 章	ACL によるネットワーク セキュ リティの設定	Access Control List(ACL; アクセス コントロール リスト)、VACL、および Mac Access Control List(MACL)の設定方法について説明します。
第 43 章	ポート ユニキャストおよびマル チキャスト フラッディング ブ ロック	ユニキャスト フラッディング ブロックの設定方法 について説明します。
第 44 章	ストーム制御の設定	ストーム制御抑制の設定方法について説明します。
第 45 章	SPAN と RSPAN の設定	Switched Port Analyzer (SPAN; スイッチド ポート アナライザ) の設定方法について説明します。
第 46 章	システム メッセージ ロギングの 設定	システム メッセージ ロギングの設定方法について説明します。
第 47 章	SNMP の設定	SNMP(簡易ネットワーク管理プロトコル)の設定 方法について説明します。
第 48 章	NetFlow の設定	NetFlow 統計情報の収集を設定する方法について説明します。
第 49 章	RMON の設定	Remote Network Monitoring(RMON)を設定する方法について説明します。
第 50 章	診断の実行	Catalyst 4500 シリーズ スイッチのさまざまな診断タ イプについて説明します。
第 51 章	WCCP バージョン 2 サービスの 設定	Web Cache Communication Protocol (WCCP)を使用してキャッシュ エンジン(Web キャッシュ)にトラフィックをリダイレクトするよう、Catalyst 4500 シリーズ スイッチを設定する方法について説明します。また、キャッシュ エンジン クラスタ (キャッシュ ファーム)を管理する方法についても説明します。
第 52 章	MIB サポートの設定	SNMP および MIB (Management Information Base; 管理情報ベース)サポートの設定方法について説明します。
第 53 章	ROM モニタ	ROM モニタについて説明します。
付録 A	略語	このマニュアルで使用される略語の定義を示します。

関連資料

Catalyst 4500 シリーズ スイッチの関連資料は次のとおりです。

Catalyst 4500 Series Switch Documentation Home

- http://www.cisco.com/en/US/products/hw/switches/ps4324/tsd_products_support_series_home.html
- - http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_guide_book09186a0080 126d3d.html
- [®] Catalyst 4500 Series Module Installation Guide

 (Customer Order Number DOC-786444=)
- http://www.cisco.com/en/US/products/hw/switches/ps4324/products_module_installation_guide_book091 86a008009c17d.html
- [□] Catalyst 4500 Series Regulatory Compliance and Safety Information a (Customer Order Number DOC-7813233=)
- http://www.cisco.com/en/US/products/hw/switches/ps4324/products_regulatory_approvals_and_complian ce09186a00800d7676.html

特定のスーパーバイザ エンジンまたはアクセサリ ハードウェアのインストレーション ノートは、 次の URL から入手できます。

http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_installation_guides_list.html

Cisco IOS コンフィギュレーション ガイドおよびコマンド リファレンス 上記のマニュアルで 扱っていない Cisco IOS ソフトウェア機能を設定する場合には、次のマニュアルを参照してください。

- F Configuration Fundamentals Configuration Guide a
- F Configuration Fundamentals Command Reference
- 『Interface Configuration Guide』
- 『Interface Command Reference』
- **Network Protocols Configuration Guide a Part 1, 2, 3
- "Network Protocols Command Reference Part 1, 2, 3
- "Security Configuration Guide "
- "Switching Services Configuration Guide a
- "Switching Services Command Reference a
- FVoice, Video, and Fax Applications Command Reference

Cisco IOS コンフィギュレーション ガイドおよびコマンド リファレンスは、次の URL から入手できます。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm

MIB については、次の URL を参照してください。

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

ソフトウェア マニュアル

サポートされるスイッチとモジュールの機能は、インストールしたソフトウェアによって大幅に異なります。一般的に、ソフトウェア リリースごとに次のガイドがあります。

- リリース ノート http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_release_notes_list.html
- コンフィギュレーション ガイド
 http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_gui
 des_list.html
- コマンドリファレンス http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_command_reference_list.html
- システム メッセージ ガイド
 http://www.cisco.com/en/US/products/hw/switches/ps4324/products_system_message_guides_list.html

ソフトウェア リリースに適したガイドをブックマークします。

 MIB の情報については、次の URL を参照してください。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

表記法

このマニュアルでは、次の表記法を使用しています。

表記	説明
太字	コマンド、コマンド オプション、およびキーワードは太字で示してい
	ます。
<i>イタリック体</i>	ユーザが値を指定するコマンド引数は、 <i>イタリック体</i> で示しています。
[]	角カッコの中のコマンド要素は、省略可能です。
{ x y z }	コマンド ラインで必ずどれか 1 つを選択しなければならない必須キー ワードは、波カッコで囲み、縦棒で区切って示しています。
[x y z]	どれか l 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。ストリングにその引用符も含まれてしまうためです。
screen フォント	システムの表示は screen フォントで表されます。
太字の screen フォント	ユーザがそのまま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	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
フォント	ています。
→	このポインタは、例の中の重要な行を強調しています。
۸	Ctrl キーを表します。たとえば、画面に表示される ^D というキーの組み合わせは、Ctrl キーを押しながら D キーを押すことを意味します。
< >	パスワードのように出力されない文字は、かぎカッコ(<>)で囲んで示しています。

(注)は、次のように表しています。



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

注意は、次のように表しています。



注意

タスク テーブルのコマンド

タスク テーブルにリストされるコマンドは、タスクを実行するための関連情報のみを表し、コマン ドで使用できるすべてのオプションについては示していません。コマンドの詳細な説明について は、『Catalyst 4500 Series Switch Cisco IOS Command Reference』のコマンドを参照してください。

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project.All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
- **2.** Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
- **3.** All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)".
- **4.** The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
- **5.** Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
- **6.** Redistributions of any form whatsoever must retain the following acknowledgment:

 This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- 1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
- **2.** Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- **3.** All advertising materials mentioning features or use of this software must display the following acknowledgement:
 - "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".
 - The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
- **4.** If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

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と一般的なシスコ マニュアルについては、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。次の URL から入手してください。

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

Japan TAC Web サイト

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

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

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

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

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



CHAPTER

1

製品概要

この章では、Catalyst 4500 シリーズ スイッチの概要について説明します。主な内容は、次のとおりです。

- レイヤ2ソフトウェアの機能(p.1-2)
- レイヤ3ソフトウェアの機能(p.1-8)
- 管理機能 (p.1-15)
- セキュリティ機能 (p.1-19)
- Metro の機能 (p.1-25)



Catalyst 4500 シリーズ スイッチがサポートするシャーシ、モジュール、およびソフトウェア機能については、次の URL の『Release Notes for the Catalyst 4500 Series Switch』を参照してください。

 $http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_release_note09186a0080758ff3.html$

レイヤ2ソフトウェアの機能

ここでは、Catalyst 4500 シリーズ スイッチ上の主要なレイヤ 2 スイッチング ソフトウェアの機能について説明します。

- 802.1Q およびレイヤ 2 プロトコル トンネリング (p.1-2)
- CDP (p.1-2)
- EtherChannel バンドル (p.1-3)
- ジャンボ フレーム (p.1-3)
- LLDP (p.1-3)
- Multiple Spanning-Tree (p.1-3)
- PVRST+ (p.1-4)
- QoS (p.1-4)
- Resilient Ethernet Protocol (p.1-5)
- STP (p.1-5)
- Stateful Switchover (p.1-5)
- SVI 自動ステート (p.1-6)
- UDLD (p.1-6)
- 単一方向イーサネット (p.1-6)
- VLAN (p.1-6)

802.1Q およびレイヤ 2 プロトコル トンネリング

802.1Q トンネリングは、サービス プロバイダー インフラストラクチャに入る夕グ付きパケットに再び夕グを付けて、VLAN (仮想 LAN) スペースを拡張する Q-in-Q 技術です。サービス プロバイダーは 802.1Q トンネリングを使用することにより、トンネル内部の元のカスタマー VLAN ID を失うことなく、各カスタマーに VLAN を割り当てることができます。トンネルに入るすべてのデータトラフィックはトンネル VLAN ID でカプセル化されます。レイヤ 2 プロトコル トンネリングは、すべてのレイヤ 2 制御トンネルに使用される類似の技術です。802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングがサポートされるのは、Supervisor Engine V、V-10GE、6-E です。

802.1Q トンネリングの設定手順については、第 23 章 「802.1Q およびレイヤ 2 プロトコル トンネリングの設定」を参照してください。

CDP

Cisco Discovery Protocol (CDP; シスコ検出プロトコル)は、メディア独立型およびプロトコル独立型のデバイス調査プロトコルです。CDP はルータ、スイッチ、ブリッジ、アクセス サーバを含むすべてのシスコ製品で使用できます。各デバイスは CDP を使用して、その存在を他のデバイスにアドバタイズし、同じ LAN 上の他のデバイスに関する情報を受け取ります。CDP を使用することで、シスコ製スイッチとルータは MAC (メディア アクセス制御) アドレス、IP アドレス、発信インターフェイスなどの情報を交換できます。CDP はデータリンク レイヤ上でのみ実行され、異なるネットワークレイヤ プロトコルをサポートする2つのシステムがお互いに認識できるようにします。CDP を設定した各デバイスは、マルチキャスト アドレスに対して定期的にメッセージを送信します。各デバイスは、SNMP (簡易ネットワーク管理プロトコル) メッセージを受信できる 1 つまたは複数のアドレスをアドバタイズします。

CDPの設定手順については、第24章「CDPの設定」を参照してください。

EtherChannel バンドル

EtherChannel ポート バンドルは、複数のポートを 1 つの論理伝送パスにグループ化して、2 つのスイッチ間に高帯域接続を確立します。

EtherChannel の設定手順については、第20章「EtherChannel の設定」を参照してください。

ジャンポ フレーム

ジャンボ フレーム機能により、(IEEE [米国電気電子学会] イーサネット最大伝送ユニット [Maximum Transmission Unit; MTU] を超える)最大で 9216 バイトのパケットをスイッチに転送でき、このようなフレームを [oversize] と宣言してドロップすることはありません。この機能は、通常大規模なデータ転送で使用されます。ジャンボ機能は、レイヤ 2 およびレイヤ 3 インターフェイスでポート単位に設定できます。サポートされているのは、WS-X4306-GB(全ポート)、WS-X4232-GB-RJ (ポート 1 ~ 2)、WS-X4418-GB (ポート 1 ~ 2)、WS-X4412-2GB-TX (ポート 13 ~ 14)、4648-GB-RJ45V、WS-X4648-GB+RJ45V、WS-X4706-10GE の各ラインカード、およびスーパーバイザのアップリンク ポートのみです。

ジャンボ フレームについては、第6章「インターフェイスの設定」を参照してください。

LLDP

他社製のデバイスをサポートし、他のデバイスとの相互運用性を確保するために、スイッチは IEEE 802.1AB Link Layer Discovery Protocol (LLDP)をサポートしています。LLDPは、ネットワークデバイスがネットワーク上の他のデバイスに自分の情報をアドバタイズするために使用する近隣探索プロトコルです。このプロトコルはデータリンクレイヤ上で動作するため、異なるネットワークレイヤプロトコルが稼働する2つのシステムで互いの情報を学習することができます。

LLDP は一連のアトリビュートをサポートし、これを使用して隣接するデバイスを検出します。アトリビュートには、Type、Length、および Value の説明が含まれていて、これらを TLV と呼びます。LLDP をサポートするデバイスは、ネイバーとの情報の送受信に TLV を使用することができます。設定情報、デバイスの機能、デバイス ID などの詳細情報は、このプロトコルを使用してアドバタイズできます。

LLDPの設定手順については、第25章「LLDPおよびLLDP-MEDの設定」を参照してください。

Multiple Spanning-Tree

IEEE 802.1s Multiple Spanning-Tree (MST)は、単一の 802.1Q または ISL(スイッチ間リンク) VLAN トランク内で複数のスパニングツリー インスタンスを許可します。MST は、IEEE 802.1w Rapid Spanning-Tree (RST) アルゴリズムを複数のスパニングツリーに拡張します。この拡張によって、VLAN 環境で高速コンバージェンスとロード バランシングの両方を実現できます。

MST を使用すると、トランクを介して複数のスパニングツリーを構築できます。VLAN をグループとしてまとめ、スパニングツリー インスタンスに対応付けることができます。各インスタンスに、他のスパニングツリー インスタンスに依存しないトポロジを与えることができます。この新しいアーキテクチャによって、データ トラフィックに複数の転送パスが与えられ、ロード バランシングが可能になります。あるインスタンス(転送パス)で障害が発生しても、他のインスタンス(転送パス)に影響を与えないので、ネットワークの耐障害性が向上します。

MST の設定手順については、第17章「STP および MST の設定」を参照してください。

PVRST+

Per-VLAN Rapid Spanning Tree Plus (PVRST+)は、VLAN 単位における 802.1w の実装です。 Spanning-Tree Protocol (STP; スパニングツリー プロトコル)モードに対しては、Per-VLAN Spanning-Tree Plus (PVST+)と同様で、802.1w に基づく Rapid Spanning-Tree Protocol (RSTP)プロトコルを実行します。

PVRST+の設定手順については、第17章「STP および MST の設定」を参照してください。

QoS

QoS (Quality Of Service) 機能は、ネットワーク トラフィックを選択し、相対的な重要性に従って プライオリティを設定することで輻輳を防止します。 QoS をネットワークに実装すると、ネット ワーク パフォーマンスを予測しやすくなり、より効果的な帯域幅使用が可能となります。

Catalyst 4500 シリーズ スイッチは、次の QoS 機能をサポートしています。

- 分類とマーキング
- ポート単位 /VLAN 単位のポリシングを含む入力および出力ポリシング
- シェアリングとシェーピング

Catalyst 4500 シリーズ スイッチは、信頼境界をサポートしています。信頼境界は、CDP を使用してスイッチ ポート上の Cisco IP Phone (Cisco IP Phone 7910、7935、7940、および 7960)の存在を検出します。電話が検出されなければ、信頼境界機能はスイッチ ポート上の trusted (信頼)設定をディセーブルにし、ハイ プライオリティ キューの誤使用を防ぎます。

Catalyst 4500 シリーズ スイッチは、QoS Automation (Auto-QoS) をサポートしています。Auto QoS は、自動設定を介して既存の QoS 機能の使用を簡略にします。

Cisco モジュラ QoS コマンドライン インターフェイス (Supervisor Engine 6-E)

Cisco Modular QoS CLI (MQC; モジュラ QoS コマンドライン インターフェイス) は Cisco IOS ソフトウェア QoS の実装に使用されるフレームワークです。MQC を使用すると、トラフィック クラスの定義、トラフィック ポリシー(トラフィック クラスに適用される QoS 機能を含む)の作成、およびインターフェイスへのトラフィック ポリシーの付加を行うことができます。MQC は Cisco 全体の基準であり、複数の製品ファミリにおいて一貫した構文の使用と QoS 機能の動作を可能にします。Cisco IOS Software Release 12.2(40)SG は、Supervisor Engine 6-E の QoS 機能の設定について MQC に準拠しています。MQC により、新機能および技術革新の迅速な配置が可能になります。そして帯域、遅延、ジッタ、およびパケット損失に関するネットワーク パフォーマンスの管理が容易になり、ミッションクリティカルなビジネス アプリケーションのパフォーマンスが強化されます。Supervisor Engine 6-E の一部としてサポートされている QoS 機能は豊富かつ高度であり、Cisco MQC を使用することで有効になります。

Two-Rate Three-Color ポリシング (Supervisor Engine 6-E)

Two-Rate Three-Color ポリシング機能(別名、*階層型 QoS*)は、ユーザが定義した基準に基づいて、トラフィック クラスの入出力伝送速度を制限します。そして、適用可能な Differentiated Services Code Point (DSCP; DiffServ コード ポイント)値を設定してパケットのマークまたは色を設定します。この機能は、ネットワークのエッジにあるインターフェイス上に設定され、トラフィックがネットワークから出入りするのを制限します。この機能を使用すると、ユーザが定義する基準に準拠するトラフィックがインターフェイスから送信されます。これらの基準を超過または違反するトラフィックはプライオリティ設定を下げて送信されるか、ドロップされることもあります。

QoS および Auto-QoS については、第34章「QoS の設定」を参照してください。

Resilient Ethernet Protocol

Resilient Ethernet Protocol (REP) はシスコ独自のプロトコルで、Spanning Tree Protocol (STP; スパニング ツリー プロトコル)の代わりにネットワーク ループを制御し、リンク障害を処理して、コンバージェンス時間を改善します。REP は、セグメントに接続されているポートのグループを制御して、セグメントで何らかのブリッジング ループが作成されないようにして、セグメント内のリンク障害に応答します。REP は、より複雑なネットワークを構築するための基盤を提供するもので、VLAN ロード バランシングをサポートしています。

QoS および Auto-QoS については、第 18 章「Resilient Ethernet Protocol の設定」を参照してください。

STP

STP は、ネットワークのすべてのノード間において、アクティブでループフリーなデータ パスを確保するフォールトトレラントなインターネットワークを作成します。 STP はアルゴリズムを使用し、スイッチド ネットワーク内のループフリーで最適なパスを計算します。

STP の設定手順については、第17章「STP および MST の設定」を参照してください。

Catalyst 4500 シリーズ スイッチは、次の STP 拡張をサポートしています。

- スパニングツリー PortFast PortFast は、ポートとポートに直接接続したホストを、リスニング ステートとラーニング ステートをバイパスして、直接フォワーディング ステートに移行します。
- スパニングツリー UplinkFast UplinkFast は、スパニングツリー トポロジの変更後に高速のコンバージェンスを行い、アップリンク グループを使用して冗長リンク間のロード バランシングを実現します。アップリンク グループは、転送中のリンクで障害が起きた場合に代替パスを提供します。UplinkFast は、直接のリンク障害が発生したスイッチに対して、スパニングツリーのコンバージェンス時間を短縮するように設計されています。
- スパニングツリーBackboneFast BackboneFast は、間接的なリンク障害によるトポロジ変更後に、スパニングツリーがコンバージェンスするのに必要な時間を短縮します。BackboneFast は、間接的なリンク障害が発生したスイッチに対して、スパニングツリーのコンバージェンス時間を短縮します。
- スパニングツリー ルート ガード ルート ガードは、ポートを強制的に指定ポートにして、リンクのもう一方でスイッチがルート スイッチにならないようにします。

STP 拡張については、第19章「任意の STP 機能の設定」を参照してください。

Stateful Switchover

Stateful Switchover (SSO) は、アクティブ スーパーバイザ エンジンが冗長スーパーバイザ エンジンに切り替わった場合、レイヤ 2 トラフィックに割り込みが瞬時に発生し、設定およびステート情報をアクティブ スーパーバイザ エンジンから冗長スーパーバイザ エンジンに伝播します。

• ステートフル IGMP スヌーピング

この機能はスイッチオーバーが発生した場合に、新しいアクティブ スーパーバイザ エンジンがマルチキャスト グループ メンバシップを認識するように、アクティブ スーパーバイザ エンジンから学習した Internet Group Management Protocol (IGMP; インターネット グループ管理プロトコル) データを冗長スーパーバイザ エンジンに伝播します。これにより、スイッチオーバー中のマルチキャスト トラフィックの中断を軽減します。

• ステートフル DHCP スヌーピング

この機能はスイッチオーバーが発生した場合に、新しいアクティブ スーパーバイザ エンジンがスヌーピングされた Dynamic Host Configuration Protocol (DHCP) データを認識し、セキュリティの利点が中断しないように、アクティブ スーパーバイザ エンジンからの DHCP スヌーピング データを冗長スーパーバイザ エンジンに伝播します。

SSO については、第9章「Cisco NSF/SSO スーパーバイザ エンジンの冗長構成の設定」を参照してください。

SVI 自動ステート

SVI ポートが VLAN 上に複数存在する場合は、VLAN のすべてのポートが停止するときに SVI も通常停止します。 SVI が「アップまたはダウン」状態であることを判断するときにいくつかのポートを考慮しないようにネットワークを設計する場合があります。 SVI 自動ステートは、 SVI の「アップまたはダウン」判断時に考慮しないポートにマーキングするつまみとなり、ポートでイネーブルになっているすべての VLAN に適用されます。

UBRL

User Based Rate Limiting (UBRL) では、マイクロフロー ポリシングが採用され、トラフィック フローが動的に学習されて、それぞれの一意のフローが個別レートにレート制限されます。UBRL は、内蔵 NetFlow がサポートされている Supervisor Engine V-10GE のみで使用できます。

UBRL については、UBRL の設定 (p.34-45) を参照してください。

UDLD

UniDirectional Link Detection (UDLD; 単一方向リンク検出)は、光ファイバまたは銅イーサネットケーブルで接続されたデバイスが、ケーブルの物理構成を監視し、単方向リンクを検出できるようにします。

UDLD については、第26章「UDLD の設定」を参照してください。

単一方向イーサネット

単一方向イーサネットは、全二重ギガポート イーサネット用に 2 つの光ファイバ ストランドを使用するのではなく、ギガポートのトラフィックの送信または受信にファイバ ストランドを 1 つだけ使用します。

単一方向イーサネットについては、第30章「単一方向イーサネットの設定」を参照してください。

VLAN

VLAN は物理トポロジではなく、論理トポロジに従ってスイッチとルータを設定します。ネットワーク管理者は VLAN を使用することで、インターネットワーク内の LAN セグメントの集合を、各セグメントがネットワーク内で単一の LAN として表示されるようにして、1 つの自律ユーザ グループにまとめることができます。VLAN は、パケットが VLAN 内のポート間でのみ交換されるように、論理的にネットワークを異なるブロードキャスト ドメインにセグメント化します。通常、VLAN は特定のサブネットに対応しますが、必ずしも対応するとは限りません。

VLAN、VLAN Trunking Protocol (VTP; VLAN トランキング プロトコル) およびダイナミック VLAN メンバシップの詳細については、第 13 章「VLAN、VTP、および VMPS の設定」を参照してください。

次の VLAN 関連の機能もサポートされます。

• VTP VTP は VTP 管理ドメインのすべてのデバイス間で、VLAN 名の一貫性と接続を維持します。 複数の VTP サーバを使用して、グローバル VLAN 情報を管理および修正できる冗長性をドメイン内にもたらすことができます。大規模なネットワークでも、わずかな VTP サーバしか要求されません。

- プライベート VLAN プライベート VLAN は、通常の VLAN の機能を持ち、スイッチ上の他のポートからレイヤ 2 をある程度分離させるポート セットです。
 - プライベート VLAN については、第36章「PVLAN の設定」を参照してください。
- プライベート VLAN トランク ポート プライベート VLAN トランク ポートを使用すると、プライベート VLAN 上のセカンダリ ポートが複数のセカンダリ VLAN を実行します。
- プライベート VLAN 混合モード トランク ポート プライベート VLAN 混合モード トランク を使用すると、混合モード ポートを 802.1Q トランク ポートに拡大し、複数のプライマリ VLAN (したがって、複数のサブネット)を伝送します。 プライベート VLAN 混合モード トランクは 一般的に、別のプライマリ VLAN 上で異なるサービスまたはコンテンツを独立サブスクライバ に提供するために使用します。 セカンダリ VLAN は、プライベート VLAN 混合モード トランク上で伝送できません。
- ダイナミック VLAN メンバシップ ダイナミック VLAN メンバシップの、ポートに接続されたデバイスの送信元 MAC に基づいて、VLAN にスイッチ ポートを動的に割り当てることができます。ネットワーク内にあるスイッチの1つのポートからネットワーク内にある別のスイッチのポートにホストを移動する場合、そのスイッチはそのホストに適切な VLAN を新しいポートへ動的に割り当てます。VLAN Management Policy Server (VMPS; VLAN マネジメント ポリシーサーバ) クライアント機能を使用すると、ダイナミック アクセス ポートを VMPS クライアントに変換できます。VMPS クライアントは VQP クエリーを使用して VMPS サーバと通信し、ポートに接続するホストの MAC アドレスに基づいてポートに VLAN を割り当てられます。

レイヤ3ソフトウェアの機能

レイヤ 3 スイッチは、キャンパス LAN またはイントラネット用に最適化され、広域イーサネット ルーティングとスイッチング サービスを提供する高性能スイッチです。レイヤ 3 スイッチングは、ルート処理とインテリジェント ネットワーク サービスの 2 つのソフトウェア機能によりネット ワーク パフォーマンスを高めます。

通常のソフトウェアベースのスイッチと比べると、レイヤ3スイッチはより多くのパケットをより高速に処理します。この場合、マイクロプロセッサをベースとするエンジンではなく、Application-Specific Integrated Circuit (ASIC; 特定用途向け集積回路)が使用されます。

ここでは、Catalyst 4500 シリーズ スイッチ上の主要なレイヤ 3 スイッチング ソフトウェアの機能について説明します。

- CEF (p.1-8)
- HSRP (p.1-8)
- IP ルーティング プロトコル (p.1-9)
- マルチキャスト サービス (p.1-12)
- NSF/SSO (p.1-13)
- PBR (p.1-13)
- UDLR (p.1-13)
- VRF-Lite (p.1-14)

CEF

Cisco Express Forwarding(CEF; シスコ エクスプレス フォワーディング)は、拡張レイヤ 3 IP スイッチング テクノロジーです。CEF は大規模で動的なトラフィック パターンを持つインターネットなどのネットワークと、集約型の Web ベース アプリケーション、すなわち対話形式のセッションを用いるネットワークでネットワーク パフォーマンスとスケーラビリティを最適化します。CEF はネットワークのどの部分にも使用できますが、高い弾力性を持つ高性能レイヤ 3 IP バックボーン スイッチング用に設計されています。

CEFの設定手順については、第28章「CEFの設定」を参照してください。

HSRP

Hot Standby Router Protocol (HSRP; ホットスタンバイ ルータ プロトコル) は、個々のレイヤ 3 スイッチのアベイラビリティに依存することなく、イーサネット ネットワーク上のホストから IP トラフィックをルーティングすることでネットワークの高いアベイラビリティを提供します。この機能は、Router Discovery Protocol (RDP)をサポートせず、また選択されたルータのリロード時または電源がオフになったときに新しいルータに切り替わる機能を持たないホストに特に有効です。

HSRP の設定については、次の URL を参照してください。

http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a008042fbb3.html

SSO 認識 HSRP

SSO 認識 HSRP は、スーパーバイザ エンジンのスイッチオーバー時に、スタンバイ HSRP ルータに パス変更することなく、連続してデータ パケットを転送します。スーパーバイザ エンジンのスイッチオーバー時に NSF/SSO は、HSRP 仮想 IP アドレスを使用し既知のルートに従って、連続してデータ パケットを転送します。両方のスーパーバイザ エンジンがアクティブ HSRP ルータで失敗した

場合、スタンバイ HSRP ルータがアクティブな HSRP ルータとして機能します。Catalyst 4500 の NSF/SSO が提供する信頼性およびアベイラビリティを、冗長シャーシのあるレイヤ 3 集約にまで拡大します。SSO 認識 HSRP は、スーパーバイザ冗長性のある Catalyst 4507R および 4510R シャーシ 上の Supervisor Engine IV、V、および V-10GE で利用可能です。

IP ルーティング プロトコル

Catalyst 4500 シリーズ スイッチでは、次のルーティング プロトコルがサポートされています。

- BGP (p.1-9)
- EIGRP (p.1-9)
- GLBP (p.1-10)
- IGRP (p.1-10)
- IS-IS (p.1-10)
- OSPF (p.1-11)
- RIP (p.1-11)
- VRRP (p.1-11)

BGP

Border Gateway Protocol (BGP; ボーダー ゲートウェイ プロトコル) は、AS 間でのルーティング情報のループフリーな交換が自動的に保証されるドメイン間ルーティング システムの設定を可能にする外部ゲートウェイ プロトコルです。BGP では、各ルートはネットワーク番号と(AS パスと呼ばれる)情報が通過する AS のリスト、その他のパス属性のリストから構成されます。

Catalyst 4500 シリーズ スイッチは BGP バージョン 4 をサポートし、これには Classless Interdomain Routing (CIDR; クラスレス ドメイン間ルーティング) も含まれます。CIDR は、集約ルートすなわ ちスーパーネットを作成して、ルーティング テーブルのサイズを縮小します。CIDR は BGP 内で ネットワーク クラスの概念を除外し、IP プレフィクスのアドバタイズをサポートしています。CIDR ルートは、OSPF、EIGRP、RIP によって搬送されます。

BGP ルートマップの継続

BGP ルートマップの継続機能では、BGP ルートマップ コンフィギュレーションの continue 句を導入します。continue 句により、プログラム可能なポリシー設定およびルート フィルタリングが提供されます。match と set 句によるエントリの実行が成功したあと、BGP ルート マップ continue 句を使用して、ルート マップの追加エントリを実行できます。continue 句により、同じルート マップ内で繰り返されるポリシー設定数を減らすために、より多くのモジュラ ポリシー定義を設定および構成できます。

EIGRP

Enhanced Interior Gateway Routing Protocol (EIGRP)は IGRPの一種で、リンクステートプロトコルの利点にディスタンスベクタプロトコルを結合したものです。EIGRPは Diffusing Update Algorithm (DUAL)を採用しています。EIGRPは高速コンバージェンス、可変長サブネットマスク、部分的境界更新、複数のネットワークレイヤサポートの各機能を備えています。ネットワークトポロジが変更されると、EIGRPはトポロジテーブルで宛先までの新しい適切なルートを確認します。テーブルにこのようなルートが見つかると、EIGRPはルーティングテーブルをただちに更新します。ユーザは EIGRPが IPXパケットのルーティング用に提供する高速コンバージェンスと部分的更新を使用できます。

EIGRP は、ルーティング情報が変更された場合にのみルーティング更新を送信することで、帯域幅を節約します。この更新には、ルーティングテーブル全体ではなく、変更されたリンクに関する情報のみが含まれます。EIGRP はまた、更新を伝送するときのレートを決定する場合に、使用可能な帯域幅を考慮に入れます。



レイヤ3スイッチングは、Next Hop Resolution Protocol (NHRP)をサポートしていません。



(注)

お客様は、EIGRP を設定して IPv6 プレフィクスをルーティングできます。IPv4 および IPv6 プレフィクス両方の EIGRP 設定およびプロトコル動作は似ているため、操作に一貫性があり、なじみやすくなっています。IPv6 向けの EIGRP により、お客様は既存の EIGRP 知識およびプロセスを使用して、IPv6 ネットワークを低コストで配置できます。

GLBP

Gateway Load Balancing Protocol (GLBP)機能は、LAN上の1つのデフォルトゲートウェイに設定された IP ホストの自動ルータ バックアップを提供します。LAN上の複数のファーストホップルータは、結合して IP パケット転送負荷の共有時に1つの仮想ファーストホップ IP ルータとなります。各 GLBP デバイスがパケット転送を行うことで、リソースの使用を最適化し、コストを削減します。LAN上のその他のルータは冗長 GLBP ルータとして動作して、既存の転送ルータのいずれかに障害が発生した場合にアクティブになります。これにより、ネットワークの弾性が向上し、管理負荷を削減します。GLBP は、Supervisor Engine 6-E およびクラシック スーパーバイザ エンジンにに適用可能な機能です。

GLBP の詳細については、次の URL を参照してください。

 $http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a008042fb97.html \\$

IGRP

Interior Gateway Routing Protocol (IGRP) は、シスコが AS 内でのルーティング用に開発した、安定したディスタンス ベクタ Interior Gateway Protocol (IGP; 内部ゲートウェイ プロトコル)です。ディスタンス ベクタ ルーティング プロトコルはスイッチに対し、ルーティング更新メッセージを使用して隣接する各ルータにルーティング テーブルのすべてのデータまたは一部のデータを定期的に送信するよう要求します。ルーティング情報がネットワークで伝播されると、ルータはインターネットワーク内のすべてのノードまでの距離を計算します。IGRP はメトリックを組み合わせて用います。インターネットワーク遅延、帯域幅、信頼性、および負荷はすべてルーティング決定の要素になります。

IS-IS

Intermediate System-to-Intermediate System (IS-IS) プロトコルは、リンクステート ルーティング アルゴリズムを使用します。これは、TCP/IP 環境で使用される OSPF ルーティング プロトコルに準拠しています。ISO IS-IS プロトコルを運用する場合には、各ルータがネットワークの完全なトポロジ マップ (つまり、どの中間システムおよびエンド システムが他のどの中間システムとエンド システムに接続しているか)を保持する必要があります。ルータは、周期的にマップ上でアルゴリズムを実行して、可能性のあるすべての宛先への最短パスを計算します。

IS-IS プロトコルは、2 つの階層を使用します。中間システム(ルータ)はレベル1 およびレベル2 に分類されます。レベル1 中間システムは単一のルーティング エリアを扱います。トラフィックは そのエリア内のみでリレーされます。他のインターネットワーク トラフィックは最も近いレベル2 中間システムに送られます。これは、レベル1 中間システムとしても動作します。レベル2 中間システムは、同一ドメイン内の異なるルーティング エリア間でトラフィックを移動します。

マルチエリアをサポートする IS-IS では単一の中間システム内に複数のレベル 1 エリアを持つことができるので、1 つの中間システムで複数のエリアを構成することもできます。単一レベル 2 エリアは、エリア間トラフィックのバックボーンとして使用されます。

IS-IS はイーサネット フレームのみをサポートしています。Internetwork Packet Exchange (IPX) についてはサポートしていません。

OSPF

Open Shortest Path First (OSPF) プロトコルは、RIP の制約を克服することを目的とした標準ベースの IP ルーティング プロトコルです。OSPF はリンク ステート ルーティング プロトコルであるため、同じ階層領域内のすべてのルータに Link-State Advertisement (LSA; リンク ステート アドバタイズメント)を送信します。OSPF LSA 内では、接続するインターフェイスとそれらのメトリックに関する情報が用いられます。ルータはリンク状態の情報を累積すると、Shortest Path First (SPF) アルゴリズムを使用して各ノードへの最短パスを計算します。この他の OSPF の機能には、等価コストマルチパス ルーティングや上位レイヤの Type of Service (ToS; タイプ オブ サービス)要求に基づくルーティングなどがあります。

OSPF は、OSPF の連続したネットワークおよびホストのグループであるエリアの概念を採用しています。OSPF エリアは、内部トポロジがエリア外のルータから見えない OSPF Autonomous System (AS; 自律システム)を論理的に分割したものです。エリアによって IP ネットワーク クラスが提供するのとは異なる階層レベルが追加され、これらを使用して、ルーティング情報の集約やネットワークの詳細事項のマスクを行うことができます。このような機能により、OSPF は大規模ネットワークにおけるスケーラビリティをより強化します。

RIP

Routing Information Protocol (RIP) は、ディスタンスベクタのドメイン内ルーティング プロトコルです。RIP は小規模で均質なネットワークで効果的に機能します。大規模で複雑なインターネットワークでは、RIP は最大ホップ カウント 15、Variable-Length Subnet Mask (VLSM; 可変長サブネットマスク)の非サポート、非効率的な帯域幅使用、コンバージェンスの遅さなど数々の制約があります。RIP II は VLSM をサポートしています。

VRRP

Virtual Router Redundancy Protocol(VRRP; 仮想ルータ冗長プロトコル)は、標準ベースのファーストホップ冗長プロトコルです。VRRP を使用すると、ルータ グループは 1 つの仮想 IP アドレスと1 つの仮想 MAC アドレスを共有することで、1 つの仮想ルータとして機能します。マスター ルータはパケット転送を実行し、バックアップ ルータはアイドル状態のままです。VRRP は一般的に、複数のベンダーのファーストホップ ゲートウェイ冗長展開で使用します。

マルチキャスト サービス

マルチキャスト サービスは、ネットワーク上のパケットを必要な場合にのみ強制的に複製し、ホスト上のグループの動的な加入および脱退を許可することで、帯域幅を節約します。次のマルチキャスト サービスがサポートされています。

- IGMP スヌーピング IGMP スヌーピングがマルチキャスト トラフィックを管理します。ス イッチ ソフトウェアは、IP マルチキャスト パケットを検証して、その内容に基づいてパケットを転送します。マルチキャスト トラフィックは、接続するホストがマルチキャスト トラフィックを要求するポートにのみ転送されます。

IGMPv3 のサポートは、IGMPv3 ホストまたはルータが存在する場合に、マルチキャスト トラフィック フラッディングの抑制を提供します。IGMPv3 スヌーピングは、IGMPv3 クエリーおよびメンバシップ レポート メッセージを待ち受け、ホスト / マルチキャスト グループの関連付けを維持します。また、スイッチがマルチキャスト データを必要とするポートだけに伝播することを可能にします。IGMPv3 スヌーピングは、IGMPv1 および IGMPv2 との完全な相互運用性があります。

Explicit Host Tracking (EHT) は、IGMPv3 スヌーピングの拡張機能です。EHT は、ポート単位の即時脱退処理を可能にします。EHT は、ホストごとのメンバシップ情報の追跡、またはすべての IGMPv3 グループ メンバに関する統計情報の収集に使用できます。

IGMP スヌーピングの設定手順については、第 21 章「IGMP スヌーピングとフィルタリングの設定」を参照してください。

• IPv6 Multicast Listener Discovery (MLD) および MLD スヌーピング MLD は IPv6 マルチキャストデバイスで使用されるプロトコルで、直接接続されたリンク上のマルチキャストリスナー (IPv6 マルチキャスト パケットを受信するノード)の存在、および隣接ノードを対象とするマルチキャスト パケットを検出します。MDL スヌーピングは、MLD v1 および MLD v2 の 2 つの異なるバージョンでサポートされています。ネットワーク スイッチは、MLD スヌーピングを使用してマルチキャストトラフィックのフラッディングを制限することで、IPv6 マルチキャストデータは VLAN 内のすべてのポートにフラッディングされるのではなく、データを受信するポートのリストに選択的に転送されます。こうすることで、ネットワーク内のデバイスに対する付加が軽減され、リンク上の不必要な帯域を最小化し、IPv6 マルチキャストデータの効率的な配布が可能になります。

マルチキャスト サービスの設定方法については、第 22 章「IPv6 MLD スヌーピングの設定」を 参照してください。

• Protocol Independent Multicast (PIM) PIM はプロトコル独立型で、EIGRP、OSPF、BGP、スタティック ルートなど、ユニキャスト ルーティング テーブルの読み込みにどのユニキャストルーティング プロトコルが使用されても利用できます。PIM はまた、Reverse Path Forwarding (RPF)チェック機能を実行するのに、完全独立型のマルチキャスト ルーティング テーブルを構築する代わりにユニキャストルーティング テーブルを使用します。

マルチキャスト サービスの設定方法については、第 31 章「IP マルチキャストの設定」を参照してください。

PIM-SSM マッピング SSM マッピングは、万が一 URD と IGMP v3lite のいずれも利用できない場合、あるいはエンド システムでの SSM のサポートが、管理上または技術上の理由で望ましくないか、不可能である場合に SSM の移行をサポートしています。SSM マッピングにより、IGMPv3 が未サポートである従来型の Set-Top Box (STB; セットトップ ボックス)に映像を配信したり、IGMPv3 ホスト スタックを利用しないアプリケーションに対して、SSM を活用できます。

PIM-SSM マッピングの詳細については、次の URL を参照してください。 http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gtssmma.html#wp1171997

NSF/SSO

Non-Stop Forwarding with Stateful Switchover(NSF/SSO)は、スーパーバイザ エンジンのスイッチオーバー時にレイヤ 3 ルーティング環境で継続してデータ パケットを転送します。Catalyst 4500 の SSO および NSF 認識が提供する信頼性およびアベイラビリティを、レイヤ 3 ネットワークにまで拡大します。スーパーバイザ エンジンのスイッチオーバー時、NSF/SSO は、ルーティング プロトコル情報を回復および検証する一方で、既知のルートに従って継続してデータ パケットを転送し、不必要なルート フラップを引き起こさず、ネットワークが不安定になるのを回避します。NSF/SSO を使用すると、IP Phone コールはドロップされません。NSF/SSO は、OSPF、BGP、EIGRP、IS-IS、および CEF でサポートされます。NSF/SSO は一般的に、企業またはサービス プロバイダーネットワークの最重要部分(レイヤ 3 集約 / コアまたはレジリエント レイヤ 3 ワイヤリング クローゼット設計など)で展開されます。これは、重要なアプリケーションの単一シャーシ展開の重要なコンポーネントです。NSF/SSO は、スーパーバイザ冗長のある Catalyst 4507R および 4510R シャーシの出荷されたスーパーバイザ エンジンすべてで利用できます。

NSF/SSO の詳細については、第9章「Cisco NSF/SSO スーパーバイザ エンジンの冗長構成の設定」を参照してください。

ISSU

SSO が機能するには、アクティブ スーパーバイザ エンジンとスタンバイ スーパーバイザ エンジンの両方の IOS バージョンが同じである必要があります。Cisco IOS ソフトウェアのアップグレードまたはダウングレード中にバージョンが一致しないと、Catalyst 4500 シリーズ スイッチは強制的に RPR モードの動作になります。このモードでは、スイッチオーバー後にリンクフラップとサービス中断が発生します。この問題は、ソフトウェアのアップグレードまたはダウングレード中に SSO/NSF モードで動作できる In Service Software Upgrade(ISSU; インサービス ソフトウェア アップグレード)機能によって解決されます。

ISSU では、アクティブおよびスタンバイ スーパーバイザ エンジンそれぞれで実行しているステートフル コンポーネント間で Version Transformation Framework を利用することにより、両方のスーパーバイザエンジン上の異なるリリース レベルの Catalyst IOS イメージをアップグレードまたはダウングレードできます。

PBR

従来の IP の転送判断は、転送するパケットの宛先 IP アドレスのみに基づいていました。Policy Based Routing (PBR; ポリシーベース ルーティング)では、送信元インターフェイス、IP 送信元アドレス、レイヤ 4 ポート等のパケットに関連したアドレス以外の情報に基づいて転送できます。この機能により、ネットワーク管理者はより柔軟にネットワークを設定および設計できるようになります。

PBR の詳細については、第32章「PBR の設定」を参照してください。

UDLR

UniDirectional Link Routing (UDLR)は、単一方向の物理インターフェイス(高帯域の衛星リンクなど)上でマルチキャスト パケットをバック チャネルを持つスタブ ネットワークに転送する手段を提供します。

UDLR の設定手順については、『Cisco IP and IP Routing Configuration Guide』の「Configuring UniDirectional Link Routing」を参照してください。

VRF-Lite

VPN Routing and Forwarding Lite (VRF-Lite) は、IP ルーティングの拡張機能で、複数のルーティング インスタンスを提供します。BGP と同様に、VRF-Lite は各 VPN カスタマーに対して別々の IP ルーティングおよび転送テーブルを維持したまま、レイヤ 3 VPN サービスの作成を可能にします。 VRF-Lite は、入力インターフェイスを使用して異なる VPN のルートを区別します。VRF-Lite は、1 つまたは複数のレイヤ 3 インターフェイスを各 VRF に対応付けて仮想パケット転送テーブルを形成し、単一のスイッチ上に複数のレイヤ 3 VPN を作成できるようにします。VRF の有効なインターフェイスは、イーサネット ポートなどの物理インターフェイス、または VLAN Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) などの論理インターフェイスです。ただし、インターフェイスは常に複数の VRF に属することができません。

VRF-Lite については、第33章「VRF-Lite の設定」を参照してください。

管理機能

Catalyst 4500 シリーズ スイッチは CLI を通じて、または SNMP などの代替アクセス方式を通じてネットワークの管理と制御を行います。スイッチ ソフトウェアは、次のネットワーク管理機能をサポートしています。

- Cisco Network Assistant および組み込み Cisco View (p.1-15)
- DHCP (p.1-15)
- FAT ファイル管理システム (Supervisor Engine 6-E のみ)(p.1-16)
- 強制 10/100 自動ネゴシエーション (p.1-16)
- インテリジェントな電源管理 (p.1-16)
- MAC アドレス通知 (p.1-16)
- MAC 通知 MIB (p.1-16)
- NetFlow 統計情報 (p.1-16)
- SSH (p.1-17)
- SNMP (p.1-17)
- SPAN および RSPAN (p.1-17)
- VRRP (p.1-17)
- WCCP (p.1-18)

Cisco Network Assistant および組み込み CiscoView

Catalyst 4500 シリーズ スイッチを設定するための Web ベースのツールです。Cisco Network Assistant は、スタンドアロン デバイス、デバイスのクラスタ、またはデバイスの集合をご使用のイントラネットのどこからでも管理します。GUI(グラフィカル ユーザ インターフェイス)を使用すると、CLI コマンドを覚える必要がなく、複数の設定作業を実行できます。組み込み Cisco View は、スイッチ フラッシュ上に組み込むことができるデバイス管理アプリケーションで、スイッチのダイナミック ステータス、モニタリング、および設定情報を提供します。

ビジュアル ポート ステータス情報 スイッチ LED からポートレベルおよびスイッチレベルのステータスを目視で管理できます。

Cisco Network Assistant および組み込み CiscoView の詳細については、第 12 章「Cisco Network Assistant による Catalyst 4500 シリーズ スイッチの設定」を参照してください。

DHCP

Catalyst 4500 シリーズ スイッチは、次の方法で DHCP を使用します。

- DHCP サーバ Cisco IOS DHCP サーバ機能は、ルータ内で指定されたアドレス プールから DHCP クライアントに IP アドレスを割り当てて管理する完全な DHCP サーバ実装です。Cisco IOS DHCP サーバが自身のデータベースで DHCP 要求を実行できない場合、この要求をネット ワーク管理者が定義した 1 つまたは複数のセカンダリ DHCP サーバに転送できます。
- DHCP の自動設定 この機能により、ご使用のスイッチ(DHCP クライアント)は起動時に IP アドレス情報およびコンフィギュレーション ファイルを使用して、自動的に設定されます。

DHCP サーバの設定の詳細については、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t1/easyip2.htm

FAT ファイル管理システム (Supervisor Engine 6-E のみ)

FAT システムは、デバイスのディスクおよびフラッシュ上のファイルを管理するために広く使用されています。FAT ファイルシステムのサポートによって、フラッシュからのイメージの削除、追加、および転送を簡単に行うことができます。

強制 10/100 自動ネゴシエーション

この機能により、ポートが自動ネゴシエーションする速度を物理最大速度よりも低い速度に制限するよう、ポートを設定できます。この方法はスループットを減らすので、Access Control List (ACL;アクセス コントロール リスト)を使用するよりも少ないオーバヘッドとなります。

インテリジェントな電源管理

この機能はシスコ製の受電装置と連動し、電力ネゴシエーションを使用して、802.3af クラスにより 提供される粒度の電力消費量を超える 802.3af 準拠の受電装置の電力消費量を最適化します。また 電力ネゴシエーションにより、802.3af および IEEE 標準で必要とされるような高電力レベルをサポートしない古いモジュールと新しい受電装置との下位互換性も可能になります。

インテリジェントな電源管理の詳細については第 11 章「PoE の設定」の「インテリジェントな電源管理」を参照してください。

MAC アドレス通知

MAC アドレス通知機能により、Catalyst 4500 シリーズ スイッチによって学習され、エージングアウトし、スイッチから削除された MAC アドレスが監視されます。通知は

CISCO-MAC-NOTIFICATION MIB 経由で送信または取得されます。これは一般的に、ホストが移動するたびに MAC アドレス通知イベントを収集する中央ネットワーク管理アプリケーションによって使用されます。潜在的な DoS 攻撃 (サービス拒絶攻撃)または man-in-the-middle 攻撃を通知するよう、ユーザ設定可能な MAC テーブル利用率しきい値を定義できます。

MAC アドレス通知の詳細については、第4章「スイッチの管理」を参照してください。

MAC 通知 MIB

MAC 通知 MIB 機能はネットワーク パフォーマンス、利用率、およびセキュリティ状態を監視します。これにより、ネットワーク管理者はイーサネット フレームを転送するスイッチ上で学習または 削除された MAC アドレスを追跡できます。

NetFlow 統計情報

NetFlow 統計情報は、グローバル トラフィックのモニタリング機能で、スイッチを通過するすべての IPv4 ルーテッド トラフィックについてフローレベルの監視を可能にします。ルーテッド IP フローおよびスイッチド IP フローの両方をサポートします。

NetFlow 統計情報の詳細については、第48章「NetFlowの設定」を参照してください。

SSH

Secure Shell (SSH; セキュア シェル) は、ネットワークを介して別のコンピュータにログインして、リモートでコマンドを実行し、あるマシンから別のマシンにファイルを移動できるようにするプログラムです。スイッチからは SSH 接続を開始できません。SSH はスイッチへのリモート ログインセッションの提供のみに限定され、サーバとしてのみ機能します。

SNMP

SNMP はネットワーク デバイス間での管理情報の交換を効率化します。Catalyst 4500 シリーズ スイッチは、次の SNMP タイプと拡張をサポートしています。

- SNMP 完全なインターネット標準
- SNMP v2 コミュニティベースの SNMP バージョン 2 用管理フレームワーク
- SNMP v3 noAuthNoPriv、authNoPriv、および authPriv の 3 つのレベルを持つセキュリティ フレームワーク (cat4000-i5k91s-mz などのクリプト イメージでのみ使用可能)
- SNMP トラップ メッセージ拡張 スパニングツリー トポロジの変更通知や設定変更通知を含む、特定の SNMP トラップ メッセージの追加情報

SNMP の詳細については、第47章「SNMPの設定」を参照してください。

SPAN および RSPAN

Switched Port Analyzer (SPAN; スイッチド ポート アナライザ) は、ネットワーク アナライザまた は Remote Monitoring (RMON)プローブによってポート上の解析用トラフィックを監視します。また、次の事項が可能になります。

- SPAN セッション上の ACL を設定します。
- SPAN 宛先ポート上の着信トラフィックが通常どおりスイッチングされるようにします。
- 宛先ポートからスパンされたパケットのカプセル化タイプを明示的に設定します。
- パケットがユニキャスト、マルチキャスト、またはブロードキャストであるか、パケットが有効であるかどうかに応じて入力スニフィングを制限します。
- トラブルシューティング目的で SPAN 宛先ポートの CPU に送信されたパケット、または SPAN 宛先ポートの CPU からのパケットをミラーリングします。

SPAN については、第45章「SPAN と RSPAN の設定」を参照してください。

Remote SPAN(RSPAN)は、SPAN の拡張機能であり、送信元ポートと宛先ポートが複数のスイッチに分散され、ネットワーク上の複数のスイッチのリモート モニタリングができます。各 RSPAN セッションのトラフィックは、参加するすべてのスイッチ上のその RSPAN セッション専用のユーザ指定 RSPAN VLAN に伝送されます。

RSPAN については、第45章「SPAN と RSPAN の設定」を参照してください。

VRRP

VRRP は、共通の LAN に接続されたルータ間で動作し、これによりルータは LAN クライアントにファーストホップ復元機能を提供します。

VRRP の詳細については、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hiap_c/ch20/haipvrrp.htm

WCCP

Web Content Communication Protocol(WCCP)バージョン 2 レイヤ 2 (L2)リダイレクションにより、Catalyst 4500 シリーズ スイッチはレイヤ 2 (MAC アドレス書き換えを使用して、コンテンツ要求を直接接続されたコンテント エンジンに透過的にリダイレクトします。WCCPv2 L2 リダイレクションはスイッチング ハードウェアで高速化されるので、Generic Routing Encapsulation(GRE; 総称ルーティング カプセル化)を使用したレイヤ 3 (L3)リダイレクションよりも効率的です。キャッシュ クラスタのコンテント エンジンは、頻繁にアクセスされるコンテンツを透過的に保存し、同じコンテンツに関する連続した要求に応じます。この結果、オリジナルのコンテンツ サーバから同ーコンテンツを繰り返し伝送する必要がなくなります。これはポートまたはダイナミック サービスのある HTTP および非 HTTP トラフィックの透過的なリダイレクションをサポートします(Webキャッシング、HTTPS キャッシング、FTP [ファイル転送プロトコル]キャッシング、プロキシキャッシング、メディア キャッシング、およびストリーミング サービスなど)。WCCPv2 L2 リダイレクションは一般的に、地域サイトまたは支店などのネットワーク エッジで透過的なキャッシングを可能にします。WCCPv2 L2 リダイレクションは、PBR または VRF-Lite が設定された同じ入力インターフェイスでイネーブルにできません。L2 リダイレクションのための ACL ベースの分類はサポートされません。

WCCP については、第51章「WCCP バージョン2サービスの設定」を参照してください。

セキュリティ機能

Catalyst 4500 シリーズ スイッチは CLI を通じて、または SNMP などの代替アクセス方式を通じてネットワークの管理と制御を行います。スイッチ ソフトウェアは、次のセキュリティ機能をサポートしています。

- 802.1X ID ベースのネットワーク セキュリティ (p.1-19)
- DAI (p.1-20)
- DHCP スヌーピング (p.1-20)
- フラッディング ブロック (p.1-20)
- ハードウェアベースのコントロール プレーン ポリシング (p.1-21)
- スタティック ホストのための IPSG (p.1-21)
- IPSG (p.1-21)
- ローカル認証、RADIUS、および TACACS+ 認証 (p.1-22)
- NAC (p.1-22)
- ACL によるネットワーク セキュリティ (p.1-22)
- ポート セキュリティ (p.1-23)
- ストーム制御 (p.1-23)
- uRPF ストリクト モード (Supervisor Engine 6-E のみ) (p.1-23)
- ユーティリティ (p.1-24)

802.1X ID ベースのネットワーク セキュリティ

このセキュリティ機能の内容は、次のとおりです。

- 802.1X プロトコル この機能は、スイッチ ポートに接続したホストにスイッチ サービスへの アクセス権を割り当てる前に、そのホストを認証するための手段を提供します。
- VLAN の割り当てを使用した 802.1X この機能により、802.1X 非対応ホストが 802.1X 認証を 使用するネットワークにアクセスできます。
- 802.1X RADIUS アカウンティング この機能により、ネットワーク デバイスの使用状況を追跡できます。
- ゲスト VLAN に対する 802.1X 認証 この機能により、VLAN 割り当てを使用して特定のユーザのネットワーク アクセスを制限できます。
- MAC 認証バイパス機能のある 802.1X この機能により、802.1X サプリカント機能のないエージェントレス デバイス (プリンタなど) へのネットワーク アクセスを提供します。 スイッチポートで新しい MAC アドレスを検出すると、Catalyst 4500 シリーズ スイッチはデバイスの MAC アドレスに基づき、802.1X 認証要求をプロキシします。
- アクセス不能認証バイパス機能のある 802.1X AAA サーバが到達不能である、または応答しない場合、この機能が適用されます。この場合、ポートがクローズされていると 802.1X ユーザ認証は一般的に失敗し、ユーザのアクセスが拒否されます。アクセス不能認証バイパス機能は、ローカルに指定された VLAN で重要なポート ネットワーク アクセスを許可するための、Catalyst 4500 シリーズ スイッチ上で設定可能な代替手段を提供します。
- 単方向制御ポートを使用する 802.1X この機能により、Wake-on-LAN (WoL) マジック パケットは無許可の 802.1X スイッチ ポートに接続されたワークステーションに到達できます。 単方向制御ポートは一般的に、中央サーバからワークステーションへオペレーティング システムまたはソフトウェアのアップデートを夜間に送出するために使用されます。
- 802.1X 認証失敗オープン割り当て この機能により、デバイスが 802.1X 経由の自身の認証に 失敗した (たとえば、正しいパスワードが提供できない)場合に処理するようスイッチを設定できます。

- 音声 VLAN 搭載の 802.1X この機能により、Cisco IP Phone と 802.1X サプリカント サポート デバイスの両方を使用する際、ポート上の 802.1X セキュリティが使用できます。
- 802.1X コンバージェンス この機能により、802.1X 設定および実装のスイッチング ビジネス ユニット間の一貫性を保ちます。
- Multi-Domain Authentication (MDA) データ デバイスと IP Phone (Cisco または Cisco 以外) などの音声デバイスの両方が、同じスイッチ ポートで認証可能になり、データ ドメインと音声ドメインに分割されます。

802.1X ID ベースのネットワーク セキュリティの詳細については、第 37 章「802.1X ポートベース 認証の設定」を参照してください。

DAI

Dynamic ARP Inspection(DAI; ダイナミック ARP インスペクション)は、すべての Address Resolution Protocol (ARP; アドレス解決プロトコル) 要求を代行受信し、信頼できないポートで応答し、各代行受信済みパケットを有効な IP/MAC バインディングと照合します。DAI は、同一の VLAN の他のポートに無効な ARP 応答をリレーしないことにより、ネットワーク攻撃を防止します。拒否された ARP パケットは、監査のためにスイッチによって記録されます。

DAIの詳細については、第41章「DAIの設定」を参照してください。

DHCP スヌーピング

DHCP スヌーピングは、DHCP サーバを構成するセキュリティ機能です。DHCP スヌーピングは、信頼できない DHCP メッセージを代行受信し、DHCP スヌーピング バインディング テーブルを構築および保守することで安全性をもたらします。信頼できないメッセージとは、ネットワークまたはファイアウォール外部からの受信メッセージのうち、ネットワーク内でトラフィック攻撃を引き起こす可能性のあるメッセージのことです。

DHCP スヌーピングは、信頼できないホストと DHCP サーバ間でファイアウォールのように機能します。また、DHCP スヌーピングはエンドユーザに接続する信頼できないインターフェイスと DHCP サーバまたは別のスイッチに接続する信頼できるインターフェイスとを見分ける方法を提供します。

DHCP サーバの設定については、次の URL の『Cisco IOS IP and IP Routing Configuration Guide』の「Configuring DHCP」を参照してください。

 $http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ip_c/ipcprt1/1cddhcp.htm$

DHCP スヌーピングの設定手順については、第 40 章「DHCP スヌーピング、IP ソース ガード、およびスタティック ホストの IPSG の設定」を参照してください。

フラッディング ブロック

フラッディング ブロックにより、ユーザはポート単位でユニキャストおよびマルチキャスト パケットのフラッディングをディセーブルにできます。MAC アドレスが期限切れ、またはスイッチによって学習されなかったために、保護されていないポートからの不明のユニキャストまたはマルチキャスト トラフィックが保護されたポートにフラッディングすることがあります。

フラッディング ブロックの詳細については、第 43 章「ポート ユニキャストおよびマルチキャストフラッディング ブロック」を参照してください。

ハードウェアベースのコントロール プレーン ポリシング

コントロール プレーン ポリシングは、ハードウェアの CPU 行きコントロール プレーン トラフィックのレートを制限する統合ソリューションを提供します。これにより、ユーザはシステム全体にコントロール プレーン ACL をインストールして、レート制限するまたは悪意のある DoS 攻撃を排除することで CPU を保護できます。コントロール プレーン ポリシングにより、ネットワークの安定、アベイラビリティ、およびパケット転送を確実にし、スイッチ上での攻撃や重い負荷にもかかわらず、プロトコル アップデートの損失などのネットワーク停止を回避します。 ハードウェア ベースのコントロール プレーン ポリシングは、出荷された Catalyst 4500 スーパーバイザ エンジンすべてで利用できます。 これは、さまざまなレイヤ 2 およびレイヤ 3 コントロール プロトコル (CDP、EAPOL、STP、DTP、VTP、ICMP、CGMP、IGMP、DHCP、RIPv2、OSPF、PIM、TELNET、SNMP、HTTP、および宛先が 224.0.0.* マルチキャスト リンク ローカル アドレスであるパケット)をサポートします。事前定義されたシステム ポリシーまたはユーザ設定可能なポリシーはこれらのプロトコルに適用できます。

コントロール プレーン ポリシングの詳細については、第 39 章「コントロール プレーン ポリシングの設定」を参照してください。

スタティック ホストのための IPSG

この機能により、ARP パケットによるスタティック ホストから学習した IP アドレスのセキュリティを保護してから、デバイスのトラッキング データベースを使用して指定された MAC アドレスにその IP アドレスをバインドできます。そのため、エントリがリンク ダウン イベント全体で存続可能です。

スタティック ホストのための IP Source Gard (IPSG; IP ソースガード) により、DHCP ホストおよびスタティック ホスト両方 (例えば、DHCP スヌーピング バインディング データベースおよびデバイスのトラッキング データベースの両方において)のポートおよび MAC アドレスごとに複数のバインドを実行できます。さらに、限度を超過した場合に処理を実行できます。

スタティック ホストのための IPSG の設定手順については、第40章「DHCP スヌーピング、IP ソース ガード、およびスタティック ホストの IPSG の設定」を参照してください。

IPSG

この機能は、DHCP スヌーピングと同様、DHCP スヌーピングに設定された信頼できないレイヤ 2 ポートでイネーブルにされます。最初に、DHCP スヌーピング処理によってキャプチャされた DHCP パケットを除くポート上のすべての IP トラフィックが、ブロックされます。クライアントが DHCP サーバから有効な IP アドレスを受信すると、Per-Port and VLAN Access Control List (PVACL) がポート上にインストールされ、割り当てられた IP アドレスを持つクライアントだけにクライアント IP トラフィックを制限します。これにより、DHCP サーバによって割り当てられていない送信元 IP アドレスを持つ IP トラフィックが排除されます。このフィルタリングは、悪意のあるホストが隣接ホストの IP アドレスをハイジャックすることによってネットワークを攻撃するのを防ぎます。

IP ソースガードの設定手順については、第 40 章「DHCP スヌーピング、IP ソース ガード、および スタティック ホストの IPSG の設定」を参照してください。

ローカル認証、RADIUS、および TACACS+ 認証

RADIUS および Terminal Access Controller Access Control System Plus (TACACS+) がスイッチへの アクセスを制御します。詳細については、次の URL の『Cisco IOS Security Configuration Guide』 Release 12.1 の「Authentication, Authorization, and Accounting (AAA)」を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/secur_c/scprt1/index.htm

NAC

Network Admission Control (NAC) は次の2つの機能で構成されます。

• NAC レイヤ 2 IP 検証

NAC L2 IP は、Cisco NAC の不可欠な機能です。この機能は、感染したホスト(LAN ポートに接続する PC および他のデバイス)が企業ネットワークに接続しようとした時点で最初に防御します。Cisco Catalyst 4500 シリーズ スイッチの NAC L2 IP は、ネットワークのレイヤ 2 エッジで、非 802.1X 対応ホスト デバイスに対するポスチャ検証を実行します。ホスト デバイスのポスチャ検証には、アンチウイルスの状態や OS パッチ レベルも含まれます。企業アクセス ポリシーとホスト デバイスのポスチャに応じて、ホストは無条件に許可されたり、制限付きアクセスが許可されたり、またはネットワークへのウイルス感染を防ぐために完全に隔離されたりすることがあります。

レイヤ2IP検証の詳細については、次のURLを参照してください。

 $http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_configuration_guide09186a00805764fd.html$

NAC レイヤ 2 802.1X 認証

Cisco Catalyst 4500 シリーズ スイッチは、802.1X 対応デバイスにまで NAC サポートを拡張します。NAC L2 IP と同様に、NAC L2 802.1X 機能でもエンドポイント情報に基づいて、ネットワーク アクセス レベルを決定します。

ACL によるネットワーク セキュリティ

ACL は、ルータ インターフェイスでのルーテッド パケットの転送またはブロックを制御して、ネットワーク トラフィックをフィルタ処理します。 Catalyst 4500 シリーズ スイッチは各パケットを調べ、アクセス リスト内で指定した基準に基づいて、パケットの転送またはドロップを決定します。

MAC Access Control List(MACL)と VACL がサポートされています。VACL は Cisco IOS では VLAN マップとして認識されます。

次のセキュリティ機能がサポートされています。

- VLAN インターフェイス上の MAC アドレスのユニキャスト トラフィックをブロックすること を可能にする MAC アドレス フィルタリング
- 着信トラフィックに対してスイッチ上のレイヤ 2 インターフェイスに ACL を適用することを可能にするポート ACL

ACL、MACL、VLAN マップ、MAC アドレス フィルタリング、およびポート ACL の詳細については、第42章「ACL によるネットワーク セキュリティの設定」を参照してください。

ポート セキュリティ

ポート セキュリティは、ポートにアクセスするワークステーションの MAC アドレスに基づいて ポートのトラフィックを制限します。トランク ポート セキュリティは、この機能を VLAN 単位の トランク (Private VLAN [PVLAN] の独立型トランクを含む) にまで拡張します。

スティッキ ポート セキュリティは、ポートのリンク ダウンおよびスイッチのリセットに備えるため、動的に学習された MAC アドレスを実行コンフィギュレーションに保存することでポート セキュリティを拡張します。これにより、ネットワーク管理者は許可される MAC アドレスまたは各ポートの MAC アドレスの最大数を制限できます。

音声 VLAN スティッキ ポート セキュリティは、スティッキ ポート セキュリティを Voice-over-IP (VoIP) 展開にまで拡張します。音声 VLAN スティッキ ポート セキュリティは、ポートをロックし、IP Phone および IP Phone の背後のワークステーションとは異なる MAC アドレスのあるステーションからのアクセスをブロックします。

ポート セキュリティの詳細については、第38章「ポート セキュリティの設定」を参照してください。

ストーム制御

プロードキャスト抑制は、1 つまたは複数のスイッチ ポート上で、LAN がプロードキャストストームによって混乱しないようにする機能です。LAN のプロードキャスト ストームは、プロードキャスト パケットが LAN にフラッディングすると発生し、過剰なトラフィックが生み出され、ネットワーク パフォーマンスを低下させます。プロトコルスタック実装またはネットワーク設定のエラーが、ブロードキャスト ストームの原因になります。マルチキャストおよびプロードキャスト抑制は、ポートを通過するブロードキャストトラフィックの量を測定し、特定のタイム インターバルでブロードキャストトラフィックを一部の設定可能なしきい値の値と比較します。ブロードキャストトラフィックの量がこのインターバルの間にしきい値に達すると、ブロードキャストフレームがドロップされ、任意でポートがシャットダウンします。

Cisco IOS Software Release 12.2(40)SG では、ブロードキャスト トラフィックおよびマルチキャストトラフィックのポート単位での抑制が可能です (Supervisor Engine 6-E のみ)。

ブロードキャスト抑制の設定手順については、第44章「ストーム制御の設定」を参照してください。

uRPF ストリクト モード (Supervisor Engine 6-E のみ)

Unicast Reverse-path Forwarding(uRPF; ユニキャスト RPF)機能は、検証可能な送信元 IP アドレスが不足している IP パケットを廃棄することで、間違ったまたは偽造(スプーフィングされた)送信元 IP アドレスがネットワークに流れて発生する問題を軽減するのに役立ちます。uRPF が IP ルーティング テーブルと整合性の取れた有効な送信元アドレスを持つパケットだけを転送することによって、DoS 攻撃および DDoS 攻撃をそらします。これにより、お客様のネットワーク、ISP、および残りのインターネットが保護されます。uRPF をストリクト モードで使用する場合は、ルータが戻りパケットの転送に使用するインターフェイスでパケットを受信する必要があります。URPF スクリプト モードは、IPv4 および IPv6 プレフィックスの両方でサポートされています。Hardware IPv6 の IPv6 Forwarding は次世代の IP プロトコルで、IP プロトコルに元々存在するさまざまな問題を解決することを目的としています。

ブロードキャスト抑制の設定手順については、第 29 章「ユニキャスト RPF の設定」を参照してください。

ユーティリティ

レイヤ 2 traceroute

レイヤ 2 traceroute により、スイッチはパケットが送信元デバイスから宛先デバイスへ送信される間に通過する物理パスを識別できます。 レイヤ 2 traceroute は、ユニキャスト送信元および宛先 MAC アドレスにのみ対応します。

レイヤ2 traceroute については、第7章「ポートのステータスと接続の確認」を参照してください。

TDR

Time Domain Reflectometry (TDR; タイム ドメイン反射率計)は、ケーブルの状態および信頼性の診断に使用されるテクノロジーです。TDR は、オープン、ショート、または終端のケーブル状態を検出します。また、障害ポイントまでの距離計算もサポートします。

TDR については、第7章「ポートのステータスと接続の確認」を参照してください。

デバッグ機能

Catalyst 4500 シリーズ スイッチには、初期設定をデバッグするためのコマンドがいくつかあります。これらのコマンドは、次のグループに含まれます。

- platform
- debug platform

詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』を参照してください。

Metro の機能

Resilient Ethernet Protocol

Resilient Ethernet Protocol (REP) はシスコ独自のプロトコルで、Spanning Tree Protocol (STP; スパニング ツリー プロトコル) の代わりにネットワーク ループを制御し、リンク障害を処理して、コンバージェンス時間を改善します。REP は、セグメントに接続されているポートのグループを制御することで、セグメントでブリッジング ループが作成されないようにし、セグメント内のリンク障害に応答します。REP は、より複雑なネットワークを構築するための基盤を提供するもので、VLANロード バランシングをサポートしています。

詳細については、次の URL を参照してください。

 $http://www.cisco.com/en/US/products/hw/switches/ps5532/products_configuration_guide_chapter09186a0080878947.html$

■ Metro の機能



CHAPTER

2

CLI

この章では、Catalyst 4500 シリーズ スイッチの設定に使用する CLI (コマンドライン インターフェイス)について説明します。この章の主な内容は、次のとおりです。

- スイッチ CLI へのアクセス (p.2-2)
- コマンドラインの処理 (p.2-4)
- ヒストリ置換 (p.2-4)
- Cisco IOS コマンド モードの概要 (p.2-5)
- コマンド リストおよび構文の取得 (p.2-7)
- ROMMON @ CLI (p.2-9)



この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/cr/index.htm

次の CLI コマンドは、その他のスーパーバイザ エンジンと比べて Supervisor Engine 6-E では変わります。

- verify および squeeze コマンドは FAT ファイル システムではサポートされません。
- rename コマンドは FAT ファイル システムではサポートされます。
 Supervisor Engine 6-E では、rename コマンドはブートフラッシュおよび slot() で追加されています。それ以外のフェパーバイザ エンジンでは、rename コマンドは NVPAM (不揮発性 PAM)
- す。それ以外のスーパーバイザ エンジンでは、rename コマンドは NVRAM(不揮発性 RAM) デバイスでのみサポートされています。
- fsck コマンドは slot0 デバイスでサポートされていますが、6-E 以外のスーパーバイザ エンジンのファイル システムではサポートされていません。

スイッチ CLI へのアクセス

ここではスイッチ CLI へのアクセス方法について説明します。

- EIA/TIA-232 コンソール インターフェイスを使用して CLI にアクセスする場合 (p.2-2)
- Telnet を使用して CLI にアクセスする場合 (p.2-2)

EIA/TIA-232 コンソール インターフェイスを使用して CLI にアクセスする場合



(注)

EIA/TIA-232 は、EIA(米国電子工業会)および TIA(米国電気通信工業会)によって標準として 認定されるまでは、Recommended Standard 232 (RS-232)と呼ばれていました。

スイッチの初期設定は、EIA/TIA-232 コンソール インターフェイスに接続して行います。コンソー ル インターフェイスのケーブル接続手順については、『Catalyst 4500 Series Switch Module Installation Guide』を参照してください。

コンソール インターフェイスを経由してスイッチにアクセスするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch> enable	ユーザ EXEC プロンプト (>) から、enable を入力して、特権
		モード(別名、特権 EXEC モード)に変更します。
ステップ 2	Password: password	パスワード プロンプトで、システムパスワードを入力します。
	Switch#	プロンプト(#)が表示され、特権モードで CLI にアクセスした ことを示します。
ステップ 3	Switch# quit	作業コマンドの実行が終了したあと、セッションを終了します。

EIA/TIA-232 インターフェイスを経由してスイッチにアクセスしたあと、次のように表示されます。

Press Return for Console prompt

Switch> enable Password: < > Switch#

Telnet を使用して CLI にアクセスする場合



スイッチに Telnet を接続する前に、スイッチの IP アドレスを設定する必要があります。「物理レイ ヤ3インターフェイスの設定」(p.27-14)を参照してください。

このスイッチは、最大8つの Telnet セッションを同時にサポートします。 Telnet セッションは、ア イドル状態のまま exec-timeout コマンドで指定した時間が経過すると、自動的に切断されます。

スイッチに Telnet を接続するには、次の作業を行います。

	コマンド	目的
ステップ 1	telnet {hostname ip_addr}	リモート ホストから telnet コマンドと、アクセスするスイッチ
		の名前または IP アドレスを入力します。
ステップ 2	Password: password	プロンプトで、CLI のパスワードを入力します。パスワードを
	Switch#	設定していない場合は、Returnキーを押します。
ステップ 3		作業に必要なコマンドを入力します。
ステップ 4	Switch# quit	Telnet セッションを終了します。

次に、スイッチとの Telnet セッションを開始する例を示します。

unix_host% telnet Switch_1
Trying 172.20.52.40...
Connected to 172.20.52.40.
Escape character is '^]'.
User Access Verification
Password:< >
Switch_1> enable
Password:
Switch_1#

コマンドラインの処理

スイッチ コマンドでは、大文字と小文字が区別されません。また、コマンドおよびパラメータは、現在使用可能な他のコマンドまたはパラメータと区別可能な文字数まで省略できます。

最後に入力した 20 個のコマンドはヒストリ バッファに保存されるので、これらのコマンドをスクロールして、プロンプトに入力または編集できます。表 2-1 に、スイッチ コマンドの入力および編集に使用するキーボード ショートカットを示します。

表 2-1 キーボード ショートカット

キーストローク	結果
Ctrl-B または 左矢印 キー ¹ を押す	カーソルを1文字分だけ後退させます。
Ctrl-F または 右矢印 キー ¹ を押す	カーソルを1文字分だけ進めます。
Ctrl-A を押す	コマンドラインの先頭にカーソルを移動します。
Ctrl-E を押す	コマンドラインの末尾にカーソルを移動します。
Esc-B を押す	1 文字分だけカーソルを後退させます。
Esc-F を押す	1 文字分だけカーソルを進めます。

^{1.} 矢印キーは、VT100 などの ANSI 互換端末でのみ有効です。

ヒストリ置換

ヒストリ バッファには、最後に入力した 20 個のコマンド ラインが保存されます。ヒストリ置換によって、再入力せずにコマンド ラインにアクセスできます。表 2-2 に、ヒストリ置換コマンドを示します。

表 2-2 ヒストリ置換コマンド

コマンド	目的
Ctrl-P または上矢印キー ¹	直前に入力したコマンドから順に、ヒストリ バッファに保存されているコマンドを呼び出します。キー シーケンスを繰り返すと、古いコマンドが順に呼び出されます。
Ctrl-N または下矢印キー ¹	Ctrl-P または 上矢印キー でコマンドを呼び出したあとで、ヒストリバッファ内のより新しいコマンドに戻ります。キー シーケンスを繰り返すと、新しいコマンドが呼び出されます。
Switch# show history	EXEC モードで、直前に入力したコマンドをいくつか表示します。

^{1.} 矢印キーは、VT100 などの ANSI 互換端末でのみ有効です。

Cisco IOS コマンド モードの概要



Cisco IOS コマンド モードの詳細については、次の URL の『Cisco IOS Configuration Fundamentals Configuration Guide』 および『Cisco IOS Configuration Fundamentals Command Reference』を参照してください。http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm

Cisco IOS ユーザ インターフェイスには、ユーザ EXEC、特権 EXEC(enable) グローバル コンフィ ギュレーション、インターフェイス、サブインターフェイス、およびプロトコル固有の各モードが あります。現在のモードによって使用できるコマンドが決まります。所定のモードで使用できるコマンドの一覧を表示するには、システム プロンプトに疑問符(?)を入力します。詳細については、「コマンド リストおよび構文の取得」(p.2-7)を参照してください。

スイッチ上でセッションを開始するときには、ユーザ モード(別名、ユーザ EXEC モード)から 始めます。EXEC モードで使用できるのは、限定的なコマンド サブセットです。すべてのコマンド にアクセスするには、特権 EXEC モード(別名、特権モード)を開始する必要があります。特権 EXEC モードにアクセスするには、パスワードを入力する必要があります。特権 EXEC モードでは、任意の EXEC コマンドを入力したり、グローバル コンフィギュレーション モードにアクセスできます。 ほとんどの EXEC コマンドは、現在の設定ステータスを表示する show コマンドや、カウン タまたはインターフェイスをリセットする clear コマンドなどの 1 回限りのコマンドです。スイッチを再起動したときに、EXEC コマンドは保存されません。

コンフィギュレーション モードでは、実行コンフィギュレーションを変更できます。コンフィギュレーションを保存すると、スイッチを再起動したときにこれらのコマンドが保存されます。まず、グローバル コンフィギュレーション モードを開始する必要があります。グローバル コンフィギュレーション モード、サブインターフェイス コンフィギュレーション モード、サブインターフェイス コンフィギュレーション モード、および各種プロトコル固有のモードを開始できます。

スイッチが正しく起動しない場合は、ROMMON と呼ばれる別のモードを使用します。たとえば、スイッチの起動時に有効なシステム イメージがなかった場合、またはコンフィギュレーションファイルが壊れていた場合、ROMMON モードが開始されることがあります。詳細については、「ROMMON の CLI」(p.2-9) を参照してください。

表 2-3 に、よく使用される Cisco IOS モードを示します。

表 2-3 使用頻度の高い Cisco IOS コマンド モード

モード	用途	アクセス方法	プロンプト
ユーザ EXEC	リモート デバイスへの接続、端末の一時的な設定変更、基本的なテストの実行、システム情報を表示します。	ログインします。	Switch>
特権 EXEC (特権)	動作パラメータの設定。特権コマンド セットには、ユーザ EXEC モードで使用できるコマンドとともに、configure コマンドが含まれます。configure コマンドを使用して、別のコマンド モードにアクセスします。	ド(パスワードが設定されている	Switch#
グローバル コンフィギュ レーション	システム時間またはスイッチ名 など、システム全体に影響する機能を設定します。	特権 EXEC モードから configure terminal コマンドを入力します。	Switch(config)#
インターフェイス コン フィギュレーション	interface コマンドで 10 ギガビット イーサネット インターフェイス、ギガビット イーサネット インターフェイス、ファスト イーサネット インターフェイスのいずれかの操作を有効化または修正します。	ション モードから interface type	Switch(config-if)#
コンソール コンフィギュ レーション	直接接続したコンソールまたは 仮想端末から、コンソール イン ターフェイスを設定します。 Telnet で使用します。		Switch(config-line)#

Cisco IOS コマンド インタープリタ (別名、EXEC)が、ユーザが入力したコマンドを解釈して実行します。コマンドおよびキーワードは、他のコマンドと区別できる文字数まで省略して入力できます。たとえば、show コマンドは sh、configure terminal コマンドは config t に省略できます。

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

コマンド リストおよび構文の取得

任意のコマンド モードで、疑問符(?)を入力すると、使用できるコマンドのリストを入手できます。

Switch> ?

特定の文字の並びで始まるコマンド リストを取得するには、該当する文字の後ろに疑問符(?)を入力します。疑問符の前にスペースを入れないでください。この形式のヘルプは、ユーザに代わって1つの単語を完成させるので、ワード ヘルプと呼びます。

キーワードまたは引数の一覧を表示するには、キーワードまたは引数の代わりに疑問符を入力します。疑問符の前にスペースを1つ入れてください。この形式のヘルプは、すでに入力したコマンド、キーワード、および引数に基づいて、使用できるキーワードまたは引数を表示するので、コマンド構文ヘルプと呼びます。

Switch# configure ?

memory Configure from NV memory

network Configure from a TFTP network host

overwrite-network Overwrite NV memory from TFTP network host

terminal Configure from the terminal

<cr>

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



コマンドの入力で問題が生じた場合は、システム プロンプトを確認し、疑問符 (?) を入力して使用できるコマンドのリストを表示してください。コマンド モードが異なる、または構文が間違っている可能性があります。

1 つ前のモードに戻るには、exit を入力します。どのモードの場合でも、Ctrl-Z を押すか、end コマンドを入力すると、ただちに特権 EXEC モードに戻ります。

スタンバイ スーパーバイザ エンジンの仮想コンソール

Catalyst 4500 シリーズ スイッチには、冗長性を持たせるため、2 つのスーパーバイザ エンジンを搭載できます。スイッチに電源が入ると、スーパーバイザ エンジンの 1 つがアクティブになり、スイッチオーバーが発生するまでアクティブのままになります。もう 1 つのスーパーバイザ エンジンはスタンバイ モードのままです。

スーパーバイザ エンジンのそれぞれには、自身のコンソール ポートがあります。スタンバイ スーパーバイザ エンジンのコンソール ポート経由でのみ、スタンバイ スーパーバイザ エンジンにアクセスできます。したがって、スタンバイ スーパーバイザに対するアクセス、監視、またはデバッグを行うには、スタンバイ コンソールに接続する必要があります。

スタンバイ スーパーバイザ エンジンの仮想コンソールを使用すると、スタンバイ コンソールへの 物理的な接続がなくてもアクティブ スーパーバイザ エンジンからスタンバイ コンソールにアクセ スできます。EOBC で IPC を使用してスタンバイ スーパーバイザ エンジンと通信し、アクティブ スーパーバイザ エンジン上でスタンバイ コンソールをエミュレートします。一度にアクティブに できるアクティブ スタンバイ コンソール セッションは 1 つのみです。

スタンバイ スーパーバイザ エンジンの仮想コンソールにより、アクティブ スーパーバイザ エンジンにログオンしているユーザは、スタンバイ スーパーバイザ エンジン上で show コマンドをリモートで実行し、アクティブ スーパーバイザ エンジンでその結果を表示できます。仮想コンソールは、アクティブ スーパーバイザ エンジンからのみ利用できます。

アクティブ スーパーバイザ エンジンからアクティブ スーパーバイザ エンジンの attach module、session module、または remote login コマンドを使用してスタンバイ仮想コンソールにアクセスできます。 これらのコマンドを実行してスタンバイ コンソールにアクセスするには、特権 EXEC モード (レベル 15) を開始している必要があります。

スタンバイ仮想コンソールを開始すると、端末プロンプトは、[<hostname>-standby-console#] に自動的に変更されます(ここで、hostname はスイッチに設定された名前です)。仮想コンソールを終了すると、このプロンプトは元のプロンプトに戻ります。

exit または quit コマンドを入力すると、仮想コンソールは終了します。ログインしたアクティブ スーパーバイザ エンジンの端末の無活動時間が設定されたアイドル時間を超えると、アクティブ スーパーバイザ エンジンの端末から自動的にログアウトします。この場合、仮想コンソール セッションも終了します。また、スタンバイが再起動すると、仮想コンソール セッションも自動的に終了します。スタンバイが起動したあとは、別の仮想コンソール セッションを作成する必要があります。

仮想コンソールを使用してスタンバイ スーパーバイザ エンジンにログインするには、次の操作を 実行します。

Switch# session module 2

Connecting to standby virtual console Type "exit" or "quit" to end this session

Switch-standby-console# **exit**Switch#

スタンバイ コンソールがイネーブルでない場合、次のメッセージが表示されます。

Switch-standby-console# Standby console disabled. Valid commands are: exit, logout



(注)

スタンバイ仮想コンソールには、コマンド履歴、コマンド補完、コマンド ヘルプ、部分コマンド キーワードなど、スーパーバイザコンソールから利用できる標準的な機能が備わっています。

次の制限事項がスタンバイ仮想コンソールに適用されます。

- 仮想コンソールで実行されたコマンドは、すべて最後まで実行されます。auto-more 機能はありません。したがって、terminal length 0 コマンドの実行時と同じように機能します。また、対話形式ではありません。したがって、アクティブ スーパーバイザ エンジン上でキー シーケンスを入力しても、コマンドの実行を中断できません。コマンドによって大量の出力が発生した場合、仮想コンソールはスーパーバイザ画面に出力を表示します。
- 仮想コンソールは対話形式ではありません。仮想コンソールはコマンドのインタラクティブ性を検出しないので、ユーザとの対話を必要とするコマンドが入力されると、RPC タイマーがコマンドを中断するまで仮想コンソールは待機します。

仮想コンソール タイマーは 60 秒に設定されています。60 秒後に仮想コンソールはプロンプトに戻ります。この間、キーボードからコマンドを中断できません。操作を続ける前に、タイマーが期限切れになるのを待つ必要があります。

• 仮想コンソールを使用して、スタンバイ スーパーバイザ エンジン上で表示されているデバッ グおよび Syslog メッセージを表示することはできません。仮想コンソールは、仮想コンソール から実行されたコマンドの出力のみを表示します。実際のスタンバイ コンソールで表示される 別の情報は、仮想コンソールでは表示できません。

ROMMON の CLI

ROMMON は起動時またはリセット時、あるいは重大な例外エラーが発生したときに関与する ROM ベースのプログラムです。スイッチで ROMMON モードが開始されるのは、スイッチが有効なソフトウェア イメージを見つけることができなかった場合、NVRAM 内の設定が壊れていた場合、またはコンフィギュレーション レジスタが ROMMON モードを開始するように設定されていた場合です。 ROMMON モードでは、フラッシュ メモリ、ネットワーク サーバ ファイル、またはブートフラッシュからソフトウェア イメージを手動でロードできます。

また、スイッチを再起動して、起動時の最初の 5 秒間に Ctrl-C を押しても、ROMMON モードを開始できます。



コンフィギュレーション レジスタの設定で、Ctrl-C がオフに設定されている場合でも、スイッチの再起動後 60 秒間は Ctrl-C を使用できます。

ROMMON モードを開始すると、プロンプトが **rommon 1**> に変わります。使用できる ROMMON コマンドを確認する場合は、? コマンドを使用します。

ROMMON コマンドの詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』を 参照してください。

 $http://www.cisco.com/en/US/products/hw/routers/ps380/products_configuration_guide_chapter09186a00801\\18d19.html$



CHAPTER

3

スイッチの初期設定

この章では、Catalyst 4500 シリーズ スイッチを初期設定する方法について説明します。ここに示す情報は、次のマニュアルの管理情報と管理手順を補足するものです。

 次の URL の『Cisco IOS Configuration Fundamentals Command Reference』 Release 12.2SR http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/cr/index.htm

この章の主な内容は、次のとおりです。

- デフォルトのスイッチ設定 (p.3-2)
- DHCP ベースの自動設定の設定 (p.3-2)
- スイッチの設定 (p.3-9)
- 特権 EXEC コマンドへのアクセス制御 (p.3-14)
- イネーブル パスワードを忘れた場合の回復方法 (p.3-26)
- スーパーバイザ エンジンのスタートアップ コンフィギュレーションの変更 (p.3-27)
- スイッチの出荷時のデフォルト設定へのリセット (p.3-34)



この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/cr/index.htm

デフォルトのスイッチ設定

ここでは、Catalyst 4500 シリーズ スイッチのデフォルト設定について説明します。表 3-1 に各機能 のデフォルト設定を示します。

デフォルト スイッチ設定 表 3-1

機能	デフォルト設定
管理用接続	通常 モード
グローバル スイッチ情報	システム名、システムの連絡先、ロケーションにはデフォルト値 が設定されていません。
システム クロック	システム クロック タイムには値が設定されていません。
パスワード	ユーザ モードまたはイネーブル モードのパスワードは設定されていません(Return キーを押してください)。
スイッチ プロンプト	Switch>
インターフェイス	イネーブル。速度とフロー制御は自動ネゴシエーションで、IP アドレスは指定されていません。

DHCP ベースの自動設定の設定

ここでは、Dynamic Host Configuration Protocol (DHCP) ベースの自動設定を設定する手順について 説明します。

- DHCP ベースの自動設定の概要(p.3-2)
- DHCP クライアントの要求プロセス (p.3-3)
- DHCP サーバの設定 (p.3-4)
- TFTP サーバの設定 (p.3-5)
- DNS サーバの設定 (p.3-5)
- リレー装置の設定 (p.3-6)
- コンフィギュレーション ファイルの入手方法 (p.3-6)
- 構成例 (p.3-7)

DHCP サーバがシスコ製デバイスの場合、またはスイッチを DHCP サーバとして設定している場 合、DHCP の設定の詳細については、『Cisco IOS IP and IP Routing Configuration Guide』 Cisco IOS Release 12.1 の「IP Addressing and Services」を参照してください。

DHCP ベースの自動設定の概要



Release 12.2(20)EW 以降では、write erase コマンドを入力することにより、DHCP の自動設定をイ ネーブルにできます。このコマンドにより、NVRAM(不揮発性 RAM)のスタートアップ コンフィ ギュレーションがクリアされます。Release 12.2(20)EW より前のイメージでは、このコマンドは自 動設定をイネーブルにしません。

DHCP は、インターネット ホストおよびインターネットワーキング デバイスに設定情報を提供し ます。このプロトコルには、2 つのコンポーネントが含まれます。1 つは DHCP サーバからデバイ スにコンフィギュレーション パラメータを提供するコンポーネント、もう1つはデバイスにネット ワーク アドレスを割り当てるコンポーネントです。DHCP はクライアント / サーバ モデルに基づいています。指定された DHCP サーバが、動的に設定されるデバイスに対して、ネットワーク アドレスを割り当て、コンフィギュレーション パラメータを提供します。スイッチは、DHCP クライアントとしても DHCP サーバとしても機能できます。

DHCP ベースの自動設定により、スイッチ (DHCP クライアント)が起動時に IP アドレス情報およびコンフィギュレーション ファイルを使用して自動的に設定されるため、スイッチ上での DHCP クライアント側の設定は必要ありません。 ただし、IP アドレスに関連付けられた各種のリース オプションに対しては、DHCP サーバ、またはスイッチ上の DHCP サーバの機能を設定する必要があります。 DHCP を使用して、ネットワーク上のコンフィギュレーション ファイルの位置をリレーする場合は、Trivial File Transfer Protocol (TFTP; 簡易ファイル転送プロトコル) サーバおよび Domain Name System (DNS; ドメイン ネーム システム) サーバの設定が必要な場合もあります。

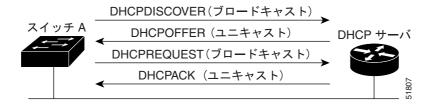
DHCP ベースの自動設定は、スイッチの BOOTP クライアント機能に代わるものです。

DHCP クライアントの要求プロセス

起動時にスイッチ上にコンフィギュレーション ファイルがない場合は、スイッチは DHCP サーバに対して自動的に設定情報を要求します。

図 3-1 に、DHCP クライアントと DHCP サーバ間で交換される一連のメッセージを示します。

図 3-1 DHCP クライアント/サーバ間のメッセージ交換



クライアントであるスイッチ A は、DHCP サーバの場所を特定するために、DHCPDISCOVER メッセージをブロードキャストします。DHCP サーバは、コンフィギュレーション パラメータ (IP アドレス、サブネット マスク、ゲートウェイ IP アドレス、DNS IP アドレス、IP アドレス用のリースなど)を、DHCPOFFER ユニキャスト メッセージでクライアントに提示します。

DHCPREQUEST ブロードキャスト メッセージでは、クライアントは、提示された設定情報に対して、DHCP サーバに正式な要求を戻します。正式な要求はブロードキャストされるため、クライアントから DHCPDISCOVER ブロードキャスト メッセージを受信した他の DHCP サーバはすべて、クライアントに提示した IP アドレスを再利用できます。

DHCP サーバは、DHCPACK ユニキャスト メッセージをクライアントに戻すことで、IP アドレスが クライアントに割り当てられたことを確認します。このメッセージによって、クライアントとサーバはバインドされ、クライアントはサーバから受信した設定情報を使用します。スイッチの受信する情報量は、DHCP サーバの設定方法によって異なります。詳細については、「DHCP サーバの設定」 (p.3-4) を参照してください。

DHCPOFFER ユニキャスト メッセージでクライアントに送信されたコンフィギュレーション パラメータが無効である (コンフィギュレーション エラーがある)場合、クライアントは DHCP サーバに、DHCPDECLINE ブロードキャスト メッセージを戻します。

DHCP サーバはクライアントに、提示されたコンフィギュレーション パラメータが割り当てられていない、パラメータのネゴシエーション中にエラーが発生した、または DHCPOFFER メッセージに対するクライアントの応答が遅れている (DHCP サーバがパラメータを別のクライアントに割り当てた) という意味の DHCPNAK 拒否ブロードキャスト メッセージを送信します。

DHCP クライアントは、複数の DHCP サーバから提示を受け取り、いずれも受け入れることができますが、通常は最初に受け取った提示を受け入れます。DHCP サーバから提示された IP アドレスが必ずしもクライアントに割り当てられるわけではありません。ただし、サーバは通常、クライアントが正式にアドレスを要求するまではアドレスを保管しておきます。

DHCP サーバの設定

スイッチは、DHCP クライアントとしても DHCP サーバとしても機能できます。デフォルトでは、 スイッチの Cisco IOS DHCP サーバおよびリレー エージェント機能はイネーブルになっています。

DHCP サーバ、またはスイッチ上で実行される DHCP サーバの機能に、スイッチ ハードウェア アドレスによって各スイッチにバインドされた専用のリースを設定する必要があります。

スイッチに IP アドレス情報を受信させる場合は、DHCP サーバに次のリース オプションを設定する必要があります。

- クライアントの IP アドレス (必須)
- クライアントのサブネットマスク(必須)
- DNS サーバの IP アドレス (任意)
- ルータの IP アドレス (必須)



ルータの IP アドレスは、スイッチのデフォルト ゲートウェイ アドレスです。

スイッチに TFTP サーバからコンフィギュレーション ファイルを受信させる場合は、DHCP サーバに次のリース オプションを設定する必要があります。

- TFTP サーバの名前または IP アドレス(必須)
- ブート ファイル名 (クライアントが必要なコンフィギュレーション ファイル名)(推奨)
- ホスト名(任意)

DHCP サーバ、またはスイッチ上で実行される DHCP サーバの機能の設定によっては、スイッチは IP アドレス情報またはコンフィギュレーション ファイル、あるいはその両方を受信できます。

DHCP サーバ、またはスイッチ上で実行される DHCP サーバの機能に、上記のリース オプションを 設定しない場合は、スイッチはクライアントの要求に対して、設定されているパラメータだけで応 答します。IP アドレスおよびサブネット マスクが応答に含まれていないと、スイッチは設定され ません。ルータの IP アドレスまたは TFTP のサーバ名 (または IP アドレス) が見つからなかった 場合、スイッチは TFTP 要求をユニキャストしないでブロードキャストする場合があります。その 他のリース オプションは、使用できなくても自動設定には影響しません。

DHCP サーバ、またはスイッチ上で実行される DHCP サーバの機能は、同じ LAN 上に配置することも、そのスイッチとは別の LAN 上に配置することもできます。DHCP サーバが別の LAN 上で稼働している場合は、2 つの直接接続された LAN 間のブロードキャスト トラフィックを転送する DHCP リレーを設定する必要があります。ルータはブロードキャスト パケットを転送しませんが、受信されるパケットの宛先 IP アドレスに基づいてパケットを転送します。リレー装置の詳細については、「リレー装置の設定」(p.3-6)を参照してください。

TFTP サーバの設定

DHCP サーバの設定に基づいて、スイッチは TFTP サーバから 1 つまたは複数のコンフィギュレーション ファイルのダウンロードを試行します。TFTP サーバへの IP 接続に必要なすべてのオプションについてスイッチに応答するよう DHCP を設定している場合、および TFTP サーバ名、アドレス、およびコンフィギュレーション ファイル名を使用して DHCP サーバを設定した場合、スイッチは指定された TFTP サーバから指定されたコンフィギュレーション ファイルをダウンロードしようとします。

コンフィギュレーション ファイル名、および TFTP サーバを指定しなかった場合、またはコンフィギュレーション ファイルをダウンロードできなかった場合は、スイッチはファイル名と TFTP サーバアドレスをさまざまに組み合わせてコンフィギュレーション ファイルをダウンロードしようとします。ファイルには、(ある場合)特定のコンフィギュレーション ファイル名と次のファイルが指定されています。network-config、cisconet.cfg、hostname.config、または hostname.cfg です。この場合、hostname はスイッチおよび router-confg と ciscortr.cfg の現在のホスト名です。使用されるTFTP サーバアドレスには、(ある場合)指定された TFTP サーバのアドレス、およびブロードキャストアドレス(255.255.255.255)が含まれています。

スイッチが正常にコンフィギュレーション ファイルをダウンロードするには、TFTP サーバは、そのベース ディレクトリに 1 つまたは複数のコンフィギュレーション ファイルを含んでいる必要があります。設定できるファイルは、次のとおりです。

- DHCP 応答の名前付きコンフィギュレーション ファイル (実際のスイッチ コンフィギュレーション ファイル)
- network-confg または cisconet.cfg ファイル (デフォルトのコンフィギュレーション ファイル)
- router-confg または ciscortr.cfg ファイル(これらのファイルには、すべてのスイッチに共通のコマンドが含まれています。通常、DHCP および TFTP サーバが適切に設定されていれば、これらのファイルはアクセスされません。)

DHCP サーバリース データベースに TFTP サーバ名を指定する場合は、DNS サーバのデータベースに TFTP サーバ名と IP アドレスのマッピングを設定する必要もあります。

使用する TFTP サーバが、スイッチとは異なる LAN 上にある場合、またはスイッチがブロードキャスト アドレスを使用してアクセスした場合(前述のすべての必須情報が DHCP サーバの応答に含まれていない場合に発生)は、リレーを設定して TFTP サーバに TFTP パケットを転送する必要があります。詳細については、「リレー装置の設定」(p.3-6)を参照してください。DHCP サーバ、またはスイッチ上で実行される DHCP サーバの機能のいずれかに、すべての必須情報を使用して設定することを推奨します。

DNS サーバの設定

DHCP サーバ、またはスイッチ上で実行される DHCP サーバの機能は、DNS サーバを使用して TFTP サーバ名を IP アドレスに変換します。 DNS サーバ上で、TFTP サーバ名から IP アドレスへのマッピングを設定する必要があります。 TFTP サーバには、スイッチのコンフィギュレーション ファイルが含まれます。

DNS サーバの IP アドレスを、DHCP 応答が IP アドレスを取得する DHCP サーバのリース データベースに設定できます。リース データベースには、DNS サーバの IP アドレスを最大 2 つまで入力できます。

DNS サーバは、スイッチと同じ LAN 上に存在しても、またスイッチとは別の LAN 上に存在していてもかまいません。 DNS サーバが別の LAN 上に存在する場合、スイッチはルータを介して DNS サーバにアクセス可能である必要があります。

リレー装置の設定

スイッチが、別の LAN 上のホストからの応答を必要とするブロードキャスト パケットを送信する場合は常に、受信されるブロードキャスト パケットを宛先ホストに転送するようリレー装置を設定する必要があります。このようなブロードキャスト パケットの例として DHCP パケット、DNS パケット、場合によっては TFTP パケットが挙げられます。

リレー装置がシスコ製 ルータである場合、IP ルーティングをイネーブルにし (ip routing グローバル コンフィギュレーション コマンド)、ヘルパー アドレスを設定します (ip helper-address インターフェイス コンフィギュレーション コマンド)。図 3-2 では、ルータ インターフェイスを次のように設定しています。

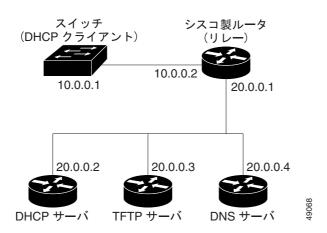
インターフェイス 10.0.0.2 では、

```
router(config-if)# ip helper-address 20.0.0.2
router(config-if)# ip helper-address 20.0.0.3
router(config-if)# ip helper-address 20.0.0.4
```

インターフェイス 20.0.0.1 では、

router(config-if)# ip helper-address 10.0.0.1

図 3-2 自動設定でのリレー装置の使用



コンフィギュレーション ファイルの入手方法

DHCP 予約リースの IP アドレスおよびコンフィギュレーション ファイル名のアベイラビリティに応じて、スイッチは次の方法で設定情報を入手します。

- IP アドレスおよびコンフィギュレーション ファイル名が、スイッチ用に予約され、DHCP 応答 (1ファイル読み込み方式)で提供されます。
 - スイッチは、DHCP サーバまたはスイッチ上で実行される DHCP サーバ機能のいずれかから、IP アドレス、サブネット マスク、TFTP サーバ アドレス、およびコンフィギュレーション ファイル名を受信します。スイッチは、TFTP サーバにユニキャスト メッセージを送信して、名前付きコンフィギュレーション ファイルをサーバのベース ディレクトリから取得して、受信後、ブートアップ プロセスを完了します。
- DHCP 応答に TFTP サーバ アドレスが含まれていない場合(1ファイル読み込み方式)、スイッチの IP アドレスおよびコンフィギュレーション ファイル名が予約されます。

スイッチは、DHCP サーバから IP アドレス、サブネット マスク、およびコンフィギュレーション ファイル名を DHCP サーバまたはスイッチ上で実行される DHCP サーバ機能のいずれかから受信します。スイッチは、TFTP サーバにブロードキャスト メッセージを送信して、名前付きコンフィギュレーション ファイルをサーバのベース ディレクトリから取得して、受信後、ブートアップ プロセスを完了します。

• IP アドレスだけがスイッチ用に予約され、DHCP 応答で提供されます。コンフィギュレーションファイル名は提供されません(2ファイル読み込み方式)。

スイッチは、DHCP サーバ、またはスイッチ上で実行される DHCP サーバ機能のいずれかから IP アドレス、サブネット マスク、および TFTP サーバ アドレスを受信します。スイッチは、TFTP サーバにユニキャスト メッセージを送り、network-confg または cisconet.cfg のデフォルトのコンフィギュレーション ファイルを取得します (network-confg ファイルが読み込めない場合、スイッチは cisconet.cfg ファイルを読み込みます)。

デフォルトのコンフィギュレーション ファイルには、スイッチのホスト名から IP アドレスへのマッピングが含まれています。スイッチは、ファイルの情報をホスト テーブルに書き込み、ホスト名を入手します。ファイルでホスト名が見つからない場合、スイッチは DHCP 応答のホスト名を使用します。DHCP 応答でホスト名が指定されていない場合、スイッチはデフォルトの Switch をホスト名として使用します。

デフォルトのコンフィギュレーション ファイルまたは DHCP 応答からホスト名を入手したあと、スイッチはホスト名と同じ名前のコンフィギュレーション ファイル (network-confg または cisconet.cfg のどちらが先に読み込まれたかに応じて、hostname-confg または hostname.cfg) を TFTP サーバから読み込みます。cisconet.cfg ファイルが読み込まれている場合は、ホストのファイル名は 8 文字に切り捨てられます。

network-confg、cisconet.cfg、またはホスト名と同じ名前のファイルを読み込むことができない場合、スイッチは router-confg ファイルを読み込みます。スイッチが router-confg ファイルを読み込めない場合は、ciscortr.cfg ファイルを読み込みます。



(注)

次のいずれかの場合に、スイッチは TFTP サーバ要求をブロードキャストします。1) DHCP 応答から TFTP サーバを入手できなかった場合、2) ユニキャスト伝送によるコンフィギュレーションファイルの読み込みに失敗した場合、3) TFTP サーバ名を IP アドレスに変換できない場合

構成例

図 3-3 に、DHCP ベースの自動設定を使用して IP 情報を取得するネットワークの例を示します。

図 3-3 DHCP ベースの自動設定を使用するネットワークの構成例

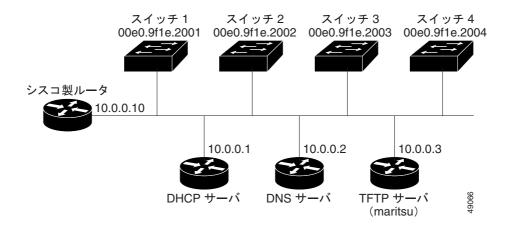


表 3-2 に、DHCP サーバ、またはスイッチ上で実行される DHCP サーバ機能の専用のリースのコンフィギュレーションを示します。

表 3-2 DHCP サーバのコンフィギュレーション

	スイッチ 1	スイッチ 2	スイッチ 3	スイッチ 4
バインディング キー	00e0.9f1e.2001	00e0.9f1e.2002	00e0.9f1e.2003	00e0.9f1e.2004
(ハードウェア アドレス)				
IP アドレス	10.0.0.21	10.0.0.22	10.0.0.23	10.0.0.24
サブネット マスク	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
ルータ アドレス	10.0.0.10	10.0.0.10	10.0.0.10	10.0.0.10
DNS サーバ アドレス	10.0.0.2	10.0.0.2	10.0.0.2	10.0.0.2
TFTP サーバ名	maritsu または 10.0.0.3	maritsu または 10.0.0.3	maritsu または 10.0.0.3	maritsu または 10.0.0.3
ブート ファイル名 (コン	switch1-confg	switch2-confg	switch3-confg	switch4-confg
フィギュレーション ファ				
イル)(任意)				
ホスト名(任意)	switch 1	switch 2	switch 3	switch 4

DNS サーバ コンフィギュレーション

DNS サーバは、TFTP サーバ名 maritsu を IP アドレス 10.0.0.3 にマッピングします。

TFTP サーバ コンフィギュレーション (UNIX)

TFTP サーバのベース ディレクトリは、/tftpserver/work/ に設定されています。このディレクトリには、2 ファイル読み込み方式で使用される network-confg ファイルがあります。このファイルには、IP アドレスに基づいてスイッチに割り当てられるホスト名が含まれています。ベース ディレクトリには、次に示すように、各スイッチのコンフィギュレーション ファイル (switch1-confg、switch2-confg など)も含まれています。

```
prompt> cd /tftpserver/work/
prompt> ls
network-confg
switch1-confg
switch3-confg
switch4-confg
prompt> cat network-confg
ip host switch1 10.0.0.21
ip host switch2 10.0.0.22
ip host switch3 10.0.0.23
ip host switch4 10.0.0.24
```

DHCP クライアント コンフィギュレーション

スイッチ1~4には、コンフィギュレーションファイルは存在しません。

コンフィギュレーションの説明

図 3-3 の場合、スイッチ 1 はコンフィギュレーション ファイルを次のようにして読み込みます。

- スイッチ 1 は、DHCP サーバから IP アドレス 10.0.0.21 を入手します。
- DHCP サーバの応答でコンフィギュレーション ファイル名が提供されない場合、スイッチ 1 は TFTP サーバのベース ディレクトリから network-confg ファイルを読み込みます。
- スイッチ1は、ホストテーブルに network-confg ファイルの内容を追加します。
- スイッチ 1 は、IP アドレス 10.0.0.21 を基にホスト テーブルを検索し、ホスト名 (switch1) を 取得します。

• スイッチ 1 は、ホスト名に対応するコンフィギュレーション ファイルを読み込みます。たとえば、TFTP サーバから *switch1-confg* を読み込みます。

スイッチ 2 ~ 4 も、同様にコンフィギュレーション ファイルおよび IP アドレスを取得します。

スイッチの設定

ここではスイッチの設定方法について説明します。

- コンフィギュレーション モードによるスイッチの設定 (p.3-9)
- 実行コンフィギュレーション設定の確認 (p.3-10)
- 実行コンフィギュレーション設定値の起動ファイルへの保存(p.3-10)
- NVRAM での設定の確認 (p.3-11)
- デフォルト ゲートウェイの設定 (p.3-11)
- スタティック ルートの設定 (p.3-12)

コンフィギュレーション モードによるスイッチの設定

コンフィギュレーションモードからスイッチを設定する手順は、次のとおりです。

- **ステップ1** スーパーバイザ エンジンのコンソール インターフェイスに、コンソール端末を接続します。
- ステップ2 数秒後に、ユーザ EXEC プロンプト(Switch>)が表示されます。このあと、特権 EXEC モード(別名、イネーブル モード)を開始できます。enable と入力して、イネーブル モードを開始します。

Switch> enable



(注)

コンフィギュレーションを変更する場合は、イネーブル モードを開始している必要があります。

プロンプトがイネーブル プロンプト(#)に変わります。

Switch#

ステップ3 イネーブル プロンプト (#) に、configure terminal コマンドを入力して、コンフィギュレーションモードを開始します。

Switch# configure terminal

Enter configuration commands, one per line. End with ${\tt CNTL/Z.}$ Switch(config)#

ステップ 4 グローバル コンフィギュレーション モード プロンプトに、interface type slot/interface コマンドを入力して、インターフェイス コンフィギュレーション モードを開始します。

Switch(config)# interface fastethernet 5/1
Switch(config-if)#

- ステップ5 これらのモードのいずれかで、スイッチ設定の変更を行います。
- ステップ6 コンフィギュレーション モードを終了するには、end コマンドを入力します。
- **ステップ7** 設定値を保存します (「実行コンフィギュレーション設定値の起動ファイルへの保存」[p.3-10] を参照)。

これで最小限のスイッチ設定が完了し、入力した設定を使用してルータを起動できるようになりました。コンフィギュレーション コマンドのリストを確認するには、プロンプトで?を入力するか、またはコンフィギュレーション モードで help キーを押します。

実行コンフィギュレーション設定の確認

入力したコンフィギュレーションまたは変更を確認するには、次の例に示すように、イネーブルプロンプト(#)で show running-config コマンドを入力します。

```
Switch# show running-config
Building configuration...
Current configuration:
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
1
hostname Switch
< テキスト出力は省略 >
line con 0
transport input none
line vty 0 4
exec-timeout 0 0
password lab
transport input lat pad dsipcon mop telnet rlogin udptn nasi
1
end
Switch#
```

実行コンフィギュレーション設定値の起動ファイルへの保存



次のコマンドで、コンフィギュレーション モードで入力した設定値を保存します。この作業を行わないと、次回システムをリロードするときに設定が失われます。

コンフィギュレーション、コンフィギュレーションへの変更内容、またはスタートアップ コンフィギュレーションへの変更を NVRAM に保存するには、イネーブル プロンプト (#) で copy running-config startup-config コマンドを入力します。

Switch# copy running-config startup-config

NVRAM での設定の確認

NVRAM に保存されている情報を表示するには、show startup-config EXEC コマンドを入力します。 次に、一般的なシステム設定の例を示します。

```
Switch# show startup-config
Using 1579 out of 491500 bytes, uncompressed size = 7372 bytes
Uncompressed configuration from 1579 bytes to 7372 bytes
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service compress-config
hostname Switch
ip subnet-zero
-!
interface GigabitEthernet1/1
no snmp trap link-status
interface GigabitEthernet1/2
no snmp trap link-status
!--More--
< テキスト出力は省略 >
line con 0
exec-timeout 0 0
 transport input none
line vty 0 4
 exec-timeout 0 0
password lab
transport input lat pad dsipcon mop telnet rlogin udptn nasi
end
```

デフォルト ゲートウェイの設定

Switch#



スイッチがデフォルト ゲートウェイを使用するのは、ルーティング プロトコルが設定されていな い場合に限られます。

スイッチにルーティング プロトコルが設定されていない場合、他のサブネットにデータを送信する デフォルト ゲートウェイを設定します。デフォルト ゲートウェイには、スイッチに直接接続する ルータ上のインターフェイスの IP アドレスを指定する必要があります。

デフォルト ゲートウェイを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# ip default-gateway IP-address	デフォルト ゲートウェイを設定します。
ステップ 2	Switch# show ip route	デフォルト ゲートウェイが IP ルーティング テーブ
		ルに正しく表示されることを確認します。

次に、デフォルトゲートウェイを設定し、その設定を確認する例を示します。

Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)# ip default-gateway 172.20.52.35

Switch(config)# end

3d17h: %SYS-5-CONFIG_I: Configured from console by console

Switch# show ip route

Default gateway is 172.20.52.35

Host Gateway Last Use Total Uses Interface

ICMP redirect cache is empty

Switch#

スタティック ルートの設定

Telnet ステーションまたは SNMP (簡易ネットワーク管理プロトコル) ネットワーク管理ワークステーションが、スイッチと異なるネットワークに存在し、ルーティング プロトコルが設定されていない場合、使用しているエンド ステーションが存在するネットワークに対応するスタティックルーティング テーブル エントリを追加しなければならない場合があります。

スタティック ルートを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# ip route dest_IP_address mask	リモート ネットワークへのスタティック ルートを
	{forwarding_IP vlan vlan_ID}	設定します。
ステップ 2	Switch# show running-config	スタティック ルートが正しく表示されることを確
		認します。

次に、スイッチ上で **ip route** コマンドを使用して、IP アドレス 171.10.5.10 のワークステーションへのスタティック ルートを設定する例を示します。この場合、サブネット マスクと転送ルータの IP アドレス 172.20.3.35 を用います。

Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)# ip route 171.10.5.10 255.255.255.255 172.20.3.35

Switch(config)# end

Switch#

次に、show running-config コマンドを使用して、スタティック ルートの設定を確認する例を示します。

```
Switch# show running-config
Building configuration...
< テキスト出力は省略 >
ip default-gateway 172.20.52.35
ip classless
ip route 171.10.5.10 255.255.255.255 172.20.3.35
no ip http server
line con 0
transport input none
line vty 0 4
 exec-timeout 0 0
password lab
login
transport input lat pad dsipcon mop telnet rlogin udptn nasi
end
Switch#
```

次に、スイッチ上で **ip route** コマンドを使用して、IP アドレス 171.20.5.3 のワークステーションへ のスタティック ルートを設定する例を示します。この場合、サブネット マスクと接続されている VLAN (仮想 LAN)1 を用います。

```
Switch# configure terminal
Switch(config)# ip route 171.20.5.3 255.255.255.255 vlan 1
Switch(config)# end
Switch#
```

次に、show running-config コマンドを使用して、スタティック ルートの設定を確認する例を示します。

```
Switch# show running-config
Building configuration...
< テキスト出力は省略 >
ip default-gateway 172.20.52.35
ip classless
ip route 171.20.5.3 255.255.255.255 Vlan1
no ip http server
x25 host z
line con 0
transport input none
line vty 0 4
 exec-timeout 0 0
password lab
transport input lat pad dsipcon mop telnet rlogin udptn nasi
end
Switch#
```

特権 EXEC コマンドへのアクセス制御

次の手順に従って、システム コンフィギュレーション ファイルと特権 EXEC コマンドへのアクセスを制御します。

- スタティック イネーブル パスワードの設定または変更 (p.3-14)
- enable password コマンドおよび enable secret コマンドの使用 (p.3-14)
- 特権パスワードの設定または変更 (p.3-15)
- パスワードの暗号化 (p.3-23)
- パスワードの暗号化 (p.3-23)
- 複数の特権レベルの設定 (p.3-24)

スタティック イネーブル パスワードの設定または変更

イネーブル モードへのアクセスを制御するスタティック パスワードを設定または変更するには、次の作業を行います。

表 3-3

コマンド	目的
Switch(config)# enable password password	特権 EXEC モードの新しいパスワードを設定す
	るか、既存のパスワードを変更します。

次に、特権 EXEC モードでイネーブル パスワードを [lab] に設定する例を示します。

Switch# configure terminal
Switch(config)# enable password lab
Switch(config)#

パスワードまたはアクセス レベルの設定を表示する方法については、「パスワード、アクセス レベル、および特権レベルの設定の表示」(p.3-25)を参照してください。

enable password コマンドおよび enable secret コマンドの使用

ネットワークで送受信されるパスワードまたは TFTP サーバに保存されるパスワードについて、セキュリティをさらに強化するには、enable password コマンドまたは enable secret コマンドを使用します。どちらのコマンドも、イネーブル モード (デフォルト)または指定したその他の特権レベルにアクセスするために、ユーザが入力しなければならない暗号化パスワードを設定します。

enable secret コマンドの使用を推奨します。

enable secret コマンドを設定した場合、このコマンドは enable password コマンドよりも優先されます。 同時に 2 つのコマンドを有効にはできません。

スイッチがイネーブル パスワードを要求するように設定するには、次のいずれかの作業を行います。

コマンド	目的
Switch(config)# enable password [level level] {password encryption-type encrypted-password}	特権 EXEC モードを開始するためのパスワードを 設定します。
Switch(config)# enable secret [level level] {password encryption-type encrypted-password}	不可逆的な暗号化方式を使用して保存されるシークレット パスワードを設定します (enable password コマンドおよび enable secret コマンドの両方を設定した場合は、イネーブルシークレット パスワードを入力する必要があります)。

level オプションを使用してどちらかのパスワード コマンドを入力すると、特定の特権レベルにアクセスするためのパスワードを定義できます。レベルを指定してパスワードを設定したあと、その特権レベルにアクセスする必要のあるユーザだけに、パスワードを通知してください。各レベルでアクセスできるコマンドを指定するには、privilege level コンフィギュレーション コマンドを使用します。

service password-encryption コマンドをイネーブルにしている場合は、入力したパスワードが暗号化されます。more system:running-config コマンドを使用してパスワードを表示すると、パスワードは暗号化形式で表示されます。

暗号化タイプを指定する場合は、暗号化パスワード(別の Catalyst 4500 シリーズ スイッチの設定からコピーした暗号化パスワード)を入力する必要があります。



暗号化パスワードを忘れた場合、回復はできません。NVRAM を消去し、新しいパスワードを設定する必要があります。詳細については、「イネーブル パスワードを忘れた場合の回復方法」(p.3-26)を参照してください。

パスワードまたはアクセス レベルの設定を表示する方法については、「パスワード、アクセス レベル、および特権レベルの設定の表示」(p.3-25)を参照してください。

特権パスワードの設定または変更

特権パスワードを設定または変更するには、次の作業を行います。

表 3-4

コマンド	目的
Switch(config-line)# password password	特権レベルの新しいパスワードを設定するか、
	既存のパスワードを変更します。

パスワードまたはアクセス レベルの設定を表示する方法については、「パスワード、アクセス レベル、および特権レベルの設定の表示」(p.3-25)を参照してください。

TACACS+ によるスイッチ アクセスの制御

ここでは、TACACS+をイネーブルにして設定する方法について説明します。TACACS+は、詳細なアカウンティング情報を収集し、認証および許可プロセスに対して柔軟な管理を行います。TACACS+は、Authentication、Authorization、Accounting(AAA;認証、認可、アカウンティング)を通じて機能し、AAA コマンドによってのみイネーブルにできます。



この章で使用するコマンドの構文および使用方法の詳細については、『Cisco IOS Security Command Reference』Release 12.2 を参照してください。

ここで説明する設定内容は次のとおりです。

- TACACS+の概要 (p.3-16)
- TACACS+の動作(p.3-18)
- TACACS+の設定 (p.3-18)
- TACACS+設定の表示 (p.3-23)

TACACS+ の概要

TACACS+ は、スイッチにアクセスしようとするユーザの評価を集中的に行うセキュリティ アプリケーションです。TACACS+ サービスは、通常 UNIX または Windows NT ワークステーション上で稼働する TACACS+ デーモンのデータベースで維持されます。スイッチに TACACS+ 機能を設定する前に、TACACS+ サーバにアクセスして設定する必要があります。

TACACS+ は、個別のモジュール式 AAA 機能を備えています。TACACS+ では、単一のアクセス制御サーバ(TACACS+ デーモン)が各サービス(認証、認可、アカウンティング)を個別に提供します。各サービスは固有のデータベースに組み込まれるため、デーモンの機能に応じてそのサーバまたはネットワークで使用できる他のサービスも利用できます。

TACACS+の目的は、単一の管理サービスから複数のネットワーク アクセス ポイントを管理する方式を提供することです。スイッチは、他のシスコルータおよびアクセス サーバとともにネットワーク アクセス サーバにできます。 ネットワーク アクセス サーバは、単一のユーザ、ネットワークまたはサブネットワーク、および相互接続されたネットワークとの接続を実現します(図 3-4 を参照)。

UNIX ワークステーション (TACACS+ Catalyst 6500 サーバ 1) シリーズ スイッチ 171.20.10.7 UNIX ワークステーション (TACACS+ サーバ 2) 171.20.10.8 スイッチに TACACS+ サーバ アドレス を設定する。 認証キーを設定する(同じ認証キーを TACACS+サーバにも設定)。 AAA をイネーブルにする。 ログイン認証方式リストを作成する。 リストを端末回線に適用する。 必要に応じて認可およびアカウンティング 方式リストを作成する。 ワークステーション ワークステーション

図 3-4 一般的な TACACS+ ネットワーク構成

TACACS+ は、AAA セキュリティ サービスによって管理され、次のようなサービスを提供します。

- 認証 ログインおよびパスワード ダイアログ、チャレンジおよび応答、メッセージング サポートによって認証を完全制御します。
 - 認証機能は、ユーザとの対話を実行できます(たとえば、ユーザ名とパスワードが入力されたあと、自宅の住所、母親の旧姓、サービスタイプ、社会保険番号などのいくつかの質問をすることによりユーザを確認します)。TACACS+認証サービスにより、ユーザ画面にメッセージを表示することもできます。たとえば、会社のパスワード有効期間ポリシーにより、パスワードを変更する必要があることをユーザに通知します。
- 認可 自動コマンド、アクセス制御、セッション期間、またはプロトコル サポートの設定を含む (ただし、これらに限定されない)ユーザ機能をユーザ セッション期間内で厳しく制限します。また、TACACS+ 許可機能によってユーザが実行できるコマンドを制限することもできます。
- アカウンティング 課金、監査、およびレポートに使用する情報を収集して TACACS+ デーモンに送信します。ネットワークの管理者はアカウンティング機能を使用して、セキュリティ監査のためにユーザのアクティビティを追跡したり、ユーザ課金用の情報を提供したりできます。アカウンティング レコードには、ユーザ ID、開始時刻および終了時刻、実行されたコマンド(PPP[ポイントツーポイントプロトコル]など)パケット数、バイト数が含まれます。

TACACS+ プロトコルは、スイッチと TACACS+ デーモンの間の認証を行います。スイッチと TACACS+ デーモンの間のプロトコル交換はすべて暗号化されるため、機密は保持されます。

スイッチで TACACS+ を使用するには、TACACS+ デーモン ソフトウェアが稼働するシステムが必要です。

TACACS+ の動作

ユーザが TACACS+ を使用してスイッチを認証することで、簡易 ASCII ログインを試行すると、次のプロセスが発生します。

1. 接続が確立すると、スイッチは TACACS+ デーモンに接続してユーザ名プロンプトを取得し、ユーザに表示します。ユーザがユーザ名を入力すると、スイッチは TACACS+ デーモンに接続してパスワード プロンプトを取得します。スイッチがパスワード プロンプトを表示し、ユーザがパスワードを入力すると、そのパスワードが TACACS+ デーモンに送信されます。

TACACS+によって、デーモンはユーザを認証するのに十分な情報を取得するまで、デーモンとユーザの間で対話が可能になります。デーモンはユーザ名とパスワードの組み合わせを入力するよう求めますが、ユーザの母親の旧姓など、その他の項目を含めることもできます。

- 2. スイッチは、最終的にTACACS+デーモンから次のいずれかの応答を受信します。
 - ACCEPT ユーザが認証され、サービスを開始できます。認可を必要とするようにスイッチが設定されている場合は、この時点で認可処理が開始されます。
 - REJECT ユーザは認証されません。TACACS+デーモンに応じて、ユーザはアクセスを 拒否されるか、ログインシーケンスを再試行するよう求められます。
 - ERROR デーモンを使用した認証のある時点で、またはデーモンとスイッチの間のネットワーク接続においてエラーが発生しました。ERROR 応答を受信した場合、スイッチは通常、別の方法でユーザを認証しようとします。
 - CONTINUE ユーザは、さらに認証情報の入力を求められます。

認証後、スイッチで許可機能がイネーブルになっている場合、ユーザは追加の認可フェーズに入ります。ユーザは TACACS+ 認可に進む前にまず、TACACS+ 認証を正常に終了する必要があります。

- 3. TACACS+認可が必要な場合、再びTACACS+デーモンに接続し、デーモンがACCEPTまたはREJECTの許可応答を返します。ACCEPT応答が返された場合は、その応答にユーザおよびサービスのEXECまたはNETWORKセッションを指示するデータが属性の形式で含まれており、ユーザがアクセスできるサービスが決まります。
 - Telnet、Secure Shell (SSH; セキュア シェル) rlogin、または特権 EXEC サービス
 - 接続パラメータ(ホストまたはクライアントの IP アドレス、アクセス リスト、ユーザ タイムアウトを含む)

TACACS+ の設定

ここでは、TACACS+をサポートするようスイッチを設定する方法を説明します。少なくとも、TACACS+デーモンを維持するホストを特定し、TACACS+認証の方式リストを定義する必要があります。さらに、任意でTACACS+認可およびアカウンティングの方式リストを定義できます。方式リストでは、ユーザの認証、認可、およびアカウントの記録を行うための順序と方式を定義します。方式リストを使用すると、1つまたは複数のセキュリティプロトコルを指定し、最初の方式が失敗した場合のバックアップシステムを確保できます。ソフトウェアは、リストされた最初の方式を使用してユーザの認証、認可、およびアカウントの記録を行います。その方式が応答しない場合、ソフトウェアはそのリストから次の方式を選択します。このプロセスは、リスト内の方式による通信が成功するか、方式リストをすべて試行し終わるまで続きます。

ここで説明する設定内容は次のとおりです。

- TACACS+ のデフォルト設定 (p.3-19)
- TACACS+ サーバ ホストの特定と認証キーの設定 (p.3-19)
- TACACS+ ログイン認証の設定 (p.3-20)
- 特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 認可の設定 (p.3-22)
- TACACS+ アカウンティングの起動 (p.3-23)

TACACS+ のデフォルト設定

TACACS+ と AAA は、デフォルトではディセーブルです。

セキュリティ上の理由により、ネットワーク管理アプリケーションを使用して TACACS+ を設定することはできません。イネーブルに設定されている場合、TACACS+ は CLI (コマンドライン インターフェイス) を介してスイッチにアクセスするユーザを認証できます。



TACACS+ の設定は CLI を介して実行しますが、TACACS+ サーバは特権レベル 15 に設定された HTTP 接続を認証します。

TACACS+ サーバ ホストの特定と認証キーの設定

認証用に単一サーバを使用する、または既存のサーバ ホストをグループ化するために AAA サーバ グループを使用するようスイッチを設定できます。サーバをグループ化して設定済みサーバ ホスト のサブセットを選択し、特定のサービスにそれらのサーバを使用できます。 サーバ グループは、グローバル サーバホスト リストと一緒に使用され、選択したサーバ ホストの IP アドレスのリストを含んでいます。

TACACS+ サーバを維持する IP ホストを特定し、任意で暗号キーを設定するには、特権 EXEC モードを開始して次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	tacacs-server host hostname [port integer] [timeout integer] [key string]	TACACS+ サーバを維持する IP ホストを特定します。このコマンドを複数回入力すると、優先ホストのリストを作成できます。ソフトウェアは、指定された順序でホストを検索します。
		hostname には、ホスト名または IP アドレスを指定します。
		• (任意) port integer には、サーバのポート番号を指定します。デフォルトはポート 49 です。指定できる範囲は1~65535 です。
		(任意) timeout integer には、スイッチがデーモンからの応答を待つ時間を秒単位で指定します。この時間を過ぎるとスイッチはタイムアウトしてエラーを宣言します。デフォルトは 5 秒です。指定できる範囲は 1 ~ 1000 秒です。
		• (任意) key string には、スイッチと TACACS+ デーモンの間のすべてのトラフィックを暗号化および復号化するための暗号キーを指定します。暗号化が正しく機能するには、TACACS+ デーモンに同じキーを設定する必要があります。
ステップ 3	aaa new-model	AAA をイネーブルにします。
ステップ 4	aaa group server tacacs+ group-name	(任意)グループ名で AAA サーバグループを定義します。
		このコマンドによって、スイッチはサーバ グループ サブコ ンフィギュレーション モードになります。

	コマンド	目的
ステップ 5	server ip-address	(任意)特定の TACACS+ サーバを定義済みサーバ グループに関連付けます。AAA サーバ グループの各 TACACS+サーバに対してこの手順を繰り返します。
		グループの各サーバは、ステップ 2 で事前に定義する必要
		があります。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show tacacs	入力を確認します。
ステップ 8	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存し
		ます。

指定された TACACS+ サーバ名またはアドレスを削除するには、**no tacacs-server host** hostname グローバル コンフィギュレーション コマンドを使用します。設定リストからサーバ グループを削除するには、**no aaa group server tacacs+** group-name グローバル コンフィギュレーション コマンドを使用します。TACACS+ サーバの IP アドレスを削除するには、**no server ip-address** サーバ グループサブコンフィギュレーション コマンドを使用します。

TACACS+ ログイン認証の設定

AAA 認証を設定するには、認証方式の名前付きリストを定義してから、さまざまなポートにそのリストを適用します。方式リストには実行する認証のタイプと実行順序を定義します。このリストを特定のポートに適用してから、定義した認証方式を実行する必要があります。唯一の例外はデフォルトの方式リスト(default と名前が付けられている)です。デフォルトの方式リストは、明示的に定義された名前付き方式リストを持つポート以外の、すべてのポートに自動的に適用されます。定義された方式リストは、デフォルトの方式リストを上書きします。

方式リストは、ユーザ認証のためクエリー送信を行う手順と認証方式を記述したものです。認証のために1つまたは複数のセキュリティプロトコルを指定できるので、最初の方式が失敗した場合のバックアップシステムが確保されます。ソフトウェアは、最初の方式を使用してユーザを認証します。その方式で応答が得られなかった場合、ソフトウェアはそのリスト内の次の認証方式を選択します。このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式を使い果たすまで続きます。このサイクルのある時点で認証が失敗した場合(つまり、セキュリティサーバまたはローカルのユーザ名データベースがユーザアクセスを拒否すると応答した場合)、認証プロセスは停止し、それ以上他の認証方式が試行されることはありません。

ログイン認証を設定するには、特権 EXEC モードを開始して次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	aaa new-model	AAA をイネーブルにします。

ステップ 3	aaa authentication login {default list-name} method1 [method2]	ログイン認証方式リストを作成します。
	method1 [method2]	
		• login authentication コマンドに名前付きリストが指定 されなかった場合に使用されるデフォルトのリストを 作成するには、default キーワードの後ろにデフォルト の状況で使用する方式を指定します。デフォルトの方 式リストは、自動的にすべてのポートに適用されます。
		• list-name には、作成するリストの名前に使用する文字 列を指定します。
		• <i>method1</i> には、認証アルゴリズムが試行する実際の方式を指定します。追加の認証方式は、その前の方式でエラーが戻された場合に限り使用されます。前の方式が失敗した場合は使用されません。
		次のいずれかの方式を選択します。
		• enable イネーブル パスワードを認証に使用します。 この認証方式を使用する前に、enable password グロー バル コンフィギュレーション コマンドを使用してイ ネーブル パスワードを定義する必要があります。
		• group tacacs+ TACACS+認証を使用します。この認証方式を使用する前に、TACACS+サーバを設定しておく必要があります。詳細については、「TACACS+サーバホストの特定と認証キーの設定」(p.3-19)を参照してください。
		• line 回線パスワードを認証に使用します。この認証 方式を使用する前に、回線パスワードを設定しておく 必要があります。それには、password password ライン コンフィギュレーション コマンドを使用します。
		• local ローカル ユーザ名データベースを認証に使用します。データベースにユーザ名情報を入力する必要があります。それには、username password グローバルコンフィギュレーション コマンドを使用します。
		• local-case 大文字と小文字が区別されたローカル ユーザ名データベースを認証に使用します。それには、 username name password グローバル コンフィギュレー ション コマンドを使用して、ユーザ名情報をデータ ベースに入力する必要があります。
	-	• none ログインに認証を使用しません。
ステップ 4	line [console tty vty] line-number [ending-line-number]	ライン コンフィギュレーション モードを開始し、認証リストを適用する回線を設定します。
ステップ 5	login authentication {default list-name}	回線または回線セットに、認証リストを適用します。
		 default を指定する場合、aaa authentication login コマンドで作成したデフォルトのリストを使用します。 list-name には、aaa authentication login コマンドで作成
ステップ 6	end	したリストを指定します。 特権 EXEC モードに戻ります。
ステップ 7	show running-config	大力を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

AAA をディセーブルにするには、no aaa new-model グローバル コンフィギュレーション コマンドを使用します。AAA 認証をディセーブルにするには、no aaa authentication login {default | list-name} method1 [method2...] グローバル コンフィギュレーション コマンドを使用します。ログインの TACACS+ 認証をディセーブルにする、またはデフォルト値に戻すには、no login authentication {default | list-name} ライン コンフィギュレーション コマンドを使用します。

特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 認可の設定

AAA 認可によってユーザが利用できるサービスが制限されます。AAA 認可がイネーブルである場合、スイッチはユーザのプロファイルから取得した情報を使用します。このプロファイルは、ローカルのユーザ データベースまたはセキュリティ サーバ上にあり、ユーザのセッションを設定します。ユーザは、ユーザ プロファイル内の情報で認められている場合に限り、要求したサービスのアクセスが認可されます。

tacacs+ キーワードを指定して aaa authorization グローバル コンフィギュレーション コマンドを使用すると、特権 EXEC モードへのユーザのネットワーク アクセスを制限するパラメータを設定できます。

aaa authorization exec tacacs+ local コマンドは、次の認可パラメータを設定します。

- 認証に TACACS+ を使用した場合は、特権 EXEC アクセス許可に TACACS+ を使用します。
- 認証に TACACS+ を使用しなかった場合は、ローカル データベースを使用します。



認可が設定されていても、CLIを介してログインし、認証されたユーザに対しては、認可は省略されます。

特権 EXEC アクセスおよびネットワーク サービスに関する TACACS+ 認可を指定するには、特権 EXEC モードを開始して、次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	aaa authorization network tacacs+	ネットワーク関連のすべてのサービス要求に対してユーザ TACACS+ 認可を行うことを設定します。
ステップ 3	aaa authorization exec tacacs+	ユーザの特権 EXEC アクセスに対してユーザ TACACS+ 認可を行うことを設定します。 exec キーワードを指定すると、ユーザ プロファイル情報(autocommand 情報など)が返されることがあります。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	入力を確認します。
ステップ 6	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

認可をディセーブルにするには、 no aaa authorization $\{network \mid exec\}\ method 1$ グローバル コンフィギュレーション コマンドを使用します。

TACACS+ アカウンティングの起動

AAA アカウンティング機能は、ユーザがアクセスしたサービスと、消費したネットワーク リソース量を追跡します。AAA アカウンティングをイネーブルにすると、スイッチはユーザのアクティビティをアカウンティング レコード形式で TACACS+ セキュリティ サーバに報告します。各アカウンティング レコードは、アカウンティングの AV のペアを含み、セキュリティ サーバに保存されます。このデータは、ネットワーク管理、クライアントへの課金、または監査用に分析できます。

各 Cisco IOS 特権レベルおよびネットワーク サービスに関する TACACS+ アカウンティングをイネーブルにするには、特権 EXEC モードを開始して、次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	aaa accounting network start-stop tacacs+	ネットワーク関連のすべてのサービス要求について、 TACACS+ アカウンティングをイネーブルにします。
ステップ 3	aaa accounting exec start-stop tacacs+	TACACS+ アカウンティングをイネーブルにして、特権 EXEC プロセスの最初に記録開始アカウンティング通知、 最後に記録停止通知を送信します。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	入力を確認します。
ステップ 6	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

アカウンティングをディセーブルにするには、no aaa accounting {network | exec} {start-stop} method1... グローバル コンフィギュレーション コマンドを使用します。

TACACS+ 設定の表示

TACACS+ サーバ統計情報を表示するには、show tacacs 特権 EXEC コマンドを使用します。

パスワードの暗号化

プロトコル アナライザでパケットを調べる (パスワードを読み取る) ことができるため、パスワードを暗号化するように Cisco IOS ソフトウェアを設定することによって、アクセス セキュリティを強化できます。暗号化を行うと、コンフィギュレーション ファイル内でのパスワード読み取りを不可能にできます。

パスワードを暗号化するように Cisco IOS ソフトウェアを設定するには、次の作業を行います。

表 3-5

コマンド	目的
Switch(config)# service password-encryption	パスワードを暗号化します。

暗号化は、現在の設定が保存されるとき、またはパスワードが設定されるときに行われます。パスワードの暗号化は、認証キーパスワード、イネーブルコマンドパスワード、コンソールおよび仮想端末回線アクセスパスワード、および Border Gateway Protocol (BGP; ボーダーゲートウェイプロトコル)ネイバーパスワードを含む、すべてのパスワードに適用されます。

service password-encryption コマンドを使用すると、認可されていないユーザがコンフィギュレーション ファイルのパスワードを表示できなくなります。



service password-encryption コマンドでは、高度なネットワーク セキュリティは提供されません。 このコマンドを使用する場合は、その他のネットワーク セキュリティ手段も講じる必要があります。

暗号化パスワードを忘れた場合、パスワードの回復はできません(元のパスワードを取り戻すことはできません)。ただし、暗号化パスワードを忘れても、スイッチの制御を取り戻すことはできます。詳細については、「イネーブル パスワードを忘れた場合の回復方法」(p.3-26)を参照してください。

パスワードまたはアクセス レベルの設定を表示する方法については、「パスワード、アクセス レベル、および特権レベルの設定の表示」(p.3-25)を参照してください。

複数の特権レベルの設定

Cisco IOS ソフトウェアには、パスワード セキュリティのモードがデフォルトで 2 つあります。ユーザ EXEC モードと特権 EXEC モードです。各モードに、最大 16 個の階層レベルから構成されるコマンドを設定できます。複数のパスワードを設定すると、ユーザ グループ別に特定のコマンドへのアクセスを許可できます。

たとえば、多くのユーザが clear line コマンドにアクセスできるようにするには、このコマンドにレベル 2 セキュリティを割り当て、レベル 2 パスワードを広範囲に配布します。一方、configure コマンドにアクセスできるユーザを限定する場合には、このコマンドにレベル 3 セキュリティを割り当て、そのパスワードを配布するユーザ数を減らします。

ここでは、追加レベルのセキュリティを設定する手順について説明します。

- コマンドの特権レベルの設定 (p.3-24)
- 回線のデフォルト特権レベルの変更 (p.3-25)
- 特権レベルへのログイン (p.3-25)
- 特権レベルの終了(p.3-25)
- パスワード、アクセス レベル、および特権レベルの設定の表示 (p.3-25)

コマンドの特権レベルの設定

コマンドの特権レベルを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# privilege mode level level command	コマンドの特権レベルを設定します。
ステップ 2	[ongrimtion_time] paggiord	特権レベルにアクセスするためのイネーブル パス ワードを指定します。

パスワードまたはアクセス レベルの設定を表示する方法については、「パスワード、アクセス レベル、および特権レベルの設定の表示」(p.3-25)を参照してください。

回線のデフォルト特権レベルの変更

特定の回線または回線グループのデフォルト特権レベルを変更するには、次の作業を行います。

表 3-6

コマンド	目的
Switch(config-line)# privilege level level	回線のデフォルト特権レベルを変更します。

パスワードまたはアクセス レベルの設定を表示する方法については、「パスワード、アクセス レベ ル、および特権レベルの設定の表示」(p.3-25)を参照してください。

特権レベルへのログイン

特定の特権レベルにログインするには、次の作業を行います。

表 3-7

コマンド	目的
Switch# enable level	指定された特権レベルにログインします。

特権レベルの終了

特定の特権レベルを終了するには、次の作業を行います。

表 3-8

コマンド	目的
Switch# disable level	特定の特権レベルを終了します。

パスワード、アクセス レベル、および特権レベルの設定の表示

詳細なパスワード情報を表示するには、次の作業を行います。

ステップ 1

ステップ 2

コマンド	目的
Switch# show running-config	パスワードおよびアクセス レベルの設定を表示します。
Switch# show privilege	特権レベルの設定を表示します。

次に、パスワードおよびアクセスレベルの設定を表示する例を示します。

```
Switch# show running-config
Building configuration...
Current configuration:
version 12.0
service timestamps debug datetime localtime
service timestamps log datetime localtime
no service password-encryption
hostname Switch
boot system flash sup-bootflash
enable password lab
< テキスト出力は省略 >
```

次に、特権レベルの設定を表示する例を示します。

Switch# show privilege
Current privilege level is 15
Switch#

イネーブル パスワードを忘れた場合の回復方法



(注)

NVRAM にあらかじめ設定されているコンフィギュレーション レジスタについては、「ソフトウェア コンフィギュレーション レジスタの設定」(p.3-28) を参照してください。

イネーブル パスワードを忘れた場合の回復手順は、次のとおりです。

- ステップ1 コンソール インターフェイスに接続します。
- ステップ 2 起動後 5 秒以内に Ctrl-C を押して、ブート シーケンスを停止し、ROM モニタを開始します。
- ステップ3 コンフィギュレーション メモリ (NVRAM) を読み込まずに起動するように、スイッチを設定します。
- **ステップ** 4 システムを再起動します。
- **ステップ 5** イネーブル モードにアクセスします(パスワードが設定されていない場合は、パスワードを指定しません)。
- ステップ6 パスワードを表示または変更するか、設定を消去します。
- ステップ7 通常どおり NVRAM を読み込んで起動するように、スイッチを再設定します。
- ステップ8 システムを再起動します。

スーパーバイザ エンジンのスタートアップ コンフィギュレーションの 変更

ここでは、スーパーバイザエンジンのスタートアップコンフィギュレーションの機能と、BOOT変数およびコンフィギュレーションレジスタを変更する手順について説明します。

- スーパーバイザ エンジンのブート コンフィギュレーションの概要(p.3-27)
- ソフトウェア コンフィギュレーション レジスタの設定 (p.3-28)
- スタートアップ システム イメージの指定 (p.3-32)
- 環境変数の制御(p.3-33)

スーパーバイザ エンジンのブート コンフィギュレーションの概要

スーパーバイザ エンジンのブート プロセスには、2 つのソフトウェア イメージが関与します。ROM モニタとスーパーバイザ エンジン ソフトウェアです。スイッチを起動またはリセットすると、 ROMMON コードが実行されます。NVRAM に保存されている設定に応じて、スーパーバイザ エンジンは ROMMON モードを継続するか、またはスーパーバイザ エンジン ソフトウェアをロードします。

ユーザ側で設定できる 2 つのパラメータによって、スイッチの起動方法が決まります。コンフィギュレーション レジスタと BOOT 環境変数です。コンフィギュレーション レジスタについては、「ブート フィールドの変更および boot コマンドの使用」(p.3-29)を参照してください。BOOT 環境変数については、「スタートアップ システム イメージの指定」(p.3-32)を参照してください。

ROM モニタの概要

ROM モニタ (ROMMON) はスイッチの起動時、リセット時、または致命的な例外が発生した場合に呼び出されます。スイッチで ROMMON モードが開始されるのは、スイッチが有効なソフトウェアイメージを見つけることができなかった場合、NVRAM 内の設定が壊れていた場合、またはコンフィギュレーション レジスタが ROMMON モードを開始するように設定されていた場合です。ROMMON モードでは、ブートフラッシュまたはフラッシュ ディスクからソフトウェア イメージを手動でロードできます。また、管理インターフェイスから起動することもできます。ROMMON モードはプライマリ イメージをロードします。このプライマリ イメージで、BOOTLDR 環境変数を使用してローカルに、またはネットワークを通じて、指定されたソースから起動するセカンダリ イメージを設定できます。この変数については、「Switch#」(p.3-33)を参照してください。

また、スイッチを再起動して、起動後の最初の5秒間にCtrl-Cを押しても、ROMMON モードを開始できます。端末サーバから接続している場合は、エスケープによってTelnetプロンプトを表示し、send break コマンドを入力すると、ROMMON モードが開始されます。



(注)

コンフィギュレーションレジスタで Ctrl-C がディセーブルに設定されているかどうかにかかわらず、スイッチの再起動後5秒間は常に Ctrl-C がイネーブルになります。

ROM モニタの機能は、次のとおりです。

- 電源投入時の信頼性テスト
- ハードウェアの初期化
- 起動能力 (手動による起動および自動起動が可能)
- ファイル システム (ROMMON の実行時は読み取り専用)

ソフトウェア コンフィギュレーション レジスタの設定

スイッチは 16 ビットのソフトウェア コンフィギュレーション レジスタを使用します。このコンフィギュレーション レジスタに特定のシステム パラメータを設定できます。ソフトウェア コンフィギュレーション レジスタの設定は、NVRAM にあらかじめ設定されています。

次の場合は、ソフトウェアコンフィギュレーションレジスタの設定値を変更する必要があります。

- 起動元およびデフォルトのブート ファイル名を選択する場合
- ブロードキャスト アドレスを制御する場合
- コンソール端末のボーレートを設定する場合
- フラッシュ メモリからオペレーティング ソフトウェアをロードする場合
- 忘れたパスワードを回復する場合
- ブートストラップ プログラム プロンプトで boot コマンドを使用し、手動でシステムを起動する場合
- システム ブートストラップ ソフトウェア (ブート イメージ) またはオンボード フラッシュ メモリ上のデフォルトのシステム イメージから自動的に起動し、NVRAM 上のコンフィギュレーション ファイル内の boot system コマンドを読み取るように強制的に設定する場合



誤って Catalyst 4500 シリーズスイッチのスイッチが停止するような事態を避けるために、コンフィギュレーション レジスタ設定を有効にするには、表 3-9 に記載されている個々の設定値を使用するのではなく、設定値を組み合わせる必要があります。たとえば、出荷時のデフォルトである 0x2101 という値は、3 つの設定値の組み合わせです。

表 3-9 に、各ソフトウェア コンフィギュレーション メモリ ビットの意味を示します。表 3-10 に、 ブート フィールドの定義を示します。

表 3-9 ソフトウェア コンフィギュレーション レジスタ ピット

ビット番号 ¹	16 進数	意味
00 ~ 03	0x0000 ~ 0x000F	ブート フィールド (表 3-10 を参照)
04	0x0010	未使用
05	0x0020	ビット2はコンソール回線速度
06	0x0040	システム ソフトウェアに NVRAM の内容を無視させます。
07	0x0080	OEM ² ビットをイネーブルにします。
08	0x0100	未使用
09	0x0200	未使用
10	0x0400	すべて0のIPブロードキャスト
11 ~ 12	$0x0800 \sim 0x1000$	コンソール回線速度のビット1と0(デフォルトは9600ボー)
13	0x2000	ネットブートの失敗後に ROM モニタをロードします。
14	0x4000	IP ブロードキャストでネットワーク番号を使用しません。

^{1.} コンフィギュレーション レジスタの出荷時のデフォルト値は 0x2101 です。この値は、次の設定値を組み合わせたものです。バイナリ ビット 13、ビット 8 = 0x0100、およびバイナリ ビット $00 \sim 03 = 0x0001$ (表 3-10 を参照)。

^{2.} OEM = Original Equipment Manufacturer

表 2-10	ブートフィールド	(コンフィギュレーション	レジフタ ビット 00	~ 03 / の試明
स्ट उ- । U	ノート ノイールト	(コノノイ キュレーソョノ	レンスツ ニット い	~ U.S) V.J. R.D.H

プート	
フィールド	意味
00	システム ブートストラップ プロンプトの状態(自動起動しません)
01	オンボード フラッシュ メモリ上で最初に検出されたシステム イメージを起動しま
	す。
02 ~ 0F	BOOT 環境変数で指定されたイメージを使用して自動起動します。複数のイメージが指定されている場合、スイッチは BOOT 変数で最初に指定されたイメージの起動を試みます。スイッチがこのイメージからの起動に成功すると、再起動時に同じイメージが使用されます。スイッチが BOOT 変数で最初に指定されたイメージからの起動に失敗すると、スイッチは BOOT 変数の次のイメージからの起動を試みます。BOOT 変数の最後のイメージからスイッチが起動できない場合、スイッチは BOOT 変数の最初に戻って起動を試みます。自動起動は、スイッチが BOOT 変数で指定されたいずれかのイメージからの起動に成功するまで続きます。

プート フィールドの変更および boot コマンドの使用

コンフィギュレーション レジスタのブート フィールドにより、スイッチはオペレーティング システム イメージをロードするかどうかを決定し、ロードする場合はシステム イメージをどこから取得するかを決定します。ここでは、コンフィギュレーション レジスタのブート フィールドの使用方法および設定手順と、コンフィギュレーション レジスタのブート フィールドを変更する場合の手順について説明します。ROMMON では、コンフィギュレーション レジスタの変更とブート設定の変更に confreg コマンドを使用できます。

ソフトウェア コンフィギュレーション レジスタのビット $0 \sim 3$ が、ブート フィールドを形成します。



(注)

システムおよびスペア製品のコンフィギュレーション レジスタの出荷時のデフォルト値は、0x2101です。ただし、推奨値は 0x0102 です。

ブート フィールドを 00 または 01 (0-0-0-0 または 0-0-0-1) に設定すると、システムはシステム コンフィギュレーション ファイルの起動命令を無視して、次の動作を行います。

- ブート フィールドが 00 に設定されている場合は、システム ブートストラップまたは ROMMON プロンプトで boot コマンドを入力し、手動でオペレーティング システムを起動する必要があります。
- ブート フィールドが 01 に設定されている場合は、ブートフラッシュ SIMM で最初に検出され たイメージを起動します。
- ブート フィールド全体が 0-0-1-0 ~ 1-1-1-1 の範囲の値である場合、スイッチはスタートアップ コンフィギュレーション ファイルの boot system コマンドで指定されるシステム イメージをロードします。



注意

ブートフィールドを 0-0-1-0 ~ 1-1-1-1 の範囲の値に設定する場合は、**boot system** コマンドで値を 指定する必要があります。そうしないと、スイッチは起動できず ROMMON のままです。 boot コマンドは単独でも入力できますが、フラッシュ メモリに保存されたファイル名、ネットワーク サーバからの起動を指定するファイル名など、追加の起動命令を含めることもできます。ファイル名または他の起動命令を指定せずに boot コマンドを使用すると、システムはデフォルトのフラッシュ イメージ (オンボード フラッシュ メモリ上の最初のイメージ) から起動します。また、特定のフラッシュ イメージから起動するように指定することもできます (boot system flash filename コマンドを使用)。

また、boot コマンドを使用して、スーパーバイザ エンジン上のスロット 0 にあるコンパクト フラッシュ カードに保存されたイメージを起動することもできます。

ブート フィールドの変更

ソフトウェア コンフィギュレーション レジスタのブート フィールドを変更します。ソフトウェア コンフィギュレーション レジスタのブート フィールドを変更するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# show version	現在のコンフィギュレーション レジスタ設定値を確認します。
ステップ 2	Switch# configure terminal	コンフィギュレーション モードを開始し、terminal オプションを指定します。
ステップ 3	Switch(config)# config-register value	スイッチへの希望するシステム イメージのロード方法に応じて、既存のコンフィギュレーション レジスタ設定値を変更します。
ステップ 4	Switch(config)# end	コンフィギュレーション モードを終了します。
ステップ 5	Switch# reload	スイッチを再起動して、変更を有効にします。

スイッチが Cisco IOS ソフトウェアを実行している場合にコンフィギュレーション レジスタを変更する手順は、次のとおりです。

ステップ1 enable コマンドおよびパスワードを入力して、特権レベルを開始します。

Switch> enable Password: Switch#

ステップ 2 EXEC モード プロンプト (#) で、configure terminal コマンドを次のように入力します。

Switch# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#

ステップ3 コンフィギュレーション レジスタを 0x102 に設定します。

Switch(config) # config-register 0x102

value コマンド変数を指定して、コンフィギュレーション レジスタの内容を設定します。*value* は、 先頭が 0x の 16 進数です (表 3-9 [p.3-28] を参照)。

ステップ4 コンフィギュレーション モードを終了するには、end コマンドを入力します。新しい設定値がメモリに保存されます。ただし、システムを再起動するまで新しい設定値は有効になりません。

■ Catalyst 4500 シリーズ スイッチ Cisco IOS ソフトウェア コンフィギュレーション ガイド

ステップ 5 show version EXEC コマンドを入力して、現在有効なコンフィギュレーション レジスタ値を表示します。これは次回のリロード時に使用されます。この値は次の出力例のように、画面の最後の行に表示されます。

Configuration register is 0x141 (will be 0x102 at next reload)

- **ステップ6** 設定値を保存します(「実行コンフィギュレーション設定値の起動ファイルへの保存」[p.3-10])を 参照。コンソールから reload コマンドを入力するなどの方法でシステムをリロードしないかぎり、 コンフィギュレーション レジスタの変更は有効になりません)。
- ステップ7 システムを再起動します。システムを再起動した時点で、新しいコンフィギュレーション レジスタ 値が有効になります。

コンフィギュレーション レジスタ設定値の確認

現在のコンフィギュレーション レジスタ設定値を確認するには、show version EXEC コマンドを使用します。コンフィギュレーション レジスタの設定を確認するには、ROMMON モードで show version コマンドを使用します。

スイッチのコンフィギュレーション レジスタ設定値を確認するには、次の作業を行います。

表 3-11

コマンド	目的
Switch# show version	コンフィギュレーション レジスタ設定値を表示します。

次に示す show version コマンドの出力例では、現在のコンフィギュレーション レジスタは、スイッチがオペレーティング システム イメージを自動的にロードしないように設定されています。 レジスタは ROMMON モードを開始し、ユーザによる ROM モニタ コマンドの入力を待機します。

Switch#show version

Cisco Internetwork Operating System Software
IOS (tm) Catalyst 4000 L3 Switch Software (cat4000-IS-M), Experimental
Version 12.1(20010828:211314) [cisco 105]
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Thu 06-Sep-01 15:40 by

Image text-base:0x00000000, data-base:0x00ADF444

ROM:1.15

Switch uptime is 10 minutes System returned to ROM by reload Running default software

cisco Catalyst 4000 (MPC8240) processor (revision 3) with 262144K bytes of memory.

Processor board ID Ask SN 12345

Last reset from Reload

Bridging software.

49 FastEthernet/IEEE 802.3 interface(s)

20 Gigabit Ethernet/IEEE 802.3 interface(s)

271K bytes of non-volatile configuration memory.

Configuration register is 0xEC60

Switch#

スタートアップ システム イメージの指定

スタートアップ コンフィギュレーション ファイルまたは BOOT 環境変数に複数のブート コマンドを入力して、システム イメージをロードするためのバックアップ手段を得ることができます。

BOOT 環境変数については、『Cisco IOS Configuration Fundamentals Configuration Guide』の「Loading and Maintaining System Images and Microcode」の章の「Specify the Startup System Image in the Configuration File」でも説明しています。

以下の項目に従って、フラッシュ メモリから起動するようにスイッチを設定してください。フラッシュ メモリは Single In-Line Memory Module (SIMM; シングル インライン メモリ モジュール)またはフラッシュ ディスクのいずれかになります。フラッシュ メモリのタイプについては、適切なハードウェアのインストールおよびメンテナンス マニュアルを確認してください。

フラッシュ メモリの使用

フラッシュ メモリを使用すると、次の作業が可能になります。

- TFTP によるシステム イメージのフラッシュ メモリへのコピー
- フラッシュ メモリからの自動または手動によるシステムの起動
- TFTP または Remote Copy Protocol (RCP; リモート コピー プロトコル) によるフラッシュ メモリ イメージのネットワーク サーバへのコピー

フラッシュ メモリの機能

フラッシュ メモリを使用すると、次の作業が可能になります。

- TFTP または RCP 転送による複数のシステム ソフトウェア イメージのリモートでのロード (ファイルのロードごとに1回の転送)
- フラッシュ メモリに保存されたシステム ソフトウェア イメージからの、手動または自動によるスイッチの起動(ROM からの直接起動も可能)

セキュリティ上の注意

フラッシュ メモリからロードする場合、次のセキュリティ上の注意を参照してください。



フラッシュ メモリに保存されたシステム イメージを変更できるのは、コンソール端末の特権 EXEC レベルからに限られます。

フラッシュ メモリの設定

スイッチがフラッシュ メモリから起動するように設定する手順は、次のとおりです。 ハードウェア のインストール方法については、適切なハードウェアのインストールおよびメンテナンス マニュア ルを参照してください。

ステップ1 TFTP またはその他のプロトコルでシステム イメージをフラッシュ メモリにコピーします。次の URL の『Cisco IOS Configuration Fundamentals Configuration Guide』Release 12.2 の「Cisco IOS File Management」および「Loading and Maintaining System Images」の章を参照してください。

http://www.cisco.com/univered/cc/td/doc/product/software/ios122/122egcr/fun_c/fcprt2/fcd203.htm

- **ステップ2** フラッシュ メモリ内の必要なファイルからシステムが自動的に起動するように設定します。コンフィギュレーション レジスタ値を変更しなければならない場合もあります。コンフィギュレーション レジスタを変更する方法については、「ブート フィールドの変更および boot コマンドの使用」(p.3-29)を参照してください。
- ステップ3 設定を保存します。
- **ステップ4** システムの電源をオフにしてから再びオンにしてシステムを再起動し、すべて正常に動作しているかどうかを確認します。

環境変数の制御

環境変数の制御は ROM モニタが行いますが、特定のコマンドを使用して環境変数を作成、変更、または表示できます。BOOT 変数と BOOTLDR 変数を作成または変更するには、それぞれ boot system と boot bootldr グローバル コンフィギュレーション コマンドを使用します。BOOT 環境変数の詳しい設定手順については、『Configuration Fundamentals Configuration Guide』の「Loading and Maintaining System Images and Microcode」の章にある「Specify the Startup System Image in the Configuration File」を参照してください。



boot system と boot bootldr グローバル コンフィギュレーション コマンドが有効なのは、実行コンフィギュレーションだけです。あとで使用できるようにコンフィギュレーションを保存する場合は、ROM モニタ制御下に情報を置くスタートアップ コンフィギュレーションに環境変数の設定を保存する必要があります。環境変数を実行コンフィギュレーションからスタートアップ コンフィギュレーションに保存するには、copy system:running-config nvram:startup-config コマンドを使用します。

BOOT 変数および BOOTLDR 変数の内容を表示するには、show bootvar コマンドを使用します。このコマンドは、スタートアップ コンフィギュレーション内のこれらの変数の設定値を表示しますが、実行コンフィギュレーションの設定値がスタートアップ コンフィギュレーションの設定値と異なっている場合には、実行コンフィギュレーション内の設定値も表示します。次に、スイッチ上のBOOT 変数と BOOTLDR 変数を確認する例を示します。

Switch# show bootvar
BOOTLDR variable = bootflash:cat4000-is-mz,1;
Configuration register is 0x0
Switch#

スイッチの出荷時のデフォルト設定へのリセット

製造元およびリペア センターでは、erase /all non-default コマンドを使用して次の作業を実行できます。

- ローカルのスーパーバイザ エンジンの不揮発設定および状態(NVRAM およびフラッシュ)を クリアします。
- カスタマーへ出荷する前に、Catalyst 4500 シリーズ スイッチ上で出荷時のデフォルト パラメータを設定します。

次に、このコマンドの出力例を示します。

```
Switch# erase /all non-default
Erase and format operation will destroy all data in non-volatile storage. Continue?
[confirm]
Formatting bootflash: ...
Format of bootflash complete
Erasing nyram:
Erasing cat4000_flash:
Clearing crashinfo:data
Clearing the last power failure timestamp
Clearing all ROMMON variables
Setting default ROMMON variables:
     ConfigReg=0x2101
     PS1=rommon ! >
     EnableAutoConfig=1
Setting vtp mode to transparent
%WARNING! Please reboot the system for the changes to take effect
Switch#
00:01:48: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#
```

Catalyst 4500 シリーズ スイッチが TFTP サーバにアクセス可能な場合は、tftp コマンドを使用して ブートフラッシュ メモリにイメージをコピーできます。

Switch# copy tftp://192.20.3.123/tftpboot/abc/cat4500-entservices-mz.bin bootflash:

コピーが完了すると、reload コマンドによりブートフラッシュ メモリに格納されたイメージにコピーされたばかりの Catalyst 4500 シリーズ スイッチのイメージを再起動できます。

Switch# reload

```
System configuration has been modified. Save? [yes/no]: no
Proceed with reload? [confirm]

00:06:17: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.
```

erase /all non-default コマンドにより設定されたデフォルト パラメータの詳細については、『Catalyst 4500 Series Switch Command Reference 』の erase コマンド ページの使用上の注意事項を参照してください。



CHAPTER

4

スイッチの管理

この章では、Catalyst 4500 シリーズ スイッチで 1 回だけ行う管理作業の実行方法について説明します。

またこの章では、Catalyst 4500 シリーズ スイッチのグラフィカル表示と、GUI (グラフィカル ユーザ インターフェイス) ベースの管理および設定インターフェイスを提供する組み込み CiscoView ネットワーク管理システムのインストールおよび設定方法についても説明します。

この章の主な内容は、次のとおりです。

- システム日時の管理 (p.4-2)
- システム名とプロンプトの設定 (p.4-15)
- バナーの作成 (p.4-18)
- MAC アドレス テーブルの管理 (p.4-20)
- ARP テーブルの管理 (p.4-31)
- 組み込み CiscoView サポートの設定 (p.4-31)

システム日時の管理

Network Time Protocol (NTP; ネットワーク タイム プロトコル)を使用して手動または自動でスイッチのシステム日時を設定できます。



この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univered/cc/td/doc/product/software/ios122sr/cr/index.htm

ここでは、次の設定情報について説明します。

- システム クロック (p.4-2)
- NTPの概要(p.4-2)
- NTP の設定 (p.4-4)
- 手動での日時の設定 (p.4-11)

システム クロック

時刻サービスの中核となるのはシステム クロックで、これによって日時を監視します。このクロックはシステムが起動した瞬間から開始します。

システムクロックは、次のサービスに時刻を提供します。

- ユーザの show コマンド
- ログ メッセージおよびデバッグ メッセージ

システム クロックは、Universal Time Coordinated (UTC; 世界標準時)(別名 Greenwich Mean Time [GMT; グリニッジ標準時])に基づいてシステム内部の時刻を常時監視します。現地の時間帯および夏時間に関する情報を設定することにより、時刻が現地の時間帯で正確に表示されるようにできます。

システム クロックは、時刻に*信頼性がある*かどうか(つまり、信頼できるとみなされる時刻源によって時刻が設定されているか)を常時監視します。信頼性のない場合は、時刻は表示目的でのみ利用され、再配信されません。詳しい設定手順については、「手動での日時の設定」(p.4-11)を参照してください。

NTP の概要

NTP は、ネットワーク上のデバイス間の時刻の同期化を目的に設計されています。NTP は User Datagram Protocol (UDP; ユーザ データグラム プロトコル)で稼働し、UDP は IP 上で稼働します。NTP は RFC 1305 に規定されています。

NTP ネットワークは通常、ラジオ クロックやタイム サーバに接続されたアトミック クロックなど、信頼できる時刻源からその時刻を取得します。そのあと、NTP はネットワーク中にこの時刻を配信します。NTP はきわめて効率的で、1 分間に1 パケットを使用するだけで、2 台のデバイスを1 ミリ秒以内に同期化できます。

NTP は、ストラタムという概念を使用して、信頼できる時刻源とデバイスの間の NTP ホップ数を表します。ストラタム 1 タイム サーバには、ラジオ クロックまたはアトミック クロックが直接接続されており、ストラタム 2 タイム サーバは、NTP を使用してストラタム 1 タイム サーバから時刻を取得します(以降のストラタムも同様です)。NTP が稼働するデバイスは、時刻源として、NTPを使用して通信するストラタム番号が最小のデバイスを自動的に選択します。この手法により、NTP スピーカーの自動編成型ツリーが効率的に構築されます。

NTP では、同期化されていないデバイスとの同期化を防ぎます。また、NTP では、複数のデバイスから報告される時刻を比較して、ストラタムの数字が小さくても、時刻が他のデバイスと大幅に異なるデバイスとは同期化しません。

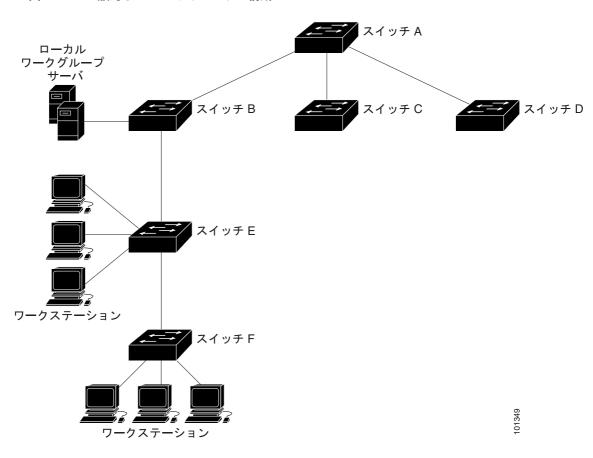
NTP が稼働するデバイス間の通信 (アソシエーション) は、通常静的に設定されます。各デバイスには、アソシエーションを行う全デバイスの IP アドレスが与えられます。アソシエーションのペアとなるデバイス間で NTP メッセージを交換することによって、正確な時刻の維持が可能になります。ただし、LAN 環境では、代わりに IP ブロードキャスト メッセージを使用するように NTP を設定できます。各デバイスを、単にブロードキャスト メッセージを送受信するように設定すればよいので、この代替手段により設定の複雑さが緩和されます。この場合は、情報の流れは一方向に限られます。

デバイス上で維持される時刻は、重要なリソースです。NTPのセキュリティ機能を使用して、不正確な時刻が誤ってあるいは意図的に設定されることを防いでください。アクセスリストを使用して制限する方式と暗号化認証メカニズムの、2つの方法を利用できます。

シスコの NTP 実装はストラタム 1 サービスをサポートしていないので、ラジオ クロックまたはアトミック クロックに接続できません。ネットワークの時刻サービスは IP インターネットで利用できるパブリック NTP サーバから取得することを推奨します。

図 4-1 に、NTP を使用した一般的なネットワーク例を示します。スイッチ A は NTP マスターです。 スイッチ B、C、および D は NTP サーバ モードで設定され、スイッチ A とのサーバ アソシエーションが設定されます。スイッチ E は、アップストリームおよびダウンストリームのスイッチ (スイッチ B およびスイッチ F) への NTP ピアとして設定されます。

図 4-1 一般的な NTP ネットワークの構成



ネットワークがインターネットから切り離されている場合、シスコの NTP 実装によって、実際には、他の方法で時刻が決定されているにもかかわらず、デバイスが NTP を使用して同期化しているように動作を設定できます。他のデバイスは、NTP によりこのデバイスと同期化されます。

NTP の時刻は、他の方法による時刻に優先します。

自社のホスト システムに NTP ソフトウェアを組み入れているメーカーもあり、また、UNIX システム用のパブリック バージョンやその派生ソフトウェアも入手できます。このソフトウェアによって、ホスト システムも時刻が同期化されます。

NTP の設定

ここでは、次の設定情報について説明します。

- NTP のデフォルト設定 (p.4-4)
- NTP 認証の設定 (p.4-4)
- NTP アソシエーションの設定 (p.4-6)
- NTP ブロードキャスト サービスの設定 (p.4-7)
- NTP アクセス制限の設定 (p.4-8)
- NTP パケット用の送信元 IP アドレスの設定 (p.4-10)
- NTP 設定の表示 (p.4-11)

NTP のデフォルト設定

表 4-1 に、NTP のデフォルト設定を示します。

表 4-1 NTP のデフォルト設定

機能	デフォルト設定
NTP 認証	ディセーブル。認証キーは指定されていません。
NTP ピアまたはサーバ アソシエーション	設定なし
NTP ブロードキャスト サービス	ディセーブル。どのインターフェイスも NTP ブロー
	ドキャストパケットを送受信しません。
NTP アクセス制限	アクセス制御は指定されていません。
NTP パケット送信元 IP アドレス	送信元アドレスは、発信インターフェイスによって 設定されます。

NTP は、すべてのインターフェイスにおいてデフォルトでイネーブルに設定されています。すべてのインターフェイスは、NTP パケットを受信します。

NTP 認証の設定

この手順は、NTP サーバの管理者と協調する必要があります。この手順で設定する情報は、時刻をNTP サーバと同期化するためにスイッチが使用するサーバの情報と一致している必要があります。

セキュリティ目的で他のデバイスとのアソシエーション(正確な時刻の維持を行うための NTP を実行するデバイス間の通信)を認証するには、次の作業を行います。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ntp authenticate	デフォルトではディセーブルに設定されている NTP 認証機能をイネーブルにします。
ステップ 3	ntp authentication-key number md5 value	認証キーを定義します。デフォルト設定では何も定義され ていません。
		• <i>number</i> には、キーの番号を指定します。有効範囲は 1 ~ 4294967295 です。
		• md5 は、Message Digest Algorithm 5 (MD5)を使用してメッセージ認証サポートが行われることを指定します。
		value には、キーに対する 8 文字までの任意のストリングを入力します。
		スイッチとデバイスの双方がいずれかの認証キーを持ち、
		ntp trusted-key key-number コマンドによってキー番号が指
		定されていないかぎり、スイッチはデバイスと同期化しません。
ステップ 4	ntp trusted-key key-number	1 つまたは複数のキー番号(ステップ 3 で定義したもの)を 指定します。ピア NTP デバイスは、このスイッチと同期化 するため、このスイッチへの NTP パケット内にこのキー番 号を設定しなければなりません。
		デフォルト設定では、信頼されるキーは定義されていませ ん。
		key-number には、ステップ 3 で定義されたキーを指定します。
		このコマンドは、スイッチが、信頼されていないデバイスと誤って同期化することを防止します。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show running-config	入力を確認します。
ステップァ	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

NTP 認証をディセーブルにするには、no ntp authenticate グローバル コンフィギュレーション コマンドを使用します。認証キーを削除するには、no ntp authentication-key number グローバル コンフィギュレーション コマンドを使用します。デバイスのアイデンティティの認証をディセーブルにするには、no ntp trusted-key key-number グローバル コンフィギュレーション コマンドを使用します。

次に、NTP パケットに認証キー 42 を設定しているデバイスとだけ同期するようにスイッチを設定する例を示します。

```
Switch# configure terminal
Switch(config)# ntp authenticate
Switch(config)# ntp authentication-key 42 md5 aNiceKey
Switch(config)# ntp trusted-key 42
Switch(config)# end
Switch#
```

NTP アソシエーションの設定

NTP アソシエーションは、ピア アソシエーション (スイッチを他のデバイスに同期化させることも、スイッチに対して他のデバイスを同期化させることも可能)に設定することも、サーバ アソシエーション (スイッチを他のデバイスに同期化させるのみで、その逆は不可)に設定することもできます。

別のデバイスとの NTP アソシエーションを形成するには、次の作業を行います。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ntp peer ip-address [version number] [key keyid] [source interface] [prefer]	スイッチのシステム クロックをピアに同期化するか、ピア によって同期化する (ピア アソシエーション)ように設定
	または	します。
	ntp server ip-address [version number]	または
	[key keyid] [source interface] [prefer]	スイッチのシステム クロックをタイム サーバによって同期化する (サーバ アソシエーション)ように設定します。
		ピアまたはサーバ アソシエーションはデフォルトでは定 義されていません。
		 ip-address には、ピア アソシエーションの場合にはクロックの同期化を行うまたは同期化の対象となるピアの IP アドレスを指定します。サーバ アソシエーションの場合には、クロックの同期化を行うタイム サーバのIP アドレスを指定します。
		• (任意) <i>number</i> には、NTP のバージョン番号を指定します。指定できる範囲は1~3です。デフォルトはバージョン3が選択されています。
		• (任意) keyid には、ntp authentication-key グローバル コンフィギュレーション コマンドで定義された認証 キーを入力します。
		• (任意) interface には、IP の送信元アドレスを取得する インターフェイスを指定します。デフォルトでは、送 信元 IP アドレスは発信インターフェイスから取得し ます。
		• (任意) prefer キーワードを入力すると、このピアまたはサーバが同期化を行う優先ピアまたはサーバになります。このキーワードは、ピアとサーバ間の切り替えを減らします。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	入力を確認します。
ステップ 5	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

設定する必要があるのは、アソシエーションの一端のみです。もう一方のデバイスには自動的にアソシエーションが設定されます。デフォルトの NTP バージョン (バージョン 3)を使用していて、NTP の同期化が発生しない場合は、NTP のバージョン 2を使用してください。インターネット上の多くの NTP サーバは、バージョン 2 で稼働しています。

ピアまたはサーバ アソシエーションを削除するには、no ntp peer *ip-address* または no ntp server *ip-address* グローバル コンフィギュレーション コマンドを使用します。

次に、NTP バージョン 2 を使用して IP アドレス 172.16.22.44 のピアのクロックに、システム クロックを同期化するようにスイッチを設定する例を示します。

Switch# configure terminal
Switch(config) # ntp server 172.16.22.44 version 2
Switch(config) # end
Switch#

NTP プロードキャスト サービスの設定

NTP が稼働するデバイス間の通信 (アソシエーション) は、通常静的に設定されます。各デバイスには、アソシエーションを行うべき全デバイスの IP アドレスが与えられます。アソシエーションのペアとなるデバイス間で NTP メッセージを交換することによって、正確な時刻の維持が可能になります。ただし、LAN 環境では、代わりに IP ブロードキャスト メッセージを使用するようにNTP を設定できます。各デバイスを、単にブロードキャスト メッセージを送受信するように設定すればよいので、この代替手段により設定の複雑さが緩和されます。ただし、この場合は、情報の流れは一方向に限られます。

ルータのようにネットワーク上で時刻情報をブロードキャストする NTP ブロードキャスト サーバがある場合、スイッチはインターフェイスごとに NTP ブロードキャスト パケットを送受信できます。スイッチは NTP ブロードキャスト パケットをピアへ送信できるので、ピアはそのスイッチに 同期化できます。スイッチは NTP ブロードキャスト パケットを受信して自身のクロックを同期化することもできます。ここでは、NTP ブロードキャスト パケットの送信と受信の両方の手順について説明します。

NTP ブロードキャスト パケットをピアに送信して、ピアが自身のクロックをスイッチに同期化するよう、スイッチを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	NTP ブロードキャスト パケットを送信するインターフェ
		イスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	ntp broadcast [version number] [key keyid]	NTP ブロードキャスト パケットをピアに送信するイン
	[destination-address]	ターフェイスをイネーブルにします。
		デフォルトでは、この機能はすべてのインターフェイスで
		ディセーブルです。
		• (任意) number には、NTP のバージョン番号を指定します。指定できる範囲は 1 ~ 3 です。バージョンを指定しなかった場合は、バージョン 3 が使用されます。
		• (任意) <i>keyid</i> には、ピアにパケットを送信するときに 使用する認証キーを指定します。
		● (任意) destination-address には、このスイッチにクロックを同期化するピアの IP アドレスを指定します。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	入力を確認します。
ステップ 6	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存し
		ます。
ステップ 7		次の手順で説明するように、接続されているピアが NTP ブロードキャスト パケットを受信するように設定します。

インターフェイスによる NTP ブロードキャスト パケットの送信をディセーブルにするには、no ntp broadcast インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートが NTP バージョン 2 パケットを送信するように設定する例を示します。

Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ntp broadcast version 2
Switch(config-if)# end
Switch#

接続したピアから NTP ブロードキャスト パケットを受信するようにスイッチを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	NTP ブロードキャスト パケットを受信するインターフェイスを 指定し、インターフェイス コンフィギュレーション モードを開始 します。
ステップ 3	ntp broadcast client	インターフェイスが NTP ブロードキャスト パケットを受信でき るようにします。
		デフォルトでは、インターフェイスは NTP プロードキャスト パケットを受信しません。
ステップ 4	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	ntp broadcastdelay microseconds	(任意)スイッチと NTP ブロードキャスト サーバ間の予測される ラウンドトリップ遅延を変更します。
		デフォルトは 3000 マイクロ秒です。指定できる範囲は 1 ~ 999999です。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show running-config	入力を確認します。
ステップ 8	copy running-config startup-config	(任意)コンフィギュレーションファイルに設定を保存します。

インターフェイスによる NTP ブロードキャスト パケットの受信をディセーブルにするには、no ntp broadcast client インターフェイス コンフィギュレーション コマンドを使用します。設定したラウンドトリップ遅延をデフォルト設定に変更するには、no ntp broadcastdelay グローバル コンフィギュレーション コマンドを使用します。

次に、ポートが NTP ブロードキャスト パケットを受信するように設定する例を示します。

Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ntp broadcast client
Switch(config-if)# end
Switch#

NTP アクセス制限の設定

ここでは、2つのレベルで NTP アクセスを制御する方法を説明します。

- アクセス グループの作成と基本 IP アクセス リストの割り当て (p.4-9)
- 特定のインターフェイスでの NTP サービスのディセーブル化 (p.4-10)

アクセス グループの作成と基本 IP アクセス リストの割り当て

アクセス リストを使用して NTP サービスへのアクセスを制御するには、次の作業を行います。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ntp access-group {query-only serve-only serve peer} access-list-number	アクセス グループを作成し、基本 IP アクセス リストを適 用します。
		キーワードの意味は次のとおりです。
		• query-only NTP 制御クエリーに限り許可します。
		• serve-only 時刻要求に限り許可します。
		• serve 時刻要求および NTP 制御クエリーは許可しますが、スイッチがリモート デバイスに同期化することは許可しません。
		• peer 時刻要求および NTP 制御クエリーを許可し、ス イッチがリモート デバイスに同期化することを許可し ます。
		access-list-number には、1 ~ 99 の範囲で標準の IP アクセス リスト番号を入力します。
ステップ 3	access-list access-list-number permit source	アクセス リストを作成します。
	[source-wildcard]	 access-list-number には、ステップ 2 で指定した番号を 入力します。
		• permit キーワードを入力すると、条件が一致した場合 にアクセスを許可します。
		 source には、スイッチへのアクセスが許可されるデバイスの IP アドレスを入力します。
		• (任意) source-wildcard には、送信元に適用するワイル ドカード ビットを入力します。
		(注) アクセス リストを作成するとき、アクセス リストの末尾にはデフォルトで、リストの末尾に達しても一致が見つからなかった場合に使用される、暗黙の拒否(deny)文がある点に留意してください。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	入力を確認します。
ステップ 6	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

アクセス グループのキーワードは、次の順序(最小の制限から最大の制限に)でスキャンされます。

- 1. peer 時刻要求および NTP 制御クエリーを許可し、さらに、スイッチが、アクセス リストの条件を満たすアドレスを持つデバイスに同期化することを許可します。
- 2. serve 時刻要求と NTP 制御クエリーを許可しますが、スイッチが、アクセス リストの条件を満たすアドレスを持つデバイスに同期化することを許可しません。
- 3. serve-only アクセス リストの条件を満たすアドレスを持つデバイスからの時刻要求に限り許可します。
- **4. query-only** アクセス リストの条件を満たすアドレスを持つデバイスからの NTP 制御クエリーに限り許可します。

複数のアクセス タイプについて送信元 IP アドレスがアクセス リストに一致する場合は、最初のタイプが認可されます。アクセス グループが指定されなかった場合は、すべてのアクセス タイプがすべてのデバイスに認可されます。いずれかのアクセス グループが指定されている場合は、指定されたアクセス タイプに限り認可されます。

スイッチ NTP サービスに対するアクセス制御を削除するには、no ntp access-group {query-only | serve-only | serve | peer} グローバル コンフィギュレーション コマンドを使用します。

次に、スイッチがアクセス リスト 99 のピアに同期化できるように設定する例を示します。ただし、 スイッチはアクセス リスト 42 に対してはアクセスを制限し、時刻要求に限り許可します。

```
Switch# configure terminal
Switch(config)# ntp access-group peer 99
Switch(config)# ntp access-group serve-only 42
Switch(config)# access-list 99 permit 172.20.130.5
Switch(config)# access list 42 permit 172.20.130.6
Switch(config)# end
Switch#
```

特定のインターフェイスでの NTP サービスのディセーブル化

NTP サービスは、すべてのインターフェイスにおいてデフォルトでイネーブルに設定されています。

インターフェイスで NTP パケットの受信をディセーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、ディ セーブルにするインターフェイスを指定します。
ステップ 3	ntp disable	インターフェイスで NTP パケットの受信をディセーブルにします。
		デフォルトでは、すべてのインターフェイスは NTP パケットを受信します。
		インターフェイスで NTP パケットの受信を再びイネーブルにするには、no ntp disable インターフェイス コンフィギュレーションコマンドを使用します。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	入力を確認します。
ステップ 6	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

NTP パケット用の送信元 IP アドレスの設定

スイッチが NTP パケットを送信すると、送信元 IP アドレスは、通常 NTP パケットが送信されたインターフェイスのアドレスに設定されます。すべての NTP パケットに特定の送信元 IP アドレスを使用する場合は、ntp source グローバル コンフィギュレーション コマンドを使用します。アドレスは指定されたインターフェイスから取得されます。インターフェイスのアドレスを返信パケットの宛先として使用できない場合に、このコマンドは便利です。

送信元 IP アドレスを取得する特定のインターフェイスを設定するには、次の作業を行います。

	コマンド	目的	
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。	
ステップ 2	ntp source type number	IP 送信元アドレスを取得するインターフェイスのタイプおよび番号を指定します。	
		デフォルトでは、送信元アドレスは、発信インターフェイスによって設定されます。	
ステップ 3	end	特権 EXEC モードに戻ります。	
ステップ 4	show running-config	入力を確認します。	
ステップ 5	copy running-config startup-config	(任意)コンフィギュレーションファイルに設定を保存します。	

指定されたインターフェイスは、すべての宛先に送信されるすべてのパケットの送信元アドレスに使用されます。送信元アドレスを特定のアソシエーションに使用する場合は、「NTP アソシエーションの設定」(p.4-6)で説明したように、ntp peer または ntp server グローバル コンフィギュレーション コマンドの source キーワードを使用します。

NTP 設定の表示

次の2つの特権 EXEC コマンドを使用して NTP 情報を表示できます。

- show ntp associations [detail]
- show ntp status

この出力に表示されるフィールドの詳細については、『Cisco IOS Configuration Fundamentals Command Reference』Release 12.3 を参照してください。

手動での日時の設定

他の時刻源が利用できない場合は、システムの再起動後、手動で日時を設定できます。時刻は、次にシステムを再起動するまで正確に維持されます。手動設定は最後の手段としてのみ使用することを推奨します。スイッチを同期化できる外部ソースがある場合は、手動でシステム クロックを設定する必要はありません。

ここでは、次の設定情報について説明します。

- システム クロックの設定 (p.4-11)
- 日時設定の表示 (p.4-12)
- 時間帯の設定 (p.4-12)
- 夏時間の設定 (p.4-13)

システム クロックの設定

ネットワーク上に、NTP サーバなどの時刻サービスを提供する外部ソースがある場合は、手動でシステム クロックを設定する必要がありません。

システム クロックを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	clock set hh:mm:ss day month year	次のいずれかの形式で、手動でシステム クロックを設定します。
または clock set hh:mm:ss month day year	• hh:mm:ss には、時刻を時間 (24 時間形式)、分、秒で指定します。指定された時刻は、設定された時間帯に基づきます。	
	clock set intimities month day year	• dayには、当月の日付で日を指定します。
		• month には、月を名前で指定します。
		year には、年を指定します(省略形不可)。

次に、システム クロックを手動で 2001 年の 7 月 23 日午後 1 時 32 分に設定する例を示します。

Switch# clock set 13:32:00 23 July 2001

日時設定の表示

日時の設定を表示するには、show clock [detail] 特権 EXEC コマンドを使用します。

システム クロックは、信頼性がある(正確性がある)かどうかを示す authoritative フラグを維持します。システム クロックが NTP などのタイミング ソースによって設定されている場合は、このフラグが設定されます。時刻が信頼できないものである場合は、表示目的でのみ使用されます。クロックが信頼できるようになって、authoritative フラグが設定されるまで、ピアの時刻が無効な場合に、このフラグによりピアがクロックと同期しないようにします。

show clock の表示の前にある記号は、次の意味があります。

- * 時刻は信頼できません。
- (空白) 時刻は信頼できます。
- . 時刻は信頼できますが、NTP は同期していません。

時間帯の設定

手動で時間帯を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	clock timezone zone hours-offset [minutes-offset]	時間帯を設定します。
		UTC に時刻を設定するには、 no clock timezone グローバル コンフィギュレーション コマンドを使用します。
		スイッチは内部時刻を UTC で管理するので、このコマンドは表示目的の場合および手動で時刻を設定した場合に限って使用します。
		• <i>zone</i> には、標準時間が施行されているときに表示され る時間帯の名前を入力します。デフォルトの設定は UTC です。
		• hours-offset には、UTC からの時差を入力します。
		• (任意) minutes-offset には、UTC からの分差を入力します。
ステップ 3	end	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	show running-config	入力を確認します。
ステップ 5	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存し
		ます。

clock timezone グローバル コンフィギュレーション コマンドの *minutes-offset* 変数は、現地の時間帯と UTC との時差が割合である場合に利用できます。たとえば、カナダ大西洋沿岸のある区域の時間帯 Atlantic Standard Time (AST; 大西洋標準時)は UTC-3.5 です。この場合、3 は 3 時間、.5 は 50% を意味します。この場合、入力するコマンドは **clock timezone AST -3 30** です。

夏時間の設定

毎年特定の日に夏時間が開始および終了する地域に夏時間を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	clock summer-time zone recurring [week day month hh:mm week day month hh:mm [offset]]	毎年指定された日に開始および終了する夏時間を設定します。
		夏時間はデフォルトでディセーブルに設定されています。 パラメータなしで clock summer-time zone recurring を指定 すると、夏時間の規則はデフォルトで米国の規則が設定さ れます。
		 zone には、夏時間が施行されているときに表示される 時間帯の名前(たとえば PDT)を指定します。
		(任意) week には、月の何番めの週かを指定します(1 ~ 5、または last)。
		• (任意) day には、曜日を指定します (Sunday、Monday など)。
		• (任意) <i>month</i> には、月を指定します(January、February など)。
		• (任意) hh:mm には、時刻を時間(24 時間形式)と分で指定します。
		• (任意) <i>offset</i> には、夏時間の間、追加する分数を指定 します。デフォルトは 60 です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	入力を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存し ます。

clock summer-time グローバル コンフィギュレーション コマンドの最初の部分では夏時間の開始時期を、2番めの部分では終了時期を指定します。すべての時刻は、現地の時間帯を基準にしています。開始時間は標準時を基準にしています。終了時間は夏時間を基準にしています。開始月が終了月よりあとの場合は、システムでは南半球にいるとみなされます。

次に、夏時間が 4 月の第一日曜日の 2 時に始まり、10 月の最終日曜日の 2 時に終わるように指定する例を示します。

Switch# configure terminal

Switch(config)# clock summer-time PDT recurring 1 Sunday April 2:00 last Sunday October 2:00

Switch(config)# end

Switch#

ユーザの居住地域の夏時間が定期的なパターンに従わない(次の夏時間の正確な日時を設定する)場合は、次の作業を行います。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	clock summer-time zone date [month date year hh:mm month date year hh:mm [offset]]	最初の日付で夏時間開始の日付を、2番めの日付で終了の日付を設定します。
	または clock summer-time zone date [date month year hh:mm date month year hh:mm [offset]]	夏時間をディセーブルにするには、no clock summer-time グローバル コンフィギュレーション コマンドを使用します。
	nn:mm aaie monin year nn:mm [ojjsei]]	夏時間はデフォルトでディセーブルに設定されています。
		• <i>zone</i> には、夏時間が施行されているときに表示される 時間帯の名前(たとえば PDT)を指定します。
		(任意) week には、月の何番めの週かを指定します(1 ~ 5、または last)。
		• (任意) day には、曜日を指定します (Sunday、Monday など)。
		• (任意) <i>month</i> には、月を指定します(January、February など)。
		• (任意) hh:mm には、時刻を時間 (24 時間形式)と分で指定します。
		 (任意) offset には、夏時間の間、追加する分数を指定 します。デフォルトは 60 です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	入力を確認します。
ステップ 5	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

clock summer-time グローバル コンフィギュレーション コマンドの最初の部分では夏時間の開始時期を、2 番めの部分では終了時期を指定します。すべての時刻は、現地の時間帯を基準にしています。開始時間は標準時を基準にしています。終了時間は夏時間を基準にしています。開始月が終了月よりあとの場合は、システムでは南半球にいるとみなされます。

夏時間をディセーブルにするには、no clock summer-time グローバル コンフィギュレーション コマンドを使用します。

次に、夏時間が 2000 年 10 月 12 日の 2 時に始まり、2001 年 4 月 26 日の 2 時に終わるよう設定する 例を示します。

Switch# configure terminal

Switch(config) # clock summer-time pdt date 12 October 2000 2:00 26 April 2001 2:00 Switch#

システム名とプロンプトの設定

スイッチにシステム名を設定すると、スイッチを識別できます。デフォルトでは、システム名とプロンプトは *Switch* です。

システム プロンプトを設定していない場合は、システム名の最初の 20 文字がシステム プロンプトとして使用されます。大なり記号 [>] が付加されます。システム名が変更された場合は、常にプロンプトも変更されます。

ここで使用するコマンドの構文および使用方法の詳細については、『Cisco IOS Configuration Fundamentals Command Reference』Release 12.3 および『Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols』Release 12.3 を参照してください。

ここでは、次の設定情報について説明します。

- デフォルトのシステム名およびプロンプトの設定(p.4-15)
- システム名の設定 (p.4-15)
- DNSの概要 (p.4-15)

デフォルトのシステム名およびプロンプトの設定

デフォルトのスイッチのシステム名およびプロンプトは Switch です。

システム名の設定

手動でシステム名を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	hostname name	手動でシステム名を設定します。
		デフォルト設定は switch です。
		名前は ARPANET ホスト名の規則に従う必要があります。この規則ではホスト名は文字で始まり、文字または数字で終わり、使用できるのは文字、数字、またはハイフンのみです。名前には 63 文字まで使用できます。
		デフォルトのホスト名に戻すには、no hostname グローバル コンフィギュレーション コマンドを使用します。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	入力を確認します。
ステップ 5	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

システム名を設定すると、システム プロンプトとしても使用されます。

DNS の概要

Domain Name System (DNS; ドメイン ネーム システム) プロトコルは、分散型データベースである DNS を制御します。これを使用することにより、ホスト名を IP アドレスに対応付けできます。スイッチに DNS を設定すると、ping、telnet、connect などのすべての IP コマンドや、関連する Telnet サポート操作時に、IP アドレスの代わりにホスト名を使用できます。

IPによって定義される階層型の命名方式では、デバイスを場所またはドメインで識別できます。ドメイン名の区切りとしては、ピリオド(.)を使用します。たとえば、シスコシステムズは、IPで com というドメイン名で識別される商業組織なので、ドメイン名は cisco.com となります。このドメイン内の特定のデバイス、たとえば FTP(ファイル転送プロトコル)システムは、ftp.cisco.com で表されます。

IP ではドメイン名を把握するために、ドメイン ネーム サーバという概念が定義されています。ドメイン ネーム サーバの役割は、名前と IP アドレスのマッピングをキャッシュ (またはデータベース)に保持することです。ドメイン名を IP アドレスにマッピングするには、まず、ホスト名を特定し、ネットワーク上に存在するネーム サーバを指定し、DNS をイネーブルにします。

ここでは、次の設定情報について説明します。

- DNS のデフォルト設定 (p.4-16)
- DNS の設定 (p.4-16)
- DNS 設定の表示 (p.4-17)

DNS のデフォルト設定

表 4-2 に、DNS のデフォルト設定を示します。

表 4-2 DNS のデフォルト設定

機能	デフォルト設定
DNS イネーブル ステート	イネーブル
DNS デフォルト ドメイン名	設定なし
DNS サーバ	ネーム サーバのアドレスの設定なし

DNS の設定

DNS を使用するようにスイッチを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip domain-name name	非完全修飾ホスト名(ドット付き 10 進表記ドメイン名のない名前)を完成させるためにソフトウェアが使用する、デフォルトのドメイン名を定義します。
		ドメイン名を削除するには、 no ip domain-name <i>name</i> グローバル コンフィギュレーション コマンドを使用します。
		ドメイン名を非完全修飾名から区切るために使用される最初のピ リオドは入れないでください。
		起動時にはドメイン名は設定されていませんが、BOOTP または Dynamic Host Configuration Protocol (DHCP) サーバからスイッチ コンフィギュレーションを取得している場合は、BOOTP または DHCP サーバによってデフォルトのドメイン名が設定されること があります (サーバにこの情報が設定されている場合)。

	コマンド	目的
ステップ 3	ip name-server server-address1 [server-address2 server-address6]	名前およびアドレスの解決に使用する、1 つまたは複数のネーム サーバのアドレスを指定します。
		ネーム サーバのアドレスを削除するには、 no ip name-server <i>server-address</i> グローバル コンフィギュレーション コマンドを使用します。
		最大 6 つのネーム サーバを指定できます。 各サーバ アドレスはスペースで区切ります。 最初に指定されたサーバが、プライマリサーバです。 スイッチは、最初にプライマリ サーバに DNS クエリーを送信します。 そのクエリーが失敗した場合は、バックアップサーバにクエリーが送信されます。
ステップ 4	ip domain-lookup	(任意)スイッチで、DNS ベースのホスト名のアドレスへの変換をイネーブルにします。この機能は、デフォルトでイネーブルに 設定されています。
		スイッチの DNS をディセーブルにするには、 no ip domain-lookup グローバル コンフィギュレーション コマンドを使用します。
		使用するネットワーク デバイスが、ユーザが名前の割り当てを制御できないネットワーク内のデバイスと接続する必要がある場合、グローバルなインターネットのネーミング方式 (DNS)を使用して、ユーザのデバイスを一意に特定するデバイス名を動的に割り当てることができます。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show running-config	入力を確認します。
ステップ 7	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

スイッチの IP アドレスをそのホスト名として使用する場合は、IP アドレスが使用され、DNS クエリーは発生しません。ピリオド(.) なしでホスト名を設定すると、ピリオドと、それに続くデフォルトのドメイン名がホスト名に追加され、そのあとで DNS クエリーが行われ、名前を IP アドレスに対応付けます。デフォルトのドメイン名は、ip domain-name グローバル コンフィギュレーション コマンドによって設定される値です。ホスト名にピリオド(.) がある場合は、Cisco IOS ソフトウェアは、ホスト名にデフォルトのドメイン名を追加せずに IP アドレスを検索します。

DNS 設定の表示

DNS 設定情報を表示するには、show running-config 特権 EXEC コマンドを使用します。

バナーの作成

Message-of-The-Day (MoTD) バナーおよびログイン バナーを設定できます。MoTD バナーはログイン時に接続しているすべての端末で表示され、すべてのネットワーク ユーザを対象としたメッセージ (システム シャットダウン予告など)を送信するのに便利です。

ログイン バナーも、接続しているすべての端末で表示されます。表示されるのは、MoTD バナーのあとで、ログイン プロンプトが表示される前です。



(注)

ここで使用するコマンドの構文および使用方法の詳細については、『Cisco IOS Configuration Fundamentals Command Reference』Release 12.3 を参照してください。

ここでは、次の設定情報について説明します。

- バナーのデフォルト設定 (p.4-18)
- MoTD ログイン バナーの設定 (p.4-18)
- ログイン バナーの設定 (p.4-19)

バナーのデフォルト設定

MoTD およびログイン バナーは設定されません。

MoTD ログイン バナーの設定

ユーザがスイッチにログインしたときに画面に表示される 1 行または複数行のメッセージ バナーを作成できます。

MoTD ログイン バナーを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	banner motd c message c	MoTD を指定します。
		MoTD バナーを削除するには、 no banner motd グローバル コンフィギュレーション コマンドを使用します。
		c には、任意の区切り文字、たとえばポンド記号(#)を入力して、 Return キーを押します。区切り文字はバナー テキストの始まりと 終わりを表します。終わりの区切り文字のあとの文字はドロップ されます。
		message には、255 文字までのバナー メッセージを入力します。 メッセージには区切り文字を使用できません。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	入力を確認します。
ステップ 5	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

次に、ポンド記号 (#) を開始および終了の区切り文字として使用し、スイッチの MoTD バナーを 設定する例を示します。

```
Switch(config)# banner motd #
This is a secure site. Only authorized users are allowed.
For access, contact technical support.
#
Switch(config)#
```

次に、前の設定により表示されたバナーを示します。

```
Unix> telnet 172.2.5.4
Trying 172.2.5.4...
Connected to 172.2.5.4.
Escape character is '^]'.

This is a secure site. Only authorized users are allowed.
For access, contact technical support.

User Access Verification
```

ログイン バナーの設定

Password:

接続されたすべての端末でログイン バナーが表示されるように設定できます。バナーが表示されるのは、MoTD バナーのあとで、ログイン プロンプトが表示される前です。

ログインバナーを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	banner login c message c	ログイン メッセージを指定します。
		ログイン バナーを削除するには、no banner login グローバル コンフィギュレーション コマンドを使用します。
		cには、任意の区切り文字、たとえばポンド記号(#)を入力して、Returnキーを押します。区切り文字はバナー テキストの始まりと終わりを表します。終わりの区切り文字のあとの文字はドロップされます。
		message には、255 文字までのログイン メッセージを入力します。 メッセージには区切り文字を使用できません。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	入力を確認します。
ステップ 5	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

次に、ドル記号(\$)を開始および終了の区切り文字として使用し、スイッチのログイン バナーを 設定する例を示します。

```
Switch# configuration terminal
Switch(config)# banner login $
Access for authorized users only. Please enter your username and password.
$
Switch(config)# end
Switch#
```

MAC アドレス テーブルの管理

MAC (メディア アクセス制御) アドレス テーブルには、スイッチがポート間のトラフィック転送 に使用するアドレス情報が含まれています。このアドレス テーブルに登録されたすべての MAC アドレスは、1 つまたは複数のポートに対応付けられています。アドレス テーブルに含まれるアドレス タイプには、次のものがあります。

- ダイナミック アドレス: スイッチが学習し、使用されなくなった時点で期限切れとなる送信元 MAC アドレス
- スタティック アドレス:手動で入力され、期限切れにならず、スイッチのリセット時にも消去されないユニキャスト アドレス

アドレス テーブルは、宛先 MAC アドレス、対応する VLAN ID、およびアドレスとタイプ(スタティックまたはダイナミック)に対応付けられたポート番号を示します。



ここで使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンド リファレンスを参照してください。

ここでは、次の設定情報について説明します。

- アドレス テーブルの作成 (p.4-20)
- MAC アドレスと VLAN (p.4-21)
- MAC アドレス テーブルのデフォルト設定 (p.4-21)
- アドレス エージング タイムの変更 (p.4-21)
- ダイナミック アドレス エントリの削除(p.4-22)
- MAC 変更通知トラップの設定 (p.4-22)
- MAC 移動通知トラップの設定 (p.4-25)
- MAC しきい値通知トラップの設定 (p.4-26)
- スタティック アドレス エントリの追加および削除 (p.4-27)
- ユニキャスト MAC アドレス フィルタリングの設定 (p.4-29)
- アドレス テーブル エントリの表示 (p.4-30)

アドレス テーブルの作成

すべてのポートでサポートされる複数の MAC アドレスによって、スイッチの任意のポートを各 ワークステーション、リピータ、スイッチ、ルータ、またはその他のネットワーク デバイスに接続 できます。各ポートで受信するパケットの送信元アドレスを学習し、アドレス テーブルにアドレス とその対応するポート番号を追加することにより、スイッチは動的なアドレス指定を行います。 ネットワークでステーションの増設または取り外しが行われると、スイッチはアドレス テーブルを 更新し、新しいダイナミック アドレスを追加したり、使用されていないアドレスを期限切れにした りします。

エージング インターバルは、グローバルに設定されています。ただし、スイッチは VLAN ごとに アドレス テーブルを維持し、STP によって VLAN 単位でエージング インターバルを短縮できます。

スイッチは、受信したパケットの宛先アドレスに基づいて、あらゆる組み合わせのポート間でパケットを送信します。MAC アドレス テーブルを使用することにより、スイッチは、宛先アドレスに対応付けられたポートにのみ、パケットを転送します。宛先アドレスがパケットを送信したポー

ト上にある場合は、パケットはフィルタリング処理され、転送されません。スイッチは、常にストア アンド フォワード方式を使用します。つまり、完全なパケットをいったん保存してエラーがないか検査してから伝送します。

MAC アドレスと VLAN

アドレスはすべて、VLAN と対応付けられます。1 つのアドレスを複数の VLAN に対応付け、それぞれで異なる宛先を設定できます。たとえば、VLAN 1 のポート 1、および VLAN 5 のポート 9、10、1 を宛先とするユニキャスト アドレスを設定できます。

VLAN ごとに、独自の論理アドレス テーブルが維持されます。ある VLAN で既知のアドレスが別の VLAN で認識されるには、別の VLAN 内のポートによって学習されるか、または別の VLAN 内のポートに静的に対応付けられる必要があります。

プライベート VLAN が設定されている場合、アドレスの学習方法は、MAC アドレスのタイプによって異なります。

- プライベート VLAN 上にある 1 つの VLAN で学習されたダイナミック MAC アドレスは、関連 VLAN で複製されます。たとえば、プライベート VLAN のセカンダリ VLAN で学習された MAC アドレスは、プライマリ VLAN に複製されます。
- プライマリまたはセカンダリ VLAN に設定されたスタティック MAC アドレスは、関連 VLAN には複製されません。プライベート VLAN のプライマリまたはセカンダリ VLAN 内にスタティック MAC アドレスを設定した場合、同じスタティック MAC アドレスをすべての 関連 VLAN にも設定する必要があります。

プライベート VLAN の詳細については、第36章「PVLAN の設定」を参照してください。

MAC アドレス テーブルのデフォルト設定

表 4-3 に、MAC アドレス テーブルのデフォルト設定を示します。

表 4-3 MAC アドレス テーブルのデフォルト設定

機能	デフォルト設定
エージング タイム	300 秒
ダイナミック アドレス	自動学習
	設定なし

アドレス エージング タイムの変更

ダイナミック アドレスは、スイッチが学習し、使用されなくなると期限切れになる送信元 MAC アドレスです。 すべての VLAN または指定した VLAN に対して、エージング タイムの設定を変更できます。

エージング タイムを短く設定しすぎると、アドレスが活用されないままテーブルから削除される可能性があります。その場合、スイッチは宛先が不明のパケットを受信すると、受信ポートと同じ VLAN 内のすべてのポートに、そのパケットをフラッディングします。この不必要なフラッディングによって、パフォーマンスに悪影響を及ぼす可能性があります。また、エージング タイムを長く設定しすぎると、アドレス テーブルが使用されないアドレスでいっぱいになり、これによって新しいアドレスを学習できなくなります。この結果フラッディングとなり、スイッチのパフォーマンスに悪影響を及ぼす可能性があります。

ダイナミック アドレス テーブルのエージング タイムを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	mac address-table aging-time [0 10-1000000] [vlan vlan-id]	ダイナミック エントリが使用または更新されたあと、MAC アドレス テーブル内に保持される時間を設定します。
		デフォルト値に戻すには、no mac address-table aging-time グローバル コンフィギュレーション コマンドを使用しま す。
		指定できる範囲は $10 \sim 1000000$ 秒です。デフォルトは 300 秒です。 0 を入力して期限切れをディセーブルにすることもできます。スタティック アドレス エントリは、期限切れになることもテーブルから削除されることもありません。 $vlan-id$ の有効範囲は、 $1 \sim 4094$ です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show mac address-table aging-time	入力を確認します。
ステップ 5	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

ダイナミック アドレス エントリの削除

ダイナミック エントリをすべて削除するには、EXEC モードで clear mac address-table dynamic コマンドを使用します。特定の MAC アドレス(clear mac address-table dynamic address mac-address) 指定された物理ポートまたはポート チャネル上のすべてのアドレス (clear mac address-table dynamic interface interface-id)、または指定された VLAN 上のすべてのアドレス (clear mac address-table dynamic vlan vlan-id) の削除もできます。

ダイナミック エントリが削除されたことを確認するには、show mac address-table dynamic 特権 EXEC コマンドを使用します。

MAC 変更通知トラップの設定

MAC 変更通知機能により、スイッチに MAC 変更アクティビティを保存することでネットワーク上のユーザを追跡できます。スイッチが MAC アドレスを学習または削除するたびに、SNMP 通知を生成してネットワーク管理システムに送信させることができます。ネットワークに多数のユーザの出入りがある場合は、トラップ インターバル タイムを設定して通知トラップをまとめ、ネットワークトラフィックを削減できます。MAC 通知履歴テーブルは、トラップがイネーブルに設定されたハードウェアのポートごとの MAC アドレス アクティビティを保存します。MAC アドレス通知は、ダイナミックおよびスタティックの MAC アドレスについて生成されます。自己アドレスまたはマルチキャスト アドレスについては、イベントは生成されません。

NMS ホストに MAC 変更通知トラップを送信するには、次の作業を行います。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	snmp-server host host-addr [traps / informs]	トラップ メッセージの受信側を指定します。
	{version {1 / 2c / 3}} [auth noauth priv] community-string [udp-port port] [notification-type]	 host-addr には、NMS の名前またはアドレスを指定します。
		• traps (デフォルト)を指定すると、SNMP トラップを ホストに送信します。informs を指定すると、SNMP イ ンフォームをホストに送信します。
		 サポートする SNMP バージョンを指定します。informs を指定した場合、バージョン 1 (デフォルト) は使用 できません。
		• community-string には、通知動作時に送信するストリングを指定します。snmp-server host コマンドを使用してこのストリングを設定できますが、このストリングを定義するには、最初に snmp-server community コマンドを使用し、次に snmp-server host コマンドを使用することを推奨します。
		• notification-type には、mac-notification キーワードを使用します。
ステップ 3	snmp-server enable traps mac-notification change	スイッチによる MAC 変更トラップの NMS への送信をイネーブルにします。
		スイッチによる MAC 変更通知トラップの送信をディセーブルにするには、no snmp-server enable traps mac-notification change グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	mac address-table notification change	MAC アドレス変更通知機能をイネーブルにします。
ステップ 5	mac address-table notification change [interval value] [history-size value]	トラップ インターバル タイムと履歴テーブルのサイズを入力します。
		(任意) interval value には、NMS に対して生成される 各トラップ セット間の通知トラップ インターバルを 秒単位で指定します。指定できる範囲は 0 ~ 2147483647 秒です。デフォルトは 1 秒です。
		 (任意)history-size value には、MAC 通知履歴テーブルの最大エントリ数を指定します。指定できる範囲は 0~500です。デフォルトは 1 です。
		MAC 変更通知機能をディセーブルにするには、no mac address-table notification change グローバル コンフィギュレーション コマンドを使用します。
ステップ 6	interface interface-id	インターフェイス コンフィギュレーション モードを開始 し、SNMP MAC 変更通知トラップをイネーブルにするインターフェイスを指定します。

	コマンド	目的
ステップィ	snmp trap mac-notification change {added removed}	MAC 変更通知トラップをイネーブルにします。
	removeu }	• added を指定すると、このインターフェイスに MAC アドレスが追加されるたびに MAC 変更通知トラップが送信されます。
		• removed を指定すると、このインターフェイスから MAC アドレスが削除されるたびに MAC 変更通知ト ラップが送信されます。
		特定のインターフェイス上で MAC 変更通知トラップを ディセーブルにするには、no snmp trap mac-notification change {added removed} インターフェイス コンフィギュ レーション コマンドを使用します。
ステップ 8	end	特権 EXEC モードに戻ります。
ステップ 9	show mac address-table notification change interface	入力を確認します。
	show running-config	
ステップ 10	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

次に、ネットワーク管理システムとして 172.69.59.93 を指定し、スイッチによるネットワーク管理システムへの MAC 変更通知トラップの送信をイネーブルにし、MAC 変更通知機能をイネーブルにし、インターバル タイムを 60 秒、履歴サイズを 100 エントリに設定し、特定のポートで MAC アドレスが追加された場合のトラップをイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config) # snmp-server host 172.69.59.93 private mac-notification
Switch(config)# snmp-server enable traps mac-notification change
Switch(config) # mac address-table notification change
Switch(config) # mac address-table notification change interval 60
Switch(config)# mac address-table notification change history-size 100
Switch(config)# interface fastethernet0/2
Switch(config-if) # snmp trap mac-notification change added
Switch(config-if)# end
Switch# show mac address-table notification change interface
MAC Notification Feature is Enabled on the switch
MAC Notification Flags For All Ethernet Interfaces :
Interface
                   MAC Added Trap MAC Removed Trap
                    -----
GigabitEthernet1/1 Enabled
                                 Enabled
                                 Enabled
GigabitEthernet1/2 Enabled
GigabitEthernet1/3
                   Enabled
                                  Enabled
                                 Enabled
GigabitEthernet1/4 Enabled
                                 Enabled
GigabitEthernet1/5 Enabled
GigabitEthernet1/6 Enabled
                                 Enabled
GigabitEthernet1/7
                   Enabled
                                  Enabled
GigabitEthernet1/8
                    Enabled
                                  Enabled
GigabitEthernet1/9
                                 Enabled
                    Enabled
GigabitEthernet1/10 Enabled
                                 Enabled
                                 Enabled
GigabitEthernet1/11 Enabled
GigabitEthernet1/12 Enabled
                                  Enabled
```

Switch#

MAC 移動通知トラップの設定

MAC 移動通知を設定すると、MAC アドレスが同一 VLAN 内の特定のポートから別のポートに移動するたびに、SNMP 通知が生成され、ネットワーク管理システムに送信されます。

MAC 移動通知を設定にするには、次の作業を行います。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	snmp-server host host-addr [traps / informs] {version {1 / 2c / 3}} [auth noauth priv]	トラップ メッセージの受信側を指定します。
	community-string [udp-port port] [notification-type]	 host-addr には、NMS の名前またはアドレスを指定します。
	[nonjteunon-type]	• traps (デフォルト)を指定すると、SNMP トラップを ホストに送信します。informs を指定すると、SNMP イ ンフォームをホストに送信します。
		 サポートする SNMP バージョンを指定します。informs を指定した場合、バージョン 1 (デフォルト) は使用 できません。
		• community-string には、通知動作時に送信するストリングを指定します。snmp-server host コマンドを使用してこのストリングを設定できますが、このストリングを
		定義するには、最初に snmp-server community コマンドを使用し、次に snmp-server host コマンドを使用することを推奨します。
		• notification-type には、mac-notification キーワードを使用します。
ステップ 3	snmp-server enable traps mac-notification	スイッチによる MAC 移動通知トラップの NMS への送信
	move	をイネーブルにします。
		スイッチによる MAC 通知トラップの送信をディセーブル
		にするには、no snmp-server enable traps mac-notification
		move グローバル コンフィギュレーション コマンドを使用
		します。
ステップ 4	mac address-table notification mac-move	MAC 移動通知機能をイネーブルにします。
		この機能をディセーブルにするには、
		no mac-address-table notification mac-move グローバル コン
		フィギュレーション コマンドを使用します。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show mac address-table notification mac-move	MAC 移動通知ステータスを表示します。
	show running-config	
ステップ 7	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

次に、ネットワーク管理システムとして 172.69.59.93 を指定し、スイッチによる MAC 移動通知トラップの NMS への送信をイネーブルにし、MAC 移動通知機能をイネーブルにし、MAC アドレスが特定のポートから別のポートに移動する場合のトラップをイネーブルにする例を示します。

Switch# configure terminal

Switch(config)# snmp-server host 171.69.59.93 private mac-notification

Switch(config)# snmp-server enable traps mac-notification move

Switch(config)# mac address-table notification mac-move

Switch(config)# end

Switch# show mac address-table notification mac-move

MAC Move Notification: Enabled

MAC しきい値通知トラップの設定

MAC しきい値通知を設定すると、MAC Address Table (MAT) しきい値の制限値に達した時点または制限値を超えた時点で、SNMP 通知が生成され、ネットワーク管理システムに送信されます。

MAC アドレスしきい値通知を設定にするには、次の作業を行います。

コマンド	目的
configure terminal	グローバル コンフィギュレーション モードを開始します。
snmp-server host host-addr [traps / informs] {version {1 / 2c / 3}} [auth neauth priv]	トラップ メッセージの受信側を指定します。
community-string [udp-port port]	host-addr には、NMS の名前またはアドレスを指定します。
[nonjieunon-type]	• traps(デフォルト)を指定すると、SNMP トラップを ホストに送信します。informs を指定すると、SNMP イ ンフォームをホストに送信します。
	 サポートする SNMP バージョンを指定します。informs を指定した場合、バージョン 1 (デフォルト) は使用 できません。
	• community-string には、通知動作時に送信するストリングを指定します。snmp-server host コマンドを使用してこのストリングを設定できますが、このストリングを定義するには、最初に snmp-server community コマンドを使用し、次に snmp-server host コマンドを使用することを推奨します。
	 notification-type には、mac-notification キーワードを使用します。
snmp-server enable traps mac-notification threshold	スイッチによる MAC しきい値通知トラップの NMS への 送信をイネーブルにします。
	スイッチによる MAC しきい値通知トラップの送信をディセーブルにするには、no snmp-server enable traps mac-notification threshold グローバル コンフィギュレーション コマンドを使用します。
mac address-table notification threshold	MAC アドレスしきい値通知機能をイネーブルにします。
	この機能をディセーブルにするには、
	no address-table notification threshold グローバル コンフィ
	ギュレーション コマンドを使用します。
	configure terminal snmp-server host host-addr [traps / informs] {version {1 / 2c / 3}} [auth noauth priv] community-string [udp-port port] [notification-type] snmp-server enable traps mac-notification threshold

	コマンド	目的
ステップ 5	mac address-table notification threshold	MAT 使用率を監視するためのしきい値を入力します。
	[limit percentage] [interval time]	 (任意) limit percentage には、MAT 利用率の割合を指定します。指定できる値は、1 ~ 100% です。デフォルトは 50% です。 (任意) interval time には、通知の間隔を指定します。指定できる値は、120 秒以上です。デフォルトは 120 秒です。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show mac address-table notification threshold	MAT 利用率しきい値通知ステータスを表示します。
	show running-config	
ステップ 8	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存し
		ます。

次に、ネットワーク管理システムとして 172.69.59.93 を指定し、MAC しきい値通知機能をイネーブルにし、スイッチによる MAC しきい値通知トラップの NMS への送信をイネーブルにし、間隔を123 秒に設定し、制限値を 78% に設定する例を示します。

スタティック アドレス エントリの追加および削除

スタティック アドレスには、次の特性があります。

- アドレステーブルに対する追加および削除は、手動で行う必要があります。
- ユニキャスト アドレスまたはマルチキャスト アドレスとして設定できます。
- 期限切れになることはなく、スイッチが再起動しても維持されます。

スタティック アドレスを追加および削除でき、また、スタティック アドレスの転送動作を定義できます。転送動作とは、パケットを受信したポートが、別のポートにパケットを転送する際の動作です。ポートは必ず最低 1 つの VLAN に対応付けられているので、スイッチは指定されたポートから、アドレスに対応する VLAN ID を取得します。送信元ポートごとに、それぞれ異なる宛先ポートのリストを指定できます。

特定のアドレスがスタティックとして入力されていない VLAN に、そのスタティック アドレスを持つパケットが到着すると、そのパケットはすべてのポートにフラッディングされ、学習されません。

アドレス テーブルにスタティック アドレスを追加するには、宛先 MAC ユニキャスト アドレスと、その宛先の VLAN を指定します。この宛先アドレスを持つ受信パケットは、*interface-id* オプションで指定されたインターフェイスに転送されます。

プライベート VLAN のプライマリまたはセカンダリ VLAN 内にスタティック MAC アドレスを設定した場合、同じスタティック MAC アドレスをすべての関連 VLAN にも設定する必要があります。 プライベート VLAN のプライマリまたはセカンダリ VLAN に設定されたスタティック MAC アドレスは、関連 VLAN には複製されません。プライベート VLAN の詳細については、第 36 章「PVLAN の設定」を参照してください。

スタティック アドレスを追加するには、次の作業を行います。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	mac address-table static mac-addr vlan vlan-id interface interface-id	MAC アドレス テーブルにスタティック アドレスを追加し ます。
		 mac-addrには、アドレステーブルに追加する宛先MAC ユニキャストアドレスを指定します。この宛先アドレスを持つパケットが指定した VLAN に着信すると、指定したインターフェイスに転送されます。
		 vlan-id には、指定した MAC アドレスを持つパケット を受信する VLAN を指定します。有効な VLAN ID は 1 ~ 4094 です。
		 interface-id には、受信したパケットの転送先インターフェイスを指定します。有効なインターフェイスは、物理ポートまたはポートチャネルです。スタティックマルチキャストアドレスの場合、複数のインターフェイス ID を入力できます。スタティックユニキャストアドレスの場合、インターフェイスは同時に1つしか入力できません。ただし、同じ MAC アドレスおよびVLAN ID を指定したコマンドを複数回入力できます。
		アドレス テープルからスタティック エントリを削除する には、no mac address-table static mac-addr vlan vlan-id [interface interface-id] グローバル コンフィギュレーション コマンドを使用します。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show mac address-table static	入力を確認します。
ステップ 5	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存し ます。

次に、MAC アドレス テーブルにスタティック アドレス c2f3.220a.12f4 を追加する例を示します。 VLAN 4 でこの MAC アドレスを宛先アドレスとして持つパケットを受信すると、パケットは指定されたポートに転送されます。

Switch# configure terminal
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface
gigabitethernet0/1
Switch(config)# end
Switch#

ユニキャスト MAC アドレス フィルタリングの設定



ユニキャスト MAC アドレス フィルタリングは、Supervisor Engine 6-E ではサポートされてIIません。

ユニキャスト MAC アドレス フィルタリングがイネーブルの場合、スイッチは、特定の送信元 MAC アドレスまたは宛先 MAC アドレスを持つパケットをドロップします。 この機能は、デフォルトではディセーブルで、ユニキャスト スタティック アドレスだけがサポートされています。

この機能を使用する場合は、次の注意事項に従ってください。

• マルチキャスト MAC アドレス、ブロードキャスト MAC アドレス、およびルータ MAC アドレスはサポートされていません。mac address-table static mac-addr vlan vlan-id drop グローバル コンフィギュレーション コマンドを入力するときに、これらのアドレスのいずれかを指定すると、次のいずれかのメッセージが表示されます。

% Only unicast addresses can be configured to be dropped

% CPU destined address cannot be configured as drop address

- CPU に転送されるパケットもサポートされていません。
- ユニキャスト MAC アドレスをスタティック アドレスとして追加し、ユニキャスト MAC アドレス フィルタリングを設定すると、最後に入力したコマンドに応じて、スイッチはその MAC アドレスをスタティック アドレスとして追加するか、その MAC アドレスを持つパケットをドロップします。2 番めに入力したコマンドは、1 番めのコマンドより優先されます。

たとえば、mac address-table static mac-addr vlan vlan-id interface グローバル コンフィギュレーション コマンドに続けて、mac address-table static mac-addr vlan vlan-id drop コマンドを入力すると、スイッチは、送信元または宛先として指定された MAC アドレスを持つパケットをドロップします。

mac address-table static mac-addr vlan vlan-id drop グローバル コンフィギュレーション コマンドに続けて、mac address-table static mac-addr vlan vlan-id interface コマンドを入力すると、スイッチは、スタティック アドレスとして MAC アドレスを追加します。

ユニキャスト MAC アドレス フィルタリングをイネーブルにして、スイッチが特定のアドレスを持つパケットをドロップするように設定するには、送信元または宛先ユニキャスト MAC アドレスおよび受信側の VLAN を指定します。

スイッチが送信元または宛先ユニキャスト スタティック アドレスをドロップするよう設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	mac address-table static mac-addr vlan vlan-id drop	ユニキャスト MAC アドレス フィルタリングをイネーブルにし、スイッチが指定した送信元または宛先ユニキャスト スタティック アドレスを持つパケットをドロップするように設定します。
		 mac-addr には、送信元または宛先ユニキャスト MAC アドレスを指定します。この MAC アドレスを持つパケットはドロップされます。
		 vlan-id には、指定した MAC アドレスを持つパケットを受信する VLAN を指定します。有効な VLAN ID は 1 ~ 4094です。
		ユニキャスト MAC アドレス フィルタリングをディセーブルにするには、no mac address-table static mac-addr vlan vlan-id グローバル コンフィギュレーション コマンドを使用します。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show mac address-table static	入力を確認します。
ステップ 5	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

次にユニキャスト MAC アドレス フィルタリングをイネーブルにし、送信元または宛先アドレスが c2f3.220a.12f4 であるパケットをスイッチがドロップするように設定する例を示します。 この MAC アドレスを送信元または宛先としたパケットを VLAN 4 で受信すると、パケットはドロップされます。

Switch# configure terminal
Switch(config)# mac Address-table static c2f3.220a.12f4 vlan 4 drop
Switch(config)# end
Switch#

アドレス テーブル エントリの表示

表 4-4 に示す 1 つまたは複数の特権 EXEC コマンドを使用すると、MAC アドレス テーブルを表示できます。

表 4-4 MAC アドレス テーブル表示用のコマンド

コマンド	説明
show ip igmp snooping groups	すべての VLAN または指定された VLAN に対するレイヤ 2 マルチキャスト エントリを表示します。
show mac address-table address	指定された MAC アドレスに対する MAC アドレス テーブル情報を表示します。
show mac address-table aging-time	すべての VLAN または指定された VLAN のエージング タイムを表示します。
show mac address-table count	すべての VLAN または指定された VLAN に存在するアドレスの数を表示します。
show mac address-table dynamic	ダイナミック MAC アドレス テーブル エントリのみを表示します。
show mac address-table interface	指定されたインターフェイスに対する MAC アドレス テーブル情報を表示します。
show mac address-table notification	MAC 通知パラメータおよび履歴テーブルを表示します。
show mac address-table static	スタティック MAC アドレス テーブル エントリのみを表示します。
show mac address-table vlan	指定された VLAN に対する MAC アドレス テーブル情報を表示します。

ARP テーブルの管理

ソフトウェアがデバイスと通信するには (イーサネット上のデバイスなど)、最初にそのデバイスの 48 ビット MAC アドレスまたはローカル データ リンク アドレスを学習する必要があります。IP アドレスからローカル データ リンク アドレスを学習するプロセスを、*アドレス解決*といいます。

Address Resolution Protocol (ARP; アドレス 解決 プロトコル)は、ホスト IP アドレスを、該当するメディアまたは MAC アドレス、および VLAN ID に対応付けます。IP アドレスを使用して、ARP は対応する MAC アドレスを見つけます。MAC アドレスが見つかると、IP と MAC アドレスとの対応を ARP キャッシュに格納し、すばやく検索できるようにします。そのあと、IP データグラムがリンク レイヤ フレームにカプセル化され、ネットワークを通じて送信されます。イーサネット以外の IEEE 802 ネットワークにおける IP データグラムのカプセル化および ARP 要求 / 応答については、Subnetwork Access Protocol (SNAP; サブネットワーク アクセス プロトコル)で指定されています。IP インターフェイスでは、標準的なイーサネット形式の ARP カプセル化 (arpa キーワードで表される)がデフォルトでイネーブルに設定されています。

手動でテーブルに追加された ARP エントリは期限切れにならないので、手動で削除する必要があります。

CLI の手順については、Cisco.com で入手可能な Cisco IOS Release 12.3 のマニュアルを参照してください。

組み込み CiscoView サポートの設定

Catalyst 4500 シリーズ スイッチは、Catalyst Web Interface (CWI) ツールを使用した CiscoView Web ベースの管理機能をサポートしています。CiscoView は、スイッチ フラッシュ上に組み込むことができるデバイス管理アプリケーションで、スイッチのダイナミック ステータス、モニタリング、および設定情報を提供します。CiscoView では、モジュールとポートが色分けされたスイッチ シャーシの物理的ビューを表示します。モニタリング機能を使用すると、スイッチのステータス、パフォーマンス、およびその他の統計情報が表示されます。必要なセキュリティ権限が与えられていれば、設定機能によって、デバイスにさまざまな変更を加えることができます。Catalyst 4500 シリーズ スイッチの設定機能およびモニタリング機能は、CiscoWorks LAN Management Solution (LMS) および CiscoWorks Routed WAN Management Solution (RWAN) を含むすべてのサーバベースのCiscoWorks ソリューションの CiscoView で使用可能な機能と同一です。

ここでは、Cisco IOS Release 12.1(20)EW 以降のリリースで使用できる組み込み CiscoView サポート について説明します。

- 組み込み CiscoView の概要 (p.4-31)
- 組み込み CiscoView のインストールおよび設定 (p.4-32)
- 組み込み CiscoView 情報の表示 (p.4-34)

組み込み CiscoView の概要

組み込み CiscoView ネットワーク管理システムは、HTTP および SNMP を使用してスイッチのグラフィカル表示を提供し、GUI ベースの管理および設定インターフェイスを提供する Web ベースのインターフェイスです。組み込み CiscoView 用の Java Archive (JAR) ファイルを次の URL からダウンロードできます。

http://www.cisco.com/cgi-bin/tablebuild.pl/cview-cat4000

組み込み CiscoView のインストールおよび設定

組み込み CiscoView をインストールおよび設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router# dir device_name	デバイスの内容を表示します。
		組み込み CiscoView を初めてインストールする場合、または CiscoView ディレクトリが空の場合には、ステップ 5 に進んでください。
ステップ 2	Switch# delete device_name:cv/*	CiscoView ディレクトリから既存のファイルを削除します。
ステップ 3	Switch# squeeze device_name:	ファイル システムのスペースを回復します。
ステップ 4	Switch# copy tftp bootflash	tar ファイルをブートフラッシュにコピーします。
ステップ 5	Switch# archive tar /xtract tftp:// ip address of tftp server/ciscoview.tar device_name:cv	Trivial File Transfer Protocol(TFTP; 簡易ファイル転送プロトコル)サーバ上の tar ファイルから CiscoView ディレクトリに、CiscoView ファイルを抽出します。
ステップ 6	Switch# dir device_name:	デバイスの内容を表示します。 冗長構成の場合、冗長スーパーバイザエンジン上のファイルシステムについてステップ 1~ステップ 6を繰り返します。
ステップ 7	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 8	Switch(config)# ip http server	HTTP Web サーバをイネーブルにします。
ステップ 9	Switch(config)# snmp-server community string ro	読み取り操作用の SNMP パスワードを設定します。
ステップ 10	Switch(config)# snmp-server community string rw	読み取り / 書き込み操作用の SNMP パスワードを設定します。



スイッチ Web ページにアクセスするためのデフォルトのパスワードは、スイッチのイネーブル レベル パスワードです。

次に、スイッチに組み込み CiscoView をインストールおよび設定する例を示します。

```
Switch# dir
Directory of bootflash:/
Directory of bootflash:/
              9572396 Dec 30 2002 01:05:01 +00:00 cat4000-i9k2s-mz.121-19.EW
   1 -rw-
   2 -rw-
              9604192 Jan 3 2003 07:46:49 +00:00 cat4000-i5k2s-mz.121-19.EW
               1985024 Jan 21 2003 03:31:20 +00:00 Cat4000IOS.v4-0.tar
   3
      -rw-
   4
               1910127 Jan 23 2003 04:23:39 +00:00 cv/Cat4000IOS-4.0.sgz
      -rw-
   5 -rw-
                  7258 Jan 23 2003 04:23:46 +00:00 cv/Cat4000IOS-4.0 ace.html
   6 -rw-
                   405 Jan 23 2003 04:23:46 +00:00 cv/Cat4000IOS-4.0_error.html
                  2738 Jan 23 2003 04:23:46 +00:00 cv/Cat4000IOS-4.0_install.html
   7
      -rw-
   8
      -rw-
                 20450 Jan 23 2003 04:23:46 +00:00 cv/Cat4000IOS-4.0_jks.jar
                 20743 Jan 23 2003 04:23:46 +00:00 cv/Cat4000IOS-4.0_nos.jar
   9
      -rw-
   10 -rw-
                 12383 Jan 23 2003 04:23:46 +00:00 cv/applet.html
   11 -rw-
                  529 Jan 23 2003 04:23:46 +00:00 cv/cisco.x509
   12 -rw-
                  2523 Jan 23 2003 04:23:46 +00:00 cv/identitydb.obj
                  1173 Mar 19 2003 05:50:26 +00:00
   13
post-2003.03.19.05.50.07-passed.txt
32578556 bytes total (38199688 bytes free)
Switch#
Switch# del cv/*
Delete filename [cv/*]?
Delete bootflash:cv/Cat4000IOS-4.0.sgz? [confirm]y
Delete bootflash:cv/Cat4000IOS-4.0_ace.html? [confirm]y
Delete bootflash:cv/Cat4000IOS-4.0_error.html? [confirm]y
Delete bootflash:cv/Cat4000IOS-4.0_install.html? [confirm]y
Delete bootflash:cv/Cat4000IOS-4.0_jks.jar? [confirm]y
Delete bootflash:cv/Cat4000IOS-4.0_nos.jar? [confirm]y
Delete bootflash:cv/applet.html? [confirm]y
Delete bootflash:cv/cisco.x509? [confirm]y
Delete bootflash:cv/identitydb.obj? [confirm]y
Switch#
Switch# squeeze bootflash:
All deleted files will be removed. Continue? [confirm]y
Squeeze operation may take a while. Continue? [confirm]y
Squeeze of bootflash complete
Switch#
Switch# copy tftp bootflash
Address or name of remote host []? 10.5.5.5
Source filename []? Cat4000IOS.v5-1.tar
Destination filename [Cat4000IOS.v5-1.tar]?
Accessing tftp://10.5.5.5/Cat4000IOS.v5-1.tar...
Loading Cat4000IOS.v5-1.tar from 10.5.5.5 (via FastEthernet2/1):
[OK - 2031616 bytes]
2031616 bytes copied in 11.388 secs (178400 bytes/sec)
Switch#
Switch# dir
Directory of bootflash:/
Directory of bootflash:/
              9572396 Dec 30 2002 01:05:01 +00:00 cat4000-i9k2s-mz.121-19.EW
   1 -rw-
   2 -rw-
               9604192 Jan 3 2003 07:46:49 +00:00 cat4000-i5k2s-mz.121-19.EW
               1985024 Jan 21 2003 03:31:20 +00:00 Cat4000IOS.v4-0.tar
   3 -rw-
                  1173 Mar 19 2003 05:50:26 +00:00
post-2003.03.19.05.50.07-passed.txt
              2031616 Mar 26 2003 05:33:12 +00:00 Cat4000IOS.v5-1.tar
   5 -rw-
32578556 bytes total (38199688 bytes free)
Switch#
Switch# archive tar /xtract Cat4000IOS.v5-1.tar /cv
extracting Cat4000IOS-5.1.sgz (1956591 bytes)
extracting Cat4000IOS-5.1_ace.html (7263 bytes)
extracting Cat4000IOS-5.1_error.html (410 bytes)
```

```
extracting Cat4000IOS-5.1 install.html (2743 bytes)
extracting Cat4000IOS-5.1_jks.jar (20450 bytes)
extracting Cat4000IOS-5.1_nos.jar (20782 bytes)
extracting applet.html (12388 bytes)
extracting cisco.x509 (529 bytes)
extracting identitydb.obj (2523 bytes)
Switch#
Switch# dir
Directory of bootflash:/
              9572396 Dec 30 2002 01:05:01 +00:00 cat4000-i9k2s-mz.121-19.EW
   1 -rw-
              9604192 Jan 3 2003 07:46:49 +00:00 cat4000-i5k2s-mz.121-19.EW
   2 -rw-
               1985024 Jan 21 2003 03:31:20 +00:00 Cat4000IOS.v4-0.tar
                 1173 Mar 19 2003 05:50:26 +00:00
post-2003.03.19.05.50.07-passed.txt
              2031616 Mar 26 2003 05:33:12 +00:00 Cat4000IOS.v5-1.tar
               1956591 Mar 26 2003 05:36:11 +00:00 cv/Cat4000IOS-5.1.sgz
   6 -rw-
                  7263 Mar 26 2003 05:36:19 +00:00 cv/Cat4000IOS-5.1_ace.html
   8 -rw-
                  410 Mar 26 2003 05:36:19 +00:00 cv/Cat4000IOS-5.1_error.html
                 2743 Mar 26 2003 05:36:19 +00:00 cv/Cat4000IOS-5.1_install.html
   9 -rw-
   10 -rw-
                20450 Mar 26 2003 05:36:19 +00:00 cv/Cat4000IOS-5.1_jks.jar
   11
                 20782 Mar 26 2003 05:36:19 +00:00 cv/Cat4000IOS-5.1_nos.jar
      -rw-
                 12388 Mar 26 2003 05:36:19 +00:00 cv/applet.html
   12
      -rw-
                  529 Mar 26 2003 05:36:19 +00:00 cv/cisco.x509
  13 -rw-
  14 -rw-
                 2523 Mar 26 2003 05:36:19 +00:00 cv/identitydb.obj
32578556 bytes total (7358284 bytes free)
Switch#
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config) # ip http server
Switch(config)# snmp-server community public ro
Switch(config) # snmp-server community public rw
Switch(config)# exit
Switch# wr
Building configuration...
Compressed configuration from 2735 bytes to 1169 bytes[OK]
Switch# show ciscoview ?
 package ADP Package Details
  version ADP version
          Output modifiers
```

スイッチへの Web アクセスについては、次の URL の『Cisco IOS Configuration Fundamentals Configuration Guide』の「Using the Cisco Web Browser」の章を参照してください。

http://www.cisco.com/univered/cc/td/doc/product/software/ios122/122cgcr/fun_c/fcprt1/fcd105.htm

組み込み CiscoView 情報の表示

組み込み CiscoView 情報を表示するには、次のコマンドを入力します。

コマンド	目的
Switch# show ciscoview package	組み込み CiscoView ファイルに関する情報を表示します。
Switch# show ciscoview version	組み込み CiscoView のバージョンを表示します。

次に、組み込み CiscoView ファイルおよびバージョン情報を表示する例を示します。

Switch# show ciscoview package

File source:

CVFILE	SIZE(in bytes)
Cat4000IOS-5.1.sgz	1956591
Cat4000IOS-5.1_ace.html	7263
Cat4000IOS-5.1_error.html	410
Cat4000IOS-5.1_install.html	2743
Cat4000IOS-5.1_jks.jar	20450
Cat4000IOS-5.1_nos.jar	20782
applet.html	12388
cisco.x509	529
identitydb.obj	2523

Switch# show ciscoview version

Engine Version: 5.3.4 ADP Device: Cat4000IOS ADP Version: 5.1 ADK: 49 Switch#

■ 組み込み CiscoView サポートの設定



CHAPTER

5

Cisco IOS ISSU プロセスの設定

冗長システムで稼働している場合、ISSU プロセスにより、Cisco IOS ソフトウェアが更新または変更される間もパケットの転送が続行されます。ほとんどのネットワークでは、計画されたソフトウェア アップグレードが大幅なダウンタイムの原因になります。ISSU により、Cisco IOS ソフトウェアが変更される間、パケットの転送が続行されます。これにより、ネットワークのアベイラビリティが向上し、計画されたソフトウェア アップグレードによって発生するダウンタイムが抑えられます。ここでは、ISSU の概念について説明し、システムで ISSU を実行するための手順について説明します。



この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/cr/index.htm

関連資料

関連トピック	資料のタイトル
ISSU の実行	© Cisco IOS Software: Guide to Performing In Service Software Upgrades a
Cisco Nonstop Forwarding(NSF)に関する情報	[©] Cisco Nonstop Forwarding a
	http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s20/fsnsf20s.htm
Stateful Switchover (SSO) に関する情報	[™] Stateful Switchover ¤
	http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snw ft/release/122s20/fssso20s.htm
ISSU クライアントおよび MPLS クライアント	F ISSU MPLS Clients ₫

内容

- ISSU を実行するための前提条件 (p.5-2)
- ISSU の実行に関する制約事項 (p.5-3)
- ISSU の実行に関する情報 (p.5-3)
- ISSU プロセスの実行方法 (p.5-14)

ISSU を実行するための前提条件

Switch#

適用される前提条件は、次のとおりです。

- ISSU を適用できるのは冗長シャーシだけです。
- アクティブスーパーバイザエンジンとスタンバイスーパーバイザエンジンの両方がシステムで使用でき、両方のエンジンのタイプが同じであることを確認します(たとえば、WS-X4516-10GE)。
- ISSU プロセスを開始する前に、アクティブ スーパーバイザ エンジンとスタンバイ スーパーバイザ エンジンの両方のファイル システム (ブートフラッシュまたはコンパクト フラッシュ) に新規および古い Cisco IOS ソフトウェア イメージがロードされている必要があります。古いイメージは、ブートフラッシュまたはコンパクト フラッシュのどちらかに格納されている必要があります。ISSU プロセスが展開される前にブート変数を変更するべきではないので、これらのいずれかのロケーションからシステムが起動されている必要があります。
- SSO が設定されており、スタンバイ スーパーバイザ エンジンが STANDBY HOT ステートである必要があります。

show module、show running-config、show redundancy state コマンドを使用すると、SSO がイネーブルかどうかを確認することができます。

次に、show redundancy state コマンドを使用して、冗長ファシリティ ステートに関する情報を表示する例を示します。

```
Switch# show redundancy states
      my state = 13 -ACTIVE
    peer state = 8 -STANDBY HOT
          Mode = Duplex
          Unit = Primary
        Unit ID = 1
Redundancy Mode (Operational) = Stateful Switchover
Redundancy Mode (Configured) = Stateful Switchover
Redundancy State
                              = Stateful Switchover
Maintenance Mode = Disabled
   Manual Swact = enabled
 Communications = Up
   client count = 39
client_notification_TMR = 240000 milliseconds
         keep_alive TMR = 9000 milliseconds
       keep alive count = 0
    keep_alive threshold = 18
          RF debug mask = 0x0
```

• NSF が設定されており、正常に稼働している必要があります。NSF をイネーブルにしていない場合は、NSF をイネーブルにし、設定する方法の詳細について、 $^{\mathbb{C}}$ Cisco Nonstop Forwarding $_{\mathbb{Z}}$ を 参照してください。

ISSU の実行に関する制約事項

適用される制約事項は、次のとおりです。

ISSU を実行する前に、システムが冗長モード SSO に設定されており、アクティブ スーパーバイザ エンジンとスタンバイ スーパーバイザ エンジンの両方のファイル システムに新しい ISSU 互換イメージが含まれていることを確認します。システムで実行されている現在の IOS バージョンも ISSU をサポートしている必要があります。

Catalyst 4500 シリーズ スイッチで各種のコマンドを実行することにより、スーパーバイザ エンジンのバージョンと IOS の互換性を判別できます。 Cisco Feature Navigator の ISSU アプリケーションを使用して判別することもできます。

- ISSU プロセスの実行中は、ハードウェアに変更を加えないでください。
- ISSU は、Cisco IOS 12.2(31)SGA およびそれ以降のリリースで使用できます。



すべてのラインカードがサポートされています。

ISSU の実行に関する情報

ISSU を実行する前に、次の概念を理解しておく必要があります。

- SSOの概要 (p.5-3)
- NSFの概要 (p.5-5)
- ISSU プロセスの概要 (p.5-6)
- ISSU をサポートする Cisco IOS ソフトウェアのバージョニング機能(p.5-11)
- ISSU に対する SNMP サポート (p.5-13)
- Cisco Feature Navigator を使用した互換性の検証 (p.5-13)

SSO の概要

SSO 機能の展開は、Cisco IOS スイッチで構築されたネットワークのアベイラビリティを向上させる全体的なプログラムの 1 ステップです。

デュアル スーパーバイザ エンジンをサポートする特定のシスコ ネットワーキング デバイス上で、SSO はスーパーバイザ エンジンの冗長構成を活用してネットワークのアベイラビリティを向上させます。SSO は、スーパーバイザ エンジンの 1 つをアクティブ プロセッサ、もう一方をスタンバイ プロセッサとして設定することにより、これを実現します。2 つのスーパーバイザ エンジン間の初期同期後に、SSO は両方のスーパーバイザ エンジンのステート情報を動的にリアルタイムで同期化します。

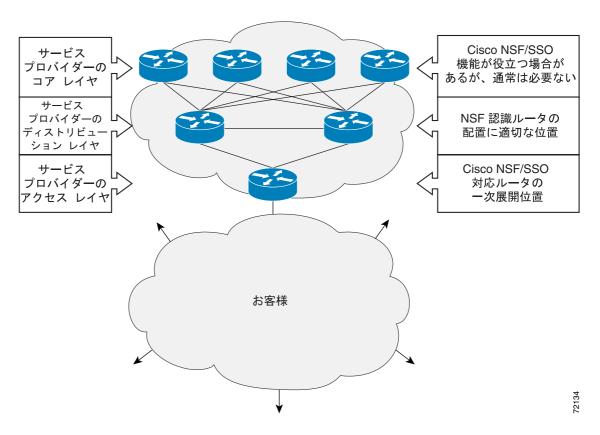
アクティブ スーパーバイザ エンジンが故障した場合、またはネットワーキング デバイスから取り 外された場合に、アクティブ スーパーバイザ エンジンからスタンバイ スーパーバイザ エンジンへ のスイッチオーバーが行われます。

Cisco NSF は、SSO と併用します。Cisco NSF によって、スイッチオーバー後にルーティング プロトコル情報が復元される間、データ パケットの転送が既知のルートで続行されます。Cisco NSF を使用すると、ピア ネットワーキング デバイスでルーティング フラップが発生することがなくなるため、カスタマーに対するサービス停止を回避できます。

図 5-1 は、サービス プロバイダー ネットワークに SSO が展開される一般的な方法を示します。この例では、Cisco NSF/SSO がサービス プロバイダー ネットワークのアクセス レイヤ (エッジ)でイネーブルにされています。このポイントで障害が発生すると、サービス プロバイダー ネットワークへのアクセスが必要なエンタープライズ カスタマーのサービスを損なう可能性があります。

Cisco NSF プロトコルでは、隣接デバイスが Cisco NSF に関与している必要があるので、これらの 隣接ディストリビューション レイヤ デバイスには、Cisco NSF 認識ソフトウェア イメージをイン ストールする必要があります。目的に応じて、ネットワークのコア レイヤで Cisco NSF および SSO 機能を展開することもできます。これを行うと、特定の障害が発生した場合のネットワーク機能およびサービスの復元にかかる時間を削減できるため、さらにアベイラビリティが向上します。

図 5-1 Cisco NSF/SSO ネットワーク構成:サービス プロバイダー ネットワーク



アベイラビリティの向上は、シングル ポイント障害が存在するネットワーク内の他のポイントに Cisco NSF/SSO を展開することによって得られます。図 5-2 は、エンタープライズ ネットワーク アクセス レイヤに Cisco NSF/SSO を適用するもう 1 つの展開方法を示します。この例では、エンタープライズ ネットワーク内の各アクセス ポイントが、ネットワーク設計内の他のシングル ポイント障害を表します。この例では、スイッチオーバーまたは計画されたソフトウェア アップグレードが行われても、エンタープライズ カスタマー セッションは中断することなくネットワーク内で稼働し続けます。

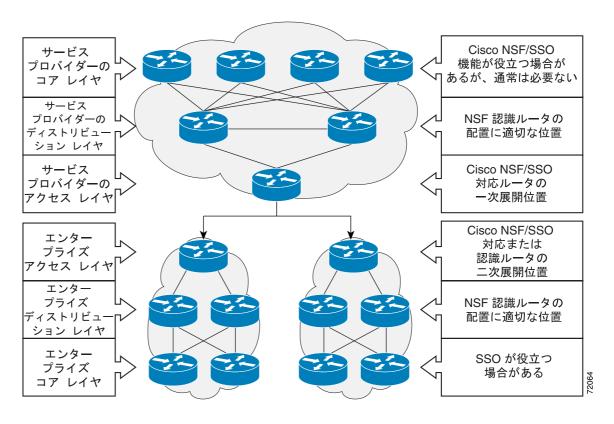


図 5-2 Cisco NSF/SSO ネットワーク構成:エンタープライズ ネットワーク

SSO の詳細については、『Stateful Switchover』を参照してください。

NSF の概要

Cisco NSF は、Cisco IOS ソフトウェアの SSO 機能と連動します。SSO は、Cisco NSF の前提条件です。NSF は、SSO と連動して、スイッチオーバー後にユーザがネットワークを使用できない時間を最小限に抑えます。Cisco NSF の主要目的は、スーパーバイザ エンジンのスイッチオーバー後にも IP パケットの転送を継続させることです。

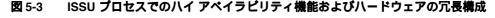
通常、ネットワーク デバイスが再起動すると、そのデバイスのすべてのルーティング ピアは、デバイスがダウンし、そのあと再びアップになったことを検知します。このような移行によって、いわゆるルーティング フラップが発生します。ルーティング フラップは、複数のルーティング ドメインに広がる場合があります。ルーティングの再起動によって発生するルーティング フラップは、ルーティング動作を不安定にし、ネットワーク全体のパフォーマンスに悪影響を及ぼします。Cisco NSF は、SSO 対応のデバイスにおけるルーティング フラップを抑止することによって、ネットワークの安定性を保ちます。

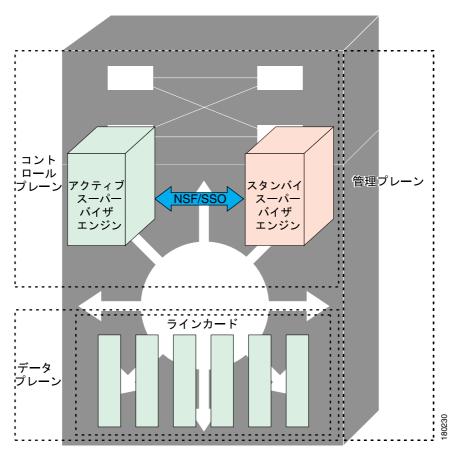
Cisco NSF によって、スイッチオーバー後にルーティング プロトコル情報が復元される間、データのパケットの転送が既知のルートで続行されます。Cisco NSF を使用すると、ピア ネットワーキング デバイスでルーティング フラップが発生することがありません。スイッチオーバー時に、故障したアクティブ スーパーバイザ エンジンからスタンバイ スーパーバイザ エンジンが制御を引き継ぐ間も、データ トラフィックが転送されます。Cisco NSF 動作で重要なのは、スイッチオーバー時に物理リンクがアップの状態を維持できる点と、アクティブ スーパーバイザ エンジン上のForwarding Information Base (FIB; 転送情報ベース)との同期性が保たれる点です。

ISSU プロセスの概要

ISSU プロセスにより、Cisco IOS ソフトウェア アップグレードまたはダウングレードを実行している間、パケットの転送が継続されます(ISSU プロセスの間に使用されるコマンドのインストレーションについては、図 5-8 [p.5-11] を参照してください)。Cisco IOS ISSU は Cisco IOS ハイ アベイラビリティ インフラストラクチャ(Cisco NSF/SSO およびハードウェアの冗長構成)を利用し、システムの稼働中に変更を行えるようにすることによって、ソフトウェア アップグレードまたはバージョン変更に伴うダウンタイムをなくします(図 5-3 を参照)。

SSO/NSF モードは、アクティブ スーパーバイザ エンジンからスタンバイ スーパーバイザ エンジンへの設定とランタイム ステートの同期をサポートしています。これには、アクティブ スーパーバイザ エンジンとスタンバイ スーパーバイザ エンジンの両方のイメージが同じである必要があります。アクティブ スーパーバイザ エンジンとスタンバイ スーパーバイザ エンジンのイメージが異なる場合、IOS のこれらの 2 つバージョンが異なるフィーチャ セットとコマンドをサポートしていても、ISSU は 2 つのスーパーバイザ エンジンを同期させたまま維持します。



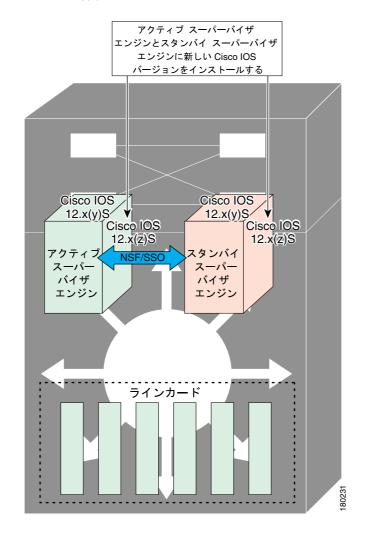


ISSU 対応スイッチは、2 つのスーパーバイザ エンジン (アクティブとスタンバイ) および 1 つまたは複数のラインカードで構成されています。 ISSU プロセスを開始する前に、両方のスーパーバイザ エンジンのファイル システムに Cisco IOS ソフトウェアをコピーします (図 5-4 を参照)。



次の図では、Cisco IOS 12.x(y)S は、IOS の*現在の*バージョンを表しています。

図 5-4 両方のスーパーパイザ エンジンへの新しい Cisco IOS ソフトウェア パージョンのインストールまたはコピー

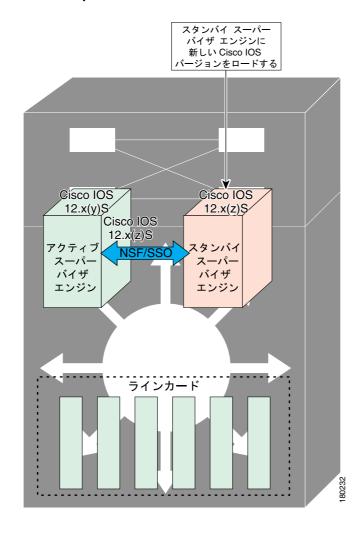


両ファイル システムに Cisco IOS ソフトウェアをコピーしたあと、新しい Cisco IOS ソフトウェア バージョンをスタンバイ スーパーバイザ エンジンにロードします (\boxtimes 5-5 を参照)。



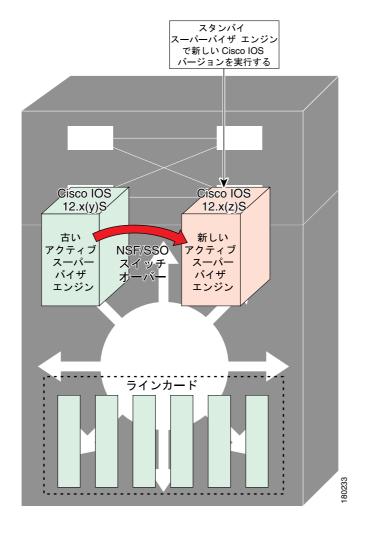
ISSU 機能がないと、アクティブ スーパーバイザ エンジンとスタンバイ スーパーバイザ エンジン が 2 つの異なる IOS イメージ バージョンを実行している場合に、両者間で SSO/NSF 機能は動作しません。

図 5-5 スタンパイ スーパーパイザ エンジンへの新しい Cisco IOS ソフトウェア パージョンのロード



スイッチオーバー (RPR ではなく、NSF/SSO) のあと、スタンバイ スーパーバイザ エンジンが新しくアクティブになったスーパーバイザ エンジンとして機能を引き継ぎます (図 5-6 を参照)。

図 5-6 スタンパイ スーパーパイザ エンジンへのスイッチオーパー



以前にアクティブだったスーパーバイザエンジンには古い IOS イメージがロードされているので、新しくアクティブになったスーパーバイザエンジンに問題が発生した場合には、中断して、すでに古いイメージを実行しているアクティブだったスーパーバイザエンジンにスイッチオーバーできます。その後、アクティブだったスーパーバイザエンジンに新しい Cisco IOS ソフトウェア バージョンがロードされ、新しいスタンバイスーパーバイザエンジンになります(図 5-7 を参照)。

図 5-7 新しくスタンバイになったスーパーバイザ エンジンへの新しい Cisco IOS ソフトウェアの ロード

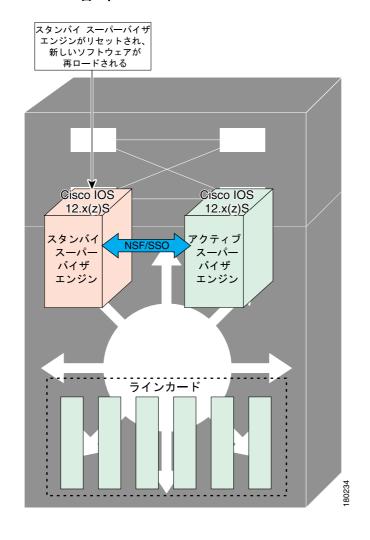
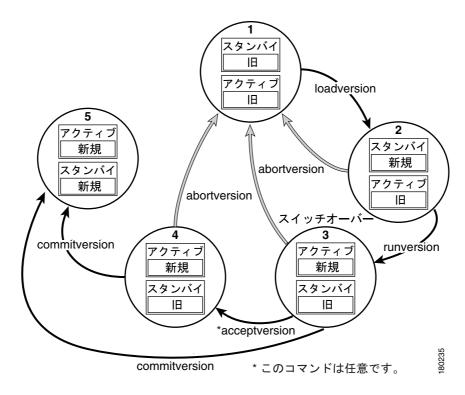


図 5-8 に、ISSU プロセス中の各ステップを示します。

図 5-8 ISSU プロセス中の各ステップ



ISSU をサポートする Cisco IOS ソフトウェアのバージョニング機能

ISSU が導入される以前は、SSO モードを実行するには、各スーパーバイザ エンジンで同じ Cisco IOS ソフトウェア バージョンを実行する必要がありました。



冗長 HA 構成のシステムの動作モードは、スタンバイ スーパーバイザ エンジンがアクティブ スーパーバイザ エンジンに登録するときにバージョン ストリングを交換することによって決まります。

システムが SSO モードを開始するのは、両方のスーパーバイザ エンジンで実行されているバージョンが同じである場合だけです。バージョンが同じでないと、冗長モードが RPR に変更されます。ISSU 機能を使用した場合、Cisco IOS イメージが同じでなくても、互換性のあるリリース レベルであれば両方のイメージを SSO モードで相互運用し、パケットの転送を継続したまま、ソフトウェアのアップグレードを行うことが可能になります。ISSU 機能が導入される前に行われていたバージョン チェックでは、システムが動作モードを決定できなくなりました。

ISSU では、ソフトウェア バージョン間の互換性を判別するための追加情報が必要になります。そのため、互換性マトリクスで、問題のバージョンにかかわる他のイメージに関する情報が定義されます。この互換性マトリクスは、2 つのソフトウェア バージョン (1 つは、アクティブ スーパーバイザ エンジンで実行されるソフトウェア バージョンで、もう一方はスタンバイ スーパーバイザ エンジンで実行されるソフトウェア バージョン)の互換性を表し、これによって、システムは実現可能な最も高度な動作モードを判別できます。バージョンに互換性がないと、SSO 動作モードに進むことができません。

Cisco IOS インフラストラクチャが内部的に変更されて、ISSU とともにサブシステム バージョニングが行われるように再設計されました。Cisco IOS サブシステムは、フィーチャ セットおよびソフトウェア コンポーネントのグループ化に対応しています。スーパーバイザ エンジン間でステート情報を維持する機能またはサブシステムは、HA 認識または、SSO クライアントです。ISSU フレームワークと呼ばれるメカニズムまたは ISSU プロトコルによって、Cisco IOS ソフトウェア内のサブシステムはアクティブ スーパーバイザ エンジンとスタンバイ スーパーバイザ エンジン間で通信を行って、スーパーバイザ エンジン間の通信のメッセージ バージョンをネゴシエーションすることができます。内部では、HA を認識するすべての NSF/SSO 対応アプリケーションまたはサブシステムが、このプロトコルに従って、異なるソフトウェア バージョンのピアとの通信を確立する必要があります (動作モードの詳細については、『 Stateful Switchover』を参照してください)。

互換性マトリクス

アクティブ スーパーバイザ エンジンとスタンバイ スーパーバイザ エンジンの両方の Cisco IOS ソフトウェアが ISSU に対応しており、古いイメージと新しいイメージに互換性がある場合に、ISSUプロセスを実行できます。互換性マトリクス情報では、次のようにリリース間の互換性が示されます。

- Compatible (互換性がある) ベースレベルのシステム インフラストラクチャとすべてのオプションの HA 認識サブシステムに互換性があります。これらのバージョン間のインサービスアップグレードまたはダウングレードが行われても、サービスに対する影響は最小限ですみます。マトリクス エントリでは、このようなイメージに対して Compatible (C) が指定されます。
- Base-level compatible (ベースレベルで互換性がある) 1 つまたは複数のオプションの HA 認識サブシステムに互換性がありません。これらのバージョン間のインサービス アップグレード またはダウングレードは正常に行われますが、IOS バージョンが旧式から新規に移行される際に、一部のサブシステムがステートを常に維持することができません。マトリクス エントリでは、このようなイメージに対して Base-level compatible (B) が指定されます。
- Incompatible(互換性がない) SSO が正常に機能するためには、IOS 内に存在するシステム インフラストラクチャのコア セットがステートフル方式で相互動作できる必要があります。必要なこれらのいずれかの機能またはサブシステムが相互動作できないと、Cisco IOS ソフトウェアイメージの 2 つのバージョンに互換性がないと判定されます。これらのバージョン間でインサービス アップグレードまたはダウングレードを行うことはできません。マトリクス エントリでは、このようなイメージに対して Incompatible(I)が指定されます。システムは、アクティブ スーパーバイザ エンジンとスタンバイ スーパーバイザ エンジンの IOS バージョンに互換性がない間は RPR モードで稼働します。

ISSU をサポートしないピアで ISSU を実行しようとすると、システムは代わりに RPR を自動的に使用します。

互換性マトリクスには、指定されたサポート ウィンドウ内の他のすべての Cisco IOS ソフトウェア バージョンに対してある Cisco IOS ソフトウェア イメージが持つ互換性の関係 (たとえば、イメージが「認識」できるすべてのソフトウェア バージョン)が示され、各イメージにデータが格納された状態でリリースされます。マトリクスには、自身のリリースと以前のリリース間の互換性の情報が含まれています。常に最新のリリースに、その分野の既存のリリースとの互換性に関する最新情報が含まれます。互換性マトリクスは Cisco IOS ソフトウェア イメージ内および Cisco.com で入手できるため、ISSU プロセスを使用してアップグレードを行えるかどうかを前もって判別できます。

任意のシステムの 2 つのソフトウェア バージョン間の互換性マトリクス データを表示するには、show issu comp-matrix stored コマンドを入力します。



このコマンドは、ISSU プロセスが開始した*あとでのみ*使用できるので、*確認する場合にのみ*有効です。ISSU を開始する前に互換性マトリクスをチェックする場合に便利です。Feature Navigator を使用すると、必要な情報を取得できます。

http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp

ISSU に対する SNMP サポート

SSO に対する SNMP は、アクティブ スーパーバイザ エンジンとスタンバイ スーパーバイザ エンジンが同じ Cisco IOS ソフトウェア バージョンを実行していることを前提として、SNMP 設定と MIB (Management Information Base; 管理情報ベース)を同期化するメカニズムを提供し、アクティブ スーパーバイザ エンジンからスタンバイ スーパーバイザ エンジンへの SSO をサポートしています。この前提は、ISSU には当てはまりません。

ISSU を使用した場合、SNMP クライアントは必要に応じて、2 つの異なる Cisco IOS バージョン間で MIB の変換を行うことができます。SNMP クライアントはすべての MIB の変換を行い、アクティブ スーパーバイザ エンジンとスタンバイ スーパーバイザ エンジン間送受信機能を行います。 SNMP の実行時に、両方の Cisco IOS リリースの MIB バージョンが同じである場合にのみ、MIB がアクティブ スーパーバーザ エンジンからスタンバイ スーパーバイザ エンジンに完全に同期化されます。

Cisco Feature Navigator を使用した互換性の検証

Cisco Feature Navigator の ISSU アプリケーションでは、次の内容を実行することができます。

- ISSU 対応イメージを選択する
- そのイメージと互換性があるイメージを確認する
- 2 つのイメージを比較して、イメージの互換性レベル (Compatible、Base-level compatible、および Incompatible) を理解する
- 2 つのイメージを比較して、各 ISSU クライアントのクライアント互換性を参照する
- イメージのリリース ノートに対するリンクを提供する

ISSU プロセスの実行方法

デバイスの動作モードであり、ISSU を実行するための前提条件である SSO とは異なり、ISSU プロセスはスイッチの稼動中に実行される一連のステップです。このステップによって、Cisco IOS ソフトウェアが新しいソフトウェアにアップグレードまたは変更されますが、トラフィックへの影響は最小限に抑えられます。



ISSU プロセスで使用されるコマンドの説明については、図 5-8 (p.5-11) を参照してください。

ISSU プロセスの実行中は、次の制約事項に注意してください。

- ISSU を使用している場合でも、メンテナンス ウィンドウの間にアップグレードを実行することを推奨します。
- ISSU プロセス中は、設定の変更が必要になるような新しい機能をイネーブルにしないでください。
- ダウングレードを行う場合、Cisco IOS ソフトウェア イメージのダウングレード リビジョンに ない機能があったときは、ISSU プロセスを開始する前にその機能をディセーブルにしてください。

ここでは、次の内容について説明します。

- ISSU ソフトウェア インストレーションの確認 (p.5-14)
- スタンバイ スーパーバイザ エンジンへの新しい Cisco IOS ソフトウェアのロード (p.5-17)(必 須)
- スタンバイ スーパーバイザ エンジンへの切り替え(p.5-20)(必須)
- ISSU ロールバック タイマーの停止 (任意)(p.5-23)(任意)
- 新しくスタンバイになったスーパーバイザ エンジンへの新しい Cisco IOS ソフトウェアのロード(p.5-24)
- ISSU プロセス中のソフトウェア アップグレードの中断 (p.5-26)
- アップグレード問題を回避するためのロールバック タイマーの設定 (p.5-27)
- ISSU 互換性マトリクス情報の表示 (p.5-28)

ISSU ソフトウェア インストレーションの確認

ISSU プロセスには、5 つのステート (Disabled、Init、Load Version、Run Version、および System Reset) があります。show issu state コマンドを使用すると、現在の ISSU ステートを取得できます。

- Disabled ステート スタンバイ スーパーバイザ エンジンがリセットされている間のこのエンジンの状態
- Init ステート ISSU プロセスが開始する前の、2 つのスーパーバイザ エンジン (1 つはアクティブで、もう一方はスタンバイ)の初期ステートです。ISSU プロセスが完了したあとの最終ステートでもあります。
- Load Version(LV)ステート スタンバイ スーパーバイザ エンジンに新しい Cisco IOS ソフトウェア バージョンがロードされています。
- Run Version (RV) ステート **issu runversion** コマンドによって、スーパーバイザ エンジンの スイッチオーバーが強制されます。新しくアクティブになったスーパーバイザ エンジンが現在 新しい Cisco IOS ソフトウェア イメージを実行しています。
- System Reset (SR) ステート このステートは Init ステートに達する前に issu abortversion コマンドを実行した場合、または issu acceptversion コマンドを実行する前にロールバック タイマーの期限が切れた場合に、発生します。

show コマンドを入力して、ISSU プロセス中のステートに関する情報を取得して、ISSU ソフトウェア インストレーションを確認できます。

手順の要約

- 1. enable
- 2. show issu state [detail]
- 3. show redundancy

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Switch> enable	特権 EXEC モードをイネーブルにします。
		プロンプトが表示されたら、パスワードを入力します。
ステップ 2	Switch# show issu state [detail]	ISSU プロセス中のスーパーバイザ エンジンのステートを表示し
		ます。
ステップ 3	Switch# show redundancy	デバイスの現在または過去のステータス、モード、および関連する冗長情報を表示します。

次に、ISSU プロセス中のスーパーバイザ エンジンのステートと現在のステータスを表示する例を示します。

Switch> enable
Switch# show issu state
Switch# show redundancy

ISSU プロセスを開始する前の冗長モードの確認

ISSU プロセスを開始する前に、システムの冗長モードを確認して、NSF/SSO を必ず設定するようにしてください。

次に、システムが SSO モードを開始しており、スロット 1 がアクティブ スーパーバイザ エンジンで、スロット 2 がスタンバイ スーパーバイザ エンジンであることを確認する例を示します。両方のスーパーバイザ エンジンで同じ Cisco IOS ソフトウェア イメージを実行しています。

```
Switch# show redundancy states
      mv state = 13 -ACTIVE
     peer state = 8 -STANDBY HOT
          Mode = Duplex
          Unit = Primary
        Unit ID = 1
Redundancy Mode (Operational) = Stateful Switchover
Redundancy Mode (Configured) = Stateful Switchover
Redundancy State
                              = Stateful Switchover
Maintenance Mode = Disabled
   Manual Swact = enabled
 Communications = Up
  client count = 39
client_notification_TMR = 240000 milliseconds
         keep_alive TMR = 9000 milliseconds
       keep_alive count = 0
    keep_alive threshold = 18
          RF debug mask = 0x0
Switch# show redundancy
Redundant System Information:
      Available system uptime = 1 minute
Switchovers system experienced = 0
              Standby failures = 0
        Last switchover reason = none
                Hardware Mode = Duplex
    Configured Redundancy Mode = Stateful Switchover
     Operating Redundancy Mode = Stateful Switchover
             Maintenance Mode = Disabled
               Communications = Up
Current Processor Information :
              Active Location = slot 1
       Current Software state = ACTIVE
       Uptime in current state = 0 minutes
                Image Version = Cisco IOS Software, Catalyst 4500 L3 Switch Software
(cat4500-ENTSERVICES-M), Version 12.2(31)SGA, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Tue 05-Sep-06 16:16 by sanjdas
                         BOOT = bootflash:old_image,1;
        Configuration register = 0x822
Peer Processor Information:
             Standby Location = slot 2
       Current Software state = STANDBY HOT
       Uptime in current state = 1 minute
                 Image Version = Cisco IOS Software, Catalyst 4500 L3 Switch Software
(cat4500-ENTSERVICES-M), Version 12.2(31)SGA, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Tue 05-Sep-06 16:16 by sanjdas
                         BOOT = bootflash:old_image,1;
        Configuration register = 0x822
```

ISSU プロセスを開始する前の ISSU ステートの確認

アクティブ スーパーバイザ エンジンとスタンバイ スーパーバイザ エンジンがアップおよび ISSU Init ステートで、ブート変数が設定されており、有効なファイルが指定されていることを確認します。

次に、プロセスが開始する前に ISSU ステートを表示する例を示します。

```
Switch# show issu state detail
                          Slot = 1
                      RP State = Active
                    ISSU State = Init
                 Boot Variable = bootflash:old_image,1;
                Operating Mode = Stateful Switchover
               Primary Version = N/A
             Secondary Version = N/A
               Current Version = bootflash:old_image
                          Slot = 2
                      RP State = Standby
                    ISSU State = Init
                 Boot Variable = bootflash:old_image,1;
                Operating Mode = Stateful Switchover
               Primary Version = N/A
             Secondary Version = N/A
               Current Version = bootflash:old_image
```

新しい Cisco IOS ソフトウェア バージョンが両方のスーパーバイザ エンジンに存在する必要があります。次に、新しいバージョンが存在することを確認するために、それぞれのスーパーバイザ エンジンのディレクトリ情報を表示する例を示します。

```
Switch# dir bootflash:
Directory of bootflash:/
                        Sep 6 2006 09:32:33 +00:00 old_image
              13636500
      -rwx
                        Sep 6 2006 09:34:07 +00:00 new_image
              13636500
      -rwx
61341696 bytes total (1111388 bytes free)
Switch# dir slavebootflash:
Directory of slavebootflash:/
              13636500 Sep 6 2006 09:40:10 +00:00 old_image
              13636500
                        Sep 6 2006 09:42:13 +00:00 new_image
   5 -rwx
61341696 bytes total (1116224 bytes free)
```

スタンバイ スーパーバイザ エンジンへの新しい Cisco IOS ソフトウェアのロード

ここでは、ISSU を使用して、スタンバイ スーパーバイザ エンジンに新しい Cisco IOS ソフトウェア バージョンをロードする方法について説明します。

前提条件

- 新しい Cisco IOS ソフトウェア イメージのバージョンがアクティブ スーパーバイザ エンジン とスタンバイ スーパーバイザ エンジンの両方にすでに存在していることを確認します。また、 適切なブート パラメータ (BOOT ストリングおよびコンフィギュレーション レジスタ) がスタンバイ スーパーバイザ エンジンに設定されていることを確認します。
- (任意)追加のテストおよびコマンドを実行して、あとで比較するために必要なピアおよびインターフェイスの現在のステートを判別します。

• システム(アクティブ スーパーバイザ エンジンとスタンバイ スーパーバイザ エンジンの両方) が SSO 冗長モードを開始していることを確認します。システムが SSO モードではなく、RPR モードである場合、ISSU CLI コマンドを使用してシステムをアップグレードすることはできますが、アップグレード中にシステムが大量のパケットを損失します。

スーパーバイザ エンジンに SSO モードを設定する方法の詳細については、『*Stateful Switchover*』を参照してください。

• ISSU が機能するためには、アクティブ スーパーバイザ エンジンとスタンバイ スーパーバイザ エンジンのイメージ名が一致する必要があります。

アクティブ スーパーバイザ エンジンで次の手順を実行します。

手順の要約

- 1. enable
- 2. issu loadversion active-slot active-image-new standby-slot standby-image-new [forced]
- 3. show issu state [detail]
- 4. show redundancy[states]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Switch> enable	特権 EXEC モードをイネーブルにします。
		プロンプトが表示されたら、パスワードを入力します。
ステップ 2	Switch# issu loadversion active-slot active-image-new standby-slot standby-image-new [forced]	ISSU プロセスを開始します。また、新しい Cisco IOS ソフトウェア バージョンに互換性がないことが検知された場合には、自動ロールバックを無効にします(任意)
		issu loadversion コマンドを入力してからスタンバイ スーパーバイザ エンジンに Cisco IOS ソフトウェアがロードされて、スタンバイ スーパーバイザ エンジンが SSO モードに移行するまでには数秒かかります。これによって、スタンバイ スーパーバイザ エンジンに新しいイメージがリロードされます。
		forced オプションを使用すると、スタンバイ スーパーバイザ エンジンが新しいイメージで起動します。スタンバイスーパーバイザ エンジンにイメージがロードされたあと、イメージに互換性がないと、システムは強制的に RPR モードになります。それ以外の場合、システムは SSO モードを続行します。
ステップ 3	Switch# show issu state [detail]	ISSU プロセス中のスーパーバイザ エンジンのステートを表示します。ISSU プロセスのこの時点で、このコマンドを使用して、スタンバイ スーパーバイザ エンジンがロードされ、SSO モードを開始していることを確認します。
		issu loadversion コマンドを入力してからスタンバイ スーパーバイザ エンジンに Cisco IOS ソフトウェアがロードされて、スタンバイ スーパーバイザ エンジンが SSO モードに移行するまでには数秒かかります。show issu state コマンドを入力するタイミングが早すぎると、必要な情報が表示されない場合があります。
ステップ 4	Switch# show redundancy [states]	冗長ファシリティ ステート情報を表示します。

Switch> enable

次に、ISSU プロセスを開始し、スタンバイ スーパーバイザ エンジンを Standby Hot ステートで起動し、スタンバイ スーパーバイザ エンジン (スロット 2) に新しいイメージをロードする例を示します。

```
Switch# issu loadversion 1 bootflash:new_image 2 slavebootflash:new_image
Switch# show issu state detail
                          Slot = 1
                     RP State = Active
                    ISSU State = Load Version
                 Boot Variable = bootflash:old_image,12
                Operating Mode = Stateful Switchover
               Primary Version = bootflash:old_image
             Secondary Version = bootflash:new_image
               Current Version = bootflash:old_image
                          Slot = 2
                      RP State = Standby
                    ISSU State = Load Version
                 Boot Variable = bootflash:new_image,12;bootflash:old_image,12
                Operating Mode = Stateful Switchover
               Primary Version = bootflash:old_image
             Secondary Version = bootflash:new_image
               Current Version = bootflash:new_image
Switch# show redundancy states
      my state = 13 - ACTIVE
     peer state = 8 -STANDBY HOT
          Mode = Duplex
          Unit = Primary
       Unit ID = 1
Redundancy Mode (Operational) = Stateful Switchover
Redundancy Mode (Configured) = Stateful Switchover
Redundancy State
                              = Stateful Switchover
Maintenance Mode = Disabled
   Manual Swact = enabled
 Communications = Up
  client count = 39
client_notification_TMR = 240000 milliseconds
         keep_alive TMR = 9000 milliseconds
       keep_alive count = 1
    keep\_alive threshold = 18
          RF debug mask = 0x0
```

次に、forced オプションによってシステムが RPR モードに移行する例を示します。

```
Switch> enable
Switch# issu loadversion 1 bootflash:new_image 2 slavebootflash:new_image forced
Switch# show issu state detail
                          Slot = 1
                      RP State = Active
                    ISSU State = Load Version
                 Boot Variable = bootflash:old_image, 12
                Operating Mode = RPR
               Primary Version = bootflash:old_image
             Secondary Version = bootflash:new_image
               Current Version = bootflash:old_image
                          Slot = 2
                      RP State = Standby
                    ISSU State = Load Version
                 Boot Variable = bootflash:new_image, 12; bootflash:old_image, 12
                Operating Mode = RPR
               Primary Version = bootflash:old_image
             Secondary Version = bootflash:new_image
               Current Version = bootflash:new_image
```

次に、冗長モードが RPR として表示される例を示します。

```
Switch# show redundancy states
   my state = 13 -ACTIVE
   peer state = 4 -STANDBY COLD
```

Mode = Duplex
Unit = Primary
Unit ID = 1

Redundancy Mode (Operational) = RPR
Redundancy Mode (Configured) = Stateful Switchover
Redundancy State = RPR
Maintenance Mode = Disabled
 Manual Swact = enabled
 Communications = Up

 client count = 39
 client_notification_TMR = 240000 milliseconds

keep_alive TMR = 9000 milliseconds
keep_alive count = 1
keep_alive threshold = 18
 RF debug mask = 0x0

スタンパイ スーパーバイザ エンジンへの切り替え

この作業では、新しい Cisco IOS ソフトウェア イメージを実行しているスタンバイ スーパーバイザ エンジンへのスイッチオーバー方法について説明します。

アクティブ スーパーバイザ エンジンで次の手順を実行します。

手順の要約

- 1. enable
- **2. issu runversion** *standby-slot* [*standby-image-new*]
- 3. show issu state [detail]
- 4. show redundancy[states]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Switch> enable	特権 EXEC モードをイネーブルにします。
		プロンプトが表示されたら、パスワードを入力します。
ステップ 2	Switch# issu runversion standby-slot [standby-image-new]	アクティブ スーパーバイザ エンジンからスタンバイ スーパーバイザ エンジンへのスイッチオーバーを強制し、アクティブだった(現在はスタンバイ)スーパーバイザ エンジンに古いイメージをリロードします。
		issu runversion コマンドを入力すると SSO のスイッチオーバーが 実行され、設定されている場合は NSF プロシージャが起動します。
ステップ 3	Switch# show issu state [detail]	ISSU プロセス中のスーパーバイザ エンジンのステートを表示します。ISSU プロセスのこの時点で、このコマンドを使用して、スロット 2 でスイッチオーバーが行われていることを確認します。
ステップ 4	Switch# show redundancy [states]	冗長ファシリティ ステート情報を表示します。

次に、スタンバイだったスーパーバイザ エンジン(スロット 2)へのスイッチオーバーを発生させ、アクティブだったスーパーバイザ エンジンをリセットしたうえで古いイメージをリロードしてスタンバイ スーパーバイザ エンジンにする例を示します。

Switch> enable

Switch# issu runversion 2 slavebootflash:new_image

This command will reload the Active unit. Proceed ? [confirm]

A switchover happens at this point. At the new active supervisor engine, do the following after old active supervisor engine comes up as standby.

Switch# show issu state detail

Slot = 2

RP State = Active

ISSU State = Run Version

Boot Variable = bootflash:new_image,12;bootflash:old_image,12

Operating Mode = Stateful Switchover
Primary Version = bootflash:new_image
Secondary Version = bootflash:old_image
Current Version = bootflash:new_image

Slot = 1

RP State = Standby

ISSU State = Run Version

Boot Variable = bootflash:old_image,12 Operating Mode = Stateful Switchover

Primary Version = bootflash:new_image Secondary Version = bootflash:old_image

Current Version = bootflash:old_image



新しくアクティブになったスーパーバイザ エンジンは現在新しいソフトウェア バージョンを実行し、スタンバイ スーパーバイザ エンジンは古いソフトウェア バージョンを実行し、STANDBY HOT ステートの状態です。

```
Switch# show redundancy states
      my state = 13 -ACTIVE
     peer state = 8 -STANDBY HOT
          Mode = Duplex
          Unit = Secondary
       Unit ID = 2
Redundancy Mode (Operational) = Stateful Switchover
Redundancy Mode (Configured) = Stateful Switchover
Redundancy State
                              = Stateful Switchover
Maintenance Mode = Disabled
   Manual Swact = enabled
  Communications = Up
  client count = 39
client_notification_TMR = 240000 milliseconds
         keep_alive TMR = 9000 milliseconds
        keep_alive count = 1
    keep_alive threshold = 18
          RF debug mask = 0x0
```

runversion が完了すると、新しくアクティブになったスーパーバイザ エンジンが新しいソフトウェア バージョンを実行し、アクティブだったスーパーバイザ エンジンがスタンバイ スーパーバイザ エンジンになります。スタンバイがリセットされたうえでリロードされますが、以前のソフトウェア バージョンのまま、STANDBY HOT ステータスでオンラインに戻ります。次に、これらの状態を確認する例を示します。

```
Switch# show redundancy
Redundant System Information:
      Available system uptime = 23 minutes
Switchovers system experienced = 1
              Standby failures = 0
        Last switchover reason = user forced
                Hardware Mode = Duplex
    Configured Redundancy Mode = Stateful Switchover
     Operating Redundancy Mode = Stateful Switchover
             Maintenance Mode = Disabled
               Communications = Up
Current Processor Information:
              Active Location = slot 2
        Current Software state = ACTIVE
       Uptime in current state = 11 minutes
                Image Version = Cisco IOS Software, Catalyst 4500 L3 Switch Software
(cat4500-ENTSERVICES-M), Version 12.2(31)SGA, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Tue 05-Sep-06 16:16 by sanjdas
                          BOOT = bootflash:new_image,12;bootflash:old_image,12
        Configuration register = 0x822
Peer Processor Information :
             Standby Location = slot 1
       Current Software state = STANDBY HOT
       Uptime in current state = 4 minutes
                Image Version = Cisco IOS Software, Catalyst 4500 L3 Switch Software
(cat4500-ENTSERVICES-M), Version 12.2(31)SGA, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Tue 05-Sep-06 16:16 by sanjdas
                          BOOT = bootflash:old_image,12
        Configuration register = 0x822
```

ISSU ロールバック タイマーの停止(任意)

ここでは、ロールバック タイマーを停止する方法について説明します。これは、任意で行う操作です。

ロールバック タイマーが「タイムアウト」する前に次の手順を実行しなかった場合、システムが自動的に ISSU プロセスを中断し、元の Cisco IOS ソフトウェア バージョンに戻ります。デフォルトのロールバック タイマーは 45 分です。

行う必要がある操作は、次のように判断します。

- スイッチを長時間この状態で維持する場合は、ロールバックタイマーを停止する必要があります(その後、確認して、直接 commitversion コマンドを実行します)。
- 45 分間のロールバック タイマー ウィンドウ内に次のステップ ([acceptversion] を実行)に進む場合は、ロールバック タイマーを停止する必要はありません。



issu runversion コマンドのあと、任意で issu acceptversion コマンドを実行することができます。

手順の要約

- 1. enable
- **2. issu acceptversion** *active-slot-number* [active-slot-number]
- 3. show issu state [detail]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Switch> enable	特権 EXEC モードをイネーブルにします。
		プロンプトが表示されたら、パスワードを入力します。
ステップ 2	Switch# issu acceptversion active-slot [active-image-new]	ロールバック タイマーを中止し、新しい Cisco IOS ISSU プロセスが ISSU プロセス中に自動的に中断されていないようにします。
		ロールバック タイマーによって指定された時間内に issu acceptversion コマンドを入力して、スーパーバイザ エンジンが外部への接続を確立したことを承認します。 そうしないと、ISSU プロセスが終了し、システムはスタンバイ スーパーバイザ エンジンに切り替えて、以前の Cisco IOS ソフトウェア バージョンに戻ります。
ステップ 3	Switch# show issu rollback-timer	自動ロールバックが行われるまでの時間を表示します。

次に、停止する前のタイマーを表示する例を示します。次の例では、[Automatic Rollback Time] 情報に、自動ロールバックが行われるまでの時間が示されています。

Switch> enable

Switch# show issu rollback-timer

Rollback Process State = In progress Configured Rollback Time = 45:00 Automatic Rollback Time = 38:30

Switch# issu acceptversion 2 bootflash:new_image

% Rollback timer stopped. Please issue the commitversion command.

Switch# show issu rollback-timer

Rollback Process State = Not in progress Configured Rollback Time = 45:00

新しくスタンバイになったスーパーバイザ エンジンへの新しい Cisco IOS ソフトウェアのロード

ここでは、新しくスタンバイになったスーパーバイザ エンジンに新しい Cisco IOS ソフトウェア バージョンをロードする方法について説明します。

アクティブ スーパーバイザ エンジンで次の手順を実行します。

手順の要約

- 1. enable
- **2. issu commitversion** *standby-slot* [*standby-image-new*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Switch> enable	特権 EXEC モードをイネーブルにします。
		• プロンプトが表示されたら、パスワードを入力します。
ステップ 2	Switch# issu commitversion standby-slot-number [standby-image-new]	新しい Cisco IOS ソフトウェア イメージがスタンバイ スーパーバイザ エンジンにロードされるようにします。
ステップ 3	Switch# show redundancy [states]	冗長ファシリティ ステート情報を表示します。
ステップ 4	Switch# show issu state [detail]	ISSU プロセス中のスーパーバイザ エンジンのステートを表示します。ISSU プロセスのこの時点で、このコマンドを使用して、スロット 2 でスイッチオーバーが行われていることを確認します。

次に、現在のスタンバイ スーパーバイザ エンジン(スロット 1)をリセットして、新しい Cisco IOS ソフトウェア バージョンをリロードする例を示します。commitversion コマンドを発行したあと、 スタンバイ スーパーバイザ エンジンが Standby Hot ステートで起動します。

```
Switch> enable
Switch# issu committeesion 1 slavebootflash:new image
Wait till standby supervisor is reloaded with the new image. Then apply the following:
Switch# show redundancy states
00:17:12: %RF-5-RF_TERMINAL_STATE: Terminal state reached for (SSO)
      my state = 13 -ACTIVE
     peer state = 8 -STANDBY HOT
          Mode = Duplex
          Unit = Secondary
        Unit ID = 2
Redundancy Mode (Operational) = Stateful Switchover
Redundancy Mode (Configured) = Stateful Switchover
Redundancy State
                              = Stateful Switchover
Maintenance Mode = Disabled
   Manual Swact = enabled
 Communications = Up
  client count = 39
client_notification_TMR = 240000 milliseconds
         keep_alive TMR = 9000 milliseconds
       keep_alive count = 0
    keep_alive threshold = 18
```

RF debug mask = 0x0

```
Switch# show redundancy
Redundant System Information:
      Available system uptime = 41 minutes
Switchovers system experienced = 1
              Standby failures = 1
       Last switchover reason = user forced
                Hardware Mode = Duplex
    Configured Redundancy Mode = Stateful Switchover
     Operating Redundancy Mode = Stateful Switchover
             Maintenance Mode = Disabled
               Communications = Up
Current Processor Information :
              Active Location = slot 2
       Current Software state = ACTIVE
       Uptime in current state = 29 minutes
                Image Version = Cisco IOS Software, Catalyst 4500 L3 Switch Software
(cat4500-ENTSERVICES-M), Version 12.2(31)SGA, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Tue 05-Sep-06 16:16 by sanjdas
                          BOOT = bootflash:new_image,12;bootflash:old_image,1;
        Configuration register = 0x822
Peer Processor Information :
             Standby Location = slot 1
        Current Software state = STANDBY HOT
       Uptime in current state = 12 minutes
                Image Version = Cisco IOS Software, Catalyst 4500 L3 Switch Software
(cat4500-ENTSERVICES-M), Version 12.2(31)SGA, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Tue 05-Sep-06 16:16 by sanjdas
                          BOOT = bootflash:new_image,12;bootflash:old_image,1;
        Configuration register = 0x822
Switch# show issu state detail
                          Slot = 2
                     RP State = Active
                    ISSU State = Init
                 Boot Variable = bootflash:new_image,12;bootflash:old_image,1;
                Operating Mode = Stateful Switchover
               Primary Version = N/A
             Secondary Version = N/A
               Current Version = bootflash:new_image
                          Slot = 1
                     RP State = Standby
                    ISSU State = Init
                 Boot Variable = bootflash:new_image,12;bootflash:old_image,1;
                Operating Mode = Stateful Switchover
               Primary Version = N/A
             Secondary Version = N/A
               Current Version = bootflash:new_image
```

ISSU プロセスが完了しました。これ以降、Cisco IOS ソフトウェア バージョンのアップグレードまたはダウングレードを行うには、新しい ISSU プロセスの起動が必要になります。

ISSU プロセス中のソフトウェア アップグレードの中断

issu abortversion コマンドを発行して、どの段階においても手動で ISSU プロセスを中断できます (issu commitversion コマンドを発行する前)。また、ソフトウェアによる障害の検知によっても、ISSU プロセスは自動的に中断します。



(注)

スタンバイ スーパーバイザ エンジンが Standby Hot ステートに移行する前に、issu abortversion コマンドを発行すると、トラフィックが中断する可能性があります。

issu loadversion コマンドを発行したあとにプロセスを手動で中断した場合、スタンバイ スーパーバイザ エンジンがリセットされ、元のソフトウェアがリロードされます。

issu runversion または issu acceptversion コマンドのいずれかを入力したあとにプロセスが中断された場合は、元のソフトウェア バージョンを引き続き実行している新しいスタンバイ スーパーバイザ エンジンで 2 回めのスイッチオーバーが実行されます。新しいソフトウェアを実行していたスーパーバイザ エンジンがリセットされ、元のソフトウェア バージョンがリロードされます。



(注)

アクティブなスーパーバイザのコマンドで abortversion コマンドを発行する \hat{n} に、スタンバイ スーパーバイザ エンジンが完全に起動されていることを確認します。

ここでは、issu commitversion コマンドを使用して ISSU プロセスを完了する前に、ISSU プロセスを中断する方法について説明します。

アクティブ スーパーバイザ エンジンで次の作業を実行します。

手順の要約

- 1. enable
- **2. issu abortversion** *active-slot* [active-image-new]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Switch> enable	特権 EXEC モードをイネーブルにします。
		• プロンプトが表示されたら、パスワードを入力します。
ステップ 2		進行中の ISSU アップグレードまたはダウングレード プロ
		セスをキャンセルし、ルータのステートを、プロセスが開 始する前のステートに戻します。

次に、スロット番号 2 (現在アクティブなスーパーバイザ エンジンのスロット) の ISSU プロセスを中断する例を示します。

Switch> enable
Switch# issu abortversion 2

アップグレード問題を回避するためのロールバック タイマーの設定

Cisco IOS ソフトウェアは、新しくアクティブになったスーパーバイザ エンジンとスタンバイ スーパーバイザ エンジンとの通信がアップグレードによって、切断された状態になるのを回避するために、ISSU ロールバック タイマーを維持します。

新しいソフトウェアがコミットされていない場合、または Run Version モード中にスイッチへの接続が失われた場合にユーザが待つ必要がないように、ロールバック タイマーを 45 分(デフォルト)以内に設定することもできます。新しいイメージをコミットする前に新しい Cisco IOS ソフトウェアの動作を確認するための十分な時間が必要な場合は、ロールバック タイマーを 45 分以上に設定することもできます。



(注)

有効なタイマー値の範囲は、 $0 \sim 7200$ 秒 (2 時間) です。0 秒の値を設定すると、ロールバック タイマーはディセーブルになります。

ISSU プロセスが正常に行われていることに満足し、現在の状態を保つ場合は、issu acceptversion コマンドを実行することにより、承諾したことを示す必要があります。これにより、ロールバック タイマーが停止します。そのため、issu acceptversion コマンドを入力することは、ISSU プロセスを進めるのに極めて重要です。

この段階で issu commitversion コマンドを実行することは、issu acceptversion コマンドと issu commitversion コマンドの両方を入力することと同じです。現在の状態で一定期間実行しない予定で、新しいソフトウェア バージョンに満足している場合は、issu commitversion コマンドを使用します。



ロールバック タイマーは、ISSU の Init ステートでのみ設定できます。

ここでは、ロールバック タイマーを設定する方法について説明します。

手順の要約

- 1. enable
- 2. configure terminal
- 3. issu set rollback-timer hh::mm::ss
- 4. show issu rollback-timer

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Switch> enable	特権 EXEC モードをイネーブルにします。
		プロンプトが表示されたら、パスワードを入力します。
ステップ 2	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	Switch(config)# issu set rollback-timer hh::mm::ss	ロールバック タイマー値を設定します。
ステップ 4	Switch(config)# exit	特権 EXEC モードに戻ります。
ステップ 5	Switch# show issu rollback-timer	ISSU ロールバック タイマーの現在の設定を表示します。

次に、ロールバック タイマーを 3600 秒に設定する例を示します。

次の例で示すように、ロールバック タイマーを LV ステートで設定することはできません。

```
Switch# show issu state detail
                          Slot = 1
                      RP State = Active
                    ISSU State = Load Version
                 Boot Variable = bootflash:old_image,12
                Operating Mode = RPR
               Primary Version = bootflash:old_image
             Secondary Version = bootflash:new_image
               Current Version = bootflash:old_image
                          Slot = 2
                      RP State = Standby
                    ISSU State = Load Version
                 Boot Variable = bootflash:new_image, 12; bootflash:old_image, 12
                Operating Mode = RPR
               Primary Version = bootflash:old_image
             Secondary Version = bootflash:new_image
               Current Version = bootflash:new image
Switch# show issu rollback-timer
        Rollback Process State = Not in progress
      Configured Rollback Time = 60:00
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config) # issu set rollback-timer 20
```

ISSU 互換性マトリクス情報の表示

ISSU 互換性マトリクスには、該当するバージョンにかかわる他のソフトウェア イメージに関する情報が含まれます。この互換性マトリクスには、2 つのソフトウェア バージョン(1 つは、アクティブ スーパーバイザ エンジンで実行されるソフトウェア バージョンで、もう一方はスタンバイ スーパーバイザ エンジンで実行されるソフトウェア バージョン)の互換性が示され、これによって、システムは実現可能な最も高度な動作モードを判別できます。この情報は、ユーザが ISSU を使用するかどうかを判断する場合にも役立ちます。

ここでは、ISSU 互換性マトリクスに関する情報を表示する方法を示します。

% ISSU state should be [init] to set the rollback timer

手順の要約

- 1. enable
- 2. show issu comp-matrix {negotiated | stored | xml}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Switch> enable	特権 EXEC モードをイネーブルにします。
		• プロンプトが表示されたら、パスワードを入力します。
ステップ 2	Switch# show issu comp-matrix {negotiated stored xml}	ISSU 互換性マトリクスに関する情報を表示します。
	, 2001011 / 1001011 / 1001011	• negotiated ネゴシエートされた互換性マトリクス情報を表示します。
		• stored 保存された互換性マトリクス情報を表示します。
		• xml ネゴシエートされた互換性マトリクス情報を XML 形式で表示します。

次に、ネゴシエートされた互換性マトリクスに関する情報を表示する例を示します。

Switch> enable

 ${\tt Switch\#} \ \, \textbf{show issu comp-matrix negotiated}$

 $\label{eq:cardType: WS-C4507R(112), Uid: 2, Image Ver: 12.2(31)SGA} % \end{substitute} % \begin{substitute} \begin{substitute$

Image Name: cat4500-ENTSERVICES-M

2 1 262151 3 1 COMPATIBLE 3 1 262160 5 1 COMPATIBLE 4 1 262163 9 1 COMPATIBLE 5 1 262186 25 1 COMPATIBLE 7 1 262156 10 1 COMPATIBLE 8 1 262148 7 1 COMPATIBLE 9 1 262155 1 1 COMPATIBLE 10 1 262158 2 1 COMPATIBLE 11 1 262172 6 1 COMPATIBLE 11 1 262172 6 1 COMPATIBLE 110 113 262159 14 1 COMPATIBLE 1200 1 262167 24 1 COMPATIBLE 1200 1 262167 24 1 COMPATIBLE 1200 1 262185 23 1 COMPATIBLE 12003 1 262185 23 1 COMPATIBLE 12004 1 262175 16 1 COMPATIBLE 12008 1 262147 26 1 COMPATIBLE 12008 1 262147 26 1 COMPATIBLE 12008 1 262147 26 1 COMPATIBLE 12010 1 262171 32 1 COMPATIBLE 12010 1 262171 32 1 COMPATIBLE 12011 1 262170 41 1 COMPATIBLE 12022 1 COMPATIBLE 12021 1 262180 31 1 COMPATIBLE 12022 1 262152 42 1 COMPATIBLE 12023 1 UNAVAILABLE 12024 1 UNAVAILABLE 12025 1 UNAVAILABLE 12026 1 UNAVAILABLE 12027 1 UNAVAILABLE 12028 1 UNAVAILABLE 12029 1 COMPATIBLE 12029 1 COMPATIBLE 12020 1 UNAVAILABLE 12021 1 COMPATIBLE 12022 1 COMPATIBLE 12023 1 UNAVAILABLE 12024 1 UNAVAILABLE 12025 1 UNAVAILABLE 12026 1 UNAVAILABLE 12027 1 UNAVAILABLE 12028 1 UNAVAILABLE 12029 1 COMPATIBLE 12030 1 COMPATIBLE 1204 1 COMPATIBLE 1205 1 UNAVAILABLE 1206 1 COMPATIBLE 1207 1 COMPATIBLE	Cid	Eid	Sid	pSid	pUid	Compatibility
3 1 262160 5 1 COMPATIBLE 4 1 262163 9 1 COMPATIBLE 5 1 262156 10 1 COMPATIBLE 7 1 262156 10 1 COMPATIBLE 8 1 262155 1 1 COMPATIBLE 9 1 262158 2 1 COMPATIBLE 10 1 262158 2 1 COMPATIBLE 10 1 262166 13 1 COMPATIBLE 10 1 262166 13 1 COMPATIBLE 200 1 262167 24 1 COMPATIBLE 200 1 262167 24 1 COMPATIBLE 2002 1 - - UNAVAILABLE 2003 1 262185 23 1 COMPATIBLE 2004 1 262173 32 1 COMPATIBLE<			262151	2	1	
4 1 262163 9 1 COMPATIBLE 5 1 262186 25 1 COMPATIBLE 7 1 262156 10 1 COMPATIBLE 8 1 262148 7 1 COMPATIBLE 9 1 262158 2 1 COMPATIBLE 10 1 262158 2 1 COMPATIBLE 11 1 262166 13 1 COMPATIBLE 100 1 262166 13 1 COMPATIBLE 200 1 262167 24 1 COMPATIBLE 2000 1 262167 24 1 COMPATIBLE 2002 1 - - UNAVAILABLE 2004 1 262185 23 1 COMPATIBLE 2008 1 262168 27 1 COMPATIBLE 2008 1 262168 27 1 COMPA						
5 1 262186 25 1 COMPATIBLE 7 1 262156 10 1 COMPATIBLE 8 1 262148 7 1 COMPATIBLE 9 1 262155 1 1 COMPATIBLE 10 1 262158 2 1 COMPATIBLE 11 1 262166 13 1 COMPATIBLE 100 1 262166 13 1 COMPATIBLE 200 1 262167 24 1 COMPATIBLE 2002 1 - - UNAVAILABLE 2003 1 262185 23 1 COMPATIBLE 2004 1 262185 23 1 COMPATIBLE 2008 1 262187 26 1 COMPATIBLE 2008 1 262168 27 1 COMPATIBLE 2010 1 262173 2 1 CO		_		-	-	
7 1 262156 10 1 COMPATIBLE 8 1 262148 7 1 COMPATIBLE 9 1 262155 1 1 COMPATIBLE 10 1 262158 2 1 COMPATIBLE 11 1 262166 13 1 COMPATIBLE 100 1 262167 24 1 COMPATIBLE 200 1 262167 24 1 COMPATIBLE 2002 1 - - UNAVAILABLE 2003 1 262185 23 1 COMPATIBLE 2004 1 262185 23 1 COMPATIBLE 2008 1 262175 16 1 COMPATIBLE 2008 1 262168 27 1 COMPATIBLE 2010 1 262168 27 1 COMPATIBLE 2012 1 262168 31 1 <t< td=""><td></td><td>_</td><td></td><td>-</td><td>-</td><td></td></t<>		_		-	-	
8 1 262148 7 1 COMPATIBLE 9 1 262155 1 1 COMPATIBLE 10 1 262158 2 1 COMPATIBLE 11 1 262172 6 1 COMPATIBLE 110 1 262166 13 1 COMPATIBLE 110 113 262159 14 1 COMPATIBLE 200 1 262167 24 1 COMPATIBLE 2002 1 UNAVAILABLE 2003 1 262185 23 1 COMPATIBLE 2004 1 262175 16 1 COMPATIBLE 2008 1 262147 26 1 COMPATIBLE 2008 1 262147 26 1 COMPATIBLE 2010 1 262171 32 1 COMPATIBLE 2010 1 262171 32 1 COMPATIBLE 2011 1 262170 41 1 COMPATIBLE 2021 1 262180 31 1 COMPATIBLE 2022 1 262152 42 1 COMPATIBLE 2023 1 UNAVAILABLE 2024 1 UNAVAILABLE 2025 1 COMPATIBLE 2026 1 UNAVAILABLE 2027 1 UNAVAILABLE 2028 1 UNAVAILABLE 2028 1 UNAVAILABLE 2029 1 262154 29 1 COMPATIBLE 2020 1 COMPATIBLE 2021 1 COMPATIBLE 2022 1 COMPATIBLE 2024 1 UNAVAILABLE 2025 1 UNAVAILABLE 2026 1 UNAVAILABLE 2027 1 UNAVAILABLE 2028 1 UNAVAILABLE 2029 1 262153 12 1 COMPATIBLE 2058 1 262154 29 1 COMPATIBLE 2059 1 262179 30 1 COMPATIBLE 2059 1 262179 30 1 COMPATIBLE 2068 1 196638 40 1 COMPATIBLE 2068 1 196638 40 1 COMPATIBLE 2070 1 262145 21 1 COMPATIBLE 2071 1 262161 28 1 COMPATIBLE 2072 1 262162 28 1 COMPATIBLE 2073 1 262167 33 1 COMPATIBLE 2074 1 262165 35 1 COMPATIBLE 2077 1 262165 35 1 COMPATIBLE 2078 1 196637 34 1 COMPATIBLE 2078 1 196637 34 1 COMPATIBLE 2079 1 262176 36 1 COMPATIBLE					-	
9 1 262155 1 1 COMPATIBLE 10 1 262158 2 1 COMPATIBLE 11 1 262172 6 1 COMPATIBLE 110 1 262166 13 1 COMPATIBLE 110 113 262159 14 1 COMPATIBLE 200 1 262167 24 1 COMPATIBLE 2002 1 UNAVAILABLE 2003 1 262185 23 1 COMPATIBLE 2004 1 262175 16 1 COMPATIBLE 2008 1 262147 26 1 COMPATIBLE 2008 1 262168 27 1 COMPATIBLE 2010 1 262171 32 1 COMPATIBLE 2010 1 262170 41 1 COMPATIBLE 2021 1 262180 31 1 COMPATIBLE 2022 1 262152 42 1 COMPATIBLE 2023 1 UNAVAILABLE 2024 1 UNAVAILABLE 2025 1 UNAVAILABLE 2026 1 UNAVAILABLE 2027 1 UNAVAILABLE 2028 1 UNAVAILABLE 2029 1 262152 42 1 COMPATIBLE 2020 1 262169 8 1 COMPATIBLE 2054 1 262169 8 1 COMPATIBLE 2059 1 262151 29 1 COMPATIBLE 2059 1 262151 1 COMPATIBLE 2068 1 196638 40 1 COMPATIBLE 2070 1 262178 11 COMPATIBLE 2071 1 262178 11 COMPATIBLE 2071 1 262178 11 COMPATIBLE 2072 1 COMPATIBLE 2073 1 COMPATIBLE 2074 1 COMPATIBLE 2075 1 COMPATIBLE 2077 1 262163 12 1 COMPATIBLE 2077 1 262178 11 COMPATIBLE 2077 1 262162 28 1 COMPATIBLE 2077 1 262165 35 1 COMPATIBLE 2078 1 196637 34 1 COMPATIBLE 2079 1 262176 36 1 COMPATIBLE	•	_			-	
10 1 262158 2 1 COMPATIBLE 11 1 262172 6 1 COMPATIBLE 100 1 262166 13 1 COMPATIBLE 110 113 262159 14 1 COMPATIBLE 200 1 262167 24 1 COMPATIBLE 2002 1 UNAVAILABLE 2003 1 262185 23 1 COMPATIBLE 2004 1 262175 16 1 COMPATIBLE 2008 1 262147 26 1 COMPATIBLE 2008 1 262147 26 1 COMPATIBLE 2010 1 262171 32 1 COMPATIBLE 2010 1 262171 32 1 COMPATIBLE 2012 1 262180 31 1 COMPATIBLE 2012 1 262180 31 1 COMPATIBLE 2021 1 262170 41 1 COMPATIBLE 2022 1 262152 42 1 COMPATIBLE 2023 1 UNAVAILABLE 2024 1 UNAVAILABLE 2025 1 UNAVAILABLE 2026 1 UNAVAILABLE 2027 1 UNAVAILABLE 2028 1 UNAVAILABLE 2028 1 UNAVAILABLE 2029 1 262153 12 1 COMPATIBLE 2059 1 262179 30 1 COMPATIBLE 2068 1 196638 40 1 COMPATIBLE 2070 1 262153 12 1 COMPATIBLE 2071 1 262165 35 1 COMPATIBLE 2071 1 262165 35 1 COMPATIBLE 2072 1 262162 28 1 COMPATIBLE 2073 1 262177 33 1 COMPATIBLE 2074 1 262165 35 1 COMPATIBLE 2075 1 COMPATIBLE 2077 1 262165 35 1 COMPATIBLE 2077 1 262165 35 1 COMPATIBLE 2078 1 196637 34 1 COMPATIBLE 2078 1 196637 34 1 COMPATIBLE 2079 1 262176 36 1 COMPATIBLE						
11 1 262172 6 1 COMPATIBLE 100 1 262166 13 1 COMPATIBLE 110 113 262159 14 1 COMPATIBLE 200 1 262167 24 1 COMPATIBLE 2002 1 UNAVAILABLE 2003 1 262185 23 1 COMPATIBLE 2004 1 262175 16 1 COMPATIBLE 2008 1 262147 26 1 COMPATIBLE 2010 1 262147 26 1 COMPATIBLE 2010 1 262168 27 1 COMPATIBLE 2010 1 262171 32 1 COMPATIBLE 2011 1 262180 31 1 COMPATIBLE 2012 1 262180 31 1 COMPATIBLE 2021 1 262170 41 1 COMPATIBLE 2022 1 262152 42 1 COMPATIBLE 2023 1 UNAVAILABLE 2024 1 UNAVAILABLE 2025 1 UNAVAILABLE 2026 1 UNAVAILABLE 2027 1 UNAVAILABLE 2028 1 UNAVAILABLE 2029 1 262154 29 1 COMPATIBLE 2059 1 262179 30 1 COMPATIBLE 2059 1 262179 30 1 COMPATIBLE 2068 1 196638 40 1 COMPATIBLE 2070 1 262145 21 1 COMPATIBLE 2070 1 262178 11 1 COMPATIBLE 2071 1 262178 11 1 COMPATIBLE 2072 1 262162 28 1 COMPATIBLE 2073 1 262177 33 1 COMPATIBLE 2074 1 262167 35 1 COMPATIBLE 2075 1 262167 35 1 COMPATIBLE 2077 1 262165 35 1 COMPATIBLE 2077 1 262165 35 1 COMPATIBLE 2078 1 196637 34 1 COMPATIBLE 2079 1 262176 36 1 COMPATIBLE						
100					-	
110						COMPATIBLE
200 1 262167 24 1 COMPATIBLE 2002 1 - - - UNAVAILABLE 2003 1 262185 23 1 COMPATIBLE 2004 1 262175 16 1 COMPATIBLE 2008 1 262168 27 1 COMPATIBLE 2008 1 262168 27 1 COMPATIBLE 2010 1 262171 32 1 COMPATIBLE 2012 1 262180 31 1 COMPATIBLE 2012 1 262170 41 1 COMPATIBLE 2021 1 262152 42 1 COMPATIBLE 2023 1 - - UNAVAILABLE 2024 1 - - UNAVAILABLE 2025 1 - - UNAVAILABLE 2026 1 - - UNAVAILABLE 2027					-	COMPATIBLE
2002 1 - - UNAVAILABLE 2003 1 262185 23 1 COMPATIBLE 2004 1 262175 16 1 COMPATIBLE 2008 1 262168 27 1 COMPATIBLE 2008 1 262168 27 1 COMPATIBLE 2010 1 262171 32 1 COMPATIBLE 2012 1 262180 31 1 COMPATIBLE 2021 1 262170 41 1 COMPATIBLE 2022 1 262152 42 1 COMPATIBLE 2023 1 - - UNAVAILABLE 2024 1 - - UNAVAILABLE 2025 1 - - UNAVAILABLE 2026 1 - - UNAVAILABLE 2027 1 - - UNAVAILABLE 2054 1 262169	110	113		14	1	COMPATIBLE
2003 1 262185 23 1 COMPATIBLE 2004 1 262175 16 1 COMPATIBLE 2008 1 262147 26 1 COMPATIBLE 2008 1 262168 27 1 COMPATIBLE 2010 1 262171 32 1 COMPATIBLE 2012 1 262180 31 1 COMPATIBLE 2021 1 262170 41 1 COMPATIBLE 2021 1 262152 42 1 COMPATIBLE 2022 1 262152 42 1 COMPATIBLE 2023 1 - - UNAVAILABLE 2024 1 - - UNAVAILABLE 2025 1 - - - UNAVAILABLE 2026 1 - - - UNAVAILABLE 2027 1 - - - UNAVAILABLE 2054 1 262169 8 1 COMPATIBLE	200	1	262167	24	1	COMPATIBLE
2004 1 262175 16 1 COMPATIBLE 2008 1 262147 26 1 COMPATIBLE 2008 1 262168 27 1 COMPATIBLE 2010 1 262171 32 1 COMPATIBLE 2012 1 262180 31 1 COMPATIBLE 2021 1 262170 41 1 COMPATIBLE 2022 1 262152 42 1 COMPATIBLE 2023 1 - - UNAVAILABLE 2024 1 - - UNAVAILABLE 2025 1 - - UNAVAILABLE 2026 1 - - UNAVAILABLE 2027 1 - - UNAVAILABLE 2028 1 - - UNAVAILABLE 2054 1 262169 8 1 COMPATIBLE 2058 1 262154 29 1 COMPATIBLE 2067 1 262153 12 </td <td>2002</td> <td>1</td> <td>-</td> <td>-</td> <td>-</td> <td>UNAVAILABLE</td>	2002	1	-	-	-	UNAVAILABLE
2008 1 262147 26 1 COMPATIBLE 2008 1 262168 27 1 COMPATIBLE 2010 1 262171 32 1 COMPATIBLE 2012 1 262180 31 1 COMPATIBLE 2021 1 262170 41 1 COMPATIBLE 2022 1 262152 42 1 COMPATIBLE 2023 1 - - UNAVAILABLE 2024 1 - - UNAVAILABLE 2025 1 - - UNAVAILABLE 2026 1 - - UNAVAILABLE 2027 1 - - UNAVAILABLE 2028 1 - - UNAVAILABLE 2054 1 262169 8 1 COMPATIBLE 2058 1 262154 29 1 COMPATIBLE 2059 1 262179 30 1 COMPATIBLE 2068 1 196638 40 </td <td>2003</td> <td>1</td> <td>262185</td> <td>23</td> <td>1</td> <td>COMPATIBLE</td>	2003	1	262185	23	1	COMPATIBLE
2008 1 262168 27 1 COMPATIBLE 2010 1 262171 32 1 COMPATIBLE 2012 1 262180 31 1 COMPATIBLE 2021 1 262170 41 1 COMPATIBLE 2022 1 262152 42 1 COMPATIBLE 2023 1 - - UNAVAILABLE 2024 1 - - UNAVAILABLE 2025 1 - - UNAVAILABLE 2026 1 - - - UNAVAILABLE 2027 1 - - - UNAVAILABLE 2028 1 - - - UNAVAILABLE 2054 1 262169 8 1 COMPATIBLE 2058 1 262154 29 1 COMPATIBLE 2059 1 262179 30 1 COMPATIBLE 2067 1 262153 12 1 COMPATIBLE 2070	2004	1	262175	16	1	COMPATIBLE
2010	2008	1	262147	26	1	COMPATIBLE
2012 1 262180 31 1 COMPATIBLE 2021 1 262170 41 1 COMPATIBLE 2022 1 262152 42 1 COMPATIBLE 2023 1 UNAVAILABLE 2024 1 UNAVAILABLE 2025 1 UNAVAILABLE 2026 1 UNAVAILABLE 2027 1 UNAVAILABLE 2028 1 UNAVAILABLE 2028 1 UNAVAILABLE 2054 1 262169 8 1 COMPATIBLE 2059 1 262179 30 1 COMPATIBLE 2059 1 262179 30 1 COMPATIBLE 2067 1 262153 12 1 COMPATIBLE 2068 1 196638 40 1 COMPATIBLE 2070 1 262145 21 1 COMPATIBLE 2071 1 262178 11 1 COMPATIBLE 2072 1 262162 28 1 COMPATIBLE 2073 1 262177 33 1 COMPATIBLE 2073 1 262177 33 1 COMPATIBLE 2077 1 262165 35 1 COMPATIBLE 2078 1 196637 34 1 COMPATIBLE 2078 1 196637 34 1 COMPATIBLE 2079 1 262176 36 1 COMPATIBLE	2008	1	262168	27	1	COMPATIBLE
2021 1 262170 41 1 COMPATIBLE 2022 1 262152 42 1 COMPATIBLE 2023 1 - - - UNAVAILABLE 2024 1 - - - UNAVAILABLE 2025 1 - - - UNAVAILABLE 2026 1 - - - UNAVAILABLE 2027 1 - - - UNAVAILABLE 2028 1 - - - UNAVAILABLE 2054 1 262169 8 1 COMPATIBLE 2054 1 262169 8 1 COMPATIBLE 2058 1 262154 29 1 COMPATIBLE 2059 1 262153 12 1 COMPATIBLE 2067 1 262153 12 1 COMPATIBLE 2068 1 196638 40 1 COMPATIBLE 2070 1 262145 21 1 COMPATI	2010	1	262171	32	1	COMPATIBLE
2022 1 262152 42 1 COMPATIBLE 2023 1 - - - UNAVAILABLE 2024 1 - - - UNAVAILABLE 2025 1 - - - UNAVAILABLE 2026 1 - - - UNAVAILABLE 2027 1 - - - UNAVAILABLE 2028 1 - - - UNAVAILABLE 2054 1 262169 8 1 COMPATIBLE 2058 1 262154 29 1 COMPATIBLE 2059 1 262154 29 1 COMPATIBLE 2067 1 262153 12 1 COMPATIBLE 2068 1 196638 40 1 COMPATIBLE 2070 1 262145 21 1 COMPATIBLE 2071 1 262162 28 1 COMPATIBLE 2073 1 262165 35 1 COMPAT	2012	1	262180	31	1	COMPATIBLE
2023 1 - - - UNAVAILABLE 2024 1 - - - UNAVAILABLE 2025 1 - - - UNAVAILABLE 2026 1 - - - UNAVAILABLE 2027 1 - - - UNAVAILABLE 2028 1 - - - UNAVAILABLE 2054 1 262169 8 1 COMPATIBLE 2058 1 262154 29 1 COMPATIBLE 2059 1 262154 29 1 COMPATIBLE 2067 1 262153 12 1 COMPATIBLE 2068 1 196638 40 1 COMPATIBLE 2070 1 262145 21 1 COMPATIBLE 2071 1 262178 11 1 COMPATIBLE 2072 1 262162 28 1 COMPATIBLE 2073 1 262165 35 1 COMPAT	2021	1	262170	41	1	COMPATIBLE
2024 1 - - UNAVAILABLE 2025 1 - - UNAVAILABLE 2026 1 - - UNAVAILABLE 2027 1 - - UNAVAILABLE 2028 1 - - UNAVAILABLE 2054 1 262169 8 1 COMPATIBLE 2058 1 262154 29 1 COMPATIBLE 2059 1 262179 30 1 COMPATIBLE 2067 1 262153 12 1 COMPATIBLE 2068 1 196638 40 1 COMPATIBLE 2070 1 262145 21 1 COMPATIBLE 2071 1 262178 11 1 COMPATIBLE 2072 1 262162 28 1 COMPATIBLE 2073 1 262165 35 1 COMPATIBLE 2078 1 196637 34 1 COMPATIBLE 2079 1 2621	2022	1	262152	42	1	COMPATIBLE
2025 1 - - UNAVAILABLE 2026 1 - - - UNAVAILABLE 2027 1 - - - UNAVAILABLE 2028 1 - - - UNAVAILABLE 2054 1 262169 8 1 COMPATIBLE 2058 1 262154 29 1 COMPATIBLE 2059 1 262179 30 1 COMPATIBLE 2067 1 262153 12 1 COMPATIBLE 2068 1 196638 40 1 COMPATIBLE 2070 1 262145 21 1 COMPATIBLE 2071 1 262178 11 1 COMPATIBLE 2072 1 262162 28 1 COMPATIBLE 2073 1 262165 35 1 COMPATIBLE 2078 1 196637 34 1 COMPATIBLE 2079 1 262176 36 1 COMPATIBLE <td>2023</td> <td>1</td> <td>-</td> <td>_</td> <td>_</td> <td>UNAVAILABLE</td>	2023	1	-	_	_	UNAVAILABLE
2026 1 - - - UNAVAILABLE 2027 1 - - - UNAVAILABLE 2028 1 - - - UNAVAILABLE 2054 1 262169 8 1 COMPATIBLE 2058 1 262154 29 1 COMPATIBLE 2059 1 262179 30 1 COMPATIBLE 2067 1 262153 12 1 COMPATIBLE 2068 1 196638 40 1 COMPATIBLE 2070 1 262145 21 1 COMPATIBLE 2071 1 262145 21 1 COMPATIBLE 2072 1 262162 28 1 COMPATIBLE 2073 1 262165 35 1 COMPATIBLE 2078 1 196637 34 1 COMPATIBLE 2079 1 262176 36 1 COMPATIBLE	2024	1	-	-	_	UNAVAILABLE
2027 1 - - - UNAVAILABLE 2028 1 - - - UNAVAILABLE 2054 1 262169 8 1 COMPATIBLE 2058 1 262154 29 1 COMPATIBLE 2059 1 262179 30 1 COMPATIBLE 2067 1 262153 12 1 COMPATIBLE 2068 1 196638 40 1 COMPATIBLE 2070 1 262145 21 1 COMPATIBLE 2071 1 262178 11 1 COMPATIBLE 2072 1 262162 28 1 COMPATIBLE 2073 1 262177 33 1 COMPATIBLE 2077 1 262165 35 1 COMPATIBLE 2078 1 196637 34 1 COMPATIBLE 2079 1 262176 36 1 COMPATIBLE	2025	1	-	_	_	UNAVAILABLE
2028 1 - - - UNAVAILABLE 2054 1 262169 8 1 COMPATIBLE 2058 1 262154 29 1 COMPATIBLE 2059 1 262179 30 1 COMPATIBLE 2067 1 262153 12 1 COMPATIBLE 2068 1 196638 40 1 COMPATIBLE 2070 1 262145 21 1 COMPATIBLE 2071 1 262178 11 1 COMPATIBLE 2072 1 262162 28 1 COMPATIBLE 2073 1 262177 33 1 COMPATIBLE 2077 1 262165 35 1 COMPATIBLE 2078 1 196637 34 1 COMPATIBLE 2079 1 262176 36 1 COMPATIBLE	2026	1	-	_	_	UNAVAILABLE
2054 1 262169 8 1 COMPATIBLE 2058 1 262154 29 1 COMPATIBLE 2059 1 262179 30 1 COMPATIBLE 2067 1 262153 12 1 COMPATIBLE 2068 1 196638 40 1 COMPATIBLE 2070 1 262145 21 1 COMPATIBLE 2071 1 262178 11 1 COMPATIBLE 2072 1 262162 28 1 COMPATIBLE 2073 1 262177 33 1 COMPATIBLE 2077 1 262165 35 1 COMPATIBLE 2078 1 196637 34 1 COMPATIBLE 2079 1 262176 36 1 COMPATIBLE	2027	1	-	_	_	UNAVAILABLE
2058 1 262154 29 1 COMPATIBLE 2059 1 262179 30 1 COMPATIBLE 2067 1 262153 12 1 COMPATIBLE 2068 1 196638 40 1 COMPATIBLE 2070 1 262145 21 1 COMPATIBLE 2071 1 262178 11 1 COMPATIBLE 2072 1 262162 28 1 COMPATIBLE 2073 1 262177 33 1 COMPATIBLE 2077 1 262165 35 1 COMPATIBLE 2078 1 196637 34 1 COMPATIBLE 2079 1 262176 36 1 COMPATIBLE	2028	1	-	_	_	UNAVAILABLE
2059 1 262179 30 1 COMPATIBLE 2067 1 262153 12 1 COMPATIBLE 2068 1 196638 40 1 COMPATIBLE 2070 1 262145 21 1 COMPATIBLE 2071 1 262178 11 1 COMPATIBLE 2072 1 262162 28 1 COMPATIBLE 2073 1 262177 33 1 COMPATIBLE 2077 1 262165 35 1 COMPATIBLE 2078 1 196637 34 1 COMPATIBLE 2079 1 262176 36 1 COMPATIBLE	2054	1	262169	8	1	COMPATIBLE
2067 1 262153 12 1 COMPATIBLE 2068 1 196638 40 1 COMPATIBLE 2070 1 262145 21 1 COMPATIBLE 2071 1 262178 11 1 COMPATIBLE 2072 1 262162 28 1 COMPATIBLE 2073 1 262177 33 1 COMPATIBLE 2077 1 262165 35 1 COMPATIBLE 2078 1 196637 34 1 COMPATIBLE 2079 1 262176 36 1 COMPATIBLE	2058	1	262154	29	1	COMPATIBLE
2068 1 196638 40 1 COMPATIBLE 2070 1 262145 21 1 COMPATIBLE 2071 1 262178 11 1 COMPATIBLE 2072 1 262162 28 1 COMPATIBLE 2073 1 262177 33 1 COMPATIBLE 2077 1 262165 35 1 COMPATIBLE 2078 1 196637 34 1 COMPATIBLE 2079 1 262176 36 1 COMPATIBLE	2059	1	262179	30	1	COMPATIBLE
2070 1 262145 21 1 COMPATIBLE 2071 1 262178 11 1 COMPATIBLE 2072 1 262162 28 1 COMPATIBLE 2073 1 262177 33 1 COMPATIBLE 2077 1 262165 35 1 COMPATIBLE 2078 1 196637 34 1 COMPATIBLE 2079 1 262176 36 1 COMPATIBLE	2067	1	262153	12	1	COMPATIBLE
2071 1 262178 11 1 COMPATIBLE 2072 1 262162 28 1 COMPATIBLE 2073 1 262177 33 1 COMPATIBLE 2077 1 262165 35 1 COMPATIBLE 2078 1 196637 34 1 COMPATIBLE 2079 1 262176 36 1 COMPATIBLE	2068	1	196638	40	1	COMPATIBLE
2072 1 262162 28 1 COMPATIBLE 2073 1 262177 33 1 COMPATIBLE 2077 1 262165 35 1 COMPATIBLE 2078 1 196637 34 1 COMPATIBLE 2079 1 262176 36 1 COMPATIBLE	2070	1	262145	21	1	COMPATIBLE
2072 1 262162 28 1 COMPATIBLE 2073 1 262177 33 1 COMPATIBLE 2077 1 262165 35 1 COMPATIBLE 2078 1 196637 34 1 COMPATIBLE 2079 1 262176 36 1 COMPATIBLE	2071	1	262178	11	1	COMPATIBLE
2077 1 262165 35 1 COMPATIBLE 2078 1 196637 34 1 COMPATIBLE 2079 1 262176 36 1 COMPATIBLE	2072	1	262162	28	1	COMPATIBLE
2077 1 262165 35 1 COMPATIBLE 2078 1 196637 34 1 COMPATIBLE 2079 1 262176 36 1 COMPATIBLE	2073	1	262177	33	1	COMPATIBLE
2078 1 196637 34 1 COMPATIBLE 2079 1 262176 36 1 COMPATIBLE						
2079 1 262176 36 1 COMPATIBLE						
	2081	1	262170	37	1	COMPATIBLE

2082 2083 2084 4001 4002 4003 4004 4005	1 1 101 201 301 401	262161 262184 262183 262181 262164 262182 262146 262149	20 38 17 18 19 22	1 1 1 1 1 1 1	COMPATI COMPATI COMPATI COMPATI COMPATI COMPATI	IBLE IBLE IBLE IBLE IBLE IBLE		
Cid	group Eid	summary: GrpId	Sid	pSid	pUid	Nego Res		
2	====== 1	1	262151	3	======= 1	======= Y	===	
3	1	1	262160		1	Y		
4	1	1	262163	9	1	Y		
5	1	1	262186	25	1	Y		
7	1	1	262156		1	Y		
8	1	1	262148		1	Y		
9	1	1	262155		1	Y		
10	1	1	262158		1	Y		
11 100	1 1	1 1	262172 262166		1	Y Y		
110	113	115	262159		1	Y		
200	1	1	262167		1	Y		
2002	1	2	-	-	_		not	negotiate
2003	1	1	262185	23	1	Y		3
2004	1	1	262175	16	1	Y		
2008	1	1	262147	26	1	Y		
2008	1	2	262168	27	1	Y		
2010	1	1	262171	32	1	Y		
2012	1	1	262180	31	1	Y		
2021	1	1	262170		1	Y		
2022	1	1	262152		1	Y		
2023	1	1	-	-	_			negotiate
2024	1	1	_	=	-			negotiate
2025 2026	1 1	1 1	_	_	_			negotiate negotiate
2027	1	1	_	_	_			negotiate
2028	1	1	_	_	_			negotiate
2054	1	1	262169		1	Y		9
2058	1	1	262154		1	Y		
2059	1	1	262179	30	1	Y		
2067	1	1	262153	12	1	Y		
2068	1	1	196638	40	1	Y		
2070	1	1	262145		1	Y		
2071	1	1	262178		1	Y		
2072	1	1	262162		1	Y		
2073 2077	1 1	1 1	262177		1 1	Y Y		
2077	1	1	262165 196637		1	Y		
2079	1	1	262176		1	Y		
2081	1	1	262150		1	Y		
2082	1	1	262161		1	Y		
2083	1	1	262184	20	1	Y		
2084	1	1	262183	38	1	Y		
4001	101	1	262181	17	1	Y		
4002	201	1	262164	18	1	Y		
4003	301	1	262182	19	1	Y		
4004	401	1	262146		1	Y		
4005	1	1	262149	4	1	Y		
List of Cid	Clie	nt Name			Non-Base			
2		======= Proto cl	ient	====== Base	=			
3	ISSU			Base				
4		CF clien	.t	Base				
5			RF client					
7		CONFIG S		Base				

```
8
         ISSU ifIndex sync
                                 Base
         ISSU IPC client
9
                                 Base
         ISSU IPC Server client Base
10
         ISSU Red Mode Client
11
100
         ISSU rfs client
                                 Base
110
        ISSU ifs client
                                 Base
200
        ISSU Event Manager clientBase
         CEF Push ISSU client Base
2002
2003
         ISSU XDR client
                                 Base
         ISSU SNMP client
2004
                                 Non-Base
2008
        ISSU Tableid Client
                                Base
        ARP HA
2010
                                 Base
2012
         ISSU HSRP Client
                                 Non-Base
2021
         XDR Int Priority ISSU cliBase
2022
        XDR Proc Priority ISSU clBase
2023
        FIB HWIDB ISSU client
2024
         FIB IDB ISSU client
                                 Base
2025
         FIB HW subblock ISSU clieBase
         FIB SW subblock ISSU clieBase
2026
2027
        Adjacency ISSU client Base
2028
         FIB IPV4 ISSU client Base
2054
         ISSU process client
                                 Base
2058
         ISIS ISSU RTR client
                                 Non-Base
         ISIS ISSU UPD client
                               Non-Base
2059
2067
        ISSU PM Client
                                 Base
2068
        ISSU PAGP_SWITCH Client Non-Base
2070
         ISSU Port Security clientNon-Base
         ISSU Switch VLAN client Non-Base
2071
2072
        ISSU dot1x client
                                 Non-Base
2073
         ISSU STP
                                 Non-Base
2077
         ISSU STP MSTP
                                 Non-Base
2078
         ISSU STP IEEE
                                 Non-Base
2079
         TSSH STP RSTP
                                 Non-Base
2081
        ISSU DHCP Snooping clientNon-Base
2082
        ISSU IP Host client Non-Base
2083
         ISSU Inline Power client Non-Base
2084
         ISSU IGMP Snooping clientNon-Base
4001
        ISSU C4K Chassis client Base
4002
         ISSU C4K Port client
                                 Base
4003
         ISSU C4K Rkios client
                                 Base
4004
         ISSU C4K HostMan client Base
         ISSU C4k GaliosRedundancyBase
4005
```

次に、保存された互換性マトリクスに関する情報を表示する例を示します。

Switch# show issu comp-matrix stored

```
Number of Matrices in Table = 1
```

■ ISSU プロセスの実行方法



CHAPTER

6

インターフェイスの設定

この章では、Catalyst 4500 シリーズ スイッチにインターフェイスを設定する手順について説明します。設定上の注意事項、設定手順、および設定例についても示します。

この章の主な内容は、次のとおりです。

- インターフェイス設定の概要 (p.6-2)
- interface コマンドの使用 (p.6-3)
- インターフェイスの範囲設定 (p.6-5)
- インターフェイス範囲マクロの定義および使用 (p.6-7)
- 10 ギガビット イーサネット ポートおよびギガビット イーサネット SFP ポートの配置 (p.6-8)
- 10 ギガビット イーサネット ポートまたはギガビット イーサネット ポートの WS-X4606-10GE-E および Supervisor Engine 6-E への配置 (p.6-10)
- Supervisor Engine 6-E での共有バックプレーン アップリンク モードの起動 (p.6-13)
- 光デジタル モニタ トランシーバのサポート (p.6-14)
- オプションのインターフェイス機能の設定 (p.6-15)
- OIR の概要 (p.6-30)
- インターフェイスのモニタリングおよびメンテナンス (p.6-31)



この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/cr/index.htm

インターフェイス設定の概要

デフォルトでは、すべてのインターフェイスがイネーブルになっています。10/100 Mbps イーサネット インターフェイスは、接続速度とデュプレックスを自動ネゴシエーションします。10/100/1000 Mbps イーサネット インターフェイスは、速度、デュプレックス、フロー制御をネゴシエーションします。1000 Mbps イーサネット インターフェイスは、フロー制御のみをネゴシエーションします。自動ネゴシエーションでは、所定の 2 ポートで最速の速度が自動的に選択されます。インターフェイスに速度が明示的に指定されている場合、そのインターフェイスが明示的に全二重に設定されている場合を除き、デフォルトで半二重に設定されます。

多くの機能は、インターフェイス単位で有効になります。interface コマンドを入力するとき、次の事項を指定する必要があります。

- インターフェイス タイプ
 - ファスト イーサネット (fastethernet キーワードを使用)
 - ギガビット イーサネット (gigabitethernet キーワードを使用)
 - 10 ギガビット イーサネット (tengigabitethernet キーワードを使用)
- スロット番号 インターフェイス モジュールの搭載先スロットです。スロットには、上から下へ、1 から始まる通し番号が付けられています。
- インターフェイス番号 モジュールのインターフェイス番号です。インターフェイス番号は、 常に1から始まります。スイッチの正面に向かって左から右に、インターフェイスに番号が付 けられています。

スイッチ上のスロット / インターフェイスの物理的位置を確認して、インターフェイスを特定できます。また、Cisco IOS の show コマンドを使用して、特定のインターフェイスまたはすべてのインターフェイスに関する情報を表示することもできます。

interface コマンドの使用

次に示す一般的な手順は、すべてのインターフェイスの設定作業に適用されます。

ステップ 1 特権 EXEC プロンプトに、configure terminal コマンドを入力して、グローバル コンフィギュレーション モードを開始します。

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#

ステップ2 グローバル コンフィギュレーション モードで、interface コマンドを入力します。インターフェイス カード上のコネクタのインターフェイス タイプおよびインターフェイス番号を識別します。次に、ファスト イーサネット、スロット 5、インターフェイス 1 を選択する例を示します。

Switch(config)# interface fastethernet 5/1
Switch(config-if)#

ステップ3 インターフェイスの番号は、インストレーション時に、またはシステムにモジュールが追加されたときに工場で割り当てられます。スイッチに搭載されているすべてのインターフェイスのリストを表示するには、show interfaces EXEC コマンドを使用します。次の出力例のように、スイッチがサポートするインターフェイスごとにレポートが作成されます。

```
Switch(config-if) #Ctrl-Z
Switch#show interfaces
Vlan1 is up, line protocol is down
 Hardware is Ethernet SVI, address is 0004.dd46.7aff (bia 0004.dd46.7aff)
 MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
 Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     O packets input, O bytes, O no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
GigabitEthernet1/1 is up, line protocol is down
 Hardware is Gigabit Ethernet Port, address is 0004.dd46.7700 (bia 0004.dd46.7700)
 MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
 Auto-duplex, Auto-speed
 ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
```

```
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     O input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     O output errors, O collisions, O interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
GigabitEthernet1/2 is up, line protocol is down
 Hardware is Gigabit Ethernet Port, address is 0004.dd46.7701 (bia 0004.dd46.7701)
 MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed
  ARP type: ARPA, ARP Timeout 04:00:00
 Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     O input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     O output errors, O collisions, O interface resets
     O babbles, O late collision, O deferred
     0 lost carrier, 0 no carrier
     {\tt 0} output buffer failures, {\tt 0} output buffers swapped out
--More-
< テキスト出力は省略 >
```

ステップ 4 次の例に示すように、インターフェイス FastEthernet 5/5 の設定を開始するには、グローバル コンフィギュレーション モードで interface キーワード、インターフェイス タイプ、スロット番号、インターフェイス番号を入力します。

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 5/5
Switch(config-if)#



(注)

インターフェイス タイプとインターフェイス番号の間にスペースは不要です。たとえば、上記の例では、fastethernet 5/5 または fastethernet5/5 のどちらを入力してもかまいません。

- ステップ 5 interface コマンドに続いて、個々のインターフェイスに必要なインターフェイス コンフィギュレーション コマンドを入力します。入力するコマンドによって、そのインターフェイス上で実行されるプロトコルおよびアプリケーションが決まります。 別の interface コマンドを入力するか、またはCtrl-Z を押してインターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻るまで、入力したコマンドが収集され、対応する interface コマンドに適用されます。
- ステップ6 インターフェイスを設定したあとで、「インターフェイスのモニタリングおよびメンテナンス」 (p.6-31)に記載されている show EXEC コマンドを使用して、インターフェイスのステータスを確認します。

インターフェイスの範囲設定

インターフェイス範囲設定モードを使用して、同じコンフィギュレーション パラメータを持つ複数 のインターフェイスを設定できます。インターフェイス範囲設定モードを開始すると、このモード を終了するまで、入力したすべてのコマンド パラメータが、その範囲内のすべてのインターフェイスに適用されます。

同じ設定を持つインターフェイスの範囲を設定するには、次の作業を行います。

コマンド	目的
Switch(config)# interface range {vlan vlan_ID - vlan_ID} {{fastethernet gigabitethernet tengigabitethernet macro	設定するインターフェイスの範囲を選択します。次の点に 注意してください。
<pre>macro_name} slot/interface - interface} [, {vlan vlan ID - vlan ID} {{fastethernet </pre>	ダッシュの前にスペースを入れます。
gigabitethernet tengigabitethernet macro	カンマで区切って、範囲を5つまで入力できます。
<pre>macro_name} slot/interface - interface}]</pre>	カンマの前後にスペースは必要ありません。



interface range コマンドを使用する場合、vlan、fastethernet、gigabitethernet、tengigabitethernet、macro キーワードとダッシュの間にスペースを入れます。たとえば、コマンド interface range fastethernet 5/1 - 5 は有効な範囲を指定していますが、コマンド interface range fastethernet 1-5 には有効な range コマンドが含まれていません。



interface range コマンドは、interface vlan コマンドを使用して設定されている VLAN(仮想 LAN)インターフェイスについてのみ有効です(設定済みの VLAN インターフェイスを表示するには、show running-configuration コマンドで表示されない VLAN インターフェイスに、interface range コマンドを使用しますとはできません。

次に、インターフェイス FastEthernet 5/1 ~ 5/5 すべてを再びイネーブルにする例を示します。

```
Switch(config)# interface range fastethernet 5/1 - 5
Switch(config-if-range)# no shutdown
Switch(config-if-range)#
*Oct 6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/1, changed state to up
*Oct 6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/2, changed state to up
*Oct 6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/3, changed state to up
*Oct 6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/4, changed state to up
*Oct 6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/5, changed state to up
*Oct 6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/
5, changed state to up
*Oct 6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/
3, changed state to up
*Oct 6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/
4, changed state to up
Switch(config-if)#
```

次に、カンマを使用して、タイプの異なるインターフェイス ストリングを追加して範囲を指定し、インターフェイス FastEthernet $5/1\sim5/5$ と、GigabitEthernet 1/1 および 1/2 を再びイネーブルにする例を示します。

```
Switch(config-if)# interface range fastethernet 5/1 - 5, gigabitethernet 1/1 - 2
Switch(config-if) # no shutdown
Switch(config-if)#
*Oct 6 08:29:28: %LINK-3-UPDOWN: Interface FastEthernet5/1, changed state to up
*Oct 6 08:29:28: %LINK-3-UPDOWN: Interface FastEthernet5/2, changed state to up
     6 08:29:28: %LINK-3-UPDOWN: Interface FastEthernet5/3, changed state to up
*Oct 6 08:29:28: %LINK-3-UPDOWN: Interface FastEthernet5/4, changed state to up
*Oct 6 08:29:28: %LINK-3-UPDOWN: Interface FastEthernet5/5, changed state to up
*Oct 6 08:29:28: %LINK-3-UPDOWN: Interface GigabitEthernet1/1, changed state to
up
*Oct 6 08:29:28: %LINK-3-UPDOWN: Interface GigabitEthernet1/2, changed state to
*Oct 6 08:29:29: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/
5, changed state to up
*Oct 6 08:29:29: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/
3, changed state to up
*Oct 6 08:29:29: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/
4, changed state to up
Switch(config-if)#
```

インターフェイス範囲設定モードで複数のコンフィギュレーション コマンドを入力するとき、各コマンドは入力するたびに実行されます(インターフェイス範囲設定モードの終了後にまとめて実行されるわけではありません)。コマンドの実行中にインターフェイス範囲設定モードを終了すると、一部のコマンドが範囲内のすべてのインターフェイスで実行されない場合もあります。コマンドプロンプトが表示されたのを確認してから、インターフェイス範囲設定モードを終了してください。

インターフェイス範囲マクロの定義および使用

インターフェイス範囲マクロを定義して、設定するインターフェイスの範囲を自動的に選択できます。interface range macro コマンドで macro キーワードを使用するには、事前にマクロを定義しておく必要があります。

インターフェイス範囲マクロを定義するには、次の作業を行います。

コマンド	目的
(-11 TD -1 TD) ((f	インターフェイス範囲マクロを定義して、実行中のコンフィギュレーション ファイルに保存します。

次に、インターフェイス FastEthernet 5/1 ~ 5/4 を選択するように、インターフェイス範囲マクロ enet_list を定義する例を示します。

Switch(config)# define interface-range enet_list fastethernet 5/1 - 4

定義済みのインターフェイス範囲マクロの設定を表示するには、次の作業を行います。

コマンド	目的			
Switch# show running-config	定義済みのインターフェイス範囲マクロの設定 を表示します。			

次に、定義済みのインターフェイス範囲マクロ enet_list を表示する例を示します。

Switch# show running-config | include define
define interface-range enet_list FastEthernet5/1 - 4
Switch#

interface range コマンドでインターフェイス範囲マクロを使用するには、次の作業を行います。

コマンド	目的
	指定したインターフェイス範囲マクロに保存された値を使用して、設定するインターフェイスの範囲を選択します。

次に、インターフェイス範囲マクロ enet_list を使用して、インターフェイス範囲設定モードに切り替える例を示します。

Switch(config)# interface range macro enet_list
Switch(config-if)#

10 ギガビット イーサネット ポートおよびギガビット イーサネット SFP ポートの配置



Catalyst 4510R シリーズ スイッチ上で、10 ギガビット イーサネット ポートおよびギガビット イー サネット Small Form-Factor Pluggable (SFP; 着脱可能小型フォーム ファクタ) アップリンク ポート の両方をイネーブルにする場合、スイッチを再起動する必要があります。Catalyst 4503、4506、お よび 4507R シリーズ スイッチ上では、この機能は自動的にイネーブルになります。

Cisco IOS Release 12.2(25)SG より前のリリースでは、Cisco Catalyst 4500 Supervisor Engine V-10GE に より、デュアル ワイヤスピード 10 ギガビット イーサネット ポートまたは代替可能に配線された 4 つのギガビット イーサネット SFP アップリンク ポートのいずれかをイネーブルにできます。Cisco IOS Release 12.2(25)SG では、デュアル 10 ギガビット イーサネット ポートおよび 4 つのギガビット イーサネット SFP ポートを Catalyst 4503、Catalyst 4506、および Catalyst 4507R シャーシに同時に配 置できます。

Catalyst 4510R シャーシの配置では、次の構成のうちいずれかがサポートされます。

- デュアル 10 ギガビット イーサネット ポート(X2 光ポート)のみ。
- 4 つのギガビット イーサネット ポート (SFP 光ポート) のみ。
- デュアル 10 ギガビット イーサネット ポートおよび 4 つのギガビット イーサネット ポートの 両方。このモード場合、10番めのスロット(フレックススロット)がサポートするのは、2ポー トの Gigabit Interface Converter (GBIC; ギガビット インターフェイス コンバータ) ラインカー ド(WS-X4302-GB)のみです。

10 ギガビット イーサネット ポートまたはギガビット イーサネット SFP アップリンク ポートを選 択するには、次の作業を行います。

コマンド		目的			
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始			
		します。			
ステップ 2	<pre>Switch(config)# hw-module uplink select [all gigabitethernet tengigabitethernet]</pre>	イネーブルにするポート タイプを選択します。			



10 スロット シャーシ (Catalyst 4510R および 4510RE) に搭載されている Supervisor Engine V-10GE (WS-X4516-10GE)では、新規アップリンク モードのスタートアップ コンフィギュレーションが フラッシュ メモリにコピーされてシステムの電源が再投入される場合、システムは新規アップリ ンク モードで起動しません。新規アップリンク モードのスタートアップ コンフィギュレーション がフラッシュ メモリにコピーされたあと、システムの電源が再投入されるまでに、コマンド イン ターフェイスを通じてアップリンク モードを新規アップリンク モードに変更する必要がありま す。これにより、システムは新規アップリンクモードで起動します。



(注)

Supervisor Engine V が Catalyst 4510R または 4510R-E シャーシで使用されている場合、スロット 10 (FlexSlot) は、2 ポート GBIC (WS-X4302-GB) およびアクセス ゲートウェイ モジュール (WS-X4604-GWY) のラインカードのみをサポートします。アップリンク選択モードが「all」に設定されている場合、Supervisor Engine V-10GE には同じ制限があります。アップリンク選択モード が「tengigabitethernet」または「gigabitethernet」に設定されている場合、Supervisor Engine V-10GE はスロット 10 にあるすべての Catalyst 4500 シリーズ ラインカードをサポートします。Supervisor Engine 6-E はスロット 10 にあるすべての Catalyst 4500 シリーズ ラインカードをサポートしています。

次に、Catalyst 4510R シリーズ スイッチ上で 10 ギガビット イーサネット ポートおよびギガビット イーサネット SFP アップリンク ポートの両方をイネーブルにする例を示します。

Switch# configure terminal

Switch(config) # hw-module uplink select all

Warning: This configuration mode will place slot 10 in flex slot mode



(注)

アップリンク モードを修正する際に、スイッチを再起動する必要があります。

10 ギガビット イーサネット ポートまたはギガビット イーサネット ポートの WS-X4606-10GE-E および Supervisor Engine 6-E への配置

Supervisor Engine 6-E および WS-X4606-10GE-E 両方の X2 ポートの柔軟性を高めるために、Catalyst 4500 スイッチは TwinGig コンバータ モジュールをサポートします。 TwinGig コンバータ モジュー ルが X2 ホールに接続していると、1 つの X2 ホール(1 つのプラグイン可能な X2 光ポートに対応) が 2 つの SFP ホール(2 つのプラグイン可能な SFP 光ポートに対応)に変換されます。これにより、 10 ギガビット ポートおよび 1 ギガビット ポートを同じラインカードに設置できます。また、ギガ ビット ポートを使用して、必要に応じて 10 ギガビット ポートへの切り替えが可能です。

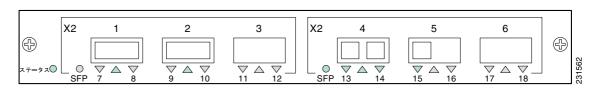
次の内容について説明します。

- ポート番号設定を行う TwinGig コンバータ (p.6-10)
- TwinGig コンバータの制限事項 (p.6-11)
- X2/TwinGig コンバータ モードの選択 (p.6-11)

ポート番号設定を行う TwinGig コンバータ

TwinGig コンバータがイネーブルまたはディセーブルである場合、ラインカード上のポート番号お よびポート タイプは動的に変わります。用語がこの動作を反映する必要があります。Cisco IOS で は、10 ギガビット ポートの名前は TenGigabit であり、1 ギガビット ポートの名前は Gigabit です。 Cisco IOS Release 12.2(40)SG 以降では、TenGigabit 1/1 および Gigabit 1/1 という名前の 2 つのポート が存在しないようにするため、10 ギガビットおよび 1 ギガビット ポート番号は独立しています。た とえば、6 個の X2 ホールを持つ WS-X4606-10GE-E モジュールでは、X2 ポートの名前は TenGigabit スロット番号/ $<1 \sim 6$ > であり、SFP ポートの名前は Gigabit スロット番号/ $<7 \sim 18$ > です。

WS-X4606-10GE の前面プレート 図 6-1



Cisco IOS ではポート 1 から 18 は常に存在します。つまり、これらのポートの設定を適用でき、CLI 出力に表示されます。ただし、X2 ポートまたは SFP ポートがある特定の時間アクティブになって いる場合のみです。たとえば、X2 が 2 番めのホールに接続している場合、X2 ポート 2 はアクティ ブで SFP ポート 9 および 10 はアクティブではありません。TwinGig コンバータが 2 番めのホール に接続している場合、X2 ポート 2 はアクティブではなく SFP ポート 9 および 10 はアクティブで す。アクティブではないポートは、スイッチング ASIC に接続してるアップリンクがない、Supervisor Engine IV および V-10GE 上のアクティブではないポートと同様に扱われます。



WS-X4606-X2 モジュールで TwinGig と X2 トランシーバの両方を使用している場合、これらをポー ト1~3で1グループにまとめておき、ポート4~6を別の1グループとします。TwinGig または X2 トランシーバを任意のポートに挿入すると、パートナ ポートの能力に影響を与え、3 つすべて が同じタイプを処理するように自動的に設定されます。ポート グループ内で混合させると、動作 しません。例えば、ポート 1 に X2 を接続かつポート 2 に TwinGig を接続することはできないし、 両方を機能させることもできません。

TwinGig コンパータの制限事項

Supervisor Engine 6-E システムでは、ポートはスタブ ASIC 経由でスイッチング エンジンに接続しています。このスタブ ASIC にはポートについて次の制限事項があります。1 つのスタブ ASIC 上ではギガビット ポートおよび 10 ギガビット ポートを併用できません。つまり、すべて 10 ギガビット (X2) か、すべてギガビット (TwinGig コンバータおよび SFP) である必要があります。X2 モジュールの前面プレートでは、実際の物理グループまたはグループの回りに描かれるボックスによって、このスタブ ポートのグループが示されています。

X2/TwinGig コンパータ モードの選択

デフォルトのコンフィギュレーション モードは X2 です。そのため、10 ギガビット インターフェイスの配置を計画する場合は、何も設定する必要はありません。ただし、ギガビット インターフェイスを配置する (つまり、TwinGig コンバータを使用する) 場合は関連するポート グループを設定する必要があります。

• モジュール上の X2 ホールをグループ化する方法を決定するには、show hw-module module <m>port-group コマンドを入力します。

WS-X4606-10GE-E シャーシでは、次のような出力が行われます。

Switch# :	. port-group	Inactive		
1	1	Te1/1-3		Gi1/7-12
1	2	Te1/4-6		Gi1/13-18

Switch# show int status mod 1

Port	Name	Status	Vlan	Duplex	Speed	Туре
Te1/1		notconnect	1	full	10G	10GBase-LR
Te1/2		connected	1	full	10G	10GBase-LR
Te1/3		notconnect	1	full	10G	No X2
Te1/4		notconnect	1	full	10G	No X2
Te1/5		notconnect	1	full	10G	No X2
Te1/6		notconnect	1	full	10G	No X2
Gi1/7		inactive	1	full	1000	No Gbic
Gi1/8		inactive	1	full	1000	No Gbic
Gi1/9		inactive	1	full	1000	No Gbic
Gi1/10		inactive	1	full	1000	No Gbic
Gi1/11		inactive	1	full	1000	No Gbic
Gi1/12		inactive	1	full	1000	No Gbic
Gi1/13		inactive	1	full	1000	No Gbic
Gi1/14		inactive	1	full	1000	No Gbic
Gi1/15		inactive	1	full	1000	No Gbic
Gi1/16		inactive	1	full	1000	No Gbic
Gi1/17		inactive	1	full	1000	No Gbic
Gi1/18		inactive	1	full	1000	No Gbic
Switch#						

• ギガビットを配置する各 X2 ポート グループに対する操作のモードを設定するには、 hw-module module <m> port-group select gigabitethernet コマンドを入力します。この設定は、電源の再投入およびリロード時に保持されます。

TwinGig コンバータを使用してギガビット イーサネット インターフェイスを配置するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config) # hw-module module m port-group p select [gigabitethernet tengigabitethernet]	各 X2 ポート グループに対する操作のモードを選択します。
		デフォルトは 10 ギガビット イーサネット (X2) です。
ステップ 3	Switch(config)# exit	コンフィギュレーション モードを終了します。
ステップ 4	Switch# show int status mod n	設定を確認します。

次に、TwinGig コンバータを使用して WS-X4606-10GE-E 上のギガビット イーサネット インタフェースを選択する例を示します。

Switch# config terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# hw-module module 1 port-group 1 select gigabitethernet
Switch(config)# exit

Switch# show int status mod 1

Port	Name	Stati	ıs Vlar	n Duplex	Speed	Тур	e
Te1/1		inac	cive 1	full	10G	No	X2
Te1/2		inac	cive 1	full	10G	No	X2
Te1/3		inac	tive 1	full	10G	No	X2
Te1/4		notco	onnect 1	full	10G	No	X2
Te1/5		notco	onnect 1	full	10G	No	X2
Te1/6		note	onnect 1	full	10G	No	X2
Gi1/7		notco	onnect 1	full	1000	No	Gbic
Gi1/8		notco	onnect 1	full	1000	No	Gbic
Gi1/9		notco	onnect 1	full	1000	No	Gbic
Gi1/10		note	onnect 1	full	1000	No	Gbic
Gi1/11		note	onnect 1	full	1000	No	Gbic
Gi1/12		note	onnect 1	full	1000	No	Gbic
Gi1/13		inac	tive 1	full	1000	No	Gbic
Gi1/14		inac	tive 1	full	1000	No	Gbic
Gi1/15		inac	tive 1	full	1000	No	Gbic
Gi1/16		inac	tive 1	full	1000	No	Gbic
Gi1/17		inac	cive 1	full	1000	No	Gbic
Gi1/18		inac	tive 1	full	1000	No	GbicI

Supervisor Engine 6-E での共有バックプレーン アップリンク モードの起動

この機能により、冗長モードの場合に、スーパーバイザ エンジン上にある 4 つの 10 ギガビット イーサネット ポートすべてをブロッキング ポートとして使用することができます。

Cisco IOS Release 12.2(44)SG より前のリリースでは、Cisco Catalyst 4500 Supervisor Engine 6-E により、デュアル ワイヤスピード 10 ギガビット イーサネット ポート、またはギガビット イーサネット SFP アップリンク ポートに基づく 4 つの Twin-Gigabit コンバータのいずれかをイネーブルにできます。Cisco IOS Release 12.2(44)SG では、(1) 4 つの 10 ギガビット イーサネット ポートのすべて、(2) アクティブ スーパーバイザ エンジン上にある 2 ブロッキング ポートと、スタンバイ スーパーバイザ エンジンの 2 ブロッキング ポート、(3) 8 つのギガビット イーサネット SFP ポートすべて(アクティブなスーパーバイザ エンジン上に 4 ポート、スタンバイ スーパーバイザ エンジン上に 4 ポート、カタンバイ スーパーバイザ エンジン上に 4 ポート)を構成可能です。この機能は、すべての Catalyst 4500 および 4500-E シリーズ シャーシでサポートされています。

共有バックプレーン モードをイネーブルにするには、次のコマンドを入力します。

コマンド	目的
	新規設定を適用するにはアクティブ スーパーバイザのリロードが必要です。

共有バックプレーン モードをイネーブルにするには、次のコマンドを入力します。

コマンド	目的
Switch(config)# no hw-mod uplink mode shared-backplane	新規設定を適用するにはアクティブ スーパーバイザのリロードが必要です。

光デジタル モニタ トランシーバのサポート

CLI(コマンドライン インターフェイス)コマンド(show inventory、show idprom interface)をトランシーバで使用すると、シリアル ナンバー、モデル名、インベントリ情報を取得できます。

次のコマンドは、DOM 機能をサポートするトランシーバ専用のコマンドです。

• 特定のインターフェイス トランシーバのセンサーすべての現在値およびしきい値を表示します。

show interfaces <int-name> transceiver [detail] [threshold]

• すべてのトランシーバのすべてのセンサーに対して、*entSensorThresholdNotification* をイネーブルまたはディセーブルにします。

snmp-server enable trap transceiver

• トランシーバ モニタリングをイネーブルまたはディセーブルにします。

transceiver type all



(注)

この機能は、DOM 対応トランシーバが存在し、モニタリング用に設定されている場合にのみ、使用できます。センサー情報の更新頻度は、トランシーバ Serial Electrically Erasable Programmable Read Only Memory (SEEPROM)で設定されたデフォルト値によって異なります。

オプションのインターフェイス機能の設定

ここでは、オプション手順について説明します。

- イーサネット インターフェイス速度およびデュプレックス モードの設定 (p.6-15)
- フロー制御の設定 (p.6-18)
- ジャンボ フレーム サポートの設定 (p.6-22)
- ベビー ジャイアント機能との対話 (p.6-25)
- ポート デバウンス タイマーの設定 (p.6-26)
- ポートでの Auto-MDIX の設定 (p.6-27)

イーサネット インターフェイス速度およびデュプレックス モードの設定

- 速度およびデュプレックス モード設定時の注意事項 (p.6-15)
- インターフェイス速度の設定 (p.6-15)
- インターフェイスのデュプレックス モードの設定 (p.6-17)
- インターフェイス速度およびデュプレックス モードの設定の表示 (p.6-17)
- インターフェイスに関する記述の追加 (p.6-18)

速度およびデュプレックス モード設定時の注意事項



(注)

クライアントのデバイスには、自動ネゴシエーションを設定しません。スイッチに自動ネゴシエーションする速度、または速度範囲を設定します。

通常の場合、インターフェイス速度およびデュプレックス モード パラメータは auto に設定し、Catalyst 4500 シリーズ スイッチがインターフェイス間でインターフェイス速度およびデュプレックス モードを自動的にネゴシエーションできるようにします。インターフェイスの speed コマンドおよび duplex コマンドを手動で設定する場合には、次の点を考慮してください。

- no speed コマンドを入力すると、スイッチは自動的にインターフェイスの speed および duplex の両方を auto に設定します。
- インターフェイス速度を **1000** (Mbps) または **auto 1000** に設定すると、デュプレックス モードが全二重になります。デュプレックス モードは変更できません。
- インターフェイス速度が 10 または 100 に設定された場合、デュプレックス モードは明示的に 設定する場合を除き、デフォルトで半二重に設定されます。



注意

インターフェイス速度およびデュプレックス モードの設定を変更すると、インターフェイスが シャットダウンされてから再起動する場合があります。

インターフェイス速度の設定

10/100 Mbps イーサネット インターフェイスでインターフェイス速度を **auto** に設定すると、速度とデュプレックスは自動ネゴシエーションされます。強制 10/100 自動ネゴシエーション機能を使用すると、10/100/1000BASE-T ポート上のインターフェイス速度の自動ネゴシエーションを最大 100 Mbps に制限できます。

オプションのインターフェイス機能が設定

10/100 Mbps イーサネット インターフェイスのポート速度を設定するには、次の作業を行います。

次に、インターフェイス FastEthernet 5/4 のインターフェイス速度を 100 Mbps に設定する例を示します。

Switch(config)# interface fastethernet 5/4
Switch(config-if)# speed 100

次に、インターフェイス FastEthernet 5/4 が速度とデュプレックス モードを自動ネゴシエーションする例を示します。

Switch(config)# interface fastethernet 5/4
Switch(config-if)# speed auto



これは、speed auto 10 100 の指定に類似しています。

次に、自動ネゴシエーション モードのインターフェイス GigabitEthernet 1/1 のインターフェイス速度を 10 Mbps および 100 Mbps に制限する例を示します。

Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# speed auto 10 100

次に、インターフェイス GigabitEthernet 1/1 の速度ネゴシエーションを 100 Mbps に制限する例を示します。

Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# speed auto 100



(注)

ギガビット イーサネット インターフェイスの自動ネゴシエーションをオフにすると、ポートが強制的に 1000 Mbps および全二重モードになります。

インターフェイス GigabitEthernet 1/1 のポート速度の自動ネゴシエーションをオフにするには、次の作業を行います。

	コマンド	目的
ステップ 1	<pre>Switch(config)# interface gigabitethernet1/1</pre>	設定するインターフェイスを指定します。
ステップ 2	Switch(config-if)# speed nonegotiate	インターフェイスの自動ネゴシエーションをディ
		セーブルにします。

自動ネゴシエーションに戻すには、インターフェイス コンフィギュレーション モードで no speed nonegotiate コマンドを入力します。



(注)

WS-X4416 モジュールのブロッキング ポートについては、速度を自動ネゴシエーションに設定しないでください。

インターフェイスのデュプレックス モードの設定



(注)

インターフェイスが 1000 Mbps に設定されている場合、デュプレックス モードを全二重から半二重に変更できません。

ファスト イーサネット インターフェイスのデュプレックス モードを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	<pre>Switch(config)# interface fastethernet slot/interface</pre>	設定するインターフェイスを指定します。
ステップ 2	1-161	インターフェイスのデュプレックス モードを設定 します。

次に、インターフェイス FastEthernet 5/4 のインターフェイスのデュプレックス モードを full に設定する例を示します。

Switch(config)# interface fastethernet 5/4
Switch(config-if)# duplex full

インターフェイス速度およびデュプレックス モードの設定の表示

インターフェイスのインターフェイス速度とデュプレックス モード設定を表示するには、次の作業を行います。

コマンド	目的
Switch# show interfaces [fastethernet gigabitethernet tengigabitethernet] slot/interface	インターフェイス速度およびデュプレックス モードの設定を表示します。

次に、インターフェイス FastEthernet 6/1 のインターフェイス速度およびデュプレックス モードを表示する例を示します。

```
Switch# show interface fastethernet 6/1
FastEthernet6/1 is up, line protocol is up
 Hardware is Fast Ethernet Port, address is 0050.547a.dee0 (bia 0050.547a.dee0)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
  ARP type: ARPA, ARP Timeout 04:00:00
 Last input 00:00:54, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 50/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     50 packets input, 11300 bytes, 0 no buffer
     Received 50 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     O input packets with dribble condition detected
     1456 packets output, 111609 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     O babbles, O late collision, O deferred
     1 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Switch#
```

インターフェイスに関する記述の追加

インターフェイスの機能をわかりやすくするため、インターフェイスに関する記述を追加できます。記述は show configuration、show running-config、および show interfaces コマンドの出力に表示されます。

インターフェイスに記述を追加するには、次のコマンドを入力します。

コマンド	目的
Switch(config-if)# description string	インターフェイスの記述を追加します。

次に、インターフェイス FastEthernet 5/5 に関する記述を追加する例を示します。

```
Switch(config)# interface fastethernet 5/5
Switch(config-if)# description Channel-group to "Marketing"
```

フロー制御の設定

ギガビット イーサネット ポートは、着信パケットの送信を遅らせるためにフロー制御を使用します。ギガビット イーサネット ポートのバッファでスペースが不足すると、そのポートは特殊なパケットを送信し、パケットの送信を一定時間遅らせるように、リモート ポートに要求します。ポートは、同じ目的で、リンクパートナーからこの特殊なパケットを受信します。この特殊なパケットをポーズ フレームといいます。

ギガビット イーサネット インターフェイスのデフォルト設定は、次のとおりです。

- ポーズ フレームの送信がオフである オーバーサブスクライブされていないギガビット イーサネット インターフェイス
- ポーズ フレームの受信が望ましい オーバーサブスクライブされていないギガビット イーサネット インターフェイス

- ポーズ フレームの送信がオンである オーバーサブスクライブされたギガビット イーサネッ トインターフェイス
- ポーズ フレームの受信が望ましい オーバーサブスクライブされたギガビット イーサネット インターフェイス

10 ギガビット イーサネット インターフェイスのデフォルト設定は、次のとおりです。

- ポーズ フレームの送信がオフである
- ポーズ フレームの受信がオンである



望ましいは 10 ギガビット イーサネット インターフェース上のフロー制御のオプションにはあり ません。

フロー制御を設定にするには、次の作業を行います。

	コマンド	目的				
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。				
		9 0				
ステップ 2	Switch(config)# interface interface-id	インターフェイス コンフィギュレーション モードを開始し、フロー制御をイネーブルにするインターフェイス を指定します。				
ステップ 3	Switch(config-if)# flowcontrol {receive send} {off on desired}	ポーズ フレームを送信または受信するようギガビット イーサネット ポートを設定します。				
ステップ 4	Switch(config-if)# end	コンフィギュレーション モードに戻ります。				
ステップ 5	Switch(config)# end	特権 EXEC モードに戻ります。				

次に、オーバーサブスクライブされたポート GigabitEthernet 7/5 にフロー制御を設定する例を示します。

```
Switch# configure terminal
```

Switch(config) # interface g7/5

Switch(config-if)# flowcontrol send on

Switch(config-if)# end

 ${\tt Switch) \, \# \, \, show \, \, interfaces \, \, gigabitEthernet \, \, 7/5 \, \, \, capabilities}$

GigabitEthernet7/5

Model: WS-X4548-GB-RJ45-RJ-45

Type: 10/100/1000-TX
Speed: 10,100,1000,auto
Duplex: half,full,auto
Trunk encap. type: 802.1Q,ISL

Trunk mode: on,off,desirable,nonegotiate

Channel: yes

Broadcast suppression: percentage(0-100), hw $\,$

Flowcontrol: rx-(off,on,desired),tx-(off,on,desired)

VLAN Membership: static, dynamic

Fast Start: yes

Queuing: rx-(N/A), tx-(1p3q1t, Sharing/Shaping)

CoS rewrite: yes
ToS rewrite: yes
Inline power: no

SPAN: source/destination

UDLD: yes
Link Debounce: no
Link Debounce Time: no
Port Security: yes
Dot1x: yes

Dot1x: yes
Maximum MTU: 1552 bytes (Baby Giants)

Multiple Media Types: no Diagnostic Monitoring: N/A

Switch) # show flowcontrol interface GigabitEthernet 7/5

Port Send FlowControl Receive FlowControl RxPause TxPause admin oper admin oper

Gi7/5 on off desired off 0 0

次に、オーバーサブスクライブされていないポート Gigabit Ethernet 5/5 で、show interfaces および show flowcontrol コマンドを実行した場合の出力例を示します。

Switch# show interfaces gigabitEthernet 5/5 capabilities

GigabitEthernet5/5

Model: WS-X4306-GB-Gbic

Type: No Gbic
Speed: 1000
Duplex: full
Trunk encap. type: 802.1Q,ISL

Trunk mode: on,off,desirable,nonegotiate

Channel: yes

Broadcast suppression: percentage(0-100), hw

Flowcontrol: rx-(off,on,desired),tx-(off,on,desired)

VLAN Membership: static, dynamic

Fast Start: yes

Queuing: rx-(N/A), tx-(1p3q1t, Sharing/Shaping)

CoS rewrite: yes
ToS rewrite: yes
Inline power: no

SPAN: source/destination

UDLD: yes
Link Debounce: no
Link Debounce Time: no
Port Security: yes
Dot1x: yes

Maximum MTU: 9198 bytes (Jumbo Frames)

Multiple Media Types: no Diagnostic Monitoring: N/A

Switch# show flowcontrol interface gigabitEthernet 5/5

Port	Send FlowControl		Receive FlowControl		RxPause	TxPause
	admin	oper	admin	oper		
Gi5/5	off	off	desired	off	0	0

次に、サポートされていない Fast Ethernet 3/5 ポートで、show interfaces および show flowcontrol コマンドを実行した場合の出力例を示します。

Switch# show interfaces fa3/5 capabilities

FastEthernet3/5

Model: WS-X4148-RJ-45
Type: 10/100BaseTX
Speed: 10,100,auto
Duplex: half,full,auto
Trunk encap. type: 802.1Q,ISL

Trunk mode: on,off,desirable,nonegotiate

Channel: yes

Broadcast suppression: percentage(0-100), sw Flowcontrol: rx-(none),tx-(none)

VLAN Membership: static, dynamic

Fast Start: yes

Queuing: rx-(N/A), tx-(1p3q1t, Shaping)

CoS rewrite: yes
ToS rewrite: yes
Inline power: no

SPAN: source/destination

UDLD: yes
Link Debounce: no
Link Debounce Time: no
Port Security: yes
Dotlx: yes

Maximum MTU: 1552 bytes (Baby Giants)

Multiple Media Types: no Diagnostic Monitoring: N/A

Switch# show flowcontrol interface fa3/5

Port Send FlowControl Receive FlowControl RxPause TxPause admin oper admin oper

Fa3/5 Unsupp. Unsupp. Unsupp. Unsupp. 0 0

ジャンボ フレーム サポートの設定

ここでは、ジャンボ フレーム サポートについて説明します。

- ジャンボ フレームをサポートするポートおよびモジュール (p.6-22)
- ジャンボ フレーム サポートの概要 (p.6-23)
- MTU サイズの設定 (p.6-25)

ジャンボ フレームをサポートするポートおよびモジュール

次のポートおよびモジュールはジャンボ フレームをサポートしています。

- スーパーバイザ アップリンク ポート
- WS-X4306-GB: すべてのポート
- WS-X4232-GB-RJ: $\pi 1 \sim 2$
- WS-X4418-GB:ポート1~2
- WS-X4412-2GB-TX:ポート13~14
- 4648-GB-RJ45V
- WS-X4648-GB+RJ45V
- WS-X4706-10GE

最後の3つのモジュールには、それぞれ2つのノンブロッキング ポートがあり、ジャンボフレームをサポートしています。ほかのポートはオーバーサブスクライブ ポートでありジャンボフレームをサポートしていません。

ジャンボ フレーム サポートの概要

ここでは、ジャンボ フレーム サポートについて説明します。

- MTU の概要 (p.6-23)
- ジャンボ フレーム サポートの概要 (p.6-23)
- イーサネット ポート (p.6-24)
- VLAN インターフェイス (p.6-24)

MTU の概要

Catalyst 4500 シリーズ スイッチでは、システム全体で最大 32 個の最大伝送ユニット (Maximum Transmission Unit; MTU) を設定できます。そのため、すべてのレイヤ 2 およびレイヤ 3 を組み合わせたインターフェイス上で system mtu、mtu、ip mtu、および ipv6 mtu コマンドを使用して設定可能な異なる MTU サイズの最大数は 32 個です。

また、システムにはインターフェイスに個別に設定される ipv4 および ipv6 MTU サイズが格納されます。そのため、すべての system mtu コマンドまたはインターフェイスごとの mtu コマンドについて、1 つは ipv4 用でもう 1 つは ipv6 用として、2 つの異なる MTU 値が格納されます。これにより利用可能なスロット数が、32 個からさらに少なくなります。ただし、各 ip mtu および ipv6 mtu コマンドについて格納される MTU 値は 1 つだけです。

設定している新しい MTU 値がシステムに存在している (つまり別のインターフェイス上で設定されている)場合は、新しい MTU 値を再度格納するために新たにスロットが割り当てられません。

最大限度である 32 に達している場合に、新しい MTU サイズを新しいインターフェイスに設定しようとすると、新しい MTU サイズがいずれかのインターフェイスで事前に設定されている場合にのみ設定を続行できます。そうでない場合は、エラーメッセージが表示され、デフォルトの MTU サイズが設定されているインターフェイスに割り当てられます。

ジャンボ フレーム サポートの概要

ジャンボ フレームとは、デフォルトのイーサネット サイズより大きなフレームのことです。ポートやインターフェイスの MTU サイズをデフォルトより大きく設定すると、ジャンボ フレーム サポートがイネーブルになります。

デフォルト以外の MTU サイズに設定された Catalyst 4500 シリーズ スイッチのイーサネット LAN ポートは、 $1500 \sim 9198$ バイトのサイズのパケットで構成されたフレームを受信できます。デフォルト以外の MTU サイズに設定した場合、入力フレームのパケット サイズがチェックされます。パケットが設定 MTU より大きい場合はドロップされます。

ルーティングする必要のあるトラフィックでは、出力ポートの MTU がチェックされます。MTU がパケット サイズより小さい場合、パケットは CPU に転送されます。[do not fragment] ビットが設定されていない場合、パケットは分割されます。設定されている場合、パケットはドロップされます。



ジャンボ フレーム サポートでは、レイヤ 2 スイッチド パケットは分割されません。

Catalyst 4500 シリーズ スイッチは、出力ポートでパケット サイズと MTU を比較しませんが、ジャンボ フレームはサポートされていないポートでドロップされます。MTU がジャンボ サイズに設定されていなくても、ジャンボ フレームをサポートしているポートへフレームを伝送できます。



(注)

ジャンボ フレーム サポートはインターフェイス単位でのみ設定されます。ジャンボ フレーム サポートをグローバルに設定することはできません。

イーサネット ポート

ここでは、イーサネット ポートでデフォルト以外の MTU サイズを設定する方法について説明します。

- イーサネット ポートの概要 (p.6-24)
- レイヤ 3 およびレイヤ 2 EtherChannel (p.6-24)

イーサネット ポートの概要

Cisco IOS Release 12.2(25)EW では、特定のイーサネット ポートにデフォルト以外の MTU サイズを 設定すると、入力パケットのサイズが制限されます。出力パケットに MTU は影響しません。

Cisco IOS Release 12.1(13)EW より前のリリースでは、ギガビット イーサネットでのみ MTU サイズを設定できます。

レイヤ3 およびレイヤ2 EtherChannel

Cisco IOS Release 12.2(25)EW 以降のリリースでは、EtherChannel のすべてのインターフェイスが同じ MTU になるように設定できます。EtherChannel の MTU を変更すると、すべてのメンバ ポートの MTU も変更されます。メンバ ポートの MTU を新しい値に変更できない場合、そのポートは中断されます(管理上シャット ダウンされます)。MTU が異なるポートは EtherChannel に加入できません。EtherChannel のメンバ ポートが MTU を変更すると、メンバ ポートは中断されます。

VLAN インターフェイス

スイッチ ポートが同じ VLAN に存在する場合、すべてのスイッチ ポートでジャンボ フレームが扱え、同じ MTU サイズをサポートするようにするか、またはいずれも設定しないようにします。ただし、このような同一 VLAN での MTU サイズの統一は必須のものではありません。

VLAN に異なる MTU サイズのスイッチ ポートがあると、MTU サイズが大きいポートから受信したパケットは、MTU サイズが小さいポートへ転送される場合にドロップされる可能性があります。

VLAN 内のスイッチ ポートでジャンボ フレームをイネーブルにしている場合、対応する Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) でもジャンボ フレームがイネーブルです。 SVI の MTU は、VLAN 内のすべてのスイッチ ポートで最小の MTU サイズのものよりも常に小さくなるはずですが、この条件は必須ではありません。

パケットの MTU は、SVI の入力側でチェックされませんが、SVI の出力側でチェックされます。パケットの MTU が出力 SVI の MTU より大きい場合、パケットは CPU に送られて分割処理されます。 [do not fragment] ビットが設定されていない場合、パケットは分割されます。設定されている場合、パケットはドロップされます。

MTU サイズの設定

MTU サイズを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# interface {{vlan vlan_ID} {{type}^1 slot/port} {port-channel port_channel_number} slot/port}}	設定するインターフェイスを選択します。
ステップ 2	Switch(config-if)# mtu mtu_size	MTU サイズを設定します。
	Switch(config-if)# no mtu	デフォルトの MTU サイズ(1500 バイト)に戻します。
ステップ 3	Switch(config-if)# end	インターフェイス コンフィギュレーション モード を終了します。
ステップ 4	Switch(config)# end	コンフィギュレーション モードを終了します。
ステップ 5	Switch# show running-config interface [{fastethernet gigabitethernet} slot/port]	実行コンフィギュレーションを確認します。

^{1.} type = fastethernet、gigabitethernet、またはtengigabitethernet



(注)

ラインカードを*削除*すると、このラインカードのポート上で設定されている MTU 値は未設定となります。そのため、ラインカードを再度挿入するときに、そのラインカードのポートに対する以前の MTU すべてを CLI から再設定する必要があります。



(注)

VLAN インターフェイスと、レイヤ 2 およびレイヤ 3 イーサネット ポートの MTU サイズを設定する場合、サポートされる MTU 値は $1500 \sim 9198$ バイトであることに注意してください。

次に、ポート GigabitEthernet 1/1 に MTU サイズを設定する例を示します。

switch# conf terminal
switch(config)# interface gi1/1
switch(config-if)# mtu 9198
switch(config-if)# end
switch(config)# end
switch# show interface gigabitethernet 1/2
GigabitEthernet1/2 is administratively down, line protocol is down
Hardware is C6k 1000Mb 802.3, address is 0030.9629.9f88 (bia 0030.9629.9f88)
MTU 9216 bytes, BW 1000000 Kbit, DLY 10 usec,
<テキスト出力は省略>
switch#

IP MTU サイズの設定については、IP MTU サイズの設定 (p.27-10) を参照してください。

ベビー ジャイアント機能との対話

ベビー ジャイアント機能は、Cisco IOS Release 12.1(12c)EW で導入されたもので、グローバル コマンド system mtu <size> を使用してグローバル ベビー ジャイアント MTU を設定します。また、この機能により、特定のインターフェイスでイーサネット ペイロード サイズが最大 1552 バイトまでサポートできるようになります。

system mtu コマンドおよびインターフェイス単位の mtu コマンドは、ジャンボ フレームをサポー トできるインターフェイスで動作しますが、インターフェイス単位の mtu コマンドが優先されま

たとえば、インターフェイス gil/l にインターフェイス単位で MTU を設定する前に、system mtu 1550 コマンドを発行して gi1/1 の MTU を 1550 バイトに変更したとします。次に、インターフェイ ス単位の mtu コマンドを発行して gi1/1 の MTU を 9198 バイトに変更します。ここで、コマンド system mtu 1540 でベビー ジャイアントの MTU を 1540 バイトに変更しても、gi1/1 の MTU は 9198 バイトのままで変更されません。

ポート デバウンス タイマーの設定

ポート デバウンス タイマーは、リンク変更の通知を遅らせて、ネットワークの再設定によるトラ フィック損失を減らすことができます。ポート デバウンス タイマーは、各 LAN ポート上に個別設 定することができます。



ポート デバウンス タイマーをイネーブルにすると、リンクアップとリンクダウンの検出が遅れる ことになり、デバウンス期間中のトラフィック損失につながります。この状況は、一部のレイヤ2 とレイヤ3プロトコルのコンバージェンスと再コンバージェンスに影響する可能性があります。

ポート上でデバウンス タイマーを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# interface tengigabitethernet slot/port	設定するポートを選択します。
ステップ 2	Switch(config-if)# link debounce [time debounce_time]	デバウンス タイマーを設定します。
	Switch(config-if)# no link debounce	デフォルト設定に戻します。
ステップ 3	Switch# show interfaces debounce	設定を確認します。

ポートにデバウンス タイマーを設定する際、10 ギガビット イーサネット ポート上で 10 ~ 5000 ミ リ秒の間でポート デバウンス タイマー値を増やすことができます。



デフォルトでは、デバウンスはディセーブルに設定されています。時間なしでデバウンスを設定し た場合、値は10ミリ秒に設定されます。

次に、10 ギガビット イーサネット ポート 2/1 でポート デバウンス タイマーをイネーブルにして、 デフォルト値(10ミリ秒)を受け入れる例を示します。

Switch# config terminal

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)# interface tenGigabitEthernet 2/1

Switch(config-if) # link debounce

Warning: Enabling debounce feature causes link down detection to be delayed

Switch(config-if)# exit

次に、10 ギガビット イーサネット ポート 2/2 で 5000 ミリ秒のポート デバウンス タイマーをイネーブルにして、設定を確認する例を示します。

Switch# config terminal

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config) # interface tenGigabitEthernet 2/2

Switch(config-if) # link debounce time 5000

Warning: Enabling debounce feature causes link down detection to be delayed

Switch(config-if)# end

Switch#

Switch# show interfaces debounce | include enable

Te2/1 enable 10 Te2/2 enable 5000

Switch#

ポートでの Auto-MDIX の設定



Supervisor Engine 6-E は、Auto-MDIX をサポートしていません。

Automatic Medium-Dependent Interface crossover (Auto-MDIX; 自動メディア依存型インターフェイスクロスオーバー)機能をポートでイネーブルにすると、ポートは自動的に必要なケーブル接続タイプ(ストレートまたはクロスケーブル)を検出し、適切に接続を設定します。Auto-MDIX機能なしでスイッチを接続した場合、サーバ、ワークステーション、ルータなどのデバイスの接続にストレートケーブルを使用し、他のスイッチまたはリピータの接続にはクロスケーブルを使用する必要があります。Auto-MDIXをイネーブルにすると、いずれのケーブルタイプを使用しても他のデバイスへ接続でき、インターフェイスは誤ったケーブル接続を自動的に修正します。ケーブル要件の詳細については、ハードウェアインストレーションガイドを参照してください。

Auto-MDIX はデフォルトではディセーブルです。また、Auto-MDIX をイネーブルにした場合、この機能を正常に動作させるため、ポート上の速度を auto に設定する必要があります。Auto-MDIX は、銅製メディア ポートでサポートされます。ファイバ メディア ポートではサポートされません。



(注)

ポートの自動ネゴシエーションがイネーブルである場合、ラインカード WS-X4424-GB-RJ45、WS-X4448-GB-RJ45、および WS-X4548-GB-RJ45 は、デフォルトで Auto-MDIX をサポートします。 **mdix** コマンドを使用して Auto-MDIX をディセーブルにできません。



(注)

ラインカード WS-X4548-GB-RJ45V、WS-X4524-GB-RJ45V、および WS-X4506-GB-T は、デフォルトでも、CLI を使用した場合も Auto-MDIX をサポートしません。



(注)

ラインカード WS-X4124-RJ45、WS-X4148-RJ45(ハードウェア リビジョン 3.0 以上)、および WS-X4232-GB-RJ45(ハードウェア リビジョン 3.0 以上)は、CLI を使用して銅製メディア ポート の Auto-MDIX を サポートします。

表 6-1 に、Auto-MDIX 設定と、正常および誤ったケーブル配線の結果によるリンク状態を示します。

表 6-1 リンク状態および Auto-MDIX 設定

ローカル側の Auto-MDIX	リモート側の Auto-MDIX	正常なケープル配線	誤ったケーブル配線
オン	オン	リンク アップ	リンク アップ
オン	オフ	リンク アップ	リンク アップ
オフ	オン	リンク アップ	リンク アップ
オフ	オフ	リンク アップ	リンク ダウン

ポート上で Auto-MDIX を設定にするには、次の手順を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	Switch(config)# interface interface-id	設定する物理インターフェイスに対して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	Switch(config-if)# speed auto	接続されたデバイスの速度を自動ネゴシエートする ようポートを設定します。
ステップ 4	Switch(config-if)# mdix auto	ポートで Auto-MDIX をイネーブルにします。
ステップ 5	Switch(config-if)# end	特権 EXEC モードに戻ります。
ステップ 6	Switch# show interfaces interface-id	インターフェイス上の Auto-MDIX 機能の設定を確認します。
ステップ 7	Switch# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を 保存します。

Auto-MDIX をディセーブルにするには、no mdix auto インターフェイス コンフィギュレーションコマンドを使用します。

次に、ポート上で Auto-MDIX をイネーブルにする例を示します。

Switch# configure terminal
Switch(config)# interface fastethernet 6/5
Switch(config-if)# speed auto
Switch(config-if)# mdix auto
Switch(config-if)# end

インターフェイスの Auto-MDIX 設定の表示

インターフェイスのインターフェイス速度とデュプレックス モード設定を表示するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch> enable	特権 EXEC モードをイネーブルにします。
		• プロンプトが表示されたら、パスワードを入力 します。
ステップ 2	Switch# show interfaces type slot/interface	インターフェイスの Auto-MDIX 設定と動作ステー
		トを表示します。

サポートされたラインカードインターフェイスでの speed auto および mdix auto コマンドの設定方法によって、show interfaces コマンドでは異なる Auto-MDIX ステータスが表示されます。

表 6-2 に、Auto-MDIX 設定と動作ステート、および Auto-MDIX ステータスを示します。

表 6-2 Auto-MDIX および動作ステート

インターフェイス上の Auto-MDIX 設定 および動作ステート	説明
Auto-MDIX on (operational : on)	Auto-MDIX はイネーブルで、完全に機能しています。
Auto-MDIX on (operational : off)	このインターフェイスでは Auto-MDIX はイネーブルですが、機能していません。Auto-MDIX 機能を正常に動作させるには、インターフェイス速度を自動ネゴシエーションに設定する必要があります。
Auto-MDIX off	no mdix auto コマンドにより、Auto-MDIX はディセーブルにされています。

次に、インターフェイス FastEthernet 6/1 で Auto-MDIX 設定と動作ステートを表示する例を示します。

```
Switch# show interfaces fastethernet 6/1
FastEthernet6/1 is up, line protocol is up (connected)
 Hardware is Fast Ethernet Port, address is 0001.64fe.e5d0 (bia 0001.64fe.e5d0)
 MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
 Keepalive set (10 sec)
  Full-duplex, 100Mb/s, link type is auto, media type is 10/100BaseTX
  input flow-control is unsupported output flow-control is unsupported
  Auto-MDIX on (operational: on)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:16, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    511 packets input, 74464 bytes, 0 no buffer
     Received 511 broadcasts (511 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
    3552 packets output, 269088 bytes, 0 underruns
     O output errors, O collisions, O interface resets
     0 babbles, 0 late collision, 0 deferred
     1 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Switch#

OIR の概要

Catalyst 4500 シリーズ スイッチでは活性挿抜 (Online Insertion and Removal; OIR)機能がサポートされているため、システムをオンラインにしたままモジュールの取り外しおよび交換を行うことができます。モジュールをシャットダウンしてから取り外しおよび交換を行い、そのあとで再起動しても、他のソフトウェアまたはインターフェイスはシャットダウンされません。

モジュールの取り外しまたは取り付けを行うとき、事前にソフトウェアに通知するコマンドを入力する必要はありません。モジュールの取り外しまたは取り付けはシステムからスーパーバイザエンジンに通知され、システムが設定変更をスキャンします。新しく取り付けられたモジュールは初期化され、システム設定について各インターフェイスタイプが確認されてから、新しいインターフェイスで診断が実行されます。モジュールの取り外しまたは取り付け中に、通常の動作が中断されることはありません。

モジュールを取り外してから交換する場合、または同じタイプの別のモジュールを同じスロットに 装着する場合、システム設定への変更は必要ありません。それまで設定されていたタイプのイン ターフェイスは、すぐにオンラインで有効になります。モジュールを取り外し、別のタイプのモジュールを装着する場合、そのモジュールのインターフェイスはそのモジュールのデフォルト設定で管理上のアップになります。

インターフェイスのモニタリングおよびメンテナンス

ここではインターフェイスのモニタリングとメンテナンスの方法について説明します。

- インターフェイスとコントローラのステータスのモニタリング (p.6-31)
- インターフェイスのクリアとリセット (p.6-31)
- インターフェイスのシャットダウンおよび再起動(p.6-32)
- インターフェイス リンク ステータス イベントおよびトランク ステータス イベントの設定 (p.6-33)
- デフォルト設定へのインターフェイスのリセット (p.6-35)

インターフェイスとコントローラのステータスのモニタリング

Catalyst 4500 シリーズ スイッチの Cisco IOS ソフトウェアには、インターフェイスに関する情報(ソフトウェアおよびハードウェアのバージョン、コントローラのステータス、インターフェイス統計情報など)を表示するためのコマンドが準備されています。これらのコマンドは、EXEC プロンプトで入力します。次の表に、インターフェイスを監視するためのコマンドをいくつか紹介します(show コマンドのすべてのリストを表示するには、EXEC プロンプトで show?コマンドを入力します)。これらのコマンドについての詳細は、『Interface Command Reference』を参照してください。

インターフェイスに関する情報を表示するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# show interfaces [type slot/interface]	すべてのインターフェイスまたは特定のインターフェイスについて、ステータスおよび設定を表示します。
ステップ 2	Switch# show running-config	RAM で現在実行中のコンフィギュレーションを表示します。
ステップ 3	Switch# show protocols [type slot/interface]	設定されている任意のプロトコルについて、グロー バル (システム全体) およびインターフェイス固有 のステータスを表示します。
ステップ 4	Switch# show version	ハードウェア構成、ソフトウェア バージョン、コンフィギュレーション ファイルの名前とソース、およびブート イメージを表示します。

次に、インターフェイス FastEthernet 5/5 のステータスを表示する例を示します。

Switch# show protocols fastethernet 5/5
FastEthernet5/5 is up, line protocol is up
Switch#

インターフェイスのクリアとリセット

show interfaces コマンドで表示されるインターフェイス カウンタをクリアするには、次のコマンドを入力します。

コマンド	目的
Switch# clear counters {type slot/interface}	インターフェイス カウンタをクリアしま
	9 .

次に、インターフェイス FastEthernet 5/5 のカウンタをクリアしてリセットする例を示します。

Switch# clear counters fastethernet 5/5
Clear "show interface" counters on this interface [confirm] y
Switch#
*Sep 30 08:42:55: %CLEAR-5-COUNTERS: Clear counter on interface FastEthernet5/5
by vty1 (171.69.115.10)
Switch#

clear counters コマンド(引数なし)は、すべてのインターフェイスの現在のインターフェイス カウンタをすべてクリアします。



clear counters コマンドは、SNMP (簡易ネットワーク管理プロトコル)で取得されたカウンタをクリアしません。show interfaces EXEC コマンドで表示されたカウンタのみをクリアします。

インターフェイスのシャットダウンおよび再起動

インターフェイスをディセーブルにすると、指定したインターフェイス上のすべての機能がディセーブルになり、そのインターフェイスはすべてのモニタコマンド出力で使用不能として表示されます。この情報は、すべてのダイナミックルーティングプロトコルを通じて他のネットワークサーバに通知されます。このインターフェイスは、ルーティングアップデートに含まれなくなります。

インターフェイスをシャットダウンしたあとで再起動するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# interface {vlan vlan_ID} {{fastethernet gigabitethernet tengigabitethernet} slot/port} {port-channel port_channel_number}	設定するインターフェイスを指定します。
ステップ 2	Switch(config-if)# shutdown	インターフェイスをシャットダウンします。
ステップ 3	Switch(config-if)# no shutdown	インターフェイスをふたたびイネーブルにします。

次に、インターフェイス FastEthernet 5/5 をシャットダウンする例を示します。

Switch(config) # interface fastethernet 5/5
Switch(config-if) # shutdown
Switch(config-if) #
*Sep 30 08:33:47: %LINK-5-CHANGED: Interface FastEthernet5/5, changed state to a administratively down
Switch(config-if) #

次に、インターフェイス FastEthernet 5/5 を再びイネーブルにする例を示します。

Switch(config-if)# no shutdown
Switch(config-if)#
*Sep 30 08:36:00: %LINK-3-UPDOWN: Interface FastEthernet5/5, changed state to up
Switch(config.if)#

インターフェイスがディセーブルになったかどうかを確認するには、show interfaces EXEC コマンドを入力します。シャット ダウンされたインターフェイスは、[administratively down] と表示されます。

インターフェイス リンク ステータス イベントおよびトランク ステータス イベントの設 定

インターフェイス リンク ステータス イベントおよびトランク ステータス イベントを設定できます。Catalyst 4500 シリーズ スイッチでは、次のインターフェイス ロギング イベント通知がグローバルおよびインターフェイス単位の両方でサポートされます。

- データ リンク ステータスが変更された場合は、常にインターフェイス上の通知がイネーブル またはディセーブルになります。
- トランキング ステータスが変更された場合は、常にトランク インターフェイス上の通知がイネーブルまたはディセーブルになります。

インターフェイス リンク ステータス イベントをイネーブルまたはディセーブルにするには、[no] logging event link-status [use-global] コマンドを使用します。インターフェイス トランク ステータス イベントをイネーブルまたはディセーブルにするには、[no] logging event trunk-status [use-global] コマンドを使用します。

各インターフェイス リンク ステータス ロギング イベントは、次のステートのいずれかで設定できます。

- logging event link-status リンク ステータス ロギング イベントは、スイッチのグローバル設 定に関係なく、インターフェイス上で明示的にイネーブルになります。
- no logging event link-status リンク ステータス ロギング イベントは、スイッチのグローバル 設定に関係なく、インターフェイス上で明示的にディセーブルになります。
- logging event link-status use-global これは、インターフェイス上のデフォルトのリンク ステータス ロギング イベント設定です。この設定は、スイッチのグローバルなリンク ステータス ロギング イベント設定に従う必要があります。

インターフェイス トランク ステータス ロギング イベントは、同じ設定ステートで設定できます。

インターフェイスのリンク ステータス イベント通知の設定

リンク ステータス ロギング イベントをイネーブルまたはディセーブルにするには、次のいずれかのコマンドを入力します。

コマンド	目的
Switch(config-if)# logging event link-status	インターフェイス リンク ステータス ロギングをイネーブルにします。
Switch(config-if)# no logging event link-status	インターフェイス リンク ステータス ロギングを ディセーブルにします。
Switch(config-if)# logging event link-status use-global	インターフェイス リンク ステータス ロギングのグローバルなデフォルト設定を指定します。

グローバルな設定

対応するロギング イベントは、グローバルに設定することもできます。グローバルな設定により、すべてのインターフェイスにデフォルト ロギング設定が提供されます。[no] logging event link-status global コマンドにより、スイッチ全体のインターフェイス リンク ステータス ロギングをイネーブルまたはディセーブルにできます。[no] logging event trunk-status global コマンドにより、スイッチ全体のインターフェイス トランク ステータス ロギングをイネーブルまたはディセーブルにできます。

各インターフェイス リンク ステータス ロギング イベントがインターフェイス レベルで設定され ていない場合、次のグローバルなロギング イベント設定を使用します。

- logging event link-status global リンク ステータス ロギング イベントがインターフェイス上 で設定されていない場合、イネーブルになります。
- no logging event link-status global リンク ステータス ロギング イベントがインターフェイス 上で設定されていない場合、ディセーブルになります。

インターフェイスのトランク ステータス ロギング イベントにも、同様のグローバル設定が提供されます。

スイッチのグローバル リンク ステータス ロギング イベントの設定

グローバル リンク ステータス ロギング イベントをイネーブルまたはディセーブルにするには、次のいずれかのコマンドを入力します。

コマンド	目的
Switch(config-if)# logging event link-status global	グローバル リンク ステータス ロギングをイネーブ ルにします。
Switch(config-if)# no logging event link-status global	グローバル リンク ステータス ロギングをディセー ブルにします。

結果

次に、グローバル設定およびインターフェイス ロギング設定の組み合わせが異なる場合のインターフェイス ロギング イベントの動作ステートの要約例を表示します。

global setting	interface setting	actual logging state
on	on	on
off	on	on
on	off	off
off	off	off
on	default(use-glob	oal) on
off	default(use-glob	oal) off

次に、リンク ステータスおよびトランク ステータスのロギング イベントの設定およびロギング メッセージの出力例を表示します。

```
// The global link status and trunk status logging events are enabled.
Switch# show running | include logging
show running | include logging
logging event link-status global
logging event trunk-status global
Switch#
// The interface link status and trunk status logging settings
// are set to default values, which follow regardless of the global
// setting.
//
Switch# show running interface g1/4
Building configuration...
Current configuration: 97 bytes
interface GigabitEthernet1/4
switchport trunk encapsulation dot1q
switchport mode trunk
end
Switch#
\ensuremath{//} The trunk status logging messages for the interface are
// displayed whenever the interface trunking status is changed.
// Here we change the other end node's trunking encapsulation
// from dot1q to is1.
3d00h: %DTP-5-ILGLCFG: Illegal config(on,isl--on,dot1q) on Gi1/4
3d00h: %DTP-5-ILGLCFG: Illegal config(on,isl--on,dot1g) on Gi1/4
3d00h: %DTP-5-ILGLCFG: Illegal config(on,isl--on,dot1q) on Gi1/4
\ensuremath{//} The link and trunk status logging message for the interface
// are displayed whenever the interface link status is changed.
// Here we do a "shut" and "no shut" on the other end link node.
3d00h: %DTP-5-NONTRUNKPORTON: Port Gi1/4 has become non-trunk
3d00h: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet1/4, changed state to down
3d00h: %LINK-3-UPDOWN: Interface GigabitEthernet1/4, changed state to
3d00h: %LINK-3-UPDOWN: Interface GigabitEthernet1/4, changed state to up
3d00h: %DTP-5-TRUNKPORTON: Port Gi1/4 has become dot1q trunk
3d00h: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet1/4, changed state to up
```

デフォルト設定へのインターフェイスのリセット

インターフェイスに多くのコマンド ラインを設定し、そのインターフェイスのすべての設定をクリアする場合、default interface グローバル コンフィギュレーション コマンドを使用します。

Switch(config)# **default interface fastEthernet 3/5**Interface FastEthernet3/5 set to default configuration

このコマンドを使用すると、すべての設定をクリアし、インターフェイスをシャットダウンすることができます。

Switch# show run interface fastethernet 3/5
Building configuration...

Current configuration : 58 bytes
!
interface FastEthernet3/5
no ip address
shutdown
end



CHAPTER

7

ポートのステータスと接続の確認

この章では、Catalyst 4500 シリーズ スイッチ上でスイッチ ポートのステータスと接続を確認する方法について説明します。

この章の主な内容は、次のとおりです。

- モジュール ステータスの確認 (p.7-2)
- インターフェイスのステータスの確認 (p.7-3)
- MAC アドレスの表示 (p.7-4)
- TDR を使用したケーブル ステータスの確認 (p.7-5)
- Telnet の使用 (p.7-7)
- ログアウト タイマーの変更 (p.7-7)
- ユーザ セッションのモニタリング (p.7-8)
- ping の使用 (p.7-9)
- IP traceroute の使用 (p.7-10)
- レイヤ 2 traceroute の使用 (p.7-11)
- ICMP の設定 (p.7-13)



この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/cr/index.htm

モジュール ステータスの確認

Catalyst 4500 シリーズ スイッチはマルチモジュール システムです。取り付けられているモジュール、および各モジュールの MAC(メディア アクセス制御)アドレス範囲とバージョン番号は、show module コマンドを使用して確認します。特定のモジュール番号を指定して、そのモジュールの詳細な情報を表示するには、 $[mod_num]$ 引数を使用します。

次に、スイッチ上のすべてのモジュール ステータスを確認する例を示します。

Switch# show module all

Mod	Ports	Card Type				Model		Serial	No.
	+	+				+		+	
1	2	1000BaseX (G	BIC) Supervis	or N	Module	WS-X4014	Į	JAB0123	845AB
5	24	10/100/1000B	aseTX (RJ45)			WS-X4424	-GB-RJ45	JAB0453	04EY
6	6 48 10/100BaseTX (RJ45)				WS-X4148	3	JAB0234	102QK	
M M	AC add	resses		Hw	Fw		Sw		Stat
+-			+		+				
1 0	004.dd	46.9f00 to 00	04.dd46.a2ff	0.0	12.1(10r)	EW(1.21)	12.1(10)E	EW (1)	Ok
5 0	050.3e	7e.1d70 to 00	50.3e7e.1d87	0.0					Ok
6 0	050.0f	10.2370 to 00	50.0f10.239f	1.0					Ok
Swit	Switch#								

インターフェイスのステータスの確認

スイッチ ポートの要約または詳細情報を表示する場合は、show interfaces status コマンドを使用します。スイッチのすべてのポートの要約情報を参照するには、引数なしの show interfaces status コマンドを入力します。特定のモジュール番号を指定すると、そのモジュールのポート情報のみが表示されます。特定のポートの詳細情報を表示するには、モジュール番号とポート番号を入力します。

特定のポートにコンフィギュレーション コマンドを適用するには、適切な論理モジュールを指定する必要があります。詳細については、「モジュールステータスの確認」(p.7-2)を参照してください。

次に、トランシーバを含む Catalyst 4500 シリーズ スイッチ上のすべてのインターフェイスのステータスを表示する例を示します。このコマンドの出力では、他社製トランシーバの「未承認の GBIC」を表示します。

Switch#show interfaces status

Port	Name	Status	Vlan	Duplex	Speed	Type
Gi1/1		notconnect	1	auto	auto	No Gbic
Gi1/2		notconnect	1	auto	auto	No Gbic
Gi5/1		notconnect	1	auto	auto	10/100/1000-TX
Gi5/2		notconnect	1	auto	auto	10/100/1000-TX
Gi5/3		notconnect	1	auto	auto	10/100/1000-TX
Gi5/4		notconnect	1	auto	auto	10/100/1000-TX
Fa6/1		connected	1	a-full	a-100	10/100BaseTX
Fa6/2		connected	2	a-full	a-100	10/100BaseTX
Fa6/3		notconnect	1	auto	auto	10/100BaseTX
Fa6/4		notconnect	1	auto	auto	10/100BaseTX

Switch#

次に、errdisable ステートのインターフェイスのステータスを表示する例を示します。

Switch# show interfaces status err-disabled

Port Name Status Reason Fa9/4 err-disabled link-flap

informational error message when the timer expires on a cause $% \left(1\right) =\left(1\right) \left(1\right$

 $5d04h: PM-SP-4-ERR_RECOVER: Attempting to recover from link-flap err-disable state on Fa9/4 Switch#$

MAC アドレスの表示

show module コマンドを使用してモジュールの MAC アドレス範囲を表示する以外に、show mac-address-table address コマンドと show mac-address-table interface コマンドを使用して、特定の MAC アドレスまたはスイッチの特定のインターフェイスの MAC アドレステーブル情報を表示できます.

次に、特定の MAC アドレスの MAC アドレス テーブル情報を表示する例を示します。

Switch# show mac-address-table address 0050.3e8d.6400

DWILL	IIT SHOW MAC-AUGI	ess-capie	address 0	030.	Je04.0400	
	mac address +		-	_		-
	0050.3e8d.6400					
100	0050.3e8d.6400	static	assigned		Switch	
5	0050.3e8d.6400	static	assigned		Switch	
4	0050.3e8d.6400	static	ipx		Switch	
1	0050.3e8d.6400	static	ipx		Switch	
1	0050.3e8d.6400	static	assigned		Switch	
4	0050.3e8d.6400	static	assigned		Switch	
5	0050.3e8d.6400	static	ipx		Switch	
100	0050.3e8d.6400	static	ipx		Switch	
200	0050.3e8d.6400	static	ipx		Switch	
100	0050.3e8d.6400	static	other		Switch	
200	0050.3e8d.6400	static	other		Switch	
5	0050.3e8d.6400	static	other		Switch	
4	0050.3e8d.6400	static	ip		Switch	
1	0050.3e8d.6400	static	ip		Route	
1	0050.3e8d.6400	static	other		Switch	
4	0050.3e8d.6400	static	other		Switch	
5	0050.3e8d.6400	static	ip		Switch	
200	0050.3e8d.6400	static	ip		Switch	
100	0050.3e8d.6400	static	ip		Switch	
Switcl	h#					

次に、特定のインターフェイスの MAC アドレス テーブル情報を表示する例を示します。

```
Switch# show mac-address-table interface gigabit 1/1 Multicast Entries
```

vlan mac address type ports

1 ffff.ffff.ffff system Switch,Gi6/1,Gi6/2,Gi6/9,Gi1/1
Switch#

TDR を使用したケーブル ステータスの確認

リンクを確立できない場合に、Time Domain Reflectometer (TDR; タイム ドメイン反射率測定)機能を使用してケーブル接続に障害があるかどうかを判別できます。



(注)

このテストは、既存スイッチの交換、ギガビット イーサネットへのアップグレード、または新しいケーブル プラントの敷設の際に特に重要となります。

概要

Catalyst 4500 シリーズ スイッチの 48 ポート 10/100/1000BASE-T モジュール (WS-X4548-GB-RJ45、WS-X4548-GB-RJ45V、WS-X4524-GB-RJ45V、WS-X4013+TS、WS-C4948、および WS-C4948-10GE) では、TDR を使用して銅ケーブルのステータスを確認できます。TDR は、信号をケーブルに送信し、反射して戻ってきた信号を読み取ることによりケーブルの障害を検出します。信号のすべてまたは一部は、ケーブルの障害箇所またはケーブルの終端により反射して戻されます。



(注)

標準のカテゴリ 5 ケーブルには 4 つのペアがあります。各ペアは、次のステート(オープン [接続されていない] 損傷、ショート、または終端)のいずれかであると想定できます。TDR テストでは 4 つすべてのステートを検出し、最初の 3 つの状態を [Fault] と表示し、4 番めの状態を [Terminated] と表示します。CLI(コマンドラインインターフェイス)出力は表示されますが、ケーブル長はステートが [Faulty] の場合にのみ表示されます。

TDR テストの実行

TDR テストを開始するには、特権モードで次の作業を実行します。

	コマンド	目的
ステップ 1	Switch# test cable-diagnostics tdr {interface {interface interface-number}}	TDR テストを開始します。
ステップ 2	Switch# show cable-diagnostics tdr {interface {interface interface-number}}	TDR テストのカウンタ情報を表示します。

次に、モジュール 2 のポート 1 上で TDR テストを開始する例を示します。

Switch# test cable-diagnostics tdr int gi2/1 Switch#

次に、モジュールで TDR テストがサポートされていない場合に表示されるメッセージ例を示します。

Switch# test cable-diagnostics tdr int gi2/1 00:03:15:%C4K_IOSDIAGMAN-4-TESTNOTSUPPORTEDONMODULE: Online cable diag tdr test is not supported on this module Switch#

次に、ポートの TDR テストの結果を表示する例を示します。

Switch# show cable-diagnostics tdr interface gi4/13

Interface	Speed	Local pair	Cable length	Remote channel	Status
Gi4/13	0Mbps	1-2	102 + -2m	Unknown	Fault
		3-6	100 + -2m	Unknown	Fault
		4-5	102 + -2m	Unknown	Fault
		7-8	102 +-2m	Unknown	Fault



このコマンドは、Cisco IOS ソフトウェアの将来のリリースでは廃止される予定です。TDR テストを実行し、テスト結果を表示するには、diagnostic start および **show diagnostic result** コマンドを使用してください。



注) TDR は、ポートのテストです。ポートは、テストの実行中(通常、1分間)はトラフィックを処理 できません。

注意事項

TDR を使用する場合は、次の注意事項が適用されます。

- TDR テストを実行中のポートと Auto-MDIX がイネーブルのポートを接続した場合、この TDR 結果は無効となる可能性があります。この場合、TDR テストを開始する前に WS-X4148-RJ45V 上のポートを管理上のダウンにする必要があります。
- TDR テストを実行中のポートと WS-X4148-RJ45V 上のポートなど 100BASE-T ポートを接続する場合、未使用のペア (4-5 および 7-8) はリモート エンドで終端処理されないため、障害としてレポートされます。
- TDR テストの実行中はポート設定を変更しないでください。
- ケーブルの特性から、正確な結果を入手するには TDR テストを複数回行う必要があります。
- (近端または遠端のケーブルを取り外すなど)ポート ステータスを変更しないでください。結果が不正確となる可能性があります。

Telnet の使用

スイッチの CLI には、Telnet を使用してアクセスできます。また、スイッチから Telnet を使用して、ネットワークの他のデバイスにアクセスすることも可能です。最大 8 つの Telnet セッションを同時に実行できます。

スイッチとの Telnet セッションを設定する前に、まずスイッチの IP アドレス (場合によりデフォルト ゲートウェイも)を設定する必要があります。IP アドレスとデフォルト ゲートウェイの設定方法については、第3章「スイッチの初期設定」を参照してください。



ホスト名を使用してホストとの Telnet 接続を確立するには、Domain Name System (DNS; ドメインネーム システム) を設定してイネーブルにします。

スイッチからネットワーク上の別のデバイスへの Telnet 接続を確立するには、次の作業を行います。

コマンド	目的
Switch# telnet host [port]	リモート ホストとの Telnet セッションを確立します。

次に、スイッチからリモート ホスト labsparc への Telnet 接続を確立する例を示します。

Switch# telnet labsparc
Trying 172.16.10.3...
Connected to labsparc.
Escape character is '^]'.
UNIX(r) System V Release 4.0 (labsparc)
login:

ログアウト タイマーの変更

ログアウト タイマーは、ユーザが指定された時間よりも長くアイドル状態にあるとき、自動的にスイッチから切断します。 ログアウト タイマーを設定するには、次の作業を行います。

コマンド	目的
	ログアウト タイマーの値を変更します(タイムアウト値に 0 を指定すると、アイドル状態のセッションが自動的に切断されるのを防ぎます)。
	デフォルト値に戻すには、no キーワードを使用します。

ユーザ セッションのモニタリング

スイッチ上で現在アクティブなユーザ セッションを表示するには、show users コマンドを使用します。このコマンドは、スイッチでアクティブなすべてのコンソール ポートと Telnet セッションのリストを出力します。

スイッチのアクティブなユーザ セッションを表示するには、特権 EXEC モードで次の作業を行います。

コマンド	目的
Switch# show users [all]	スイッチで現在アクティブなユーザ セッションを表示し
	ます。

次に、コンソールと Telnet セッションでローカル認証がイネーブルの場合の、show users コマンドの出力例を示します (アスタリスク [*] が現在のセッションを示します)。

Switch# show	users				
Line	User	Host(s)	Idle	Location	
* 0 con 0		idle	00:00:00		
Interface	User	Mode	Id	le Pee	r Address
Switch# show	users all				
Line	User	Host(s)	Idle	Location	
* 0 con 0		idle	00:00:00		
1 vty 0			00:00:00		
2 vty 1			00:00:00		
3 vty 2			00:00:00		
4 vty 3			00:00:00		
5 vty 4			00:00:00		
Interface Switch#	User	Mode	Id	le Pee	r Address

アクティブなユーザ セッションを切断するには、次の作業を行います。

コマンド	目的
Switch# disconnect {console ip_addr}	スイッチのアクティブなユーザ セッションを切断しま
	す。

次に、アクティブなコンソール ポートのセッションとアクティブな Telnet セッションを切断する例を示します。

```
Switch> disconnect console

Console session disconnected.

Console> (enable) disconnect tim-nt.bigcorp.com

Telnet session from tim-nt.bigcorp.com disconnected. (1)

Switch# show users

Session User Location

telnet jake jake-mac.bigcorp.com

* telnet suzy suzy-pc.bigcorp.com

Switch#
```

ping の使用

ここでは、IP ping を使用する手順について説明します。

- ping の機能(p.7-9)
- ping の実行 (p.7-9)

ping の機能

ping コマンドを使用すると、リモート ホストとの接続を確認できます。異なる IP サブネットワークのホストに ping を実行する場合、ネットワークへのスタティック ルートを定義するか、サブネット間をルーティングするルータを設定する必要があります。

ping コマンドは、ユーザ モードおよび特権 EXEC モードから設定できます。ping は次のいずれかの応答を返します。

- 通常の応答 ネットワーク トラフィックに応じて、1 ~ 10 秒間通常の応答(hostname が有効) が行われます。
- 宛先の応答なし ホストが応答しない場合、No Answer メッセージが返されます。
- ホスト不明 ホストが存在していない場合、Unknown Host メッセージが返されます。
- 宛先到達不能 デフォルト ゲートウェイが指定されたネットワークに到達できない場合、 Destination Unreachable メッセージが返されます。
- ネットワークまたはホスト到達不能 ホストまたはネットワークにルート テーブルが存在しない場合、Network または Host Unreachable メッセージが返されます。

実行中の ping を停止するには、Ctrl-C を押します。

ping の実行

スイッチからネットワーク上の別のデバイスに ping を実行するには、ユーザ モードおよび特権 EXEC モードで次の作業を行います。

コマンド	目的
Switch# ping host	リモート ホストとの接続を確認します。

次に、ユーザ モードからリモート ホストに ping を実行する例を示します。

Switch# ping labsparc labsparc is alive Switch> ping 72.16.10.3 12.16.10.3 is alive Switch#

次に、パケット数、パケット サイズ、タイムアウト時間を指定して、特権 EXEC モードで ping コマンドを入力する例を示します。

```
Switch# ping
Target IP Address []: 12.20.5.19
Number of Packets [5]: 10
Datagram Size [56]: 100
Timeout in seconds [2]: 10
Source IP Address [12.20.2.18]: 12.20.2.18
!!!!!!!!!
----12.20.2.19 PING Statistics----
10 packets transmitted, 10 packets received, 0% packet loss round-trip (ms) min/avg/max = 1/1/1
Switch
```

IP traceroute の使用

ここでは、IP traceroute 機能を使用する手順について説明します。

- IP traceroute の機能 (p.7-10)
- IP traceroute の実行 (p.7-10)

IP traceroute の機能

ネットワークでパケットがホップ単位で通過するパスを識別する場合は、IP traceroute を使用します。このコマンドは、トラフィックが宛先に到達するまでに通過する、ルータなどのすべてのネットワーク レイヤ (レイヤ 3) デバイスを出力します。

レイヤ 2 スイッチは、trace コマンドの送信元または宛先として参加できますが、trace コマンド出力ではホップとして表示されません。

trace コマンドは IP ヘッダーの Time To Live (TTL; 存続可能時間) フィールドを使用して、ルータとサーバで特定のリターン メッセージが生成されるようにします。traceroute はまず TTL フィールドを 1 に設定して、宛先ホストに UDP データグラムを送信します。ルータが 1 または 0 の TTL 値を検出すると、ルータはデータグラムをドロップして Internet Control Message Protocol (ICMP; インターネット制御メッセージ プロトコル) Time-Exceeded メッセージを送信側に返します。traceroute は、ICMP Time-Exceeded メッセージの送信元アドレス フィールドを調べて、最初のホップのアドレスを判断します。

次のホップを確認するために、traceroute は TTL 値を 2 に設定して UDP パケットを送信します。最初のルータは TTL フィールドの値を 1 だけ減らし、次のルータにデータグラムを送信します。2 番めのルータは TTL の値 1 を確認し、データグラムをドロップして、送信元に Time-Exceeded メッセージを返します。このプロセスは、データグラムが宛先ホストに到達できるだけの値まで TTL が増加するか、最大 TTL に到達するまで続けられます。

データグラムが宛先に到達したことを判断するために、traceroute はデータグラムの UDP 宛先ポートを宛先ホストが使用すると予測される非常に大きな値に設定します。ホストが未確認のポート番号を指定したデータグラムを受け取ると、送信元に ICMP Port Unreachable エラー メッセージを送信します。Port Unreachable エラー メッセージは、宛先に到達していることを traceroute に通知します。

IP traceroute の実行

パケットがネットワークで通過するパスを追跡するには、EXEC モードまたは特権 EXEC モードで次の作業を行います。

コマンド	目的
Switch# trace [protocol] [destination]	IP traceroute を実行して、ネットワークでパケットが通過
	するパスを追跡します。

次に、trace コマンドを使用して、パケットがネットワークで宛先に到達するまでのルートを表示する例を示します。

Switch# trace ip ABA.NYC.mil

Type escape sequence to abort.

Tracing the route to ABA.NYC.mil (26.0.0.73)

- 1 DEBRIS.CISCO.COM (192.180.1.6) 1000 msec 8 msec 4 msec
- 2 BARRNET-GW.CISCO.COM (192.180.16.2) 8 msec 8 msec 8 msec
- 3 EXTERNAL-A-GATEWAY.STANFORD.EDU (192.42.110.225) 8 msec 4 msec 4 msec
- 4 BB2.SU.BARRNET.NET (192.200.254.6) 8 msec 8 msec 8 msec
- 5 SU.ARC.BARRNET.NET (192.200.3.8) 12 msec 12 msec 8 msec
- 6 MOFFETT-FLD-MB.in.MIL (192.52.195.1) 216 msec 120 msec 132 msec
- 7 ABA.NYC.mil (26.0.0.73) 412 msec 628 msec 664 msec

Switch#

レイヤ 2 traceroute の使用

レイヤ2 traceroute 機能により、スイッチはパケットが送信元デバイスから宛先デバイスへ送信され る間に通過する物理パスを識別できます。レイヤ 2 traceroute は、ユニキャスト送信元および宛先 MAC アドレスにのみ対応します。パス内のスイッチが保持する MAC アドレス テーブルを使用し てパスを判別します。スイッチがレイヤ 2 traceroute をサポートしないデバイスをパス内で検出した 場合、スイッチはレイヤ2に追跡クエリーを送信し続けてタイムアウトにします。

スイッチが送信元デバイスのホストから宛先デバイスのホストへのパスを追跡する場合、スイッチ は送信元デバイスから宛先デバイスへのパスのみを識別します。パケットが送信元ホストから送信 元デバイス、または宛先デバイスから宛先ホストへ送信される場合に通過するパスを識別すること はできません。

ここでは、レイヤ2 traceroute 機能を使用する手順について説明します。

- レイヤ 2 traceroute の使用上の注意事項 (p.7-11)
- レイヤ 2 traceroute の実行 (p.7-12)

レイヤ 2 traceroute の使用上の注意事項

レイヤ 2 traceroute の使用上の注意事項は次のとおりです。

Cisco Discovery Protocol (CDP; シスコ検出プロトコル)は、ネットワーク上のすべてのデバイ スでイネーブルになっている必要があります。レイヤ2 traceroute を適切に機能させるために、 CDP をディセーブルにしないでください。

物理パス内のいずれかのデバイスが CDP に対してトランスペアレントである場合、スイッチは このデバイスを通過するパスを識別できません。



(注) CDP のイネーブル化の詳細については、第 24 章「CDP の設定」を参照してください。

- 物理パス内のすべてのスイッチは IP 接続が可能でなければなりません。 スイッチが別のスイッ チから到達可能である場合、特権 EXEC モードで ping コマンドを使用して接続をテストでき ます。
- パス内で識別可能な最大ホップ数は10です。
- 送信元デバイスから宛先デバイスへの物理パスにないスイッチにおいて、特権 EXEC モードで traceroute mac または traceroute mac ip コマンドを入力できます。物理パス内のすべてのスイッ チはこのスイッチから到達可能でなければなりません。
- 指定した送信元および宛先 MAC アドレスが同一 VLAN (仮想 LAN)に属している場合のみ、 traceroute mac コマンド出力はレイヤ 2 パスを表示します。異なる VLAN に属する送信元およ び宛先 MAC アドレスを指定した場合、レイヤ 2 パスは識別されず、エラー メッセージが表示 されます。
- マルチキャスト送信元または宛先 MAC アドレスを指定した場合、レイヤ 2 パスは識別されず、 エラー メッセージが表示されます。
- 送信元または宛先 MAC アドレスが複数の VLAN に属している場合、送信元および宛先 MAC アドレスの両方が属する VLAN を指定しなければなりません。このような VLAN を指定しな いと、レイヤ2パスは識別されず、エラーメッセージが表示されます。
- 指定した送信元および宛先 IP アドレスが同一サブネットに属している場合、traceroute mac ip コマンド出力はレイヤ2パスを表示します。IPアドレスを指定する場合、スイッチはAddress Resolution Protocol (ARP: アドレス 解決 プロトコル) を使用して IP アドレスと対応する MAC アドレスおよび VLAN ID を対応付けます。

- 指定した IP アドレスに対して ARP エントリが存在する場合、スイッチは関連 MAC アドレスを使用して物理パスを識別します。
- ARP エントリがない場合、スイッチは ARP クエリーを送信して IP アドレスを解決しよう とします。IP アドレスが解決されない場合、レイヤ 2 パスは識別されず、エラー メッセー ジが表示されます。
- 複数のデバイスがハブを通じて1つのポートに接続されている場合(たとえば、複数のCDPネイバーがポートで検出される場合)レイヤ2 traceroute 機能はサポートされません。複数のCDPネイバーが1つのポートで検出されると、レイヤ2パスは識別されず、エラーメッセージが表示されます。
- この機能は、トークンリング VLAN ではサポートされていません。

レイヤ 2 traceroute の実行

送信元デバイスから宛先デバイスへ送信されるパケットが通過する物理パスを表示するには、特権 EXEC モードで次の作業のいずれかを行います。

コマンド	目的
Switch# traceroute mac {source-mac-address}	レイヤ 2 traceroute を実行して、ネットワークで
$\{destination-mac-address\}$	パケットが通過するパスを追跡します。

または

コマンド	目的
Switch# traceroute mac ip {source-mac-address}	IP traceroute を実行して、ネットワークでパケッ
$\{destination-mac-address\}$	トが通過するパスを追跡します。

次に、traceroute mac および traceroute mac ip コマンドを使用して、パケットがネットワークを通じて宛先に到達するまでの物理パスを表示する例を示します。

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201
```

```
Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 (2.2.6.6) : Fa0/1 => Fa0/3
                     (2.2.5.5
                                     )
                                             Fa0/3 => Gi0/1
                                        :
con1
                     (2.2.1.1
                                     )
                                             Gi0/1 => Gi0/2
                     (2.2.2.2
                                     ) :
                                            Gi0/2 => Fa0/1
con2
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
Switch#
Switch# traceroute mac ip 2.2.66.66 2.2.22.22 detail
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201
Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 / WS-C2950G-24-EI / 2.2.6.6 :
       Fa0/1 [auto, auto] => Fa0/3 [auto, auto]
con5 / WS-C2950G-24-ET / 2.2.5.5 :
       Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
       Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
       Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
Switch#
```

ICMP の設定

ICMP は、IP 接続を制御および管理するための多くのサービスを提供します。インターネット ヘッダーに問題が検出された場合に、ICMP メッセージがルータまたはアクセス サーバによってホストまたはその他のルータに送信されます。ICMP の詳細については、RFC 792 を参照してください。

ICMP Protocol Unreachable メッセージのイネーブル化

Cisco IOS ソフトウェアが不明なプロトコルを使用する非ブロードキャスト パケットを受け取ると、送信元に ICMP Protocol Unreachable メッセージを返します。

同様に、宛先アドレスまでのルートを認識していないため最終的な宛先に届かないパケットをソフトウェアが受け取ると、送信元に ICMP Host Unreachable メッセージを返します。この機能は、デフォルトでイネーブルに設定されています。

ICMP Protocol Unreachable と Host Unreachable メッセージの生成をイネーブルにするには、インターフェイス コンフィギュレーション モードで次のコマンドを入力します。

コマンド	目的
Switch (config-if)# [no] ip unreachables	ICMP 宛先到達不能メッセージをイネーブルに します。
	ICMP 宛先到達不能メッセージをディセーブル にするには、no キーワードを使用します。



no ip unreachables コマンドを実行すると、「パス MTU 検出」機能が停止します。ネットワークの中のルータは、パケットを強制的に分割します。

ICMP 宛先到達不能メッセージが生成されるレートを制限するには、次の作業を行います。

コマンド	目的
unroaghable [dfl milligagands	ICMP 宛先メッセージが生成されるレートを制限します。
	レート制限を削除し、CPU 利用を低減させるには、no キーワードを使用します。

ICMP Redirect メッセージのイネーブル化

最適なデータルートが使用されない場合があります。たとえば、受信したその同じインターフェイスを使用したパケットの再送をルータに強制できます。この場合、Cisco IOS ソフトウェアはパケットの発信元に ICMP Redirect メッセージを送信して、ルータが受信デバイスに直接接続するサブネット上にあること、また、ルータは同じサブネット上の別のシステムにパケットを転送する必要があることを発信元に通知します。ソフトウェアはパケットの発信元に ICMP Redirect メッセージを送信します。これは発信側ホストがすでにネクストホップにそのパケットを送信し、それを発信元が全く認識していない可能性があるためです。Redirect メッセージは、ルートから受信デバイスを削除し、よりダイレクトなパスを示す指定されたデバイスに代えるよう送信側に指示します。この機能は、デフォルトでイネーブルに設定されています。

ただし、Hot Standby Router Protocol (HSRP; ホットスタンバイ ルータ プロトコル) がインターフェイスに設定されている場合、そのインターフェイスでは ICMP Redirect メッセージは (デフォルトで) ディセーブルになります。HSRP の詳細については、次の URL を参照してください。http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_c/ipcprt1/1cdip.htm

Cisco IOS ソフトウェアが受信したインターフェイスからパケットを再送するように指定されている場合、ICMP Redirect メッセージの送信をイネーブルにするには、インターフェイス コンフィギュレーション モードで次のコマンドを入力します。

コマンド	目的
Switch (config-if)# [no] ip redirects	ICMP Redirect メッセージをイネーブルにします。
	ICMP Redirect メッセージをディセーブルにし、 CPU 利用を低減させるには、 no キーワードを使 用します。

ICMP Mask Reply メッセージのイネーブル化

ネットワーク デバイスがインターネットワークの特定のサブネットワークに関して、サブネットマスクを認識していなければならない場合があります。この情報を取得するために、デバイスは ICMP Mask Request メッセージを送信します。これらのメッセージには、要求された情報を保有するデバイスの ICMP Mask Reply メッセージが応答します。Cisco IOS ソフトウェアは、ICMP Mask Reply 機能がイネーブルの場合に、ICMP Mask Request メッセージに応答できます。

Cisco IOS ソフトウェアが ICMP Mask Reply メッセージを送信して、ICMP マスク要求に応答するように指定するには、次の作業を行います。

コマンド	目的
Switch (config-if)# [no] ip mask-reply	ICMP 宛先マスク要求への応答をイネーブルに します。
	この機能をディセーブルにするには、no キー ワードを使用します。



CHAPTER

RPR および SSO を使用したスーパーバイザ エンジンの冗長設定

Catalyst 4500 シリーズ スイッチでは、アクティブ スーパーバイザ エンジンが故障した場合に、冗 長スーパーバイザ エンジンが処理を引き継ぎます。ソフトウェアでは、冗長スーパーバイザ エン ジンを Route Processor Redundancy (RPR) または Stateful Switchover (SSO) 動作モードで稼働する ことで、スーパーバイザエンジン冗長構成をイネーブルにします。



SSO を稼働する ROMMON 最小要件は、Cisco IOS Release 12.1(20r)EW1 または Cisco IOS Release 12.2(20r)EW1 です。

この章では、Catalyst 4507R および Catalyst 4510R スイッチ上でスーパーバイザ エンジンの冗長構 成を設定する方法について説明します。



Cisco Nonstop Forwarding (NSF) with SSO (NSF/SSO) の詳細については、第9章「Cisco NSF/SSO スーパーバイザエンジンの冗長構成の設定」を参照してください。

この章の主な内容は、次のとおりです。

- スーパーバイザ エンジンの冗長構成 (p.8-2)
- スーパーバイザ エンジンの冗長構成の同期化 (p.8-5)
- スーパーバイザエンジンの冗長構成に関する注意事項および制約事項(p.8-6)
- スーパーバイザ エンジンの冗長設定 (p.8-8)
- 手動による切り替え (p.8-14)
- ソフトウェア アップグレードの実行 (p.8-15)
- 冗長スーパーバイザ エンジンでの Bootflash 操作 (p.8-17)



この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference 』 および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/cr/index.htm

スーパーバイザ エンジンの冗長構成

ここでは、スーパーバイザ エンジンの冗長構成について説明します。

- 概要 (p.8-2)
- RPR 動作 (p.8-3)
- SSO 動作 (p.8-3)
- 「スーパーバイザ エンジンの冗長構成の同期化」(p.8-5)

概要

スーパーバイザ エンジンが冗長構成の場合、アクティブ スーパーバイザ エンジンが故障する、または手動で切り替えると、冗長スーパーバイザ エンジンがアクティブ スーパーバイザ エンジンとなります。冗長スーパーバイザ エンジンはアクティブ スーパーバイザ エンジンのスタートアップ コンフィギュレーション時に自動的に初期化されていて、スイッチオーバー時間が短縮されます (コンフィギュレーションに応じて、RPR モードでは 30 秒以上、SSO モードでは 1 秒以下)。

スーパーバイザ エンジンの冗長性は、スイッチオーバー時間の削減以外にも次の内容をサポートしています。

- 冗長スーパーバイザ エンジンの活性挿抜 (online insertion and removal; OIR) スーパーバイザ エンジンの冗長構成により、メンテナンス時に冗長スーパーバイザ エンジンの OIR が可能になります。冗長スーパーバイザ エンジンが搭載されている場合、アクティブスーパーバイザ エンジンがその存在を検出し、冗長スーパーバイザ エンジンは RPR モードでは部分的初期化ステート、および SSO モードでは完全初期化ステートで起動します。
- ソフトウェアのアップグレード (「ソフトウェア アップグレードの実行」[p.8-15] を参照)。 スーパーバイザ エンジンのソフトウェア変更中のダウン時間を最小限にするために、冗長スーパーバイザ エンジンに新しいイメージをロードしてスイッチオーバーを実施します。

スイッチを最初に起動して、最初に起動するスーパーバイザ エンジンがアクティブ スーパーバイザ エンジンとなって、スイッチオーバーが発生するまでアクティブのままとなります。

次のイベントが1つまたは複数発生するとスイッチオーバーが発生します。

- アクティブ スーパーバイザ エンジンの障害 (ハードウェアまたはソフトウェア機能による)、 または取り外し
- ユーザによる強制的なスイッチオーバー
- ユーザによるアクティブ スーパーバイザ エンジンのリロード

表 8-1 では、冗長用のシャーシおよびスーパーバイザエンジンについて説明します。

表 8-1 シャーシおよびスーパーパイザのサポート

シャーシ (製品番号)	サポート対象のスーパーパイザ エンジン	
Catalyst 4507R (WS-C4507R)	冗長 Supervisor Engine II-Plus(WS-X4013+) 冗長 Supervisor Engine II-Plus (WS-X4013+GE) Supervisor Engine IV (WS-X4515) 冗長 Supervisor Engine V (WS-X4516) および冗長 Supervisor Engine V (WS-X4516-10GE)	
Catalyst 4510R (WS-C4510R)	冗長 Supervisor Engine V(WS-X4516)および冗長 Supervisor Engine V (WS-X4516-10GE)	

RPR 動作

RPR は、Cisco IOS Release 12.2(12c)EW 以降のリリースでサポートされます。冗長スーパーバイザ エンジンが RPR モードで稼働している場合、部分的に初期化されたステートで起動し、アクティ ブスーパーバイザエンジンの固定コンフィギュレーションで同期化されます。



(注)

固定コンフィギュレーションには、startup-config、ブート変数、config-register、VLAN(仮 想 LAN)データベースが含まれます。

冗長スーパーバイザ エンジンは基本的なシステム初期化のあとで起動シーケンスを中止します。ア クティブ スーパーバイザ エンジンに障害が発生した場合、冗長スーパーバイザ エンジンが新しい アクティブ スーパーバイザ エンジンになります。

スーパーバイザ エンジンのスイッチオーバーでは、モジュール タイプとステータスに関連する スーパーバイザ エンジンの間ではステートが維持されず、RPR モードの物理ポートすべてが再起 動するので、トラフィックが中断します。 冗長スーパーバイザ エンジンの初期化が完全に終了する と、モジュールからハードウェア情報を読み込みます。

SSO 動作



SSO は Supervisor Engine 6-E ではサポートされていません。

SSO は、Cisco IOS Release 12.2(20)EWA 以降のリリースでサポートされます。冗長スーパーバイザ エンジンが SSO モードで稼働した場合、完全に初期化されたステートで起動し、アクティブ スー パーバイザ エンジンの固定コンフィギュレーションと実行コンフィギュレーションを同期化しま す。冗長スーパーバイザエンジンはそのあと、次のプロトコルのステートを維持し、ステートフル スイッチオーバーをサポートする機能に関するハードウェアおよびソフトウェア ステートの変更 すべてを同期化して維持します。そのため、冗長スーパーバイザ エンジン構成内のレイヤ 2 セッ ションへの割り込みはありません。

冗長スーパーバイザ エンジンは、各リンクのハードウェア リンク ステータスを認識するので、ス イッチオーバーになる前にアクティブだったポートはアップリンク ポートを含め、アクティブのま まです。 ただし、 アップリンク ポートは物理的にスーパーバイザ エンジン上にあるので、 スーパー バイザエンジンが取り外されると切断されます。

アクティブ スーパーバイザ エンジンに障害が発生した場合、冗長スーパーバイザ エンジンがアク ティブになります。この新しいアクティブ スーパーバイザ エンジンは既存のレイヤ 2 スイッチン グ情報を使用して、トラフィック転送を続けます。 ルーティング テーブルが新しいアクティブ スー パーバイザエンジンに追加されるまで、レイヤ3の転送は延期されます。

SSO は、次のレイヤ 2 機能のステートフル スイッチオーバーをサポートします。 次の機能のステー トは、アクティブおよび冗長スーパーバイザエンジンの間で保存されます。

- 802.3
- 802.3u
- 802.3x(フロー制御)
- 802.3ab (GE)

- 802.3z (Coarse Wavelength Division Multiplexing [CWDM; 低密度波長分割多重] を含めたギガビット イーサネット)
- 802.3ad (Link Aggregation Control Protocol [LACP])
- 802.1p (レイヤ 2 QoS [Quality Of Service])
- 802.1Q
- 802.1X (認証)
- 802.1D (Spanning-Tree Protocol [STP; スパニングツリー プロトコル])
- 802.3af (インラインパワー)
- PAgP
- VTP
- Dynamic ARP Inspection (DAI; ダイナミック ARP インスペクション)
- DHCP スヌーピング
- IP ソース ガード
- Internet Group Management Protocol(IGMP; インターネット グループ管理プロトコル) バージョン 1 および 2)
- Dynamic Trunking Protocol (DTP; ダイナミック トランキング プロトコル)(802.1Q および ISL [スイッチ間リンク])
- MST
- PVST+
- Rapid Per-VLAN Spanning-Tree plus (Rapid PVST+)
- PortFast/UplinkFast/BackboneFast
- Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット)およびフィルタリング
- 音声 VLAN
- ポート セキュリティ
- ユニキャスト MAC (メディア アクセス制御) フィルタリング
- Access Control List (ACL; アクセス コントロール リスト)(VACL、PACL、RACLS)
- QoS (DBL)
- マルチキャスト ストーム制御 / ブロードキャストストーム制御

SSO は、次の機能と互換性があります。ただし、次の機能のプロトコル データベースは冗長スーパーバイザ エンジンとアクティブ スーパーバイザ エンジンの間では同期化されていません。

- Layer 2 Protocol Tunneling (L2PT; レイヤ 2 プロトコル トンネリング) を備えた 802.1Q トンネリング
- ベビージャイアント
- ジャンボ フレーム サポート
- Cisco Discovery Protocol (CDP; シスコ検出プロトコル)
- フラッディング ブロック
- UDLD
- SPAN/RSPAN
- NetFlow

SSO 機能がイネーブルの場合、次の機能が冗長スーパーバイザ エンジンで学習されます。

• Catalyst 4500 シリーズ スイッチ上のレイヤ 3 プロトコルすべて (Switch Virtual Interface [SVI; スイッチ仮想インターフェイス])

スーパーバイザ エンジンの冗長構成の同期化

通常の動作中、固定コンフィギュレーション (RPR および SSO) と実行コンフィギュレーション (SSO のみ)は、2 台のスーパーバイザ エンジンの間のデフォルトで同期化されます。 スイッチオー バー時には、新しいアクティブ スーパーバイザ エンジンが現在の設定を使用します。



(注)

冗長スーパーバイザ エンジン コンソールに CLI(コマンドライン インターフェイス) コマンドを入力することはできません。

ここでは、スーパーバイザ エンジンの冗長構成の同期化について説明します。

- RPR スーパーバイザ エンジンの設定の同期化 (p.8-5)
- SSO スーパーバイザ エンジンの設定の同期化 (p.8-5)

RPR スーパーバイザ エンジンの設定の同期化

冗長スーパーバイザ エンジンは RPR モードで部分的に初期化されているだけなので、起動時にコンフィギュレーション変更を受信し、コンフィギュレーション変更を保存する場合にのみ、アクティブ スーパーバイザ エンジンと交信します。

冗長スーパーバイザ エンジンが RPR モードで稼働している場合は、次のイベントによってコンフィギュレーション情報の同期化が発生します。

- 冗長スーパーバイザ エンジンが起動した場合に auto-sync コマンドを使用すると、固定コンフィギュレーションを同期化します。このコマンドは、デフォルトでイネーブルに設定されています。詳細については、「スーパーバイザ エンジンの設定の同期化」(p.8-12)を参照してください。
- アクティブ スーパーバイザ エンジンが冗長スーパーバイザ エンジンを検出すると、コンフィギュレーション情報がアクティブ スーパーバイザ エンジンから冗長スーパーバイザ エンジンに同期化されます。この同期によって、冗長スーパーバイザ エンジン上のすべてのスタートアップ コンフィギュレーション ファイルが上書きされます。
- コンフィギュレーションを変更する場合、write コマンドを使用して、冗長スーパーバイザエンジンのスタートアップコンフィギュレーションを保存および同期化する必要があります。

SSO スーパーバイザ エンジンの設定の同期化



<u>—</u> (計)

SSO は Supervisor Engine 6-E ではサポートされていません。

冗長スーパーバイザ エンジンが SSO モードで稼働している場合は、次のイベントがトリガーとなってコンフィギュレーション情報の同期化が発生します。

- アクティブ スーパーバイザ エンジンが冗長スーパーバイザ エンジンを検出した場合、固定および実行コンフィギュレーションの同期化が発生し、冗長スーパーバイザ エンジンが完全初期 化ステートに移行できます。
- リアルタイムで変更が発生すると、アクティブ スーパーバイザ エンジンは必要に応じて、実行コンフィギュレーションおよび(または)固定コンフィギュレーションと冗長スーパーバイザ エンジンを同期化します。
- コンフィギュレーションを変更する場合に write コマンドを使用して、アクティブ スーパーバイザ エンジンが冗長スーパーバイザ エンジンのスタートアップ コンフィギュレーションを保存および同期化できるようにする必要があります。

スーパーバイザ エンジンの冗長構成に関する注意事項および制約事項

スーパーバイザ エンジンの冗長構成に関する注意事項および制約事項は、次のとおりです。

- RPR では Cisco IOS Release 12.1(12c)EW、Release 12.1(19)E 以降のリリースが必要です。SSO では Cisco IOS Release 12.2(20)EWA 以降のリリースが必要です。
- Catalyst 4507R スイッチおよび 4510R スイッチは、スーパーバイザ エンジンの冗長構成に対応 する唯一の Catalyst 4500 シリーズ スイッチです。
- Catalyst 4510R シリーズ スイッチは、WS-X4516 および WS-X4516-10GE スーパーバイザ エンジンのみをサポートします。 Catalyst 4507R シリーズ スイッチは WS-X4013+、WS-X4013+10GE、WS-X4515、WS-X4516、および WS-X4516-10GE スーパーバイザ エンジンをサポートします。
- Catalyst 4507R シリーズスイッチの Cisco IOS Release 12.2(25)SG 以降のリリースでは、10 ギガビット イーサネットおよびギガビット イーサネット アップリンクは、Supervisor Engine V-10GE(WS-X4516-10GE)と Supervisor Engine II+10GE(WS-4013+10GE)で同時に使用できます。Cisco IOS Release 12.2(25)SG より前のリリースでは、10 ギガビット イーサネット アップリンクまたはギガビット イーサネット アップリンクを選択するには hw-module uplink select コンフィギュレーション コマンドを使用する必要があります。
- Cisco IOS Release 12.2(25)SG 以降のリリースでは、Catalyst 4510R シリーズ スイッチで Supervisor Engine V-10GE (WS-X4516-10GE) を使用するとき、スロット 10 に WS-X4302-GB が搭載されている場合に限り、10 ギガビット イーサネットおよびギガビット イーサネット アップリンク両方を選択して同時に使用できます。10 ギガビット イーサネット アップリンクまたはギガビット イーサネット アップリンクのいずれかを選択する場合、任意のラインカードをスロット 10 に搭載できます。アップリンクを選択するには、hw-module uplink select コンフィギュレーション コマンドを使用します。Cisco IOS Releases 12.2(25)SG より前のリリースでは、10 ギガビット イーサネットおよびギガビット イーサネットのアップリンク両方を同時に使用できません。
- RPR または SSO モードで、WS-X4516-10GE および WS-X4013+10GE Supervisor Engines で 10 ギガビット イーサネット アップリンクを選択する場合、インターフェイス TenGigabitEthernet 1/1 および 2/1 のみを使用できます。同様に、ギガビット イーサネット アップリンクを選択する場合、インターフェイス GigabitEthernet 1/3、1/4、2/3、および 2/4 のみを使用できます。両方のアップリンクを同時に選択すると、インターフェイス TenGigabitEthernet 1/1 および 2/1 と、インターフェイス GigabitEthernet 1/3、1/4、2/3、および 2/4 を使用できます。
- 冗長構成では、同じスーパーバイザエンジンモデルで同じ Cisco IOS ソフトウェアイメージを使用する、シャーシに搭載されているスーパーバイザエンジンが必要です。
- WS-X4013+ および WS-X4515 スーパーバイザ エンジンで RPR または SSO モードを使用する場合に使用できるのは、Gig1/1 および Gig2/1 ギガビット イーサネット インターフェイスのみです。Gig1/2 および Gig2/2 アップリンク ポートは使用できません。
- WS-X4516 アクティブおよび冗長スーパーバイザ エンジンが同じシャーシに搭載されている場合、アップリンク ポート (Gig1/1、Gig2/1、Gig1/2、Gig2/2) を使用できます。
- シャーシのアクティブ スーパーバイザ エンジンおよび冗長スーパーバイザ エンジンは、スロット 1 およびスロット 2 に搭載する必要があります。
- シャーシの各スーパーバイザエンジンには、スイッチを稼働させるための独自のフラッシュデバイスとコンソールポート接続を備えている必要があります。
- 各スーパーバイザ エンジンには、個別のコンソール ポート接続を行う必要があります。コンソール ポートに Y 字型ケーブルを接続しないでください。
- スーパーバイザ エンジンの冗長構成にはスーパーバイザ エンジンのロード バランシング機能 がありません。
- スイッチオーバー時に Cisco Express Forwarding (CEF; シスコ エクスプレス フォワーディング) テーブルがクリアされます。したがって、ルート テーブルの再コンバージェンスまでの間、トラフィックのルーティングが中断されます。SSO 機能がスーパーバイザ エンジンの冗長スイッチオーバー時間を 30 秒以上から 1 秒以下に削減するので、この再コンバージェンス時間は最小となります。また、スイッチが SSO 用に設定された場合のレイヤ 3 のフェールオーバー時間も早くなります。

- スタティック IP ルートは、コンフィギュレーション ファイルのエントリに基づいて設定されるので、スイッチオーバー後も維持されます。
- アクティブ スーパーバイザ エンジン上で維持されているレイヤ 3 ダイナミック ステート情報 は、冗長スーパーバイザ エンジンへの同期化が行われず、スイッチオーバー時に失われます。
- Cisco IOS Release 12.2 以降、サポートされていない状態が検出された場合(アクティブ スーパーバイザ エンジンが Cisco IOS Release 12.2(20)EW を、冗長スーパーバイザ エンジンが Cisco IOS Release 12.1(20)EW を稼働している場合など)、冗長スーパーバイザ エンジンが複数回リセットされ、ROMMON モードになります。したがって、「ソフトウェア アップグレードの実行」(p.8-15)に示す正しい手順に従ってください。
- Cisco IOS Release 12.2(20)EWA または Cisco IOS Release 12.2(25)EW を実行(またはアップグレード)して、冗長シャーシ(Catalyst 4507R または Catalyst 4510R シリーズ スイッチ)で単一のスーパーバイザ エンジンを使用し、ルーテッド ポートを使用する場合は、次のいずれかを実行します。
 - ルーテッドポートの代わりに、SVIを使用します。
 - 冗長モードを SSO から RPR に変更します。
- SSO モードでの SNMP (簡易ネットワーク管理プロトコル) 同期および SNMP 設定操作による 冗長スーパーバイザ エンジンの設定変更は、冗長スーパーバイザ エンジンと同期化されませ ん。SSO モードでの SNMP 設定操作は可能ですが、予期しない動作が発生することがあります。 SSO モードで SNMP によってスイッチを設定したあとで、アクティブ スーパーバイザ エンジン上の running-config ファイルを startup-config ファイルにコピーすると、冗長スーパーバイザ エンジン上の startup-config ファイルの同期化が発生します。新しい設定が冗長スーパーバイザ エンジンに適用されるように冗長スーパーバイザ エンジンをリロードします。
- スタートアップ (一括)同期中は、設定を変更できません。このプロセス中に設定を変更しようとすると、次のメッセージが生成されます。

Config mode locked out till standby initializes

設定変更がスーパーバイザエンジンのスイッチオーバーと同時に発生した場合、それらの設定変更は失われます。

スーパーバイザ エンジンの冗長設定

ここでは、スーパーバイザエンジンの冗長構成を設定する手順について説明します。

- 冗長構成の設定 (p.8-8)
- スタンバイ スーパーバイザ エンジンの仮想コンソール (p.8-10)
- スーパーバイザ エンジンの設定の同期化 (p.8-12)

冗長構成の設定

冗長構成を設定にするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# redundancy	冗長コンフィギュレーション モードを開始します。
ステップ 2	Switch(config-red)# mode {sso rpr}	SSO または RPR を設定します。このコマンドを入力すると、冗長スーパーバイザ エンジンはリロードされて SSO または RPR モードで動作開始します。
ステップ 3	Switch# show running-config	SSO または RPR がイネーブルであることを確認します。
ステップ 4	Switch# show redundancy [clients counters history states]	アクティブおよび冗長スーパーバイザ エンジン用 に冗長構成情報(カウンタ、ステートなど)を表示 します。

冗長構成を設定する場合、次の点に注意してください。

- sso キーワードは、Cisco IOS Release 12.2(20)EWA 以降のリリースでサポートされます。
- rpr キーワードは、Cisco IOS Release 12.1(12c)EW 以降のリリースでサポートされます。

次に、SSO にシステムを設定し、冗長ファシリティ情報を表示する例を示します。

```
Switch> enable
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config) # redundancy
Switch(config-red) # mode sso
Switch(config-red)# end
Switch# show redundancy
Redundant System Information :
      Available system uptime = 2 days, 2 hours, 39 minutes
Switchovers system experienced = 0
             Standby failures = 0
       Last switchover reason = none
                Hardware Mode = Duplex
    Configured Redundancy Mode = Stateful Switchover
    Operating Redundancy Mode = Stateful Switchover
             Maintenance Mode = Disabled
               Communications = Up
Current Processor Information :
______
              Active Location = slot 1
       Current Software state = ACTIVE
      Uptime in current state = 2 days, 2 hours, 39 minutes
                Image Version = Cisco Internetwork Operating System Software
IOS (tm) Catalyst 4000 L3 Switch Software (cat4000-I5S-M), Version 12.2(20)EWA(3
.92), CISCO INTERNAL USE ONLY ENHANCED PRODUCTION VERSION
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Wed 14-Jul-04 04:42 by esi
                        BOOT = bootflash:cat4000-i5s-mz.122_20_EWA_392,1
        Configuration register = 0x2002
Peer Processor Information :
             Standby Location = slot 2
       Current Software state = STANDBY HOT
      Uptime in current state = 2 days, 2 hours, 39 minutes
                Image Version = Cisco Internetwork Operating System Software
IOS (tm) Catalyst 4000 L3 Switch Software (cat4000-I5S-M), Version 12.2(20)EWA(3
.92), CISCO INTERNAL USE ONLY ENHANCED PRODUCTION VERSION
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Wed 14-Jul-04 0
                         BOOT = bootflash:cat4000-i5s-mz.122_20_EWA_392,1
       Configuration register = 0x2002
Switch#
```

次に、冗長ファシリティステート情報を表示する例を示します。

```
Switch# show redundancy states
my state = 13 -ACTIVE
     peer state = 8 -STANDBY HOT
          Mode = Duplex
          Unit = Primary
       Unit ID = 2
Redundancy Mode (Operational) = Stateful Switchover
Redundancy Mode (Configured) = Stateful Switchover
     Split Mode = Disabled
   Manual Swact = Enabled
Communications = Up
  client count = 21
client\_notification\_TMR = 240000 milliseconds
         keep_alive TMR = 9000 milliseconds
       keep_alive count = 0
    keep_alive threshold = 18
          RF debug mask = 0x0
Switch#
```

次に、システム設定を RPR モードから SSO モードに変更する例を示します。

```
Switch(config) # redundancy
Switch(config-red) # mode
Switch(config-red) # mode sso
Changing to sso mode will reset the standby. Do you want to continue?[confirm]
Switch(config-red) # end
Switch#
*Aug 1 13:11:16: %C4K_REDUNDANCY-3-COMMUNICATION: Communication with the peer
Supervisor has been lost
*Aug 1 13:11:16: %C4K_REDUNDANCY-3-SIMPLEX_MODE: The peer Supervisor has been lost
```

次に、システム設定を SSO モードから RPR モードに変更する例を示します。

```
Switch(config)# redundancy
Switch(config-red)# mode rpr
Changing to rpr mode will reset the standby. Do you want to continue?[confirm]
Switch(config-red)# end
*Aug 1 13:11:16: %C4K_REDUNDANCY-3-COMMUNICATION: Communication with the peer
Supervisor has been lost
*Aug 1 13:11:16: %C4K_REDUNDANCY-3-SIMPLEX_MODE: The peer Supervisor has been lost
```

スタンバイ スーパーバイザ エンジンの仮想コンソール

Catalyst 4500 シリーズ スイッチには、冗長性を持たせるため、2 つのスーパーバイザ エンジンを搭載できます。スイッチに電源が入ると、スーパーバイザ エンジンの 1 つがアクティブになり、スイッチオーバーが発生するまでアクティブのままになります。もう 1 つのスーパーバイザ エンジンはスタンバイ モードのままです。

スーパーバイザ エンジンのそれぞれには、自身のコンソール ポートがあります。スタンバイ スーパーバイザ エンジンのコンソール ポート経由でのみ、スタンバイ スーパーバイザ エンジンにアクセスできます。したがって、スタンバイ スーパーバイザに対するアクセス、監視、またはデバッグを行うには、スタンバイ コンソールに接続する必要があります。

スタンバイ スーパーバイザ エンジンの仮想コンソールを使用すると、スタンバイ コンソールへの 物理的な接続がなくてもアクティブ スーパーバイザ エンジンからスタンバイ コンソールにアクセ スできます。EOBC で IPC を使用してスタンバイ スーパーバイザ エンジンと通信し、アクティブ スーパーバイザ エンジン上でスタンバイ コンソールをエミュレートします。一度にアクティブに できるアクティブ スタンバイ コンソール セッションは 1 つのみです。

スタンバイ スーパーバイザ エンジンの仮想コンソールにより、アクティブ スーパーバイザ エンジンにログオンしているユーザは、スタンバイ スーパーバイザ エンジン上で show コマンドをリモートで実行し、アクティブ スーパーバイザ エンジンでその結果を表示できます。仮想コンソールは、アクティブ スーパーバイザ エンジンからのみ利用できます。

アクティブ スーパーバイザ エンジンからアクティブ スーパーバイザ エンジンの attach module、session module、または remote login コマンドを使用してスタンバイ仮想コンソールにアクセスできます。これらのコマンドを実行してスタンバイ コンソールにアクセスするには、特権 EXEC モード (レベル 15) を開始している必要があります。

スタンバイ仮想コンソールを開始すると、端末プロンプトは、[<hostname>-standby-console#] に自動的に変更されます(ここで、hostname はスイッチに設定された名前です)。仮想コンソールを終了すると、このプロンプトは元のプロンプトに戻ります。

exit または quit コマンドを入力すると、仮想コンソールは終了します。ログインしたアクティブスーパーバイザ エンジンの端末の無活動時間が設定されたアイドル時間を超えると、アクティブスーパーバイザ エンジンの端末から自動的にログアウトします。この場合、仮想コンソール セッションも終了します。また、スタンバイが再起動すると、仮想コンソール セッションも自動的に終了します。スタンバイが起動したあとは、別の仮想コンソール セッションを作成する必要があります。

仮想コンソールを使用してスタンバイ スーパーバイザ エンジンにログインするには、次の操作を 実行します。

Switch# session module 2

Connecting to standby virtual console
Type "exit" or "quit" to end this session

Switch-standby-console# exit
Switch#

スタンバイ コンソールがイネーブルでない場合、次のメッセージが表示されます。

Switch-standby-console# Standby console disabled. Valid commands are: exit, logout



スタンバイ仮想コンソールには、コマンド履歴、コマンド補完、コマンド ヘルプ、部分コマンド キーワードなど、スーパーバイザ コンソールから利用できる標準的な機能が備わっています。

次の制限事項がスタンバイ仮想コンソールに適用されます。

- 仮想コンソールで実行されたコマンドは、すべて最後まで実行されます。auto-more 機能はありません。したがって、terminal length 0 コマンドの実行時と同じように機能します。また、対話形式ではありません。したがって、アクティブスーパーバイザエンジン上でキーシーケンスを入力しても、コマンドの実行を中断できません。コマンドによって大量の出力が発生した場合、仮想コンソールはスーパーバイザ画面に出力を表示します。
- 仮想コンソールは対話形式ではありません。仮想コンソールはコマンドのインタラクティブ性を検出しないので、ユーザとの対話を必要とするコマンドが入力されると、RPC タイマーがコマンドを中断するまで仮想コンソールは待機します。

仮想コンソール タイマーは 60 秒に設定されています。60 秒後に仮想コンソールはプロンプトに戻ります。この間、キーボードからコマンドを中断できません。操作を続ける前に、タイマーが期限切れになるのを待つ必要があります。

• 仮想コンソールを使用して、スタンバイ スーパーバイザ エンジン上で表示されているデバッ グおよび Syslog メッセージを表示することはできません。仮想コンソールは、仮想コンソール から実行されたコマンドの出力のみを表示します。実際のスタンバイ コンソールで表示される 別の情報は、仮想コンソールでは表示できません。

スーパーバイザ エンジンの設定の同期化

2 台のスーパーバイザエンジンが使用する設定を手動で同期化するには、アクティブスーパーバイザエンジン上で次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# redundancy	冗長コンフィギュレーション モードを開始します。
ステップ 2	Switch(config-red)# main-cpu	main-cpu コンフィギュレーション サブモードを開始します。
ステップ 3	Switch(config-r-mc)# auto-sync {startup-config config-register bootvar standard}	設定要素を同期化します。
ステップ 4	Switch(config-r-mc)# end	特権 EXEC モードに戻ります。
ステップ 5	Switch# copy running-config startup-config	Dynamic Random-Access Memory(DRAM; ダイナミック ランダム メモリ)の実行コンフィギュレーションファイルを NVRAM(不揮発性 RAM)のスタートアップ コンフィギュレーション ファイルに同期化します。
		(注) DRAM 上の実行コンフィギュレーション ファイルを同期化する場合、このステップは 不要です。



(注)

SNMP によるアクティブ スーパーバイザ エンジンの設定変更は、冗長スーパーバイザ エンジンに 同期化されません。この場合の詳細な取り扱いについては、「スーパーバイザ エンジンの冗長構成 に関する注意事項および制約事項」(p.8-6)を参照してください。



(注)

auto-sync コマンドは、config-reg、bootvar、および startup/private コンフィギュレーション ファイル の同期化のみを制御します。カレンダーおよび VLAN データベース ファイルは、変更するたびに常に同期化されます。SSO モードでは、running-config は常に同期化されます。

次に、auto-sync standard コマンドを使用して、デフォルトの自動同期化機能を再びイネーブルにし、アクティブ スーパーバイザ エンジンの startup-config および config-register 設定を冗長スーパーバイザ エンジンと同期化させる例を示します。ブート変数のアップデートは自動的に行われるため、ディセーブルにできません。

Switch(config) # redundancy
Switch(config-red) # main-cpu
Switch(config-r-mc) # auto-sync standard
Switch(config-r-mc) # end
Switch# copy running-config startup-config



(注)

標準の自動同期対象の設定要素を個別に手動で同期化するには、デフォルトの自動同期化機能をディセーブルにします。



(注)

auto-sync standard を設定すると、個別の同期化オプション (no auto-sync startup-config など) は無視されます。

次に、デフォルトの自動同期化をディセーブルにして、アクティブ スーパーバイザ エンジンの config-register のみを冗長スーパーバイザ エンジンに自動的に同期化し、スタートアップ コンフィギュレーションの同期化を許可しない例を示します。

Switch(config)# redundancy
Switch(config-red)# main-cpu
Switch(config-r-mc)# no auto-sync standard
Switch(config-r-mc)# auto-sync config-register
Switch(config-r-mc)# end

手動による切り替え

ここでは、テストのため手動による切り替え(アクティブ スーパーバイザ エンジンから冗長スーパーバイザ エンジンへ)を行う方法を説明します。ご使用の稼働環境に SSO を展開する前に、手動で切り替えることを推奨します。



(注)

これは、SSO が冗長モードとして設定されていることを前提としています。

手動で切り替えるには、アクティブスーパーバイザエンジンで次の作業を行います。

	コマンド	目的
ステップ 1	Switch# show redundancy	ピア ステートが STANDBY HOT ステートであることを確認します。
		p.6-9 の show redundancy states コマンドの例を参照してください。
ステップ 2	Switch# redundancy force-switchover	アクティブ スーパーバイザ エンジンから冗長スーパーバ イザ エンジンへのスイッチオーバーが開始されます。
		冗長スーパーバイザ エンジンのステートが STANDBY HOT でない場合、このコマンドは実行されません。

次の使用上の注意事項に留意してください。

- 強制的にスイッチオーバーを実施するには、冗長スーパーバイザ エンジンを STANDBY HOT ステートにする必要があります。show redundancy コマンドを使用すると、ステートを確認できます。ステートが STANDBY HOT でない場合、redundancy force-switchover コマンドは実行されません。
- スイッチオーバーを開始するには、reload コマンドではなく、redundancy force-switchover コマンドを使用します。redundancy force-switchover コマンドが、冗長スーパーバイザ エンジンが正しいステートであるかどうかを最初に確認します。reload コマンドを使用してステータスが STANDBY HOT でない場合、reload コマンドは現在のスーパーバイザ エンジンのみをリセットします。

最初のスイッチオーバーのあと、シャーシのスロット 1 のスーパーバイザ エンジンをアクティブスーパーバイザ エンジンにする必要が生じる場合があります。スーパーバイザ エンジン 1 上のイメージが、両方のスーパーバイザ エンジン上で実行したいイメージの場合、冗長構成にするためにスロット 1 のスーパーバイザ エンジン上のイメージを再起動する必要はありません。代わりに、別のスイッチオーバーを強制的に実行できます。ただし、両方のスーパーバイザ エンジン上で実行するイメージのバージョンを新しくする場合、次の「ソフトウェア アップグレードの実行」(p.8-15)の手順に従ってください。どのスロットにアクティブ スーパーバイザ エンジンが含まれているかを判断し、必要に応じて別のスイッチオーバーを強制的に実行するには、show module コマンドを使用します。

ソフトウェア アップグレードの実行

スーパーバイザ エンジンの冗長構成がサポートするソフトウェアのアップグレード手順によって、 冗長スーパーバイザ エンジン上の Cisco IOS ソフトウェア イメージをリロードし、そのあとでもう 一度、アクティブ スーパーバイザ エンジンにリロードできます。

アクティブ スーパーバイザ エンジンが Cisco IOS Release 12.2(x)S を実行している場合、スタンバイスーパーバイザ エンジンは Cisco IOS Release 12.1(x)E を実行できません。スタンバイスーパーバイザエンジンのシステムの起動後すぐに、スイッチがリセットされることになります。この逆の設定 (スタンバイエンジンが Cisco IOS Release 12.2(x)S を実行して、アクティブ スーパーバイザエンジンが Cisco IOS Release 12.1(x)E を実行する場合)は、完全にサポートされます。

ソフトウェアのアップグレードを実行するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# copy source_device:source_filename slot0:target_filename	スーパーバイザ エンジンのブートフラッシュに、新 しい Cisco IOS ソフトウェア イメージをコピーしま
	または	す。
	Switch# copy source_device:source_filename bootflash:target_filename	
ステップ 2	Switch# copy source_device:source_filename slaveslot0:target_filename	スレーブ デバイス(slavebootflash、slaveslot0 など) に、新しいイメージをコピーします。
	または	
	Switch# copy source_device:source_filename slavebootflash:target_filename	
ステップ 3	Switch# config terminal Switch(config)# config-register 0x2 Switch(config)# boot system flash device:file_name	新しいイメージが起動されるように、スーパーバイザ エンジンを設定します。
		システムが古いイメージを自動的に起動するよう設定されている場合、次のコマンドストリングを発行して代わりに新しいイメージを起動します。 no boot system flash device:old_file_name
ステップ 4	Switch(config)# redundancy	冗長コンフィギュレーション モードを開始します。
ステップ 5	Switch(config-red)# main-cpu	main-cpu コンフィギュレーション サブモードを開始します。
ステップ 6	Switch(config-r-mc)# auto-syn standard	設定要素を同期化します。
ステップ 7	Switch(config-r-mc)# end	特権 EXEC モードに戻ります。
ステップ 8	Switch# copy running-config start-config	設定を保存します。
ステップ 9	Switch# redundancy reload peer	冗長スーパーバイザ エンジンをリロードし、オンラインに戻します (新しいリリースの Cisco IOS ソフトウェアを使用します)。
		(注) ステップ 10 に進む前に、スイッチが RPR モードで稼働していることを確認します。

	コマンド	目的
ステップ 10	Switch# redundancy force-switchover	冗長スーパーバイザ エンジンに手動で切り替えます。冗長スーパーバイザ エンジンが、新しい Cisco IOS ソフトウェア イメージを使用するアクティブスーパーバイザ エンジンになります。
		以前のアクティブ スーパーバイザ エンジンが新し いイメージで再起動され、冗長スーパーバイザ エン ジンになります。

次に、ソフトウェア アップグレードの実行例を示します。

```
Switch# config terminal
Switch(config)# config-register 0x2
Switch(config)# boot system flash slot0:cat4000-i5s-mz.122-20.EWA
Switch(config)# redundancy
Switch(config-red)# main-cpu
Switch(config-r-mc)# auto-syn standard
Switch(config-r-mc)# end
Switch# copy running-config start-config
Switch# redundancy reload peer
Switch# redundancy force-switchover
Switch#
```

次に、アクティブ スーパーバイザ エンジン上の実行コンフィギュレーションと冗長スーパーバイザ エンジンとの同期化が成功したことを確認する例を示します。

```
Switch# config terminal
Switch(config)# redundancy
Switch(config-red)# main-cpu
Switch(config-r-mc)# auto-sync standard
4d01h: %C4K_REDUNDANCY-5-CONFIGSYNC: The bootvar has been successfully synchronized to the standby supervisor
4d01h: %C4K_REDUNDANCY-5-CONFIGSYNC: The config-reg has been successfully synchronized to the standby supervisor
4d01h: %C4K_REDUNDANCY-5-CONFIGSYNC: The startup-config has been successfully synchronized to the standby supervisor
4d01h: %C4K_REDUNDANCY-5-CONFIGSYNC: The private-config has been successfully synchronized to the standby supervisor
```

上記の例では、アクティブ スーパーバイザ エンジンからのブート変数、config-register、スタートアップ コンフィギュレーションが冗長スーパーバイザ エンジンに同期化したことを示します。

冗長スーパーバイザ エンジンでの Bootflash 操作



(注)

冗長スーパーバイザ エンジン上のコンソール ポートは使用できません。

冗長スーパーバイザ エンジン bootflash を操作するには、次のうち 1 つまたは複数の作業を行います。

コマンド	目的
Switch# dir slaveslot0:target_filename	冗長スーパーバイザ エンジンの slot0: デバイスの内容を表
または Switch# dir slavebootflash: target_filename	示します。 冗長スーパーバイザ エンジンの bootflash: デバイスの内容 を表示します。
Switch# delete slaveslot0:target_filename	冗長スーパーバイザ エンジンの slot0: デバイスから特定のファイルを削除します。
または Switch# delete slave bootflash: target_filename	冗長スーパーバイザ エンジンの bootflash: デバイスから特定のファイルを削除します。
Switch# squeeze slaveslot0:target_filename	冗長スーパーバイザ エンジンの slot0: デバイスをスクイー ズします。
Switch# squeeze slavebootflash:target_filename	冗長スーパーバイザ エンジンの bootflash: デバイスをスク イーズします。
Switch# format slaveslot0:target_filename	冗長スーパーバイザ エンジンの slot0: デバイスをフォーマットします。
Switch# format slavebootflash: target_filename	冗長スーパーバイザ エンジンの bootflash: デバイスを フォーマットします。
Switch# copy source_device:source_filename slaveslot0:target_filename	アクティブ スーパーバイザ エンジンから冗長スーパーバイザ エンジンの slot0: デバイスへファイルをコピーしま
または Switch# copy source_device:source_filename slavebootflash:target_filename	す。 冗長スーパーバイザ エンジンの bootflash: デバイスにファ イルをコピーします。
	(注) 送信元はアクティブ スーパーバイザ エンジン、または Trivial File Transfer Protocol(TFTP; 簡易ファイル転送プロトコル) サーバです。

■ 冗長スーパーパイザ エンジンでの Bootflash 操作



CHAPTER

9

Cisco NSF/SSO スーパーバイザ エンジンの冗長構成の設定

この章では、Stateful Switchover (SSO)を備えた Cisco Nonstop Forwarding (NSF)を使用してスーパーバイザ エンジンの冗長構成を設定する方法について説明します。

この章の内容は、次のとおりです。

- NSF/SSO スーパーバイザエンジンの冗長構成の概要 (p.9-2)
- NSF/SSO スーパーバイザ エンジンの冗長構成の設定 (p.9-11)



(注)

この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference, Release 12.2(37)SG』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univered/cc/td/doc/product/software/ios122sr/cr/index.htm

NSF/SSO スーパーバイザ エンジンの冗長構成の概要

ここでは、NSF/SSO を使用したスーパーバイザエンジンの冗長構成について説明します。

- Cisco IOS NSF 認識および NSF 対応サポートの概要 (p.9-2)
- NSF/SSO スーパーバイザ エンジンの冗長構成の概要 (p.9-4)
- SSO の動作 (p.9-5)
- NSF の動作 (p.9-5)
- CEF (p.9-6)
- ルーティング プロトコル (p.9-6)
- NSF の注意事項と制約事項 (p.9-10)

Cisco IOS NSF 認識および NSF 対応サポートの概要

Cisco IOS NSF には2つの主なコンポーネントがあります。

NSF 認識 スーパーバイザ エンジン スイッチオーバーが発生していても NSF ルータがまだ パケットを転送可能なことを隣接ルータ デバイスが検出する機能を NSF 認識といいます。レイヤ 3 ルーティング プロトコル (OSPF、Border Gateway Protocol [BGP; ボーダー ゲートウェイ プロトコル] EIGRP、IS-IS) に対する Cisco IOS 拡張機能は、Cisco Express Forwarding (CEF; シスコ エクスプレス フォワーディング)ルーティング テーブルが時間切れにならないように、または NSF ルータがルートをドロップしないように、ルート フラッピングを防ぐよう設計されています。NSF 認識ルータは、ルーティング プロトコル情報を近接 NSF ルータに送信します。 NSF 機能 NSF は SSO と連動して IP パケットを転送し続けることにより、スーパーバイザエンジン スイッチオーバーのあとのレイヤ 3 ネットワークを利用できない時間を最小限にします。 レイヤ 3 ルーティング プロトコル (BGP、EIGRP、OSPFv2、IS-IS) の再コンバージェ

ンスは、ユーザに対してトランスペアレントであり、バックグラウンドで自動的に発生します。 ルーティング プロトコルは隣接デバイスから情報を回復し、CEF テーブルを再構築します。



(注) NSF は、VRF および IPv6 をサポートしていません。



(井)

NSF 対応デバイスには、Catalyst 4500 シリーズ スイッチ、Catalyst 6500 シリーズ スイッチ、Cisco 7500 シリーズ ルータ、Cisco 10000 シリーズ ルータ、および Cisco 12000 シリーズ ルータがあります。

次に、NSF および NSF 認識ルータの一般的なトポロジを示します。

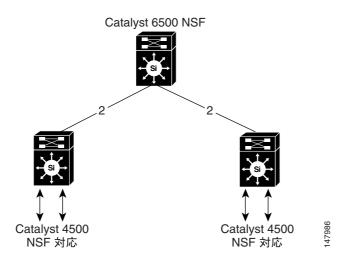


図 9-1 NSF および NSF 対応スイッチのトポロジ

表 9-1 に、NSF 認識をサポートするスーパーバイザ エンジンおよび Catalyst 4500 シリーズ スイッチを示します。

表 9-1 NSF 認識スーパーパイザ エンジン

NSF 認識スーパーパイザ エンジン	サポート対象スイッチ
Supervisor Engine II-Plus (WS-X4013)	Catalyst 4507R シリーズ スイッチ、Catalyst 4506 シリーズ スイッチ、Catalyst 4503 シリーズ ス イッチ
Supervisor Engine II-Plus+TS (WS-X4013+TS)	Catalyst 4507R シリーズ スイッチ、Catalyst 4506 シリーズ スイッチ、Catalyst 4503 シリーズ ス イッチ
Supervisor Engine II-Plus+10GE (WS-X4013+10GE)	Catalyst 4507R シリーズ スイッチ、Catalyst 4506 シリーズ スイッチ、Catalyst 4503 シリーズ ス イッチ
Supervisor Engine IV (WS-X4515)	Catalyst 4507R シリーズ スイッチ、Catalyst 4506 シリーズ スイッチ、Catalyst 4503 シリーズ ス イッチ
Supervisor Engine V (WS-X4516)	Catalyst 4507R シリーズ スイッチおよび Catalyst 4510R シリーズ スイッチ
Supervisor Engine V-10GE (WS-X4516-10GE)	Catalyst 4506 シリーズ スイッチ、Catalyst 4507R シリーズ スイッチ、Catalyst 4510R シリーズ ス イッチ
Supervisor Engine 6-E (WS-X45-Sup6-E)	Catalyst 4500 E シリーズ スイッチ
固定スイッチ(WS-C4948 および WS-C4948-10GE)	Catalyst 4948 スイッチおよび Catalyst 4948-10GE スイッチ

Cisco IOS Release 12.2(20)EWA 以降、Catalyst 4500 シリーズ スイッチでは、EIGRP、IS-IS、OSPF、および BGP プロトコルに対する NSF 認識がサポートされています。Cisco IOS Release 12.2(31)SG 以降、Catalyst 4500 シリーズ スイッチでは IP Base イメージの EIGRP スタブの NSF 認識がすべての

スーパーバイザ エンジンに対してサポートされています。NSF 認識は、EIGRP スタブ、EIGRP、IS-IS、および OSPF プロトコルに対してはデフォルトでオンになります。BGP の場合、手動でオンにする必要があります。

スーパーバイザ エンジンが BGP (graceful-restart コマンドを使用)、EIGRP、OSPF、または IS-IS ルーティング プロトコル用に設定された場合、ルーティング アップデートは、近接 NSF 対応スイッチ (一般的に Catalyst 6500 シリーズ スイッチ) のスーパーバイザ エンジンのスイッチオーバー中に自動的に送信されます。

Cisco IOS Release 12.2(31)SG から、Catalyst 4500 シリーズ スイッチでは NSF 機能がサポートされて います。表 9-2 に、NSF 対応であるスーパーバイザ エンジンおよび Catalyst 4500 シリーズ スイッチを示します。

表 9-2 NSF 対応スーパーパイザ エンジン

NSF 対応スーパーパイザ エンジン	サポート対象スイッチ
Supervisor Engine IV (WS-X4515)	Catalyst 4507R シリーズ スイッチ
Supervisor Engine V (WS-X4516)	Catalyst 4507R シリーズ スイッチおよび Catalyst 4510R シリーズ スイッチ
Supervisor Engine V-10GE (WS-X4516-10GE)	Catalyst 4507R シリーズ スイッチおよび Catalyst 4510R シリーズ スイッチ

NSF/SSO スーパーバイザ エンジンの冗長構成の概要

Catalyst 4500 シリーズ スイッチでは、プライマリ スーパーバイザ エンジンが故障した場合に冗長 スーパーバイザ エンジンに処理を引き継ぐことにより、耐障害性をサポートしています。NSF は、SSO と連動して、スイッチオーバー後にユーザがネットワークを使用できない時間を最小限に抑えます。

NSF には次の利点があります。

- ネットワークのアベイラビリティの向上
 NSF は、ユーザのセッション情報がスイッチオーバー後も維持されるように、ネットワークトラフィックとアプリケーションのステート情報を転送し続けます。
- 全体的なネットワークの安定 ネットワークの安定性は、ネットワーク内のルータで障害が発生してルーティング テーブルが 消失したときに生成されるルート フラップ数を減らすことで改善できます。
- 隣接ルータがリンク フラップを検出しない スイッチオーバー中もインターフェイスはアップのままなので、隣接ルータはリンク フラップ を検出しません(リンクがダウン後にアップに戻るということがありません)。
- ルーティング フラップの回避
 SSO がスイッチオーバー時にネットワーク トラフィックを転送し続けるので、ルーティング フラップが回避されます。
- スイッチオーバーの前に確立したユーザ セッションの維持

Catalyst 4500 シリーズ スイッチは、Route Processor Redundancy (RPR) もサポートします。これらの冗長モードの詳細については、第 8 章「RPR および SSO を使用したスーパーバイザ エンジンの冗長設定」を参照してください。

SSO の動作

SSO は、スーパーバイザ エンジンの 1 つをアクティブに設定してもう 1 つのスーパーバイザ エンジンをスタンバイに指定し、その後これらの間で情報を同期させます。アクティブ スーパーバイザ エンジンで障害が発生したり、スイッチから取り外されたり、またはメンテナンスのため手動でシャットダウンされたりした場合に、アクティブ スーパーバイザ エンジンから冗長スーパーバイザ エンジンへのスイッチ オーバーが発生します。

SSO を実行しているネットワーキング デバイスでは、アクティブ スーパーバイザ エンジンが故障 したあとに冗長スーパーバイザ エンジンがいつでも制御を行えるように、両方のスーパーバイザ エンジンが同じ Cisco IOS ソフトウェア バージョンと ROMMON バージョンで動作している必要が あります。また SSO スイッチオーバーでは、Forwarding Information Base(FIB; 転送情報ベース) および隣接関係エントリが維持され、スイッチオーバー後もレイヤ 3 トラフィックを転送できます。設定情報とデータ構造は、起動時やアクティブ スーパーバイザ エンジンの設定変更が発生したときに、アクティブ スーパーバイザエンジンから冗長スーパーバイザ エンジンへ同期するように なっています。2 つのスーパーバイザ エンジン間の初期同期後に、SSO は転送情報などの両者間のステート情報を維持しています。

スイッチオーバー時に、システム制御とルーティング プロトコル実行はアクティブ スーパーバイザから冗長スーパーバイザ エンジンに転送されます。



[no] service slave-log コンフィギュレーション コマンドを使用して、すべてのエラー メッセージをスタンバイ スーパーバイザ エンジンからアクティブ エンジンに転送できることに注意してください。デフォルトでは、この機能はイネーブルに設定されています。詳細については、『Catalyst 4500 Series Switch Cisco IOS System Error Message Guide』Release 12.2(37)SG を参照してください。

NSF の動作

NSF は、常に SSO とともに実行され、レイヤ 3 トラフィックの冗長機能を提供します。NSF は、ルーティングについては BGP、OSPF、IS-IS、EIGRP ルーティング プロトコルで、転送については CEF でサポートされています。ルーティング プロトコルは NSF 機能と NSF 認識によって強化されています。つまり、これらのプロトコルを実行しているルータは、スイッチオーバーを検出し、ネットワーク トラフィックの転送を継続して、ピア デバイスからルート情報を回復するための必要な処理を行います。スイッチオーバー後のルート情報を回復するために、ピア デバイスから情報を受信するのではなく、アクティブ スーパーバイザ エンジンと冗長スーパーバイザ エンジンとの間で同期しているステート情報を使用するように、IS-IS プロトコルを設定できます。

ネットワーキング デバイスは、NSF 互換ソフトウェアを実行している場合に NSF を認識します。 NSF をサポートするようにデバイスを設定した場合にデバイスは NSF 対応になります。NSF 認識 ネイバーまたは NSF 対応ネイバーからルーティング情報を再構築します。

スイッチオーバー中にルーティング プロトコルが Routing Information Base (RIB) テーブルを再構築している間、各プロトコルは CEF に依存してパケット転送を継続します。ルーティング プロトコルが収束したあと、CEF が FIB テーブルを更新して失効したルート エントリを削除します。次に、CEF は新しい FIB 情報でラインカードを更新します。

CEF

NSFで重要となる要素は、パケット転送です。シスコのネットワーキングデバイスでは、パケット転送は CEF で提供されます。 CEF は FIB を維持し、スイッチオーバーの時点の FIB 情報を使用してスイッチオーバー中のパケット転送を継続します。この機能は、スイッチオーバー中のトラフィックの中断を低減します。

通常の NSF 動作中に、アクティブ スーパーバイザ エンジンの CEF が現行の FIB および隣接関係 データベースを冗長スーパーバイザ エンジンの FIB および隣接関係データベースと同期させます。 アクティブ スーパーバイザ エンジンのスイッチオーバーでは、冗長スーパーバイザ エンジンに最 初からアクティブ スーパーバイザ エンジンで使用中の FIB と隣接関係データベースのミラー イメージがあります。 転送エンジンが存在するプラットフォームでは、アクティブ スーパーバイザエンジンの CEF によって送信される変更を使用して、CEF が冗長スーパーバイザエンジンの転送エンジンを最新の状態に保ちます。 転送エンジンは、インターフェイスおよびデータ パスが使用可能になりしだい、スイッチオーバー後も転送を継続できます。

ルーティング プロトコルがプレフィクス単位で RIB を再び読み込み始めるため、CEF に対してプレフィクス単位のアップデートが行われます。CEF はこれを使用して FIB と隣接データベースを更新します。既存エントリと新規エントリには、最新であることを示す新しいバージョン(「エポック」)番号が付けられます。転送エンジンでは、コンバージェンス中に転送情報が更新されます。RIB が収束すると、スーパーバイザ エンジンが信号通知を行います。ソフトウェアが、現在のスイッチオーバー エポックよりも古いエポックを持つすべての FIB および隣接関係エントリを削除します。これで、FIB には最新のルーティング プロトコル転送情報が反映されます。

ルーティング プロトコル



(汗) <u>一</u>

Catalyst 4500 シリーズ スイッチでは、ルーティング プロトコルを使用するのに、Enterprise Services (ES) Cisco IOS ソフトウェア イメージが必要です。

ルーティング プロトコルは、アクティブ スーパーバイザ エンジン上でのみ動作し、隣接ルータからルーティング アップデートを受信します。ルーティング プロトコルは、スタンバイ スーパーバイザ エンジンでは実行されません。スイッチオーバー後に、ルーティング プロトコルは、ルーティング テーブルの再構築に役立てるために、NSF を認識する隣接デバイスに、ステート情報を送信するように要求します。またこの代わりに、隣接デバイスが NSF を認識しないような環境にある NSF 対応デバイスのルーティング テーブルの再構築に役立つように、アクティブ スーパーバイザ エンジンからのステート情報を冗長スーパーバイザ エンジンと同期させるように、IS-IS プロトコルを設定できます。NSF は BGP、OSPF、IS-IS、および EIGRP プロトコルをサポートしています。



(注)

NSF 動作の場合、ルーティング プロトコルがルーティング情報を再構築している間、ルーティング プロトコルは CEF に依存してパケット転送を継続します。

BGP の動作

NSF 対応ルータが BGP ピアと BGP セッションを開始するときに、OPEN メッセージをピアに送信します。メッセージには、NSF 対応デバイスに「グレースフル」リスタート機能があることを示す文が含まれています。グレースフル リスタートとは、スイッチオーバー後に BGP ルーティング ピアでルーティング フラップが発生しないようにするためのメカニズムです。BGP ピアがこのステートメントを受信すると、メッセージを送信しているデバイスが NSF 対応であることを認識します。NSF 対応ルータと BGP ピアの両方は、セッション確立時に OPEN メッセージでグレースフル リスタート機能を示すステートメントを交換する必要があります。両方のピアがグレースフル リスタート機能を示すステートメントを交換しない場合、このセッションでグレースフル リスタートは行われません。

スーパーバイザ エンジンのスイッチオーバー中に BGP セッションが切断された場合、NSF 認識 BGP ピアは、NSF 対応ルータに関連したすべてのルートを失効とマーキングします。ただし、所定 の時間内は、引き続きこれらのルートを転送の決定に使用します。この機能により、新しくアクティブになったスーパーバイザ エンジンが BGP ピアとのルーティング情報のコンバージェンスを 待機している間にパケットが消失することを防げます。

スーパーバイザ エンジンのスイッチオーバーが発生したあと、NSF 対応ルータは BGP ピアとの セッションを再確立します。新しいセッションの確立中に、NSF 対応ルータが再起動したことを示す新しいグレースフル リスタート メッセージを送信します。

この時点で、ルーティング情報は2つのBGPピア間で交換されています。この交換が完了すると、NSF対応デバイスはルーティング情報を使用してRIBとFIBを新しい転送情報で更新します。NSF認識デバイスは、ネットワーク情報を使用して失効したルートをBGPテーブルから削除し、これでBGPプロトコルが完全に収束します。

BGP ピアがグレースフル リスタート機能をサポートしていない場合、OPEN メッセージ内のグレースフル リスタート機能は無視されますが、NSF 対応デバイスとの BGP セッションは確立します。この機能により、NSF 非認識 (つまり NSF 機能のない) BGP ピアとの相互運用が可能になりますが、NSF 非認識 BGP ピアとの BGP セッションではグレースフル リスタートは使用できません。



<u>一</u> (注)

NSF での BGP サポートでは、隣接ネットワーキング デバイスが NSF を認識できなければなりません。 つまり、デバイスはグレースフル リスタート機能に対応している必要があり、 セッション確立中に OPEN メッセージでその機能をアドバタイズする必要があります。 NSF 対応ルータが特定の BGP ネイバーにグレースフル リスタート機能がないことを検出すると、 NSF 対応セッションをそのネイバーと確立しません。 グレースフル リスタート機能のある他のすべてのネイバーは、この NSF 対応ネットワーキング デバイスと NSF 対応セッションを継続します。

OSPF の動作

OSPF NSF 対応ルータがスーパーバイザ エンジンのスイッチオーバーを実行する場合、リンク ステート データベースを OSPF ネイバーと再同期するために、次の処理を実行する必要があります。

- ネイバー関係をリセットせずに、ネットワーク上の使用可能な OSPF ネイバーを再学習します。
- ネットワークのリンク ステート データベースの内容を再取得します。

スーパーバイザ エンジンのスイッチオーバー後できるだけ早く、NSF 対応ルータは OSPF NSF 信号を隣接 NSF 認識デバイスに送信します。隣接ネットワーキング デバイスは、この信号をこのルータとのネイバー関係がリセットされるべきでないことを示すインジケータとして認識します。NSF 対応ルータがネットワーク上の他のルータから信号を受信すると、隣接リストを再構築できます。

ネイバー関係が再確立されたあと、NSF 対応ルータはすべての NSF 認識ネイバーとのデータベースの再同期を開始します。この時点で、ルーティング情報は OSPF ネイバー間で交換されています。この交換が完了すると、NSF 対応デバイスは、ルーティング情報を使用して失効したルートを削除し、RIB を更新し、FIB を新しい転送情報で更新します。ここで OSPF プロトコルが完全に収束されます。



OSPF NSF では、すべての隣接ネットワーキング デバイスが NSF を認識できなければなりません。 NSF 対応ルータが特定のネットワーク セグメントで NSF 非認識ネイバーを検出すると、そのセグ メントで NSF 機能をディセーブルにします。NSF 対応または NSF 認識ルータで完全に構成された 他のネットワーク セグメントに対しては、継続して NSF 機能を提供します。

IS-IS の動作

IS-IS NSF 対応ルータがスーパーバイザ エンジンのスイッチオーバーを実行する場合、リンク ステート データベースを IS-IS ネイバーと再同期するために、次の処理を実行する必要があります。

- ネイバー関係をリセットせずに、ネットワーク上の使用可能な IS-IS ネイバーを再学習します。
- ネットワークのリンク ステート データベースの内容を再取得します。

NSF を設定する場合、IS-IS NSF 機能には次の2つのオプションがあります。

- Internet Engineering Task Force (IETF; インターネット技術特別調査委員会) IS-IS
- Cisco IS-IS

あるネットワーク セグメントの隣接ルータがルータの再起動に関する IETF インターネット ドラフトをサポートするソフトウェア バージョンを実行している場合、再起動する IETF NSF ルータを支援します。IETF を使用すると、隣接ルータはスイッチオーバー後のルーティング情報の再構築に役立つ隣接関係およびリンク ステート情報を提供します。IETF IS-IS 設定の利点は、標準案に基づくピア デバイス間の動作にあります。



ネットワーキング デバイスで IETF を設定したにもかかわらず、隣接ルータが IETF と互換性がない場合、スイッチオーバー後に NSF が打ち切られます。

あるネットワーク セグメントの隣接ルータが NSF を認識しない場合、シスコの設定オプションを使用する必要があります。Cisco IS-IS 設定は、プロトコル隣接関係情報とリンク ステート情報の両方をアクティブ スーパーバイザ エンジンから冗長スーパーバイザ エンジンに転送します。シスコの設定のメリットは、NSF 認識ネイバーに依存していないことです。

IETF IS-IS 設定

スーパーバイザ エンジンのスイッチオーバー後できるだけ早く、NSF 対応ルータは IETF IS-IS 設定を使用して、IS-IS NSF 再起動要求を隣接 NSF 認識デバイスに送信します。隣接ネットワーキングデバイスは、この再起動要求をこのルータとのネイバー関係がリセットされるべきでないが、再起動ルータとの間でデータベースの再同期を開始すべきであることを示すインジケータとして認識します。再起動ルータがネットワーク上のルータから再起動要求に対する応答を受信すると、ネイバーリストを再構築できます。

この交換が完了すると、NSF 対応デバイスはリンク ステート情報を使用して失効したルートを削除し、RIB を更新し、FIB を新しい転送情報で更新します。ここで IS-IS が完全に収束されます。

あるスーパーバイザ エンジンから別のスーパーバイザ エンジンへのスイッチオーバーは、数秒間 以内に発生します。IS-IS は、その後の数秒間のうちにルーティング テーブルを再確立し、ネット ワークと再同期します。この時点で、IS-IS は次の NSF 再起動を試行する前に特定の期間待機します。この期間に、新しい冗長スーパーバイザ エンジンが起動してアクティブ スーパーバイザ エンジンとの設定を同期します。IS-IS NSF 動作では、IS-IS NSF がもう一度再起動を試行する前に接続が確実に安定するように特定の期間待機します。この機能により、IS-IS が失効した情報で連続して NSF 再起動を試行しないようにします。

Cisco IS-IS 設定

シスコの設定オプションを使用することで、冗長スーパーバイザ エンジンに対して、すべての隣接 関係および LSP 情報が保存 (*検査*) されます。スイッチオーバーのあと、新しくアクティブになったスーパーバイザ エンジンは検査済みのデータを使用して隣接関係を維持し、ルーティング テーブルを迅速に再構築できます。



(注)

スイッチオーバーのあと、Cisco IS-IS NSF には完全なネイバー隣接関係および LSP 情報が含まれます。ただし、スイッチオーバーの前に隣接であったすべてのインターフェイスがオンラインになるまで待機する必要があります。割り当てられたインターフェイス待機時間内にインターフェイスがオンラインにならない場合、これらの隣接デバイスから学習したルートは、ルーティング テーブルの再計算で考慮されません。IS-IS NSF には、何らかの理由で時間内にオンラインにならないインターフェイスに対して、待機時間を延長するコマンドがあります。

あるスーパーバイザ エンジンから別のスーパーバイザ エンジンへのスイッチオーバーは、数秒間 以内に発生します。IS-IS は、その後の数秒間のうちにルーティング テーブルを再確立し、ネット ワークと再同期します。この時点で、IS-IS は次の NSF 再起動を試行する前に特定の期間待機します。この期間に、新しい冗長スーパーバイザ エンジンが起動してアクティブ スーパーバイザ エンジンとの設定を同期します。この同期が完了したあと、IS-IS 隣接関係および LSP データは検査され、冗長スーパーバイザ エンジンに保存されます。ただし、新しい NSF 再起動は、待機期間が経過しないと IS-IS で試行されません。この機能により、IS-IS が連続して NSF 再起動を試行しないようにします。

EIGRP の動作

EIGRP NSF 対応ルータが NSF 再起動後に最初に再起動したときには、ネイバーはなくトポロジテーブルは空です。ルータはインターフェイスを立ち上げてネイバーを再取得し、トポロジとルーティング テーブルを再構築する必要があるときに、冗長(現在アクティブな)スーパーバイザエンジンから通知を受けます。ルータとピアの再起動の際は、再起動するルータへ向かうデータトラフィックを中断せずに、これらの処理を実行する必要があります。EIGRP ピア ルータは、再起動するルータから学習したルートを維持し、NSF 再起動プロセス中もトラフィックを転送し続けます。

ネイバーによって隣接関係がリセットされないように、再起動するルータは再起動を示すために EIGRP パケット ヘッダーの新しい再起動 (RS) ビットを使用します。RS ビットは、NSF 再起動中に hello パケットと初期 INIT アップデート パケットに設定されます。hello パケットの RS ビットにより、ネイバーに迅速に NSF 再起動を通知できます。RS ビットを調べない場合、ネイバーは INIT アップデートを受信するか hello ホールド タイマーの期間が満了することでしか、隣接関係のリセットを検出することができません。RS ビットがないと、ネイバーは NSF を使用して隣接関係のリセットが処理されたか、通常のスタートアップ方式で処理されたかを判断できません。

hello パケットまたは INIT パケットを受信することでネイバーが再起動の知らせを受信すると、ピアリスト内で再起動したピアを見つけ、再起動しているルータとの隣接関係を維持します。次にネイバーは、再起動しているルータに対して、最初のアップデート パケットに RS ビットを設定してトポロジ テーブルを送信します。この アップデート パケットでは、NSF を認識することが可能でルータの再起動を支援できることが示されています。ネイバーが NSF 再起動ネイバーでない場合は、hello パケットに RS ビットを設定しません。



ルータが NSF を認識できていても、コールド スタートで起動されたために NSF 再起動ネイバーを 支援しない場合もあります。

少なくとも1つのピアルータがNSFを認識できる場合、再起動ルータはアップデートを受信しデータベースを再構築します。次に再起動ルータは、RIBを通知できるように収束されているかどうかを調べる必要があります。各NSF認識ルータは、テーブルの内容が終わりであることを示すために、最後のアップデートパケットでEnd of Table(EOT)マーカーを送信する必要があります。EOTマーカーを受信すると、再起動ルータは収束していることがわかります。ここで再起動ルータがアップデートを送信し始めることができます。

NSF 認識ピアは、再起動ルータから EOT 表示を受信したときにいつ再起動ルータが収束したかを認識します。次にピアは、再起動ネイバーを送信元としてルートを検索するために、トポロジテーブルをスキャンします。ピアは、ルートのタイムスタンプと再起動イベントのタイムスタンプを比較して、ルートがまだ使用可能かどうかを判断します。次に、ピアはアクティブになり、再起動されたルータで使用できなくなったルートの代替パスを検索します。

再起動ルータがすべての EOT 表示をネイバーから受信した場合、または NSF 収束タイマーが満了した場合、EIGRP は RIB にコンバージェンスを通知します。EIGRP は RIB コンバージェンス信号を待機し、待機しているすべての NSF 認識ピアに対してトポロジ テーブルをフラッディングします。

NSF の注意事項と制約事項

NSF/SSO には次のような制約事項があります。

- NSFの動作では、デバイスにSSOを設定しておく必要があります。
- NSF/SSO は、IP バージョン 4 トラフィックおよびプロトコルのみをサポートします。IPv6 トラフィックはサポートしていません。
- Virtual Redundancy Router Protocol (VRRP; 仮想ルータ冗長プロトコル) は SSO を認識しないので、通常の動作中にアクティブ スーパーバイザ エンジンとスタンバイ スーパーバイザ エンジン間でステート情報が維持されません。VRRP と SSO は共存できますが、いずれも別々に機能します。VRRP に依存しているトラフィックは、スーパーバイザのスイッチオーバー時に VRRPスタンバイに切り替わる場合があります。
- BGP NSF に参加しているすべての隣接デバイスは、NSF 対応で、BGP のグレースフル リスタート用に設定されている必要があります。
- 仮想リンクの OSPF NSF はサポートされていません。
- 同じネットワーク セグメントにあるすべての OSPF ネットワーキング デバイスは、NSF を認識できる必要があります (NSF ソフトウェア イメージを実行している必要があります)。
- IETF IS-IS の場合、すべての隣接デバイスは NSF 認識ソフトウェア イメージを実行している必要があります。

NSF/SSO スーパーバイザ エンジンの冗長構成の設定

次のセクションでは、NSF 機能の設定作業について説明します。

- SSO の設定 (p.9-11)
- CEF NSF の設定 (p.9-12)
- CEF NSF の確認 (p.9-12)
- BGP NSF の設定 (p.9-13)
- BGP NSF の確認 (p.9-13)
- OSPF NSF の設定 (p.9-14)
- OSPF NSF の確認 (p.9-15)
- IS-IS NSF の設定 (p.9-15)
- IS-IS NSF の確認 (p.9-16)
- EIGRP NSF の設定 (p.9-18)
- EIGRP NSF の確認 (p.9-18)

SSO の設定

NSF をサポートしているプロトコルで NSF を使用するには SSO を設定する必要があります。SSO を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# redundancy	冗長コンフィギュレーション モードを開始します。
ステップ 2	Switch(config-red)# mode sso	SSO を設定します。このコマンドを入力すると、冗長スーパーバイザ エンジンはリロードされ、SSO モードでの動作が開始されます。
ステップ 3	Switch(config-red)# end	EXEC モードに戻ります。
ステップ 4	Switch# show running-config	SSO がイネーブルになっていることを確認します。
ステップ 5	Switch# show redundancy states	動作中の冗長モードを表示します。



sso キーワードは、Cisco IOS Release 12.2(20)EWA 以降のリリースでサポートされます。

次に、SSOにシステムを設定し、冗長ステートを表示する例を示します。

```
Switch> enable
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config) # redundancy
Switch(config-red) # mode sso
Switch(config-red)# end
Switch# show redundancy states
mv state = 13 -ACTIVE
    peer state = 8 -STANDBY HOT
          Mode = Duplex
          Unit = Primary
       Unit ID = 5
Redundancy Mode (Operational) = sso
Redundancy Mode (Configured) = sso
    Split Mode = Disabled
  Manual Swact = Enabled
Communications = Up
  client count = 29
client_notification_TMR = 30000 milliseconds
         keep_alive TMR = 9000 milliseconds
       keep_alive count = 1
   keep\_alive threshold = 18
          RF debug mask = 0x0
Switch#
```

CEF NSF の設定

ネットワーキング デバイスが SSO モードで動作している間、CEF NSF 機能はデフォルトで動作します。したがって設定作業は不要です。

CEF NSF の確認

CEF が NSF に対応していることを確認するには、show cef state コマンドを入力します。

Switch# show cef state

```
CEF Status [RP]
CEF enabled/running
dCEF enabled/running
CEF switching enabled/running
CEF default capabilities:
Always FIB switching:
Default CEF switching:
Default dCEF switching: yes
Update HWIDB counters:
Drop multicast packets:
                          no
CEF NSF capable:
                           yes
IPC delayed func on SSO:
                          no
RRP state:
I am standby RRP:
                          no
My logical slot:
RF PeerComm:
                          no
```

BGP NSF の設定



(注)

BGP NSF に参加しているすべてのピア デバイスに BGP のグレースフル リスタートを設定する必要があります。

BGP で NSF を設定するには、次の作業を行います(各 BGP NSF ピア デバイスでこの手順を繰り返します)。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	Switch(config)# router bgp as-number	BGP ルーティング プロセスをイネーブルして、スイッチをスイッチ コンフィギュレーション モードにします。
ステップ 3	Switch(config-router)# bgp graceful-restart	BGP のグレースフル リスタート機能をイネーブル にして、BGP の NSF を開始します。
		BGP セッションが確立されたあとにこのコマンドを 入力した場合、BGP ネイバーと機能を交換するため にセッションを再起動する必要があります。
		再起動スイッチとすべてのピアでこのコマンドを入 力します。

BGP NSF の確認

BGP の NSF を確認するには、BGP のグレースフル リスタートが SSO 対応ネットワーキング デバイスと隣接デバイスに設定されているかどうかを確認する必要があります。これを確認するには、次の作業を行います。

ステップ1 show running-config コマンドを入力して、[bgp graceful-restart] が SSO 対応スイッチの BGP 設定に表示されていることを確認します。

Switch# show running-config

. . router bgp 120

bgp graceful-restart
neighbor 10 2 2 2 remote-as

neighbor 10.2.2.2 remote-as 300

ステップ2 各 BGP ネイバーでステップ 1 を繰り返します。

ステップ3 SSO デバイスと隣接デバイスで、グレースフル リスタート機能に [advertised and received] と表示されているかどうかを確認し、グレースフル リスタート機能のあるアドレス ファミリーを確認します。アドレス ファミリーが表示されていない場合、BGP NSF も発生しません。

Switch# show ip bgp neighbors x.x.x.x

BGP neighbor is 192.168.2.2, remote AS YY, external link
BGP version 4, remote router ID 192.168.2.2
BGP state = Established, up for 00:01:18
Last read 00:00:17, hold time is 180, keepalive interval is 60 seconds
Neighbor capabilities:
Route refresh:advertised and received(new)
Address family IPv4 Unicast:advertised and received
Address family IPv4 Multicast:advertised and received
Graceful Restart Capabilty:advertised and received
Remote Restart timer is 120 seconds
Address families preserved by peer:
IPv4 Unicast, IPv4 Multicast
Received 1539 messages, 0 notifications, 0 in queue
Sent 1544 messages, 0 notifications, 0 in queue
Default minimum time between advertisement runs is 30 seconds

OSPF NSF の設定



<u>一</u> (注)

OSPF NSF に参加しているすべてのピア デバイスは OSPF NSF を認識できるようにする必要があります。 NSF ソフトウェア イメージをデバイスにインストールすれば自動的に認識するようになります。

OSPF NSF を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# router ospf processID	OSPF ルーティング プロセスをイネーブルして、スイッチ をルータ コンフィギュレーション モードにします。
ステップ 3	Switch(config-router)# nsf	OSPF の NSF 動作をイネーブルにします。

OSPF NSF の確認

OSPF の NSF を確認するには、NSF 機能が SSO 対応ネットワーキング デバイスに設定されている かどうかを確認する必要があります。OSPF NSF を確認するには、次の作業を行います。

ステップ 1 show running-config コマンドを入力して、[nsf] が SSO 対応デバイスの OSPF 設定に表示されていることを確認します。

```
Switch# show running-config
```

```
route ospf 120
log-adjacency-changes
nsf
network 192.168.20.0 0.0.0.255 area 0
network 192.168.30.0 0.0.0.255 area 1
network 192.168.40.0 0.0.0.255 area 2
.
```

ステップ2 show ip ospf コマンドを入力して NSF がデバイスでイネーブルであることを確認します。

```
Switch> show ip ospf
```

```
Routing Process "ospf 1" with ID 192.168.2.1 and Domain ID 0.0.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x0
Number of opaque AS LSA 0. Checksum Sum 0x0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
Non-Stop Forwarding enabled, last NSF restart 00:02:06 ago (took 44 secs)
Area BACKBONE(0)
Number of interfaces in this area is 1 (0 loopback)
Area has no authentication
SPF algorithm executed 3 times
```

IS-IS NSF の設定

IS-IS NSFを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2		IS-IS ルーティング プロセスをイネーブルして、スイッチを
		ルータ コンフィギュレーション モードにします。

	コマンド	目的
ステップ 3	Switch(config-router)# nsf [cisco ietf]	IS-IS の NSF 動作をイネーブルにします。
		ietf キーワードを入力して、IETF ドラフト ベースの再起動 をサポートしているネットワーキング デバイスとの隣接
		関係が保証されている同種ネットワークで IS-IS をイネーブルにします。
		cisco キーワードを入力して、NSF 認識ネットワーキング デバイスとの隣接関係がないことがある異種ネットワークでIS-IS を実行します。
ステップ 4	<pre>Switch(config-router)# nsf interval [minutes]</pre>	(任意) NSF 再起動試行間隔の最小時間を指定します。 <i>連続する</i> NSF 再起動のデフォルトの時間間隔は、5分です。
ステップ 5	<pre>Switch(config-router)# nsf t3 {manual [seconds] adjacency}</pre>	(任意) IS-IS 自身のリンク ステート情報の生成が過負荷になり、その情報がネイバーにフラッディングする前に、IS-IS が IS-IS データベースの同期を待機する時間を指定します。
		IETF 動作を選択した場合のみ、t3 キーワードを使用します。adjacency を指定した場合、再起動しているスイッチは隣接デバイスから待機時間を取得します。
ステップ 6	<pre>Switch(config-router)# nsf interface wait seconds</pre>	(任意)再起動が完了する前に、IS-IS 隣接関係があるインターフェイスがすべて立ち上がるまで、IS-IS NSF の再起動を待機する時間を指定します。デフォルトは 10 秒です。

IS-IS NSF の確認

IS-IS の NSF を確認するには、NSF 機能が SSO 対応ネットワーキング デバイスに設定されているか どうかを確認する必要があります。 IS-IS NSF を確認するには、次の作業を行います。

ステップ1 show running-config コマンドを入力して、[nsf] が SSO 対応デバイスの IS-IS 設定に表示されていることを確認します。 Cisco IS-IS または IETF IS-IS 設定のいずれかが表示されます。次の表示は、デバイスで IS-IS NSF の Cisco 実装を使用していることを示しています。

Switch# show running-config <テキスト出力は省略> router isis nsf cisco <テキスト出力は省略>

ステップ2 NSF 設定が cisco に設定されている場合、show isis nsf コマンドを入力して NSF がデバイスでイネーブルであることを確認します。シスコの設定を使用すると、表示出力はアクティブ RP と冗長 RP で異なります。次の表示は、アクティブ RP 上のシスコの設定の出力例です。この例で、[NSF restart enabled] が表示されていることを確認してください。

Switch# show isis nsf

NSF is ENABLED, mode 'cisco'

RP is ACTIVE, standby ready, bulk sync complete
NSF interval timer expired (NSF restart enabled)
Checkpointing enabled, no errors
Local state:ACTIVE, Peer state:STANDBY HOT, Mode:SSO

次の表示は、スタンバイ RP 上のシスコの設定の出力例です。この例で、[NSF restart enabled] が表示されていることを確認してください。

Switch# show isis nsf

NSF enabled, mode 'cisco'
RP is STANDBY, chkpt msg receive count:ADJ 2, LSP 7
NSF interval timer notification received (NSF restart enabled)
Checkpointing enabled, no errors
Local state:STANDBY HOT, Peer state:ACTIVE, Mode:SSO

ステップ3 NSF 設定が ietf に設定されている場合、show isis nsf コマンドを入力して NSF がデバイスでイネーブルであることを確認します。次の表示は、ネットワーキング デバイス上の IETF IS-IS 設定の出力例です。

Switch# show isis nsf

```
NSF is ENABLED, mode IETF
NSF pdb state: Inactive
NSF L1 active interfaces:0
NSF L1 active LSPs:0
NSF interfaces awaiting L1 CSNP:0
Awaiting L1 LSPs:
NSF L2 active interfaces:0
NSF L2 active LSPs:0
NSF interfaces awaiting L2 CSNP:0
Awaiting L2 LSPs:
Interface:Serial3/0/2
    NSF L1 Restart state: Running
    NSF p2p Restart retransmissions:0
    Maximum L1 NSF Restart retransmissions:3
    L1 NSF ACK requested: FALSE
    L1 NSF CSNP requested: FALSE
    NSF L2 Restart state:Running
    NSF p2p Restart retransmissions:0
    Maximum L2 NSF Restart retransmissions:3
    L2 NSF ACK requested: FALSE
Interface: GigabitEthernet2/0/0
    NSF L1 Restart state:Running
    NSF L1 Restart retransmissions:0
    Maximum L1 NSF Restart retransmissions:3
    L1 NSF ACK requested: FALSE
    L1 NSF CSNP requested: FALSE
    NSF L2 Restart state: Running
    NSF L2 Restart retransmissions:0
    Maximum L2 NSF Restart retransmissions:3
    L2 NSF ACK requested: FALSE
    L2 NSF CSNP requested: FALSE
Interface:Loopback1
    NSF L1 Restart state: Running
    NSF L1 Restart retransmissions:0
    Maximum L1 NSF Restart retransmissions:3
    L1 NSF ACK requested: FALSE
    L1 NSF CSNP requested: FALSE
    NSF L2 Restart state: Running
    NSF L2 Restart retransmissions:0
    Maximum L2 NSF Restart retransmissions:3
    L2 NSF ACK requested: FALSE
    L2 NSF CSNP requested: FALSE
```

EIGRP NSF の設定

EIGRP NSF を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# router eigrp as-number	EIGRP ルーティング プロセスをイネーブルして、スイッチ をルータ コンフィギュレーション モードにします。
ステップ 3	Switch(config-router)# nsf	EIGRP NSF をイネーブルにします。
		「再起動」スイッチとすべてのピアでこのコマンドを入力します。

EIGRP NSF の確認

EIGRP の NSF を確認するには、NSF 機能が SSO 対応ネットワーキング デバイスに設定されている ことを確認する必要があります。 EIGRP NSF を確認するには、次の作業を行います。

ステップ 1 show running-config コマンドを入力して、[nsf] が SSO 対応デバイスの EIGRP 設定に表示されていることを確認します。

```
Switch# show running-config
.
.
.
router eigrp 100
auto-summary
nsf
.
```

ステップ 2 show ip protocols コマンドを入力して NSF がデバイスでイネーブルであることを確認します。

```
Switch# show ip protocols
*** IP Routing is NSF aware ***
Routing Protocol is "eigrp 100"
 Outgoing update filter list for all interfaces is not set
 Incoming update filter list for all interfaces is not set
 Default networks flagged in outgoing updates
 Default networks accepted from incoming updates
 EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
 EIGRP maximum hopcount 100
 EIGRP maximum metric variance 1
  Redistributing: eigrp 100
 EIGRP NSF-aware route hold timer is 240s
  EIGRP NSF enabled
    NSF signal timer is 20s
    NSF converge timer is 120s
 Automatic network summarization is in effect
 Maximum path: 4
 Routing for Networks:
 Routing Information Sources:
                  Distance
                                 Last Update
   Gateway
 Distance: internal 90 external 170
```



CHAPTER

10

環境モニタリングおよび電源管理



(注)

この章を読み進める前に、『Catalyst 4500 Series Installation Guide』の「Preparing for Installation」に目を通してください。Power over Ethernet (PoE) の導入によって電気負荷と熱が加わっても、それに対応する十分な電力と冷却装置が設置場所にあることを確認してください。

この章では、Catalyst 4500 シリーズ スイッチの電源管理および環境モニタリング機能について説明します。設定上の注意事項、設定手順、および設定例も示します。

この章の主な内容は、次のとおりです。

- 環境モニタリングの概要 (p.10-2)
- 電源管理 (p.10-6)



(注)

この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/cr/index.htm

環境モニタリングの概要

ここでは、次の内容について説明します。

- CLI コマンドによる環境のモニタリング (p.10-2)
- 環境状態の表示 (p.10-2)
- 緊急処理 (p.10-3)
- システム アラーム (p.10-4)

シャーシ コンポーネントの環境モニタは、コンポーネント障害の兆候を早期に警告します。この警告により、安全で信頼性の高いシステム運用を実現し、ネットワーク障害を防止できます。

ここでは、重要なシステム コンポーネントを監視する方法について説明します。これにより、ハードウェア関連の問題点を特定し、速やかに対応できるようになります。

CLI コマンドによる環境のモニタリング

show environment CLI (コマンドライン インターフェイス)コマンドを使用して、システムを監視します。ここでは、使用するコマンドおよびキーワードの基本概要について説明します。

システム ステータス情報を表示するには、show environment [alarm | status | temperature] コマンドを使用します。表 10-1 にキーワードを示します。

表 10-1 show environment コマンドのキーワード

キーワード	目的
alarm	システムの環境アラームを表示します。
status	Field-Replaceable Unit (FRU; 現場交換可能ユニット)の動作ステータスおよび電源と電源装置ファン センサーの情報を表示します。
temperature	シャーシの温度を表示します。

環境状態の表示

次の内容について説明します。

- Supervisor Engine II-Plus から V-10GE の状態 (p.10-2)
- Supervisor Engine 6-E の状態 (p.10-3)

Supervisor Engine II-Plus から V-10GE の状態

次に、Supervisor Engine II-Plus から V-10GE の環境状態を表示する例を示します。この出力では、電源装置が異なっていることがわかります。スイッチは片方の電源装置だけを使用し、もう一方をディセーブルにします。

Switch# show environment

no alarm

 Power
 Fan
 Inline

 Supply
 Model No
 Type
 Status
 Sensor
 Status

 PS1
 PWR-C45-2800AC
 AC 2800W
 good
 good
 good
 good

 PS2
 PWR-C45-1000AC
 AC 1000W
 err-disable
 good
 n.a.

*** Power Supplies of different types have been detected*** Switch#

Supervisor Engine 6-E の状態

Supervisor Engine 6-E およびこれに関連するラインカードは、複数の温度センサーをカード単位でサポートしています。環境状態の出力には、各センサーから読み取った温度および各センサーの温度しきい値が表示されます。これらのラインカードは、警告、重大、シャットダウンの 3 つのしきい値をサポートしています (Supervisor Engine II-Plus ~ V - 10GE は 2 つのしきい値をサポートしています)。

次に、Supervisor Engine 6-E の環境状態を表示する例を示します。しきい値はカッコ内に表示されています。

Switch# show environment

no temperature alarms

Module Sensor		emperature		Status					
2 air inlet 2 air outlet 5 air inlet 6 air outlet 6 air inlet 6 air outlet	23 29 38 38	3C (51C,65C,6 9C (69C,83C,8 3C (51C,65C,6 3C (69C,83C,8 4C (51C,65C,6 7C (69C,83C,8	8C) 6C) 8C) 6C) 8C)	ok					
Power Supply Model No			Sensor						
PS1 PWR-C45-2800AC PS2 none									
Power supplies needed by Power supplies currently	_								
Chassis Type : WS-C4510R	-E								
Power consumed by backpla	ane : 40 Wat	its							
Switch Bandwidth Utiliza	tion : 0%								
Supervisor Led Color : Green									
Module 2 Status Led Color : Green Module 5 Status Led Color : Green Module 6 Status Led Color : Orange Module 10 Status Led Color : Green									
Fantray : Good									
Power consumed by Fantray : 80 Watts									

緊急処理

Supervisor Engine 6-E のあるシャーシは、1 枚のカードの電源を切断して、ラインカードの過熱状態に対してきめ細かな対応を行うことができます。ただし、スーパーバイザ自体の温度が重大しきい値を超過する場合は、Supervisor Engine 6-E は安全に動作できません。したがって、スーパーバイザはシャーシの電源装置をオフにして、スーパーバイザ自体が過熱しないようにします。このような場合、電源装置の電源オン / オフ スイッチまたは電源装置の AC または DC 入力電源をオフにしてから再びオンにして、スイッチを回復できます。

重大およびシャットダウン温度という緊急状態により同じ処理が行われます。したがって、次の表 (表 10-2)に緊急状態の温度を示しますが、重大およびシャットダウンの緊急状態は区別しません。

表 10-2 Sup	ervisor Engines	s 6-E の撃	急状態お	よび処理
------------	-----------------	----------	------	------

ケース 1. ファンの完全な障害による緊急状態	シャーシの電源を切断します。
ケース 2. ラインカードの温度による緊急状態	ラインカードの電源を切断します。
ケース 3. スタンバイ スーパーバイザ エンジンの温 度による緊急状態	スタンバイ スーパーバイザの電源を切断します。
ケース 4. ホットスタンバイまたはコールドスタンバイス長ステートのスタンバイ スーパーバイザ エンジンがあるアクティブ スーパーバイザ エンジンの温度による緊急状態	アクティブ スーパーバイザ エンジンをリセットします。
ケース 5. スタンバイ スーパーバイザ エンジンを備えていないか、ホットスタンバイまたはコールドスタンバイ冗長ステートではないスタンバイ スーパーバイザ エンジンがあるアクティブ スーパーバイザエンジンの温度による緊急状態	シャーシの電源を切断します。

ケース 4 では、アクティブ エンジンが自身のリセットを行うと、スタンバイ スーパーバイザ エンジンが機能を引き継ぎます。そして、温度による緊急状態のままである場合は、新たにアクティブ になったスーパーバイザ エンジンが現在のスタンバイ スーパーバイザ エンジンをリセットします。

ケース 5 は、非冗長シャーシまたはシャットダウンされているか完全に起動されていないスタンバイスーパーバイザエンジンがあるシャーシに適用されます。

システム アラーム

システムは、メジャーおよびマイナーの2種類のアラームを使用します。メジャー アラームは、システムのシャットダウンにつながる可能性のある重大な問題を示します。マイナー アラームは情報で、対処しないと重大な問題となる可能性がある点について通知します。

表 10-3 に、発生する可能性のある環境アラームを示します。

表 10-3 発生する可能性のある環境アラーム

警告しきい値を超える温度センサー	マイナー
重大しきい値を超える温度センサー	メジャー
シャットダウンしきい値を超える温度センサー	メジャー
ファンの部分的な障害	マイナー
ファンの完全な障害	メジャー

ファン障害アラームは、ファン障害状態が検知されると発生し、ファン障害状態が解消すると取り消されます。温度アラームは、温度が温度のしきい値に達すると発生し、温度がしきい値を 5 °C 下回ると取り消されます。5 °C は、アラームの切り替えが行われないようにするためのヒステリシス値です。

スーパーバイザ エンジンの LED は、アラームが発生したかどうかを示します。

システムによってメジャー アラームが発生するとタイマーが始動しますが、その期間はアラームによって異なります。 タイマーが切れるまでにアラームが取り消されない場合は、 過熱による影響が生じないようにするためにシステムは緊急処理を行います。 タイマー値および緊急処理は、 スーパーバイザのタイプによって異なります。



スーパーバイザ エンジンの SYSTEM LED の起動動作など、LED の詳細については、『Catalyst 4500 Series Switch Module Installation Guide』を参照してください。

表 10-4 で、Supervisor Engines II-Plus から V-10GE のアラームについて説明します。

表 10-4 Supervisor Engine II-Plus から V-10GE のアラーム

イベント	アラームの 種類	スーパーパイザ LED の色	タイムアウト	説明およびアクション
シャーシの温度が重大しきい値を超過	メジャー	レッド	5分	アラームが発生すると、Syslog メッセージが表示されます。
				タイムアウトが経過すると、ライン カードはリセット状態にされます。
スーパーバイザが Power-on Self-Test	メジャー	レッド	_	Syslog メッセージが表示されます。
(POST; 電源投入時自己診断テスト)に 失敗				スーパーバイザの起動が失敗します。
シャーシ ファン トレイの障害	メジャー	レッド	4 分	アラームが発生すると、Syslog メッセージが表示されます。
				タイムアウトが経過すると、ライン カードはリセット状態にされます。
シャーシの温度が警告しきい値を超過	マイナー	オレンジ		アラームが発生すると、Syslog メッセージが表示されます。
シャーシ ファン トレイの部分的な障害	マイナー	オレンジ	_	アラームが発生すると、Syslog メッセージが表示されます。

表 10-5 で、Supervisor Engine 6-E のアラームについて説明します。

表 10-5 Supervisor Engine 6-E のアラーム

イベント	アラームの 種類	スーパーパイザ LED の色	タイムアウト	説明およびアクション
カードの温度が重大しきい値を超過	メジャー	レッド	15 分	アラームが発生すると、Syslog メッセージが表示されます。
				タイムアウトの処理については、表 10-2 を参照してください。
カードの温度がシャットダウンしきい 値を超過	メジャー	レッド	30 秒	アラームが発生すると、Syslog メッセージが表示されます。
				タイムアウトの処理については、表 10-2 を参照してください。
スーパーバイザが Power-on Self-Test	メジャー	レッド		Syslog メッセージが表示されます。
(POST)に失敗				スーパーバイザの起動が失敗します。
シャーシ ファン トレイの障害	メジャー	レッド	30 秒	アラームが発生すると、Syslog メッセージが表示されます。
				タイムアウトの処理については、表 10-2 を参照してください。

表 10-5 Supervisor Engine 6-E のアラーム (続き)

イベント	アラームの 種類	スーパーパイザ LED の色		説明およびアクション
シャーシの温度が警告しきい値を超過	マイナー	オレンジ	_	アラームが発生すると、Syslog メッセージが表示されます。
シャーシ ファン トレイの部分的な障害	マイナー	オレンジ		アラームが発生すると、Syslog メッセージが表示されます。

電源管理

ここでは、Catalyst 4500 シリーズ スイッチの電源管理機能について説明します。主な内容は次のとおりです。

- Catalyst 4500 シリーズ スイッチの電源管理 (p.10-6)
- モジュールの電源切断 (p.10-20)
- Catalyst 4948 スイッチの電源管理 (p.10-21)



Catalyst 4000/4500 ファミリ モジュールすべての電力消費量については、『*Catalyst 4500 Series Module Installation Guide*』の Appendix A「Specifications」を参照してください。現在の電力冗長構成およびシステム電力消費量を表示するには、**show power** コマンドを使用します。

Catalyst 4500 シリーズ スイッチの電源管理

ここでは、次の内容について説明します。

- サポート対象の電源装置 (p.10-7)
- Catalyst 4500 スイッチの電源管理モード (p.10-8)
- 電源管理モードの選択 (p.10-8)
- Catalyst 4500 シリーズ スイッチでの電源管理の制限事項 (p.10-9)
- Catalyst 4500 シリーズ スイッチの電源装置で利用できる電力 (p.10-13)
- Supervisor Engine II-TS でインライン パワーが不足した場合の処理 (p.10-18)
- 複合モードの電力維持機能 (p.10-15)
- 1400 W DC 電源装置に関する特記事項 (p.10-17)
- 1400 W DC SP トリプル入力電源装置に関する特記事項 (p.10-18)
- Supervisor Engine II-TS でインライン パワーが不足した場合の処理 (p.10-18)
- Catalyst 4948 スイッチの電源管理モード (p.10-21)

サポート対象の電源装置

数種類の電源装置を選択して、スイッチに搭載したモジュールに十分な電力を確保できます。



(注)

Cisco Power Calculator を使用して、モジュールと適切な PoE 電力量に基づいて電源装置を選択する必要があります。お客様がシャーシに使用するラインカード タイプに応じて、 $1000\sim1400~{\rm AC}$ の間で選択します。

Catalyst 4500 シリーズ スイッチでは、次の電源装置を使用できます。

- 固定ワット数 この電源装置は、常に一定量の PoE およびシステム電力を供給します。
 - 1000 W AC 最大 1050 W のシステム電力をサポートします(Catalyst 4510R スイッチでは 推奨しません。PoE をサポートしません)。
 - 1400 W AC 最大 1400 W のシステム電力をサポートします (PoE をサポートしません)。
 - 2800 W AC 最大 1400 W のシステム電力および PoE をサポートします。
- 可変ワット数 この電源装置は、PoE およびシステム所要電力に対応するためにワット数を自動的に調整します。
 - 1300 W AC 最大 1050 W のシステム電力および 800 W の PoE を合計 1300 W に制限してサポートします。
 - 1400 W DC 最大 1400 W のシステム電力、電源装置への給電量に応じた可変ワット数の PoE をサポートします。詳細については、「1400 W DC 電源装置に関する特記事項(p.10-17)を参照してください
 - 1400 W DC Service Provider DC 入力の 3 本までの回線 (12.5 A、15 A、15 A)を使用し、電力供給している回線により、400 ~ 1400 W の範囲でさまざまなシステム電源を供給します。詳細については、「1400 W DC SP トリプル入力電源装置に関する特記事項」(p.10-18)を参照してください (PoE をサポートしません)。
 - 4200 W AC 電源供給している入力電力数および入力電圧数により、さまざまなシステム電力および PoE をサポートします。



(注)

Catalyst 4500 シリーズ スイッチの AC 入力電源装置には、単一フェーズ送信元 AC が必要です。AC 電源装置の入力はすべて独立しているので、送信元 AC では、複数の電源装置、または同じ電源装置上にある複数の AC 電源プラグの間の位相が一致しません。各シャーシの電源装置には、地域および各国の規定に適合するサイズの専用の分岐回路が装備されている必要があります。

スイッチに電源装置を取り付ける場合は、同じワット数の電源装置を使用してください。 $1400~\rm W~\rm DC~\rm F$ リプル入力などのマルチ入力電源装置および $4200~\rm W~\rm AC~\rm C$ は、このほかにも制限事項があります。これらの電源装置の特記事項を参照してください。ワット数の異なる電源装置を併用すると、スイッチはワット数の小さい方を使用し、もう一方を無視します。 ${\bf show~power~}$ コマンドの出力では、電源装置の状況は ${\bf err-disable~}$ として表示され、サマリーでは出力のワット数がすべて 0として示されます。

次に、ワット数の異なる電源装置を併用した場合の show power コマンドの出力例を示します。

	DWT CCII#	SHOW DOWEL				
	Power				Fan	Inline
	Supply	Model No	Type	Status	Sensor	Status
	PS1	PWR-C45-2800AC	AC 2800W	good	good	good
\rightarrow	PS2	PWR-C45-1000AC	AC 1000W	err-disable	aoog	n.a.

*** Power Supplies of different type have been detected***

Power supplies needed by system :1 Power supplies currently available :1

Power Summary (in Watts)	Used	Maximum Available	
System Power (12V)	328	1360	
Inline Power (-50V)	0	1400	
Backplane Power (3.3V)	10	40	
Total Used Switch#	338	(not to exceed T	Total Maximum Available = 750)

Catalyst 4500 スイッチの電源管理モード

Catalyst 4500 シリーズ スイッチでは、次の2つの電源管理モードをサポートしています。

- 冗長(Redundant)モード 冗長モードでは1つめの電源装置を主電源装置、2つめの電源装置をバックアップ電源装置として使用します。主電源装置に障害が発生すると、2つめの電源装置がネットワークを中断させることなく、ただちにスイッチをサポートします。両方の電源装置は同じワット数でなければなりません。また、電源装置は、単独でスイッチの構成をサポートできるだけの電力を備えている必要があります。
- 複合(Combined)モード 複合モードでは、搭載されたすべての電源装置からの電力を使用して、スイッチ構成に必要な電源をサポートします。ただし、複合モードでは電源の冗長性は設定されません。電源装置に障害が発生すると、1 つまたは複数のモジュールがシャットダウンする可能性があります。



(注)

Catalyst 4510R スイッチでは、すべての可能な構成用の冗長モードをサポートするのに 1000 W AC 電源装置は十分ではありません。必要電力が 1050 W より少ない、限られた構成で冗長モードをサポートできます。



(注)

1400~W~DC 電源装置では、データ電力で複合モードがサポートされます。PoE 電力では、複合モードがサポートされません。

電源管理モードの選択

デフォルトでは、スイッチは冗長モードに設定されています。show power コマンドでは、power supplies needed by system が 1 の場合、スイッチは冗長モードです。power supplies needed by system が 2 の場合、スイッチは複合モードです。

使用する電源装置とその数は、使用するスイッチのハードウェア構成によって決まります。たとえばスイッチ構成が、1 つの電源装置で供給できる以上の電力を必要とする場合は、複合モードを使用します。ただし、複合モードではスイッチに電源の冗長性は設定されません。次の点に留意してください。

- 消費電力はそれぞれ、スーパーバイザ エンジンで 110 W、Catalyst 4503 スイッチのファン ボックスで各 30 W、Catalyst 4506 および Catalyst 4507 スイッチのファン ボックスで各 50 W、Catalyst 4503 および Catalyst 4506 スイッチのバックプレーンで 10 W、Catalyst 4507 スイッチのバックプレーンで 40 W です。
- 1000 W では、受電装置をサポートしないフル装備の Catalyst 4503 スイッチをサポートします。
- 1300 W では、シスコの受電装置をサポートするフル装備の Catalyst 4503 スイッチをサポート します。
- WS-X4148-RJ45V モジュール上の各 PoE ポートでの必要電力は、6.3 W です。スイッチのフル 装備の 5 つの WS-X4148-RJ45V モジュールは、240 ポートを構成します。この構成には、PoE 用に 1512 W、モジュール用に 300 W が必要です。

Catalyst 4500 シリーズ スイッチでの電源管理の制限事項

制限事項1

電源装置が供給する以上の電力を必要とするスイッチを構成する可能性があります。給電能力を超 えるスイッチを構成する状況として、次の2つが挙げられます。

• 搭載したモジュールの所要電力が、電源装置によって供給される電力を超える場合 電源装置を1つ取り付け、スイッチを複合モードに設定すると、スイッチは次のエラー メッセージを表示します。

Insufficient power supplies present for specified configuration.

このエラー メッセージは、show power コマンドの出力にも表示されます。このエラー メッセージが表示されるのは、定義上複合モードで動作する電源装置が 2 つスイッチに搭載されている必要があるためです。

搭載されたモジュールの所要電力が電源装置によって供給される電力を超える場合、スイッチは次のエラー メッセージを表示します。

Insufficient power available for the current chassis configuration.

このエラー メッセージは、show power コマンドの出力にも表示されます。

スイッチにモジュールを増設しようとして電源装置によって供給される電力を超える場合、スイッチはただちに増設分のモジュールをリセット モードにし、次のエラー メッセージを表示します。

Module has been inserted Insufficient power supplies operating.

また、機能しているスイッチの電源を切り、モジュールを増設するか、モジュール構成を変更 して所要電力が使用できる電力を超えるようになった場合、再度スイッチの電源を入れると、 1 つまたは複数のモジュールがリセット モードになります。

PoE の所要電力が、電源装置によって供給される PoE を超える場合
 システムの電力を消費している IP Phone が多すぎる場合、IP Phone への電力が削減され、電源
装置に適切な所要電力に削減されるように、一部の IP Phone の電源が切断されることもあります。

前者のシナリオでは(所要電力が供給電力を超える場合)、システムは搭載されているモジュールのタイプおよび個数を判断して、電力消費に関する問題を解決しようとします。判断サイクル中に、システムはシャーシの下から順に、サポート不可能な(または電力が供給されていない)モジュールをリセット モードにします。十分な電力が供給されているスーパーバイザ エンジンおよびモジュールは常にイネーブルであり、ネットワーク接続は中断されません。モジュールはリセットモードになっても多少の電力を消費します。さらに所要電力を低下させるには、シャーシからこれらのモジュールを取り外してください。シャーシの構成が適切であれば、システムが評価サイクルに入ることはありません。

リセット モードのモジュールは、シャーシに取り付けられているかぎり、電力を消費し続けます。 モジュールをオンライン状態にするときに必要な電力は、show power module コマンドを使用する とわかります。

使用するシステムの所要電力を算出し、システムの電源が十分であるかどうかを確認するには、スーパーバイザ エンジン モジュール、ファン ボックス、および搭載したモジュール (PoE を含む)が消費する電力を合算します。PoE には、すべての電話の所要電力を合計します。使用するスイッチの各種コンポーネントの電力消費量については、「モジュールの電源切断」(p.10-20)を参照してください。

802.3af 準拠の PoE モジュールは、FPGA やモジュールのその他のハードウェア コンポーネントに電力を供給する場合、最大で 20~W の PoE を消費することがあります。スイッチに接続された受電装置に十分な電力が供給されるように、802.3af 準拠の PoE モジュールごとに、PoE 所要電力に少なくとも 20~W を追加してください。

WS-X4148-RJ45V PoE モジュールでは、PoE の消費電力を測定できません。したがって、PoE を計算する場合は常に、このモジュールの PoE 消費電力が管理上の PoE と等しいと推定します。

どのモジュールがアクティブで、どのモジュール(ある場合)がリセット状態かを確認するには、 show module コマンドを使用します。

次に、すべての搭載済みモジュールをサポートする十分な電力がないシステムに対する show **module** コマンドの出力例を示します。このシステムでは Module 5 に対する電力が不十分です。 [*Status*] カラムに [*PwrDeny*] として表示されています。

モジュールで消費される PoE が、power inline consumption default コマンドを使用して割り当てられた PoE を 50~W 以上超過している場合、[Status] カラムに [PwrOver] と表示されます。モジュールで消費される PoE が PoE モジュールの制限値を 50~W 以上超過している場合は、[Status] カラムに [PwrFault] と表示されます。

	Swi	.tch# sh	ow modul	Le									
		l Ports	-	-							le1	-	erial No.
	1	•	1000Bas								X4014		AB054109GH
	2	6	1000Bas	seX	(GBIC)				WS-	X4306	00	0000110
	3	18	1000Bas	seX	(GBIC)				WS-	X4418	J	AB025104WK
\rightarrow	5	0	Not end	ougl	n powe	r for	modi	ıle		WS-	X4148-FX-MT	00	000000000
	6	48	10/100	Base	eTX (R	J45)				WS-	X4148	J	AB023402RP
		MAC add									Sw		Status
											12.1(20020313:0		
	2	0010.7ba	ab.9920	to	0010.	7bab.	.9925	0.2					Ok
	3	0050.73	56.2b36	to	0050.	7356.	2b47	1.0					Ok
\rightarrow	5	0001.64	fe.a930	to	0001.	64fe.	.a95f	0.0					PwrDeny
	6	0050.0f3	10.28b0	to	0050.	0f10.	.28df	1.0					Ok
	Swi	tch#											

制限事項2

Cat4507R および Cat4510R シャーシの設定によっては、利用可能なデータ電力の最大量を超えます。 これらの設定には、次の PID の組み合わせがあります。

- 7スロット構成
- シャーシ: WS-C4507R-E、WS-C4510R-E
- デュアル スーパーバイザ: WS-X45-Sup6-E
- 1 つ以上: WS-X4448-GB-RJ45 または WS-X4148-FX-MT

Supervisor Engine 6-E を使用して 7 および 10 スロット シャーシの 10/100/1000 ポート密度を最大化 するためには、WS-X4448-GB-RJ45 ラインカードではなく WS-X4548-GB-RJ45 ラインカードを取り 付けます。 WS-X4448-GB-RJ45 ラインカードが必要な場合は、次の 2 つのオプションが可能です。

オプション 1

Cat4507R の 4 ラインカード スロット、Cat4510R シャーシの 6 ラインカード スロットのみが使用されます。

オプション 2

すべてのスロットが必要な場合でも、使用できるのは 1 つの WS-X4448-GB-RJ45 ラインカードのみです。

冗長 Supervisor Engine 6-E を使用して 7 および 10 スロット シャーシの 100 BASE-FX ポート密度を最大化するためには、WS-X4148-FX-MT ラインカードではなく FX 光ポートを持つ WS-4248-FE-SFP ラインカードを取り付けます。 WS-X4148-FX-MT ラインカードが必要な場合は、次の 2 つのオプションが可能です。

オプション 1

Cat4507R の 4 ラインカード スロット、Cat4510R シャーシの 6 ラインカード スロットのみが使用されます。

オプション 2

すべてのスロットが必要な場合でも、使用できるのは 1 つの WS-X4448-GB-RJ45 ラインカードのみです。

Catalyst 4500 シリーズ スイッチでの冗長モードの設定

デフォルトでは、Catalyst 4500 シリーズ スイッチの電源装置は冗長モードで動作するように設定されています。冗長モードを効果的に使用するには、次の注意事項に従ってください。

- 同じタイプの電源装置を2つ使用します。
- 電源管理モードを冗長モードに設定していて、電源装置が1つしか搭載されていない場合、スイッチはその設定を受け入れますが、冗長性なしで動作します。



スイッチに搭載されている電源装置のタイプやワット数が異なる場合、スイッチは電源装置の一方を認識せず、スイッチに電源の冗長性は設定されません。

- 固定電源装置には、単独でスイッチ構成をサポートできるだけの電力を備えた電源装置を選択してください。
- 可変電源装置には、十分な電力を供給できる電源装置を選択し、シャーシおよび PoE 所要電力が最大電力を超えないようにします。可変電源装置は、起動時にシャーシおよび PoE 所要電力に対応するように、自動的に電源リソースを調整します。最初にモジュールが、続いて IP Phoneが起動します。
- シャーシおよび PoE に使用できる各電源装置の最大電力については、表 10-6 (p.10-13) を参照してください。

Catalyst 4500 シリーズ スイッチに冗長モードを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# power redundancy-mode redundant	電源管理モードを冗長モードに設定します。
ステップ 3	Switch(config)# end	コンフィギュレーション モードを終了します。
ステップ 4	Switch# show power supplies	スイッチの電源冗長モードを確認します。

次に、電源管理モードを冗長モードに設定する例を示します。

Switch (config)# power redundancy-mode redundant
Switch (config)# end
Switch#

次に、現在の電源冗長モードを表示する例を示します。システムで必要な電源装置 1 は、スイッチが冗長モードであることを示しています。

Switch# show power supplies
Power supplies needed by system:1
Switch#

複合モードには、4200 W AC 電源でのみ任意で使用できる冗長方法があります。「複合モードの電力維持機能」(p.10-15) を参照してください。

Catalyst 4500 シリーズ スイッチでの複合モードの設定

電源装置が単独で供給できる以上の電力がスイッチ構成により必要とされる場合は、電源管理モードを複合モードに設定します。複合モードは両方の電源装置の電力を使用します。ただし、スイッチに電源の冗長性は設定されません。

複合モードを効果的に使用するには、次の注意事項に従ってください。

- 同じタイプとワット数 (固定または可変、AC または DC) の電源装置を使用します。
- タイプの異なる、またはワット数の異なる電源装置を使用した場合、スイッチはいずれか一方の電源装置しか使用しません。
- 可変電源装置には、十分な電力を供給できる電源装置を選択し、シャーシおよび PoE 所要電力が最大電力を超えないようにします。可変電源装置は、起動時にシャーシおよび PoE 所要電力に対応するように、自動的に電源リソースを調整します。
- 電源管理モードを複合モードに設定していて、電源装置が1つしか搭載されていない場合、スイッチはその設定を受け入れますが、電力は1つの電源装置からしか利用できません。
- スイッチが複合モードに設定されている場合、供給される電力の合計は、個々の電源装置の正確な合計値とはなりません。電源装置にはあらかじめ電流の共有比率が決められています(詳細については、表 10-6 [p.10-13] を参照)。
- シャーシおよび PoE に使用できる各電源装置の最大電力については、表 10-6 (p.10-13) を参照してください。

Catalyst 4500 シリーズ スイッチに複合モードを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# power redundancy-mode combined	電源管理モードを複合モードに設定します。
ステップ 3	Switch(config)# end	コンフィギュレーション モードを終了します。
ステップ 4	Switch# show power supplies	スイッチの電源冗長モードを確認します。

次に、電源管理モードを複合モードに設定する例を示します。

Switch (config)# power redundancy-mode combined
Switch (config)# end
Switch#

次に、現在の電源冗長モードを表示する例を示します。システムで必要な電源装置 2 は、スイッチが複合モードであることを示しています。

Switch# show power supplies
Power supplies needed by system:2
Switch#

Catalyst 4500 シリーズ スイッチの電源装置で利用できる電力

表 10-6 に、さまざまな Catalyst 4500 シリーズ スイッチの電源装置で利用できる電力を示します。スイッチが複合モードに設定されている場合、供給される電力の合計は、個々の電源装置の正確な合計値とはなりません。電源装置は、ハードウェアによりあらかじめ共有比率が決められています。複合モードでは、使用できる総電力が $P+(P \times + T)$ になり、P は電源装置の電力量を示します。

表 10-6 スイッチの電源装置で利用できる電力

電源装置	冗長モード(W)	複合モード (W)	共有比率
1000 W AC	$\mathcal{Y} = \mathcal{Y}^1 = 1050$	シャーシ = 1667	2/3
	PoE = 0	PoE = 0	
1300 W AC	シャーシ (最大)=1050	シャーシ (最小)=767	2/3
	PoE (最大)=800	PoE (最大)=1333	
	シャーシ + PoE + バックプレーン ≤	シャーシ (最大)=1667	
	1300	PoE (最小) = 533	
		シャーシ + PoE + バック プレーン ≤ 2200	
1400 W DC	シャーシ (最小)=200	シャーシ = 22674	シャーシ 2/3
	シャーシ (最大)=1360	PoE ⁵	PoE 0
	PoE(最大) ² =(DC 入力 ³ – [シャーシ(最小)+ バックプレーン]/0.75) × 0.96		
1400 W AC	シャーシ = 1360	シャーシ = 2473	9/11
	$PoE = 0^6$	PoE = 0	
2800 W AC	シャーシ = 1360	シャーシ = 2473	シャーシ ⁷ 9/11
	PoE = 1400	PoE = 2333	PoE ⁸ 2/3

- 1. シャーシ電力は、スーパーバイザエンジン、すべてのラインカード、およびファントレイの電力で構成されます。
- 2. 1400 W DC 電源装置の効率は 0.75 で、0.96 は PoE に適用されます。
- 3. 1400~W~DC 電源装置の DC 入力は変更可能で、設定可能です。詳細については、「1400~W~DC 電源装置に関する特記事項」(p.10-17) を参照してください。
- 4. PoE では使用不可
- 5. PoE では使用不可
- 6. 音声電力なし
- 7. データ専用
- 8. インライン パワー

4200 W AC 電源装置に関する特記事項

4200 W AC 電源装置には 2 つの入力があり、それぞれ 110 V または 220 V で電力供給されます。

4200 W AC 電源装置の show power コマンド出力は、1400 W DC トリプル入力電源装置と同様です(つまり、サブモジュール[複数の入力]の状態が表示されます)。2 つの電源装置が搭載されている場合は、サブモジュールの「故障中」と「オフ」、およびサブモジュールの状態(正常、異常、オフ)を区別できます。

Switch#	show power				
Power				Fan	Inline
Supply	Model No	Type	Status	Sensor	Status
PS1 PS1-1 PS1-2	PWR-C45-4200ACV	AC 4200W 220V	good good off	good	good
PS2 PS2-1 PS2-2	PWR-C45-4200ACV	AC 4200W 220V 220V	bad/off good bad	good	bad/off

Power supplies needed by system : 1 Power supplies currently available : 2

Power Summary		Maximum
(in Watts)	Used	Available
System Power (12V)	140	1360
Inline Power (-50V)	0	1850
Backplane Power (3.3V)	0	40

Total 140 (not to exceed Total Maximum Available = 2100)

Switch#

他の電源装置と同様に、これら 2 つの電源装置は同じタイプである必要があります (4200 W AC または 1400 W DC)。そうでない場合、右側の電源装置は errdisable ステートになり、左側の電源装置が選択されます。さらに、シャーシへのすべての入力が同じ電圧である必要があります。冗長モードでは、左右の電源装置の入力が同じである必要があります。冗長モードで左右の電源装置に電力供給されている場合、その電力値は 2 つの電源装置の弱い方に基づきます。



(注)

システムが 110 V または 220 V の複合モードで 4200 W の電源装置により電力供給されている場合、利用可能な電力はシステム構成 (ラインカードのタイプ、ラインカード数、インライン パワーを消費するポート数など)により決定され、絶対最大電力は反映されません。



(注)

一致した冗長電源装置設定で電源装置のサブモジュールが故障した場合、もう一方の(正常な)電源装置がすべての機能に電力供給します。

表 10-7 に、冗長モードでの電源装置の評価方法を示します。

表 10-7 冗長モードでの出力

電源装置	12 V	3.3 V	–50 V	合計
110 V	660	40	700	1050
110 V + 110 V または 220 V	1360	40	1850	2100
220 V + 220 V	1360	40	3700	4200

複合モードでは、シャーシへのすべての入力が同じ電圧である必要があります。

表 10-8 に、複合モードでの電源装置の評価方法を示します。

表 10-8 複合モードでの出力

電源装置	12 V	3.3 V	–50 V	合計
両方 (ベイ)で 110 V	1200	40	1200	1873
一方で 110 V + 110 V、	1360	40	2000	2728
反対側で 110 V				
両方で 110 V + 110 V	1360	40	3100	3782
両方で 220 V	1360	40	3100	3782
一方で 220 V + 220 V、	1360	40	4700	5493
反対側で 220 V				
両方で 220 V + 220 V	1360	40	6800	7600

複合モードの電力維持機能



(注)

この機能は、両方の電源装置ベイに 4200 W AC 電源装置が搭載されている場合、複合モードでのみ使用できます。

複合モードの電力維持機能を使用して、電力の使用を最大2つまたは3つの入力(設定可能)に制限できます。

4200~W~AC 電源装置が 2 台の場合、最大 4 つの入力を使用できます。この機能により、電力の使用を 2 つまたは 3 つの入力に制限できます。電源装置の 1 つに障害が発生しても、電力消費を小さい入力数に制限してあるので、電力の損失は発生しません。

複合モードの電力維持機能を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# power redundancy combined max inputs {2 3}	電力の使用を2つまたは3つの入力へ制限します。
		(注) コマンドの最大入力部分は、4200 W AC 以外の電源装置すべてに対しては無視されます。
ステップ 3	Switch(config)# end	コンフィギュレーション モードを終了します。

次に、4 つの「正常」な入力(220 V)で max inputs 3 を設定し、電力を 7600 W ではなく 5500 W に制限する例を示します。1 つのサブユニットに障害が発生したり、電源がオフになったりした場合でも、ユーザには 5500 W を提供する 3 つの「正常」な入力が確保され、シャーシは障害が発生する前と同じレートで電力供給されます。

Switch# configuration terminal

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config) # power redundancy combined max inputs 3

Switch(config)# end

Switch#

14:32:01: %SYS-5-CONFIG_I: Configured from console by console

次に、この機能が起動される前の show power コマンドの出力を示します。

Switch# show power

SII DOWE	T-				
Power				Fan	Inline
Supply	Model No	Type	Status	Sensor	Status
PS1	PWR-C45-4200ACV	AC 4200W	good	good	good
PS1-1		110V	good		
PS1-2		110V	good		
PS2	PWR-C45-4200ACV	AC 4200W	good	good	good
PS2-1		110V	good		
PS2-2		110V	good		

Power supplies needed by system : 1 Power supplies currently available : 2

Power Summary		Maximum
(in Watts)	Used	Available
System Power (12V)	140	1360
Inline Power (-50V)	0	1850
Backplane Power (3.3V)	0	40

Total 140 (not to exceed Total Maximum Available = 2100)

次に、この機能が起動されたあとの出力を示します。複合モードは show power コマンドの出力では Power supplies needed = 2 と表示されていましたが、複合モードは現在、Power supplies needed by system :2 Maximum Inputs = 3 と表示されます。

Switch# show power

sh power		W	G hahaan	Fan	Inline
Supply	Model No	Type	Status	Sensor	Status
PS1	PWR-C45-4200ACV	AC 4200W	good	good	good
PS1-1		110V	good		
PS1-2		110V	good		
PS2	PWR-C45-4200ACV	AC 4200W	good	good	good
PS2-1		110V	good		
PS2-2		110V	good		

Power supplies needed by system : 2 Maximum Inputs = 3

Power supplies currently available : 2

Power Summary		Maximum
(in Watts)	Used	Available
System Power (12V)	140	2400
Inline Power (-50V)	0	2000
Backplane Power (3.3V)	0	40

Total 140 (not to exceed Total Maximum Available = 2728)

Switch#

1400 W DC 電源装置に関する特記事項



注意

1400 W DC 電源装置は、他のいかなる電源装置とも併用できません。ホット スワップやその他の 短期間の緊急の場合でも併用しないでください。併用するとスイッチが重大な損傷を受ける場合が あります。

Catalyst 4500 シリーズ スイッチで 1400 W DC 電源装置を使用する場合は、次の注意事項を考慮して ください。

- 1400 W DC 電源装置では、さまざまな DC 電源が使用できます。DC 入力は 300 W ~ 7500 W の 範囲で変動することがあります。詳細については、電源装置のマニュアルを参照してください。
- スーパーバイザ エンジンは、1400 W DC 電源装置に接続された DC 電源を検出できません。 1400 W DC 電源装置を使用する場合、power dc input コマンドを使用して DC 入力電源を設定 してください。このコマンドの詳細については、「電源装置への DC 入力の設定」(p.10-17) を 参照してください。
- ソフトウェアはシステム電力(モジュール、バックプレーン、およびファン)と PoE を自動的 に調整します。PoE の効率は 96% ですが、システム電力は 75% の効率しかありません。たと えば、120 W のシステム電力には、DC 入力から 160 W が必要です。この要件は、show power available コマンド出力の [Power Used] のカラムに反映されています。
- 1400 W DC 電源装置は、PoE 用の電源オン / オフ スイッチを別個に備えています。電源装置 ファンのステータスおよび主電源のステータスは、連動しています。どちらか一方が故障する と、電源装置とファンの両方が不良 / オフとしてレポートします。インライン スイッチの電源 を投入する前に、主電源がオンになっていることを確認する必要があります。さらに、主電源 を切断する前に、インライン スイッチの電源がオフになっていることを確認する必要がありま す。

電源装置への DC 入力の設定

1400 W DC 電源装置または電源シェルフに DC 入力パワーを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# power dc input watts	DC 入力電源の容量を設定します。
ステップ 3	Switch(config)# end	コンフィギュレーション モードを終了します。

同一の設定が、両方の電源スロットに適用されます。たとえば、dc power input を 1000 W に設定 した場合、スイッチはスロット 1 とスロット 2 (装着されている場合) の外部 DC 電源として、そ れぞれ 1000 W を想定します。

次に、外部 DC 電源装置を 1000 W に設定する例を示します。

Switch# configure terminal Switch (config) # power dc input 1000 Switch (config)# end Switch#

1400 W DC SP 電源装置を複合モードで使用する場合、入力が一致する必要はありません。

1400 W DC SP トリプル入力電源装置に関する特記事項

1400 W DC 電源装置とは異なり、1400 W DC SP 電源装置にはサブモジュール(複数の入力)が含まれており、電源のオン/オフを行うことができるようになっています。Cisco IOS Release 12.2(25)EW の場合、show power コマンドの出力は修正され、次のようにこのサブモジュールのステータスが表示されます。

Switch#	show power				
Power				Fan	Inline
Supply	Model No	Type	Status	Sensor	Status
PS1	PWR-C45-1400DC	DCSP1400W	good	good	n.a.
PS1-1		12.5A	good		
PS1-2		15.0A	bad		
PS1-3		15.0A	off		
PS2	none				

Catalyst 4500 シリーズ スイッチで 1400 W DC SP 電源装置を使用する場合は、次の注意事項を考慮してください。

- 2本の48V電力レールを使用して2つの電源装置を動かす場合は、クロスワイヤリングを採用して電源装置をレールに接続し、最初の電源投入中に引き込まれる「突入」電流を最小限に抑えることができます。この状況では、スイッチを複合モードに設定してからレールをメンテナンス用にダウンします。
- 通常の場合、冗長性を設定するときは、2 つの電源装置が「一致」する必要があります(入力が同一)。たとえば、PS1 および PS2 の両方で、入力 1 および 3 に電力を供給します。ブート時に電源装置が一致していない場合は、右側の(第2)電源装置が errdisable 状態になります。

一致した冗長電源装置設定で電源装置のサブモジュールが故障した場合、もう一方の(正常な)電源装置がすべての機能に電力供給します。

Supervisor Engine II-TS でインライン パワーが不足した場合の処理

Supervisor Engine II-TS で 1400 W DC 電源装置 (PWR-C45-1400DC) が使用されていて、電源装置の 12.5 A 入力の 1 つだけが使用される場合、使用されるラインカードのタイプおよびラインカードの 搭載場所 (スロット 2 またはスロット 3) のいずれに搭載されているかによってスーパーバイザエンジンの電力消費量は異なります。電力消費量は 155 ~ 330 W の範囲で異なり、これはスーパーバイザエンジンで利用可能な最大インライン パワー量 (0 ~ 175 W) にも影響します。そのため、1 つまたは複数のラインカードがシャーシに挿入されている場合、スーパーバイザエンジンは接続されたインライン パワー デバイスへのインライン パワーの供給を拒否できます。

次の show power detail および show power module コマンド出力では、スーパーバイザ エンジンに 起因するさまざまな可変電力消費量およびスーパーバイザ エンジンのインライン パワーの概要が 示されています。

Switch# show power detail

show power detail

Power				Fan	Inline
Supply	Model No	Type	Status	Sensor	Status
PS1	PWR-C45-1400DC	DCSP1400W	good	good	n.a.
PS1-1		12.5A	good		
PS1-2		15.0A	off		
PS1-3		15.0A	off		
PS2	none				

Power supplies needed by system : 1 Power supplies currently available : 1

Power Summary		Maximum
(in Watts)	Used	Available
System Power (12V)	360	360
Inline Power (-50V)	0	0
Backplane Power (3.3V)	0	40
Total	360	400

Module Inline Power Summary (Watts)

(12V -> -48V on board conversion)

		Maximum
Mod	Used	Available
1	5	25

Mod	Model		d of System Po out of reset	, ,
1	WS-X4013+TS	180	180	180
2	WS-X4506-GB-T	60	60	20
3	WS-X4424-GB-RJ45	90	90	50
	Fan Tray	30		
	Total	360	330	250

Watts used of Chassis Inline Power (-50V)
Inline Power Admin Inline Power Oper

Mod	Model	PS	Device	PS	Device	Efficiency
2	WS-X4506-GB-T WS-X4424-GB-RJ45	0 -	0 -	0 -	0 -	89 -
	Total	0	0	0	0	

Watts used of Module Inline Power (12V -> -50V)
Inline Power Admin Inline Power Oper

		TITT TITC I	OWCI HAMILII	TITTITIC IC	WCI OPCI	
Mod	Model	PS	Device	PS	Device	Efficiency
1	WS-X4013+TS	6	5	3	3	90

Switch# show power module

sh power module

		Watts Use	d of System Po	wer (12V)
Mod	Model	currently	out of reset	in reset
1	WS-X4013+TS	180	180	180
2	WS-X4506-GB-T	60	60	20
3	WS-X4424-GB-RJ45	90	90	50
	Fan Tray	30		
	Total	360	330	250

Watts used of Chassis Inline Power (-50V)
Inline Power Admin Inline Power Oper

		11111110 1	OWCI MUNITI	TITTIIC I	OWCI OPCI	
Mod	Model	PS	Device	PS	Device	Efficiency
2	WS-X4506-GB-T	0	0	0	0	89
3	WS-X4424-GB-RJ45	-	-	_	-	_
	Total	0	0	0	0	

Watts used of Module Inline Power (12V \rightarrow -50V)

		Inline F	Power Admin	Inline P	ower Oper	
Mod	Model	PS	Device	PS	Device	Efficiency
1	WS-X4013+TS	6	5	3	3	90

Switch#

モジュールの電源切断

スイッチに搭載されたすべてのモジュールに供給する十分な電力がシステムにない場合は、モジュールの電源を切断して、低電力モードにできます。モジュールの電源を切断するには、次の作業を行います。

コマンド	目的
Switch(config)# no hw-module module num power	指定されたモジュールを低電力モードにし
	て、そのモジュールへの電源を切断します。

電源が切断されたモジュールに電源を投入するには、次の作業を行います。

コマンド	目的
Switch(config)# hw-module module num power	指定されたモジュールに電源を投入しま
	ब

次に、モジュール6の電源を切断する例を示します。

Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# no hw-module module 6 power
Switch(config)# end
Switch#

Catalyst 4948 スイッチの電源管理

スイッチに十分な電力を確実に供給できるようにするため、AC または DC 電源装置を選択できます。Catalyst 4948 スイッチでは、次の電源装置を使用できます。

- 300 W AC
- 300 W DC

この電源装置には、Catalyst 4500 シリーズ スイッチとの互換性がありません。PoE は Catalyst 4948 スイッチではサポートされていないため、制限されたワット数のみが必要です。PoE の詳細については、第 11 章「PoE の設定」を参照してください。スイッチに電源装置を取り付けると、電源が投入されていない場合でもシステム ソフトウェアによって電源装置の EEPROM が読み込まれます。AC 電源装置と DC 電源装置は併用できます。

Catalyst 4948 スイッチの電源管理モード

Catalyst 4948 スイッチでは、冗長電源管理モードをサポートします。このモードでは、2 台の電源 装置が正常に動作している場合、各電源装置は常に必要な総システム電力の 20 と 80 ~ 45 と 55% を供給します。一方の電源装置が故障した場合、もう一方の装置は必要な総電力の 100% まで増加させます。

■電源管理



CHAPTER

11

PoE の設定



(注)

この章を読み進める前に、『Catalyst 4500 Series Installation Guide』の「Preparing for Installation」に目を通してください。Power over Ethernet (PoE) の導入によって電気負荷と熱が加わっても、それに対応する十分な電力と冷却装置が設置場所にあることを確認してください。

この章では、Catalyst 4500 シリーズ スイッチで PoE を設定する方法について説明します。 この章の内容は、次のとおりです。

- 概要 (p.11-2)
- 電源管理モード (p.11-3)
- インターフェイス上の受電装置に対する消費電力量の設定 (p.11-6)
- インターフェイスの動作ステータスの表示 (p.11-9)
- モジュールで消費される PoE の表示 (p.11-11)
- E シリーズにおける Enhanced Power PoE のサポート (p.11-15)



(注)

この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_command_reference_list.html

概要

Catalyst 4500 シリーズ スイッチは、シスコ先行標準 PoE および IEEE 802.3af 準拠(2003 年に承認)の両方に関する PoE をサポートします。PoE は、すべての Catalyst 4500 シリーズ スイッチ シャーシでサポートされ、PoE モジュールおよび電源装置を必要とします。使用可能な PoE 電力量は、個々の電源装置の PoE 容量により異なります。PoE のサポートにより、システムがインライン装置(IP Phone、IP ビデオ フォン、および標準の銅ケーブル接続 [カテゴリ 5、5e、6 のケーブル接続]上のワイヤレス アクセス ポイントなど)に電力供給できるようになります。

また、PoE により個々の PoE 対応装置に壁面コンセントを準備する必要がなくなります。これにより、接続先の装置に必要であった追加の電気配線にかかる費用が削減されます。さらに、PoE は単一の電源システム上のクリティカル デバイスを分離し、UPS バックアップがすべてのシステムをサポートできるようにします。

通常、Catalyst 4500 シリーズ スイッチは 2 つの配置シナリオのいずれかで配置されます。最初のシナリオはデータ専用で、スイッチおよび対応モジュールを稼働させる電力が必要となります。2 番めのシナリオは、接続された装置がイーサネット ポートから受電する配置で、データおよび PoE (別名「インライン パワー」)をサポートします。

Catalyst 4500 シリーズ スイッチは、受電装置が PoE モジュールに接続されているかどうかを感知できます。回路に電力がない場合は、受電装置に PoE が供給されます。回路上に電力がある場合は供給されません。受電装置を AC 電源に接続して、音声回路に独自の電力を供給することもできます。



この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/index.htm

ハードウェア要件

PoE を使用してデバイスに電力を供給するには、シャーシでは 表 11-1 に示す電源装置を少なくとも 1 つ使用し、表 11-1 に示すスイッチング モジュールの少なくとも 1 つにデバイスを接続します。

表 11-1 ハードウェア要件

スイッチング モジュール	電源装置
WS-X4148-RJ45V	PWR-C45-1300ACV=
WS-X4224-RJ45V	PWR-C45-1400DCV=
WS-X4248-RJ21V	PWR-C45-2800ACV=
WS-X4248-RJ45V	PWR-C45-4200ACV=
WS-X4505-GB-T	
WS-X4524-GB-RJ45V	
WS-X4548-GB-RJ45V	
WS-X4648-RJ45V-E	
WS-X4648-RJ45V+E	

電源管理モード

エンド ステーションに PoE を供給できるモジュールがスイッチに組み込まれている場合は、そのエンド ステーションが電力を必要とするときに PoE を自動的に検出して適用するように、モジュール上の各インターフェイスを設定できます。

Catalyst 4500 シリーズ スイッチには、3 つの PoE モードがあります。

- auto PoE インターフェイス。スーパーバイザ エンジンは、スイッチング モジュールが電話 を検出し、スイッチに十分な電力がある場合にだけ、インターフェイスに電力を投入するよう にスイッチング モジュールに指示します。インターフェイス上の最大ワット数を指定できます。ワット数を指定しない場合、スイッチはハードウェアでサポートされる最大値以上は供給 しません。このモードでは、インターフェイスが PoE の供給に対応していなくとも影響はありません。
- static ハイ プライオリティの PoE インターフェイス。スーパーバイザ エンジンは、インターフェイスが接続されていない場合でも、インターフェイスに電力を事前に割り当て、インターフェイスに電力が供給されるようにします。インターフェイス上の最大ワット数を指定できます。ワット数を指定しない場合、スイッチはハードウェアでサポートされる最大値を事前に割り当てます。スイッチの割り当てに十分な電力がない場合、コマンドは失敗します。スーパーバイザ エンジンは、スイッチング モジュールが受電装置を検出した場合に だけ、インターフェイスに電力を投入するようにスイッチング モジュールに指示します。
- never データ インターフェイスのみ。スーパーバイザ エンジンは、電力が供給されていない 電話が接続されている場合でも、インターフェイスに電力を投入しません。このモードは、電力が PoE 対応インターフェイスに適用されないようにする場合にのみ必要です。

スイッチは 802.3af 準拠 PoE モジュールの実際の PoE 消費電力を測定できます。この測定値は show power module コマンドの出力に表示されます。

WS-X4148-RJ45V PoE モジュールでは、PoE の消費電力を測定できません。 したがって、PoE を計算する場合は常に、このモジュールの PoE 消費電力が管理上の PoE と等しいと推定します。

詳細については、「モジュールで消費される PoE の表示」(p.11-11) を参照してください。

ほとんどのユーザに対しては、デフォルトの [auto] 設定が十分に機能し、プラグアンドプレイ機能が提供されます。したがって、さらに設定を行う必要はありません。ただし、インターフェイスのプライオリティを高くする場合、データのみにする場合、最大ワット数を指定する場合は、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# interface {fastethernet gigabitethernet} slot/port	設定するインターフェイスを選択します。
ステップ 2	Switch(config-if)# power inline {auto [max milli-watts] never static [max milli-watts]}	auto キーワードは、インターフェイスが受電装置を自動検出し、電力を供給するように設定します。これがデフォルトの設定です。
		static キーワードは、インターフェイスを auto より高い プライオリティに設定します。
		必要であれば、 \max キーワードを使用して、インターフェイスの最大ワット数を指定できます(ほとんどのスイッチング モジュールで $4000 \sim 15400$ ミリワット。Cisco IOS release $12.2(44)$ SG より、WS-X4648-RJ45V+E はポートごとに最大 20 W を利用可能で、WS-X4648-RJ45V-E は最大 20 W をサポートしています。詳細については、「E シリーズにおける Enhanced Power PoE のサポート」[p.11-15] を参照してください)。
		PoE 対応インターフェイスの検出と電力供給をディセーブルにするには、never キーワードを使用します。
ステップ 3	Switch(config-if)# end	コンフィギュレーション モードを終了します。
ステップ 4	Switch# show power inline {fastethernet gigabitethernet} slot/port	スイッチの PoE ステートを表示します。



PoE 未対応インターフェイスについて自動検出と電源供給を設定すると、エラー メッセージが表示され、設定が無効であることが示されます。

次に、PoE を自動検出し、インターフェイスを通じて電力を供給し、インターフェイス FastEthernet 4/1 を設定し、PoE 設定を確認する例を示します。

Switch# configure terminal

Enter configuration commands, one per line. End with ${\tt CNTL/Z.}$

Switch(config)# interface fastethernet 4/1

Switch(config-if)# power inline auto

Switch(config-if)# end

Switch# show power inline fastethernet 4/1

 ${\tt Available:677(w) \quad Used:11(w) \quad Remaining:666(w)}$

Interface A	Admin Oper		(Watts) To Device	Device	Class
Fa4/1 a	uto on	11.2	10.0	Ieee PD	0
Interface	AdminPowerMax (Watts)	AdminConsum (Watts)	-		
Fa4/1 Switch#	15.4		10.0		

次に、インターフェイスを通じて電力を供給しないようにインターフェイスを設定する例を示します。

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 5/2
Switch(config-if)# power inline never
Switch(config-if)# end
Switch#

インテリジェントな電源管理

すべての Catalyst 4500 PoE 対応モジュールは、インテリジェントな電源管理を使用して各インターフェイスに電力供給します。受電装置が PoE 対応ポートに接続されると、ポートが受電装置を検出し、それに応じて電力供給します。シスコ製の受電装置が使用されている場合、スイッチおよび受電装置は Cisco Discovery Protocol (CDP; シスコ検出プロトコル) パケットを使用して電力をネゴシエートして、受電装置が必要とする電力量を正確に判断します。受電装置が 802.3af 準拠の場合、802.3af クラスにより命令された内容と受電装置が実際に必要とする内容の相違分は、その他の装置で使用されるようパワー バジェットに戻されます。このように、電力ネゴシエーションによりカスタマーはパワー バジェットを拡張し、より効果的に使用できるようになります。

また、電力ネゴシエーションにより、新しいシスコ製の受電装置とシスコの古いレガシー PoE 対応ポートとの相互連用が可能になります。新しいシスコ製受電装置は、スイッチポートが提供可能な電力しか消費しません。

インターフェイス上の受電装置に対する消費電力量の設定

ここでは、次の内容について説明します。

- 概要 (p.11-6)
- PoE およびサポートされているケーブル接続トポロジ(p.11-8)

概要

デフォルトでは、スイッチがインターフェイス上で受電装置を検出する場合、受電装置はポートが 供給できる最大電力を消費すると想定します(レガシー PoE モジュールでは 7 W、Cisco IOS Release 12.2(18)EW で導入された IEEE PoE モジュールでは 15.4 W)。次に、スイッチが受電装置から CDP パケットを受信すると、この装置で必要な電力までワット数を自動的に低下させます。通常、この 自動調整は十分機能し、追加設定は不要であり、推奨されません。ただし、スイッチ全体(または 特定のスイッチ)に対する受電装置の電力消費量を指定して、スイッチの特別な機能を提供できま す。これは、CDPがディセーブル、または使用できない場合に便利です。



手動で受電装置の電力消費量を設定する場合、スイッチと受電装置の間のケーブルによる電力損失 を計上する必要があります。

スイッチ全体の電力消費量を変更するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# [no] power inline consumption default milli-watts	スイッチに接続されたすべての受電装置の PoE 電力 消費量 (ミリワット単位)を設定します。電力消費 量の許容範囲は、4000 ~ 15,400 です。
		電力消費量の自動調整を再びイネーブルにするには、 no キーワードを使用するか、または 15,400 ミリワットを指定します。
ステップ 2	Switch(config)# end	コンフィギュレーション モードを終了します。
ステップ 3	Switch# show power inline consumption default	スイッチに接続された受電装置の管理上の PoE 電力 消費量を表示します。管理上の PoE は測定された PoE 値と異なります。

次に、スイッチに接続された受電装置のデフォルトの PoE 電力消費量を 5000 ミリワットに設定し、 PoE 電力消費量を確認する例を示します。

Switch# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config) # power inline consumption default 5000 Switch(config)# end Switch# show power inline consumption default Default PD consumption: 5000 mW

単一の受電装置の電力消費量を変更するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# interface {fastethernet gigabitethernet} slot/port	設定するインターフェイスを選択します。
ステップ 2	Switch(config-if)# [no] power inline consumption milli-watts	特定のインターフェイスに接続された受電装置の PoE 電力消費量 (ミリワット単位)を設定します。 電力消費量の許容範囲は、4000 ~ 15,400 です。 電力消費量の自動調整を再びイネーブルにするに
		は、 no キーワードを使用するか、または 15,400 ミリワットを指定します。
ステップ 3	Switch(config-if)# end	コンフィギュレーション モードを終了します。
ステップ 4	Switch# show power inline consumption {fastethernet gigabitethernet} slot/port	インターフェイスの PoE 電力消費量を表示します。

次に、検出された装置の 802.3af クラスまたは受電装置で受信した CDP パケットの命令にかかわらず、インターフェイス gi 7/1 の PoE 電力消費量を 5000 ミリワットに設定する例を示します。設定のあとでは、インターフェイス gi 7/1 の PoE 電力消費量を確認しています。

次の出力には、インターフェイスの初期電力消費量が表示されます。

Switch# show power inline gi 7/1

Available:627(w) Used:267(w) Remaining:360(w)

Interface	Admin	0per			(Watts) To Device	Device		Class
Gi7/1	auto	on	7.9		7.0	IP Phone	7941	3
Interface		PowerMax tts)	Admin(Consum Vatts)	ption			
Gi7/1		15.4			15.4			

Switch# conf t

Gi7/1

Enter configuration commands, one per line. End with ${\tt CNTL/Z}.$

Switch(config) # int gi 7/1

Switch(config-if) # power inline consumption 5000

15.4

Switch(config-if)# exit

Switch(config)# exit

次の出力には、インターフェイスに対する power inline consumption コマンドの発行後の電力消費量が表示されます。

Switch# sh power inline gi Available:627(w) Used:265		ing:362(w)		
Interface Admin Oper	Power	(Watts)	Device	Class
	From PS	To Device		
Gi7/1 auto on	5.6	5.0	Ieee PD	3
Interface AdminPowerMax (Watts)	AdminConsum (Watts)	-		

5.0

PoE およびサポートされているケーブル接続トポロジ

PoE を使用する場合は、標準 Unshielded Twisted-Pair (UTP; シールドなしツイストペア) ケーブルの4つペアのうちペア 2 および 3 (ピン 1、2、3、6) が、イーサネット データ信号および DC 電力に同時に使用されます。DC の場合、PoE は PoE ポートを使用してペア 3 (ピン 3 および 6) からデバイスに伝送されて、ペア 2 (ピン 1 および 2) に戻ります。その間、イーサネット ポートでは別の信号がペア 2 内(ピン 1 と 2 の間) で送信されます。この方式による DC 電力供給は、イーサネット信号送信に使用されるものと同じ 2 ペアで電源信号が伝送されるので、「ファントム 電源」と呼ばれる場合もあります。インライン パワー信号はイーサネット信号とはトランスペアレントであり、相互の動作を妨げることはありません。インライン パワーの動作およびパフォーマンスに影響する主な電気的パラメータは、ケーブルの DC 抵抗です。インライン パワー方式は、100 m 以下でカテゴリ 3 以上のケーブルで機能するように設計されています。

PoE は、トークン リング対ファスト イーサネット アダプタと使用する場合、IBM Token Ring Shielded Twisted-Pair (STP; シールド付きツイストペア) ケーブル (100 m) と動作することがテストによって確認されています。

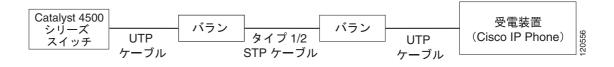
タイプ 1/2 STP ケーブル (90 m および 125 m) を使用した構成で PoE モジュールを使用する場合、モジュールは、10 Mbps および 100 Mbps で、IEEE 802.3af 標準のカテゴリ 5 ケーブルを使用した場合と同じように動作します。

シスコでは次のアダプタをテストしており、このアダプタのみをサポートしています。

- LanTel Silver Bullet (SB-LN/VIP-DATA アダプタ)
- BIP-1236/S (BATM)
- RIT P/N 13712017
- 長さが 6 フィートおよび 24 フィートの UTP ケーブルが統合された RIT バラン

図 11-1 では、Catalyst 4500 シリーズ スイッチが、短いカテゴリ 5 UTP ケーブルによってバランに接続されています。このバランは、タイプ 1 またはタイプ 2 の STP ケーブルにより、2 番めのバランに接続されています。短いカテゴリ 5 UTP ケーブルは、2 番めのバランを他の受電装置 (Cisco IP Phone など) に接続します。

図 11-1 サポートされているアダプタ トポロジ



インターフェイスの動作ステータスの表示

各インターフェイスには、インターフェイスの PoE ステータスを反映する動作ステータスがあります。インターフェイスの動作ステータスは次のように定義されています。

- on ポートによって電力が供給されています。
- off ポートによって電力が供給されていません。受電装置が外部電源を使用してインターフェイスに接続されている場合、スイッチはこの受電装置を認識しません。show power inline コマンド出力の [Device] のカラムには、n/a (該当しない)として表示されます。
- Power-deny スーパーバイザ エンジンの電力が不足しているため、ポートに電力を割り当てることができないか、ポートに設定された電力が必要とする電力より少ないので、ポートが電力を供給していません。
- err-disable スタティック モードで設定された接続デバイスにポートが電力を供給できません。
- faulty ポートが診断テストに失敗しました。

show power inline コマンドを使用して、インターフェイスの動作ステータスを表示できます。

次に、モジュール 3 上のすべてのインターフェイスの動作ステータスを表示する例を示します。

Switch# show power inline module 3
Available:677(w) Used:117(w) Remaining:560(w)

Interface	Admin	Oper		P	ower	(Watts)	Device			Class
				From P	S	To Device				
Fa3/1	auto	on		17.3		15.4	Ieee PD			0
Fa3/2	auto	on		4.5		4.0	Ieee PD			1
Fa3/3	auto	on		7.1		6.3	Cisco IP	Phone	7960	0
Fa3/4	auto	on		7.1		6.3	Cisco IP	Phone	7960	n/a
Fa3/5	auto	on		17.3		15.4	Ieee PD			0
Fa3/6	auto	on		17.3		15.4	Ieee PD			0
Fa3/7	auto	on		4.5		4.0	Ieee PD			1
Fa3/8	auto	on		7.9		7.0	Ieee PD			2
Fa3/9	auto	on		17.3		15.4	Ieee PD			3
Fa3/10	auto	on		17.3		15.4	Ieee PD			4
Fa3/11	auto	off		0		0	n/a			n/a
Fa3/12	auto	off		0		0	n/a			n/a
Fa3/13	auto	off		0		0	n/a			n/a
Fa3/14	auto	off		0		0	n/a			n/a
Fa3/15	auto	off		0		0	n/a			n/a
Fa3/16	auto	off		0		0	n/a			n/a
Fa3/17	auto	off		0		0	n/a			n/a
Fa3/18	auto	off		0		0	n/a			n/a
Totals:		10	on	117.5		104.6				

Switch#

Switch#

次に、インターフェイス FastEthernet 4/1 の動作ステータスを表示する例を示します。

Switch# show power inline fa4/1

Available:677(w) Used:11(w) Remaining:666(w)

Interface	Admin	Oper	From		(Watts) To Device	Device	Class
Fa4/1	auto	on	11.2		10.0	Ieee PD	0
Interface		PowerMax tts)		Consum Watts)	ption		
Fa4/1		15	. 4		10.0		

モジュールで消費される PoE の表示

スイッチは 802.3af 準拠 PoE モジュールの実際の PoE 消費電力を測定できます。測定値は show power module および show power detail コマンドの出力に表示されます。

PoE を計算する場合は常に、WS-X4148-RJ45V モジュールの PoE 消費電力が管理上の PoE と等しい と推定します。

802.3af 準拠の PoE モジュールは、FPGA やモジュールのその他のハードウェア コンポーネントに 電力を供給する場合、最大で 20 W の PoE を消費することがあります。スイッチに接続された受電 装置に十分な電力が供給されるように、802.3af 準拠の PoE モジュールごとに、PoE 所要電力に少な くとも 20 W を追加してください。

次に、show power module コマンドを使用して、802.3af 準拠モジュールの PoE 消費電力を表示する 例を示します。

[Inline Power Oper] カラムには、モジュールに接続された受電装置で消費される PoE、および FPGA やモジュール上のその他のハードウェア コンポーネントで消費される PoE が表示されます。[Inline Power Admin] カラムには、モジュールに接続された受電装置によって割り当てられた PoE のみが表 示されます。



モジュールに受電装置が接続されていない場合でも、802.3af 準拠モジュールで稼働している PoE 消費電力が0にならないことがあります。これは、FPGAやモジュール上のその他のコンポーネン トで PoE が消費されるためです。また、ハードウェア コンポーネントで消費される PoE は一定で ないため、稼働中の PoE が変動することがあります。

Switch# show power module

Watts	Used of System Powe	r (12V)		
Mod	Model	currently	out of reset	in reset
1	WS-X4013+TS	330	330	330
2	WS-X4548-GB-RJ45V	60	60	20
3	WS-X4548-GB-RJ45V	60	60	20
	Fan Tray	30		
	Total	480	450	370

Watts used of Chassis Inline Power (-50V)

		Inline	Power Admin	Inline P	ower Oper	
Mod	Model	PS	Device	PS	Device	Efficiency
2	WS-X4548-GB-RJ45V	138	123	73	65	89
3	WS-X4548-GB-RJ45V	0	0	22	20	89
	Total	138	123	95	85	

Watts used of Module Inline Power (12V -> -50V) Inline Power Admin Inline Power Oper

Mod	Model	PS	Device	PS	Device	Efficiency
1	WS-X4013+TS	128	128	63	63	100

Switch#

次に、show power detail コマンドと show power inline コマンドを使用して、802.3af 準拠モジュールの PoE 消費電力を表示する例を示します。

[Inline Power Oper] カラムには、モジュールに接続された受電装置で消費される PoE、および FPGA やモジュール上のその他のハードウェア コンポーネントで消費される PoE が表示されます。[Inline Power Admin] カラムには、モジュールに接続された受電装置によって割り当てられた PoE のみが表示されます。

Switch# show power detail

Power				Fan	Inline
Supply	Model No	Туре	Status	Sensor	Status
PS1	PWR-C45-1300ACV	AC 1300W	good	good	good
PS2	none				

Power supplies needed by system : 1 Power supplies currently available : 1

Power Summary		Maximum
(in Watts)	Used	Available
System Power (12V)	480	1000
Inline Power (-50V)	138	800
Backplane Power (3.3V)	0	0

Total 618 (not to exceed Total Maximum Available = 1300)

______,

		Maximum
Mod	Used	Available
1	128	158

		Watts Use	d of System Po	wer (12V)
Mod	Model	currently	out of reset	in reset
1	WS-X4013+TS	330	330	330
2	WS-X4548-GB-RJ45V	60	60	20
3	WS-X4548-GB-RJ45V	60	60	20
	Fan Tray	30		
	Total	480	450	370

Watts used of Chassis Inline Power (-50V)

Mod	Model	Inline PS	Power Admin Device	Inline PS	Power Oper Device	Efficiency
2	WS-X4548-GB-RJ45V WS-X4548-GB-RJ45V	138	123 0	73 22	65 20	89 89
	Total	138	123	95	85	

_ 1	DC	D.		DC	D		meeill
	Inline	Power	Admin	Inline	Power 0	Oper	
	Watts ı	used o	f Module	Inline	Power	(12V	-> -50V)

1	WS-X4013+TS	128	128	64	64	100
Mod	Model	PS	Device	PS	Device	Efficiency

Interface	Admin	Oper		er(Watts) To Device	Device	Class
Gi1/1	auto	on	10.3	10.3	CNU Platform	3
Interface			AdminCons (Watt			
Gi1/1		15.4		15.4		
switch# sl	how pow	er inline	g2/1			
Chassis I	nline P	ower Suppl	y: Availab	le:800(w) Us	ed:138(w) Remaini	ing:662(v
Interface	Admin			er(Watts) To Device	Device	Class
C; 2 / 1	211+0		11 E	10.2	CNII Dlatform	~ / a
					CNU Platform	II/a
Interface	(Wa		AdminCons (Watt			
Gi2/1		15.4		15.4		
		ver inline Power Supp		ble:158(w) U	sed:128(w) Remair	ning:30(v
				er(Watts)		
Interface			From PS	To Device		Class
Gi1/1	auto auto		10.3		CNU Platform CNU Platform	
Gi1/2 Gi1/3	auto	on				3
Gi1/3 Gi1/4	auto	on	10.3	10.3	CNU Platform CNU Platform CNU Platform	3
Gi1/4 Gi1/5	211+0	on	10.3	10.3	CNU Platform	3
Gi1/5 Gi1/6	auto	on	10.3	10.3	CNII Platform	
	auto		10.3	10.3	CNU Platform CNU Platform	3
Gi1/8	auto	on	10.3	10.3	CNU Platform	3
Gi1/9	auto	on	10.3	10.3	CNU Platform	3
	auto	on	15.4	15.4	Cisco/Ieee PD	3
Gi1/10 Gi1/11	auto	on	10.3		CNU Platform	3
					CNU Platform	3
C:1/12	auto	on	10.3	10.3	CNU PIACIOIM	
Gi1/12 						
Totals:		12 on	128.2	128.2		
Totals:		12 on				
Totals: switch# switch# sl Chassis In	how pow nline P	ver inline Power Suppl	module 2 y: Availab	128.2 le:800(w) Us	ed:138(w) Remaini	
Totals: switch# switch# sl Chassis In	how pow nline P	ver inline Power Suppl	module 2 y: Availab	128.2		
Totals: switch# switch# sl Chassis In	how pow nline P	ver inline Power Suppl	module 2 y: Availab Pow	128.2 le:800(w) Us	Device	ing:662(v
Totals: switch# switch# sl Chassis In Interface	how pow nline P Admin	ver inline Power Suppl Oper	module 2 y: Availab Pow From PS	128.2 le:800(w) Us er(Watts) To Device	Device	ing:662(v Class
Totals: switch# sl Chassis In Interface Gi2/1	how pow nline P Admin	ver inline Power Suppl Oper Oper	module 2 y: Availab Pow From PS	128.2 le:800(w) User(Watts) To Device	Device CNU Platform	ing:662(t Class
Totals: switch# sl Chassis In Interface Gi2/1 Gi2/2	how pow nline P Admin auto auto	or inline Ower Suppl Oper on on	module 2 y: Availab Pow From PS 11.5 11.5	128.2 le:800(w) User(Watts) To Device	Device CNU Platform CNU Platform	ng:662(Clas n/a n/a
Totals: switch# sl Chassis In Interface Gi2/1 Gi2/2 Gi2/3	how pownline PAdmin auto auto auto	or inline Ower Suppl Oper on on on	module 2 y: Availab Pow From PS 11.5 11.5 11.5	128.2 le:800(w) User(Watts) To Device 10.2 10.2 10.2	Device CNU Platform CNU Platform CNU Platform	ng:662(v Class n/a n/a n/a
Totals: switch# sl Chassis In Interface Gi2/1 Gi2/2 Gi2/3 Gi2/4	how pownline PAdmin auto auto auto auto auto	or inline Ower Suppl Oper on on on on on	module 2 y: Availab Pow From PS 11.5 11.5 11.5	128.2 le:800(w) User(Watts) To Device 10.2 10.2 10.2 10.2 10.2	CNU Platform CNU Platform CNU Platform CNU Platform CNU Platform	n/a n/a n/a n/a n/a
Totals: switch# sl Chassis In Interface Gi2/1 Gi2/2 Gi2/3 Gi2/4	how pownline PAdmin auto auto auto	or inline Ower Suppl Oper on on on	module 2 y: Availab Pow From PS 11.5 11.5 11.5	128.2 le:800(w) User(Watts) To Device 10.2 10.2 10.2	Device CNU Platform CNU Platform CNU Platform	ng:662(v Class n/a n/a n/a
Totals: switch# sl Chassis In Interface Gi2/1 Gi2/2 Gi2/3 Gi2/4 Gi2/5	how pownline PAdmin auto auto auto auto auto	or inline Ower Suppl Oper on on on on on	module 2 y: Availab Pow From PS 11.5 11.5 11.5	128.2 le:800(w) User(Watts) To Device 10.2 10.2 10.2 10.2 10.2	CNU Platform CNU Platform CNU Platform CNU Platform CNU Platform	n/a n/a n/a n/a n/a
Totals: switch# sl Chassis In Interface Gi2/1 Gi2/2 Gi2/3 Gi2/4 Gi2/5 Gi2/6	how pownline PAdmin auto auto auto auto auto auto auto	orer inline Ower Suppl Oper on on on on on off	module 2 y: Availab Pow From PS 11.5 11.5 11.5 0.0	128.2 le:800(w) User(Watts) To Device 10.2 10.2 10.2 10.2 0.0	CNU Platform CNU Platform CNU Platform CNU Platform CNU Platform n/a	n/a n/a n/a n/a n/a n/a
Totals: switch# sl Chassis In Interface Gi2/1 Gi2/2 Gi2/3 Gi2/4 Gi2/5 Gi2/6	how pownline PAdmin auto auto auto auto auto auto auto auto	orer inline Ower Suppl Oper on on on on on off off	module 2 y: Availab Pow From PS 11.5 11.5 11.5 0.0 0.0	128.2 le:800(w) User(Watts) To Device 10.2 10.2 10.2 10.2 0.0 0.0	CNU Platform CNU Platform CNU Platform CNU Platform CNU Platform n/a n/a	n/a n/a n/a n/a n/a n/a n/a n/a

Gi2/10	auto	on	11.5	10.2	CNU Platform	n/a
Gi2/11	auto	on	11.5	10.2	CNU Platform	n/a
Gi2/12	auto	on	11.5	10.2	CNU Platform	n/a
Gi2/13	auto	on	11.5	10.2	CNU Platform	3
Gi2/14	auto	on	11.5	10.2	CNU Platform	3
Gi2/15	auto	on	11.5	10.2	CNU Platform	3
Gi2/16	auto	on	11.5	10.2	CNU Platform	3
Gi2/17	auto	off	0.0	0.0	n/a	n/a
Gi2/18	auto	off	0.0	0.0	n/a	n/a
Interface	Admin	Oper	Power	(Watts)	Device	Class
			From PS	To Device		
Gi2/19	auto	off	0.0	0.0	n/a	n/a
Gi2/20	auto	off	0.0	0.0	n/a	n/a
Gi2/21	auto	off	0.0	0.0	n/a	n/a
Gi2/22	auto	off	0.0	0.0	n/a	n/a
Gi2/23	auto	off	0.0	0.0	n/a	n/a
Gi2/24	auto	off	0.0	0.0	n/a	n/a
Gi2/25	auto	off	0.0	0.0	n/a	n/a
Gi2/26	auto	off	0.0	0.0	n/a	n/a
Gi2/27	auto	off	0.0	0.0	n/a	n/a
Gi2/28	auto	off	0.0	0.0	n/a	n/a
Gi2/29	auto	off	0.0	0.0	n/a	n/a
Gi2/30	auto	off	0.0	0.0	n/a	n/a
Gi2/31	auto	off	0.0	0.0	n/a	n/a
Gi2/32	auto	off	0.0	0.0	n/a	n/a
Gi2/33	auto	off	0.0	0.0	n/a	n/a
Gi2/34	auto	off	0.0	0.0	n/a	n/a
Gi2/35	auto	off	0.0	0.0	n/a	n/a
Gi2/36	auto	off	0.0	0.0	n/a	n/a
Gi2/37	auto	off	0.0	0.0	n/a	n/a
Gi2/38	auto	off	0.0	0.0	n/a	n/a
Gi2/39	auto	off	0.0	0.0	n/a	n/a
Gi2/40	auto	off	0.0	0.0	n/a	n/a
Interface	Admin	Oper	Power	(Watts)	Device	Class
		_	From PS	To Device		
Gi2/41	auto	off	0.0	0.0	n/a	n/a
Gi2/42	auto	off	0.0	0.0	n/a	n/a
Gi2/43	auto	off	0.0	0.0	n/a	n/a
Gi2/44	auto	off	0.0	0.0	n/a	n/a
Gi2/45	auto	off	0.0	0.0	n/a	n/a
Gi2/46	auto	off	0.0	0.0	n/a	n/a
Gi2/47	auto	off	0.0	0.0	n/a	n/a
Gi2/48	auto	off	0.0	0.0	n/a	n/a
Totals:		12 on	138.2	123.0		
Switch#						

Eシリーズにおける Enhanced Power PoE のサポート

WS-X4648-RJ45V-E および WS-X4648-RJ45V+E スイッチング モジュールは IEEE 802.3af Power over Ethernet (PoE) とシスコ独自のインライン パワー標準をサポートしていて、Cisco IOS release 12.2(44)SG より、WS-X4648-RJ45V+E は IEEE 802.3at 標準もサポート可能になり、ポートごとに最大 20 W 利用可能になりました。WS-X4648-RJ45V-E は Cisco IOS release 12.2(44)SG より最大 20 W をサポートします。これらのスイッチング モジュールでは、power inline コマンドでの有効なミリワット範囲がモジュールに対応して増加しています。

一般的なアプリケーションでは、デフォルトのパワー インライン設定で十分であり、Cisco AP1250 ワイヤレス アクセス ポイントなど高電力消費型のシスコの受電装置に対しても、追加設定は不要です。高電力消費型のデバイスが WS-X4648-RJ45V-E や WS-X4648-RJ45V+E のポートに接続されると、スイッチとデバイスが CDP パケットを使用して電力使用をネゴシエートし、自動的にデバイスで必要となる電力量を決定します。

構成要件や設計によって、power inline コマンドで特定の設定を入力することができます。次に、検出された装置の 802.3af クラスまたは受電装置で受信した CDP パケットの指定に関係なく、ギガビット インターフェイス 2/1 の PoE 割当を事前に 16500 ミリワット割り当てる例を示します。

Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet 2/1
Switch(config-if)# power inline static max 16500
Switch(config-if)# end
Switch#



CHAPTER

12

Cisco Network Assistant による Catalyst 4500 シリーズ スイッチの 設定

この章では、ワークステーション上に Network Assistant をインストールして、Catalyst 4500 (または Catalyst 4900) シリーズ スイッチが Network Assistant と通信するように設定する方法について説明します(これまでの Catalyst 4500 シリーズ スイッチという用語は、両方のスイッチ タイプを意味するように使用されています)。また、コミュニティおよびクラスタの作成方法についても説明します。Network Assistant は 2 つのテクノロジーを使用して、Catalyst 4500 シリーズ スイッチなどのネットワーク デバイスのグループを管理します。

Network Assistant は、無料のネットワーク管理ツールで、GUI(グラフィカル ユーザ インターフェイス)による Catalyst 4500 シリーズ スイッチの設定および管理を可能にします。Network Assistant は、セキュア環境および非セキュア環境の両方で稼働します。Network Assistant は、ご使用のイントラネットのどこからでもスタンドアロン デバイス、デバイス グループ、またはスイッチ グループ(コミュニティまたはクラスタ内)を管理します。Network Assistant を使用すると、コマンドを覚える必要がなく、複数の設定作業を実行できます。



この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

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

Network Assistant の設定および使用法

この章の内容は、次のとおりです。

- Network Assistant の関連機能およびデフォルト設定 (p.12-2)
- CLI コマンドの概要 (p.12-3)
- スイッチでの Network Assistant の設定 (p.12-4)
- コミュニティを使用したネットワーク管理(p.12-6)
- クラスタのコミュニティへの変換 (p.12-10)
- クラスタを使用したネットワーク管理 (p.12-11)
- コミュニティ モードまたはクラスタ モードでの Network Assistant の設定 (p.12-14)



(注)

Network Assistant は Cisco.com 上のオンライン ソフトウェア イメージとバンドルされていません。 Network Assistant は次の URL からダウンロードできます。http://www.cisco.com/go/NetworkAssistant



(注)

Network Assistant のソフトウェアおよびハードウェア要件、インストール方法、起動方法、およびデバイスへの接続方法の詳細については、次の URL の『Getting Started with Cisco Network Assistant』を参照してください。http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cna/v2_0/gsg/index.htm

Network Assistant の関連機能およびデフォルト設定

表 12-1 に、Catalyst 4500 シリーズ スイッチの Network Assistant 関連の設定パラメータを示します。

表 12-1 Catalyst 4500 シリーズ スイッチの Network Assistant 関連の設定

機能	デフォルト値	推奨値
認証	ディセーブル	任意
IP アドレス	コミュニティまたは検出オプ ションにより異なります。 ¹	ユーザ選択可能 (注) コミュニティは Supervisor Engine 6-E ではサポートされていません。
IP HTTP ポート番号	80	任意 ²
IP HTTPS ポート番号	443	任意3
IP HTTP サーバ	ディセーブル	イネーブル ⁴
Cluster run	ディセーブル	イネーブル ⁵

^{1.} コミュニティのデバイス検出およびクラスタ コマンダには、スイッチごとに IP アドレスを設定する必要があります。

- 2. Network Assistant のポート番号と Catalyst 4500 シリーズ スイッチは一致させる必要があります。
- 3. デバイスのクラスタのこの値のみ、変更できます。Network Assistant のポート番号と Catalyst 4500 シリーズ スイッチは一致させる必要があります。値は、1024 より上の任意の非デフォルト番号に変更できます。
- 4. Network Assistant がデバイスにアクセスするのに必要です。
- 5. デバイスのクラスタを管理する場合にのみ、イネーブルです。

CLI コマンドの概要

表 12-2 に、Network Assistant 関連の CLI (コマンドライン インターフェイス) コマンドの概要を示します。

表 12-2 CLI コマンド

コマンド	機能
[no] cluster enable	クラスタに名前を付けます。
[no] cluster run	クラスタリングをイネーブルにします。
	•
	(注) このコマンドは、クラスタリング専用です。
[no] ip http server	スイッチで HTTP を設定します。
[no] ip http port port_number	HTTP ポートを設定します。
[no] ip domain-name domain_name	スイッチ上でドメインを設定します。
[no] ip http secure-server	スイッチ上で HTTPS を設定して、イネーブルに します。
[no] ip http secure-port port_number	HTTPS ポートを設定します。
[no] ip http max-connections connection_number	HTTP サーバへの最大同時接続数を設定します。
[no] ip http timeout-policy	HTTPS ポートを設定します。
idle idle_time life life_time	 180 秒の idle 値を推奨します。
requests requests	180 秒の life 値を推奨します。
	許可できる requests の最大数は 25 を推奨します。
line vty	CNA が使用する追加の VTY を設定します。
show version	Cisco IOS リリースを表示します。
show running-config	スイッチ設定を表示します。
vtp domain	VLAN(仮想 LAN)を管理する VLAN Trunking
	Protocol(VTP; VLAN トランキング プロトコル) ドメインを作成します。
vtp mode	VLAN の VTP 管理に関する動作を設定します。

スイッチでの Network Assistant の設定

ここでは、次の内容について説明します。

- CNA から Catalyst 4500 ヘアクセスするのに必要な最小設定 (p.12-4)
- コミュニティを使用する必要がある場合の追加設定(p.12-5)
- クラスタを使用する必要がある場合の追加設定 (p.12-5)

CNA から Catalyst 4500 ヘアクセスするのに必要な最小設定

デフォルトの設定を使用する場合は、Catalyst 4500 シリーズ スイッチにアクセスして、**ip http server** (HTTP 用)または **ip http secure-server** (HTTPS 用) グローバル コンフィギュレーション コマンドを入力します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	Switch(config)# ip http server または	(HTTP の場合のみ)スイッチ上で HTTP サーバを イネーブルにします。デフォルトでは、HTTP サー バはディセーブルに設定されています。
	Switch(config)# ip domain-name domain_name	スイッチでドメイン名をイネーブルにして、HTTPS を設定します。
ステップ 3	Switch(config)# ip http secure-server	スイッチ上で HTTPS サーバをイネーブルにします。 デフォルトでは、HTTPS サーバはディセーブルに設 定されています。
ステップ 4	Switch(config)# ip http max-connections connection_number	HTTP サーバへの最大同時接続数を設定します。 16 の connection number を推奨します。
ステップ 5	Switch(config)# ip http timeout-policy idle idle_time life life_time requests requests	HTTPS ポートを設定します。 idle キーワードでは、接続がアイドル状態でいる最大時間数を指定します。180 秒の idle 値を推奨します。 life キーワードでは、接続が確立してからオープンでいる最大時間数を指定します。180 秒の life 値を推奨します。 requests キーワードでは、接続での最大要求数を指定します。許可できる requests の最大数は 25 を推奨します。
ステップ 6	Switch(config-if)# end	特権 EXEC モードに戻ります。
ステップ 7	Switch# show running-config	設定を確認します。



クラスタリングがイネーブルの場合、コミュニティを設定する前にクラスタリングをディセーブルにします (表 12-2 を参照)。

コミュニティを使用する必要がある場合の追加設定



<u>一</u> (注) コミュニティは Supervisor Engine 6-E ではサポートされてIIません。

コミュニティを使用する場合は、スイッチごとに IP アドレスを定義します。

	コマンド	目的
ステップ 1	Switch# configuration terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	Switch(config)# interface {vlan vlan_ID {fastethernet gigabitethernet} slot/interface Port-channel number}	インターフェイスを選択します。
ステップ 3	Switch(config-if)# ip address ip_address address_mask	(任意) Catalyst 4500 シリーズに IP アドレスを割り 当てます。
ステップ 4	Switch(config-if)# end	特権 EXEC モードに戻ります。
ステップ 5	Switch# show running-config	設定を確認します。

クラスタを使用する必要がある場合の追加設定

クラスタリングを使用する場合、デバイスごとに cluster run グローバル コンフィギュレーション コマンドを入力し、クラスタ コマンダで ip address インターフェイス コンフィギュレーション コマンドを入力します。

=	コマンド	目的	
Sī	witch# configuration terminal	グロ <i>-</i> します	-バル コンフィギュレーション モードを開始 - 。
2 St	witch(config)# cluster run	クラス	(タリングをイネーブルにします。
		(注)	クラスタの一部となる可能性のあるスイッ チすべてでクラスタリングをイネーブルに します。
St	witch(config)# cluster enable	クラス	くタに名前を付けます。
{:	<pre>witch(config)# interface {vlan vlan_ID fastethernet gigabitethernet} lot/interface Port-channel number}</pre>	インタ	7ーフェイスを選択します。

	コマンド	目的
ステップ 5	Switch(config-if)# ip address ip_address address_mask	(任意) Catalyst 4500 シリーズ スイッチのクラスタ マスターに IP アドレスを割り当てます。
		(注) スイッチがコミュニティの一部またはクラスタ コマンド スイッチの場合、この手順は必須です。スイッチがクラスタ メンバ候補の場合、この手順は任意です。
ステップ 6	Switch(config-if)# end	特権 EXEC モードに戻ります。
ステップ 7	Switch# show running-config	設定を確認します。

コミュニティを使用したネットワーク管理



(注)

コミュニティは Supervisor Engine 6-E ではサポートされていません。

ここでは、Network Assistant アプリケーションによる デバイス (Catalyst 4500 シリーズ スイッチ、ルータ、アクセス ポイント、および PIX ファイアウォールを含む)管理におけるコミュニティの使用方法について説明します。

コミュニティを使用してネットワーク内のスイッチを分類する場合、唯一の要件は HTTP サーバおよびスイッチごとの IP アドレスの設定です。

コミュニティ内のデバイスの総数は、20 以下になるようにします(最大 4 つの Catalyst 4500 シリーズ スイッチ [モジュラ式] 16 の Catalyst 2900/3500 または Catalyst 4948/4948-10GE スイッチ [非モジュラ式] 2 つのルータ、および 2 つの PIX ファイアウォールも含む)。



(注)

アクセス ポイントはデバイス制限から除外されました。現在、CNA が管理できるアクセス ポイント数に制限はありません。



注,

Add to Community ダイアログにより、多数のデバイスが表示されますが、20 のデバイスしか選択できません。21 番めのデバイスを追加しようとすると、ダイアログは 21 番めのデバイスを表示して、不要なデバイスの選択が要求されます。



(注)

Network Assistant を使用してスイッチ コミュニティを設定する詳細な手順については、次の URL の『Getting Started with Cisco Network Assistant』を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cna/v2_0/gsg/index.htm

CLI クラスタ コマンドについては、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univered/cc/td/doc/product/software/ios123/123cgcr/index.htm

ここでは、コミュニティを作成する前に理解する必要がある注意事項、要件について説明します。 ここでは、次の内容について説明します。

- 候補およびメンバの特性 (p.12-7)
- 候補およびメンバの自動検出 (p.12-7)
- コミュニティ名(p.12-8)
- ホスト名(p.12-8)
- パスワード (p.12-8)
- Network Assistant のアクセス モード (p.12-8)
- コミュニティ情報(p.12-9)

候補およびメンバの特性

候補は、IP アドレスを持ちますが、コミュニティには追加されていないネットワーク デバイスで す。メンバは、現在コミュニティに含まれるネットワークデバイスです。

コミュニティに加入するには、候補は次の要件を満たす必要があります。

- IP アドレスが指定されていること。
- デバイスを自動検出する場合、Cisco Discovery Protocol(CDP; シスコ検出プロトコル)バージョ ン2がイネーブルに設定されていること(デフォルト)。
- HTTP (または HTTPS) がイネーブルであること。



(注) クラスタ メンバはコミュニティに追加できますが、逆はできません。



(注) クラスタ コマンダがコミュニティに追加されても、クラスタのその他のメンバ デバイスは 自動的に追加されません。クラスタ メンバを管理するには、個別にコミュニティに追加す る必要があります。

候補およびメンバの自動検出

Network Assistant は、CDP を使用してネットワーク内の利用可能なデバイスのすべてを確認または 検出し、コミュニティを形成します。起動デバイスの IP アドレスおよび HTTP(または HTTPS)プ ロトコルのポート番号から始めて、Network Assistant は CDP を使用して起動デバイスに隣接するコ ミュニティ候補のリストをコンパイルします。Network Assistant は、有効な IP アドレスを持つかぎ り、複数のネットワークおよび VLAN 間で候補デバイスおよびメンバ デバイスを検出できます。



デフォルトでは、コミュニティ モードの Network Assistant は最大 4 ホップ先まで検出します。

ネットワーク デバイスが検出されるための要件のリストについては、「候補およびメンバの特性」 (p.12-7)を参照してください。



(注)

Network Assistant により検出する場合は、候補、メンバ、またはネットワーク デバイスで CDP を ディセーブルにしないでください。



PIX ファイアウォールは CDP をサポートしないため、Topology ビューにネイバーとして自動表示されません。Create Community または Modify Community ウィンドウを使用してコミュニティに追加した場合にのみ表示されます。PIX ファイアウォールと他のコミュニティ メンバとのリンクを確認するには、Topology ポップアップ メニューで ADD Link を選択して手動でリンクを追加する必要があります。

検出されたデバイスのリストを編集し、必要に応じてコミュニティに追加できます。デバイスがコミュニティに追加されるたびに、そのネイバーが検出され、候補デバイスのリストに追加されます。 Network Assistant がデバイスを検出できない場合は、IP 管理アドレスにより手動で追加できます。

コミュニティ名

メンバデバイスのリストにコミュニティの設定情報を適用すると、Network Assistant によりコミュニティの名前(または IP アドレス)の入力が要求されます。コミュニティを管理するには、まず名前を割り当てる必要があります。Network Assistant は、この名前をご使用の PC に保存します。

コミュニティ名には、 $0 \sim 9$ 、 $a \sim z$ 、および $A \sim Z$ の文字と、文字間のスペースを使用できます。



クラスタには、IP アドレスによってのみ接続できます。名前を選択すると、常にそのコミュニティの名前となります。

ホスト名

起動デバイスまたはコミュニティ メンバには、ホスト名を割り当てる必要はありません。ただし、シスコではホスト名の割り当てを推奨しています。Network Assistant は、デフォルトでは割り当てません。検出されたデバイスにホスト名がある場合、Network Assistant はこのデバイスの情報を識別するために、IP アドレス、通信プロトコル、および指定されたプロトコル ポートとともにホスト名をご使用の PC に保存します。

パスワード

コミュニティ メンバとなるデバイスにはパスワードを割り当てる必要はありませんが、シスコではパスワードの割り当てを推奨しています。

コミュニティ メンバごとに別々のパスワードを割り当てることができます。

通信プロトコル

Network Assistant は、HTTP (または HTTPS) プロトコルを使用してネットワーク デバイスと通信します。候補デバイスの検出に CDP を使用すると、HTTP (または HTTPS)と通信しようとします。

Network Assistant のアクセス モード

Network Assistant がコミュニティまたはクラスタに接続されている場合、パスワードにより読み書きモードおよび読み出し専用モードの2つのモードが使用できます。

コミュニティ情報

Network Assistant は、すべてのコミュニティの設定情報および個別のデバイス情報(IP アドレス、 ホスト名、通信プロトコルなど)をご使用のローカル PC に保存します。Network Assistant がコミュ ニティに接続するとき、ローカルに保存されたデータを使用してメンバ デバイスを再検出します。

別の PC を使用して既存のコミュニティを管理しようとすると、メンバ デバイスの情報は使用でき ません。再度コミュニティを作成し、これと同じメンバ デバイスを追加する必要があります。

デバイスの追加

コミュニティにメンバを追加するには、次の3つの方法があります。

1つめの方法では、Network Assistant 上の Devices Found ウィンドウを使用して、検出したデバイス を新しいコミュニティに追加します。

- a. Devices Found ウィンドウで、追加する候補デバイスを選択します。 複数の候補デバイスを追加するには、Ctrl を押して選択をするか、Shift を押して範囲の 最初と最後のデバイスを選択します。
- b. Add をクリックします。

2 つめの方法では、Modify Community ウィンドウを使用して、既存のコミュニティにデバイスを追 加します。

- a. Application > Communities を選択し、Community ウィンドウを開きます。
- b. Community ウィンドウで、デバイスを追加するコミュニティ名を選択し、Modify をクリッ クします。
- c. 手動で単一のデバイスを追加するには、Modify Community ウィンドウで所定のデバイスの IP アドレスを入力し、Add をクリックします。
- d. 候補デバイスを検出するには、起動デバイスの IP アドレスを入力し、Discover をクリック
- e. リストから候補デバイスを選択し、Add をクリックしてから、OK をクリックします。 複数の候補デバイスを追加するには、Ctrl を押して選択をするか、Shift を押して範囲の 最初と最後のデバイスを選択します。

デバイスを追加する3つめの方法では、Topology ビューを使用します。

- a. Topology ビューが表示されない場合は、機能バーから View window> Topology を選択しま す。
- b. 候補アイコンを右クリックして、Add to Community を選択します。

候補はシアン、メンバはグリーンになります。複数の候補を追加するには、Ctrl を押し て、追加する候補を左クリックします。

コミュニティに20のメンバが所属している場合、そのコミュニティではAdd to Community オプションは使用できません。この場合、新しいメンバを追加する前に1つ のメンバを削除する必要があります。



コミュニティにログインしていて、他の CNA インスタンスからそのコミュニティを削除する場合、 このコミュニティ セッションを終了しないかぎり、セッションを介してすべての設定を実行でき ます。セッションの終了(つまり、コミュニティの削除)後は、このコミュニティに接続できなく なります。

クラスタのコミュニティへの変換



(注)

コミュニティは Supervisor Engine 6-E ではサポートされていません。

Cluster Conversion ウィザードにより、クラスタをコミュニティに変換できます。変換が完了するとただちに、デバイス グループをコミュニティとして管理できます。コミュニティ管理の利点は、コミュニティ内のデバイスとの通信がクラスタ内のデバイスとの通信よりもセキュアである(複数のパスワードおよび HTTPS を介するため)ことです。さらに、デバイスのアベイラビリティは高く、メンバにできるデバイスの範囲も広くなります。



(注)

Cluster Conversion ウィザードでは、クラスタ定義は変更されません。そのため、デバイスをクラスタとしても管理できます。

Cluster Conversion ウィザードを開始するには、次の手順を実行します。

- ステップ1 Network Assistant を開始し、コマンダの IP アドレスを介して既存のクラスタに接続します。
- ステップ 2 機能バーで、Configure > Cluster > Cluster Conversion Wizard をクリックします。

[Do you want to convert this cluster to a community?] (このクラスタをコミュニティに変換しますか) という質問が表示されます。

ステップ3 Yes を選択して次に進むか、Cluster Conversion ウィザードを手動で立ち上げる場合は No を選択します。

Yes を選択すると、初期画面が表示され、クラスタ、コミュニティ、およびその利点に関する情報が提供されます。

次に、クラスタ内のデバイスを示す表が IP アドレスおよびサブネット マスクを持たないデバイス から表示されます。コミュニティのメンバとなるには、クラスタ内のすべてのデバイスで IP アドレスおよびサブネット マスクを持つ必要があることに注意してください。



(注)

デバイスに IP アドレスおよびサブネット マスクを持つインターフェイスが複数ある場合は、セルをクリックすると複数のインターフェイスが表示されます。最初に表示されたものとは異なるインターフェイスを選択できます。

- **ステップ 4** IP Address カラムでは、IP アドレスを持たない各デバイスの IP アドレスを入力します。
- ステップ5 Subnet Mask カラムでは、サブネット マスクを持たない各デバイスのセルをクリックし、サブネット マスクを選択します。
- ステップ6 コミュニティ名を入力します。

ステップ7 変換を開始するには、Finish をクリックします。

変換が完了すると、Network Assistant が再開し、新しく作成されたコミュニティに自動的に接続します。



(注)

クラスタリングがイネーブルの場合、コミュニティを設定する前にクラスタリングをディセーブルにする必要があります (表 12-2 を参照)。

クラスタを使用したネットワーク管理

ここでは、クラスタリングを使用して、スタンドアロンの Network Assistant アプリケーションまたは CLI を使用する Catalyst 4500 シリーズ スイッチの作成および管理方法について説明します。

ネットワーク内のスイッチを分類するには、クラスタリングを使用できます。管理されるスイッチごとにクラスタ実行コマンドを入力する必要があります。主な利点は、1 つの IP アドレスで 16 のデバイスを管理できることです。



(注

クラスタリングは、CNA 1.0 で使用される自動検出メカニズムです。



(注)

Network Assistant を使用してスイッチ クラスタを設定する詳細な手順については、次の URL の『Getting Started with Cisco Network Assistant』を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cna/v2_0/gsg/index.htm

CLI クラスタ コマンドについては、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/index.htm

ここでは、次の内容について説明します。

- スイッチ クラスタの概要 (p.12-11)
- CLI を使用したスイッチ クラスタ管理 (p.12-14)

スイッチ クラスタの概要

ここでは、次の内容について説明します。

- クラスタリングの概要 (p.12-12)
- クラスタ コマンド スイッチの特性 (p.12-12)
- 候補スイッチとクラスタ メンバ スイッチの特性 (p.12-13)

クラスタリングの概要

スイッチ クラスタは、最大 16 個の接続されたクラスタ対応 Catalyst スイッチで、単一エンティティとして管理されます。1 つの IP アドレスを介して異なる Catalyst 4500 シリーズ スイッチ プラットフォーム グループを設定およびトラブルシューティングできるように、クラスタのスイッチはスイッチ クラスタリング技術を使用します。

スイッチ クラスタを使用すると、スイッチの物理的なロケーションやプラットフォーム ファミリ に関係なく、複数のスイッチの管理を簡略にします。



(注)

デフォルトでは、クラスタリング モードの Network Assistant は最大 7 ホップ先まで検出します。

スイッチ クラスタでは、1 つのスイッチはクラスタ コマンダ スイッチになる必要があります。最大 15 個の残りのスイッチはクラスタ メンバ スイッチになります。クラスタのスイッチ総数は 16 個を超えることはできません。クラスタ コマンド スイッチは、クラスタ メンバ スイッチを設定、管理、監視する単独のアクセス ポイントです。クラスタ メンバは、同時に 1 つのクラスタにのみ属することができます。



(注)

必ずクラスタ コマンド スイッチとして Catalyst 4500 または 4948 シリーズ スイッチを選択してください。

クラスタ コマンド スイッチの特性

クラスタ コマンド スイッチは次の要件を満たす必要があります。

- Cisco IOS Release 12.2(20)EWA 以降を使用していること。
- IP アドレスが指定されていること。
- CDP バージョン 2 がイネーブル (デフォルト) に設定されていること。
- クラスタ対応ソフトウェアを使用し、クラスタリングがイネーブルであること。
- IP HTTP (または HTTPS) サーバがイネーブルであること。



(注)

Catalyst 4500 シリーズ スイッチでは、HTTP および HTTPS はデフォルトでイネーブルに設定されていません。

• 16本の VTY 回線があること。



(注)

Catalyst 4500 シリーズ スイッチのデフォルトは 4 回線です。スイッチでの値が 16 になるよう設定します。

• 別のクラスタのコマンドまたはクラスタ メンバ スイッチではないこと。



注)

ご使用のスイッチ クラスタに Catalyst 4500 シリーズ スイッチが含まれている場合、クラスタ コマンド スイッチも Catalyst 4500 シリーズ スイッチにする必要があります。

Network Assistant ∠ VTY

Network Assistant は VTY 回線を使用して、クラスタ コマンド デバイスと通信します。Catalyst 4500 シリーズ スイッチには、デフォルト設定で 5 本の VTY 回線が設定されています。Network Assistant では、その他に 8 本の回線を採用できます。このため、最大数の回線(または最低 8+5=13)を設定し、Network Assistant がスイッチとやり取りできるようにして、Telnet で必要となる可能性がある VTY 回線を使用しないでください。

line vty コンフィギュレーション コマンドを使用して、適切な VTY 回線数をサポートするよう Catalyst 4500 シリーズ スイッチを設定できます。たとえば、VTY 回線を 9 本含めるようスイッチを設定するには、line vty 6 15 コマンドを使用します。



(注)

既存の VTY 回線がデフォルト以外の設定の場合、この設定を新しい VTY 回線に適用する必要があります。

候補スイッチとクラスタ メンバ スイッチの特性

候補スイッチとは、クラスタに含まれないクラスタ対応スイッチです。クラスタ メンバ スイッチ とは、現在スイッチ クラスタに含まれているスイッチです。候補スイッチまたはクラスタ メンバスイッチには独自の IP アドレスおよびパスワードがありますが、必須ではありません。



(注)

候補のホスト名では、[a-zA-Z0-9]-n 形式は禁止されています。n は $0 \sim 16$ です。これらの名前は予約済みです。

クラスタに加入するには、候補スイッチは次の要件を満たす必要があります。

- クラスタ対応ソフトウェアを実行し、クラスタリングがイネーブルであること。
- CDP バージョンがイネーブルであること。
- HTTP サーバがイネーブルであること。



(注)

コマンダ スイッチ上で HTTP がイネーブルの場合でも、 コマンダ スイッチとメンバ スイッチ間の通信は HTTP を通じて行われます。 そのため、 セキュアではありません。

- 16本の VTY 回線があること。
- 別のクラスタのコマンドまたはクラスタ メンバ スイッチではないこと。
- 最低 1 つの共通 VLAN を介してクラスタ コマンド スイッチに接続していること。 Catalyst 4500 候補スイッチおよびクラスタ メンバ スイッチを設定する場合は、クラスタ コマンド スイッチとの VLAN 接続上の Switch Virtual Interface (SVI; スイッチ仮想インターフェイス)を使用することを推奨します。

CLI を使用したスイッチ クラスタ管理

クラスタ コマンド スイッチに最初にログインすると、CLI からクラスタ コマンド スイッチを設定できます。Telnet セッションを(コンソールまたは Telnet 接続によって)開始し、クラスタ メンバスイッチ CLI にアクセスするには、rcommand ユーザ EXEC コマンドを使用し、クラスタ メンバスイッチ番号を入力します。コマンド モードは変更され、Cisco IOS コマンドは通常どおり動作します。コマンドスイッチ CLI に戻すには、クラスタ メンバスイッチの exit 特権 EXEC コマンドを使用します。

次に、コマンドスイッチ CLI からメンバ スイッチ 3 にログインする例を示します。

switch# rcommand 3

メンバスイッチ番号がわからない場合、クラスタコマンドスイッチの show cluster members 特権 EXEC コマンドを使用します。rcommand コマンドおよびその他すべてのクラスタコマンドの詳細 については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』を参照してください。

Telnet セッションは、クラスタ コマンド スイッチと同じ特権レベルでメンバ スイッチ CLI にアクセスします。そのあと、Cisco IOS コマンドは通常どおり動作します。Telnet セッションのスイッチの設定方法については、「Telnet を使用して CLI にアクセスする場合」(p.2-2)を参照してください。



CISCO-CLUSTER_MIB はサポートされません。

コミュニティ モードまたはクラスタ モードでの Network Assistant の設定



(**注**) コミュニティは Supervisor Engine 6-E ではサポートされて*いません*。

ここでは、コミュニティまたはクラスタで稼働する Network Assistant の設定で使用される CLI の詳細を説明します。Network Assistant は、HTTP (または HTTPS)接続で Cisco IOS コマンドを送信することで、Catalyst 4500 シリーズ スイッチと通信します。

ここでは、次の内容について説明します。

- コミュニティ モードのネットワーク スイッチ上での Network Assistant の設定 (p.12-14)
- クラスタ モードのネットワーク スイッチ上での Network Assistant の設定 (p.12-18)

コミュニティ モードのネットワーク スイッチ上での Network Assistant の設定

コミュニティ モードのネットワーク スイッチ上で Network Assistant を設定するには、スイッチで次の手順を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	Switch(config)# enable password name	コンフィギュレーション モードのパスワード保護 をイネーブルにします。
ステップ 3	Switch(config)# vtp domain name	VLAN を管理するために、VTP ドメインを作成します。

	コマンド	目的
ステップ 4	Switch(config)# vlan vlan_id	VLAN を作成します。
ステップ 5	<pre>Switch(config-vlan)# interface {vlan vlan_ID {fastethernet gigabitethernet} slot/interface Port-channel number}</pre>	ご使用の CNA 対応 PC に接続するインターフェイス を選択します。
ステップ 6	Switch(config-if)# switchport access vlan vlan_id	指定の VLAN で選択されたインターフェイスをイネーブルにします。
ステップァ	Switch(config-if)# interface {vlan vlan_ID slot/interface Port-channel number}	設定用の VLAN インスタンスを選択します。
ステップ 8	Switch(config-if)# ip address ip_address	SVI に IP アドレスを割り当てます。
ステップ 9	Switch(config-if)# no shutdown	インターフェイスをイネーブルにします。
ステップ 10	Switch(config-if)# ip http server	Network Assistan がスイッチと対話できるよう HTTP サーバを開始します。
ステップ 11	Switch(config)# ip domain-name domain_name	スイッチでドメイン名をイネーブルにして、HTTPS を設定します。
ステップ 12	Switch(config)# ip http secure-server	スイッチ上で HTTPS サーバをイネーブルにします。 デフォルトでは、HTTPS サーバはディセーブルに設 定されています。
ステップ 13	<pre>Switch(config)# ip http max-connections connection_number</pre>	HTTP サーバへの最大同時接続数を設定します。 16 の connection_number を推奨します。
ステップ 14	Switch(config)# ip http timeout-policy idle idle_time life life_time requests requests	HTTPS ポートを設定します。
		idle キーワードでは、接続がアイドル状態でいる最大時間数を指定します。180 秒の idle 値を推奨します。
		life キーワードでは、接続が確立してからオープンでいる最大時間数を指定します。180 秒の life 値を推奨します。
		requests キーワードでは、接続の最大要求数を指定します。25の requests 値を推奨します。
ステップ 15	Switch(config-if)# ip http secure-server	(任意)スイッチが Network Assistant からの HTTPS 接続を受け入れるようにします。
ステップ 16	Switch(config)# ip route a.b.c	デフォルト ルータとのルートを確立します。これは 通常、ローカル インターネット プロバイダーにより 供給されます。
		(注) この回線のみが、スタンドアロン スイッチ とネットワーク スイッチの設定の相違点で す。
ステップ 17	Switch(config)# line con 0	コンソール ポートを選択して設定を実行します。
ステップ 18	Switch(config-line)# exec-timeout x y	端末にキーボード入力または出力が表示されない場合、自動セッション ログアウトを設定します。
ステップ 19	Switch(config-line)# password password	コンソール ポートのパスワードを指定します。
	Switch(config-line)# login	コンソール ポートへのログインを許可します。
ステップ 21	Switch(config-line)# line vty x y	CNA がスイッチにアクセスするための追加の VTY 回線を作成します。
ステップ 22	Switch(config-line)# password password	スイッチのパスワードを指定します。

	コマンド	目的
ステップ 23	Switch(config-line)# login	スイッチへのログインを許可します。
ステップ 24	Switch(config-line)# line vty x y	CNA がスイッチにアクセスするための追加の VTY 回線を作成します。
ステップ 25	Switch(config-line)# password password	スイッチのパスワードを指定します。
ステップ 26	Switch(config-line)# login	スイッチへのログインを許可します。
ステップ 27	Switch(config-line)# end	特権 EXEC モードに戻ります。
ステップ 28	Switch# show running-config	設定を確認します。

ここでは、コミュニティ モードのネットワーク スイッチ上で Network Assistant を設定する例を示します。

```
Switch# configure terminal
Switch(config) # vtp domain cnadoc
Changing VTP domain name from cisco to cnadoc
Switch(config) # vlan 2
Switch(config-vlan)# exit
Switch(config)# interface GigabitEthernet 2/1
Switch(config-if) # switchport access vlan 2
Switch(config-if)# exit
Switch(config)# interface vlan 2
Switch(config-if) # ip address 123.123.123.1 255.255.255.0
Switch(config-if) # no shutdown
Switch(config-if)# exit
Switch(config) # ip http server
Switch(config) # ip domain-name cisco.com
Switch(config) # ip http secure-server
Switch(config) # ip http max-connections 16
Switch(config)# ip http timeout-policy idle 180 life 180 requests 25
Switch(config) # ip route 0.0.0.0 0.0.0.0 123.123.123.2
Switch(config) # line con 0
Switch(config-line) # exec-timeout 0 0
Switch(config-line) # password keepout
Switch(config-line) # login
Switch(config-line) # line vty 5 15
Switch(config-line) # password keepout
Switch(config-line) # login
Switch(config-line) # line vty 5 15
Switch(config-line) # end
Switch# show running-config
Building configuration...
Current configuration: 1426 bytes
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service compress-config
hostname Switch
boot-start-marker
boot-end-marker
enable password cna
no aaa new-model
ip subnet-zero
ip domain-name cisco.com
vtp domain cnadoc
```

```
vtp mode transparent
crypto pki trustpoint TP-self-signed-913087
enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-913087
revocation-check none
rsakeypair TP-self-signed-913087
crypto pki certificate chain TP-self-signed-913087
 certificate self-signed 01
  3082028E 308201F7 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  52312B30 29060355 04031322 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 39313330 38373123 30210609 2A864886 F70D0109 02161456
  61646572 2D343531 302E6369 73636F2E 636F6D30 1E170D30 36303432 30323332
 3435305A 170D3230 30313031 30303030 30305A30 52312B30 29060355 04031322
  494F532D 53656C66 2D536967 6E65642D 43657274 69666963 6174652D 39313330
  38373123 30210609 2A864886 F70D0109 02161456 61646572 2D343531 302E6369
  73636F2E 636F6D30 819F300D 06092A86 4886F70D 01010105 0003818D 00308189
  02818100 F2C86FEA 49C37856 D1FA7CB2 9AFF748C DD443295 F6EC900A E83CDA8E
  FF8F9367 0A1E7A20 C0D3919F 0BAC2113 5EE37525 94CF24CF 7B313C01 BF177A73
  494B1096 B4D24729 E087B39C E44ED9F3 FCCD04BB 4AD3C6BF 66E0902D E234D08F
  E6F6C001 BAC80854 D4668160 9299FC73 C14A33F3 51A17BF5 8C0BEA07 3AC03D84
  889F2661 02030100 01A37430 72300F06 03551D13 0101FF04 05300301 01FF301F
  0603551D 11041830 16821456 61646572 2D343531 302E6369 73636F2E 636F6D30
 1F060355 1D230418 30168014 BB013B0D 00391D79 B628F2B3 74FC62B4 077AD908
  301D0603 551D0E04 160414BB 013B0D00 391D79B6 28F2B374 FC62B407 7AD90830
  0D06092A 864886F7 0D010104 05000381 81002963 26762EFA C52BA4B3 6E641A9D
  742CE404 E45FECB1 B5BD2E74 6F682476 A7C3DAA5 94393AE3 AA103B6E 5974F81B
  09DF16AE 7F9AE67C 5CB3D5B1 B945A5F3 36A8CC8C 8F142364 F849344D 5AE36410
 51182EB9 24A9330B 3583E1A3 79151470 D304C157 3417E240 52BE2A91 FC7BBEDE
  562BEDAD E6C46D9A F7FF3148 4CE9CEE1 5B17
  quit
!
- !
power redundancy-mode redundant
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
vlan 2
- 1
interface GigabitEthernet1/1
switchport access vlan 2
interface GigabitEthernet1/2
interface GigabitEthernet1/3
interface GigabitEthernet1/4
interface GigabitEthernet1/5
interface GigabitEthernet1/6
interface GigabitEthernet1/7
interface GigabitEthernet1/8
interface GigabitEthernet1/9
interface GigabitEthernet1/10
interface GigabitEthernet1/11
interface GigabitEthernet1/12
1
```

```
interface GigabitEthernet1/13
interface GigabitEthernet1/14
interface GigabitEthernet1/15
interface GigabitEthernet1/16
interface GigabitEthernet1/17
interface GigabitEthernet1/18
interface GigabitEthernet1/19
interface GigabitEthernet1/20
interface Vlan1
no ip address
interface Vlan2
ip address 123.123.123.1 255.255.255.0
ip route 0.0.0.0 0.0.0.0 123.123.123.2
ip http server
ip http secure-server
ip http max-connections 16
ip http timeout-policy idle 180 life 180 requests 25
line con 0
password cna
login
 stopbits 1
line vty 0 4
password cna
login
line vty 5 15
password cna
login
!
end
Switch#
```

クラスタ モードのネットワーク スイッチ上での Network Assistant の設定

クラスタ モードのネットワーク スイッチ上で Network Assistant を設定するには、スイッチで次の手順を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	Switch(config)# enable password name	コンフィギュレーション モードのパスワード保護 をイネーブルにします。
ステップ 3	Switch(config)# vtp domain name	VLAN および名前を管理するために、VTP ドメイン を作成します。
ステップ 4	Switch(config)# cluster run	クラスタ コマンダ上でクラスタを開始します。
ステップ 5	<pre>Switch(config)# cluster enable cluster_name</pre>	スイッチをクラスタコマンダに設定します。
ステップ 6	Switch(config)# vlan vlan_id	VLAN を作成します。

	コマンド	目的
ステップ 7	Switch(config-vlan)# interface {vlan vlan_ID {fastethernet gigabitethernet} slot/interface Port-channel number}	ご使用の CNA 対応 PC に接続するインターフェイス を選択します。
ステップ 8	Switch(config-if)# switchport access vlan vlan_id	指定の VLAN 内の物理ポートをイネーブルにします。
ステップ 9	Switch(config-if)# interface {vlan vlan_ID slot/interface Port-channel number}	設定用の VLAN インスタンスを選択します。
ステップ 10	Switch(config-if)# ip address ip_address	SVI に IP アドレスを割り当てます。
ステップ 11	Switch(config-if)# no shut	インターフェイスをイネーブルにします。
ステップ 12	Switch(config-if)# ip http server	Network Assistan がスイッチと対話できるよう HTTP サーバを開始します。
ステップ 13	Switch(config)# ip http secure-server	(任意)スイッチが Network Assistant からの HTTPS 接続を受け入れるようにします。
ステップ 14	Switch(config)# ip route a.b.c	デフォルト ルータとのルートを確立します。これは 通常、ローカル インターネット プロバイダーにより 供給されます。
		(注) この回線のみが、スタンドアロン スイッチ とネットワーク スイッチの設定の相違点で す。
ステップ 15	Switch(config)# line con 0	コンソール ポートを選択して設定を実行します。
ステップ 16	Switch(config-line)# exec-timeout x y	端末にキーボード入力または出力が表示されない場 合、自動セッション ログアウトを設定します。
ステップ 17	Switch(config-line)# password password	コンソール ポートのパスワードを指定します。
ステップ 18	Switch(config-line)# login	コンソール ポートへのログインを許可します。
ステップ 19	Switch(config-line)# line vty x y	CNA がスイッチにアクセスするための追加の VTY 回線を作成します。
ステップ 20	Switch(config-line)# password password	スイッチのパスワードを指定します。
ステップ 21	Switch(config-line)# login	スイッチへのログインを許可します。
ステップ 22	Switch(config-line)# line vty x y	CNA がスイッチにアクセスするための追加の VTY 回線を作成します。
ステップ 23	Switch(config-line)# password password	スイッチのパスワードを指定します。
ステップ 24	Switch(config-line)# login	スイッチへのログインを許可します。
ステップ 25	Switch(config-line)# end	特権 EXEC モードに戻ります。
ステップ 26	Switch# show running-config include http	HTTP サーバがイネーブルであることを確認します。

ここでは、クラスタ モードのネットワーク スイッチ上で Network Assistant を設定する例を示します。

```
Switch# configure terminal
Switch(config)# vtp domain cnadoc
Switch(config)# cluster run
Switch(config) # cluster enable cnadoc
Switch(config) # vlan 10
Switch(config-vlan) # interface GigabitEthernet 2/1
Switch(config-if) # switchport access vlan 10
Switch(config-if) # interface vlan10
Switch(config-if) # ip address aa.bb.cc.dd
Switch(config-if)# no shut
Switch(config-if)# ip http server
Switch(config-if)# ip http secure-server
Switch(config)# ip route 0.0.0.0 0.0.0.0 123.123.123.2
Switch(config) # line con 0
Switch(config-line) # exec-timeout 0 0
Switch(config-line)# password keepout
Switch(config-line) # login
Switch(config-line) # line vty 5 15
Switch(config-line) # password keepout
Switch(config-line) # login
Switch(config-line) # line vty 5 15
Switch(config-line) # end
Switch# show running-config
Building configuration...
Current configuration: 1469 bytes
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service compress-config
hostname Switch
boot-start-marker
boot-end-marker
enable password cna
no aaa new-model
ip subnet-zero
- 1
vtp domain cnadoc
vtp mode transparent
cluster run
cluster enable cnadoccluster 0
power redundancy-mode redundant
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
vlan 2
1
interface GigabitEthernet1/1
switchport access vlan 2
interface GigabitEthernet1/2
```

```
interface GigabitEthernet1/3
interface GigabitEthernet1/4
interface GigabitEthernet1/5
interface GigabitEthernet1/6
interface GigabitEthernet1/7
interface GigabitEthernet1/8
interface GigabitEthernet1/9
interface GigabitEthernet1/10
1
interface GigabitEthernet1/11
interface GigabitEthernet1/12
interface GigabitEthernet1/13
interface GigabitEthernet1/14
interface GigabitEthernet1/15
interface GigabitEthernet1/16
interface GigabitEthernet1/17
interface GigabitEthernet1/18
interface GigabitEthernet1/19
1
interface GigabitEthernet1/20
interface Vlan1
no ip address
interface Vlan2
ip address 123.123.123.1 255.255.255.0
ip route 0.0.0.0 0.0.0.0 123.123.123.2
ip http server
no ip http secure-server
line con 0
Switch#
```

Network Assistant の設定および使用法



CHAPTER

13

VLAN、VTP、および VMPS の設定

この章では、Catalyst 4500 シリーズ スイッチの VLAN (仮想 LAN) について説明します。また、VLAN Trunking Protocol(VTP; VLAN トランキング プロトコル)をイネーブルにして、Catalyst 4500 シリーズ スイッチを VLAN Membership Policy Server(VMPS; VLAN メンバシップ ポリシー サーバ) クライアントとして設定する方法についても説明します。

この章の主な内容は、次のとおりです。

- VLAN (p.13-2)
- VTP (p.13-9)
- VMPS (p.13-19)



この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/cr/index.htm

VLAN

ここでは、主に次の内容について説明します。

- VLAN の概要 (p.13-2)
- VLAN 設定時の注意事項および制約事項 (p.13-4)
- VLAN のデフォルト設定 (p.13-5)
- VLAN の設定 (p.13-6)

VLAN の概要

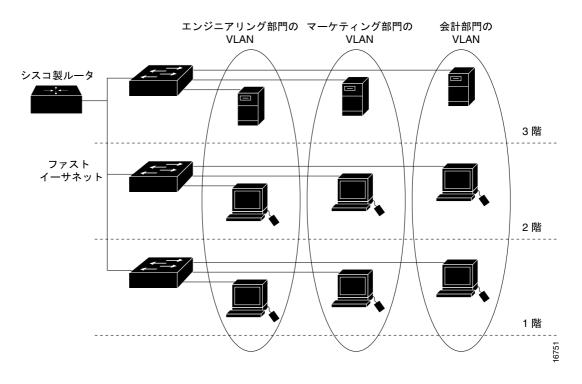
VLAN は、1 つまたは複数の LAN 上のデバイス グループで、実際には複数の異なる LAN セグメント上にある場合でも、同じワイヤに接続するように通信設定されています。 VLAN は物理的な接続ではなく論理的な接続に基づくため、非常に柔軟性があります。

VLAN は、レイヤ 2 ネットワークのブロードキャスト ドメインを決定します。ブロードキャスト ドメインは、設定内のいずれかのデバイスから発信されたブロードキャスト フレームを受信するす べてのデバイス セットです。ブロードキャスト ドメインは通常、ルータによって分割されます。これはルータがブロードキャスト フレームを転送しないためです。レイヤ 2 スイッチは、スイッチの設定に基づいてブロードキャスト ドメインを作成します。スイッチは、複数のブロードキャスト ドメイン作成を可能にするマルチポート ブリッジです。ブロードキャスト ドメインは、スイッチ内の個々の仮想ブリッジのように機能します。

スイッチ内で 1 つまたは複数の仮想ブリッジを定義できます。スイッチ内で作成した仮想ブリッジは、新しいブロードキャスト ドメイン (VLAN) を定義します。スイッチ内、または 2 つのスイッチ間で、トラフィックが直接別の VLAN (ブロードキャスト ドメイン間) に接続されることはありません。 2 つの異なる VLAN を相互接続するには、ルータまたはレイヤ 3 スイッチが必要です。 Catalyst 4500 シリーズ スイッチの VLAN 間ルーティングについての詳細は、「レイヤ 3 インターフェイスの概要」 (p.27-2) を参照してください。

図 13-1 に、論理的に定義されたネットワークを作成する 3 つの VLAN の例を示します。

図 13-1 VLAN の例



VLAN は多くの場合、IP サブネットワークと対応付けられています。たとえば、特定の IP サブネットに含まれるすべてのエンド ステーションを同じ VLAN に所属させる場合などです。VLAN 相互間のトラフィックは、ルーティングする必要があります。LAN インターフェイスの VLAN メンバシップは、インターフェイス別に割り当てる必要があります(これはインターフェイスベースまたはスタティックな VLAN メンバシップと呼ばれます)。

管理ドメイン内に VLAN を作成する場合、次のパラメータを設定できます。

- VLAN 番号
- VLAN 名
- VLAN タイプ
- VLAN ステート (アクティブまたは中断)
- VLAN の 最大伝送ユニット (maximum transmission unit[MTU])
- Security Association Identifier (SAID)
- VLAN タイプを別のタイプに変換する場合に使用する VLAN 番号



ソフトウェアを使用して VLAN のタイプを変換する場合は、各メディア タイプごとに異なる VLAN 番号が必要になります。

VLAN 設定時の注意事項および制約事項

ネットワーク上で VLAN を作成および変更するときは、次の注意事項および制約事項に従ってください。

- VLAN を作成する前に、Catalyst 4500 シリーズ スイッチを VTP サーバ モードまたは VTP トランスペアレント モードに変更してください。Catalyst 4500 シリーズ スイッチが VTP サーバであれば、VTP ドメインを定義する必要があります。VTP の設定手順については、VTP (p.13-9)を参照してください。
- VLAN データベース モードでは、Cisco IOS の end コマンドはサポートされていません。
- Ctrl-Z を押して、VLAN データベース モードを終了することはできません。

VLAN 範囲



4094 の VLAN を使用するには、拡張システム ID をイネーブルにする必要があります。「ブリッジ ID の概要」(p.17-2) を参照してください。

Cisco IOS Release 12.2(25)EWA 以降では、Catalyst 4500 シリーズ スイッチは IEEE 802.1Q 規格に準拠し、4096 の VLAN をサポートしています。これらの VLAN は、予約、標準、拡張の 3 つの範囲に分けられます。

4096 の VLAN の一部は、VTP を使用した場合、ネットワーク内の他のスイッチに伝播されます。 拡張範囲 VLAN は伝播されないので、各ネットワーク デバイス上で拡張範囲 VLAN を手動で設定 する必要があります。

表 13-1 で、VLAN 範囲の使い方について説明します。

表 13-1 VLAN 範囲

VLAN	範囲	用途	VTP による 伝播
0、4095	予約	システム専用。ユーザがこれらの VLAN を表示または使用することはできません。	_
1	標準	シスコのデフォルト。ユーザはこの VLAN を使用できますが、削除はできません。	含まれる
2 ~ 1001	標準	イーサネット VLAN 用。 ユーザはこれらの VLAN を作成、使用、削除できます。	含まれる
1002 ~ 1005	標準	Fiber Distributed Data Interface (FDDI; ファイバ分散データ インターフェイス) およびトークンリングの場合のシスコのデフォルト。ユーザは VLAN 1002 ~ 1005 を削除できません。	含まれる

表 13-1 VLAN 範囲(続き)

VLAN	範囲	用途	VTP による 伝播
1006 ~ 4094	拡張	イーサネット VLAN 専用。拡張範囲 VLAN を設定する場合、次の点に注意してください。	含まれない
		• レイヤ 3 ポートおよび一部のソフトウェア機能には、内部 VLAN が必要です。内部 VLAN は 1006 以上から割り当てます。このような用途にすでに割り当てられている VLAN を使用できません。内部利用の VLAN を表示するには、show vlan internal usage コマンドを入力します。	
		• Catalyst 製品ファミリ ソフトウェアが稼働しているスイッチでは、VLAN 1006 ~ 1024を設定できません。VLAN 1006 ~ 1024を設定する場合は、その VLAN が Catalyst 製品ファミリ ソフトウェアが稼働しているスイッチに拡張されないようにしてください。	
		• 拡張範囲 VLAN を使用するには、拡張システム ID をイネーブルにする必要があります。「拡張システム ID のイネーブル化」 $(p.17-10)$ を参照してください。	

標準範囲の VLAN で設定できるパラメータ



(注)

イーサネット VLAN 1 および 1006 ~ 4094 で使用するのは、デフォルト値だけです。

VLAN 2 ~ 1001 には次のパラメータを設定できます。

- VLAN 名
- VLAN タイプ
- VLAN ステート (アクティブまたは中断)
- SAID
- VLAN の Spanning-Tree Protocol (STP; スパニングツリー プロトコル) タイプ

VLAN のデフォルト設定

表 13-2 に、VLAN のデフォルト設定の値を示します。

表 13-2 イーサネット VLAN のデフォルトおよび範囲

パラメータ	デフォルト	有効な値
VLAN ID	1	1 ~ 4094
VLAN 名	$VLANx_o x$ はソフトウェアで割り当てられた番号です。	範囲なし
802.10 SAID	100,001	1 ~ 4,294,967,294
MTU サイズ	1500	1500 ~ 18,190
トランスレーショナル ブリッジ 1	1002	0 ~ 1005
トランスレーショナル ブリッジ2	1003	0 ~ 1005
VLAN ステート	active	アクティブ、サスペンド、 シャットダウン



Catalyst 4500 シリーズ スイッチは、トークンリングまたは FDDI メディアをサポートしません。スイッチは FDDI、FDDI-Net、Token Ring Concentrator Relay Function (TrCRF; トークンリング コンセントレータ リレー機能) または Token Ring Bridge Relay Function (TrBRF; トークンリング ブリッジ リレー機能) トラフィックを転送しませんが、VTP を通して VLAN 設定を伝播します。ソフトウェアはこれらのメディア タイプのパラメータを保存しますが、実際にはサポートされていません

VLAN の設定



(注)

VLAN を設定する前に、VTP を使用して、ネットワークのグローバル VLAN 設定情報を管理する必要があります。VTP については、VTP (p.13-9) を参照してください。



(注)

VLAN は多くのパラメータをサポートしています。ここでは、すべてのパラメータについては詳しく説明しません。詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』を参照してください。



(注)

VLAN の設定は **vlan.dat** ファイルに保存され、vlan.dat ファイルは不揮発性メモリに保存されます。 **vlan.dat** ファイルを手動で削除すると、VLAN データベースに矛盾が生じる可能性があります。 VLAN の設定または VTP を変更する場合は、ここに記載されているコマンドおよび『*Catalyst 4500 Series Switch Cisco IOS Command Reference*』に記載されているコマンドを使用してください。

ここでは、VLAN の設定手順について説明します。

- グローバル コンフィギュレーション モードでの VLAN の設定 (p.13-6)
- VLAN へのレイヤ 2 LAN インターフェイスの割り当て (p.13-8)

グローバル コンフィギュレーション モードでの VLAN の設定

スイッチが VTP サーバ モードまたはトランスペアレント モードの場合は(「VTP $_{
m IP}$ $_{
m IP}$

スイッチが VLAN トランスペアレント モードの場合に、copy running-config startup-config コマンドを実行すると、VLAN の設定が startup-config ファイルに保存されます。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として保存したあとに、show running-config コマンドおよび show startup-config コマンドを実行すると、VLAN の設定が表示されます。



(注)

スイッチの起動時に、startup-config ファイルおよび vlan.dat ファイル内の VTP ドメイン名と VTP モードが異なる場合、スイッチは vlan.dat ファイル内の設定を使用します。

ポート メンバシップ モードを定義したり、VLAN のポートを追加および削除するには、インターフェイス コンフィギュレーション コマンド モードを使用します。これらのコマンドの結果は、running-config ファイルに書き込まれます。このファイルを表示するには、show running-config コマンドを使用します。

ユーザが設定した VLAN には、 $1\sim4094$ の一意の ID が割り当てられます。VLAN を作成する場合、未使用の ID で vlan コマンドを入力します。特定の ID が使用されているかどうかを確認するには、show vlan id ID コマンドを使用します。VLAN を修正する場合は、既存の VLAN に vlan コマンドを使用します。

VLAN の作成時に割り当てられるデフォルト パラメータの一覧は、「VLAN のデフォルト設定」 (p.13-5)を参照してください。media キーワードを使用しないで VLAN タイプを指定する場合、 VLAN はイーサネット VLAN になります。

VLAN を作成するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# vlan vlan_ID Switch(config-vlan)#	イーサネット VLAN を追加します。 (注) 次のメディア タイプのデフォルト VLAN は削除できません。イーサネット VLAN 1、FDDI またはToken Ring VLAN 1002 ~ 1005 です。 VLAN を削除する場合は、この VLAN に割り当てられたアクセス ポートとして設定された LAN インターフェイスはいずれも、非アクティブになります。これらのインターフェイスは、新しい VLANに割り当てられるまで、元の VLANに(非アクティ
ステップ 3	Switch(config-vlan)# end	プのまま)対応付けられています。 VLAN を削除する場合は、no キーワードを使用します。 Switch(config-vlan)#と表示される場合、VLAN コンフィギュレーション モードで実行しています。新しく作成された VLAN のパラメータを変更する場合は、このモードを使用します。 VLAN コンフィギュレーション モードからイネーブル
ステップ 4	Switch# show vlan [id name] vlan_name	モードに戻ります。 VLAN の設定を確認します。

イーサネット VLAN を作成または変更する場合は、次の点に注意してください。

- レイヤ 3 ポートおよび一部のソフトウェア機能には、1006 以上から昇順に内部 VLAN を割り 当てる必要があるため、拡張範囲 VLAN は 4094 から降順に設定してください。
- 拡張範囲 VLAN はグローバル コンフィギュレーション モードでのみ設定できます。VLAN データベース モードで拡張範囲 VLAN を設定することはできません。
- レイヤ 3 ポートおよび一部のソフトウェア機能は、拡張範囲 VLAN を使用します。作成または 変更対象の VLAN がレイヤ 3 ポートまたはソフトウェア機能によって使用中の場合、スイッチ からメッセージが表示され、VLAN 設定は変更されません。

次に、グローバル コンフィギュレーション モードでイーサネット VLAN を作成し、設定を確認する例を示します。

VLAN へのレイヤ 2 LAN インターフェイスの割り当て

Switch#

管理対象ドメイン内で作成された VLAN は、VLAN に 1 つまたは複数の LAN を割り当てるまで未使用の状態のままとなります。



適切なタイプの VLAN に LAN インターフェイスを割り当ててください。イーサネットタイプの VLAN には、ファスト イーサネット インターフェイス、ギガビット イーサネット インターフェイス、10 ギガビット イーサネット インターフェイスを割り当てます。

VLAN に 1 つまたは複数の LAN インターフェイスを割り当てるには、「レイヤ 2 スイッチング用のイーサネット インターフェイスの設定」(p.15-7) に記載されている作業を行います。

VTP

ここでは、Catalyst 4500 シリーズ スイッチの VTP について説明します。

ここでは、主に次の内容について説明します。

- VTPの概要 (p.13-9)
- VTP 設定時の注意事項および制約事項 (p.13-13)
- VTP のデフォルト設定 (p.13-13)
- VTPの設定 (p.13-14)

VTP の概要

VTP はレイヤ 2 のメッセージ プロトコルで、VTP ドメインにおける VLAN の追加、削除、名前変更などを管理することにより、VLAN 設定の一貫性を維持します。VTP ドメイン (別名 VLAN 管理ドメイン)は、同じ VTP ドメイン名を共有し、トランクで相互接続された 1 つまたは複数のネットワーク デバイスで構成されます。VTP を使用すると、VLAN 名の重複、無効な VLAN タイプの指定、セキュリティ違反などのさまざまな問題によって生じる不正な設定および設定の矛盾を最小限に抑えることができます。

VLAN を作成する前に、ネットワークで VTP を使用するかどうかを決定する必要があります。VTP を使用すると、1 台または複数のネットワーク デバイス上で中央集約的に設定変更を行い、それらの変更を自動的にネットワーク上の他のネットワーク デバイスに伝達できます。VLAN の設定の詳細については、「VLAN」(p.13-2) を参照してください。

ここでは、VTP の機能について説明します。

- VTP ドメインの概要 (p.13-9)
- VTP モードの概要 (p.13-10)
- VTP アドバタイズの概要 (p.13-10)
- VTP バージョン 2 の概要 (p.13-11)
- VTP プルーニングの概要 (p.13-11)

VTP ドメインの概要

VTP ドメインは、同じ VTP ドメイン名を共有し、相互接続された 1 つまたは複数のネットワーク デバイスで構成されます。1 台のネットワーク デバイスが所属できる VTP ドメインは 1 つだけで す。ドメインのグローバル VLAN 設定を変更するには、CLI (コマンドライン インターフェイス) または SNMP (簡易ネットワーク管理プロトコル)を使用します。

デフォルトでは、Catalyst 4500 シリーズ スイッチは VTP トランスペアレント モードで、スイッチがトランク リンクを介してドメインに関するアドバタイズを受信するか、またはユーザが管理ドメインを設定しないかぎり、非管理ドメインのままです。管理ドメイン名を指定するか、ルータがドメイン名を学習するまで、VTP サーバ上での VLAN の作成または変更はできません。

スイッチがトランク リンクを介して VTP アドバタイズを受信すると、ルータは管理ドメイン名および VTP 設定リビジョン番号を継承します。スイッチは、別の管理ドメイン名または古い設定リビジョン番号が指定されたアドバタイズについては、一切無視します。

スイッチを VTP トランスペアレントとして設定した場合、VLAN の作成および変更は可能ですが、その変更が作用するのは個々のスイッチに限られます。

VTP サーバ上の VLAN 設定を変更すると、その変更は VTP ドメイン内のすべてのネットワーク デバイスに伝播されます。 VTP アドバタイズは、すべての ISL(スイッチ間リンク)と IEEE 802.1Qトランク接続に伝送されます。

VTP は、固有の名前と内部インデックスの対応によって、複数の LAN タイプに対して VLAN を動的にマッピングします。このマッピングにより、ネットワーク管理者の不要なデバイス管理が軽減されます。

VTP モードの概要

次のいずれかの VTP モードで動作するように Catalyst 4500 シリーズ スイッチを設定できます。

- サーバ VTP サーバ モードでは、VLAN の作成、変更、および削除を行うことができます。また、VTP ドメイン全体に対して他の設定パラメータ(VTP バージョン、VTP プルーニングなど)を指定できます。VTP サーバは、同一 VTP ドメイン内の他のネットワーク デバイスに VLAN 設定をアドバタイズし、トランク リンクを介して受信したアドバタイズに基づいて、VLAN 設定を他のネットワーク デバイスと同期させます。
- クライアント VTP クライアントは、VTP サーバと同様に動作しますが、VTP クライアント 上で VLAN の作成、変更、または削除を行うことはできません。
- トランスペアレント VTP トランスペアレント ネットワーク デバイスは、VTP に参加しません。VTP トランスペアレント ネットワーク デバイスは、VLAN 設定をアドバタイズせず、受信したアドバタイズに基づいて同期させることもありません。ただし VTP バージョン 2 では、トランスペアレント ネットワーク デバイスは、トランキング LAN インターフェイスで受信した VTP アドバタイズを転送します。VTP トランスペアレントがデフォルトのモードです。



Catalyst 4500 シリーズ スイッチは、スイッチが NVRAM(不揮発性 RAM)への設定の書き込み中に障害を検出すると、自動的に VTP サーバ モードから VTP クライアント モードに切り替わります。この場合、NVRAM が正常に動作するまで、スイッチを VTP サーバ モードに戻すことはできません。

VTP アドバタイズの概要

VTP ドメインの各ネットワーク デバイスは、予約されたマルチキャスト アドレスに対して、各トランキング LAN インターフェイスからアドバタイズを定期的に送信します。 VTP アドバタイズを 受信した近接するネットワーク デバイスは、必要に応じて各自の VTP 設定および VLAN 設定を更新します。

VTP アドバタイズでは、次のグローバル設定情報が配布されます。

- VLAN ID (ISL および 802.10)
- エミュレートされた LAN 名 (Asynchronous Transfer Mode [ATM; 非同期転送モード] LAN emulation [LANE; LAN エミュレーション]用)
- 802.10 SAID 値 (FDDI)
- VTPドメイン名
- VTP 設定リビジョン番号
- 各 VLAN の MTU サイズを含めた VLAN 設定
- フレーム フォーマット

VTP バージョン2の概要

ネットワークで VTP を使用する場合は、VTP バージョン 1 またはバージョン 2 のどちらを使用するかを決定する必要があります。



Catalyst 4500 シリーズ スイッチは、トークンリングまたは FDDI メディアをサポートしません。スイッチは、FDDI、FDDI-Net、TrCRF、または TrBRF トラフィックを転送しませんが、VTP を通じて VLAN 設定を伝播します。

VTP バージョン 1 ではサポートされず、バージョン 2 でサポートされる機能は、次のとおりです。

- トークンリング サポート VTP バージョン 2 はトークンリング LAN スイッチングと VLAN (TrBRF と TrCRF) をサポートします。
- 認識不能な Type-Length-Value (TLV) のサポート VTP サーバまたはクライアントは、TLV が解析不能であっても、設定の変更を他のトランクに伝播します。認識されなかった TLV は、NVRAM に保存されます。
- バージョン依存型トランスペアレント モード VTP バージョン 1 の場合、VTP トランスペアレント ネットワーク デバイスは、VTP メッセージの中のドメイン名およびバージョンを調べ、バージョンおよびドメイン名が一致する場合に限ってメッセージを転送します。スーパーバイザ エンジン ソフトウェアでサポートされるドメインは 1 つだけなので、VTP バージョン 2 は、バージョンをチェックせずに VTP メッセージをトランスペアレント モードで転送します。
- 整合性検査 VTP バージョン 2 では、CLI または SNMP によって新しい情報が入力された場合に限り、VLAN 整合性検査(VLAN 名、値など)を行います。VTP メッセージから新しい情報を取得した場合、または NVRAM から情報を読み込んだ場合には、整合性検査を行いません。受信した VTP メッセージのダイジェストが有効であれば、整合性検査を行わずに情報が受け入れられます。

VTP プルーニングの概要

VTP プルーニングは、ブロードキャスト パケット、マルチキャスト パケット、ユニキャスト パケットなど、不要なフラッディング トラフィックを削減することにより、ネットワークの帯域幅を拡張します。 VTP プルーニングを使用すると、トラフィックが適切なネットワーク デバイスにアクセスするために使用しなければならないトランク リンクへのフラッディング トラフィックが制限されるので、使用可能な帯域幅が増大します。 VTP プルーニングは、デフォルトではディセーブルに設定されています。

VTP プルーニングを有効にするには、管理ドメイン内のすべてのデバイスが VTP プルーニングを サポートする必要があります。VTP プルーニングをサポートしないデバイスについては、トランク 上で VLAN を使用できるように手動で設定する必要があります。

図 13-2 に、VTP プルーニングを使用しない場合のスイッチド ネットワークを示します。スイッチ 1 のインターフェイス 1 およびスイッチ 4 のインターフェイス 2 は、Red という VLAN に割り当て られています。スイッチ 1 に接続されたホストから、ブロードキャストが送信されます。スイッチ 1 は、このブロードキャストをフラッディングします。Red VLAN にインターフェイスを持たない スイッチ 3、5、6 も含めて、ネットワーク内のすべてのネットワーク デバイスがこのブロードキャストを受信します。

プルーニングの設定は、Catalyst 4500 シリーズ スイッチ上でグローバルに行います (「VTP プルーニングのイネーブル化」[p.13-14] を参照)。

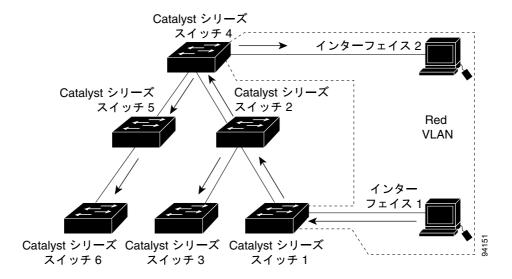


図 13-2 VTP プルーニングを使用しない場合のフラッディング トラフィック

図 13-3 は、VTP プルーニングを使用する場合の同じスイッチド ネットワークを示しています。Red VLAN へのトラフィックは指定されたリンク (スイッチ 4 のインターフェイス 4) でプルーニング されるので、スイッチ 1 からのブロードキャスト トラフィックは、スイッチ 5、6 に転送されません。

スイッチ4~ インタ インター フェイス 4 フラッディング トラフィックの プルーニング スイッチ 2 Red **VLAN** インタ スイッチ 5 フェイス 5 インタ-フェイス スイッチ6 スイッチ3 スイッチ 1

図 13-3 VTP プルーニングを使用した場合のフラッディング トラフィック

VTP サーバで VTP プルーニングをイネーブルにすると、管理ドメイン全体でプルーニングが有効になります。VTP プルーニングは、イネーブルに設定してから数秒後に有効になります。デフォルトでは、VLAN 2 ~ 1000 がプルーニング適格です。VTP プルーニング不適格の VLAN からのトラフィックは、プルーニングの対象になりません。VLAN 1 は常にプルーニング不適格です。VLAN 1 からのトラフィックをプルーニングすることはできません。

トランキング LAN インターフェイスに VTP プルーニングを設定するには、switchport trunk pruning vlan コマンドを使用します。VTP プルーニングは、LAN インターフェイスがトランキング を実行している場合に作用します。VTP ドメインで VTP プルーニングがイネーブルまたはディセーブルのどちらに設定されているか、特定の VLAN が存在するかどうか、および LAN インターフェイスが現在トランキングを実行しているかどうかにかかわらず、VLAN プルーニングを設定できます。

VTP 設定時の注意事項および制約事項

ネットワークに VTP を実装する場合、次の注意事項および制約事項に従ってください。

- VTP ドメイン内のすべてのネットワーク デバイスで、同じ VTP バージョンを実行する必要があります。
- VTP がセキュア モードの場合、管理ドメイン内の各ネットワーク デバイスにパスワードを設定する必要があります。



注意

VTP をセキュア モードで設定した場合、ドメイン内の各ネットワーク デバイスに管理ドメイン パスワードを割り当てるまで、管理ドメインは正常に動作しません。

- VTP バージョン 2 対応のネットワーク デバイス上で VTP バージョン 2 をディセーブルに設定 している場合、その VTP バージョン 2 対応ネットワーク デバイスは、同一 VTP ドメイン内で VTP バージョン 1 が稼働しているネットワーク デバイスとして動作します(VTP バージョン 2 は、デフォルトでディセーブルに設定されています)。
- 同一 VTP ドメイン内のすべてのネットワーク デバイスがバージョン 2 に対応する場合を除き、ネットワーク デバイス上で VTP バージョン 2 をイネーブルにしないでください。1 台のサーバ上で VTP バージョン 2 をイネーブルにすると、ドメイン内のすべてのバージョン 2 対応ネットワーク デバイスで VTP バージョン 2 がイネーブルになります。
- VTP サーバ上で VTP プルーニングをイネーブルまたはディセーブルにすると、管理ドメイン 全体で VTP プルーニングがイネーブルまたはディセーブルになります。
- Catalyst 4500 シリーズ スイッチ上で VLAN をプルーニング適格または不適格として設定する 場合、設定が有効なのは、そのスイッチ上の VLAN のプルーニングだけです。VTP ドメイン内 のすべてのネットワーク デバイスに対して有効となるわけではありません。

VTP のデフォルト設定

表 13-3 に、VTP のデフォルト設定を示します。

表 13-3 VTP のデフォルト設定

機能	デフォルト値
VTP ドメイン名	ヌル
VTP モード	トランスペアレント
VTP バージョン 2 のイネーブル ステート	バージョン 2 はディセーブル
VTP パスワード	なし
VTP プルーニング	ディセーブル

新たに出荷された Catalyst 4500 スーパーバイザ エンジン、Catalyst 4900 シリーズ スイッチ、および Cisco ME 4924-10GE スイッチのデフォルト VTP モードはトランスペアレントです。vlan.dat を削除 するか erase cat4000_flash: コマンドを発行して、スイッチをリセットすると、VTP モードがサーバモードに変わります。

VTP の設定

ここでは、VTP の設定手順について説明します。

- VTP グローバル パラメータの設定 (p.13-14)
- VTP サーバとしてのスイッチの設定 (p.13-15)
- VTP クライアントとしてのスイッチの設定 (p.13-16)
- VTP のディセーブル化 (VTP トランスペアレント モード)(p.13-17)
- VTP 統計情報の表示 (p.13-18)

VTP グローバル パラメータの設定

ここでは、VTP グローバル パラメータの設定について説明します。

- VTP パスワードの設定 (p.13-14)
- VTP プルーニングのイネーブル化 (p.13-14)
- VTP バージョン 2 のイネーブル化 (p.13-15)

VTP パスワードの設定

VTP パスワードを設定するには、次の作業を行います。

コマンド	目的
	VTP ドメインのパスワードを設定します。パス ワードの長さは 8 ~ 64 文字です。
	パスワードを削除するには、no キーワードを使用します。

次に、VTPパスワードを設定する例を示します。

Switch# vtp password WATER
Setting device VLAN database password to WATER.
Switch#show vtp password
VTP Password:WATER
Switch#

VTP プルーニングのイネーブル化

管理ドメイン内で VTP プルーニングをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# [no] vtp pruning	管理ドメイン内で VTP プルーニングをイネーブルにしま
		す。
		管理ドメイン内で VTP プルーニングをディセーブルにす
		るには、no キーワードを使用します。
ステップ 2	Switch# show vtp status	設定を確認します。

次に、管理ドメイン内で VTP プルーニングをイネーブルにする例を示します。

Switch# vtp pruning Pruning switched ON 次に、設定を確認する例を示します。

Switch# show vtp status | include Pruning VTP Pruning Mode : Enabled Switch#

VTP パージョン 2 のイネーブル化

VTP バージョン 2 対応のネットワーク デバイスでは、デフォルトで VTP バージョン 2 がディセーブルに設定されています。サーバ上で VTP バージョン 2 をイネーブルにすると、VTP ドメイン内のすべての VTP バージョン 2 対応ネットワーク デバイスで VTP バージョン 2 がイネーブルになります。



同一 VTP ドメイン内のネットワーク デバイス上で、VTP バージョン 1 とバージョン 2 の間の相互 運用性はありません。VTP ドメイン内のすべてのネットワーク デバイスで、同じ VTP バージョン を使用する必要があります。VTP ドメイン内のすべてのネットワーク デバイスが VTP バージョン 2 をサポートしている場合を除き、VTP バージョン 2 をイネーブルにしないでください。

VTP バージョン 2 をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# [no] vtp version {1 2}	VTP バージョン 2 をイネーブルにします。
		デフォルト値に戻すには、no キーワードを使用します。
ステップ 2	Switch# show vtp status	設定を確認します。

次に、VTP バージョン 2 をイネーブルにする例を示します。

Switch# vtp version 2 V2 mode enabled. Switch#

次に、設定を確認する例を示します。

Switch# show vtp status | include V2
VTP V2 Mode : Enabled
Switch#

VTP サーバとしてのスイッチの設定

Catalyst 4500 シリーズ スイッチを VTP サーバとして設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configuration terminal	コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# vtp mode server	VTP サーバとしてスイッチを設定します。
ステップ 3	Switch(config)# vtp domain domain_name	最大 32 文字までの VTP ドメイン名を定義します。
ステップ 4	Switch(config)# end	VLAN コンフィギュレーション モードを終了します。
ステップ 5	Switch# show vtp status	設定を確認します。

次に、スイッチを VTP サーバとして設定する例を示します。

Switch# configuration terminal
Switch(config)# vtp mode server
Setting device to VTP SERVER mode.
Switch(config)# vtp domain Lab_Network
Setting VTP domain name to Lab_Network
Switch(config)# end
Switch#

次に、設定を確認する例を示します。

Switch# show vtp status

VTP Version : running VTP1 (VTP2 capable)

Configuration Revision : 247

Maximum VLANs supported locally : 1005

Number of existing VLANs : 33

VTP Operating Mode : Server

VTP Domain Name : Lab_Network

VTP Pruning Mode : Enabled

VTP V2 Mode : Disabled

VTP Traps Generation : Disabled

MD5 digest : 0x45 0x52 0xB6 0xFD 0x63 0xC8 0x49 0x80

Configuration last modified by 0.0.0.0 at 8-12-99 15:04:49

Local updater ID is 172.20.52.34 on interface Gil/1 (first interface found)

Switch#

VTP クライアントとしてのスイッチの設定

Catalyst 4500 シリーズ スイッチを VTP クライアントとして設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configuration terminal	コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# [no] vtp mode client	VTP クライアントとしてスイッチを設定します。
		サーバ モードをイネーブルに戻すには、 no キーワードを使用します。
ステップ 3	Switch(config)# end	コンフィギュレーション モードを終了します。
ステップ 4	Switch# show vtp status	設定を確認します。

次に、スイッチを VTP クライアントとして設定する例を示します。

Switch# configuration terminal Switch(config)# vtp mode client Setting device to VTP CLIENT mode. Switch(config)# exit Switch#

次に、設定を確認する例を示します。

Switch# show vtp status

VTP Version : running VTP1 (VTP2 capable)

Configuration Revision : 247

Maximum VLANs supported locally : 1005

Number of existing VLANs : 33

VTP Operating Mode : Client

VTP Domain Name : Lab_Network

VTP Pruning Mode : Enabled

VTP V2 Mode : Disabled

VTP Traps Generation : Disabled

MD5 digest : 0x45 0x52 0xB6 0xFD 0x63 0xC8 0x49 0x80

Configuration last modified by 0.0.0.0 at 8-12-99 15:04:49

Switch#

VTP のディセーブル化 (VTP トランスペアレント モード)

Catalyst 4500 シリーズ スイッチの VTP をディセーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configuration terminal	コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# [no] vtp mode transparent	スイッチの VTP をディセーブルにします。
		サーバ モードをイネーブルにするには、no キーワードを使用します。
ステップ 3	Switch(config)# end	コンフィギュレーション モードを終了します。
ステップ 4	Switch# show vtp status	設定を確認します。

次に、スイッチの VTP をディセーブルにする例を示します。

Switch# configuration terminal Switch(config)# vtp transparent Setting device to VTP mode. Switch(config)# end Switch#

次に、設定を確認する例を示します。

Switch# show vtp status

VTP Version : 2
Configuration Revision : 247
Maximum VLANs supported locally : 1005
Number of existing VLANs : 33
VTP Operating Mode : Tran

VTP Operating Mode : Transparent
VTP Domain Name : Lab_Network
VTP Pruning Mode : Enabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled

MD5 digest : 0x45 0x52 0xB6 0xFD 0x63 0xC8 0x49 0x80

Configuration last modified by 0.0.0.0 at 8-12-99 15:04:49

Switch#

VTP 統計情報の表示

VTP に関する統計情報(送受信された VTP アドバタイズ、VTP エラーなど)を表示するには、次の作業を行います。

コマンド	目的
Switch# show vtp counters	VTP の統計情報を表示します。

次に、VTP の統計情報を表示する例を示します。

Switch# show vtp counters VTP statistics: Summary advertisements received : 7 Subset advertisements received : 5 Request advertisements received : 0 Summary advertisements transmitted : 997 Subset advertisements transmitted : 13 Request advertisements transmitted : 3 Number of config revision errors : 0 Number of V1 summary errors : 0

VTP pruning statistics:

Trunk	Join Transmitted	Join Received	Summary advts received from non-pruning-capable device
Fa5/8	43071	42766	5

VMPS

ここでは、VMPS を使用してダイナミック ポート VLAN メンバシップを設定する方法について説明します。

ここでは、次の内容について説明します。

- VMPSの概要 (p.13-19)
- VMPS クライアントの概要 (p.13-21)
- ダイナミック ポート VLAN メンバシップの設定例(p.13-27)
- VMPS データベース コンフィギュレーション ファイルの例 (p.13-31)

VMPS の概要

ここでは、VMPS サーバの機能と動作を説明します。

- VMPS サーバの概要 (p.13-19)
- VMPS サーバのセキュリティ モード (p.13-20)
- 代替 VLAN (p.13-21)
- 不正な VMPS クライアント要求 (p.13-21)

VMPS サーバの概要

VMPS は、ポートに接続されたデバイスの MAC (メディア アクセス制御) アドレスに基づいて、ポート用の VLAN を動的に選択する中央集中型サーバを提供します。ネットワーク内にあるスイッチの 1 つのポートからネットワーク内にある別のスイッチのポートにホストを移動する場合、そのスイッチはそのホストに適切な VLAN を新しいポートへ動的に割り当てます。

Cisco IOS ソフトウェアを実行する Catalyst 4500 シリーズ スイッチは、VMPS 機能をサポートしません。このスイッチは VLAN Query Protocol (VQP) クライアントとしてのみ機能し、VQP を介して VMPS と通信します。VMPS 機能については、Catalyst オペレーティング システム ソフトウェアを実行する Catalyst 4500 シリーズ スイッチ (または Catalyst 6500 シリーズ スイッチ) を使用する必要があります。

VMPS は UDP ポートを使用して、クライアントから VQP 要求を待ち受けます。したがって、VMPS がネットワーク上のローカルまたはリモート デバイスに存在するかどうかを VMPS クライアントが知る必要はありません。VMPS サーバは VMPS クライアントから有効な要求を受信すると、MAC アドレス /VLAN マッピングのエントリ データベースを検索します。

要求に対する応答では、VMPS は次のいずれかのアクションを実行します。

- 割り当てられた VLAN がポート グループに限定されている場合、VMPS はこのグループに対する要求ポートを確認し、次のように応答します。
 - VLAN がポートで許可されている場合、VMPS は VLAN 名を応答としてクライアントに送信します。
 - VLAN がポートで許可されておらず、VMPS がセキュア モードでない場合、VMPS は [access-denied] 応答を送信します。
 - VLAN がポートで許可されておらず、VMPS がセキュア モードの場合、VMPS は [port-shutdown] 応答を送信します。
- データベース内の VLAN が現在のポートの VLAN と一致せず、またポート上にアクティブ ホストがある場合、VMPS は VMPS のセキュア モード設定に応じて、[access-denied] (open)、[fallback VLAN name] (代替 VLAN 設定で open)、[port-shutdown] (secure)、または [new VLAN name] (multiple) 応答を送信します。

スイッチは [access-denied] 応答を VMPS から受信すると、MAC アドレスとポート間のトラフィックをブロックし続けます。スイッチはポート向けのパケットを監視し続け、新しいアドレスを識別すると VMPS にクエリーを送信します。スイッチが VMPS から [port-shutdown] 応答を受信すると、スイッチはポートをディセーブルにします。CLI、Cisco Visual Switch Manager (CVSM)、または SNMP を使用してポートを手動で再びイネーブルにする必要があります。

また、セキュリティ上の理由から、コンフィギュレーション テーブル内の明示的なエントリを使用して特定の MAC アドレスへのアクセスを拒否できます。VLAN 名に **none** キーワードを入力すると、VMPS は [access-denied] または [port-shutdown] 応答を送信します。

Catalyst オペレーティング システム ソフトウェアを実行する Catalyst 6500 シリーズ スイッチ VMPS の詳細については、次の URL の「Configuring Dynamic Port VLAN Membership with VMPS」の章を参照してください。

http://www.cisco.com/univered/cc/td/doc/product/lan/cat6000/sw_8_3/confg_gd/vmps.htm

VMPS サーバのセキュリティ モード

VMPS は次のモードで動作します。VMPS サーバが不正な要求に応答する方法は、VMPS が設定されているモードによって異なります。

- open モード (p.13-20)
- secure モード (p.13-20)
- multiple モード (p.13-21)

open モード

このポートに VLAN が割り当てられていない場合、VMPS がこのポートに対する MAC アドレスの要求を確認します。

- この MAC アドレスに関連付けられた VLAN がポートで許可されている場合、VLAN 名はクライアントに返されます。
- この MAC アドレスに関連付けられた VLAN がポートで許可されていない場合、ホストは [access denied] 応答を受信します。

このポートに VLAN が割り当てられている場合、VMPS がこのポートに対する MAC アドレスの要求を確認します。

- この MAC アドレスに関連付けられたデータベース内の VLAN が現在のポートの VLAN と一致 せず、代替 VLAN 名が設定されている場合、VMPS は代替 VLAN 名をクライアントに送信し ます。
- この MAC アドレスに関連付けられたデータベース内の VLAN が現在のポートの VLAN と一致せず、代替 VLAN 名が設定されていない場合、ホストは [access denied] 応答を受信します。

secure モード

このポートに VLAN が割り当てられていない場合、VMPS がこのポートに対する MAC アドレスの要求を確認します。

- この MAC アドレスに関連付けられた VLAN がポートで許可されている場合、VLAN 名はクライアントに返されます。
- この MAC アドレスに関連付けられた VLAN がポートで許可されていない場合、ポートは シャット ダウンされます。

このポートに VLAN が割り当てられている場合、VMPS がこのポートに対する MAC アドレスの要求を確認します。

• この MAC アドレスに関連付けられたデータベース内の VLAN が現在のポートの VLAN と一致 しない場合、代替 VLAN 名が設定されていてもポートはシャットダウンされます。

multiple モード

複数のホスト(MAC アドレス)がすべて同じ VLAN にある場合、これらをダイナミック ポートでアクティブにできます。ダイナミック ポートでリンクがダウンすると、ポートは割り当てられていない状態に戻ります。ポートを通じてオンラインになるホストは、ポートが VLAN に割り当てられる前に、VMPS ですべて再チェックされます。

ダイナミック ポートに接続された複数のホストが別の VLAN に属する場合、VMPS サーバに multiple モードが設定されていれば、最新の要求での MAC アドレスと一致する VLAN がクライアントに返されます。



(注)

Catalyst オペレーティング システム ソフトウェアを実行する Catalyst 4500 シリーズおよび Catalyst 6500 シリーズ スイッチは、この 3 つの操作モードで VMPS をサポートします。ただし、User Registration Tool (URT) は open モードのみをサポートします。

代替 VLAN

代替 VLAN 名を VMPS サーバで設定できます。

このポートに VLAN が割り当てられていない場合、VMPS がこのポートに対する MAC アドレスの要求を比較します。

- データベースにない MAC アドレスを持つデバイスを接続する場合、VMPS は代替 VLAN 名を クライアントに送信します。
- 代替 VLAN 名が設定されておらず、MAC アドレスがデータベースにない場合、VMPS は [access-denied] 応答を送信します。

このポートに VLAN が割り当てられている場合、VMPS がこのポートに対する MAC アドレスの要求を比較します。

• VMPS が secure モードの場合、代替 VLAN がサーバに設定されているかどうかに関係なく、 VMPS は [port-shutdown] 応答を送信します。

不正な VMPS クライアント要求

次に、不正な VMPS クライアント要求の例を示します。

- MAC アドレス マッピングが VMPS データベースに存在せず、[no fall back] VLAN が VMPS に 設定されている場合
- ポートがすでに VLAN に割り当てられ (VMPS モードは [multiple] でない) 2番めの VMPS クライアント要求が異なる MAC アドレスの VMPS で受信された場合

VMPS クライアントの概要

ここでは、VMPS クライアントとしてスイッチを設定する方法、およびそのスイッチのポートをダイナミック VLAN メンバシップに設定する方法について説明します。

ここでは、次の内容について説明します。

- ダイナミック VLAN メンバシップの概要 (p.13-22)
- デフォルトの VMPS クライアント設定 (p.13-22)
- VMPS クライアントとしてのスイッチの設定 (p.13-23)
- VMPS の管理およびモニタリング (p.13-26)
- ダイナミック ポート VLAN メンバシップのトラブルシューティング(p.13-27)

ダイナミック VLAN メンバシップの概要

ポートが [dynamic] として設定されている場合、ポート上の MAC アドレスに基づき VLAN 情報を受信します。VLAN が静的にポートに割り当てられていない場合、ポート上の MAC アドレスに基づき VMPS から動的に取得されます。

ダイナミック ポートは、1 つの VLAN にのみ属することができます。リンクがアクティブになる際、ポートが VLAN に割り当てられるまでスイッチはこのポートへトラフィックを転送しません。ダイナミック ポート上にある新規ホストの最初のパケットにある送信元 MAC アドレスは、VQP 要求の一部として VMPS に送信され、VMPS データベース内で MAC アドレスと VLAN の照合が行われます。一致する場合、VMPS はそのポート用の VLAN 番号を送信します。一致しない場合、(VMPS セキュリティ モード設定に応じて) VMPS は要求を拒否するか、またはポートをシャット ダウンします。想定される VMPS 応答の詳細については「VMPS の概要」(p.13-19)を参照してください。

複数のホスト(MAC アドレス)がすべて同じ VLAN にある場合、これらをダイナミック ポートでアクティブにできます。ダイナミック ポートでリンクがダウンすると、ポートは割り当てられていないステートに戻り、VLAN に属さなくなります。ポートを通じてオンラインになるホストは、ポートが VLAN に割り当てられる前に、VMPS ですべて再チェックされます。

この動作を行うには、クライアント デバイスが VMPS に到達可能である必要があります。VMPS クライアントは UDP パケットとして VQP 要求を送信し、中止する前に複数回試行します。再試行の間隔については、「再試行間隔の設定」(p.13-25) を参照してください。

また、VMPS クライアントは定期的に VLAN メンバシップを再確認します。再確認の回数については、「VMPS の管理およびモニタリング」(p.13-26) を参照してください。

最大 50 台のホストは常に特定のポートでサポートされます。最大数を超えると、VMPS サーバの動作モードに関係なくポートをシャットダウンします。



(注)

ポートで 50 を超えるホストがアクティブになると、VMPS はダイナミック ポートをシャットダウンします。

デフォルトの VMPS クライアント設定

表 13-4 に、クライアント スイッチのデフォルトの VMPS およびダイナミック ポート設定を示します。

表 13-4 デフォルトの VMPS クライアントおよびダイナミック ポート設定

機能	デフォルト設定
VMPS ドメイン サーバ	なし
VMPS 再確認間隔	60 分
VMPS サーバ再試行回数	3
ダイナミック ポート	設定なし

VMPS クライアントとしてのスイッチの設定

ここでは、次の内容について説明します。

- VMPS サーバの IP アドレスの設定 (p.13-23)
- VMPS クライアントでのダイナミック アクセス ポートの設定 (p.13-24)
- VLAN メンバシップの再確認 (p.13-24)
- 再確認間隔の設定 (p.13-25)
- VLAN メンバシップの再確認 (p.13-24)

VMPS サーバの IP アドレスの設定

Catalyst 4500 シリーズ スイッチを VMPS クライアントとして設定するには、VMPS として機能する スイッチの IP アドレスおよびホスト名を入力する必要があります。

Catalyst 4500 シリーズ スイッチ上でプライマリおよびセカンダリ VMPS を定義するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# vmps server { ipaddress hostname} primary	プライマリ VMPS サーバとして機能するスイッチの IP アドレス、またはホスト名を指定します。
ステップ 3	Switch(config)# vmps server { ipaddress hostname}	セカンダリ VMPS サーバとして機能するスイッチの IP アドレス、またはホスト名を指定します。
ステップ 4	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 5	Switch# show vmps	VMPS サーバ エントリを確認します。

次に、プライマリおよびセカンダリ VMPS デバイスを定義する例を示します。

```
Switch# configure terminal
```

Enter configuration commands, one per line. End with ${\tt CNTL/Z}$. Switch(config)# ${\tt wmps}$ ${\tt server}$ 172.20.128.179 ${\tt primary}$

Switch(config) # vmps server 172.20.128.178

Switch(config)# end



VMPS クライアントでこの CLI を使用して、最大 4 つの VMPS サーバを設定できます。

VMPS クライアントでのダイナミック アクセス ポートの設定

VMPS クライアント スイッチにダイナミック アクセス ポートを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	Switch(config)# interface interface	インターフェイス コンフィギュレーション モードを開始し、設定するポートを指定します。
ステップ 3	Switch(config-if)# switchport mode access	ポートをアクセス モードに設定します。
ステップ 4	Switch(config-if)# switchport access vlan dynamic	ダイナミック VLAN アクセスの対象となるように ポートを設定します。
ステップ 5	Switch(config-if)# end	特権 EXEC モードに戻ります。
ステップ 6	Switch# show interface interface switchport	入力を確認します。

次に、ダイナミック アクセス ポートを設定し、入力を確認する例を示します。

Switch# configure terminal

Enter configuration commands, one per line. End with ${\tt CNTL/Z.}$

Switch(config)# interface fa1/1

Switch(config-if) # switchport mode access

Switch(config-if)# switchport access vlan dynamic

Switch(config-if)# end

Switch# show interface fal/1 switchport

Name: Fa0/1

Switchport: Enabled

Administrative mode: dynamic auto Operational Mode: dynamic access

Administrative Trunking Encapsulation: isl Operational Trunking Encapsulation: isl Negotiation of Trunking: Disabled

Access Mode VLAN: 0 ((Inactive))
Trunking Native Mode VLAN: 1 (default)

Trunking VLANs Enabled: NONE Pruning VLANs Enabled: NONE

音声ポート

ダイナミック アクセス ポートに VVID (音声 VLAN ID) が設定されている場合、ポートはアクセス VLAN および音声 VLAN 両方に属することができます。そのため、IP Phone に接続するよう設定されたアクセス ポートでは、次のために異なる VLAN を指定できます。

- IP Phone のアクセス ポート(アクセス VLAN)を介してスイッチに接続された PC へ、PC からのデータ トラフィック
- IP Phone へ、IP Phone からの音声トラフィック (音声 VLAN)

VLAN メンバシップの再確認

スイッチが VMPS から受信したダイナミック ポート VLAN メンバシップの割り当てを確認するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# vmps reconfirm	ダイナミック ポート VLAN メンバシップを再確認します。
ステップ 2	Switch# show vmps	ダイナミック VLAN 再確認ステータスを確認します。

再確認間隔の設定

VMPS クライアントは、VMPS から受信した VLAN メンバシップ情報を定期的に再確認します。 VLAN/MAC アドレス割り当てを再確認するまで VMPS クライアントが待機する時間 (分)を設定できます。

再確認間隔を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# vmps reconfirm minutes	ダイナミック VLAN メンバシップの再確認間隔を分単位 で指定します。
ステップ 3	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 4	Switch# show vmps	ダイナミック VLAN 再確認ステータスを確認します。

次に、再確認間隔を60分に変更し、その変更を確認する例を示します。

Switch# configure terminal

Enter configuration commands, one per line. End with ${\tt CNTL/Z}$.

Switch(config) # vmps reconfirm 60

Switch(config)# end
Switch# show vmps
VQP Client Status:

VMPS VQP Version: 1

Reconfirm Interval: 60 min Server Retry Count: 10

VMPS domain server: 172.20.130.50 (primary, current)

Reconfirmation status

VMPS Action: No Host

再試行間隔の設定

次のサーバにクエリーを実行するまで VMPS クライアントが VMPS に連絡を試行する回数を設定できます。

再試行間隔を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# vmps retry count	VPQ クエリーの再試行回数を指定します。デフォルトは 3 です。 $1 \sim 10$ の数値を指定できます。
ステップ 3	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 4	Switch# show vmps	再試行回数を確認します。

次に、再試行回数を5回に変更し、その変更を確認する例を示します。

Switch# configure terminal

Enter configuration commands, one per line. End with $\mathtt{CNTL}/\mathtt{Z}\text{.}$

Switch(config)# vmps retry 5

Switch(config)# end

Switch# show vmps

VQP Client Status:

VMPS VQP Version: 1
Reconfirm Interval: 60 min

Server Retry Count: 5

VMPS domain server: 172.20.130.50 (primary, current)

Reconfirmation status

VMPS Action: No Host

VMPS の管理およびモニタリング

show vmps コマンドを使用することにより、次の VMPS 情報を表示できます。

VQP バージョン VMPS との通信に使用する VQP のバージョン。スイッチは、VQP バー

ジョン1を使用してVMPSにクエリーを実行します。

再確認間隔 VLAN/MAC アドレス割り当てを再確認するまでスイッチが待機する

時間(分)

サーバ再試行回数 VQP が VMPS ヘクエリーを再送信する回数。この回数を超えても応答

がない場合、スイッチはセカンダリ VMPS のクエリーを開始します。

VMPS ドメイン サーバ 設定された VMPS の IP アドレス。スイッチは、現在 [current] とマーク

されたものヘクエリーを送信しています。[primary] とマークされたも

のは、プライマリ サーバです。

VMPS アクション 最新の再確認試行の結果。再確認間隔が経過した場合に自動的に再確

認されるか、vmps reconfirm コマンドまたは CVSM や SNMP の同様の

コマンドを入力することで自動的に再確認できます。

次に、VMPS情報を表示する例を示します。

```
Switch# show vmps
VQP Client Status:
VMPS VQP Version: 1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server:
Reconfirmation status
______
VMPS Action:
                   other
The following example shows how to display VMPS statistics:
Switch# show vmps statistics
VMPS Client Statistics
VOP Oueries:
VQP Responses:
VMPS Changes:
                          0
VQP Shutdowns:
VQP Denied:
VQP Wrong Domain:
VQP Wrong Version:
VQP Insufficient Resource: 0
```



VMPS 統計情報の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』を参照してください。

ダイナミック ポート VLAN メンバシップのトラブルシューティング

VMPS は次の条件でダイナミック ポートを errdisable にします。

- VMPS がセキュア モードで、ホストがポートへ接続できない場合。VMPS は、ホストがネット ワークに接続しないようにポートを errdisable にします。
- 50 以上のアクティブ ホストがダイナミック ポートにある場合

errdisable ステートのインターフェイスのステータスの表示方法については、第7章「ポートのステータスと接続の確認」を参照してください。errdisable ポートを回復するには、errdisable recovery cause vmps グローバル コンフィギュレーション コマンドを使用します。

ダイナミック ポート VLAN メンバシップの設定例

図 13-4 (p.13-28)に、VMPS サーバとダイナミック ポートを持つ VMPS クライアント スイッチで構成されるネットワークを示します。この例の前提条件は、次のとおりです。

- VMPS サーバおよび VMPS クライアントは、それぞれ異なるスイッチです。
- Catalyst 4000 ファミリ スイッチ 1 (CatOS を稼働) は、プライマリ VMPS サーバです。
- Catalyst 6000 ファミリスイッチ 3(CatOS を稼働)および URT は、セカンダリ VMPS サーバです。
- エンドステーションは、次のクライアントに接続されています。
 - Catalyst 4500 シリーズ XL スイッチ 2 (Catalyst IOS を稼働)
 - Catalyst 4500 シリーズ XL スイッチ 9 (Catalyst IOS を稼働)
- データベース コンフィギュレーション ファイルは Bldg-G.db という名前で、IP アドレスが 172.20.22.7 の TFTP サーバに保存されています。

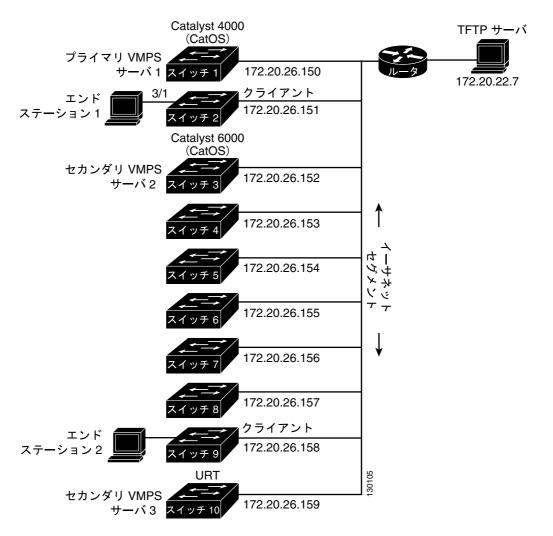


図 13-4 ダイナミック ポート VLAN メンパシップの設定

可能なトポロジは、2 種類あります。図 13-5 に、1 つのエンド ステーションに VMPS クライアント として稼働する Catalyst 4500 シリーズ スイッチが直接接続されたトポロジを示します。図 13-6 に、1 つのエンド ステーションに Catalyst 4500 シリーズ スイッチと接続する Cisco IP Phone が接続されたトポロジを示します。

図 13-5 ダイナミック ポート VLAN メンバシップの設定

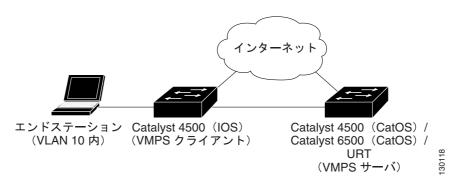
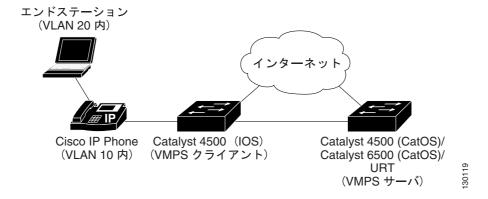


図 13-6 ダイナミック ポート VLAN メンバシップの設定



次の手順では、Catalyst 4000 および Catalyst 6000 シリーズ スイッチ (CatOS を稼働) が VMPS サーバとなります。 ネットワーク内の Catalyst 4500 シリーズ スイッチのクライアントを設定するには、この手順を実行します。

ステップ1 クライアント スイッチであるスイッチ2の VMPS サーバアドレスを設定します。

- a. 特権 EXEC モードから、グローバル コンフィギュレーション モードを開始します。 switch# configuration terminal
- b. プライマリ VMPS サーバの IP アドレスを入力します。
 switch(config)# vmps server 172.20.26.150 primary
- c. セカンダリ VMPS サーバの IP アドレスを入力します。 switch(config)# vmps server 172.20.26.152
- **d.** VMPS IP アドレスの設定を確認するには、特権 EXEC モードに戻ります。 switch#(config) **exit**
- e. スイッチに設定された VMPS 情報を表示します。

```
switch# show vmps
VQP Client Status:
------
VMPS VQP Version: 1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server: 172.20.26.152
172.20.26.150 (primary, current
```

ステップ2 スイッチ2のポート Fa0/1 をダイナミック ポートとして設定します。

- a. グローバル コンフィギュレーション モードに戻ります。
 switch# configure terminal
- b. インターフェイス コンフィギュレーション モードを開始します。switch(config)# interface fa2/1

c. スタティック アクセス ポートの VLAN メンバシップ モードを設定します。

switch(config-if)# switchport mode access

d. ポートのダイナミック VLAN メンバシップを割り当てます。

switch(config-if)# switchport access vlan dynamic

e. 特権 EXEC モードに戻ります。

switch(config-if)# exit
switch#

- ステップ3 ポート Fa2/1 のエンド ステーション 2 を接続します。エンド ステーション 2 がパケットを送信すると、スイッチ 2 がプライマリ VMPS サーバであるスイッチ 1 にクエリーを送ります。スイッチ 1 は、ポート Fa2/1 の VLAN ID で応答します。スパニングツリー PortFast モードが Fa2/1 上でイネーブルの場合、ポート Fa2/1 はただちに接続されて転送を開始します。
- ステップ 4 VMPS 再確認間隔を 60 分に設定します。再確認間隔とは、VLAN/MAC アドレス割り当てを再確認 するまでスイッチが待機する時間 (分)です。

switch# config terminal
switch(config)# vmps reconfirm 60

ステップ5 特権 EXEC モードでエントリを確認します。

switch# show vmps

VQP Client Status:

VMPS VQP Version: 1
Reconfirm Interval: 60 min
Server Retry Count: 3

VMPS domain server:

Reconfirmation status

VMPS Action: No Dynamic Port

ステップ 6 ステップ 1 およびステップ 2 を繰り返して、VMPS サーバ アドレスを設定し、各 VMPS クライアント スイッチのダイナミック ポートを割り当てます。

VMPS データペース コンフィギュレーション ファイルの例

次に、VMPS サーバに表示される VMPS データベース コンフィギュレーション ファイルの例を示します。VMPS データベース コンフィギュレーション ファイルは ASCII テキスト ファイルで、VMPS サーバとして機能するスイッチにアクセス可能な TFTP サーバに保存されます。

```
!vmps domain <domain-name>
! The VMPS domain must be defined.
!vmps mode { open | secure }
! The default mode is open.
!vmps fallback <vlan-name>
!vmps no-domain-req { allow | deny }
! The default value is allow.
vmps domain WBU
vmps mode open
vmps fallback default
vmps no-domain-req deny
!MAC Addresses
!
vmps-mac-addrs
! address <addr> vlan-name <vlan name>
address 0012.2233.4455 vlan-name hardware
address 0000.6509.a080 vlan-name hardware
address aabb.ccdd.eeff vlan-name Green
address 1223.5678.9abc vlan-name ExecStaff
address fedc.ba98.7654 vlan-name --NONE--
address fedc.ba23.1245 vlan-name Purple
!Port Groups
!vmps-port-group <group-name>
! device <device-id> { port <port-name> | all-ports }
vmps-port-group WiringCloset1
device 198.92.30.32 port Fa1/3
device 172.20.26.141 port Fa1/4
vmps-port-group "Executive Row
device 198.4.254.222 port es5%Fa0/1
device 198.4.254.222 port es5%Fa0/2
device 198.4.254.223 all-ports
!VLAN groups
!vmps-vlan-group <group-name>
! vlan-name <vlan-name>
vmps-vlan-group Engineering
vlan-name hardware
vlan-name software
!VLAN port Policies
!vmps-port-policies {vlan-name <vlan_name> | vlan-group <group-name> }
! { port-group <group-name> | device <device-id> port <port-name> }
vmps-port-policies vlan-group Engineering
port-group WiringCloset1
vmps-port-policies vlan-name Green
device 198.92.30.32 port Fa0/9
vmps-port-policies vlan-name Purple
device 198.4.254.22 port Fa0/10
port-group "Executive Row"
```



CHAPTER

14

IP アンナンバード インターフェイス の設定



IP UnControl Plane Policing (アンコントロール プレーン ポリシング)は Supervisor Engine 6-E ではサポートされていません。

この章では、IP アンナンバード インターフェイス機能について説明します。この機能を使用すると、明示的に IP アドレスを割り当てないで、インターフェイス上で IP 処理を行うことが可能になります。

この章の内容は、次のとおりです。

- IP アンナンバード サポートの概要 (p.14-2)
- DHCP サーバにおける IP アンナンバード インターフェイス サポートの設定 (p.14-4)
- 接続ホストのポーリングを行う IP アンナンバード インターフェイス サポートの設定 (p.14-6)
- IP アンナンバード インターフェイス設定の表示 (p.14-8)
- IP アンナンバードのトラブルシューティング (p.14-9)



<u>一</u> (注)

この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/cr/index.htm

関連資料

関連トピック	資料のタイトル
DHCP およびその他の IP アドレッシングの設定作業	© Cisco IOS IP Addressing Services Configuration Guide Release 12.4
	の「IP Addressing and Services」
DHCP およびその他の IP アドレッシングのコマンド	© Cisco IOS IP Addressing Services Command Reference a Release 12.4 T
VLAN の設定作業	© Cisco IOS LAN Switching Configuration Guide Release 12.4 D
	「Virtual LANs」の章
VLAN コンフィギュレーション コマンド	© Cisco IOS LAN Switching Command Reference Release 12.4 T

IP アンナンバード サポートの概要

IP アンナンバード インターフェイスを使用した VLAN および LAN インターフェイスを設定する前に、次の概念を理解する必要があります。

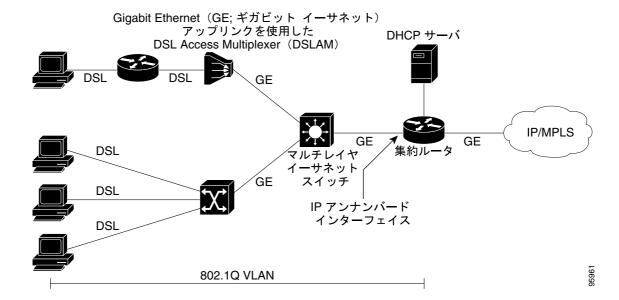
- DHCP サーバとリレー エージェントでの IP アンナンバード インターフェイス サポート (p.14-2)
- 接続ホストのポーリングを行う IP アンナンバード (p.14-3)

DHCP サーバとリレー エージェントでの IP アンナンバード インターフェイス サポート

IP アンナンバード インターフェイスの構成では、明示的に IP アドレスを割り当てないで、インターフェイス上で IP 処理を行うことが可能になります。IP アンナンバード インターフェイスは、Catalyst 4500 シリーズ スイッチにすでに設定されている別のインターフェイスから IP アドレスを「借りる」ことができるので、ネットワークとアドレス スペースを節約できます。DHCP サーバ/リレー エージェントでこの機能を使用すると、DHCP サーバによって割り当てられたホスト アドレスを DHCP リレー エージェントで動的に学習できます。

図 14-1 に、IP アンナンバード インターフェイス機能を実装するネットワーク トポロジ例を示します。このトポロジでは、DHCP サーバが IP アドレスをホストに割り当てるときに、集約スイッチが IP ルートを動的に確立します。

図 14-1 VLAN 上で IP アンナンバード インターフェイス機能を使用するネットワーク トポロジ例



DHCP オプション 82

DHCP は、TCP/IP ネットワーク上のホストに設定情報を渡すフレームワークを提供します。設定パラメータと他の制御情報は、DHCP メッセージのオプション フィールドに保存されているタグ付き データ項目で伝送されます。データ項目は、オプションとも呼ばれます。オプション 82 は、リレーエージェントが認識する情報を含んだ単一の DHCP オプションとして構成されています。

IP アンナンバード インターフェイス機能は、エージェント リモート ID と呼ばれる DHCP リレーエージェント情報オプションのサブオプションを使用して、DHCP サーバに情報を伝えます。エージェント リモート ID で送信された情報には、リレー エージェントを特定する IP アドレス、インターフェイスに関する情報、および DHCP 要求を入力した接続に関する情報が含まれます。DHCPサーバはこの情報を使用して、IP アドレスの割り当てとセキュリティ ポリシーの決定を行うことができます。

図 14-2 に、IP アンナンバード インターフェイス機能で使用されるエージェント リモート ID サブオプションの形式を示します。

図 14-2 エージェント リモート ID サブオプションの形式

12 バイト

タイプ (バイト 1)	長さ (バイト2)	予約済 (バイト 3 ~ 4)	NAS IP アドレス (バイト 5 ~ 8)	インター フェイス (バイト 9)	予約済 (バイト 10)	VLAN ID (バイト 11 ~ 12)	103088
----------------	--------------	--------------------	----------------------------	-------------------------	-----------------	-----------------------------	--------

表 14-1 で、図 14-2 に示されたエージェント リモート ID サブオプション フィールドについて説明 します。

表 14-1 エージェント リモート ID サブオプション フィールドの説明

フィールド	説明
タイプ	形式タイプ。値2はこの機能で使用する形式を指定します(1バイト)。
長さ	エージェント リモート ID サブオプションの長さ。タイプ フィールドと長さフィールドは含まれません (1 バイト)。
予約	予約済み(2バイト)
NAS IP アドレス	ip unnumbered コマンドで指定したインターフェイスの IP アドレス(4 バイト)
インターフェイス	物理インターフェイス。このフィールドの形式は、次のとおりです。 スロット(4 ビット) モジュール(1 ビット) ポート(3 ビット)
	たとえば、インターフェイス名がインターフェイス Ethernet 2/1/1 の場合、スロットは 2、モジュールは 1、およびポートは 1 です(1 バイト)。
予約	予約済み(1バイト)
VLAN ID	イーサネット インターフェイスの VLAN ID (2 バイト)

接続ホストのポーリングを行う IP アンナンバード



この機能オプションは、LAN および VLAN インターフェイスにのみ適用できます。

場合によっては、ホスト IP アドレスが静的に割り当てられていることがあります。IP アンナンバード インターフェイス機能は、動的にスタティック ホスト IP アドレスを学習できます。

DHCP サーバにおける IP アンナンバード インターフェイス サポートの 設定



DHCP が設定されており、動作可能な状態である必要があります。

ここでは、次の手順について説明します。

- LAN および VLAN インターフェイスに対する IP アンナンバード インターフェイス サポート の設定 (p.14-4)
- イーサネット VLAN 範囲に対する IP アンナンバード インターフェイス サポートの設定 (p.14-5)

LAN および VLAN インターフェイスに対する IP アンナンバード インターフェイス サポートの設定

単一 LAN または VLAN インターフェイスに IP アンナンバード インターフェイス サポートを設定するには、次の作業を行います。

手順の要約

- 1. enable
- 2. configure terminal
- 3. interface [fastethernet | gigabitethernet | tengigabitethernet | vlan vlan} port-channel | loopback]
- **4. ip unnumbered** *type number*

手順の詳細

	コマンド	目的
ステップ 1	Switch# enable	特権 EXEC モードをイネーブルにします。
		プロンプトが表示されたら、パスワードを入力します。
ステップ 2	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	Switch(config)# interface [fastethernet gigabitethernet tengigabitethernet vlan vlan port-channel loopback]	インターフェイス コンフィギュレーション モードを開始 し、トンネル ポートとして設定するインターフェイスを入 力します。
ステップ 4	Switch(config-if)# ip unnumbered type number	明示的な IP アドレスをインターフェイスに割り当てずに インターフェイス上の IP 処理をイネーブルにします。
		type および number 引数は、IP アドレスが割り当てられているスイッチ上の別のインターフェイスを指定します。指定したインターフェイスを別のアンナンバード インターフェイスに設定することはできません。
ステップ 5	Switch(config-if)# exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 7	Switch# show running-config	IP アンナンバード サポートが正しく設定されていること を確認します。

次に、イーサネット VLAN 10 が IP アンナンバード インターフェイスとして設定されている例を示します。

Switch> enable

Switch# configure terminal

Enter configuration commands, one per line. End with $\mathtt{CNTL}/\mathtt{Z}\text{.}$

Switch(config) # interface vlan 10

Switch(config-if)# ip unnumbered Lookback 0

イーサネット VLAN 範囲に対する IP アンナンバード インターフェイス サポートの設定

特定の範囲のイーサネット VLAN インターフェイスに IP アンナンバード インターフェイス サポートを設定するには、次の作業を行います。

手順の要約

- 1. enable
- 2. configure terminal
- **3.** interface range {{fastethernet | gigabitethernet | vlan vlan} slot/interface {fastethernet | gigabitethernet | vlan vlan} slot/interface macro macro-name}
- **4. ip unnumbered** *type number*

手順の詳細

	コマンドまたはアクション	目的	
ステップ 1	Switch# enable	特権 EXEC モードをイネーブルにします。	
		プロンプトが表示されたら、パスワードを入力します。	
ステップ 2	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。	
ステップ 3	Switch(config)# interface range {{fastethernet gigabitethernet vlan	複数のインターフェイスで同時にコマンドを実行します。	
	vlan} slot/interface {fastethernet	範囲情報を分けるために、両側にスペースを付けた形でハ	
	<pre>gigabitethernet vlan vlan} slot/interface macro macro-name}</pre>	イフンを入力する必要があります。	
ステップ 4	Switch(config-if)# ip unnumbered type number	明示的な IP アドレスをインターフェイスに割り当てずに インターフェイス上の IP 処理をイネーブルにします。	
		type および number 引数は、IP アドレスが割り当てられているスイッチ上の別のインターフェイスを指定します。 指定したインターフェイスを別のアンナンバード インターフェイスに設定することはできません。	
ステップ 5	Switch(config-if)# exit	グローバル コンフィギュレーション モードに戻ります。	
ステップ 6	Switch(config)# end	特権 EXEC モードに戻ります。	
ステップ 7	Switch# show running-config	IP アンナンバード サポートが正しく設定されていること を確認します。	

次に、 $1 \sim 10$ の範囲の VLAN を IP アンナンバード インターフェイスとして設定する例を示します。 FastEthernet 3/1 の IP アドレスを共有しています。

Switch> enable

Switch# configure terminal

Enter configuration commands, one per line. End with $\mathtt{CNTL}/\mathtt{Z}.$

 ${\tt Switch(config)\#\ interface\ range\ vlan\ 1\ -\ 10}$

 ${\tt Switch(config-if)\#\ ip\ unnumbered\ fastethernet\ 3/1}$

Switch(config-if)# exit

Switch(config)# end

接続ホストのポーリングを行う IP アンナンバード インターフェイス サポートの設定

接続ホストのポーリングを使用する IP アンナンバード インターフェイス サポートを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# enable	特権 EXEC モードをイネーブルにします。
		プロンプトが表示されたら、パスワードを入力しま
		す。
ステップ 2	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 3	Switch(config)# interface vlan vlan-id	インターフェイス コンフィギュレーション モード を開始し、トンネル ポートとして設定するインター フェイスを入力します。
ステップ 4	<pre>Switch(config-if)# ip unnumbered type number pol1</pre>	明示的な IP アドレスをインターフェイスに割り当 てずに、インターフェイス上の IP 処理および、接続 ホストのポーリングをイネーブルにします。
		type および number は、IP アドレスが割り当てられているスイッチ上の別のインターフェイスを指定します。指定したインターフェイスを別のアンナンバード インターフェイスに設定することはできません。
		type 引数には、loopback、fastethernet、gigabitethernet、svi、および portchannel の値を設定できます。
ステップ 5	Switch(config-if)# exit	グローバル コンフィギュレーション モードに戻り ます。
ステップ 6	Switch(config)# ip arp poll queue <10-10000>	ホスト アドレスのグローバル バックログ キューが 検出されるように設定します。 キュー サイズのデフォルトは 1000 です。
ステップ 7	Switch(config)# ip arp poll rate <10-10000>	アンナンバード インターフェイスで送信される Address Resolution Protocol(ARP; アドレス 解決 プロトコル) 要求の最大数を設定します。 ARP 要求のデフォルト数は、1000 pps です。
ステップ 8	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 9	Switch# show running-config	IP アンナンバード サポートが正しく設定されていることを確認します。

次に、インターフェイス FastEthernet 6/2 での IP 処理および接続ホストのポーリングをイネーブルにする例を示します。また、グローバル バックログ キューを 2000 に設定し、ARP 要求の最大数を 500 に設定する例も示します。

Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config) # interface fastEthernet 6/2

Switch(config-if) # no switchport

Switch(config-if)# ip unnumbered loopback 0 poll

Warning: dynamic routing protocols will not work on non-point-to-point interfaces with IP unnumbered configured.

Switch(config-if)# exit

Switch(config)# ip arp poll queue 2000

Switch(config) # ip arp poll rate 500

Switch(config)# end

IP アンナンバード インターフェイス設定の表示

show ip interface [type number] unnumbered [detail] コマンドを使用して、接続ホストのポーリングを行うアンナンバード インターフェイスのステータスを表示します。

アンナンバード インターフェイスのステータスを表示するには、次の作業を1つまたは複数行います。

コマンド	目的
	Catalyst 4500 シリーズ スイッチ上の接続ホストのポーリングを行うアンナンバード インターフェイスのステータスを表示します。

次に、接続ホストのポーリングを行うアンナンバード インターフェイスのステータスを表示する例を示します。

```
Switch# show ip interface loopback 0 unnumbered detail

Number of unnumbered interfaces with polling: 1

Number of IP addresses processed for polling: 2

10.1.1.7

10.1.1.8

Number of IP addresses in queue for polling: 2(high water mark: 3)

10.1.1.17

10.1.1.18
```

スイッチ上の、接続ホストのポーリングを行うアンナンバード インターフェイス バックログの主要な統計情報を表示するには、show ip arp poll コマンドを使用します。

コマンド	目的
Switch# show ip arp poll [detail]	スイッチ上の、接続ホストのポーリングを行うアンナンバード インターフェイス バックログの主要な統計情報を表示します。

次に、接続ホストのポーリングを行うアンナンバード インターフェイスのバックログの主要な統計情報を表示する例を示します。

```
Switch# show ip arp poll

Number of IP addresses processed for polling: 439

Number of IP addresses in queue for polling: 3 (high water mark: 0, max: 1000)

Number of requests dropped:

Queue was full: 0

Request was throttled by incomplete ARP: 0

Duplicate request was found in queue: 0
```

アンナンバード インターフェイス バックログの主要な統計情報をクリアするには、次のように clear ip arp poll statistic コマンドを使用します。

```
Switch# clear ip arp poll statistic
Switch# show ip arp poll
Number of IP addresses processed for polling: 0
Number of IP addresses in queue for polling: 0 (high water mark: 0, max: 1000)
Number of requests dropped:
Queue was full: 0
Request was throttled by incomplete ARP: 0
Duplicate request was found in queue: 0
```

IP アンナンバードのトラブルシューティング

接続ホストのポーリングをデバッグする方法については、Cisco.com で **debug arp** コマンドの IOS マニュアルを参照してください。

プレフィクスが OSPF ネットワークにアドバタイズされているループバック インターフェイスの IP アドレスを IP アンナンバード インターフェイスが共有する場合、ループバック インターフェイスをポイントツーポイント インターフェイスに変更する必要があります。そうしないと、ループバック インターフェイスのホスト ルートだけが OSPF ネイバーにアドバタイズされます。

Switch(config)# int loopback 0
Switch(config-if)# ip address
Switch(config-if)# ip address 10.1.0.1 255.255.0.0
Switch(config-if)# ip ospf network point-to-point
Switch(config-if)# end

■ IP アンナンパードのトラブルシューティング



CHAPTER

15

レイヤ 2 イーサネット インターフェイ スの設定

この章では、CLI (コマンドラインインターフェイス)を使用して、Catalyst 4500 シリーズスイッチ上でレイヤ 2 スイッチング用のファスト イーサネットとギガビット イーサネットを設定する手順について説明します。設定上の注意事項、設定手順、および設定例についても示します。この章の設定は、スーパーバイザ エンジンのアップリンク ポートを含むすべてのモジュールのファストイーサネットおよびギガビットイーサネットインターフェイスに適用されます。

この章の主な内容は、次のとおりです。

- レイヤ2イーサネットスイッチングの概要(p.15-2)
- レイヤ2 イーサネット インターフェイスのデフォルト設定 (p.15-6)
- レイヤ 2 インターフェイス設定時の注意事項および制約事項 (p.15-6)
- レイヤ2スイッチング用のイーサネットインターフェイスの設定(p.15-7)



レイヤ 3 インターフェイスの設定手順については、第 27 章「レイヤ 3 インターフェイスの設定」を参照してください。



(注)

この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/cr/index.htm

レイヤ2 イーサネット スイッチングの概要

ここでは、Catalyst 4500 シリーズ スイッチでのレイヤ 2 イーサネット スイッチングの機能について 説明します。

- レイヤ2イーサネットスイッチングの概要(p.15-2)
- VLAN トランクの概要 (p.15-3)
- レイヤ2インターフェイスモード(p.15-4)

レイヤ2 イーサネット スイッチングの概要

Catalyst 4500 シリーズ スイッチでは、レイヤ 2 イーサネット セグメント間のパラレル接続を複数同時に確立できます。 イーサネット セグメント間のスイッチド接続は、パケットの有効期間のみ存続します。 以降のパケットには、別のセグメント間に新しい接続が確立されます。



(注)

Cisco IOS Release 12.1(13)EW の場合、Catalyst 4500 シリーズ スイッチは 1600 バイトのパケットを処理できます。「オーバーサイズ」として処理して廃棄することはありません。このサイズは、一般的な IEEE (米国電気電子学会) イーサネット最大伝送ユニット (Maximum Transmission Unit; MTU)(1518 バイト) および 802.1Q MTU (1522 バイト) よりも大きな値です。大容量パケットを処理するには、ネットワーク上で 2 つのネスト化した 802.1Q ヘッダーと Multiprotocol Label Switching (MPLS; マルチプロトコル ラベル スイッチング) のサポートが必要です。

Catalyst 4500 シリーズは、高帯域のデバイスおよび多数のユーザに起因する輻輳問題を解決するために、デバイス(サーバなど)ごとに専用の 10 Mbps、100 Mbps、または 1000 Mbps セグメントを割り当てます。スイッチの各イーサネット インターフェイスは、それぞれ別のイーサネット セグメントに接続されているので、スイッチング環境が適切に設定されていれば、サーバは全帯域幅にアクセスできます。

衝突はイーサネット ネットワークにおける大きな障害になりますが、有効な解決策の1つは全二重通信です。イーサネットは通常、半二重モードで動作します。つまり、各ステーションは送信または受信のどちらか一方しか実行できません。全二重モードでは、2つのステーション間で同時に送受信を行うことができます。パケットを同時に双方向に流すことができる場合、有効イーサネット帯域幅は2倍になり、10 Mbps インターフェイスで 20 Mbps、ファスト イーサネット インターフェイスで 200 Mbps になります。Catalyst 4500 シリーズ スイッチのギガビット イーサネット インターフェイスは全二重モード専用で、2 Gbps の有効帯域幅を提供します。

セグメント間のフレーム スイッチング

Catalyst 4500 シリーズ スイッチ上の各イーサネット インターフェイスは、1 台のワークステーションまたはサーバに接続することも、ハブに接続し、ハブを経由して複数のワークステーションまたはサーバをネットワークに接続することもできます。

標準的なイーサネットハブでは、すべてのポートがハブ内の共通のバックプレーンに接続され、ハブに接続されたすべてのデバイスが、ネットワークの帯域幅を共用します。2 つのデバイス間で、帯域幅を大量に使用するセッションを確立した場合には、そのハブに接続された他のすべてのステーションで、ネットワーク パフォーマンスが低下します。

パフォーマンスの低下を抑えるために、スイッチは各インターフェイスを個々のセグメントとして 処理します。異なるインターフェイス上のステーションが相互に通信する必要がある場合、スイッチは一方のインターフェイスから他方のインターフェイスにワイヤ速度でフレームを転送して、各 セッションが全帯域幅を利用できるようにします。

インターフェイス間でフレームのスイッチングを効率的に行うため、スイッチはアドレス テーブルを維持します。フレームがスイッチに着信すると、ルータは送信元ステーションの MAC (メディア アクセス制御) アドレスと、フレームを受信したインターフェイスを対応付けます。

MAC アドレス テーブルの作成

Catalyst 4500 シリーズは、受信したフレームの送信元アドレスを使用して、MAC アドレス テーブルを作成します。MAC アドレス テーブルに登録されていない宛先アドレスを持つフレームをスイッチが受信すると、そのフレームを受信したインターフェイスを除き、同一 VLAN (仮想 LAN)のすべてのインターフェイスにフレームをフラッディングします。宛先デバイスから応答があると、スイッチは該当する送信元アドレスおよびインターフェイス ID をアドレス テーブルに追加します。スイッチは以降のフレームについて、すべてのインターフェイスにフラッディングすることなく1つのインターフェイスに転送します。

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

VLAN トランクの概要

トランクは 1 つまたは複数のイーサネット スイッチ インターフェイスと、ルータまたはスイッチ など別のネットワーキング デバイス間のポイントツーポイント リンクです。トランクは 1 つのリンクを介して複数の VLAN トラフィックを伝送するので、VLAN をネットワーク全体に拡張できます。

次の 2 種類のトランク カプセル化方式が、すべてのイーサネット インターフェイスで使用可能です。

ISL(スイッチ間リンク)プロトコル ISLは、シスコ独自のトランクカプセル化方式です。



(注) Supervisor Engine 6-E は、ISL トランキングをサポートして*いません*。そのため、**switchport trunk encapsulute** コマンドはサポートされていません。



(注) WS-X4418-GB および WS-X4412-2GB-T モジュール上のブロッキング ギガビット ポートは、ISL をサポートしていません。WS-X4418-GB モジュールでは、ポート $3 \sim 18$ がブロッキング ギガビット ポートです。WS-X4412-2GB-T モジュールでは、ポート $1 \sim 12$ がブロッキング ギガビット ポートです。

802.1Q 802.1Q は、業界標準のトランク カプセル化方式です。

トランクは、1 つのイーサネット インターフェイスまたは EtherChannel バンドルに対して設定できます。 EtherChannel の詳細については、第 20 章「EtherChannel の設定」を参照してください。

イーサネット トランク インターフェイスは、複数のトランキング モードをサポートしています(表 15-2 を参照)。 さらに、トランクでの ISL または 802.1Q カプセル化の使用、またはカプセル化タイプの自動ネゴシエーションを指定することもできます。

トランキングの自動ネゴシエーションを実行する場合は、インターフェイスが同一 VLAN Trunking Protocol (VTP; VLAN トランキング プロトコル)ドメインにあることを確認してください。異なるドメイン内のインターフェイスを強制的にトランキングするには、trunk キーワードまたは nonegotiate キーワードを使用します。VTP ドメインの詳細については、VTP を参照してください。

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

カプセル化タイプ

表 15-1 に、イーサネット トランクのカプセル化タイプを示します。

表 15-1 イーサネット トランクのカプセル化タイプ

カプセル化タイプ	カプセル化コマンド	目的
ISL	switchport trunk encapsulation isl	トランク リンクに ISL カプセル化を指定します。
802.1Q	switchport trunk encapsulation dot1q	トランク リンクに 802.1Q カプセル化を指定します。
ネゴシエーション	switchport trunk encapsulation negotiate	インターフェイスが近接インターフェイスとネゴシエーションを行い、近接インターフェイスの設定および機能に応じて、ISL トランク(優先)または802.1Q トランクになるよう指定します。

リンクが ISL トランクまたは 802.1Q トランクのどちらになるかは、接続された 2 つのインターフェイスのトランキング モード、トランク カプセル化タイプ、およびハードウェア機能によって決まります。

レイヤ 2 インターフェイス モード

表 15-2 に、レイヤ 2 インターフェイス モードを示し、イーサネット インターフェイスにおける各 モードの機能について説明します。

表 15-2 レイヤ 2 インターフェイス モード

モード	目的
switchport mode access	インターフェイスは永続的な非トランキング モードになり、リンクを非トランキング リンクに変換するためにネゴシエーションを行います。インターフェイスは、近接インターフェイスが変更されない場合でも、非トランク インターフェイスになります。
switchport mode dynamic desirable	リンクからトランキング リンクへの変換をインターフェイスに アクティブに試行させます。近接インターフェイスが trunk、 desirable、または auto モードに設定されていれば、インターフェ イスはトランク インターフェイスになります。
switchport mode dynamic auto	近接インターフェイスが trunk モードまたは desirable モードに設定されている場合、インターフェイスのリンクをトランキング リンクに変換します。このモードは、すべてのイーサネット インターフェイスのデフォルト モードです。

表 15-2 レイヤ 2 インターフェイス モード (続き)

モード	目的
switchport mode trunk	インターフェイスは永続的なトランキング モードになり、リンク
	をトランキング リンクに変換するためにネゴシエーションを行
	います。インターフェイスは、近接インターフェイスが変更され
	ない場合でも、トランク インターフェイスになります。
switchport nonegotiate	インターフェイスを永続的なトランキング モードにしますが、イ
	ンターフェイスが DTP フレームを生成しないようにします。トラ
	ンキング リンクを確立するには、近接するインターフェイスを手
	動でトランク インターフェイスとして設定する必要があります。



DTP は PPP (ポイントツーポイント プロトコル)です。ただし、インターネットワーキング デバイスによっては、DTP フレームが正しく転送されないことがあります。この問題を避けるために、これらのリンク上でトランキングを行わない場合は、DTP をサポートしないデバイスに接続されているインターフェイスが、access キーワードを使用して設定されていることを確認してください。DTP をサポートしないデバイスへのトランキングをイネーブルにするには、nonegotiate キーワードを使用して、インターフェイスをトランクにし、DTP フレームが生成されないようにします。

レイヤ 2 イーサネット インターフェイスのデフォルト設定

表 15-3 に、レイヤ 2 イーサネット インターフェイスのデフォルト設定を示します。

表 15-3 レイヤ 2 イーサネット インターフェイスのデフォルト設定

機能	デフォルト値
インターフェイス モード	switchport mode dynamic auto
トランク カプセル化	switchport trunk encapsulation negotiate
VLAN 許容範囲	VLAN 1 ~ 1005
プルーニングに適格な VLAN 範 囲	VLAN 2 ~ 1001
デフォルト VLAN (アクセスポート用)	VLAN 1
ネイティブ VLAN (802.1Q 専用 トランク用)	VLAN 1
STP ¹ STP	すべての VLAN でイネーブル
STP ポート プライオリティ	128
STP ポート コスト	• 10 Mbps イーサネット LAN ポートでは 100
	• 10/100 Mbps ファスト イーサネット ポートでは 19
	• 100 Mbps ファスト イーサネット ポートでは 19
	• 1000 Mbps ギガビット イーサネット ポートでは 4
	• 10,000 Mbps 10 ギガビット イーサネット LAN ポートでは 2

^{1.} STP = Spanning-Tree Protocol (スパニングツリー プロトコル)

レイヤ2インターフェイス設定時の注意事項および制約事項

レイヤ2インターフェイスを設定する場合は、次の注意事項および制約事項に留意してください。

• 802.1Q トランクを使用して接続しているシスコ製スイッチのネットワークでは、トランク上で 許容される VLAN ごとに 1 つのスパニングツリー インスタンスが維持されます。他社製の 802.1Q スイッチが維持するのは、トランク上で許容されるすべての VLAN に対してスパニン グツリー インスタンス 1 つのみです。

802.1Q トランクを使用してシスコ製スイッチを他社製のデバイスに接続する場合、シスコ製スイッチは、トランクのネイティブ VLAN のスパニングツリー インスタンスを、他社製の 802.1Q スイッチのスパニングツリー インスタンスと結合します。 ただし、各 VLAN のスパニングツリー情報は、他社製の 802.1Q スイッチのクラウドと切り離され、シスコ製スイッチで維持されます。シスコ製スイッチを切り離している他社製の 802.1Q のクラウドは、スイッチ間の単ートランク リンクとして扱われます。

- 802.1Q トランクのネイティブ VLAN が、トランク リンクの両端で同一であることを確認してください。トランクの一端の VLAN と反対側の VLAN が異なると、スパニングツリー ループの原因になります。
- 802.1Q トランクのいずれかの VLAN でスパニングツリーをディセーブルにしても、スパニングツリー ループが発生する場合があります。

レイヤ 2 スイッチング用のイーサネット インターフェイスの設定

ここでは、Catalyst 4500 シリーズ スイッチにおけるレイヤ 2 スイッチングの設定手順について説明 します。

- レイヤ 2 トランクとしてのイーサネット インターフェイスの設定 (p.15-7)
- レイヤ2アクセスポートとしてのインターフェイスの設定(p.15-10)
- レイヤ2設定のクリア(p.15-11)

レイヤ 2 トランクとしてのイーサネット インターフェイスの設定



レイヤ 2 インターフェイスのデフォルトは、switchport mode dynamic auto です。 近接インターフェ イスがトランキングをサポートし、trunk モードまたは dynamic desirable モードに設定されている場 合、リンクはレイヤ2トランクになります。デフォルトでは、トランクはカプセル化方式をネゴシ エーションします。近接インターフェイスがそれぞれ ISL と 802.1Q のカプセル化方式をサポート し、いずれのインターフェイスもカプセル化タイプのネゴシエーションに設定されている場合、ト ランクは ISL カプセル化方式を使用します。



Supervisor Engine 6-E は、ISL トランキングをサポートしていません。

インターフェイスをレイヤ2トランクとして設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# interface {fastethernet gigabitethernet tengigabitethernet} slot/port	設定するインターフェイスを指定します。
ステップ 2	Switch(config-if)# shutdown	(任意)設定が完了するまでトラフィックを流さない ようにするため、インターフェイスをシャットダウ ンします。
ステップ 3	Switch(config-if)# switchport trunk encapsulation {isl dot1q negotiate}	(任意)カプセル化方式を指定します。
		(注) このコマンドと一緒に isl または dot1q キーワードを指定して、デフォルト モード (negotiate) ではサポートされない switchport mode trunk コマンドをサポートするようにします。
		(注) Supervisor Engine 6-E は、ISL トランキングを サポートして <i>いません</i> 。
ステップ 4	Switch(config-if)# switchport mode {dynamic {auto desirable} trunk}	インターフェイスをレイヤ 2 トランクとして設定します(インターフェイスがレイヤ 2 アクセス ポートの場合、またはトランキング モードを指定する場合のみ)。

	コマンド	目的
ステップ 5	Switch(config-if)# switchport access vlan vlan_num	(任意)インターフェイスがトランキングを停止した 場合に使用するアクセス VLAN を指定します。アク セス VLAN がネイティブ VLAN として使用される ことはありません。
		(注) vlan_num パラメータは、1 ~ 1005 の単一の VLAN 番号または 2 つの VLAN 番号(小さい方が先、ダッシュで区切る)で指定する VLAN 範囲です。カンマで区切った vlan パラメータの間、またはダッシュで指定した範囲の間には、スペースを入れないでください。
ステップ 6	Switch(config-if)# switchport trunk native vlan vlan_num	802.1Q トランクの場合、ネイティブ VLAN を指定します。 (注) ネイティブ VLAN を設定しない場合、デフォルトが使用されます (VLAN 1)。
ステップ 7	Switch(config-if)# switchport trunk allowed vlan {add except all remove} vlan_num[,vlan_num[,vlan_num[,]]	(任意)トランク上で許容される VLAN のリストを 設定します。デフォルトでは、すべての VLAN が許 容されます。トランクからデフォルト VLAN を削除 することはできません。
ステップ 8	Switch(config-if)# switchport trunk pruning vlan {add except none remove} vlan_num[,vlan_num[,vlan_num[,]]	(任意)トランクでプルーニングが許容されている VLANのリストを設定します(「VTP」[p.13-9]を参 照)。デフォルトでは、プルーニングが許容される VLANのリストに、VLAN 1を除くすべての VLAN が含まれます。
ステップ 9	Switch(config-if)# no shutdown	インターフェイスをアクティブにします (インターフェイスをシャットダウンした場合のみ)。
ステップ 10	Switch(config-if)# end	インターフェイス コンフィギュレーション モード を終了します。
ステップ 11	Switch# show running-config interface {fastethernet gigabitethernet tengigabitethernet} slot/port	インターフェイスの実行コンフィギュレーションを 表示します。
ステップ 12	Switch# show interfaces [fastethernet gigabitethernet tengigabitethernet] slot/port switchport	インターフェイスのスイッチ ポート設定を表示します。
ステップ 13	Switch# show interfaces [{fastethernet gigabitethernet tengigabitethernet} slot/port] trunk	インターフェイスのトランク設定を表示します。

次に、インターフェイス FastEthernet 5/8 を 802.1Q トランクとして設定する例を示します。この例では、近接インターフェイスが 802.1Q トランキングをサポートするように設定され、ネイティブ VLAN のデフォルトが VLAN 1 に設定されているものとします。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 5/8
Switch(config-if)# shutdown
Switch(config-if)# switchport mode dynamic desirable
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# no shutdown
Switch(config-if)# end
Switch# exit
```

次に、実行コンフィギュレーションを確認する例を示します。

```
Switch# show running-config interface fastethernet 5/8
Building configuration...
Current configuration:
!
interface FastEthernet5/8
switchport mode dynamic desirable
switchport trunk encapsulation dot1q
```

次に、スイッチ ポートの設定を確認する例を示します。

```
Switch# show interfaces fastethernet 5/8 switchport
Name: Fa5/8
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: trunk
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Enabled
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
```

次に、トランクの設定を確認する例を示します。

Pruning VLANs Enabled: 2-1001

Switch#

Switch# show interfaces fastethernet 5/8 trunk

```
Port
       Mode
                  Encapsulation Status
                                         Native vlan
Fa5/8
       desirable
                n-802.1q
                              trunking
       Vlans allowed on trunk
Port
Fa5/8 1-1005
       Vlans allowed and active in management domain
02,850,917,999,1002-1005
       Vlans in spanning tree forwarding state and not pruned
Fa5/8 1-6,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-8
02,850,917,999,1002-1005
```

レイヤ2アクセス ポートとしてのインターフェイスの設定



(注)

存在しない VLAN にインターフェイスを割り当てると、VLAN データベースにその VLAN を作成 するまで、インターフェイスは機能しません(「グローバル コンフィギュレーション モードでの VLAN の設定」[p.13-6] を参照)。

インターフェイスをレイヤ2アクセスポートとして設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# interface {fastethernet gigabitethernet tengigabitethernet} slot/port	設定するインターフェイスを指定します。
ステップ 2	Switch(config-if)# shutdown	(任意)設定が完了するまでトラフィックを流さない ようにするため、インターフェイスをシャットダウ ンします。
ステップ 3	Switch(config-if)# switchport	インターフェイスをレイヤ 2 スイッチング用に設定 します。
		 インターフェイスをレイヤ2ポートとして設定するには、キーワードを指定せずにswitchportコマンドを1回入力する必要があります。そのあとで、キーワードとともに他のswitchportコマンドを入力してください。
		 それまでにインターフェイスに対して no switchport コマンドを入力している場合にの み必要です。
ステップ 4	Switch(config-if)# switchport mode access	インターフェイスをレイヤ 2 アクセス ポートとして 設定します。
ステップ 5	Switch(config-if)# switchport access vlan vlan_num	インターフェイスを VLAN 内に配置します。
ステップ 6	Switch(config-if)# no shutdown	インターフェイスをアクティブにします (インターフェイスをシャットダウンした場合のみ)。
ステップ 7	Switch(config-if)# end	インターフェイス コンフィギュレーション モード を終了します。
ステップ 8	Switch# show running-config interface {fastethernet gigabitethernet} slot/port	インターフェイスの実行コンフィギュレーションを 表示します。
ステップ 9	Switch# show interfaces [{fastethernet gigabitethernet tengigabitethernet} slot/port] switchport	インターフェイスのスイッチ ポート設定を表示します。

次に、インターフェイス FastEthernet 5/6 を VLAN 200 のアクセス ポートとして設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 5/6
Switch(config-if)# shutdown
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 200
Switch(config-if)# no shutdown
Switch(config-if)# end
Switch# exit
```

次に、実行コンフィギュレーションを確認する例を示します。

```
Switch# show running-config interface fastethernet 5/6
Building configuration...!

Current configuration :33 bytes
interface FastEthernet 5/6
switchport access vlan 200
switchport mode access
end
```

次に、スイッチ ポートの設定を確認する例を示します。

```
Switch# show running-config interface fastethernet 5/6 switchport
Name:Fa5/6
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation:negotiate
Operational Trunking Encapsulation:native
Negotiation of Trunking:On
Access Mode VLAN:1 (default)
Trunking Native Mode VLAN:1 (default)
Administrative private-vlan host-association:none
Administrative private-vlan mapping:none
Operational private-vlan:none
Trunking VLANs Enabled:ALL
Pruning VLANs Enabled: 2-1001
Switch#
```

レイヤ 2 設定のクリア

インターフェイス上のレイヤ2設定をクリアするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# default interface {fastethernet gigabitethernet tengigabitethernet} slot/port	クリアするインターフェイスを指定します。
ステップ 2	Switch(config-if)# end	インターフェイス コンフィギュレーション モード を終了します。
ステップ 3	Switch# show running-config interface {fastethernet gigabitethernet tengigabitethernet} slot/port	インターフェイスの実行コンフィギュレーションを 表示します。
ステップ 4	Switch# show interfaces [{fastethernet gigabitethernet tengigabitethernet} slot/port] switchport	インターフェイスのスイッチ ポート設定を表示します。

次に、インターフェイス FastEthernet 5/6 のレイヤ 2 設定をクリアする例を示します。

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# default interface fastethernet 5/6
Switch(config)# end
Switch# exit

次に、レイヤ2設定のクリアを確認する例を示します。

Switch# show running-config interface fastethernet 5/6
Building configuration...
Current configuration:
!
interface FastEthernet5/6
end

次に、スイッチ ポートの設定を確認する例を示します。

Switch# show interfaces fastethernet 5/6 switchport Name: Fa5/6 Switchport: Enabled Switch#



CHAPTER

16

SmartPort マクロの設定

この章では、スイッチに SmartPort マクロを設定して適用する方法について説明します。 この章の内容は、次のとおりです。

- SmartPort マクロの概要 (p.16-2)
- SmartPort マクロの設定 (p.16-3)
- SmartPort マクロの表示 (p.16-15)



この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/cr/index.htm

SmartPort マクロの概要

SmartPort マクロは、一般的な設定を保存したり、共有する作業を簡単に実行するための方法を提供します。SmartPort マクロを使用すると、ネットワーク内のスイッチの位置に基づいて機能および設定をイネーブルにしたり、ネットワーク中に多数の設定を導入したりできます。

各 SmartPort マクロは、ユーザが定義した CLI(コマンドライン インターフェイス)コマンドのセットです。SmartPort マクロ セットには新しい CLI コマンドは含まれません。各 SmartPort マクロは既存の CLI コマンドの集合です。

SmartPort マクロをインターフェイスに適用すると、マクロに含まれる CLI コマンドがインターフェイスに設定されますが、既存のインターフェイス設定は失われません。新しいコマンドはインターフェイスに追加されて、実行コンフィギュレーション ファイルに保存されます。

シスコのデフォルト SmartPort マクロはスイッチ ソフトウェアに組み込まれています(表 16-1 を参照)。 show parser macro ユーザ EXEC コマンドを使用して、マクロとマクロに含まれるコマンドを表示できます。

表 16-1 シスコのデフォルト SmartPort マクロ

マクロ名1	説明
cisco-global	Rapid PVST+、ループガード、およびリンク ステート障害のダイナミック ポート エラー回復をイネーブルにするには、このグローバル コンフィギュレーション マクロを使用します。
cisco-desktop	PC などのデスクトップ デバイスをスイッチ ポートに接続する場合、ネット ワーク セキュリティおよび信頼性を強化するには、このインターフェイス コンフィギュレーション マクロを使用します。
cisco-phone	Cisco IP Phone が接続されている PC などのデスクトップ デバイスをスイッチポートに接続する場合、このインターフェイス コンフィギュレーション マクロを使用します。このマクロは cisco-desktop マクロの拡張版で、同じセキュリティと信頼性を提供しますが、専用音声 VLAN (仮想 LAN)のサポートが追加されているため、遅延の影響を受けやすい音声トラフィックを適切に処理できます。
cisco-switch	GigaStack モジュールまたは GBIC (ギガビット インターフェイス コンバータ)を使用して、アクセス スイッチとディストリビューション スイッチ、またはアクセス スイッチ同士を接続する場合、このインターフェイス コンフィギュレーション マクロを使用します。
cisco-router	スイッチと WAN ルータを接続する場合、このインターフェイス コンフィ ギュレーション マクロを使用します。

^{1.} シスコのデフォルト SmartPort マクロは、スイッチで稼働するソフトウェア バージョンによって異なります。

シスコでは、事前テスト済みの、シスコが推奨する Catalyst スイッチ用ベースライン コンフィギュレーション テンプレート集を提供しています。オンライン リファレンス ガイド テンプレートは、ポートの使用状況に基づいて SmartPort マクロを作成するのに使用できる CLI コマンドを提供します。シスコ推奨のネットワーク設計や設定を構築し、展開するために、コンフィギュレーション テンプレートを使用して SmartPort マクロを作成できます。シスコ推奨のコンフィギュレーション テンプレートの詳細については、次の SmartPort Web サイトにアクセスしてください。

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

SmartPort マクロの設定

新しい SmartPort マクロを作成するか、既存のマクロをテンプレートとして使用すると、ご使用のアプリケーション専用の新しいマクロを作成できます。作成したマクロは、特定のインターフェイスまたはインターフェイス範囲に適用できます。

ここでは、次の内容について説明します。

- マクロに渡されるパラメータ (p.16-3)
- SmartPort マクロのデフォルト設定 (p.16-4)
- SmartPort マクロの設定時の注意事項 (p.16-6)
- SmartPort マクロの作成 (p.16-8)
- SmartPort マクロの適用 (p.16-9)

マクロに渡されるパラメータ

コマンドの一部にはすべてのインターフェイスに対する汎用性のないものがあります。たとえば、レイヤ 2 インターフェイスの VLAN ID およびレイヤ 3 インターフェイスの IP アドレスです。マクロにこのようなコマンドを定義すると、このマクロを別のインターフェイスに適用する前に、パラメータ(VLAN ID または IP アドレス)の値を変更する必要があります。あるいは、パラメータの各値を設定するために別々のマクロを作成する必要があります。

マクロのインフラストラクチャは、マクロを適用している間にパラメータを受け入れるよう拡張できます。パラメータは*キーワードと値*のペアとして、渡されます。

CLI で入力できるキーワード / 値ペア数は最大 3 つです。最初のパラメータはキーワードである必要があります。2 番めのパラメータは対応する値です。3 番めのパラメータは 2 番めのキーワード / 値ペアのキーワードです。次に、パラメータをコマンドマクロに渡す例を示します。

Switch(config)# macro name parameter-test

Enter macro commands one per line. End with the character '@'. switchport mode access switchport access vlan VLANID switchport port-security switchport port-security maximum AXHOST

上記のマクロがパラメータなしでインターフェイスに適用された場合、無効なコマンドは失敗します。代わりに、適切なキーワード / 値ペアのパラメータを使用して、マクロを次のように適用する必要があります。

Switch(config-if) # macro apply parameter-test \$VLANID 1 \$MAXHOST 5

上記のコマンドを実行すると、\$VLANID を 1 に、\$MAXHOST を 5 に置き換えたあとでマクロが適用されます。マクロ内では任意のストリングをキーワードとして指定できることに注意してください。

マクロ パラメータのヘルプ

マクロをインターフェイスまたはスイッチに適用する場合、マクロのキーワードを覚えておくこと は困難です。マクロには、必須キーワードの定義を含めることができます。これらのキーワード値 を入力せずにマクロを適用した場合、コマンドは無効とみなされ失敗します。

マクロで定義されたキーワードに関するヘルプを提供するようマクロ インフラストラクチャを拡張できます。マクロを作成するとき、ヘルプ ストリングを (コメントとして)指定し、そのマクロの必須キーワードを一覧表示するように設定できます。

次に、キーワードに関するヘルプストリングを指定する例を示します。

Switch(config)# macro name test
switchport access vlan \$VLANID
switchport port-security maximum \$MAX
#macro keywords \$VLANID \$MAX

ヘルプ ストリングはマクロ内のどこにでも配置できます。次に、ヘルプ ストリングを指定する別の例を示します。

Switch(config) # macro name test switchport access vlan \$VLANID #macro keywords \$VLANID switchport port-security maximum \$MAX #macro keywords \$MAX

SmartPort マクロのデフォルト設定

ここでは、サポートされているマクロのデフォルト設定を示します。これらのマクロは表示および 適用のみが可能です。ユーザはこれらを変更できません。

- cisco-global (p.16-4)
- cisco-desktop (p.16-5)
- cisco-phone (p.16-5)
- cisco-router (p.16-6)
- cisco-switch (p.16-6)

cisco-global

次に、cisco-global マクロの例を示します。

```
# Enable dynamic port error recovery for link state failures.
errdisable recovery cause link-flap
errdisable recovery interval 60

# VTP requires Transparent mode for future 802.1x Guest VLAN
# and current Best Practice
vtp domain [smartports]
vtp mode transparent

# Enable aggressive mode UDLD on all fiber uplinks
udld aggressive

# Enable Rapid PVST+ and Loopguard
spanning-tree mode rapid-pvst
spanning-tree loopguard default
spanning-tree extend system-id
```

cisco-desktop

次に、cisco-desktop マクロの例を示します。

```
# Basic interface - Enable data VLAN only
# Recommended value for access vlan (AVID) should not be 1
switchport access vlan $AVID
switchport mode access
# Enable port security limiting port to a single
# MAC address -- that of desktop
switchport port-security
# Ensure port-security age is greater than one minute
# and use inactivity timer
\mbox{\tt\#} "Port-security maximum 1" is the default and will not
# Show up in the config
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
# Configure port as an edge network port
spanning-tree portfast
spanning-tree bpduguard enable
```

cisco-phone

次に、cisco-phone マクロの例を示します。

```
# VoIP enabled interface - Enable data VLAN
# and voice VLAN (VVID)
\# Recommended value for access vlan (AVID) should not be 1\
switchport access vlan $AVID
switchport mode access
# Update the Voice VLAN (VVID) value which should be
# different from data VLAN
# Recommended value for voice vlan (VVID) should not be 1
switchport voice vlan $VVID
# Enable port security limiting port to a 2 MAC
# addressess -- One for desktop and two for phone
switchport port-security
switchport port-security maximum 2
# Ensure port-security age is greater than one minute
\# and use inactivity timer
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
# Enable auto-qos to extend trust to attached Cisco phone
auto gos voip cisco-phone
# Configure port as an edge network port
spanning-tree portfast
spanning-tree bpduguard enable@
```

cisco-router

次に、cisco-router マクロの例を示します。

```
# Access Uplink to Distribution
switchport trunk encapsulation dot1q
# Define unique Native VLAN on trunk ports
# Recommended value for native vlan (NVID) should not be 1
switchport trunk native vlan $NVID
# Update the allowed VLAN range (VRANGE) such that it
# includes data, voice and native VLANs
# switchport trunk allowed vlan $VRANGE
# Hardcode trunk and disable negotiation to
# speed up convergence
# Hardcode speed and duplex to router
switchport mode trunk
switchport nonegotiate
speed 100
duplex full
# Configure qos to trust this interface
auto gos voip trust
qos trust dscp
# Ensure fast access to the network when enabling the interface.
# Ensure that switch devices cannot become active on the interface.
spanning-tree portfast
spanning-tree bpduguard enable
```

cisco-switch

次に、cisco-switch マクロの例を示します。

```
# Access Uplink to Distribution
switchport trunk encapsulation dot1q
# Define unique Native VLAN on trunk ports
# Recommended value for native vlan (NVID) should not be 1
switchport trunk native vlan $NVID
# Update the allowed VLAN range (VRANGE) such that it
# includes data, voice and native VLANs
# switchport trunk allowed vlan $VRANGE
# Hardcode trunk and disable negotiation to
# speed up convergence
switchport mode trunk
switchport nonegotiate
# Configure gos to trust this interface
auto qos voip trust
# 802.1w defines the link as pt-pt for rapid convergence
spanning-tree link-type point-to-point
```

SmartPort マクロの設定時の注意事項

スイッチにマクロを設定する場合は、次の注意事項に従ってください。

- マクロを適用した際に、構文エラーまたは設定エラーが発生してコマンドが失敗した場合、マクロは残りのコマンドを引き続きインターフェイスに適用します。
- cisco-global はグローバル コンフィギュレーション モードで適用する必要があります。他のインターフェイス レベルのマクロよりも先にこのマクロを適用することを推奨します。
- インターフェイス上でシステム定義マクロ (cisco-desktop、cisco-phone、cisco-switch、および cisco-router)を適用する場合は、特定のキーワードが必要です。
- cisco-phone マクロを使用してポート セキュリティを適用する場合、最大のポート セキュリティは 2 となります (switchport port-security maximum 2)。
- キーワード / 値のペアは、システム定義マクロごとに最大3つまで指定できます。

- マクロを作成する場合、exit または end コマンドを使用しないでください。また、interface interface-id を使用してコマンド モードを変更しないでください。これらのコマンドを使用すると、exit、end、または interface interface-id のあとに続くコマンドが別のコマンド モードで実行されることがあります。
- マクロを作成する場合は、同じコンフィギュレーション モードの CLI コマンドを使用してください。
- 一意の値の割り当てが必要なマクロを作成する場合、parameter value キーワードを使用してインターフェイスに固有の値を指定します。キーワードの照合では、大文字と小文字が区別されます。キーワードが一致した場合はすべて、対応する値に置き換えられます。キーワードが完全一致する場合、これが長いストリングの一部であっても一致とみなされ、対応する値に置き換えられます。
- マクロ名は大文字と小文字が区別されます。たとえば、コマンド macro name Sample-Macro と macro name sample-macro は、別のマクロになります。
- マクロの中に、パラメータ値が必要なキーワードが含まれている場合があります。macro global apply macro-name? グローバル コンフィギュレーション コマンドまたは macro apply macro-name? インターフェイス コンフィギュレーション コマンドを使用すると、マクロで必要な値のリストを表示できます。キーワード値を入力せずにマクロを適用した場合、コマンドは無効になり適用されません。
- マクロがスイッチまたはスイッチ インターフェイスにグローバルに適用されても、そのインターフェイスの既存の設定はすべて保持されます。これは、設定を差分的に適用する場合に便利です。
- コマンドを追加または削除してマクロ定義を変更しても、元のマクロが適用されたインターフェイスには変更が反映されません。新しいコマンドまたは変更されたコマンドを適用するには、更新されたマクロをインターフェイスに再適用する必要があります。
- macro global trace macro-name グローバル コンフィギュレーション コマンドまたは macro trace macro-name インターフェイス コンフィギュレーション コマンドを使用して、構文または設定エラーを調べるためのマクロを適用してデバッグできます。構文エラーまたは設定エラーによりコマンドが失敗した場合、マクロは続けて残りのコマンドを適用します。
- 一部の CLI コマンドは、特定のインターフェイス タイプ専用です。マクロが設定を受け入れないインターフェイスに適用された場合、マクロは構文チェックや設定チェックを通らず、スイッチがエラー メッセージを返します。
- インターフェイスの範囲にマクロを適用する方法は、単一インターフェイスにマクロを適用する場合と同じです。インターフェイス範囲を使用した場合、マクロは範囲内のインターフェイスに順に適用されます。1つのインターフェイス上でマクロコマンドが失敗しても、他のインターフェイスにマクロが適用されます。
- マクロをスイッチまたはスイッチ インターフェイスに適用すると、マクロ名が自動的にスイッチまたはインターフェイスのマクロの説明に追加されます。show parser macro description ユーザ EXEC コマンドを使用して、適用されたコマンドとマクロ名を表示できます。
- ユーザ設定可能なマクロには、最大 3000 文字のコマンドとコメントを保持できるバッファがあります。新しく 1 行入力するたびに、2 文字使用されます。空の行はそのままカウントされます。

シスコのデフォルト SmartPort マクロはスイッチ ソフトウェアに組み込まれています(表 16-1 を参照)。 show parser macro ユーザ EXEC コマンドを使用して、マクロとマクロに含まれるコマンドを表示できます。

シスコのデフォルト SmartPort マクロをインターフェイスに適用する場合には、次の注意事項に 従ってください。

- スイッチ上のすべてのマクロを表示するには、show parser macro ユーザ EXEC コマンドを使用します。特定のマクロの内容を表示するには、show parser macro macro-name ユーザ EXEC コマンドを使用します。
- \$ で始まるキーワードには、一意のパラメータ値が必要です。parameter value キーワードを使用して、必要な値とともにシスコ デフォルト マクロに必要な値を追加します。

シスコ デフォルト マクロでは、必要なキーワードを識別するのに \$ 文字を使用します。 \$ 文字の使用に制限はありません。

SmartPort マクロの作成

SmartPort マクロを作成するには、次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	macro name macro-name	マクロ定義を作成し、マクロ名を入力します。マクロ定義の文字数は最大で 3000 文字です。
		マクロ コマンドを 1 行に 1 つずつ入力します。マクロを終了するには、@ 文字を入力します。マクロ内にコメント テキストを入力するには、行の先頭に # 文字を使用します。
		マクロ名は大文字と小文字が区別されます。たとえば、 コマンド macro name Sample-Macro と macro name sample-macro は、別のマクロになります。
		マクロ内で exit または end コマンドを使用したり、interface interface-id を使用してコマンドモードを変更したりしないことを推奨します。これらのコマンドを使用すると、exit、end、または interface interface-id のあとに続くコマンドが別のコマンドモードで実行されることがあります。最良の結果を得るには、マクロ内のすべてのコマンドが同じコンフィギュレーション モードである必要があります。
		(注) macro name グローバル コンフィギュレーションコマンドの no 形式を使用しても、マクロ定義の削除が行われるだけです。このコマンドを実行しても、マクロがすでに適用されているインターフェイスの設定には影響しません。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show parser macro name macro-name	マクロが作成されたことを確認します。

SmartPort マクロの適用

SmartPort マクロを適用するには、次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	macro global {apply trace} macro-name [parameter {value}] [parameter {value}] [parameter {value}]	マクロで定義された各コマンドをスイッチに適用するには、macro global apply macro-name を入力します。構文または設定エラーを調べるためのマクロを適用し、デバッグするには、macro global trace macro-name を指定します。
		(任意)スイッチに固有の一意なパラメータ値を指定します。最大3つのキーワード/値ペアを入力できます。パラメータキーワードの照合では、大文字と小文字が区別されます。キーワードが一致した場合はすべて、対応する値に置き換えられます。
		マクロの中に、パラメータ値が必要なキーワードが含まれている場合があります。マクロで必要な値のリストを表示するには、macro global apply macro-name?コマンドを使用します。キーワード値を入力せずにマクロを適用した場合、コマンドは無効になり適用されません。
ステップ 3	macro global description text	(任意)スイッチに適用されるマクロの説明を入力します。
ステップ 4	interface interface-id	(任意)インターフェイス コンフィギュレーション モード を開始して、マクロを適用するインターフェイスを指定し ます。
ステップ 5	default interface interface-id	(任意)指定したインターフェイスからすべての設定を消去 します。
ステップ 6	macro {apply trace} macro-name [parameter {value}] [parameter {value}] [parameter {value}]	マクロで定義された各コマンドをインターフェイスに適用するには、macro apply macro-name を入力します。構文または設定エラーを調べるためマクロを適用し、デバッグするには、macro trace macro-name を指定します。
		(任意)インターフェイスに固有の一意なパラメータ値を指定します。最大3つのキーワード/値ペアを入力できます。 パラメータ キーワードの照合では、大文字と小文字が区別 されます。キーワードが一致した場合はすべて、対応する 値に置き換えられます。
		マクロの中に、パラメータ値が必要なキーワードが含まれている場合があります。マクロで必要な値のリストを表示するには、macro apply macro-name?コマンドを使用します。キーワード値を入力せずにマクロを適用した場合、コマンドは無効になり適用されません。
		次に、このコマンドを適用する例を示します。
		Switch(config-if)# macro apply cisco-phone ? WORD Keyword to replace with a value e.g. \$AVID, \$VVID <cr></cr>
ステップ 7	macro description text	(任意)インターフェイスに適用されるマクロの説明を入力します。
ステップ 8	end	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 9	show parser macro description [interface	マクロがインターフェイスに適用されたことを確認しま
	interface-id]	す。
ステップ 10	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存し
		ます。

スイッチ上のグローバルマクロによって適用された設定を削除するには、マクロ内の各コマンドの no バージョンを入力するしかありません。マクロによって特定のインターフェイスに適用された設定を削除するには、default interface interface-id インターフェイス コンフィギュレーション コマンドを入力します。

macro name グローバル コンフィギュレーション コマンドの no 形式を使用しても、マクロ定義の削除が行われるだけです。このコマンドを実行しても、マクロがすでに適用されているインターフェイスの設定には影響しません。マクロによって特定のインターフェイスに適用された設定を削除するには、default interface interface-id インターフェイス コンフィギュレーション コマンドを入力します。また、元のマクロ内の対応するすべてのコマンドの no 形式を含む、既存のマクロに対するアンチマクロを作成できます。そのあと、このアンチマクロをインターフェイスに適用します。

ここでは、サポートされている各マクロを適用して、内容を表示する例を示します。

- cisco-global (p.16-10)
- cisco-desktop (p.16-11)
- cisco-phone (p.16-12)
- cisco-switch (p.16-13)
- cisco-router (p.16-14)

cisco-global

次に、cisco-global というシステム定義マクロを使用する例を示します。

```
Switch(config) # macro global apply cisco-global
Changing VTP domain name from gsg-switch to [smartports]
Setting device to VTP TRANSPARENT mode.
Switch(config) # end
Switch# show parser macro name cisco-global
Macro name : cisco-global
Macro type : default global
# Enable dynamic port error recovery for link state failures.
errdisable recovery cause link-flap
errdisable recovery interval 60
# VTP requires Transparent mode for future 802.1x Guest VLAN
# and current Best Practice vtp domain [smartports] vtp mode transparent
# Enable aggressive mode UDLD on all fiber uplinks udld aggressive
# Enable Rapid PVST+ and Loopguard
spanning-tree mode rapid-pvst
spanning-tree loopguard default
spanning-tree extend system-id
```

cisco-desktop

次に、システム定義マクロ cisco-desktop を使用して、35 の値をインターフェイス FastEthernet 2/9 のアクセス VLAN に割り当てる例を示します。



このマクロでは、ポートのアクセス VLAN を指定する \$AVID キーワードが必要です。

```
Switch(config)# interface fastethernet2/9
{\tt Switch(config-if)\# macro\ apply\ cisco-desktop\ \$AVID\ 35}
Switch(config-if)# end
Switch# show parser macro name cisco-desktop
Macro name : cisco-desktop
Macro type : customizable
# Basic interface - Enable data VLAN only
# Recommended value for access vlan (AVID) should not be 1
switchport access vlan $AVID [access_vlan_id]
switchport mode access
# Enable port security limiting port to a single
\# MAC address -- that of desktop
switchport port-security
# Ensure port-security age is greater than one minute
# and use inactivity timer
# "Port-security maximum 1" is the default and will not
# Show up in the config
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
# Configure port as an edge network port
spanning-tree portfast
spanning-tree bpduguard enable
Switch# show parser macro description
Interface Macro Description
Fa2/9
           cisco-desktop
```

cisco-phone

次に、システム定義マクロ cisco-phone を使用して、インターフェイス FastEthernet 2/9 上のアクセス VLAN に 35 の値を、音声 VLAN に 56 の値を割り当てる例を示します。



このマクロでは、ポートのアクセス VLAN を指定する **\$AVID**、および音声 VLAN を指定する **\$VVID** キーワードが必要です。

```
Switch(config) # interface fastethernet2/9
Switch(config-if)# macro apply cisco-phone
Switch(config-if)# macro description cisco-phone $AVID 35 $VVID 56
Switch(config-if)# end
Switch# show parser macro name cisco-phone
Macro name : cisco-phone
Macro type : customizable
# VoIP enabled interface - Enable data VLAN
# and voice VLAN (VVID)
\# Recommended value for access vlan (AVID) should not be 1\
switchport access vlan $AVID [access_vlan_id]
switchport mode access
# Update the Voice VLAN (VVID) value which should be
# different from data VLAN
# Recommended value for voice vlan (VVID) should not be 1
switchport voice vlan $VVID [voice_vlan_id]
# Enable port security limiting port to a 2 MAC
# addressess -- One for desktop and one for phone
switchport port-security
switchport port-security maximum 2
# Ensure port-security age is greater than one minute
# and use inactivity timer
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
# Enable auto-qos to extend trust to attached Cisco phone
auto qos voip cisco-phone
# Configure port as an edge network port
spanning-tree portfast
spanning-tree bpduguard enable@
Switch# show parser macro description
Interface Macro Description
Fa2/9
         cisco-phone
```

cisco-switch

次に、システム定義マクロ cisco-switch を使用して、38 の値をインターフェイス FastEthernet 2/9 上のネイティブ VLAN に割り当てる例を示します。



このマクロでは、ポートのネイティブ VLAN を指定する \$NVID キーワードが必要です。

```
Switch(config)# interface fastethernet2/9
Switch(config-if)# macro apply cisco-switch
Switch(config-if) # macro description cisco-switch $NVID 38
Switch(config-if)# end
Switch# show parser macro name cisco-switch
Macro name : cisco-switch
Macro type : customizable
# Access Uplink to Distribution
switchport trunk encapsulation dot1q
# Define unique Native VLAN on trunk ports
# Recommended value for native vlan (NVID) should not be 1
switchport trunk native vlan $NVID [native_vlan_id]
\mbox{\tt\#} Update the allowed VLAN range (VRANGE) such that it
# includes data, voice and native VLANs
# switchport trunk allowed vlan $VRANGE [vlan_range]
# Hardcode trunk and disable negotiation to
# speed up convergence
switchport mode trunk
switchport nonegotiate
# Configure qos to trust this interface
auto gos voip trust
# 802.1w defines the link as pt-pt for rapid convergence
spanning-tree link-type point-to-point
Switch# show parser macro description
Interface Macro Description
Fa2/9
            cisco-switch
```

cisco-router

次に、システム定義マクロ **cisco-router** を使用して、451 の値をインターフェイス FastEthernet 2/9 上のネイティブ VLAN に割り当てる例を示します。



このマクロでは、ポートのネイティブ VLAN を指定する \$NVID キーワードが必要です。

```
Switch(config)# interface fastethernet2/9
Switch(config-if)# macro apply cisco-router
Switch(config-if) # macro description cisco-router $NVID 45I
Switch(config-if)# end
Switch# show parser macro name cisco-router
Macro name : cisco-router
Macro type : customizable
# Access Uplink to Distribution
switchport trunk encapsulation dot1q
# Define unique Native VLAN on trunk ports
# Recommended value for native vlan (NVID) should not be 1
switchport trunk native vlan $NVID [native_vlan_id]
# Update the allowed VLAN range (VRANGE) such that it
# includes data, voice and native VLANs
# switchport trunk allowed vlan $VRANGE [vlan_range]
# Hardcode trunk and disable negotiation to
# speed up convergence
# Hardcode speed and duplex to router
switchport mode trunk
switchport nonegotiate
speed 100
duplex full
# Configure qos to trust this interface
auto qos voip trust
gos trust dscp
# Ensure fast access to the network when enabling the interface.
# Ensure that switch devices cannot become active on the interface.
spanning-tree portfast
spanning-tree bpduguard enable
Switch# show parser macro description
Interface Macro Description
______
Fa2/9
           cisco-router
```

SmartPort マクロの表示

SmartPort マクロを表示するには、表 16-2 に示す特権 EXEC コマンドの 1 つまたは複数のコマンドを使用します。

表 16-2 SmartPort マクロを表示するためのコマンド

コマンド	目的
show parser macro	設定されたすべてのマクロを表示します。
show parser macro name macro-name	特定のマクロを表示します。
show parser macro brief	設定されたマクロの名前を表示します。
show parser macro description [interface interface-id]	すべてのインターフェイスまたは指定されたインターフェ イスのマクロの説明を表示します。

■ SmartPort マクロの表示



CHAPTER

17

STP および MST の設定

この章では、Catalyst 4500 シリーズ スイッチ上で Spanning-Tree Protocol (STP; スパニングツリー プロトコル)を設定する方法について説明します。この章では、Catalyst 4500 シリーズ スイッチ 上の IEEE 802.1s Multiple Spanning-Tree (MST) プロトコルの設定手順についても説明します。 MST は、シスコ独自の Multi-Instance Spanning-Tree Protocol (MISTP) 実装から派生した新しい IEEE (米国電気電子学会)標準です。 MST により、単一のスパニングツリー インスタンスを複数の VLAN (仮想 LAN) にマッピングできます。

設定上の注意事項、設定手順、および設定例も示します。この章の主な内容は、次のとおりです。

- STPの概要 (p.17-2)
- STP のデフォルト設定 (p.17-8)
- STP の設定 (p.17-9)
- MST の概要 (p.17-25)
- MST 設定時の注意事項および制約事項 (p.17-32)
- MST の設定 (p.17-33)



PortFast、UplinkFast、および BackboneFast とその他のスパニングツリー拡張機能の設定手順については、第 19 章「任意の STP 機能の設定」を参照してください。



この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univered/cc/td/doc/product/software/ios122sr/cr/index.htm

STP の概要

STP は、ネットワーク上でパスの冗長性を確保し、不要なループの発生を防ぐレイヤ 2 リンク管理プロトコルです。レイヤ 2 イーサネット ネットワークの正常な動作を実現するには、どの 2 つのステーション間でもアクティブ パスを 1 つにする必要があります。ネットワーク トポロジのループフリーのサブセットは、スパニングツリーと呼ばれます。スパニングツリーの動作はエンド ステーションに対してトランスペアレントなので、エンド ステーションが特定の LAN セグメントに接続されているのか、それとも複数セグメントから構成されるスイッチド LAN に接続されているのかを検出できません。

Catalyst 4500 シリーズ スイッチは、すべての VLAN(仮想 LAN)上で STP (IEEE 802.1D ブリッジ プロトコル)を使用します。デフォルトでは、(スパニングツリーを手動でディセーブルにしない かぎり)設定されている VLAN ごとに 1 つのスパニングツリーが動作します。スパニングツリーは、VLAN 単位でイネーブルまたはディセーブルにできます。

フォールトトレラントなインターネットワークを作成する場合、ネットワーク上のすべてのノード間にループフリー パスを形成する必要があります。スパニングツリー アルゴリズムは、スイッチドレイヤ 2 ネットワーク上で最良のループフリー パスを算出します。スイッチは定期的にスパニングツリー フレームを送受信します。スイッチは、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。

エンド ステーション間に複数のアクティブ パスがあると、ネットワーク内でループが発生する原因になります。ネットワークにループが存在すると、エンド ステーションがメッセージを重複して受信する可能性があります。また、スイッチが複数のレイヤ 2 インターフェイス上のエンド ステーション MAC (メディア アクセス制御) アドレスを学習する可能性があります。このような状況により、ネットワークが不安定になります。

スパニングツリーは、ルート スイッチおよびそのルートからレイヤ 2 ネットワーク上のすべてのスイッチへのループフリー パスを備えたツリーを定義します。スパニングツリーは、冗長データ パスを強制的にスタンバイ(ブロック)ステートにします。スパニングツリーのネットワーク セグメントの 1 つで障害が発生し、かつ冗長パスが存在する場合、スパニングツリー アルゴリズムはスパニングツリー トポロジを再計算し、スタンバイ パスをアクティブにします。

スイッチ上の 2 つのポートがループの一部になっている場合、フォワーディング ステートになる ポートと、ブロッキング ステートになるポートは、スパニングツリー ポート プライオリティおよ びポート パス コストの設定によって決まります。スパニングツリー ポート プライオリティ値は、ネットワーク トポロジにおけるインターフェイスの位置を表すとともに、ポートがトラフィックを 伝送する場合にどの程度適した位置にあるかを表します。スパニングツリー ポート パス コスト値は、メディア速度を表します。

ブリッジ ID の概要

各ネットワーク デバイス上の各 VLAN には、一意の 64 ビット ブリッジ ID が設定されています。 ブリッジ ID はブリッジ プライオリティ値、拡張システム ID、および STP MAC アドレス割り当て で構成されています。

ブリッジ プライオリティ値

ブリッジ プライオリティ値は、特定の冗長リンクがプライオリティを指定され、スパニングツリーの特定のスパンに含まれるとみなされるかどうかを決定します。値が低いほど優先されるので、手動で優先度を設定する場合は、リンクに割り当てるブリッジ プライオリティの値を冗長リンクの場合よりも低くします。Cisco IOS Release 12.1(12c)EW より前のリリースでは、ブリッジ プライオリ

ティは 16 ビット値です (表 17-1 を参照)。 Cisco IOS Release 12.1(12c)EW 以降のリリースでは、ブリッジ プライオリティは拡張システム ID がイネーブルの場合は 4 ビット値です(表 17-2 を参照)。 「VLAN のブリッジ プライオリティの設定」(p.17-19)を参照してください。

拡張システム ID

拡張システム ID は、 $1025 \sim 4096$ の VLAN ID です。Cisco IOS Release 12.1(12c)EW 以降のリリースでは、ブリッジ ID の一部として 12 ビット拡張システム ID フィールドをサポートしています(表 17-2 を参照)。MAC アドレスを 64 個だけサポートするシャーシは、常に 12 ビットの拡張システム ID を使用します。1024 個の MAC アドレスをサポートするシャーシでは、拡張システム ID の使用をイネーブルにできます。STP は拡張システム ID として VLAN ID を使用します。「拡張システム ID のイネーブル化」(p.17-10) を参照してください。

表 17-1 拡張システム ID がディセーブルの場合のブリッジ プライオリティ値

プリッ	プリッジ プライオリティ値														
ピット 16	ピット 15	ピット 14	ピット 13	ピット 12	ピット 11	ピット 10	ピット 9	ピット 8	ピット 7	ピット 6	ピット 5	ピット 4	ピット 3	ピット 2	ピット 1
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

表 17-2 拡張システム ID がイネーブルの場合のブリッジ プライオリティ値および拡張システム ID

ブリッジ プライオリティ値				拡張シ	拡張システム ID (VLAN ID と同じに設定)										
ピット 16	ピット 15	ピット 14	ピット 13	ピット 12	ピット 11	ピット 10	ピット 9	ピット 8	ピット 7	ピット 6	ピット 5	ピット 4	ピット 3	ピット 2	ピット 1
32768	16384	8192	4096	VLAN	ID										

STP MAC アドレスの割り当て

Catalyst 4500 シリーズ スイッチのシャーシには、64 個または 1024 個の MAC アドレスがあり、STP のようなソフトウェア機能をサポートするために使用できます。シャーシの MAC アドレスの範囲を表示するには、show module コマンドを入力します。

Cisco IOS Release 12.1(12c)EW 以降のリリースでは、64 個または 1024 個の MAC アドレスを持つ シャーシをサポートしています。64 個の MAC アドレスを持つシャーシの場合、STP は拡張システム ID と MAC アドレスを使用して、VLAN ごとに一意のブリッジ ID を作成します。

Release 12.1(12c)EW より前のリリースでは、1024 個の MAC アドレスを持つシャーシをサポートしています。これらのリリースでは、STP は VLAN ごとに 1 つの MAC アドレスを使用して、VLAN ごとに一意のブリッジ ID を作成します。

BPDU

スイッチド ネットワークで常にアクティブなスパニングツリー トポロジを決定するのは、次の要素です。

- 各スイッチの VLAN ごとに関連付けられた一意のブリッジ ID (ブリッジ プライオリティと MAC アドレス)
- ルート ブリッジまでのスパニングツリー パス コスト (またはブリッジ プライオリティ値)
- 各レイヤ2インターフェイスに関連付けられたポート ID(ポート プライオリティと MAC アドレス)

Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) には、送信側ブリッジと そのポートについて、ブリッジおよび MAC アドレス、ブリッジ プライオリティ、ポート プライオリティ、パス コストなどの情報が含まれます。システムは接続するスイッチ間で BPDU を伝送して、ルート スイッチから一方向のスパニングツリー トポロジを計算します。各設定 BPDU には、少なくとも次の項目が含まれます。

- 送信側のスイッチがルート スイッチとみなしているスイッチの一意のブリッジ ID
- ルートまでのスパニングツリー パス コスト
- 送信側ブリッジの ID
- メッセージの有効期間
- 送信側ポートの ID
- hello タイマー、 *転送遅延*タイマー、および *最大エージング* プロトコル タイマーの値

スイッチが BPDU フレームを送信すると、そのフレームが伝送される LAN に接続されたすべてのスイッチが BPDU を受信します。スイッチが BPDU を受信すると、スイッチはそのフレームを転送するのではなく、フレームに含まれる情報を使用して BPDU を計算し、トポロジに変更があれば、BPDU の送信を開始します。

BPDU 交換によって次の動作が行われます。

- スイッチの1つがルートブリッジとして選定されます。
- パスコストに基づいて、各スイッチのルートブリッジまでの最短距離が計算されます。
- LAN セグメントごとに指定ブリッジが選択されます。これはルート ブリッジに最も近いスイッチで、このスイッチを経由してルートにフレームが転送されます。
- ルート ポートが選択されます。これはブリッジからルート ブリッジまでの最適パスを提供するポートです。
- スパニングツリーに含まれるポートが選択されます。

ルート ブリッジの選定

VLAN ごとに、最高のブリッジ プライオリティ (最小のプライオリティ値)を持つスイッチがルート ブリッジとして選定されます。すべてのスイッチがデフォルト プライオリティ値 (32,768) に設定されている場合は、VLAN 内で最小の MAC アドレスを持つスイッチがルート ブリッジになります。

スパニングツリー ルート ブリッジは、スイッチド ネットワークで論理的にスパニングツリー トポロジの中心に位置します。スイッチド ネットワーク内のどの場所からのパスも、ルート ブリッジに到達するために必要とされない場合は、すべてスパニングツリー ブロッキング モードになります。

スパニングツリーは BPDU から提供される情報を使用して、スイッチド ネットワークのルート ブリッジとルート ポート、および各スイッチド セグメントのルート ポートと指定されたポートを選定します。

STP タイマー

表 17-3 で、スパニングツリー全体のパフォーマンスに影響する STP タイマーについて説明します。

表 17-3 STP タイマー

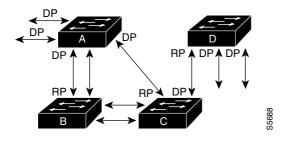
変数	説明
hello_time	スイッチがほかのスイッチに hello メッセージをプロードキャストする間隔 を指定します。
forward_time	ポートが転送を開始するまでの、リスニング ステートおよびラーニング ステートが継続する時間を決定します。
max_age	ポートで受信したプロトコル情報がスイッチで保持される期間を決定します。

STP トポロジの作成

スパニングツリー アルゴリズムの目標は、最もダイレクトなリンクをルート ポートにすることです。スパニングツリー トポロジがデフォルトのパラメータに基づいて計算されている場合、リンク速度により、スイッチド ネットワーク上の送信元から宛先エンド ステーションまでのパスが最適にならない可能性があります。たとえば、現在のルート ポートよりも数値の大きいポートに高速リンクを接続すると、ルート ポートの変更が必要になる場合があります。

図 17-1 では、スイッチ A がルート ブリッジとして選定されています (これは、すべてのスイッチ のブリッジ プライオリティがデフォルト値 [32,768] に設定され、スイッチ A が最も低い MAC アドレスを持つ場合に起こります)。ただし、トラフィック パターン、転送ポートの数、またはリンクタイプによっては、スイッチ A が最適なルート ブリッジであるとは限りません。最適なスイッチの STP ポート プライオリティを上げて (プライオリティの数値を小さくして)、そのスイッチをルート ブリッジに設定すると、最適なスイッチをルートとして持つ新しいスパニングツリー トポロジが強制的に再計算されます。

図 17-1 スパニングツリー トポロジ



RP = ルート ポート DP = 指定ポート

たとえば、スイッチ B の 1 つのポートが光ファイバ リンクで、同じスイッチの別のポート (Unshielded Twisted-Pair [UTP; シールドなしツイストペア]リンク) がルート ポートになっている と仮定します。ネットワーク トラフィックは高速の光ファイバ リンクに流す方が効率的です。光ファイバ ポートのスパニングツリー ポート プライオリティをルート ポートよりも高く(数値を小さく)すると、光ファイバ ポートが新しいルート ポートになります。

STP ポート ステート

プロトコル情報がスイッチド LAN を通過するとき、伝送遅延が生じることがあります。その結果、スイッチドネットワークのさまざまな時点および場所でトポロジが変化します。レイヤ 2 インターフェイスがスパニングツリートポロジに含まれていない状態からフォワーディング ステートに直接移行すると、一時的にデータのループが形成される可能性があります。ポートは新しいトポロジ情報がスイッチド LAN 経由で伝達されるまで待機し、そのあとでフレーム転送を開始する必要があります。さらに、古いトポロジで転送されたフレームの存続時間を満了させることも必要です。

スパニングツリーを使用するスイッチ上の各レイヤ2インターフェイスは、次の5つのステートのいずれかの状態で存在します。

- ブロッキング このステートでは、レイヤ2インターフェイスはフレームフォワーディングに参加しません。
- リスニング このステートは、スパニングツリーによりレイヤ2インターフェイスのフレームフォワーディングへの参加が決定されると、ブロックステートから最初に移行するステートです。
- ラーニング このステートでは、レイヤ 2 インターフェイスはフレーム フォワーディングに 参加する準備をします。
- フォワーディング このステートでは、レイヤ2インターフェイスはフレームを転送します。
- ディセーブル このステートでは、レイヤ 2 インターフェイスはスパニングツリーに参加せず、フレームを転送しません。

MAC アドレスの割り当て

スーパーバイザ エンジンは 1024 個の MAC アドレスを持ち、VLAN スパニングツリーのブリッジ ID として使用されます。スパニングツリーがアルゴリズムに使用する MAC アドレス範囲(スーパーバイザの割り当て範囲)を表示する場合は、show module コマンドを使用します。

Catalyst 4506 スイッチの MAC アドレスは連番で割り当てられます。すなわち、範囲の最初の MAC アドレスは VLAN 1 に割り当てられ、範囲の 2 番めの MAC アドレスは VLAN 2 に割り当てられます。たとえば、MAC アドレス範囲が 00-e0-1e-9b-2e-00 ~ 00-e0-1e-9b-31-ff の場合、VLAN 1 ブリッジ ID は 00-e0-1e-9b-2e-00、VLAN 2 ブリッジ ID は 00-e0-1e-9b-2e-01、VLAN 3 ブリッジ ID は 00-e0-1e-9b-2e-02 となります。ほかの Catalyst 4500 シリーズ プラットフォームでは、すべての VLAN は個々の MAC アドレスではなく、同一の MAC アドレスにマッピングします。

STP および IEEE 802.1Q トランク

802.1Q VLAN トランクによって、ネットワークのスパニングツリーの構築方法に、いくつかの制約が課せられます。802.1Q トランクを使用して接続しているシスコ製スイッチのネットワークでは、トランク上で許容される VLAN ごとに 1 つのスパニングツリー インスタンスが維持されます。他社製の 802.1Q スイッチでは、トランク上で許容されるすべての VLAN に対してスパニングツリーインスタンスが 1 つのみ維持されます。

802.1Q トランクを使用してシスコ製スイッチを (802.1Q をサポートする) 他社製のデバイスに接続する場合、シスコ製スイッチは、トランクの 802.1Q ネイティブ VLAN のスパニングツリー インスタンスを、他社製の 802.1Q スイッチのスパニングツリー インスタンスと統合します。ただし、VLAN 単位のスパニングツリー情報は、他社製の 802.1Q スイッチのネットワークと切り離して、シスコ製スイッチで維持されます。シスコ製スイッチを切り離している他社製の 802.1Q ネットワークは、スイッチ間の単一トランク リンクとして扱われます。



802.1Q トランクの詳細については、第 15 章「レイヤ 2 イーサネット インターフェイスの設定」を 参照してください。

PVRST+

Per-VLAN Rapid Spanning-Tree Plus (PVRST+) は PVST+ と同じですが、より高速なコンバージェ ンスを提供するために、802.1D ではなく IEEE 802.1w に基づいた Rapid STP(RSTP)を使用します。 PVRST+ は、PVST+ とほぼ同一の設定を使用し、最小限の設定で済みます。PVRST+ では、トポロ ジの変更時にポート単位でダイナミック CAM(連想メモリ)エントリがただちに消去されます。機 能が RSTP に組み込まれているため、このモードでは UplinkFast および BackboneFast はイネーブル に設定されていますが、アクティブになりません。PVRST+ は、ブリッジ、ブリッジ ポートまたは LAN 障害が発生したのち、迅速な接続の回復を提供します。

イネーブル化に関する情報については、「PVRST+のイネーブル化」(p.17-22)を参照してください。

STP のデフォルト設定

表 17-4 に、デフォルトのスパニングツリー設定を示します。

表 17-4 スパニングツリーのデフォルト設定値

機能	デフォルト値
イネーブル ステート	すべての VLAN に対してスパニングツ リーがイネーブル
ブリッジ プライオリティ値	32,768
スパニングツリー ポート プライオリティ値 (インターフェイス単位で設定可能 レイヤ 2 アクセス ポートとして設定されたインターフェイスで使用)	128
スパニングツリー ポート コスト(インターフェイス単位 で設定可能 レイヤ 2 アクセス ポートとして設定され たインターフェイスで使用)	 10 ギガビット イーサネット:2 ギガビット イーサネット:4 ファスト イーサネット:19
スパニングツリー VLAN ポート プライオリティ値 (VLAN 単位で設定可能 レイヤ 2 トランク ポートとして設定されたインターフェイスで使用)	128
スパニングツリー VLAN ポート コスト(VLAN 単位で設定可能 レイヤ 2 トランク ポートとして設定されたインターフェイスで使用)	 10 ギガビット イーサネット:2 ギガビット イーサネット:4 ファスト イーサネット:19
hello タイム	2秒
転送遅延時間	15 秒
最大エージング タイム	20 秒

STP の設定

ここでは、VLAN 上でスパニングツリーを設定する手順について説明します。

- STP のイネーブル化 (p.17-9)
- 拡張システム ID のイネーブル化 (p.17-10)
- ルート ブリッジの設定 (p.17-11)
- セカンダリ ルート スイッチの設定 (p.17-13)
- STP ポート プライオリティの設定 (p.17-15)
- STP ポート コストの設定 (p.17-17)
- VLAN のブリッジ プライオリティの設定 (p.17-19)
- hello タイムの設定 (p.17-20)
- VLAN の最大エージング タイムの設定 (p.17-20)
- VLAN の転送遅延時間の設定 (p.17-21)
- STP のディセーブル化 (p.17-22)
- PVRST+のイネーブル化 (p.17-22)



(注)

この章で説明するスパニングツリー コマンドは、no switchport コマンドで設定されるインターフェイスを除き、すべてのインターフェイス上で設定できます。

STP のイネーブル化



(注)

デフォルトでは、すべての VLAN でスパニングツリーはイネーブルになっています。

スパニングツリーは、VLAN 単位でイネーブルにできます。スイッチは (スパニングツリーをディセーブルにした VLAN を除き) 各 VLAN についてスパニングツリーの個別のインスタンスを維持します。

VLAN 単位でスパニングツリーをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始
		します。
ステップ 2	Switch(config)# spanning-tree vlan vlan_ID	VLAN vlan_ID のスパニングツリーをイネーブルに
		します。 <i>vlan_ID</i> 値は、1 ~ 4094 の範囲で指定します。
ステップ 3	Switch(config)# end	コンフィギュレーション モードを終了します。
ステップ 4	Switch# show spanning-tree vlan vlan_ID	スパニングツリーがイネーブルになっていることを
		確認します。

次に、VLAN 200 上でスパニングツリーをイネーブルにする例を示します。

Switch# configure terminal
Switch(config)# spanning-tree vlan 200
Switch(config)# end
Switch#



スパニングツリーはデフォルトでイネーブルに設定されているので、show running コマンドを入力して作成されたコンフィギュレーションを表示しても、スパニングツリーをイネーブルにするために入力したコマンドは表示されません。

次に、VLAN 200 上でスパニングツリーがイネーブルになっていることを確認する例を示します。

Switch# show spanning-tree vlan 200

VLAN200 is executing the ieee compatible Spanning Tree protocol Bridge Identifier has priority 32768, address 0050.3e8d.6401 Configured hello time 2, max age 20, forward delay 15 Current root has priority 16384, address 0060.704c.7000 Root port is 264 (FastEthernet5/8), cost of root path is 38 Topology change flag not set, detected flag not set Number of topology changes 0 last change occurred 01:53:48 ago Times: hold 1, topology change 24, notification 2 hello 2, max age 14, forward delay 10 Timers: hello 0, topology change 0, notification 0

Port 264 (FastEthernet5/8) of VLAN200 is forwarding
Port path cost 19, Port priority 128, Port Identifier 129.9.
Designated root has priority 16384, address 0060.704c.7000
Designated bridge has priority 32768, address 00e0.4fac.b000
Designated port id is 128.2, designated path cost 19
Timers: message age 3, forward delay 0, hold 0
Number of transitions to forwarding state: 1
BPDU: sent 3, received 3417

Switch#

拡張システム ID のイネーブル化



64 個の MAC アドレスをサポートするシャーシの拡張システム ID は、常にイネーブルになっています。

1024 個の MAC アドレスをサポートするシャーシで拡張システム ID をイネーブルにするには、 spanning-tree extend system-id コマンドを使用します。「ブリッジ ID の概要」(p.17-2) を参照して ください。

拡張システム ID をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# spanning-tree extend system-id	拡張システム ID をイネーブルにします。
		拡張システム ID をディセーブルにします。
		(注) 64 個の MAC アドレスをサポートするシャーシでは、または拡張範囲 VLAN を設定している場合には、拡張システム ID をディセーブルにできません (表 17-4 [p.17-8] を参照)。
ステップ 2	Switch(config)# end	コンフィギュレーション モードを終了します。
ステップ 3	Switch# show spanning-tree vlan vlan_ID	設定を確認します。



(注)

拡張システム ID をイネーブルまたはディセーブルにすると、すべてのアクティブな STP インスタンスのブリッジ ID が更新されるため、これによってスパニングツリー トポロジが変更される場合があります。

次に、拡張システム ID をイネーブルにする例を示します。

Switch# configure terminal
Switch(config)# spanning-tree extend system-id
Switch(config)# end
Switch#

次に、設定を確認する例を示します。

Switch# show spanning-tree summary | include extended Extended system ID is enabled.

ルート ブリッジの設定

Catalyst 4000 ファミリ スイッチは、スイッチ上に設定されたアクティブな VLAN ごとにスパニング ツリーのインスタンスを維持します。各インスタンスには、ブリッジ プライオリティおよびブリッジ MAC アドレスで構成されるブリッジ ID が対応付けられます。 VLAN ごとに、最小のブリッジ ID を持つスイッチが、その VLAN のルート ブリッジとして選定されます。 ブリッジ プライオリティが変更されると、常にブリッジ ID も変化します。この結果、VLAN のルート ブリッジが再計算されます。

指定された VLAN のルート ブリッジになるようにスイッチを設定するには、spanning-tree vlan vlan-ID root コマンドを入力して、ブリッジ プライオリティをデフォルト値(32,768)から非常に 小さな値へと変更します。指定された VLAN のブリッジ プライオリティに設定する 8192 は、この 値によってスイッチが VLAN のルートになる場合に使用します。 VLAN のブリッジのプライオリティが 8192 よりも低い場合、スイッチは最も低いブリッジ プライオリティより 1 小さい数値をプライオリティに設定します。

たとえば、ネットワークのすべてのスイッチが、VLAN 100 のブリッジ プライオリティにデフォルト値の 32,768 を設定していると仮定します。スイッチに spanning-tree vlan 100 root primary コマンドを指定すると、VLAN 100 のブリッジ プライオリティが 8192 に設定されるため、このスイッチは VLAN 100 のルート ブリッジになります。



スパニングツリーの各インスタンスのルート ブリッジは、バックボーン スイッチまたはディストリビューション スイッチである必要があります。アクセス スイッチをスパニングツリーのプライマリルートとして設定しないでください。

レイヤ 2 ネットワークの直径(ネットワーク上の任意の 2 つのエンド ステーション間における最大ブリッジ ホップ数)を指定するには、diameter キーワードを指定します。ネットワークの直径を指定すると、スイッチは自動的に最適な hello タイム、転送遅延時間、その直径のネットワークの最大エージング タイムをピックアップします。これによって、スパニングツリーのコンバージェンス時間が大幅に短縮されます。

hello-time キーワードを使用して、自動的に計算される hello タイムを上書きできます。



スイッチをルート ブリッジとして設定したあとで、hello タイム、転送遅延時間、および最大エージング タイムを手動で設定しないでください。

スイッチをルートスイッチとして設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# [no] spanning-tree vlan vlan_ID root primary [diameter hops	スイッチをルート ブリッジとして設定します。
	[hello-time seconds]]	デフォルトの設定に戻すには、no キーワードを使用しま
		す。
ステップ 2	Switch(config)# end	コンフィギュレーション モードを終了します。

次に、スイッチを VLAN~10~0ルート ブリッジとして設定し、ネットワーク直径を 4~ に設定する例を示します。

Switch# configure terminal
Switch(config)# spanning-tree vlan 10 root primary diameter 4
Switch(config)# end
Switch#

次に、スイッチがスパニングツリー ルートになったときに設定が変わる例を示します。次に示すのは、スイッチが VLAN 1 のルートになる前の設定です。

Switch#show spanning-tree vlan 1

VLAN1 is executing the ieee compatible Spanning Tree protocol Bridge Identifier has priority 32768, address 0030.94fc.0a00 Configured hello time 2, max age 20, forward delay 15 Current root has priority 32768, address 0001.6445.4400 Root port is 323 (FastEthernet6/3), cost of root path is 19 Topology change flag not set, detected flag not set Number of topology changes 2 last change occurred 00:02:19 ago from FastEthernet6/1 Times: hold 1, topology change 35, notification 2 hello 2, max age 20, forward delay 15 Timers:hello 0, topology change 0, notification 0, aging 300 Port 323 (FastEthernet6/3) of VLAN1 is forwarding Port path cost 19, Port priority 128, Port Identifier 129.67. Designated root has priority 32768, address 0001.6445.4400 Designated bridge has priority 32768, address 0001.6445.4400 Designated port id is 129.67, designated path cost 0 Timers:message age 2, forward delay 0, hold 0 Number of transitions to forwarding state:1 BPDU:sent 3, received 91 Port 324 (FastEthernet6/4) of VLAN1 is blocking Port path cost 19, Port priority 128, Port Identifier 129.68. Designated root has priority 32768, address 0001.6445.4400 Designated bridge has priority 32768, address 0001.6445.4400 Designated port id is 129.68, designated path cost 0 Timers:message age 2, forward delay 0, hold 0 $\,$ Number of transitions to forwarding state:0 BPDU:sent 1, received 89

スイッチをルートとして設定します。

```
Switch# configure terminal
Switch(config)# spanning-tree vlan 1 root primary
Switch(config)# spanning-tree vlan 1 root primary
VLAN 1 bridge priority set to 8192
VLAN 1 bridge max aging time unchanged at 20
VLAN 1 bridge hello time unchanged at 2
VLAN 1 bridge forward delay unchanged at 15
Switch(config)# end
```

次に示すのは、スイッチがルートになったあとの設定です。

Switch# show spanning-tree vlan 1

```
VLAN1 is executing the ieee compatible Spanning Tree protocol
 Bridge Identifier has priority 8192, address 0030.94fc.0a00
 Configured hello time 2, max age 20, forward delay 15
  We are the root of the spanning tree
 Topology change flag set, detected flag set
  Number of topology changes 3 last change occurred 00:00:09 ago
  Times: hold 1, topology change 35, notification 2
         hello 2, max age 20, forward delay 15
 Timers:hello 0, topology change 25, notification 0, aging 15
Port 323 (FastEthernet6/3) of VLAN1 is forwarding
  Port path cost 19, Port priority 128, Port Identifier 129.67.
  Designated root has priority 8192, address 0030.94fc.0a00
  Designated bridge has priority 8192, address 0030.94fc.0a00
  Designated port id is 129.67, designated path cost 0
  Timers:message age 0, forward delay 0, hold 0
  Number of transitions to forwarding state:1
  BPDU:sent 9, received 105
 Port 324 (FastEthernet6/4) of VLAN1 is listening
  Port path cost 19, Port priority 128, Port Identifier 129.68.
   Designated root has priority 8192, address 0030.94fc.0a00
  Designated bridge has priority 8192, address 0030.94fc.0a00
  Designated port id is 129.68, designated path cost 0
  Timers:message age 0, forward delay 5, hold 0
  Number of transitions to forwarding state:0
  BPDU:sent 6, received 102
```

Switch#



ブリッジ プライオリティが 8192 に設定されたため、このスイッチがスパニングツリーのルートになります。

セカンダリ ルート スイッチの設定

スイッチをセカンダリ ルートとして設定すると、スパニングツリー ブリッジ プライオリティはデフォルト値 (32,768) から 16,384 に変更されます。その結果、プライマリ ルート ブリッジが故障した場合に(ネットワーク上のほかのスイッチがデフォルトのブリッジ プライオリティ 32,768 を使用していることが前提)、そのスイッチが指定された VLAN のルート ブリッジになる可能性が高くなります。

このコマンドを複数のスイッチに対して実行し、複数のバックアップ ルート スイッチを設定できます。プライマリ ルート スイッチを設定するときに使用したものと同じネットワーク直径および hello タイムを使用してください。



スイッチをルート ブリッジとして設定したあとで、hello タイム、転送遅延時間、および最大エー ジング タイムを手動で設定しないでください。

スイッチをセカンダリ ルート スイッチとして設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# [no] spanning-tree vlan vlan ID root secondary [diameter hops	スイッチをセカンダリ ルート スイッチとして設定します。
	[hello-time seconds]]	デフォルトの設定に戻すには、no キーワードを使用します。
ステップ 2	Switch(config)# end	コンフィギュレーション モードを終了します。

次に、スイッチを VLAN 10 のセカンダリ ルート スイッチとして設定し、ネットワーク直径を 4 に 設定する例を示します。

Switch# configure terminal Switch(config) # spanning-tree vlan 10 root secondary diameter 4 VLAN 10 bridge priority set to 16384 ${\tt VLAN~10~bridge~max~aging~time~set~to~14}$ VLAN 10 bridge hello time unchanged at 2

VLAN 10 bridge forward delay set to 10 Switch(config)# end

Switch#

次に、VLAN 1 の設定を確認する例を示します。

Switch#sh spanning-tree vlan 1

VLAN0001

Spanning tree enabled protocol ieee

Root ID Priority 32768

Address 0003.6b10.e800 This bridge is the root

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768

> Address 0003.6b10.e800

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 300

terface	Role Sts	Cost	Prio.Nbr	Status
3/2	Desg FWD Desg FWD	19	128.129 128.130 128.176	P2p

Switch#

STP ポート プライオリティの設定

ループが発生した際、スパニングツリーはフォワーディング ステートに移行するインターフェイス を選択する場合にポート プライオリティを考慮します。スパニングツリーで最初に選択するインターフェイスに高いプライオリティ値を、最後に選択するインターフェイスに低いプライオリティ 値を割り当てることができます。すべてのインターフェイスが同じプライオリティ値を使用している場合、スパニングツリーはインターフェイス番号が最も小さいインターフェイスをフォワーディング ステートにして、残りのインターフェイスをブロックします。指定できるプライオリティの範囲は $0 \sim 240$ で、16 ずつ増分して設定できます(デフォルトは 128)。



Cisco IOS ソフトウェアは、インターフェイスがアクセス ポートとして設定されている場合には ポート プライオリティ値を使用し、インターフェイスがトランク ポートとして設定されている場合には VLAN ポート プライオリティ値を使用します。

インターフェイスのスパニングツリー ポート プライオリティを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	<pre>Switch(config)# interface {{fastethernet gigabitethernet tengigabitethernet} slot/port} {port-channel port_channel_number}</pre>	設定するインターフェイスを選択します。
ステップ 2	Switch(config-if)# [no] spanning-tree port-priority port_priority	インターフェイスのポート プライオリティを設定します。指定できる $port_priority$ 値の範囲は $0\sim240$ で、 16 ずつ増分できます。
		デフォルトの設定に戻すには、no キーワードを使用します。
ステップ 3	Switch(config-if)# [no] spanning-tree vlan vlan_ID port-priority port_priority	インターフェイスのVLANポート プライオリティを 設定します。指定できる <i>port_priority</i> 値の範囲は 0 ~ 240 で、16 ずつ増分できます。
		デフォルトの設定に戻すには、no キーワードを使用します。
ステップ 4	Switch(config-if)# end	コンフィギュレーション モードを終了します。
ステップ 5	Switch# show spanning-tree interface {{fastethernet gigabitethernet} slot/port} {port-channel port_channel_number} show spanning-tree vlan vlan_ID	設定を確認します。

次に、ファスト イーサネット インターフェイスのスパニングツリー ポート プライオリティを設定する例を示します。

Switch# configure terminal
Switch(config)# interface fastethernet 5/8
Switch(config-if)# spanning-tree port-priority 100
Switch(config-if)# end
Switch#

次に、ファスト イーサネット インターフェイスをアクセス ポートとして設定した場合の、設定を 確認する例を示します。

Switch# show spanning-tree interface fastethernet 3/1

```
Vlan
             Role Sts Cost
                             Prio.Nbr Status
 ______
                             128.129 P2p
             Desg FWD 19
VT.AN0001
VLAN1002
            Desg FWD 19
                            128.129 P2p
                            128.129 P2p
VI.AN1003
            Desg FWD 19
VT.AN1004
             Desg FWD 19
                             128.129 P2p
VLAN1005
             Desg FWD 19
                             128.129 P2p
Switch#
```

次に、インターフェイスをアクセス ポートとして設定した場合の、インターフェイスの設定の詳細

```
を表示する例を示します。
Switch# show spanning-tree interface fastethernet 3/1 detail
Port 129 (FastEthernet3/1) of VLAN0001 is forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.129.
  Designated root has priority 32768, address 0003.6b10.e800
  Designated bridge has priority 32768, address 0003.6b10.e800
  Designated port id is 128.129, designated path cost 0
  Timers:message age 0, forward delay 0, hold 0
  Number of transitions to forwarding state:1
  Link type is point-to-point by default
  BPDU:sent 187, received 1
 Port 129 (FastEthernet3/1) of VLAN1002 is forwarding
  Port path cost 19, Port priority 128, Port Identifier 128.129.
  Designated root has priority 32768, address 0003.6b10.ebe9
  Designated bridge has priority 32768, address 0003.6b10.ebe9
  Designated port id is 128.129, designated path cost 0
  Timers:message age 0, forward delay 0, hold 0
  Number of transitions to forwarding state:1
  Link type is point-to-point by default
  BPDU:sent 94, received 2
 Port 129 (FastEthernet3/1) of VLAN1003 is forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.129.
  Designated root has priority 32768, address 0003.6b10.ebea
  Designated bridge has priority 32768, address 0003.6b10.ebea
  Designated port id is 128.129, designated path cost 0
  Timers:message age 0, forward delay 0, hold 0
  Number of transitions to forwarding state:1
  Link type is point-to-point by default
  BPDU:sent 94, received 2
 Port 129 (FastEthernet3/1) of VLAN1004 is forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.129.
  Designated root has priority 32768, address 0003.6b10.ebeb
  Designated bridge has priority 32768, address 0003.6b10.ebeb
  Designated port id is 128.129, designated path cost 0
  Timers:message age 0, forward delay 0, hold 0
  Number of transitions to forwarding state:1
  Link type is point-to-point by default
  BPDU:sent 95, received 2
 Port 129 (FastEthernet3/1) of VLAN1005 is forwarding
  Port path cost 19, Port priority 128, Port Identifier 128.129.
   Designated root has priority 32768, address 0003.6b10.ebec
  Designated bridge has priority 32768, address 0003.6b10.ebec
  Designated port id is 128.129, designated path cost 0
  Timers:message age 0, forward delay 0, hold 0
  Number of transitions to forwarding state:1
  Link type is point-to-point by default
```

BPDU:sent 95, received 2

Switch#



show spanning-tree port-priority コマンドは、リンクがアクティブになっているポートの情報のみを表示します。リンクがアクティブなポートがない場合は、show running-config interface コマンドを使用して設定を確認してください。

次に、ファスト イーサネット インターフェイスのスパニングツリー VLAN ポート プライオリティを設定する例を示します。

Switch# configure terminal
Switch(config) # interface fastethernet 5/8
Switch(config-if) # spanning-tree vlan 200 port-priority 64
Switch(config-if) # end
Switch#

次に、インターフェイスの VLAN 200 をトランク ポートとして設定した場合の設定を確認する例を示します。

Switch# **show spanning-tree vlan 200** <テキスト出力は省略>

Port 264 (FastEthernet5/8) of VLAN200 is forwarding
Port path cost 19, Port priority 64, Port Identifier 129.8.

Designated root has priority 32768, address 0010.0d40.34c7
Designated bridge has priority 32768, address 0010.0d40.34c7
Designated port id is 128.1, designated path cost 0
Timers: message age 2, forward delay 0, hold 0
Number of transitions to forwarding state: 1
BPDU: sent 0, received 13513

<テキスト出力は省略> Switch#

STP ポート コストの設定

スパニングツリー ポート パス コストのデフォルト値には、インターフェイス メディア速度の値が使用されます。ループが発生した場合、スパニングツリーはフォワーディング ステートに移行する インターフェイスを選択する際にポート コストを考慮します。スパニングツリーで最初に選択する インターフェイスに低いコスト値を、最後に選択するインターフェイスに高いコスト値を割り当て ることができます。すべてのインターフェイスが同じコスト値を使用している場合、スパニングツリーは、インターフェイス番号が最も小さいインターフェイスをフォワーディング ステートにして、残りのインターフェイスをブロックします。指定できるコストの範囲は、1 ~ 200,000,000 です (デフォルトは、メディアによって異なります)。

スパニングツリーはインターフェイスがアクセス ポートとして設定されている場合にはポート コスト値を使用し、インターフェイスがトランク ポートとして設定されている場合には VLAN ポート コスト値を使用します。

インターフェイスのスパニングツリー ポート コストを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# interface {{fastethernet gigabitethernet tengigabitethernet} slot/port} {port-channel port_channel_number}	設定するインターフェイスを選択します。
ステップ 2	<pre>Switch(config-if)# [no] spanning-tree cost port_cost</pre>	インターフェイスのポート コストを設定します。 port_cost 値は、1 ~ 200,000,000 の範囲で指定します。
		デフォルトの設定に戻すには、no キーワードを使用 します。
ステップ 3	<pre>Switch(config-if)# [no] spanning-tree vlan vlan_ID cost port_cost</pre>	インターフェイスのVLANポート コストを設定します。 $port_cost$ 値は、 $1 \sim 200,000,000$ の範囲で指定します。
		デフォルトの設定に戻すには、no キーワードを使用します。
ステップ 4	Switch(config-if)# end	コンフィギュレーション モードを終了します。
ステップ 5	Switch# show spanning-tree interface {{fastethernet gigabitethernet} slot/port} {port-channel port_channel_number} show spanning-tree vlan vlan_ID	設定を確認します。

次に、ファスト イーサネット インターフェイスのスパニングツリー ポート コストを変更する例を示します。

Switch# configure terminal
Switch(config)# interface fastethernet 5/8
Switch(config-if)# spanning-tree cost 18
Switch(config-if)# end
Switch#

次に、インターフェイスをアクセスポートとして設定した場合の設定を確認する例を示します。

```
Switch# show spanning-tree interface fastethernet 5/8

Port 264 (FastEthernet5/8) of VLAN200 is forwarding

Port path cost 18, Port priority 100, Port Identifier 129.8.

Designated root has priority 32768, address 0010.0d40.34c7

Designated bridge has priority 32768, address 0010.0d40.34c7

Designated port id is 128.1, designated path cost 0

Timers: message age 2, forward delay 0, hold 0

Number of transitions to forwarding state: 1

BPDU: sent 0, received 13513

Switch#
```

次に、ファスト イーサネット インターフェイスのスパニングツリー VLAN ポート コストを設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/8
Switch(config-if)# spanning-tree vlan 200 cost 17
Switch(config-if)# end
Switch#
```

次に、インターフェイスの VLAN 200 をトランク ポートとして設定した場合の設定を確認する例を示します。

Switch# show spanning-tree vlan 200

< テキスト出力は省略 >

Port 264 (FastEthernet5/8) of VLAN200 is forwarding
Port path cost 17, Port priority 64, Port Identifier 129.8.

Designated root has priority 32768, address 0010.0d40.34c7
Designated bridge has priority 32768, address 0010.0d40.34c7
Designated port id is 128.1, designated path cost 0
Timers: message age 2, forward delay 0, hold 0
Number of transitions to forwarding state: 1
BPDU: sent 0, received 13513

< テキスト出力は省略 >

Switch#



(注)

show spanning-tree コマンドは、リンクがアクティブになっている(グリーンに点灯)ポートの情報のみを表示します。リンクがアクティブなポートがない場合は、show running-config コマンドを使用して設定を確認してください。

VLAN のブリッジ プライオリティの設定



(注)

VLAN のブリッジ プライオリティを設定する場合は、注意が必要です。ブリッジ プライオリティを変更するには、通常の場合、spanning-tree vlan vlan_ID root primary コマンドおよび spanning-tree vlan vlan_ID root secondary コマンドの使用を推奨します。

VLAN のスパニングツリー ブリッジ プライオリティを設定するには、次の作業を行います。

	コマンド	目的			
ステップ 1 Switch(config)# [no] spanning-tree vlan vlan_ID priority bridge_priority		VLAN のブリッジ プライオリティを設定します。 bridge_priority 値は、1 ~ 65,534 の範囲で指定します。			
		デフォルトの設定に戻すには、no キーワードを使用します。			
ステップ 2	Switch(config)# end	コンフィギュレーション モードを終了します。			
ステップ 3	Switch# show spanning-tree vlan vlan_ID bridge [brief]	設定を確認します。			

次に、VLAN 200 のブリッジ プライオリティを 33,792 に設定する例を示します。

Switch# configure terminal
Switch(config)# spanning-tree vlan 200 priority 33792
Switch(config)# end
Switch#

次に、設定を確認する例を示します。

Switch# show spanning-tree vlan 200 bridge brief

			петто	max	rwa	
Vlan		Bridge ID	Time	Age	Delay	Protocol
VLAN200	33792	0050.3e8d.64c8	2	20	15	ieee
Switch#						

hello タイムの設定



(注)

hello タイムを設定する場合は、注意が必要です。hello タイムを変更するには、通常の場合 **spanning-tree vlan** *vlan_ID* **root primary** コマンドおよび **spanning-tree vlan** *vlan_ID* **root secondary** コマンドの使用を推奨します。

VLAN のスパニングツリー hello タイムを設定するには、次の作業を行います。

	コマンド	目的			
ステップ 1	Switch(config)# [no] spanning-tree vlan vlan_ID hello-time hello_time	VLAN の hello タイムを設定します。 <i>hello_time</i> 値は、1 ~ 10 秒の範囲で指定します。			
		デフォルトの設定に戻すには、no キーワードを使用します。			
ステップ 2	Switch(config)# end	コンフィギュレーション モードを終了します。			
ステップ 3	Switch# show spanning-tree vlan vlan_ID bridge [brief]	設定を確認します。			

次に、VLAN 200 の hello タイムを 7 秒に設定する例を示します。

Switch# configure terminal
Switch(config)# spanning-tree vlan 200 hello-time 7
Switch(config)# end
Switch#

次に、設定を確認する例を示します。

 ${\tt Switch\#} \ \ \textbf{show spanning-tree vlan 200 bridge brief}$

			Hello	Max	Fwd	
Vlan		Bridge ID	Time	Age	Delay	Protocol
VLAN200	49152	0050.3e8d.64c8	7	20	15	ieee
Switch#						

VLAN の最大エージング タイムの設定



(注)

エージング タイムを設定する場合は、注意が必要です。最大エージング タイムを変更するには、通常の場合、spanning-tree vlan *vlan_ID* root primary コマンドおよび spanning-tree vlan *vlan_ID* root secondary コマンドの使用を推奨します。

VLAN のスパニングツリー最大エージング タイムを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# [no] spanning-tree vlan vlan_ID max-age max_age	$VLAN$ の最大エージング タイムを設定します。 max_age 値は、 $6 \sim 40$ 秒の範囲で指定します。
		デフォルトの設定に戻すには、no キーワードを 使用します。
ステップ 2	Switch(config)# end	コンフィギュレーション モードを終了します。
ステップ 3	Switch# show spanning-tree vlan vlan_ID bridge [brief]	設定を確認します。

次に、VLAN 200 の最大エージング タイムを 36 秒に設定する例を示します。

Switch# configure terminal
Switch(config)# spanning-tree vlan 200 max-age 36
Switch(config)# end
Switch#

次に、設定を確認する例を示します。

Switch# show spanning-tree vlan 200 bridge brief

			Hello	Max	Fwd	
Vlan		Bridge ID	Time	Age	Delay	Protocol
VLAN200	49152	0050.3e8d.64c8	2	36	15	ieee
Switch#						

VLAN の転送遅延時間の設定



(注)

転送遅延時間を設定する場合は、注意が必要です。転送遅延時間を変更するには、通常の場合、spanning-tree vlan *vlan_ID* root primary コマンドおよび spanning-tree vlan *vlan_ID* root secondary コマンドの使用を推奨します。

VLAN のスパニングツリー転送遅延時間を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# [no] spanning-tree vlan vlan_ID forward-time forward_time	VLAN の転送時間を設定します。forward_time 値は、4 ~ 30 秒の範囲で指定します。
		デフォルトの設定に戻すには、no キーワードを 使用します。
ステップ 2	Switch(config)# end	コンフィギュレーション モードを終了します。
ステップ 3	Switch# show spanning-tree vlan vlan_ID bridge [brief]	設定を確認します。

次に、VLAN 200 の転送遅延時間を 21 秒に設定する例を示します。

Switch# configure terminal
Switch(config)# spanning-tree vlan 200 forward-time 21
Switch(config)# end
Switch#

次に、設定を確認する例を示します。

Switch# show spanning-tree vlan 200 bridge brief

			петто	Max	rwa	
Vlan		Bridge ID	Time	Age	Delay	Protocol
VLAN200	49152	0050.3e8d.64c8	2	20	21	ieee
Switch#						

次に、ブリッジのスパニングツリー情報を表示する例を示します。

Switch# show spanning-tree bridge

		Hello	Max	Fwd	
Vlan	Bridge ID	Time	Age	Dly	Protocol
VLAN200	49152 0050.3e8d.64c8	2	20	15	ieee
VLAN202	49152 0050.3e8d.64c9	2	20	15	ieee
VLAN203	49152 0050.3e8d.64ca	2	20	15	ieee
VLAN204	49152 0050.3e8d.64cb	2	20	15	ieee
VLAN205	49152 0050.3e8d.64cc	2	20	15	ieee
VLAN206	49152 0050.3e8d.64cd	2	20	15	ieee
Switch#					

STP のディセーブル化

VLAN 単位でスパニングツリーをディセーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# no spanning-tree vlan vlan_ID	VLAN 単位でスパニングツリーをディセーブルにし
		ます。
ステップ 2	Switch(config)# end	コンフィギュレーション モードを終了します。
ステップ 3	Switch# show spanning-tree vlan vlan_ID	スパニングツリーがディセーブルになっていること
		を確認します。

次に、VLAN 200 上でスパニングツリーをディセーブルにする例を示します。

Switch# configure terminal
Switch(config)# no spanning-tree vlan 200
Switch(config)# end
Switch#

次に、設定を確認する例を示します。

Switch# show spanning-tree vlan 200 Spanning tree instance for VLAN 200 does not exist. Switch#

PVRST+ のイネーブル化

PVRST+ は、既存の PVST+ フレームワークを設定および他の機能との相互作用に使用しています。 また、PVST+ 拡張機能の一部をサポートします。

PVRST+を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# [no] spantree mode rapid-pvst	Rapid-PVST+ をイネーブルにします。
ステップ 2	Switch(config)# interface interface/port	インターフェイス コンフィギュレーション モード に切り替えます。
ステップ 3	Switch(config)# spanning-tree link-type point-to-point	ポートのリンク タイプをポイントツーポイント モードに設定します。
ステップ 4	Switch(config-if)# exit	インターフェイス モードを終了します。
ステップ 5	Switch(config)# exit	コンフィギュレーション モードを終了します。
ステップ 6	Switch(config-if)# clear spantree detected-protocols mod/port	ポート上のすべてのレガシー ブリッジを検出します。
ステップ 7	Switch# show spanning-tree summary total	Rapid-PVST+ 設定を確認します。

次に、Rapid-PVST+を設定する例を示します。

```
Switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# spanning-tree mode rapid-pvst
Switch(config)# int fa 6/4
Switch(config-if)# spanning-tree link-type point-to-point
Switch(config-if)# end
Switch(config)# end
Switch#
23:55:32:%SYS-5-CONFIG_I:Configured from console by console
Switch# clear spanning-tree detected-protocols
```

次に、設定を確認する例を示します。

```
Switch# show spanning-tree summary totals
Switch is in rapid-pvst mode
Root bridge for:VLAN0001
Extended system ID
                       is disabled
                        is disabled
Portfast Default
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default
                        is disabled
EtherChannel misconfig guard is enabled
UplinkFast
                        is disabled
BackboneFast
                        is disabled
Pathcost method used
                       is short
                  Blocking Listening Learning Forwarding STP Active
1 vlan
                               0
                                       0
Switch#
```

リンク タイプの指定

高速接続が確立されるのは、ポイントツーポイント リンク上に限られます。スパニングツリーは、ポイントツーポイント リンクをスパニングツリー アルゴリズムを実行する 2 つのスイッチだけを接続するセグメントとみなします。スイッチは、すべての全二重リンクをポイントツーポイント リンクとしてみなし、半二重リンクを共有リンクとみなすため、明示的なリンク タイプの設定を回避できます。特定のリンク タイプを設定するには、spanning-tree linktype コマンドを使用します。

プロトコル移行の再開

Multiple Spanning-Tree Protocol (MSTP) および RSTP の両方が稼働するスイッチは、組み込み型のプロトコル移行プロセスをサポートし、レガシー 802.1D スイッチとの相互運用が可能となります。このスイッチがレガシー 802.1D 設定 BPDU (プロトコルのバージョンが 0 に設定されている BPDU) を受信した場合は、そのポート上で 802.1D BPDU だけを送信します。さらに、MSTP スイッチがレガシー BPDU を受信する場合、次の事項も検出します。

- ポートがリージョンの境界にある
- 異なるリージョンに関連付けられた MST BPDU (バージョン3)
- RST BPDU (バージョン 2)

ただし、スイッチは、802.1D BPDU を受信しなくなった場合であっても、自動的に MSTP モードに は戻りません。これは、レガシー スイッチが指定スイッチでなければ、リンクから削除されたかど うかを判別できないためです。また、あるスイッチの接続先のスイッチがリージョンに加入した場合でも、このスイッチはポートに境界の役割を割り当て続けることもあります。

スイッチ全体でプロトコル移行プロセスを再開する(強制的に近接スイッチと再度ネゴシエートさせる)には、特権 EXEC モードで clear spanning-tree detected-protocols コマンドを使用します。特定のインターフェイス上でプロトコル移行プロセスを再開するには、*interface-id* 特権 EXEC モードで clear spanning-tree detected-protocols interface コマンドを使用します。

MST の概要

ここでは、Catalyst 4000 ファミリ スイッチにおける MST の機能について説明します。

- IEEE 802.1s MST (p.17-25)
- IEEE 802.1w RSTP (p.17-26)
- MST/SST 間のインターオペラビリティ (p.17-28)
- CST (p.17-29)
- MSTI (p.17-29)
- MST のコンフィギュレーション パラメータ (p.17-29)
- MST リージョン (p.17-29)
- メッセージ エージおよびホップ カウント (p.17-31)
- MST/PVST+ 間のインターオペラビリティ(p.17-31)

IEEE 802.1s MST

MST は、IEEE 802.1w Rapid Spanning-Tree (RST)アルゴリズムを複数のスパニングツリーに拡張します。この拡張によって、VLAN 環境で高速コンバージェンスとロード バランシングの両方を実現できます。MST は Per VLAN Spanning-Tree Plus (PVST+)よりもコンバージェンスが速く、802.1D Spanning-Tree Protocol (STP; スパニングツリー プロトコル) 802.1w (Rapid Spanning-Tree Protocol [RSTP]) およびシスコ PVST+ アーキテクチャに対して下位互換性があります。

MST を使用すると、トランクを介して複数のスパニングツリーを構築できます。VLAN をグループとしてまとめ、スパニングツリー インスタンスに対応付けることができます。各インスタンスに、他のスパニングツリー インスタンスに依存しないトポロジを与えることができます。このアーキテクチャによって、データ トラフィックに複数の転送パスが与えられ、ロード バランシングが可能になります。あるインスタンス(転送パス)で障害が発生しても、他のインスタンスに影響を与えないので、ネットワークの耐障害性が向上します。

大規模なネットワークで、ネットワーク管理が容易になり、ネットワークのさまざまな部分にさまざまな VLAN を配置し、スパニングツリー インスタンスを割り当てることによって、冗長パスを使用できます。スパニングツリー インスタンスが存在できるのは、矛盾しない VLAN インスタンスが割り当てられているブリッジに限られます。1 組のブリッジを同じ MST 設定情報を使用して設定する必要があります。この結果、特定のスパニングツリー インスタンス セットに参加させることができます。同じ MST コンフィギュレーションが与えられて相互接続されたブリッジは、MST リージョンといいます。

MST は修正済みの RSTP、MSTP を使用します。MST には次のような特徴があります。

- MST は Internal Spanning-Tree(IST)という形式のスパニングツリーを実行します。IST は、MST リージョンに関する内部情報によって Common Spanning-Tree(CST)情報を補います。MST リージョンは、隣接する Single Spanning-Tree(SST)および MST リージョンで、単一ブリッジとして認識されます。
- MST が稼働しているブリッジは、次のように、SST ブリッジとのインターオペラビリティを確保します。
 - MST ブリッジは IST を実行し、MST リージョンに関する内部情報によって、CST 情報を補います。
 - IST はリージョン内のすべての MST ブリッジを結合するので、そのブリッジ ドメイン全体 が含まれる CST では、1 つのサブツリーとして認識されます。 MST リージョンは、隣接する SST ブリッジおよび MST リージョンにとって、仮想ブリッジとして認識されます。

- Common and Internal Spanning-Tree (CIST) は、各 MST リージョンの IST、MST リージョンと相互接続する CST、および SST ブリッジの要素の集まりです。CIST は MST リージョン内部の IST、および MST リージョン外部の CST と同一です。STP、RSTP、および MSTP は合同で、1 つのブリッジを CIST のルートとして選定します。
- MST は各 MST リージョン内で、追加のスパニングツリーを確立して維持します。これらのスパニングツリーを MST Instance (MSTI) といいます。IST の番号は 0、MSTI の番号は 1、2、3 (以下同様)になります。MSTI は MST リージョンに対してローカルで、MST リージョンが相互接続されている場合でも、他のリージョンの MSTI とは無関係です。

MSTI は次のように、MST リージョン境界で IST と結合し、CST になります。

- MSTI のスパニングツリー情報が MSTP レコード (M レコード)に格納されます。
 M レコードは常に、MST BPDU 内でカプセル化されます。MSTP で計算されたオリジナルのスパニングツリーは、MST リージョン内でのみアクティブとなり、M ツリーと呼ばれます。M ツリーは MST リージョン境界で IST と組み合わされ、CST を形成します。
- MST は、非 CST VLAN 用の PVST+ BPDU を生成し、PVST+ とのインターオペラビリティを維持します。
- MST は次のように、MSTP の PVST+ 拡張機能の一部をサポートします。
 - UplinkFast および BackboneFast は、MST モードで使用できません。これらは RSTP に組み 込まれています。
 - PortFast はサポートされています。
 - BPDU フィルタおよび BPDU ガードは、MST モードでサポートされています。
 - ループ ガードおよびルート ガードは MST でサポートされています。MST は、BPDU が引き続き VLAN 1 で送信される点を除き、VLAN 1 でディセーブルの機能をそのままの状態で維持します。
 - MST スイッチは、MAC (メディア アクセス制御)縮小がイネーブルの場合と同様に動作します。
 - Private VLAN (PVLAN) の場合、セカンダリ VLAN をプライマリと同じインスタンスにマッピングする必要があります。

IEEE 802.1w RSTP

802.1w で規定されている RSTP は、802.1D で規定された STP に代わるものですが、STP との互換性は維持されています。RSTP は、MST 機能とともに設定します。詳細については、「MST の設定」 (p.17-33) を参照してください。

MST は RSTP が提供する構造上で動作し、物理トポロジまたは設定パラメータが変更されたときにネットワークのアクティブなトポロジを再設定する時間を短縮します。RSTP は、スパニングツリーに接続されたアクティブ トポロジのルートとしてスイッチを 1 つ選択し、スイッチの個々のポートに、そのポートがアクティブ トポロジに含まれるかどうかに応じて、ポートの役割を割り当てます。

RSTP はスイッチ、スイッチ ポート、または LAN 障害の発生後に、短時間で接続できるようにします。新しいルート ポートとブリッジの反対側の指定ポートが、両者間の明示的ハンドシェイクによってフォワーディング ステートに移行します。RSTP を使用すると、スイッチの再初期化時にポートが直接フォワーディング ステートに移行できるように、スイッチ ポートを設定できます。

RSTP は、802.1D ブリッジに対して次のような下位互換性があります。

- RSTP はポート単位で、802.1D で設定された BPDU および Topology Change Notification (TCN; トポロジ変更通知) BPDU を選択して送信します。
- ポートの初期化時に、移行遅延タイマーが開始され、RSTP BPDU が送信されます。移行遅延タイマーがアクティブな間、ブリッジはそのポートで受信したすべての BPDU を処理します。
- ポートの移行遅延タイマーが満了したあとでブリッジが 802.1D BPDU を受信した場合、ブリッジは 802.1D ブリッジに接続されているとみなして、802.1D BPDU だけを使用するようになります。

• RSTP がポート上で 802.1D BPDU を使用していて、移行遅延タイマーの満了後に RSTP BPDU を受信した場合、RSTP によって移行遅延タイマーが再起動され、そのポート上で RSTP BPDU の使用が開始されます。

RSTP のポートの役割

RSTP では、ポートの役割は次のように定義されます。

- ルート スパニングツリートポロジ用に選択された転送ポート
- 指定 すべてのスイッチド LAN セグメント用に選択された転送ポート
- 代替 現在のルート ポートによって提供されるルート ブリッジへの代替パス
- バックアップ スパニングツリーのリーフ近くで、指定ポートによって提供されるパスのバックアップ。バックアップ ポートが存在できるのは、2つのポートがループバックモードで、または共有LAN セグメントに対して複数の接続を持つブリッジで結合されている場合だけです。
- ディセーブル スパニング ツリーの動作において役割を持たないポート

ポートの役割は次のように割り当てられます。

- ルートポートまたは指定ポートの役割の場合、ポートはアクティブトポロジに含まれます。
- 代替ポートまたはバックアップ ポートの役割の場合、ポートはアクティブ トポロジから除外 されます。

RSTP ポート ステート

ポート ステートは、フォワーディングおよびラーニング プロセスを制御し、廃棄、ラーニング、およびフォワーディングの値を提供します。 表 17-5 に、STP ポート ステートと RSTP ポート ステートを示します。

表 17-5 STP ポート ステートおよび RSTP ポート ステートの比較

動作ステータス	STP ポート ステート	RSTP ポート ステート	アクティブ トポロジ にポートが含まれるか どうか
イネーブル	ブロッキング ¹	廃棄 ²	含まれない
イネーブル	リスニング	廃棄	含まれない
イネーブル	ラーニング	ラーニング	含まれる
イネーブル	フォワーディング	フォワーディング	含まれる
ディセーブル	ディセーブル	廃棄	含まれない

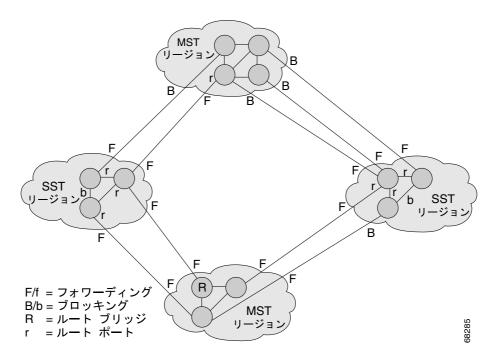
- 1. IEEE 802.1D のポート ステート指定
- 2. IEEE 802.1w のポート ステート指定。廃棄は、MST ではブロッキングと同じです。

RSTP は安定したトポロジで、すべてのルート ポートおよび指定ポートがフォワーディング ステートに移行し、すべての代替ポートおよびバックアップ ポートが必ず廃棄ステートになるようにします。

MST/SST 間のインターオペラビリティ

仮想ブリッジで結ばれた LAN には、SST ブリッジおよび MST ブリッジから構成される相互接続されたリージョンが含まれる場合があります。図 17-2 に、この関係を示します。





SST リージョンで稼働している STP において、MST リージョンは次のように動作する単一 SST または擬似ブリッジとして認識されます。

- すべての擬似ブリッジにおいて、BPDU のルート ID とルート パス コストの値は一致しますが、 擬似ブリッジは単一の SST ブリッジと次の点が異なります。
 - 擬似ブリッジの BPDU には、異なるブリッジ ID が与えられます。ルート ID とルート コストが同じなので、この相違が近接する SST リージョンの STP 動作に影響を与えることはありません。
 - 擬似ブリッジ ポートから送信された BPDU では、メッセージ有効期間が多少異なることがあります。 メッセージ エージはホップごとに 1 秒ずつ増えるので、 メッセージ エージの相違は秒単位で測定されます。
- 擬似ブリッジのあるポート(リージョン エッジにあるポート)から別のポートへのデータ トラフィックは、擬似ブリッジまたは MST リージョンに完全に含まれるパスをたどります。異なる VLAN に属するデータ トラフィックは、MST によって確立された MST リージョン内で異なるパスをたどる場合があります。
- システムは次のいずれかの方法でループの発生を防ぎます。
 - 境界上のフォワーディング ポートを 1 つ許可し、他のすべてのポートをブロックして、該当する擬似ブリッジ ポートをブロックします。
 - CST パーティションを設定して、SST リージョンのポートをブロックします。

CST

CST(802.1Q)は、すべての VLAN に対応する単一のスパニングツリーです。PVST+ が稼働してい る Catalyst 4500 シリーズ スイッチでは、VLAN 1 スパニングツリーが CST に対応します。MST が 稼働している Catalyst 4500 シリーズ スイッチでは、IST (インスタンス 0) が CST に対応します。

MSTI

このリリースは、最大 16 のインスタンスをサポートします。各スパニングツリー インスタンスは、 0 ~ 15 の範囲のインスタンス ID によって識別されます。インスタンス 0 は必須で、必ず存在しま す。インスタンス1~15の使用は任意です。

MST のコンフィギュレーション パラメータ

MST のコンフィギュレーションは次の3つの部分から構成されます。

- 名前 MST リージョンを特定する32文字のストリング(ヌルの埋め込みあり)
- リビジョン番号 現在の MST コンフィギュレーションのリビジョンを表す、符号なし 16 ビッ



(注) MST コンフィギュレーションの一部として必要な場合は、リビジョン番号を設定する 必要があります。リビジョン番号は、MST コンフィギュレーションを実行するたびに、 自動的に増えるわけではありません。

• MST コンフィギュレーション テーブル 4096 バイトの配列。各バイトは、符号なし整数とし て解釈され、VLAN に対応します。値は、VLAN を対応付けるインスタンス番号です。VLAN 0 に対応する先頭バイト、および VLAN 4095 に対応する 4096 番めのバイトは使用しません。 常に0に設定します。

各バイトを手動で設定する必要があります。SNMP(簡易ネットワーク管理プロトコル)またはCLI (コマンドラインインターフェイス)を使用して設定できます。

MST BPDU には、MST コンフィギュレーション ID およびチェックサムが入ります。MST ブリッ ジは、MST BPDU のコンフィギュレーション ID およびチェックサムが自身の MST リージョンのコ ンフィギュレーション ID およびチェックサムと一致した場合に限り、MST BPDU を受け入れます。 いずれかの値が異なる場合、その MST BPDU は SST BPDU とみなされます。

MST リージョン

ここでは、MST リージョンについて説明します。

- MST リージョンの概要 (p.17-30)
- 境界ポート (p.17-30)
- IST マスター (p.17-30)
- エッジ ポート (p.17-30)
- リンク タイプ (p.17-31)

MST リージョンの概要

同じ MST コンフィギュレーションが与えられ、相互接続されたブリッジを MST リージョンといい ます。ネットワークで使用できる MST リージョンの数に制限はありません。

MST リージョンを形成する場合、使用できるブリッジは次のどちらかです。

- MST リージョンの唯一のメンバである MST ブリッジ
- LAN によって相互接続された MST ブリッジ。LAN の指定ブリッジには、MST ブリッジと同じ MST コンフィギュレーションを与えます。LAN 上のすべてのブリッジが MST BPDU を処理します。

MST コンフィギュレーションが異なる 2 つの MST リージョンを接続した場合、MST リージョンは次のように動作します。

- ネットワークの冗長パス間でロード バランシングを図ります。2 つの MST リージョンが冗長 接続されている場合、すべてのトラフィックは MST リージョンとの単一接続を使用して、ネットワーク上を流れます。
- RSTP ハンドシェイクによって、リージョン間の高速接続を可能にします。ただし、このハンドシェイクは 2 つのブリッジ間の場合ほど高速ではありません。ループを防止するためには、リージョン内のすべてのブリッジが他のリージョンとの接続時に合意している必要があります。この状況によって遅延が生じるため、ネットワークを多数のリージョンに分割することは推奨できません。

境界ポート

境界ポートは LAN に接続するポートで、その指定ブリッジは SST ブリッジまたは異なる MST コンフィギュレーションのブリッジのどちらかです。指定ポートは、STP ブリッジを検出した場合、またはコンフィギュレーションの異なる RST/MST ブリッジから同意メッセージを受信した場合、境界上にあることを認識します。

境界では、MST ポートの役割に関係なく、ポート ステートが強制的に IST ポート ステートと同じになります。ポートに境界フラグが設定されている場合、MST ポート ロール選択メカニズムによって、境界にポートの役割が割り当てられ、IST ポートと同じステートが設定されます。境界の IST ポートは、バックアップ ポートの役割以外のすべてのポートの役割を担うことができます。

IST マスター

MST リージョンの IST マスターは最小ブリッジ ID を持ち、CST ルートに対するパス コストが最小のブリッジです。MST ブリッジが CST のルート ブリッジになっている場合は、それがその MST リージョンの IST マスターです。CST ルートが MST リージョン外にある場合は、境界上の MST ブリッジの 1 つが IST マスターとして選択されます。同じリージョンに属する境界上の他のブリッジは、ルートに接続する境界ポートを最終的にブロックします。

リージョン境界の複数のブリッジで、ルートへのパスがまったく同じ場合、わずかに小さいブリッジプライオリティを設定することで、特定のブリッジをISTマスターにすることができます。

リージョン内でのルート パス コストおよびメッセージ エージは一定のままですが、ホップごとに IST パス コストは増加し、IST 残りホップ数は減少します。show spanning-tree mst コマンドを入力 すると、IST マスター、パス コスト、ブリッジの残りホップ数に関する情報が表示されます。

エッジ ポート

非ブリッジング デバイス (ホスト、スイッチなど)に接続するポートが、エッジ ポートです。ハブに接続するポートも、ハブまたはハブによって接続された LAN にブリッジがない場合、エッジポートです。エッジ ポートは、リンクがアップになると同時に転送を開始します。

MST では各ポートをホストに接続する設定が必要です。障害発生後に高速で接続を確立するには、中間ブリッジの非エッジ指定ポートをブロックする必要があります。ポートが同意メッセージを送り返すことができる別のブリッジに接続した場合、そのポートはただちに転送を開始します。それ以外の場合、ポートが再び転送を開始するまでに、転送遅延時間の 2 倍の時間がかかります。ホストおよびスイッチに接続されたポートを MST 使用時のエッジ ポートとして、明示的に設定する必要があります。

誤って設定されることがないように、ポートが BPDU を受信すると、PortFast 動作がオフになります。**show spanning-tree mst** *interface* コマンドを使用すると、PortFast の設定および動作ステータスを表示できます。

リンク タイプ

高速接続が確立されるのは、ポイントツーポイント リンク上に限られます。ホストまたはスイッチに対して、ポートを明示的に設定する必要があります。ただし、大部分のネットワークでは、ケーブル接続がこの条件を満たしているので、spanning-tree linktype コマンドを入力し、すべての全二重リンクをポイントツーポイント リンクとして扱うことで、明示的設定を回避できます。

メッセージ エージおよびホップ カウント

IST および MSTI は、BPDU のメッセージ有効期間および最大エージング タイマーの設定値を使用しません。IST および MST は、IP Time to Live (TTL; 存続可能時間) メカニズムにきわめて類似した別個のホップ カウント メカニズムを使用します。最大ホップ カウントを指定して、各 MST ブリッジを設定できます。インスタンスのルート ブリッジは、最大ホップ カウントと同じ残りホップ カウントを指定して、BPDU (または M レコード)を送信します。BPDU (または M レコード)を受信したブリッジは、受信した残りのホップ カウントを 1 だけ減らします。この結果、カウントが 0 になった場合、ブリッジはこの BPDU (または M レコード)を廃棄し、ポートのために保持していた情報を期限切れにします。非ルート ブリッジは、生成した BPDU (または M レコード)で、減らされたカウントを残りのホップ カウントとして伝播します。

BPDU の RST 部分に指定されているメッセージ エージおよび最大エージング タイマーの設定値は、リージョン内のどこでも同じです。境界上にあるリージョンの指定ポートによって、同じ値が伝達されます。

MST/PVST+ 間のインターオペラピリティ

(同一リージョン内の)MST スイッチが PVST+ スイッチと対話するように設定する場合、次の注意事項に留意してください。

• MST リージョン内のすべての VLAN に対するルートを設定します。次の例を参照してください。

Switch# show spanning-tree mst interface gigabitethernet 1/1

```
GigabitEthernet1/1 of MST00 is root forwarding
                                        port guard : none
                                                                 (default)
Edge port: no
                        (trunk)
Link type: point-to-point (auto)
                                         bpdu filter: disable
                                                                 (default)
Boundary : boundary
                                         bpdu quard : disable
                                                                 (default)
Bpdus sent 10, received 310
                          Prio.Nbr Vlans mapped
Instance Role Sts Cost
        Root FWD 20000
                          128.1
                                   1-2,4-2999,4000-4094
       Boun FWD 20000 128.1 3,3000-3999
3
```

MST スイッチに属する境界ポートは、PVST+ をシミュレートし、すべての VLAN に PVST+ BPDU を送信します。

PVST+ スイッチ上でループ ガードをイネーブルにすると、MST スイッチの設定が変更されたときに、ポートが loop-inconsistent ステートに変化する可能性があります。 loop-inconsistent ステートを修正するには、その PVST+ スイッチでループ ガードをディセーブルにし、再びイネーブルにする必要があります。

• MST スイッチの PVST+ サイド内にある VLAN の一部またはすべてに対して、ルートを配置しないでください。 境界の MST スイッチが指定ポート上の VLAN のすべてまたは一部に対する PVST+ BPDU を受信すると、ルート ガードによってそのポートがブロッキング ステートになります。

PVST+ スイッチを 2 つの異なる MST リージョンに接続すると、PVST+ スイッチからのトポロジ変更が最初の MST リージョンから先へ伝達されません。この場合、トポロジ変更は VLAN がマッピングされているインスタンスで伝播されるだけです。トポロジ変更は最初の MST リージョンに対してローカルのままで、その他のリージョンの Cisco Access Manager (CAM) エントリはフラッシュされません。他の MST リージョンにもトポロジ変更が認識されるようにするには、IST に VLANをマッピングするか、またはアクセス リンクを介して 2 つのリージョンに PVST+ スイッチを接続します。

MST 設定時の注意事項および制約事項

設定時に問題が起こらないようにするため、次の制約事項と注意事項に従ってください。

- すべての PVST ブリッジのすべての VLAN でスパニングツリーをディセーブルにしないでく ださい。
- CST のルートとして PVST ブリッジを使用しないでください。
- アクセス リンクは VLAN を分割することがあるので、アクセス リンクでスイッチを接続しないでください。
- すべての PVST ルート ブリッジに、CST ルート ブリッジより低い (数値の大きい) プライオリティを設定してください。
- トランクがインスタンスにマッピングされたすべての VLAN を伝送するようにしてください。 そのインスタンスに対応する VLAN は絶対に伝送しないでください。
- 既存または新規の論理 VLAN ポートが多数関係する MST コンフィギュレーションは、メンテナンス ウィンドウで完了する必要があります。変更が追加(インスタンスへの新規 VLAN の追加、インスタンス間での VLAN の移動など)されるたびに、MST データベース全体が再初期化されるためです。

MST の設定

ここでは、MST の設定手順について説明します。

- MST のイネーブル化 (p.17-33)
- MSTI パラメータの設定 (p.17-35)
- MSTI ポート パラメータの設定 (p.17-36)
- プロトコル移行の再開 (p.17-36)
- MST コンフィギュレーションの表示 (p.17-37)

MST のイネーブル化

Catalyst 4500 上で MST をイネーブルにして設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# spanning-tree mode mst	MST モードを開始します。
ステップ 2	Switch(config)# spanning-tree mst configuration	MST コンフィギュレーション サブモードを開始します。
		MST コンフィギュレーションをクリアする場合は、 no キーワードを使用します。
ステップ 3	Switch(config-mst)# show current	現在の MST コンフィギュレーションを表示します。
ステップ 4	Switch(config-mst)# name name	MST リージョン名を設定します。
ステップ 5	Switch(config-mst)# revision revision_number	MST コンフィギュレーション リビジョン番号を設定します。
ステップ 6	Switch(config-mst)# instance instance_number vlan vlan_range	VLAN を MSTI にマッピングします。 vlan キーワードを指定しない場合、MSTI にマッピングされたすべての VLAN のマップを無効にするには、no キーワードを使用します。
		vlan キーワードを指定する場合、MSTI から指定された VLAN のマップを無効にするには、no キーワードを使用します。
ステップ 7	Switch(config-mst)# show pending	適用する新しい MST コンフィギュレーションを表示します。
ステップ 8	Switch(config-mst)# end	設定を適用し、MST コンフィギュレーション サブ モードを終了します。
ステップ 9	Switch# show spanning-tree mst configuration	現在の MST コンフィギュレーションを表示します。

次に、MST をイネーブルにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# spanning-tree mode mst
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# show current
Current MST configuration
Name
        []
Revision 0
Instance Vlans mapped
1-4094
0
Switch(config-mst) # name cisco
Switch(config-mst)# revision 2
Switch(config-mst)# instance 1 vlan 1
Switch(config-mst)# instance 2 vlan 1-1000
Switch(config-mst)# show pending
Pending MST configuration
Name
       [ciscol
Revision 2
Instance Vlans mapped
                        _____
        1001-4094
0
2
        1-1000
Switch(config-mst)# no instance 2
Switch(config-mst)# show pending
Pending MST configuration
Name [cisco]
Revision 2
Instance Vlans mapped
        1-4094
______
\textbf{Switch}(\texttt{config-mst}) \, \# \, \, \, \textbf{instance 1 vlan 2000-3000}
Switch(config-mst)# no instance 1 vlan 1500
Switch(config-mst)# show pending
Pending MST configuration
       [cisco]
Revision 2
Instance Vlans mapped
     1-1999,2500,3001-4094
       2000-2499,2501-3000
1
Switch(config-mst)# end
Switch(config) # no spanning-tree mst configuration
Switch(config)# end
Switch# show spanning-tree mst configuration
Name
       []
Revision 0
Instance Vlans mapped
0 1-4094
```

MSTI パラメータの設定

MSTI パラメータを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# spanning-tree mst X priority Y	MSTI のプライオリティを設定します。
ステップ 2	<pre>Switch(config)# spanning-tree mst X root [primary secondary]</pre>	MSTI のルートとしてブリッジを設定します。
ステップ 3	Switch(config)# Ctrl-Z	コンフィギュレーション モードを終了します。
ステップ 4	Switch# show spanning-tree mst	設定を確認します。

次に、MSTI パラメータの設定例を示します。

```
Switch(config)# spanning-tree mst 1 priority ?
<0-61440> bridge priority in increments of 4096
Switch(config)# spanning-tree mst 1 priority 1
% Bridge Priority must be in increments of 4096.
% Allowed values are:
  0 4096 8192 12288 16384 20480 24576 28672
  32768 36864 40960 45056 49152 53248 57344 61440
Switch(config) # spanning-tree mst 1 priority 49152
Switch(config)#
Switch(config)# spanning-tree mst 0 root primary
mst 0 bridge priority set to 24576
mst bridge max aging time unchanged at 20
mst bridge hello time unchanged at 2
mst bridge forward delay unchanged at 15
Switch(config) # ^Z
Switch#
Switch# show spanning-tree mst
##### MST00
                   vlans mapped: 11-4094
Bridge address 00d0.00b8.1400 priority 24576 (24576 sysid 0)
```

Root	this switch for CST and IST	
Configured	hello time 2, forward delay 15, max age 20, max hops 20	
	Role Sts Cost Prio.Nbr Status	
Fa4/4	Back BLK 1000 240.196 P2p	
Fa4/5	Desg FWD 200000 128.197 P2p	
Fa4/48	Desg FWD 200000 128.240 P2p Bound(STP)	
	01 vlans mapped: 1-10	
-	address 00d0.00b8.1400 priority 49153 (49152 sysid 1)	
Root	this switch for MST01	
Interface	Role Sts Cost Prio.Nbr Status	
Fa4/4	Back BLK 1000 160.196 P2p	
Fa4/5	Desg FWD 200000 128.197 P2p	
Fa4/48	Boun FWD 200000 128.240 P2p Bound(STP)	
Switch#		

MSTI ポート パラメータの設定

MSTI ポート パラメータを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config-if)# spanning-tree mst x cost y	MSTI ポート コストを設定します。
ステップ 2	Switch(config-if)# spanning-tree mst x port-priority y	MSTI ポート プライオリティを設定します。
ステップ 3	Switch(config-if)# Ctrl-Z	コンフィギュレーション モードを終了します。
ステップ 4	Switch# show spanning-tree mst x interface y	設定を確認します。

次に、MSTI ポート パラメータの設定例を示します。

```
Switch(config) # interface fastethernet 4/4
Switch(config-if)# spanning-tree mst 1 ?
               Change the interface spanning tree path cost for an instance
 port-priority Change the spanning tree port priority for an instance
Switch(config-if)# spanning-tree mst 1 cost 1234567
Switch(config-if)# spanning-tree mst 1 port-priority 240
Switch(config-if)# ^Z
Switch# show spanning-tree mst 1 interface fastethernet 4/4
FastEthernet4/4 of MST01 is backup blocking
Edge port:no
                       (default) port guard :none
                                                                (default)
Link type:point-to-point (auto)
                                        bpdu filter:disable
                                                                (default)
Boundary :internal
                                        bpdu guard :disable
                                                               (default)
Bpdus (MRecords) sent 125, received 1782
Instance Role Sts Cost
                          Prio.Nbr Vlans mapped
       Back BLK 1234567 240.196 1-10
Switch#
```

プロトコル移行の再開

RSTP と MST には、他のリージョンまたは別のバージョンの IEEE スパニングツリーと正しく対話 するための互換メカニズムが組み込まれています。たとえば、レガシー ブリッジに接続された RSTP ブリッジは、ポートのいずれかで 802.1D BPDU を送信します。 同様に、 MST ブリッジがレガシー BPDU または別のリージョンの MST BPDU を受信する場合は、ポートがリージョンの境界にある かどうかを検出します。

しかし、このようなメカニズムは効率的なモードへの復帰を妨げます。たとえば、レガシー 802.1D に指定された RSTP ブリッジは、レガシー ブリッジがリンクから取り外されたあとも 802.1D モードの状態にとどまります。同様に、MST ポートは接続しているブリッジが同じリージョンに加入したあとも、自身を境界ポートとみなします。Catalyst 4500 シリーズ スイッチに強制的に近接スイッチと再ネゴシエーションさせる場合(プロトコル移行を再開する場合)、次のように clear spanning-tree detected-protocols コマンドを使用します。

Switch# clear spanning-tree detected-protocols fastethernet 4/4 Switch#

MST コンフィギュレーションの表示

MST のコンフィギュレーションを表示するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# show spanning-tree mst configuration	アクティブなリージョンの設定情報を表示します。
ステップ 2	Switch# show spanning-tree mst [detail]	MST プロトコルの詳細情報を表示します。
ステップ 3	Switch# show spanning-tree mst instance-id [detail]	特定の MSTI に関する情報を表示します。
ステップ 4	Switch# show spanning-tree mst interface interface [detail]	特定のポートに関する情報を表示します。
ステップ 5	Switch# show spanning-tree mst instance-id interface interface [detail]	特定のポートおよび特定のインスタンスに関する MST 情報を表示します。
ステップ 6	Switch# show spanning-tree vlan vlan_ID	MST モードの VLAN 情報を表示します。

```
次に、MST モードのスパニングツリー VLAN コンフィギュレーションを表示する例を示します。
Switch(config) # spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 1-10
Switch(config-mst) # name cisco
Switch(config-mst)# revision 1
Switch(config-mst)# Ctrl-D
Switch# show spanning-tree mst configuration
        [ciscol
Revision 1
Instance Vlans mapped
_____
        1-10
Switch# show spanning-tree mst
###### MST00
                vlans mapped: 11-4094
Bridge address 00d0.00b8.1400 priority 32768 (32768 sysid 0)
         address 00d0.004a.3c1c priority 32768 (32768 sysid 0)
port Fa4/48
IST master this switch
                              path cost 203100
Operational hello time 2, forward delay 15, max age 20, max hops 20
Configured hello time 2, forward delay 15, max age 20, max hops 20
Interface
              Role Sts Cost
                              Prio.Nbr Status
_____ ___ ___
             Back BLK 1000
                             240.196 P2p
Fa4/5
             Desg FWD 200000 128.197 P2p
             Root FWD 200000
                              128.240 P2p Bound(STP)
###### MST01
               vlans mapped: 1-10
Bridge address 00d0.00b8.1400 priority 32769 (32768 sysid 1)
         this switch for MST01
Root
Interface
              Role Sts Cost
                              Prio.Nbr Status
Fa4/4
             Back BLK 1000
                             240.196 P2p
                             128.197 P2p
              Desg FWD 200000
Fa4/5
Fa4/48
              Boun FWD 200000
                              128.240 P2p Bound(STP)
Switch# show spanning-tree mst 1
##### MST01
                vlans mapped: 1-10
Bridge address 00d0.00b8.1400 priority 32769 (32768 sysid 1)
```

Root this switch for MST01 Role Sts Cost Prio.Nbr Status Interface 240.196 P2p Fa4/4 Back BLK 1000 Desg FWD 200000 128.197 P2p Fa4/48 Boun FWD 200000 128.240 P2p Bound(STP) Switch# show spanning-tree mst interface fastethernet 4/4 FastEthernet4/4 of MST00 is backup blocking (default) Edge port:no (default) port guard :none Link type:point-to-point (auto) bpdu filter:disable (default) bpdu guard :disable Boundary :internal (default) Bpdus sent 2, received 368 Prio.Nbr Vlans mapped Instance Role Sts Cost 0 Back BLK 1000 240.196 11-4094 1 Back BLK 1000 240.196 1-10 Switch# show spanning-tree mst 1 interface fastethernet 4/4 FastEthernet4/4 of MST01 is backup blocking port guard :none (default) bpdu filter:disable (default) bpdu guard :disable (default) Edge port:no (default) port guard :none Link type:point-to-point (auto) bpdu guard :disable Boundary :internal Bpdus (MRecords) sent 2, received 364 Prio.Nbr Vlans mapped Instance Role Sts Cost Back BLK 1000 240.196 1-10 Switch# show spanning-tree mst 1 detail vlans mapped: 1-10 ###### MST01 Bridge address 00d0.00b8.1400 priority 32769 (32768 sysid 1) this switch for MST01 FastEthernet4/4 of MST01 is backup blocking Port info port id 240.196 priority 240 cost 1000 Designated root address 00d0.00b8.1400 priority 32769 cost 0 Designated bridge address 00d0.00b8.1400 priority 32769 port id 128.197 Timers:message expires in 5 sec, forward delay 0, forward transitions 0 Bpdus (MRecords) sent 123, received 1188 ${\tt FastEthernet4/5}$ of MST01 is designated forwarding Port info port id 128.197 priority 128 cost 200000 Designated root address 00d0.00b8.1400 priority 32769 cost 0 Designated bridge address 00d0.00b8.1400 priority 32769 port id 128.197 Timers:message expires in 0 sec, forward delay 0, forward transitions 1 Bpdus (MRecords) sent 1188, received 123 FastEthernet4/48 of MST01 is boundary forwarding Port info port id 128.240 priority 128 cost 200000 Designated root address 00d0.00b8.1400 priority 32769 cost 0 Designated bridge address 00d0.00b8.1400 priority 32769 port id 128.240 Timers:message expires in 0 sec, forward delay 0, forward transitions 1 Bpdus (MRecords) sent 78, received 0 Switch# show spanning-tree vlan 10 Spanning tree enabled protocol mstp Root ID Priority 32769 Address 00d0.00b8.1400

This bridge is the root

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 00d0.00b8.1400

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface Role Sts Cost Prio.Nbr Status Back BLK 1000 240.196 P2p Desg FWD 200000 128.197 P2p Fa4/4 Fa4/5

Switch# show spanning-tree summary

Root bridge for:MST01

EtherChannel misconfiguration guard is enabled

Extended system ${\tt ID}$ is enabled

Portfast is disabled by default PortFast BPDU Guard is disabled by default Portfast BPDU Filter is disabled by default is disabled by default is disabled Loopguard

UplinkFast is disabled BackboneFast Pathcost method used is long

Name	Blocking	Listening	Learning	Forwarding	STP Active	9
MST00 MST01	1 1	0	0	2 2	3	-
2 msts Switch#	2	0	0	4	6	_

■ MST の設定



CHAPTER

18

Resilient Ethernet Protocol の設定

この章では、Catalyst 4500 シリーズ スイッチに Resilient Ethernet Protocol (REP)を設定する方法を説明します。REP はシスコ独自のプロトコルで、Spanning Tree Protocol (STP; スパニング ツリー プロトコル)に代わるプロトコルとして、ネットワーク ループの制御、リンク障害の処理、コンバージェンス時間の改善を実現します。REP は、セグメントに接続されているポートのグループを制御することで、セグメントがブリッジング ループを作成するのを防ぎ、セグメント内のリンク障害に応答します。REP は、より複雑なネットワークを構築するための基盤を提供し、VLAN ロード バランシングをサポートします。

この章の内容は、次のとおりです。

- REPの概要 (p.18-2)
- REPの設定 (p.18-7)
- REP のモニタリング (p.18-15)

REP の概要

1 REP セグメントは、相互接続しているポートのチェーンで、セグメント ID が設定されています。各セグメントは、標準(非エッジ)セグメント ポートと、2 つのユーザ設定エッジ ポートで構成されています。1 スイッチは同じセグメントに属するポートを複数持たず、各セグメント ポートにある外部ネイバーは1 つだけです。セグメントは共有メディアを通過できますが、どのリンクであっても同じセグメントに属することができるのは2 ポートだけです。REP は、レイヤ2 トランクおよび PVLAN 混合モード トランク インターフェイスでのみサポートされます。

図 18-1 に、4 つのスイッチにまたがる 6 つのポートで構成されているセグメントの例を示します。ポート E1 および E2 がエッジ ポートとして設定されています。(左側のセグメントのように)すべてのポートが動作可能の場合、斜線で表しているように単一ポートがブロックされます。右側の図のようにネットワークに障害が発生すると、ブロックされたポートがフォワーディング ステートに復帰して、ネットワークの中断を最小限にします。

図 18-1 REP オープン セグメント

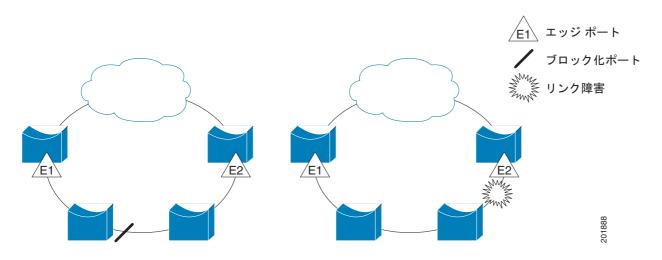
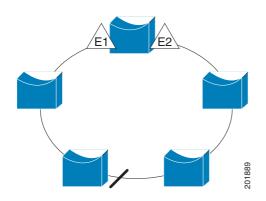


図 18-1 に示されたセグメントは、オープン セグメントで、2 つのエッジ ポート間は接続されていません。REP セグメントは、ブリッジング ループとなる可能性がなく、セグメント エッジが安全 に任意のネットワークに接続されます。セグメント内のスイッチに接続されているすべてのホスト には、エッジ ポートを通じて残りのネットワークに接続する方法が 2 つありますが、いつでもアクセス可能なのは 1 つだけです。障害により、ホストが通常のゲートウェイにアクセスできない場合、REP がすべてのポートのブロックを解除して、他のゲートウェイを通じた接続を確保します。

図 18-2 で示しているセグメントは、両方のエッジが同じスイッチ内にあるリング セグメントです。この設定では、セグメントを通じてエッジ ポートと接続します。この設定を使用すると、セグメント内の任意の 2 スイッチ間で冗長接続を形成することができます。

図 18-2 REP リング セグメント



REP セグメントには次のような特徴があります。

- セグメント内の全ポートが動作可能な場合、1 ポート (*代替*ポートと呼ばれる)が各 VLAN でブロック ステートとなります。VLAN ロード バランシングが設定された場合、セグメント内の 2 ポートが VLAN のブロック ステートを制御します。
- セグメント内の1つまたは複数のポートが動作不能になると、リンク障害が発生して、すべてのポートがすべての VLAN トラフィックを転送して、接続性を確保します。
- リンク障害の場合、できるだけ早期に代替ポートのブロックが解除されます。障害リンクが復旧すると、ネットワークの中断を最小限に抑えながら VLAN ごとにブロックされたポートが論理的に選択されます。

REP セグメントに基づいて、ほとんどのネットワーク タイプを構成することができます。また REP は、プライマリ エッジ ポートで制御されていてもセグメント内のポートで発生する、VLAN ロード バランシングをサポートしています。

REP には次のような制限事項があります。

- 各セグメント ポートを設定する必要があります。設定を間違えると、ネットワーク内でフォワーディング ループが発生します。
- REP はセグメント内の単一障害ポートのみを管理できます。REP セグメント内の複数ポート障害の場合、ネットワークの接続が中断します。
- 冗長ネットワーク内にのみ REP を設定します。冗長性のないネットワークに REP を設定すると、接続が失われます。

リンク完全性

REP は、リンク完全性を確認するためにエッジ ポート間でエンドツーエンド ポーリング メカニズムを使用していません。ローカル リンク障害検出を実装しています。インターフェイスがイネーブルの場合、REP Link Status Layer (LSL; リンク ステータス レイヤ)が REP 対応ネイバーを検出して、セグメント内の接続性を確立します。すべての VLAN は、ネイバーが検出されるまでインターフェイス上でブロックされます。ネイバーが特定された後、REP が代替ポートとなるネイバー ポートと、トラフィックを転送するポートを決定します。

セグメント内の各ポートには一意のポート ID があります。ポート ID フォーマットは、スパニング ツリー アルゴリズムで使用されるものと似ていて、ポート番号(ブリッジ上で一意)と、関連 MAC アドレス (ネットワーク内で一意)というフォーマットです。セグメント ポートが起動すると、ポートの LSL がセグメント ID とポート ID を含むパケットの送信を開始します。ポートは、同じ セグメント内のネイバーとのスリーウェイ ハンドシェイクを実行したあとで、動作可能と宣言されます。次のような場合、セグメント ポートは動作可能になりません。

- ネイバーに同じセグメント ID がない
- 複数のネイバーに同じセグメント ID がある
- ネイバーがピアとして、ローカルポートに確認応答しない

各ポートは、直近のネイバーと隣接関係を確立します。隣接関係が確立されると、ポートがセグメントの1つのブロックされたポート(代替ポート)を決定するようにネゴシエートします。その他のポートのブロックは解除されます。デフォルトで、REPパケットは BPDU クラス MAC アドレスに送信されます。パケットは、シスコ マルチキャスト アドレスにも送信できますが、現時点でセグメントで障害が発生した場合に Blocked Port Advertisement (BPA)メッセージの送信のみに使用されます。パケットは、REPが動作していないデバイスによってドロップされます。

ファスト コンパージェンス

REP が物理リンク ベースで動作し、VLAN 単位ベースで動作しないため、必要なのは全 VLAN で 1 hello メッセージのみなので、プロトコルの負荷が低減します。指定セグメント内の全スイッチで継続的に VLAN を作成し、REP トランクと PVLAN の混合モード トランク ポート上に同じ許容 VLAN を設定することを推奨します。ソフトウェアでのメッセージのリレーによって発生する遅延を回避するために、REP ではいくつかのパケットを通常のマルチキャスト アドレスにフラッディングすることも可能です。これらのメッセージは Hardware Flood Layer (HFL) で動作し、REP セグメントだけではなくネットワーク全体にフラッディングされます。セグメントに属していないスイッチは、これらのメッセージをデータ トラフィックとして扱います。ドメイン全体で専用の管理 VLAN を設定することで、これらのメッセージのフラッディングを制御することができます。

予想されるコンバージェンス復旧時間はローカル セグメントで 200 ミリ秒未満です。

VLAN ロード パランシング

REP セグメント内の 1 エッジ ポートがプライマリ エッジ ポートとして機能し、もう一方がセカンダリ エッジ ポートとなります。セグメント内の VLAN ロード バランシングに常に参加しているのがプライマリ エッジ ポートです。REP VLAN バランシングは、設定された代替ポートでいくつかの VLAN をブロックし、プライマリ エッジ ポートでその他の全 VLAN をブロックすることで実行されます。VLAN ロード バランシングを設定する際に、次の 3 種類の方法のいずれかを使用して代替ポートを指定できます。

- インターフェイスにポート ID を入力します。セグメント内のポート ID を識別するには、ポートの show interface rep detail インターフェイス コンフィギュレーション コマンドを入力します。
- セグメント内のポートのネイバー オフセット番号を入力します。これは、エッジ ポートのダウンストリーム ネイバー ポートを識別するものです。ネイバー オフセット番号の範囲は、-256 ~ +256 で、0 値は無効です。プライマリ エッジ ポートはオフセット番号 1 です。1 を越える正数はプライマリ エッジ ポートのダウンストリーム ネイバーを識別します。負数は、セカンダリ エッジ ポート (オフセット番号 -1) とそのダウンストリーム ネイバーを示します。



(注)

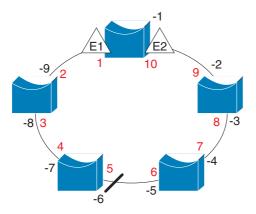
プライマリ(またはセカンダリ)エッジ ポートからポートのダウンストリーム位置を特定することで、プライマリ エッジ ポートのオフセット番号を設定します。番号 1 はプライマリエッジ ポート自体のオフセット番号なので、オフセット番号 1 は入力しないでください。

図 18-3 に、E1 がプライマリ エッジ ポートで E2 がセカンダリ エッジ ポートの場合の、セグメントのネイバー オフセット番号を示します。リングの内側にある赤い番号は、プライマリエッジ ポートからのオフセット番号で、リングの外側にある黒い番号がセカンダリ エッジポートからのオフセット番号です。正のオフセット番号(プライマリ エッジ ポートからのダ

ウンストリーム位置)または負のオフセット番号(セカンダリ エッジ ポートからのダウンストリーム位置)のいずれかにより、(プライマリ エッジ ポートを除く)全ポートを識別することができます。E2 がプライマリ エッジ ポートになるとオフセット番号 1 となり、E1 のオフセット番号が-1 になります。

• preferred キーワードを入力します。これにより、rep segment segment-id preferred インターフェイス コンフィギュレーション コマンドで優先代替ポートとしてすでに設定されているポートを選択します。

図 18-3 セグメント内のネイバー オフセット番号



E1 = プライマリ エッジ ポート E2 = セカンダリ エッジ ポート

プライマリ エッジ ポートからのオフセット番号 セカンダリ エッジ ポートからのオフセット番号(負数)

01890

REP セグメントが完了すると、すべての VLAN がブロックされます。 VLAN ロード バランシング を設定する際に、次の 2 種類の方法のいずれかでトリガーされます。

- プライマリ エッジ ポートのあるスイッチ上で rep preempt segment segment-id 特権 EXEC コマンドを入力することで、いつでも手動で VLAN ロード バランシングをトリガーすることができます。
- rep preempt delay seconds インターフェイス コンフィギュレーション コマンドを入力すると、 プリエンプト遅延時間を設定できます。リンク障害が発生して復旧すると、設定されたプリエ ンプション期間が経過後に VLAN ロード バランシングが開始されます。設定時間が経過する 前に別のポートで障害が発生した場合、遅延タイマーが再開されることに注意してください。



VLAN ロード バランシングが設定されている場合、手動介入またはリンク障害および復旧によってトリガーされるまで、動作が開始されません。

VLAN ロード バランシングがトリガーされると、プライマリ エッジ ポートがメッセージを送信して、セグメント内の全インターフェイスにプリエンプションについて警告します。メッセージがセカンダリ エッジ ポートで受信されると、これがネットワークに反映され、メッセージ内で特定された VLAN セットをブロックするように代替ポートに通知し、残りの VLAN をブロックするようにプライマリ エッジ ポートに通知します。

またすべての VLAN をブロックするために、セグメント内の特定ポートを設定できます。プライマリ エッジ ポートによってのみ VLAN ロード バランシングが開始され、セグメントが各エンドでエッジ ポートによって終端されていない場合開始することができません。プライマリ エッジ ポートは、ローカル VLAN ロード バランシング設定を決定します。

ロード バランシングを再設定するには、プライマリ エッジ ポートを再設定します。ロード バランシング 設定を変更するには、プライマリ エッジ ポートで rep preemt segement コマンドを待機するか、ポート障害および復旧のあとで新規設定を実行する前に設定済プリエンプト遅延期間を待機します。エッジ ポートを通常のセグメント ポートに変更しても、既存の VLAN ロード バランシングステータスは変更されません。新規エッジ ポートを設定すると、新規トポロジ設定になる可能性があります。

スパニング ツリー インタラクション

REP は STP とは対話しませんが、共存は可能です。セグメントに属しているポートがスパニングツリーの制御から削除され、STP BPDU がセグメント ポートで受け入れられないか、送信されません。したがって、STP はセグメント上で実行できません。

STP リング コンフィギュレーションから REP セグメント コンフィギュレーションに移行するには、まずリング内の単一ポートをセグメントの一部として設定し、次にセグメント数を最小限にするように隣接するポートを設定します。各セグメントには、常にブロックされたポートが含まれているので、セグメントが複数になるとブロックされたポートも複数になり、接続が失われる可能性があります。セグメントがエッジ ポートの場所まで両方向に設定されたら、次にエッジ ポートを設定します。

REP ポート

REP セグメント内のポートは、3 つのロールまたはステート (障害、オープン、代替) のうちのいずれかを取得します。

- 通常セグメント ポートとして設定されているポートは、障害ポートとして開始されます。
- ネイバールータとの隣接関係が確立されると、ポートは代替ポート ステートに移行して、インターフェイス内の全 VLAN をブロックします。ブロックされたポートのネゴシエーションが発生して、セグメントが安定すると、ブロックされたポートが代替ロールのままになって他のすべてのポートがオープン ポートになります。
- リンク内に障害が発生すると、すべてのポートが障害ステートに移行します。代替ポートが障害通知を受信すると、これがオープンステートに変化して、すべての VLAN を転送します。

通常セグメント ポートをエッジ ポートに変換しても、エッジ ポートを通常セグメント ポートに変換しても、必ずトポロジ変更が発生するわけではありません。エッジ ポートを通常のセグメントポートに変更する場合、設定されるまで VLAN ロード バランシングは実装されません。VLAN ロード バランシングの場合、セグメント内に 2 つのエッジ ポートを設定する必要があります。

スパニング ツリー ポートとして再設定されたセグメント ポートは、スパニング ツリー設定に従って再起動します。デフォルトでは、これは指定ブロッキング ポートです。PortFast が設定されていたり、STP がディセーブルの場合、ポートはフォワーディング ステートになります。

REP の設定

セグメントは、チェーンで相互接続しているポートの集合で、セグメント ID が設定されています。 REP セグメントを設定するには、REP 管理 VLAN を設定し(あるいはデフォルト VLAN 1 を使用し、次にインターフェイス コンフィギュレーション モードを使用してセグメントにポートを追加します。2 つのエッジ ポートをセグメント内に設定して、1 つをプライマリ エッジ ポート、もう1 つをデフォルトでセカンダリ エッジ ポートにします。1 セグメント内のプライマリ エッジ ポートは 1 つだけです。別のスイッチのポートなど、セグメント内で 2 つのポートをプライマリ エッジ ポートに設定すると、REP がそのうちのいずれかを選択してセグメントのプライマリ エッジ ポートとして機能させます。オプションで、Segment Topology Change Notice (STCN; セグメントトポロジ変更通知) および VLAN ロード バランシングを送信する場所を設定することもできます。

ここでは、次の情報について説明します。

- REP のデフォルト設定 (p.18-7)
- REP 設定時の注意事項 (p.18-7)
- REP 管理 VLAN の設定 (p.18-8)
- REP インターフェイスの設定 (p.18-9)
- VLAN ロード バランシングの手動によるプリエンプションの設定 (p.18-13)
- REPのSMMPトラップ設定(p.18-14)

REP のデフォルト設定

REP はすべてのインターフェイス上でディセーブルです。イネーブルにする際に、エッジ ポートとして設定されていなければインターフェイスは通常セグメント ポートになります。

REP をイネーブルにする際に、STCN の送信はディセーブルで、すべての VLAN はブロックされ、管理 VLAN は VLAN 1 になります。

VLAN ロード バランシングがイネーブルの場合、デフォルトは手動でのプリエンプションで、遅延 タイマはディセーブルになっています。VLAN ロード バランシングが設定されていない場合、手動 でのプリエンプション後のデフォルト動作は、プライマリ エッジ ポートで全 VLAN がブロックとなります。

REP 設定時の注意事項

REP の設定時には、次の注意事項に従ってください。

- まず1ポートの設定から始めて、セグメント数とブロックされたポートの数を最小限に抑えるように隣接ポートを設定することを推奨します。
- 外部ネイバーが設定されておらずセグメント内では複数のポートに障害が発生した場合、1 ポートがデータ パス用のフォワーディング ステートになり、設定中の接続性の維持に役立ち ます。show rep inteface 特権 EXEC コマンド出力では、このポートのポート ロールは Fail Logical Open と表示され、他の障害ポートのポート ロールは Fail No Ext Neighbor と表示されます。障 害ポートの外部ネイバーが設定されている場合、ポートは代替ポート ステートに移行して、代 替ポート選択メカニズムに基づいて最終的にオープン ステートになるか、代替ポートのままに なります。
- REP ポートは、レイヤ 2 dot1Q トランクまたは PVLAN 混合モード トランク ポートのいずれかである必要があります。
- telnet 接続を通じて REP を設定する際には注意してください。別の REP インターフェイスが メッセージを送信してブロック解除するまで REP はすべての VLAN をブロックするため、同 じインターフェイスを通じてスイッチがアクセスする Telnet セッションで REP をイネーブル にすると、スイッチへの接続が失われる可能性があります。

- 同じセグメントやインターフェイスで REP と STP を実行することはできません。
- STP ネットワークを REP セグメントに接続する場合、接続はセグメント エッジであることを 確認してください。エッジで実行されていない STP 接続は、STP が REP セグメントを実行し ないため、ブリッジング ループが発生する可能性があります。すべての STP BPDU は、REP インターフェイスでドロップされます。
- 同じ許容 VLAN セットでセグメント内のすべてのトランクと PVLAN 混合モード トランクポートを設定する必要があります。そうでない場合、設定ミスが発生します。
- REP がスイッチの 2 ポートでイネーブルの場合、両方のポートが通常セグメント ポートまたは エッジ ポートである必要があります。 REP ポートは以下の規則に従います。
 - セグメント内にスイッチ上の 1 ポートのみが設定されている場合、そのポートがエッジポートとなります。
 - 同じセグメント内に属するスイッチに 2 つのポートがある場合、両方のポートがエッジポートになるか、両方のポートが通常セグメント ポートである必要があります。
 - スイッチ上の 2 ポートが同じセグメントに属していて、1 つがエッジ ポートとして設定され、もう 1 つが通常セグメント ポートに設定されている場合 (設定ミス) エッジ ポートは通常セグメント ポートとして扱われます。
- REP インターフェイスがブロックされたステートになり、ブロック解除しても安全であると通知されるまでブロックされたステートのままになります。突然の接続消失を避けるために、これを意識しておく必要があります。
- REP がネイティブ VLAN 上においてすべての LSL PDU をタグなしフレームで送信します。シスコ マルチキャスト アドレスに送信された BPA メッセージは、管理 VLAN で送信されます。これはデフォルトで VLAN 1 です。
- REPポートは、これらのポートタイプのいずれかに設定できません。
 - SPAN 宛先ポート
 - プライベート VLAN ポート
 - トンネル ポート
 - アクセス ポート
- REP は EtherChannel でサポートされていますが、EtherChannel に属する個別ポートではサポートされません。
- スイッチごとに最大で384 REP セグメントです。

REP 管理 VLAN の設定

リンク障害用のソフトウェアまたはロード バランシング中の VLAN ブロッキング通知のソフトウェアでの、メッセージのリレーによって発生する遅延を回避するために、REP は HFL で通常マルチキャスト アドレスにフラッディングします。これらのメッセージは REP セグメントだけではなくネットワーク全体にフラッディングされます。ドメイン全体の管理 VLAN を設定することで、これらのメッセージのフラッディングを制御することができます。

REP 管理 VLAN を設定する場合、次の注意事項に従ってください。

- 管理 VLAN を設定しない場合、デフォルトは VLAN 1 です。
- スイッチとセグメントで 1 つの管理 VLAN のみが可能です。ただし、これはソフトウェアによって強制的に設定されません。
- 管理 VLAN は RSPAN VLAN になりません。

REP 管理 VLAN を設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	rep admin vlan vlan-id	管理 VLAN を指定します。有効範囲は 2 ~ 4094 です。デ
		フォルトは VLAN 1 です。管理 VLAN を 1 に設定するには、
		no rep admin vlan グローバル コンフィギュレーション コ
		マンドを実行します。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show interface [interface-id] rep detail	REP インターフェイスのいずれか 1 つの設定を確認しま
		す。
ステップ 5	copy running-config startup config	(任意)スイッチ スタートアップ コンフィギュレーション
		ファイルに設定を保存します。

次に、管理 VLAN を VLAN 100 として設定して、REP インターフェイスの 1 つに show interface rep detail コマンドを入力して設定を確認する例を示します。

Switch# configure terminal
Switch (conf)# rep admin vlan 100
Switch (conf-if)# end

 ${\tt Switch\#\ show\ interface\ gigabitethernet0/1\ rep\ detail}$

GigabitEthernet0/1 REP enabled
Segment-id: 2 (Edge)

PortID: 00010019E7144680 Preferred flag: No

Operational Link Status: TWO_WAY Current Key: 0002001121A2D5800E4D

Port Role: Open Blocked Vlan: <empty> Admin-vlan: 100

Admin-Vian: 100
Preempt Delay Timer: disabled
Load-balancing block port: none
Load-balancing block vlan: none
STCN Propagate to: none
LSL PDU rx: 3322, tx: 1722
HFL PDU rx: 32, tx: 5
BPA TLV rx: 16849, tx: 508
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 118, tx: 118
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 4214, tx: 4190

REP インターフェイスの設定

REP 動作の場合、各セグメントインターフェイスでこれをイネーブルにして、セグメント ID を特定します。このステップは必須で、他の REP 設定の前に実行します。また、各セグメントにプライマリおよびセカンダリ エッジ ポートを設定する必要があります。その他のステップはすべて任意です。

インターフェイス上で REP をイネーブルにして設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	interface interface-id	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは物理レイヤ 2 インターフェイスにすることもポート チャネル (論理インターフェイス)にすることもできます。指定できるポートチャネルの範囲は 1 ~ 48 です。
ステップ 3	switchport mode trunk または switchport mode private-vlan trunk promiscuous	レイヤ 2 インターフェイスをレイヤ 2 トランク ポートとして設定します。 レイヤ 2 インターフェイスを PVLAN 混合モード トランク ポートとして設定します。
		PVLAN 混合モードトランク ポートのコマンド オプションの詳細については、レイヤ 2 インターフェイスの PVLAN 混合モードトランク ポートとしての設定($p.36-19$)を参照してください。
		(注) REP を使用すると、switchport mode private-vlan trunk promiscuous コマンドのみがサポートされます。他の PVLAN トランク関連設定はサポート <i>されません</i> 。

コマンド 目的 ステップ 4 rep segment segment-id [edge [primary]] [preferred] インターフェイス上で REP をイネーブルにして、セ グメント番号を特定します。セグメント ID の有効範 囲は1~1024です。これらのオプションキーワー ドは利用可能です。 (注) 各セグメントに 1 つのプライマリ エッジ ポートを含めて、2 つのエッジ ポートを設定 する必要があります。 • edge を入力して、ポートをエッジ ポートとして 設定します。primary キーワードなしで edge を 入力すると、ポートがセカンダリ エッジ ポート として設定されます。各セグメントにあるエッ ジポートは2つのみです。 • (任意)エッジ ポート上で、primary を入力し てポートをプライマリ エッジ ポートとして設 定し、VLAN ロード バランシングを設定するこ とができます。 (注) 各セグメントのプライマリ エッジ ポートは 1 つのみ可能ですが、2 つの異なるスイッチ にエッジ ポートを設定して primary キー ワードを両方のスイッチに入力しても、その 設定は許容されます。ただし、REP はセグメ ント プライマリ エッジ ポートとして 1 つの ポートのみが選択されます。show rep topology 特権 EXEC コマンドを入力すると、 セグメントのプライマリ エッジ ポートを特 定することができます。 (任意) preferred を入力して、ポートが優先代 替ポートであるか、VLAN ロード バランシング の優先ポートであるのかを示します。 (注) ポートを優先に設定しても、代替ポートにな るとは限りません。同等に可能性のあるポー トよりやや可能性が高くなるだけです。通 常、前に障害が発生したポートが、代替ポー トとなります。 ステップ 5 rep stcn {interface interface-id | segment id-list | stp} (任意)STCN を送信するようにエッジ ポートを設定 します。 interface interface-id を入力して、STCN を受信す るための物理インターフェイスまたはポート チャネルを指定します。 • **segment** *id-list* を入力して、STCN を受信するた めの1つまたは複数のセグメントを特定しま す。有効範囲は1~1024です。 stp を入力して、STCN を STP ネットワークに送 信します。

	コマンド	目的
ステップ 6	rep block port {id port-id neighbor_offset preferred} vlan {vlan-list all}	(任意)プライマリエッジポートに VLAN ロードバランシングを設定して、3 つの方法のいずれかを使用して REP 代替ポートを特定し、代替ポートでブロックされるように VLAN を設定します。
		• id port-id を入力して、ポート ID によって代替ポートを特定します。セグメント内の各ポートにポート ID が自動的に生成されます。show interface interface-id rep [detail] 特権 EXEC コマンドを入力して、インターフェイス ポート ID を表示できます。
		• neighbor_offset 番号を入力して、代替ポートをエッジ ポートからのダウンストリーム ネイバーとして特定します。有効範囲は -256 ~ 256で、負数はセカンダリエッジ ポートからのダウンストリーム ネイバーを示します。値 0 は無効です -1 を入力して、セカンダリエッジ ポートを代替ポートとして識別します。ネイバーオフセット番号付けの例については、図 18-3(p.18-5)を参照してください。
		(注) プライマリ エッジ ポート (オフセット番号 1)にこのコマンドを入力するので、代替ポートを特定するのにオフセット値 1を入力しません。
		• preferred を入力して、すでに VLAN ロード バランシングの優先代替ポートとして特定されている通常セグメント ポートを選択します。
		• vlan <i>vlan-list</i> を入力して、1 VLAN または VLAN 範囲をプロックします。
		● vlan all を入力して、すべての VLAN をブロックします。
		(注) REP プライマリ エッジ ポート上にのみこの コマンドを入力します。
ステップ 7	rep preempt delay seconds	(任意)リンク障害および復旧の後に自動的に VLAN ロード バランシングをトリガーする場合、このコマンドを入力して、プリエンプト時間遅延を設定する必要があります。時間遅延範囲は 15 ~ 300 秒です。デフォルトは、時間遅延のない手動によるプリエンプションです。
		(注) REP プライマリ エッジ ポート上にのみこの コマンドを入力します。
ステップ 8	end	特権 EXEC モードに戻ります。
ステップ 9	show interface [interface-id] rep [detail]	REP インターフェイス コンフィギュレーションを 確認します。
ステップ 10	copy running-config startup config	(任意)スイッチ スタートアップ コンフィギュレー ション ファイルに設定を保存します。

デフォルトの設定に戻すには、各コマンドの no 形式を使用します。show rep topology 特権 EXEC コマンドを入力して、セグメント内のどのポートがプライマリ エッジ ポートなのかを確認します。

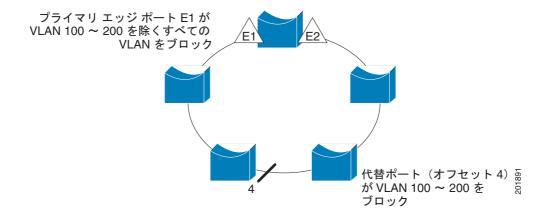
次に、インターフェイスをセグメント 1 のプライマリ エッジ ポートに設定し、STCN をセグメント $2\sim5$ に送信し、代替ポートを ポート 1D 0009001818D68700 のポートとして設定して、セグメント ポート障害および復旧後のプリエンプション遅延 60 秒後にすべての VLAN をブロックする例を示します。

```
Switch# configure terminal
Switch (conf)# interface gigabitethernet0/1
Switch (conf-if)# rep segment 1 edge primary
Switch (conf-if)# rep stcn segment 2-5
Switch (conf-if)# rep block port 0009001818D68700 vlan all
Switch (conf-if)# rep preempt delay 60
Switch (conf-if)# end
```

次に、図 18-4 に、VLAN ブロッキング コンフィギュレーションを設定する例を示します。代替ポートは、ネイバー オフセット番号 4 のネイバーです。手動によるプリエンプションのあとに、VLAN 100 ~ 200 がこのポートでブロックされ、その他のすべての VLAN がプライマリ エッジ ポート E1 (ギガビット イーサネット ポート E1 0/1) でブロックされます。

```
Switch# configure terminal
Switch (conf)# interface gigabitethernet0/1
Switch (conf-if)# rep segment 1 edge primary
Switch (conf-if)# rep block port 4 vlan 100-200
Switch (conf-if)# end
```

図 18-4 VLAN プロッキングの例



VLAN ロード バランシングの手動によるプリエンプションの設定

プライマリエッジポートで rep preempt delay second インターフェイス コンフィギュレーション コマンドを入力しないで、プリエンプション時間遅延を設定するには、デフォルトのセグメントで VLAN ロード バランシングを手動でトリガーします。手動で VLAN ロード バランシングをプリエンプトする前に、他のすべてのセグメント設定が完了しているかどうか確認してください。 rep preempt segment segment-id コマンドを入力すると、プリエンプションによってネットワークが中断する可能性があるため、コマンド実行前に確認メッセージが表示されます。

セグメント プライマリ エッジ ポートのあるスイッチのセグメント上で、手動により VLAN ロード バランシングをトリガーするには、以下を実行します。

	コマンド	目的
ステップ 1	rep preempt segment segment-id	手動により、 セグメント上の VLAN ロード バランシングを
		トリガーします。
		実行前にコマンドを確認する必要があります。
ステップ 2	show rep topology	REP トポロジ情報を表示します。

REP の SMMP トラップ設定

リンク動作ステータス変更およびポート ロール変更について SNMP サーバに通知するために、REP 固有のトラップの送信をスイッチに設定できます。REP トラップを設定するには、特権 EXEC モードを開始して次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	snmp mib rep trap-rate value	スイッチで REP トラップの送信をイネーブルして、 1 秒あたりのトラップの送信数を設定します。範囲は $0 \sim 1000$ で、デフォルトは 0 (制限なし、発生するたびにトラップが送信される)です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	REP トラップ コンフィギュレーションを確認します。
ステップ 5	copy running-config startup config	(任意)スイッチ スタートアップ コンフィギュレーションファイルに設定を保存します。

トラップを削除するには、no snmp mib rep trap-rate グローバル コンフィギュレーション コマンドを入力します。

次に、1 秒あたり 10 の割合で REP トラップを送信するようにスイッチを設定する例を示します。

Switch(config) # snmp mib rep trap-rate 10

REP のモニタリング

REP を監視するには、次の特権 EXEC コマンドを使用します (表 18-1)。

表 18-1 REP モニタリング コマンド

コマンド	目的
show interface [interface-id] rep [detail]	特定のインターフェイスまたは全てのインター
	フェイスの REP コンフィギュレーションとス
	テータスを表示します。
show rep topology [segment segment_id] [archive]	セグメント内のプライマリおよびセカンダリ
[detail]	エッジ ポートを含む、1 セグメントまたは全セ
	グメントの REP トポロジ情報を表示します。

■ REP のモニタリング



CHAPTER

任意の STP 機能の設定

この章では、Catalyst 4500 シリーズ スイッチ上でサポートされる Spanning-Tree Protocol (STP; スパ ニングツリー プロトコル)の機能について説明します。設定上の注意事項、設定手順、および設定 例についても示します。

この章の主な内容は、次のとおりです。

- ルート ガードの概要 (p.19-2)
- ルート ガードのイネーブル化 (p.19-3)
- ループ ガードの概要 (p.19-4)
- ループ ガードのイネーブル化 (p.19-6)
- PortFast の概要 (p.19-7)
- PortFast のイネーブル化 (p.19-8)
- BPDU ガードの概要 (p.19-9)
- BackboneFast のイネーブル化 (p.19-19)
- PortFast BPDU フィルタリングの概要 (p.19-10)
- BackboneFast のイネーブル化 (p.19-19)
- UplinkFast の概要 (p.19-13)
- UplinkFast のイネーブル化 (p.19-14)
- BackboneFast の概要 (p.19-16)
- BackboneFast のイネーブル化 (p.19-19)



STP の設定手順については、第17章「STP および MST の設定」を参照してください。



この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univered/cc/td/doc/product/software/ios122sr/cr/index.htm

ルート ガードの概要

スパニングツリーのルート ガードを設定すると、インターフェイスは強制的に指定ポートになり、現在のルート ステータスを保護して、周辺のスイッチがルート スイッチになるのを防ぎます。

ルート ガードをポート単位でイネーブルにすると、ポートが所属するすべてのアクティブ VLAN (仮想 LAN)にルート ガードが自動的に適用されます。ルート ガードをディセーブルにすると、指定されたポートのルート ガードがディセーブルになり、そのポートは自動的にリスニング ステートになります。

ルート ガードがイネーブルになっているポートを持つスイッチが新しいルートを検出すると、ポートは root-inconsistent ステートになります。そのあとスイッチが新しいルートを検出しなければ、そのポートは自動的にリスニング ステートになります。

ルート ガードのイネーブル化

レイヤ 2 アクセス ポート上のルート ガードをイネーブルにする (このポートを強制的に指定ポートにする)には、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# interface {{fastethernet gigabitethernet tengigabitethernet} slot/port}	設定するインターフェイスを選択します。
ステップ 2	Switch(config-if)# [no] spanning-tree guard root	ルート ガードをイネーブルにします。
		ルート ガードをディセーブルにする場合は、no キーワードを使用します。
ステップ 3	Switch(config-if)# end	コンフィギュレーション モードを終了します。
ステップ 4	Switch# show spanning-tree	設定を確認します。

次に、インターフェイス FastEthernet 5/8 上でルート ガードをイネーブルにする例を示します。

```
Switch(config) # interface fastethernet 5/8
Switch(config-if) # spanning-tree guard root
Switch(config-if) # end
Switch#
```

次に、設定を確認する例を示します。

```
Switch# show running-config interface fastethernet 5/8
Building configuration...

Current configuration: 67 bytes
!
interface FastEthernet5/8
switchport mode access
spanning-tree guard root
end

Switch#
```

次に、root-inconsistent ステートのポートがあるかどうかを判別する例を示します。

Switch# show spanning-tree inconsistentports

Name	Interface	Inconsistency
VLAN0001	FastEthernet3/1	Port Type Inconsistent
VLAN0001	FastEthernet3/2	Port Type Inconsistent
VLAN1002	FastEthernet3/1	Port Type Inconsistent
VLAN1002	FastEthernet3/2	Port Type Inconsistent
VLAN1003	FastEthernet3/1	Port Type Inconsistent
VLAN1003	FastEthernet3/2	Port Type Inconsistent
VLAN1004	FastEthernet3/1	Port Type Inconsistent
VLAN1004	FastEthernet3/2	Port Type Inconsistent
VLAN1005	FastEthernet3/1	Port Type Inconsistent
VLAN1005	FastEthernet3/2	Port Type Inconsistent

Number of inconsistent ports (segments) in the system :10

ループ ガードの概要

ループ ガードは、ポイントツーポイント リンク上の単方向リンク障害が原因で発生するブリッジング ループの防止に有効です。グローバルにイネーブル化した場合、ループ ガードはシステム上のすべてのポイントツーポイント ポートに適用されます。ループ ガードは、ルート ポートおよびブロック ポートを検出し、それらのポートがセグメントの指定ポートから送られた Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット)を受信し続けるようにします。ループガード対応のルート ポートまたはブロック ポートが指定ポートから送られた BPDU の受信を停止した場合、そのポートは物理リンク エラーがポートで発生したと判断して、ブロッキング ステートに移行します。ポートは BPDU を受信すると、ただちにこのステートから回復します。

ループ ガードは、ポート単位でイネーブルにできます。ループ ガードをイネーブルにすると、ポートが所属するすべてのアクティブ インスタンスまたは VLAN にループ ガードが自動的に適用されます。ループ ガードをディセーブルにすると、指定されたポートのループ ガードがディセーブルになります。ループ ガードをディセーブルにすると、すべての loop-inconsistent ポートがリスニング ステートに移行します。

チャネル上でループ ガードをイネーブルに設定し、最初のリンクが単方向になった場合、ループ ガードは影響を受けたポートがチャネルから除外されるまで、チャネル全体をブロックします。図 19-1 に、3 台のスイッチ構成におけるループ ガードを示します。

図 19-1 ループ ガードが設定されたスイッチ 3 台の構成

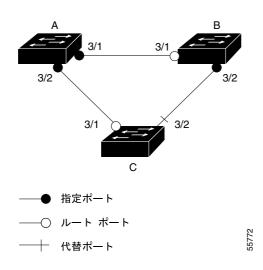


図 19-1 の構成は、次のとおりです。

- スイッチ A およびスイッチ B は、ディストリビューション スイッチです。
- スイッチ C は、アクセス スイッチです。
- ループ ガードはスイッチ A、B、および C のポート 3/1 および 3/2 でイネーブルです。

ルート スイッチでループ ガードをイネーブルにしても効果はありませんが、ルート スイッチが非 ルート スイッチになった場合に保護されます。

ループ ガードを使用するときには、次の注意事項に従ってください。

- PortFast 対応ポートまたはダイナミック VLAN ポートでは、ループ ガードをイネーブルにしないでください。
- ルート ガードがイネーブルの場合は、ループ ガードをイネーブルにしないでください。

ループガードと他の機能の相互作用は、次のとおりです。

- ループ ガードは、UplinkFast または BackboneFast の機能に影響を与えません。
- ポイントツーポイント リンクに接続されていないポート上でループ ガードをイネーブルにしても、機能しません。
- ルート ガードは強制的に、常にポートがルート ポートになるようにします。ループ ガードが 有効なのは、ポートがルート ポートまたは代替ポートの場合だけです。1 つのポートでループ ガードおよびルート ガードを同時にイネーブルにはできません。
- ループ ガードは、スパニングツリーが認識しているポートを使用します。ループ ガードは、Port Aggregation Protocol (PagP; ポート集約プロトコル)が提供する論理ポートの利点を活用できます。ただし、チャネルを形成するには、チャネルとしてまとめたすべての物理ポートを相互に矛盾のない設定にしておく必要があります。PAgP は、チャネルを形成するすべての物理ポート上で、ルート ガードまたはループ ガードを強制的に統一して設定します。

ループガードの注意事項は、次のとおりです。

- スパニングツリーは常に、チャネル内で最初の動作可能ポートを選択して BPDU を送信します。そのリンクが単方向になると、チャネル内の他のリンクが正常に動作していても、 ループ ガードはそのチャネルをブロックします。
- ループ ガードによってすでにブロックされている一連のポートをグループ化してチャネルが形成された場合、スパニングツリーはそれらのポートのすべてのステート情報を失います。したがって、新しいチャネルポートは、指定された役割とともに、フォワーディングステートを取得する可能性があります。
- ループ ガードによってチャネルがブロックされ、チャネルが分断された場合、スパニング ツリーはすべてのステート情報を失います。チャネルを形成していた 1 つまたは複数のリンクが単方向でも、個々の物理ポートは、指定された役割とともにフォワーディング ステートを取得する場合があります。



(注)

UniDirectional Link Detection (UDLD; 単一方向リンク検出)をイネーブルにすると、リンク障害の分離に有効です。UDLD が障害を検出するまでは、ループが発生する可能性がありますが、ループ ガードでは検出できません。

• ループ ガードは、ディセーブルのスパニングツリー インスタンスまたは VLAN では無効です。

ループ ガードのイネーブル化

ループ ガードはグローバルに、またはポートごとにイネーブルにできます。

スイッチ上でループ ガードをグローバルにイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1		スイッチ上でループ ガードをグローバルにイ ネーブルにします。
ステップ 2	Switch(config)# end	コンフィギュレーション モードを終了します。
ステップ 3	Switch# show spanning tree interface 4/4 detail	設定がポートに与える影響を確認します。

次に、ループガードをグローバルにイネーブルにする例を示します。

Switch(config) # spanning-tree loopguard default
Switch(config) # Ctrl-Z

次に、ポート FastEthernet 4/4 のそれまでの設定を確認する例を示します。

Switch# show spanning-tree interface fastethernet 4/4 detail

Port 196 (FastEthernet4/4) of VLAN0010 is forwarding
Port path cost 1000, Port priority 160, Port Identifier 160.196.
Designated root has priority 32768, address 00d0.00b8.140a
Designated bridge has priority 32768, address 00d0.00b8.140a
Designated port id is 160.196, designated path cost 0
Timers:message age 0, forward delay 0, hold 0
Number of transitions to forwarding state:1
The port is in the portfast mode by portfast trunk configuration
Link type is point-to-point by default
Bpdu filter is enabled
Loop guard is enabled by default on the port
BPDU:sent 0, received 0

特定のインターフェイス上でループガードをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# interface {type slot/port} {port-channel port_channel_number}	設定するインターフェイスを選択します。
ステップ 2	Switch(config-if)# spanning-tree guard loop	ループ ガードを設定します。
ステップ 3	Switch(config)# end	コンフィギュレーション モードを終了します。
ステップ 4	Switch# show spanning tree interface 4/4 detail	設定がそのポートに与える影響を確認します。

次に、ポート FastEthernet 4/4 でループ ガードをイネーブルにする例を示します。

Switch(config) # interface fastEthernet 4/4
Switch(config-if) # spanning-tree guard loop
Switch(config-if) # ^Z

次に、設定がポート FastEthernet 4/4 に与える影響を確認する例を示します。

Switch# show spanning-tree interface fastEthernet 4/4 detail

Port 196 (FastEthernet4/4) of VLAN0010 is forwarding

Port path cost 1000, Port priority 160, Port Identifier 160.196.

Designated root has priority 32768, address 00d0.00b8.140a

Designated bridge has priority 32768, address 00d0.00b8.140a

Designated port id is 160.196, designated path cost 0

Timers:message age 0, forward delay 0, hold 0

Number of transitions to forwarding state:1

The port is in the portfast mode by portfast trunk configuration

Link type is point-to-point by default

Bpdu filter is enabled

Loop guard is enabled on the port

BPDU:sent 0, received 0

Switch#

PortFast の概要

スパニングツリー PortFast を使用すると、レイヤ 2 アクセス ポートとして設定されたインターフェイスは、リスニング ステートおよびラーニング ステートを経ずに、ただちにフォワーディング ステートに移行します。1 台のワークステーションまたはサーバに接続されたレイヤ 2 アクセス ポート上で PortFast を使用すると、スパニングツリーのコンバージェンスを待たずに、装置がただちにネットワークに接続されます。インターフェイスが BPDU を受信した場合でも、スパニングツリーはそのポートをブロッキング ステートにせずに、ポートの動作ステートを non-port fast に設定します。これは設定されたステートが port fast のままであり、トポロジ変更に参加している場合でも同様です。



PortFast の目的は、アクセス ポートがスパニングツリーのコンバージェンスを待機する時間を最小限に抑えることです。したがって、PortFast はアクセス ポートで使用すると最も効果的です。別のスイッチに接続しているポートで PortFast をイネーブルにすると、スパニングツリー ループが作成されるリスクがあります。

PortFast のイネーブル化



PortFast は、単一のエンド ステーションをレイヤ 2 アクセス ポートに接続する場合に*限って*使用してください。そのほかの場合に使用すると、ネットワーク ループが発生する可能性があります。

レイヤ 2 アクセス ポート上で PortFast をイネーブルにして、ただちにフォワーディング ステートに移行させるには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config) # interface {{fastethernet gigabitethernet tengigabitethernet} slot/port} {port-channel port_channel_number}	設定するインターフェイスを選択します。
ステップ 2	Switch(config-if)# [no] spanning-tree portfast	単一のワークステーションまたはサーバに接続 されたレイヤ 2 アクセス ポート上で PortFast を イネーブルにします。
		PortFast をディセーブルにする場合は、 no キーワードを使用します。
ステップ 3	Switch(config-if)# end	コンフィギュレーション モードを終了します。
ステップ 4	Switch# show running interface {{fastethernet gigabitethernet tengigabitethernet} slot/port} {port-channel port_channel_number}	設定を確認します。

次に、インターフェイス FastEthernet 5/8 上で PortFast をイネーブルにする例を示します。

```
Switch(config)# interface fastethernet 5/8
Switch(config-if)# spanning-tree portfast
Switch(config-if)# end
Switch#
```

次に、設定を確認する例を示します。

Switch#

```
Switch# show running-config interface fastethernet 5/8
Building configuration...

Current configuration:
!
interface FastEthernet5/8
no ip address
switchport
switchport access vlan 200
switchport mode access
spanning-tree portfast
end
```

BPDU ガードの概要

スパニングツリー BPDU ガードは、BPDU を受信する、PortFast が設定されたインターフェイスをスパニングツリー ブロッキング ステートに移行させずに、シャットダウンします。有効な設定では、PortFast が設定されたインターフェイスは BPDU を受信しません。PortFast が設定されたインターフェイスは BPDU を受信しません。PortFast が設定されたインターフェイスが BPDU を受信した場合、認証されていないデバイスが接続された場合と同じように、無効な設定として通知されます。管理者は手動でインターフェイスを再び動作させなければならないので、BPDU ガード機能により、無効な設定に対する確実な対処が可能になります。



(注)

BPDU ガード機能がイネーブルの場合、スパニングツリーは BPDU ガード機能を PortFast が設定されたすべてのインターフェイスに適用します。

BPDU ガードのイネーブル化

BPDU ガードをイネーブルにして、PortFast が設定された、BPDU を受信するインターフェイスを シャットダウンするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# [no] spanning-tree portfast bpduguard	スイッチの PortFast が設定されたすべてのインター フェイス上で BPDU ガードをイネーブルにします。
		BPDU ガードをディセーブルにする場合は、 no キーワードを使用します。
ステップ 2	Switch(config)# end	コンフィギュレーション モードを終了します。
ステップ 3	Switch# show spanning-tree summary totals	BPDU の設定を確認します。

次に、BPDU ガードをイネーブルにする例を示します。

Switch(config)# spanning-tree portfast bpduguard
Switch(config)# end
Switch#

次に、BPDU 設定を確認する例を示します。

Switch# show spanning-tree summary totals

Root bridge for: none.
PortFast BPDU Guard is enabled
Etherchannel misconfiguration guard is enabled
UplinkFast is disabled
BackboneFast is disabled
Default pathcost method used is short

Name			Blocking	Listening	Learning	Forwarding	STP	Active
	34	VLANs	0	0	0	36	36	
Switch#								

PortFast BPDU フィルタリングの概要

Cisco IOS Release 12.2(25)EW 以降でサポートされる PortFast BPDU フィルタリングによって、管理者はシステムが特定のポートで BPDU を送受信しないようにできます。

グローバルに設定した場合、PortFast BPDU フィルタリングは動作可能なすべての PortFast ポートに適用されます。動作可能 PortFast ステートのポートは、ホストに接続されているとみなされ、通常は BPDU をドロップします。BPDU を受信した動作可能 PortFast は、ただちに動作可能 PortFast ステートではなくなります。その場合、そのポートでは PortFast BPDU フィルタリングがディセーブルになり、STP はそのポートでの BPDU の送信を再開します。

PortFast BPDU フィルタリングは、ポート単位での設定もできます。ポート上で PortFast BPDU フィルタリングを明示的に設定すると、そのポートは BPDU をまったく送信せず、受信したすべての BPDU をドロップします。



ホストに接続されていないポート上で PortFast BPDU フィルタリングを明示的に設定した場合、ポートは受信したすべての BPDU を無視してフォワーディング ステートになるので、ブリッジング ループが発生する可能性があります。

PortFast BPDU フィルタリングをグローバルにイネーブル化し、PortFast BPDU フィルタリングのデフォルトでポートを設定した場合(「BackboneFast のイネーブル化」[p.19-19] を参照)、PortFast が PortFast BPDU フィルタリングをイネーブルまたはディセーブルにします。

ポートがデフォルトに設定されていない場合、PortFast の設定が PortFast BPDU フィルタリングに影響することはありません。表 19-1 に、可能性のあるすべての PortFast BPDU フィルタリングの組み合わせを示します。PortFast BPDU フィルタリングによって、アクセス ポートはエンド ホストが接続されるとただちに、フォワーディング ステートに直接移行します。

表 19-1 PortFast BPDU フィルタリング ポートの設定

ポート単位の設定	グローバルな設定	PortFast ステート	PortFast BPDU フィルタリングステート
デフォルト	イネーブル	イネーブル	イネーブル ¹
デフォルト	イネーブル	ディセーブル	ディセーブル
デフォルト	ディセーブル	該当しない	ディセーブル
ディセーブル	該当しない	該当しない	ディセーブル
イネーブル	該当しない	該当しない	イネーブル

^{1.} ポートは少なくとも 10 個の BPDU を送信します。そのポートが BPDU を 1 つでも受信すると、PortFast および PortFast BPDU フィルタリングがディセーブルになります。

PortFast BPDU フィルタリングのイネーブル化

PortFast BPDU フィルタリングをグローバルにイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	hmd6:1+om dofo1+	スイッチ上で BPDU フィルタリングをグローバルに イネーブルにします。
ステップ 2	Switch# show spanning-tree summary totals	BPDU の設定を確認します。

次に、ポート上で PortFast BPDU フィルタリングをイネーブルにする例を示します。

Switch(config)# spanning-tree portfast bpdufilter default
Switch(config)# Ctrl-Z

次に、PVST+モードでBPDU設定を確認する例を示します。

 ${\tt Switch\#} \ \ \textbf{show spanning-tree summary totals}$

Root bridge for:VLAN0010

EtherChannel misconfiguration guard is enabled

Extended system ID is disabled

Portfast is enabled by default PortFast BPDU Guard is disabled by default Portfast BPDU Filter is enabled by default Loopguard is disabled by default

UplinkFast is disabled BackboneFast is disabled Pathcost method used is long

 Name
 Blocking Listening Learning Forwarding STP Active

 2 vlans
 0
 0
 0
 3
 3

Switch#



PVST+については、第17章「STP および MST の設定」を参照してください。

PortFast BPDU フィルタリングをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# interface fastEthernet 4/4	設定するインターフェイスを選択します。
ステップ 2	<pre>Switch(config-if)# spanning-tree bpdufilter enable</pre>	BPDU フィルタリングをイネーブルにします。
ステップ 3	Switch# show spanning-tree interface fastethernet 4/4	設定を確認します。

次に、ポート FastEthernet 4/4 上で PortFast BPDU フィルタリングをイネーブルにする例を示します。

Switch(config)# interface fastethernet 4/4
Switch(config-if)# spanning-tree bpdufilter enable
Switch(config-if)# ^Z

次に、PortFast BPDU フィルタリングがイネーブルになっていることを確認する例を示します。

Switch# show spanning-tree interface fastethernet 4/4

Vlan Role Sts Cost Prio.Nbr Status
----VLAN0010 Desg FWD 1000 160.196 Edge P2p

次に、ポート上の詳細を表示する例を示します。

Switch# show spanning-tree interface fastEthernet 4/4 detail

Port 196 (FastEthernet4/4) of VLAN0010 is forwarding
Port path cost 1000, Port priority 160, Port Identifier 160.196.
Designated root has priority 32768, address 00d0.00b8.140a
Designated bridge has priority 32768, address 00d0.00b8.140a
Designated port id is 160.196, designated path cost 0
Timers:message age 0, forward delay 0, hold 0
Number of transitions to forwarding state:1
The port is in the portfast mode by portfast trunk configuration
Link type is point-to-point by default
Bpdu filter is enabled
BPDU:sent 0, received 0
Switch#

UplinkFast の概要



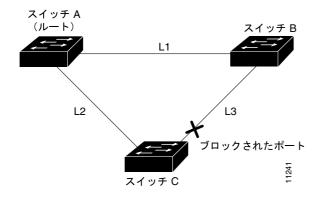
(注)

UplinkFast は、ワイヤリング クローゼット スイッチに使用すると最も効果的です。それ以外の用途に、この機能は有効ではありません。

スパニングツリー UplinkFast 機能は直接リンク障害後のコンバージェンスを高速化し、アップリンク グループを使用して冗長レイヤ 2 リンク間のロード バランシングを実行します。コンバージェンスは、特定のルーティング プロトコルを実行するインターネットワーキング デバイス グループがインターネットワークのトポロジ変更後にそのトポロジに合意する速度と能力です。アップリンク グループは、(VLAN ごとの) レイヤ 2 インターフェイスの集合で、どの時点でも、その中の 1 つのインターフェイスだけが転送を行います。つまり、アップリンク グループは、転送を行う 1 つのルート ポートと、(セルフ ループ ポートを除く) ブロックされたポートの集合で構成されます。アップリンク グループは、転送中のリンクで障害が起きた場合に代替パスを提供します。

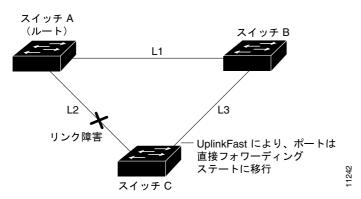
図 19-2 は、リンク障害が発生していないときのトポロジ例です。スイッチ A (ルート スイッチ) は、リンク L1 を通じてスイッチ B に、リンク L2 を通じてスイッチ C に直接接続されています。スイッチ B に直接接続されているスイッチ C のレイヤ 2 インターフェイスは、ブロッキング ステートです。





スイッチ C が、現在アクティブ リンクであるルート ポート上の L2 でリンク障害(直接リンク障害)を検出すると、UplinkFast はスイッチ C でブロックされていたポートのブロックを解除し、リスニング ステートおよびラーニング ステートを経由せずに、ただちにフォワーディング ステートに移行させます(図 19-3 を参照)。このスイッチオーバーに要する時間は $1 \sim 5$ 秒程度です。

図 19-3 直接リンク障害が発生したあとの UplinkFast



UplinkFast のイネーブル化

UplinkFast は、ブリッジ プライオリティを 49,152 に高め、スイッチ上のすべてのインターフェイス のスパニングツリー ポート コストに 3000 を追加して、スイッチがルート スイッチになるのを防ぎます。 max_update_rate 値は、1 秒間に送信されるマルチキャスト パケット数を表します(デフォルトは 150 pps です)。

ブリッジ プライオリティを設定している VLAN 上で、UplinkFast をイネーブルにすることはできません。 ブリッジ プライオリティを設定している VLAN 上で UplinkFast をイネーブルにするには、 グローバル コンフィギュレーション モードで no spanning-tree vlan $vlan_ID$ priority コマンドを入力し、 VLAN のブリッジ プライオリティをデフォルトの値に戻します。



UplinkFast をイネーブルにすると、スイッチ上のすべての VLAN に作用します。個々の VLAN について UplinkFast を設定することはできません。

UplinkFast をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# [no] spanning-tree uplinkfast [max-update-rate max_update_rate]	UplinkFast をイネーブルにします。
		UplinkFast をディセーブルにして、デフォルト レー
		トを復元し、コマンドを使用する場合は、no キー
		ワードを使用します。
ステップ 2	Switch(config)# end	コンフィギュレーション モードを終了します。
ステップ 3	Switch# show spanning-tree vlan vlan_ID	VLAN 上で UplinkFast がイネーブルになっているこ
		とを確認します。

次に、UplinkFast をイネーブルにして、最大アップデート速度を 400 pps に設定する例を示します。

Switch(config)# spanning-tree uplinkfast max-update-rate 400
Switch(config)# exit
Switch#

次に、UplinkFast がイネーブルになった VLAN を確認する例を示します。

Switch# show spanning-tree uplinkfast

UplinkFast is enabled

Station update rate set to 150 packets/sec.

UplinkFast statistics

Number of transitions via uplinkFast (all VLANs) :14

Number of proxy multicast addresses transmitted (all VLANs) :5308

Name	Interface List
VLAN1	Fa6/9(fwd), Gi5/7
VLAN2	Gi5/7(fwd)
VLAN3	Gi5/7(fwd)
VLAN4	
VLAN5	
VLAN6	
VLAN7	
VLAN8	
VLAN10	
VLAN15	
VLAN1002	Gi5/7(fwd)
VLAN1003	Gi5/7(fwd)
VLAN1004	Gi5/7(fwd)
VLAN1005	Gi5/7(fwd)
Switch#	

BackboneFast の概要

BackboneFast は、UplinkFast を補足するテクノロジーです。UplinkFast は、リーフノード スイッチ に直接接続するリンク上での障害に、迅速に対応するよう設計されていますが、バックボーン コア の間接的な障害には効果がありません。BackboneFast は最大エージング設定に基づいて最適化を行います。間接的な障害に対するデフォルトのコンバージェンス時間が、50 秒から 30 秒に短縮されます。ただし、BackboneFast によって転送遅延が解消されることはないため、直接の障害には効果がありません。



BackboneFast は、ネットワークのすべてのスイッチ上でイネーブルにする必要があります。

スイッチが指定スイッチから、ルート ブリッジと指定ブリッジを同じスイッチとして識別する BPDU を受信する場合があります。これは本来ありえないことなので、この BPDU は不良とみなされます。

BPDU が不良とみなされるのは、指定スイッチからのリンクがルート ブリッジとのリンクを損失した場合です。指定スイッチは、BPDU を送信して現在のルート ブリッジおよび指定ブリッジとしての状態を伝えます。受信側スイッチは、最大エージング設定で定義された期間、不良 BPDU を無視します。

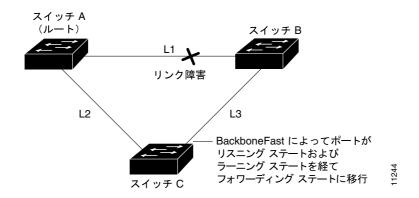
不良 BPDU を受信したあと、受信側スイッチはルート ブリッジへの代替パスがあるかどうかを確認しようとします。

- 不良 BPDU を受け取ったポートがすでにブロッキング モードであれば、スイッチ上のルートポートとその他のブロックされたポートがルート ブリッジへの代替パスになります。
- 不良 BPDU がルート ポートに到達した場合には、そのときにブロックされたすべてのポートが ルート ブリッジへの代替パスになります。また、不良 BPDU をルート ポートで受け取り、スイッチ上にブロックされたポートがほかにない場合、受信側スイッチはルート ブリッジへのリンクがダウンし、最大エージング設定で定義された時間が経過したと判断し、スイッチをルート スイッチに変更します。

スイッチがルート ブリッジへの代替パスを見つけると、この新しい代替パスを使用します。この新しいパスと、他のすべての代替パスは、Root Link Query (RLQ) BPDU の送信に使用されます。BackboneFast がイネーブルの場合、不良 BPDU を受け取るとただちに RLQ BPDU が送信されます。このプロセスにより、バックボーン リンク障害の場合にコンバージェンスが速くなる場合があります

図 19-4 は、リンク障害が発生していないときのトポロジ例です。スイッチ A (ルート スイッチ) は、リンク L1 を通じてスイッチ B に、リンク L2 を通じてスイッチ C に直接接続されています。この例では、スイッチ B のプライオリティがスイッチ A よりも低く、スイッチ C よりも高いため、スイッチ B が L3 の指定ブリッジになります。最終的に、スイッチ B に直接接続されているスイッチ C のレイヤ 2 インターフェイスは、ブロッキング ステートになる必要があります。

図 19-4 間接リンク障害が発生する前の BackboneFast



次に、L1 に障害が発生したと仮定します。このセグメントに直接接続されているスイッチ A とスイッチ B は、すぐにリンクのダウンを認識します。スイッチ C のブロッキング インターフェイスは、ネットワークが自己回復できるようにフォワーディング ステートを開始する必要があります。ただし、スイッチ C は L1 に直接接続していないため、最大エージング設定で定義された時間が経過するまで、通常の STP のルールに従って L3 上での BPDU 送信を開始しません。

BackboneFast が設定されていない STP 環境では、L1 に障害が発生した場合、スイッチ C はリンク L1 に直接接続していないため、この障害を検出できません。ただし、スイッチ B は L1 を経由して 直接ルート スイッチに接続しているため障害を検出し、スイッチ B 自身をルートに選定します。スイッチ B はスイッチ C への設定 BDPU の送信を開始し、スイッチ B 自身をルートとしてリストします。

BackboneFast を使用して最大エージング設定で定義された時間 (20 秒) の遅延を解消する場合、次の処理も行われます。

- **1.** スイッチ C がスイッチ B から不良設定 BPDU を受信すると、スイッチ C は間接障害が発生したことを推測します。
- 2. スイッチ C は RLQ を送信します。
- 3. スイッチ A は RLQ を受信します。 スイッチ A はルート ブリッジであるため、 RLQ 応答で自身をルート ブリッジにリストして応答します。
- 4. スイッチ C が既存のルート ポート上で RLQ 応答を受信すると、スイッチ C はルート ブリッジ と安定した接続を維持していることを認識します。 スイッチ C は RLQ 要求を発信しているため、 RLQ 応答を他のスイッチに転送する必要はありません。
- **5.** BackboneFast により、スイッチ C のブロックされたポートは、そのポートの最大エージング設定で定義されている時間の経過を待たずに、ただちにリスニング ステートに移行します。
- **6.** BackboneFast はスイッチ C のレイヤ 2 インターフェイスをフォワーディング ステートに移行させ、スイッチ B からスイッチ A へのパスを提供します。

このスイッチオーバーに要する時間は約30秒で、デフォルトの転送遅延時間15秒が設定されている場合の転送遅延時間の2倍です。

図 19-5 に、BackboneFast でリンク L1 の障害に応じてトポロジを再設定する方法を示します。

図 19-5 間接リンク障害が発生したあとの BackboneFast

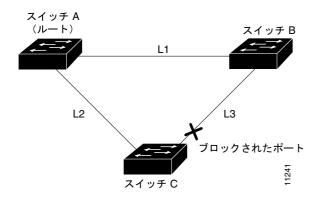
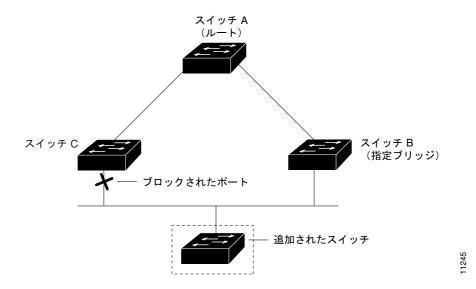


図 19-6 に示すメディア共有型トポロジに新しいスイッチが組み込まれた場合、BackboneFast は起動されません。これは、認識されている指定ブリッジ(スイッチ B)から不良 BPDU が着信しないためです。新しいスイッチは、ルート スイッチと称される不良 BPDU の送信を開始します。ただし、他のスイッチはこれらの不良 BPDU を無視します。その結果、新しいスイッチはスイッチ B がルート スイッチであるスイッチ A への指定ブリッジであることを学習します。

図 19-6 メディア共有型トポロジにおけるスイッチの追加



BackboneFast のイネーブル化



(注)

BackboneFast を有効にするには、ネットワークのすべてのスイッチ上で BackboneFast をイネーブルにする必要があります。BackboneFast はサードパーティ製スイッチに対応していますが、トークンリング VLAN 上ではサポートされていません。

BackboneFast をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# [no] spanning-tree backbonefast	BackboneFast をイネーブルにします。
		BackboneFast をディセーブルにする場合は、 no キーワードを使用します。
ステップ 2	Switch(config)# end	コンフィギュレーション モードを終了します。
ステップ 3	Switch# show spanning-tree backbonefast	BackboneFast がイネーブルになっていることを 確認します。

次に、BackboneFast をイネーブルにする例を示します。

```
Switch(config)# spanning-tree backbonefast
Switch(config)# end
Switch#
```

次に、BackboneFast がイネーブルになっていることを確認する例を示します。

```
{\tt Switch\#} \ \ \textbf{show spanning-tree backbonefast}
```

 ${\tt BackboneFast \ is \ enabled}$

```
BackboneFast statistics
```

```
Number of transition via backboneFast (all VLANs) : 0
Number of inferior BPDUs received (all VLANs) : 0
Number of RLQ request PDUs received (all VLANs) : 0
Number of RLQ response PDUs received (all VLANs) : 0
Number of RLQ request PDUs sent (all VLANs) : 0
Number of RLQ response PDUs sent (all VLANs) : 0
Switch#
```

次に、ポート ステートの要約を表示する例を示します。

Switch#show spanning-tree summary

Root bridge for:VLAN0001, VLAN1002-VLAN1005

Extended system ID is disabled

Portfast is enabled by default
PortFast BPDU Guard is disabled by default
Portfast BPDU Filter is enabled by default
Loopguard is disabled by default
EtherChannel misconfiguration guard is enabled

UplinkFast is enabled BackboneFast is enabled Pathcost method used is short

Name	Blocking	Listening	Learning	Forwarding	STP Active	
VLAN0001	0	0	0	3	3	
VLAN1002	0	0	0	2	2	
VLAN1003	0	0	0	2	2	
VLAN1004	0	0	0	2	2	
VLAN1005	0	0	0	2	2	
5 vlans	0	0	0	11	11	

BackboneFast statistics

Number of transition via backboneFast (all VLANs) :0
Number of inferior BPDUs received (all VLANs) :0
Number of RLQ request PDUs received (all VLANs) :0
Number of RLQ response PDUs received (all VLANs) :0
Number of RLQ request PDUs sent (all VLANs) :0
Number of RLQ response PDUs sent (all VLANs) :0

Switch#

次に、スパニングツリー ステート セクションのすべての行を表示する例を示します。

Switch#show spanning-tree summary totals

Root bridge for:VLAN0001, VLAN1002-VLAN1005

Extended system ID is disabled

Portfast is enabled by default
PortFast BPDU Guard is disabled by default
Portfast BPDU Filter is enabled by default
Loopguard is disabled by default
EtherChannel misconfiguration guard is enabled

UplinkFast is enabled BackboneFast is enabled Pathcost method used is short

Name	Blocking	Listening	Learning	Forwarding	STP Active
5 vlans	0	0	0	11	11

BackboneFast statistics

Number of transition via backboneFast (all VLANs) :0
Number of inferior BPDUs received (all VLANs) :0
Number of RLQ request PDUs received (all VLANs) :0
Number of RLQ response PDUs received (all VLANs) :0
Number of RLQ request PDUs sent (all VLANs) :0
Number of RLQ response PDUs sent (all VLANs) :0

Switch#



CHAPTER

20

EtherChannel の設定

この章では、CLI (コマンドライン インターフェイス)を使用して Catalyst 4500 シリーズ スイッチレイヤ 2 またはレイヤ 3 インターフェイス上で EtherChannel を設定する方法について説明します。設定上の注意事項、設定手順、および設定例についても示します。

この章の主な内容は、次のとおりです。

- EtherChannel の概要 (p.20-2)
- EtherChannel 設定時の注意事項および制約事項 (p.20-6)
- EtherChannel の設定 (p.20-7)



<u>一</u> (注)

以降のコマンドは、スーパーバイザ エンジンのアップリンク ポートを含む Catalyst 4500 シリーズ スイッチ上のすべてのイーサネット インターフェイスで使用できます。



(注)

この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/cr/index.htm

EtherChannel の概要

EtherChannel は、個々のイーサネット リンクを 1 つの論理リンクにバンドルし、Catalyst 4500 シリーズ スイッチと別のスイッチまたはホスト間で最大 1600 Mbps (Fast EtherChannel 全二重) 16 Gbps (Gigabit EtherChannel) または 40 Gbps (10 Gigabit EtherChannel)の帯域幅を可能にします。

Catalyst 4500 シリーズ スイッチ スイッチは、最大 64 個の EtherChannel をサポートしています。 Catalyst 4500 シリーズ スイッチ スイッチにある複数のモジュール上の(設定に互換性のある)イー サネット インターフェイスを 8 つまで使用して、1 つの EtherChannel を形成できます。各 EtherChannel のすべてのインターフェイスは同じ速度で、レイヤ 2 またはレイヤ 3 インターフェイスとして設定されている必要があります。



(注)

Catalyst 4500 シリーズ スイッチ スイッチに接続するネットワーク デバイスによって、1 つの EtherChannel にバンドルできるインターフェイス数が制限される場合があります。

Ether Channel 内のセグメントで障害が発生すると、障害リンク上でそれまで伝送されていたトラフィックがその Ether Channel 内の残りのセグメントに切り替えられます。セグメントに障害が発生すると、スイッチ、Ether Channel、障害リンクを特定する SNMP (簡易ネットワーク管理プロトコル)トラップが送信されます。 Ether Channel の 1 つのセグメントに着信したブロードキャスト パケットおよびマルチキャスト パケットが、Ether Channel の別のセグメントに戻されることはありません。



(注)

Catalyst 4500 シリーズ スイッチのポート チャネル リンク障害のスイッチオーバーには、50 ミリ秒 かかり、SONET のようなリンク障害のスイッチオーバーには十分です。

ここでは、EtherChannel の機能について説明します。

- ポートチャネル インターフェイス (p.20-2)
- EtherChannel の設定方法 (p.20-3)
- ロード バランシング (p.20-5)

ポートチャネル インターフェイス

各 EtherChannel には、番号付きのポートチャネル インターフェイスが 1 つずつあります。ポートチャネル インターフェイスに適用される設定は、そのインターフェイスに割り当てられたすべての物理インターフェイスに影響します。



(注)

QoS (Quality Of Service) はメンバに伝播しません。デフォルトは QoS $\cos = 0$ および QoS dscp = 0 で、ポートチャネルに適用されます。個々のインターフェイスに適用される入力および出力ポリシーは無視されます。

EtherChannel を設定したあとで、ポートチャネルインターフェイスに適用する設定は、EtherChannel に対して有効になります。一方、物理インターフェイスに適用する設定は、適用先のインターフェイスだけに有効です。EtherChannel のすべてのポートのパラメータを変更するには、ポートチャネ

ル インターフェイスに対してコンフィギュレーション コマンドを適用してください (このようなコマンドには、Spanning-Tree Protocol [STP; スパニングツリー プロトコル] コマンドや、レイヤ 2 EtherChannel をトランクとして設定するコマンドがあります)。

EtherChannel の設定方法

ここでは、EtherChannel の設定方法について説明します。

- EtherChannel 設定の概要 (p.20-3)
- EtherChannel の手動設定 (p.20-3)
- PAgP EtherChannel の設定 (p.20-4)
- IEEE 802.3ad LACP EtherChannel 設定 (p.20-4)

EtherChannel 設定の概要

EtherChannel を手動で設定することもできますが、Port Aggregation Control Protocol (PAgP)を使用することも、または Cisco IOS Release 12.2(25)EWA 以降のリリースでは Link Aggregation Control Protocol (LACP)を使用して EtherChannel を形成することもできます。EtherChannel プロトコルにより、同様の特性を持つポートが、接続されたネットワーク デバイスとのダイナミック ネゴシエーションを通じて EtherChannel を形成できます。PAgP はシスコ独自のプロトコルで、LACP は IEEE 802.3ad で定義されています。

PAgP と LACP は相互動作しません。PAgP を使用するように設定されたポートは、LACP を使用するように設定されたポートと EtherChannel を形成できず、その逆もまた不可能です。

表 20-1 に、ユーザが設定できる EtherChannel モードを示します。

表 20-1 EtherChannel のモード

モード	説明
on	LAN ポートを無条件にチャネル化するモード。on モードでは、on モードの LAN ポート グループが、on モードの別の LAN ポート グループに接続されている場合に限り、使用可能な EtherChannel が存在します。on モードで設定されたポートはネゴシエーションを行わないため、ポート間のネゴシエーション トラフィックはありません。
auto	PAgP モード。LAN ポートをパッシブ ネゴシエーション ステートにします。ポートは受信した PAgP パケットには応答しますが、PAgP ネゴシエーションは開始しません。
desirable	PAgP モード。LAN ポートをアクティブ ネゴシエーション ステートにします。ポートは PAgP パケットを送信して、他の LAN ポートとのネゴシエーションを開始します。
passive	LACP モード。ポートをパッシブ ネゴシエーション ステートにします。ポートは受信した LACP パケットには応答しますが、LCAP ネゴシエーションは開始しません。
active	LACP モード。ポートをアクティブ ネゴシエーション ステートにします。ポートは LACP パケットを送信して、他のポートとのネゴシエーションを開始します。

EtherChannel の手動設定

手動で設定された EtherChannel ポートは、EtherChannel プロトコル パケットを交換しません。EtherChannel 内のすべてのポートを互換性がある設定にした場合のみ、手動で設定された EtherChannel が形成されます。

PAgP EtherChannel の設定

PAgP は、LAN ポート間で PAgP パケットを交換することにより、EtherChannel を自動的に作成します。PAgP パケットが交換されるのは、auto モードおよび desirable モードのポート間に限られます。

このプロトコルは、LAN ポート グループの機能を動的に学習し、他の LAN ポートに通知します。 PAgP は、正確に一致しているイーサネット リンクを識別すると、これらのリンクを 1 つの EtherChannel としてまとめます。形成された EtherChannel は、単一ブリッジ ポートとしてスパニングツリーに追加されます。

auto モードおよび **desirable** モードでは、PAgP が LAN ポート間でネゴシエーションを行い、ポート速度やトランキング ステートなどの基準に従って EtherChannel を形成できるかどうかを判別します。レイヤ 2 EtherChannel は VLAN 数も基準として使用します。

PAgP モードが異なる場合でも、モードに互換性があるかぎり、LAN ポートで EtherChannel を形成できます。次に例を示します。

- desirable モードの LAN ポートは、desirable モードの他の LAN ポートと EtherChannel を形成できます。
- **desirable** モードの LAN ポートは、**auto** モードの他の LAN ポートと EtherChannel を形成できます。
- auto モードの LAN ポートは、双方のポートがネゴシエーションを開始しないので、auto モードの他の LAN ポートと EtherChannel を形成できません。

IEEE 802.3ad LACP EtherChannel 設定

Cisco IOS Release 12.2(25)EWA 以降のリリースは、IEEE 802.3ad LACP EtherChannel をサポートしています。LACP は、LAN ポート間でLACP パケットを交換することにより、EtherChannel を自動的に作成します。LACP パケットが交換されるのは、passive および active モードのポート間に限られます。

このプロトコルは、LAN ポート グループの機能を動的に学習し、他の LAN ポートに通知します。 LACP は、正確に一致しているイーサネット リンクを識別すると、これらのリンクを 1 つの EtherChannel としてまとめます。形成された EtherChannel は、単一ブリッジ ポートとしてスパニングツリーに追加されます。

passive および active モードでは、LACP が LAN ポート間でネゴシエーションを行い、ポート速度 やトランキング ステートなどの基準に従って EtherChannel を形成できるかどうかを判別します。レ イヤ 2 EtherChannel は VLAN 数も基準として使用します。

LACP モードが異なる場合でも、モードに互換性があるかぎり、LAN ポートで EtherChannel を形成できます。次に例を示します。

- active モードの LAN ポートは、active モードの他の LAN ポートと EtherChannel を形成できます。
- active モードの LAN ポートは、passive モードの他の LAN ポートと EtherChannel を形成できます。
- passive モードの LAN ポートは、双方のポートがネゴシエーションを開始しないので、passive モードの他の LAN ポートと EtherChannel を形成できません。

LACP の設定に使用するパラメータは、次のとおりです。

• LACP システム プライオリティ LACP が稼働する各 スイッチ上で、LACP システム プライオリティを設定できます。システム プライオリティは、自動的に設定することも、CLI を使用して設定することもできます。「LACP システム プライオリティおよびシステム ID の設定」(p.20-13)を参照してください。LACP は、システム プライオリティとスイッチの MAC(メ

ディア アクセス制御) アドレスを組み合わせてシステム ID を形成します。また、これを他のシステムとのネゴシエーション時にも使用します。



(注) LACP システム ID は、LACP システム プライオリティ値とスイッチの MAC アドレス を組み合わせたものです。

- LACP ポート プライオリティ LACP を使用するように設定されている各ポート上で、LACP ポート プライオリティを設定する必要があります。ポート プライオリティは、自動的に設定することも、CLI を使用して設定することもできます。「レイヤ 2 EtherChannel の設定(p.20-10)を参照してください。LACP は、ポート プライオリティとポート番号を組み合わせて、ポート ID を形成します。
- LACP 管理キー LACP は、LACP を使用するように設定された各ポートのチャネル グループ ID 番号と等しい管理キー値を自動的に設定します。他のポートに合算されるポートの能力は、管理キーを使用して定義します。他のポートに合算されるポートの能力は、次の要因によって決定します。
 - ポートの物理特性 (データ レート、デュプレックス能力、ポイントツーポイントまたは共有メディアなど)
 - ユーザが設定したコンフィギュレーション制約

LACP は、最大数の互換ポートを EtherChannel に設定しようとします (ハードウェア上の最大許容数は 8 ポートです)。ポートをチャネルにアクティブとして組み込めない場合は、チャネル ポートで障害が発生した場合にも自動的に組み込まれません。



(注) スタンバイおよび「サブチャネル化」は LACP および PAgP でサポートされません。

ロード パランシング

EtherChannel は、チャネルのリンクに対するトラフィック負荷のバランスを取ります。つまり EtherChannel は、フレーム内のアドレスやポートで構成されるバイナリ パターンの一部を数値化 し、チャネル内のリンクの 1 つを選択します。負荷のバランスを取るために、EtherChannel は、MAC アドレス、IP アドレス、またはレイヤ 4 ポート番号と、メッセージの送信元、メッセージの宛先、または両方を使用します。

最も多様な設定が可能なオプションを使用してください。たとえば、チャネルのトラフィックが単一の MAC アドレスのみに送信される場合、宛先 MAC アドレスを使用すると、常にチャネル内の同じリンクが選択されてしまいます。送信元アドレスまたは IP アドレスを使用する方が、ロードバランシングの効果が上がります。



<u>一</u> (注)

ロード バランシングは、グローバルにのみ設定可能です。したがって、すべてのチャネル(手動設定、PAgP、またはLACP)は同じロードバランシング方式を使用します。

ロード バランシングについての詳細は、「EtherChannel ロード バランシングの設定」(p.20-14)を参照してください。

EtherChannel 設定時の注意事項および制約事項

EtherChannel インターフェイスの設定に問題があると、ネットワーク ループなどの問題を回避する ために、EtherChannel インターフェイスが自動的にディセーブルになります。次の注意事項と制約 事項に従って、設定時に問題が起こらないようにしてください。

- すべてのモジュールのイーサネット インターフェイスはすべて、物理的に連続しているかまた は同一モジュール上といったインターフェイスに関する要件のない EtherChannel (最大 8 つの インターフェイス) をサポートしています。
- EtherChannel のすべてのインターフェイスを、同じ速度およびデュプレックス モードで動作するように設定します。
- EtherChannel のすべてのインターフェイスをイネーブルにします。EtherChannel 内のインターフェイスを 1 つダウンにするとリンク障害として処理され、そのインターフェイスのトラフィックが EtherChannel 内の残りのインターフェイスの 1 つに転送されます。
- インターフェイスの 1 つが Switched Port Analyzer (SPAN; スイッチド ポート アナライザ) 宛先ポートの場合、EtherChannel は形成されません。
- レイヤ 3 EtherChannel の場合
 - レイヤ3アドレスを、チャネルの物理インターフェイスではなく、ポートチャネル論理インターフェイスに割り当てます。
- レイヤ 2 EtherChannel の場合
 - EtherChannel 内のすべてのインターフェイスを同じ VLAN に割り当てるか、またはトランクとして設定してください。
 - トランク インターフェイスから EtherChannel を設定する場合は、すべてのトランクでトランキング モードとネイティブ VLAN が同じであることを確認してください。 EtherChannel のインターフェイスのトランク モードが異なる、またはネイティブ VLAN が異なる場合、予期しない結果を招くことがあります。
 - EtherChannel は、トランキング レイヤ 2 EtherChannel 内のすべてのインターフェイスで同 じ許容範囲の VLAN をサポートしています。選択したインターフェイスの許容範囲が異な る場合、インターフェイスは EtherChannel を形成しません。
 - STP ポート パス コストが異なるインターフェイスは、互換性がある設定を行っているかぎ り、EtherChannel を形成できます。異なる STP ポート パス コストを設定しても、 EtherChannel のインターフェイスの互換性は損なわれません。
- EtherChannel を設定したあとで、ポートチャネルインターフェイスに適用する設定は、 EtherChannel に対して有効になります。一方、物理インターフェイスに適用する設定は、設定 するインターフェイスだけに有効です。

ストーム制御はこの規則の例外です。たとえば、EtherChannel の一部のメンバにストーム制御を設定することはできません。ストーム制御はすべてのポートに対して設定するか、設定しないかのどちらかにする必要があります。一部のポートのみにストーム制御を設定する場合、そのポートは EtherChannel インターフェイスからドロップされます(中断ステート)。したがって、物理インターフェイス レベルではなく、ポートチャネル インターフェイス レベルでストーム制御を設定してください。

- ポート セキュリティがイネーブルである物理インターフェイスは、ポート セキュリティが EtherChannel 上でもイネーブルである場合にのみ、レイヤ 2 EtherChannel に加入できます。イネーブルでない場合、コマンドは CLI によって拒否されます。
- 802.1X ポートに EtherChannel は設定できません。

EtherChannel の設定

ここでは、EtherChannel を設定する手順について説明します。

- レイヤ 3 EtherChannel の設定 (p.20-7)
- レイヤ 2 EtherChannel の設定 (p.20-10)
- LACP システム プライオリティおよびシステム ID の設定 (p.20-13)
- EtherChannel ロード バランシングの設定 (p.20-14)
- EtherChannel からのインターフェイスの削除 (p.20-15)
- EtherChannel の削除 (p.20-15)



(注)

インターフェイスが正しく設定されていることを確認してください (「EtherChannel 設定時の注意事項および制約事項」[p.20-6]を参照)。

レイヤ 3 EtherChannel の設定

レイヤ 3 EtherChannel を設定するには、ポートチャネル論理インターフェイスを作成し、イーサネット インターフェイスをポートチャネルにします。

ここでは、レイヤ3 EtherChannel の設定について説明します。

- ポートチャネル論理インターフェイスの作成 (p.20-7)
- 物理インターフェイスのレイヤ 3 EtherChannel としての設定 (p.20-8)

ポートチャネル論理インターフェイスの作成



(注)

IP アドレスを物理インターフェイスから EtherChannel に移動させるには、ポートチャネル インターフェイスを設定する前に物理インターフェイスから IP アドレスを削除する必要があります。

レイヤ 3 EtherChannel 用のポートチャネル インターフェイスを作成するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# interface port-channel port_channel_number	ポートチャネル インターフェイスを作成します。 $port_channel_number$ の値は $1 \sim 64$ です。
ステップ 2	Switch(config-if)# ip address ip_address mask	EtherChannel に IP アドレスおよびサブネット マスクを割り当てます。
ステップ 3	Switch(config-if)# end	コンフィギュレーション モードを終了します。
ステップ 4	Switch# show running-config interface port-channel port_channel_number	設定を確認します。

次に、インターフェイス port-channel 1 を作成する例を示します。

Switch# configure terminal
Switch(config) # interface port-channel 1
Switch(config-if) # ip address 172.32.52.10 255.255.255.0
Switch(config-if) # end

次に、インターフェイス port-channel 1 の設定を確認する例を示します。

```
Switch# show running-config interface port-channel 1
Building configuration...

Current configuration:
!
interface Port-channel1
ip address 172.32.52.10 255.255.255.0
no ip directed-broadcast
end

Switch#
```

物理インターフェイスのレイヤ 3 EtherChannel としての設定

物理インターフェイスをレイヤ 3 EtherChannel として設定するには、各インターフェイスで次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# interface {fastethernet gigabitethernet tengigabitethernet} slot/port	設定する物理インターフェイスを選択します。
ステップ 2	Switch(config-if)# no switchport	このインターフェイスをレイヤ 3 ルーテッド ポートにします。
ステップ 3	Switch(config-if)# no ip address	この物理インターフェイスに IP アドレスが割り 当てられていないことを確認します。
ステップ 4	Switch(config-if)# channel-group port_channel_number mode {active on auto passive desirable}	ポートチャネルでインターフェイスを設定し、 PAgP または LACP モードを指定します。
		PAgP を使用する場合、キーワード auto または desirable を入力します。
		LACP を使用する場合は、キーワード active または passive を入力します。
ステップ 5	Switch(config-if)# end	コンフィギュレーション モードを終了します。
ステップ 6	Switch# show running-config interface port-channel port_channel_number	設定を確認します。
	Switch# show running-config interface {fastethernet gigabitethernet tengigabitethernet} slot/port	
	Switch# show interfaces {fastethernet gigabitethernet tengigabitethernet} slot/port etherchannel	
	Switch# show etherchannel 1 port-channel	

次に、インターフェイス FastEthernet 5/4 および 5/5 を、port-channel 1、PAgP モード **desirable** に設定する例を示します。

```
Switch# configure terminal
Switch(config) # interface range fastethernet 5/4 - 5 (Note: Space is mandatory.)
Switch(config-if) # no switchport
Switch(config-if) # no ip address
Switch(config-if) # channel-group 1 mode desirable
Switch(config-if) # end
```



range キーワードの詳細については、「インターフェイスの範囲設定」(p.6-5)を参照してください。

```
次に、インターフェイス FastEthernet 5/4 の設定を確認する例を 2 つ示します。
Switch# show running-config interface fastethernet 5/4
Building configuration...
Current configuration:
interface FastEthernet5/4
no ip address
no switchport
no ip directed-broadcast
channel-group 1 mode desirable
Switch# show interfaces fastethernet 5/4 etherchannel
Port state = EC-Enbld Up In-Bndl Usr-Config
                    Mode = Desirable
Channel group = 1
                                              Gcchange = 0
                         GC = 0 \times 00010001
Port-channel = Po1
                                            Pseudo-port-channel = Po1
Port indx
                         Load = 0x55
           = 0
Flags: S - Device is sending Slow hello. C - Device is in Consistent state.
       A - Device is in Auto mode.
                                  P - Device realing Q - Quit timer is running.
                                        P - Device learns on physical port.
Timers: H - Hello timer is running.
       S - Switching timer is running. I - Interface timer is running.
Local information:
                                     Partner PAgP
                             Hello
                                                       Learning Group
        Flags State Timers Interval Count Priority Method Ifindex
Fa5/4
       SC U6/S7
                             30s
                                     1
                                              128
Partner's information:
                             Partner
         Partner
                                             Partner
                                                           Partner Group
Port
        Name
                             Device ID
                                             Port
                                                       Age Flags Cap.
Fa5/4
         JAB031301
                             0050.0f10.230c 2/45
                                                        1s SAC
```

Age of the port in the current state: 00h:54m:52s

Switch#

次に、インターフェイス port-channel 1 を設定したあとで、インターフェイスの設定を確認する例を示します。

Switch# show etherchannel 1 port-channel

Channel-group listing: Group: 1 Port-channels in the group: Port-channel: Pol Age of the Port-channel = 01h:56m:20s Number of ports = 2 Logical slot/port = 10/1 $= 0 \times 00010001$ HotStandBy port = null Port state = Port-channel L3-Ag Ag-Inuse Ports in the Port-channel: Index Load Port Fa5/6 00 Ω 0.0 Fa5/7 Time since last port bundled: 00h:23m:33s Fa5/6

レイヤ 2 EtherChannel の設定

Switch#

レイヤ 2 EtherChannel を設定するには、 ${\bf channel-group}$ コマンドでイーサネット インターフェイスを設定します。これにより、ポートチャネル論理インターフェイスが作成されます。



channel-group コマンドでレイヤ 2 イーサネット インターフェイスを設定すると、Cisco IOS ソフトウェアはレイヤ 2 EtherChannel のポートチャネル インターフェイスを作成します。

レイヤ 2 イーサネット インターフェイスをレイヤ 2 EtherChannel として設定するには、各インターフェイスで次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# interface {fastethernet gigabitethernet tengigabitethernet} slot/port	設定する物理インターフェイスを選択します。
ステップ 2	Switch(config-if)# channel-group port_channel_number mode {active on auto passive desirable}	ポートチャネルでインターフェイスを設定し、 PAgP または LACP モードを指定します。
		PAgP を使用する場合、キーワード auto または desirable を入力します。
		LACP を使用する場合は、キーワード active または passive を入力します。
ステップ 3	Switch(config-if)# end	コンフィギュレーション モードを終了します。

	コマンド	目的
ステップ 4	Switch# show running-config interface {fastethernet gigabitethernet} slot/port	設定を確認します。
	Switch# show interface {fastethernet gigabitethernet tengigabitethernet} slot/port etherchannel	

次に、インターフェイス FastEthernet 5/6 および 5/7 を、port-channel 2、PAgP モード **desirable** に設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface range fastethernet 5/6 - 7 (Note: Space is mandatory.)
Switch(config-if-range)# channel-group 2 mode desirable
Switch(config-if-range)# end
Switch# end
```



range キーワードの詳細については、「インターフェイスの範囲設定」(p.6-5)を参照してください。

次に、インターフェイス port-channel 2 の設定を確認する例を示します。

```
Switch# show running-config interface port-channel 2
Building configuration...

Current configuration:
!
interface Port-channel2
switchport access vlan 10
switchport mode access
end

Switch#
```

次に、インターフェイス FastEthernet 5/6 の設定を確認する例を 2 つ示します。

```
Switch# show running-config interface fastethernet 5/6
Building configuration...
Current configuration:
interface FastEthernet5/6
switchport access vlan 10
switchport mode access
channel-group 2 mode desirable
Switch# show interfaces fastethernet 5/6 etherchannel
Port state = EC-Enbld Up In-Bndl Usr-Config
                   Mode = Desirable
Channel group = 1
                                             Gcchange = 0
                         GC = 0x00010001
Port-channel = Po1
Port indx
          = 0
                         Load = 0x55
Flags: S - Device is sending Slow hello. C - Device is in Consistent state.
       A - Device is in Auto mode.
                                       P - Device learns on physical port.
       d - PAgP is down.
Timers: H - Hello timer is running.
                                      Q - Quit timer is running.
      S - Switching timer is running. I - Interface timer is running.
Local information:
                             Hello Partner PAgP
                                                     Learning Group
       Flags 5...
SC U6/S7
        Flags State Timers Interval Count Priority Method Ifindex
Fa5/6
                             30s
                                    1
                                              128
                                                        Any
                                                                 56
Partner's information:
         Partner
                             Partner
                                            Partner
                                                            Partner Group
                            Device ID
                                                      Age Flags Cap.
Port
        Name
                                            Port
Fa5/6
        JAB031301
                             0050.0f10.230c 2/47
                                                       18s SAC
                                                                  2F
```

Age of the port in the current state: 00h:10m:57s

次に、インターフェイス port-channel 2 を設定したあとで、インターフェイスの設定を確認する例を示します。

```
Switch# show etherchannel 2 port-channel
               Port-channels in the group:
Port-channel: Po2
Age of the Port-channel = 00h:23m:33s
                   = 10/2 Number of ports in agport = 2 = 0 \times 00020001 HotStandBurger
Logical slot/port = 10/2
GC
                  = Port-channel Ag-Inuse
Port state
Ports in the Port-channel:
Index Load Port
    00
           Fa5/6
 1
       00
               Fa5/7
Time since last port bundled: 00h:23m:33s Fa5/6
Switch#
```

LACP システム プライオリティおよびシステム ID の設定

LACP システム ID は、LACP システム プライオリティ値とスイッチの MAC アドレスを組み合わせたものです。

LACP システム プライオリティおよびシステム ID を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# lacp system-priority priority_value	(LACP で任意)有効な値は1 ~ 65535 です。数値が大きいほど、プライオリティは低くなります。デフォルトは32768 です。
	<pre>Switch(config)# no system port-priority</pre>	デフォルト値に戻します。
ステップ 2	Switch(config)# end	コンフィギュレーション モードを終了します。
ステップ 3	Switch# show lacp sys-id	設定を確認します。

次に、LACP システム プライオリティを設定する例を示します。

Switch# configure terminal
Switch(config)# lacp system-priority 23456
Switch(config)# end
Switch# show module

		Card Type					Serial No	
	+	+			+	+		
1	2	1000BaseX (GBIC) Supervis	sor(a	active)	WS-	-X4014	JAB063808	ΥZ
2	48	10/100BaseTX (RJ45)			WS-	-X4148-RJ	JAB044707	2W
3	48	10/100BaseTX (RJ45)V			WS-	-X4148-RJ45V	JAE061704	J6
4	48	10/100BaseTX (RJ45)V			WS-	-X4148-RJ45V	JAE061704	ML
M M	IAC addı	resses	Hw	Fw		Sw	Status	
+-			+	+		+	-+	
1 0	005.9a3	39.7a80 to 0005.9a39.7a81	2.1	12.1(12r)	EW	12.1(13)EW(0.26) Ok	
2 0	002.fd8	30.f530 to 0002.fd80.f55f	0.1				Ok	
3 0	009.7c4	15.67c0 to 0009.7c45.67ef	1.6				Ok	
4 0	009.7c4	15.4a80 to 0009.7c45.4aaf	1.6				Ok	

次に、設定を確認する例を示します。

Switch# **show lacp sys-id** 23456,0050.3e8d.6400 Switch#

最初にシステム プライオリティが表示され、次にスイッチの MAC アドレスが表示されます。

EtherChannel ロード バランシングの設定



(注)

ロード バランシングは、グローバルにのみ設定可能です。したがって、すべてのチャネル(手動設定、PAgP、またはLACP)は同じロード バランシング方式を使用します。

EtherChannel ロードバランシングを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# [no] port-channel load-balance {src-mac dst-mac src-dst-mac	EtherChannel ロード バランシングを設定します。
	src-ip dst-ip src-dst-ip src-port dst-port src-dst-port}	EtherChannel ロード バランシングをデフォルト設定に戻すには、no キーワードを使用します。
ステップ 2	Switch(config)# end	コンフィギュレーション モードを終了します。
ステップ 3	Switch# show etherchannel load-balance	設定を確認します。

ロード バランシングのキーワードは次のとおりです。

- src-mac 送信元 MAC アドレス
- dst-mac 宛先 MAC アドレス
- src-dst-mac 送信元および宛先 MAC アドレス
- src-ip 送信元 IP アドレス
- dst-ip 宛先 IP アドレス
- src-dst-ip 送信元および宛先 IP アドレス (デフォルト)
- src-port 送信元レイヤ 4 ポート
- dst-port 宛先レイヤ 4 ポート
- src-dst-port 送信元および宛先レイヤ 4 ポート

次に、送信元および宛先 IP アドレスを使用するように EtherChannel を設定する例を示します。

```
Switch# configure terminal
Switch(config)# port-channel load-balance src-dst-ip
Switch(config)# end
Switch#
```

次に、設定を確認する例を示します。

```
Switch# show etherchannel load-balance
EtherChannel Load-Balancing Configuration:
    src-dst-ip
```

EtherChannel Load-Balancing Addresses Used Per-Protocol:
Non-IP: Source XOR Destination MAC address
IPv4: Source XOR Destination IP address
IPv6: Source XOR Destination IP address
Switch#

EtherChannel からのインターフェイスの削除

EtherChannel からイーサネット インターフェイスを削除するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# interface {fastethernet gigabitethernet tengigabitethernet} slot/port	設定する物理インターフェイスを選択します。
ステップ 2	Switch(config-if)# no channel-group	ポートチャネル インターフェイスからインター フェイスを削除します。
ステップ 3	Switch(config-if)# end	コンフィギュレーション モードを終了します。
ステップ 4	Switch# show running-config interface {fastethernet gigabitethernet tengigabitethernet} slot/port Switch# show interface {fastethernet gigabitethernet tengigabitethernet} slot/port etherchannel	設定を確認します。

次に、インターフェイス FastEthernet 5/4 および 5/5 を、port-channel 1 から削除する例を示します。

Switch# configure terminal
Switch(config)# interface range fastethernet 5/4 - 5 (Note: Space is mandatory.)
Switch(config-if)# no channel-group 1
Switch(config-if)# end

EtherChannel の削除

EtherChannel を削除すると、メンバ ポートがシャットダウンされ、チャネル グループから削除されます。



EtherChannel をレイヤ2からレイヤ3に、またはレイヤ3からレイヤ2に変更する場合、EtherChannel を削除し、適切な設定で再び作成する必要があります。

EtherChannel を削除するには、次の作業を行います。

	コマンド	目的
ステップ 1	<pre>Switch(config)# no interface port-channel port_channel_number</pre>	ポートチャネル インターフェイスを削除します。
ステップ 2	Switch(config)# end	コンフィギュレーション モードを終了します。
ステップ 3	Switch# show etherchannel summary	設定を確認します。

次に、port-channel 1 を削除する例を示します。

Switch# configure terminal
Switch(config)# no interface port-channel 1
Switch(config)# end

EtherChannel の設定



CHAPTER

21

IGMP スヌーピングとフィルタリング の設定

この章では、Catalyst 4500 シリーズ スイッチ上で Internet Group Management Protocol (IGMP; インターネット グループ管理プロトコル)スヌーピングを設定する方法について説明します。設定上の注意事項、設定手順、および設定例も示します。

この章の主な内容は、次のとおりです。

- IGMP スヌーピングの概要 (p.21-2)
- IGMP スヌーピングの設定 (p.21-5)
- IGMP スヌーピング情報の表示 (p.21-15)
- IGMP フィルタリングの設定 (p.21-20)
- IGMP フィルタリングの設定の表示 (p.21-25)



(注)

Cisco Group Management Protocol (CGMP) クライアント デバイスをサポートするには、スイッチを CGMP サーバとして設定します。詳細については、次の URL の『Cisco IOS IP and IP Routing Configuration Guide』Cisco IOS Release 12.2 の「IP Multicast」および「Configuring IP Multicast Routing」の章を参照してください。

http://www.cisco.com/univered/cc/td/doc/product/software/ios123/123cgcr/ip_c/ipcprt3/1cdmulti.htm



(注)

この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univered/cc/td/doc/product/software/ios122sr/cr/index.htm

IGMP スヌーピングの概要

ここでは、次の内容について説明します。

- 即時脱退処理 (p.21-3)
- IGMP 設定可能な Leave タイマー (p.21-4)
- EHT (p.21-4)



QoS (Quality Of Service)は、IGMP パケットに適用しません。

IGMP スヌーピングにより、スイッチはホストとルータ間で送信される IGMP パケットの情報をスヌーピングまたはキャプチャします。この情報に基づいて、スイッチはアドレス テーブルに対してマルチキャスト アドレスの追加または削除を行い、マルチキャスト トラフィックの個々のホストポートへのフローをイネーブル (またはディセーブル)に設定します。IGMP スヌーピングは、IGMPv1、IGMPv2、および IGMPv3 のすべてのバージョンの IGMP をサポートします。

IGMPv1 および IGMPv2 とは対照的に、IGMPv3 スヌーピングはデフォルトで即時脱退処理を提供します。IGMPv3 スヌーピングは、Explicit Host Tracking (EHT)を提供し、ネットワーク管理者は実際に IGMPv3 をサポートするレイヤ 2 デバイス上に Source-Specific Multicast (SSM)機能を配置できます(「EHT」[p.21-4]を参照)。

IGMP が設定されているサブネットにおいて、IGMP スヌーピングはレイヤ 2 でマルチキャスト トラフィックを管理します。switchport キーワードを使用して、受信に関心のあるインターフェイスにのみマルチキャスト トラフィックを動的に転送するようにインターフェイスを設定できます。

IGMP スヌーピングは、MAC(メディア アクセス制御) マルチキャスト グループ $0010.5e00.0001 \sim 01-00-5e$ -ff-ff のトラフィックを制限します。 IGMP スヌーピングは、ルーティング プロトコルによって生成されたレイヤ 2 マルチキャスト パケットを制限しません。



IP マルチキャストおよび IGMP の詳細については、RFC 1112、RFC 2236、RFC 3376 (IGMPv3)を参照してください。

(ルータ上で設定された)IGMP は定期的に IGMP 一般クエリーを送信します。ホストは、関心のあるグループの IGMP メンバシップ レポートでこれらのクエリーに応答します。IGMP スヌーピングがイネーブルの場合、スイッチは IGMP Join 要求を受信する各レイヤ 2 マルチキャスト グループに、VLAN(仮想 LAN)ごとに 1 つのエントリを作成します。このマルチキャスト トラフィックに関心を示しているすべてのホストは IGMP メンバシップ レポートを送信し、転送テーブル エントリに追加されます。

レイヤ 2 マルチキャスト グループは IGMP スヌーピングを通じて動的に学習されます。ただし、ip igmp snooping static コマンドを使用して、レイヤ 2 マルチキャスト グループを静的に設定することもできます。静的にグループ メンバシップを指定する場合、その設定は IGMP スヌーピングによる自動的な処理より優先されます。マルチキャスト グループ メンバシップのリストは、ユーザが定義した設定値と、IGMP スヌーピング設定値の両方で構成できます。

 $0100.5E00.0001 \sim 0100.5E00.00FF$ 範囲のマルチキャスト MAC アドレスにマッピングする 224.0.0.0 $\sim 224.0.0.255$ の範囲の IP アドレスを持つグループは、ルーティング コントロール パケット専用です。これらのグループは、IGMPv3 メンバシップ レポートに使用される 224.0.0.22 を除いて、VLAN のすべての転送ポートにフラッディングされます。



VLAN でスパニングツリー トポロジが変更された場合、PortFast がイネーブルになっていないすべての VLAN ポート、および Topology Change Notification (TCN; トポロジ変更通知) クエリー カウント期間に no igmp snooping tcn flood コマンドが設定されたポートに、IP マルチキャスト トラフィックがフラッディングします。

レイヤ 2 IGMPv2 ホスト インターフェイスは IP マルチキャスト グループに加入するため、IP マルチキャスト グループの IGMP メンバシップ レポートを送信します。ホストをマルチキャスト グループから脱退させるには、そのホストで定期的な IGMP 一般クエリーを無視するか、または IGMP Leave メッセージを送信します。スイッチはホストから IGMP Leave メッセージを受け取ると、IGMP グループ固有のクエリーを送信して、そのインターフェイスに接続されたデバイスが特定のマルチキャスト グループのトラフィックに関心を示しているかどうかを判別します。スイッチはそのレイヤ 2 マルチキャスト グループのテーブル エントリを更新して、グループのマルチキャスト トラフィックの受信に関心を示しているホストのみがリストされるようにします。

対照的に、IGMPv3 ホストは、特定のマルチキャスト グループに加入するために(allow グループレコード モードで)IGMPv3 メンバシップ レポートを送信します。IGMPv3 ホストが、以前の送信元リストにあるすべての送信元からのトラフィックを拒否するために(block グループ レコードで)メンバシップ レポートを送信する場合、EHT がイネーブルにされていると、ポートの最後のホストは即時脱退によって削除されます。

即時脱退処理

IGMP スヌーピングの即時脱退処理を使用すると、スイッチはインターフェイスに IGMP グループ 固有のクエリーを事前に送信せず、そのインターフェイスを転送テーブル エントリから削除します。VLAN インターフェイスは、オリジナルの IGMP Leave メッセージで指定されたマルチキャスト グループのマルチキャスト ツリーからプルーニングされます。複数のマルチキャスト グループ が同時に使用される場合でも、即時脱退処理により、スイッチド ネットワーク上のすべてのホスト に対して最適な帯域幅管理が可能になります。

IGMP スヌーピングをイネーブルにしたスイッチが IGMPv2 または IGMPv3 Leave メッセージを受け取ると、Leave メッセージを受け取ったインターフェイスから IGMP グループ固有のクエリーを送信し、MAC マルチキャスト グループへの加入に関心を示した他のホストがそのインターフェイスに接続するタイミングを判断します。スイッチがクエリー応答間隔で IGMP Join メッセージを受信しない場合、レイヤ 2 転送テーブルのポート リスト (MAC-group、VLAN) エントリからインターフェイスが削除されます。



(注) デフォルトでは、すべての IGMP Join はすべてのマルチキャスト ルータ ポートに転送されます。

VLAN 上で即時脱退処理をイネーブルに設定すると、マルチキャスト ルータがポート上で学習されている場合を除き、IGMP Leave メッセージを受信した時点で、レイヤ 2 エントリのポート リストからインターフェイスをただちに削除できます。



(注)

IGMPv2 スヌーピングを使用する場合、即時脱退処理は各インターフェイスに 1 つのホストしか接続されていない VLAN でのみ使用してください。インターフェイスに複数のホストが接続されている VLAN 上で即時脱退処理をイネーブルにすると、一部のホストが偶発的にドロップされる可能性があります。IGMPv3 を使用する場合、即時脱退処理がデフォルトでイネーブルにされており、

EHT(下記参照)により、スイッチはポートに IGMPv3 ホストのスイッチによって維持されるホストが単一または複数であるときを検出できます。その結果、スイッチは特定のポートの背後で単一のホストを検出すると即時脱退処理を実行できます。



IGMPv3 は、古いバージョンの IGMP との相互運用が可能です。

特定の VLAN の IGMP バージョンを表示するには、show ip igmp snooping querier vlan コマンドを使用します。

スイッチが IGMPv3 スヌーピングをサポートするかどうかを表示するには、show ip igmp snooping vlan コマンドを使用します。

IGMPv2 の即時脱退をイネーブルにするには、ip igmp snooping immediate-leave コマンドを使用します。



(注)

IGMPv3 では、デフォルトで即時脱退処理がイネーブルに設定されています。

IGMP 設定可能な Leave タイマー

複数のホストが単一インターフェイスに接続されている VLAN では、即時脱退処理は使用できません。このような状況での脱退の遅れを減少させるため、IGMPv3 では設定可能な Leave タイマーを提供します。

Cisco IOS Release 12.2(25)SG 以前のリリースでは、IGMP スヌーピング脱退時間はクエリーの応答時間に基づいていました。クエリーのクエリー応答時間が満了する前にスイッチがメンバシップ レポートを受信しなかった場合、ポートはマルチキャスト グループ メンバシップから削除されました。

Cisco IOS Release 12.2(31)SG 以降のリリースでは、ホストの特定マルチキャスト グループへの関心が続いているかどうかを判断するために、グループ固有のクエリーを送信したあとにスイッチが待機する時間を設定できます。IGMP 脱退応答時間は、 $100\sim5000$ ミリ秒で設定できます。このタイマーは、グローバルでも、VLAN 単位でも設定できます。脱退時間の VLAN 設定は、グローバル設定を上書きします。

詳しい設定手順については、「IGMP Leave タイマーの設定」(p.21-9)を参照してください。

EHT

EHT は、IGMPv3 メンバシップ レポートを送信するホストを追跡することによって、グループ メンバシップを監視します。この追跡によって、スイッチは各ポートのグループに対応付けられたホスト情報を検出できます。さらに、ユーザは EHT によってメンバシップおよび各種の統計情報を追跡できます。

EHT では、スイッチはポート単位でメンバシップを追跡できます。そのため、スイッチは各ポートに存在するホストを認識し、ポートの背後にホストが1つだけ存在する場合に即時脱退処理を実行できます。

EHT が VLAN 上でイネーブルにされているかどうかを判別するには、show ip igmp snoop vlan コマンドを使用します。

IGMP スヌーピングの設定



IGMP を設定する場合は、VLAN データベース モードで VLAN を設定してください (第 13 章「VLAN、VTP、および VMPS の設定」を参照)。

IGMP スヌーピングにより、スイッチで IGMP パケットを調べ、パケットの内容に基づいて転送先を決定できます。

ここでは、IGMP スヌーピングを設定する手順について説明します。

- IGMP スヌーピングのデフォルト設定 (p.21-5)
- IGMP スヌーピングのグローバルなイネーブル化 (p.21-5)
- VLAN 上での IGMP スヌーピングのイネーブル化 (p.21-6)
- 学習方式の設定 (p.21-7)
- マルチキャスト ルータへの静的な接続の設定 (p.21-8)
- IGMP 即時脱退処理のイネーブル化 (p.21-8)
- IGMP Leave タイマーの設定 (p.21-9)
- EHT の設定 (p.21-10)
- ホストの静的な設定 (p.21-11)
- マルチキャスト フラッディングの抑制 (p.21-11)

IGMP スヌーピングのデフォルト設定

表 21-1 に、IGMP スヌーピングのデフォルト設定値を示します。

表 21-1 IGMP スヌーピングのデフォルト設定値

機能	デフォルト値
IGMP スヌーピング	イネーブル
マルチキャスト ルータ	設定なし
ЕНТ	IGMPv3 ではイネーブル。IGMPv2 では使用不可
即時脱退処理	IGMPv3 ではイネーブル。IGMPv2 ではディセーブル
レポート抑制	イネーブル
IGMP スヌーピングの学習方式	PIM/DVMRP ¹

^{1.} PIM/DVMRP = Protocol Independent Multicast/Distance Vector Multicast Routing Protocol

IGMP スヌーピングのグローバルなイネーブル化

IGMP スヌーピングをグローバルにイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# [no] ip igmp snooping	IGMP スヌーピングをイネーブルにします。
		IGMP スヌーピングをディセーブルにするには、 no キーワードを使用します。

	コマンド	目的
ステップ 3	Switch(config)# end	コンフィギュレーション モードを終了します。
ステップ 4	Switch# show ip igmp snooping include	設定を確認します。

次に、IGMP スヌーピングをグローバルにイネーブルにし、設定を確認する例を示します。

Switch# configure terminal Switch(config)# ip igmp snooping Switch(config)# end Switch# show ip igmp snooping Global IGMP Snooping configuration: _____ IGMP snooping : Enabled IGMPv3 snooping : Enabled Report suppression : Disabled TCN solicit query TCN flood query count : 2 Vlan 1: IGMP snooping : Enabled IGMPv2 immediate leave : Disabled : Enabled Explicit host tracking Multicast router learning mode : pim-dvmrp CGMP interoperability mode : IGMP_ONLY Vlan 2: IGMP snooping : Enabled : Disabled : Enabled IGMPv2 immediate leave Explicit host tracking Multicast router learning mode : pim-dvmrp CGMP interoperability mode : IGMP_ONLY

VLAN 上での IGMP スヌーピングのイネーブル化

VLAN 上で IGMP スヌーピングをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# [no] ip igmp snooping vlan vlan_ID	IGMP スヌーピングをイネーブルにします。
		IGMP スヌーピングをディセーブルにするには、 no キーワードを使用します。
ステップ 2	Switch(config)# end	コンフィギュレーション モードを終了します。
ステップ 3	Switch# show ip igmp snooping vlan vlan_ID	設定を確認します。

次に、VLAN 2 上で IGMP スヌーピングをイネーブルにし、設定を確認する例を示します。

```
Switch# configure terminal
Switch(config) # ip igmp snooping vlan 2
Switch(config)# end
Switch# show ip igmp snooping vlan 2
Global IGMP Snooping configuration:
IGMP snooping
IGMPv3 snooping
                        : Enabled
                        : Enabled
Report suppression
TCN solicit query
                        : Disabled
TCN flood query count
Vlan 2:
IGMP snooping
                              : Enabled
                        : Disabled
: Enabled
IGMPv2 immediate leave
Explicit host tracking
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode : IGMP_ONLY
```

学習方式の設定

ここでは IGMP スヌーピングの学習方式について説明します。

- PIM/DVMRP 学習方式の設定 (p.21-7)
- CGMP 学習方式の設定 (p.21-7)

PIM/DVMRP 学習方式の設定

IGMP スヌーピングを PIM/DVMRP パケットから学習するように設定するには、次の作業を行います。

コマンド	目的
Switch(config)# ip igmp snooping vlan vlan_ID mrouter learn [cgmp pim-dvmrp]	VLAN の学習方式を指定します。

次に、IP IGMP スヌーピングが PIM/DVMRP パケットから学習するように設定する例を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 1 mrouter learn pim-dvmrp
Switch(config)# end
Switch#
```

CGMP 学習方式の設定

IGMP スヌーピングを CGMP self-join パケットから学習するように設定するには、次の作業を行います。

コマンド	目的
Switch(config)# ip igmp snooping vlan vlan_ID mrouter learn [cgmp pim-dvmrp]	VLAN の学習方式を指定します。

次に、IP IGMP スヌーピングが CGMP self-join パケットから学習するように設定する例を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 1 mrouter learn cgmp
Switch(config)# end
Switch#
```

マルチキャスト ルータへの静的な接続の設定

マルチキャスト ルータに静的な接続を設定するには、スイッチに ip igmp snooping vlan mrouter interface コマンドを入力します。

マルチキャストルータへの静的な接続を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	<pre>witch(config) # ip igmp snooping vlan vlan_ID mrouter interface interface_num</pre>	VLAN のマルチキャスト ルータとの静的な接続を 指定します。
		(注) ルータとのインターフェイスは、コマンドを 入力する VLAN 内になければなりません。 ルータとライン プロトコルはアップ状態で ある必要があります。
ステップ 3	Switch(config)# end	コンフィギュレーション モードを終了します。
ステップ 4	Switch# show ip igmp snooping mrouter vlan vlan_ID	設定を確認します。

次に、マルチキャストルータへの静的な接続を設定する例を示します。

Switch# configure terminal
Switch(config)# ip igmp snooping vlan 200 mrouter interface fastethernet 2/10
Switch# show ip igmp snooping mrouter vlan 200
vlan ports
----+
200 Fa2/10
Switch#

IGMP 即時脱退処理のイネーブル化

VLAN 上で IGMP 即時脱退処理をイネーブルにした場合、インターフェイス上で IGMPv2 Leave メッセージを検出すると、スイッチはマルチキャスト グループからインターフェイスを削除します。



IGMPv3 では、EHT とのデフォルトで即時脱退処理がイネーブルに設定されています。

IGMPv2 インターフェイスで即時脱退処理をイネーブルにするには、次の作業を行います。

コマンド	目的
Switch(config)# ip igmp snooping vlan vlan_ID immediate-leave	VLAN で即時脱退処理をイネーブルにします。
	(注) このコマンドは、IGMPv2 ホストだけに 適用します。

次に、VLAN 200 インターフェイス上で IGMP 即時脱退処理をイネーブルにし、設定を確認する例を示します。

Switch# configure terminal

 ${\tt Switch(config)\,\#\,\,ip\,\,\,igmp\,\,\,snooping\,\,vlan\,\,200\,\,\,immediate-leave}$

Configuring immediate leave on vlan 200

Switch(config)# end

 ${\tt Switch\#\ show\ ip\ igmp\ interface\ vlan\ 200\ |\ include\ immediate\ leave}$

Immediate leave : Disabled

Switch(config)#

IGMP Leave タイマーの設定

IGMP Leave タイマーを設定する場合、次の注意事項に従ってください。

- 脱退時間は、グローバルでも、VLAN単位でも設定できます。
- VLAN で脱退時間を設定すると、グローバル設定は上書きされます。
- デフォルトの脱退時間は、1000 ミリ秒です。
- IGMP の設定可能な脱退時間は、IGMP バージョン 2 を稼働するホストでのみサポートされます。
- ネットワークの実際の脱退の遅れは通常、設定した脱退時間になります。ただし、リアルタイムの CPU 負荷条件、ネットワーク遅延、インターフェイスによって送信されたトラフィック量により、脱退時間は設定した時間付近でばらつくことがあります。

IGMP の設定可能な Leave タイマーをイネーブルにするには、次の手順を実行します。

	コマンド	目的	
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。	
ステップ 2	Switch(config)# ip igmp snooping last-member-query-interval time	IGMP Leave タイマーをグローバルに設定します。指定できる範囲は 100 ~ 5000 ミリ秒です。デフォルトは 1000 秒です。	
		IGMP Leave タイマーをグローバルにリセットして デフォルト設定に戻すには、no ip igmp snooping last-member-query-interval グローバル コンフィ ギュレーション コマンドを使用します。	
ステップ 3	Switch(config)# ip igmp snooping vlan vlan_ID last-member-query-interval time	(任意)IGMP 脱退時間を VLAN インターフェイス」 で設定します。 指定できる範囲は 100 ~ 5000 ミリ利 です。	
		特定の VLAN から設定した IGMP 脱退時間設定を削除するには、 no ip igmp snooping vlan <i>vlan-id</i> last-member-query-interval グローバル コンフィギュレーション コマンドを使用します。	
		(注) VLAN で脱退時間を設定すると、グローバル に設定したタイマーは上書きされます。	
ステップ 4	Switch(config)# end	特権 EXEC モードに戻ります。	
ステップ 5	Switch# show ip igmp snooping	(任意)設定した IGMP 脱退時間を表示します。	
ステップ 6	Switch# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を 保存します。	

次に、IGMP 設定可能な Leave タイマーをイネーブルにし、設定を確認する例を示します。

```
Switch# configure terminal
Switch(config) # ip igmp snooping last-member-query-interval 200
Switch(config)# ip igmp snooping vlan 10 last-member-query-interval 500
Switch(config)# end
Switch# show ip igmp snooping show ip igmp snooping
Global IGMP Snooping configuration:
-----
IGMP snooping
IGMPv3 snooping
                        : Enabled
Report suppression
                        : Enabled
TCN solicit query
                         : Disabled
TCN flood query count
Last Member Query Interval: 200
Vlan 1:
IGMP snooping
                                 : Enabled
IGMPv2 immediate leave
                                 : Disabled
Explicit host tracking
                                 : Enabled
                                 : pim-dvmrp
Multicast router learning mode
                                 : 200
Last Member Query Interval
CGMP interoperability mode
                                 : IGMP ONLY
Vlan 10:
IGMP snooping
                                 : Enabled
IGMPv2 immediate leave
                                 : Disabled
Explicit host tracking
                                 : Enabled
                                 : pim-dvmrp
Multicast router learning mode
Last Member Query Interval
                                  : 500
CGMP interoperability mode

    TGMP ONLY

Switch#
```

EHT の設定

IGMPv3 では、EHT はデフォルトでイネーブルに設定されており、VLAN 単位でディセーブルにできます。

VLAN 上で EHT 処理をディセーブルにするには、次の作業を行います。

コマンド	目的	
Switch(config)#[no] ip igmp snooping vlan vlan_ID explicit-tracking	VLAN 上で EHT をイネーブルにします。	
	EHT をディセーブルにするには、no キーワード	
	を使用します。	

次に、VLAN 200 上で IGMP EHT をディセーブルにし、設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# no ip igmp snooping vlan 200 explicit-tracking
Switch(config)# end
Switch# show ip igmp snooping vlan 200 | include Explicit host tracking
Explicit host tracking : Disabled
```

ホストの静的な設定

ホストは通常、マルチキャスト グループに動的に加入しますが、インターフェイス上でホストを静的に設定することもできます。

インターフェイス上でホストを静的に設定するには、次の作業を行います。

コマンド	目的
Switch(config-if)# ip igmp snooping vlan vlan_ID static mac_address interface interface_num	VLAN でホストを静的に設定します。 (注) このコマンドは、特定の送信元 IP アドレスのトラフィックを受信するようには設定できません。

次に、VLAN 200 でインターフェイス FastEthernet 2/11 にホストを静的に設定する例を示します。

Switch# configure terminal

Switch(config) # ip igmp snooping vlan 200 static 0100.5e02.0203 interface fastethernet 2/11

Configuring port FastEthernet2/11 on group 0100.5e02.0203 vlan 200 Switch(config)# **end**

マルチキャスト フラッディングの抑制

IGMP スヌーピングがイネーブルに設定されたスイッチは、スパニングツリー TCN を受信すると、VLAN のすべてのポートにマルチキャスト トラフィックをフラッディングします。マルチキャストフラッディングの抑制により、スイッチはこのようなトラフィックの送信を停止します。フラッディングの抑制をサポートするため、Cisco IOS Release 12.1(11b)EW では次のインターフェイスコマンドおよびグローバルコマンドが導入されました。

インターフェイス コマンドは次のとおりです。

[no | default] ip igmp snooping ten flood

グローバル コマンドは次のとおりです。

[no | default] ip igmp snooping tcn flood query count [1 - 10]

[no | default] ip igmp snooping ten query solicit

Cisco IOS Release 12.1(11b)EW より前のリリースでは、スイッチがスパニングツリー TCN を受信すると、3回の IGMP クエリー インターバルの間、VLAN のすべてのポートにマルチキャスト トラフィックがフラッディングされていました。これは冗長構成に必要でしたが、Cisco IOS Release 12.1(11b)EW では、スイッチがマルチキャスト フラッディングを停止するまでのデフォルト時間は、2回の IGMP クエリー インターバルに変更されました。

このフラッディング動作は、フラッディングを行うスイッチが別のグループに属する多くのポートを保有している場合には望ましくありません。トラフィックがスイッチとエンド ホスト間でリンク容量を超え、パケットが失われることもあります。

no ip igmp snooping tcn flood コマンドを使用すると、トポロジ変更後にスイッチ インターフェイス 上のマルチキャスト フラッディングをディセーブルにできます。トポロジが変更されている間で も、ポートが加入しているマルチキャスト グループのみがそのポートに送信されます。

IGMP クエリーしきい値を設定して、トポロジ変更後すぐにスイッチ インターフェイス上のマルチ キャスト フラッディングをイネーブルにするには、 ip igmp snooping ten flood query count コマンドを使用します。

トポロジが変更された場合、通常スパニングツリー ルート スイッチはグループ マルチキャスト アドレス 0.0.0.0 を使用してグローバル IGMP Leave メッセージ (「クエリー要求」と呼ばれる)を発行します。スイッチはこの要求を受け取ると、スパニングツリーが変更された VLAN のすべてのポートで要求をフラッディングします。アップストリーム ルータがこの要求を受け取ると、ただちに IGMP 一般クエリーを発行します。

ip igmp snooping ten query solicit コマンドを使用すると、スパニングツリー以外のルート スイッチに同じクエリー要求を発行するように指示できます。

次のセクションで新しいコマンドの詳細と、その使用方法について説明します。

IGMP スヌーピング インターフェイスの設定

VLAN でトポロジが変更されると、それまでに学習された IGMP スヌーピング情報が無効になる場合があります。トポロジ変更前に 1 つのポートに存在していたホストは、トポロジ変更後に別のポートに移動することがあります。トポロジが変更される場合、Catalyst 4500 シリーズ スイッチは、マルチキャスト トラフィックが VLAN 内のすべてのマルチキャスト レシーバーに送信されるように特別なアクションを実行します。

Spanning-Tree Protocol(STP; スパニングツリー プロトコル)が VLAN で実行されている場合、VLAN のルート スイッチによってスパニングツリー TCN が発行されます。Catalyst 4500 シリーズ スイッチは、IGMP スヌーピングがイネーブルに設定されている VLAN で TCN を受信すると、ただちに「マルチキャスト フラッディング モード」を開始します。トポロジが再度安定し、すべてのマルチキャスト レシーバーの新しい位置が学習されるまでの間、このモードが継続されます。

「マルチキャスト フラッディング モード」の IP マルチキャスト トラフィックは、マルチキャスト グループ メンバが検出されたポートだけでなく、VLAN のすべてのポートに送られます。

Cisco IOS Release 12.1(11b)EW 以降、スイッチポート上で **no ip igmp snooping tcn flood** コマンドを 使用すると、IP マルチキャスト トラフィックがそのポートにフラッディングされるのを手動で防 ぐことができます。

トランク ポートの場合、この設定はすべての VLAN に適用されます。

デフォルトでは、マルチキャスト フラッディングはイネーブルです。フラッディングをディセーブルにするには no キーワードを、デフォルトの動作(フラッディングがイネーブル)に戻すには default を使用します。

インターフェイス上のマルチキャスト フラッディングをイネーブルにするには、次の作業を行います。

コマンド	目的
Switch(config)# interface {fastethernet gigabitethernet tengigabitethernet} slot/port	設定するインターフェイスを選択します。
Switch(config-if)# no ip igmp snooping tcn flood	スイッチが TCN を受信した場合、インターフェイス上のマルチキャスト フラッディングをディセーブルにします。
	インターフェイス上のマルチキャスト フラッディングをイネーブルにするには、次のコマンドを入力します。 default ip igmp snooping tcn flood
Switch(config)# end	コンフィギュレーション モードを終了します。
Switch# show running interface {fastethernet gigabitethernet tengigabitethernet} slot/port	設定を確認します。

次に、インターフェイス FastEthernet 2/11 上でマルチキャスト フラッディングをディセーブルにする例を示します。

Switch(config)# interface fastethernet 2/11
Switch(config-if)# no ip igmp snooping tcn flood
Switch(config-if)# end
Switch#

IGMP スヌーピング スイッチの設定

デフォルトでは、スイッチが 2 つの IGMP 一般クエリーを受信するまで「フラッディング モード」が継続されます。この期間を変更するには、**ip igmp snooping tcn flood query count** n コマンドを使用します。n は $1 \sim 10$ の数値です。

このコマンドはグローバル コンフィギュレーション レベルで作用します。

クエリーのデフォルトは2です。no および default キーワードでデフォルトに戻ります。

IGMP クエリーのしきい値を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	<pre>Switch(config)# ip igmp snooping tcn flood query count <n></n></pre>	スイッチがマルチキャスト トラフィックのフラッ ディングを停止するまでの、IGMP クエリーの数を 変更します。
		スイッチを IGMP クエリーのデフォルトの数に戻す には、次のコマンドを入力します。 default ip igmp snooping tcn flood query count
ステップ 2	Switch(config)# end	コンフィギュレーション モードを終了します。

次に、4回のクエリー実行後にマルチキャスト トラフィックのフラッディングを停止するように、 スイッチを修正する例を示します。

Switch(config)# ip igmp snooping tcn flood query count 4
Switch(config)# end
Switch#

IGMP スヌーピングがイネーブルの VLAN でのトポロジ変更をスパニングツリー ルート スイッチが確認すると、IOS ルータが 1 つまたは複数の一般クエリーを送信するというクエリー要求をスイッチが発行します。この新しいコマンド ip igmp snooping tcn query solicit によって、スイッチはスパニングツリー ルートでない場合も、トポロジ変更を確認すると、常にクエリー要求を送信します。

このコマンドはグローバル コンフィギュレーション レベルで作用します。

デフォルトでは、スイッチがスパニングツリー ルートの場合を除き、クエリー要求はディセーブルに設定されています。default キーワードでデフォルトの動作に戻ります。

スイッチにクエリー要求を送信するように指示するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# ip igmp snooping tcn query solicit	TCN が検出された場合に、クエリー要求を送信するように スイッチを設定します。
		スイッチによるクエリー要求の送信を停止するには(スイッチがスパニングツリー ルート スイッチでない場合)、次のコマンドを入力します。 no ip igmp snooping tcn query solicit
ステップ 2	Switch(config)# end	コンフィギュレーション モードを終了します。

次に、TCN を検出したあと、クエリー要求を送信するようにスイッチを設定する例を示します。

Switch(config)# ip igmp snooping tcn query solicit
Switch(config)# end
Switch#

IGMP スヌーピング情報の表示

ここでは IGMP スヌーピング情報を表示する方法について説明します。

- クエリア情報の表示 (p.21-15)
- IGMP ホスト メンバシップ情報の表示 (p.21-15)
- グループ情報の表示(p.21-16)
- マルチキャスト ルータ インターフェイスの表示 (p.21-18)
- MAC アドレス マルチキャスト エントリの表示 (p.21-18)
- VLAN インターフェイス上の IGMP スヌーピング情報の表示 (p.21-19)

クエリア情報の表示

クエリア情報を表示するには、次の作業を行います。

コマンド	目的
Switch# show ip igmp snooping querier [vlan vlan_ID]	マルチキャスト ルータ インターフェイスを表示します。

次に、スイッチ上のすべての VLAN の IGMP スヌーピング クエリア情報を表示する例を示します。

SW1tcn#	snow ip igmp	snooping querier	
Vlan	IP Address	IGMP Version	Port
2	10.10.10.1	v2	Router
3	172.20.50.2	22 v3	Fa3/15

次に、VLAN3のIGMPスヌーピングクエリア情報を表示する例を示します。

Switch#	show	ip igmp	snooping	querier	vlan 3		
Vlan	IP	Address	IGMP	Version		Port	
3	172	2.20.50.2	22 v3			Fa3/15	5

IGMP ホスト メンバシップ情報の表示



デフォルトでは、EHT は EHT データベースに最大 1000 エントリを維持します。上限に達すると、 エントリはそれ以上作成されません。さらにエントリを作成するには、clear ip igmp snooping membership vlan コマンドを使用してデータベースをクリアします。

ホストメンバシップ情報を表示するには、次の作業を行います。

コマンド	目的
Switch# show ip igmp snooping membership [interface interface_num] [vlan vlan_ID] [reporter a.b.c.d] [source a.b.c.d group a.b.c.d]	EHT 情報を表示します。 (注) このコマンドは、スイッチ上で EHT が イネーブルにされている場合にのみ有 効です。

次に、VLAN 20 のホスト メンバシップ情報を表示し、EHT データベースを削除する例を示します。

Switch# show ip igmp snooping membership vlan 20

#channels: 5 #hosts: 1 Source/Group Interface Uptime Last-Join Reporter Last-Leave Gi4/1 .20 00:23: 37 00:06: 5 20 00:23: 37 00:06:5 0 .20 00:39: 42 00:09:17 -40.40.40.2/224.10.10.10 20.20.20 50 00.22 0 00:20:30 50 00:20:30 40.40.40.3/224.10.10.10 Gi4/2 20.20.20 Gi4/1 40.40.40.4/224.10.10.10 20.20.20 Fa2/1 20.20.20. 20 00:39: 42 00:09:17 20.20.20 .20 00:09: 47 00:09:17 40.40.40.5/224.10.10.10 Fa2/1 40.40.40.6/224.10.10.10

Switch# clear ip igmp snooping membership vlan 20

次に、インターフェイス gi4/1 のホスト メンバシップを表示する例を示します。

Switch# show ip igmp snooping membership interface gi4/1

#channels: 5 #hosts : 1

Source/Group Interface Reporter Uptime Last-Join Last-Leave .20 00:23: 37 00:06: 40.40.40.2/224.10.10.10 Gi 4/1 20.20.20 50 00:20:30 .20 00:39: 42 00:09:17 40.40.40.4/224.10.10.10 Gi4/1 20.20.20

次に、VLAN 20 およびグループ 224.10.10.10 のホスト メンバシップを表示する例を示します。

Switch# show ip igmp snooping membership vlan 20 source 40.40.40.2 group 224.10.10.10

#channels: 5

#hosts : 1

Source/Group Interface Reporter Uptime Last-Join Last-Leave Gi4/1 40.40.40.2/224.10.10.10 20.20.20 .20 00:23: 37 00:06: 50 00:20:30

グループ情報の表示

グループに対応付けられた詳細な IGMPv3 情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
Switch# show ip igmp snooping groups [vlan vlan_ID]	グループ、グループ (ホスト タイプ) に対して受信 されたレポート タイプ、およびレポートが受信され たポートのリストを表示します。
	レポート リストには、マルチキャスト ルータ ポートまたはグループの詳細な転送ポート設定は含まれません。その代わりに、レポートが受信されたポートのリストを表示します。
	グループの詳細な転送ポート設定を表示するには、 show mac-address-table multicast コマンドを使用し て、このグループに対応する MAC アドレスの CLI (コマンドライン インターフェイス) 出力を表示し ます。

コマンド	目的	
Switch# show ip igmp snooping groups [vlan vlan_ID a.b.c.d] [summary sources hosts]	グループ アドレス固有の情報を表示します。送信元 およびホストに対してグループの現在のステートの 詳細を提供します。	
	(注) このコマンドは、完全な IGMPv3 スヌーピング サポートにのみ適用され、IGMPv1、IGMPv2、または IGMPv3 グループに使用できます。	
Switch# show ip igmp snooping groups [vlan vlan_ID] [count]	グローバルまたは VLAN 単位でシステムによって 学習されたグループ アドレスの総数を表示します。	

次に、VLAN 1 のホスト タイプおよびグループのポートを表示する例を示します。

Switch# show ip igmp snooping groups vlan 10 226.6.6.7

Vlan	Group	Version	Ports
10	226.6.6.7	v3	Fa7/13, Fa7/14
Switch>			

次に、送信元 IP アドレスに対する現在のグループのステートを表示する例を示します。

Switch# show ip igmp snooping groups vlan 10 226.6.6.7 sources

Source information for group 226.6.6.7:

Timers: Expired sources are deleted on next IGMP General Query

SourceIP	Expires	Uptime	Inc Hosts	Exc Hosts
2.0.0.1	00:03:04	00:03:48	2	0
2.0.0.2	00:03:04	00:02:07	2	0
Switch>				

次に、ホスト MAC アドレスに対する現在のグループのステートを表示する例を示します。

Switch# show ip igmp snooping groups vlan 10 226.6.6.7 hosts

IGMPv3 host information for group 226.6.6.7

Timers: Expired hosts are deleted on next IGMP General Query

Host	(MAC/IP)	Filter mode	Expires	Uptime	# Sources
175.1	.0.29	INCLUDE	stopped	00:00:51	2
175.2	.0.30	INCLUDE	stopped	00:04:14	2

次に、IGMPv3 グループのサマリー情報を表示する例を示します。

Switch# show ip igmp snooping groups vlan 10 226.6.6.7 summary

Group Address (Vlan 10) : 226.6.6.7 Host type : v3

Member Ports : Fa7/13, Fa7/14 Filter mode : INCLUDE

Expires : stopped Sources : 2 Reporters (Include/Exclude) : 2/0

次に、システムによってグローバルに学習されたグループ アドレスの総数を表示する例を示します。

Switch# show ip igmp snooping groups count

Total number of groups: 54

次に、VLAN 5 で学習されたグループ アドレスの総数を表示する例を示します。

Switch# show ip igmp snooping groups vlan 5 count Total number of groups: 30

マルチキャスト ルータ インターフェイスの表示

IGMP スヌーピングをイネーブルにすると、スイッチはマルチキャスト ルータの接続先インターフェイスを自動的に学習します。

マルチキャストルータインターフェイスを表示するには、次の作業を行います。

コマンド	目的
Switch# show ip igmp snooping mrouter vlan vlan_ID	マルチキャスト ルータ インターフェイスを表示します。

次に、VLAN 1 のマルチキャスト ルータ インターフェイスを表示する例を示します。

Switch#	show	ip	igmp	snooping	mrouter	vlan	1
vlan			ports	5			
+							
1		Gi:	L/1,G	i2/1,Fa3/	48,Route	ŗ	
Switch#							

MAC アドレス マルチキャスト エントリの表示

Switch#

VLAN の MAC アドレス マルチキャスト エントリを表示するには、次の作業を行います。

コマンド	目的
lon rilan ID [gount]	VLAN の MAC アドレス マルチキャスト エント リを表示します。

次に、VLAN 1 の MAC アドレス マルチキャスト エントリを表示する例を示します。

Switch# show mac-address-table multicast vlan 1

Multicast Entries vlan mac address type ports igmp Switch, Gi6/1 0100.5e01.0101 1 1 0100.5e01.0102 igmp Switch, Gi6/1 igmp Switch, Gi6/1 0100.5e01.0103 1 0100.5e01.0104 igmp Switch, Gi6/1 0100.5e01.0105 1 igmp Switch, Gi6/1 0100.5e01.0106 igmp Switch, Gi6/1

次に、VLAN 1 の MAC アドレス エントリの総数を表示する例を示します。

Switch# show mac-address-table multicast vlan 1 count Multicast MAC Entries for vlan 1: 4
Switch#

VLAN インターフェイス上の IGMP スヌーピング情報の表示

特定の VLAN 上の IGMP スヌーピング情報を表示するには、次の作業を行います。

コマンド	目的
	特定の VLAN インターフェイス上の IGMP ス ヌーピング情報を表示します。

次に、VLAN 5上の IGMP スヌーピング情報を表示する例を示します。

Switch# show ip igmp snooping vlan 5
Global IGMP Snooping configuration:

IGMP snooping :Enabled
IGMPv3 snooping support :Full
Report suppression :Enabled
TCN solicit query :Disabled
TCN flood query count :2

Vlan 5:

IGMP snooping :Enabled
Immediate leave :Disabled
Explicit Host Tracking :Disabled
Multicast router learning mode :pim-dvmrp
CGMP interoperability mode :IGMP_ONLY

IGMP フィルタリングの設定

ここでは、次の内容について説明します。

- IGMP フィルタリングのデフォルト設定 (p.21-20)
- IGMP プロファイルの設定 (p.21-20)
- IGMP プロファイルの適用 (p.21-22)
- IGMP グループの最大数の設定 (p.21-23)



(注)

IGMP フィルタリング機能は、IGMPv1 および IGMPv2 だけで動作します。

メトロポリタンまたは Multiple-Dwelling Unit (MDU) インストールなど一部の環境では、管理者はスイッチ ポート上のユーザが所属するマルチキャスト グループを制御できます。管理者は加入計画またはサービス計画の種類に基づいて、IP/TV などのマルチキャスト サービスの配布を制御できます。

管理者はこのような制御を実行する場合に、IGMP フィルタリング機能を使用します。この機能を使用すると、IP マルチキャスト プロファイルを設定して、これらを個々のスイッチ ポートに関連付けることで、ポート単位でマルチキャスト加入をフィルタリングできます。IGMP プロファイルには I つまたは複数のマルチキャスト グループを収めることができ、グループへのアクセス許可または拒否はこのプロファイルで指定されます。マルチキャスト グループへのアクセスを拒否する IGMP プロファイルがスイッチ ポートに適用された場合、IP マルチキャスト トラフィックのストリームを要求する IGMP 加入レポートがドロップされ、ポートはそのグループから IP マルチキャスト トラフィックを受信できなくなります。フィルタリング アクションがマルチキャスト グループへのアクセスを許可する場合、ポートからの IGMP レポートが通常の処理として転送されます。

IGMP フィルタリングは、IGMP メンバシップの Join 要求のみを制御し、IP マルチキャスト トラフィックの転送指示機能には関与しません。

ip igmp max-groups < n > コマンドを使用すると、レイヤ 2 インターフェイスが加入できる IGMP グループの最大数も設定できます。

IGMP フィルタリングのデフォルト設定

表 21-2 に、IGMP フィルタリングのデフォルト設定を示します。

表 21-2 IGMP フィルタリングのデフォルト設定

機能	デフォルト設定
IGMP フィルタリング	フィルタリングなし
IGMP グループの IGMP 最大数	制限なし
IGMP プロファイル	定義なし

IGMP プロファイルの設定

IGMP プロファイルを設定し、IGMP プロファイル コンフィギュレーション モードを開始するには、 ip igmp profile グローバル コンフィギュレーション コマンドを使用します。IGMP プロファイル コ ンフィギュレーション モードで、ポートからの IGMP Join 要求のフィルタリングに使用される IGMP プロファイルのパラメータを指定できます。IGMP プロファイル コンフィギュレーション モードでは、次のコマンドを使用してプロファイルを作成できます。

- deny: 一致するアドレスが拒否されるように指定します。これはデフォルト状態です。
- exit: IGMP プロファイル コンフィギュレーション モードを終了します。
- no:コマンドが破棄されるか、デフォルトが設定されます。
- permit: 一致するアドレスを許可するように指定します。
- range: プロファイルの一連の IP アドレスを指定します。単一の IP アドレスまたは開始アドレスと終了アドレスを指定した IP アドレス範囲を入力します。

デフォルトでは、IGMP プロファイルは設定されていません。permit または deny キーワード以外 でプロファイルが設定されている場合、デフォルトは IP アドレス範囲へのアクセス拒否になります。

ポートの IGMP プロファイルを作成するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	Switch(config)# ip igmp profile profile number	IGMP プロファイル コンフィギュレーション モードを開始し、設定するプロファイルに数値を割り当てます。1 ~ 4、294、967、295 の数値を指定できます。
ステップ 3	Switch(config-igmp-profile)# permit deny	(任意) IP マルチキャスト アドレスへのアクセスを 許可または拒否するアクションを設定します。アク ションを設定しない場合、プロファイルのデフォル トはアクセスの拒否になります。
ステップ 4	Switch(config-igmp-profile)# range ip multicast address	アクセスを制御する IP マルチキャスト アドレスまたは IP マルチキャスト アドレスの範囲を入力します。範囲を入力する場合、小さい方の IP マルチキャスト アドレスを入力してからスペースを入れ、大きい方の IP マルチキャスト アドレスを入力します。 複数のアドレスまたはアドレス範囲を入力する場合は、range コマンドを繰り返します。
ステップ 5	Switch(config-igmp-profile)# end	特権 EXEC モードに戻ります。
ステップ 6	Switch# show ip igmp profile profile number	プロファイルの設定を確認します。
ステップ 7	Switch# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を 保存します。

プロファイルを削除するには、**no ip igmp profile** *profile number* グローバル コンフィギュレーションコマンドを使用します。

IP マルチキャスト アドレスまたは IP マルチキャスト アドレス範囲を削除するには、**no range** ip multicast address IGMP プロファイル コンフィギュレーション コマンドを使用します。

次に、IGMP プロファイル 4 を作成し(単一の IP マルチキャスト アドレスへのアクセスを許可)、設定を確認する例を示します。アクションが拒否(デフォルト)であれば、show ip igmp profile コマンド出力には表示されません。

Switch# configure terminal
Switch(config)# ip igmp profile 4
Switch(config-igmp-profile)# permit
Switch(config-igmp-profile)# range 229.9.9.0
Switch(config-igmp-profile)# end
Switch# show ip igmp profile 4
IGMP Profile 4
 permit
 range 229.9.9.0 229.9.9.0

IGMP プロファイルの適用

IGMP プロファイルで定義されたアクセスを制御するには、ip igmp filter インターフェイス コンフィギュレーション コマンドを使用して、適切なインターフェイスにプロファイルを適用します。1つのプロファイルを複数のインターフェイスに適用できますが、各インターフェイスに適用できるプロファイルは1つだけです。



IGMP プロファイルはレイヤ 2 ポートにのみ適用できます。ルーテッド ポート (または Switch Virtual Interface [SVI; スイッチ仮想インターフェイス])あるいは EtherChannel ポート グループに属するポートに IGMP プロファイルは適用できません。

スイッチ ポートに IGMP プロファイルを適用するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開 始します。
ステップ 2	Switch(config)# interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定する物理インターフェイス (fastethernet2/3 など)を入力します。インターフェイスは、EtherChannel ポート グループに属さないレイヤ 2 ポートでなければなりません。
ステップ 3	Switch(config-if)# ip igmp filter profile number	インターフェイスに指定された IGMP プロファイルを適用します。プロファイル番号には、1 ~4,294,967,295 を指定できます。
ステップ 4	Switch(config-if)# end	特権 EXEC モードに戻ります。
ステップ 5	Switch# show running configuration interface interface-id	設定を確認します。
ステップ 6	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定 を保存します。

インターフェイスからプロファイルを削除するには、no ip igmp filter コマンドを使用します。

次に、IGMP プロファイル 4 をインターフェイスに適用し、設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# interface fastethernet2/12
Switch(config-if)# ip igmp filter 4
Switch(config-if)# end
Switch# show running-config interface fastethernet2/12
Building configuration...

Current configuration : 123 bytes
!
interface FastEthernet2/12
no ip address
shutdown
snmp trap link-status
ip igmp max-groups 25
ip igmp filter 4
end
```

IGMP グループの最大数の設定

ip igmp max-groups インターフェイス コンフィギュレーション コマンドを使用すると、レイヤ 2 インターフェイスが加入できる IGMP グループの最大数を設定できます。制限のないデフォルトに最大数を戻す場合は、no 形式を使用します。



この制限はレイヤ 2 ポートにのみ適用できます。ルーテッド ポート (または SVI) あるいは EtherChannel ポート グループに属するポートには、IGMP グループの最大数を設定できません。

スイッチ ポートに IGMP プロファイルを適用するには、次の作業を行います。

コマンド	目的
Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
Switch(config)# interface interface-id	インターフェイス コンフィギュレーション モードを 開始 し、設定する物理インターフェイス (gigabitethernet1/1 など)を入力します。インターフェイスは、EtherChannel グループに属さないレイヤ 2 ポートでなければなりません。
Switch(config-if)# ip igmp max-groups number	インターフェイスが加入できる IGMP グループの最大数を設定します。0 ~ 4,294,967,294 の数値を指定できます。デフォルトでは最大数が設定されていません。
	最大グループ制限を削除し、最大数なしのデフォルトに戻すには、no ip igmp max-groups コマンドを使用します。
Switch(config-if)# end	特権 EXEC モードに戻ります。
Switch# show running-configuration interface interface-id	設定を確認します。
Switch# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を 保存します。

次に、インターフェイスが加入できる IGMP グループの数を 25 に制限する例を示します。

```
Switch# configure terminal
Switch(config)# interface fastethernet2/12
Switch(config-if)# ip igmp max-groups 25
Switch(config-if)# end
Switch# show running-config interface fastethernet2/12
Building configuration...

Current configuration : 123 bytes
!
interface FastEthernet2/12
no ip address
shutdown
snmp trap link-status
ip igmp max-groups 25
ip igmp filter 4
end
```

IGMP フィルタリングの設定の表示

スイッチ上のすべてのインターフェイス、または指定されたインターフェイスの IGMP プロファイルと最大グループ設定を表示できます。

IGMP プロファイルを表示するには、次の作業を行います。

コマンド	目的
Switch# show ip igmp profile [profile number]	指定された IGMP プロファイル、またはスイッチ上で定義された
	すべての IGMP プロファイルを表示します。

インターフェイス コンフィギュレーションを表示するには、次の作業を行います。

コマンド	目的
interface idl	指定されたインターフェイスまたはスイッチ上のすべてのインターフェイスに関する、(設定されている場合は)インターフェイスが所属できる IGMP グループの最大数と、インターフェイスに適用された IGMP プロファイルを含む設定を表示します。

次に、プロファイル番号が入力されていない場合の show ip igmp profile 特権 EXEC コマンドの例を示します。スイッチ上で定義されたすべてのプロファイルが表示されます。

```
Switch# show ip igmp profile
IGMP Profile 3
   range 230.9.9.0 230.9.9.0
IGMP Profile 4
   permit
   range 229.9.9.0 229.255.255.255
```

次に、インターフェイスに IGMP の最大設定グループ数が指定され、IGMP プロファイル 4 がインターフェイスに適用されている場合の show running-config 特権 EXEC コマンドの例を示します。

```
Switch# show running-config interface fastethernet2/12
```

```
Building configuration...

Current configuration : 123 bytes !

interface FastEthernet2/12

no ip address

shutdown

snmp trap link-status

ip igmp max-groups 25

ip igmp filter 4

end
```

■ IGMP フィルタリングの設定の表示



CHAPTER

22

IPv6 MLD スヌーピングの設定



(注)

IPv6 MLD スヌーピングは、Supervisor Engine 6-E でのみサポートされます。

Catalyst 4500 シリーズ スイッチ上で、Multicast Listener Discovery (MLD)スヌーピングを使用して、スイッチド ネットワーク内のクライアントおよびルータへの IP Version 6 (IPv6) マルチキャストデータをクライアントに効率的に配信できます。



(井)

この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/cr/index.htm

この章の内容は、次のとおりです。

- 「MLD スヌーピングの概要」(p.22-2)
- 「IPv6 MLD スヌーピングの設定」(p.22-6)
- 「MLD スヌーピング情報の表示」(p.22-13)

MLD スヌーピングの概要

IP Version 4 (IPv4) では、レイヤ 2 スイッチは Internet Group Management Protocol (IGMP; インターネットグループ管理プロトコル) スヌーピングを使用して、動的にレイヤ 2 インターフェイスを設定することにより、マルチキャスト トラフィックのフラッディングを抑制します。そのため、マルチキャスト トラフィックは IP マルチキャスト デバイスに対応付けられたインターフェイスにだけ転送されます。 IPv6 では、MLD スヌーピングが同様の機能を実行します。 MLD スヌーピングを使用すると、IPv6 マルチキャスト データは VLAN のすべてのポートにフラッディングすることなく、データを受信するポートのリストに対して選択的に転送されます。このリストは、IPv6 マルチキャスト制御パケットをスヌーピングすることにより構築されます。

MLD は IPv6 マルチキャスト ルータで使用されるプロトコルで、ルータに直接接続されたリンク上のマルチキャスト リスナー (IPv6 マルチキャスト パケットを受信するノード)の存在、および隣接ノードを対象とするマルチキャスト パケットを検出します。MLD は IGMP から派生しています。つまり、MLD バージョン 1 (MLDv1)は IGMPv2 と、MLD バージョン 2 (MLDv2)は IGMPv3 とそれぞれ同等です。MLD は Internet Control Message Protocol バージョン 6 (ICMPv6)のサブプロトコルです。MLD メッセージは ICMPv6 メッセージのサブセットで、IPv6 パケット内で先頭の Next Header 値 58 により識別されます。

スイッチは、次の2つのバージョンの MLD スヌーピングをサポートします。

- MLDv1 スヌーピングは MLDv1 制御パケットを検出し、IPv6 宛先マルチキャスト アドレスに基づいてトラフィックのブリッジングを設定します。
- MLDv2 Basic Snooping (MBSS) は MLDv2 制御パケットを使用して、IPv6 宛先マルチキャストアドレスに基づいてトラフィックの転送を設定します。

スイッチは MLDv1 プロトコル パケットと MLDv2 プロトコル パケットの両方でスヌーピングでき、IPv6 宛先マルチキャスト アドレスに基づいて IPv6 マルチキャスト データをブリッジングします。



スイッチは、IPv6 送信元および宛先マルチキャスト アドレスベースの転送を設定する MLDv2 Enhanced Snooping (MESS) をサポートしません。

MLD スヌーピングは、グローバルまたは VLAN 単位でイネーブルまたはディセーブルに設定できます。MLD スヌーピングがイネーブルの場合、VLAN 単位の IPv6 マルチキャスト MAC アドレステーブルはソフトウェアで構築され、VLAN 単位の IPv6 マルチキャスト アドレス テーブルはソフトウェアで構築されます。そのあと、スイッチはハードウェアで IPv6 マルチキャスト アドレスに基づくブリッジングを実行します。

次に、IPv6 MLD スヌーピングの一部のパラメータについて説明します。

- MLD メッセージ (p.22-3)
- MLD **/DU** (p.22-3)
- マルチキャスト クライアント エージングの堅牢性 (p.22-3)
- マルチキャスト ルータ検出 (p.22-4)
- MLD レポート (p.22-4)
- MLD Done メッセージおよび即時脱退 (p.22-4)
- TCN 処理 (p.22-5)

MLD メッセージ

MLDv1 は、次の3種類のメッセージをサポートします。

- Listener Query は、IGMPv2 クエリーと同等で、General Query または Mulicast-Address-Specific Query (MASQ) のいずれかになります。
- Multicast Listener Report は、IGMPv2 レポートと同等です。
- Multicast Listener Done メッセージは、IGMPv2 Leave メッセージと同等です。

MLDv2 では、MLDv1 レポートおよび Done メッセージに加えて、MLDv2 クエリーおよび MLDv2 レポートもサポートします。

メッセージの送受信の結果生じるメッセージ タイマーおよびステート移行は、IGMPv2 メッセージ の場合と同じです。IPv6 の有効な link-local 送信元アドレスを持たない MLD メッセージは、MLD ルータおよび MLD スイッチで無視されます。

MLD クエリー

スイッチは MLD クエリーを送信し、IPv6 マルチキャスト アドレス データベースを構築し、MLD Group Specific (GS; グループ固有) クエリー、MLD Group-and-Source-Specific (GSS; グループおよび送信元固有) クエリーを生成して、MLD Done メッセージに応答します。また、スイッチはレポート抑制、レポート プロキシング、即時脱退機能、およびスタティックな IPv6 マルチキャスト MAC アドレス設定もサポートします。

MLD スヌーピングがディセーブルの場合、すべての MLD クエリーが入力 VLAN でフラッディングされます。

MLD スヌーピングがイネーブルの場合、受信された MLD クエリーが入力 VLAN でフラッディングされ、クエリーのコピーは CPU に送信され、処理されます。MLD スヌーピングでは、受信されたクエリーから IPv6 マルチキャスト アドレス データベースを構築します。MLD スヌーピングは、マルチキャスト ルータ ポートを検出して、タイマーを維持し、レポート応答時間を設定します。また、VLAN のクエリア IP 送信元アドレス、VLAN 内のクエリア ポートを学習して、マルチキャストアドレスエージングを維持します。

グループが MLD スヌーピング データベースに存在する場合、スイッチは MLDv1 レポートを送信して、GS クエリーに応答します。このグループが不明の場合、GS クエリーは入力 VLAN にフラッディングされます。

ホストがマルチキャスト グループから脱退する場合、MLD Done メッセージ(IGMP Leave メッセージと同等)を送信できます。スイッチが MLDv1 Done メッセージを受信した際に、即時脱退がイネーブルでなければ、スイッチはメッセージを受信したポートに MASQ を送信して、ポートに接続する他のデバイスがマルチキャスト グループに残る必要があるかどうか判別します。

マルチキャスト クライアント エージングの堅牢性

クエリー数に基づいて、アドレスからのポート メンバシップの削除を設定できます。1 つのアドレスへのメンバシップからポートが削除されるのは、設定された数のクエリーに関してポート上のアドレスへのレポートがない場合のみです。デフォルト値は2です。

マルチキャスト ルータ検出

IGMP スヌーピングと同様に、MLD スヌーピングでは次の特性を持つマルチキャスト ルータ検出を行います。

- ユーザにより設定されたポートは、エージングアウトしません。
- 動的なポート学習は、MLDv1 スヌーピング クエリーおよび IPv6 PIMv2 パケットにより行われます。
- 複数のルータが同じレイヤ 2 インターフェイス上にある場合、MLD スヌーピングではポート 上の単一のマルチキャスト ルータ (直前にルータ制御パケットを送信したルータ)を追跡しま す。
- マルチキャスト ルータ ポートの動的なエージングは、5 分間のデフォルトタイマーに基づきます。ポート上で制御パケットが5 分間受信されない場合、マルチキャスト ルータはルータのポート リストから削除されます。
- IPv6 マルチキャスト ルータ検出が実行されるのは、MLD スヌーピングがスイッチでイネーブルの場合のみです。
- 受信された IPv6 マルチキャスト ルータ制御パケットは、スイッチで MLD スヌーピングがイネーブルかどうかにかかわらず、常に入力 VLAN にフラッディングされます。
- 最初の IPv6 マルチキャスト ルータ ポートが検出されたあとは、不明の IPv6 マルチキャスト データは、検出されたルータ ポートに対してのみ転送されます (それまでは、すべての IPv6 マルチキャスト データは入力 VLAN にフラッディングされます)。

MLD レポート

MLDv1 join メッセージは、本質的には IGMPv2 と同じように処理されます。IPv6 マルチキャストルータが VLAN で検出されない場合は、レポートが処理されないか、またはスイッチから転送されません。IPv6 マルチキャスト ルータが検出され、MLDv1 レポートが受信されると、IPv6 マルチキャスト グループ アドレスおよび IPv6 マルチキャスト MAC アドレスが VLAN の MLD データベースに入力されます。そのあと、VLAN 内のグループに対するすべての IPv6 マルチキャスト トラフィックが、このアドレスを使用して転送されます。MLD スヌーピングがディセーブルの場合、レポートは入力 VLAN でフラッディングされます。

MLD スヌーピングがイネーブルの場合は、MLD レポート抑制(リスナーメッセージ抑制)は自動的にイネーブルになります。レポート抑制により、スイッチはグループで受信した最初の MLDv1 レポートを IPv6 マルチキャスト ルータに転送します。グループのそれ以降のレポートはルータに送信されません。MLD スヌーピングがディセーブルの場合は、レポート抑制がディセーブルになり、すべての MLDv1 レポートは入力 VLAN にフラッディングされます。

スイッチは、MLDv1 プロキシ レポーティングもサポートします。MLDv1 MASQ が受信されると、スイッチに他のポートのグループが存在する場合、およびクエリーを受信したポートとアドレスの最後のメンバー ポートが異なる場合は、スイッチはクエリーを受信したアドレスに関する MLDv1 レポートで応答します。

MLD Done メッセージおよび即時脱退

即時脱退機能がイネーブルの場合にホストが MLDv1 Done メッセージ (IGMP Leave メッセージと同等)を送信すると、Done メッセージを受信したポートはグループからただちに削除されます。 VLAN で即時脱退をイネーブルにする場合は (IGMP スヌーピングと同様に)、ポートに単一のホストが接続されている VLAN でのみこの機能を使用します。ポートがグループの最後のメンバーである場合、グループも削除され、検出された IPv6 マルチキャスト ルータに脱退情報が転送されます。

VLAN で即時脱退がイネーブルでない場合に(1 つのポート上にグループのクライアントが複数ある場合)、Done メッセージがポートで受信されると、このポートで MASQ が生成されます。ユーザは、既存アドレスのポート メンバシップが削除される時期を MASQ 数の観点から制御できます。1 つのアドレスへのメンバシップからポートが削除されるのは、設定された数のクエリーに関してポート上のアドレスへの MDLv1 レポートがない場合のみです。

生成される MASQ 数は、ipv6 mld snooping last-listener-query count グローバル コンフィギュレーション コマンドにより設定されます。デフォルト値は 2 です。

MASQ は、Done メッセージが送信された IPv6 マルチキャスト アドレスに送信されます。スイッチの最大応答時間内に MASQ で指定された IPv6 マルチキャスト アドレスにレポートが送信されなければ、MASQ が送信されたポートは IPv6 マルチキャスト アドレス データベースから削除されます。最大応答時間は、ipv6 mld snooping last-listener-query-interval グローバル コンフィギュレーションコマンドにより設定されます。削除されたポートがマルチキャスト アドレスの最後のメンバーである場合は、マルチキャスト アドレスも削除され、スイッチは検出されたマルチキャスト ルータすべてにアドレス脱退情報を送信します。

TCN 処理

ipv6 mld snooping tcn query solicit グローバル コンフィギュレーション コマンドを使用して、Topology Change Notification (TCN; トポロジ変更通知) 送信要求をイネーブルにすると、MLDv1 スヌーピングは、設定された数の MLDv1 クエリーによりすべての IPv6 マルチキャスト トラフィックをフラッディングするように VLAN に設定してから、選択されたポートにのみマルチキャストデータの送信を開始します。この値は、ipv6 mld snooping tcn flood query count グローバル コンフィギュレーション コマンドを使用して設定します。デフォルトでは、2 つのクエリーが送信されます。スイッチが VLAN 内の Spanning-Tree Protocol (STP; スパニング ツリー プロトコル) ルートになる場合、またはスイッチがユーザにより設定された場合は、IPv6 の有効な link-local 送信元アドレスを持つ MLDv1 グローバル Done メッセージも生成されます。これは IGMP スヌーピングの場合と同じです。

IPv6 MLD スヌーピングの設定

ここでは、IPv6 MLD スヌーピングを設定する手順について説明します。

- MLD スヌーピングのデフォルト設定 (p.22-6)
- MLD スヌーピング設定時の注意事項 (p.22-7)
- MLD スヌーピングのイネーブル化またはディセーブル化 (p.22-7)
- スタティックなマルチキャスト グループの設定 (p.22-8)
- マルチキャスト ルータ ポートの設定 (p.22-9)
- MLD 即時脱退のイネーブル化 (p.22-10)
- IGMP スヌーピング クエリーの設定 (p.22-10)
- MLD リスナー メッセージ抑制のディセーブル化 (p.22-12)

MLD スヌーピングのデフォルト設定

表 22-1 に、MLD スヌーピングのデフォルト設定を示します。

表 22-1 MLD スヌーピングのデフォルト設定

機能	デフォルト設定
MLD スヌーピング(グローバル)	ディセーブル。
MLD スヌーピング(VLAN 単位)	イネーブル VLAN MLD スヌーピングが実行されるためには、MLD スヌーピングがグローバルにイネーブルである必要があります。
IPv6 マルチキャスト アドレス	設定なし
IPv6 マルチキャスト ルータ ポート	設定なし
MLD スヌーピング即時脱退	ディセーブル。
MLD スヌーピングのロバストネス変数	グローバル: 2、VLAN 単位: 0
最後のリスナー クエリー カウント	 (注) VLAN 値はグローバル設定を上書きします。 VLAN 値が 0 の場合、VLAN はグローバル数 を使用します。 グローバル: 2、VLAN 単位: 0 (注) VLAN 値はグローバル設定を上書きします。 VLAN 値が 0 の場合、VLAN はグローバル数 を使用します。
最後のリスナー クエリー インターバル	グローバル:1000 (1秒)、VLAN:0 (注) VLAN 値はグローバル設定を上書きします。 VLAN 値が 0 の場合、VLAN はグローバル インターバルを使用します。
TCN クエリー送信要求	ディセーブル。
TCN クエリー カウント	2
MLD リスナー抑制	ディセーブル。

MLD スヌーピング設定時の注意事項

MLD スヌーピングの設定時は、次の注意事項に従ってください。

- MLD スヌーピングの特性はいつでも設定できますが、設定を有効にする場合は、ipv6 mld snooping グローバル コンフィギュレーション コマンドを使用して MLD スヌーピングをグローバルにイネーブルにする必要があります。
- MLD スヌーピングと IGMP スヌーピングは相互に独立して動作します。スイッチで両方の機能を同時にイネーブルにできます。Catalyst 4500 シリーズ スイッチで共存可能な IPv4 および IPv6 マルチキャスト グループの合計エントリ数は、16384 個に制限されています。
- 512 MB のメモリを持つ Supervisor Engine 6-E は、11000 個の MLD スヌーピング マルチキャスト グループをサポートしますが、1 GB のメモリを持つ Supervisor Engine 6-E は、16384 個の MLD スヌーピング マルチキャスト グループをサポートします。

MLD スヌーピングのイネーブル化またはディセーブル化

デフォルトでは、IPv6 MLD スヌーピングはスイッチではグローバルにディセーブルで、すべての VLAN ではイネーブルです。MLD スヌーピングがグローバルにディセーブルの場合は、すべての VLAN でもディセーブルです。MLD スヌーピングをグローバルにイネーブルにすると、VLAN 設定はグローバル設定を上書きします。つまり、MLD スヌーピングはデフォルト ステート (イネーブル)の VLAN インターフェイスでのみイネーブルになります。

VLAN 単位または VLAN 範囲で MLD スヌーピングをイネーブルおよびディセーブルにできますが、MLD スヌーピングをグローバルにディセーブルにした場合は、すべての VLAN でディセーブルになります。グローバル スヌーピングがイネーブルの場合、VLAN スヌーピングをイネーブルまたはディセーブルに設定できます。

スイッチで MLD スヌーピングをグローバルにイネーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# ipv6 mld snooping	スイッチで MLD スヌーピングをグローバルにイネーブル
		にします。
ステップ 3	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 4	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

スイッチで MLD スヌーピングをグローバルにディセーブルにするには、no ipv6 mld snooping グローバル コンフィギュレーション コマンドを使用します。

VLAN で MLD スヌーピングをイネーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# ipv6 mld snooping	スイッチで MLD スヌーピングをグローバルにイネーブル
		にします。

	コマンド	目的
ステップ 3	Switch(config)# ipv6 mld snooping vlan vlan-id	VLAN で MLD スヌーピングをイネーブルにします。VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。
		(注) VLAN スヌーピングをイネーブルにするには、 MLD スヌーピングがグローバルにイネーブルであ る必要があります。
ステップ 4	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 5	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

VLAN インターフェイスで MLD スヌーピングをディセーブルにするには、指定された VLAN 番号 に対して no ipv6 mld snooping vlan vlan-id グローバルコンフィギュレーション コマンドを使用します。

スタティックなマルチキャスト グループの設定

ホストまたはレイヤ 2 ポートは、通常マルチキャスト グループに動的に加入しますが、VLAN に IPv6 マルチキャスト アドレスおよびメンバー ポートを静的に設定することもできます。

マルチキャスト グループのメンバーとしてレイヤ 2 ポートを追加するには、次の手順を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開 始します。
ステップ 2	Switch(config)# ipv6 mld snooping vlan vlan-id static ipv6_multicast_address interface interface-id	マルチキャスト グループのメンバーとしてレイヤ 2 ポートにマルチキャスト グループを静的に設定します。
		 vlan-id は、マルチキャスト グループの VLAN ID です。VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。
		 ipv6_multicast_address は、128 ビットのグ ループ IPv6 アドレスです。このアドレスは RFC 2373 で指定された形式でなければなり ません。
		 interface-id はメンバー ポートです。物理インターフェイスまたはポート チャネル(1 ~64)に設定できます。
ステップ 3	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 4	Switch# show mac-address-table multicast mld-snooping	スタティックなメンバー ポートおよび IPv6 アドレスを確認します。
ステップ 5	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定 を保存します。

マルチキャスト グループからレイヤ 2 ポートを削除するには、no ipv6 mld snooping vlan vlan-id static mac-address interface interface-id グローバル コンフィギュレーション コマンドを使用します。 グループからすべてのメンバー ポートが削除された場合、このグループは削除されます。

次に、IPv6 マルチキャスト グループを静的に設定する例を示します。

Switch# configure terminal Switch(config)# ipv6 mld snooping vlan 2 static 3333.0000.0003 interface gigabitethernet1/1

Switch(config)# end

マルチキャスト ルータ ポートの設定

MLD スヌーピングは、MLD クエリーおよび PIMv6 クエリーを介してルータ ポートについて学習 しますが、CLI (コマンドライン インターフェイス) を使用しても VLAN にマルチキャスト ルータ ポートを追加できます。マルチキャスト ルータ ポートを追加する (マルチキャスト ルータにスタティック接続を追加する)には、スイッチで ipv6 mld snooping vlan mrouter グローバル コンフィギュレーション コマンドを使用します。



マルチキャスト ルータへのスタティック接続は、スイッチ ポートに限りサポートされます。

VLAN にマルチキャスト ルータ ポートを追加するには、次の手順を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	Switch(config)# ipv6 mld snooping vlan vlan-id mrouter interface interface-id	マルチキャスト ルータの VLAN ID を指定して、マルチキャスト ルータにインターフェイスを指定します。
		• VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。
		 インターフェイスは物理インターフェイスにすることもポート チャネルにすることもできます。指定できるポートチャネルの範囲は1~64です。
ステップ 3	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 4	Switch# show ipv6 mld snooping mrouter [vlan $vlan-id$]	VLAN インターフェイスで IPv6 MLD スヌーピング がイネーブルになっていることを確認します。
ステップ 5	Switch# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を 保存します。

VLAN からマルチキャスト ルータ ポートを削除するには、no ipv6 mld snooping vlan vlan-id mrouter interface interface-id グローバル コンフィギュレーション コマンドを使用します。

次に、VLAN 200 にマルチキャスト ルータ ポートを追加する例を示します。

Switch# configure terminal

 $\label{eq:config} \begin{tabular}{ll} Switch(config) \# ipv6 mld snooping vlan 200 mrouter interface gigabitethernet $\frac{1}{0}$/2 $Switch(config) \# exit $$ $$$

MLD 即時脱退のイネーブル化

MLDv1 即時脱退をイネーブルにした場合、スイッチはポートで MLD Done メッセージを検出するとただちに、マルチキャスト グループからポートを削除します。即時脱退機能を使用するのは、VLAN の各ポート上にレシーバーが 1 つだけ存在する場合に限定してください。同一ポートにマルチキャスト グループのクライアントが複数ある場合は、VLAN で即時脱退をイネーブルにしないでください。

MLDv1 即時脱退をイネーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	Switch(config)# ipv6 mld snooping vlan vlan-id immediate-leave	VLAN インターフェイスで MLD 即時脱退をイネーブルにします。
ステップ 3	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 4	Switch# show ipv6 mld snooping vlan vlan-id	VLAN インターフェイス上で即時脱退がイネーブル になっていることを確認します。
ステップ 5	Switch# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を 保存します。

VLAN で MLD 即時脱退をディセーブルにするには、**no ipv6 mld snooping vlan** *vlan-id* **immediate-leave** グローバル コンフィギュレーション コマンドを使用します。

次に、VLAN 130 で MLD 即時脱退をイネーブルにする例を示します。

Switch# configure terminal
Switch(config) # ipv6 mld snooping vlan 130 immediate-leave
Switch(config) # exit

IGMP スヌーピング クエリーの設定

即時脱退がイネーブルでない場合に、ポートが MLD Done メッセージを受信すると、スイッチはポートで MASQ を生成して、Done メッセージが送信された IPv6 マルチキャスト アドレスに送信します。ポートがマルチキャスト グループから削除される前に、送信される MASQ 数およびスイッチが応答を待機する時間を任意で設定できます。

スイッチまたは VLAN に MLD スヌーピング クエリーの特性を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始しま
		す。
ステップ 2	robustness-variable value	(任意)スイッチが一般クエリーに応答しないリスナー (ポート)を削除する前に、送信されるクエリー数を設 定します。指定できる範囲は1~3です。デフォルトは 2です。

	コマンド	目的
ステップ 3	Switch(config)# ipv6 mld snooping vlan vlan-id robustness-variable value	(任意) VLAN 単位でロバストネス変数を設定します。これにより、MLD レポート応答がない場合にマルチキャスト アドレスがエージング アウトされるまでに、MLD スヌーピングが送信する一般クエリー数が決定されます。指定できる範囲は1~3です。デフォルトは0です。0に設定すると、使用される数はグローバルなロバストネス変数の値になります。
ステップ 4	Switch(config)# ipv6 mld snooping last-listener-query-count count	(任意) MLD クライアントがエージング アウトされる 前にスイッチが送信する MASQ 数を設定します。指定 できる範囲は 1 ~ 7 で、デフォルト値は 2 です。クエ リーは 1 秒後に送信されます。
ステップ 5	Switch(config)# ipv6 mld snooping vlan vlan-id last-listener-query-count count	(任意)VLAN単位で last-listener クエリー カウントを設定します。この値はグローバルに設定された値を上書きします。指定できる範囲は1~7です。デフォルトは0です。0に設定すると、グローバルなカウント値が使用されます。クエリーは1秒後に送信されます。
ステップ 6	Switch(config)# ipv6 mld snooping last-listener-query-interval interval	(任意)スイッチが MASQ を送信したあと、マルチキャスト グループからポートを削除するまで待機する最大応答時間を設定します。指定できる範囲は、100~32,768ミリ秒です。デフォルト値は1000(1秒)です。
ステップ 7	Switch(config)# ipv6 mld snooping vlan vlan-id last-listener-query-interval interval	(任意)VLAN単位で last-listener クエリー インターバルを設定します。この値はグローバルに設定された値を上書きします。指定できる範囲は、0 ~ 32,768 ミリ秒です。デフォルト値は0です。0に設定すると、グローバルな last-listener クエリー インターバルが使用されます。
ステップ 8	Switch(config)# ipv6 mld snooping tcn query solicit	(任意) TCN 送信要求をイネーブルにします。これにより、VLAN は設定された数のクエリーに関する IPv6 マルチキャスト トラフィックすべてをフラッディングしてから、マルチキャスト データの受信を要求するポートに対してのみ送信します。デフォルトでは、TCN はディセーブルに設定されています。
ステップ 9	Switch(config)# ipv6 mld snooping tcn flood query count count	(任意) TCN がイネーブルの場合、送信される TCN クエリー数を指定します。指定できる範囲は 1 ~ 10 で、デフォルトは 2 です。
ステップ 10	Switch(config)# end	特権 EXEC モードに戻ります。
	Switch# show ipv6 mld snooping querier [vlan $vlan-id$]	(任意)スイッチまたは VLAN の MLD スヌーピング クエリア情報を確認します。
ステップ 12	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

次に、MLD スヌーピングのグローバルなロバストネス変数を3に設定する例を示します。

Switch# configure terminal
Switch(config)# ipv6 mld snooping robustness-variable 3
Switch(config)# exit

次に、VLAN の MLD スヌーピングの last-listener クエリー カウントを 3 に設定する例を示します。

Switch# configure terminal

Switch(config)# ipv6 mld snooping vlan 200 last-listener-query-count 3
Switch(config)# exit

次に、MLD スヌーピングの last-listener クエリー インターバル (最大応答時間)を 2000 (2 秒)に 設定する例を示します。

Switch# configure terminal
Switch(config)# ipv6 mld snooping last-listener-query-interval 2000
Switch(config)# exit

MLD リスナー メッセージ抑制のディセーブル化

デフォルトでは、MLD スヌーピング リスナー メッセージ抑制はイネーブルに設定されています。この機能がイネーブルの場合、スイッチはマルチキャスト ルータ クエリーごとに 1 つの MLD レポートのみを転送します。メッセージ抑制がディセーブルの場合は、複数のマルチキャスト ルータに MLD レポートが転送されます。

MLD リスナー メッセージ抑制をディセーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	Switch(config) # no ipv6 mld snooping listener-message-suppression	MLD メッセージ抑制をディセーブルにします。
ステップ 3	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 4	Switch# show ipv6 mld snooping	IPv6 MLD スヌーピング レポート抑制がディセーブ ルであることを確認します。
ステップ 5	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を 保存します。

MLD メッセージ抑制を再びイネーブルにするには、ipv6 mld snooping listener-message-suppression グローバル コンフィギュレーション コマンドを使用します。

MLD スヌーピング情報の表示

動的に学習された、あるいは静的に設定されたルータ ポートおよび VLAN インターフェイスの MLD スヌーピング情報を表示できます。MLD スヌーピング用に設定した VLAN の MAC アドレス マルチキャスト エントリも表示できます。

MLD スヌーピング情報を表示するには、表 22-2 に示す 1 つまたは複数の特権 EXEC コマンドを使用します。

表 22-2 MLD スヌーピング情報を表示するためのコマンド

コマンド	目的
show ipv6 mld snooping [vlan vlan-id]	スイッチのすべての VLAN または指定された VLAN の MLD スヌーピング設定情報を表示します。
	(任意)個々の VLAN に関する情報を表示するには、 vlan <i>vlan-id</i> を入力します。VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。
show ipv6 mld snooping mrouter [vlan $vlan ext{-}id$]	動的に学習された、あるいは手動で設定されたマルチキャストルータ インターフェイスの情報を表示します。MLD スヌーピングをイネーブルにすると、スイッチはマルチキャストルータの接続先であるインターフェイスを自動的に学習します。これらのインターフェイスは動的に学習されます。
	(任意)個々の VLAN に関する情報を表示するには、 vlan <i>vlan-id</i> を入力します。VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。
show ipv6 mld snooping querier [vlan vlan-id]	VLAN 内で直前に受信した MLD クエリー メッセージの IPv6 アドレスおよび着信ポートに関する情報を表示します。
	(任意) vlan vlan-id を入力して、単一の VLAN 情報を表示します。 VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。

■ MLD スヌーピング情報の表示



CHAPTER

23

802.1Q およびレイヤ 2 プロトコル トンネリングの設定

Virtual Private Network (VPN: バーチャル プライベート ネットワーク) は、共有インフラストラク チャ(通常はイーサネットベース)上で、私設網と同じセキュリティ、プライオリティ、信頼性、 および管理性を持つ企業規模の接続を提供します。トンネリングは、ネットワークで複数のカスタ マーのトラフィックを伝送するサービス プロバイダーを対象に設計された機能です。このような サービス プロバイダーは、各カスタマーの VLAN (仮想 LAN) およびレイヤ 2 プロトコル設定を 他のカスタマーのトラフィックに影響を与えずに維持する必要があります。Catalyst 4500 シリーズ スイッチは、IEEE 802.10 トンネリングおよびレイヤ 2 プロトコル トンネリングをサポートしてい ます。



Supervisor Engine 6-E は、レイヤ 2 プロトコル トンネリングをサポートしていません。



802.10 には Cisco Catalyst 4948、Cisco Catalyst 4948-10GE、または Catalyst 4500 シリーズ スイッチ スーパーバイザ エンジン II-Plus-10GE V または V-10GE が必要であることに注意してください。 レ イヤ2プロトコルトンネリングは、すべてのスーパーバイザエンジン上でサポートされます。

この章の内容は、次のとおりです。

- 802.1Q トンネリングの概要 (p.23-2)
- 802.1Q トンネリングの設定 (p.23-4)
- レイヤ 2 プロトコル トンネリングの概要 (p.23-8)
- レイヤ 2 プロトコル トンネリングの設定 (p.23-10)
- トンネリング ステータスのモニタリングおよびメンテナンス (p.23-14)



この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univered/cc/td/doc/product/software/ios122sr/cr/index.htm

802.1Q トンネリングの概要

同じサービス プロバイダー ネットワーク内の各カスタマーが要求する VLAN 範囲は重複する場合があり、インフラストラクチャを経由するカスタマー トラフィックが混合する場合もあります。カスタマーごとに一意の VLAN ID 範囲を割り当てると、カスタマーの設定が制限され、802.1Q 仕様の VLAN に関する上限 (4096 個)を容易に超えてしまいます。

802.1Q トンネリングを使用すると、サービス プロバイダーは単一の VLAN を使用して、複数の VLAN を持つカスタマーをサポートできます。このときに、カスタマーの VLAN ID は保護され、各 カスタマー VLAN のトラフィックは分離されます。

802.1Q トンネリングをサポートするように設定されたポートを、トンネル ポートといいます。トンネリングを設定する場合は、トンネリング専用の VLAN ID にトンネル ポートを割り当てます。カスタマーごとに個別のサービス プロバイダー VLAN ID が必要ですが、その VLAN ID はすべてのカスタマーの VLAN をサポートします。

対応する VLAN ID を使用して通常の方法でタグ付けされたカスタマーのトラフィックは、カスタマー デバイスの 802.1Q トランク ポートから送信されて、サービス プロバイダー エッジ スイッチのトンネル ポートに着信します。カスタマー デバイスとエッジ スイッチ間のリンクは、非対称リンクです。これは、リンクの一端が 802.1Q トランク ポートとして設定されているのに対し、もう一端はトンネル ポートとして設定されているためです。トンネル ポート インターフェイスに、カスタマーごとに一意のアクセス VLAN ID を割り当てます。図 23-1 を参照してください。

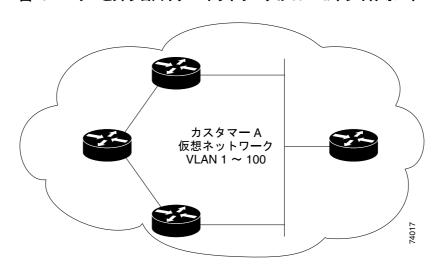
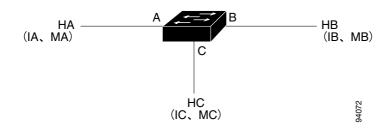


図 23-1 サービス プロバイダー ネットワークの 802.1Q トンネル ポート

カスタマー トランク ポートからサービス プロバイダー エッジ スイッチのトンネル ポートに着信するパケットは、該当する VLAN ID を使用して通常の方法で 802.1Q がタグ付けされます。トランク ポートからサービス プロバイダー ネットワークに送信されたタグ付きパケットは、カスタマーごとに一意の VLAND ID を含む別のレイヤの 802.1Q タグ (メトロ タグ) でカプセル化されています。元のカスタマー 802.1Q タグは、カプセル化されたパケット内に保存されます。したがって、サービス プロバイダー ネットワークに入るパケットは二重にタグ付けされます。メトロ タグにはカスタマーのアクセス VLAN ID が格納され、内側のタグには着信トラフィックの VLAN となる VLAN ID が格納されます。

二重タグ付きパケットがサービス プロバイダー コア スイッチの別のトランク ポートに着信する と、スイッチがパケットを処理するときに、メトロ タグが除去されます。同じコア スイッチ上の 別のトランク ポートからパケットが送信されるときに、パケットには同じメトロ タグが再び追加されます。図 23-2 に、元の(通常の)フレームで開始するイーサネットパケットタグ構造を示します。

図 23-2 元の (通常の) 802.1Q、および二重タグ付きイーサネット パケット形式



パケットがサービス プロバイダー出力スイッチのトランク ポートに着信すると、スイッチがパケットを処理するときに、メトロ タグが再び除去されます。ただし、パケットがエッジ スイッチのトンネル ポートから送信されて、カスタマーのネットワークに入るときは、メトロ タグが追加されません。パケットは通常の 802.1Q タグ付きフレームとして送信され、カスタマーのネットワーク内にある元の VLAN 番号は保存されます。

エッジ スイッチのトンネル ポートを通じてサービス プロバイダー ネットワークに入るパケットは、タグなしの場合も、802.1Q ヘッダーがタグ付けされている場合も、すべてタグなしパケットとして取り扱われます。これらのパケットは、802.1Q トランク ポートのサービス プロバイダー ネットワークを通じて送信されるときに、メトロ タグ VLAN ID (トンネル ポートのアクセス VLAN に設定) でカプセル化されます。メトロ タグのプライオリティ フィールドは、トンネル ポートのインターフェイス Class of Service (CoS; サービス クラス) プライオリティに設定されています (未設定の場合のデフォルトは 0 です)。

図 23-1 では、カスタマー A には VLAN 30 が、カスタマー B には VLAN 40 が割り当てられています。サービス プロバイダー ネットワークに入って、エッジ スイッチのトンネル ポートに着信する 802.1Q タグ付きパケットは、二重タグ付きになります。この場合、メトロ タグには VLAN ID 30 または 40 が格納され、内側のタグには元のカスタマー VLAN 番号(VLAN 100 など)が格納されています。カスタマー A とカスタマー B の両方にネットワーク内で VLAN 100 が設定されている場合でも、メトロ タグが異なるため、トラフィックはサービス プロバイダー ネットワーク内で分離されたままです。各カスタマーは独自の VLAN 番号スペースを制御します。これは、他のカスタマーが使用する VLAN 番号スペースや、サービス プロバイダー ネットワークが使用する VLAN 番号スペースとは無関係です。

802.1Q トンネリングの設定

ここでは、802.1Q トンネリングの設定について説明します。

- 802.1Q トンネリングの設定時の注意事項 (p.23-4)
- 802.1Q トンネリングおよび他の機能 (p.23-5)
- 802.10 トンネルポートの設定(p.23-6)



デフォルトのスイッチポート モードが dynamic auto であるため、802.1Q トンネリングはデフォルトでディセーブルです。802.1Q ネイティブ VLAN パケットのタギングも、すべての 802.1Q トランク ポートでディセーブルです。

802.1Q トンネリングの設定時の注意事項

802.1Q トンネリングを設定する場合は、トンネルを通過するトラフィックに対して常に非対称リンクを使用し、トンネルごとに 1 つの VLAN を専用にする必要があります。また、ネイティブ VLAN の設定要件と Maximum Transmission Unit (MTU; 最大伝送ユニット)にも注意する必要があります。 MTU の詳細については、「システム MTU」(p.23-5) を参照してください。

ネイティブ VLAN

エッジ スイッチ上に 802.1Q トンネリングを設定する場合は、サービス プロバイダー ネットワークへのパケット送信に 802.1Q トランク ポートを使用する必要があります。ただし、サービス プロバイダー ネットワークのコアを通過するパケットは、802.1Q トランク、ISL (スイッチ間リンク)トランク、または非トランク リンクを通じて伝送されることがあります。802.1Q トランクをこれらのコア スイッチで使用する場合には、802.1Q トランクのネイティブ VLAN を、同じスイッチ上の非トランク(トンネリング)ポートのどのネイティブ VLAN にも一致させないでください。ネイティブ VLAN 上のトラフィックが VLAN とのトラフィックが VLAN とのトラフィック VL

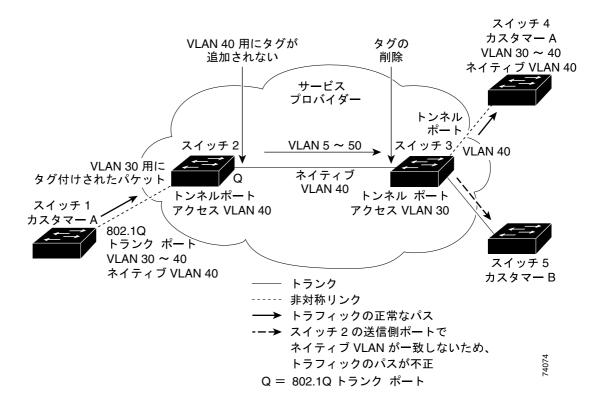
図 23-3 を参照してください。VLAN 40 は、サービス プロバイダー ネットワーク (スイッチ 2) の入力エッジ スイッチで、カスタマー A の 802.1Q トランク ポートのネイティブ VLAN として設定されています。カスタマー A のスイッチ 1 は、タグ付きパケットを VLAN 30 から、アクセス VLAN 40 に属するサービス プロバイダー ネットワーク内のスイッチ 2 の入力トンネル ポートに送信します。トンネル ポートのアクセス VLAN (VLAN 40) は、エッジ スイッチ トランク ポートのネイティブ VLAN (VLAN 40) と同じなので、メトロ タグはトンネル ポートから受信したタグ付きパケットに追加されません。パケットは、サービス プロバイダー ネットワークを通じて VLAN 30 タグだけを出力エッジ スイッチ (スイッチ 3) のトランク ポートに伝送し、出力スイッチ トンネルポートを通じてカスタマー B に誤って転送してしまいます。

この問題の解決には、次のような方法があります。

- サービス プロバイダー ネットワークのコア スイッチ間で ISL トランクを使用します。エッジスイッチに接続したカスタマー インターフェイスは 802.1Q トランクに設定する必要がありますが、コア レイヤ内のスイッチの接続には ISL トランクを使用することを推奨します。
- ネイティブ VLAN を含めて、802.1Q トランクから送信されるすべてのパケットがタグ付けされるようにエッジスイッチを設定するには、switchport trunk native vlan tag ポート単位コマンドおよび vlan dot1q tag native グローバル コンフィギュレーション コマンドを使用します。すべての802.1Q トランクでネイティブ VLAN パケットにタグ付けするようにスイッチを設定すると、スイッチは、トランクから送信されるパケットすべてにタグ付けされているか確認し、トランクポート上でタグのないパケットを受信しません。

• エッジ スイッチ トランク ポートのネイティブ VLAN ID がカスタマー VLAN の範囲内にない ことを確認します。たとえば、トランク ポートが VLAN 100 ~ 200 のトラフィックを伝送する 場合は、ネイティブ VLAN にはその範囲外の番号を割り当てます。

図 23-3 802.1Q トンネリングとネイティブ VLAN で予想される問題



システム MTU

Catalyst 4500 シリーズ スイッチ上のトラフィックに対するデフォルトのシステム MTU は、1500 バイトです。system mtu グローバル コンフィギュレーション コマンドを使用すると、より大きなフレームをサポートするようにスイッチを設定できます。メトロ タグが追加されたときに、802.1Q トンネリング機能によってフレーム サイズが 4 バイト増えるので、スイッチのシステム MTU サイズを 1504 バイト以上に増やして、サービス プロバイダー ネットワーク内のすべてのスイッチがより大きなフレームを処理できるように設定する必要があります。Catalyst 4500 ギガビット イーサネット スイッチの最大許容システム MTU は、9198 バイトです。ファスト イーサネット スイッチの最大システム MTU は、1552 バイトです。

802.1Q トンネリングおよび他の機能

802.1Q トンネリングは、レイヤ 2 パケット スイッチングに対して適切に機能しますが、レイヤ 2 機能とレイヤ 3 スイッチングとは一部互換性がありません。

- トンネル ポートはルーテッド ポートにできません。
- IP ルーティングは、802.1Q ポートを含む VLAN ではサポートされません。トンネル ポートから受信されたパケットは、レイヤ 2 情報にのみ基づいて転送されます。トンネル ポートを含む Switch Virtual Interface (SVI; スイッチ仮想インターフェイス)上でルーティングがイネーブルの場合は、トンネル ポートから受信したタグなし IP パケットがスイッチによって認識され、

ルーティングされます。カスタマーはネイティブ VLAN を介してインターネットにアクセスできます。このアクセスが必要ない場合は、トンネル ポートを含む VLAN に SVI を設定しないでください。

- トンネル ポートは、IP Access Control List (ACL; アクセス コントロール リスト)をサポートしません。
- レイヤ 3 QoS (Quality of Service) ACL とレイヤ 3 情報に関連するその他の QoS 機能はトンネル ポートではサポートされていません。トンネル ポートでは、MAC(メディア アクセス制御) ベースの QoS はサポートされません。
- EtherChannel ポート グループは、802.1Q 設定が EtherChannel ポート グループ内で一貫している かぎりは、トンネル ポートと互換性があります。
- 802.1Q トンネル ポートでは、Port Aggregation Protocol(PAgP) Link Aggregation Control Protocol (LACP) および UniDirectional Link Detection (UDLD; 単一方向リンク検出)がサポートされます。
- Dynamic Trunking Protocol (DTP; ダイナミック トランキング プロトコル)は、802.1Q トンネリングと互換性がありません。これは、トンネル ポートおよびトランク ポートとの非対称リンクを手動で設定しなければならないためです。
- ループバック検出は、802.1Q トンネル ポートでサポートされています。
- 802.1Q トンネル ポートとしてポートが設定されている場合、スパニングツリー Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) フィルタリングは、インターフェイスで自動的にイネーブルに設定されます。Cisco Discovery Protocol (CDP; シスコ検出プロトコル) は、インターフェイスで自動的にディセーブルに設定されます。

802.1Q トンネル ポートの設定

ポートを 802.1Q トンネル ポートとして設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開 始します。
ステップ 2	Switch(config)# interface interface-id	インターフェイス コンフィギュレーション モードを開始し、トンネル ポートとして設定するインターフェイスを入力します。このインターフェイスは、カスタマー スイッチに接続するサービス プロバイダー ネットワークのエッジ ポートである必要があります。有効なインターフェイスには、物理インターフェイスとポートチャネル論理インターフェイス(ポートチャネル1 ~ 64)があります。
ステップ 3	Switch(config-if)# switchport access vlan vlan-id	インターフェイスがトランキングを停止した場合に使用されるデフォルト VLAN を指定します。この VLAN ID は、特定のカスタマーに対して固有です。
ステップ 4	Switch(config-if)# switchport mode dot1q-tunnel	インターフェイスを 802.1Q トンネル ポートとし て設定します。
ステップ 5	Switch(config-if)# exit	グローバル コンフィギュレーション モードに戻 ります。

	コマンド	目的			
ステップ 6	Switch(config)# vlan dot1q tag native	(任意) すべての 802.1Q トランク ポートでネイティブ VLAN パケットのタギングがイネーブルとなるようにスイッチを設定します。このように設定されていない場合、カスタマー VLAN ID がネイティブ VLAN と同じときは、トランク ポートはメトロ タグを適用せず、パケットが誤った			
		宛先に送信されることがあります。			
ステップ 7	Switch(config)# end	特権 EXEC モードに戻ります。			
ステップ 8	Switch# show dot1q-tunnel	スイッチ上のトンネル ポートを表示します。			
ステップ 9	Switch# show vlan dot1q tag native	802.1Q ネイティブ VLAN タギング ステータスを 表示します。			
ステップ 10	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定 を保存します。			

ポートを dynamic auto のデフォルト ステートに戻すには、no vlan dot1q tag native グローバル コマンドおよび no switchport mode dot1q-tunnel インターフェイス コンフィギュレーション コマンドを使用します。ネイティブ VLAN パケットのタギングをディセーブルにするには、no vlan dot1q tag native グローバル コンフィギュレーション コマンドを使用します。

次に、インターフェイスをトンネル ポートとして設定し、ネイティブ VLAN パケットのタギング をイネーブルにして、設定を確認する方法を示します。この設定では、インターフェイス Gigabit Ethernet 2/7 に接続しているカスタマーの VLAN ID は VLAN 22 です。

```
Switch(config) # interface gigabitethernet2/7
Switch(config-if) # switchport access vlan 22
% Access VLAN does not exist. Creating vlan 22
Switch(config-if) # switchport mode dot1q-tunnel
Switch(config-if) # exit
Switch(config) # vlan dot1q tag native
Switch(config) # end
Switch# show dot1q-tunnel interface gigabitethernet2/7
Port
----
LAN Port(s)
----
Gi2/7
Switch# show vlan dot1q tag native
dot1q native vlan tagging is enabled globally
```

レイヤ 2 プロトコル トンネリングの概要



Supervisor Engine 6-E は、レイヤ 2 プロトコル トンネリングをサポートしていません。

サービス プロバイダー ネットワークを通して接続された各サイトのカスタマーは、各種のレイヤ 2 プロトコルを使用してトポロジを拡張し、すべてのリモート サイトおよびローカル サイトを組み込む必要があります。Spanning-Tree Protocol (STP; スパニングツリー プロトコル) が正常に実行され、すべての VLAN で、サービス プロバイダー ネットワークを通してローカル サイトおよびすべてのリモート サイトを組み込んだ適切なスパニングツリーを構築する必要があります。CDP は、ローカルおよびリモート サイトから近接するシスコ製デバイスを検出する必要があります。VLAN Trunking Protocol (VTP; VLAN トランキング プロトコル)は、カスタマー ネットワークのすべてのサイトに一貫した VLAN 設定を提供する必要があります。

プロトコル トンネリングがイネーブルになると、サービス プロバイダー ネットワークの着信側の エッジ スイッチは、特殊 MAC アドレスでレイヤ 2 プロトコル パケットをカプセル化し、サービス プロバイダー ネットワークに送信します。ネットワークのコア スイッチはこれらパケットを処理 しないで、通常パケットとして転送します。CDP、STP、または VTP 用のレイヤ 2 Protocol Data Unit (PDU; プロトコル データ ユニット) は、サービス プロバイダー ネットワークを通過し、サービス プロバイダー ネットワークの発信側にあるカスタマー スイッチに配信されます。同じ VLAN 上の すべてのカスタマー ポートで同じパケットが受信され、次のような結果となります。

- 各カスタマー サイトのユーザは、正常に STP を実行できます。また、すべての VLAN は、ローカル サイトからだけでなくすべてのサイトのパラメータに基づいて、正しいスパニングツリーを構築できます。
- CDP は、サービス プロバイダー ネットワークを介して接続した他のシスコ製デバイスに関する情報を検出して、表示します。
- VTP は、サービス プロバイダーを通じてすべてのスイッチに VLAN 設定を伝播し、カスタマーネットワーク全体で統一します。

レイヤ 2 プロトコル トンネリングは、トランク、アクセス、およびトンネル ポートでイネーブル にすることができます。プロトコル トンネリングがイネーブルでない場合、サービス プロバイダーネットワークの受信側にあるリモート スイッチは PDU を受信せず、STP、CDP、および VTP を正常に実行できません。プロトコル トンネリングがイネーブルの場合、各カスタマー ネットワークのレイヤ 2 プロトコルは、サービス プロバイダー ネットワーク内で稼働しているプロトコルとは全面的に切り離されます。

たとえば、図 23-4 では、カスタマー A は、サービス プロバイダー ネットワークを介して接続された同じ VLAN に 4 つのスイッチを持っています。ネットワークが PDU をトンネリングしない場合、ネットワークの遠端のスイッチは STP、CDP、および VTP を正常に実行できません。たとえば、カスタマー A のサイト 1 にあるスイッチ上の VLAN に対する STP は、サイト 2 にあるカスタマー A のスイッチに基づくコンバージェンス パラメータを考慮しないで、そのサイトにあるスイッチ上にスパニングツリーを構築します。図 23-5 に、スパニングツリートポロジの一例を示します。

図 23-4 レイヤ 2 プロトコル トンネリング

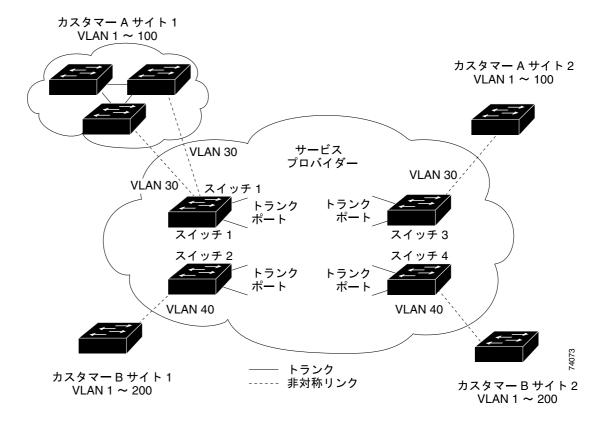
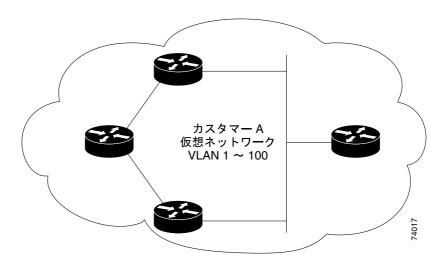


図 23-5 コンパージェンスが不適切なレイヤ 2 ネットワーク トポロジ



レイヤ 2 プロトコル トンネリングの設定

サービス プロバイダー ネットワークのエッジ スイッチのカスタマーに接続されたアクセス ポート、トンネル ポート、またはトランク ポートで、レイヤ 2 プロトコル トンネリング (プロトコルを使用)をイネーブルにできます。カスタマー スイッチに接続されたサービス プロバイダーのエッジ スイッチは、トンネリング プロセスを実行します。エッジ スイッチのトンネル ポートまたは通常のトンネル ポートは、カスタマーの 802.1Q トランク ポートに接続できます。エッジ スイッチのアクセス ポートは、カスタマーのアクセス ポートに接続されます。

サービス プロバイダーの着信エッジ スイッチ ポートに入ったレイヤ 2 PDU が、トランク ポートを介してサービス プロバイダー ネットワークに入ると、スイッチは、カスタマー PDU 宛先 MAC アドレスをシスコ独自の well-known マルチキャスト アドレス (01-00-0c-cd-cd-d0) で上書きします。802.1Q トンネリングが入力ポートでイネーブルの場合、パケットも二重タグ付きです。外側のタグはカスタマーのメトロ タグで、内側のタグはカスタマーの VLAN タグです。

トンネル ポートまたはアクセス ポートを介してサービス プロバイダーの着信エッジ スイッチに入ったレイヤ 2 PDU が、トランク ポートを介してサービス プロバイダー ネットワークに入ると、スイッチは、カスタマー PDU 宛先 MAC アドレスをシスコ独自の well-known マルチキャスト アドレス (01-00-0c-cd-cd-d0) で上書きします。ここで、802.1Q トンネリングがイネーブルの場合、パケットは二重タグ付きです。外側のタグはカスタマーのメトロ タグで、内側のタグはカスタマーの VLAN タグです。コア スイッチは内側のタグを無視して、同じメトロ VLAN のすべてのトランク ポートにパケットを転送します。発信側のエッジ スイッチは、正しいレイヤ 2 プロトコルと MAC アドレス情報を復元して、同じメトロ VLAN のすべてのトンネル ポートまたはアクセス ポートにパケットを転送します。したがって、レイヤ 2 PDU は完全な状態のままで保持され、サービスプロバイダーネットワークを介してカスタマーネットワークの反対側に配信されます。

図 23-4 を参照してください。カスタマー A とカスタマー B は、それぞれアクセス VLAN 30 と 40 内にあります。非対称リンクは、サイト 1 のカスタマーをサービス プロバイダー ネットワークの エッジ スイッチに接続します。サイト 1 のカスタマー B からスイッチ 2 に着信するレイヤ 2 PDU (BPDU など) は、宛先 MAC アドレスとして well-known MAC アドレスを持つ二重タグ付きパケットとしてインフラストラクチャに転送されます。この二重タグ付きパケットは、内側の VLAN タグ (VLAN 100 など) だけでなく、メトロ VLAN タグ (40) も備えています。二重タグ付きパケットがスイッチ 4 に着信すると、メトロ VLAN タグ 40 は削除されます。well-known MAC アドレスは各レイヤ 2 プロトコル MAC アドレスに置き換わり、パケットは VLAN 100 の一重タグ付きフレームとしてサイト 2 のカスタマー B に送信されます。

カスタマー スイッチのアクセス ポートに接続されたエッジ スイッチのアクセス ポートで、レイヤ2 プロトコル トンネリングをイネーブルにすることもできます。この場合、カプセル化とカプセル化解除のプロセスは、上記の説明と同じです。ただし、パケットはサービス プロバイダー ネットワークで二重タグ付けされません。一重タグは、カスタマー固有のアクセス VLAN タグです。

ここでは、次の内容について説明します。

- レイヤ2プロトコルトンネリングのデフォルト設定(p.23-11)
- レイヤ 2 プロトコル トンネリングの設定時の注意事項 (p.23-11)
- レイヤ 2 トンネリングの設定 (p.23-12)

レイヤ 2 プロトコル トンネリングのデフォルト設定

表 23-1 に、レイヤ 2 プロトコル トンネリングのデフォルト設定を示します。

表 23-1 レイヤ 2 イーサネット インターフェイス VLAN のデフォルト設定

機能	デフォルト設定
レイヤ 2 プロトコル トンネリング	ディセーブル。
シャットダウンしきい値	未設定
ドロップしきい値	未設定
CoS 値	データ パケット用のインターフェイスに CoS 値が設定されている場合は、その値がレイヤ 2 PDU に使用されるデ
	フォルトです。未設定の場合、デフォルトは5です。

レイヤ2プロトコルトンネリングの設定時の注意事項

ここでは、レイヤ 2 プロトコル トンネリングの設定時の注意事項および動作特性について説明します。

- スイッチは、CDP、Multiple STP (MSTP) を含めた STP、および VTP のトンネリングをサポートします。プロトコル トンネリングはデフォルトでディセーブルに設定されていますが、802.1Q トンネル ポート、アクセス ポート、またはトランク ポート上でプロトコルごとにイネーブルにできます。
- DTP はレイヤ 2 プロトコル トンネリングと互換性がありません。これは、トンネル ポートおよびトランク ポートとの非対称リンクを手動で設定しなければならないためです。
- 802.1Q 設定が EtherChannel ポート グループ内で一貫している場合、EtherChannel ポート グループはトンネル ポートと互換性があります。
- レイヤ 2 トンネリングがイネーブルに設定されたポートでカプセル化 PDU (独自の宛先 MAC アドレス付き)を受信した場合は、ループを防止するためポートはシャットダウンされます。
- プロトコルに設定されたシャットダウンしきい値に達した場合も、ポートはシャットダウンされます。ポートは手動で再びイネーブルにできます(shutdown および no shutdown コマンドを続けて入力します)。エラーディセーブル回復がイネーブルの場合は、指定インターバル後に処理が再試行されます。
- カプセル化が解除された PDU のみが、カスタマーネットワークに転送されます。サービス プロバイダー ネットワーク上で稼働するスパニングツリー インスタンスは、レイヤ 2 プロトコルトンネリング ポートに BPDU を転送しません。CDP パケットはレイヤ 2 プロトコルトンネリング ポートから転送されません。
- インターフェイスでプロトコル トンネリングがイネーブルの場合は、カスタマー ネットワークによって生成された PDU に対して、プロトコル単位、ポート単位でシャットダウンしきい値を設定できます。上限を超過すると、ポートはシャットダウンします。レイヤ 2 プロトコルトンネリング ポートに QoS ACL およびポリシー マップを使用して、BPDU レートを制限することもできます。
- インターフェイスでプロトコル トンネリングがイネーブルの場合は、カスタマー ネットワークによって生成された PDU に対して、プロトコル単位、ポート単位でドロップしきい値を設定できます。限度を超過した場合は、受信レートがドロップしきい値を下回るまで、PDU はドロップされます。
- カスタマーの仮想ネットワークが正常に動作するように、トンネリングされた PDU (特に STP BPDU)をすべてのリモート サイトに配信する必要があるので、サービス プロバイダー ネットワーク内の PDU には、同じトンネル ポートで受信したデータ パケットより高いプライオリティを設定してください。デフォルトでは、PDU はデータ パケットと同じ CoS 値を使用します。

レイヤ2トンネリングの設定

特定のポートにレイヤ2プロトコルトンネリングを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# interface interface-id	インターフェイス コンフィギュレーション モードを開始し、トンネル ポートとして設定するインターフェイスを入力します。このインターフェイスは、カスタマー スイッチに接続するサービス プロバイダー ネットワークのエッジポートである必要があります。有効なインターフェイスには、物理インターフェイスとポートチャネル論理インターフェイス(ポートチャネル1~64)があります。
ステップ 3	Switch(config-if)# switchport mode access または Switch(config-if)# switchport mode dot1q-tunnel または Switch(config-if)# switchport mode trunk	インターフェイスをアクセス ポート、802.1Q トンネル ポート、またはトランク ポートとして設定します。
ステップ 4	Switch(config-if)# 12protocol-tunnel [cdp stp vtp]	目的のプロトコルに対してプロトコル トンネリングをイネーブルにします。キーワードを入力しない場合、トンネリングはすべてのレイヤ 2 プロトコルに対してイネーブルです。
ステップ 5	Switch(config-if)# 12protocol-tunnel shutdown-threshold [cdp stp vtp] value	(任意)1 秒間にカプセル化可能なパケット数を表すしきい値を設定します。設定されたしきい値を超過すると、インターフェイスはディセーブルになります。プロトコル オプションを指定しない場合、しきい値はトンネリングされた各レイヤ2プロトコル タイプに適用されます。指定できる範囲は1~4096です。デフォルトでは、しきい値は設定されていません。
		(注) 現在のインターフェイスにドロップしきい値も設定する場合は、シャットダウンしきい値にドロップしきい値以上の値を指定する必要があります。
ステップ 6	Switch(config-if)# 12protocol-tunnel drop-threshold [cdp stp vtp] value	(任意)1秒間にカプセル化可能なパケット数を表すしきい値を設定します。設定されたしきい値を超過すると、インターフェイスはパケットをドロップします。プロトコルオプションを指定しない場合、しきい値はトンネリングされた各レイヤ2プロトコルタイプに適用されます。指定できる範囲は1~4096です。デフォルトでは、しきい値は設定されていません。 【注】 現在のインターフェイスにシャットダウンしきい
ステップィ	Switch(config-if)# exit	値も設定する場合は、ドロップしきい値にシャット ダウンしきい値以下の値を指定する必要がありま す。 グローバルコンフィギュレーション モードに戻ります。
A) 9) 1	- Switch (Contrag - 11) # CAIC	ツローハル コノノイヤュレーション モートに戻りより。

	コマンド	目的		
ステップ 8	Switch(config)# errdisable recovery cause l2ptguard	(任意)レイヤ2最大レートエラーからの復旧メカニズムを設定して、インターフェイスがふたたびイネーブルになり、再試行できるようにします。エラーディセーブル回復はデフォルトでディセーブルに設定されています。イネーブルにした場合、デフォルトのタイムインターバルは300秒です。		
ステップ 9	Switch(config)# 12protocol-tunnel cos value	(任意) トンネリングされたすべてのレイヤ 2 PDU に対して CoS 値を設定します。指定できる範囲は $0 \sim 7$ です。デフォルトは、インターフェイスのデフォルトの CoS 値です。未設定の場合、デフォルトは 5 です。		
ステップ 10	Switch(config)# end	特権 EXEC モードに戻ります。		
ステップ 11	Switch# show 12protocol	設定済みのプロトコル、しきい値、カウンタも含めてスイッチのレイヤ 2 トンネル ポートを表示します。		
ステップ 12	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。		

3 つのレイヤ 2 プロトコルのいずれか、またはすべてに対してプロトコルトンネリングをディセーブルにするには、no l2protocol-tunnel [cdp | stp | vtp] インターフェイス コンフィギュレーション コマンドを使用します。シャットダウンしきい値およびドロップしきい値をデフォルト設定に戻すには、no l2protocol-tunnel shutdown-threshold [cdp | stp | vtp] および no l2protocol-tunnel drop-threshold [cdp | stp | vtp] コマンドを使用します。

次に、802.1Q トンネル ポートに CDP、STP、および VTP のレイヤ 2 プロトコル トンネリングを設定し、その設定を確認する例を示します。

```
Switch(config) # interface FastEthernet2/1
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# 12protocol-tunnel cdp
Switch(config-if)# 12protocol-tunnel stp
Switch(config-if)# 12protocol-tunnel vtp
Switch(config-if) # 12protocol-tunnel shutdown-threshold 1500
Switch(config-if) # 12protocol-tunnel drop-threshold 1000
Switch(config-if)# exit
Switch(config) # 12protocol-tunnel cos 7
Switch(config)# end
Switch# show 12protocol
COS for Encapsulated Packets: 7
Port Protocol Shutdown Drop
                                   Encapsulation Decapsulation Drop
               Threshold Threshold Counter Counter Counter
Fa2/11 cdp 1500 1000 2288 2282
stp 1500 1000 116 13
vtp 1500 1000 3 67
                                                               0
                                                               0
        vtp
```

トンネリング ステータスのモニタリングおよびメンテナンス

表 23-2 に、802.1Q およびレイヤ 2 プロトコル トンネリングをモニタリングおよびメンテナンスするためのコマンドを示します。

表 23-2 トンネリングを監視およびメンテナンスするためのコマンド

コマンド	目的
Switch# clear 12protocol-tunnel counters	レイヤ 2 プロトコル トンネリング ポートのプロトコル カウンタをクリアします。
Switch# show dot1q-tunnel	スイッチの 802.1Q トンネル ポートを表示します。
Switch# show dot1q-tunnel interface interface-id	特定のインターフェイスがトンネル ポートであるかどうかを確認します。
Switch# show 12protocol-tunnel	レイヤ 2 プロトコル トンネリング ポートに関する情報を表示します。
Switch# show errdisable recovery	レイヤ 2 プロトコル トンネル エラーディセーブル ステートの 回復タイマーがイネーブルかどうかを確認します。
Switch# show 12protocol-tunnel interface interface-id	特定のレイヤ 2 プロトコル トンネリング ポートに関する情報 を表示します。
Switch# show 12protocol-tunnel summary	レイヤ2プロトコルのサマリー情報のみを表示します。
Switch# show vlan dot1q native	スイッチのネイティブ VLAN タギングのステータスを表示します。



Cisco IOS Release 12.2(20)EW では、dot1q およびレイヤ 2 プロトコル トンネリング用の BPDU フィルタリング設定は、実行コンフィギュレーションで [spanning-tree bpdufilter enable] として表示されません。代わりに、show spanning tree int detail コマンドの出力に表示されます(下記を参照)。

Switch# show spann int f6/1 detail

Port 321 (FastEthernet6/1) of VLAN0001 is listening
Port 321 (FastEthernet6/1) of VLAN0001 is listening
Port path cost 19, Port priority 128, Port Identifier 128.321.
Designated root has priority 32768, address 0008.e341.4600
Designated bridge has priority 32768, address 0008.e341.4600
Designated port id is 128.321, designated path cost 0
Timers: message age 0, forward delay 2, hold 0
Number of transitions to forwarding state: 0
Link type is point-to-point by default
** Bpdu filter is enabled internally **
BPDU: sent 0, received 0



CHAPTER

24

CDP の設定

この章では、Catalyst 4500 シリーズ スイッチ上で Cisco Discovery Protocol (CDP; シスコ検出プロトコル) を設定する方法について説明します。設定上の注意事項、設定手順、および設定例についても示します。

この章の主な内容は、次のとおりです。

- CDPの概要 (p.24-2)
- CDPの設定(p.24-2)



この章のコマンドの構文および使用方法の詳細については、次の URL のマニュアルを参照してください。

[®] Cisco IOS Configuration Fundamentals Configuration Guide ^a Release 12.4

 $http://www.cisco.com/univered/cc/td/doc/product/software/ios124/124cr/hcf_r/index.htm$

[©] Cisco IOS Configuration Fundamentals Command Reference ^a Release 12.4

 $http://www.cisco.com/univered/cc/td/doc/product/software/ios124/124tcr/tcf_r/index.htm$



この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/cr/index.htm

CDP の概要

CDP は、すべてのシスコルータ、ブリッジ、アクセス サーバ、およびスイッチ上のレイヤ 2 (データ リンク レイヤ)で動作するプロトコルです。CDP を使用すると、ネットワーク管理アプリケーションで、既知のデバイスに近接しているシスコ製デバイス、特に下位レイヤのトランスペアレント プロトコルを実行している近接デバイスを検索できます。また、近接デバイスのデバイス タイプと SNMP (簡易ネットワーク管理プロトコル)エージェント アドレスも学習できます。さらに、CDP によって、アプリケーションから近接デバイスに SNMP クエリーを送信することもできます。

CDP は、Subnetwork Access Protocol(SNAP)をサポートしているすべてのLAN およびWAN メディア上で稼働します。

CDP を設定した各デバイスは、マルチキャスト アドレスに対して定期的にメッセージを送信します。各デバイスは、SNMP メッセージを受信できるアドレスを少なくとも 1 つアドバタイズします。このアドバタイズには、受信側デバイスで CDP 情報を廃棄せずに保持しておく時間を表す Time To Live (TTL; 存続可能時間)またはホールドタイム情報も含まれます。

CDP の設定

ここでは、CDPの設定手順について説明します。

- CDP のグローバルなイネーブル化 (p.24-2)
- CDP のグローバル設定の表示 (p.24-2)
- インターフェイス上での CDP のイネーブル化 (p.24-3)
- CDP インターフェイスの設定の表示 (p.24-3)
- CDP のモニタリングおよびメンテナンス (p.24-4)

CDP のグローバルなイネーブル化

CDP をグローバルにイネーブルにするには、次の作業を行います。

コマンド	目的
Switch(config)# [no] cdp run	CDP をグローバルにイネーブルにします。
	CDP をグローバルにディセーブルにするには、 no キーワードを使用します。

次に、CDP をグローバルにイネーブルにする例を示します。

Switch(config)# cdp run

CDP のグローバル設定の表示

CDPの設定を表示するには、次の作業を行います。

コマンド	目的
Switch# show cdp	グローバルな CDP 情報を表示します。

次に、CDP の設定を表示する例を示します。

Switch# show cdp
Global CDP information:
Sending CDP packets every 120 seconds
Sending a holdtime value of 180 seconds
Sending CDPv2 advertisements is enabled
Switch#

その他の CDP show コマンドについては、「CDP のモニタリングおよびメンテナンス」(p.24-4) を 参照してください。

インターフェイス上での CDP のイネーブル化

特定のインターフェイス上で CDP をイネーブルにするには、次の作業を行います。

コマンド	目的
Switch(config-if)# [no] cdp enable	特定のインターフェイス上で CDP をイネーブ ルにします。
	特定のインターフェイス上で CDP をディセーブルにするには、no キーワードを使用します。

次に、インターフェイス FastEthernet 5/1 上で CDP をイネーブルにする例を示します。

Switch(config)# interface fastethernet 5/1
Switch(config-if)# cdp enable

次に、インターフェイス FastEthernet 5/1 上で CDP をディセーブルにする例を示します。

Switch(config)# interface fastethernet 5/1
Switch(config-if)# no cdp enable

CDP インターフェイスの設定の表示

インターフェイスの CDP 設定を表示するには、次の作業を行います。

コマンド	目的	
Switch# show cdp interface [type/number]	CDP がイネーブルに設定されているインター	
	フェイスの情報を表示します。	

次に、インターフェイス FastEthernet 5/1 の CDP の設定を表示する例を示します。

Switch# show cdp interface fastethernet 5/1
FastEthernet5/1 is up, line protocol is up
Encapsulation ARPA
Sending CDP packets every 120 seconds
Holdtime is 180 seconds
Switch#

CDP のモニタリングおよびメンテナンス

装置上の CDP をモニタリングおよびメンテナンスするには、次の作業を 1 つまたは複数行います。

コマンド	目的
Switch# clear cdp counters	トラフィック カウンタを 0 にリセットします。
Switch# clear cdp table	近接デバイスに関する情報を収めた CDP テーブルを削除します。
Switch# show cdp	送信の頻度、送信されたパケットを保持する時間など、グローバルな情報を表示します。
Switch# show cdp entry entry_name [protocol version]	特定の近接デバイスに関する情報を表示します。プロトコル情報またはバージョン情報に表示を限定できます。
Switch# show cdp interface [type/number]	CDP がイネーブルに設定されているインターフェイスの情報を表示します。
Switch# show cdp neighbors [type/number] [detail]	近接装置に関する情報を表示します。特定のインターフェイス上の近接デバイスに関する情報に表示を限定することも、より詳細な情報を要求することもできます。
Switch# show cdp traffic	CDP カウンタ (送受信されたパケット数および チェックサム エラーを含む)を表示します。
Switch# show debugging	スイッチでイネーブルに設定されているデバッ グのタイプに関する情報を表示します。

次に、スイッチの CDP カウンタ設定をクリアする例を示します。

Switch# clear cdp counters

次に、近接装置に関する情報を表示する例を示します。

Switch# show cdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch, H - Host, I - IGMP, r - Repeater

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
JAB023807H1	Fas 5/3	127	T S	WS-C2948	2/46
JAB023807H1	Fas 5/2	127	T S	WS-C2948	2/45
JAB023807H1	Fas 5/1	127	T S	WS-C2948	2/44
JAB023807H1	Gig 1/2	122	T S	WS-C2948	2/50
JAB023807H1	Gig 1/1	122	T S	WS-C2948	2/49
JAB03130104	Fas 5/8	167	T S	WS-C4003	2/47
JAB03130104	Fas 5/9	152	T S	WS-C4003	2/48



CHAPTER

25

LLDP および LLDP-MED の設定

この章では、Link Layer Discovery Protocol (LLDP) および LLDP Media Endpoint Discovery (LLDP-MED) を設定する方法について説明します。



この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンド リファレンスおよび『Cisco IOS Configuration Fundamentals Command Reference』Release 12.2 の「System Management Commands」セクションを参照してください。

この章の内容は、次のとおりです。

- LLDP および LLDP-MED の概要 (p.25-2)
- LLDP および LLDP-MED の設定 (p.25-4)
- LLDP と LLDP-MED のモニタリングおよびメンテナンス (p.25-8)

LLDP および LLDP-MED の概要

ここでは、次の概念情報について説明します。

- LLDP の概要 (p.25-2)
- LLDP-MED の概要 (p.25-2)

LLDP の概要

Cisco Discovery Protocol (CDP; シスコ検出プロトコル)は、すべてのシスコ製デバイス (ルータ、ブリッジ、アクセス サーバ、スイッチ)のレイヤ 2 (データ リンク レイヤ)上で稼働するデバイス検出プロトコルです。CDP により、ネットワーク管理アプリケーションは、ネットワークに接続している他のシスコ製デバイスを自動的に検出および学習できます。

シスコ製以外のデバイスをサポートし、他のデバイスとの相互運用性を確保するために、IEEE 802.1AB Link Layer Discovery Protocol (LLDP)をサポートしています。LLDPは、ネットワークデバイスがネットワーク上の他のデバイスに自身についての情報をアドバタイズするために使用する近隣探索プロトコルです。このプロトコルはデータリンクレイヤ上で動作するため、異なるネットワークレイヤプロトコルが稼働する2つのシステムで互いの情報を学習することができます。

LLDP は一連のアトリビュートをサポートし、これを使用して隣接するデバイスを検出します。アトリビュートには、Type、Length、および Value の説明が含まれていて、これらを *TLV* と呼びます。LLDP をサポートするデバイスは、ネイバーとの情報の送受信に TLV を使用することができます。設定情報、デバイスの機能、デバイス ID などの詳細情報は、このプロトコルを使用してアドバタイズできます。

スイッチは、以下の基本管理 TLV をサポートします (オプション)。

- ポート説明 TLV
- システム名 TLV
- システム説明 TLV
- システム機能 TLV
- 管理アドレス TLV

これらの組織的に特定された LLDP TLV は、LLDP-MED をサポートするためにもアドバタイズされます。

- ポート VLAN ID TLV (IEEE 802.1 組織的に特定された TLV)
- MAC/PHY コンフィギュレーション / ステータス TLV (IEEE 802.3 組織的に特定された TLV)

LLDP-MED の概要

LLDP for Media Endpoint Devices (LLDP-MED)は、IP 電話などのエンドポイント デバイスとスイッチなどのネットワーク デバイス間で稼働する LLDP の拡張です。特に、VoIP アプリケーションへのサポートを提供すると同時に、機能検出、ネットワーク ポリシー、Power over Ethernet (PoE; イーサネット経由の電源供給) およびコンポーネント管理に追加の TLV も提供します。デフォルトで、すべての LLDP-MED TLV はイネーブルになっています。

LLDP-MED はこれらの TLV をサポートします。

• LLDP-MED 機能 TLV

LLDP-MED エンドポイントが、接続されたデバイスのサポートする機能およびデバイスでイネーブルになっている機能を判別できるようにします。

• ネットワーク ポリシー TLV

ネットワーク接続デバイスとエンドポイントの両方が、VLAN コンフィギュレーションおよびそのポートの特定アプリケーションの関連レイヤ2およびレイヤ3アトリビュートをアドバタイズできるようにします。たとえば、スイッチは使用すべき VLAN 番号を電話機に通知することができます。電話機は任意のスイッチに接続して、VLAN 番号を取得し、コール制御との通信を開始できます。

• 電源管理 TLV

LLDP-MED エンドポイントとネットワーク接続デバイス間の拡張電源管理をイネーブルにします。スイッチと電話機が、デバイスへの電源供給方法、電源のプライオリティ、デバイスに必要な電源量などの電源情報を伝達できるようにします。

• コンポーネント管理 TLV

エンドポイントが、ハードウェア リビジョン、ファームウェア バージョン、ソフトウェア バージョン、シリアル番号、製造社名、モデル名、および資産 ID TLV などの情報を含む、自身についての詳細なコンポーネント情報を、スイッチに伝送できるようにします。



(注)

スイッチは、LLDP および LLDP-MED を同時にエンド ポイント デバイスに送信することはできません。デフォルトでは、ネットワーク デバイスはエンドポイント デバイスから LLDP-MED パケットを受信するまで LLDP パケットのみを送信します。次にネットワーク デバイスは、LLDP パケットを受信するまで LLDP-MED パケットを送信します。

LLDP および LLDP-MED の設定

ここで説明する設定内容は次のとおりです。

- デフォルトの LLDP 設定 (p.25-4)
- LLDP-MED 特性の設定 (p.25-4)
- LLDP のグローバルなディセーブルにおよびイネーブルに (p.25-5)
- インターフェイス上での LLDP のディセーブルおよびイネーブル (p.25-6)
- LLDP-MED TLV の設定 (p.25-7)

デフォルトの LLDP 設定

表 25-1 に、LLDP のデフォルト設定を示します。デフォルト設定を変更するには、LLDP グローバル コンフィギュレーション コマンドおよび LLDP インターフェイス コンフィギュレーション コマンドを使用します。

表 25-1 デフォルトの LLDP 設定

機能	デフォルト設定
LLDP グローバル ステート	ディセーブル
LLDP ホールドタイム(廃棄までの時間)	120 秒
LLDP タイマー(パケット更新頻度)	30 秒
LLDP 再初期化遅延	2 秒
LLDP tlv-select	すべての TLV の送受信をイネーブルに
LLDP インターフェイス ステート	イネーブル
LLDP 受信	イネーブル
LLDP 転送	イネーブル
LLDP med-tlv-select	すべての MMDP-MED TLV の送信をイネーブルに

LLDP-MED 特性の設定

LLDP アップデートの頻度、情報を廃棄するまでに保持する時間、初期化遅延時間を設定できます。 また、LLDP および LLDP-MED TLV が送受信されるように選択できます。

これらの特性を設定するには、次の作業を行います。



ステップ2~5は任意であり、どの順番で実行してもかまいません。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	(g, <u>.</u>	(任意)デバイスから送信された情報を受信側デバイスが廃棄するまで保持する期間を指定します。
		指定できる範囲は 0 ~ 65535 秒です。デフォルトは 120 秒 です。

	コマンド	目的
ステップ 3	Switch(config)# 11dp reinit	(任意)LLDP が任意のインターフェイスを初期化するとき の遅延時間を秒数で指定します。
		指定できる範囲は2~5秒です。デフォルトは2秒です。
ステップ 4	Switch(config)# 11dp timer seconds	(任意)LLDP更新の送信頻度を秒数で設定します。
		指定できる範囲は 5 ~ 65534 秒です。デフォルトは 30 秒です。
ステップ 5	Switch(config)# 11dp tlv-select	(任意)送受信する LLDP TLV を指定します。
ステップ 6	Switch(config)# exit	特権 EXEC モードに戻ります。
ステップ 7	Switch# copy running-config startup-config	コンフィギュレーション ファイルに設定を保存します。
ステップ 8	Switch# 11dp med-tlv-select	(任意) 送受信する LLDP-MED TLV を指定します。



デフォルトの設定に戻すには、各 LLDP コマンドの no 形式を使用します。

次に、ホールドタイムを 120 秒、遅延時間を 2 秒、更新頻度を 30 に設定する例を示します。

Switch# configure terminal
Switch(config)# 11dp holdtime 120
Switch(config)# 11dp reinit 2
Switch(config)# 11dp timer 30
Switch(config)# end

次に、LLDP パケットのみを転送する例を示します。

switch# configure terminal
siwtch(config)# no lldp receive
switch(config)# end

再び LLDP パケットを受信したい場合は、以下を実行します。

switch# configure terminal
siwtch(config)# lldp receive
switch(config)# end

その他の LLDP show コマンドについては、「LLDP と LLDP-MED のモニタリングおよびメンテナンス」(p.25-8) を参照してください。

LLDP のグローバルなディセーブルにおよびイネーブルに



LLDP はデフォルトでディセーブルです。

LLDP をグローバルにディセーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# no lldp run	LLDP をディセーブルにします。
ステップ 3	Switch# end	特権 EXEC モードに戻ります。

ディセーブルにされている LLDP をグローバルにイネーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# 11dp run	LLDP をイネーブルにします。
ステップ 3	Switch# end	特権 EXEC モードに戻ります。

次に、グローバルに LLDP をディセーブルにする例を示します。

Switch# configure terminal
Switch(config)# no lldp run
Switch(config)# end

次に、グローバルに LLDP をイネーブルにする例を示します。

Switch# configure terminal
Switch(config)# 11dp run
Switch(config)# end

インターフェイス上での LLDP のディセーブルおよびイネーブル

LLDP は、すべてのサポートされているインターフェイス上でグローバルにディセーブルにされています。デバイスで LLDP パケットを送信できるようにするためには、LLDP をグローバルでイネーブルにする必要があり余す。 ただし、インターフェイス レベルでの変更は不要です。

no lldp transmit および no lldp receive コマンドを使用して LLDP パケットを送受信しないようにインターフェイスを設定するように選択することができます。



インターフェイスがトンネル ポートとして設定されている場合、LLDP は自動的にディセーブルになります。

LLDP をインターフェイスでディセーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始しま
		す 。
ステップ 2	Switch(config)# interface interface-id	LLDP をディセーブルにするインターフェイスを指定
		し、インターフェイス コンフィギュレーション モード
		を開始します。
ステップ 3	Switch(config-if)# no lldp transmit	インターフェイスで LLDP パケットが送信できなくな
		ります。

	コマンド	目的
ステップ 4	Switch(config-if)# no lldp receive	インターフェイスで LLDP パケットが受信できなくな
		ります。
ステップ 5	Switch(config-if)# end	特権 EXEC モードに戻ります。
ステップ 6	Switch# copy running-config startup-config	コンフィギュレーション ファイルに設定を保存しま
		す。

ディセーブルにされている LLDP をインターフェイスでイネーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始しま
		す。
ステップ 2	Switch(config# interface interface-id	LLDP をイネーブルにするインターフェイスを指定し、
		インターフェイス コンフィギュレーション モードを開
		始します。
ステップ 3	Switch(config-if)# 11dp transmit	インターフェイスで LLDP パケットを送信します。
ステップ 4	Switch(config-if)# 11dp receive	インターフェイスで LLDP パケットを受信します。
ステップ 5	Switch(config-if)# end	特権 EXEC モードに戻ります。
ステップ 6	Switch# copy running-config startup-config	コンフィギュレーション ファイルに設定を保存しま
		す 。

次に、インターフェイスで LLDP をイネーブルにする例を示します。

Switch# configure terminal
Switch(config)# interface GigabitEthernet 1/1
Switch(config-if)# 1ldp transmit
Switch(config-if)# 1ldp receive
Switch(config-if)# end

LLDP-MED TLV の設定

デフォルトでは、スイッチはエンド デバイスから LLDP-MED パケットを受信するまで、LLDP パケットのみを送信します。デバイスは、LLDP パケットのみを受信するまで LLDP-MED パケットの 送信を続けます。

 ${f lldp}$ インターフェイス コンフィギュレーション コマンドを使用して、表 25-2 に列挙した TLV をインターフェイスに送信しないように設定できます。

表 25-2 LLDP-MED TLV

LLDP-MED TLV	説明
inventory-management	LLDP-MED コンポーネント管理 TLV
location	LLDP-MED ロケーション TLV
network-policy	LLDP-MED ネットワーク ポリシー TLV
power-management	LLDP-MED 電源管理 TLV

TLV をインターフェイスでディセーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	Switch(config# interface interface-id	LLDP-MED TLV を設定するインターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。
ステップ 3	Switch(config-if)# no lldp med-tlv-select $t1v$	ディセーブルにする TLV を指定します。
ステップ 4	Switch(config-if)# end	特権 EXEC モードに戻ります。
ステップ 5	Switch# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を 保存します。

TLV をインターフェイスでイネーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	Switch(config# interface interface-id	LLDP-MED TLV を設定するインターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。
ステップ 3	Switch(config-if)# 11dp med-tlv-select tlv	イネーブルにする TLV を指定します。
ステップ 4	Switch(config-if)# end	特権 EXEC モードに戻ります。
ステップ 5	Switch# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を 保存します。

次に、インターフェイスでディセーブルにされている TLV をイネーブルにする例を示します。

Switch# configure terminal
Switch(config)# interface GigabitEthernet1/0/1
Switch(config-if)# lldp med-tlv-select inventory management
Switch(config-if)# end

LLDP と LLDP-MED のモニタリングおよびメンテナンス

デバイス上で LLDP と LLDP-MED をモニタリングおよびメンテナンスするには、特権 EXEC モードで次の手順の 1 つまたは複数実行します。

コマンド	説明
clear lldp counters	トラフィック カウンタおよびエラー カウンタをゼロにリセットします。
clear lldp table	ネイバーに関する情報を収めた LLDP テーブルを削除します。
show lldp	送信の頻度、送信されたパケットのホールドタイム、LLDP 初期化の遅延時間など、インターフェイス上のグローバル情報を表示します。
show lldp entry entry-name	特定のネイバーに関する情報を表示します。
	アスタリスク(*)を入力して、すべてのネイバーを表示することも、情報 が必要なネイバーの名前を入力することもできます。
show lldp errors	LLDP カプセル化エラーおよびオーバーフローを表示します。

コマンド	説明
show lldp interface [interface-id]	LLDP がイネーブルに設定されているインターフェイスに関する情報を表示します。
	必要なインターフェイスの情報だけを表示できます。
show lldp neighbors [interface-id] [detail]	デバイス タイプ、インターフェイスのタイプや番号、ホールドタイム設定、機能、ポート ID など、ネイバーに関する情報を表示します。
	特定のインターフェイスに関するネイバー情報の表示を制限したり、詳細情報にするために表示を拡張することもできます。
show lldp traffic	送受信パケットの数、廃棄したパケットの数、認識できない TLV の数など、 LLDP カウンタを表示します。

■ LLDP および LLDP-MED の設定



CHAPTER

26

UDLD の設定

この章では、Catalyst 4000 ファミリスイッチ上で UniDirectional Link Detection (UDLD; 単一方向リンク検出) および単一方向イーサネットを設定する方法について説明します。設定上の注意事項、設定手順、および設定例についても示します。

この章の主な内容は、次のとおりです。

- UDLD の概要 (p.26-2)
- UDLD のデフォルト設定 (p.26-3)
- スイッチ上での UDLD の設定 (p.26-3)



この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/cr/index.htm

UDLD の概要

UDLD により、光ファイバまたは銅製イーサネット ケーブル (カテゴリ 5 ケーブルなど)を使用して接続されたデバイスで、ケーブルの物理構成を監視し、単方向リンクの存在を検出できます。リンク上でローカル デバイスが送信したトラフィックを近接デバイスが受信し、近接デバイスから送信されたトラフィックをローカル デバイスが受信しない場合には、単方向リンクが発生します。単方向リンクが検出されると、UDLD が関係のあるインターフェイスをシャットダウンし、ユーザに通知します。単方向リンクは、スパニングツリートポロジ ループをはじめ、さまざまな問題を引き起こす可能性があります。

UDLD は、レイヤ1メカニズムと連動し、リンクの物理的ステータスを判別するレイヤ2プロトコルです。レイヤ1では、物理的シグナリングおよび障害検出は、自動ネゴシエーションによって処理されます。UDLD は、近接デバイスの ID の検知、誤って接続されたインターフェイスのシャットダウンなど、自動ネゴシエーションでは実行不可能な処理を実行します。自動ネゴシエーションと UDLD の両方をイネーブルにすると、レイヤ1とレイヤ2の検知機能が連動し、物理的および論理的な単方向接続、および他のプロトコルの誤動作を防止します。

対になっているファイバストランドのどちらかの接続が切断された場合、自動ネゴシエーションがアクティブであるかぎり、そのリンクは存続できません。この場合、論理リンクは不確定で、UDLDは何の処理も行いません。レイヤ1から見て両方のファイバが正常に稼働していれば、レイヤ2のUDLDはそれらのファイバが正しく接続されているかどうか、トラフィックが正しい近接デバイス間で双方向に流れているかどうかを判別します。自動ネゴシエーションはレイヤ1の機能なので、このチェックは自動ネゴシエーションでは不可能です。

スイッチは、近接デバイスの UDLD がイネーブルのインターフェイスに、UDLD パケットを定期的に送信します。このパケットが一定時間内にエコー バックされるのに、特定の確認応答(エコー)が欠落している場合には、そのリンクは単方向リンクとしてフラグ付けされ、インターフェイスがシャットダウンされます。プロトコルが単方向リンクを正しく識別し、その使用を禁止するには、リンクの両側のデバイスで UDLD をサポートする必要があります。

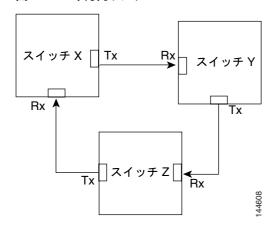


(注)

デフォルトでは、UDLD は銅製インターフェイス上ではローカルでディセーブルに設定されています。この種類のメディアは、アクセス インターフェイスに使用されることが多いので、メディアに不要な制御トラフィックを送信しないようにするためです。

図 26-1 に、単方向リンクの例を示します。各スイッチは近接スイッチにパケットを送信できますが、パケットの送信先と同じスイッチからのパケットは受信できません。UDLD は単方向接続を検出し、ディセーブルにします。

図 26-1 単方向リンク



UDLD のデフォルト設定

表 26-1 に、UDLD のデフォルト設定を示します。

表 26-1 UDLD のデフォルト設定

機能	デフォルト ステータス
UDLD グローバル イネーブル ステート	グローバルにディセーブル
インターフェイス別の UDLD イネーブル ステート(光ファ	
イバ メディア用)	ネーブル
インターフェイス別の UDLD イネーブル ステート(ツイス	インターフェイス Ethernet 10/100 と 1000BASE-TX でディ
トペア[銅製]メディア用)	セーブル

スイッチ上での UDLD の設定

ここでは、UDLD の設定手順について説明します。

- UDLD のグローバルなイネーブル化 (p.26-3)
- インターフェイス上で UDLD をイネーブルにする方法 (p.26-4)
- 光ファイバ以外のインターフェイス上での UDLD のディセーブル化 (p.26-4)
- 光ファイバインターフェイス上での UDLD のディセーブル化 (p.26-4)
- ディセーブルになったインターフェイスのリセット (p.26-4)

UDLD のグローバルなイネーブル化

スイッチ上のすべての光ファイバ インターフェイス上で UDLD をグローバルにイネーブルにするには、次の作業を行います。

コマンド	目的	
Switch(config)# [no] udld enable	スイッチの光ファイバ インターフェイス上で UDLD をグローバルにイネーブルにします。 光ファイバ インターフェイス上で UDLD をグローバルにディセーブルにするには、no キーワードを使用します。	
	(注) このコマンドは、光ファイバ インターフェイスだけを設定します。このコマンドによる設定は、個々のインターフェイスの設定によって上書きされます。	
	(注) Stateful Switchover (SSO) と UDLD の相互運用性に注意してください。 UDLD がグローバルでイネーブルの場合、UDLD に参加しているインターフェイスは errdisable ステートになる可能性があります。そのようなインターフェイスは、SSO のあとでも errdisable ステートのままになります。SSO の間、UDLD 内部ステートはアクティブ スーパーバイザとスタンバイ スーパーバイザとの間で同期しません。その結果、UDLDがグローバルにディセーブルになってもインターフェイスは errdisable ステートのままになりますこのような状況では、「errdisable recover cause udld」コマンドを設定して errdisable ステートから抜けることができます。	

インターフェイス上で UDLD をイネーブルにする方法

各インターフェイス上で UDLD をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config-if)# udld enable	特定のインターフェイス上で UDLD をイネーブルにしま
		す。光ファイバ インターフェイスの場合、このコマンドは
		udld enable グローバル コンフィギュレーション コマンド
		による設定を上書きします。
ステップ 2	Switch# show udld interface	設定を確認します。

光ファイバ以外のインターフェイス上での UDLD のディセーブル化

個々の光ファイバ以外のインターフェイス上で UDLD をディセーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config-if)# no udld enable	光ファイバ以外のインターフェイス上で UDLD をディセーブルにします。 ◇ (注) 光ファイバ インターフェイスの場合、no udld enable コマンドを使用すると、インターフェイスの設定は udld enable グローバル コンフィギュレーション コマンドによる設定に戻ります。
ステップ 2	Switch# show udld interface	設定を確認します。

光ファイバ インターフェイス上での UDLD のディセーブル化

特定の光ファイバインターフェイス上で UDLD をディセーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config-if)# udld disable	光ファイバインターフェイス上でUDLDをディセーブルにします。
		(注) このコマンドは、光ファイバ以外のインターフェイ ス上ではサポートされていません。
		udld enable グローバル コンフィギュレーション コマンド の設定に戻すには、no キーワードを使用します。
ステップ 2	Switch# show udld interface	設定を確認します。

ディセーブルになったインターフェイスのリセット

UDLD によってシャットダウンされたすべてのインターフェイスをリセットするには、次の作業を行います。

コマンド	目的
Switch# udld reset	UDLD によってシャットダウンされたすべてのインター
	フェイスをリセットします。



CHAPTER

27

レイヤ3インターフェイスの設定

この章では、Catalyst 4500 シリーズ スイッチ上のレイヤ 3 インターフェイスについて説明します。 設定上の注意事項、設定手順、および設定例についても示します。

この章の主な内容は、次のとおりです。

- レイヤ 3 インターフェイスの概要 (p.27-2)
- 設定時の注意事項 (p.27-6)
- 論理レイヤ 3 VLAN インターフェイスの設定 (p.27-7)
- レイヤ 3 インターフェイスとしての VLAN の設定 (p.27-9)
- 物理レイヤ 3 インターフェイスの設定 (p.27-14)
- EIGRP スタブ ルーティングの設定 (p.27-15)



この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/cr/index.htm

レイヤ3インターフェイスの概要

ここでは、次の内容について説明します。

- 論理レイヤ 3 VLAN インターフェイス (p.27-2)
- 物理レイヤ3インターフェイス(p.27-3)
- SVI 自動ステート除外の概要 (p.27-3)
- レイヤ3インターフェイスカウンタの概要(p.27-4)

Catalyst 4500 ファミリ スイッチは、Cisco IOS IP および IP ルーティング プロトコルでレイヤ 3 インターフェイスをサポートしています。 ネットワーク レイヤであるレイヤ 3 は、主にパケット内データの論理インターネットワーク パスへのルーティングを行います。

データ リンク レイヤであるレイヤ 2 は、物理レイヤ (レイヤ 1)を制御するプロトコルと、メディアに伝送される前のデータのフレーミング方法が含まれています。LAN 上の 2 つのセグメント間でフレーム内のデータをフィルタリングおよび転送するレイヤ 2 の機能を、 ブリッジングといいます。

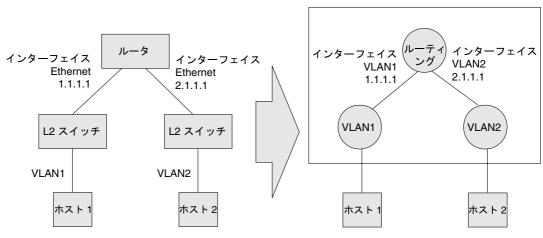
Catalyst 4500 シリーズ スイッチは、2 種類のレイヤ 3 インターフェイスをサポートしています。論理レイヤ 3 VLAN (仮想 LAN)インターフェイスは、ルーティングとブリッジングの機能を統合します。Catalyst 4500 シリーズ スイッチは、物理レイヤ 3 インターフェイスを使用して従来のルータのように設定できます。

論理レイヤ 3 VLAN インターフェイス

論理レイヤ 3 VLAN インターフェイスは、レイヤ 2 スイッチ上の VLAN への論理ルーティング インターフェイスとして機能します。従来のネットワークでは、ルータとスイッチ間の物理インターフェイスが VLAN 間ルーティングを実行する必要がありました。Catalyst 4500 シリーズ スイッチは単一の Catalyst 4500 シリーズ スイッチでのルーティングとブリッジング機能を統合することで、VLAN 間ルーティングをサポートします。

図 27-1 では、従来のネットワークで 3 台の物理デバイスによって実行されていたルーティングとブリッジング機能が、どのようにして 1 台の Catalyst 4500 シリーズ スイッチ上で論理的に実行されているかを示します。

図 27-1 Catalyst 4500 シリーズ スイッチの論理レイヤ 3 VLAN インターフェイス



VLAN 間ルーティングでの従来の ネットワーク トポロジ

1 台の Catalyst 4500 シリーズ スイッチ での VLAN 間論理ルーティング

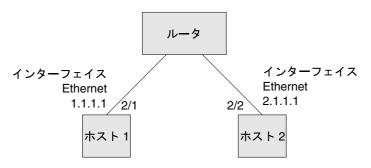
94169

物理レイヤ3インターフェイス

物理レイヤ 3 インターフェイスは、従来のルータに等しい機能をサポートします。これらのレイヤ 3 インターフェイスは、Catalyst 4500 シリーズ スイッチへの物理ルーティング インターフェイスを ホストに提供します。

図 27-2 に、Catalyst 4500 シリーズ スイッチが従来のルータとして機能する例を示します。

図 27-2 Catalyst 4500 シリーズ スイッチの物理レイヤ 3 インターフェイス



Catalyst 4500 シリーズ スイッチでの VLAN 間物理ルーティング⁵

SVI 自動ステート除外の概要



Supervisor Engine 6-E は、SVI 自動ステート除外をサポートして*いません*。

ルータ VLAN インターフェイスは「アップ / アップ 」状態となるために、次の一般的な条件を満たす必要があります。

- VLAN がスイッチの VLAN データベースに存在し、「アクティブ」であること。
- VLAN インターフェイスがルータに存在し、管理上のダウン状態であること。
- 少なくとも1つのレイヤ2(アクセスポートまたはトランク)ポートが存在し、この VLAN 上でリンクが「アップ」状態であり、VLAN でスパニングツリー フォワーディング ステートであること。



(注)

対応する VLAN リンクに属する最初のスイッチポートがアップになり、スパニングツリー フォワーディング ステートとなると、VLAN インターフェイスのプロトコル ライン ステートがアップになります。

通常、VLAN 内に VLAN インターフェイスのポートが複数ある場合は、VLAN 内のすべてのポートが「ダウン」するときに SVI が「ダウン」します。 SVI 自動ステート除外機能は、 SVI の「アップおよびダウン」カウント時にカウントしないポートをマーキングするノブになり、ポートでイネーブルであるすべての VLAN に適用されます。

VLAN インターフェイスは、レイヤ 2 ポートがコンバージェンス (つまり、リスニングおよびラーニングからフォワーディングに移行) する時間を経過した後、起ち上がります。これにより、ルーティング プロトコルおよびその他の機能が VLAN インターフェイスをフル稼働させるまで使用しないようにします。また、ブラック ホール ルーティングなどの別の問題が発生しないようにします。

レイヤ3インターフェイス カウンタの概要



(注)

Supervisor Engine 6-E は、レイヤ 2 インターフェイス カウンタをサポートしてI ません。Supervisor Engine 6-E は、レイヤ 3 (SVI) インターフェイス カウンタをサポートしています。

Supervisor Engine 6-E では、IPv4 パケットおよび IPv6 パケットはハードウェア転送エンジンによりルーティングされます。このエンジンは、最大 4095 個のインターフェイスについてルーティングされたパケットのカウントの統計情報をサポートします。この統計は、次のカウンタが含まれます。

- 入力ユニキャスト
- 入力マルチキャスト
- 出力ユニキャスト
- 出力マルチキャスト

各種のカウンタについて、パケット数および送受信される合計バイト数の両方がカウントされます。

サポートされるカウンタの合計数が、サポートされるレイヤ 3 インターフェイスの合計数より少ないため、レイヤ 3 インターフェイスのカウンタがなくなる場合もあります。そのため、ユーザがレイヤ 3 インターフェイスにカウンタを割り当てると、あるレイヤ 3 インターフェイスのデフォルト設定にはカウンタがなくなります。



<u>~</u>

レイヤ 3 インターフェイス カウンタをイネーブルにするには、インターフェイス モードで counter コマンドを発行する必要があります。レイヤ 3 インターフェイス カウンタを設定する手順については、「レイヤ 3 インターフェイス カウンタの設定」(p.27-12) を参照してください。

これらのハードウェア カウンタは、show interface コマンドの出力に表示されます。次に例を示します。

```
Switch# show interface vlan 1
Vlan1 is up, line protocol is up
 Hardware is Ethernet SVI, address is 0005.9a38.6cff (bia 0005.9a38.6cff)
  Internet address is 10.0.0.1/8
 MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
 Encapsulation ARPA, loopback not set
 Keepalive not supported
  ARP type: ARPA, ARP Timeout 04:00:00
 Last input never, output never, output hang never
 Last clearing of "show interface" counters never
 Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
 Output queue: 0/40 (size/max)
 5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
 L3 in Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes
                                                                    <====
  L3 out Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes
     0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicasts)
    0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     1 packets output, 46 bytes, 0 underruns
     0 output errors, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

設定時の注意事項

Catalyst 4500 シリーズ スイッチは、AppleTalk ルーティングおよび IPX ルーティングをサポートします。AppleTalk ルーティングおよび IPX ルーティングについては、次の URL の『Cisco IOS AppleTalk and Novell IPX Configuration Guide』の「Configuring AppleTalk」および「Configuring Novell IPX」を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/atipx_c/index.htm



(注)

Supervisor Engine 6-E は、AppleTalk および IPX ルーティングをサポートしていません。

Catalyst 4500 シリーズ スイッチは、レイヤ 3 ファスト イーサネット、ギガビット イーサネット、10 ギガビット イーサネット インターフェイスでサブインターフェイスまたは encapsulation キーワードをサポートしていません。



Cisco IOS ソフトウェアが稼働するすべてのレイヤ 3 インターフェイスと同様に、Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) に割り当てられる IP アドレスおよびネットワークは、スイッチ上の他のレイヤ 3 インターフェイスに割り当てられるものと重複できません。

論理レイヤ3 VLAN インターフェイスの設定



(注)

論理レイヤ 3 VLAN インターフェイスを設定する前に、スイッチ上に VLAN を作成および設定し、レイヤ 2 インターフェイスに VLAN メンバシップを割り当てる必要があります。 また、IP ルーティングがディセーブルの場合は IP ルーティングをイネーブルにし、IP ルーティング プロトコルを指定する必要があります。

論理レイヤ3 VLAN インターフェイスを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# vlan vlan_ID	VLAN を作成します。
ステップ 2	Switch(config)# interface vlan vlan_ID	設定するインターフェイスを選択します。
ステップ 3	Switch(config-if)# ip address ip_address subnet_mask	IP アドレスおよび IP サブネットを設定します。
ステップ 4	Switch(config-if)# no shutdown	インターフェイスをイネーブルにします。
ステップ 5	Switch(config-if)# end	コンフィギュレーション モードを終了します。
ステップ 6	Switch# copy running-config startup-config	設定変更内容を NVRAM に保存します。
ステップ 7	Switch# show interfaces [type slot/interface] Switch# show ip interfaces [type slot/interface] Switch# show running-config interfaces [type slot/interface] Switch# show running-config interfaces vlan vlan_ID	設定を確認します。

次に、論理レイヤ 3 VLAN インターフェイス vlan 2 を設定し、IP アドレスを割り当てる例を示します。

Switch> enable
Switch# config term
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# vlan 2
Switch(config)# interface vlan 2
Switch(config-if)# ip address 10.1.1.1 255.255.255.248
Switch(config-if)# no shutdown
Switch(config-if)# end

次に、show interfaces コマンドを使用して、レイヤ 3 VLAN インターフェイス vlan 2 のインターフェイス IP アドレスの設定およびステータスを表示する例を示します。

Switch# show interfaces vlan 2 Vlan2 is up, line protocol is down Hardware is Ethernet SVI, address is 00D.588F.B604 (bia 00D.588F.B604) Internet address is 172.20.52.106/29 MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation ARPA, loopback not set ARP type: ARPA, ARP Timeout 04:00:00 Last input never, output never, output hang never Last clearing of "show interface" counters never Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0 Queueing strategy: fifo Output queue: 0/40 (size/max) 5 minute input rate 0 bits/sec, 0 packets/sec 5 minute output rate 0 bits/sec, 0 packets/sec 0 packets input, 0 bytes, 0 no buffer Received 0 broadcasts, 0 runts, 0 giants, 0 throttles 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored 0 packets output, 0 bytes, 0 underruns 0 output errors, 0 interface resets 0 output buffer failures, 0 output buffers swapped out Switch#

次に、show running-config コマンドを使用して、レイヤ 3 VLAN インターフェイス vlan 2 のインターフェイス IP アドレスの設定を表示する例を示します。

```
Switch# show running-config
Building configuration...

Current configuration : !
interface Vlan2
  ip address 10.1.1.1 255.255.255.248
!
ip classless
no ip http server
!
!
line con 0
line aux 0
line vty 0 4
!
end
```

レイヤ 3 インターフェイスとしての VLAN の設定

ここでは、次の内容について説明します。

- SVI 自動ステート除外の設定 (p.27-9)
- IP MTU サイズの設定 (p.27-10)
- レイヤ3インターフェイスカウンタの設定(p.27-12)

SVI 自動ステート除外の設定



(注)

Supervisor Engine 6-E は、SVI 自動ステート除外機能をサポートしていません。



(注)

SVI 自動ステート除外機能は、デフォルトでイネーブルであり、STP ステートと同期しています。

SVI 自動ステート除外機能は、次のポート設定変更が発生した場合に、スイッチのレイヤ 3 インターフェイスのシャットダウン (または起動)を行います。

- VLAN 上の最後のポートがダウンし、その VLAN 上のレイヤ 3 インターフェイスがシャットダウンする場合 (SVI 自動ステート)。
- VLAN 上の最初のポートが立ち上がった状態に戻り、それまでシャットダウンしていた VLAN 上のレイヤ 3 インターフェイスが起ち上がる場合。

SVI 自動ステート除外は、SVI のステータス定義(アップまたはダウン)に含まれるアクセス ポートまたはトランクを、それが同じ VLAN に属する場合でも除外します。さらに、除外されたアクセス ポートまたはトランクがアップ状態であり、VLAN 内の別のポートがダウン状態である場合でも、SVI ステートはダウンに変更されます。

SVI ステートを「アップ」にするには、少なくとも VLAN 内の 1 つのポートがアップ状態であり、除外されていない必要があります。これは、SVI ステータスの決定時にモニタリング ポートのステータスを除外するために役立ちます。

SVI自動ステート除外を適用するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開 始します。
ステップ 2	Switch(config)# interface interface-id	インターフェイス コンフィギュレーション モー ドを開始します。
ステップ 3	Switch(config-if)# switchport autostate exclude	SVI のステータス定義 (アップまたはダウン) に 含まれるアクセス ポートまたはトランクを除外 します。
ステップ 4	Switch(config)# end	コンフィギュレーション モードを終了します。
ステップ 5	Switch# show run int g3/4	実行コンフィギュレーションを表示します。
ステップ 6	Switch# show int g3/4 switchport	設定を確認します。

次に、SVI 自動ステート除外をインターフェイス g3/1 に適用する例を示します。

```
Switch# conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config) # interface g3/1
Switch(config-if) # switchport autostate exclude
Switch(config-if)# end
Switch# show run int q3/4
Building configuration...
Current configuration: 162 bytes
interface GigabitEthernet3/4
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 2,3
switchport autostate exclude
                                                               <=====
switchport mode trunk
Switch# show int g3/4 switchport
Name: Gi3/4
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On Access Mode VLAN: 1 (default) Trunking Native Mode VLAN: 1
(default) Administrative Native VLAN tagging: enabled Voice VLAN: none Administrative
private-vlan host-association: none Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none Administrative private-vlan trunk
Native VLAN tagging: enabled Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none Administrative private-vlan trunk
associations: none Administrative private-vlan trunk mappings: none Operational
private-vlan: none Trunking VLANs Enabled: 2,3 Pruning VLANs Enabled: 2-1001 Capture
Mode Disabled Capture VLANs Allowed: ALL
Autostate mode exclude
                                                           <=====
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
```

IP MTU サイズの設定

Appliance trust: none

Switch#

インターフェイスから送信された IPv4 パケットまたは IPv6 パケットの Maximum Transmission Unit (MTU: 最大伝送ユニット) サイズをプロトコルごとに設定できます。

MTU の制限事項については、MTU の概要 (p.6-23) を参照してください。



インターフェイスにプロトコルに限定されない MTU 値を設定するには、mtu インターフェイス コンフィギュレーション コマンドを使用します。MTU 値の (mtu インターフェイス コンフィギュレーション コマンドを使用した)変更は、IP MTU 値に影響を与えます。現在の IP MTU 値が MTU 値と一致する場合に MTU 値を変更すると、IP MTU 値は新しい MTU と一致するよう自動的に変更されます。ただし、逆の場合は同様ではありません。IP MTU 値を変更しても mtu コマンドの値には影響がありません。

MTU サイズの設定については、MTU サイズの設定 (p.6-25) を参照してください。

インターフェイスから送信された IPv4 パケットまたは IPv6 パケットの Maximum Transmission Unit (MTU; 最大伝送ユニット) サイズをプロトコルごとに設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	Switch(config)# interface interface-id	インターフェイス コンフィギュレーション モー ドを開始します。
ステップ 3	Switch(config-if)# [no] ip mtu <mtu_size> または Switch(config-if)# [no] ipv6 mtu <mtu_size></mtu_size></mtu_size>	MPv4 MTU サイズを設定します。 MPv6 MTU サイズを設定します。 このコマンドの no 形式を使用すると、デフォルトの MTU サイズ(1500 バイト)に戻ります。
ステップ 4	Switch(config-if)# exit	インターフェイス コンフィギュレーション モード を終了します。
ステップ 5	Switch(config)# end	コンフィギュレーション モードを終了します。
ステップ 6	Switch# show run interface interface-id	実行コンフィギュレーションを表示します。

次に、インターフェイスで IPv4 MTU を設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface vlan 1
Switch(config-if)# ip mtu 68
Switch(config-if)# exit
Switch(config)# end
Switch# show ip interface vlan 1
Vlan1 is up, line protocol is up
 Internet address is 10.10.10.1/24
  Broadcast address is 255.255.255.255
 Address determined by setup command
  MTU is 68 bytes
 Helper address is not set
.....(continued)
The following example shows how to configure ipv6 mtu on an interface
Switch# configure terminal
Enter configuration commands, one per line. End with {\tt CNTL/Z.}
Switch(config) # interface vlan 1
Switch(config-if) # ipv6 mtu 1280
Switch(config) # end
Switch# show ipv6 nterface vlan 1
This example shows how to verify the configuration
Vlan1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::214:6AFF:FEBC:DEEA
  Global unicast address(es):
   1001::1, subnet is 1001::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF00:1
   FF02::1:FFBC:DEEA
 MTU is 1280 bytes
.....(continued)
```



CLI を使用して IPv6 をインターフェイスでイネーブルにする場合、次のメッセージが表示される 場合があります。

% Hardware MTU table exhausted このようなシナリオでは、ハードウェアでプログラムされてい る IPv6 MTU 値が IPv6 インターフェイス MTU 値と異なっています。この状況は、ハードウェア MTU テーブルにさらに値を保存する容量がない場合に発生します。使用していない MTU 値の設定 を解除することでテーブル内のスペースを空けてから、インターフェイスで IPv6 をディセーブル にして再度イネーブルにするか、MTU 設定を再度適用します。

レイヤ3インターフェイス カウンタの設定



Supervisor Engine 6-E は、インターフェイス カウンタをサポートして*いません*。



ラインカードを*削除*すると、このラインカードのポート上でイネーブルにされているレイヤ 3 カウ ンタは未設定となります。そのため、ラインカードを再度挿入するときにレイヤ 3 カウンタを再度 イネーブルにするには、そのラインカードのレイヤ 3 ポートに対してカウンタ CLI を再設定する必 要があります。

レイヤ3インターフェイス カウンタを設定する(カウンタをレイヤ3インターフェイスに割り当て る)には、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2		インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	Switch(config-if)# counter	カウンタををイネーブルにします。
ステップ 4	Switch(config)# end	コンフィギュレーション モードを終了します。
ステップ 5	Switch# show run interface interface-id	実行コンフィギュレーションを表示します。

次に、インターフェイス VLAN 1上でカウンタをイネーブルにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface vlan 1
Switch(config-if) # counter
Switch(config-if)# end
00:17:15: %SYS-5-CONFIG_I: Configured from console by console
Switch# show run interface vlan 1
Building configuration...
Current configuration: 63 bytes
interface Vlan1
ip address 10.0.0.1 255.0.0.0
 counter
end
```



<u>一</u> (注)

カウンタを削除するには、counter コマンドの no 形式を使用します。

最大数のカウンタがすでに割り当てられている場合は、counter コマンドは失敗し、エラー メッセージが表示されます。

Switch# config terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fa3/2
Switch(config-if)# no switchport
Switch(config-if)# counter
Counter resource exhausted
Switch(config-if)# end
Switch#

00:24:18: %SYS-5-CONFIG_I: Configured from console by console

この場合、別のインターフェイスのカウンタを解放して新しいインターフェイスが使用できるようにする必要があります。

物理レイヤ3インターフェイスの設定



(注)

物理レイヤ 3 インターフェイスを設定する前に、IP ルーティングがディセーブルの場合は IP ルーティングをイネーブルにし、IP ルーティング プロトコルを指定する必要があります。

物理レイヤ3インターフェイスを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)#ip routing	IP ルーティングをイネーブルにします (IP ルーティングがディセーブルになっている場合のみ)。
ステップ 2	<pre>Switch(config)# interface {fastethernet gigabitethernet tengigabitethernet} slot/port} {port-channel port_channel_number}</pre>	設定するインターフェイスを選択します。
ステップ 3	Switch(config-if)#no switchport	このポートを物理レイヤ 2 ポートから物理レイヤ 3 ポートに変換します。
ステップ 4	<pre>Switch(config-if)# ip address ip_address subnet_mask</pre>	IP アドレスおよび IP サブネットを設定します。
ステップ 5	Switch(config-if)# no shutdown	インターフェイスをイネーブルにします。
ステップ 6	Switch(config-if)# end	コンフィギュレーション モードを終了します。
ステップ 7	Switch# copy running-config startup-config	設定変更内容を NVRAM に保存します。
ステップ 8	Switch# show interfaces [type slot/interface] Switch# show ip interfaces [type slot/interface] Switch# show running-config interfaces [type slot/interface]	設定を確認します。

次に、インターフェイス FastEthernet 2/1 に IP アドレスを設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# interface fastethernet 2/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.1.1.1 255.255.255.248
Switch(config-if)# no shutdown
Switch(config-if)# end
Switch#
```

次に、**show running-config** コマンドを使用して、インターフェイス FastEthernet 2/1 のインターフェイス IP アドレスの設定を表示する例を示します。

```
Switch# show running-config
Building configuration...
!
interface FastEthernet2/1
  no switchport
  ip address 10.1.1.1 255.255.255.248
!
...
ip classless
  no ip http server
!
!
line con 0
line aux 0
line vty 0 4
!
end
```

EIGRP スタブ ルーティングの設定

ここでは、次の内容について説明します。

- 概要 (p.27-15)
- EIGRP スタブ ルーティングの設定方法 (p.27-16)
- EIGRP のモニタリングおよびメンテナンス (p.27-21)
- EIGRP の設定例 (p.27-21)

概要

EIGRP スタブ ルーティング機能は、すべてのイメージで使用することができ、エンド ユーザの近くにルーテッド トラフィックを移動することでリソースの利用率を低減させます。

IP ベース イメージには EIGRP スタブ ルーティングのみが含まれています。IP サービス イメージには、完全な EIGRP ルーティングが含まれています。

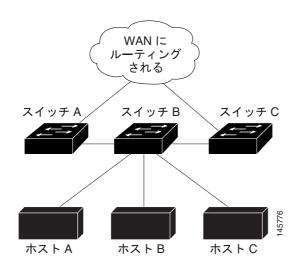
EIGRP スタブ ルーティングを使用するネットワークでは、IP トラフィックがユーザに到達するには、ルート EIGRP スタブ ルーティングを設定しているスイッチを通過する必要があります。スイッチは、ユーザ インターフェイスとして設定されているインターフェイスまたは他のデバイスに接続されているインターフェイスにルーテッド トラフィックを送信します。

EIGRP スタブ ルーティングを使用する場合、EIGRP を使用するように、ディストリビューション ルータおよびリモート ルータを設定し、さらにスイッチのみをスタブとして設定する必要があります。指定したルートのみがスイッチから伝播されます。スイッチは、サマリー、接続ルート、およびルーティング アップデートに対するすべてのクエリーに応答します。

スタブであることを通知するパケットを受信するネイバーは、スタブ ルータに対してルートのクエリーを実行せず、スタブ ピアを有するルータはそのピアに対するクエリーを実行しません。スタブルータは、ディストリビューション ルータに依存してすべてのピアに適切なアップデートを送信します。

図 27-3 では、スイッチ B が EIGRP スタブ ルータとして設定されています。スイッチ A および C は残りの WAN に接続されています。スイッチ B は、接続ルート、スタティック ルート、再配布ルート、集約ルートをスイッチ A および C からホスト A、B、および C にアドバタイズします。スイッチ B はスイッチ A から学習したルートをアドバタイズしません(逆の場合も同様です)。

図 27-3 EIGRP スタブ ルータの構成



EIGRP スタブ ルーティングの詳細については、『Cisco IOS IP Configuration Guide, Volume 2 of 3: Routing Protocols』Release 12.2 の「Configuring EIGRP Stub Routing」を参照してください。

EIGRP スタブ ルーティングの設定方法

EIGRP スタブ ルーティング機能は、ネットワークの安定性を高め、リソース利用率を抑え、スタブ ルータ構成を簡素化します。

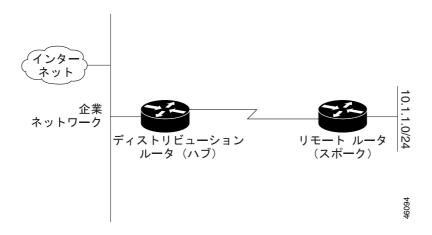
スタブルーティングは、一般的に、ハブアンドスポーク型のネットワークトポロジで使用されます。ハブアンドスポーク型ネットワークでは、1 つまたは複数のエンドネットワーク(スタブ)が、1 つまたは複数のディストリビューションルータ(ハブ)に接続したリモートルータ(スポーク)に接続しています。リモートルータは1 つまたは複数のディストリビューションルータにのみ隣接します。IP トラフィックがリモートルータに到達する唯一のルートは、ディストリビューションルータが直接 WAN に接続している WANトポロジで使用されています。ディストリビューションルータが直接 WANに接続している WANトポロジで使用されています。ディストリビューションルータは多くのリモートルータに接続できます。多くの場合、ディストリビューションルータは100以上のリモートルータに接続されます。ハブアンドスポーク型のトポロジでは、リモートルータはすべての非ローカルトラフィックをディストリビューションルータに転送する必要があるため、リモートルータが完全なルーティングテーブルを保持する必要はなくなります。一般に、ディストリビューションルータはデフォルトルート以外の情報をリモートルータに送信する必要はありません。

EIGRP スタブ ルーティング機能を使用する場合、EIGRP を使用するように、ディストリビューション ルータおよびリモート ルータを設定し、さらにリモート ルータのみをスタブとして設定する必要があります。指定したルートのみがリモート (スタブ)ルータから伝播されます。スタブ ルータはサマリー、接続ルート、再配布スタティック ルート、外部ルート、および内部ルートのすべてのクエリーを「アクセス不可」のメッセージで応答します。スタブとして設定されたルータは、すべての隣接ルータに特別なピア情報パケットを送信し、自身がスタブ ルータであることを報告します。

スタブであることを通知するパケットを受信するネイバーは、スタブ ルータに対してルートのクエリーを実行せず、スタブ ピアを有するルータはそのピアに対するクエリーを実行しません。スタブルータは、ディストリビューション ルータに依存してすべてのピアに適切なアップデートを送信します。

図 27-4 に、単純なハブ アンド スポーク構成を示します。

図 27-4 単純なハブ アンド スポーク型ネットワーク



スタブルーティング機能自体は、ルートがリモート ルータにアドバタイズされるのを防ぐことはありません。図 27-4 の例では、リモート ルータはディストリビューション ルータのみを通じて企業ネットワークおよびインターネットにアクセスできます。この例では、リモート ルータが完全なルート テーブルを保有しても機能面での意味はありません。企業ネットワークとインターネットへのパスは常にディストリビューション ルータを経由するためです。ルート テーブルが大きくなると、リモート ルータに必要なメモリ量が減るだけです。帯域幅とメモリは、ディストリビューション ルータのルートを集約およびフィルタリングすることによって節約できます。リモート ルータは、宛先に関わりなく、ディストリビューション ルータにすべての非ローカル トラフィックを送信する必要があるため、他のネットワークから学習されたルートを受け取る必要がありません。真のスタブ ネットワークが望ましい場合、ディストリビューション ルータはリモート ルータにデフォルト ルートのみを送信するように設定する必要があります。EIGRP スタブ ルーティング機能では、自動的にディストリビューション ルータでの要約をイネーブルにしません。ほとんどの場合、ネットワーク管理者がディストリビューション ルータでの集約を設定する必要があります。



ディストリビューション ルータがリモート ルータにデフォルト ルートのみを送信するように設定する場合、リモート ルータで ip classless コマンドを使用する必要があります。デフォルトでは、EIGRP スタブ ルーティング機能をサポートするすべての Cisco IOS イメージで ip classless コマンドがイネーブルになっています。

スタブ機能を使用しない場合、ディストリビューション ルータからリモート ルータに送信される ルートがフィルタリングまたは集約されたあとでも、問題が生じることがあります。ルートが企業 ネットワーク内のどこかで失われた場合、EIGRP はディストリビューション ルータにクエリーを 送信できます。そのあと、ディストリビューション ルータはルートが集約されている場合でもリモート ルータにクエリーを送信します。WAN リンクを使用したディストリビューション ルータと リモート ルータ間の通信に問題がある場合、EIGRP Stuck In Active (SIA) 状態が発生し、ネットワークのどこかで不安定になる可能性があります。EIGRP スタブ ルーティング機能を使用することにより、ネットワーク管理者はリモート ルータへクエリーが送信されないようにできます。

デュアルホーム リモート トポロジ

リモート ルータを単一のディストリビューション ルータに接続する簡単なハブ アンド スポーク型 ネットワーク以外に、リモート ルータを複数のディストリビューション ルータにデュアルホーム 接続できます。この構成では冗長性が増し、一意性の問題が生じますが、スタブ機能がこれらの問題の対処に役立ちます。

デュアルホーム リモート ルータは、複数のディストリビューション ルータ (ハブ) を使用します。 ただし、スタブ ルーティングの原理はハブ アンド スポーク型トポロジの場合と同じです。図 27-5 にリモート ルータを 1 つ使用した一般的なデュアルホーム リモート トポロジを示していますが、ディストリビューション ルータ 1 とディストリビューション ルータ 2 の同じインターフェイスに 100 以上のルータを接続できます。 リモート ルータは最適なルートを使用して宛先に到達します。 ディストリビューション ルータ 1 に障害が発生した場合、リモート ルータはディストリビューション ルータ 2 を使用して企業ネットワークに到達できます。

図 27-5 単純なデュアルホーム リモート トポロジ

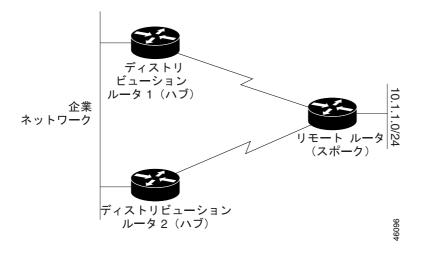


図 27-5 に、リモート ルータ 1 つとディストリビューション ルータ 2 つから構成される簡単なデュアルホーム リモートを示します。いずれのディストリビューション ルータも企業ネットワークとスタブ ネットワーク 10.1.1.0/24 へのルートを維持します。

デュアルホーム ルーティングによって、EIGRP ネットワークが不安定になる場合があります。図 27-6 では、ディストリビューション ルータ 1 はネットワーク 10.3.1.0/24 に直接接続しています。ディストリビューション ルータ 1 に集約またはフィルタリングが適用された場合、このルータは直接接続したすべての EIGRP ネイバー(ディストリビューション ルータ 2 およびリモート ルータ)にネットワーク 10.3.1.0/24 をアドバタイズします。

図 27-6 ディストリビューション ルータ 1 を 2 つのネットワークに接続したデュアルホーム リモートトポロジ

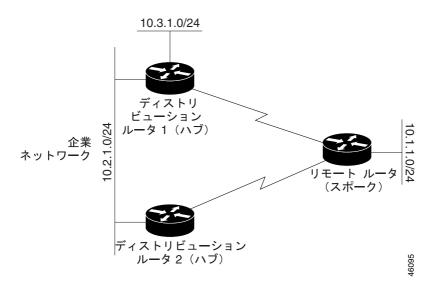
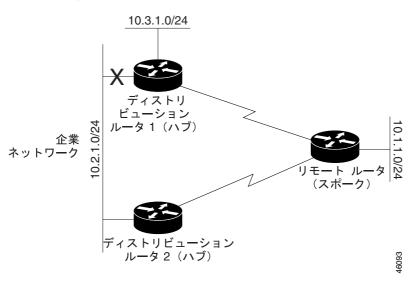


図 27-6 に、ディストリビューション ルータ 1 をネットワーク 10.3.1.0/24 とネットワーク 10.2.1.0/24 の両方に接続した単純なデュアルホーム リモート ルータを示します。

ディストリビューション ルータ 1 とディストリビューション ルータ 2 間の 10.2.1.0/24 リンクに障害が発生した場合、ディストリビューション ルータ 2 からネットワーク 10.3.1.0/24 までの最低コストパスはリモート ルータを経由します(図 27-7 を参照)。それまで企業ネットワーク 10.2.1.0/24 を通過していたトラフィックが今度は帯域幅の相当低い接続を介して送信されるため、このルートは望ましくありません。低帯域幅 WAN 接続の利用率が高くなりすぎると、企業ネットワーク全体に影響するような多くの問題の原因になります。リモート ルータを通過する低帯域幅ルートの利用によって、WAN EIGRP ディストリビューション ルータがドロップする場合があります。ディストリビューションおよびコア ルータで EIGRP SIA エラーが発生する可能性があります。

図 27-7 ディストリピューション ルータへのルートに障害が発生したデュアルホーム リモート トポロジ



ディストリビューション ルータ 2 からのトラフィックがネットワーク 10.3.1.0/24 に到達するため に、リモート ルータを通過するのは望ましくありません。リンクが負荷を処理できるサイズであれば、バックアップ ルートの 1 つを使用することもできます。ただし、このタイプのほとんどのネットワークは、リモート ルータをリンク速度が比較的遅いリモート オフィスに配置しています。この問題は、ディストリビューション ルータとリモート ルータで適切な集約が設定されていれば防ぐことができます。

通常、ディストリビューション ルータからのトラフィックが中継パスとしてリモート ルータを使用するのは不適切です。ディストリビューション ルータからリモート ルータへの一般的な接続は、ネットワーク コアにおける接続よりも帯域幅が相当低くなります。中継パスとして接続帯域幅に限りがあるリモート ルータを使用した場合、一般にリモート ルータに過度の輻輳が生じます。EIGRP スタブ ルーティング機能は、リモート ルータがディストリビューション ルータにコア ルートをアドバタイズしないようにしてこの問題を防ぎます。ディストリビューション ルータ 1 を通じてリモート ルータが学習したルートは、ディストリビューション ルータ 2 にアドバタイズされません。リモート ルータはディストリビューション ルータ 2 にコア ルートをアドバタイズしないため、ディストリビューション ルータはネットワーク コアに向けられたトラフィックにはリモート ルータを中継点として使用しません。

EIGRP スタブ ルーティング機能は、ネットワークの安定性を高めるのに役立ちます。ネットワークが不安定になった場合、この機能は EIGRP クエリーが帯域幅に限りのあるリンクを使用して非中継ルータに送信されるのを防ぎます。その代わりに、スタブ ルータが接続されたディストリビューション ルータが、スタブ ルータに代わってクエリーに応答します。この機能は輻輳のある、または問題のある WAN リンクによってネットワークが不安定になる可能性を大幅に減らします。

また EIGRP スタブ ルーティング機能は、ハブ アンド スポーク型ネットワークの設定とメンテナン スを簡易化します。 デュアルホーム リモート構成でスタブ ルーティングがイネーブルになっている場合、 リモート ルータにフィルタリングを設定して、 リモート ルータがハブ ルータへの中継パスのように見えないようにする必要はありません。



EIGRP スタブ ルーティングはスタブ ルータでのみ使用します。スタブ ルータは、コア中継トラフィックが通過すべきでないネットワーク コアまたはディストリビューション レイヤに接続されたルータとして定義されます。スタブ ルータは、ディストリビューション ルータ以外の EIGRP ネイバーを持つことはできません。この制約事項を無視すると、好ましくない動作が生じます。



(注)

ATM、イーサネット、フレーム リレー、ISDN PRI、X.25 などのマルチアクセス インターフェイス は、そのインターフェイス上のすべてのルータ(ハブ以外)がスタブ ルータとして設定されている場合にのみ、EIGRP スタブ ルーティング機能がサポートされます。

EIGRP スタブ ルーティングの設定作業リスト

ここでは、EIGRP スタブ ルーティングを設定するために実行する作業について説明します。最初に説明する作業は必須で、最後の作業はオプションです。

- EIGRP スタブ ルーティングの設定(必須)
- EIGRP スタブ ルーティングの確認 (任意)

EIGRP スタブ ルーティングの設定

EIGRP スタブ ルーティングをリモート ルータまたはスポーク ルータに設定するには、ルータ コンフィギュレーション モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	router(config)# router eigrp 1	EIGRP プロセスを実行するリモート ルータまたは
		ディストリビューション ルータを設定します。
ステップ 2	<pre>router(config-router)# network network-number</pre>	EIGRP ディストリビューション ルータのネット
		ワーク アドレスを指定します。
ステップ 3	router(config-router)# eigrp stub [receive-only connected static summary]	リモート ルータを EIGRP スタブ ルータとして設定します。

EIGRP スタブ ルーティングの確認

リモート ルータが EIGRP でスタブ ルータとして設定されていることを確認するには、特権 EXEC モードでディストリビューション ルータから show ip eigrp neighbor detail コマンドを使用します。 出力の最後の行は、リモート ルータまたはスポーク ルータのスタブ ステータスを示します。次の 例は、show ip eigrp neighbor detail コマンドの出力を示します。

```
router# show ip eigrp neighbor detail

IP-EIGRP neighbors for process 1

H Address Interface Hold Uptime SRTT RTO Q Seq Type (sec) (ms) Cnt Num

0 10.1.1.2 Se3/1 11 00:00:59 1 4500 0 7

Version 12.1/1.2, Retrans:2, Retries: 0

Stub Peer Advertising (CONNECTED SUMMARY) Routes
```

EIGRP のモニタリングおよびメンテナンス

ネイバーテーブルからネイバーを削除するには、EXEC モードで次のコマンドを使用します。

コマンド	目的
Router# clear ip eigrp neighbors [ip-address interface]	ネイバー テーブルからネイバーを削除します。

各種のルーティング統計を表示するには、EXEC モードで次のコマンドを使用します。

コマンド	目的
Router# show ip eigrp interfaces [interface] [as-number]	EIGRP に設定されているインターフェイスに関する 情報を表示します。
Router# show ip eigrp neighbors [type number static]	EIGRP によって検出されたネイバーを表示します。
Router# show ip eigrp topology [autonomous-system-number [[ip-address] mask]]	指定されたプロセスの EIGRP トポロジ テーブルを 表示します。
Router# show ip eigrp traffic [autonomous-system-number]	すべてまたは指定された EIGRP プロセスの送受信パケット数を表示します。

EIGRP の設定例

ここでは、次の例について説明します。

- 経路集約の例
- ルート認証の例
- スタブルーティングの例

経路集約の例

次の例では、インターフェイス上に経路集約を設定し、また、自動サマリー機能を設定します。この設定によって、EIGRP は、イーサネット インターフェイス 0 からのネットワーク 10.0.0.0 だけを集約するようになります。さらに、この例では自動集約をディセーブルにします。

```
interface Ethernet 0
  ip summary-address eigrp 1 10.0.0.0 255.0.0.0
!
router eigrp 1
  network 172.16.0.0
  no auto-summary
```



<u>一</u>"

インターフェイスからのデフォルト ルート (0.0.0.0) を生成するのに、ip summary-address eigrp サマライズ コマンドは使用しないでください。このコマンドを使用すると、管理ディスタンスが 5 で、ヌル 0 インターフェイスへの EIGRP 集約デフォルト ルートが作成されます。このデフォルトルートの管理ディスタンスの値が小さいと、ルーティング テーブル内の他のネイバーから学習されたデフォルト ルートにこのルートが置き換えられてしまうことがあります。ネイバーによって学習されたデフォルト ルートが集約デフォルト ルートによって置き換えられた場合、または集約ルートが存在する唯一のデフォルト ルートである場合、そのデフォルト ルート宛てのすべてのトラフィックはルータを離れず、その代わりに、このトラフィックがヌル 0 インターフェイスに送信され、そこでドロップされます。

所定のインターフェイスからのデフォルト ルートだけを送信するようにするには、distribute-list コマンドを使用することを推奨します。このコマンドを設定して、インターフェイスから送信されるデフォルト (0.0.0.0) 以外のすべての発信ルート アドバタイズメントをフィルタリングできます。

ルート認証の例

次の例では、自律システム 1 で EIGRP パケットの MD5 認証をイネーブルにします。

ルータ A

```
interface ethernet 1
  ip authentication mode eigrp 1 md5
  ip authentication key-chain eigrp 1 holly
key chain holly
  key 1
   key-string 0987654321
   accept-lifetime 04:00:00 Dec 4 1996 infinite
   send-lifetime 04:00:00 Dec 4 1996 04:48:00 Dec 4 1996
exit
  key 2
  key-string 1234567890
  accept-lifetime 04:00:00 Dec 4 1996 infinite
  send-lifetime 04:45:00 Dec 4 1996 infinite
```

ルータ B

```
interface ethernet 1
  ip authentication mode eigrp 1 md5
  ip authentication key-chain eigrp 1 mikel
key chain mikel
  key 1
   key-string 0987654321
   accept-lifetime 04:00:00 Dec 4 1996 infinite
   send-lifetime 04:00:00 Dec 4 1996 infinite
  exit
  key 2
   key-string 1234567890
   accept-lifetime 04:00:00 Dec 4 1996 infinite
  send-lifetime 04:45:00 Dec 4 1996 infinite
```

ルータ A は 1 のキーを使用した EIGRP パケットの MD5 ダイジェストを受け入れ、確認を試みます。また、2 のキーを使用したパケットも受け入れ、他のすべての MD5 パケットがドロップされます。ルータ A は、キー 2 を使用したすべての EIGRP パケットを送信します。

ルータ B はキー 1 またはキー 2 を受け入れ、キー 1 を送信します。このシナリオでは、MD5 が認証します。

スタブ ルーティングの例

eigrp stub コマンドでスタブとして設定されたルータは、デフォルトで接続および集約ルーティング情報をすべての隣接ルータと共有します。この動作を変更する場合、eigrp stub コマンドで 4 つのオプション キーワードを使用できます。

- · receive-only
- connected
- static
- summary

ここでは、eigrp stub コマンドのすべての形式の設定例を示します。eigrp stub コマンドはいくつかのオプションを指定して変更できます。これらのオプションは、receive-only キーワードを除いて、どのような組み合わせも可能です。receive-only キーワードは、ルータがその EIGRP 自律システム内の他のルータとルートを共有することを制限します。また receive-only キーワードを使用すると、すべてのタイプのルートの送信が停止するため、他のオプションと併用できません。他の3つのオプションキーワード(connected、static、および summary)は、どのように組み合わせても使用で

きますが、receive-only キーワードと一緒には使用できません。これらの3つのキーワードのいずれかを eigrp stub コマンドで個別に使用した場合、接続および集約ルートは自動的に送信されません。

connected キーワードを指定すると、EIGRP スタブ ルーティング機能によって接続ルートが送信されます。接続ルートがネットワーク文で扱われない場合、EIGRP プロセスで redistribute connected コマンドを使用して接続ルートを再配布する必要が生じる場合があります。このオプションは、デフォルトでイネーブルに設定されています。

static キーワードを指定すると、EIGRP スタブ ルーティング機能によってスタティック ルートが送信されます。このオプションを指定しない場合、EIGRP は通常は自動的に再配布される内部スタティック ルートを含むすべてのスタティック ルートを送信しません。ただし、redistribute static コマンドを使用してスタティック ルートを再配布する必要があります。

summary キーワードを使用すると、EIGRP スタブ ルーティング機能によって集約ルートが送信されます。集約ルートは、summary address コマンドを使用して手動で作成することもでき、auto-summary コマンドをイネーブルにしてメジャー ネットワークの境界ルータで自動的に作成することもできます。このオプションは、デフォルトでイネーブルに設定されています。

次に、接続および集約ルートをアドバタイズするスタブとしてルータを設定するために eigrp stub コマンドが使用する例を示します。

router eigrp 1
network 10.0.0.0
eigrp stub

次に、接続およびスタティック ルート (集約ルートの送信は禁止)をアドバタイズするスタブとしてルータを設定するために eigrp stub connected static コマンドを使用する例を示します。

router eigrp 1
network 10.0.0.0
eigrp stub connected static

次に、ルータをスタブとして設定するのに eigrp stub receive-only コマンドを使用する例を示します。この設定では、接続、集約、またはスタティック ルートは送信されません。

router eigrp 1
network 10.0.0.0 eigrp
stub receive-only

■ EIGRP スタブ ルーティングの設定



CHAPTER

28

CEF の設定

この章では、Catalyst 4000 ファミリ スイッチ上の Cisco Express Forwarding (CEF) について説明します。この機能の注意事項、設定手順、および設定例についても紹介します。

この章の主な内容は、次のとおりです。

- CEFの概要 (p.28-2)
- Catalyst 4500 シリーズ スイッチでの CEF の実装 (p.28-4)
- CEF 設定の制限事項 (p.28-7)
- CEFの設定 (p.28-7)
- CEF のモニタリングおよびメンテナンス (p.28-9)



この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/cr/index.htm

CEF の概要

ここでは、CEFの動作を構成する2つの主なコンポーネントについて説明します。

- CEF の利点 (p.28-2)
- FIB (p.28-2)
- 隣接関係テーブル (p.28-2)

CEF の利点

CEF は、先進的なレイヤ 3 IP スイッチング テクノロジーです。ダイナミック トラフィック パターンを特長とする大規模ネットワーク、または Web ベースのアプリケーションおよび対話型セッションを多用するネットワークで、パフォーマンスおよびスケーラビリティを最適化します。

CEF には次の利点があります。

- ルーティング テーブル情報が変更されると、キャッシュ全体がフラッシュされる場合がありますが、CEF はマルチレイヤ スイッチのキャッシュ方式のパフォーマンスを向上させます。
- レイヤ3ルーティング情報に基づいて、複数のリンクにパケットを分散させる形式でロードバランシングを行います。ネットワーク装置が宛先に対して複数のパスを検出した場合、その宛先に対応する複数のエントリでルーティングテーブルが更新されます。その宛先へのトラフィックは、それらのパスの間で分散されます。

CEF は、マルチレイヤ スイッチのルート キャッシュではなく、複数のデータ構造で情報を保存します。このデータ構造によって検索が最適化され、効率的なパケット転送が実現されます。

FIB

Forwarding Information Base (FIB; 転送情報ベース)は、IP ルーティング テーブルの転送情報のミラーイメージを格納したテーブルです。ネットワークでルーティングまたはトポロジが変更されると、ルート プロセッサが IP ルーティング テーブルを更新し、CEF が FIB を更新します。FIB エントリとルーティング テーブル エントリは 1 対 1 の関係なので、FIB には既知のすべてのルートが含まれます。したがって、高速スイッチング、最適スイッチングなど、スイッチング パスに関連するルート キャッシュのメンテナンスが不要になります。CEF は FIB を使用し、IP 宛先プレフィクスに基づいてスイッチングを決定し、IP ルーティング テーブルの情報に基づいてネクストホップ アドレス情報を維持します。

Catalyst 4500 シリーズ スイッチでは、CEF は Integrated Switching Engine ハードウェアに FIB をロードして、転送のパフォーマンスを向上させます。Integrated Switching Engine には、ルーティング情報を保存できる、決まった数のフォワーディング スロットがあります。この限度を超えると、CEFは自動的にディセーブルになり、すべてのパケットがソフトウェアで転送されます。この場合、スイッチ上のルート数を減らしてから、ip cef コマンドでハードウェア スイッチングを再度イネーブルにする必要があります。

隣接関係テーブル

CEF は、FIB のほかに、隣接関係テーブルを使用してレイヤ 2 アドレス情報を前に付け加えます。 ネットワーク内のノードは、相互間の距離が 1 ホップ以内の場合に、「*隣接*」しているといいます。 隣接関係テーブルで、すべての FIB エントリのレイヤ 2 ネクストホップ アドレスが維持されます。

隣接関係の検出

隣接関係テーブルは、新しい隣接ノードが検出されたときに更新されます。(Address Resolution Protocol [ARP; アドレス解決プロトコル] などを使用して) 隣接関係エントリが作成されるたびに、その隣接ノードのリンクレイヤ ヘッダーが隣接関係テーブルに保存されます。ルートが確定すると、リンクレイヤ ヘッダーはネクストホップおよび対応する隣接関係エントリを指し示します。リンクレイヤ ヘッダーはそのあと、CEF パケット スイッチング時のカプセル化に使用されます。

隣接関係の解決

ロード バランシングと冗長性に同時に対応するようにルータが設定されている場合など、宛先プレフィクスへのルートに複数のパスが含まれることがあります。解決されたパスごとに、そのパスのネクストホップ インターフェイスに対応する隣接関係にポインタが追加されます。このメカニズムは、複数パス間でのロード バランシングに使用されます。

特殊な処理が必要な隣接関係タイプ

特定の例外条件が存在する場合、スイッチングを迅速に処理する目的で、ネクストホップインターフェイスの隣接関係(ホストルートの隣接関係)に加え、他のタイプの隣接関係が使用されます。プレフィクスが定義されると、例外処理が必要なプレフィクスは、表 28-1 に示した特殊な隣接関係の1つを指定して、キャッシュに格納されます。

表 28-1 例外処理を伴う隣接タイプ

隣接タイプ	処理
Null	インターフェイス NullO を宛先とするパケットはドロップされます。インターフェイス NullO は、効果的なアクセス フィルタリング形式として使用できます。
Glean	ルータが複数のホストに直接接続されている場合、ルータ上の FIB テーブルは、個々のホストではなく、サブネットに対応するプレフィクスを維持します。サブネット プレフィクスは、Glean 隣接関係を指し示します。特定のホストにパケットを転送する必要がある場合、隣接データベースから特定のプレフィクスが集められます。
Punt	特殊な処理を必要とする機能や CEF スイッチングでまだサポートされていない機能は、次に上位のスイッチング レベルに送られます (パントされます)。
Discard	パケットがドロップされます。
Drop	パケットがドロップされます。

未解決の隣接関係

パケットの前にリンクレイヤへッダーが追加された場合、FIB はネクストホップに対応する隣接関係を指し示すプリペンドを要求します。隣接関係が FIB によって作成され、ARP などのメカニズムでは検出されなかった場合、レイヤ 2 アドレッシング情報が不明であるため、その隣接関係は不完全とみなされます。レイヤ 2 情報が認識されると、パケットはルート プロセッサに転送され、ARPによって隣接関係が判別されます。

Catalyst 4500 シリーズ スイッチでの CEF の実装

ここでは、次の内容について説明します。

- ハードウェアおよびソフトウェアのスイッチング(p.28-4)
- ロード バランシング (p.28-6)
- ソフトウェア インターフェイス (p.28-6)

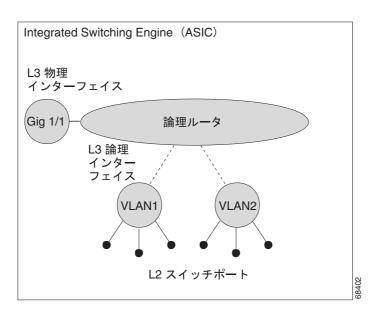
Catalyst 4000 ファミリ スイッチは、Application Specific Intergrated Circuit (ASIC; 特定用途向け集積 回路) ベースの Integrated Switching Engine をサポートすることにより、次の処理を行います。

- レイヤ2でのイーサネットブリッジング
- レイヤ3でのIPルーティング

ASIC はパケット転送専用に設計されているので、Integrated Switching Engine ハードウェアは、CPU サブシステム ソフトウェアより、はるかに高速でこの処理を実行できます。

図 28-1 に、Integrated Switching Engine 上の ASIC ベース レイヤ 2 およびレイヤ 3 スイッチング プロセスの概念を示します。

図 28-1 論理 L2/L3 スイッチング コンポーネント



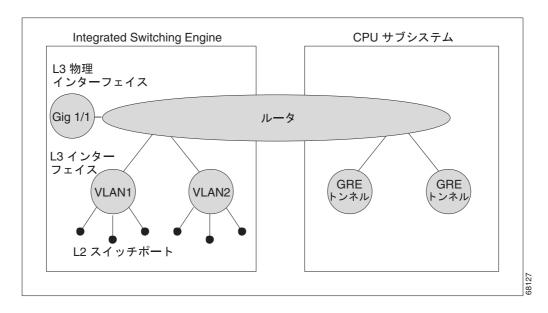
Integrated Switching Engine は、ASIC ハードウェアを使用して、論理レイヤ 3 インターフェイス上で VLAN (仮想 LAN)間ルーティングを実行します。ASIC ハードウェアは、ホスト、スイッチ、またはルータに接続するように設定できる物理レイヤ 3 インターフェイスもサポートしています。

ハードウェアおよびソフトウェアのスイッチング

通常のパケットについては、Integrated Switching Engine はハードウェアでパケット転送機能を実行します。これらのパケットは非常に高速でハードウェアスイッチングされます。例外のパケットは、CPU サブシステム ソフトウェアによって転送されます。Integrated Switching Engine が大部分のパケットをハードウェアで転送していることは、統計レポートからわかります。ソフトウェア転送の速度はハードウェア転送に比べて大幅に下がりますが、CPU サブシステムによってパケットが転送されても、ハードウェア転送の速度が下がることはありません。

図 28-2 は、Integrated Switching Engine および CPU サブシステムのスイッチング コンポーネントの概念図です。

図 28-2 ハードウェアおよびソフトウェア スイッチングのコンポーネント



Integrated Switching Engine は、ハードウェアで VLAN 間ルーティングを実行します。CPU サプシステム ソフトウェアは、Subnetwork Access Protocol (SNAP)カプセル化を使用する、VLAN へのレイヤ 3 インターフェイスをサポートします。CPU サブシステム ソフトウェアはさらに、Generic Routing Encapsulation (GRE; 総称ルーティング カプセル化)トンネルもサポートしています。

ハードウェア スイッチング

ハードウェア スイッチングは、Supervisor Engine III および Supervisor Engine IV の標準動作です。

ソフトウェア スイッチング

ソフトウェア スイッチングは、ハードウェアでトラフィックを処理できない場合に行われます。次のタイプの例外パケットがソフトウェアで処理されますが、速度は大幅に低下します。

IP ヘッダー オプションを使用しているパケット



(注)

TCP ヘッダー オプションを使用しているパケットは、転送の決定に影響しないので、 ハードウェアでスイッチングされます。

- IP Time To Live (TTL; 存続可能時間) カウンタが満了しているパケット
- トンネル インターフェイスに転送されるパケット
- サポート対象外のカプセル化タイプを指定して送られてきたパケット
- サポート対象外のカプセル化タイプが設定されたインターフェイスにルーティングされるパケット

- 出力インターフェイスの Maximum Transmission Unit (MTU; 最大伝送ユニット) を超えている ため分割が必要なパケット
- Internet Group Management Protocol (IGMP; インターネット グループ管理プロトコル) リダイレクトのルーティングが必要なパケット
- 802.3 イーサネット パケット

ロード バランシング

Catalyst 4000 ファミリ スイッチは、Integrated Switching Engine ハードウェアで、パケット ルーティングのロード バランシングをサポートします。ロード バランシング機能は常にイネーブルです。この機能は、同一ネットワークに複数の異なるネクストホップ アドレスで複数のルートが設定されている場合に動作します。このようなルートは、スタティックに設定することも、Open Shortest Path First (OSPF)、Enhanced Interior Gateway Routing Protocol (EIGRP) などのルーティング プロトコルによって設定することもできます。

ハードウェアは、ハードウェア ハッシュ機能を使用し、送信元および宛先 IP アドレス、送信元および宛先 TCP ポート番号(該当する場合)に基づいて値を計算することによって、転送を決定します。さらに、この負荷分散型ハッシュ値を使用して、パケット転送に使用するルートが選択されます。特定のフロー(TCP 接続など)内のすべてのハードウェア スイッチングが同じネクストホップにルーティングされるので、パケットの順序変更が発生する可能性が小さくなります。1 つのネットワークに対して最大 8 種類のルートがサポートされます。

ソフトウェア インターフェイス

Catalyst 4000 ファミリ スイッチ対応の Cisco IOS は、ハードウェア転送エンジンには組み込まれて いない GRE および IP トンネル インターフェイスをサポートしています。これらのインターフェイスとの間を流れるパケットはすべて、ソフトウェアで処理する必要があります。転送速度はハードウェア スイッチング インターフェイスに比べて大幅に低下します。また、これらのインターフェイスでは、レイヤ 2 機能はサポートされません。

CEF 設定の制限事項

Integrated Switching Engine がハードウェアでのレイヤ 3 スイッチングでサポートするカプセル化タイプは、Advanced Research Projects Agency (ARPA) および ISL (スイッチ間リンク)/802.1Q だけです。CPU サブシステムは、レイヤ 2 対応の SNAP など、ソフトウェアでのレイヤ 3 スイッチングに使用できるさまざまなカプセル化をサポートします。

CEF の設定

ここでは、CEFを設定する手順について説明します。

- CEF のイネーブル化 (p.28-7)
- CEF のロード バランシングの設定 (p.28-7)

CEF のイネーブル化

Catalyst 4000 ファミリ スイッチでは、CEF はデフォルトの設定でグローバルにイネーブルになっています。 したがって設定作業は不要です。

CEF を再度イネーブルにするには、次の作業を行います。

コマンド	目的
Switch(config)# ip cef distributed	標準の CEF 動作をイネーブルにします。

CEF のロード バランシングの設定

CEF のロード バランシングは、送信元および宛先パケット情報の組み合わせに基づいて行われます。宛先へデータを転送するときに、複数のパスにトラフィックを分散させることによって、リソースの利用を最適化できます。ロード バランシング機能は、宛先単位で設定できます。ロード バランシングの決定は、発信インターフェイスで行われます。ロード バランシングを設定するときには、宛先単位で発信インターフェイスに設定してください。

ここでは、次の内容について説明します。

- 宛先別ロード バランシングの設定 (p.28-7)
- 負荷分散型ハッシュ機能の設定 (p.28-8)
- CEF 情報の表示 (p.28-8)

宛先別ロード バランシングの設定

CEF がイネーブルの場合、宛先別ロード バランシングはデフォルトでイネーブルです。宛先別ロード バランシングを使用する場合は、CEF をイネーブルにすれば、追加の作業は必要ありません。

宛先別ロード バランシングにより、ルータは複数のパスを使用して負荷を分散させます。特定の送信元または宛先ホストのペアに対応するパケットは、複数のパスが使用できる場合でも、必ず同じパスを通ることになります。異なるペア宛てのトラフィックは、それぞれ異なるパスを通る傾向があります。CEF をイネーブルにすると、宛先別ロード バランシングはデフォルトでイネーブルになります。このロード バランシング方式はさまざまな環境に適しています。

宛先別ロード バランシングは、統計上のトラフィック分散に依存するので、送信元ペアまたは宛先ペアの数が増えるほど、負荷分散の効果が大きくなります。

宛先別ロード バランシングを使用すると、特定のホスト ペア宛てのパケットが順番に届くようになります。特定のホスト ペア宛てのパケットはすべて、同じリンク (1 つまたは複数のリンク) を使用してルーティングされます。

負荷分散型ハッシュ機能の設定

宛先 IP プレフィクスに対して複数のユニキャスト ルートが存在する場合、ハードウェアは、プレフィクスに一致するパケットを使用可能なすべてのルートで送信するので、すべてのネクストホップ ルータで負荷が分散されます。デフォルトでは、送信元および宛先 IP アドレスのハッシュを計算し、ルート選択用に導き出された値を使用して使用されるルートが選択されます。この結果、1つの送信元フローまたは宛先フロー内のすべてのパケットが必ず同じルート上で送信されるため、複数のパケットについてパケット順序が保持されますが、ルートに対してフローをほぼランダムに分散します。

負荷分散型ハッシュ機能は変更できるので、送信元および宛先 IP アドレス以外に、送信元 TCP/UDP ポート、宛先 TCP/UDP ポート、またはその両方をハッシュに組み込むことができます。

送信元または宛先ポート、あるいはその両方を使用するように負荷分散型ハッシュ機能を設定するには、次の作業を行います。

コマンド	目的
Switch (config) # [no] ip cef load-sharing algorithm include-ports source destination]	送信元および宛先ポートを使用する負荷分散型 ハッシュ機能をイネーブルにします。
	デフォルトの Cisco IOS 負荷分散アルゴリズム を使用するようにスイッチを設定するには、no キーワードを指定します。

負荷分散の詳細については、次の URL で Cisco IOS マニュアルの『Configuring Cisco Express Forwarding』モジュールを参照してください。

http://www.cisco.com/univered/cc/td/doc/product/software/ios122/122cgcr/fwitch_c/swprt1/xcfcefc.htm



include-ports オプションは、Catalyst 4500 シリーズ スイッチ上のソフトウェアでスイッチングされるトラフィックには適用されません。

CEF 情報の表示

収集された CEF 情報を表示できます。CEF を表示するには、次の作業を行います。

コマンド	目的
Switch# show ip cef	収集された CEF 情報を表示します。

CEF のモニタリングおよびメンテナンス

IP トラフィックに関する情報を表示するには、次の作業を行います。

コマンド	目的
Switch# show interface type slot/interface begin L3	IP ユニキャスト トラフィックのサマリーを 表示します。

次に、インターフェイス FastEthernet 3/3 上の IP ユニキャスト トラフィック情報を表示する例を示します。

Switch# show interface fastethernet 3/3 \mid begin L3

L3 in Switched: ucast: 0 pkt, 0 bytes - mcast: 12 pkt, 778 bytes mcast
L3 out Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes
4046399 packets input, 349370039 bytes, 0 no buffer
Received 3795255 broadcasts, 2 runts, 0 giants, 0 throttles

<テキスト出力は省略>

Switch#



IP ユニキャスト パケット カウントは、約5秒間隔で更新されます。

IP 統計情報の表示

IP ユニキャスト統計情報は、インターフェイス単位で収集されます。IP 統計情報を表示するには、次の作業を行います。

コマンド	目的
Switch# show interface type number counters detail	IP 統計情報を表示します。

次に、インターフェイス FastEthernet 3/1 の IP ユニキャスト統計情報を表示する例を示します。

Switch# show interface fastethernet 3/1 counters detail

Port Fa3/1	InBytes 7263539133			InBcastPkts 156
Port Fa3/1	OutBytes 7560137031		OutMcastPkts 12140475	OutBcastPkts
Port Fa3/1	InPkts 64 11274	OutPkts 64 168536	InPkts 65-127 7650482	OutPkts 65-127 12395769
Port Fa3/1	InPkts 128-255 31191	OutPkts 128-255 55269	InPkts 256-511 26923	
Port Fa3/1	InPkts 512-1023 133807	OutPkts 512-1023 151582		
Port Fa3/1	InPkts 1024-1518 N/A	OutPkts 1024-1518 N/A		
Port Fa3/1	InPkts 1024-1522 4557008	OutPkts 1024-1522 4384192	InPkts 1523-1548 0	OutPkts 1523-1548 0
Port Fa3/1	Tx-Bytes-Queue-1	Tx-Bytes-Queue-2	Tx-Bytes-Queue-3 91007	Tx-Bytes-Queue-4 7666686162
Port Fa3/1	Tx-Drops-Queue-1	Tx-Drops-Queue-2	Tx-Drops-Queue-3	Tx-Drops-Queue-4
Port Fa3/1	Rx-No-Pkt-Buff 0	RxPauseFrames	TxPauseFrames	PauseFramesDrop N/A
Port Fa3/1 Switch#	UnsupOpcodePause 0			

CEF (ソフトウェア スイッチング) およびハードウェア IP ユニキャスト隣接テーブル情報を表示 するには、次の作業を行います。

コマンド	目的
4 4	オプションの detail キーワードを指定すると、レイヤ 2 情報を含めた詳細な隣接情報が表示されます。

次に、隣接統計情報を表示する例を示します。

Switch# show adjacency gigabitethernet 3/5 detail

Protocol Interface Address

IP GigabitEthernet9/5 172.20.53.206(11)
504 packets, 6110 bytes
00605C865B82

000164F83FA50800 ARP 03:49:31



隣接統計情報は、約10秒間隔で更新されます。



CHAPTER

29

ユニキャスト RPF の設定

この章では、ユニキャスト Reverse Path Forwarding (ユニキャスト RPF)機能について説明します。 ユニキャスト RPF 機能は、間違ったまたは偽造送信元 IP アドレスがルータを流れて発生する問題 を軽減するのに役立ちます。

この章のユニキャスト RPF コマンドの詳細については、『Cisco IOS Security Command Reference』の「Unicast Reverse Path Forwarding Commands」の章を参照してください。この章に記載されたその他のコマンドに関するマニュアルを特定するには、コマンド リファレンスのマスター インデックスを使用するか、オンラインで検索してください。

機能に関するハードウェア プラットフォームまたはソフトウェア イメージの情報を確認するには、Cisco.com の Feature Navigator を使用してその機能に関する情報を検索するか、特定のリリースに対応するソフトウェア リリース ノートを参照してください。詳細については、「Using Cisco IOS Software」の章の「Identifying Supported Platforms」を参照してください。

章の内容

この章の内容は、次のとおりです。

- ユニキャスト RPF について
- ユニキャスト RPF の設定作業リスト
- ユニキャスト RPF のモニタリングおよびメンテナンス
- ユニキャスト RPF のモニタリングおよびメンテナンス
- ユニキャスト RPF の設定例

ユニキャスト RPF について

ユニキャスト RPF 機能は、検証可能な送信元 IP アドレスが不足している IP パケットを廃棄することで、間違ったまたは偽造(スプーフィングされた)送信元 IP アドレスがネットワークに流れて発生する問題を軽減するのに役立ちます。たとえば、Smurf や Tribal Flood Network (TFN) など、多くの一般的なタイプの DoS 攻撃は、偽造された、または次々に変わる送信元 IP アドレスを使用して、攻撃を突き止めたりフィルタしたりすることを攻撃者が阻止できるようにします。パブリック アクセスを提供する Internet Service Provider (ISP; インターネットサービスプロバイダー) の場合、ユニキャスト RPF が IP ルーティング テーブルと整合性の取れた有効な送信元アドレスを持つパケットだけを転送することによって、これらの攻撃をそらします。この処理により、ISP のネットワークとお客様、および残りのインターネットの他の部分が保護されます。

ここでは、次の情報について説明します。

- ユニキャスト RPF の概要
- ユニキャスト RPF の実装
- 制約事項
- 関連機能および技術
- ユニキャスト RPF 設定の前提条件

ユニキャスト RPF の概要

ユニキャスト RPF がインターフェイスでイネーブルのときは、ルータはそのインターフェイスに対する入力として受信したすべてのパケットを検証して、送信元アドレスおよび送信元インターフェイスがルーティング テーブルに存在し、パケットを受信したインターフェイスと一致することを確認します。「後方検索」機能は、Cisco Express Forwarding (CEF)がルータでイネーブルの場合にのみ利用可能です。これは、検索が Forwarding Information Base (FIB; 転送情報ベース)に基づいて行われるためです。FIB は CEF の動作の一部として生成されます。



ユニキャスト RPF は入力機能であり、接続のアップストリーム終端にあるルータの入力インターフェイスにのみ適用されます。

ユニキャスト RPF は、ルータ インターフェイスで受信したパケットが、パケットの送信元への最適な戻りパス (戻りルート)で到着しているかどうかを確認します。ユニキャスト RPF は、CEF テーブルの逆引きを行うことでこれを確認します。最適なリバース パス ルートのいずれかでパケットの受信が行われた場合は、パケットは通常通り転送されます。パケットを受信したインターフェイスと同じインターフェイスにリバース パス ルートがない場合は、送信元アドレスが変更されている可能性があります。ユニキャスト RPF がそのパケットのリバース パスを見つけられない場合は、パケットはドロップされます。



(注)

ユニキャスト RPF では、「最適な」等コスト戻りパスのすべてが有効とされます。そのため、ユニキャスト RPF は、複数の戻りパスが存在する場合に、各パスがルーティング コスト(ホップ数、重みなど)に関してその他のパスと等しく、ルートが FIB に存在するという条件で動作します。ユニキャスト RPF はまた、EIGRP バリアントが使用されていて、送信元 IP アドレスに戻る不等候補パスが存在する場合にも機能します。

ユニキャスト RPF および ACL が設定されているインターフェイスでパケットを受信する場合は、次の動作が発生します。

- ステップ1 受信インターフェイスで設定されている入力 ACL を確認します。
- **ステップ2** ユニキャスト RPF は、FIB テーブルの逆引きを行うことで、パケットが送信元への最適な戻りパスで到着しているかどうかを確認します。
- ステップ3 パケット転送のため CEF テーブル (FIB) のルックアップを実行します。
- ステップ4 送信インターフェイス上の出力 ALC の確認が行われます。
- ステップ5 パケットが転送されます。

ここでは、ユニキャスト RPF 拡張の内容について説明します。

- アクセス コントロール リストおよびロギング
- インターフェイス単位の統計情報

図 29-1 は、ユニキャスト RPF および CEF が連動して、パケットの戻りパスを確認することで IP 送信元アドレスを確認する方法を示します。この例では、お客様は送信元アドレスが 192.168.1.1 であるパケットをインターフェイス GigabitEthernet 1/1 から送信しています。ユニキャスト RPF は、192.168.1.1 に GigabitEthernet 1/1 へのパスがあるかどうか FIB を確認します。一致するパスがある場合にパケットが送信されます。一致するものがない場合、パケットはドロップされます。

図 29-1 ユニキャスト RPF による IP 送信元アドレスの確認

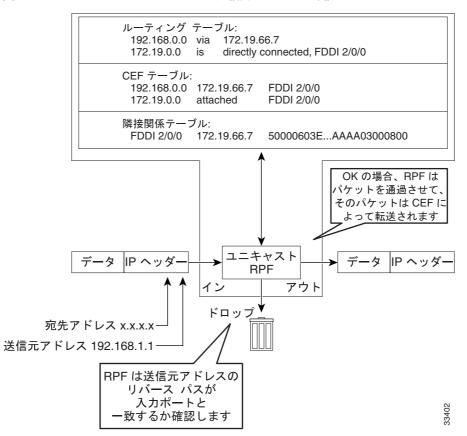


図 29-2 は、ユニキャスト RPF が確認に失敗したパケットをドロップする方法を示します。この例では、お客様は送信元アドレスが 209.165.200.225 であるパケットを送信していて、そのパケットをインターフェイス GigabitEthernet 1/1 で受信します。ユニキャスト RPF は、209.165.200.225 に GigabitEthernet 1/1 への戻りパスがあるかどうか FIB を確認します。一致するパスがある場合にパケットが送信されます。この場合、お客様のパケットを GigabitEthernet 1/1 上の送信元アドレス 209.165.200.225 に戻るルートのエントリがルーティング テーブルにないため、パケットはドロップされます。

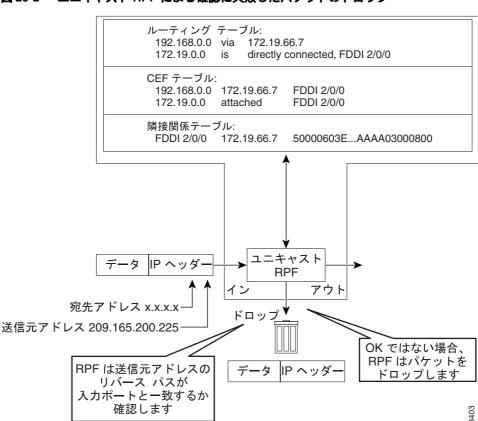


図 29-2 ユニキャスト RPF による確認に失敗したパケットのドロップ

ユニキャスト RPF の実装

ユニキャスト RPF には、次の主要な実装原理があります。

- パケットの受信は、パケットの送信元への最適な戻りパス(ルート)があるインターフェイスで行われる必要があります(対称ルーティングと呼ばれるプロセス)。FIBに、受信するインターフェイスへのルートと一致するルートが存在する必要があります。FIBへのルートの追加は、スタティックルート、ネットワークステートメント、またはダイナミックルーティングによって行われます(ACLは、パッケージが特定の、最適ではない非対称入力パスで到着すると分かっている場合には、ユニキャストRPFの使用を許可します。
- 受信するインターフェイスにある IP 送信元アドレスが、インターフェイスのルーティング エントリと一致する必要があります。
- ユニキャスト RPF は入力機能であり、接続のアップストリーム終端にあるルータの入力インターフェイスにのみ適用されます。

これらの実装原理においては、ユニキャスト RPF は、ネットワーク管理者がお客様のためだけでなく、ダウンストリーム ネットワークまたは ISP にインターネットに対する別の接続がある場合でも、ダウンストリーム ネットワークまたは ISP のために使用可能なツールとなります。



重みおよびローカル プリファレンスなどのオプションの BGP 属性を使用して、送信元アドレスに 戻る最善のパスを変更できます。変更は、ユニキャスト RPF の動作に影響を与える場合がありま す。

ここでは、ユニキャスト RPF の実装について説明します。

- セキュリティ ポリシーとユニキャスト RPF
- ユニキャスト RPF を使用する場所
- ルーティング テーブルの要件
- ユニキャスト RPF を使用できない場所
- BOOTP および DHCP を使用したユニキャスト RPF

セキュリティ ポリシーとユニキャスト RPF

ユニキャスト RPF を展開するポリシーの決定時には、次の点を考慮してください。

- ユニキャスト RPF は、大規模なネットワークのダウンストリーム インターフェイス (ネット ワークのエッジに存在することが望ましい) に適用する必要があります。
- ユニキャスト RPF をさらに下位のダウンストリームに適用すればするほど、アドレス スプーフィングの軽減時およびスプーフィングされたアドレスの送信元の特定時にさらにきめ細やかに対応できます。たとえば、ユニキャスト RPF を集約ルータに適用すると、多くのダウンストリーム ネットワークまたはクライアントからの攻撃の軽減に役立ち、管理が簡単になりますが、攻撃の送信元の特定には有益ではありません。ユニキャスト RPF をネットワーク アクセス サーバに適用すると、攻撃の範囲の制限や、攻撃の送信元の追跡に役立ちますが、多くのサイト間でユニキャスト RPF を展開することで、ネットワーク オペレーションの管理コストが増大します。
- インターネット、イントラネット、およびエクストラネット リソース全体でユニキャスト RPF を展開するエンティティがさらに増加すれば、インターネット コミュニティ全体の大規模な ネットワーク中断がさらに軽減し、攻撃の送信元を追跡する機会がさらに増えます。
- ユニキャスト RPF は、GRE、LT2P、または PPTP などのトンネルにカプセル化した IP パケット を検査しません。ユニキャスト RPF が、トンネリングが行われて暗号化レイヤがパケット から取り除かれたあとにだけネットワーク トラフィックを処理するには、ユニキャスト RPF をホーム ゲートウェイで設定する必要があります。

ユニキャスト RPF を使用する場所

ユニキャスト RPF は、原則的にネットワーク内のアクセス ポイントが 1 つだけ (つまり、アップストリーム接続が 1 つだけ) である「シングルホーム」環境であれば使用できます。アクセス ポイントが 1 つあるネットワークは、対称ルーティングの良い例となります。これは、パケットがネットワークに入るときのインターフェイスが、IP パケットの送信元への最適な戻りパスでもあるということを表します。ユニキャスト RPF は、インターネット、イントラネット、またはエクストラネット環境のネットワーク境界または顧客ネットワーク終端の ISP 環境において最適に使用されます。

次のセクションで、2 つのネットワーク環境におけるユニキャスト RPF 実装の概要について説明します。

- ISP への接続を1つ備えるエンタープライズ ネットワーク
- ネットワーク アクセス サーバ アプリケーション(ユニキャスト RPF を PSTN/ISDN PoP 集約ルータに適用)

ISP への接続を 1 つ備えるエンタープライズ ネットワーク

エンタープライズ ネットワークでは、ユニキャスト RPF を使用して入力インターフェイスでのトラフィックをフィルタリングする (*入力フィルタリング*と呼ばれるプロセス)目的の1つは、インターネットから誤ったパケットが届かないようにすることです。従来、インターネットへの接続が1つあるローカル ネットワークは、受信するインターフェイスで ACL を使用して、スプーフィングされたパケットがインターネットからローカル ネットワークに入ってこないようにしていました。

ACL は、シングルホームを使用する多くのお客様については効果的に機能しますが、ACL を入力フィルタとして使用する場合には、次の2つの一般的に言及される制限を含めたトレードオフが存在します。

非常に高速なパケット レートでのパケット / 秒 (PPS) パフォーマンス



(注)

この制限は、ソフトウェアパケットの転送にのみ適用されます。ハードウェアパケットの転送は、ACLおよびuRPFの両方で同じです。

• ACL のメンテナンス (ネットワークに新しいアドレスが追加された場合)

ユニキャスト RPF は両方の制限に対応するツールです。ユニキャスト RPF を使用すると、入力フィルタリングは CEF PPS レートで行われます。この処理スピードは、リンク速度が 1 Mbps を超えたときに効果があります。さらに、ユニキャスト RPF は FIB を使用するため、ACL メンテナンスが不要になり、したがって従来の ACL の管理オーバーヘッドが減少します。次に、ユニキャスト RPFを入力フィルタリング向けに設定する方法を示す図および例を示します。

図 29-3 に、アップストリーム ISP へのリンクが 1 つあるエンタープライズ ネットワークを示します。この例では、間違ったパケットがインターネットから届かないようにするために、ユニキャスト RPF はエンタープライズ ルータのインターフェイス GigabitEthernet 1/1 で適用されます。また、間違ったパケットがエンタープライズ ネットワークから届かないようにするために、ユニキャストRPF は ISP ルータのインターフェイス GigabitEthernet 2/1 で適用されます。

図 29-3 入力フィルタリングのためにユニキャスト RPF を使用するエンタープライズ ネットワーク

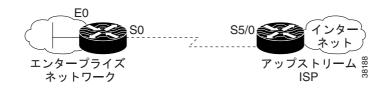


図 29-3 の関係図を使用すると、ISP ルータの典型的な構成は (CEF が有効になっていると想定して)次のとおりです。

interface Gigabit Ethernet 2/1
 description Link to Enterprise Network
 ip address 192.168.3.1 255.255.255.255
 no switchport
 ip address 10.1.1.2 255.255.255.0
 ip route 192.168.10.0 255.255.255.0 10.1.1.1
 ip verify unicast source reachable-via rx allow-default

エンタープライズ ネットワークのゲートウェイ ルータ設定は (CEF が有効になっていると想定して) 次のとおりです。

```
interface Gigabit Ethernet 1/2
  description ExampleCorp LAN
  ip address 192.168.10.1 255.255.252.0
  no ip redirects
  no ip directed-broadcast
  no ip proxy-arp

interface Gigabit Ethernet 1/1
  description Link to Internet
  no switchport
  ip address 10.1.1.1 255.255.255.0
  ip route 0.0.0.0 0.0.0.0 10.1.1.2
  ip verify unicast source reachable-via allow-default
  no ip proxy-arp
  no ip redirects
  no ip directed-broadcast
```

ユニキャスト RPF は、1 つのデフォルト ルートで動作することに注意してください。追加のルートまたはルーティング プロトコルはありません。ネットワーク 192.168.10.0/22 は接続されたネットワークです。したがって、送信元アドレスが 192.168.10.0/22 の範囲内の、インターネットから届くパケットは、ユニキャスト RPF によってドロップされます。

ネットワーク アクセス サーバ アプリケーション (ユニキャスト RPF を PSTN/ISDN PoP 集約ルータに適用)

集約ルータは、シングルホームを使用するお客様にとってはユニキャストを使用する最適な場所です。ユニキャスト RPF は、インターネットへの接続に専用線または PSTN/ISDN/xDSL を使用するお客様にとって等しく効果的に動作します。実際、ダイヤルアップ接続は偽造 IP アドレスを使用した DoS 攻撃の送信元とみなされることが非常に多くあります。ネットワーク アクセス サーバが CEF をサポートしているかぎり、ユニキャスト RPF は動作します。この関係図では、お客様の集約ルータに完全なインターネット ルーティング テーブルを用意する必要はありません。集約ルータは、プレフィクス情報 (IP アドレス ブロック)をルーティングする必要があります。したがって、Interior Gateway Protocol (IGP; 内部ゲートウェイ プロトコル)または Internal Border Gateway Protocol (IBGP; 内部ボーダー ゲートウェイ プロトコル)で設定または再配布された情報であれば、ユニキャストはその機能を十分に発揮できます。

図 29-4 は、お客様にダイヤルアップ接続を提供する ISP ルータとの ISP アクセス ポイント向けの 集約ルータおよびアクセス ルータへのユニキャスト RPF の適用を示します。この例では、ユニキャ スト RPF は ISP 集約ルータの受信する (入力) インターフェイスの、お客様のダイヤルアップ接続 ルータからのアップストリームに適用されます。

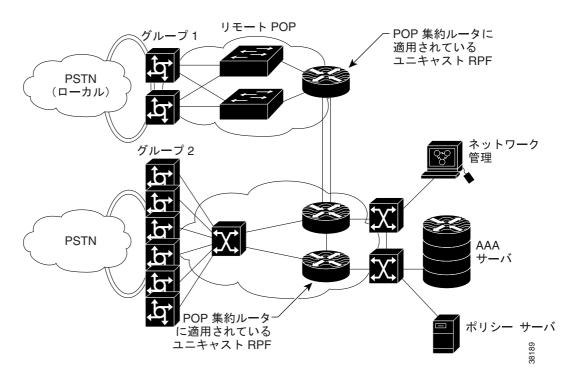


図 29-4 お客様の PSTN/ISDN 接続に適用されるユニキャスト RPF

ルーティング テーブルの要件

ユニキャスト RPF が正しく動作するには、CEF テーブルに適切な情報が存在する必要があります。この要件は、ルータに完全なインターネット ルーティング テーブルが存在する必要があるという意味ではありません。CEF テーブルに必要なルーティング情報の量は、ユニキャスト RPF の設定場所およびルータがネットワークで実行している機能によって異なります。例えば、ISP 環境では、お客様向けの専用線集約ルータであるルータが必要とするのは IGP または IBGP (ネットワークでどちらの技術を使用しているかにより異なります)で再配布されたスタティック ルートに関する情報のみです。ユニキャスト RPF がお客様のインターフェイス上で設定されるため、必要になるのは最低限のルーティング情報のみです。また別のシナリオで、シングルホームの ISP が、ユニキャスト RPF をインターネットにリンクするゲートウェイ上に配置する場合は、完全なインターネットルーティング テーブルが必要になります。完全なルーティング テーブルを要求することで、インターネット ルーティング テーブルにないアドレスを使用する外部 DoS 攻撃から ISP を保護するのに役立ちます。

ユニキャスト RPF を使用できない場所

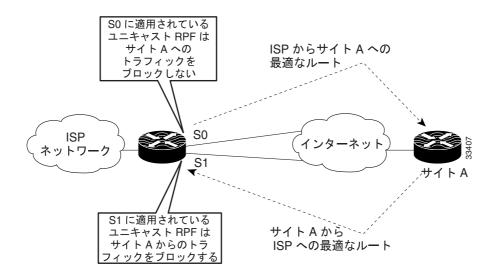
ユニキャスト RPF は、ネットワークの内側にあるインターフェイスで使用しないでください。内側にあるインターフェイスでは、ルーティングの非対称性(図 29-5 を参照)が発生しやすく、パケットの送信元への複数のルートが存在することになるためです。ユニキャスト RPF は、対称性が自然に発生するか、対称性が設定されている環境にのみ適用する必要があります。管理者がユニキャスト RPF を有効化するインターフェイスを注意深く計画するかぎり、ルーティングの非対称性は深刻な問題ではありません。

たとえば、ISP ネットワークのコアにあるルータよりも、ISP のネットワークのエッジにあるルータには、対称リバース パスがあることが多くあります。ISP ネットワークのコアにあるルータには、ルータからの最適な転送パスが、パケットがルータに戻るときに選択されるパスであるという保証がありません。 したがって、ACL を使用して、ルータが着信パケットを受け入れる場合を除いて、ユニキャスト RPF を非対称ルーティングが発生する可能性がある場所に適用することを推奨しま

せん。ACL は、パケットが特定の、最適ではない非対称入力パスで到着すると分かっている場合には、ユニキャスト RPF の使用を許可します。ただし、ISP にとっては、ユニキャスト RPF をネットワークのエッジまたはお客様のネットワークのエッジにのみ配置するのが最も簡単です。

図 29-5 は、ユニキャスト RPF が非対称ルーティング環境で正規のトラフィックをブロックする方法を示します。

図 29-5 非対称ルーティング環境においてトラフィックをブロックするユニキャスト RPF



BOOTP および DHCP を使用したユニキャスト RPF

Bootstrap Protocol (BOOTP; ブートストラップ プロトコル)および Dynamic Host Configuration Protocol (DHCP) 機能が正しく動作するようにするために、ユニキャスト RPF は、送信元として 0.0.0.0、宛 先として 255.255.255.255 を持つパケットの通過を許可します。

制約事項

マルチホームを使用するクライアントへのユニキャスト RPF の適用には、いくつかの基本的な制約事項があります。

- マルチホーミングはクライアントが冗長サービスを構築する目的と合わないため、クライアントは同じルータに対してマルチホームをしないでください。
- お客様は、(インターネットから)リンクに流れるパケットが、リンクからアドバタイズされたルートと一致することを確認する必要があります。一致しない場合、ユニキャスト RPF はそれらのパケットを間違ったパケットとしてフィルタリングします。

関連機能および技術

ユニキャスト RPF に関連する機能および技術に関する詳細については、次の項目を参照してください。

• ユニキャスト RPF がルータ上で適切に機能するには CEF が必要です。CEF の詳細については、 『Cisco IOS Switching Services Configuration Guide』を参照してください。

- Cisco IOS Access Control List (ACL; アクセス コントロール リスト)を使用して*入力*および*出力* フィルタリングのポリシーを組み合わせると、スプーフィング攻撃の軽減に対するユニキャスト RPF の効果が大きくなります。
 - 入力フィルタリングでは、内部または外部ネットワークのネットワーク インターフェイス で受信したトラフィックにフィルタを適用します。入力フィルタリングを使用すると、別の ネットワークまたはインターネットから到着したパケットのうち、その送信元アドレスが ローカル ネットワーク、プライベート、またはブロードキャスト アドレスと一致するパケットがドロップされます。たとえば ISP 環境では、入力フィルタリングはクライアント(お客様) またはインターネットのいずれかのルータで受信したトラフィックに適用できます。
 - 出力フィルタリングでは、ネットワーク インターフェイス(送信するインターフェイス) から送信されるトラフィックにフィルタを適用します。ネットワークをインターネットま たは他のネットワークに接続するルータ上のパケットをフィルタリングすることで、ネットワークから送信するために有効な送信元 IP アドレスを持つパケットのみを許可できます。

ネットワーク フィルタリングの詳細については、『RFC 2267』および『Cisco IOS IP Configuration Guide』を参照してください。

- Cisco IOS ソフトウェアは、DoS 攻撃を軽減するために役立つ機能をさらに提供しています。
 - Committed Access Rate (CAR; 専用アクセス レート)。 CAR を使用すると、アクセス リストと一致するネットワーク トラフィックに対して、帯域ポリシーを強制できます。 たとえば CAR は、ICMP トラフィックなどの量が少ないと思われるトラフィックにレート制限を課すことができます。 CAR の詳細については、『Cisco IOS Quality of Service Solutions Configuration Guide』を参照してください。
 - Context-based Access Control (CBAC; コンテキストベース アクセス コントロール)。CBAC は、保護されたネットワークから発信されていないネットワーク トラフィックを選択的にプロックします。CBAC は、タイムアウトおよびしきい値を使用してセッション ステート情報を管理します。これは、完全に確立された状態ではなくなっているセッションをいつドロップするか決定するのに役立ちます。ネットワーク セッションのタイムアウト値を設定することは、システム リソースを解放し、特定の時間が経過したあとでセッションをドロップするので、DoS 攻撃の軽減に役立ちます。CBAC の詳細については、『Cisco IOS Security Configuration Guide』を参照してください。
 - TCP 代行受信。TCP 代行受信機能はソフトウェアに実装され、DoS 攻撃の一種である TCP SYN フラッディング攻撃から TCP サーバを保護します。SYN フラッディング攻撃は、ハッカーが接続要求を集中させてサーバにフラッディングさせるときに発生します。CBAC と同様に、TCP 代行受信機能もまた、タイムアウトおよびしきい値を使用してセッション ステート情報を管理します。これは、完全に確立された状態ではなくなっているセッションをいつドロップするか決定するのに役立ちます。TCP 代行受信の詳細については、『Cisco IOS Security Configuration Guide』を参照してください。

ユニキャスト RPF 設定の前提条件

ユニキャスト RPF を設定する前に、ACL を次のように設定します。

- 標準または拡張 ACL を設定して、無効な IP アドレスの送信を削減します(出力フィルタリングを実行します)。有効な送信元アドレスのみネットワークに出入りすることを許可して、それ以外の送信元すべてがインターネットに向けてネットワークを出ないようにします。
- 標準または拡張 ACL エントリを設定して、無効な送信元 IP アドレスを持つパケットをドロップ(拒否)します(入力フィルタリングを実行します)。無効な送信元 IP アドレスには、次の種類があります。
 - 予約されたアドレス
 - ループバック アドレス
 - プライベートアドレス (RFC 1918、「Address Allocation for Private Internets」)
 - ブロードキャスト アドレス (マルチキャスト アドレスを含む)
 - 保護されたネットワークに関連する有効なアドレスの範囲外の送信元アドレス

ユニキャスト RPF の設定作業リスト

次のセクションでは、ユニキャスト RPF の設定作業について説明します。リスト内の各作業は、任意または必須です。

- ユニキャスト RPF の設定 (必須)
- ユニキャスト RPF の確認 (任意)

この章の最後にある「ユニキャスト RPF の設定例」を参照してください。

ユニキャスト RPF の設定

ユニキャスト RPF は、いかなる種類のカプセル化でもサポートし、ルータによって受信された IP パケットの操作を行うインターフェイスまたはサブインターフェイス上でイネーブルとなる入力 側の機能です。

ユニキャスト RPF を設定するには、次の作業を行います。

	コマンド	目的		
ステップ 1	Router(config-if)# interface type	ユニキャスト RPF を適用する入力インターフェイスを選択します。これは受信するインターフェイスで、これによってユニキャスト RPF はパケットを次の宛先に転送する前に最適な戻りパスを確認できます。		
		インターフェイスのタイプは使用しているルータおよび ルータに取り付けられているインターフェイス カードの タイプ専用です。利用可能なインターフェイスのタイプの 一覧を表示するには、interface?コマンドを入力します。		
ステップ 2	Router(config-if)# ip verify unicast source reachable-via rx allow-default	インターフェイスのユニキャスト RPF をイネーブルにします。		
ステップ 3	Router(config-if)# exit	インターフェイス コンフィギュレーション モードを終了 します。ユニキャスト RPF を適用するインターフェイスご とに、ステップ 2 および 3 を繰り返します。		

ユニキャスト RPF の確認

ユニキャスト RPF が動作可能かどうかを確認するには、show cef interface コマンドを使用します。 次に、ユニキャスト RPF がインターフェイス GigabitEthernet 3/1 でイネーブルになっている例を示します。

Switch# show cef interface gigabitEthernet 3/1 GigabitEthernet3/1 is up (if number 79) Corresponding hwidb fast_if_number 79 Corresponding hwidb firstsw->if_number 79 Internet address is 10.1.1.1/24 ICMP redirects are always sent IP unicast RPF check is enabled <===== Input features: uRPF <=====</pre> Inbound access list is not set Outbound access list is not set IP policy routing is disabled BGP based policy accounting on input is disabled BGP based policy accounting on output is disabled Hardware idb is GigabitEthernet3/1 Fast switching type 1, interface type 155 IP CEF switching enabled IP CEF switching turbo vector IP Null turbo vector IP prefix lookup IPv4 mtrie 8-8-8-8 optimized Input fast flags 0x4000, Output fast flags 0x0 ifindex 78(78) Slot 3 Slot unit 1 VC -1 Transmit limit accumulator 0x0 (0x0) TP MTTI 1500

ユニキャスト RPF のモニタリングおよびメンテナンス

ここでは、ユニキャスト RPF のモニタリングおよびメンテナンスに使用されるコマンドについて説明します。

コマンド	目的
Router# show ip traffic	ユニキャスト RPF によるドロップまたはドロップ抑制に関するグローバル ルータの統計情報を表示します。
Router(config-if)# no ip verify unicast	インターフェイスのユニキャスト RPF をディセーブルにします。

ユニキャスト RPF は、間違ったまたは偽造送信元アドレスのためドロップまたは抑制されたパケット数をカウントします。 ユニキャスト RPF は、次のインターフェイス単位のグローバル情報を含めてドロップまたは転送されたパケット数をカウントします。

- グローバル ユニキャスト RPF ドロップ
- インターフェイス単位のユニキャスト RPF ドロップ
- インターフェイス単位のユニキャスト RPF ドロップ抑制

show ip traffic コマンドは、ルータのすべてのインターフェイスについてドロップまたは抑制されたパケットの合計数 (グローバル カウント) を示します。ユニキャスト RPF ドロップ カウントは、IP 統計情報セクションに表示されます。

Router# show ip traffic

```
IP statistics:
```

Rcvd: 1471590 total, 887368 local destination

0 format errors, 0 checksum errors, 301274 bad hop count

0 unknown protocol, 0 not a gateway

O security failures, O bad options, O with options

Opts: 0 end, 0 nop, 0 basic security, 0 loose source route

0 timestamp, 0 extended security, 0 record route

0 stream ID, 0 strict source route, 0 alert, 0 other

Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble

0 fragmented, 0 couldn't fragment

Bcast: 205233 received, 0 sent

Mcast: 463292 received, 462118 sent

Sent: 990158 generated, 282938 forwarded
! The second line below ("0 unicast RPF") displays Unicast RPF packet dropping

information.

Drop: 3 encapsulation failed, 0 unresolved, 0 no adjacency

0 no route, 0 unicast RPF, 0 forced drop

ドロップまたは抑制されたパケットのカウントがノンゼロ値である場合は、次の 2 つのいずれかを 意味します。

- ユニキャスト RPF は、不良送信元アドレスを持つパケットをドロップまたは抑制しています (通常の動作)。
- ユニキャスト RPF は、非対称ルーティングが存在する(つまり、送信元アドレスに対する最適な戻りパスとして複数のパスが存在する)環境においてユニキャスト RPF を使用するためにルートが誤って設定されているため、正規のパケットをドロップまたは抑制しています。

show ip interface コマンドは、特定のインターフェイスにおいてドロップまたは抑制されたパケットの合計を示します。ユニキャスト RPF が特定の ACL を使用するよう設定されている場合は、このドロップ統計情報とともに ACL 情報が表示されます。

Router> show ip interface ethernet0/1/1

Unicast RPF ACL 197 1 unicast RPF drop 1 unicast RPF suppressed drop

show access-lists コマンドは、特定のエントリについて特定のアクセス リスト内で一致する項目が見つかった数を表示します。

Router> show access-lists

Extended IP access list 197

deny ip 192.168.201.0 0.0.0.63 any log-input (1 match)

permit ip 192.168.201.64 0.0.0.63 any log-input (1 match)

deny ip 192.168.201.128 0.0.0.63 any log-input

permit ip 192.168.201.192 0.0.0.63 any log-input

ユニキャスト RPF の設定例

ここでは、次の設定例を示します。

- 専用線集約ルータでのユニキャスト RPF の例
- Cisco AS5800 でのダイヤルアップ ポートを使用したユニキャスト RPF の例
- 着信および発信フィルタを使用したユニキャスト RPF の例
- ACL およびロギングを使用したユニキャスト RPF の例

専用線集約ルータでのユニキャスト RPF の例

次のコマンドは、ユニキャスト RPF をシリアル インターフェイス上でイネーブルにします。

```
ip cef
! or "ip cef distributed" for RSP+VIP based routers
!
interface serial 5/0/0
  ip verify unicast reverse-path
```

Cisco AS5800 でのダイヤルアップ ポートを使用したユニキャスト RPF の例

次の例では、Cisco AS5800 でユニキャスト RPF をイネーブルにします。**interface Group-Async** コマンドを使用すると、すべてのダイヤルアップ ポートにユニキャスト RPF を適用することが容易になります。

```
ip cef
!
interface Group-Async1
ip verify unicast reverse-path
```

着信および発信フィルタを使用したユニキャスト RPF の例

次に、非常に簡単なシングルホームを使用する ISP を使用して、ユニキャスト RPF とともに使用する入力および出力フィルタの概念の例を示します。この例は、アップストリーム インターフェイスで着信および発信フィルタの両方を使用する、ISP が割り当てた Classless Interdomain Routing (CIDR) ブロック 209.165.202.128/28 を示します。ISP は一般的にシングルホームを使用しないことに注意してください。したがって、非対称フローについての規定(発信トラフィックが1つのリンクから発信され、別のリンクから戻る場合)を設計して ISP の境界ルータ上のフィルタに組み込む必要があります。

```
ip cef distributed
interface Serial 5/0/0
 description Connection to Upstream ISP
ip address 209.165.200.225 255.255.255.252
no ip redirects
no ip directed-broadcast
no ip proxv-arp
ip verify unicast reverse-path
 ip access-group 111 in
ip access-group 110 out
access-list 110 permit ip 209.165.202.128 0.0.0.31 any
access-list 110 deny ip any any log
access-list 111 deny ip host 0.0.0.0 any log
access-list 111 deny ip 127.0.0.0\ 0.255.255.255 any \log
access-list 111 deny ip 10.0.0.0 0.255.255.255 any log
access-list 111 deny ip 172.16.0.0 0.15.255.255 any log
access-list 111 deny ip 192.168.0.0\ 0.0.255.255 any \log
access-list 111 deny ip 209.165.202.128 0.0.0.31 any log
access-list 111 permit ip any any
```

ACL およびロギングを使用したユニキャスト RPF の例

次に、ユニキャスト RPF を使用して ACL およびロギングを使用する例を示します。この例では、 拡張 ACL 197 が特定のアドレス範囲についてネットワーク トラフィックを拒否または許可するエ ントリを示します。ユニキャスト RPF は、インターフェイス Ethernet() で設定され、そのインター フェイスに到着したパケットを確認します。

たとえば、インターフェイス Ethernet0 に到着する送信元アドレスが 192.168.201.10 であるパケットは、ACL 197 にある拒否 (deny) ステートメントのため、ドロップされます。この場合、ACL 情報は口グに記録され(ロギング オプションが ACL エントリについてオンになっている)、ドロップされたパケットはインターフェイス単位でグローバルにカウントされます。インターフェイス Ethernet0 に到着する送信元アドレスが 192.168.201.100 であるパケットは、ACL 197 にある許可 (permit) ステートメントのため、転送されます。ドロップまたは抑制されたパケットに関する ACL 情報はログ サーバに記録されます(ロギング オプションが ACL エントリについてオンになっている)。

```
ip cef distributed
!
int eth0/1/1
  ip address 192.168.200.1 255.255.255.0
  ip verify unicast reverse-path 197
!
int eth0/1/2
  ip address 192.168.201.1 255.255.255.0
!
access-list 197 deny ip 192.168.201.0 0.0.0.63 any log-input access-list 197 permit ip 192.168.201.64 0.0.0.63 any log-input access-list 197 deny ip 192.168.201.128 0.0.0.63 any log-input access-list 197 permit ip 192.168.201.192 0.0.0.63 any log-input access-list 197 permit ip 192.168.201.192 0.0.0.63 any log-input access-list 197 deny ip host 0.0.0.0 any log
```



CHAPTER

30

単一方向イーサネットの設定



(注) Supervisor Engine 6-E は、この機能をサポートしていません。

この章では、Catalyst 4000 ファミリ スイッチ上で単一方向イーサネットを設定する手順について説明します。この章の内容は、次のとおりです。

- 単一方向イーサネットの概要 (p.30-2)
- 単一方向イーサネットの設定 (p.30-2)



この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univered/cc/td/doc/product/software/ios122sr/cr/index.htm

単一方向イーサネットの概要

スタブレス ギガビット イーサネット ポートは、単方向のトラフィックを送信または受信するように設定できます。単一方向イーサネットでは、全二重ギガポート イーサネット用に 2 つの光ファイバ ストランドを使用するのではなく、ギガポートの単方向トラフィックの送信または受信にファイバ ストランドを 1 つだけ使用します。ギガポートをそれぞれ送信または受信トラフィックに設定すると、ほとんどのトラフィックが無応答の単方向ビデオ ブロードキャスト ストリームであるような動画ストリーミングなどのアプリケーションで、トラフィック容量が 2 倍になります。

単一方向イーサネットの設定



(注)

ポートの UniDirectional Link Detection (UDLD; 単一方向リンク検出)を自動的にディセーブルにするには、単一方向イーサネットをノンブロッキング ギガポートで設定する必要があります。

単一方向イーサネットをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config) # interface {vlan vlan_ID {fastethernet gigabitethernet tengigabitethernet} slot/interface Port-channel number}	設定するインターフェイスを選択します。
ステップ 2	Switch(config-if)# [no] unidirectional {send-only receive-only}	単一方向イーサネットをイネーブルにします。 単一方向イーサネットをディセーブルにするに
		は、no キーワードを使用します。
ステップ 3	Switch(config-if)# end	コンフィギュレーション モードを終了します。
ステップ 4	Switch# show interface {vlan vlan_ID {fastethernet gigabitethernet tengigabitethernet} slot/interface} unidirectional	設定を確認します。

次に、インターフェイス GigabitEthernet 1/1 でトラフィックを単方向で送信するように設定する例を示します。

Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config) # interface gigabitethernet 1/1
Switch(config-if) # unidirectional send-only
Switch(config-if) # end

Warning!

Enable 12 port unidirectional mode will automatically disable port udld. You must manually ensure that the unidirectional link does not create a spanning tree loop in the network.

Enable 13 port unidirectional mode will automatically disable ip routing on the port. You must manually configure static ip route and arp entry in order to route ip traffic.

次に、インターフェイス GigabitEthernet 1/1 でトラフィックを単方向で受信するように設定する例を示します。

Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# unidrectional receive-only
Switch(config-if)# end

Warning!

Enable 12 port unidirectional mode will automatically disable port udld. You must manually ensure that the unidirectional link does not create a spanning tree loop in the network.

Enable 13 port unidirectional mode will automatically disable ip routing on the port. You must manually configure static ip route and arp entry in order to route ip traffic.

次に、設定を確認する例を示します。

Switch>show interface gigabitethernet 1/1 unidirectional

show interface gigabitethernet 1/1 unidirectional
Unidirectional configuration mode: send only
CDP neighbour unidirectional configuration mode: receive only

次に、インターフェイス GigabitEthernet 1/1 上で単一方向イーサネットをディセーブルにする例を示します。

Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# no unidirectional
Switch(config-if)# end

次に、単一方向イーサネットをサポートしないポートに show interface コマンドを発行した場合の 結果を示します。

Switch#show interface f6/1 unidirectional Unidirectional Ethernet is not supported on FastEthernet6/1

単一方向イーサネットの設定



CHAPTER

31

IP マルチキャストの設定

この章では、Catalyst 4500 シリーズ スイッチ上での IP マルチキャスト ルーティングについて説明します。IP マルチキャスト ルーティングの設定手順および設定例も示します。



この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univered/cc/td/doc/product/software/ios122sr/cr/index.htm



IP マルチキャストの詳細については、次の URL のディスカッションを参照してください。

http://www.cisco.com/univered/cc/td/doc/product/software/ios123/123cgcr/fipr_c/ipcpt3/

この章の主な内容は、次のとおりです。

- IP マルチキャストの概要 (p.31-2)
- IP マルチキャスト ルーティングの設定 (p.31-14)
- IP マルチキャスト ルーティングのモニタリングおよびメンテナンス (p.31-17)
- 設定例 (p.31-24)

IP マルチキャストの概要

ここでは、次の内容について説明します。

- IP マルチキャスト プロトコル (p.31-3)
- Catalyst 4500 シリーズ スイッチ上での IP マルチキャスト (p.31-5)
- サポートされない機能(p.31-13)

IP 通信の一端である IP ユニキャストでは、送信元 IP ホストが特定の宛先 IP ホストにパケットを送信します。この場合、IP パケットに指定される宛先アドレスは、IP ネットワーク上で一意に識別される単一ホストのアドレスです。これらの IP パケットは、ネットワーク上の送信元ホストから、一連のルータによって宛先ホストに転送されます。送信元と宛先間のパス上の各ポイントでは、ルータがユニキャスト ルーティング テーブルを使用して、パケットの IP 宛先アドレスに基づきユニキャスト転送先を決定します。

IP 通信で IP ユニキャストの対極にある IP ブロードキャストでは、送信元ホストはネットワーク セグメント上のすべてのホストにパケットを送信します。IP ブロードキャスト パケットの宛先アドレスでは、宛先 IP アドレスのホスト部分がすべて 1 に設定され、ネットワーク部分がサブネットのアドレスに設定されています。一連の IP ホスト (ルータを含む) は、宛先アドレスとして IP ブロードキャスト アドレスを指定されたパケットが、サブネット上のすべての IP ホスト向けであることを認識しています。特に設定しないかぎり、ルータは IP ブロードキャスト パケットを転送しないので、一般的に IP ブロードキャスト通信はローカル サブネットに限定されます。

IP マルチキャストは、IP ユニキャスト通信と IP ブロードキャスト通信の中間に位置します。IP マルチキャスト通信によって、ホストは IP ネットワーク上の任意の場所にあるホストのグループに IP パケットを送信します。IP マルチキャスト通信では、特定のグループに情報を送信するために、IP マルチキャスト グループ アドレスという特殊な形式の IP 宛先アドレスを使用します。IP マルチキャスト グループ アドレスは、パケットの IP 宛先アドレス フィールドに指定されます。

IP 情報をマルチキャストするには、レイヤ 3 スイッチおよびルータが、IP マルチキャスト グループのメンバに接続するすべての出力インターフェイスに、着信 IP パケットを転送する必要があります。Catalyst 4000 ファミリ スイッチ上のマルチキャスト プロセスでは、Integrated Switching Engineでパケットが複製されて適切な出力インターフェイスに転送され、マルチキャスト グループの各メンバに送信されます。

IP マルチキャストはビデオ会議とほとんど同じものと見られがちです。ネットワークに初めて導入する IP マルチキャスト アプリケーションは、多くの場合ビデオ会議ですが、ビデオは企業のビジネス モデルに付加価値をもたらす、さまざまな IP マルチキャスト アプリケーションの 1 つに過ぎません。生産性の向上につながるこのほかの IP マルチキャスト アプリケーションとしては、マルチメディア会議、データ複製、リアルタイム データ マルチキャスト、シミュレーション アプリケーションなどがあります。

ここでは、次の内容について説明します。

- IP マルチキャスト プロトコル (p.31-3)
- Catalyst 4500 シリーズ スイッチ上での IP マルチキャスト (p.31-5)
- サポートされない機能(p.31-13)

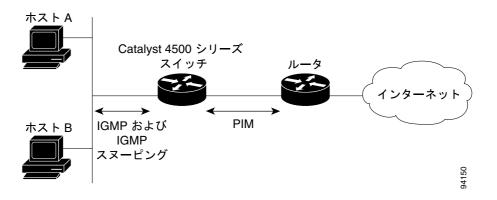
IP マルチキャスト プロトコル

Catalyst 4000 ファミリ スイッチでは、主に次のプロトコルを使用して IP マルチキャスト ルーティングを実行します。

- Internet Group Management Protocol (IGMP; インターネット グループ管理プロトコル)
- Protocol Independent Multicast (PIM)
- IGMP スヌーピングおよび Cisco Group Management Protocol (CGMP)

図 31-1 に、IP マルチキャスト環境でこれらのプロトコルが動作する箇所を示します。

図 31-1 IP マルチキャスト ルーティング プロトコル



IGMP

IP マルチキャスト ホストは IGMP メッセージを使用して、ローカルのレイヤ 3 スイッチまたはルータに要求を送信し、特定のマルチキャスト グループに加入して、マルチキャスト トラフィックの 受信を開始します。IGMPv2 の一部の拡張機能を使用すると、IP ホストはレイヤ 3 スイッチまたは ルータに対し、IP マルチキャスト グループを脱退してマルチキャスト グループ トラフィックを受信しないように求める要求も送信します。

レイヤ 3 スイッチまたはルータは、IGMP によって得た情報を使用して、マルチキャスト グループメンバシップのリストをインターフェイス単位で維持します。インターフェイス上で少なくとも 1 つのホストが、マルチキャスト グループ トラフィックを受信するための IGMP 要求を送信しているかぎり、そのインターフェイスのマルチキャスト グループ メンバシップはアクティブです。

PIM

PIM が プロトコルに依存しない 理由は、使用されている任意のユニキャスト ルーティング プロトコルを利用してルーティング テーブルへの書き込みを行い (Enhanced Interior Gateway Routing Protocol [EIGRP]、Open Shortest Path First [OSPF]、Border Gateway Protocol [BGP]、およびスタティック ルートを含む)、IP マルチキャストをサポートするからです。PIM はさらに、完全に独立したマルチキャスト ルーティング テーブルを作成する代わりに、ユニキャスト ルーティング テーブルを使用して Reverse Path Forwarding (RPF) チェック機能を実行します。PIM は、他のルーティング プロトコルが行うような、ルータ間でのマルチキャスト ルーティング アップデートの送受信は行いません。

PIM 稠密モード

PIM 稠密モード (PIM-DM) は、プッシュモデルを使用してネットワークのすべての部分にマルチキャストトラフィックをフラッディングさせます。PIM-DM は、LAN TV や企業情報または財務情報ブロードキャストなど、大部分の LAN でマルチキャストの受信が必要とされるネットワークでの使用を目的としています。ネットワーク上のすべてのサブネットにアクティブな受信者が存在する場合、効率的な配信メカニズムになります。

PIM 希薄モード

PIM 希薄モード(PIM-SM)は、プルモデルを使用してマルチキャスト トラフィックを配信します。明示的にデータを要求していて、かつアクティブな受信者のいるネットワークだけに、トラフィックが転送されます。PIM-SM は、デスクトップ ビデオ会議や企業コンピューティングなど、少数の受信者がそれぞれ異なるマルチキャストを一般に同時使用するネットワークでの使用を目的としています。

PIM 稠密モードおよび PIM 希薄モードの詳細については、次の URL を参照してください。 http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcpt3

IGMP スヌーピングおよび CGMP

IGMP スヌーピングは、レイヤ 2 スイッチング環境でのマルチキャストに使用します。IGMP スヌーピングを使用する場合、レイヤ 3 スイッチまたはルータは、ホストとルータ間で転送される IGMP パケットのレイヤ 3 情報を検証します。スイッチが特定のマルチキャスト グループのホストから IGMP Host Report を受信すると、スイッチはそのホストのポート番号を対応するマルチキャストテーブル エントリに追加します。スイッチがホストから IGMP Leave Group メッセージを受信すると、スイッチはテーブル エントリからそのホストのポートを削除します。

IGMP 制御メッセージはマルチキャストパケットとして送信されるので、レイヤ 2 ヘッダーのみが検証される場合は、マルチキャストデータと区別できません。IGMP スヌーピングが稼働しているスイッチは、すべてのマルチキャストデータパケットについて、関連する IGMP 制御情報が含まれていないかどうかを調べます。低速の CPU を搭載したローエンドのスイッチに IGMP スヌーピングを実装すると、データを高速で送信する場合、パフォーマンスに重大な影響が出る可能性があります。Catalyst 4500 シリーズ スイッチでは、IGMP スヌーピングがフォワーディング Application Specific Integrated Circuit (ASIC; 特定用途向け集積回路)で実装されているので、転送速度に影響が出ることはありません。



Catalyst 4000 ファミリスイッチは、IGMP スヌーピングをサポートしていないスイッチ (Supervisor Engine I および Supervisor Engine II を搭載した Catalyst 4500 ファミリスイッチなど)の CGMP サーバとして動作します。スイッチを CGMP クライアントとして設定することはできません。 Catalyst 4000 ファミリスイッチをクライアントとして設定するには、IGMP スヌーピングを使用します。

CGMP は、Catalyst スイッチがシスコ ルータの IGMP 情報を活用してレイヤ 2 で転送先の決定を行うための、シスコの独自仕様プロトコルです。CGMP は、マルチキャスト ルータおよびレイヤ 2 スイッチ上で設定します。その結果、トラフィックを要求したホストのある Catalyst スイッチポートだけに、IP マルチキャスト トラフィックが配信されます。トラフィックを明示的に要求していないスイッチポートは、トラフィックを受信しません。

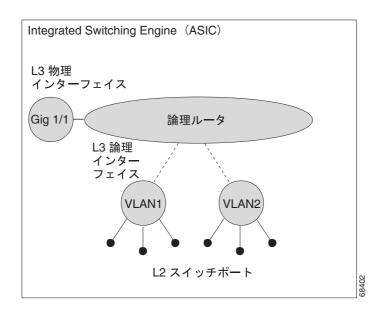
Catalyst 4500 シリーズ スイッチ上での IP マルチキャスト

Catalyst 4000 ファミリ スイッチは、レイヤ 2 でイーサネット ブリッジング、レイヤ 3 で IP ルーティングを行う ASIC ベースの Integrated Switching Engine をサポートしています。この ASIC はパケット転送専用に設計されているので、Access Control List (ACL; アクセス コントロール リスト) および QoS (Quality Of Service) をイネーブルにした状態で、Integrated Switching Engine ハードウェアにより非常に高いパフォーマンスを実現します。ハードウェアによるワイヤスピードでの転送は、例外パケットを処理するように設計された CPU サブシステム ソフトウェアよりもきわめて高速となります。

Integrated Switching Engine ハードウェアは、VLAN(仮想 LAN)間ルーティング用のインターフェイスおよびレイヤ 2 ブリッジング用のスイッチポートをサポートしています。また、ホスト、スイッチ、またはルータとの接続を設定できる物理レイヤ 3 インターフェイスともなります。

図 31-2 に、Integrated Switching Engine ハードウェアでのレイヤ 2 およびレイヤ 3 フォワーディングの概念図を示します。

図 31-2 ハードウェアでのレイヤ 2 およびレイヤ 3 フォワーディングの概念図



ここでは、次の内容について説明します。

- CEF、MFIB、およびレイヤ 2 フォワーディング (p.31-6)
- IP マルチキャスト テーブル (p.31-8)
- ハードウェアおよびソフトウェアによる転送(p.31-9)
- 非 RPF トラフィック (p.31-10)
- マルチキャスト高速ドロップ (p.31-11)
- MFIB (p.31-12)
- S/M,224/4 (p.31-13)

CEF、MFIB、およびレイヤ2フォワーディング

Catalyst 4000 ファミリ スイッチに実装された IP マルチキャストは、中央集中型 Cisco Express Forwarding (CEF; シスコ エクスプレス フォワーディング) の拡張機能です。CEF は、上位レイヤ のユニキャスト ルーティング テーブル(BGP、OSPF、EIGRP などのユニキャスト ルーティング プロトコルによって作成される) から情報を抽出し、この情報をハードウェア Forwarding Information Base (FIB; 転送情報ベース) にロードします。FIB のユニキャスト ルートを使用すると、上位レイヤのルーティング テーブルでルートが変更された場合でも、ハードウェア ルーティング ステートの 1 つのルートを変更するだけです。ハードウェアでユニキャスト パケットを転送するために、Integrated Switching Engine は Ternary CAM (TCAM) から送信元および宛先ルートを検索し、ハードウェア FIB から隣接インデックスを取り出して、ハードウェア ネイバー テーブル関係からレイヤ 2 リライト情報およびネクストホップ アドレスを取得します。

Multicast Forwarding Information Base (MFIB) サプシステムは、ユニキャスト CEF のマルチキャスト版です。この MFIB サプシステムは、PIM および IGMP によって作成されるマルチキャストルートを抽出し、ハードウェア転送のためのプロトコル独立フォーマットにします。 MFIB サプシステムは、プロトコル固有の情報を削除し、必要なフォワーディング情報だけを残します。 MFIB テーブルの各エントリは、(S,G)または(*,G)ルート、入力 RPF VLAN、およびレイヤ 3 出力インターフェイスのリストで構成されます。 MFIB サプシステムは、プラットフォーム依存の管理ソフトウェアと連携して、このマルチキャスト ルーティング情報をハードウェア FIB およびハードウェア Multicast Expansion Table (MET) にロードします。

Catalyst 4000 ファミリ スイッチは、レイヤ 3 ルーティングとレイヤ 2 ブリッジングを同時に実行します。1 つの VLAN インターフェイスに複数のレイヤ 2 スイッチポートを設定できます。マルチキャスト パケットを転送すべき出力スイッチポートの集合を判別するため、Supervisor Engine III はレイヤ 3 の MFIB 情報をレイヤ 2 のフォワーディング情報と組み合わせ、ハードウェア MET に保存してパケット複製を行います。

図 31-3 に、Catalyst 4000 ファミリ スイッチがどのようにユニキャスト ルーティング、マルチキャスト ルーティング、およびレイヤ 2 ブリッジング情報を組み合わせ、ハードウェアで転送を実行するかを示します。

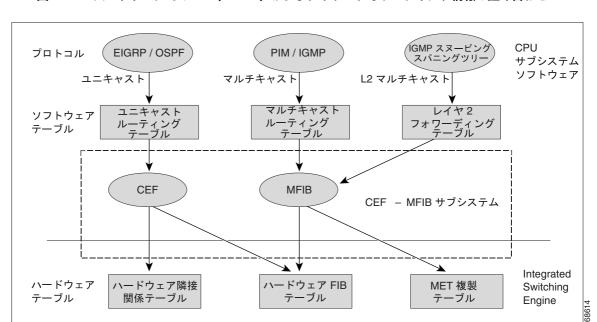


図 31-3 ハードウェアでの CEF、MFIB、およびレイヤ 2 フォワーディング情報の組み合わせ

MFIB ルートは、CEF ユニキャスト ルートと同様にレイヤ 3 であるため、該当するレイヤ 2 情報と 結合する必要があります。MFIB ルートの例を示します。

(*,224.1.2.3)
RPF interface is Vlan3
Output Interfaces are:
Vlan 1
Vlan 2

ルート(*,224.1.2.3)がハードウェア FIB テーブルにロードされ、出力インターフェイスのリストが MET にロードされます。出力インターフェイスのリストへのポインタ、MET インデックス、および RPF インターフェイスも、(*,224.1.2.3) ルートとともにハードウェア FIB にロードされます。ハードウェアにこの情報をロードすることで、レイヤ 2 情報との結合を開始できるようになります。VLAN 1 上の出力インターフェイスについて、Integrated Switching Engine は VLAN 1 上でスパニングツリー フォワーディング ステートにあるすべてのスイッチポートにパケットを送信する必要があります。VLAN 2 についても同じプロセスが適用されます。VLAN 2 のスイッチポートの集合を判別するには、レイヤ 2 フォワーディング テーブルが使用されます。

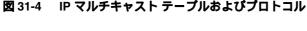
ハードウェアがパケットをルーティングする場合、すべての出力インターフェイスのすべてのスイッチポートにパケットを送信するだけでなく、ハードウェアは入力 VLAN の(パケットが到着したスイッチポートを除く)すべてのスイッチポートにも、パケットを送信します。たとえば、VLAN 3 に 2 つのスイッチポート Gig 3/1 および Gig 3/2 があると仮定します。Gig 3/1 上のホストがマルチキャスト パケットを送信すると、Gig 3/2 上のホストもそのパケットを受信しなければならない場合があります。Gig 3/2 上のホストにマルチキャスト パケットを送信するには、MET にロードされるポートセットに入力 VLAN のすべてのスイッチポートを追加する必要があります。

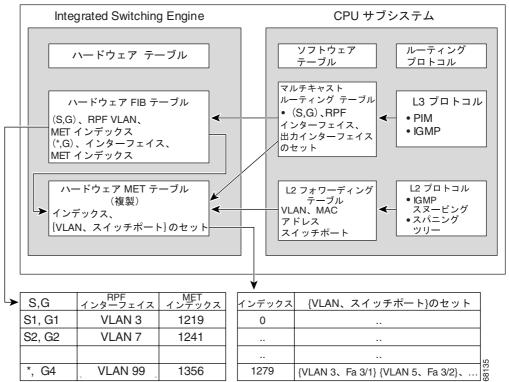
VLAN 1 に 1/1 および 1/2、VLAN 2 に 2/1 および 2/2、VLAN 3 に 3/1 および 3/2 が含まれていれば、このルート用の MET チェーンには、スイッチポート 1/1、1/2、2/1、2/2、3/1、および 3/2 が含まれることになります。

IGMP スヌーピングがオンの場合、パケットは VLAN 2 のすべての出力スイッチポートに転送されるとは限りません。IGMP スヌーピングによって、グループ メンバまたはルータが存在すると判断されたスイッチポートだけに、パケットが転送されます。たとえば、VLAN 1 で IGMP スヌーピングがイネーブルで、IGMP スヌーピングによってポート 1/2 のみにグループ メンバが存在すると判断された場合、MET チェーンには、スイッチポート 1/1、1/2、2/1、2/2、3/1、および 3/2 が含まれることになります。

IP マルチキャスト テーブル

図 31-4 に、Catalyst 4000 ファミリ スイッチがハードウェアで IP マルチキャスト パケットを転送する目的で使用する主なデータ構造を示します。





Integrated Switching Engine は、個々の IP マルチキャスト ルートを識別する目的で、ハードウェア FIB テープルを維持します。各エントリは、宛先グループの IP アドレスおよびオプションの送信元 IP アドレスで構成されます。マルチキャスト トラフィックは、主に (S,G) および (*,G) の 2 種類のルート上を流れます。(S,G) ルートは、マルチキャスト送信元の IP アドレスと、マルチキャスト グループ宛先の IP アドレスに基づいて、送信元からグループへ流れます。(*,G) ルートのトラフィックは、PIM RP からグループ G のすべての受信者へ流れます。(*,G) ルートを使用するのは、希薄モード グループだけです。Integrated Switching Engine ハードウェアには、合計 128,000 のルート用のスペースが準備されています。これらがユニキャストルート、マルチキャストルート、およびマルチキャスト高速ドロップ エントリによって共有されます。

出力インターフェイスのリストは、MET に保存されます。MET には、最大 32,000 の出力インターフェイス リスト用のスペースがあります。MET リソースは、レイヤ 3 マルチキャスト ルートおよびレイヤ 2 マルチキャスト エントリによって共有されます。ハードウェアで使用できる出力インターフェイス リストの実際の数は、設定によって異なります。マルチキャスト ルートの総数が32,000 を超えると、Integrated Switching Engine によってマルチキャスト パケットをスイッチングできなくなる場合があります。そのパケットは、CPU サブシステムによってきわめて低い速度で転送されることになります。

ハードウェアおよびソフトウェアによる転送

Integrated Switching Engine は通常、パケットをハードウェアで非常に高速で転送します。CPU サブシステムは、例外パケットをソフトウェアで転送します。Integrated Switching Engine が大部分のパケットをハードウェアで転送していることは、統計レポートからわかります。

図31-5に、ハードウェアとソフトウェアの転送コンポーネントの概念を示します。

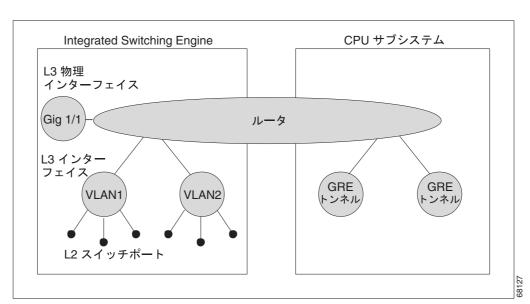


図 31-5 ハードウェアおよびソフトウェアの転送コンポーネント

Integrated Switching Engine は、通常の動作モードでは、ハードウェアで VLAN 間ルーティングを実行します。CPU サブシステムは、ソフトウェアによる転送のために、Generic Routing Encapsulation (GRE; 総称ルーティング カプセル化) トンネルをサポートしています。

複製は、パケットの1コピーを送信する代わりに、パケットを複製して複数のコピーを送信する転送の一種です。レイヤ3で複製が行われるのは、マルチキャストパケットに限られます。ユニキャストパケットが複数のレイヤ3インターフェイス用に複製されることはありません。IP マルチキャスト動作では、着信した IP マルチキャストパケットごとに、そのパケットの多くの複製が送信されます。

IP マルチキャスト パケットを伝送するルートのタイプは、次のとおりです。

- ハードウェア ルート
- ソフトウェア ルート
- 部分的なルート

ハードウェア ルートは、Integrated Switching Engine ハードウェアがパケットのすべての複製を転送する場合に発生します。ソフトウェア ルートは、CPU サブシステム ソフトウェアがパケットのすべての複製を転送する場合に発生します。部分的なルートは、Integrated Switching Engine が一部の複製をハードウェアで転送し、CPU サブシステムが一部の複製をソフトウェアで転送する場合に発生します。

部分的なルート



(注)

以下に記載する条件が成立する場合、CPU サブシステム ソフトウェアによって複製が転送されますが、ハードウェアによる複製の転送パフォーマンスに影響はありません。

あるルートに対するパケットの複製の一部が CPU サブシステムによって転送される条件は、次のとおりです。

- ip igmp join-group コマンドを使用して、マルチキャスト送信元の RPF インターフェイス上の IP マルチキャスト グループのメンバとしてスイッチを設定している場合
- スイッチが PIM 希薄モードの送信元へのファースト ホップである場合。この場合、スイッチは RP に PIM Register メッセージを送信する必要があります。

ソフトウェア ルート



(注)

RPF インターフェイスまたは出力インターフェイスの設定について次の条件が 1 つでも成立する と、出力のすべての複製はソフトウェアで実行されます。

あるルートに対するパケットの複製の一部が CPU サブシステム ソフトウェアによって転送される条件は、次のとおりです。

- インターフェイスがマルチキャスト ヘルパーを使用して設定されている場合
- インターフェイスが GRE トンネルまたは Distance Vector Multicast Routing Protocol (DVMRP) トンネルである場合
- インターフェイスが Advanced Research Products Agency (ARPA) 以外のカプセル化を使用している場合

次のパケットは、常にソフトウェアによって転送されます。

- 224.0.0.* (* は 0 ~ 255) の範囲のマルチキャスト グループに送信されるパケット。この範囲は、ルーティング プロトコルが使用します。レイヤ 3 スイッチングでは、この範囲以外のすべてのマルチキャスト グループ アドレスがサポートされています。
- IP オプション付きのパケット

非 RPF トラフィック

RPF チェックに失敗したトラフィックを、非 RPF トラフィックといいます。Integrated Switching Engine は、非 RPF トラフィックをフィルタリング (持続的にドロップ) するか、またはレート制限して転送します。

複数のレイヤ3スイッチまたはルータが同一のLAN セグメントに接続されている冗長な構成で、送信元から発信インターフェイス上の受信側へマルチキャスト トラフィックを転送するのは、1 台の装置だけです。 図 31-6 に、一般的なネットワーク構成で非 RPF トラフィックが発生した状況を示します。

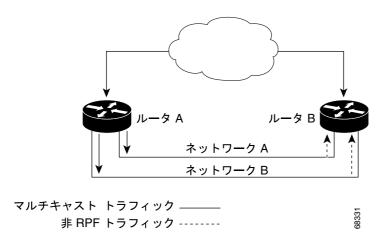


図 31-6 スタブ ネットワークにおける冗長マルチキャスト ルータ構成

この種のトポロジでは、PIM DR 指定ルータ (PIM DR) であるルータ A だけが共通の VLAN にデータを転送します。ルータ B は転送されたマルチキャスト トラフィックを受信しますが、このトラフィックをドロップします。不正なインターフェイスでこのトラフィックが着信したので、RPF チェックに失敗するためです。このように RPF チェックに失敗するトラフィックを、非 RPF トラフィックといいます。

マルチキャスト高速ドロップ

PIM-SM、PIM-DM などの IP マルチキャスト プロトコルでは、(S,G) または (*,G) ルートごとに、対応する着信インターフェイスがあります。このインターフェイスを、RPF インターフェイスといいます。予測される RPF インターフェイスとは異なるインターフェイスにパケットが到着することもあります。その場合、PIM によってパケットに特殊なプロトコル処理を行うために、そのパケットを CPU サブシステム ソフトウェアに転送する必要があります。PIM が実行する特殊なプロトコル処理の例としては、PIM アサートプロトコルがあります。

デフォルトでは、Integrated Switching Engine ハードウェアは、非 RPF インターフェイスに着信したすべてのパケットを CPU サブシステム ソフトウェアに送信します。ただし、これらの非 RPF パケットはほとんどの場合、マルチキャスト ルーティング プロトコルに必要ではないので、多くの場合、ソフトウェアによる処理は不要です。何の処置も行わなければ、ソフトウェアに送信される非 RPF パケットのため、CPU に負荷がかかる恐れがあります。

MFIB 高速ドロップをイネーブルまたはディセーブルにするには、ip mfib fastdrop コマンドを使用します。

この問題を回避するため、CPU サブシステム ソフトウェアは、RPF に失敗したパケットのうち、スイッチ上で稼働している PIM プロトコルが必要としないパケットを受信した時点で、高速ドロップエントリをハードウェアにロードします。高速ドロップエントリは、(S,G,着信インターフェイス)によって表されます。高速ドロップエントリに一致するパケットは、入力 VLAN でブリッジングされますが、ソフトウェアには送信されません。したがって、CPU サブシステム ソフトウェアがこれらの RPF エラーを処理し、必ずしも過負荷になるものではありません。

リンクのダウン、ユニキャストルーティング テーブルの変更などのプロトコル イベントによって、安全に高速ドロップが可能なパケットの集合に影響が出ることがあります。以前は高速ドロップを行っても問題のなかったパケットを、トポロジの変更後、PIM ソフトウェアに処理させるため、CPU サブシステム ソフトウェアに転送する必要があります。CPU サブシステム ソフトウェアは、プロトコル イベントに応答して高速ドロップ エントリのフラッシュを行い、IOS の PIM コードが必要な RPF エラーをすべて処理できるようにします。

一部のトポロジでは、RPF エラーが繰り返し発生する可能性があるので、ハードウェアにおける高速ドロップ エントリの使用が特に重要になります。高速ドロップ エントリがなければ、処理する必要のない RPF エラー パケットによって CPU が過負荷になる可能性があります。

MFIB

MFIB サブシステムは、Catalyst 4000 ファミリ スイッチ上の Integrated Switching Engine ハードウェアの IP マルチキャスト ルーティングをサポートします。MFIB は、論理的には CPU サブシステムソフトウェアの IP マルチキャスト ルーティング プロトコル (PIM、IGMP、MSDP、MBGP、および DVMRP)と、ハードウェアで IP マルチキャスト ルーティングを管理するためのプラットフォーム固有のコードとの中間に存在します。MFIB は、マルチキャスト ルーティング プロトコルによって作成されたルーティング テーブル情報を、Integrated Switching Engine ハードウェアが効率的に処理して転送に使用可能な、簡易なフォーマットに変換します。

マルチキャスト ルーティング テーブルの情報を表示するには、show ip mroute コマンドを使用します。 MFIB テーブルの情報を表示するには、show ip mfib コマンドを使用します。



Supervisor Engine 6-E システムでは、show ip mfib コマンドはハードウェア カウンタを出力しません。

MFIB テーブルには、IP マルチキャスト ルートの集合が含まれます。IP マルチキャスト ルートには、(S,G) ルート、(*,G) ルートなど、いくつかのタイプがあります。MFIB テーブルの各ルートに、オプションの 1 つまたは複数のフラグを対応付けることができます。ルート フラグは、ルートに一致するパケットの転送方法を指示します。たとえば、MFIB ルートに付けられた Internal Copy (IC) フラグは、スイッチ上のプロセスがパケットのコピーを受信する必要があることを意味します。MFIB ルートに対応付けできるフラグは、次のとおりです。

- Internal Copy (IC) フラグ ルータ上のプロセスが、特定のルートに一致するすべてのパケットのコピーを受信する必要がある場合に設定します。
- Signalling (S) フラグ このルートに一致するパケットを受信したときに、プロセスに通知する必要がある場合に設定します。 シグナリング インターフェイス上でのパケット受信に応答して、プロトコル コードが MFIB ステートを更新するなどの動作を行うことが考えられます。
- Connected(C)フラグ このフラグを MFIB ルートに設定した場合、直接接続されたホストによってルートに送信されたパケットだけをプロトコル プロセスに通知する必要があるという点を除き、Signalling(S)フラグと同じ意味を持ちます。

ルートには、1 つまたは複数のインターフェイスに対応するオプションのフラグを設定することもできます。たとえば、 $VLAN\ 1$ に関するフラグを設定した (S,G) ルートは、 $VLAN\ 1$ に着信するパケットの取り扱いを指示するとともに、このルートに一致するパケットを $VLAN\ 1$ に転送すべきかどうかも示します。MFIB でサポートされるインターフェイス単位のフラグは、次のとおりです。

- Accepting(A) マルチキャスト ルーティングで RPF インターフェイスであることが明らかな インターフェイスに設定します。Accepting (A) をマークされたインターフェイスに着信した パケットは、すべての Forwarding (F) インターフェイスに転送されます。
- Forwarding(F) 上記のように、Accepting(A)フラグと組み合わせて使用します。Forwarding インターフェイスの集合は、マルチキャスト olist (output interface list) と呼ばれるものを形成します。
- Signalling(S) このインターフェイスにパケットが着信したとき、IOS の何らかのマルチキャスト ルーティング プロトコル プロセスに通知する必要がある場合に設定します。

• Not Platform fast-switched (NP) Forwarding (F) フラグと組み合わせて使用します。出力インターフェイスをプラットフォームによって高速スイッチングできない場合に、Forwarding インターフェイスには Not Platform fast-switched というマークも付けられます。NP フラグは通常、ハードウェアで Forwarding インターフェイスをルーティングできず、ソフトウェア転送が必要な場合に使用されます。たとえば、Catalyst 4000 ファミリ スイッチ トンネル インターフェイスはハードウェア スイッチングされないので、これらのインターフェイスには NP フラグが付けられます。ルートに対応付けられた NP インターフェイスがある場合、Accepting インターフェイスに着信するパケットごとに、パケットのコピーが 1 つずつソフトウェア転送パスに送信され、ハードウェア スイッチングされなかったインターフェイス用にパケットがソフトウェアで複製されます。



PIM-SM ルーティングを使用している場合、MFIB ルートには、PimTunnel [1.2.3.4] などのインターフェイスが含まれる場合があります。このインターフェイスは、パケットが特定の宛先アドレスに対してトンネリングされていることを表すために、MFIB サブシステムが作成する仮想インターフェイスです。PimTunnel インターフェイスは、通常の show interface コマンドでは表示できません。

S/M,224/4

MFIB では、マルチキャスト対応のインターフェイスごとに (S/M,224/4)エントリが作成されます。このエントリによって、直接接続されたネイバーから送信されたすべてのパケットが、PIM-SM RPに Register カプセル化されるようになります。一般に、PIM-SM によって (S,G)ルートが確立されるまでの間、ごく少数のパケットだけが (S/M,224/4)ルートを使用して転送されます。

たとえば、IP アドレス 10.0.0.1 およびネットマスク 255.0.0.0 のインターフェイスで、送信元アドレスがクラス A ネットワーク 10 に所属する IP マルチキャスト パケットにすべて一致するルートが作成されると仮定します。このルートは、慣例的なサブネット / マスク長の表記では(10/8,224/4)と記述されます。インターフェイスに複数の IP アドレスが割り当てられている場合には、これらの IP アドレスごとに 1 つずつルートが作成されます。

サポートされない機能

このリリースでは、次の IP マルチキャスト機能はサポートされません。

- マルチキャスト グループへの伝送速度の制御
- 等コスト パス間での IP マルチキャスト トラフィックの負荷分割

IP マルチキャスト ルーティングの設定

ここでは、IP マルチキャスト ルーティングの設定作業について説明します。

- IP マルチキャスト ルーティングのデフォルト設定 (p.31-14)
- IP マルチキャスト ルーティングのイネーブル化 (p.31-15)
- インターフェイス上での PIM のイネーブル化 (p.31-15)

Auto-RP、PIM バージョン 2、および IP マルチキャスト スタティック ルートなどの IP マルチキャスト ルーティングの詳細については、 $^{\mathbb{C}}$ Cisco IOS IP and IP Routing Configuration Guide $_{\mathbb{Z}}$ Release 12.3 を参照してください。

IP マルチキャスト ルーティングのデフォルト設定

表 31-1 に、IP マルチキャストのデフォルト設定を示します。

表 31-1 IP マルチキャストのデフォルト設定

機能	デフォルト値		
RPF のレート制限	グローバルでイネーブル		
IP マルチキャスト ルーティング	グローバルでディセーブル ▲		
	(注) IP マルチキャスト ルーティングがディセーブルになっている場合、IP マルチキャスト トラフィック データは Catalyst 4000 ファミリ スイッチによって転送されません。ただし、IP マルチキャスト制御トラフィックは引き続き処理および転送されます。したがって、IP マルチキャスト ルーティングをディセーブルにしても、IP マルチキャスト ルートはルーティング テーブルに残ります。		
PIM	すべてのインターフェイス上でディセーブル		
IGMP スヌーピング	すべての VLAN インターフェイス上でイネーブル		
	特定のインターフェイス上で IGMP スヌーピングをディセーブルにすると、すべての出力ポートが Integrated Switching Engine によって転送されます。入力 VLAN インターフェイス上で IGMP スヌーピングをディセーブルにすると、そのインターフェイスに関連するマルチキャストパケットは、VLAN上のすべてのフォワーディング スイッチポートに送信されます。		



Source Specific Multicast および IGMPv3 がサポートされています。

IGMPv3 および IGMP を備えた Source Specific Multicast の詳細については、次の URL を参照してください。

 $http://www.cisco.com/univered/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcpt3/1cfssm.htm$

IP マルチキャスト ルーティングのイネーブル化

IP マルチキャスト ルーティングをイネーブルにすると、Catalyst 4000 ファミリ スイッチでマルチキャスト パケットを転送できるようになります。ルータ上で IP マルチキャスト ルーティングをイネーブルにするには、グローバル コンフィギュレーション モードで次の作業を行います。

コマンド	目的
Switch(config)# ip multicast-routing	IPマルチキャストルーティングをイネーブルにします。

インターフェイス上での PIM のイネーブル化

インターフェイス上で PIM をイネーブルにすると、そのインターフェイス上で IGMP 動作もイネーブルになります。インターフェイスは、稠密モード、希薄モード、または 希薄 / 稠密モードのいずれかに設定できます。これらのモードは、レイヤ 3 スイッチまたはルータによるマルチキャストルーティング テーブルの書き込み方法と、レイヤ 3 スイッチまたはルータが直接接続された LAN から受信したマルチキャスト パケットの転送方法を決定します。インターフェイスで IP マルチキャスト ルーティングを実行するには、PIM を上記のモードのいずれかでイネーブルにする必要があります。

マルチキャストルーティング テーブルの書き込みでは、稠密モード インターフェイスは常にテーブルに追加されます。希薄モード インターフェイスは、ダウンストリーム ルータから定期的な Join メッセージを受信した場合、またはインターフェイス上に直接接続されたメンバが存在する場合にかぎり、テーブルに追加されます。LAN から転送する場合、グループが認識している RP があれば、希薄モード動作が行われます。その場合、パケットはカプセル化され、その RP に送信されます。認識している RP がなければ、パケットは稠密モードの方式でフラッディングされます。特定の送信元からのマルチキャスト トラフィックが十分であれば、受信側のファーストホップ ルータがその送信元に Join メッセージを送信し、送信元を基点とするディストリビューション ツリーが構築されます。

デフォルトで設定されるモードはありません。デフォルトでは、インターフェイス上でマルチキャスト ルーティングはディセーブルに設定されています。

稠密モードのイネーブル化

インターフェイス上の PIM を稠密モードに設定するには、次の作業を行います。

コマンド	目的		
Switch(config-if)# ip pim dense-mode	インターフェイス上で稠密モード PIM をイネーブルにします。		

PIM インターフェイスを稠密モードに設定する例については、この章の最後にある「PIM 稠密モードの例」を参照してください。

希薄モードのイネーブル化

インターフェイス上の PIM を希薄モードに設定するには、次の作業を行います。

コマンド	目的
Switch(config-if)# ip pim sparse-mode	インターフェイス上で希薄モード PIM をイネー ブルにします。

PIM インターフェイスを希薄モードに設定する例については、この章の最後にある「PIM 希薄モードの例」を参照してください。

希薄/稠密モードのイネーブル化

ip pim sparse-mode または ip pim dense-mode コマンドを使用すると、インターフェイス全体に希薄モードまたは稠密モードが適用されます。ただし、環境によっては、単一リージョン内の一部のグループについては PIM を希薄モードで実行し、残りのグループについては稠密モードで実行しなければならない場合があります。

稠密モードだけ、または希薄モードだけをイネーブルにするのではなく、希薄/稠密モードをイネーブルにできます。この場合、グループが稠密モードであればインターフェイスは稠密モードとして扱われ、グループが希薄モードであればインターフェイスは希薄モードとして扱われます。グループを希薄グループとして扱い、インターフェイスが希薄/稠密モードである場合には、RPが必要です。

希薄/稠密モードを設定する場合、希薄または稠密の概念はスイッチ上のグループに適用され、ネットワーク管理者は同じ概念をネットワーク全体に適用する必要があります。

希薄 / 稠密モードのもう 1 つの利点は、Auto-RP 情報を稠密モードの方式で配布しながら、ユーザグループのマルチキャスト グループを希薄モードの方式で使用できるという点です。したがって、リーフ ルータ上にデフォルト RP を設定する必要はありません。

インターフェイスが 稠密モードで取り扱われる場合、次のいずれかの条件が満たされると、そのインターフェイスはマルチキャスト ルーティング テーブルの発信インターフェイス リストに追加されます。

- インターフェイス上にメンバまたは DVMRP ネイバーが存在する場合
- PIM ネイバーが存在し、グループがプルーニングされていない場合

インターフェイスが希薄モードで取り扱われる場合、次のいずれかの条件が満たされると、そのインターフェイスはマルチキャスト ルーティング テーブルの発信インターフェイス リストに追加されます。

- インターフェイス上にメンバまたは DVMRP ネイバーが存在する場合
- インターフェイス上の PIM ネイバーが明示的な Join メッセージを受信している場合

PIM がグループと同じモードで動作できるようにするには、次の作業を行います。

コマンド	目的
Switch(config-if)# ip pim sparse-dense-mode	PIM がグループに応じて、希薄モードまたは 稠密モードのいずれかで動作できるようにし ます。

IP マルチキャスト ルーティングのモニタリングおよびメンテナンス

特定のキャッシュ、テーブル、またはデータベースの内容をすべて削除できます。さらに、特定の統計情報を表示することもできます。ここでは、IP マルチキャストのモニタリングおよびメンテナンス方法について説明します。

- システムおよびネットワーク統計情報の表示 (p.31-17)
- マルチキャスト ルーティング テーブルの表示 (p.31-18)
- IP MFIB の表示 (p.31-21)
- IP MFIB 高速ドロップの表示 (p.31-22)
- PIM 統計情報の表示 (p.31-22)
- テーブルおよびデータベースの削除 (p.31-23)

システムおよびネットワーク統計情報の表示

IP ルーティング テーブルやデータベースの内容など、特定の統計情報を表示できます。表示された情報に基づいて、リソースの利用状況を調べたり、ネットワーク上で発生した問題を解決できます。また、ノードの到達可能性に関する情報を表示し、使用する装置のパケットがネットワーク上でたどるルーティング パスを明らかにすることもできます。

各種のルーティング統計情報を表示するには、次の作業を行います。

コマンド	目的		
Switch# ping [group-name group-address]	マルチキャスト グループ アドレスに Internet		
	Control Message Protocol (ICMP)エコー要求		
	を送信します。		
Switch# show ip mroute [hostname	IP マルチキャスト ルーティング テーブルの		
<pre>group_number]</pre>	内容を表示します。		
Switch# show ip pim interface [type number]	PIM に設定されているインターフェイスに関		
[count]	する情報を表示します。		
Switch# show ip interface	すべてのインターフェイスについて PIM 情		
	報を表示します。		

マルチキャスト ルーティング テーブルの表示

稠密モードで動作しているルータに関する show ip mroute コマンドの出力例を示します。このコマンドでは、マルチキャスト グループ cbone-audio に関する IP マルチキャスト FIB テーブルの内容が表示されます。

Switch# show ip mroute cbone-audio

```
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned
R - RP-bit set, F - Register flag, T - SPT-bit set
Timers: Uptime/Expires
Interface state: Interface, Next-Hop, State/Mode

(*, 224.0.255.1), uptime 0:57:31, expires 0:02:59, RP is 0.0.0.0, flags: DC
    Incoming interface: Null, RPF neighbor 0.0.0.0, Dvmrp
    Outgoing interface list:
    Ethernet0, Forward/Dense, 0:57:31/0:02:52
    Tunnel0, Forward/Dense, 0:56:55/0:01:28

(198.92.37.100/32, 224.0.255.1), uptime 20:20:00, expires 0:02:55, flags: C
    Incoming interface: Tunnel0, RPF neighbor 10.20.37.33, Dvmrp
    Outgoing interface list:
    Ethernet0, Forward/Dense, 20:20:00/0:02:52
```

次に、希薄モードで動作しているルータに関する show ip mroute コマンドの出力例を示します。

Switch# show ip mroute

```
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned
R - RP-bit set, F - Register flag, T - SPT-bit set
Timers: Uptime/Expires
Interface state: Interface, Next-Hop, State/Mode

(*, 224.0.255.3), uptime 5:29:15, RP is 198.92.37.2, flags: SC
   Incoming interface: Tunnel0, RPF neighbor 10.3.35.1, Dvmrp
   Outgoing interface list:
      Ethernet0, Forward/Sparse, 5:29:15/0:02:57

(198.92.46.0/24, 224.0.255.3), uptime 5:29:15, expires 0:02:59, flags: C
   Incoming interface: Tunnel0, RPF neighbor 10.3.35.1
   Outgoing interface list:
      Ethernet0, Forward/Sparse, 5:29:15/0:02:57
```



ハードウェアで転送されるパケットについては、インターフェイス タイマーは更新されません。エントリタイマーは、約5秒ごとに更新されます。

次に、show ip mroute コマンドに summary キーワードを指定した場合の出力例を示します。

Switch# show ip mroute summary

次に、show ip mroute コマンドに active キーワードを指定した場合の出力例を示します。

Switch# show ip mroute active

```
Active IP Multicast Sources - sending >= 4 kbps

Group: 224.2.127.254, (sdr.cisco.com)
    Source: 146.137.28.69 (mbone.ipd.anl.gov)
        Rate: 1 pps/4 kbps(1sec), 4 kbps(last 1 secs), 4 kbps(life avg)

Group: 224.2.201.241, ACM 97
    Source: 130.129.52.160 (webcast3-e1.acm97.interop.net)
        Rate: 9 pps/93 kbps(1sec), 145 kbps(last 20 secs), 85 kbps(life avg)

Group: 224.2.207.215, ACM 97
    Source: 130.129.52.160 (webcast3-e1.acm97.interop.net)
        Rate: 3 pps/31 kbps(1sec), 63 kbps(last 19 secs), 65 kbps(life avg)
```

Switch# show ip mroute count

次に、show ip mroute コマンドに count キーワードを指定した場合の出力例を示します。

```
IP Multicast Statistics - Group count: 8, Average sources per group: 9.87
Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Group: 224.255.255.255, Source count: 0, Group pkt count: 0
 RP-tree: 0/0/0/0
Group: 224.2.127.253, Source count: 0, Group pkt count: 0
 RP-tree: 0/0/0/0
Group: 224.1.127.255, Source count: 0, Group pkt count: 0
 RP-tree: 0/0/0/0
Group: 224.2.127.254, Source count: 9, Group pkt count: 14
 RP-tree: 0/0/0/0
 Source: 128.2.6.9/32, 2/0/796/0
  Source: 128.32.131.87/32, 1/0/616/0
  Source: 128.125.51.58/32, 1/0/412/0
  Source: 130.207.8.33/32, 1/0/936/0
  Source: 131.243.2.62/32, 1/0/750/0
 Source: 140.173.8.3/32, 1/0/660/0
  Source: 146.137.28.69/32, 1/0/584/0
  Source: 171.69.60.189/32, 4/0/447/0
  Source: 204.162.119.8/32, 2/0/834/0
Group: 224.0.1.40, Source count: 1, Group pkt count: 3606
 RP-tree: 0/0/0/0
  Source: 171.69.214.50/32, 3606/0/48/0, RPF Failed: 1203
Group: 224.2.201.241, Source count: 36, Group pkt count: 54152
 RP-tree: 7/0/108/0
  Source: 13.242.36.83/32, 99/0/123/0
  Source: 36.29.1.3/32, 71/0/110/0
  Source: 128.9.160.96/32, 505/1/106/0
  Source: 128.32.163.170/32, 661/1/88/0
  Source: 128.115.31.26/32, 192/0/118/0
  Source: 128.146.111.45/32, 500/0/87/0
  Source: 128.183.33.134/32, 248/0/119/0
  Source: 128.195.7.62/32, 527/0/118/0
  Source: 128.223.32.25/32, 554/0/105/0
  Source: 128.223.32.151/32, 551/1/125/0
  Source: 128.223.156.117/32, 535/1/114/0
  Source: 128.223.225.21/32, 582/0/114/0
  Source: 129.89.142.50/32, 78/0/127/0
  Source: 129.99.50.14/32, 526/0/118/0
  Source: 130.129.0.13/32, 522/0/95/0
  Source: 130.129.52.160/32, 40839/16/920/161
  Source: 130.129.52.161/32, 476/0/97/0
```



マルチキャスト ルートのバイトおよびパケット統計情報がサポートされるのは、最初の 1024 個のマルチキャスト ルートに限られます。出力インターフェイスの統計情報は維持されません。

Source: 130.221.224.10/32, 456/0/113/0 Source: 132.146.32.108/32, 9/1/112/0

IP MFIB の表示

MFIB のすべてのルート(上位レイヤのルーティング プロトコル データベースには存在しないが、高速スイッチングをさらに高速化するために使用されるルートも含む)を表示できます。これらのルートは、稠密モード転送が使用されている場合でも、MFIB に表示されます。

MFIB の各種のルーティング ルートを表示するには、次の作業のいずれかを行います。

コマンド	目的
Switch# show ip mfib	パケット転送に使用されている(S,G)ルートおよび(*,G)ルートを表示します。すべてのマルチキャストルートについて、高速スイッチング、低速スイッチング、およびパーシャルスイッチングされたパケットの数が表示されます。
Switch# show ip mfib all	MFIB のすべてのルート(上位レイヤのルーティング プロトコル データベースには存在しないが、高速スイッチングをさらに高速化するために使用されるルートも含む)を表示します。これらのルートには、(S/M,224/4)ルートが含まれます。
Switch# show ip mfib log [n]	最近発生した n 個の MFIB 関連イベント ログを、新しい順に表示します。
Switch# show ip mfib counters	MFIB 関連イベントのカウンタを表示します。0 以外のカウンタだけが表示されます。

次に、show ip mfib コマンドの出力例を示します。

```
IP Multicast Forwarding Information Base
Entry Flags: C - Directly Connected, S - Signal,
            IC - Internal Copy
Interface Flags: A - Accept, F - Forward, S - Signal,
            NP - Not platform switched
Packets: Fast/Partial/Slow Bytes: Fast/Partial/Slow:
(171.69.10.13, 224.0.1.40), flags (IC)
  Packets: 2292/2292/0, Bytes: 518803/0/518803
  Vlan7 (A)
  Vlan100 (F NS)
  Vlan105 (F NS)
(*, 224.0.1.60), flags ()
  Packets: 2292/0/0, Bytes: 518803/0/0
  Vlan7 (A NS)
(*, 224.0.1.75), flags ()
   Vlan7 (A NS)
(10.34.2.92, 239.192.128.80), flags ()
  Packets: 24579/100/0, 2113788/15000/0 bytes
  Vlan7 (F NS)
  Vlan100 (A)
(*, 239.193.100.70), flags ()
  Packets: 1/0/0, 1500/0/0 bytes
  Vlan7 (A)
```

高速スイッチング パケットの数は、該当するルート上でハードウェアによってスイッチングされた パケット数を表します。

部分的スイッチング パケットの数は、高速スイッチング パケットが、ソフトウェア処理のため、あるいは 1 つまたは複数の非プラットフォーム スイッチド インターフェイス (PimTunnel インターフェイスなど) に転送されるため、CPU にコピーされた回数を表します。

低速スイッチング パケットの数は、該当するルート上で完全にソフトウェアによってスイッチング されたパケット数を表します。

IP MFIB 高速ドロップの表示



Supervisor Engine 6-E は、show ip mfib fastdrop コマンドをサポートしていません。

高速ドロップエントリを表示するには、次の作業を行います。

コマンド	目的		
	現在アクティブになっているすべての高速ドロップエントリを表示し、fastdrop がイネーブルに設定されているかどうかを示します。		

次に、show ip mfib fastdrop コマンドの出力例を示します。

Switch> show ip mfib fastdrop
MFIB fastdrop is enabled.
MFIB fast-dropped flows:
(10.0.0.1, 224.1.2.3, Vlan9) 00:01:32
(10.1.0.2, 224.1.2.3, Vlan9) 00:02:30
(1.2.3.4, 225.6.7.8, Vlan3) 00:01:50

着信パケットがドロップされた、(S,G) フル フローおよび入力インターフェイスが表示されます。 タイムスタンプは、エントリの有効時間を表します。

PIM 統計情報の表示

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

 ${\tt Switch\#} \ \ \textbf{show ip pim interface}$

Address	Interface	Mode	Neighbor Count	Query Interval	DR
198.92.37.6	Ethernet0	Dense	2	30	198.92.37.33
198.92.36.129	Ethernet1	Dense	2	30	198.92.36.131
10.1.37.2	Tunnel0	Dense	1	3.0	0.0.0.0

次に、show ip pim interface コマンドに count を指定した場合の出力例を示します。

Switch# show ip pim interface count

Address	Interface	FS	Mpackets In/Out
171.69.121.35	Ethernet0	*	548305239/13744856
171.69.121.35	Serial0.33	*	8256/67052912
198 92 12 73	Serial0 1719	*	219444/862191

次に、IP マルチキャストがイネーブルに設定されている状態で show ip pim interface コマンドに count を指定した場合の出力例を示します。この例では、高速スイッチングおよびプロセス スイッチングされる PIM インターフェイスのリストと、これらのパケット数が表示されます。IP マルチキャストがイネーブルに設定されているインターフェイスには、H が表示されます。

Switch# show ip pim interface count

States: FS -	Fast Switched,	H - Hardware Switched
Address	Interface	FS Mpackets In/Out
192.1.10.2	Vlan10	* H 40886/0
192.1.11.2	Vlan11	* H 0/40554
192.1.12.2	Vlan12	* H 0/40554
192.1.23.2	Vlan23	* 0/0
192.1.24.2	Vlan24	* 0/0

テーブルおよびデータベースの削除

特定のキャッシュ、テーブル、またはデータベースの内容をすべて削除できます。特定のキャッシュ、テーブル、またはデータベースの内容が無効である場合、または無効であると考えられる場合に、これらの削除が必要になります。

IP マルチキャスト キャッシュ、テーブル、およびデータベースを削除するには、次の作業のいずれかを行います。

コマンド	目的
Switch# clear ip mroute	IP ルーティング テーブルのエントリを削除します。
Switch# clear ip mfib counters	ルート単位およびグローバルの MFIB カウンタをすべて 削除します。
Switch# clear ip mfib fastdrop	高速ドロップ エントリをすべて削除します。



IP マルチキャスト ルートは、データ パケットが着信した時点で、プロトコル イベントへの応答として再生成されます。

設定例

ここでは、IP マルチキャスト ルーティングの設定例を示します。

- PIM 稠密モードの例 (p.31-24)
- PIM 希薄モードの例 (p.31-24)
- BSR の設定例 (p.31-24)

PIM 稠密モードの例

次に、イーサネット インターフェイス上の稠密モード PIM の設定例を示します。

```
ip multicast-routing
interface ethernet 0
ip pim dense-mode
```

PIM 希薄モードの例

次に、希薄モード PIM の設定例を示します。RP ルータは、アドレス 10.8.0.20 のルータです。

```
ip multicast-routing
  ip pim rp-address 10.8.0.20 1
interface ethernet 1
  ip pim sparse-mode
```

BSR の設定例

次に、候補 BSR (候補 RPも兼ねる)の設定例を示します。

```
version 11.3
1
ip multicast-routing
interface Ethernet0
 ip address 171.69.62.35 255.255.255.240
1
interface Ethernet1
ip address 172.21.24.18 255.255.255.248
ip pim sparse-dense-mode
interface Ethernet2
ip address 172.21.24.12 255.255.255.248
ip pim sparse-dense-mode
router ospf 1
network 172.21.24.8 0.0.0.7 area 1
network 172.21.24.16 0.0.0.7 area 1
ip pim bsr-candidate Ethernet2 30 10
ip pim rp-candidate Ethernet2 group-list 5
access-list 5 permit 239.255.2.0 0.0.0.255
```



CHAPTER

32

PBR の設定



E) PBR は Supervisor Engine 6-E ではサポートされていません。

この章では、ルータ上での Policy-Based Routing (PBR; ポリシーベース ルーティング) の設定作業 について説明します。主な内容は次のとおりです。

- PBR の概要 (p.32-2)
- PBR の設定作業リスト (p.32-4)
- PBR の設定例 (p.32-6)



この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/cr/index.htm



(注)

機能に関するハードウェア プラットフォームまたはソフトウェア イメージの情報を確認するには、Cisco.com の Feature Navigator を使用してその機能に関する情報を検索するか、特定のリリースに対応するソフトウェア リリース ノートを参照してください。

PBR の概要

ここでは、次の内容について説明します。

- PBR の概要 (p.32-2)
- PBR フロー スイッチングの概要 (p.32-2)
- PBR の使用 (p.32-3)

PBR は、トラフィック フローに定義ポリシーを設定し、ルートにおけるルーティング プロトコルへの依存度を軽くして、パケットのルーティングを柔軟に行えるようにします。このため PBR は、ルーティング プロトコルが提供する既存のメカニズムを拡張、補完することでルーティングの制御を強化します。 PBR により、高コスト リンクにおけるプライオリティ トラフィックなど、特定のトラフィックのパスを指定できます。

設定したポリシーに基づいてパケットをルーティングする方法として、PBR を設定できます。たとえば、特定のエンド システムの ID、アプリケーション プロトコル、またはパケット サイズに基づいてパスの permit や deny を行うルーティング ポリシーを実装できます。

PBR を使用すると、次の作業が可能になります。

- 拡張アクセス リスト基準に基づいたトラフィックの分類。リストにアクセスし、一致基準を設定します。
- 特定のトラフィック処理が行われたパスへのパケットのルーティング

ポリシーは、IP アドレス、ポート番号、またはプロトコルをベースとします。ポリシーを単純にするには、これらの記述子のいずれか1つを使用します。複雑なポリシーにするには、これらをすべて使用します。

PBR の概要

PBR がイネーブルのインターフェイスで受信されたすべてのパケットは、ルート マップという拡張パケット フィルタを通過します。PBR で使用するルート マップはポリシーを要求し、パケットの転送先を判断します。

ルート マップは文で構成されています。ルート マップ文は permit または deny とマークでき、次の方法で解釈されます。

- 文が deny とマークされている場合、一致基準に合致したパケットは通常転送チャネルを通じて 送り返され、宛先ベースのルーティングを実行します。
- 文が permit とマークされていてパケットがアクセス リストと一致している場合、最初の有効な set 句がそのパケットに適用されます。

PBR を着信インターフェイス(パケットを受信するインターフェイス)に指定できますが、発信インターフェイスには指定できません。

PBR フロー スイッチングの概要

Catalyst 4500 スイッチング エンジンは、[set next-hop] ルートマップ アクションと許可 Access Control List (ACL; アクセス コントロール リスト) のパケットとの照合をサポートします。その他すべて のルートマップ アクション (拒否 ACL の照合を含む) は、フロー スイッチング モデルによってサポートされています。このモデルでは、ルートマップに一致するフローの最初のパケットは、転送目的でソフトウェアに配信されます。ソフトウェアは、パケットの正しい宛先を判別し、Ternary CAM (TCAM)にエントリをインストールするので、そのあとのフローのパケットがハードウェアでスイッチングされるようになります。Catalyst 4500 スイッチング エンジンは、最大 4096 のフローをサポートします。

PBR の使用

PBR をイネーブルにして、特定のパケットのルーティング パスを最短と思われるパスから変更できます。たとえば、PBR は次のような機能を提供します。

- 同等アクセス
- プロトコル依存ルーティング
- 送信元依存ルーティング
- 双方向対バッチ トラフィックに基づくルーティング
- 専用リンクに基づくルーティング

アプリケーションまたはトラフィックによっては、送信元依存ルーティングが有効です。たとえば、在庫記録を本社に送信する場合は高帯域幅で高コストのリンクを短時間使用し、電子メールなどの日常的に使うアプリケーション データは低帯域幅で低コストのリンクで送信します。

PBR の設定作業リスト

ここでは、PBR を設定するために実行する作業について説明します。最初に説明する作業は必須で、そのあとの作業は任意です。この章の最後にある「PBR の設定例」を参照してください。

- PBR のイネーブル化(必須)
- ローカル PBR のイネーブル化 (任意)

PBR のイネーブル化

PBR をイネーブルにするには、一致基準とすべての match コマンドが一致した場合の動作を指定するルート マップを作成する必要があります。次に、特定のインターフェイスでそのルート マップ 用の PBR をイネーブルにします。指定したインターフェイスに着信したパケットのうち、match コマンドと一致したものはすべて PBR の対象になります。

特定のインターフェイス上で PBR をイネーブルにするには、次の作業を行います。

	コマンド	目的							
ステップ 1	Switch(config)# route-map map-tag [permit deny] [sequence-number]	パケットが出力される場所を制御するルート マップを定義します。このコマンドを入力すると、ルータはルートマップ コンフィギュレーション モードになります。							
ステップ 2	Switch(config-route-map)# match ip address {access-list-number name} [access-list-number name]	一致基準を指定します。1 つまたは複数の標準または拡張 アクセス リストで許可された送信元および宛先 IP アドレ スを照合します。							
ステップ 3、	4、5、または6を実行します。								
ステップ 3	Switch(config-route-map)# set ip next-hop ip-address [ip-address]	基準と一致するパケットの動作を指定します。							
		パケットをルーティングするネクスト ホップを指定します (ネクスト ホップは隣接している必要があります)。この動作は、通常のルーティング テーブルで指定されている							
	または	ネクスト ホップと同じです。							
ステップ 4	Switch(config-route-map)# set interface interface-type interface-number	基準と一致するパケットの動作を指定します。							
	[type number] または	パケットの出力インターフェイスを設定します。この動作は、パケットがローカルインターフェイスの外に転送されるように指定します。インターフェイスは(スイッチ ポートではない)レイヤ3インターフェイスでなければならず、パケットの宛先アドレスはそのインターフェイスに割り当てられた IP ネットワーク内に存在している必要があります。パケットの宛先アドレスがネットワークにない場合、パケットはドロップされます。							
ステップ 5	Switch(config-route-map)# set ip								
,,,,,,	default next-hop ip-address [ip-address]	その宛先に明示パスがない場合にパケットをルーティングするネクスト ホップを設定します。ネクスト ホップにパケットを転送する前に、スイッチはパケットの宛先アドレスをユニキャスト ルーティング テーブル内で検索します。一致するものが見つかった場合、パケットはルーティングテーブルを経由して転送されます。一致するものが見つからなかった場合、パケットは指定されたネクスト ホップに							
	または	転送されます。							

	コマンド	目的
ステップ 6	Switch(config-route-map)# set default interface interface-type	基準と一致するパケットの動作を指定します。
	<pre>interface-number [typenumber]</pre>	その宛先に明示パスがない場合のパケットの出力インターフェイスを設定します。ネクストホップにパケットを転送する前に、スイッチはパケットの宛先アドレスをユニキャストルーティングテーブル内で検索します。一致するものが見つかった場合、パケットはルーティングテーブルを経由して転送されます。一致するものが見つからなかった場合、パケットは指定された出力インターフェイスに転送さ
		れます。パケットの宛先アドレスがネットワークにない場合、パケットはドロップされます。
ステップ 7	Switch(config-route-map)# interface interface-type interface-number	インターフェイスを設定します。このコマンドを入力する と、ルータはインターフェイス コンフィギュレーション モードになります。
ステップ 8	Switch(config-if)# ip policy route-map map-tag	PBR で使用するルート マップを識別します。1 つのインターフェイスに対して使用できるルート マップ タグは 1 つだけですが、異なるシーケンス番号を持つルート マップ エントリを複数設定できます。これらのエントリは、一致するものが見つかるまでシーケンス番号順に評価されます。一致するものがない場合、パケットは通常どおりルーティングされます。

set コマンドは、他のコマンドとともに使用できます。これらのコマンドは、上記のステップ 3 に示す順序に従って評価されます。使用可能なネクスト ホップはインターフェイスで暗黙指定されます。ローカル ルータがネクスト ホップを見つけ、それが使用可能なインターフェイスである場合、ローカル ルータはパケットをルーティングします。

ローカル PBR のイネーブル化

ルータで生成されたパケットは、通常どおりにポリシー ルーティングされません。これらのパケットのためのローカル PBR をイネーブルにするには、ルータが使用すべきルート マップを示すために、次の作業を行います。

コマンド	目的
Switch(config)# ip local policy route-map map-tag	ローカル PBR で使用するルート マップを識別します。

これで、ルータから発信されたパケットはすべて、ローカル PBR の対象となります。

ローカル PBR で使用するルート マップ (ある場合)を表示するには、show ip local policy コマンドを使用します。

サポートされない機能

ルートマップ コンフィギュレーション モードの次の PBR コマンドは CLI (コマンドライン インターフェイス) のものですが、Catalyst 4500 シリーズ スイッチの Cisco IOS ではサポートされていません。これらのコマンドを使用しようとすると、エラー メッセージが表示されます。

- match-length
- set ip qos

- set ip tos
- set ip precedence

PBR の設定例

ここでは、PBR の設定例を示します。

- 同等アクセス例 (p.32-6)
- ネクスト ホップを変更する例 (p.32-7)
- ACE の拒否例 (p.32-7)

PBR の設定方法については、この章の「PBR の設定作業リスト」を参照してください。

同等アクセス例

次に、2 つの送信元が、異なるサービス プロバイダーに対して同等アクセスを持つ例を示します。 ルータにパケットの宛先について明示パスがない場合、送信元 1.1.1.1 からインターフェイス FastEthernet 3/1 に着信したパケットは、6.6.6.6 にあるルータへ送信されます。ルータにパケットの 宛先について明示パスがない場合、送信元 2.2.2.2 から着信したパケットは、7.7.7.7 にあるルータへ 送信されます。ルータに宛先の明示パスがない他のすべてのパケットは廃棄されます。

```
Switch (config)# access-list 1 permit ip 1.1.1.1
access-list 1 permit ip 1.1.1.1
!
interface fastethernet 3/1
ip policy route-map equal-access
!

route-map equal-access permit 10
match ip address 1
set ip default next-hop 6.6.6.6
route-map equal-access permit 20
match ip address 2
set ip default next-hop 7.7.7.7
route-map equal-access permit 30
set default interface null0
```



ドロップするパケットが最初の2つの route-map 句と一致しない場合、**set default interface null0** を **set interface null0** に変更します。

ネクスト ホップを変更する例

次に、異なる送信元から異なる場所 (ネクスト ホップ) ヘルーティングする例を示します。送信元 1.1.1.1 から着信したパケットは 3.3.3.3 にあるネクスト ホップに送信され、送信元 2.2.2.2 から着信 したパケットは 3.3.3.5 にあるネクスト ホップへ送信されます。

```
access-list 1 permit ip 1.1.1.1
access-list 2 permit ip 2.2.2.2
!
interface fastethernet 3/1
ip policy route-map Texas
!
route-map Texas permit 10
match ip address 1
set ip next-hop 3.3.3.3
!
route-map Texas permit 20
match ip address 2
set ip next-hop 3.3.3.5
```

ACE の拒否例

次に、指定されたルート マップ シーケンスの処理を停止し、次のシーケンスに飛ぶ例を示します。 送信元 1.1.1.1 から着信したパケットは、シーケンス 10 をスキップしてシーケンス 20 に飛びます。 サブネット 1.1.1.0 から着信する他のすべてのパケットは、シーケンス 10 の set 文に従います。

```
access-list 1 deny ip 1.1.1.1
access-list 1 permit ip 1.1.1.0 0.0.0.255
access-list 2 permit ip 1.1.1.1
access-list 2 permit ip 2.2.2.2
!
interface fastethernet 3/1
ip policy route-map Texas
!
route-map Texas permit 10
match ip address 1
set ip next-hop 3.3.3.3
!
route-map Texas permit 20
match ip address 2
set ip next-hop 3.3.3.5
```

■ PBR の設定例



CHAPTER

33

VRF-Lite の設定

Virtual Private Network(VPN; バーチャル プライベート ネットワーク)は、ISP バックボーン ネットワーク上で帯域幅を共有する安全な手段をカスタマーに提供します。VPN は、共通のルーティング テーブルを共有するサイトの集まりです。カスタマーのサイトは、1 つまたは複数のインターフェイスでサービス プロバイダーのネットワークに接続され、サービス プロバイダーが各インターフェイスを VPN ルーティング テーブルに対応付けます。VPN ルーティング テーブルは、VPN Routing/Forwarding(VRF; VPN ルーティング / 転送)テーブルと呼ばれます。

Catalyst 4500 シリーズ スイッチは、VRF-Lite 機能を使用して Customer Edge (CE; カスタマー エッジ) デバイスで複数の VRF インスタンスをサポートします (VRF-Lite は、Multi-VRF CE、または Multi-VRF CE デバイスともいいます)。 VRF-Lite によって、サービス プロバイダーは 1 つのインターフェイスを使用して、重複する IP アドレスを持つ複数の VPN をサポートできます。



スイッチは、VPN をサポートするのに Multiprotocol Label Switching (MPLS; マルチプロトコル ラベル スイッチング)を使用しません。MPLS VRF については、次の URL で『Cisco IOS Switching Services Configuration Guide』Release 12.3 を参照してください。

http://www.cisco.com/univerd/cc/td/doc/product/software/ios123/123cgcr/swit_vcg.htm

この章の内容は、次のとおりです。

- VRF-Lite の概要 (p.33-2)
- VRF-Lite のデフォルト設定 (p.33-4)
- VRF-Lite 設定時の注意事項 (p.33-4)
- VRFの設定 (p.33-5)
- VPN ルーティング セッションの設定 (p.33-6)
- CE ルーティング セッションへの BGP PE の設定 (p.33-7)
- VRF-Lite の設定例 (p.33-8)
- VRF-Lite ステータスの表示 (p.33-12)



この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univered/cc/td/doc/product/software/ios124/124cr/index.htm

VRF-Lite の概要

VRF-Lite の機能によって、サービス プロバイダーは、VPN 間で重複した IP アドレスを使用できる 複数の VPN をサポートできます。VRF-Lite は入力インターフェイスを使用して異なる VPN のルートを区別し、各 VRF に 1 つまたは複数のレイヤ 3 インターフェイスを対応付けて仮想パケット転送テーブルを形成します。VRF のインターフェイスには、イーサネット ポートなどの物理インターフェイス、または VLAN(仮想 LAN)Switch Virtual Interface(SVI; スイッチ仮想インターフェイス)などの論理インターフェイスが有効ですが、レイヤ 3 インターフェイスは、複数の VRF に属することは常にできません。



VRF-Lite インターフェイスは、レイヤ3インターフェイスである必要があります。

VRF-Lite には次のデバイスが含まれます。

- CE デバイスにおいて、カスタマーは、1 つまたは複数の Provider Edge (PE; プロバイダー エッジ) ルータへのデータ リンクを介してサービス プロバイダー ネットワークにアクセスできます。CE デバイスは、サイトのローカル ルートを PE ルータヘアドバタイズし、PE ルータからリモート VPN ルートを学習します。Catalyst 4500 シリーズ スイッチは CE にすることができます。
- PE ルータは、スタティック ルーティング、または Border Gateway Protocol (BGP)、Routing Information Protocol バージョン 1 (RIPv1)、Routing Information Protocol バージョン 2 (RIPv2) などのルーティング プロトコルを使用して CE デバイスとルーティング情報を交換します。
- PEでは、直接接続された VPN の VPN ルートを維持することだけが必要とされます。サービスプロバイダーのすべての VPN ルートを PE が維持する必要はありません。各 PE ルータは、直接接続されたサイトごとの VRF を維持します。このようなサイトのすべてが同一の VPN に参加する場合は、PE ルータ上の複数のインターフェイスを単一の VRF に対応付けることができます。各 VPN は、指定された VRF にマッピングされます。CE からローカルの VPN ルートが学習されると、PE ルータは Internal BGP (IBGP) を使用してその他の PE ルータと VPN ルーティング情報を交換します。
- プロバイダー ルータ (またはコア ルータ)は、CE デバイスに接続されていないサービス プロバイダー ネットワーク内のルータです。

VRF-Lite により、複数のカスタマーが 1 つの CE を共有でき、CE と PE の間には物理リンクが 1 つだけ使用されます。共有された CE は、カスタマーの別個の VRF テーブル、独自のルーティングテーブルに基づいて各カスタマーのパケットをスイッチングまたはルーティングします。 VRF-Lite は、制限された PE 機能を CE デバイスに拡張して、VPN のプライバシーおよびセキュリティを支店に拡張するために、別個の VRF テーブルを維持する機能を提供しています。

図 33-1 は、各 Catalyst 4500 シリーズ スイッチが複数の仮想 CE として動作する構成を示します。 VRF-Lite はレイヤ 3 機能であるため、VRF の各インターフェイスはレイヤ 3 インターフェイスである必要があります。

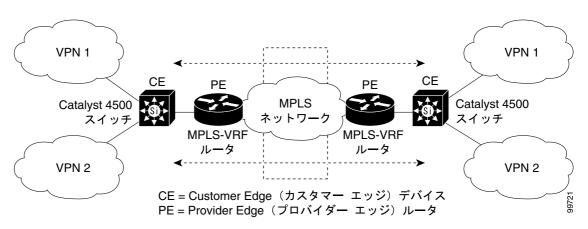


図 33-1 複数の仮想 CE として動作する Catalyst 4500 シリーズ スイッチ

次に、図 33-1 に表示される VRF-Lite CE 対応ネットワークのパケット転送プロセスを示します。

- CE が VPN からパケットを受信すると、CE は入力インターフェイスに基づいたルーティング テーブルを検索します。ルートが見つかると、CE はパケットを PE に転送します。
- 入力 PE が CE からのパケットを受信すると、VRF 検索を実行します。ルートが見つかると、 ルータは対応する MPLS ラベルをパケットに追加して、それを MPLS ネットワークに送信しま す。
- 出力 PE がネットワークからパケットを受信すると、ラベルを除去し、そのラベルを使用して正しい VPN ルーティング テーブルを識別します。次に、出力 PE が通常のルート検索を行います。ルートが見つかると、PE はパケットを正しい隣接デバイスに転送します。
- CE が出力 PE からパケットを受信すると、CE は入力インターフェイスを使用して正しい VPN ルーティング テーブルを検索します。ルートが見つかると、CE はパケットを VPN 内に転送します。

VRF を設定するには、VRF テーブルを作成し、VRF に対応付けられたレイヤ 3 インターフェイス を指定します。次に、VPN、および CE と PE の間にルーティング プロトコルを設定します。BGP は、VPN ルーティング情報をプロバイダーのバックボーン上に配布するのに最適なルーティング プロトコルです。VRF-Lite ネットワークには、次の 3 つの主要なコンポーネントがあります。

- VPN ルート ターゲット コミュニティ VPN コミュニティの他のすべてのリストです。各 VPN コミュニティ メンバに VPN ルート ターゲットを設定する必要があります。
- VPN コミュニティ PE ルータのマルチプロトコル BGP ピアリング VPN コミュニティのすべてのメンバに VRF の到着可能性情報を伝播します。VPN コミュニティ内のすべての PE ルータに BGP ピアリングを設定する必要があります。
- VPN 転送 VPN サービスプロバイダー ネットワークのすべての VPN コミュニティ メンバ間 のすべてのトラフィックを転送します。

VRF-Lite のデフォルト設定

表 33-1 に、VRF のデフォルト設定を示します。

表 33-1 VRF のデフォルト設定

機能	デフォルト設定
VRF	ディセーブル。VRF は定義されていません。
マップ	インポート マップ、エクスポート マップ、またはルート マップは定義され
	ていません。
VRF の最大ルート	なし
転送テーブル	インターフェイスのデフォルトは、グローバル ルーティング テーブルです。

VRF-Lite 設定時の注意事項

ネットワークに VRF を設定する場合に、次の点に留意してください。

- VRF-Lite が設定されたスイッチは複数のカスタマーで共有され、すべてのカスタマーが独自のルーティング テーブルを持ちます。
- カスタマーは異なる VRF テーブルを使用するので、同一の IP アドレスを再使用できます。重 複した IP アドレスは、異なる VPN で使用できます。
- VRF-Lite では、複数のカスタマーが PE と CE の間で同一の物理リンクを共有できます。複数 の VLAN があるトランク ポートは、パケットをカスタマーごとに分類します。すべてのカス タマーが独自の VLAN を持ちます。
- VRF-Lite は、すべての MPLS-VRF 機能(ラベル交換、Label Distribution Protocol [LDP] の隣接 関係、またはラベル付きパケット)をサポートしていません。
- PE ルータでは、VRF-Lite の使用と複数の CE の使用には違いがありません。図 33-1 では、複数の仮想レイヤ 3 インターフェイスが VRF-Lite デバイスに接続されています。
- Catalyst 4500 シリーズ スイッチは、物理ポート、VLAN SVI、またはその 2 つの組み合わせを 使用した VRF の設定をサポートしています。SVI は、アクセス ポートまたはトランク ポートを介して接続できます。
- カスタマーは、他のカスタマーと重複しないかぎり複数の VLAN を使用できます。カスタマー の VLAN は、スイッチに格納された適切なルーティング テーブルを識別するのに使用する、特 定のルーティング テーブル ID にマッピングされます。
- レイヤ 3 Ternary CAM (TCAM) リソースは、すべての VRF 間で共有されます。各 VRF が十分な CAM (連想メモリ) 領域を持つようにするには、maximum routes コマンドを使用します。
- VRF を使用した Catalyst 4500 シリーズ スイッチは、1 つのグローバル ネットワークと最大 64 の VRF をサポートできます。サポートされるルートの総数は、TCAM のサイズに制限されます。
- ほとんどのルーティング プロトコル (BGP、Open Shortest Path First [OSPF]、Enhanced Interior Gateway Routing Protocol [EIGRP]、Routing Information Protocol [RIP]、およびスタティック ルーティング) を CE と PE 間で使用できます。ただし、次のような理由から External BGP (EBGP) の使用を推奨しています。
 - BGPは、複数のCEと通信するのに複数のアルゴリズムを必要としません。
 - BGP は、異なる管理下で実行されるシステム間でルーティング情報を渡すために設計されています。
 - BGPを使用すると、CEにルートのアトリビュートを譲渡することが容易になります。
- VRF-Lite は、Interior Gateway Routing Protocol (IGRP) および ISIS をサポートしません。
- VRF-Lite は、パケット スイッチング レートに影響しません。
- マルチキャストを同時に同一のレイヤ3インターフェイス上に設定することはできません。
- router ospf の capability vrf-lite サブコマンドは、PE と CE 間のルーティング プロトコルとして OSPF が設定されている場合に使用する必要があります。

VRF の設定

1つまたは複数の VRF を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	Switch(config)# ip routing	IP ルーティングをイネーブルにします。
ステップ 3	Switch(config)# ip vrf vrf-name	VRF 名を指定し、VRF コンフィギュレーション モードを開始します。
ステップ 4	Switch(config-vrf)# rd route-distinguisher	ルート識別子を指定して VRF テーブルを作成します。Autonomous System(AS; 自律システム)番号および任意の数(xxx:y)または IP アドレスおよび任意の数(A.B.C.D:y)のどちらかを入力します。
ステップ 5	Switch(config-vrf)# route-target {export import both} route-target-ext-community	指定された VRF のインポート、エクスポート、またはインポートおよびエクスポート ルート ターゲット コミュニティのリストを作成します。AS 番号および任意の数 (xxx:y)、IP アドレスおよび任意の数 (A.B.C.D:y) のどちらかを入力します。 (注) このコマンドは、BGP が稼働している場合にのみ有効です。
ステップ 6	Switch(config-vrf)# import map route-map	(任意) VRF にルート マップを対応付けます。
ステップ 7	Switch(config-vrf)# interface interface-id	インターフェイス コンフィギュレーション モード を開始して、VRF に対応付けるレイヤ 3 インターフェイスを指定します。有効なインターフェイスは、ルーテッド ポートまたは SVI です。
ステップ 8	Switch(config-if)# ip vrf forwarding vrf-name	VRF をレイヤ 3 インターフェイスに対応付けます。
ステップ 9	Switch(config-if)# end	特権 EXEC モードに戻ります。
ステップ 10	Switch# show ip vrf [brief detail interfaces] [vrf-name]	設定を確認します。設定した VRF に関する情報を表示します。
ステップ 11	Switch# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を 保存します。



コマンドの構文および使用方法の詳細については、このリリースに対するスイッチ コマンド リファレンスおよび $^{\mathbb{C}}$ Cisco IOS Switching Services Command Reference $_{\mathbb{Z}}$ Release 12.2 を参照してください。

VRF を削除、および VRF からすべてのインターフェイスを削除するには、**no ip vrf** vrf-name グローバル コンフィギュレーション コマンドを使用します。 VRF から 1 つのインターフェイスを削除するには、**no ip vrf forwarding** インターフェイス コンフィギュレーション コマンドを使用します。

VPN ルーティング セッションの設定

VPN 内のルーティングは、サポートされるルーティング プロトコル (RIP、OSPF、または BGP) またはスタティック ルーティングで設定できます。ここで表示する設定は OSPF 用ですが、その他のプロトコルでもプロセスは同じです。

VPNにOSPFを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	Switch(config)# router ospf process-id vrf vrf-name	OSPF ルーティングをイネーブルにし、VPN 転送 テーブルを指定して、ルータ コンフィギュレーショ ン モードを開始します。
ステップ 3	Switch(config-router)# log-adjacency-changes	(任意)隣接ステートの変更を記録します。これは、 デフォルトのステートです。
ステップ 4	Switch(config-router)# redistribute bgp autonomous-system-number subnets	BGP ネットワークから OSPF ネットワークに情報を 再配布するようにスイッチを設定します。
ステップ 5	Switch(config-router)# network network-number area area-id	OSPF が稼働するネットワーク アドレスとマスク、 およびそのネットワーク アドレスのエリア ID を定 義します。
ステップ 6	Switch(config-router)# end	特権 EXEC モードに戻ります。
ステップ 7	Switch# show ip ospf process-id	OSPF ネットワークの設定を確認します。
ステップ 8	Switch# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を 保存します。

OSPF ルーティング プロセスから VPN 転送テーブルの対応付けを解除するには、no router ospf process-id vrf vrf-name グローバル コンフィギュレーション コマンドを使用します。

CE ルーティング セッションへの BGP PE の設定

CE ルーティング セッションに BGP PE を設定するには、次の作業を行います。

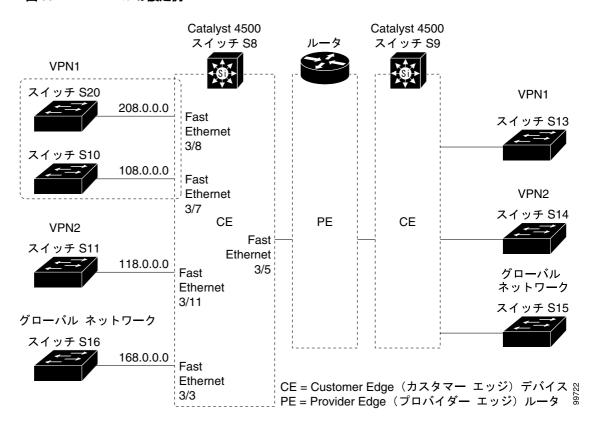
	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	Switch(config)# router bgp autonomous-system-number	その他の BGP ルータに渡された AS 番号で BGP ルーティング プロセスを設定し、ルータ コンフィ ギュレーション モードを開始します。
ステップ 3	Switch(config-router)# network network-number mask network-mask	BGP を使用してアナウンスするネットワークおよび マスクを指定します。
ステップ 4	Switch(config-router)# redistribute ospf process-id match internal	OSPF 内部ルートを再配布するようにスイッチを設定します。
ステップ 5	Switch(config-router)# network network-number area area-id	OSPF が稼働するネットワーク アドレスとマスク、 およびそのネットワーク アドレスのエリア ID を定 義します。
ステップ 6	Switch(config-router-af)# address-family ipv4 vrf vrf-name	PE から CE のルーティング セッションの BGP パラメータを定義し、VRF アドレス ファミリ モードを開始します。
ステップ 7	Switch(config-router-af)# neighbor address remote-as as-number	PE と CE ルータの間の BGP セッションを定義します。
ステップ 8	Switch(config-router-af)# neighbor address activate	IPv4 アドレス ファミリのアドバタイズをアクティ ブ化します。
ステップ 9	Switch(config-router-af)# end	特権 EXEC モードに戻ります。
ステップ 10	Switch# show ip bgp [ipv4] [neighbors]	BGP 設定を確認します。
ステップ 11	Switch# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を 保存します。

BGP ルーティング プロセスを削除するには、**no router bgp** autonomous-system-number グローバル コンフィギュレーション コマンドを使用します。ルーティングの特性を削除するには、キーワードとともにコマンドを使用します。

VRF-Lite の設定例

図 33-2 は、図 33-1 と類似したネットワークの物理接続を簡略化した例です。OSPF は、VPN1、VPN2、およびグローバルネットワークで使用されるプロトコルです。BGP は、CE と PE の接続に使用されます。次の例のコマンドは、CE スイッチ S8 を設定する方法を示し、スイッチ S20 および S11 の VRF 設定、およびスイッチ S8 のトラフィックに関連する PE ルータ コマンドが含まれます。その他のスイッチの設定のコマンドは含まれていませんが、類似したものになります。

図 33-2 VRF-Lite の設定例



スイッチ S8 の設定

スイッチ S8 上のルーティングをイネーブルにし、VRF を設定します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# ip vrf v11
Switch(config-vrf)# rd 800:1
Switch(config-vrf)# route-target export 800:1
Switch(config-vrf)# route-target import 800:1
Switch(config-vrf)# exit
Switch(config)# ip vrf v12
Switch(config-vrf)# rd 800:2
Switch(config-vrf)# route-target export 800:2
Switch(config-vrf)# route-target import 800:2
Switch(config-vrf)# route-target import 800:2
Switch(config-vrf)# exit
```

スイッチ S8 上でループバックおよび物理インターフェイスを設定します。インターフェイス FastEthernet 3/5 は、PE へのトランク接続です。インターフェイス 3/7 および 3/11 は、VPN に接続します。

```
Switch(config) # interface loopback1
Switch(config-if) # ip vrf forwarding v11
Switch(config-if) # ip address 8.8.1.8 255.255.255.0
Switch(config-if)# exit
Switch(config)# interface loopback2
Switch(config-if)# ip vrf forwarding v12
Switch(config-if) # ip address 8.8.2.8 255.255.255.0
Switch(config-if)# exit
Switch(config) # interface FastEthernet3/5
Switch(config-if) # switchport trunk encapsulation dot1q
Switch(config-if) # switchport mode trunk
Switch(config-if) # no ip address
Switch(config-if)# exit
Switch(config)# interface FastEthernet3/8
Switch(config-if) # switchport access vlan 208
Switch(config-if) # no ip address
Switch(config-if)# exit
Switch(config)# interface FastEthernet3/11
Switch(config-if) # switchport trunk encapsulation dot1q
Switch(config-if) # switchport mode trunk
Switch(config-if) # no ip address
Switch(config-if) # exit
```

スイッチ S8 上で使用される VLAN を設定します。VLAN 10 は、CE と PE の間で VRF 11 によって使用されます。VLAN 20 は、CE と PE の間で VRF 12 によって使用されます。VLAN 118 および 208 は、それぞれスイッチ S11 およびスイッチ S20 を含む VPN の VRF に使用されます。

```
Switch(config) # interface Vlan10
Switch(config-if)# ip vrf forwarding v11
Switch(config-if)# ip address 38.0.0.8 255.255.255.0
Switch(config-if)# exit
Switch(config) # interface Vlan20
Switch(config-if) # ip vrf forwarding v12
Switch(config-if) # ip address 83.0.0.8 255.255.255.0
Switch(config-if)# exit
Switch(config)# interface Vlan118
Switch(config-if)# ip vrf forwarding v12
Switch(config-if)# ip address 118.0.0.8 255.255.255.0
Switch(config-if)# exit
Switch(config) # interface Vlan208
Switch(config-if) # ip vrf forwarding v11
Switch(config-if)# ip address 208.0.0.8 255.255.255.0
Switch(config-if)# exit
VPN1 および VPN2 に OSPF ルーティングを設定します。
Switch(config) # router ospf 1 vrf vl1
Switch(config-router)# redistribute bgp 800 subnets
Switch(config-router) # network 208.0.0.0 0.0.0.255 area 0
Switch(config-router)# exit
Switch(config) # router ospf 2 vrf v12
Switch(config-router) # redistribute bgp 800 subnets
Switch(config-router) # network 118.0.0.0 0.0.0.255 area 0
Switch(config-router)# exit
```

CE から PE のルーティングに BGP を設定します。

```
Switch(config) # router bgp 800
Switch(config-router) # address-family ipv4 vrf vl2
Switch(config-router-af) # redistribute ospf 2 match internal
Switch(config-router-af) # neighbor 83.0.0.3 remote-as 100
Switch(config-router-af) # neighbor 83.0.0.3 activate
Switch(config-router-af) # network 8.8.2.0 mask 255.255.255.0
Switch(config-router-af) # exit

Switch(config-router) # address-family ipv4 vrf vll
Switch(config-router-af) # redistribute ospf 1 match internal
Switch(config-router-af) # neighbor 38.0.0.3 remote-as 100
Switch(config-router-af) # neighbor 38.0.0.3 activate
Switch(config-router-af) # network 8.8.1.0 mask 255.255.255.0
Switch(config-router-af) # network 8.8.1.0 mask 255.255.255.0
```

スイッチ S20 の設定

CE に接続するように S20 を設定します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# interface Fast Ethernet 0/7
Switch(config-if)# no switchport
Switch(config-if)# ip address 208.0.0.20 255.255.255.0
Switch(config-if)# exit

Switch(config)# router ospf 101
Switch(config-router)# network 208.0.0.0 0.0.255 area 0
Switch(config-router)# end
```

スイッチ S11 の設定

CE に接続するように S11 を設定します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# interface Gigabit Ethernet 0/3
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# no ip address
Switch(config-if)# exit

Switch(config)# interface Vlan118
Switch(config-if)# ip address 118.0.0.11 255.255.255.0
Switch(config-if)# exit

Switch(config-router)# exit
Switch(config-router)# network 118.0.0.0 0.0.255 area 0
Switch(config-router)# end
```

PE スイッチ S3 の設定

スイッチ S3 (ルータ)上では、次のコマンドはスイッチ S8 への接続だけを設定します。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config) # ip vrf v1
Router(config-vrf)# rd 100:1
Router(config-vrf)# route-target export 100:1
Router(config-vrf)# route-target import 100:1
Router(config-vrf)# exit
Router(config) # ip vrf v2
Router(config-vrf)# rd 100:2
Router(config-vrf)# route-target export 100:2
Router(config-vrf)# route-target import 100:2
Router(config-vrf)# exit
Router(config) # ip cef
Router(config) # interface Loopback1
Router(config-if) # ip vrf forwarding v1
Router(config-if) # ip address 3.3.1.3 255.255.255.0
Router(config-if)# exit
Router(config) # interface Loopback2
Router(config-if) # ip vrf forwarding v2
Router(config-if) # ip address 3.3.2.3 255.255.255.0
Router(config-if)# exit
Router(config) # interface Fast Ethernet3/0.10
Router(config-if)# encapsulation dot1q 10
Router(config-if)# ip vrf forwarding v1
Router(config-if) # ip address 38.0.0.3 255.255.255.0
Router(config-if)# exit
Router(config)# interface Fast Ethernet3/0.20
Router(config-if)# encapsulation dot1q 20
Router(config-if)# ip vrf forwarding v2
Router(config-if) # ip address 83.0.0.3 255.255.255.0
Router(config-if)# exit
Router(config)# router bgp 100
Router(config-router) # address-family ipv4 vrf v2
Router(config-router-af) # neighbor 83.0.0.8 remote-as 800
Router(config-router-af)# neighbor 83.0.0.8 activate
Router(config-router-af)# network 3.3.2.0 mask 255.255.255.0
Router(config-router-af)# exit
Router(config-router)# address-family ipv4 vrf vl
Router(config-router-af)# neighbor 83.0.0.8 remote-as 800
Router(config-router-af) # neighbor 83.0.0.8 activate
Router(config-router-af) # network 3.3.1.0 mask 255.255.255.0
Router(config-router-af)# end
```

VRF-Lite ステータスの表示

VRF-Lite の設定およびステータスに関する情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
Switch# show ip protocols vrf vrf-name	VRF に対応付けられたルーティング プロトコル情報を表示します。
Switch# show ip route vrf vrf-name [connected] [protocol [as-number]] [list] [mobile] [odr] [profile] [static] [summary] [supernets-only]	VRF に対応付けられた IP ルーティング テーブル情報を表示します。
Switch# show ip vrf [brief detail interfaces] [vrf-name]	定義された VRF インスタンスに関する情報を表示します。



この出力の情報の詳細については、次の URL の『Cisco IOS Switching Services Command Reference』 Release 12.2 を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fswtch_r



CHAPTER

34

QoS の設定

この章では、Automatic QoS (auto-QoS) コマンドまたは標準の QoS (Quality Of Service) コマンドを使用して Catalyst 4500 シリーズ スイッチ上で QoS を設定する方法について説明します。ここでは、VLAN だけでなくさまざまな種類のインターフェイス (アクセス、レイヤ 2 トランク、レイヤ 3 ルーティング、EtherChannel) での QoS 設定を指定する方法を説明します。また、所定のインターフェイスの異なる VLAN 上で異なる QoS (per-Port per-VLAN QoS [PVQoS]) を設定する方法についても説明します。この章では、Supervisor Engine II-Plus から V-10GE まで、および Supervisor Engine 6-E での QoS サポートについて説明します。

Supervisor Engines II-Plus から V-10G でサポートされている QoS コンフィギュレーション モデルは、スイッチ QoS モデルと呼ばれています。ただし、Supervisor Engine 6-E は Modular QoS CLI (MQC; モジュラ QoS コマンドライン インターフェイス) と呼ばれる別の QoS コンフィギュレーション モデルをサポートしています。 QoS が設定されているスーパーバイザ エンジンの該当する設定セクションを参照してください。MQC についての詳細は、 $^{\mathbb{C}}$ Cisco IOS Quality of Service Solutions Configuration Guide』Release 12.3 の「Modular Quality of Service Command-Line Interface」を参照してください。

この章の内容は、次のとおりです。

- Catalyst 4500 シリーズ スイッチでの QoS の概要 (p.34-2)
- Supervisor Engine II-Plus、II+10GE、VI、V、V-10GE、4924、4948、および 4948-10GE での Auto-QoS の設定 (p.34-19)
- Supervisor Engine II-Plus、II+10GE、VI、V、V-10GE、4924、4948、および 4948-10GE での QoS の設定(p.34-25)
- Supervisor Engine 6-E での Auto-QoS の設定 (p.34-70)
- Supervisor Engine 6-E での QoS の設定 (p.34-72)



この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/cr/index.htm

Catalyst 4500 シリーズ スイッチでの QoS の概要

ネットワークは通常、ベスト エフォート型の配信方式で動作します。したがって、すべてのトラフィックに等しいプライオリティが与えられるため、正しいタイミングで配信される可能性はどのトラフィックでも同等です。輻輳が発生した場合にドロップされる可能性についても、すべてのトラフィックで同等です。

QoS は、ネットワーク トラフィック(ユニキャストおよびマルチキャスト)を選択して、トラフィックの相対的な重要度に従ってプライオリティを与え、プライオリティ ベースの処理を実行して、輻輳を回避します。 QoS はさらに、ネットワーク トラフィックが使用する帯域幅を制限します。 QoS を実装すると、ネットワーク パフォーマンスが予測可能になり、帯域幅をより効率的に利用できます。

ここでは、次の内容について説明します。

- プライオリティ(p.34-2)
- QoS の用語 (p.34-4)
- QoS の基本モデル (p.34-6)
- 分類 (p.34-7)
- ポリシングおよびマーキング (p.34-10)
- マッピング テーブル (p.34-15)
- キューイングおよびスケジューリング (p.34-15)
- パケットの変更 (p.34-17)
- PVQoS (p.34-17)
- QoS およびソフトウェア処理されるパケット (p.34-17)

プライオリティ

QoS の実装は、DiffServ アーキテクチャに基づきます。このアーキテクチャでは、ネットワークの入口で各パケットを分類すると規定されています。この分類は、IP パケット ヘッダーで伝送され、現在ほとんど使用されていない IP Type of Service (ToS; サービス タイプ)フィールドの 6 ビットを使用して分類 (クラス)情報が伝送されます。分類は、レイヤ 2 フレームで伝送される場合もあります。レイヤ 2 フレームまたはレイヤ 3 パケットのこのような特殊ビットについては、図 34-1 を参照してください。

• レイヤ2フレーム内のプライオリティ値:

レイヤ 2 の ISL(スイッチ間リンク)フレーム ヘッダーには、1 バイトのユーザ フィールドが あり、Least Significant Bit (LSB; 最下位ビット) 3 ビットで IEEE (米国電気電子学会) 802.1p Class of Service (CoS; サービス クラス)値が伝送されます。レイヤ 2 ISL トランクとして設定 されたインターフェイス上では、すべてのトラフィックが ISL フレームを使用します。

レイヤ 2 802.1Q フレーム ヘッダーには、2 バイトのタグ制御情報フィールドがあり、Most Significant Bit (MSB; 最上位ビット) 3 ビット (ユーザ プライオリティ ビットと呼ばれる) で CoS 値が伝送されます。レイヤ 2 802.1Q トランクとして設定されたインターフェイスでは、ネイティブ VLAN のトラフィックを除き、すべてのトラフィックが 802.1Q フレームに収められます。

その他のフレーム タイプでは、レイヤ 2 CoS 値は伝送されません。

レイヤ 2 CoS 値の範囲は、0 (ロー プライオリティ) ~ 7 (ハイ プライオリティ) です。

• レイヤ3パケット内の優先順位ビット:

レイヤ 3 IP パケットは、IP precedence 値または Differentiated Services Code Point(DSCP; DiffServ コード ポイント) 値のいずれかを伝送します。 DSCP 値は IP precedence 値と下位互換性があるので、 QoS ではどちらの値でも使用できます。

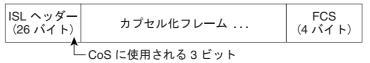
IP precedence 値の範囲は、 $0 \sim 7$ です。 DSCP 値の範囲は $0 \sim 63$ です。

図 34-1 フレームおよびパケット内の QoS 分類レイヤ

カプセル化パケット



レイヤ2ISLフレーム



レイヤ 2 802.Q/P フレーム



レイヤ3IPv4パケット



インターネット上のすべてのスイッチおよびルータはクラス情報に基づき、同じクラス情報を持ったパケットに対しては転送上、同じ取り扱いを行い、クラス情報が異なるパケットに対しては異なった取り扱いを行います。設定されたポリシー、パケットの詳しい検証、またはその両方に基づき、エンドホストあるいは途中にあるスイッチまたはルータによって、パケット内のクラス情報が割り当てられる場合があります。パケットの詳しい検証は、コアスイッチおよびルータが過負荷にならないように、ネットワークエッジに近い位置で行われることが前提になります。

パス上にあるスイッチおよびルータは、クラス情報を使用して、トラフィック クラスごとに割り当てられるリソースの量を制限できます。DiffServ アーキテクチャで個々の装置がトラフィックを処理するときの動作を、Per-Hop Behavior (PHB)といいます。パス上のすべての装置が一貫性のあるPHBを提供する場合、エンドツーエンドの QoS ソリューションを構築できます。

ネットワークに QoS を実装する作業は、インターネットワーキング装置が提供する QoS 機能、ネットワーク上のトラフィック タイプおよびトラフィック パターン、着信トラフィックおよび発信トラフィックに対して適用すべき制御の粒度に応じて、簡単なものにも複雑なものになります。

QoS の用語

QoS 機能についての説明では、次の用語が使用されます。

- パケット レイヤ3でトラフィックを伝送します。
- フレーム レイヤ 2 でトラフィックを伝送します。レイヤ 2 フレームは、レイヤ 3 パケットを伝送します。
- *ラベル* レイヤ 3 パケットおよびレイヤ 2 フレームで伝送されるプライオリティ値です。
 - レイヤ $2 \cos$ 値。範囲は 0(ロー プライオリティ) ~ 7(ハイ プライオリティ)です。 レイヤ $2 \operatorname{ISL}$ フレーム ヘッダーには、1 バイトのユーザ フィールド(LSB 3 ビットで IEEE $802.1p \cos$ 値を伝送)があります。

レイヤ 2 802.1Q フレーム ヘッダーには、2 バイトのタグ制御情報フィールドがあり、MSB 3 ビット (ユーザ プライオリティ ビット) で CoS 値が伝送されます。

その他のフレーム タイプでは、レイヤ 2 CoS 値は伝送されません。



(注)

レイヤ 2 ISL トランクとして設定されたインターフェイスでは、すべてのトラフィックが ISL フレームに収められます。レイヤ 2 802.1Q トランクとして設定されたインターフェイスでは、ネイティブ VLAN のトラフィックを除き、すべてのトラフィックが 802.1~Q フレームに収められます。

- レイヤ 3 IP precedence 値 IPv4 の仕様では、1 バイトの ToS フィールドの MSB 3 ビットを IP precedence と定義しています。IP precedence 値の範囲は、0(ロー プライオリティ)~7(ハイ プライオリティ)です。
- レイヤ 3 DSCP 値 Internet Engineering Tasks Force (IETF; インターネット技術特別調査委員会)は、1 バイトの IP ToS フィールドのうち MSB 6 ピットを DSCP と定義しています。 個々の DSCP 値が表す PHB は、設定変更可能です。DSCP 値の範囲は 0 ~ 63 です。「DSCP マップの設定」(p.34-61)を参照してください。



(注)

レイヤ 3 の IP パケットは、IP precedence 値または DSCP 値のいずれかを伝送します。 DSCP 値は IP precedence 値と下位互換性があるので、QoS ではどちらの値でも使用できます。表 34-1 を参照してください。

3 ピットの IP	ToS O 6 MSB1						6 ピットの	3 ピットの IP	To	S	の 6	M	6 ピットの			
precedence	8	7	6	5	4	3	DSCP		precedence	8	7	6	5	4	3	DSCP
0	0	0	0	0	0	0	0		4	1	0	0	0	0	0	32
	0	0	0	0	0	1	1			1	0	0	0	0	1	33
	0	0	0	0	1	0	2			1	0	0	0	1	0	34
	0	0	0	0	1	1	3			1	0	0	0	1	1	35
	0	0	0	1	0	0	4			1	0	0	1	0	0	36
	0	0	0	1	0	1	5			1	0	0	1	0	1	37
	0	0	0	1	1	0	6			1	0	0	1	1	0	38
	0	0	0	1	1	1	7			1	0	0	1	1	1	39
1	0	0	1	0	0	0	8		5	1	0	1	0	0	0	40
	0	0	1	0	0	1	9			1	0	1	0	0	1	41
	0	0	1	0	1	0	10			1	0	1	0	1	0	42
	0	0	1	0	1	1	11			1	0	1	0	1	1	43
	0	0	1	1	0	0	12			1	0	1	1	0	0	44
	0	0	1	1	0	1	13			1	0	1	1	0	1	45
	0	0	1	1	1	0	14			1	0	1	1	1	0	46
	0	0	1	1	1	1	15			1	0	1	1	1	1	47
2	0	1	0	0	0	0	16		6	1	1	0	0	0	0	48
	0	1	0	0	0	1	17			1	1	0	0	0	1	49
	0	1	0	0	1	0	18			1	1	0	0	1	0	50
	0	1	0	0	1	1	19			1	1	0	0	1	1	51
	0	1	0	1	0	0	20			1	1	0	1	0	0	52
	0	1	0	1	0	1	21			1	1	0	1	0	1	53
	0	1	0	1	1	0	22			1	1	0	1	1	0	54
	0	1	0	1	1	1	23			1	1	0	1	1	1	55
3	0	1	1	0	0	0	24		7	1	1	1	0	0	0	56
	0	1	1	0	0	1	25			1	1	1	0	0	1	57
	0	1	1	0	1	0	26			1	1	1	0	1	0	58
	0	1	1	0	1	1	27			1	1	1	0	1	1	59
	0	1	1	1	0	0	28			1	1	1	1	0	0	60
	0	1	1	1	0	1	29			1	1	1	1	0	1	61
	0	1	1	1	1	0	30			1	1	1	1	1	0	62
	0	1	1	1	1	1	31			1	1	1	1	1	1	63

表 34-1 IP precedence 値および DSCP 値

- 1. MSB = Most Significant Bit (最上位ビット)
- 分類 マーク付けするトラフィックを選択することです。
- マーキング RFC 2475 に従い、レイヤ 3 の DSCP 値をパケットに設定する処理です。このマニュアルでは、マーキングの定義を拡大して、レイヤ 2 CoS 値の設定までを含めています。
- スケジューリング レイヤ 2 フレームをキューに割り当てることです。QoS は、内部 DSCP 値 (内部 DSCP 値 [p.34-14] を参照)に基づいて、キューにフレームを割り当てます。
- *ポリシング* トラフィック フローが使用する帯域幅を制限する処理です。ポリシングによって、トラフィックのマーキングまたはドロップが可能になります。

QoS の基本モデル

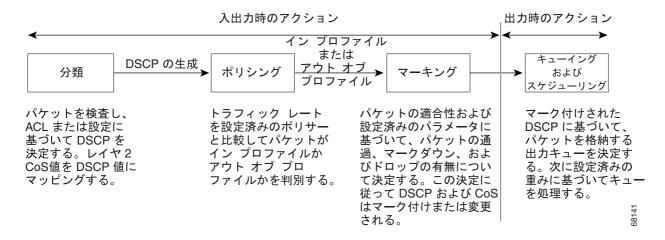
図 34-2 に、QoS の基本モデル(スイッチ QoS モデルとも呼びますが、MQC 準拠ではありません)を示します。入力インターフェイスおよび出力インターフェイスで行われるアクションには、トラフィックの分類、ポリシング、およびマーキングがあります。

- 分類は、トラフィックの種類を区別します。このプロセスによって、パケットの内部 DSCP が 生成されます。内部 DSCP は、今後このパケットに対して実行されるすべての QoS アクション を表します。詳細については、「分類」(p.34-7) を参照してください。
- ポリシングは、トラフィック レートを設定済みのポリサーと比較することによって、パケットがイン プロファイルであるか、それともアウト オブ プロファイルであるかを判別します。ポリサーは、トラフィック フローが消費する帯域幅を制限します。この判別の結果が、マーカーに引き渡されます。詳細については、「ポリシングおよびマーキング」(p.34-10)を参照してください。
- マーキングは、パケットがアウト オブ プロファイルのときに行われるアクションに関してポリサーの設定情報を評価し、パケットの処置(変更なしにパケットを通過させるか、パケット内の DSCP 値をマーク ダウンするか、パケットをドロップするか)を決定します。詳細については、「ポリシングおよびマーキング」(p.34-10)を参照してください。

出力インターフェイスで行われるアクションには、キューイングおよびスケジューリングがあります。

- キューイングは、内部 DSCP を評価し、4 つの出力キューのどれにパケットを入れるかを決定します。
- スケジューリングは、出力(送信)ポートの共有およびシェーピング設定に基づいて、4 つの 出力(送信)キューを処理します。共有およびシェーピング設定については、「キューイング およびスケジューリング」(p.34-15)を参照してください。

図 34-2 QoS の基本モデル



分類

分類は、パケットの各フィールドを検証することで、トラフィックの種類を区別するプロセスです。 スイッチ上で QoS がグローバルにイネーブルに設定されている場合に限り、分類がイネーブルになります。デフォルトでは、QoS はグローバルでディセーブルに設定されているため、分類は行われません。

フレームまたはパケットの、どのフィールドを使用して着信トラフィックを分類するかを、ユーザが指定します。

図 34-3 に、さまざまな分類オプションを示します。

IP以外のトラフィックについては、次の分類オプションがあります。

- ポート デフォルトを使用します。パケットが IP 以外のパケットである場合、デフォルトのポート DSCP 値を着信パケットに割り当てます。
- 着信フレームの CoS 値を信頼します (ポートを Trust CoS に設定する)。この場合、設定変更可能な CoS/DSCP マップを使用して、内部 DSCP 値を生成します。レイヤ 2 ISL フレーム ヘッダーでは、1 バイトのユーザ フィールドの LSB 3 ビットを使用して CoS 値を伝送します。レイヤ 2 802.1Q フレーム ヘッダーでは、タグ制御情報フィールドの MSB 3 ビットを使用して CoS 値を伝送します。CoS 値の範囲は、0 (ロー プライオリティ) ~ 7 (ハイ プライオリティ)です。フレームに CoS 値が含まれていない場合は、着信フレームにデフォルトのポート CoS を割り当てます。

Trust DSCP の設定は、IP 以外のトラフィックに対しては無意味です。ポートを Trust DSCP に設定し、IP 以外のトラフィックを受信した場合、スイッチはデフォルトのポート DSCP を割り当てます。

IP トラフィックについては、次の分類オプションがあります。

- 着信パケットの IP DSCP を信頼し(ポートを Trust DSCP に設定し)、パケットに同じ DSCP を割り当てて内部的に使用します。IETF は、1 バイトの ToS フィールドの MBB 6 ビットを DSCP として定義しています。個々の DSCP 値が表すプライオリティは、設定変更可能です。DSCP 値の範囲は $0\sim63$ です。
- 着信パケットの CoS 値(存在する場合)を信頼し、CoS/DSCP マップを使用して DSCP を生成します。
- 設定された IP 標準 Access Control List (ACL; アクセス コントロール リスト) または拡張 ACL (IP ヘッダーの各種のフィールドを検証する) に基づいて、分類を実行します。ACL を設定していない場合は、入力ポートの信頼状態に基づいてデフォルトの DSCP がパケットに割り当てられます。ACL を設定している場合は、ポリシー マップによって着信フレームに割り当てる DSCP が指定されます。



(注)

入力 QoS ポリシーが実行するマーキングに基づいてトラフィックを分類することはできません。 Catalyst 4500 プラットフォームでは、入力および出力 QoS の検索が平行して実行されるため、出力 QoS ポリシーでトラフィックを分類するのに入力時にマーク付けされた DSCP 値を使用できません。

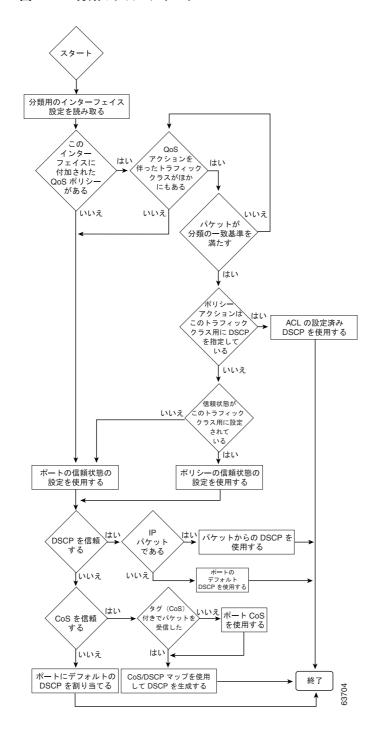


(注)

内部DSCP に基づいてトラフィックを分類することはできません。内部DSCP は、すべてのパケットで送信キューおよび送信 CoS 値を決定するのにのみ使用される純粋な内部分類メカニズムです。

ここで説明するマップについての詳細は、「マッピング テーブル」(p.34-15)を参照してください。ポートの信頼状態の設定手順については、「インターフェイスの信頼状態の設定」(p.34-56)を参照してください。

図 34-3 分類のフローチャート



QoS ACL に基づく分類

QoS のパケット分類は、複数の一致基準を使用して行うことができ、指定された一致基準をパケットがすべて満たしている必要があるか、または少なくとも 1 つの一致基準を満たしていればよいかを指定できます。 QoS 分類基準を定義するには、クラス マップで一致 (match) 文を使用して一致基準を指定します。一致文では、マッチングの対象になるパケットのフィールドを指定することも、IP 標準 ACL または IP 拡張 ACL を使用することもできます。詳細については、「クラス マップおよびポリシー マップに基づく分類」(p.34-10) を参照してください。

すべての一致基準に一致するようにクラス マップを設定した場合、パケットがクラス マップ内のすべての一致文を満たしていないと、QoS アクションは実行されません。パケットがクラス マップの一致基準を1つでも満たさない場合、そのパケットについて QoS アクションは実行されません。

最低 1 つの一致基準に一致するようにクラス マップを設定した場合、パケットがクラス マップ内 の少なくとも 1 つの一致文を満たしていれば、QoS アクションが実行されます。パケットがクラス マップの一致基準をどれも満たしていない場合、そのパケットについて QoS アクションは実行されません。



<u>—</u> (注)

IP 標準 ACL および IP 拡張 ACL を使用する場合、QoS コンテキストでは、ACL の中の許可(permit) Access Control Entry (ACE; アクセス コントロール エントリ)と拒否 (deny) ACE の意味は多少異なります。

- [permit] を指定している ACE を検出し、なおかつパケットがそれを満たしている場合、そのパケットは QoS 分類の一致基準に「一致した」ことになります。
- [deny] を指定している ACE を検出し、なおかつパケットがそれを満たしている場合、そのパケットは QoS 分類の一致基準に「一致しない」ことになります。
- 一致する許可(permit)アクションが検出されないまま、すべての ACE の検証が終わった場合、 そのパケットは QoS 分類の基準に「一致しない」ことになります。



(注)

アクセス リストを作成するとき、アクセス リストの末尾にはデフォルトで、リストの末尾に達しても一致が見つからなかった場合に使用される、暗黙の拒否 (deny) 文がある点に留意してください。

クラスマップを使用してトラフィッククラスを定義したあとで、トラフィッククラスに対するQoSアクションを定義するポリシーを作成できます。ポリシーでは、複数のクラスのそれぞれについて、アクションを指定できます。ポリシーには、クラスを集約的に分類する(たとえば、DSCPを割り当てる)コマンド、またはクラスをレート制限するコマンドを組み込めます。このポリシーを特定のポートに付加して、そのポート上でポリシーを有効にします。

IP トラフィックを分類するための IP ACL を実装するには、access-list グローバル コンフィギュレーション コマンドを使用します。詳しい設定手順については、「QoS ポリシーの設定」(p.34-35)を参照してください。

クラス マップおよびポリシー マップに基づく分類

クラス マップは、特定のトラフィック フロー(クラス)を、他のすべてのトラフィックから切り離して名前を付けるためのメカニズムです。クラス マップは、特定のトラフィック フローを分類する目的で使用する一致基準を定義します。基準としては、ACL で定義されるアクセス グループとのマッチング、または特定の DSCP 値、IP precedence 値、または L2 CoS 値のリストとのマッチングを指定できます。複数のタイプのトラフィックを分類する必要がある場合は、別のクラス マップを別の名前で作成します。クラス マップの基準に関するパケットのマッチングが終わったあとで、ポリシー マップを使用して QoS アクションを指定できます。

ポリシー マップは、各トラフィック クラスに対する QoS アクションを指定します。アクションとしては、トラフィック クラスの CoS 値または DSCP 値を信頼すること、トラフィック クラスの特定の DSCP 値または IP precedence 値の設定、またはトラフィックの帯域幅制限の指定およびトラフィックがアウト オブ プロファイルであるときのアクションを含めることができます。ポリシーマップを有効にするには、インターフェイスにポリシーマップを付加する必要があります。

クラス マップを作成するには、class-map グローバル コンフィギュレーション コマンドを使用します。class-map コマンドを入力すると、スイッチはクラス マップ コンフィギュレーション モードになります。このモードでは、match クラス マップ コンフィギュレーション コマンドを使用して、トラフィックの一致基準を定義します。

ポリシー マップを作成して名前を付けるには、policy-map グローバル コンフィギュレーション コマンドを使用します。このコマンドを入力すると、スイッチはポリシー マップ コンフィギュレーション モードになります。このモードで、trust または set ポリシー マップ コンフィギュレーション コマンドおよびポリシー マップ クラス コンフィギュレーション コマンドを使用して、特定のトラフィック クラスに対して実行すべきアクションを指定します。ポリシー マップを有効にするには、service-policy インターフェイス コンフィギュレーション コマンドを使用して、ポリシー マップをインターフェイスに対応付けます。

ポリシー マップには、ポリサーを定義するコマンド (トラフィックの帯域幅制限) および制限を超過した場合に実行するアクションを含めることもできます。詳細については、「ポリシングおよびマーキング」 (p.34-10) を参照してください。

ポリシー マップには、次のような特性もあります。

- 1 つのポリシー マップに、最大 255 のクラス文を指定できます。
- 1 つのポリシーマップで異なるクラスを指定できます。
- ポリシーマップの信頼状態は、インターフェイスの信頼状態を上書きします。

詳しい設定手順については、「QoS ポリシーの設定」(p.34-35)を参照してください。

ポリシングおよびマーキング

パケットが分類され、パケットに内部 DSCP 値が割り当てられると、ポリシングおよびマーキングのプロセスが開始可能になります(図 34-4 を参照)。

ポリシングを行うには、トラフィックの帯域幅制限を指定するポリサーを作成します。この制限を超過するパケットは、アウト オブ プロファイルつまり 不適合パケットです。各ポリサーは、インプロファイルまたはアウト オブ プロファイル パケットに対して実行すべきアクションを指定します。これらのアクション(マーカーによって実行される)では、パケットを変更せずにそのまま通過させること、パケットをドロップすること、または、設定変更可能なポリシング済み DSCP マップから得られる新しい DSCP 値にパケットをマークダウンすることが可能です。ポリシング済みDSCP マップの詳細については、「マッピング テーブル」(p.34-15)を参照してください。

次の種類のポリサーを作成できます。

• 個別

ポリシー マップが付加されている各ポート /VLAN に対して、QoS がポリサーで指定される帯域幅制限を一致する各トラフィック クラスに個別に適用します。ポリシー マップでこのタイプのポリサーを設定するには、ポリシー マップ クラス コンフィギュレーション モードで police コマンドを使用します。

集約

一致するすべてのトラフィック フローに、集約ポリサーで指定される帯域幅制限を QoS が累積的に適用します。ポリシー マップで、集約ポリサー名を指定してこのタイプのポリサーを設定するには、police aggregate ポリシー マップ コンフィギュレーション コマンドを使用します。ポリサーの帯域幅制限を指定するには、qos aggregate-policer グローバル コンフィギュレーション コマンドを使用します。集約ポリサーは、1 つのポリシー マップ内で複数のトラフィック クラスによって共有されます。

フローまたはマイクロフロー

フローベースのポリシングでは、識別されたすべてのフローが、指定したレートに個別にポリシングされます。フローはダイナミックなので、キー識別フィールドをクラス マップで設定する必要があります。2 つのフロー一致オプション、送信元 IP ベース(送信元 IP アドレスが一意であるそれぞれのフローを新しいフローとして扱う) および宛先 IP ベース(宛先 IP アドレスが一意であるそれぞれのフローを新しいフローとして扱う) を指定できます。フローベースのポリサーの設定については、「UBRL の設定」(p.34-45) を参照してください。

ポリシングおよびポリサーを設定する場合、次の点に注意してください。

• IP パケットでは、IP ペイロードの長さ(IP ヘッダーの全長フィールド)だけがポリシング演算でポリサーに使用されます。レイヤ 2 ヘッダーとトレーラーの長さは計上されていません。たとえば、64 バイトの Ethernet II IP パケットでは、46 バイトだけがポリシングに計上されます(64 バイト - 14 バイトのイーサネット ヘッダー - 4 バイトのイーサネット CRC)。

IP 以外のパケットでは、レイヤ 2 ヘッダーに指定されたレイヤ 2 の長さは、ポリシング演算でポリサーに使用されます。IP パケットをポリシングする場合、さらにレイヤ 2 カプセル化の長さを指定するには、gos account layer2 encapsulation コマンドを使用します。

- デフォルトで設定されるポリサーはありません。
- 設定できるのは、平均レートおよび認定バースト パラメータだけです。
- 個別ポリサーおよび集約ポリサーのポリシングは、入力インターフェイスと出力インターフェイスのどちらでも行えます。
 - Supervisor Engine V-10GE(WS-X4516-10GE)の場合は、8192 個のポリサーが入力および出力でサポートされます。
 - その他のスーパーバイザエンジンでは、1024個のポリサーが入力および出力でサポートされます。



E) 入力および出力の方向で4個のポリサーが予約されています。

- ポリサーは、個別タイプか集約タイプにすることができます。Supervisor Engine V-10GE では、フローベース ポリサーがサポートされます。
- フローポリサーのポリシングは、入力レイヤ3インターフェイスのみで行えます。
 - Supervisor Engine V-10GE では、512 個の一意のフロー ポリサーを設定できます。



1 つのフロー ポリサーがソフトウェアによって予約されているので、511 個の一意のフローポリサーを定義できます。

- 100,000 より多いフローをマイクロフロー ポリシングできます。



(注)

マイクロフローでは、現在のところ 2 つのフロー一致オプション (送信元 IP アドレス ベースおよび宛先 IP アドレス ベース) がサポートされます。マイクロフロー ポリシングを Netflow 統計情報収集と併用するとき、送信元 IP アドレスか宛先 IP アドレスが一致するフローの完全なフロー統計は使用できません。Netflow 統計の設定については、「NetFlow 統計情報収集機能のイネーブル化」(p.48-8) を参照してください。

• QoS を設定したインターフェイス上では、そのインターフェイス経由で送受信されるすべてのトラフィックが、インターフェイスに付加されたポリシー マップに従って、分類、ポリシング、およびマーク付けされます。ただし、インターフェイスが qos vlan-based コマンドによって VLAN ベース QoS を使用するように設定されている場合は、そのインターフェイス経由で送受信されるトラフィックは、パケットの所属先 VLAN に付加されたポリシー マップ(VLAN インターフェイス上に設定されている)に従って、分類、ポリシング、およびマーク付けされます。パケットの所属先 VLAN にポリシー マップが付加されていない場合には、インターフェイスに付加されたポリシー マップが使用されます。

ポリシー マップおよびポリシング アクションを設定したあと、service-policy インターフェイス コンフィギュレーション コマンドを使用して、入力インターフェイスまたは出力インターフェイスにポリシーを付加します。詳しい設定手順については、「QoS ポリシーの設定」(p.34-35) および「名前付き集約ポリサーの作成」(p.34-33) を参照してください。

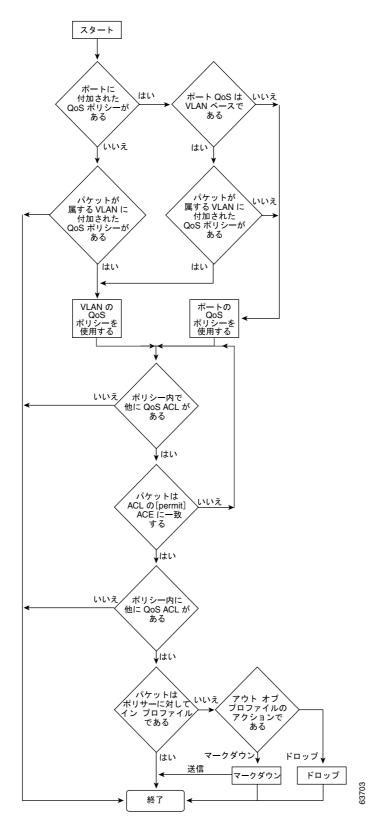


図 34-4 ポリシングおよびマーキングのフローチャート

内部 DSCP 値

ここでは、内部 DSCP 値について説明します。

- 内部 DSCP の作成元 (p.34-14)
- 出力 ToS および CoS の作成元 (p.34-14)

内部 DSCP の作成元

QoS は処理中、すべてのトラフィック (IP 以外のトラフィックを含む) のプライオリティを、内部 DSCP 値で表します。 QoS は、以下に基づいて内部 DSCP 値を導き出します。

- Trust CoS トラフィックの場合、受信したレイヤ 2 CoS 値または入力インターフェイスのレイヤ 2 CoS 値
- Trust DSCP トラフィックの場合、受信した DSCP 値または入力インターフェイスの DSCP 値
- 信頼されない(untrusted)トラフィックの場合、入力インターフェイスの DSCP 値

トラフィックの信頼状態は、入力インターフェイスの信頼状態です。ただし、ポリシー アクション によりトラフィック クラスに対して別の設定が行われる場合を除きます。

QoS は、設定変更可能な各種のマッピング テーブルを使用して、3 ビットの CoS から 6 ビットの内部 DSCP 値を導き出します (「DSCP マップの設定」[p.34-61] を参照)。

出力 ToS および CoS の作成元

出力 IP トラフィックについては、QoS は内部 DSCP 値から ToS バイトを作成して、出力インターフェイスに送信し、それが IP パケットに書き込まれます。 trust dscp および untrusted IP トラフィックの場合、ToS バイトには、受信した ToS バイトの元の LSB 2 ビットが含まれます。



内部 ToS 値は IP precedence 値を使用します (表 34-1 [p.34-5] を参照)。

すべての出力トラフィックについて、QoS は設定変更可能なマッピング テーブルを使用して、トラフィックと対応付けられた内部 ToS 値から CoS 値を導き出します (「DSCP/CoS マップの設定」 [p.34-63] を参照)。

すべての出力トラフィックについて、QoS は設定変更可能なマッピング テーブルを使用して、トラフィックと対応付けられた内部 ToS 値から CoS 値を導き出します (「DSCP/CoS マップの設定」 [p.34-63] を参照)。QoS は CoS 値を送信して、ISL フレームおよび 802.1Q フレームに書き込ませます。

qos trust cos コマンドを使用して *trust cos* に設定された入力インターフェイスに着信したトラフィックの場合、送信される CoS は、常に着信パケットの CoS (または、パケットをタグなしで受信した場合には、入力インターフェイスのデフォルト CoS)です。

qos trust dscp コマンドを使用してインターフェイスの信頼状態を *trust dscp* に設定していない場合、セキュリティおよび QoS ACL 分類では、常にインターフェイス DSCP が使用され、着信パケットの DSCP は使用されません。

マッピング テーブル

QoS の処理中、スイッチはすべてのトラフィック(IP 以外のトラフィックを含む)のプライオリティを、内部 DSCP 値で表します。

- 分類の際、QoS は設定変更可能なマッピング テーブルを使用して、受信した CoS から内部 DSCP (6 ビット値)を導き出します。これらのマップには、CoS/DSCP マップが含まれます。
- ポリシングの際、QoS は IP パケットまたは IP 以外のパケットに別の DSCP 値を割り当てることがあります (パケットがアウト オブ プロファイルであり、なおかつポリサーでマークダウン後の DSCP 値が指定されている場合)。この設定変更可能なマップを、ポリシング済み DSCPマップといいます。
- トラフィックがスケジューリング段階に達する前に、QoS は内部 DSCP を使用して、4 つの出力キューのうち 1 つを出力処理用に選択します。DSCP から出力キューへのマッピングは、qos map dscp to tx-queue コマンドを使用して設定します。

CoS/DSCP および DSCP/CoS マップのデフォルト値は、ネットワークに適している場合も、適していない場合もあります。

詳しい設定手順については、「DSCPマップの設定」(p.34-61)を参照してください。

キューイングおよびスケジューリング

各物理ポートには、4 つの送信キュー(出力キュー)があります。送信する必要がある各パケットは、いずれかの送信キューに格納されます。各送信キューは、送信キュー スケジューリング アルゴリズムに基づいて処理されます。

(DSCP のマークダウンも含めて)最終的な送信 DSCP が算出されると、送信 DSCP と送信キューのマッピング設定によって、送信キューが決定されます。パケットは、送信 DSCP から決定された送信ポートの送信キューに格納されます。送信 DSCP と送信キューのマッピングを設定するには、qos map dscp to tx-queue コマンドを使用します。パケットが入力ポートおよび出力ポートの QoS ポリシーおよび信頼状態の設定によって判別された IP 以外のパケットである場合、送信 DSCP は内部 DSCP 値です。

詳しい設定手順については、「送信キューの設定」(p.34-59)を参照してください。

AQM

Active Queue Management (AQM) は、バッファ オーバーフローが発生する前に輻輳に関して通知する先行型の手法です。AQM は、Dynamic Buffer Limiting (DBL) を使用して実行されます。DBL はスイッチ内の各トラフィックのキュー長を追跡します。フローのキュー長が制限を超えると、DBL はパケットをドロップするか、パケット ヘッダーの Explicit Congestion Notification (ECN; 明示的輻輳通知) ビットを設定します。

DBL は、フローをアダプティブとアグレッシブの 2 つのカテゴリに分類します。アダプティブ フローは、輻輳通知を受信するとパケット伝送レートを減らします。アグレッシブ フローは、輻輳通知に対してどのような修正措置も行いません。すべてのアクティブ フローに対して、スイッチは [buffersUsed] および [credits] という 2 つのパラメータを保持します。すべてのフローは、グローバル パラメータの [max-credits] から開始されます。credits が [aggressive-credits] (別のグローバル パラメータ) より少ないフローの場合、アグレッシブ フローとみなされ、[aggressiveBufferLimit] と呼ばれる小さなバッファ制限が指定されます。

キュー長は、パケット数によって測定されます。キュー内のパケット数により、フローに与えられるバッファスペースのサイズが決定します。フローのキュー長が長い場合、算出値は低下します。これにより、新規着信フロー用のバッファスペースがキュー内に確保されます。この結果、すべてのフローが、キュー内につり合いがとれた割合のパケットを置くことができます。

インターフェイスごとに 4 つの送信キューがあり、DBL はキュー単位のメカニズムであるため、DSCP 値により DBL の適用がさらに複雑になる可能性があります。

次の表に、デフォルトの DSCP と送信キューのマッピングを示します。

DSCP	txQueue
0 ~ 15	1
16 ~ 31	2
32 ~ 48	3
49 ~ 63	4

たとえば、2 つのストリームを送信するとき、1 つのストリームは 16 の DSCP で、もう1 つのストリームは値が0 の場合、これらのストリームは別々のキューから送信されます。 $txQueue\ 2$ のアグレッシブ フロー(16 の DSCP を持つパケット)がリンクを飽和させる可能性があっても、0 の DSCP のパケットは $txQueue\ 1$ から送信されるため、アグレッシブ フローでブロックされません。したがって、DBL がなくても、DSCP 値によって $txQueue\ 1$ 、3、4 に配置されるパケットはアグレッシブ フローによって廃棄されません。

送信キュー間のリンク帯域幅の共有

送信ポートの4つの送信キューは、その送信ポートで使用できるリンク帯域幅を共有します。送信キュー間でリンク帯域幅を共有する方法を変更するには、インターフェイス送信キュー コンフィギュレーション モードで bandwidth コマンドを使用します。このコマンドを使用して、各送信キューに最低限保証される帯域幅を指定します。

デフォルトでは、すべてのキューがラウンド ロビン方式でスケジューリングされています。

Supervisor Engine II-Plus、Supervisor Engine III、Supervisor Engine IV を使用するシステムの場合、帯域幅を設定できるのは次のポートに限られます。

- スーパーバイザ エンジン上のアップリンク ポート
- WS-X4306-GB GBIC モジュール上のポート
- WS-X4506-GB-T CSFP モジュール上のポート
- WS-X4232-GB-RJ モジュール上の 2 つの 1000BASE-X ポート
- WS-X4418-GB モジュール上の最初の 2 つのポート
- WS-X4412-2GB-TX モジュール上の 2 つの 1000BASE-X ポート

Supervisor Engine V を使用するシステムの場合、帯域幅はすべてのポート (10/100 ファスト イーサネット、10/100/1000BASE-T、1000BASE-X) で設定できます。

ストリクト プライオリティ / 低遅延キューイング

インターフェイスコンフィギュレーション モードで priority high 送信キュー コンフィギュレーション コマンドを使用し、各ポートの送信キュー 3 に高いプライオリティを設定できます。送信キュー 3 に高いプライオリティを設定した場合、送信キュー 3 のパケットは、他のキューのパケットよりも優先的にスケジューリングされます。

送信キュー3に高いプライオリティを設定した場合、パケットが他の送信キューよりも優先的にスケジューリングされるのは、割り当てられた帯域幅共有の設定を超えていない場合に限られます。設定されたシェープレートを超過するトラフィックは、キューに格納されたあと、設定された速度で送信されます。バーストトラフィックによってキューの容量を超過した場合には、設定されたシェープレートを維持するために、パケットがドロップされます。

トラフィック シェーピング

トラフィック シェーピングは、トラフィックが設定上の最大送信速度に従うように、発信トラフィックの速度を制御する能力を提供します。ある制限に適合するトラフィックを、ダウンストリーム トラフィックの速度要件を満たすようにシェーピングし、データ速度の不一致を解消できます。

各送信キューに最大速度を設定するには、shape コマンドを使用します。この設定により、トラフィックの最大速度を指定できます。設定されたシェープレートを超過するトラフィックは、キューに格納されたあと、設定された速度で送信されます。バーストトラフィックによってキューの容量を超過した場合には、設定されたシェープレートを維持するために、パケットがドロップされます。

パケットの変更

パケットの分類、ポリシング、およびキューイングによって、QoS が提供されます。次のプロセスで、パケットの変更が行われることがあります。

- IP パケットの場合、分類によって、パケットに DSCP が割り当てられます。ただし、この段階でパケットは変更されません。割り当てられた DSCP が伝送されるだけです。その理由は、QoSの分類と ACL の検索が並行して実行され、ACL によってパケットの拒否とロギングが指示される場合があるためです。この状況では、パケットは元の DSCP 付きで CPU に転送され、CPUで再び ACL ソフトウェアによって処理されます。
- IP 以外のパケットの場合、分類によってパケットに内部 DSCP が割り当てられますが、非 IP パケットに DSCP はないので、上書きは行われません。代わりに、内部 DSCP がキューイングおよびスケジューリング決定の両方で使用され、さらにパケットが ISL または 802.1Q トランクポートのいずれかで送信される場合、タグへの CoS プライオリティ値の書き込みに使用されます。
- ポリシングでは、IP パケットおよび IP 以外のパケットに別の DSCP が割り当てられます(パケットがアウト オブ プロファイルであり、なおかつポリサーでマークダウン DSCP が指定されている場合)。この場合にも、パケットの DSCP は変更されませんが、マークダウン後の値が伝えられます。IP パケットの場合、あとの段階でパケットの変更が行われます。

PVQoS

PVQoS により、トランク ポート上の個別の VLAN に差別化された QoS が提供されます。この機能により、サービス プロバイダーはビジネスまたは住宅への各トランク ポートの個々の VLAN ベース サービスをレート制限できるようになります。企業の Voice over IP(VoIP) 環境で、攻撃者が IP Phone になりすましている場合でも、この機能を使用して音声 VLAN をレート制限できます。ポート単位 VVLAN 単位サービス ポリシーは、入力トラフィックまたは出力トラフィックのいずれかに 別々に適用できます。

QoS およびソフトウェア処理されるパケット

Catalyst 4500 プラットフォームは、Cisco IOS ソフトウェアによって転送または生成されるパケットに、QoS マーキングまたはポリシング コンフィギュレーションを適用しません。これは、Cisco IOS がパケットを転送または生成している場合、ポートあるいは VLAN で設定された入力または出力 QoS ポリシーはパケットに適用されないためです。

ただし、Cisco IOS は生成された制御パケットすべてを正しくマーク付けし、内部 IP DSCP を使用して出力送信インターフェイスで送信キューを判断します。IP パケットの場合、内部 IP DSCP は IP パケットの IP DSCP フィールドにあります。IP 以外のパケットの場合、Cisco IOS は内部でパケットプライオリティを割り当て、内部 IP DSCP 値にマッピングします。

Cisco IOS は IP precedence 値 6 をコントロール プレーン上のルーティング プロトコル パケットに割り当てます。RFC 791 での記載のとおり、「インターネットワークの制御指定は、ゲートウェイ制御発信元が使用するためだけのものです」。つまり、Cisco IOS は IP ベースの制御パケット (Open Shortest Path First [OSPF]、Routing Information Protocol [RIP]、Enhanced Interior Gateway Routing Protocol [EIGRP] hello、キープアライブ)をマーク付けします。ルータへの、およびルータからの Telnet パケットにも IP precedence 値 6 が与えられます。出力インターフェイスがパケットをネットワークに送信した場合、割り当てられた値はパケットとともに残ります。

レイヤ 2 制御プロトコルの場合、ソフトウェアは内部 IP DSCP を割り当てます。通常、レイヤ 2 制御プロトコル パケットは、内部 DSCP 値 48 (IP precedence 値 6 に対応)が割り当てられます。

内部 IP DSCP は、送信インターフェイス上で待機状態のパケットの送信キューを特定するために使用します。キューを送信するよう DSCP を設定する方法については、「送信キューの設定」(p.34-59) を参照してください。

内部 IP DSCP は、トランク インターフェイス上でパケットが IEEE 802.1Q または ISL タグ付きで送信される場合、送信 CoS マーキングを決定するのにも使用します。 DSCP/CoS マッピングを設定する方法については、「DSCP/CoS マップの設定」(p.34-63) を参照してください。

Supervisor Engine II-Plus、II+10GE、VI、V、V-10GE、4924、4948、および 4948-10GE での Auto-QoS の設定

Auto-QoS 機能を使用すると、既存の QoS 機能の使用を簡略化できます。Auto-QoS はネットワーク 設計に関する予測を行うもので、それによってスイッチは、デフォルトの QoS 動作を使用せずにトラフィック フローごとに優先順位を付け、適切に出力キューを使用できます(デフォルトでは、 QoS はディセーブルです。スイッチではパケットの内容やサイズに関係なく、各パケットにベストエフォート型サービスが提供され、単一キューでパケットを送信します)。

Auto-QoS をイネーブルにすると、入力パケット ラベルに基づいてトラフィックを自動的に分類します。スイッチはこの分類結果を使用して適切な出力キューを選択します。

Auto-QoS コマンドを使用し、Cisco IP Phone と接続しているポートを識別し、アップリンクを通じて信頼できる VoIP トラフィックを受信するポートを識別します。そのあと、Auto-QoS は次の機能を実行します。

- IP Phone の有無を検出します。
- QoS 分類を設定します。
- 出力キューを設定します。

ここでは、スイッチ上で Auto-QoS を設定する手順について説明します。

- 生成される Auto-QoS 設定 (p.34-19)
- Auto-QoS の設定上の影響(p.34-20)
- 設定時の注意事項 (p.34-21)
- VoIP 用の Auto-QoS のイネーブル化 (p.34-21)

生成される Auto-QoS 設定

デフォルトでは、Auto-QoS はすべてのインターフェイス上でディセーブルに設定されています。

最初のインターフェイス上で Auto-QoS 機能をイネーブルにすると、次の動作が自動的に発生します。

- QoS がグローバルにイネーブルになります (qos グローバル コンフィギュレーション コマンド)。
- DBL がグローバルにイネーブルになります (qos dbl グローバル コンフィギュレーション コマンド)。
- auto qos voip trust インターフェイス コンフィギュレーション コマンドを入力すると、指定されたインターフェイスがレイヤ 2 として設定されている場合、インターフェイス上の入力分類は、パケット内で受信される CoS ラベルを信頼するように設定されます。インターフェイスがレイヤ 3 として設定されている場合は、DSCP を信頼するように設定されます(表 34-2 を参照)。
- auto qos voip cisco-phone インターフェイス コンフィギュレーション コマンドを入力すると、信頼境界機能がイネーブルになります。この機能は、Cisco Discovery Protocol (CDP; シスコ検出プロトコル)を使用して Cisco IP Phone の有無を検出します。Cisco IP Phone が検出されたとき、インターフェイスをレイヤ 2 として設定している場合、インターフェイスの入力分類は、パケットで受信した CoS ラベルを信頼するように設定されます。インターフェイスをレイヤ 3 として設定している場合、分類は DSCP を信頼するように設定されます。Cisco IP Phone が存在しない場合、パケットの CoS ラベルを信頼しないようにインターフェイスの入力分類が設定されます。



注) 指定ポートでは、Cisco IP Phone 検出情報がスタンバイ スーパーバイザ エンジンで更新されません。スタンバイ エンジンがアクティブになると、CDP を通じて Cisco IP Phone を再検出します。したがって、SSO スイッチオーバー後に短期間ポートが信頼状態になりません。

信頼境界機能の詳細については、「信頼境界の設定によるポート セキュリティの確保 (p.34-28) を参照してください。

auto qos voip cisco-phone または auto qos voip trust インターフェイス コンフィギュレーション コマンドを使用して Auto-QoS をイネーブルにすると、スイッチはトラフィック タイプと入力パケットラベルに基づいて自動的に QoS 設定を生成し、表 34-2 に示されるコマンドをインターフェイスに適用します。

表 34-2 生成される Auto-QoS 設定

説明	自動的に生成されるコマンド
スイッチが標準 QoS を自動的にイネーブルにし、DBL が CoS/DSCP マップ(着信パケット内の CoS 値を DSCP 値に マッピングします)を設定します。	Switch(config)# qos Switch(config)# qos map cos 3 to 26 Switch(config)# qos dbl Switch(config)# qos map cos 5 to 46
スイッチが自動的に DSCP/Tx キュー マッピングを設定します。	Switch(config) # qos map dscp 24 25 26 27 b28 29 30 31 to tx-queue 4 Switch(config) # qos map dscp 32 33 34 35 36 37 38 39 to tx-queue 4
スイッチが、パケットで受信される CoS/DSCP 値を信頼するように、インターフェイス上の入力分類を自動的に設定します。	Switch(config-if)# qos trust cos または Switch(config-if)# qos trust dscp
スイッチは、自動的に QoS サービス ポリシーを作成し、ポリシー上で DBL をイネーブルにし、インターフェイスに付加します。	Switch(config) # policy-map autoqos-voip-policy Switch(config-pmap) # class class-default Switch(config-pmap-c) # dbl
auto qos voip cisco-phone コマンドを入力すると、スイッチは自動的に信頼境界機能をイネーブルにします。この機能は、CDP を使用して Cisco IP Phone の有無を検出するものです。	Switch(config-if)# qos trust device cisco-phone
スイッチがより高いプライオリティをキュー 3 に割り当てます。キュー 3 のシェーピング制限が選択されるので、リンク速度は 33% です。共有がサポートされているポートにシェーピングを 33% として設定します。	Switch(config-if)# tx-queue 3 Switch(config-if-tx-queue)# priority high Switch(config-if-tx-queue)# shape percent 33 Switch(config-if-tx-queue)# bandwidth percent 33
これにより、より高いプライオリティのキューが他の キューを停止させないようになります。	

Auto-QoS の設定上の影響

Auto-QoS がイネーブルの場合、auto qos voip インターフェイス コンフィギュレーション コマンド および生成された設定が、実行コンフィギュレーションに追加されます。

設定時の注意事項

Auto-QoS を設定する前に、次の点を理解する必要があります。

- このリリースでは、Cisco IP Phone の VoIP に対してのみ Auto-QoS がスイッチを設定します。
- Auto-QoS のデフォルト設定を使用する場合、Auto-QoS コマンドを入力する前にいかなる標準 QoS コマンドも設定しないでください。必要であれば、QoS 設定をきめ細かく調整できますが、Auto-QoS 設定が完了したあとに行うことを推奨します。
- スタティックアクセス、ダイナミックアクセス、音声 VLAN アクセス、およびトランク ポート上で Auto-QoS をイネーブルにできます。
- デフォルトでは、CDP はすべてのインターフェイス上でイネーブルになっています。Auto-QoS を適切に機能させるには、CDP をディセーブルにしないでください。
- レイヤ 3 インターフェイス上で auto qos voip trust をイネーブルにするには、ポートをレイヤ 3 に変更してから、Auto-QoS を適用し、DSCP を信頼するようにします。

VoIP 用の Auto-QoS のイネーブル化

VoIP 用の Auto-QoS を QoS ドメイン内でイネーブルにするには、次の作業を行います。

	コマンド	目的	
ステップ 1	Switch# debug auto qos	(任意)Auto-QoSのデバッグをイネーブルにします。デバッグがイネーブルに設定された場合、スイッチはAuto-QoSがイネーブルまたはディセーブルに設定されると自動的に生成および適用されるQoSコマンドを表示します。	
ステップ 2	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。	
ステップ 3	Switch(config)# interface interface-id	インターフェイス コンフィギュレーション モードを開始し、Cisco IP Phone に接続されているインターフェイス、またはネットワーク内部にある他のスイッチやルータに接続されているアップリンク インターフェイスを指定します。	
	Switch(config-if)# auto qos voip {cisco-phone trust}	Auto-QoS をイネーブルにします。 キーワードの意味は次のとおりです。 • cisco-phone インターフェイスが Cisco IP Phone に接続されている場合、着信パケットの CoS ラベルは電話機が検出された場合のみ信頼されます。 • trust アップリンク インターフェイスが信頼できるスイッチまたはルータに接続されていて、入力パケット内の VoIP トラフィック分類が信頼されます。	
ステップ 5	Switch(config)# end	特権 EXEC モードに戻ります。	
ステップ 6	Switch# show auto qos interface interface-id	入力を確認します。 このコマンドは、最初に適用された Auto-QoS 設定を表示するもので、ユーザにより有効になった変更は反映されません。	

インターフェイス上で Auto-QoS をディセーブルにするには、**no auto qos voip** インターフェイス コンフィギュレーション コマンドを使用します。このコマンドを入力すると、スイッチは Auto-QoS 設定を、そのインターフェイスの標準 QoS デフォルト設定に変更します。このコマンドは、Auto-QoS によって実行されるグローバル コンフィギュレーションを変更しません。グローバル コンフィギュレーションは、同じ状態のままです。

次に、インターフェイス FastEthernet 1/1 に接続されているデバイスが Cisco IP Phone として検出された場合に、Auto-QoS をイネーブルにして、着信パケット内の CoS ラベルを信頼する例を示します。

Switch(config)# interface fastethernet1/1
Switch(config-if)# auto qos voip cisco-phone

次に、インターフェイス GigabitEthernet 1/1 に接続されたスイッチまたはルータが信頼できるデバイスの場合に、Auto-QoS をイネーブルにして、着信パケット内の CoS/DSCP ラベルを信頼する例を示します。

Switch(config)# interface gigabitethernet1/1
Switch(config-if)# auto qos voip trust

次に、Auto-QoS がイネーブルにされた場合に、自動的に生成される QoS コマンドを表示する例を示します。

Switch# debug auto qos
AutoQoS debugging is on
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# auto qos voip cisco-phone

Auto-QoS 情報の表示

初期 Auto-QoS 設定を表示するには、show auto qos [interface [interface-id]] 特権 EXEC コマンドを使用します。ユーザが変更した設定を表示するには、show running-config 特権 EXEC コマンドを使用します。show auto qos コマンドと show running-config コマンド出力を比較することで、ユーザが定義した QoS 設定を識別できます。

Auto-QoS の影響を受ける QoS 設定に関する情報を表示するには、次のいずれかのコマンドを使用します。

- · show qos
- show qos map
- show qos interface [interface-id]

これらのコマンドの詳細については、このリリースに対応するコマンド リファレンスを参照してく ださい。

Auto-QoS 設定例

ここでは、ネットワーク内で Auto-QoS を実装する方法について説明します(図 34-5 を参照)。

図 34-5 Auto-QoS を設定したネットワークの例

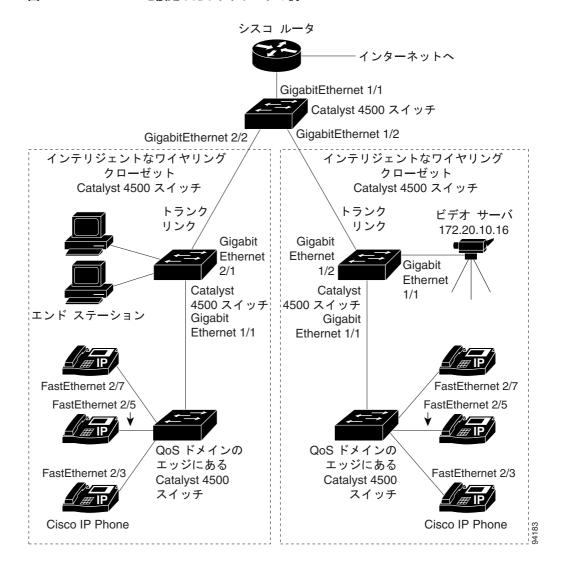


図 34-5 のインテリジェントなワイヤリング クローゼットは、Catalyst 4500 スイッチで構成されています。この例では、VoIP トラフィックを他のすべてのトラフィックよりも優先させることを目的としています。これを実行するには、ワイヤリング クローゼット内の QoS ドメインのエッジにあるスイッチ上で Auto-QoS をイネーブルにします。



Auto-QoS コマンドを入力する前にいかなる標準 QoS コマンドも設定しないでください。 QoS 設定をきめ細かく調整できますが、Auto-QoS 設定が完了したあとに行うことを推奨します。

VoIP トラフィックを他のすべてのトラフィックよりも優先させるために、QoS ドメインのエッジにあるスイッチを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# debug auto qos	Auto-QoS のデバッグをイネーブルにします。デバッグがイネーブルに設定されると、スイッチはAuto-QoS がイネーブルになる場合に自動的に生成される QoS 設定を表示します。
ステップ 2	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 3	Switch(config)# cdp enable	CDP をグローバルにイネーブルにします。デフォルトでは、CDP はイネーブルに設定されています。
ステップ 4	Switch(config)# interface fastethernet2/3	インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	Switch(config-if)# auto qos voip cisco-phone	インターフェイス上で Auto-QoS をイネーブルにし、 インターフェイスが Cisco IP Phone に接続されてい ることを指定します。
		着信パケット内の CoS ラベルは、IP Phone が検出された場合のみ信頼されます。
ステップ 6	Switch(config)# interface fastethernet2/5	インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	Switch(config)# auto qos voip cisco-phone	インターフェイス上で Auto-QoS をイネーブルにし、 インターフェイスが Cisco IP Phone に接続されてい ることを指定します。
ステップ 8	Switch(config)# interface fastethernet2/7	インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	Switch(config)# auto qos voip cisco-phone	インターフェイス上で Auto-QoS をイネーブルにし、 インターフェイスが Cisco IP Phone に接続されてい ることを指定します。
ステップ 10	Switch(config)# interface gigabit1/1	インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	Switch(config)# auto qos voip trust	インターフェイス上で Auto-QoS をイネーブルにし、 インターフェイスが信頼できるルータまたはスイッ チに接続されていることを指定します。
ステップ 12	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 13	Switch# show auto qos	入力を確認します。
		このコマンドは、最初に適用された Auto-QoS 設定を表示するもので、ユーザにより有効になった変更は反映されません。
		Auto-QoS の影響を受ける QoS 設定に関する情報については、「Auto-QoS 情報の表示」(p.34-22)を参照してください。
ステップ 14	Switch# show auto qos interface interface-id	入力を確認します。
		このコマンドは、最初に適用された Auto-QoS 設定を表示するもので、ユーザにより有効になった変更は反映されません。
ステップ 15	Switch# copy running-config startup-config	auto qos voip インターフェイス コンフィギュレーション コマンドと生成された Auto-QoS 設定をコンフィギュレーション ファイルに保存します。

Supervisor Engine II-Plus、II+10GE、VI、V、V-10GE、4924、4948、および 4948-10GE での QoS の設定

QoS を設定する前に、次の事項を完全に理解する必要があります。

- 使用するアプリケーションのタイプ、およびネットワーク上のトラフィック パターン
- トラフィックの特性およびネットワークの要件。バースト性のトラフィックかどうか。音声およびビデオストリーム用に帯域幅を予約する必要があるかどうか
- 帯域幅の要件およびネットワークの速度
- ネットワーク上の輻輳発生箇所

ここでは、Catalyst 4000 ファミリ スイッチ上で QoS を設定する手順について説明します。

- QoS のデフォルト設定 (p.34-26)
- 設定時の注意事項 (p.34-27)
- QoS のグローバルなイネーブル化 (p.34-27)
- 信頼境界の設定によるポート セキュリティの確保 (p.34-28)
- DBL のイネーブル化 (p.34-29)
- 名前付き集約ポリサーの作成 (p.34-33)
- QoS ポリシーの設定 (p.34-35)
- CoS 変換の設定 (p.34-44)
- UBRL の設定 (p.34-45)
- PVQoS のイネーブル化 (p.34-52)
- インターフェイス上での QoS のイネーブル化またはディセーブル化 (p.34-55)
- レイヤ 2 インターフェイス上での VLAN ベース QoS の設定 (p.34-55)
- インターフェイスの信頼状態の設定 (p.34-56)
- インターフェイスの CoS 値の設定 (p.34-57)
- インターフェイスの DSCP 値の設定 (p.34-58)
- 送信キューの設定 (p.34-59)
- DSCP マップの設定 (p.34-61)
- レイヤ 2 制御パケット QoS のイネーブル化 (p.34-64)

QoS のデフォルト設定

表 34-3 に、QoS のデフォルト設定を示します。

表 34-3 QoS のデフォルト設定

機能	デフォルト値	
QoS のグローバルな設定	ディセーブル	
インターフェイス QoS の設定(ポート単位)	QoS がグローバルにイネーブルの場合、イネーブル	
インターフェイス CoS 値	0	
インターフェイス DSCP 値	0	
CoS/DSCP マップ (CoS 値から設定された	CoS 0 = DSCP 0	
DSCP)	CoS 1 = DSCP 8	
	CoS 2 = DSCP 16	
	CoS 3 = DSCP 24	
	CoS 4 = DSCP 32	
	$\cos 5 = \text{DSCP } 40$	
	CoS 6 = DSCP 48	
	CoS 7 = DSCP 56	
DSCP/CoS マップ (DSCP 値から設定された	DSCP $0 \sim 7 = \cos 0$	
CoS)	DSCP $8 \sim 15 = \text{CoS } 1$	
	DSCP 16 $\sim 23 = \text{CoS } 2$	
	$DSCP 24 \sim 31 = CoS 3$	
	$DSCP 32 \sim 39 = CoS 4$	
	$DSCP 40 \sim 47 = CoS 5$	
	$DSCP 48 \sim 55 = CoS 6$	
	$DSCP 56 \sim 63 = CoS 7$	
DSCP からマークダウンされた DSCP への	マークダウンされた DSCP 値は元の DSCP 値(マークダウンなし)と等	
マッピング(ポリシング後の DSCP)	LIN	
ポリサー	<u>なし</u>	
ポリシー マップ	なし	
送信キューの共有	リンク帯域幅の 1/4	
送信キュー容量	ポートの送信キュー エントリの 1/4。ポートの送信キュー容量はポート のタイプによって異なり、送信キュー1 つ当たり 240 ~ 1920 パケット	
送信キューのシェーピング	なし	
DCSP/ 送信キュー マップ	DSCP 0 ~ 15 \(\dagger = 1 - 1	
	DSCP 16 ~ $31 \pm 2 - 2$	
	DSCP 32 $\sim 47 \pm 1 - 3$	
	DSCP 48 ~ 63 = 1 - 4	
ハイ プライオリティ送信キュー	ディセーブル	
QoS がディセーブルの場合		
インターフェイスの信頼状態	trust dscp	
QoS がイネーブルの場合	QoS がイネーブルに設定され、その他の QoS パラメータがすべてデフォ	
	ルト値である場合、送信されるすべてのトラフィックで IP DSCP が 0、	
	レイヤ 2 CoS が 0 に設定される	
インターフェイスの信頼状態	untrusted (信頼性がない)	

設定時の注意事項

QoS の設定を始める前に、次の点を理解する必要があります。

- スイッチ上に EtherChannel ポートを設定している場合、EtherChannel に QoS の分類およびポリシングを設定する必要があります。EtherChannel を形成する個々の物理ポートに、送信キューの設定が必要です。
- IP フラグメントが、QoS 用にトラフィックを分類するために使用される ACL で設定された送信元および宛先に一致するが、ACL のレイヤ 4 ポート番号には一致しない場合、ACL とは引き続き一致するとされ、優先されます。意図する動作が IP フラグメントにベスト エフォートのサービスを提供する場合、次の 2 つの ACE が、トラフィックの分類に使用される ACL に追加される必要があります。

```
access-list xxx deny udp any any fragments access-list xxx deny tcp any any fragments
```

- 設定されている IP 拡張 ACL と IP オプションのマッチングによって、QoS を強制することはできません。これらのパケットは CPU に送信され、ソフトウェアによって処理されます。IP オプションは、IP ヘッダー内のフィールドで示されます。
- スイッチが受信した制御トラフィック(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] ルーティング アップデート パケットなど)は、すべての入力 QoS 処理の対象になります。
- IP ルーティングがディセーブルの場合、set コマンドをポリシー マップで使用することはできません (デフォルトではイネーブル)。
- dot1q トンネル ポートでは、レイヤ 2 一致基準だけがタグ付きパケットに適用できます。ただし、タグなしパケットにはすべての一致基準を適用できます。
- トランク ポートでは、レイヤ 2 一致基準のみを複数の 802.1q タグを持つパケットに適用できます。



QoS は、ユニキャスト トラフィックとマルチキャスト トラフィックの両方を処理します。

QoS のグローバルなイネーブル化

QoS をグローバルにイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# conf terminal	コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# qos	スイッチ上で QoS をイネーブルにします。
		${ m QoS}$ をグローバルにディセーブルにするには、 ${ m no~qos}$ コマンドを使用します。
ステップ 3	Switch(config)# end	コンフィギュレーション モードを終了します。
ステップ 4	Switch# show qos	設定を確認します。

次に、QoS をグローバルにイネーブルにし、設定を確認する例を示します。

Switch# config terminal
Switch(config)# qos
Switch(config)# end
Switch#
Switch# show qos
 QoS is enabled globally

Switch#

信頼境界の設定によるポート セキュリティの確保

通常のネットワークでは、Cisco IP Phone をスイッチ ポートに接続します (第35章「音声インターフェイスの設定」を参照)。通常の場合、電話機からスイッチに送信されたトラフィックは、802.1Q ヘッダーを使用するタグによってマーク付けされます。このヘッダーには VLAN 情報、およびパケットのプライオリティを決定する CoS の 3 ビット フィールドが格納されます。ほとんどの Cisco IP Phone 設定では、電話機からスイッチに送信されたトラフィックは信頼され、音声トラフィックがネットワーク内の他のタイプのトラフィックよりも適切に優先されます。 qos trust cos インターフェイス コンフィギュレーション コマンドを使用することにより、ポートで受信されたすべてのトラフィックの CoS ラベルを信頼するように、電話機の接続先であるスイッチ ポートを設定できます。



(注)

Cisco IOS Release 12.2(31)SG 以降では、Supervisor Engine V-10GE を使用すれば、ポートの信頼状態 に関わらずパケットの IP DSCP 値に基づいてトラフィックを分類できます。このため、Cisco IP Phone が検出されない場合でも、データ トラフィックは IP DSCP 値に基づいて分類されます。これ により出力キュー選択が影響されることはありません。出力キュー選択はこれまでと同じく着信 ポート信頼設定に基づきます。送信キューの設定については、「送信キューの設定」(p.34-59)を参照してください。

場合により、IP Phone に PC またはワークステーションを接続することもできます。この場合は、switchport priority extend cos インターフェイス コンフィギュレーション コマンドを使用して、PC から受信したトラフィックよりも優先するように、スイッチ CLI (コマンドライン インターフェイス)を通して電話機を設定できます。このコマンドを使用すると、PC がハイプライオリティのデータ キューを利用しないように設定できます。

ただし、ユーザが電話機を省略して PC を直接スイッチに接続した場合、スイッチは PC によって 生成された CoS ラベルを信頼し(信頼された CoS 設定のため) ハイプライオリティ キューが誤っ て使用される可能性があります。信頼境界機能は、CDP を使用してスイッチ ポート上で Cisco IP Phone(Cisco IP Phone 7910、7935、7940、7960)の存在を検出することにより、この問題を解決します。



(注)

スイッチまたは該当するポートで CDP がグローバルに稼働していない場合、信頼境界は機能しません。

ポート上に信頼境界を設定する場合、信頼がディセーブルにされます。電話機が接続されて検出されると、信頼がイネーブルになります(電話機を検出するには数分かかります)。そして、電話機が取り外され(検出されなければ)、信頼境界機能はスイッチ ポートの trusted 設定をディセーブルにし、ハイ プライオリティのキューの誤使用を防ぎます。



(注)

指定ポートでは、Cisco IP Phone 検出情報がスタンバイ スーパーバイザ エンジンで更新されません。 スタンバイ エンジンがアクティブになると、CDP を通じて Cisco IP Phone を差異検出します。した がって、SSO スイッチオーバー後に短期間ポートが信頼状態になりません。

ポート上の信頼境界をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	Switch(config)# interface interface-id	インターフェイス コンフィギュレーション モード を開始し、IP Phone に接続されているインターフェ イスを指定します。
		有効なインターフェイスは物理インターフェイスな どです。
ステップ 3	Switch(config)# qos trust [cos dscp]	受信したトラフィックの CoS 値を信頼するように、 インターフェイスを設定します。デフォルトで、ポー トは trusted になっていません。
ステップ 4	Switch(config)# qos trust device cisco-phone	Cisco IP Phone が信頼できるデバイスであることを 指定します。
		信頼境界と Auto-QoS (auto qos voip インターフェイス コンフィギュレーション コマンド)は相互に排他的なので、同時にイネーブルにできません。
ステップ 5	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 6	Switch# show qos interface interface-id	入力を確認します。
ステップ 7	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を 保存します。

信頼境界機能をディセーブルにするには、no qos trust device cisco-phone インターフェイス コンフィギュレーション コマンドを使用します。

DBL のイネーブル化



Supervisor Engine 6-E は、この機能をサポートして*いません*。

DBL は、Catalyst 4500 プラットフォームでのアクティブ キュー管理を提供します (詳細については、「AQM」[p.34-15] を参照してください。

「選択的」DBL を介して、DBL アルゴリズムの対象となる (または対象とならない) フローを選択できます。特定の IP DSCP 値で、または特定の CoS 値で、DBL をグローバルにイネーブルにできます。

ここでは、次の作業について説明します。

- DBL のグローバルなイネーブル化 (p.34-30)
- DBL の選択的イネーブル化 (p.34-30)

DBL のグローバルなイネーブル化

DBL をグローバルにイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# qos dbl	スイッチ上で DBL をイネーブルにします。
		AQM をディセーブルにするには、 $oldsymbol{no}$ $oldsymbol{qos}$ $oldsymbol{dbl}$ コマンドを使用します。
ステップ 2	Switch(config)# end	コンフィギュレーション モードを終了します。
ステップ 3	Switch# show qos dbl	設定を確認します。

次に、DBLをグローバルにイネーブルにし、設定を確認する例を示します。

サービスポリシーを適用して、出力インターフェイス方向で DBL をイネーブルにできます。

```
Switch# conf terminal
Switch(config)# policy-map dbl
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# dbl
Switch(config-pmap-c)# end
Switch#
00:08:12: %SYS-5-CONFIG_I: Configured from console by console
Switch# conf terminal
Switch(config)# int gig 1/2
Switch(config-if)# service-policy output dbl
Switch# config-if)# end
Switch#
```

DBL の選択的イネーブル化

DSCP 値により、IP パケット(単一またはタグなし)に対してのみ選択的に DBL を適用できます(「特定 IP DSCP 値での DBL のイネーブル化」[p.34-31] を参照)。非 IP パケットまたは二重タグ付きパケット(Q-in-Q など)に DBL を選択的に適用するには、次に説明するように CoS 値を使用する必要があります(「特定 CoS 値での DBL のイネーブル化」[p.34-32] を参照)。

次の事項が可能です。

- 特定 IP DSCP 値での DBL のイネーブル化 (p.34-31)
- 特定 CoS 値での DBL のイネーブル化 (p.34-32)

特定 IP DSCP 値での DBL のイネーブル化

DBL アクションは、送信キュー(インターフェイスごとに 4 つ) で実行されます。キューを送信するために IP DSCP からのマッピングを操作するには、qos map dscp dscp-values to tx-queue queue-id コマンドを使用します (方法については、「送信キューの設定」[p.34-59] を参照)。

特定の IP DSCP 値で DBL をイネーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	Switch(config)# [no] qos dbl dscp-based <value, value_range=""></value,>	特定の IP DSCP 値で DBL をイネーブルにします。
ステップ 2	Switch(config)# end	コンフィギュレーション モードを終了します。
ステップ 3	Switch# show qos dbl	設定を確認します。

次に、DSCP値1~10でDBLを選択的にイネーブルにする例を示します。

次に、DSCP値1~10でDBLを選択的にディセーブルにし、設定を確認する例を示します。

DSCP 以外のクラス属性に基づいて DBL を適用しても、引き続きポリシーマップを出力インターフェイスに付加する必要があります (「ポリシーマップ クラス アクションの設定」[p.34-39])。

ネットワーク ポリシーに従って値が設定されている場合、DBL が抑圧するアグレッシブ フローの 出力インターフェイスで「Trust DSCP」を設定する必要があります。

```
Interface <ingress>
  qos trust dscp
```

特定 CoS 値での DBL のイネーブル化

非 IP パケットまたは二重タグ付きパケット (たとえば、Q-in-Q)を使用するつもりであれば、CoS値を使用して、選択的に DBL を適用する必要があります。

一重タグ付き IP パケットの場合は、次のアプローチを使用します。「特定 IP DSCP 値での DBL のイネーブル化」(p.34-31)に示すように、グローバル qos dbl dscp-based コマンドを指定します。

Interface <ingress>
 switchport mode trunk
 qos trust cos

非 IP パケットまたは二重タグ付きパケットの場合、次の方法を使用します。

	コマンド	目的
ステップ 1	Switch(config)# qos dbl	DBL をグローバルにイネーブルにします。
ステップ 2	Switch(config)# end	コンフィギュレーション モードを終了します。
ステップ 3	Switch(config)# class-map cos	トラフィック クラスを定義します。
ステップ 4	Switch(config-cmap)# match cos x y	一致基準として使用する CoS 値を指定します。
ステップ 5	Switch(config-cmap)# exit	グローバル コンフィギュレーション モードに戻 ります。
ステップ 6	Switch(config)# policy-map cos	ユーザが指定する名前でポリシー マップを作成します。
ステップ 7	Switch(config-pmap)# class cos	ポリシー マップが使用するクラス マップを指定 します。
ステップ 8	Switch(config-pmap-c)# dbl	ポリシー上で DBL をイネーブルにします。
ステップ 9	Switch(config-pmap-c)# end	EXEC モードに戻ります。
ステップ 10	Switch# show policy-map cos	設定を確認します。
ステップ 11	Switch# configure terminal	グローバル コンフィギュレーション モードを開 始します。
ステップ 12	Switch(config)# interface gigabitEthernet 1/20	設定をインターフェイスに適用します。
ステップ 13	Switch(config-if)# service-policy output cos	ポリシー マップをインターフェイスに付加しま す。
ステップ 14	Switch# show policy-map interface	設定を確認します。



CoS 変換の使用の詳細については、「CoS 変換の設定」(p.34-44)を参照してください。

CoS値2および3でDBLを選択的にイネーブルにするには、次の手順を実行します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config) # qos dbl
Switch(config) # end
Switch# configure terminal
Switch(config)# class-map cos
Switch(config-cmap) # match cos 2 3
Switch(config-cmap)# exit
Switch(config) # policy-map cos
Switch(config-pmap) # class cos
Switch(config-pmap-c)# dbl
Switch(config-pmap-c)# end
Switch# show policy-map cos
    Policy Map cos
     Class cos
        db1
Switch# configure terminal
Switch(config) # interface gigabitEthernet 1/20
Switch(config-if)# service-policy output cos
Switch# show policy-map interface
GigabitEthernet1/20
  Service-policy output: cos
    Class-map: cos (match-all)
      0 packets
      Match: cos 2 3
      db1
    Class-map: class-default (match-any)
      0 packets
      Match: any
       0 packets
```

名前付き集約ポリサーの作成

名前付き集約ポリサーを作成するには、次の作業を行います。

コマンド	目的
<pre>Switch(config)# qos aggregate-policer policer_name rate burst [[conform-action {transmit drop}] [exceed-action {transmit drop policed-dscp-transmit}]]</pre>	名前付き集約ポリサーを作成します。

集約ポリサーは、1 つまたは複数のインターフェイスに適用できます。ただし、あるインターフェイスの入力方向と、別のインターフェイスの出力方向に同じポリサーを適用すると、スイッチングエンジン上で 2 つの異なる同等の集約ポリサーを作成したことになります。各ポリサーは同じポリシングパラメータを使用し、1 つのポリサーは 1 つのインターフェイスの入力トラフィックのポリシング、もう 1 つのポリサーは別のインターフェイスの出力トラフィックのポリシングを行います。集約ポリサーを複数のインターフェイスに同じ方向で適用した場合、スイッチングエンジン上に作成されるそのポリサーのインスタンスは 1 つだけです。

同様に、集約ポリサーをポートまたは VLAN に適用できます。同じ集約ポリサーをポートおよび VLAN に適用した場合、スイッチング エンジン上で 2 つの異なる同等の集約ポリサーを作成したことになります。各ポリサーは同じポリシング パラメータを使用し、1 つのポリサーは設定されたポート上のトラフィックのポリシング、もう 1 つのポリサーは設定された VLAN 上のトラフィックのポリシングを行います。集約ポリサーを複数のポートのみ、または複数の VLAN のみに適用した場合、スイッチング エンジン上に作成されるそのポリサーのインスタンスは 1 つだけです。

1 つの集約ポリサーを複数のポートおよび VLAN に異なる方向で適用した場合、実質的には、同等の 4 つの集約ポリサー(入力方向でポリサーを共有するすべてのポート用、出力方向でポリサーを共有するすべての VLAN 用、および出力方向でポリサーを共有するすべての VLAN 用の集約ポリサー)を作成したことになります。

名前付き集約ポリサーを作成する場合、次の点に注意してください。

- rate パラメータ値の有効範囲は、次のとおりです。
 - 最小 32 Kbps (キロビット/秒)
 - 最大 32 Gbps (ギガビット/秒)

「設定時の注意事項」(p.34-27)を参照してください。

- 速度(rate)はビット/秒で入力できますが、次の簡略表記を使用することもできます。
 - kは、1,000 bps を表します。
 - m は、1,000,000 bps を表します。
 - gは、1,000,000,000 bps を表します。



(注) 小数点を使用することもできます。たとえば、1,100,000 bps という速度は、1.1m と入力できます。

- *burst* パラメータ値の有効範囲は、次のとおりです。
 - 最小 1 KB
 - 最大 512 MB
- バースト サイズ(burst)はバイトで入力できますが、次の簡略表記を使用することもできます。
 - kは、1,000 バイトを表します。
 - m は、1,000,000 バイトを表します。
 - gは、1,000,000,000 バイトを表します。



- (注) 小数点を使用することもできます。たとえば、1,100,000 バイトのバーストは、1.1m と 入力できます。
- 一致するイン プロファイルトラフィックに対する conform アクションを、任意で次のように指定できます。
 - デフォルトの conform アクションは、transmit です。
 - 一致するトラフィックをすべてドロップするには、drop キーワードを入力します。



(注) drop を conform アクションとして設定すると、QoS は **drop** を exceed アクションとして 設定します。

- Committed Information Rate (CIR; 認定情報レート)を超過するトラフィックについて、exceed アクションを任意で次のように指定できます。
 - デフォルトの exceed アクションは、drop です。
 - 一致するアウト オブ プロファイルトラフィックを、マークダウン マップの指定に従って マークダウンするには、policed-dscp-transmit キーワードを入力します。
 - ポリシングをまったく行わないようにするには、transmit キーワードを入力して、一致したアウト オブ プロファイルトラフィックをすべて送信します。

• 名前付き集約ポリサーを削除するには、**no qos aggregate-policer** *policer_name* コマンドを使用します。

次に、10 Mbps のレート制限および 1 MB のバースト サイズを指定し、適合するトラフィックを送信して、不適合トラフィックをマークダウンする、名前付き集約ポリサーの作成例を示します。

Switch# config terminal

Switch(config)# qos aggregate-policer aggr-1 10000000 1000000 conform-action transmit exceed-action policed-dscp-transmit

Switch(config)# end
Switch#

次に、設定を確認する例を示します。

Switch# show qos aggregate-policer aggr-1

Policer aggr-1

Rate(bps):10000000 Normal-Burst(bytes):1000000 conform-action:transmit exceed-action:policed-dscp-transmit Policymaps using this policer:

Strite oh#

QoS ポリシーの設定

ここでは、QoS ポリシーの設定について説明します。

- QoS ポリシー設定の概要 (p.34-35)
- クラスマップの設定(任意)(p.34-36)
- ポリシーマップの設定 (p.34-38)
- インターフェイスへのポリシー マップの付加 (p.34-43)



(注)

QoS ポリシーは、ユニキャスト トラフィックおよびマルチキャスト トラフィックの両方を処理します。

QoS ポリシー設定の概要

QoS ポリシーを設定するには、トラフィック クラスを設定して、それらのトラフィック クラスに 適用するポリシーを設定し、さらに、次のコマンドを使用してポリシーをインターフェイスに付加 する必要があります。

- access-list (IP トラフィックに対して任意 class-map コマンドを使用して IP トラフィックをフィルタリングできます。)
 - QoS では、次のアクセス リスト タイプがサポートされています。

	番号付きアクセス リスト のサポート	拡張アクセス リストの サポート	名前付きアクセス リスト のサポート
IP	あり:	あり:	含まれる
	1 ~ 99	100 ~ 199	
	1300 ~ 1999	2000 ~ 2699	

- Catalyst 4500 シリーズ スイッチ上の ACL については、第 42 章「ACL によるネットワーク セキュリティの設定」を参照してください。
- class-map(任意) class-map コマンドを使用してトラフィックの分類基準を指定し、1 つまた は複数のトラフィック クラスを定義します(「クラス マップの設定(任意)」[p.34-36] を参照)。

- policy-map 各トラフィック クラスに以下を定義するには、policy-map コマンドを使用します。
 - 内部 DSCP の作成元
 - 集約または個別のポリシングおよびマーキング
- service-policy service-policy コマンドを使用して、ポリシー マップをインターフェイスに付加します。

クラス マップの設定(任意)

ここでは、クラス マップの設定手順について説明します。

- クラスマップの作成(p.34-36)
- クラス マップでのフィルタリングの設定 (p.34-36)
- クラスマップの設定の確認 (p.34-37)

トラフィック クラスを定義し、そのクラスに属するトラフィックを識別するための一致基準を指定するには、class-map コンフィギュレーション コマンドを使用します。一致文には、ACL、IP precedence 値、DSCP 値などの基準を指定できます。一致基準は、クラス マップ コンフィギュレーション モードで 1 つの一致文を入力して定義します。

クラス マップの作成

クラスマップを作成するには、次の作業を行います。

コマンド	目的
Switch(config)# [no] class-map [match-all match-any] class name	名前付きクラス マップを作成します。
,	クラス マップを削除するには、no キーワードを使用します。

クラス マップでのフィルタリングの設定

クラス マップにフィルタリングを設定するには、次のいずれかの作業を行います。

コマンド	目的		
<pre>Switch(config-cmap)# [no] match access-group {acl_index name acl_name}</pre>	(任意)トラフィックのフィルタリングに使用する ACL の名前を指定します。		
	クラス マップから文を削除するには、no キーワードを使用 します。		
	(注) アクセス リストについては、このマニュアルでは 説明しません。「QoS ポリシーの設定」(p.34-35)に 記載されている access-list の説明を参照してくださ い。		
Switch (config-cmap)# [no] match ip precedence ipp_value1 [ipp_value2 [ipp_valueN]]	(任意 IPトラフィックのみ)一致基準として使用する IP precedence 値(最大8つ)を指定します。クラス マップから文を削除するには、noキーワードを使用します。		
Switch (config-cmap)# [no] match ip dscp dscp_value1 [dscp_value2 [dscp_valueN]]	(任意 IP トラフィックのみ) 一致基準として使用する DSCP 値(最大 8 つ)を指定します。クラス マップから文 を削除するには、no キーワードを使用します。		

コマンド	目的	
Switch (config-cmap)# [no] match cos value1 [value2] [value3} [value4}	+(任意 非 IPv4 トラフィックのみ) 一致基準として使用する CoS 値(最大 8 つ)を指定します。クラス マップから文を削除するには、no キーワードを使用します。	
	非 IPv4 トラフィックについては、「設定時の注意事項」 (p.34-21)を参照してください。	
Switch (config-cmap)# [no] match any	(任意) すべての IP トラフィックまたは IP 以外のトラフィックを一致させます。	
Switch (config-cmap)# match flow ip {source-address destination-address	(任意) IP 送信元アドレスまたは宛先アドレスが一意であるそれぞれのフローを新しいフローとして扱います。	



match ip precedence または match ip dscp クラス マップ コマンドを指定したクラス マップを使用す る入力ポリシーまたは出力ポリシーでは、パケットを受信するポートが trust dscp に設定されてい る必要があります。設定されていない場合、IP パケット DSCP/IP precedence はトラフィックのマッ チングには使用されず、受信ポートのデフォルト DSCP が使用されます。Cisco IOS Release 12.2(31)SG 以降では、Supervisor Engine V-10GE を使用すれば、ポートの信頼状態に関わらずパケッ トの IP DSCP 値に基づいてトラフィックを分類できます。



Cisco IOS Release 12.2(31) では、Catalyst 4500 シリーズ スイッチは match cos をサポートします。



Catalyst 4000 ファミリ スイッチ上のインターフェイスは、match classmap、match destinationaddress、match input-interface、match mpls、match not、match protocol、match qos-group、およ び match source-address キーワードをサポートしていません。

クラス マップの設定の確認

クラス マップの設定を確認するには、次の作業を行います。

コマンド ステップ 1 Switch (config-cmap) # end コンフィギュレーション モードを終了します。 ステップ 2 Switch# show class-map class_name 設定を確認します。

> 次に、ipp5 という名前のクラス マップを作成し、IP precedence 5 のトラフィックと一致するように フィルタリングを設定する例を示します。

Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z. Switch(config) # class-map ipp5 Switch(config-cmap) # match ip precedence 5 Switch(config-cmap)# end Switch#

次に、設定を確認する例を示します。

```
Switch# show class-map ipp5
Class Map match-all ipp5 (id 1)
Match ip precedence 5
Switch#
```

次に、非 IPv4 トラフィックの CoS マッチングを設定する例を示します。ここでは、CoS 値が 5 のトラフィックをフィルタリングします。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# class-map maptwo
Switch(config-cmap)# match cos 5
Switch(config-cmap)# end
Switch#
```

次に、設定を確認する例を示します。

```
Switch# show class-map maptwo
Class Map match-all maptwo (id 1)
Match cos 5
Switch#
```

ポリシー マップの設定

1 つのインターフェイスに付加できるポリシー マップは、1 つに限られます。 ポリシー マップには、一致基準およびポリサーがそれぞれ異なる 1 つまたは複数のポリシー マップ クラスを含めることができます。

インターフェイスで受信するトラフィック タイプごとに、個別のポリシー マップ クラスをポリシー マップ内に設定します。各トラフィック タイプ用のすべてのコマンドを、同一のポリシー マップ クラスに入れます。 QoS が、一致したトラフィックに複数のポリシー マップ クラスのコマンドを適用することはありません。

ここでは、ポリシー マップの設定手順について説明します。

- ポリシーマップの作成(p.34-38)
- ポリシー マップ クラス アクションの設定 (p.34-39)

ポリシー マップの作成

ポリシーマップを作成するには、次の作業を行います。

コマンド	目的	
Switch(config)# [no] policy-map policy_name	ユーザが指定する名前でポリシー マップを 作成します。	
	ポリシー マップを削除するには、no キーワー ドを使用します。	

ポリシー マップ クラス アクションの設定

ここでは、ポリシー マップ クラスのアクションを設定する手順について説明します。

- ポリシー マップ マーキング状態の設定 (p.34-39)
- ポリシー マップ クラスの信頼状態の設定 (p.34-39)
- ポリシー マップ クラスの DBL 状態の設定 (p.34-40)
- ポリシーマップクラスのポリシングの設定(p.34-40)
- 名前付き集約ポリサーの使用 (p.34-40)
- インターフェイス別ポリサーの設定 (p.34-40)

ポリシー マップ マーキング状態の設定

ポリシー マップを設定してパケットに IP precedence または DSCP をマーク付けするには、次の作業を実行します。

コマンド	目的	
Switch(config-pmap-c)# [no] set ip [precedence prec_value dscp_dscp_value]	ポリシー マップ マーキング状態を設定します。この設定によって、後続処理のためにパケットの内部 DSCP が決定します。	
	設定した値をクリアし、デフォルトに戻すに は、no キーワードを使用します。	

ポリシー マップ クラスの信頼状態の設定

ポリシー マップ クラスの信頼状態を設定するには、次の作業を行います。

コマンド	目的	
<pre>Switch(config-pmap-c)# [no] trust {cos dscp]</pre>	ポリシー マップ クラスの信頼状態を設定します。この設定によって、QoS が内部 DSCP 値の作成元として使用する値が選択されます (「内部 DSCP 値」[p.34-14] を参照)。	
	設定した値をクリアし、デフォルトに戻すに は、no キーワードを使用します。	

ポリシー マップ クラスの信頼状態を設定する際、次の点に注意してください。

- **no trust** コマンドを入力すると、入力インターフェイス上に設定されている信頼状態を使用できます(これがデフォルトです)。
- cos キーワードを使用すると、QoS は受信した CoS またはインターフェイス CoS に基づいて、 内部 DSCP 値を設定します。
- dscp キーワードを使用すると、QoS は受信した DSCP を使用します。

ポリシー マップ クラスの DBL 状態の設定

ポリシー マップ クラスの DBL 状態を設定するには、次の作業を行います。

コマンド	目的
Switch(config-pmap-c)# [no] db1	ポリシー マップ クラスの DBL 状態を設定します。この設定によって、トラフィック フローのキュー長を追跡します (「AQM」[$p.34-15$] を参照)。
	DBL 値をクリアし、デフォルトに戻すには、 no キーワードを使用します。

ポリシー マップ クラスの DBL 状態を設定する場合、次の点に注意してください。

• 名前付き集約ポリサーを使用しているクラスは、機能するために同じ DBL 設定でなければなりません。

ポリシー マップ クラスのポリシングの設定

ここでは、ポリシー マップ クラスによるポリシングを設定する手順について説明します。

- 名前付き集約ポリサーの使用 (p.34-40)
- インターフェイス別ポリサーの設定(p.34-40)

名前付き集約ポリサーの使用

名前付き集約ポリサーを使用するには(「名前付き集約ポリサーの作成」[p.34-33] を参照) 次の作業を行います。

コマンド	目的	
aggregate name	あらかじめ定義されている集約ポリサーを使 用します。	
	ポリシー マップ クラスからポリサーを削除 するには、no キーワードを使用します。	

インターフェイス別ポリサーの設定

インターフェイスにインターフェイス単位のポリサーを設定するには (「ポリシングおよびマーキング」[p.34-10] を参照) 次の作業を行います。

コマンド	目的
Switch(config-pmap-c)# [no] police rate burst [[conform-action {transmit drop}]]	インターフェイス別のポリサーを設定します。
<pre>[exceed-action {transmit drop policed-dscp-transmit}]]</pre>	ポリシー マップ クラスからポリサーを削除するには、no キーワードを使用します。

インターフェイス別ポリサーを設定する際、次の点に注意してください。

- rate パラメータ値の有効範囲は、次のとおりです。
 - 最小 32 Kbps (32000 と入力)
 - 最大 32 Gbps (320000000000 と入力)



(注)

「設定時の注意事項」(p.34-27)を参照してください。

- 速度 (rate) はビット / 秒で入力できますが、次の簡略表記を使用することもできます。
 - kは、1,000 bps を表します。
 - m は、1,000,000 bps を表します。
 - gは、1,000,000,000 bps を表します。



(注)

小数点を使用することもできます。たとえば、1,100,000 bps という速度は、1.1m と入力できます。

- *burst* パラメータ値の有効範囲は、次のとおりです。
 - 最小 1 KB
 - 最大 512 MB
- バースト サイズ(burst)はバイトで入力できますが、次の簡略表記を使用することもできます。
 - k は、1,000 バイトを表します。
 - m は、1,000,000 バイトを表します。
 - gは、1,000,000,000 バイトを表します。



(注)

小数点を使用することもできます。たとえば、1,100,000 バイトのバーストは、 $1.1 \mathrm{m}$ と入力できます。

- 一致するイン プロファイルトラフィックに対する conform アクションを、任意で次のように指定できます。
 - デフォルトの conform アクションは、transmit です。
 - 一致するトラフィックをすべてドロップするには、drop キーワードを入力します。
- 任意で、CIR を超過するトラフィックについて、一致するアウト オブ プロファイルトラフィックをすべてマークダウン マップの指定に従ってマークダウンするには、policed-dscp-transmit キーワードを入力します。「ポリシング済み DSCP マップの設定 (p.34-62)を参照してください。
 - ポリシングをまったく行わないようにするには、transmit キーワードを入力して、一致するアウト オブ プロファイルトラフィックをすべて送信します。

次の例は、ipp5 という名前のクラス マップを使用する、ipp5-policy という名前のポリシー マップを作成する方法を示しています。クラス マップ ipp5 は、パケット優先順位を 6 に書き換えて、IP precedence 値の 5 と一致するトラフィックを集約ポリシングするように設定されています。

```
Switch# configure terminal
```

```
Enter configuration commands, one per line. End with {\tt CNTL/Z.}
```

Switch(config)# policy-map ipp5-policy

Switch(config-pmap) # class ipp5

Switch(config-pmap-c)# set ip precedence 6

Switch(config-pmap-c)# dbl

 ${\tt Switch (config-pmap-c) \# \ police \ 20000000000 \ 2000000 \ conform-action \ transmit \ exceed-action}$

policed-dscp-transmit

Switch(config-pmap-c)# end

次の例は、cs2 という名前のクラス マップを使用する、cs2-policy という名前のポリシー マップを 作成する方法を示しています。クラス マップ cos5 は CoS 5 で一致するように設定されており、ト ラフィックを集約ポリシングするように設定されています。

```
Switch(config) # class-map cs2
Switch(config-cmap) # match cos 5
Switch(config-cmap) # exit
Switch(config) # policy-map cs2-policy
Switch(config-pmap) # class cs2
\verb"police 2000000000 2000000 conform-action transmit exceed-action policed-dscp-transmit \\
Switch(config) # int g5/1
Switch(config-if) # service-policy input cs2-policy
Switch(config-if)# end
Switch# sh class-map cs2
Class Map match-all cs2 (id 2)
  Match cos 5
Switch# sh policy-map cs2-policy
  Policy Map cs2-policy
    Class cs2
      police 2000000000 bps 2000000 byte conform-action transmit exceed-action
policed-dscp-transmit Switch#
```

ポリシー マップの設定の確認

ポリシーマップの設定を確認するには、次の作業を行います。

	コマンド	目的 ポリシー マップ クラス コンフィギュレーション モードを終了します。		
ステップ 1	Switch(config-pmap-c)# end			
		▲ (注) ポリシー マップに別のクラスを作成するには class コマンドを入力します。		
ステップ 2	Switch# show policy-map policy_name	設定を確認します。		

次に、設定を確認する例を示します。

```
Switch# show policy-map ipp5-policy
show policy ipp5-policy
Policy Map ipp5-policy
class ipp5
set ip precedence 6
dbl
police 2000000000 2000000 conform-action transmit exceed-action
policed-dscp-transmit
Switch#
```

インターフェイスへのポリシー マップの付加

ポリシー マップをインターフェイスに付加するには、次の作業を行います。

	コマンド	設定するインターフェイスを選択します。	
ステップ 1	Switch(config) # interface {vlan vlan_ID {fastethernet gigabitethernet} slot/interface Port-channel number}		
ステップ 2	Switch(config-if)# [no] service-policy input policy_map_name	ポリシー マップをインターフェイスの入力方向に付加します。インターフェイスからポリシー マップの付加を解除するには、no キーワードを使用します。	
ステップ 3	Switch(config-if)# end	コンフィギュレーション モードを終了します。	
ステップ 4	Switch# show policy-map interface {vlan vlan_ID {fastethernet gigabitethernet} slot/interface}	設定を確認します。	



IP ルーティングをグローバルにイネーブルにするまでは、インターフェイスのマーキング コマンドをイネーブルにできません。IP ルーティングがグローバルにディセーブルのときインターフェイスにサービス ポリシーを設定すると、設定は受け付けられても有効にはなりません。このような場合には、[Set command will not take effect since CEF is disabled. Please enable IP routing and CEF globally. "(CEF がディセーブルなので設定されたコマンドは有効になりません。IP ルーティングおよび CEF をグローバルにイネーブルにしてください。)] というエラー メッセージが表示されます。IP ルーティングをグローバルにイネーブルにするには、ip routing および ip cef global コンフィギュレーション コマンドを実行します。その後、マーキング コマンドが有効になります。

次に、ポリシー マップ pmap1 をインターフェイス FastEthernet 5/36 に付加し、設定を確認する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 5/36
Switch(config-if)# service-policy input pmap1
Switch(config-if)# end
Switch# show policy-map interface fastethernet 5/36
FastEthernet6/1
  service-policy input:p1
     class-map:c1 (match-any)
      238474 packets
      match:access-group 100
       38437 packets
       police:aggr-1
        Conform:383934 bytes Exceed:949888 bytes
    class-map:class-default (match-any)
      0 packets
      match:any
        0 packets
Switch#
```

CoS 変換の設定



Supervisor Engine 6-E は、この機能をサポートして*いません*。

レイヤ 2 VPN を提供するサービス プロバイダーは、サービス プロバイダーの VLAN を示す外部タグと顧客の VLAN を示す内部タグを持つ二重タグ トラフィックまたは Q-in-Q トラフィックを伝送します。外部タグの CoS に基づいて、SP ネットワーク内に Differentiated Service (diffserv; ディファレンシエーテッド サービス)を提供できます。

dot1q トンネル ポートで CoS 変換を使用すると、プロバイダーのコア ネットワークに入る dot1q トンネル パケットの外部タグの CoS 値を顧客の VLAN タグの CoS から導き出すことができます。その結果、プロバイダーは顧客の QoS セマンティックスをネットワーク内で保つことができます。

CoS 変換は、特定の着信 CoS 値に一致させ、一致したパケットに関連付けられている内部 DSCP を 指定するようにユーザーが明示的に設定することによって実現されます。この内部 DSCP は、ス イッチからの送信時に DSCP/CoS マッピングを通じて CoS に変換されます。外部 VLAN タグには この CoS 値がマーク付けされます。

このプロセス中に内部タグの CoS が保存され、サービス プロバイダーのネットワーク内で伝送されます。

次に、ポリシー マップが顧客の VLAN ID と CoS 値をネットワーク内で保つ例を示します。

```
Class Map match-any c0
  Match cos 0
Class Map match-anv c1
  Match cos 1
Class Map match-any c2
  Match cos 2
Class Map match-any c3
  Match cos 3
Class Map match-anv c4
  Match cos 4
Class Map match-any c5
  Match cos 5
Class Map match-any c6
  Match cos 6
Class Map match-anv c7
  Match cos
Policy Map cos_mutation
   Class c0
     set dscp default
   Class c1
     set dscp cs1
    Class c2
     set dscp cs2
    Class c3
     set dscp cs3
    Class c4
     set dscp cs4
```

```
Class c5
set dscp cs5

Class c6
set dscp cs6

Class c7
set dscp cs7

interface GigabitEthernet5/1
switchport access vlan 100

switchport mode dot1q-tunnel
service-policy input cos_mutation
```

UBRL の設定

User Based Rate Limiting (UBRL) ではマイクロフロー ポリシング機能が採用され、トラフィックフローがダイナミックに学習されて、それぞれの一意のフローが個別レートにレート制限されます。UBRL は、内蔵 NetFlow がサポートされている Supervisor Engine V-10GE で使用できます。UBRL は、送信元または宛先フローマスクを持つルーテッド インターフェイス上の入力トラフィックに適用できます。最大 85,000 の個別フローおよび 511 の異なるレートをサポートできます。UBRL は、通常ユーザ単位のきめ細かいレート制限メカニズムが必要な環境(ユーザ単位の発信トラフィックレートがユーザ単位の着信トラフィックレートと異なる場合など)で使用されます。



(注)

デフォルトでは、UBRL はルーティングされた IP トラフィックのみをポリシングします。スイッチングされる IP トラフィックをポリシングするには、ip flow ingress layer2-switched グローバル コマンドを使用します。ただし、レイヤ 3 インターフェイス上に UBRL 設定を残す必要があります。 UBRL 設定と ip flow ingress layer2-switched グローバル コマンドを使用すれば、VLAN 間フローをポリシングできます(「スイッチド / ブリッジド IP フローの設定」 [p.48-8] を参照)。ip flow ingress コマンドを入力する必要はありません。

フローは 5 タプルとして定義されます (IP 送信元アドレス、IP 宛先アドレス、IP ヘッド プロトコル フィールド、レイヤ 4 送信元ポート、宛先ポート 。 フローベース ポリサーでは、フローごとにトラフィックをポリシングできます。フローはダイナミックなので、クラス マップで識別値が必要です。

source-address キーワードを使用して match flow コマンドを指定すると、送信元アドレスが一意であるそれぞれのフローは、新しいフローとして扱われます。 destination-address キーワードを使用して match flow コマンドを指定すると、宛先アドレスが一意であるそれぞれのフローは、新しいフローとして扱われます。ポリシー マップによって使用されるクラス マップは、フロー オプションが設定されている場合、フローベース ポリシー マップとして扱われます。ip destination-address ip protocol L4 source-address L4 destination-address キーワードを使用して match flow コマンドを指定すると、一意の IP 送信元、IP 宛先、IP プロトコル、およびレイヤ 4 送信元、宛先アドレスを含む各フローは、新しいフローとして扱われます。



マイクロフローは、Supervisor Engine V-10GE でのみサポートされます。

フローベース クラス マップとポリシー マップを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# class-map match-all class_name	名前付きクラス マップを作成します。
ステップ 2	Switch(config-cmap)# match flow ip {source-address ip destination-address ip protocol L4 source-address L4 destination-address destination-address}	フローのキーフィールドを指定します。
ステップ 3	Switch(config-cmap)# end	クラスマップ コンフィギュレーション モードを終了し ます。
ステップ 4	Switch# show class-map class-name	設定を確認します。

例

例 1

次の例では、送信元アドレスに関連付けられたフローベース クラス マップを生成する方法を示します。

```
Switch(config) # class-map match-all c1
Switch(config-cmap) # match flow ip {source-address [ip destination_address ip protocol
L4 source-address L4 destination address]}
Switch(config-cmap) # end
Switch#
Switch# show class-map c1
Class Map match-all c1 (id 2)
    Match flow ip source-address
```

例 2

次の例では、宛先アドレスに関連付けられたフローベース クラス マップを生成する方法を示します。

```
Switch(config)# class-map match-all c1
Switch(config-cmap)# match flow ip destination-address
Switch(config-cmap)# end
Switch#
Switch# show class-map c1
Class Map match-all c1 (id 2)
    Match flow ip destination-address
```

例3

インターフェイス FastEthernet 6/1 に 2 つのアクティブなフローがあり、送信元アドレスが 192.168.10.20 と 192.168.10.21 であるとします。次の例は、許可されるバースト値を 9000 バイトにして 1 Mbps でそれぞれのフローを維持する方法を示しています。

```
Switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# class-map c1
Switch(config-cmap) # match flow ip source-address
Switch(config-cmap)# exit
Switch(config)# policy-map p1
Switch(config-pmap) # class c1
Switch(config-pmap-c)# police 1000000 9000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config) # interface fa6/1
Switch(config-if)# service-policy input p1
Switch(config-if)# end
Switch# write memory
Switch# show policy-map interface
FastEthernet6/1
 Service-policy input: p1
   Class-map: c1 (match-all)
    15432182 packets
     Match: flow ip source-address
    police: Per-interface
      Conform: 64995654 bytes Exceed: 2376965424 bytes
   Class-map: class-default (match-any)
     0 packets
     Match: any
      0 packets
```

例 4

インターフェイス FastEthernet 6/1 に 2 つのアクティブなフローがあり、宛先アドレスが 192.168.20.20 と 192.168.20.21 であるとします。次の例は、許可されるバースト値を 9000 バイトにして 1 Mbps でそれぞれのフローを維持する方法を示しています。

```
Switch# conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# class-map c1
Switch(config-cmap) # match flow ip destination-address
Switch(config-cmap) # exit
Switch(config)# policy-map p1
Switch(config-pmap) # class c1
Switch(config-pmap-c)# police 1000000 9000
Switch(config-pmap-c)# exit
Switch(config-pmap) # exit
Switch(config) # interface fa6/1
Switch(config-if) # service-policy input p1
Switch(config-if)# end
Switch# write memory
Switch# show policy-map interface
FastEthernet6/1
  Service-policy input: p1
    Class-map: c1 (match-all)
      2965072 packets
     Match: flow ip destination-address
     police: Per-interface
        Conform: 6105636 bytes Exceed: 476652528 bytes
   Class-map: class-default (match-any)
      0 packets
     Match: any
        0 packets
```

例 5

インターフェイス FastEthernet 6/1 上に 2 つのアクティブ フローが存在すると想定します。

SrcIp	DstIp	IpProt	SrcL4Port	DstL4Port
192.168.10.10	192.168.20.20	20	6789	81
192.168.10.10	192.168.20.20	20	6789	21

次の設定の場合、各フローは許可されるバースト値を 9000 にして 1000000 bps にポリシングされます。



match flow ip source-address|destination-address コマンドを使用する場合、これら 2 つのフローは同じ送信元および宛先アドレスを持つため、1 つのフローに統合されます。

```
Switch# conf terminal
Enter configuration commands, one per line. End with {\tt CNTL/Z.}
Switch(config) # class-map c1
Switch(config-cmap)# match flow ip source-address ip destination-address ip protocol
14 source-port 14 destination-port
Switch(config-cmap)# exit
Switch(config) # policy-map p1
Switch(config-pmap) # class c1
Switch(config-pmap-c)# police 1000000 9000
Switch(config-pmap-c)# exit
Switch(config-pmap) # exit
Switch(config)# interface fastEthernet 6/1
Switch(config-if)# service-policy input p1
Switch(config-if)# end
Switch# write memory
Switch# show policy-map interface
FastEthernet6/1
class-map c1
  match flow ip source-address ip destination-address ip protocol 14 source-port 14
destination-port
policy-map p1
   class c1
      police 1000000 bps 9000 byte conform-action transmit exceed-action drop
interface FastEthernet 6/1
 service-policy input p1
Switch# show class-map c1
Class Map match-all c1 (id 2)
  Match flow ip source-address ip destination-address ip protocol 14 source-port 14
destination-port
Switch# show policy-map p1
 Policy Map p1
   Class c1
      police 1000000 bps 9000 byte conform-action transmit exceed-action drop
Switch# show policy-map interface
FastEthernet6/1
 Service-policy input: p1
    Class-map: c1 (match-all)
      15432182 packets
     Match: flow ip source-address ip destination-address ip protocol 14 source-port
14 destination-port
     police: Per-interface
        Conform: 64995654 bytes Exceed: 2376965424 bytes
    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets
```

階層型ポリサーの設定



(注)

階層型ポリサーは、Supervisor Engine V-10GE 上でのみサポートされます。

フロー ポリサーを既存ポリサーと結合し、2 つのポリシング レートをインターフェイスで作成できます。 たとえばデュアル ポリシングを使用すると、特定インターフェイスのすべての着信トラフィック レートを $50~{
m Mbps}$ に制限し、このトラフィックの一部であるそれぞれのフローのレートを $2~{
m Mbps}$ に制限できます。

階層型ポリサーは、service-policy ポリシーマップ設定コマンドで設定できます。ポリシー マップで使用されるクラス マップが、フローベース一致基準 (match flow ip source-address など)と一致する場合、ポリシー マップは フローベースと呼ばれます。それぞれの子ポリシー マップは、親のすべての match access-group コマンドを継承します。



(注)

フローベース ポリシー マップのみを子ポリシー マップとして設定できます。 親ポリシー マップをフローベース ポリシー マップにすることはできません。 子ポリシー マップと親ポリシー マップの両方で、 クラスマップ設定に match-all が含まれている必要があります。

個別ポリサーか集約ポリサーの子としてフローベース ポリシー マップを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# policy_map policy_name	個別ポリシーマップ名か集約ポリシーマップ名を指定しま
		す。
ステップ 2	Switch(config-pmap)# class_class_name	このポリシー マップのクラスマップ名を指定します。
ステップ 3	Switch(config-flow-cache)# service-policy service_policy_name	フローベース ポリシー マップの名前を指定します。



(注)

親が集約ポリサー、子がマイクロフロー ポリサーである階層型ポリサー設定では、子のマイクロフロー ポリサーに一致するパケットはイン プロファイルであるパケットだけを報告します (つまり、ポリシング レートを一致させます) ポリシング レートを超過するパケットは、クラスマップパケット一致統計情報では報告されません。

次の例は、階層型ポリシー マップの作成方法を示しています。名前が aggregate-policy であるポリシー マップには、名前が aggregate-class であるクラス マップが含まれます。名前が flow-policy であるフローベース ポリシー マップは、子ポリシー マップとしてこのポリシー マップに付加されます。

Switch# config terminal

Switch(config) # policy-map aggregate-policy
Switch(config-pmap) # class aggregate-class
Switch(config-pmap-c) # service-policy flow-policy
Switch(config-pmap-c) # end
Switch#

次の例では、IP アドレス範囲が $101.237.0.0 \sim 101.237.255.255$ であるトラフィックが 50 Mbps にポリシングされます。 $101.237.10.0 \sim 101.237.10.255$ の範囲のフローは、2 Mbps の速度で個別にポリシングされます。このトラフィックは、集約ポリサーとその他のフローベース ポリサーという 2 つのポリサーを通過します。

次の例は、このシナリオの設定を示しています。

class-map match-all flow-class

```
match flow ip source-address
match access-group 20
class-map match-all aggregate-class
match access-group 10
policy-map flow-policy
class flow-class
  police 2000000 bps 10000 byte conform-action transmit exceed-action drop
policy-map aggregate-policy
class aggregate-class
  police 50000000 bps 40000 byte conform-action transmit exceed-action drop
  service-policy flow-policy
access-list 10 permit 101.237.0.0 0.0.255.255
access-list 20 permit 0.0.10.0 255.255.0.255
次に、設定を確認する例を示します。
Switch# show policy-map flow-policy
Policy Map flow-policy
  Class flow-class
     police 2000000 bps 10000 byte conform-action transmit exceed-action drop
Switch# show policy-map aggregate-policy
Policy Map aggregate-policy
  Class aggregate-class
     police 50000000 bps 40000 byte conform-action transmit exceed-action drop
     service-policy flow-policy
Switch# show policy-map interface
FastEthernet6/1
Service-policy input: aggregate-policy
  Class-map: aggregate-class (match-all)
     132537 packets
     Match: access-group 10
     police: Per-interface
      Conform: 3627000 bytes Exceed: 0 bytes
     Service-policy : flow-policy
      Class-map: flow-class (match-all)
        8867 packets
        Match: access-group 20
        Match: flow ip source-address
        police: Per-interface
       Conform: 1649262 bytes Exceed: 59601096 bytes
       Class-map: class-default (match-any)
         0 packets
        Match: any
                              0 packets
  Class-map: class-default (match-any)
     5 packets
     Match: any
                       5 packets
```

PVQoS のイネーブル化

PVQoS 機能により、所定のインターフェイスの異なる VLAN 上で異なる QoS 設定を指定できます。 通常、この機能はトランク ポートまたは音声 VLAN (Cisco IP Phone) ポートなど、複数の VLAN に所属するポート上で使用します。

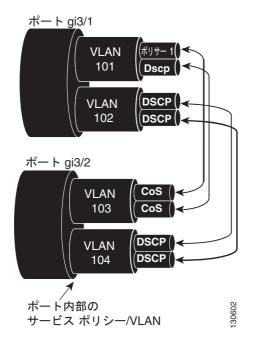
PVQoS を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# interface {fastethernet gigabitethernet tengigabitethernet} slot/interface Port-channel number	設定するインターフェイスを選択します。
ステップ 2	Switch(config-if)# vlan-range vlan_range	関連する VLAN を指定します。
ステップ 3	Switch(config-if-vlan-range)# service-policy {input output} policy-map	ポリシーマップおよび方向を指定します。
ステップ 4	Switch(config-if-vlan-range)# exit	クラスマップ コンフィギュレーション モードを 終了します。
ステップ 5	Switch(config-if)# end	インターフェイス コンフィギュレーション モードを終了します。
ステップ 6	Switch# show policy-map interface interface_name	設定を確認します。

例 1

図 34-6 に、PVQoS 構成のトポロジ例を示します。トランク ポート gi3/1 は、複数の VLAN (101 および 102) で構成されています。ポート内部には、独自のサービス ポリシーを VLAN 単位で作成できます。このポリシーはハードウェアで実行され、入力および出力ポリシング、DSCP の信頼、またはデータよりも音声パケットへの優先制御で構成されます。





次のコンフィギュレーション ファイルでは、ポート GigabitEthernet 3/1 に適用されるポリシーマップ P31_QOS を使用して、VLAN 単位で入力および出力ポリシングを実行する方法について示しています。

```
ip access-list 101 permit ip host 1.2.2.2 any
ip access-list 103 permit ip any any
Class-map match-all RT
match ip access-group 101
Class-map Match all PD
match ip access-group 103
Policy-map P31_QoS
Class RT
Police 200m 16k conform transmit exceed drop
Class PD
Police 100m 16k conform transmit exceed drop
Interface Gigabit 3/1
Switchport
Switchport trunk encapsulation dot1q
Switchport trunk allowed vlan 101-102
   Vlan range 101
       Service-policy input P31_QoS
       Service-policy output P31_QoS
   Vlan range 102
       Service-policy input P32_QoS
       Service-policy output P32_QoS
```

例 2

たとえば、インターフェイス GigabitEthernet 6/1 はトランク ポートで、VLAN 20、 $300 \sim 301$ 、および 400 に属していると仮定します。次に、VLAN 20 と VLAN 400 のトラフィックにポリシーマップ p1、VLAN $300 \sim 301$ のトラフィックにポリシーマップ p2 を適用する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 6/1
Switch(config-if)# vlan-range 20,400
Switch(config-if-vlan-range)# service-policy input p1
Switch(config-if-vlan-range)# exit
Switch(config-if)# vlan-range 300-301
Switch(config-if-vlan-range)# service-policy output p2
Switch(config-if-vlan-range)# end
Switch#
```

例3

次に、インターフェイス GigabitEthernet 6/1 上で設定された VLAN 20 のポリシーマップの統計情報を表示する例を示します。

```
Switch# show policy-map interface gigabitethernet 6/1 vlan 20

GigabitEthernet6/1 vlan 20

Service-policy input: p1

Class-map: class-default (match-any)
0 packets
Match: any
0 packets
police: Per-interface
Conform: 0 bytes Exceed: 0 bytes
```

例 4

次に、インターフェイス GigabitEthernet 6/1 上で設定されたすべての VLAN のポリシーマップの統計情報を表示する例を示します。

```
Switch# show policy-map interface gigabitethernet 6/1
GigabitEthernet6/1 vlan 20
  Service-policy input: p1
    Class-map: class-default (match-any)
      0 packets
     Match: any
       0 packets
      police: Per-interface
       Conform: 0 bytes Exceed: 0 bytes
GigabitEthernet6/1 vlan 300
  Service-policy output: p2
    Class-map: class-default (match-any)
      0 packets
      Match: any
       0 packets
      police: Per-interface
       Conform: 0 bytes Exceed: 0 bytes
GigabitEthernet6/1 vlan 301
  Service-policy output: p2
    Class-map: class-default (match-any)
      0 packets
     Match: any
        0 packets
      police: Per-interface
        Conform: 0 bytes Exceed: 0 bytes
GigabitEthernet6/1 vlan 400
  Service-policy input: p1
    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets
      police: Per-interface
        Conform: 0 bytes Exceed: 0 bytes
```

インターフェイス上での QoS のイネーブル化またはディセーブル化

qos インターフェイス コマンドを使用すると、設定されている QoS 機能が再びイネーブルになります。 **qos** インターフェイス コマンドは、インターフェイスのキュー設定に影響しません。

インターフェイスからのトラフィックに対して QoS 機能をイネーブルまたはディセーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# interface {vlan vlan_ID {fastethernet gigabitethernet} slot/interface Port-channel number}	設定するインターフェイスを選択します。
ステップ 2	Switch(config-if)# [no] qos	インターフェイス上で QoS をイネーブルにします。
		インターフェイス上で QoS をディセーブルにする には、no キーワードを使用します。
ステップ 3	Switch(config-if)# end	コンフィギュレーション モードを終了します。
ステップ 4	Switch# show qos interface	設定を確認します。

次に、インターフェイス VLAN 5上で QoS をディセーブルにする例を示します。

Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface vlan 5
Switch(config-if)# no qos
Switch(config-if)# end
Switch#

次に、設定を確認する例を示します。

Switch# show qos | begin QoS is disabled
 QoS is disabled on the following interfaces:
 V15
<テキスト出力は省略>
Switch#

レイヤ 2 インターフェイス上での VLAN ベース QoS の設定

デフォルトでは、QoS は物理インターフェイスに付加されたポリシー マップを使用します。レイヤ 2 インターフェイスについては、VLAN に付加されたポリシー マップを使用するように QoS を設定できます。(「インターフェイスへのポリシー マップの付加」[p.34-43] を参照)。

レイヤ2インターフェイス上で VLAN ベースの QoS を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# interface {fastethernet gigabitethernet} slot/interface Port-channel number	設定するインターフェイスを選択します。
ステップ 2	Switch(config-if)# [no] qos vlan-based	レイヤ2インターフェイス上で VLAN ベースの QoS を設定します。
		インターフェイス上で VLAN ベース QoS をディセーブルにするには、no キーワードを使用します。
ステップ 3	Switch(config-if)# end	コンフィギュレーション モードを終了します。
ステップ 4	Switch# show qos	設定を確認します。



レイヤ 2 インターフェイスに入力 QoS ポリシーが付加されていない場合、ポートが VLAN ベース で設定されていなくても、(パケットが着信する)VLAN に付加された入力 QoS ポリシーがあれば それが使用されます。このデフォルトが望ましくない場合には、レイヤ 2 インターフェイスにプレースホルダの入力 QoS ポリシーを付加します。同様に、レイヤ 2 インターフェイスに出力 QoS ポリシーが付加されていない場合、ポートが VLAN ベースで設定されていなくても、(パケットを送信する)VLAN に付加された出力 QoS ポリシーがあればそれが使用されます。このデフォルトが望ましくない場合には、レイヤ 2 インターフェイスにプレースホルダの出力 QoS ポリシーを付加します。

次に、インターフェイス FastEthernet 5/42 で VLAN ベースの QoS を設定する例を示します。

Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 5/42
Switch(config-if)# qos vlan-based
Switch(config-if)# end

次に、設定を確認する例を示します。

Switch# show qos | begin QoS is vlan-based QoS is vlan-based on the following interfaces: Fa5/42 Switch#



レイヤ 2 インターフェイスに VLAN ベース QoS が設定されている場合に、QoS ポリシーがない VLAN のポートにパケットが着信すると、ポートに付加された QoS ポリシーがある場合はそれが 使用されます。これは、入力および出力 QoS ポリシーの両方に適用されます。

インターフェイスの信頼状態の設定

このコマンドは、インターフェイスの信頼状態を設定します。デフォルトでは、すべてのインターフェイスが untrusted です。

インターフェイスの信頼状態を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config) # interface {vlan vlan_ID {fastethernet gigabitethernet} slot/interface Port-channel number}	設定するインターフェイスを選択します。
ステップ 2	Switch(config-if)# [no] qos trust [dscp cos]	インターフェイスの信頼状態を設定します。
		設定した値をクリアし、デフォルトに戻すには、no キーワードを使用します。
ステップ 3	Switch(config-if)# end	コンフィギュレーション モードを終了します。
ステップ 4	Switch# show qos	設定を確認します。

インターフェイスの信頼状態を設定する際、次の点に注意してください。

- インターフェイスの状態を untrusted に戻すには、no gos trust コマンドを使用します。
- qos trust cos コマンドを使用して trust cos に設定された入力インターフェイスに着信したトラフィックの場合、送信される CoS は、常に着信パケットの CoS (または、パケットをタグなしで受信した場合には、入力インターフェイスのデフォルト CoS)です。
- qos trust dscp コマンドを使用してインターフェイスの信頼状態を trust dscp に設定していない 場合、セキュリティおよび QoS ACL 分類では、常にインターフェイス DSCP が使用され、着 信パケットの DSCP は使用されません。
- Cisco IOS Release 12.2(31)SG 以降では、Supervisor Engine V-10GE を使用すれば、ポートの信頼 状態に関わらずパケットの IP DSCP 値に基づいてパケットを分類できます。パケット送信 キューイングは影響を受けません。送信キューについては、「送信キューの設定」(p.34-59)を 参照してください。

次に、**trust cos** キーワードを使用してインターフェイス GigabitEthernet 1/1 を設定する例を示します。

Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# qos trust cos
Switch(config-if)# end
Switch#

次に、設定を確認する例を示します。

Switch# show qos interface gigabitethernet 1/1 | include trust
Trust state: trust COS
Switch#

インターフェイスの CoS 値の設定

QoS は、trusted として設定された入力インターフェイスからのタグなしフレーム、および untrusted として設定された入力インターフェイスからのすべてのフレームに、このコマンドで指定された CoS 値を割り当てます。

入力インターフェイスの CoS 値を設定するには、次の作業を行います。

	コマンド	目的				
ステップ 1	Switch(config)# interface {fastethernet gigabitethernet} slot/interface Port-channel number}	設定するインターフェイスを選択します。				
ステップ 2	Switch(config-if)# [no] qos cos default_cos	入力インターフェイスの CoS 値を設定します。				
		設定した値をクリアし、デフォルトに戻すには、no キーワードを使用します。				
ステップ 3	Switch(config-if)# end	コンフィギュレーション モードを終了します。				
ステップ 4	Switch# show qos interface {fastethernet gigabitethernet} slot/interface	設定を確認します。				

次に、インターフェイス FastEthernet 5/24 にデフォルトとして CoS 5 を設定する例を示します。

Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 5/24
Switch(config-if)# qos cos 5
Switch(config-if)# end
Switch#

次に、設定を確認する例を示します。

Switch# show qos interface fastethernet 5/24 | include Default COS Default COS is 5 Switch#

インターフェイスの DSCP 値の設定

QoS は、trust dscp に設定されたインターフェイスで受信した非 IPv4 フレーム、および untrusted として設定されたインターフェイスで受信したすべてのフレームに、このコマンドで指定されたDSCP 値を割り当てます。

入力インターフェイスの DSCP 値を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# interface {fastethernet gigabitethernet} slot/interface Port-channel number	設定するインターフェイスを選択します。
ステップ 2	Switch(config-if)# [no] qos dscp default_dscp	入力インターフェイスの DSCP 値を設定します。
		設定した値をクリアし、デフォルトに戻すには、no キーワードを使用します。
ステップ 3	Switch(config-if)# end	コンフィギュレーション モードを終了します。
ステップ 4	Switch# show qos interface {fastethernet gigabitethernet} slot/interface	設定を確認します。

次に、インターフェイス FastEthernet 5/24 のデフォルトとして DSCP 5 を設定する例を示します。

Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 5/24
Switch(config-if)# qos dscp 5
Switch(config-if)# end
Switch#

次に、設定を確認する例を示します。

Switch# show qos interface fastethernet 6/1

QoS is enabled globally Port QoS is enabled Port Trust State:CoS Default DSCP:0 Default CoS:0

Tx-Queue	Bandwidth (bps)	ShapeRate (bps)	Priority	QueueSize (packets)
1	31250000	disabled	N/A	240
2	31250000	disabled	N/A	240
3	31250000	disabled	normal	240
4	31250000	disabled	N/A	240
Switch#				

送信キューの設定

ここでは、送信キューを設定する手順について説明します。

- DSCP 値から特定の送信キューへのマッピング (p.34-59)
- 送信キュー間での帯域幅の割り当て (p.34-60)
- 送信キューのトラフィック シェーピングの設定 (p.34-60)
- ハイ プライオリティ送信キューの設定 (p.34-61)

ネットワークと QoS ソリューションの複雑さによっては、次に挙げる手順のすべてを実行する必要があります。 たし、最初に次の質問に答えてください。

- 各キューへの (DSCP 値による) パケットの割り当て
- 特定のポートでの送信キューと他のキューとの相対的なサイズ
- 各キューへの使用可能な帯域幅の割り当て
- 各送信キューの最大速度、および各送信キューから送信できる最大バースト トラフィック

DSCP 値から特定の送信キューへのマッピング

DSCP 値を送信キューにマッピングするには、次の作業を行います。

	コマンド	目的	
ステップ 1	Switch(config)# [no] qos map dscp dscp-values to tx-queue queue-id	DSCP 値を送信キューにマッピングします。 dscp-values には、最大 8 つの DSCP 値を指定できま す。queue-id の範囲は、1 ~ 4 です。	
		送信キューから DSCP 値を削除するには、no qos map dscp to tx-queue コマンドを使用します。	
ステップ 2	Switch(config)# end	コンフィギュレーション モードを終了します。	
ステップ 3	Switch# show qos maps dscp tx-queues	設定を確認します。	

次に、送信キュー2に DSCP 値をマッピングする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# qos map dscp 50 to tx-queue 2
Switch(config)# end
Switch#
```

次に、設定を確認する例を示します。

送信キュー間での帯域幅の割り当て

送信キューの帯域幅を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# interface gigabitethernet slot/interface	設定するインターフェイスを選択します。
ステップ 2	Switch(config-if)# tx-queue queue_id	設定する送信キューを選択します。
ステップ 3	Switch(config-if-tx-queue)# [no] [bandwidth rate percent percent]	送信キューの帯域幅レートを設定します。
		送信キューの帯域幅の比率をデフォルト値に戻すに
		は、no キーワードを使用します。
ステップ 4	Switch(config-if-tx-queue)# end	コンフィギュレーション モードを終了します。
ステップ 5	Switch# show qos interface	設定を確認します。

帯域幅レートは、インターフェイスによって異なります。

帯域幅を設定できるのは、次のインターフェイスに限られます。

- Supervisor Engine III (WS-X4014) 上のアップリンク ポート
- WS-X4306-GB モジュール上のポート
- WS-X4232-GB-RJ モジュール上の 2 つの 1000BASE-X ポート
- WS-X4418-GB モジュール上の最初の 2 つのポート
- WS-X4412-2GB-TX モジュール上の 2 つの 1000BASE-X ポート

次に、送信キュー2に1 Mbps の帯域幅を設定する例を示します。

Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# tx-queue 2
Switch(config-if-tx-queue)#bandwidth 1000000
Switch(config-if-tx-queue)# end
Switch#

送信キューのトラフィック シェーピングの設定

送信キューから送信されるパケットが指定の最大速度を超えないように設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# interface {fastethernet gigabitethernet} slot/interface	設定するインターフェイスを選択します。
ステップ 2	Switch(config-if)# tx-queue queue_id	設定する送信キューを選択します。
ステップ 3	Switch(config-if-tx-queue)# [no] [shape rate percent percent]	送信キューの送信レートを設定します。
		送信キューの最大速度を削除するには、no キーワードを使用します。
ステップ 4	Switch(config-if-tx-queue)# end	コンフィギュレーション モードを終了します。
ステップ 5	Switch# show qos interface	設定を確認します。

次に、送信キュー 2 のシェープ レートを 1 Mbps に設定する例を示します。

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet 1/1
Switch(config-if-tx-queue)# tx-queue 2
Switch(config-if-tx-queue)# shape 1000000
Switch(config-if-tx-queue)# end
Switch#

ハイ プライオリティ送信キューの設定

送信キュー3をハイプライオリティに設定するには、次の作業を行います。

	コマンド	目的		
ステップ 1	Switch(config)# interface {fastethernet gigabitethernet} slot/interface	設定するインターフェイスを選択します。		
ステップ 2	Switch(config-if)# tx-queue 3	設定する送信キュー3を選択します。		
ステップ 3	Switch(config-if)# [no] priority high	この送信キューをハイ プライオリティに設定します。		
		送信キューのプライオリティをクリアするには、no キー ワードを使用します。		
ステップ 4	Switch(config-if)# end	コンフィギュレーション モードを終了します。		
ステップ 5	Switch# show qos interface	設定を確認します。		

次に、送信キュー3をハイプライオリティに設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet 1/1
Switch(config-if-tx-queue)# tx-queue 3
Switch(config-if-tx-queue)# priority high
Switch(config-if)# end
Switch#
```

DSCP マップの設定

ここでは、DSCPマップを設定する方法について説明します。内容は次のとおりです。

- CoS/DSCP マップの設定 (p.34-61)
- ポリシング済み DSCP マップの設定 (p.34-62)
- DSCP/CoS マップの設定 (p.34-63)

マップはいずれもグローバルに定義され、すべてのポートに適用されます。

CoS/DSCP マップの設定

CoS/DSCP マップは、着信パケットの CoS 値を、DSCP 値(トラフィックのプライオリティを表すために QoS が内部的に使用する)にマッピングする目的で使用します。

表 34-4 に、デフォルトの CoS/DSCP マップを示します。

表 34-4 デフォルトの CoS/DSCP マップ

CoS 値	0	1	2	3	4	5	6	7
DSCP 値	0	8	16	24	32	40	48	56

これらの値がネットワークに適さない場合は、値を変更する必要があります。

CoS/DSCP マップを変更するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	Switch(config)# qos map cos cos1 cos8 to dscp dscp	CoS/DSCP マップを変更します。 cos1cos8 には、最大 8 つの CoS を入力できます。指定できる値の範囲は 0 ~ 7 です。各 CoS 値をスペースで区切ります。 dscp の範囲は 0 ~ 63 です。
ステップ 3	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 4	Switch# show qos maps cos-dscp	入力を確認します。
ステップ 5	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を 保存します。

次に、入力 CoS/DSCP マッピングで CoS を 0 に設定する例を示します。

Switch# configure terminal
Switch(config)# qos map cos 0 to dscp 20
Switch(config)# end
Switch# show qos maps cos dscp

Cos-DSCP Mapping Table:
Cos: 0 1 2 3 4 5 6 7
----DSCP: 20 8 16 24 32 40 48 56
Switch(config)#



デフォルトのマップに戻すには、no qos cos to dscp グローバル コンフィギュレーション コマンドを使用します。

次に、CoS/DSCPマッピングテーブル全体をクリアする例を示します。

Switch(config) # no qos map cos to dscp Switch(config) #

ポリシング済み DSCP マップの設定

ポリシング済み DSCP マップは、ポリシングおよびマーキング アクションの結果、DSCP 値を新しい値にマークダウンする目的で使用します。

デフォルトのポリシング済み DSCP マップはヌルで、着信 DSCP 値が同じ DSCP 値にマッピングされます。

CoS/DSCP マップを変更するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	Switch(config)# qos map dscp policed dscp-list to dscp mark-down-dscp	ポリシング済み DSCP マップを変更します。 • dscp-list には、最大 8 つの DSCP 値をスペースで 区切って入力します。その後ろに、to キーワードを入力します。 • mark-down-dscp には、対応するポリシング済み (マークダウンされた) DSCP 値を入力します。
ステップ 3	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 4	Switch# show qos maps dscp policed	入力を確認します。
ステップ 5	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を 保存します。

デフォルトのマップに戻すには、no qos dscp policed グローバル コンフィギュレーション コマンドを使用します。

次に、DSCP $50 \sim 57$ を、マークダウンされた DSCP 値 0 にマッピングする例を示します。

Switch# configure terminal

Switch(config) # qos map dscp policed 50 51 52 53 54 55 56 57 to dscp 0

Switch(config)# end

Switch# show qos maps dscp policed

Policed-dscp map:

 d1:
 d2 0 1 2 3 4 5 6 7 8 9

 0:
 00 01 02 03 04 05 06 07 08 09

 1:
 10 11 12 13 14 15 16 17 18 19

 2:
 20 21 22 23 24 25 26 27 28 29

 3:
 30 31 32 33 34 35 36 37 38 39

 4:
 40 41 42 43 44 45 46 47 48 49

 5:
 00 00 00 00 00 00 00 00 00 58 59

 6:
 60 61 62 63



前述のポリシング済み DSCP マップでは、マークダウンされた DSCP 値がマトリクスの本体に示されています。カラム d1 は、元の DSCP の上位桁を表し、行 d2 は、元の DSCP の下位桁を表します。d1 と d2 が交わった部分にある値が、マークダウン後の値です。たとえば、元の DSCP 値が 53 である場合、対応するマークダウン後の DSCP 値は 0 です。

DSCP/CoS マップの設定

DSCP/CoS マップは、CoS 値を生成する目的で使用します。

表 34-5 に、デフォルトの DSCP/CoS マップを示します。

表 34-5 デフォルトの DSCP/CoS マップ

DSCP 値	0 ~ 7	8 ~ 15	16 ~ 23	24 ~ 31	32 ~ 39	40 ~ 47	48 ~ 55	56 ~ 63
CoS 値	0	1	2	3	4	5	6	7

これらの値がネットワークに適さない場合は、値を変更する必要があります。

DSCP/CoS マップを変更するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	Switch(config)# [no] qos map dscp dscp-list to cos cos	DSCP/CoS マップを変更します。
		• <i>dscp-list</i> には、最大 8 つの DSCP 値をスペースで 区切って入力します。その後ろに、to キーワー ドを入力します。
		 cos には、一連の DSCP 値を対応させる CoS 値を1 つだけ入力します。
		DSCP の範囲は 0 ~ 63、CoS の範囲は 0 ~ 7 です。
		デフォルトのマップに戻すには、no qos dscp to cos グローバル コンフィギュレーション コマンドを使 用します。
ステップ 3	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 4	Switch# show qos maps dscp to cos	入力を確認します。
ステップ 5	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を 保存します。

次に、DSCP 値 0、8、16、24、32、40、48、および 50 を CoS 値 0 にマッピングし、マップを表示する例を示します。

Switch# configure terminal

 $\label{eq:switch} \textbf{Switch(config)} \ \# \ \textbf{qos} \ \textbf{map} \ \textbf{dscp} \ \textbf{0} \ \textbf{8} \ \textbf{16} \ \textbf{24} \ \textbf{32} \ \textbf{40} \ \textbf{48} \ \textbf{50} \ \textbf{to} \ \textbf{cos} \ \textbf{0}$

Switch(config)# end

Switch# show qos maps dscp cos

Dscp-cos map:

d1	:	d2 0	1	2	3	4	5	6	7	8	9	
0	:	00	00	00	00	00	00	00	00	00	01	
1	:	01	01	01	01	01	01	00	02	02	02	
2	:	02	02	02	02	00	03	03	03	03	03	
3	:	03	03	00	04	04	04	04	04	04	04	
4	:	00	05	05	05	05	05	05	05	00	06	
5	:	00	06	06	06	06	06	07	07	07	07	
6	:	07	07	07	07							



(注)

前述の DSCP/CoS マップでは、CoS 値がマトリクスの本体に示されています。カラム d1 は、DSCP の上位桁を表し、行 d2 は、DSCP の下位桁を表します。d1 と d2 が交わった部分にある値が、CoS 値です。たとえば、この DSCP/CoS マップでは、DSCP 値 08 は CoS 値 0 に対応しています。

レイヤ 2 制御パケット QoS のイネーブル化



レイヤ 2 制御パケット QoS は、Supervisor Engine 6-E ではサポートされていません。

この機能では、大量の制御パケットの入力による高 CPU 利用率の問題を解決します。問題の解決は、制御したハプロトコル (QoS CAM にインストール済み) に対応する QoS スタティック エントリを無効にすることで行われます。

解決法では、ハードウェアは、レイヤ 2 制御トラフィックに一致するユーザ定義サービス ポリシーに対応するアクションを適用します。この制御モードは、デフォルト モードが既存のモードであるため、CLI を介して展開できます。

必須レイヤ2パケットに一致するようにポリシーを設定し、希望するレベルにポリシングする必要があります。レイヤ2制御パケットは、基本的に宛先MACアドレスで識別されます。この機能が、そのパケットタイプでイネーブルになっていると、目的の制御パケットに一致する MACL およびそれらの MACL に一致する対応クラスマップがまだ存在しない場合、自動生成されます。

制御パケットのポリシングを行うには、ポリシーマップでこれらのクラスマップを使用する必要があるだけです。その後他のポリシーマップと同様に、ポート単位、VLAN単位、またはポート単位/VLAN単位でポリシーマップを適用できます。

レイヤ2制御パケット QoS をイネーブルにするには、次の作業を実行します。

	コマンド	目的	
ステップ 1	Switch# interface t	コンフィギュレーション モードを開始します。	
ステップ 2	Switch(config)# qos control-packets [bpdu-range cdp-vtp sstp]	レイヤ 2 制御ポリシングをイネーブルにします。 この機能をイネーブルにするパケット タイプを指 定できます。	
		デフォルトでは、すべてのパケット タイプが選択されます。	
ステップ 3	Switch(config)# end	コンフィギュレーション モードを終了します。	
ステップ 4	Switch# show run inc qos control-packets	設定を確認します。	

次の表では、この機能で影響を受けるパケットタイプを一覧にします。

表 34-6 パケット タイプとアクション可能なアドレス範囲

機能がイネーブルになるパケット タイプ	動作するアドレス範囲
BPDU 範囲	0180.C200.0000 BPDU
	0180.C200.0002 OAM、LACP
	0180.C200.0003 Eapol
CDP-VTP	0100.0CCC.CCCC
SSTP	0100.0CCC.CCCD

次に、レイヤ 2 制御パケット QoS を CDP-VTP パケットに設定する例を示します。

Switch# config terminal
Switch(config)# qos control-packets cdp-vtp
Switch(config)# end
Switch# show run | inc qos control-packets
qos control-packets cdp-vtp

すべてのパケット タイプでこの機能がイネーブルになっているとき、show running コマンドの出力には、gos control-packets 文字列が表示されます。

Switch# show running | inc qos control-packets qos control-packets

ここで、SSTP パケットに対してこの機能をディセーブルにしている場合、次の出力が表示されます。

Switch# show running | inc qos control-packets qos control-packets bpdu-range qos control-packets cdp-vtp

show running コマンドおよび一般的な関連コマンドで、目的の制御パケットをキャプチャ、ドロップ、およびポリシングする、MACL およびユーザ設定ポリシーのステータスを確認できます。

この機能をディセーブルにするには、no qos control-packets [bpdu-range | cdp-vtp | sstp] コマンドを実行します。たとえば、CDP-VTP パケットで機能をディセーブルにするには、no qos control-packets cdp-vtp コマンドを実行します。



指定したプロトコルタイプに対してこの機能の設定を解除すると、そのプロトコルタイプを処理するユーザ設定ポリシーは、直ちに無効な状態になります。TCAM リソースを保存するには、MACL およびクラスマップ(自動生成またはユーザ定義)とともにポリシーも削除します。

次の表に、対応パケット タイプで機能がイネーブルになっているときに作成されるクラスマップを示します。

表 34-7 パケット タイプおよび自動生成 MACL/ クラスマップ

パケット タイプ	自動生成 MACL/ クラスマップ
BPDU 範囲	mac access-list extended system-control-packet-bpdu-range
	permit any 0180.c200.0000 0000.0000.000c
	class-map match-any system-control-packet-bpdu-range
	match access-group name system-control-packet-bpdu-range
SSTP	mac access-list extended system-control-packet-sstp
	permit any host 0100.0ccc.cccd
	class-map match-any system-control-packet-sstp
	match access-group name system-control-packet-sstp
CDP-VTP	mac access-list extended system-control-packet-cdp-vtp
	permit any host 0100.0ccc.cccc
	class-map match-any system-control-packet-cdp-vtp
	match access-group name system-control-packet-cdp-vtp

次に、BPDU 範囲パケットに MACL およびポリサー設定を適用する例を示します。

• BPDU 範囲でこの機能をイネーブルにします。

qos control-packets bpdu-range

• 対応 MACL/ クラスマップを作成します (自動的に実行)。

mac access-list extended system-control-packet-bpdu-range
 permit any 0180.C200.0000 0000.0000.000C

class-map match-any system-control-packet-bpdu-range
 match access-group name system-control-packet-bpdu-range

• ポリシーマップを作成し、目的のインターフェイス /VLAN に付加します。

policy-map police-bpdu
 class system-control-packet-bpdu-range
 police 32000 bps 1000 byte conform-action transmit exceed-action drop

interface GigabitEthernet 1/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 vlan-range 100
 service-policy input police_bpdu

システムが生成したクラスマップおよび MACL を変更しないでください。変更すると、スイッチがリロードを行うとき、または実行コンフィギュレーションをファイルから更新するとき、予期せぬ動作になることがあります。

これらのシステム生成クラスマップまたは MACL を調整または変更する必要がある場合、ユーザ 定義クラスマップおよび MACL を作成する必要があります。次に、作成した新しいユーザ定義 MACL/ クラスマップを使用して、目的のポリシングを実行します。



<u>___</u>(注)

ユーザ定義クラスマップ名をプレフィクス system-control-packet- で始める必要がある点だけが唯一の制限事項です。クラスマップが system-control-packet- で始まらない場合、特定のスーパーバイザエンジンでは、設定された QoS アクションが実行されないことがあります。



(注)

ユーザ定義 MACL に使用する名前には、制限事項はありません。

たとえば、次に挙げる名前は、制御パケットをポリシングする、有効なユーザ定義クラスマップ名です。

system-control-packet-bpdu1
system-control-packet-control-packet
system-control-packet-bla

たとえば、EAPOL、OAM、または BPDU パケットに異なるクラスマップを定義する予定である場合、自動生成クラスマップの system-control-packet-bpdu-range はすべてのパケットに一致するため、ユーザ定義 MACL/ クラスマップ (前述の例) の作成が役立ちます。

```
mac access-list extended system-control-packet-bpdu
permit any 0180.c200.0000

class-map match-any system-control-packet-bpdu
match access-group name system-control-packet-bpdu

mac access-list extended system-control-packet-eapol
permit any 0180.c200.0003

class-map match-any system-control-packet-eapol
match access-group name system-control-packet-eapol

mac access-list extended system-control-packet-oam
permit any 0180.c200.0002

class-map match-any system-control-packet-oam
match access-group name system-control-packet-oam
```

次にこれらのクラスマップを使用して、共通ポリサーを system-control-packet-bpdu-range に適用する 代わりに、各パケットに異なるポリサーを定義できます。

使用上の注意事項

この機能がイネーブルになっているとき、ポートおよび VLAN に適用された既存のポリシーは、制御したいレイヤ 2 制御パケットが偶発的に希望しない QoS アクションの対象になることがなく、この機能がスイッチ上で設定された他のポリシーから影響を受けることがないというポリシーであることを確認する必要があります。

前述の制御パケットで QoS をイネーブルにする前に、新規および既存のポリシーを調べて編集し、選択した制御パケットに一致するポリシーマップの分類子が正しい順番で定義および設定されていることを確認する必要があります。同じポリシーマップ内の後半に出現する別の分類子のアクションで意図しない結果になることを避けるため、制御パケットに一致する分類子をポリシーマップの冒頭に配置する必要があります。

class-default クラスに関連付けられたアクションの場合、その動作はスーパーバイザ エンジンの種類によって変わります。

- 内蔵 NetFlow がサポートされている Supervisor Engine V-10GE class-default に関連付けられたアクションは、一致しない制御パケットには適用されず、control-packet クラスマップがそれより前に制御パケットを取得していない場合、デフォルトの許可アクションは適用されません。system-control-packet-で始まるクラスマップを使用するポリサーに関連付けられたアクションだけが、制御パケットに適用されます。
- 他のすべてのスーパーバイザエンジン class-default に関連付けられたアクションは、一致しない制御パケットに適用されます。



内蔵 NetFlow がサポートされている Supervisor Engine V-10GE では、これらのタイプのパケットでマイクロフロー統計は使用できません。



(注)

BPDU 範囲でこの機能がイネーブルになっている場合、最初の 802.1X 認証フェーズが完了した後でのみ EAPOL パケットをポリシングできます。

34-68



(注)

フォワーディング スパニングツリー ステートになっているポートでポート セキュリティがイネー ブルになっているとき、レイヤ 2 制御パケットはそのポート上でポリシングできません。

機能の相互作用

各単一フローにユーザ設定ポリシーを適用したあと、レイヤ 2 制御パケット QoS の最初にある CoPP ポリシーを設定し、CPU へ送信される集約フローをレート制限します。その場合、基本的に CoPP は、ユーザ定義ポリシーによりポート単位 /VLAN 単位ベースですでに入力側でフィルタされ たパケットの出力側でさらにレート制限を行って、CPU のための別レベルの保護を提供します。 CoPP は、ポート上にユーザ定義ポリシーが適用されている間は、第 2 レベルの防御となり、VLAN は第 1 レベルの防御になります。

たとえば、ポリシーマップマッチングおよびインターフェイス GigabitEthernet 1/1 から送信される BPDU 範囲トラフィックのポリシングを設定する場合、VLAN 1 は次のようになります。

```
policy-map police_bpdu_1
    class system-control-packet-bpdu-range
police 32000 bps 1000 byte conform-action transmit exceed-action drop

interface GigabitEthernet1/1
    switchport trunk encapsulation dot1q
    switchport mode trunk
    vlan-range 1
    service-policy input police_bpdu_1
```

さらに、インターフェイス GigabitEthernet 1/2 VLAN 2 で 2 番めを設定すると、BPUD 範囲パケットのマッチングおよびポリシングは次のようになります。

```
policy-map police_bpdu_2
    class system-control-packet-bpdu-range
police 34000 bps 1000 byte conform-action transmit exceed-action drop

interface GigabitEthernet1/2
    switchport trunk encapsulation dot1q
    switchport mode trunk
    vlan-range 2
    service-policy input police_bpdu_2
```

CoPP は次のように設定します。

```
policy-map system-cpp-policy
     class system-cpp-bpdu-range
   police 50000 bps 1000 byte conform-action transmit exceed-action drop
```

次の点に注意してください。

- インターフェイス 1/1、VLAN 1 では、BPDU 範囲パケットは、police_bpdu_1 に従って毎秒 32000 ビットのレートでポリシングされます。
- インターフェイス 1/2、VLAN 2 では、BPDU 範囲パケットは、police_bpdu_2 に従って毎秒 34000 ビットのレートでポリシングされます。
- 集約フローは、毎秒 50000 ビットのレートで CPU ポートの CoPP からポリシングされます。

また、ポートまたは VLAN のグループに適用された名前付き集約ポリサーを使用して、ポリサーリソースの消費を減らすこともできます。



フォワーディング スパニングツリー ステートになっているポートでポート セキュリティがイネーブルになっているとき、レイヤ 2 制御パケットはそのポート上でポリシングできません。

Supervisor Engine 6-E での Auto-QoS の設定

Supervisor Engine II-Plus から V-10GE までの Auto-QoS とは異なり、Supervisor Engine 6-E の Auto-QoS は MQC モデルを採用しています。特定のグローバル コンフィギュレーション(qos や qos dbl など) を使用する代わりに、Supervisor Engine 6-E のスイッチ上のインターフェイスに適用された Auto-QoS は、いくつかのグローバル クラスマップおよびポリシーマップを設定します。

クラスマップは次のとおりです。

```
class-map match-all AutoQos-VoIP-Control-Dscp26
 match dscp af31
class-map match-all AutoQos-VoIP-Control-Dscp24
 match dscp cs3
class-map match-all AutoQos-VoIP-Bearer-Cos
 match cos 5
class-map match-all AutoQos-VoIP-Control-QosGroup24
  match qos-group 24
class-map match-all AutoQos-VoIP-Control-QosGroup26
 match gos-group 26
class-map match-all AutoQos-VoIP-Bearer-QosGroup
 match qos-group 46
class-map match-all AutoQos-VoIP-Bearer-Dscp
 match dscp ef
class-map match-all AutoQos-VoIP-Control-Cos
 match cos 3
```

これらのクラスマップは、レイヤ 2 またはレイヤ 3 いずれかのインターフェイスの制御およびデータ (ベアラ)音声トラフィックを識別することが意図されています。

ポリシー マップは次のとおりです。

```
policy-map AutoQos-VoIP-Input-Dscp-Policy
 class AutoOos-VoIP-Bearer-Dscp
  set gos-group 46
 class AutoQos-VoIP-Control-Dscp26
  set qos-group 26
 class AutoOos-VoIP-Control-Dscp24
  set gos-group 24
policy-map AutoQos-VoIP-Input-Cos-Policy
 class AutoQos-VoIP-Bearer-Cos
  set gos-group 46
 class AutoQos-VoIP-Control-Cos
   set qos-group 24
policy-map AutoQos-VoIP-Output-Policy
 class AutoQos-VoIP-Bearer-QosGroup
  set dscp ef
  set cos 5
   priority
  police cir percent 33
  class AutoQos-VoIP-Control-QosGroup26
  set dscp af31
  set cos 3
   bandwidth remaining percent 5
  class AutoQos-VoIP-Control-QosGroup24
  set dscp cs3
  set cos 3
   bandwidth remaining percent 5
  class class-default
```

3 つのポリシーマップは次のように定義されます。

 ポリシーマップ AutoQos-VoIP-Input-Dscp-Policy
 このポリシー マップは、Auto-QoS がポート上で設定されるとき、レイヤ 3 インターフェイス (ネイバースイッチへのアップリンク接続など)に入力サービス ポリシーとして適用されます。

- ポリシーマップ AutoQos-VoIP-Input-Cos-Policy
 このポリシー マップは、アップリンク接続または Cisco IP Phone にフックされたポートのいずれかの、レイヤ 2 インターフェイスに入力サービス ポリシーとして適用されます。
- ポリシーマップ AutoQos-VoIP-Output-Policy
 このポリシー マップは、Auto-QoS が設定されている任意のポートの出力ポリシーとして適用
 され、トラフィックが音声データか制御トラフィックかに従ってポート上で出力トラフィック
 を管理するポリシーを確立します。

入力ポリシー マップの目的は、音声データまたは制御トラフィック識別し、マーク付けしながらスイッチを通過させることです。出力ポリシー マップは、入力時に発生するマーク付けでパケットに一致させ、帯域幅、ポリシングまたはプライオリティ キューイングなどの出力パラメータを適用します。

Supervisor Engine 6-E に採用されているスイッチでの Auto-QoS の呼び出しでは、Supervisor Engine II-Plus から V-10GE までで使用されるのと同じコンフィギュレーション コマンドを使用します。

スイッチ対スイッチの接続の場合、インターフェイス上での入力および出力サービス ポリシーの適用には、[no] auto gos voice trust コマンドが使用されます。

service-policy input AutoQos-VoIP-Input-Cos-Policy

または

service-policy input AutoQos-VoIP-Input-Dscp-Policy

および

service-policy output AutoQos-VoIP-Output-Policy

入力ポリシーの選択は、ポートがレイヤ 2 かレイヤ 3 かによって異なります。レイヤ 2 の場合、ポリシーでは受信パケット内の Cos 設定を信頼します。レイヤ 3 ポートの場合、パケットに含まれる DSCP 値に依存します。

電話接続ポートの場合、ポートへの次のサービス ポリシーの適用には、[no] auto qos voice cisco-phone コマンドが使用されます。

qos trust device cisco-phone

service-policy input AutoQos-VoIP-Input-Cos-Policy

および

service-policy output AutoQos-VoIP-Output-Policy

ここでは、Cisco IP Phone を認識する信頼境界が確立され、電話からのパケットの CoS 設定を信頼します。Cisco IP Phone が検出されない場合、CoS フィールドは無視され、パケットは音声トラフィックとして分類されません。Cisco Phone が検出されると、パケット内の CoS 値に基づいて入力パケットにマークが付けられます。このマーキングは、出力で適切なトラフィック分類と処理のために使用されます。

Supervisor Engine 6-E での QoS の設定

次の内容について説明します。

- MQC ベースの QoS の設定 (p.34-72)
- 概要 (p.34-72)
- プラットフォームでサポートされる分類基準および QoS 機能 (p.34-74)
- プラットフォーム ハードウェアの機能 (p.34-75)
- QoS サービス ポリシーを適用するための前提条件(p.34-75)
- QoS サービス ポリシーの適用に関する制約事項 (p.34-75)
- 分類 (p.34-75)
- ポリシング (p.34-76)
- ネットワーク トラフィックのマーク付け (p.34-77)
- シェーピング、共有(帯域幅) プライオリティ キュー、キュー制限、および DBL (p.34-84)

MQC ペースの QoS の設定

Cisco IOS Release 12.2(40)SG 以降では、Supervisor Engine 6-E を使用している Catalyst 4500 シリーズスイッチは、QoS の MQC モデルを採用しています。QoS を適用するには、次の作業を完了できるCLI 構造であるモジュラ QoS コマンドライン インターフェイス (MQC) を使用します。

- トラフィック クラスの定義に使用する一致基準を指定します。
- トラフィック ポリシー(ポリシー マップ)を作成します。トラフィック ポリシーは、各トラフィック クラスに実行する QoS ポリシー アクションを定義します。
- ポリシー マップで指定されたポリシー アクションをインターフェイス、VLAN、またはポート および VLAN に適用します。

MQC についての詳細は、『Cisco IOS Quality of Service Solutions Configuration Guide』Release 12.3 の「Modular Quality of Service Command-Line Interface」を参照してください。



(注)

MQC モデルでは、Supervisor Engines II-Plus から V-10GE のZイッチ QoS モデルで利用可能な 信頼機能がサポートされていません。Supervisor Engine 6-E でサポートされている MQC モデルでは、着信トラフィックはデフォルトで信頼できると見なされます。インターフェイスで 信頼境界機能がイネーブルの場合のみ、ポートを非信頼モードにすることができます。このモードでは、スイッチは IP パケットの DSCP 値とイーサネット フレーム上にある VLAN タグの Cos 値を「0」とマークします。

概要

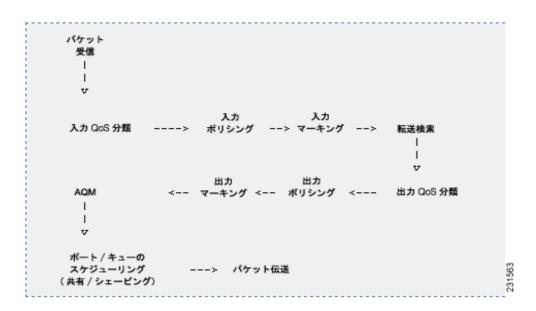
Supervisor Engine 6-E は、ベスト エフォートと QoS の DiffServ タイプの展開 (RFC 2597、2598、2474、2475 は DiffServ 基準を定義) をサポートします。高レベル Supervisor Engine 6-E の QoS モデルは次のとおりです。

- **ステップ1** 着信パケットは、異なるパケットフィールド、受信ポートおよび / または VLAN に基づいてトラフィック クラスに割り当てられます。
- **ステップ2** トラフィック クラスによっては、パケットはレート制限またはポリシングされ、低プライオリティパケットがドロップされるか、パケット フィールド (DSCP および CoS) に低プライオリティのマークが付くように、任意で(通常はネットワークのエッジで) *マーク付けされ*ます。

- **ステップ3** パケットがマーク付けされると、転送用に*検索*されます。このアクションでは、送信ポートとパケットを送信する VLAN が取得されます。
- ステップ4 パケットは、送信ポートおよび VLAN に基づいて出力方向で分類されます。分類では、入力 QoS によるパケットのマーキングが考慮されます。
- **ステップ 5** 出力分類によって、パケットはポリシングされ、そのプライオリティは任意で (*再び) マーク付け* されて、パケットの送信キューがトラフィック クラスに従って決定されます。
- **ステップ6** 送信キューのステートは、AQM アルゴリズムおよびドロップしきい値設定を介してダイナミック に監視され、そのパケットをドロップするか、送信用にキューに入れるかが判別されます。
- ステップ7 伝送に適格である場合、パケットは送信キューに入れられます。送信キューは、出力 QoS 分類基準 に基づいて選択されます。選択されたキューは、遅延および帯域幅に関して目的の動作を行います。

図 34-7 に、Supervisor Engine 6-E の高レベル モデルを示します。

図 34-7 QoS パケットの処理



プラットフォームでサポートされる分類基準および QoS 機能

次の表に、Supervisor Engine 6-E でサポートされるさまざまな分類基準およびアクションのまとめを示します。詳細については、『Catalyst 4500 Series Switch Command Reference』を参照してください。

サポートされる分類アクション	説明		
match access-group	指定した ACL をベースにクラス マップに対して一致基準を設定します。		
match any	すべてのパケットに一致する一致基準を、クラス マップに対して設定します。		
match cos	レイヤ 2 の CoS マーキングに基づいてパケットを照合します。		
match destination-address mac	宛先 MAC アドレスを一致基準として使用します。		
match source-address mac	送信元 MAC アドレスを一致基準として使用します。		
match [ip] dscp	特定の DSCP 値を一致基準として指定します。1 つの一致文に 8 つまでの DSCP 値を含めることができます。		
match [ip] precedence	IP Precedence 値を一致基準として指定します。		
match protocol	指定したプロトコルに基づいてクラス マップに対して一致基準を設定します。		
match qos-group	特定の QoS グループ値を一致基準として指定します。出力方向でのみ適用されます。		
サポートされる QoS 機能	説明		
police	トラフィック ポリシングを設定します。		
police (percent)	インターフェイスで使用可能な帯域幅のパーセンテージに基づいてトラフィック ポリシングを設定します。		
police (two rates)	CIR と PIR(Peak Information Rate;最大情報レート)の 2 つのレートを使用して、トラフィック ポリシングを設定します。		
service-policy	(互いの内部でトラフィック ポリシーをネスト化 [階層型トラフィック ポリシー]するための) 一致基準として使用されるトラフィック ポリシーの名前を指定します。最大 2 レベルがサポートされます。		
set cos	発信パケットのレイヤ 2 CoS 値を設定します。		
set dscp	IPv4 の ToS バイトまたは IPv6 パケットのトラフィック クラス バイトで DSCP 値を設定して、パケットにマークを付けます。		
set precedence	パケット ヘッダーに Precedence 値を設定します。		
set qos-group	あとでパケットの分類に使用できる QoS グループの ID を設定します。		
table map support	別のパケット フィールドに基づいてパケット フィールドに無条件にマーク付けします。		
priority	ポリシー マップに属しているトラフィックのクラスにプライオリティを設定します。		
shape	指定したアルゴリズムに基づいて、指示されたビット レートにトラフィックをシェーピングします。		
bandwidth	8 つのキューそれぞれに、保障されている最小帯域幅を提供します。		
dbl	Dynamic Buffer Limiting です。		
queue-limit	送信キューが保持できるパケットの最大数を指定します。		

プラットフォーム ハードウェアの機能

QoS アクション	サポートされるエントリ数
分類	64k 入力および 64k 出力分類エントリがサポートされます。
	1 つのポリシーでは、最大 24k ACL を使用できます。
ポリシング	16K ポリサーがサポートされています。ポリサーは、2k のブロックの指定方向に割り当てられます。たとえば、2k ポリサーを入力に、14k ポリサーを出力に、それぞれ使用できます。単一レート ポリサーは、1 つのポリサー エントリを使用します。Single Rate Three Color Marker(srTCM) RFC 2697)および Two Rate Three Color Marker(trTCM) (RFC 2698)は、2 つのポリサーエントリを使用します。
マーキング	CoS および $DSCP/Precedence$ は、それぞれが 512 エントリをサポートできる 2 つの マーキング テーブルを介してサポートされます。各方向にそれぞれ別個のテーブルがあります。
キューイング	キュー サイズは、シャーシおよびライン カードのタイプに応じてポートごとに設定可能な最大エントリ数で設定されます。
DBL	設定されたすべてのクラスマップで DBL アクションをイネーブルにできます。

QoS サービス ポリシーを適用するための前提条件

スイッチ OoS モデルとは異なり、さまざまなターゲットで OoS をイネーブルにするための前提条 件はありません。サービス ポリシーを適用すれば QoS がイネーブルになり、そのポリシーの適用 を解除すると、ターゲット上で QoS がディセーブルになります。

QoS サービス ポリシーの適用に関する制約事項

インターフェイス、VLAN、またはポートおよび VLAN 上で、トラフィック マーキングを設定でき ます。インターフェイスは、レイヤ2アクセスポート、レイヤ2スイッチトランク、レイヤ3ルー テッド ポート、または EtherChannnel が考えられます。ポリシーは、vlan configuration モードを使 用して VLAN に付加されます。



(注) ポリシーの SVI への付加はサポートされていません。

分類

Supervisor Engine 6-E は、レイヤ 2、IP および IPv6 パケットの分類をサポートします。入力で実行 されるパケット マーキングは、出力方向で照合できます。前述の表では、すべての機能が一覧に なっています。デフォルトでは、Supervisor Engine 6-E は、分類リソースも共有します。

デフォルトでは、ポート、VLAN、またはポート単位 /VLAN 単位 ターゲットに同じポリシーが付 加されている場合、ACL エントリが Supervisor Engine 6-E で共有されます。 CAM エントリが共有 されていたとしても、QoS アクションは各ターゲットで一意です。

次に例を示します。

class-map c1 match ip anv Policy Map p1 class ipp5 police rate 1 m burst 200000 ポリシーマップ p1 がインターフェイス $Gig\ 1/1$ および $Gig\ 1/2$ に適用されている場合、1 つの CAM エントリ (IP パケットに一致する 1 つの ACE) が使用されますが、2 つのポリサー (9-6 クーゲットごとに 1 つずつ) が割り当てられます。したがって、すべての IP パケットがインターフェイス $Gig\ 1/1$ で 1 mbps にポリシングされ、インターフェイス $Gig\ 1/2$ 上のパケットも 1 mbps にポリシングされます。

ポリシング

Supervisor Engine 6-E は、次の操作モードでポリサーをサポートします。

Single Rate Policer Two Color Marker

この種類のポリサーは、CIR と通常バーストでのみ設定され、conform アクションと exceed アクションのみがあります。

これは、Supervisor Engine II-Plus から V-10GE ベース システムでサポートされる唯一の形式です。

- srTCM (RFC 2697)
- trTCM (RFC 2698)
- Color Blind Mode

設定済みポリサー レートの 0.75% のポリシング精度

Supervisor Engine 6-E は、16384 (16×1024 、16K) 単一レート、単一バースト ポリサーをサポートします。16K ポリサーは、2K ポリサーの バンク 8 個で編成されています。ポリサー バンクは、QoS 設定に従い、ソフトウェアによってダイナミックに割り当てられます (入力または出力ポリサー バンク)。したがって、16K ポリサーは、次のようにダイナミックにソフトウェアで分割されます。

- 0入力ポリサーと 16K 出力ポリサー
- 2K 入力ポリサーと 14K 出力ポリサー
- 4K 入力ポリサーと 12K 出力ポリサー
- 6K 入力ポリサーと 10K 出力ポリサー
- 8K 入力ポリサーと 8K 出力ポリサー
- 10K 入力ポリサーと 6K 出力ポリサー
- 12K 入力ポリサーと 4K 出力ポリサー14K 入力ポリサーと 2K 出力ポリサー
- 16K 入力ポリサーと 0 出力ポリサー

これらの数値は、単一レートおよびバースト パラメータをサポートするハードウェア内の個々のポリサー エントリを表します。この数値に基づき、Supervisor Engine 6-E は、次の数のポリサーをサポートします。

- 単一バースト付き 16K 単一レート ポリサー (Two Color Marker)
- 8K srTCM
- 8K trTCM

これらのポリサーは、2K ポリサー バンクの塊で、入力と力の間で分割されます。さまざまなタイプのポリサーは、すべてシステム内に共存できます。ただし、ポリサーの特定タイプ (srTCM、trTCM など) は、128 個のポリサーのブロックとして設定可能です。

ポリシングの実装方法

Catalyst 4500 シリーズ スイッチにポリシング機能を実装する方法の詳細については、次のリンク先にある Cisco IOS マニュアルを参照してください。

http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_book09186a0080435d50.html

プラットフォームの制約事項

プラットフォームの制約事項は、次のとおりです。

- マルチポリサー アクションを指定できます(CoS および IP DSCP の設定がサポートされています)。
- 無条件マーキングとポリサーベースマーキングは同時にはサポートされません。
- ポリサー ベースのサービスポリシーがポートと VLAN の両方に付加されている場合、ポート ベースのポリシングがデフォルトで優先されます。特定の VLAN ポリシーを指定ポートで優先 させるには、ポート単位 /VLAN 単位ポリシーを設定する必要があります。
- PVQoS ポリシーのあるポートチャネルを削除すると、スイッチはクラッシュします。

回避策:ポートチャネルを削除する前に、次の作業を実行します。

- 1. 存在する場合は PVQoS ポリシーを削除します。
- 2. no vlan-range コマンドを使用して、ポートチャネル上の VLAN 設定を削除します。

ネットワーク トラフィックのマーク付け

ネットワーク トラフィックのマーク付けにより、特定のクラスまたはカテゴリに属するトラフィック(パケット)の属性を設定または変更できます。ネットワーク トラフィックの分類とともに使用すると、ネットワーク トラフィックのマーク付けは、ネットワーク上で多くの QoS 機能をイネーブルにする基礎となります。ここでは、ネットワーク トラフィックのマーク付けのための概念的情報と設定作業を説明します。

- ネットワーク トラフィックのマーク付け (p.34-77)
- アクションドライバのマーク付け(p.34-80)
- トラフィック マーキング手順のフローチャート (p.34-80)
- ネットワーク トラフィックのマーク付けに関する制約事項 (p.34-81)
- マルチ属性マーキングのサポート (p.34-81)
- マーキング用のハードウェア機能 (p.34-82)
- ポリシーマップマーキングアクションの設定(p.34-82)
- マーキング統計(p.34-84)

ネットワーク トラフィックのマーク付け

ネットワーク トラフィックをマーク付けするには、次の概念を理解しておく必要があります。

- ネットワーク トラフィックのマーク付けの目的 (p.34-78)
- ネットワーク トラフィックのマーク付けの利点(p.34-78)
- トラフィック属性をマーク付けする 2 つの方法 (p.34-78)

ネットワーク トラフィックのマーク付けの目的

トラフィック マーキングは、特定のトラフィック タイプを識別して個別に処理し、ネットワークトラフィックを異なるカテゴリに分割するために使用されます。

トラフィック分類でネットワーク トラフィックをクラスに編成したあとには、トラフィック マーキングにより特定クラスに属するトラフィックに対して値(属性)をマーク付け(設定または変更)できます。たとえば、あるクラスで CoS 値を 2 から 1 に変更したり、別のクラスで DSCP 値を 3 から 2 に変更したりします。ここでは、これらの値は属性またはマーキング フィールドと呼ばれています。

設定および変更可能な属性は、次のとおりです。

- タグ付きイーサネット フレームの CoS 値
- IPv4の ToS バイトでの DSCP/Precedence 値
- OoS グループ ID
- IPv6 のトラフィック クラス バイトでの DSCP/Precedence 値

ネットワーク トラフィックのマーク付けの利点

トラフィック マーキングにより、ネットワーク上のトラフィックの属性を細かく調整できます。より細かく調整できるようになったことで、特別な処理が必要なトラフィックを分離し、それによって最適なアプリケーション パフォーマンスの実現に役立ちます。

トラフィック マーキングにより、ネットワーク トラフィックの属性がどのように設定されている のかに基づき、トラフィックを処理する方法を決定できます。これにより、ネットワーク トラフィックは、次のように属性に基づいて複数のプライオリティ レベルまたは CoS にセグメント化できます。

- トラフィック マーキングは、ネットワークに入っていくトラフィックの IP Precedence 値または IP DSCP 値の設定によく使用されます。ネットワーク内のネットワーク デバイスは、新たに マーク付けされた IP Precedence 値を使用して、トラフィックの処理方法を決定します。たとえば、音声トラフィックには特定の IP Precedence または DSCP でマーク付けし、そのマーキング のすべてのパケットをキューに入れるように完全優先を設定できます。この場合、マーキング は完全優先キューのトラフィックを識別するために使用されます。
- トラフィック マーキングは、クラスベースの QoS 機能(一部、制約事項があるものの、ポリシー マップ クラス設定モードで使用可能な機能)のトラフィックを識別するために使用できます。
- トラフィック マーキングは、スイッチ内の QoS グループにトラフィックを割り当てるために使用できます。スイッチは QoS グループを使用し、送信用にトラフィックのプライオリティを設定する方法を決定します。通常 QoS グループ値は、次の2つの理由のうちいずれかのために使用されます。
 - 広範囲のトラフィック クラスを利用するため。QoS グループ値には、DSCP に類似する、 64 の異なる個別マーキングがあります。
 - Precedence または DSCP 値の変更が望ましくない場合にこれらを変更するため

トラフィック属性をマーク付けする2つの方法



(注)

ここでは、*ポリサー ベース*のマーキングとは異なる*無条件*マーキングを説明します。無条件マーキングは、分類にのみ基づきます。

方法 1: 無条件明示的マーキング (set コマンドを使用)

ポリシー マップで設定された set コマンドを使用して、変更するトラフィック属性を指定します。次の表に、使用可能な set コマンドと対応する属性を示します。set コマンドの詳細については、『Catalyst 4500 Series Switch Command Reference』を参照してください。

表 34-8 set コマンドおよび適用可能なパケット タイプ

set コマンド	トラフィック属性	パケット タイプ
set cos	発信トラフィックのレイヤ 2 CoS 値	イーサネット IPv4、IPv6
set dscp	ToS バイトの DSCP 値	IPv4、IPv6
set precendence	パケット ヘッダーの Precedence 値	IPv4、IPv6
set qos-group	QoS グループ ID	イーサネット、IPv4、IPv6

個別の **set** コマンドを使用している場合、それらの set コマンドはポリシー マップで指定されます。 次に、表 34-8 に一覧になっている **set** コマンドの1つで設定されたポリシーマップの例を示します。

この設定例では、**set cos** コマンドがポリシー マップ (policy1) で設定され、CoS 属性をマーク付けしています。

```
enable
configure terminal
policy map p1
    class class1
    set cos 3
end
```

ポリシー マップの設定の詳細については、「ポリシー マップの作成 (p.34-38)を参照してください。

最後の作業として、インターフェイスにポリシー マップを付加します。インターフェイスへのポリシー マップの付加の詳細については、「インターフェイスへのポリシー マップの付加」(p.34-43)を 参照してください。

方法2:無条件テーブルマップペースマーキング

トラフィック属性のマーク付けに使用できるテーブル マップを作成できます。テーブル マップとは、1 つのトラフィック属性を別のトラフィック属性にリストしてマップする、一種の 2 方向変換チャートです。テーブル マップは、多数対 1 タイプの変換とマッピング スキームをサポートします。テーブル マップは、トラフィック属性の to-from 関係を確立し、属性に行われる変更を定義します。つまり属性は、別の値から取得された 1 つの値に設定されます。値は、変更される特定の属性に基づきます。たとえば、Precedence 属性は $0 \sim 7$ の数値に、一方 DSCP 属性は $0 \sim 63$ の数値にそれぞれ設定できます。

次に、テーブル マップ設定の例を示します。

```
table-map table-map1
map from 0 to 1
map from 2 to 3
exit
```

次の表に、テーブル マップを使用して to-from 関係を確立できるトラフィック属性の一覧を示します。

表 34-9 to-from 関係を確立できるトラフィック属性

「to」属性	「from」属性
Precedence	CoS、QoS グループ、DSCP、Precedence
DSCP	CoS、QoS グループ、DSCP、Precedence
CoS	DSCP、QoS グループ、CoS、Precedence

次に、前に作成したテーブル マップ (table-map1)を使用するように設定されたポリシー マップ (policy2)の例を示します。

Policy map policy
class class-default
set cos dscp table table-map

exit

この例では、テーブル マップで定義されたように、CoS 属性と DSCP 属性の間にマッピング関係が確立されています。

テーブル マップを使用するためのポリシー マップの設定の詳細については、「ポリシー マップの設定」(p.34-38) を参照してください。

最後の作業として、インターフェイスにポリシー マップを付加します。インターフェイスへのポリシー マップの付加の詳細については、「インターフェイスへのポリシー マップの付加」(p.34-43)を 参照してください。

アクション ドライバのマーク付け

マーキング アクションは、2 つの QoS 処理手順のうちの1 つに基づいてトリガーされます。

- 分類ベース:この場合、クラスに一致するすべてのトラフィックは、明示的方法またはテーブルマップベースの方法のいずれかを使用してマーク付けされます。この方法は、*無条件*マーキングと呼ばれます。
- ポリサー結果ベース:この場合、トラフィックのクラスは、パケットで使用可能なポリサー結果(conform/exceed/violate)に基づいて、別にマーキングされます。この方法は、*条件付き*マーキングと呼ばれます。

トラフィック マーキング手順のフローチャート

図 34-8 に、トラフィック マーキングの設定手順の順番を示します。

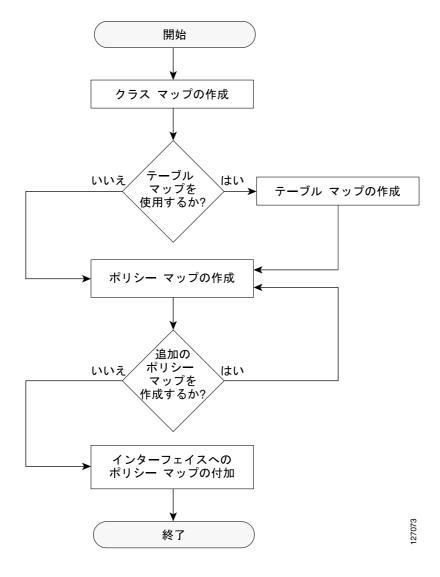


図 34-8 トラフィック マーキング手順のフローチャート

ネットワーク トラフィックのマーク付けに関する制約事項

パケットマーキングアクションには、次の制約事項が適用されます。

- QoS グループは、入力方向でのみマーク付けでき、無条件明示的マーキングのみをサポートします。
- 明示的マーキングは、ポリサーベース マーキングに対してのみサポートされます。

マルチ属性マーキングのサポート

Supervisor Engine 6-E は、トラフィックのクラスに一致するパケットの複数の QoS 属性をマーク付けできます。たとえば、DSCP、CoS、および QoS グループは、明示的マーキングまたはテーブルマップベース マーキングのいずれかを使用して、すべて一緒に設定できます。



(注)

複数フィールドまたはポリサーベース マルチフィールドの無条件明示的マーキングを使用するとき、ToS または CoS マーキング テーブルで設定可能なテーブルマップ数をマーク付けするマルチリージョン (conform/exceed/violate) は、サポートされる最大数より少なくなります。

マーキング用のハードウェア機能

Supervisor Engine 6-E は、パケットを送信、マークダウン、ドロップするポリサー アクションだけでなく、CoS および DSCP/Precedence フィールドでのマーキング アクションの種類を各エントリが指定する、128 エントリのマーキング アクション テーブルを提供します。このテーブルは、入力および出力の各方向でサポートされます。このテーブルは、無条件マーキングとポリサーベース マーキングの両方に使用されます。128 の一意のマーキング アクションまたは 32 の一意のポリサーベース アクション、またはこの 2 つの組み合わせをサポートするために使用可能です。

各マーキング フィールド (CoS および DSCP) のために、Supervisor Engine 6-E は、各方向に 512 エントリのマーキング テーブルを提供します。これらのテーブルは、スイッチ QoS モデルをサポートするスーパーバイザ エンジンで使用可能なマッピング テーブルに類似しています。ただし、ユーザが設定する複数の固有マッピング テーブルを保持する機能を持ちます。

たとえば、ToS マーキング テーブルは、DSCP/Precedence フィールド マーキングを提供し、次のいずれかとして使用できます。

- それぞれが 64 の DSCP または QoS グループ値を他の DSCP にマッピングする 8 つの異なる テーブルマップ
- それぞれが8つのCoS(16のCoSおよびCFi)値を入力(出力)方向のDSCPにマッピングする64(32)の異なるテーブルマップ
- 上記2種類のテーブルマップの組み合わせ

512 エントリの CoS マーキング テーブルでは、同様のマッピングが使用可能です。

ポリシー マップ マーキング アクションの設定

ここでは、ネットワーク トラフィックに無条件マーキング アクションを確立する方法を説明します。

前提条件

次の手順を実行します。

- クラス マップ (*ipp5*) およびポリシー マップを作成します (「QoS ポリシーの設定」[p.34-35] を参照)。
- マーキング アクションを設定します(「ポリシー マップ クラス アクションの設定」[p.34-39] を参照)。



(注)

Supervisor Engine 6-E では、マーキング アクション コマンド オプションが拡張されています (表 34-8 [p.34-79] および表 34-9 [p.34-80] を参照)。

テーブルマップベース無条件マーキングの設定

テーブルマップ ベースの無条件マーキングを設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始
		します。
ステップ 2	Switch(config)# table-map name	テーブルマップを設定します。
ステップ 3	Switch(config-tablemap)# map from from_value to to_value	from_value から to_value ヘマップを作成します。

	コマンド	目的
ステップ 4	Switch(config-tablemap)# exit	テーブルマップ コンフィギュレーション モードを
		終了します。
ステップ 5	Switch(config)# policy-map name	ポリシーマップ コンフィギュレーション モードを 開始します。
ステップ 6	Switch(config-p)# class name	QoS アクションのクラスを選択します。
ステップ 7	Switch(config-p-c)# set cos dscp prec cos dscp prec qos-group [table name]	暗黙の、または明示的テーブルマップに基づいて、 マーキング アクションを選択します。
ステップ 8	Switch(config-p-c)# end	コンフィギュレーション モードを終了します。
ステップ 9	Switch# show policy-map name	ポリシーマップの設定を確認します。
ステップ 10	Switch# show table-map name	テーブルマップの設定を確認します。

次に、テーブルマップを使用してマーキング アクションをイネーブルにする例を示します。

```
Switch(config)# table-map dscp2Cos
Switch(config-tablemap)# map from 8 to 1
Switch(config-tablemap)# exit
Switch(config)# policy-map p1
Switch(config-pmap)# class ipp5
Switch(config-pmap-c)# set cos dscp table dscp2Cos
Switch(config-pmap-c)# end
Switch# show policy-map p1

Policy Map p1
Class ipp5
set cos dscp table dscp2Qos

Switch# show table-map dscp2Cos
Table Map dscp2Cos
from 8 to 1
default copy
```

ポリサー結果ベースの条件付きマーキングの設定

ポリサー結果ベースの条件付きマーキングを設定するには、単一レートまたはデュアル レート ポリサーを設定します。「ポリシングの実装方法」(p.34-77) を参照してください。

次に、各ポリサー リージョンの明示的アクションで Two Rate Three Color ポリサーを設定する例を示します。

```
Switch# configure terminal
Switch(config-pmap-c)# policer cir percent 20 pir percent 30
Switch(config-pmap-c-policer)# conform-action set-cos-transmit 3 set-dscp-transmit 10
Switch(config-pmap-c-policer)# exceed-action set-cos-transmit 4 set-dscp-transmit 20
Switch(config-pmap-c-policer)# violate action drop
Switch# show policy-map p1

Policy Map police
Class ipp5
police cir percent 20 pir percent 30
conform-action set-cos-transmit 3
conform-action set-dscp-transmit af11
exceed-action set-cos-transmit 4
exceed-action set-dscp-transmit af22
violate-action drop
```

マーキング統計

マーキング統計では、マーク付けされたパケット数を示します。

無条件マーキングの場合、*分類エントリ*は、マーク付けされたパケットにあるフィールドを代わりに示すマーキング アクション テーブルのエントリを示します。したがって、分類統計はそれ自身で無条件マーキング統計を示します。

ポリサーを使用する条件付きマーキングでは、ポリサーがパケット レート ポリサーである場合、ポリサーは異なるポリシング結果のバイト統計のみを提供するため、マーク付けされたパケット数は判別できません。

シェーピング、共有(帯域幅)、プライオリティ キュー、キュー制限、および DBL

Supervisor Engine 6-E は、送信キューの選択にあたり、分類ベース(クラスベース)モードをサポートします。このモードでは、送信キューは、出力 QoS 分類検索に基づいて選択されます。



出力キューのみがサポートされます。

Supervisor Engine 6-E ハードウェアは、ポートごとに 8 つの送信キューをサポートします。パケットをポートから転送することが決定されると、出力 QoS 分類により、パケットが入れられる必要がある送信キューが決定されます。

デフォルトでは、ポートにサービス ポリシーが関連付けられていない Supervisor Engine 6-E には、 帯域幅または一種のプライオリティに関して保証のない 2 つのキュー(制御パケット キューおよび デフォルト キュー)があります。唯一の例外は、制御トラフィックに多少の最小リンク帯域幅が与えられるように、システム生成制御パケットが制御パケット キューに入れられることです。

出力ポリシーが、1 つまたは複数のトラフィックのクラスに対する 1 つまたは複数のキューイング 関連アクションでポートに付加されるとき、キューが割り当てられます。ポートごとに 8 つの キューしかないので、キューイング アクションを持つトラフィック クラスは最大でも 8 つ (予約 クラス、class-default を含む)となります。キュー アクションを持たないトラフィックのクラスは、キューイングなしクラスと呼ばれます。キューイングなしのクラス トラフィックは、最終的にクラス class-default に対応するキューを使用します。

キューイング ポリシー (キューイング アクションを持つポリシー)が付加されると、制御パケット キューが削除され、制御パケットは、分類ごとに関連キューに入れられます。

キューのダイナミックなサイズ変更(キュー制限クラスマップ アクション)は、queue-limit コマンドを使用することでサポートされています。シャーシとライン カードの種類に基づいて、ポート上の 8 つのキューすべては、同じキュー サイズで設定されます。

シェーピング

シェーピングにより、キューにあるアウト オブ プロファイル パケットを遅延させるて指定のプロファイルに適合させることができます。シェーピングは、ポリシングとは異なります。ポリシングは、設定したしきい値を超えたパケットをドロップしますが、シェーピングは、パケットをバッファし、トラフィックを指定のしきい値内に保ちます。シェーピングでは、トラフィックの処理がポリシングよりも*滑らかに*行われます。policy-map クラス コンフィギュレーション コマンドを使用して、トラフィック クラスの平均レート トラフィック シェーピングをイネーブルにします。

Supervisor Engine 6-E は、約 1.5% の精度で 32 kbps ~ 10 gbps の範囲のシェーピングをサポートします。

キューイング クラスが明示的シェーピング設定を使用せずに設定されているとき、キュー シェーピングはリンク レートに設定されます。

サービス ポリシーにクラスレベル シェーピングを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# policy-map policy-map-name	ポリシーマップ名を入力してポリシー マップを作成し、ポリシーマップ コンフィギュレーション モードを開始します。
		デフォルト設定では、ポリシー マップは定義されていません。
ステップ 3	Switch(config-pmap)# class class-name	トラフィック ポリシーを作成または変更するクラスの名前を指定し、ポリシーマップ クラス コンフィギュレーション モードを開始します。
		デフォルト設定では、トラフィック クラスは定義されていません。
ステップ 4	Switch(config-pmap-class)# shape average {cir-bps kbps percent percent}	平均レート トラフィック シェーピングをイネーブルにします。
		帯域幅は、kbps またはパーセンテージで指定できます。
		• <i>cir-bps</i> の場合、トラフィックがシェーピングされる ビット レートである、CIR を bps で指定します。有効 範囲は 32000 ~ 100000000000 bps です。
		 percent の場合、トラフィックのクラスをシェーピング するリンク レートのパーセンテージを指定します。有 効範囲は1~100です。
		デフォルト設定では、平均レート トラフィック シェーピン グはディセーブルになっています。
ステップ 5	Switch(config-pmap-class)# exit	ポリシーマップ コンフィギュレーション モードに戻りま す。
ステップ 6	Switch(config-pmap)# exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	Switch(config)# interface interface-id	物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	Switch(config-interface)# service-policy output policy-map-name	ポリシーマップ名を指定し、物理インターフェイスに適用 します。
ステップ 9	Switch(config-interface)# end	特権 EXEC モードに戻ります。
ステップ 10	Switch# show policy-map [policy-map-name [class class-map-name]]	入力を確認します。
	または	
	Switch# show policy-map interface interface-id	
ステップ 11	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

既存のポリシー マップを削除するには、no policy-map policy-map-name グローバル コンフィギュレーション モードを使用します。既存のクラスを削除するには、no class class-name policy-map コンフィギュレーション コマンドを使用します。平均レート トラフィック シェーピングをディセーブルにするには、no shape average policy-map クラス コンフィギュレーション コマンドを使用します。

次に、クラスレベル、平均レート シェーピングを設定する例を示します。ここでは、トラフィック クラス class1 をデータ伝送レート 256 kbps に制限します。

```
Switch# configure terminal
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# shape average 256000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# end
Switch#
Switch# show policy-map policy1
Policy Map policy1
Class class1
shape average 256000
```

次に、queuing-class トラフィックについて、クラスレベル、平均シェーピング パーセンテージを、リンク帯域幅の 32% に設定する例を示します。

```
Switch# configure terminal
Switch(config)# policy-map queuing-policy
Switch(config-pmap)# class queuing-class
Switch(config-pmap-c)# shape average percent 32
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# end
Switch #

Switch# show policy-map queuing-policy
Policy Map queuing-policy
Class queuing-class
Average Rate Traffic Shaping
cir 32%
```

共有(帯域幅)

トラフィックのクラスに割り当てられた帯域幅は、輻輳中にクラスに対して保証される最小帯域幅です。送信キュー シェーピングは、出力リンク帯域幅が指定ポートの複数キューで共有されるプロセスです。

Supervisor Engine 6-E は、約 1.5% の精度で $32~{\rm kbps}\sim 10~{\rm gbps}$ の範囲の共有をサポートします。すべてのキューイング クラスにわたる設定帯域幅の合計は、リンク帯域幅を超えないようにしてください。

サービス ポリシーにクラスレベル帯域幅アクションを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# policy-map policy-map-name	ポリシーマップ名を入力してポリシー マップを作成し、ポリシーマップ コンフィギュレーション モードを開始します。
		デフォルト設定では、ポリシー マップは定義されていません。
ステップ 3	Switch(config-pmap)# class class-name	トラフィック ポリシーを作成または変更するクラスの名前を指定し、ポリシーマップ クラス コンフィギュレーション モードを開始します。
		デフォルト設定では、トラフィック クラスは定義されていません。
ステップ 4	Switch(config-pmap-class)# bandwidth {bandwidth-kbps percent percent}	スイッチにトラフィックの輻輳があるとき、このポリシーマップに属するクラスに提供される最小帯域幅を指定します。スイッチが輻輳していない場合、クラスは bandwidth コマンドで指定した以上の帯域幅が与えられます。
		デフォルト設定では、帯域幅は指定されていません。
		帯域幅は、kbps またはパーセンテージで指定できます。
		・ bandwidth-kbps では、クラスに割り当てられる帯域幅をkbps で指定します。有効範囲は 32 ~ 10000000 です。
		<i>percent</i> では、クラスに割り当てられる使用可能帯域幅の パーセンテージを指定します。有効範囲は1~100です。
		すべてのクラス帯域幅を kbps またはパーセンテージ(混在は不可) で指定します。
ステップ 5	Switch(config-pmap-class)# exit	ポリシーマップ コンフィギュレーション モードに戻りま す。
ステップ 6	Switch(config-pmap)# exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	Switch(config)# interface interface-id	物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	Switch(config-interface)# service-policy output policy-map-name	ポリシーマップ名を指定し、物理インターフェイスに適用します。
ステップ 9	Switch(config-interface)# end	特権 EXEC モードに戻ります。
ステップ 10	Switch# show policy-map [policy-map-name [class class-map-name]]	入力を確認します。
	または	
	Switch# show policy-map interface interface-id	
ステップ 11	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

既存のポリシー マップを削除するには、no policy-map policy-map-name グローバル コンフィギュレーション モードを使用します。既存のクラスを削除するには、no class class-name policy-map コンフィギュレーション コマンドを使用します。デフォルトの帯域幅に戻すには、no bandwidth policy-map クラス コンフィギュレーション コマンドを使用します。

次に、*prec1*、*prec2*、および *prec3* という 3 つのクラスに対して、*policy11* という名前のクラスレベル ポリシー マップを作成する例を示します。これらのクラスのポリシーでは、最初のクラスのキューに 30%、2 番めのクラスのキューに 20%、3 番めのクラスのキューに 10% の使用可能帯域幅が、それぞれ割り当てられます。

```
Switch # configure terminal
Switch(config) # policy-map policy11
Switch(config-pmap) # class prec1
Switch(config-pmap-c)# bandwidth percent 30
Switch(config-pmap-c)# exit
Switch(config-pmap) # class prec2
Switch(config-pmap-c) # bandwidth percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap) # class prec3
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# exit
Switch(config-pmap) # exit
Switch(config) # interface gigabitethernet1/1
Switch(config-if) # service-policy output policy11
Switch(config-if)# end
Switch #
Switch# show policy-map policy11
 Policy Map policy11
    Class prec1
     bandwidth percent 30
    Class prec2
     bandwidth percent 20
    Class prec3
     bandwidth percent 10
```

次に、prec1、prec2、および prec3 という 3 つのクラスに対して、policy11 という名前のクラスレベル ポリシー マップを作成する例を示します。これらのクラスのポリシーでは、最初のクラスのキューに 300 mbps、2 番めのクラスのキューに 200 mbps、3 番めのクラスのキューに 100 mbps の使用可能帯域幅が、それぞれ割り当てられます。

```
Switch # configure terminal
Switch(config) # policy-map policy11
Switch(config-pmap) # class prec1
Switch(config-pmap-c)# bandwidth 300000
Switch(config-pmap-c)# exit
Switch(config-pmap) # class prec2
Switch(config-pmap-c)# bandwidth 200000
Switch(config-pmap-c)# exit
Switch(config-pmap) # class prec3
Switch(config-pmap-c)# bandwidth 100000
Switch(config-pmap-c)# exit
Switch(config-pmap) # exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if) # service-policy output policy11
Switch(config-if)# end
Switch #
Switch# show policy-map policy11
 Policy Map policy11
   Class prec1
     bandwidth 300000 (kbps)
    Class prec2
      bandwidth 200000 (kbps)
    Class prec3
      bandwidth 100000 (kbps)
```

キューで最小帯域幅が保証されない場合、明示的な帯域幅設定にキューが設定されると、ポート上の未割当帯域幅の一部を受け取るとプログラミングされます。以下の例を参照してください。

新しいキューに対して帯域幅が残っていない場合、または明示的共有/帯域幅設定を持たないすべ てのキューの最小設定可能レート (32 kbps) を満たすのに未割り当て帯域幅が十分でない場合、ポ リシーの関連付けは拒否されます。

たとえば、次のような2つのキューがあるとします。

```
policy-map queue-policy
   class q1
    bandwidth percent 10
  class q2
     bandwidth percent 20
```

そのキューの帯域幅割り当ては次のようになります。

```
q1 = 10%
           q2 = 20%
class-default = 70%
```

同様に、もう1つのキューイングクラス(q3とします)が明示的帯域幅なしで(たとえば、shape コマンドだけで)追加されると、帯域幅割り当ては次のようになります。

```
\alpha 1 = 10\%
            q2 = 20%
           q3 = min(35\%, q3-shape-rate)
class-default = max(35\%, (100 - (q1 + q2 + q3)))
```

プライオリティ キューイング

Supervisor Engine 6-E では、ポート上の伝送キューを 1 つだけ、 完全優先 低遅延キューまたは LLQ) として設定できます。

LLQ では、トラフィック クラスに対して完全優先キューイングが提供されます。これにより、他 のキューのパケットの*前に*、音声など遅延の影響を受けやすいデータを送信できます。プライオリ ティ キューは、空になるまでまたはシェーピング レートを下回るまで、最初に処理されます。ク ラスレベル ポリシーごとのプライオリティ キューの宛先にできるのは、1 つのトラフィック スト リームだけです。トラフィック クラスのプライオリティ キューをイネーブルにするには、クラス モードで priority policy-map class コンフィギュレーション コマンドを使用します。

LLQ は、レート制限されていないかぎり、他のキューを停止させることがあります。Supervisor Engine 6-E は、キューが*輻輳*すると(キュー長に基づく) 2 パラメータ ポリサー(レート、バース ト)が有効になる*条件付きポリシング*をサポートしません。ただし、完全優先 キューに入れられた パケットのレート制限のための無条件ポリサーの適用はサポートします。

サービス ポリシーにクラスレベル プライオリティ キューイングを設定するには、次の手順を実行 します。

ステップ 1 ステップ 2

コマンド	目的
Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
Switch(config)# policy-map policy-map-name	ポリシーマップ名を入力してポリシー マップを作成し、ポリシーマップ コンフィギュレーション モードを開始します。
	デフォルト設定では、ポリシー マップは定義されていません。

	コマンド	目的
ステップ 3	Switch(config-pmap)# class class-name	トラフィック ポリシーを作成または変更するクラスの名前を指定し、ポリシーマップ クラス コンフィギュレーション モードを開始します。
		デフォルト設定では、トラフィック クラスは定義されてい ません。
ステップ 4	Switch(config-pmap-class)# priority	完全優先 キューをイネーブルにし、トラフィックのクラス のプライオリティを設定します。
		デフォルト設定では、完全優先 キューイングはディセーブ ルになっています。
ステップ 5	Switch(config-pmap-class)# exit	ポリシーマップ コンフィギュレーション モードに戻りま す。
ステップ 6	Switch(config-pmap)# exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	Switch(config)# interface interface-id	物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	Switch(config-interface)# service-policy output policy-map-name	ポリシーマップ名を指定し、物理インターフェイスに適用 します。
ステップ 9	Switch(config-interface)# end	特権 EXEC モードに戻ります。
ステップ 10	Switch# show policy-map [policy-map-name [class class-map-name]]	入力を確認します。
	または	
	Switch# show policy-map interface interface-id	
ステップ 11	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

既存のポリシー マップを削除するには、no policy-map policy-map-name グローバル コンフィギュレーション モードを使用します。既存のクラスを削除するには、no class class-name policy-map コンフィギュレーション コマンドを使用します。プライオリティ キューをディセーブルにするには、no priority policy-map class コンフィギュレーション コマンドを使用します。

次に、*policyI* というクラスレベル ポリシーを設定する例を示します。class 1 は、プライオリティキューとして設定され、空になるまで最初に処理されます。

```
Switch# configure terminal
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# end
Switch #
Switch# show policy-map policy1
Policy Map policy1
Class class1
priority
```

キュー制限

クラスベース キューが物理ポートでインスタンス化される際に、デフォルト サイズで設定されます。このサイズは、このトラフィック クラスに属するパケットがキューイング可能なキュー エントリの数を表します。スケジューラは、キュー シェーピング、帯域幅、およびプライオリティ設定に基づいて、すでに送信可能なキューからパケットを移動します。

キュー制限は、指定時間内のキュー内にあるパケットの最大数を指定します。キューが一杯になった場合に、後続のパケットをキューイングしようとするとテール ドロップになります。ただし、DBL がキューでイネーブルである場合は、キューが一杯になっていなくても DBL アルゴリズムに基づいてパケットが確率的に廃棄されます。

帯域幅、シェーピング、またはプライオリティなどのキュースケジューリングがすでに設定されている場合のみ、queue-limit コマンドをクラスの下に設定できます。この要件の例外は、クラスデフォルトクラス上でスタンドアロン queue-limit コマンドをサポートしている場合です。

キュー メモリ

割当可能なキュー エントリ数は 8 の倍数でなければならず、 $16 \sim 8184$ の範囲です。クラスベースキューが物理ポートでインスタンス化される際に、エントリのデフォルト数が指定されます。このデフォルト キュー サイズは、シャーシ内のスロット数と、各スロットの前面パネル ポート数に基づいています。

Supervisor Engine 6-E には、512K (524,288) キュー エントリがあり、そのうち 100K (102,400) キュー エントリが空いているリザーブ プール内に保留されています。残りの 412K (421,88) のうち、ドロップ ポートに 8184 エントリが提供され、CPU ポートに 11704 エントリが割り当てられます。残りのエントリは、シャーシ内のスロットへ均等に分けられます。冗長シャーシ内では、このエントリ分配のために 2 つのスーパーバイザ スロットが 1 つとして扱われます。各スロット内では、そのスロットにあるライン カード上に存在する前面パネルのポート間でキュー エントリの数が均等に分割されます。

インターフェイス上にあるキュー エントリのユーザ設定が専用割当分を越えた場合、システムが空いているリザーブ プールを活用して設定に対応しようとします。 空いているリザーブ プールからのエントリは、先着順でインターフェイスに割り当てられます。

サーバ ポリシーの関連付け

キューイング アクションのある QoS サービス ポリシーが設定されているものの、明示的に queue-limit コマンドが物理インターフェイスの出方向に添付されていない場合、クラスベースの各 キューはその物理ポートの専用割当分から同数のキュー エントリを取得します。queue-limit コマンドを使用してキューに明示的にサイズが指定されている場合、スイッチはインターフェイスの専用割当から全エントリを割り当てようとします。必要なエントリ数がインターフェイスの専用割当分を越える場合、スイッチは空いているリザーブからエントリを割り当てようとします。

キューに関連付けられたキュー エントリは常に連続している必要があります。この要件により、スイッチ間で共有されている 512K のキューエントリにフラグメンテーションが発生する可能性があります。たとえば、あるインターフェイスで専用割当分のキュー エントリが十分ない場合、そのキューを設定するために空いているリザーブ分を使用することになります。この場合、他のポートやスロットと共有できないため、専用割当分のキューエントリは未使用のままになります。

インターフェイスに関連付けられている QoS サービスポリシーが削除された場合、空いているリザープ分から取得したキュー エントリは空いているリザーブ プールに戻されます。インターフェイス キューイング コンフィギュレーションは、2 つのキュー (デフォルトのシェーピング、帯域幅、サイズを有するクラスデフォルトおよび制御パケット キュー)に戻ります。制御パケットキューはサイズ 16 で設定されていて、デフォルト キューはインターフェイスの専用割当分に基づいて可能な最大サイズに設定されています。

キュー割当障害

キュー メモリのフラグメンテーションや十分な空いているリザーブ エントリがないために、スイッチがインターフェイス上の 1 つまたは複数のキューで必要な明示的キュー サイズを満たすことができない場合があります。このシナリオでは、スイッチはエラー メッセージをログして、ユーザに障害を通知します。QoS サービス ポリシーはインターフェイス上に設定されたままになります。QoS サービスポリシーを削除し、スイッチ上の他のポートで、空いているリザーブ分からキューエントリの現在の利用率を調査することで、エラーを修復することができます。

サービス ポリシーにクラスレベル queue-limit を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# policy-map policy-map-name	ポリシーマップ名を入力してポリシー マップを作成し、ポリシーマップ コンフィギュレーション モードを開始します。
		デフォルト設定では、ポリシー マップは定義されていません。
ステップ 3	Switch(config-pmap)# class class-name	トラフィック ポリシーを作成または変更するクラスの名前を指定し、ポリシーマップ クラス コンフィギュレーション モードを開始します。
		デフォルト設定では、トラフィック クラスは定義されていません。
ステップ 4	<pre>Switch(config-pmap-class)# shape average {cir-bps kbps percent percent}</pre>	平均レート トラフィック シェーピングをイネーブルにします。
		帯域幅は、kbps またはパーセンテージで指定できます。
		• <i>cir-bps</i> の場合、トラフィックがシェーピングされる ビット レートである、CIR を bps で指定します。有効 範囲は 32000 ~ 100000000000 bps です。
		 percent の場合、トラフィックのクラスをシェーピング するリンク レートのパーセンテージを指定します。有 効範囲は1~100です。
		デフォルト設定では、平均レート トラフィック シェーピン グはディセーブルになっています。
ステップ 5	Switch(config-pmap-class)# queue-limit number-of-packets	パケット内の明示的なキュー サイズを提示します。サイズ は8の倍数で、16~8184の範囲にする必要があります。
ステップ 6	Switch(config-pmap-class)# exit	ポリシーマップ コンフィギュレーション モードに戻りま す。
ステップ 7	Switch(config-pmap)# exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	Switch(config)# interface interface-id	物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	Switch(config-interface)# service-policy output policy-map-name	ポリシーマップ名を指定し、物理インターフェイスに適用 します。
ステップ 10	Switch(config-interface)# end	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 11	Switch# show policy-map [policy-map-name [class class-map-name]]	入力を確認します。
	または	
	Switch# show policy-map interface interface-id	
ステップ 12	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

明示的キュー サイズを削除するには、ポリシーマップ内のクラスで no queue-limit コマンドを使用します。

次に、明示的な queue-limit コマンドを使用してクラスベースのキューを設定する例を示します。ここでは、トラフィック クラス class1 をキュー サイズ 4048 に制限します。

```
Switch# configure terminal
Switch(config) # policy-map policy1
Switch(config-pmap) # class class1
Switch(config-pmap-c)# shape average 256000
Switch(config-pmap-c)# queue-limit 4048Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# end
Switch#
Switch# show policy-map policy1
 Policy Map policy1
   Class class1
      shape average 256000
      queue-limit 4048
Switch#
```

DBL を経由した AQM

AQM は、パケットをポートの伝送キューに入れる前の、トラフィック フローのバッファ制御を提供します。この機能は、共有メモリ スイッチで非常に役立ち、特定のフローによるスイッチ パケット メモリの占有が行われないようにします。



Supervisor Engine 6-E は、DBL 経由のアクティブ スイッチ バッファ管理をサポートします。

トラフィックのデフォルト クラス (クラス class-default) を除き、他のキューイング アクションが 少なくとも 1 つ設定されている場合にのみ DBL アクションを設定できます。

サービス ポリシーのシェーピングとともにクラスレベル DBL アクションを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# policy-map policy-map-name	ポリシーマップ名を入力してポリシー マップを作成し、ポリシーマップ コンフィギュレーション モードを開始します。
		デフォルト設定では、ポリシー マップは定義されていません。
ステップ 3	Switch(config-pmap)# class class-name	トラフィック ポリシーを作成または変更するクラスの名前を指定し、ポリシーマップ クラス コンフィギュレーション モードを開始します。
		デフォルト設定では、トラフィック クラスは定義されていません。
ステップ 4	Switch(config-pmap-class)# shape average cir-bps	平均レート トラフィック シェーピングをイネーブルにします。
		トラフィックがシェーピングされるビット レートである、 CIR を bps で指定します。有効範囲は 32000 ~ 10000000000 bps です。
		デフォルト設定では、平均レート トラフィック シェーピン グはディセーブルになっています。
ステップ 5	Switch(config-pmap-class)# db1	トラフィックのこのクラスに関連付けられたキューで DBL をイネーブルにします。
ステップ 6	Switch(config-pmap-class)# exit	ポリシーマップ コンフィギュレーション モードに戻りま す。
ステップ 7	Switch(config-pmap)# exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	Switch(config)# interface interface-id	物理ポートを指定し、インターフェイス コンフィギュレー ション モードを開始します。
ステップ 9	Switch(config-interface)# service-policy output policy-map-name	ポリシーマップ名を指定し、物理インターフェイスに適用 します。
ステップ 10	Switch(config-interface)# end	特権 EXEC モードに戻ります。
ステップ 11	Switch# show policy-map [policy-map-name [class class-map-name]]	入力を確認します。
	または	
	Switch# show policy-map interface interface-id	
ステップ 12	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

既存のポリシー マップを削除するには、no policy-map policy-map-name グローバル コンフィギュレーション モードを使用します。既存のクラスを削除するには、no class class-name policy-map コンフィギュレーション コマンドを使用します。関連付けられたキューで DBL をディセーブルにするには、no dbl policy-map class コンフィギュレーション コマンドを使用します。

次に、クラスレベルの DBL アクションを平均レート シェーピングとともに設定する例を示します。 トラフィッククラス *class1* に関連付けられたキューで DBL をイネーブルにします。

```
Switch# configure terminal
Switch(config) # policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# shape average 256000
Switch(config-pmap-c)# db1
Switch(config-pmap-c)# exit
Switch(config-pmap) # exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# end
Switch#
Switch# show policy-map policy1
 Policy Map policy1
   Class class1
       shape average 256000
    dbl
```

伝送キューの統計

伝送キューの統計情報を表示するには、show policy-map interface コマンドを使用します。

階層型ポリシー

論理 QoS セマンティクスをサポートするには、階層型ポリシーのサポートが必要です。次に、階層型ポリシーを設定して異なる動作を実現するためのさまざまな方法の例を示します。

例 1

次の例では、特定のキューに送信されたトラフィックのポリシングまたはマーキングされたサブネットと、デフォルト キューにポリシングまたはマーキングされた残りのトラフィックがあるとします。

```
Policy-map queue-policy
  class queue-class
     shape <...>
     bandwidth <...>
{\tt service-policy\ police-and-mark-traffic-class-1}
   class queue2-class
    set <...>
     police <...>
service-policy police-and-mark-traffic-class-2
   class class-default
     set <...>
     police <...>
policy-map police-and-mark-traffic-class-1
  class traffic-class-1
     set <...>
     police <...>
```

例 2

次の例では、すべてのトラフィックが集約でポリシングまたはマーキングされ、同じキュー分類ポリシーを使用するとします。MQC セマンティックスのように、クラスがキューイング アクションを使用しない場合、class-default は、そのトラフィックのクラスのキューとして動作します。

```
Policy-map queue-policy
  class queue1-class
    shape <...>
    bandwidth <...>
   class queue8-class
     shape <...>
     bandwidth < ...>
class queue8-class
    shape <...>
    bandwidth <...>
policy-map port-level-policy
class traffic-class-1
    set <...>
    police <...>
class traffic-class-n
    set <...>
    police <...>
class class-default
service-policy police-and-mark-traffic-class-2
```

例1とは対照的に、例2はキュー設定の標準的な方法です。

例 3

次に、指定ポートをサブレートにシェーピングして、キューイングまたはポリシング ポリシーを適用する例を示します。



<u>一</u>(注)

ポートシェーピングは、Supervisor Engine 6-E ではサポートされていません。

この設定モデルには、次の手順が含まれます。

- **ステップ 1** ポリシングまたはマーキング ポリシー アクションの設定(最下位の子ポリシー)
- **ステップ2** ステップ 1 で設定した各キューでのキューイング アクションおよびポリシングまたはマーキング パケットの設定(中位子ポリシー)
- ステップ3 ポート レベル シェーピングの設定 (親ポリシー)

ポリシー設定は、次のようになります。

```
Policy-map port-level-policy
   class class-default
    shape percent 100
service-policy queuing-policy
Policy-map queuing-policy
   class queue1-class
    shape <...>
    bandwidth <...>
service-policy police-and-mark-traffic-class-1
class class-default
    shape <...>
     bandwidth <...>
service-policy police-and-mark-traffic-class-default
Policy-map police-and-mark-traffic-class-1
  class traffic-class-1
    shape <...>
    police <...>
```

ポリシーの関連付け

Supervisor Engine 6-E は、ポート単位 /VLAN 単位ポリシーをサポートします。関連付けられたポリシーは、インターフェイス、VLAN、および指定ポートの特定 VLAN にそれぞれ付加されます。

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/ps6350/products_configuration_guide_book09186a0080435d50.html

QoS アクションの制約事項

- 異なるターゲット上で指定した方向に同じアクションを複数回実行することはできません。入力方向で、ポートと VLAN の両方にパケットをポリシングすることはできません。ただし、入力ポートと出力 VLAN 上ではポリシングできます。
- キューイング アクションは、物理ポートの出力方向でのみ許可されます。

QoS ポリシーのプライオリティ

- ポートおよび VLAN 上のポリシーが、競合アクション (ポートと VLAN の両方でのポリシン グまたはマーキング アクションなど)で設定されている場合、ポート ポリシーが取得されます。
- 指定ポートの VLAN 上でのポリシーが上書きされる必要がある場合、ユーザは PV ポリシーを 設定できます。

QoS ポリシーの統合

適用可能ポリシーは、指定方向の指定パケットに適用されます。たとえば、出力 VLAN ベース ポリシングおよびマーキングを設定し、さらにそのポートでの選択的キューイングを設定すると、このパケットに対し、両方のポリシーからのアクションが適用されます。

ソフトウェア QoS

最高レベルには、ローカルで送信された、スイッチからの 2 種類のトラフィック (制御プロトコルパケット、ping、および Telnet) があります。この 2 種類とは、高プライオリティ トラフィック (通常は、OSPF Hello や STP などの制御プロトコルパケット) と低プライオリティ パケット (他のすべてのパケット タイプ) です。

ローカルで送信されたパケットの QoS 処理には、次の2つの方法があります。

Supervisor Engine 6-E には、ソフトウェア パスで処理されたパケットに QoS を適用する方法が用意されています。ソフトウェアでのこの QoS 処理を受けるパケットは、ソフトウェア スイッチド パケットとソフトウェア生成パケットの 2 つの種類に分類できます。

受信時には、ソフトウェア スイッチド パケットは、パケットを代わりに別のインターフェイスから送信する CPU に送信されます。そういったパケットの場合、入力ソフトウェア QoS は入力マーキングを提供し、出力ソフトウェア QoS は出力マーキングとキュー選択を提供します。

ソフトウェア生成パケットは、スイッチによりローカルで送信されたパケットです。これらのパケットに適用された出力ソフトウェア QoS 処理のタイプは、ソフトウェア スイッチド パケットに適用されたタイプと同じです。これら 2 つの処理タイプの唯一の違いは、ソフトウェア スイッチドパケットが、出力分類を目的として、パケットの入力マーキングを考慮する点です。

高プライオリティ パケット

高プライオリティパケットは、次のいずれかとしてマーク付けされます。

- PAK PRIORITY を使用して内部的に
- IP Precedence 6 を使用して (IP パケット用)
- CoS 6 を使用して (VLAN タグ付きパケット用)

これらのパケットは、次のように動作します。

- これらのパケットは、出力サービス ポリシーのように設定されたポリシング、AQM、ドロップしきい値(またはパケットをドロップすることができる機能)が原因でドロップされることはありません。ただし、ハードウェア リソースの制約(パケット バッファ、キューが満杯など)が原因でドロップされることはあります。
- これらのパケットは、ポートまたは VLAN である出力サービス ポリシーのマーキング設定に 従って、分類およびマーク付けされます (「ポリシーの関連付け」 [p.34-97] を参照)。
- これらの高プライオリティ パケットは、次の基準に従って出力ポートのキューに入れられます。
 - ポートに出力キューイング ポリシーがない場合、パケットは、デフォルト キューとは別に 設定され、5% のリンク帯域幅が予約されている制御パケット キューに入れられます。
 - ポートに出力キューイング ポリシーがある場合、そのパケットに適用可能な分類基準に基づいてキューが選択されます。

低プライオリティ パケット

高プライオリティ(前述)と見なされないパケットは、*重要ではない*と見なされます。これらのパケットには、ローカルで送信された ping、Telnet、およびその他のプロトコル パケットが含まれます。これらのパケットは、指定の伝送ポートを通過する他のパケットと同様に(出力分類、マーキングおよびキューイングを含む)、処理されます。



CHAPTER

35

音声インターフェイスの設定

この章では、Catalyst 4500 シリーズ スイッチの音声インターフェイスを設定する方法について説明します。

この章の主な内容は、次のとおりです。

- 音声インターフェイスの概要 (p.35-2)
- Cisco 7960 IP Phone への接続用のポートの設定 (p.35-4)
- 音声およびデータ トラフィック用の音声ポートの設定 (p.35-5)
- 着信フレームの CoS プライオリティの変更 (p.35-7)
- 電力の設定 (p.35-7)



この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/cr/index.htm

音声インターフェイスの概要

Catalyst 4500 シリーズ スイッチは、Cisco 7960 IP phone に接続して、IP 音声トラフィックを伝送します。必要に応じて、Cisco 7960 IP phone に接続する回路に電力を供給します。

データ伝送が均質性に欠ける場合、IP Phone の音質が低下することがあります。そのため、このスイッチでは、IEEE (米国電気電子学会) 802.1p Class of Service (CoS; サービス クラス) に基づく QoS (Quality Of Service) をサポートしています。 QoS は、分類およびスケジューリングを使用して、スイッチからのネットワーク トラフィックを予測可能な方法で伝送します。 QoS の詳細については、第 34 章「QoS の設定」を参照してください。

Cisco 7960 IP phone は、802.1p プライオリティに基づいてトラフィックを伝送するように設定できます。CLI (コマンドライン インターフェイス) を使用して、Cisco 7960 IP phone によって割り当てられたトラフィック プライオリティを信頼または無視するように Catalyst 4000 ファミリを設定できます。

Cisco 7960 IP phone には、統合 3 ポート 10/100 スイッチが装備されています。これらのポートは、次の装置への接続専用です。

- ポート 1 は、Catalyst 4500 シリーズ スイッチまたは他の Voice over IP(VoIP)装置に接続します。
- ポート2は内部 10/100 インターフェイスで、IP Phone のトラフィックを伝送します。
- ポート 3 は、PC または他の装置に接続します。

図 35-1 に、Cisco 7960 IP phone の接続方法を示します。

図 35-1 Catalyst 4500 シリーズ スイッチに接続された Cisco 7960 IP Phone



Cisco IP Phone の音声トラフィック

接続された Cisco IP Phone でアクセス ポートを設定し、一方の VLAN を音声トラフィック用に、もう一方の VLAN を電話に接続された装置からのデータ トラフィック用にすることができます。スイッチのアクセス ポートを、Cisco Discovery Protocol (CDP; シスコ検出プロトコル) パケットを送信するように設定できます。接続された電話はこの CDP パケットによる指示に従って、次のいずれかの方法で音声トラフィックをスイッチに送信します。

- レイヤ 2 CoS プライオリティ値のタグ付き音声 VLAN
- レイヤ 2 CoS プライオリティ値のタグ付きアクセス VLAN
- タグなしアクセス VLAN (レイヤ 2 CoS プライオリティ値なし)



どの設定でも、音声トラフィックはレイヤ 3 IP precedence 値を伝送します (音声トラフィックのデフォルトは 5、音声制御トラフィックのデフォルトは 3)。

Cisco IP Phone のデータ トラフィック

スイッチでは、Cisco IP Phone のアクセス ポートに接続された装置からのタグ付きデータ トラフィック (IEEE 802.1Q または IEEE 802.1p フレーム タイプのトラフィック) も処理できます (図 35-1 を参照)。 スイッチのレイヤ 2 アクセス ポートで CDP パケットを送信するように設定します。接続された電話はこの CDP パケットによる指示に従って、電話でのアクセス ポートを次のいずれかのモードに設定します。

- trusted モードの場合、Cisco IP Phone のアクセス ポートで受信したすべてのトラフィックはそのまま電話を通過し、変更されません。
- untrusted モードの場合、Cisco IP Phone のアクセス ポートで受信した IEEE 802.1Q または IEEE 802.1p フレームのすべてのトラフィックは、設定されたレイヤ 2 CoS 値を受信します。デフォルトのレイヤ 2 CoS 値は 0 です。デフォルトは untrusted モードです。



(注)

Cisco IP Phone に接続された装置からのタグなしトラフィックは、電話のアクセス ポートの信頼状態に関わらず、そのまま電話を通過し、変更されません。

Cisco 7960 IP Phone への接続用のポートの設定

Cisco 7960 IP phone は、PC または他の装置との接続にも対応しているので、Catalyst 4500 シリーズスイッチを Cisco 7960 IP phone に接続するインターフェイスは、音声およびデータ トラフィックを一緒に伝送します。

Cisco 7960 IP phone に接続されるポートを設定する方法には、次の3通りがあります。

- ポートのデフォルトの CoS プライオリティに基づいてすべてのトラフィックを送信します。これがデフォルト設定です。
- 音声トラフィックには電話によって高いプライオリティが与えられ (CoS プライオリティは常に 5)、すべてのトラフィックが同じ VLAN (仮想 LAN)内にあります。
- 音声およびデータ トラフィックは個別の VLAN で伝送されます。

音声トラフィックに高いプライオリティを与え、すべてのトラフィックを 802.1Q ネイティブ VLAN を介して伝送するように電話に指示するポートを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# interface {fastethernet gigabitethernet} slot/port	設定するインターフェイスを指定します。
ステップ 3	Switch(config-if)# switchport voice vlan dot1p	音声トラフィックに 802.1p プライオリティ タギ ングを使用し、VLAN 1 (デフォルトのネイティ ブ VLAN)を使用してすべてのトラフィックを伝 送するようにスイッチを設定します。
ステップ 4	Switch(config-if)# end	特権 EXEC モードに戻ります。
ステップ 5	Switch# show interface {fastethernet gigabitethernet} slot/port switchport	ポートの設定を確認します。

音声およびデータ トラフィック用の音声ポートの設定

音声およびデータ トラフィックは同じ音声ポートを通じて移動するので、トラフィック タイプご とに個別に VLAN を指定する必要があります。異なる VLAN で音声およびデータ トラフィックを 伝送するようにスイッチ ポートを設定できます。



(注)

音声 VLAN にスティッキ ポート セキュリティを設定する場合は、音声ポート上のポート セキュリティの設定 (p.38-25) を参照してください。



(注)

音声 VLAN で 802.1X を使用する場合は、「音声 VLAN ポートを使用した 802.1X 認証の利用」 (p.37-19) を参照してください。

Cisco IP Phone からの音声トラフィックおよびデータ トラフィックを異なる VLAN で受信するようにポートを設定するには、次の作業を行います。

	コマンド	目的
	Switch# configure terminal	コンフィギュレーション モードを開始します。
2	Switch(config)# interface {fastethernet gigabitethernet} slot/port	設定するインターフェイスを指定します。
	Switch(config-if)# switchport mode access	インターフェイスをアクセス ポートとして設定し ます。
		音声 VLAN は、アクセス ポート上でのみアクティブ になります。
	Switch(config-if)# switchport voice vlan vlan_num	すべての音声トラフィックを指定された VLAN を通じて伝送するように Cisco IP Phone を設定します。 Cisco IP Phone は、802.1p プライオリティ 5 でトラフィックを伝送します。
	Switch(config-if)# switchport access vlan data_vlan_num	ポート上でアクセス VLAN(データ VLAN)を設定 します。
	Switch(config-if)# end	特権 EXEC モードに戻ります。
	Switch# show interface {fastethernet gigabitethernet} slot/port switchport	設定を確認します。

Switch# configure terminal

次に、 $VLAN\ 1$ がデータトラフィックを伝送し、 $VLAN\ 2$ が音声トラフィックを伝送する例を示します。この設定では、すべての Cisco IP Phone および他の音声関連装置を $VLAN\ 2$ に属するスイッチ ポートに接続する必要があります。

```
Enter configuration commands, one per line. End with {\tt CNTL/Z.}
Switch(config)# interface fastEthernet 3/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 2
Switch(config-if)# switchport access vlan 3
Switch(config-if)# end
Switch# show interfaces fastEthernet 3/1 switchport
Name: Fa3/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 3 (VLAN0003)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 2 (VLAN0002)
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
Switch#
```

着信フレームの CoS プライオリティの変更

PC またはその他のデータ装置を Cisco 7960 IP phone ポートに接続できます。PC は、CoS 値が割り当てられたパケットを生成します。また、必要に応じて、スイッチの CLI を使用し、接続先装置から IP Phone ポートに着信したフレームのプライオリティを上書きできます。ポートに着信したフレームのプライオリティを受け入れる(信頼する)ように IP Phone ポートを設定することもできます。

Cisco 7960 IP phone の非音声ポートから受信した CoS プライオリティ設定を上書きするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# interface {fastethernet gigabitethernet} slot/port	設定するインターフェイスを指定します。
ステップ 3	Switch(config-if)# [no] qos trust extend cos 3	PC または接続先装置から受信したプライオリティを上書きして、受信データをプライオリティ3 で転送するように IP Phone ポートを設定します。
		ポートをデフォルト設定に戻すには、noキーワードを使用します。
ステップ 4	Switch(config-if)# end	特権 EXEC モードに戻ります。
ステップ 5	Switch# show interface {fastethernet gigabitethernet} slot/port switchport	変更を確認します。

電力の設定

Catalyst 4500 シリーズ スイッチは、Cisco 7960 IP phone に接続しているかどうかを検知できます。 回路に電力がない場合は、Catalyst 4500 シリーズ スイッチが Cisco 7960 IP phone に Power over Ethernet (PoE) を供給します。Cisco 7960 IP phone が AC 電源に接続して、音声回路に独自の電力 を供給することもできます。回路上に電力がある場合は、スイッチは電力を供給しません。

Cisco 7960 IP phone に電力を供給しないようにスイッチを設定し、検知メカニズムをディセーブルにできます。 Cisco 7960 IP phone への PoE の供給に使用する CLI コマンドについては、第 11 章 「PoE の設定」を参照してください。

■電力の設定



CHAPTER

36

PVLAN の設定



(注)

Supervisor Engine 6-E は、コミュニティ PVLAN、独立 PVLAN トランク、および混合モード トランク ポートをサポートしません。

この章では、Catalyst 4500 シリーズ スイッチ上の Private VLAN (PVLAN; プライベート VLAN) について説明します。また、注意事項、手順、設定例についても示します。

この章の主な内容は、次のとおりです。

- コマンド リスト (p.36-2)
- PVLAN の概要 (p.36-3)
- PVLAN の設定 (p.36-10)



(注)

この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univered/cc/td/doc/product/software/ios122sr/cr/index.htm

コマンド リスト

この表には、主に PVLAN で共通に使用されるコマンドを示します。

目的	参照先
VLAN を PVLAN として設定します。	PVLAN としての VLAN の設定
	(p.36-13)
	セカンダリ VLAN のプライマリ VLAN
	との関連付け (p.36-14)
ができる VLAN は 1 つだけです。	
設定を確認します。	PVLAN としての VLAN の設定 (p.36-13)
	セカンダリ VLAN のプライマリ VLAN との関連付け (p.36-14)
設定を確認します。	セカンダリ VLAN 入力トラフィックの
	ルーティングの許可(p.36-21)
レイヤ 2 インターフェイスを PVI AN	
	1 VLAN 078XE (p.30-10)
3. Testination	
PVLAN 混合モード ポートをプライマ	レイヤ 2 インターフェイスの PVLAN
リ VLAN および選択したセカンダリ	混合モード ポートとしての設定
VLAN にマッピングします。	(p.36-15)
	レイヤ 2 インターフェイスの PVLAN
	混合モード トランク ポートとしての
	設定 (p.36-19)
レイヤ 2 インターフェイスを PVLAN	レイヤ2インターフェイスの PVLAN
	ホストポートとしての設定 (p.36-16)
	(pico 10)
プライマリ VLAN とセカンダリ VLAN	レイヤ 2 インターフェイスの PVLAN
のアソシエーションを設定し、PVLAN	トランク ポートとしての設定
	(p.36-17)
ます。	
PVLAN トランク ポートで許容される	レイヤ 2 インターフェイスの PVLAN
通常の VLAN のリストを設定します。	トランク ポートとしての設定
	(p.36-17)
PVLAN トランク ポートに(IEEE	レイヤ 2 インターフェイスの PVLAN
802.1Q タグとしての) タグなしパケッ	トランク ポートとしての設定
トが割り当てられる VLAN を設定しま す。	(p.36-17)
	VLANをPVLANとして設定します。 セカンダリ VLANをプライマリ VLANに関連付けます。リストに含めることができる VLANは1つだけです。 設定を確認します。 レイヤ 2 インターフェイスを PVLANポートとして設定します。 PVLAN混合モードポートをプライマリ VLANおよび選択したセカンダリ VLANにマッピングします。 プライマリ VLANとセカンダリ VLANに関連付けます。 プライマリ VLANとセカンダリ VLANのアソシエーションを設定し、PVLANトランクポートを PVLANに関連付けます。 PVLANトランクポートで許容される通常の VLANのリストを設定します。 PVLANトランクポートに(IEEE 802.1Q タグとしての)タグなしパケットが割り当てられる VLANを設定しま

PVLAN の概要

PVLAN 機能を使用すると、サービス プロバイダーが VLAN を使用したときに直面する 2 つの問題 に対処できます。

- スイッチがサポートするアクティブ VLAN は最大で 1005。サービス プロバイダーが顧客ごと に VLAN を 1 つ割り当てる場合、サポートできる顧客数に限界が生じます。
- IP ルーティングをイネーブルにするために、各 VLAN にサブネット アドレス スペースを割り 当てるかアドレス ブロックを割り当てます。このために未使用の IP アドレスが増え、IP アドレスの管理に問題が発生します。

PVLAN の使用により、サービス プロバイダーにはスケーラビリティと IP アドレス管理上の利点がもたらされ、顧客にはレイヤ 2 セキュリティが提供されます。PVLAN では、通常の VLAN ドメインをサブドメインに分割します。サブドメインは、プライマリ VLAN とセカンダリ VLAN という VLAN のペアで表されます。PVLAN には複数の VLAN のペアがあり、各サブドメインに 1 組のペアが対応します。PVLAN のすべての VLAN ペアは、同じプライマリ VLAN を共有します。セカンダリ VLAN ID によって各サブドメインは識別されます。図 36-1 を参照してください。

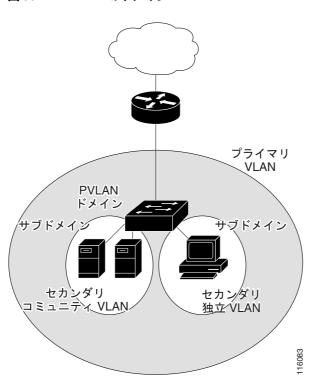


図 36-1 PVLAN のドメイン

セカンダリ VLAN には次の2種類があります。

- 独立 VLAN 独立 VLAN のポートは、レイヤ 2 レベルでは相互に通信できません。
- コミュニティ VLAN コミュニティ VLAN のポートは相互に通信できますが、レイヤ 2 レベルでは他のコミュニティのポートとは通信できません。

混合モード ポートは、1 つの PVLAN、1 つの独立 VLAN、および複数のコミュニティ VLAN だけで使用できます。レイヤ 3 ゲートウェイは、通常、混合モード ポート経由でスイッチに接続されます。

スイッチング環境では、個々のエンド ステーションまたは一連のエンド ステーションに、個別の PVLAN や関連する IP サブネットを割り当てることができます。エンド ステーションが PVLAN の外とやり取りする際に通信する必要があるのは、デフォルト ゲートウェイのみです。

PVLAN を使用して端末へのアクセスをコントロールするには、次の方法があります。

- 端末に接続する選択したインターフェイスを独立ポートとして設定し、レイヤ2での通信ができないようにします。たとえば、端末がサーバであれば、サーバ間のレイヤ2通信ができなくなります。
- デフォルト ゲートウェイおよび選択した端末(バックアップ サーバなど)に接続するインターフェイスを混合モード ポートとして設定して、すべての端末をデフォルト ゲートウェイにアクセスさせることができます。
- VLAN および IP サブネット内のトラフィック量を減らせば、端末が同じ VLAN および IP サブネット内にある場合でも端末間のトラフィックを防止できます。

混合モード ポートを使用すると、さまざまなデバイスを PVLAN への「アクセス ポイント」として接続できます。たとえば、混合モード ポートを LocalDirector のサーバ ポートに接続して、サーバに独立 VLAN または多数のコミュニティ VLAN を接続できます。LocalDirector は、独立またはコミュニティ VLAN 内にあるサーバのロード バランシングを行います。混合モードポートを使用して、管理ワークステーションからすべての PVLAN サーバのモニタまたはバックアップを行うことも可能です。

ここでは、次の内容について説明します。

- 定義一覧 (p.36-4)
- 標準トランク ポート(p.36-5)
- 複数のスイッチの PVLAN (p.36-5)
- PVLAN と他の機能との相互作用 (p.36-8)

定義一覧

用語	定義	
Private VLANs	プライマリ ID を共有し、ポート間をレイヤ 2 で分離しながら 1 つのレイヤ 3 ルータ ポートおよび IP サブネットを共有するメカニズムを提供する VLAN ペアのセット	
Secondary VLAN	PVLAN を実装するために使用する VLAN の種類。プライマリ VLAN に関連付けられており、ホストから他の許容ホストおよびルータにトラフィックを送信します。	
Community Port	コミュニティ セカンダリ VLAN に属するホスト ポート。同一コミュニティ VLAN 内の他のポートや混合モード ポートと通信します。これらのインターフェイスは、他のコミュニティのすべてのインターフェイスから、および自身の PVLAN 内の独立ポートから、レイヤ 2 で隔離されています。	
コミュニティ VLAN	アップストリーム トラフィックをコミュニティ ポートから混合モード ポート ゲート ウェイおよび同一コミュニティ内の他のホスト ポートに送信するセカンダリ VLAN。PVLAN には複数のコミュニティ VLAN を設定できます。	
	(注) Supervisor Engine 6-E は、コミュニティ PVLAN をサポートしません。	
Isolated Port	独立セカンダリ VLAN に属するホスト ポート。同一の PVLAN 内の他のポートからは、混合モード ポートを除き、レイヤ 2 で完全に分離されています。PVLAN は、混合モード ポートからのトラフィックを除く、独立ポートへのすべてのトラフィックをプロックします。独立ポートから受信したトラフィックは、混合モード ポートにのみ転送されます。	

	定義	
Isolated VLAN	PVLAN には独立 VLAN が 1 つだけあります。独立 VLAN とは、ホストから混合モード ポートおよびゲートウェイに単方向トラフィック アップストリームを送信するセカンダリ VLAN です。	
Primary VLAN	PVLAN にはプライマリ VLAN が 1 つだけあります。PVLAN のどのポートもプライマリ VLAN のメンバです。 プライマリ VLAN は、混合モード ポートから(独立およびコミュニティ)ホスト ポートおよび他の混合モード ポートに単方向トラフィック ダウンストリームを送信します。	
Private VLAN Trunk Port	PVLAN トランク ポートは、複数のセカンダリ(独立のみ)PVLAN および非 PVLAN を伝送します。パケットは、PVLAN トランク ポートでセカンダリ VLAN タグまたは 通常の VLAN タグとともに送受信されます。	
	(注) IEEE 802.1Q カプセル化方式のみサポートされています。	
Promiscuous Port	混合モード ポートはプライマリ VLAN に属し、すべてのインターフェイスと通信できます。 これらのインターフェイスには、 コミュニティおよび独立ホスト ポートと、プライマリ VLAN に関連付けられたセカンダリ VLAN に属する PVLAN トランク ポートが含まれます。	
Promiscuous Trunk Port	混合モード トランク ポートは、複数のプライマリ VLAN および通常の VLAN を伝送します。プライマリ VLAN タグまたは通常の VLAN タグを持つパケットが送受信されます。これ以外は、ポートは混合モード アクセス ポートと同じように動作します。 (注) IEEE 802.1Q カプセル化方式のみサポートされています。	
	(注) Supervisor Engine 6-E は、混合モード トランク ポートをサポートしません。	

複数のスイッチの PVLAN

ここでは、次の内容について説明します。

- 標準トランク ポート (p.36-5)
- PVLAN トランク (p.36-6)

標準トランク ポート

通常の VLAN と同じく、PVLAN も複数のスイッチにまたがって使用できます。1 つのトランク ポートが、プライマリ VLAN およびセカンダリ VLAN を近接スイッチに伝送します。 トランク ポートは、PVLAN をその他の VLAN として扱います。 複数のスイッチにまたがる PVLAN では、スイッチ A の独立ポートからのトラフィックはスイッチ B の独立ポートに到達しません。図 36-2 を参照してください。

PVLAN 構成のセキュリティを保持し、PVLAN として設定された VLAN が他の目的で利用されないようにするために、PVLAN ポートを持たないデバイスを含むすべての中継デバイスに PVLAN を設定します。

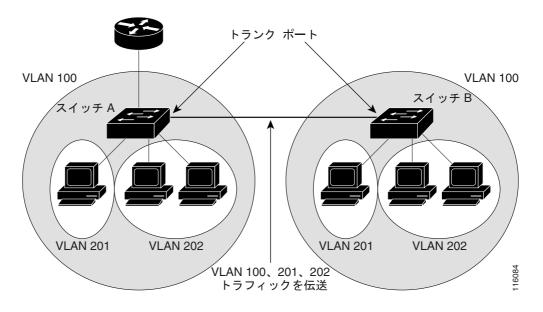


トランク ポートは通常の VLAN のトラフィックを伝送します。また、プライマリ、独立、およびコミュニティ VLAN のトラフィックも伝送します。



トランキングを実行するスイッチが両方とも PVLAN をサポートする場合は、標準トランク ポートを使用します。

図 36-2 スイッチのプライベート VLAN



VLAN 100 = プライマリ VLAN VLAN 201 = セカンダリ独立 VLAN VLAN 202 = セカンダリ コミュニティ VLAN

VTP (可変端末プロトコル)は PVLAN をサポートしないので、レイヤ 2 ネットワークのすべてのスイッチで PVLAN を手動で設定する必要があります。ネットワークの一部のスイッチにプライマリ/セカンダリ VLAN アソシエーションを設定しなかった場合、これらのスイッチのレイヤ 2 データベースは統合されません。その結果、これらのスイッチで PVLAN トラフィックのフラッディングが発生します。

PVLAN トランク

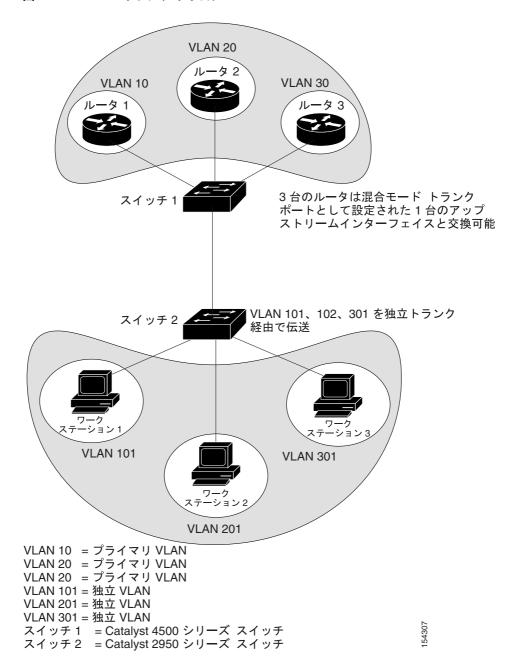
プライベート VLAN ポートで複数のセカンダリ VLAN を伝送する場合、PVLAN 独立トランクが使用されます。



Supervisor Engine 6-E は、独立トランク ポートをサポート *しません*。

図 36-3 に一般的なトポロジを示します。

図 36-3 PVLAN トランク トポロジ



このトポロジでは、スイッチ 1 はすべての独立 VLAN のトラフィックを PVLAN トランクを通じてスイッチ 2 にトランキングしますが、スイッチ 2 は PVLAN を認識しません。スイッチ 1 は異なる混合モード ポートに接続する異なるルータとも通信します。スイッチ 2 は異なるセカンダリ VLAN に属する複数のホストに接続します。

独立トランク ポートを使用すると、すべてのセカンダリ ポートのトラフィックが 1 つのトランク を通じて結合できます。

混合モード トランク ポートを使用すると、このトポロジで必要な複数の混合モード ポートを 1 つのトランク ポートにまとめることができ、複数のプライマリ VLAN を伝送します。

PVLAN と他の機能との相互作用

PVLAN には他の機能との相互作用があります。詳しくは次のセクションで説明します。

- PVLAN & VLAN ACL/QoS (p.36-8)
- PVLAN とユニキャスト、ブロードキャスト、およびマルチキャスト トラフィック (p.36-8)
- PVLAN **\(\subseteq \)** SVI (p.36-9)

「PVLAN 設定時の注意事項および制約事項」(p.36-11)も参照してください。

PVLAN & VLAN ACL/QoS

PVLAN ポートは、次のようにプライマリおよびセカンダリ VLAN を使用します。

- PVLAN ホスト ポートで受信されたパケットは、セカンダリ VLAN に属します。
- セカンダリ VLAN によりパケットにタグが設定されている場合、またはパケットのタグが解除 され、ポートのネイティブ VLAN がセカンダリ VLAN の場合、PVLAN トランク ポートで受信 されたパケットはセカンダリ VLAN に属します。

PVLAN ホストまたはトランク ポートで受信され、セカンダリ VLAN に割り当てられているパケットは、セカンダリ VLAN 上でブリッジングされます。このブリッジングにより、セカンダリ VLAN ACL(アクセス コントロール リスト)と(入力方向の)セカンダリ VLAN QoS(Quality Of Service)が適用されます。

パケットが PVLAN ホストまたはトランク ポートから送信される場合、パケットは論理的にはプライマリ VLAN に属します。この関係は、セカンダリ VLAN によるタグ付けが PVLAN 用であった場合にも適用されます。この状況では、出力時のプライマリ VLAN ACL およびプライマリ VLAN QoS がパケットに適用されます。

- 同様に、PVLAN 混合モード アクセス ポートで受信されるパケットもプライマリ VLAN に属します。
- 着信 VLAN によっては、PVLAN 混合モード トランク ポートで受信されるパケットがプライマリ VLAN または通常の VLAN に属することもあります。

混合モード トランク ポートに着信する、通常の VLAN へのトラフィックの場合、通常の VLAN ACL および QoS ポリシーが適用されます。PVLAN ドメインへのトラフィックの場合、混合モードポートで受信するパケットはプライマリ VLAN にブリッジングされます。このため、入力ではプライマリ VLAN ACL および QoS ポリシーが適用されます。

パケットが混合モード トランク ポートから送信される場合、セカンダリ ポートから受信されたパケットであればセカンダリ VLAN に論理的に属し、別の混合モード ポートからブリッジングされたパケットであればプライマリ VLAN に属します。パケットは区別できないので、混合モード トランク ポートから出力するパケットについては、VLAN QoS ポリシーはすべて無視されます。

PVLAN とユニキャスト、プロードキャスト、およびマルチキャスト トラフィック

通常の VLAN では、同じ VLAN のデバイスはレイヤ 2 レベルで相互に通信できますが、別の VLAN のインターフェイスに接続されているデバイスはレイヤ 3 レベルで通信します。PVLAN の場合、混合モード ポートはプライマリ VLAN のメンバですが、ホスト ポートはセカンダリ VLAN に属します。 セカンダリ VLAN はプライマリ VLAN に関連付けられているので、 これらの VLAN のメンバはレイヤ 2 レベルで相互に通信できます。

通常の VLAN では、ブロードキャストはその VLAN のすべてのポートに転送されます。PVLAN ブロードキャストの場合の転送先は、ブロードキャストを送信するポートによって異なります。

- 独立ポートは、混合モード ポートまたはトランク ポートにのみブロードキャストを送信します。
- コミュニティ ポートは、すべての混合モード ポート、トランク ポート、および同じコミュニティ VLAN のポートにブロードキャストを送信します。
- 混合モード ポートは、PVLAN のすべてのポートにブロードキャストを送信します (他の混合 モード ポート、トランク ポート、独立ポート、およびコミュニティ ポート)。

マルチキャスト トラフィックは、PVLAN の境界を超えて、1 つのコミュニティ VLAN 内で、ルーティングまたはブリッジングされます。マルチキャスト トラフィックは、同じ独立 VLAN のポート間または異なるセカンダリ VLAN のポート間では転送されません。

PVLAN & SVI

レイヤ 3 スイッチでは、Switch Virtual Interface (SVI; スイッチ仮想インターフェイス)が VLAN のレイヤ 3 インターフェイスとなります。レイヤ 3 デバイスと PVLAN の通信は、セカンダリ VLAN ではなく、プライマリ VLAN を介してのみ行われます。レイヤ 3 VLAN インターフェイス (SVI)はプライマリ VLAN だけに設定してください。セカンダリ VLAN には、レイヤ 3 VLAN インターフェイスを設定できません。VLAN がセカンダリ VLAN として設定されていれば、セカンダリ VLAN の SVI はインタラクティブになります。

- アクティブ SVI をセカンダリ VLAN として VLAN に設定しようとしても、SVI をディセーブルにしなければ設定できません。
- VLAN がセカンダリ VLAN として設定されており、そのセカンダリ VLAN がレイヤ 3 でマップされている場合は、この VLAN に SVI を作成しようとしても SVI は作成されず、エラー メッセージが表示されます。 SVI がレイヤ 3 でマップされていなければ SVI は作成されますが、自動的にシャット ダウンされます。

プライマリ VLAN がセカンダリ VLAN に関連付けられ、マップされている場合、プライマリ VLAN の設定はセカンダリ VLAN SVI に伝播されます。たとえば、IP サブネットをプライマリ VLAN SVI に割り当てると、このサブネットは PVLAN 全体の IP サブネット アドレスになります。

PVLAN の設定

ここでは、PVLAN の設定手順について説明します。

- PVLAN の設定手順 (p.36-10)
- PVLAN のデフォルト設定 (p.36-11)
- PVLAN 設定時の注意事項および制約事項 (p.36-11)
- PVLAN としての VLAN の設定 (p.36-13)
- セカンダリ VLAN のプライマリ VLAN との関連付け (p.36-14)
- レイヤ 2 インターフェイスの PVLAN 混合モード ポートとしての設定 (p.36-15)
- レイヤ 2 インターフェイスの PVLAN ホスト ポートとしての設定 (p.36-16)
- レイヤ 2 インターフェイスの PVLAN トランク ポートとしての設定 (p.36-17)
- レイヤ 2 インターフェイスの PVLAN 混合モード トランク ポートとしての設定 (p.36-19)
- セカンダリ VLAN 入力トラフィックのルーティングの許可 (p.36-21)

PVLAN の設定手順

PVLAN を設定する手順は、次のとおりです。

- **ステップ1** VTP を透過モードに設定します。「VTP のディセーブル化(VTP トランスペアレント モード)」 (p.13-17)を参照してください。
- ステップ2 セカンダリ VLAN を作成します。「PVLAN としての VLAN の設定」(p.36-13)を参照してください。
- ステップ3 プライマリ VLAN を作成します。「PVLAN としての VLAN の設定」(p.36-13)を参照してください。
- ステップ4 セカンダリ VLAN をプライマリ VLAN に関連付けます。「セカンダリ VLAN のプライマリ VLAN との関連付け」(p.36-14)を参照してください。



<u>一</u>(注)

プライマリ VLAN にマッピングできる独立 VLAN は 1 つだけですが、コミュニティ VLAN は複数をマッピングできます。

- **ステップ5** インターフェイスを、独立ホスト、コミュニティ ホスト、またはトランク ポートとして設定します。「レイヤ 2 インターフェイスの PVLAN ホスト ポートとしての設定」(p.36-16) および「レイヤ 2 インターフェイスの PVLAN トランク ポートとしての設定」(p.36-17) を参照してください。
- ステップ 6 独立ポートまたはコミュニティ ポートをプライマリ / セカンダリ VLAN ペアに関連付けます。「セカンダリ VLAN のプライマリ VLAN との関連付け」(p.36-14)を参照してください。
- ステップ7 インターフェイスを混合モード ポートとして設定します。「レイヤ 2 インターフェイスの PVLAN 混合モード ポートとしての設定」(p.36-15) を参照してください。
- ステップ8 混合モード ポートをプライマリ/セカンダリ VLAN ペアにマッピングします。「レイヤ 2 インターフェイスの PVLAN 混合モード ポートとしての設定」(p.36-15) を参照してください。
- ステップ9 VLAN 間ルーティングを使用する場合は、プライマリ SVI を設定し、セカンダリ VLAN をマッピングします。「セカンダリ VLAN 入力トラフィックのルーティングの許可」(p.36-21)を参照してください。

ステップ 10 PVLAN の設定を確認します。「Switch#」(p.36-22)を参照してください。

PVLAN のデフォルト設定

PVLAN は設定されていません。

PVLAN 設定時の注意事項および制約事項

PVLAN の設定時には、次の注意事項に従ってください。

- PVLAN を正しく設定するには、VTP のトランスペアレント モードでイネーブルにします。 VTP モードを PVLAN のクライアントまたはサーバに変更することはできません。
- PVLAN に VLAN 1 または VLAN 1002 ~ 1005 を設定しないでください。
- ポートをプライマリ VLAN、独立 VLAN、またはコミュニティ VLAN に割り当てる場合は、 PVLAN コマンドのみを使用します。

プライマリ VLAN、独立 VLAN、またはコミュニティ VLAN 上のレイヤ 2 インターフェイスは、PVLAN では非アクティブになります。レイヤ 2 トランク インターフェイスは、STP (スパニングツリー プロトコル)フォワーディング ステートのままです。

- セカンダリ VLAN には、レイヤ 3 VLAN インターフェイスを設定できません。
 独立 VLAN およびコミュニティ(セカンダリ) VLAN のレイヤ 3 VLAN インターフェイスは、VLAN が独立 VLAN またはコミュニティ VLAN として設定されている場合、非アクティブです。
- VLAN ポートを、EtherChannel として設定しないでください。ポートが PVLAN の設定に含まれる場合、これに対応する EtherChannel の設定は非アクティブです。
- プライマリ VLAN には、ダイナミック Access Control Entry (ACE; アクセス コントロール エントリ)を適用できません。

プライマリ VLAN に適用されている Cisco IOS ダイナミック ACL 設定は、VLAN が PVLAN の設定に含まれている場合、非アクティブです。

- 不正な設定によるスパニングツリー ループを防止するために、spanning-tree portfast trunk コマンドを使用して PVLAN トランク上で PortFast をイネーブルにします。
- セカンダリ VLAN に設定された VLAN ACL は、すべて入力方向で有効です。また、セカンダリ VLAN に関連付けられたプライマリ VLAN に設定された VLAN ACL はすべて出力方向で有効です。
- 独立 VLAN またはコミュニティ VLAN のレイヤ 3 スイッチングを停止する場合は、その VLAN のプライマリ VLAN へのマッピングを削除します。
- デバイスがトランク接続され、プライマリ VLAN およびセカンダリ VLAN がトランクに関連付けられているかぎり、異なるネットワーク デバイス上に PVLAN ポートを設定できます。
- 2 つの異なるデバイス上の独立ポートは相互通信できませんが、コミュニティ VLAN ポートの場合は可能です。
- PVLAN は、次の SPAN 機能をサポートしています。
 - PVLAN 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)を使用して、または単一の VLAN 上で SPAN を使用して、入力および出力トラフィックを個別に監視することができます。

SPAN の詳細については、第45章「SPAN と RSPAN の設定」を参照してください。

• プライマリ VLAN には複数のコミュニティ VLAN を関連付けできますが、独立 VLAN は 1 つだけです。

- 独立 VLAN またはコミュニティ VLAN には、1 つのプライマリ VLAN のみを関連付けることができます。
- PVLAN の設定で使用された VLAN を削除すると、この VLAN に関連付けられた PVLAN ポートは非アクティブになります。
- VTP は、PVLAN をサポートしていません。PVLAN ポートを使用する場合は、デバイスごとに PVLAN を設定する必要があります。
- 使用する PVLAN の設定のセキュリティを確保して、PVLAN として設定された VLAN が他の目的に使用されないようにするには、PVLAN ポートがないデバイスを含めて、すべての中間デバイスで PVLAN を設定します。
- PVLAN でトラフィックを伝送しないデバイスのトランクから、PVLAN をプルーニングします。
- ポート ACLS 機能が使用できる場合、セカンダリ VLAN ポートに Cisco IOS ACLS を、および PVLAN(VACL)に Cisco IOS ACLS を適用できます。VACL の詳細については、第42章「ACL によるネットワーク セキュリティの設定」を参照してください。
- プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN には、さまざまな QoS 設定を適用できます (第 34 章「QoS の設定」を参照)。プライマリ VLAN のレイヤ 3 VLAN インターフェイスに適用された Cisco IOS ACL は、関連する独立 VLAN およびコミュニティ VLAN にも自動的に適用されます。
- PVLAN トランク ポートでは、入力トラフィックにセカンダリ VLAN ACL、出力トラフィック にプライマリ VLAN ACL が適用されます。
- 混合モード ポートでは、入力トラフィックにプライマリ VLAN ACL が適用されます。
- PVLAN セカンダリ トランク ポートと混合モード トランク ポートはどちらも IEEE 802.1q カプセル化だけをサポートします。
- PVLAN トランク上では、コミュニティ VLAN を伝播または伝送できません。
- レイヤ 3 PVLAN インターフェイス上で学習された ARP エントリは、[sticky] ARP エントリと いいます (PVLAN インターフェイス ARP エントリを表示して確認することを推奨します)。
- セキュリティ上の理由から、PVLAN ポート sticky ARP エントリは期限切れになりません。異なる MAC アドレスでも同じ IP アドレスを持つデバイスを接続すると、エラー メッセージが生成されて ARP エントリは作成されません。
- PVLAN ポート sticky ARP エントリは期限切れしないので、MAC アドレスを変更する場合は手動でエントリを削除する必要があります。 sticky ARP エントリを上書きするには、まず no arp コマンドでエントリを削除してから、arp コマンドでエントリを上書きします。
- DHCP 環境では、PC をシャットダウンしても自分の IP アドレスを他人に譲ることはできません。この問題を解決するために、Catalyst 4500 シリーズ スイッチでは no ip sticky-arp コマンドをサポートしています。このコマンドを使用すると、DHCP 環境での IP アドレスの上書きおよび再使用ができます。
- 通常の VLAN は混合モード トランク ポートで伝送されます。
- 混合モード トランク ポートのデフォルト ネイティブ VLAN は VLAN 1 で、管理 VLAN です。 タグのないパケットはすべてネイティブ VLAN で転送されます。プライマリ VLAN または通 常の VLAN をネイティブ VLAN として設定できます。
- 混合モード トランクは、セカンダリ VLAN を伝送するようには設定できません。許容 VLAN リストでセカンダリ VLAN を指定した場合、設定は受け入れられますが、セカンダリ VLAN のポートは動作せず、転送しません。これは、セカンダリ VLAN ではあってもプライマリ VLAN に関連付けられていない VLAN のポートの場合にも当てはまります。
- 混合モード トランク ポートでは、プライマリ VLAN に着信する入力トラフィックにプライマリ VLAN ACL および QoS が適用されます。
- VLAN ACL または QoS は、混合モードトランク ポートの出力トラフィックには適用されません。PVLAN のトラフィックのアップストリームは、論理的にセカンダリ VLAN に向かうからです。ハードウェアの VLAN 変換により、受信したセカンダリ VLAN の情報は失われます。このため、ポリシーは適用されません。この制約は、同じプライマリ VLAN の他のポートからブリッジングされるトラフィックにも当てはまります。

• PVLAN 混合モード トランク ポートでポート セキュリティを設定しないでください。逆の場合 も行わないでください。

混合モード トランク ポートのポートセキュリティをイネーブルにした場合、この機能はサポートされていないので、ポートは予測できない動作をする可能性があります。

• PVLAN 混合モード トランク ポートに IEEE 802.1X を設定しないでください。

PVLAN としての VLAN の設定



Supervisor Engine 6-E は、コミュニティ PVLAN をサポートしません。

VLAN を PVLAN として設定するには、次の作業を行います。

	コマンド	目的	
ステップ 1	Switch# configure terminal	コンフィギュレーション モードを開始します。	
ステップ 2	Switch(config)# vlan vlan_ID	VLAN コンフィギュレーション モードを開始します。	
ステップ 3	Switch(config-vlan) # private-vlan {community isolated primary}	VLAN を PVLAN として設定します。 • このコマンドは、VLAN コンフィギュレーション サブモードを終了するまで有効になりません。 PVLAN のステータスをクリアするには、no キーワードを使用します。 (注) Supervisor Engine 6-E は、コミュニティおよび独立 PVLAN トランク ポートをサポートしません。	
ステップ 4	Switch(config-vlan)# end	VLAN コンフィギュレーション モードを終了します。	
ステップ 5	Switch# show vlan private-vlan [type]	設定を確認します。	

次に、VLAN 202 をプライマリ VLAN として設定し、その設定を確認する例を示します。

次に、VLAN 303 をコミュニティ VLAN として設定し、その設定を確認する例を示します。

Switch# configure terminal
Switch(config) # vlan 303
Switch(config-vlan) # private-vlan community
Switch(config-vlan) # end
Switch# show vlan private-vlan

202 primary 303 community

次に、VLAN 440 を独立 VLAN として設定し、その設定を確認する例を示します。

Switch# configure terminal Switch(config)# vlan 440 Switch(config-vlan)# private-vlan isolated Switch(config-vlan)# end Switch# show vlan private-vlan

Primary Secondary Type Interfaces

202 primary
303 community
440 isolated

セカンダリ VLAN のプライマリ VLAN との関連付け

セカンダリ VLAN をプライマリ VLAN に関連付けるには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# vlan primary_vlan_ID	プライマリ VLAN の VLAN コンフィギュレーション モードを開始します。
ステップ 3	Switch(config-vlan)# private-vlan association {secondary_vlan_list add secondary_vlan_list remove secondary_vlan_list}	セカンダリ VLAN をプライマリ VLAN に関連付けます。リストに含めることができる VLAN は 1 つだけです。
		すべてのセカンダリ アソシエーションをクリアす るには、no キーワードを使用します。
ステップ 4	Switch(config-vlan)# end	VLAN コンフィギュレーション モードを終了します。
ステップ 5	Switch# show vlan private-vlan [type]	設定を確認します。

セカンダリ VLAN をプライマリ VLAN と関連付ける場合、次の点に注意してください。

- secondary_vlan_list パラメータにはスペースを含めないでください。カンマで区切ると、複数の項目を含めることができます。各項目として入力できるのは、単一の PVLAN ID またはハイフンで連結した PVLAN ID の範囲です。
- secondary_vlan_list パラメータには、複数のコミュニティ VLAN ID を含めることができます。
- secondary_vlan_list パラメータには、独立 VLAN ID を 1 つだけ含めることができます。
- セカンダリ VLAN を PVLAN に関連付けるには、*secondary_vlan_list* を入力するか、または *secondary_vlan_list* と add キーワードを使用します。
- セカンダリ VLAN と PVLAN 間のアソシエーションをクリアするには、secondary_vlan_list と remove キーワードを使用します。

• これらのコマンドは、VLAN コンフィギュレーション サブモードを終了するまで有効になりません。

次に、プライマリ VLAN 202 にコミュニティ VLAN 303 ~ 307 および 309、独立 VLAN 440 を関連付け、その設定を確認する例を示します。

Switch# configure terminal
Switch(config)# vlan 202
Switch(config-vlan)# private-vlan association 303-307,309,440
Switch(config-vlan)# end
Switch# show vlan private-vlan

Primary	Secondary	Type	Interfaces
202	303	community	
202	304	community	
202	305	community	
202	306	community	
202	307	community	
202	309	community	
202	440	isolated	
	308	community	



セカンダリ VLAN 308 は、プライマリ VLAN と関連付けされません。

レイヤ 2 インターフェイスの PVLAN 混合モード ポートとしての設定

レイヤ2インターフェイスをPVLAN混合モードポートとして設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開 始します。
ステップ 2	Switch(config) # interface {fastethernet gigabitethernet tengigabitethernet} slot/port	設定する LAN インターフェイスを指定します。
ステップ 3	Switch(config-if)# switchport mode private-vlan {host promiscuous trunk promiscuous trunk [secondary]}	レイヤ 2 インターフェイスを PVLAN 混合モード ポートとして設定します。
ステップ 4	Switch(config-if)# [no] switchport private-vlan mapping [trunk] primary_vlan_ID {secondary_vlan_list add secondary_vlan_list remove secondary_vlan_list}	PVLAN 混合モード ポートをプライマリ VLAN および選択したセカンダリ VLAN にマッピング します。
ステップ 5	Switch(config-if)# end	コンフィギュレーション モードを終了します。
ステップ 6	Switch# show interfaces {fastethernet gigabitethernet tengigabitethernet} slot/port switchport	設定を確認します。



上記の switchport private-vlan mapping trunk コマンドでサポートされる一意のプライベート VLAN ペアの最大数は 500 です。 たとえば、1000 のセカンダリ VLAN を 1 つのプライマリ VLAN にマッピングしたり、1000 のセカンダリ VLAN を 1000 のプライマリ VLAN と 1 対 1 でマッピングしたりすることができます。

レイヤ 2 インターフェイスを PVLAN 混合モード ポートとして設定する場合、次の点に注意してください。

- secondary_vlan_list パラメータにはスペースを含めないでください。カンマで区切ると、複数の 項目を含めることができます。各項目として入力できるのは、単一の PVLAN ID またはハイフンで連結した PVLAN ID の範囲です。
- セカンダリ VLAN を PVLAN 混合モード ポートにマッピングするには、secondary_vlan_list を 入力するか、または secondary_vlan_list と add キーワードを使用します。
- セカンダリ VLAN と PVLAN 混合モード ポート間のマッピングをクリアするには、 secondary_vlan_list と remove キーワードを使用します。

次に、インターフェイス FastEthernet 5/2 を PVLAN 混合モード ポートとして設定し、PVLAN にマッピングして、その設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/2
Switch(config-if) # switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 200 2
Switch(config-if)# end
Switch# show interfaces fastethernet 5/2 switchport
Name:Fa5/2
Switchport: Enabled
Administrative Mode:private-vlan promiscuous
Operational Mode:private-vlan promiscuous
Administrative Trunking Encapsulation:negotiate
Operational Trunking Encapsulation:native
Negotiation of Trunking:Off
Access Mode VLAN:1 (default)
Trunking Native Mode VLAN:1 (default)
Voice VLAN: none
Administrative Private VLAN Host Association:none
Administrative Private VLAN Promiscuous Mapping:200 (VLAN0200) 2 (VLAN0002)
Private VLAN Trunk Native VLAN:none
Administrative Private VLAN Trunk Encapsulation:dot1q
Administrative Private VLAN Trunk Normal VLANs:none
Administrative Private VLAN Trunk Private VLANs:none
Operational Private VLANs:
 200 (VLAN0200) 2 (VLAN0002)
Trunking VLANs Enabled:ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed:ALL
```

レイヤ2インターフェイスの PVLAN ホスト ポートとしての設定

レイヤ2インターフェイスを PVLAN ホスト ポートとして設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# interface {fastethernet gigabitethernet tengigabitethernet} slot/port	設定する LAN ポートを指定します。
ステップ 3	Switch(config-if)# switchport mode private-vlan {host promiscuous trunk promiscuous trunk [secondary]}	レイヤ 2 インターフェイスを PVLAN ホストポートとして設定します。
ステップ 4	Switch(config-if)# [no] switchport private-vlan host-association primary_vlan_ID secondary_vlan_ID	レイヤ 2 インターフェイスを PVLAN に関連付けます。
		プライマリ VLAN からすべてのアソシエーションを削除するには、no キーワードを使用します。
ステップ 5	Switch(config-if)# end	コンフィギュレーション モードを終了します。
ステップ 6	Switch# show interfaces {fastethernet gigabitethernet tengigabitethernet} slot/port switchport	設定を確認します。

次に、インターフェイス FastEthernet 5/1 を PVLAN ホスト ポートとして設定し、その設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/1
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 202 440
Switch(config-if)# end
Switch# show interfaces fastethernet 5/1 switchport
Name: Fa5/1
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: private-vlan host
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Appliance trust: none
Administrative Private Vlan
 Host Association: 202 (VLAN0202) 440 (VLAN0440)
  Promiscuous Mapping: none
 Trunk encapsulation : dot1q
  Trunk vlans:
Operational private-vlan(s):
 202 (VLAN0202) 440 (VLAN0440)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

レイヤ 2 インターフェイスの PVLAN トランク ポートとしての設定

レイヤ2インターフェイスを PVLAN トランク ポートとして設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	Switch(config)# interface {fastethernet gigabitethernet tengigabitethernet} slot/port	設定する LAN ポートを指定します。
ステップ 3	Switch(config-if)# switchport mode private-vlan {host promiscuous trunk promiscuous trunk [secondary]}	レイヤ 2 インターフェイスを PVLAN トランク ポートとして設定します。

	コマンド	目的
ステップ 4	Switch(config-if)# [no] switchport private-vlan association trunk primary_vlan_ID secondary_vlan_ID	プライマリ VLAN とセカンダリ VLAN のアソシ エーションを設定し、PVLAN トランク ポートを PVLAN に関連付けます。
		↑ PVLAN トランク ポートが複数のセカンダリ VLAN を伝送できるように、このコマンドを使用して複数の PVLAN ペアを指定できます。既存のプライマリ VLAN にアソシエーションを指定した場合、既存のアソシエーションと置き換えられます。トランクにアソシエーションが指定されていない場合、セカンダリ VLAN で受信されたパケットはすべてドロップされます。
		プライマリ VLAN からすべてのアソシエーション を削除するには、no キーワードを使用します。
ステップ 5	Switch(config-if)# [no] switchport private-vlan trunk allowed vlan vlan_list all none [add remove except] vlan_atom[,vlan_atom]	PVLAN トランク ポートで許容される通常の VLAN のリストを設定します。
		PVLAN トランク ポートで許容される通常の VLAN をすべて削除するには、no キーワードを使用します。
ステップ 6	Switch(config-if)# switchport private-vlan trunk native vlan vlan_id	PVLAN トランク ポートに(IEEE 802.1Q タグとしての) タグなしパケットが割り当てられる VLAN を設定します。
		ネイティブ VLAN が設定されていない場合、タグな しのパケットはすべてドロップされます。
		ネイティブ VLAN がセカンダリ VLAN で、ポートに セカンダリ VLAN の関連付けが指定されていない 場合、タグなしパケットはドロップされます。
		PVLAN トランク ポートのネイティブ LAN すべてを 削除するには no キーワードを使用します。
ステップ 7	Switch(config-if)# end	コンフィギュレーション モードを終了します。
ステップ 8	Switch# show interfaces {fastethernet gigabitethernet tengigabitethernet} slot/port switchport	設定を確認します。

次に、インターフェイス FastEthernet 5/2 をセカンダリ トランク ポートとして設定し、その設定を 確認する例を示します。

```
Switch# configure terminal
Switch(config) # interface fastethernet 5/2
{\tt Switch(config-if)\# \ switchport \ mode \ private-vlan \ trunk \ secondary}
Switch(config-if) # switchport private-vlan trunk native vlan 10
Switch(config-if)# switchport private-vlan trunk allowed vlan 10. 3-4
Switch(config-if)# switchport private-vlan association trunk 3 301
Switch(config-if)# end
Switch# show interfaces fastethernet 5/2 switchport
Name: Fa5/2
   Switchport: Enabled
   Administrative Mode: private-vlan trunk secondary
   Operational Mode: private-vlan trunk secondary
   Administrative Trunking Encapsulation: negotiate
   Operational Trunking Encapsulation: dot1q
   Negotiation of Trunking: On
   Access Mode VLAN: 1 (default)
   Trunking Native Mode VLAN: 1 (default)
   Administrative Native VLAN tagging: enabled
   Voice VLAN: none
   Administrative private-vlan host-association: none A
   dministrative private-vlan mapping: none
   Administrative private-vlan trunk native VLAN: 10
   Administrative private-vlan trunk Native VLAN tagging: enabled
   Administrative private-vlan trunk encapsulation: dot1q
   Administrative private-vlan trunk normal VLANs: none
   Administrative private-vlan trunk associations:
        3 (VLAN0003) 301 (VLAN0301)
   Administrative private-vlan trunk mappings: none
   Operational private-vlan: none
   Operational Normal VLANs: none
   Trunking VLANs Enabled: ALL
   Pruning VLANs Enabled: 2-1001
   Capture Mode Disabled Capture VLANs Allowed: ALL
   Unknown unicast blocked: disabled
   Unknown multicast blocked: disabled
   Appliance trust: none
```

レイヤ 2 インターフェイスの PVLAN 混合モード トランク ポートとしての設定



Supervisor Engine 6-E は、混合モードトランク ポートをサポート しません。

レイヤ 2 インターフェイスを PVLAN 混合モード トランク ポートとして設定するには、次の作業を 行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	Switch(config)# interface {fastethernet gigabitethernet tengigabitethernet} slot/port	設定する LAN インターフェイスを指定します。
ステップ 3	Switch(config-if)# switchport mode private-vlan {host promiscuous trunk promiscuous trunk [secondary]}	レイヤ 2 インターフェイスを PVLAN 混合モード トランク ポートとして設定します。

	コマンド	目的
ステップ 4	Switch(config-if)# [no] switchport private-vlan mapping [trunk] primary_vlan_ID {secondary_vlan_list add	PVLAN 混合モード ポートをプライマリ VLAN およ び選択したセカンダリ VLAN にマッピングします。
	secondary_vlan_list remove secondary_vlan_list}	このコマンドの削除には 3 つのレベルがあります。 この表に続く例を参照してください。
ステップ 5	Switch(config-if)# end	コンフィギュレーション モードを終了します。
ステップ 6	Switch# show interfaces {fastethernet gigabitethernet tengigabitethernet} slot/port switchport	設定を確認します。



(注)

上記の switchport private-vlan mapping trunk コマンドでサポートされる一意のプライベート VLAN ペアの最大数は 500 です。たとえば、1000 のセカンダリ VLAN を 1 つのプライマリ VLAN にマッピングしたり、1000 のセカンダリ VLAN を 1000 のプライマリ VLAN と 1 対 1 でマッピン グしたりすることができます。



(注)

REP を使用すると、switchport mode private-vlan trunk promiscuous コマンドのみがサポートされます。他の PVLAN トランク関連設定はサポート*されません*。



(注)

デフォルトでは、PVLAN トランク混合モードに設定すると、ネイティブ VLAN は 1 に設定されます。

[no] switchport private-vlan mapping コマンドには、次の3つの削除レベルがあります。

- リストから 1 つまたは複数のセカンダリ VLAN を削除するレベル。次に例を示します。 Switch(config-if)# switchport private-vlan mapping trunk 2 remove 222
- PVLAN 混合モード トランク ポートから指定したプライマリ VLAN(およびそれ自身の選択したセカンダリ VLAN)へのマッピングをすべて削除するレベル。次に例を示します。

 ${\tt Switch(config-if)\#\ no\ switchport\ private-vlan\ mapping\ trunk\ 2}$

• PVLAN 混合モード トランク ポートから事前に設定されていたすべてのプライマリ VLAN(およびそれら自身の選択したセカンダリ VLAN)へのマッピングを削除するレベル。次に例を示します。

Switch(config-if) # no switchport private-vlan mapping trunk

レイヤ 2 インターフェイスを PVLAN 混合モード ポートとして設定する場合、次の点に注意してください。

- 混合モード トランク ポートで複数のプライマリ VLAN を伝送できるようにするには、 switchport private-vlan mapping trunk コマンドを使用して複数の PVLAN ペアを指定します。
- secondary_vlan_list パラメータにはスペースを含めないでください。カンマで区切ると、複数の項目を含めることができます。各項目として入力できるのは、単一の PVLAN ID またはハイフンで連結した PVLAN ID の範囲です。

- セカンダリ VLAN を PVLAN 混合モード ポートにマッピングするには、secondary_vlan_list を 入力するか、または secondary_vlan_list と add キーワードを使用します。
- セカンダリ VLAN と PVLAN 混合モード ポート間のマッピングをクリアするには、 secondary_vlan_list と remove キーワードを使用します。

次に、インターフェイス FastEthernet 5/2 を混合モード トランク ポートとして設定し、その設定を確認する例を示します。

```
Switch# configure terminal
Switch(config) # interface fastethernet 5/2
Switch(config-if) # switchport mode private-vlan trunk promiscuous
Switch(config-if)# switchport private-vlan trunk native vlan 10
Switch(config-if) # switchport private-vlan trunk allowed vlan 10, 3-4
Switch(config-if)# switchport private-vlan mapping trunk 3 301, 302
Switch(config-if)# end
Switch# show interfaces fastethernet 5/2 switchport
Name: Fa5/2
Switchport: Enabled
Administrative Mode: private-vlan trunk promiscuous
Operational Mode: private-vlan trunk promiscuous
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: 10
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: 3-4,10
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings:
    3 (VLAN0003) 301 (VLAN0301) 302 (VLAN0302)
Operational private-vlan:
 3 (VLAN0003) 301 (VLAN0301) 302 (VLAN0302)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

セカンダリ VLAN 入力トラフィックのルーティングの許可



独立 VLAN とコミュニティ VLAN は、いずれもセカンダリ VLAN と呼ばれます。

セカンダリ VLAN 入力トラフィックのルーティングを許可するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始
		します。
ステップ 2		プライマリ VLAN のインターフェイス コンフィ ギュレーション モードを開始します。

	コマンド	目的
ステップ 3	Switch(config-if)# [no] private-vlan mapping primary_vlan_ID {secondary_vlan_list add secondary_vlan_list remove secondary_vlan_list}	セカンダリ VLAN 入力トラフィックのルーティングを許可するために、セカンダリ VLAN をプライマリ VLAN にマッピングします。
		プライマリ VLAN からすべてのアソシエーション を削除するには、no キーワードを使用します。
ステップ 4	Switch(config-if)# end	コンフィギュレーション モードを終了します。
ステップ 5	Switch# show interface private-vlan mapping	設定を確認します。

セカンダリ VLAN 入力トラフィックのルーティングを許可する場合、次の点に注意してください。

- private-vlan mapping インターフェイス コンフィギュレーション コマンドは、レイヤ 3 スイッチングされた PVLAN 入力トラフィックのみに影響します。
- secondary_vlan_list パラメータにはスペースを含めないでください。カンマで区切ると、複数の項目を含めることができます。各項目として入力できるのは、単一の PVLAN ID またはハイフンで連結した PVLAN ID の範囲です。
- セカンダリ VLAN をプライマリ VLAN にマッピングするには、secondary_vlan_list を入力するか、または secondary_vlan_list と add キーワードを使用します。
- セカンダリ VLAN とプライマリ VLAN 間のマッピングを消去するには、secondary_vlan_list パラメータと remove キーワードを使用します。

次に、PVLAN 303 ~ 307、309、および 440 からのセカンダリ VLAN 入力トラフィックのルーティングを許可し、設定を確認する例を示します。

Switch# configure terminal

Switch(config) # interface vlan 202

 ${\tt Switch(config-if)\# private-vlan\ mapping\ add\ 303-307,309,440}$

Switch(config-if)# end

Switch# show interfaces private-vlan mapping

Interface Secondary VLAN Type

vlan202	303	community
vlan202	304	community
vlan202	305	community
vlan202	306	community
vlan202	307	community
vlan202	309	community
vlan202	440	isolated

Switch#



CHAPTER

37

802.1X ポートベース認証の設定

この章では、IEEE(米国電気電子学会)802.1X ポートベース認証を設定して、不正なデバイス(クライアント)によるネットワークへのアクセスを防止する方法について説明します。

この章の主な内容は、次のとおりです。

- 802.1X ポートベース認証の概要 (p.37-2)
- 802.1X の設定 (p.37-22)
- 802.1X 統計情報およびステータスの表示 (p.37-51)



この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/cr/index.htm

802.1X ポートベース認証の概要

802.1X では、クライアント/サーバベースのアクセス コントロールと認証プロトコルとして 802.1X ポートベース認証を定義し、不正なクライアントが一般的にアクセス可能なポートを通じて LAN に接続するのを制限します。認証サーバは、オーセンティケータ(ネットワーク アクセス スイッチ)ポートに接続された各サプリカント(クライアント)を確認してから、スイッチまたは LAN が提供するサービスを利用できるようにします。



802.1X をサポートするには、Remote Authentication Dial-In User Service(RADIUS)用に設定された認証サーバが必要です。ネットワーク アクセス スイッチが設定済みの RADIUS サーバにパケットをルーティングできないと、802.1X 認証は機能しません。スイッチがパケットをルーティングできることを確認するには、スイッチからサーバに ping を送信します。

クライアントが認証されるまでは、クライアントが接続されたポートを経由する Extensible Authentication Protocol over LAN (EAPOL)トラフィックだけが許容されます。認証が成功すると、通常のトラフィックがポートを通過できるようになります。

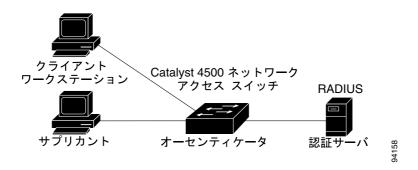
802.1X ポートベースの認証を設定するには、以下に説明する概念を理解する必要があります。

- 装置の役割 (p.37-3)
- 802.1X とネットワーク アクセス コントロール (p.37-4)
- 認証の開始とメッセージ交換 (p.37-4)
- 許可ステートおよび無許可ステートのポート(p.37-5)
- 802.1X ホストモード (p.37-7)
- VLAN 割り当てを使用した 802.1X 認証の利用 (p.37-7)
- ゲスト VLAN を使用した 802.1X 認証の使用 (p.37-9)
- MAC 認証バイパスを使用した 802.1X 認証の利用 (p.37-10)
- アクセス不能認証バイパスを使用した 802.1X 認証の利用 (p.37-12)
- 単方向制御ポートを使用した 802.1X 認証の利用 (p.37-12)
- 認証失敗 VLAN 割り当てを使用した 802.1X 認証の利用 (p.37-13)
- ポート セキュリティを使用した 802.1X 認証の利用 (p.37-15)
- RADIUS によるセッション タイムアウトを使用した 802.1X 認証の利用 (p.37-16)
- RADIUS アカウンティングを使用した 802.1X 認証の利用 (p.37-16)
- 音声 VLAN ポートを使用した 802.1X 認証の利用 (p.37-19)
- 複数ドメイン認証の使用 (p.37-20)
- サポート対象トポロジ(p.37-21)

装置の役割

802.1X ポートベース認証では、ネットワーク装置は特定の役割を果たします。図 37-1 に、下記の各装置の役割を示します。

図 37-1 802.1X 装置の役割



• クライアント LAN へのアクセスを要求し、スイッチからの要求に応答するワークステーション。ワークステーションは、802.1X 準拠のクライアント ソフトウェアが稼働するものでなければなりません。



(注)

802.1X 準拠のクライアント アプリケーション ソフトウェア(Microsoft の Windows 2000 Professional や Windows XP など) の詳細については、次の URL にある Microsoft Knowledge Base Article の資料を参照してください。http://support.microsoft.com

• オーセンティケータ クライアントの認証ステータスに基づいて、ネットワークへの物理アクセスを制御します。Catalyst 4500 シリーズ スイッチは、クライアントと認証サーバ間の仲介装置として機能し、クライアントに識別情報を要求してその情報を認証サーバで確認し、クライアントに応答をリレーします。スイッチは Extensible Authentication Protocol (EAP) フレームのカプセル化およびカプセル化解除を行い、RADIUS 認証サーバと対話します。

スイッチが EAPOL フレームを受信して認証サーバにリレーすると、イーサネット ヘッダーが 取り除かれ、残りの EAP フレームが RADIUS 形式で再度カプセル化されます。カプセル化の間は EAP フレームの変更や検査が行われないので、認証サーバはネイティブのフレーム形式内で EAP をサポートする必要があります。スイッチが認証サーバからフレームを受信すると、サーバからフレーム ヘッダーが削除され、EAP フレームが残ります。これがイーサネット用にカプセル化されてクライアントに送信されます。



(注)

Catalyst 4500 シリーズ スイッチでは、RADIUS クライアントおよび 802.1X をサポートする ソフトウェアを実行している必要があります。

• 認証サーバ クライアントの実際の認証を行います。認証サーバは、クライアントの識別情報を確認し、LAN およびスイッチ サービスへのクライアントのアクセスを許可することをスイッチに通知します(サポートされる認証サーバは、EAP 拡張機能を備えた RADIUS 認証サーバのみです。これは、Cisco Secure Access Control Server バージョン 3.2 以上で使用できます)。

802.1X とネットワーク アクセス コントロール

ネットワーク アクセス コントロールは、ポート アクセス ポリシーが認証装置のアンチウイルス ポスチャによって影響を受ける機能です。

アンチウイルス ポスチャの要素には、装置で実行するオペレーティング システム、オペレーティング システムのバージョン、アンチウイルス ソフトウェアのインストールの有無、使用可能なアンチウイルス シグニチャのバージョンなどがあります。認証装置に NAC 認識 802.1X サプリカントがあり、認証サーバが 802.1X 経由で NAC をサポートする設定の場合、アンチウイルス ポスチャ情報は自動的に 802.1X 認証交換の一部になります。

NAC の設定については、次の URL を参照してください。

 $http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_configuration_guide09186a00805764fd.html \\$

認証の開始とメッセージ交換

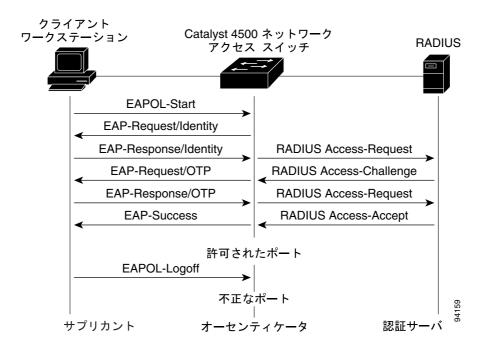
スイッチまたはクライアントのどちらからでも、認証を開始できます。dot1x port-control auto インターフェイス コンフィギュレーション コマンドを使用してポート上で認証をイネーブルにする場合、スイッチは、ポートのリンク ステートが移行したことを確認したときに、認証を開始する必要があります。次に、スイッチは EAP-Request/Identity フレームをクライアントに送信して識別情報を要求します(一般に、スイッチは最初の Request/Identity フレームを送信して、そのあとで 1 つまたは複数の認証情報要求を送信します)。フレームの受信後、クライアントは EAP-Responce/Identity フレームで応答します。

ただし、起動中にクライアントがスイッチから EAP-Request/Identity フレームを受信しなかった場合、クライアントは、EAPOL-Start フレームを送信することによって認証を開始できます。これにより、スイッチはクライアントの識別情報を要求します。

ネットワーク アクセス スイッチで 802.1X がイネーブルになっていない場合、またはサポートされていない場合は、クライアントからの EAPOL フレームはドロップされます。認証の開始を 3 回試行してもクライアントが EAP-Request/Identity フレームを受信できなかった場合、クライアントは、ポートが許可ステートにある場合と同じようにフレームを送信します。ポートが認証ステートであるということは、クライアントが正しく認証されていることを意味します。クライアントが識別情報を送るとスイッチは仲介装置としての役割を開始し、認証が成功または失敗するまでクライアントと認証サーバ間で EAP フレームを送受信します。認証が成功すると、スイッチ ポートは許可された状態になります。

特定の EAP フレーム交換は、使用される認証方式によって異なります。 図 37-2 に、認証サーバで One-Time-Password (OTP) 認証方式を使用するクライアントによって開始されるメッセージ交換を示します。

図 37-2 メッセージ交換



許可ステートおよび無許可ステートのポート

スイッチ ポートのステートによって、クライアントがネットワーク アクセスを許可されているか どうかがわかります。ポートは、無許可ステートで開始します。ポートはこのステートにある間、802.1X プロトコル パケットを除いてすべての入力トラフィックおよび出力トラフィックを許容しません。クライアントが正常に認証されると、ポートは許可ステートに移行し、そのクライアントへのすべてのトラフィックが許容されます。

802.1X 非対応クライアントが無許可の 802.1X ポートに接続する場合、スイッチはクライアントに識別情報を要求します。この場合、クライアントは要求に応答しないので、ポートは無許可ステートにとどまり、クライアントにはネットワーク アクセスが許可されません。802.1X 非対応クライアントに接続されたポート上にゲスト VLAN が設定されている場合、このポートは設定されたゲスト VLAN に追加され、許可ステートになります。詳細については、「ゲスト VLAN を使用した 802.1X 認証の使用」(p.37-9) を参照してください。

それに対して、802.1X 対応クライアントが 802.1X プロトコルを実行していないポートに接続する場合、クライアントは EAPOL-Start フレームを送信して認証プロセスを開始します。応答を受信しなかった場合、クライアントは要求を固定回数だけ送信します。応答が得られないので、クライアントはポートが許可ステートにある場合と同じようにフレームの送信を開始します。

ポートの許可ステートを制御するには、dot1x port-control インターフェイス コンフィギュレーション コマンドと以下のキーワードを使用します。

- **force-authorized** 802.1X 認証をディセーブルにして、認証交換を要求せずにポートを許可ステートに移行させます。ポートは、クライアントの 802.1X ベース認証なしで通常のトラフィックを送受信します。これはデフォルト設定です。
- force-unauthorized ポートを無許可ステートのままにして、クライアントが認証を試みても すべて無視します。スイッチは、インターフェイスを介してクライアントに認証サービスを提 供できません。

• auto 802.1X 認証をイネーブルにして、ポートに無許可ステートを開始させ、EAPOL フレームだけがポートを通じて送受信できるようにします。ポートのリンク ステートがダウンからアップに移行するか、EAPOL-Start フレームを受信すると、認証プロセスが開始されます。スイッチは、クライアントの識別情報を要求し、クライアントと認証サーバ間で認証メッセージのリレーを開始します。スイッチはクライアントの MAC (メディア アクセス制御)アドレスを使用して、ネットワーク アクセスを試みる各クライアントを一意に識別します。

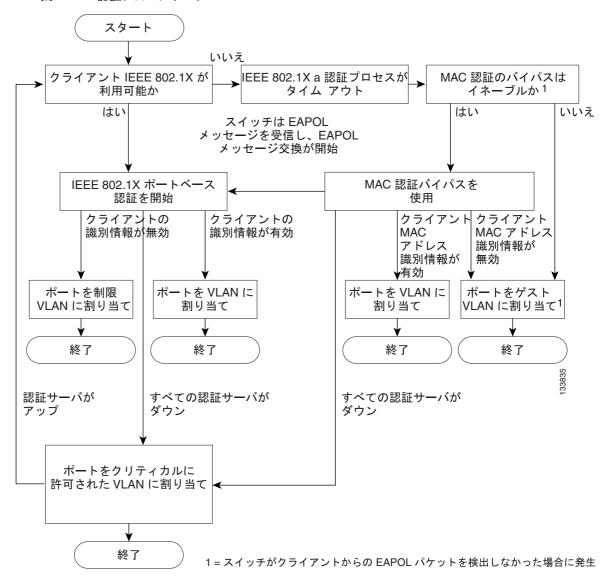
クライアントが正常に認証されると(認証サーバから Accept フレームを受信すると)、ポート ステートが許可に切り替わり、認証されたクライアントのフレームはすべてそのポートを通じて許容されます。認証が失敗した場合、ポートは無許可ステートのままですが、認証を再試行できます。認証サーバにアクセスできない場合、スイッチは要求を再送信できます。指定された回数試行してもサーバから応答が得られない場合は、認証が失敗し、ネットワーク アクセスは許可されません。

ポートのリンク ステートがアップからダウンに移行した場合、または EAPOL-Logoff フレームを受信した場合、ポートは無許可ステートに戻ります。

図 37-3 に認証プロセスを示します。

MDA がポートでイネーブルになっている場合、音声認証に適用可能な一部の例外付きでこのフローを使用できます。MDA の詳細については、「複数ドメイン認証の使用」(p.37-20)を参照してください。

図 37-3 認証フローチャート



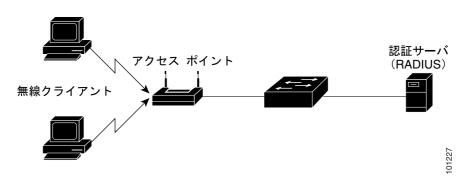
802.1X ホスト モード

単一ホストまたは複数ホスト モードの 802.1X ポートを設定できます。単一ホスト モード(図 37-1 [p.37-3] を参照)では、802.1X 対応スイッチ ポートに接続できるのは 1 つのクライアントだけです。スイッチは、ポートのリンク ステートがアップ ステートに変化すると、EAPOL フレームを送信してクライアントを検出します。クライアントが脱退するか、別のクライアントに交換されると、スイッチはポートのリンク ステートをダウンに変更し、ポートは無許可ステートに戻ります。

複数ホスト モードでは、複数ホストを単一 802.1X 対応ポートに接続できます。図 37-4 に、ワイヤレス LAN での 802.1X ポートベース認証を示します。このモードでは、接続されたクライアントのうち 1 つだけを、ネットワーク アクセスが付与されるすべてのクライアントに対して許可する必要があります。ポートが無許可になると(再認証が失敗するか、EAPOL-Logoff メッセージを受信すると)、スイッチは、接続されたすべてのクライアントに対してネットワーク アクセスを拒否します。このトポロジでは、無線アクセス ポイントは、接続しているクライアントを認証する役割があり、スイッチに対してクライアントとして機能します。

複数ホスト モードがイネーブルになっている場合、802.1X 認証を使用してポートおよびポート セキュリティを認証し、クライアントも含めて、すべての MAC アドレスへのネットワーク アクセスを管理できます。

図 37-4 複数ホスト モードの例



Cisco IOS Release 12.2(37)SG およびそれ以降のリリースは、データ デバイスと IP Phone (Cisco または Cisco 以外) などの音声デバイスの両方が同じスイッチ ポートに接続することを許可する MDA をサポートします。MDA の設定方法については、「複数ドメイン認証の使用」(p.37-20) を参照してください。

VLAN 割り当てを使用した 802.1X 認証の利用

VLAN 割り当てを使用すると、ネットワーク アクセスを特定のユーザに限定できます。VLAN 割り当てでは、802.1X で認証されたポートはポートに接続したクライアントのユーザ名に基づいて VLAN に割り当てられます。RADIUS サーバ データベースは、ユーザ名 /VLAN マッピングを保持します。ポートの 802.1X 認証が成功すると、RADIUS サーバは VLAN 割り当てをスイッチに送信します。この場合の VLAN は、「標準」 VLAN または PVLAN です。

PVLAN をサポートするプラットフォームでは、ポートを PVLAN に割り当てることによってホストを分離できます。

スイッチおよび RADIUS サーバ上で設定する場合、VLAN 割り当てを使用した 802.1X 認証には次の特性があります。

- RADIUS サーバから VLAN が提供されない場合は、認証が成功したときにポートは自身のアクセス VLAN または独立 PVLAN に設定されます。
- 認証サーバが無効な VLAN 情報を提供した場合、ポートは無許可ステートのままになります。 これは、設定エラーによって不適切な VLAN 上にポートが突然現れることを防ぐためです。
- 認証サーバが有効な VLAN 情報を提供した場合、認証に成功すると、ポートは許可ステートになり、指定された VLAN に追加されます。
- 複数ホスト モードがイネーブルの場合、すべてのホストは最初に認証されたユーザと同じ VLAN 内にあります。
- ポート上で 802.1X がディセーブルになると、そのポートは設定されたアクセス VLAN に戻ります。
- ポートは、アクセス ポート(「通常の」VLAN にのみ割り当て可能)か、または PVLAN ホストポート(PVLAN にのみ割り当て可能)として設定される必要があります。ポートを PVLAN ホストポートとして設定すると、ポート上のすべてのホストはそのポスチャが適合か不適合かにかかわらず、PVLAN に割り当てられることになります。Access-Accept に示された VLAN タイプが、ポートに割り当てられると予測される VLAN タイプ(アクセス ポートには通常の VLAN、PVLAN ホストポートにはセカンダリ PVLAN)と一致しない場合、VLAN 割り当ては失敗します。
- ゲスト VLAN が応答しないホストを処理するよう設定されている場合、ゲスト VLAN として 設定されている VLAN タイプがポート タイプと一致する必要があります(つまり、アクセス ポート上で設定されたゲスト VLAN の場合は標準 VLAN、PVLAN ホスト ポート上で設定され たゲスト VLAN の場合は PVLAN)。ゲスト VLAN のタイプが、ポート タイプと一致しない場 合、応答しないホストはゲスト VLAN が設定されていない場合と同じように処理されます(つ まり、ネットワーク アクセスを拒否されます)。
- ポートを PVLAN に割り当てるには、示された VLAN がセカンダリ PVLAN である必要があります。スイッチは、ローカルに設定されたセカンダリ / プライマリの関連付けから暗黙のプライマリ VLAN を判別します。



RADIUS が割り当てた VLAN で認証されているポートのアクセス VLAN または PVLAN ホスト VLAN マッピングを変更すると、ポートは RADIUS が割り当てた VLAN に残ったままになります。

VLAN 割り当てを設定するには、次の作業を実行する必要があります。

- **network** キーワードを使用して Authentication, Authorization, Accounting (AAA; 認証、認可、アカウンティング) 許可をイネーブルにし、RADIUS サーバからのインターフェイス設定を可能にします。 aaa authorization network group radius コマンドを適用する方法については、「802.1X 認証のイネーブル化」(p.37-24) を参照してください。
- 802.1X をイネーブルにします (VLAN 割り当て機能は、アクセス ポートに 802.1X が設定されると自動的にイネーブルになります)。
- RADIUS サーバにベンダー固有のトンネル アトリビュートを割り当てます。VLAN を適切に割り当てるには、RADIUS サーバが次のアトリビュートをスイッチに返す必要があります。
 - トンネル タイプ = VLAN
 - トンネル メディア タイプ = 802
 - トンネル プライベート グループ ID = VLAN NAME

ゲスト VLAN を使用した 802.1X 認証の使用



(注) Supervisor Engine 6-E は、この機能をサポートして*いません*。

ゲスト VLAN を使用すると、802.1X 非対応ホストが 802.1X 認証を使用するネットワークにアクセスできるようになります。たとえば、802.1X 認証をサポートするようにシステムをアップグレードしている間も、ゲスト VLAN を使用できます。

ゲスト VLAN はポート単位でサポートされ、その VLAN タイプがポート タイプと一致するかぎり、すべての VLAN をゲスト VLAN として使用できます。ポートがすでにゲスト VLAN 上で転送を行っている場合に、そのホストのネットワーク インターフェイス上で 802.1X サポートをイネーブルにすると、ポートはただちにゲスト VLAN から除外され、オーセンティケータは認証の開始を待機します。

ポート上での 802.1X 認証をイネーブルにすると、802.1X プロトコルが開始されます。ホストが一定期間内にオーセンティケータからのパケットに応答できなかった場合、オーセンティケータはそのポートを設定済みのゲスト VLAN に追加します。

ポートが PVLAN ホスト ポートとして設定されている場合、ゲスト VLAN はセカンダリ PVLAN である必要があります。ポートがアクセス ポートとして設定されている場合、ゲスト VLAN は通常の VLAN である必要があります。ポート上で設定されたゲスト VLAN が、ポート タイプに適さない場合、スイッチはゲスト VLAN が設定されていないように動作します(すなわち、応答しないホストはネットワーク アクセスを拒否されます)。

ゲスト VLAN の設定方法については、「ゲスト VLAN を使用した 802.1X 認証の設定」(p.37-33) を 参照してください。

ゲスト VLAN を使用した 802.1X 認証の使用上の注意事項

ゲスト VLAN を使用した 802.1X 認証の使用上の注意事項は次のとおりです。

- ゲスト VLAN を別の VLAN に再設定すると、認証失敗ポートもすべて移動され、ポートは現在の許可ステートのままです。
- ゲスト VLAN をシャット ダウンするか、または VLAN データベースから削除すると、すべて の認証失敗ポートはただちに無許可ステートに移行し、認証プロセスがふたたび開始されます。



(注)

ゲスト VLAN では定期的な再認証を行うことはできません。

Windows XP ホスト上でのゲスト VLAN 使用 802.1X 認証の使用上の注意事項

Windows XP ホスト上でのゲスト VLAN に対する 802.1X 認証の使用上の注意事項は次のとおりです。

- ホストがオーセンティケータに応答しない場合、ポートは接続を3回試行します(試行間隔は30秒です)。このあとは、ログイン/パスワードウィンドウはホストに表示されなくなります。 ネットワークインターフェイスケーブルを取り外し、再接続する必要があります。
- 不正なログイン/パスワードで応答するホストは、認証に失敗します。認証に失敗したホストは、ゲスト VLAN に追加されません。ホストが初めて認証に失敗すると、待機時間タイマーが始動し、タイマーが満了するまでアクティビティが一切発生しません。待機時間タイマーが満

了すると、ホストにログイン / パスワード ウィンドウが表示されます。ホストが 2 度めも認証 に失敗すると、待機時間タイマーが再度始動し、タイマーが満了するまでアクティビティは一 切発生しません。ホストにはこのあとさらに、3 度めのログイン / パスワード ウィンドウが表示されます。ホストが 3 度めの認証に失敗すると、ポートは無許可ステートになり、ネット ワーク インターフェイス ケーブルを取り外して再接続することが必要になります。

MAC 認証パイパスを使用した 802.1X 認証の利用

802.1X プロトコルには、クライアント (サプリカント)、オーセンティケータ、認証サーバの 3 つのエンティティがあります。通常、ホスト PC はサプリカント ソフトウェアを実行し、自分自身を認証するためにクレデンシャルをオーセンティケータに送信します。オーセンティケータはその情報を認証サーバに送信して認証を求めます。

しかし、すべてのホストにサプリカント機能があるわけではありません。802.1X を使用して自分自身を認証できないがネットワークにアクセスする必要がある装置は、MAC Authentication Bypass (MAB; MAC 認証バイパス)が使用できます。MAB は、接続先装置の MAC アドレスを使用してネットワーク アクセスを認可または拒否します。

通常、この機能はプリンタなどの装置が接続されているポートで使用します。これらの装置には 802.1X サプリカント機能がありません。

通常の構成では、RADIUS サーバはアクセスが必要な MAC アドレスのデータベースを保持します。この機能によって新しい MAC アドレスがポートで検出されると、装置の MAC アドレスとしてユーザ名とパスワードが使用された RADIUS 要求が生成されます。認証に成功したら、802.1X サプリカントを処理するときに 802.1X 認証で行われるのと同じコード パスを通じて、ポートからその装置にアクセスできるようになります。認証に失敗すると、ポートはゲスト VLAN に移動するか (ゲスト VLAN が設定されている場合)、未認証のままになります。

Catalyst 4500 シリーズ スイッチは、ポート レベルごとの MAC の再認証もサポートします。再認証機能は802.1X から提供され、MAB 固有ではありません。再認証モードでは、ポートは RADIUS から送信された VLAN にとどまり、自分自身を再認証しようとします。再認証に成功すると、ポートは RADIUS から送信された VLAN にとどまります。失敗した場合は、ポートは未認証になり、ゲスト VLAN が設定されている場合はゲスト VLAN に移動します。

MAB の設定方法については、「MAC 認証バイパスを使用した 802.1X 認証の設定」(p.37-36) を参照してください。

機能の相互作用

ここでは、MAB がイネーブルの場合の機能の相互作用と制約事項を示します。MAB とシームレス に相互作用する機能については説明していません(単方向制御ポートなど)。

• MAB は、ポートに 802.1X が設定されている場合にだけイネーブルにできます。MAB は MAC を認証するフォール バック メカニズムとしてのみ機能します。ポートに MAB と 802.1X を同時に設定すると、ポートは 802.1X を使用して認証しようとします。ホストが EAPOL 要求への 応答に失敗した場合に MAB が設定されていると、802.1X ポートが開かれパケットを受信して MAC アドレスを取得します。無限に認証が続くことはありません。

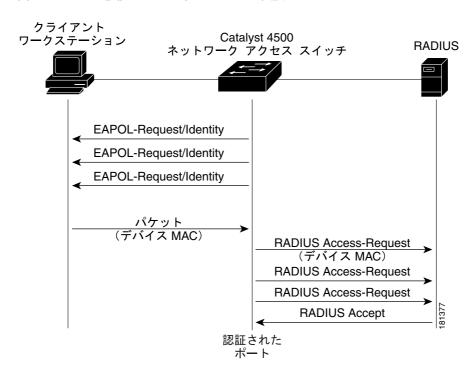
デフォルトの 802.1X タイマー値に基づき、メカニズム間の移行にはおよそ 90 秒かかります。転送時間の値を小さくすれば時間を短くできますが、EAPOL 転送頻度に影響を与えます。値が小さくなると EAPOL の送信間隔が短くなります。MAB がイネーブルな状態で 802.1X が EAPOL のフルセットを 1 回実行すると、学習された MAC アドレスが認証サーバに送信されて処理されます。

MAB モジュールは、ライン上で検出された最初の MAC アドレスの許可を実行します。RADIUS が承認する有効な MAC アドレスが受信されると、ポートは許可されたと見なされます。

MAB の結果として最初に許可されたポートで EAPOL パケットが受信されると、802.1X 認証 は再起動できます。

図 37-5 に、MAB 時のメッセージ交換を示します。

図 37-5 MAC 認証パイパス時のメッセージ交換



- 認証に失敗した VLAN は、802.1X 認証に失敗したユーザだけが使用します。MAB は 802.1X 認証に失敗したユーザに対しては試みられません。802.1X 認証に失敗すると、MAB の設定の有無にかかわらずポートは認証失敗 VLAN(設定されている場合)に移動します。
- MAB とゲスト VLAN の両方が設定されており EAPOL パケットがポートで受信されなかった 場合、802.1X ステート マシンは MAB ステートに移行し、ここでポートが開いてトラフィック を受信し MAC アドレスを取得します。ポートは、MAC を認識するまではこのステートのまま です。アドレスが認証に失敗すると、ポートはゲスト VLAN(設定されている場合)に移動し ます。

ゲスト VLAN 内のポートは、指定されたゲスト VLAN のすべてのトラフィックに対してオープンです。このため、通常は認証されるが、認証に失敗した装置が早い段階で検出されたためにゲスト VLAN になった非 802.1X サプリカントは、いつまでもゲスト VLAN に残ります。ただし、リンクが消失したりライン上で EAPOL が検出されるとゲスト VLAN 外に移動し、デフォルトの 802.1X モードに戻ります。

- MABによって新しいMACが認証されると、802.1X オーセンティケータ(またはポートセキュリティ)によってアクセスが制限されるようになり、ポートのセキュリティが保護されます。802.1X デフォルトホストパラメータは、シングルホストだけに定義されます。ポートがマルチユーザポストに変更されると、ポートセキュリティが採用され、このポートで許容されるMACアドレスの数が適用されます。
- Catalyst 4500 シリーズ スイッチは VVID を持つ MAB をサポートしますが、MAC アドレスはポート データ VLAN だけに表示されます。CDP を通じて学習したすべての IP 電話の MAC は、音声 VLAN で許容されます。
- MAB と VMPS の機能は重複しており、相互に排他的です。

アクセス不能認証バイパスを使用した 802.1X 認証の利用



(注) Supervisor Engine 6-E は、この機能をサポートしていません。

> スイッチが設定された RADIUS サーバに到達できないためにクライアント(サプリカント)が認証 されない場合、アクセス不能認証バイパスがイネーブルのクリティカルポートに接続するホストに ネットワークアクセスできるようにスイッチを設定できます。

> この機能がイネーブルの場合、スイッチは設定された RADIUS サーバのステータスをモニタしま す。使用できる RADIUS サーバがない場合、アクセス不能認証バイパスがイネーブルのポートは許 可されます。アクセス不能認証バイパス VLAN はポート ベースごとに設定できます。

> RADIUS が使用できなくなった時点で許可されているポートは、アクセス不能認証バイパスの影響 を受けません。ただし、再認証時に次のポーリング サイクルで RADIUS が復旧しない場合、すで に許可されているポートはクリティカル認証 VLAN に戻ります。

> RADIUS が使用できるようになると、クリティカル許可されたポートは、自動的に自分自身を再認 証するように設定されます。

> アクセス不能認証バイパスの設定方法については、「アクセス不能認証バイパスを使用した 802.1X 認証の設定」(p.37-37)を参照してください。

単方向制御ポートを使用した 802.1X 認証の利用



Supervisor Engine 6-E は、この機能をサポートしていません。

単方向制御ポートはハードウェアおよびソフトウェア機能が組み合わせられており、 マジック パ ケットと呼ばれる特別なイーサネット フレームを受信すると、休止 PC の電源を投入します。通常、 単方向制御ポートは、システムの電源が切断されていると考えられるような時間帯に管理者がリ モートシステムを管理する環境で使用されます。

802.1X ポート経由で接続されているホストで単方向制御ポートを使用した場合、ホストの電源が切 断されると 802.1X ポートが未認証になるという独特の問題が発生します。この場合、ポートでは EAPOL パケットだけしか送受信できません。このため単方向制御ポートのマジック パケットはホ ストに到達できず、電源を投入しないかぎり PC で認証することもポートを開くこともできません。

単方向制御ポートは、未許可802.1Xポートでパケットの送信を許容することにより、この問題を 解決します。



単方向制御ポートは、ポートのスパニング ツリー PortFast がイネーブルである場合のみ機能。

802.1X 単方向制御ポートの設定方法については、「単方向制御ポートを使用した 802.1X 認証の設 定」(p.37-40)を参照してください。

単方向ステート

dot1x control-direction in インターフェイス コンフィギュレーション コマンドを使用してポートを 単一方向に設定すると、そのポートはスパニングツリー フォワーディング ステートに移行します。

単方向制御ポートをイネーブルにすると、接続ホストはスリープ モードまたは電源切断状態になります。ホストはそのネットワークの他の装置とトラフィックを交換しません。ホストがネットワークにトラフィックを送信できない単方向ポートに接続されている場合、ホストはネットワークの他の装置からのトラフィックだけを受信します。

双方向ステート

dot1x control-direction both インターフェイス コンフィギュレーション コマンドを使用してポート を双方向に設定すると、ポートは両方向のアクセスを制御します。この場合、スイッチ ポートは EAPOL パケット以外のパケットを送受信をしません。

認証失敗 VLAN 割り当てを使用した 802.1X 認証の利用



Supervisor Engine 6-E は、この機能をサポートして*いません*。

ポート単位で認証失敗 VLAN 割り当てを使用すると、認証失敗ユーザがアクセスできるようにします。認証失敗ユーザは、802.1X には対応できるが認証サーバ内に有効なクレデンシャルを持たないエンド ホストか、またはユーザ側の認証ポップアップ ウィンドウでユーザ名とパスワードの組み合わせが入力されていないエンド ホストです。

ユーザが認証プロセスに失敗した場合、このポートは認証失敗 VLAN に置かれます。このポートは再認証タイマーが切れるまで、認証失敗 VLAN に残ります。再認証タイマーが切れると、スイッチはポート再認証要求の送信を開始します。ポートが再認証に失敗した場合は、認証失敗 VLAN に残ります。ポートが再認証に成功した場合は、RADIUS サーバにより送信された VLAN、または新たに認証されたポートに設定された VLAN に移動されます。移動先は、RADIUS サーバが VLAN 情報を送信するように設定されているかどうかによって異なります。



. 汗 ノ

定期的な再認証をイネーブルにする場合 (「定期的再認証のイネーブル化」[p.37-44] を参照) ローカル再認証タイマー値だけが使用できます。 RADIUS サーバを利用して再認証タイマー値を割り当てることはできません。

ポートが認証失敗 VLAN に移動される前に、オーセンティケータが送信する最大認証試行回数を設定できます。オーセンティケータは、各ポートの失敗した認証試行回数をカウントします。失敗した認証試行とは、空の応答または EAP 失敗のいずれかを指します。オーセンティケータは、認証試行回数に対して失敗した認証のすべての試行をまとめてカウントします。最大試行回数を超えると、ポートは再認証タイマーが次に切れるまで認証失敗 VLAN に置かれます。



(注)

EAP をサポートしない RADIUS は、EAP パケットを含まない応答を送信する場合があります。また、サードパーティ製の RADIUS サーバも空の応答を送信する場合があります。このような場合、認証試行カウンタは増加します。

認証失敗 VLAN 割り当てを設定する方法については、「認証失敗 VLAN 割り当てを使用した 802.1X 認証の設定」(p.37-41) を参照してください。

認証失敗 VLAN 割り当ての使用上の注意事項

- 再認証をイネーブルにする必要があります。再認証がディセーブルの場合、認証失敗 VLAN 内のポートは再認証試行を受け入れません。再認証プロセスを開始するには、認証失敗 VLAN がポートからのリンク ダウン イベントまたは EAP ログオフ イベントを受信する必要があります。ホストがハブの背後にある場合は、次の再認証が試行されるまでリンク ダウン イベントを受信しなかったり、新しいホストを検出しなかったりする可能性があります。したがって、このような場合は再認証をイネーブルにすることを推奨します。
- EAP 失敗メッセージは、ユーザに送信されません。ユーザが認証に失敗した場合、ポートは認証失敗 VLAN に移され、EAP 成功メッセージがユーザに送信されます。ユーザには認証失敗が通知されないため、ネットワークへのアクセスが制限される理由がわからない場合があります。EAP 成功メッセージが送信される理由は、次のとおりです。
 - EAP 成功メッセージが送信されなければ、ユーザは EAP 開始メッセージを送信して 60 秒 ごとに (デフォルト) 認証を試行します。
 - 場合によっては、ユーザが EAP 成功に DHCP を設定していて、成功を確認しないかぎりポート上で DHCP が稼働しないこともあります。
- ユーザはオーセンティケータから EAP 成功メッセージを受信したあと、不正なユーザ名とパスワードの組み合わせをキャッシュして、再認証ごとにこの情報を再利用する場合があります。ユーザが正確なユーザ名とパスワードの組み合わせを渡すまで、ポートは認証失敗 VLAN に残されます。
- 認証失敗ポートが無許可ステートに移行すると、認証プロセスが再開されます。再度認証プロセスに失敗する場合には、オーセンティケータは保留ステートで待機します。正しく再認証されると、すべての802.1X ポートは再度初期化され、通常の802.1X ポートとして扱われます。
- 認証失敗 VLAN を別の VLAN に再設定すると、認証失敗ポートもすべて移動され、ポートは現在の許可ステートのままになります。
- 認証失敗 VLAN をシャット ダウンするか、または VLAN データベースから削除すると、すべての認証失敗ポートはただちに無許可ステートに移行され、認証プロセスが再開されます。認証失敗 VLAN 設定がまだ存在するため、オーセンティケータは保留ステートで待機しません。認証失敗 VLAN が非アクティブである間は、すべての認証試行がカウントされ、VLAN がアクティブになるとすぐにポートは認証失敗 VLAN に置かれます。
- VLAN で許容される最大認証失敗数を再設定した場合、この変更は再認証タイマーが切れたあとで有効になります。
- レイヤ 3 ポートで使用されるすべての内部 VLAN は、認証失敗 VLAN として設定できません。
- 1 つの VLAN を認証失敗 VLAN と音声 VLAN の両方に設定することはできません。同時に設定すると、ポートが認証失敗 VLAN でアップになろうとするたびに Syslog メッセージが生成されます。
- 認証失敗 VLAN は、シングルホスト モード(デフォルトのポート モード)でのみサポートされます
- ポートが認証失敗 VLAN に置かれると、ユーザの MAC アドレスが MAC アドレス テーブルに 追加されます。ポートで新しい MAC アドレスが検出されると、セキュリティ違反として扱われます。
- 認証失敗ポートが認証失敗 VLAN に移動されると、Catalyst 4500 シリーズ スイッチは通常の802.1X 認証の場合とは異なり、RADIUS-Account Start メッセージを送信しません。

ポート セキュリティを使用した 802.1X 認証の利用

シングル ホスト モードまたは複数ホスト モードのどちらかの 802.1X ポートでポート セキュリティをイネーブルにできます(そのためには、switchport port-security インターフェイス コンフィギュレーション コマンドを使用して、ポート セキュリティを設定する必要があります。第 nb 章を参照)。ポート上のポート セキュリティと 802.1X をイネーブルにすると、802.1X がポートを認証し、ポート セキュリティがポート上で許容される MAC アドレス数(クライアントの MAC アドレスを含む)を管理します。したがって、ポート セキュリティがイネーブルの状態で 802.1X ポートを使用すると、ネットワークにアクセスできるクライアントの数とグループを制限できます。

マルチ ホスト モードの指定については、「802.1X 設定をデフォルト値にリセットする方法」 (p.37-50) を参照してください。

次に、スイッチ上の 802.1X とポート セキュリティ間の対話の例を示します。

• クライアントが認証されていて、ポート セキュリティ テーブルがフルでなければ、そのクライアントの MAC アドレスが、セキュア ホストのポート セキュリティ リストに追加されます。 そのあと、ポートが正常に起動します。

クライアントが認証されていて、手動でポート セキュリティが設定されている場合、ポート セキュリティはセキュア ホスト テーブルへのエントリが保証されます (ポート セキュリティの スタティック エージングがイネーブルになっている場合は除く)。

ポート上で別のホストが学習されると、セキュリティ違反が発生します。その場合に取られる処置は、セキュリティ違反を検出した機能(802.1X またはポート セキュリティ)によって異なります。

- 802.1X が違反を検出した場合は、ポートが errdisable になります。
- ポート セキュリティが違反を検出した場合は、ポートがシャットダウンするか、または制限されます(対処法は設定可能です)。

ポート セキュリティおよび 802.1X セキュリティ違反が発生した場合の説明を、次に示します。

- シングル ホスト モードの場合にポートが許可されると、クライアント MAC アドレス以外 の受信されたすべての MAC アドレスによって、802.1X セキュリティ違反が引き起こされ ます。
- シングル ホスト モードの場合に、(設定済みのセキュア MAC アドレスによって)ポート セキュリティが限度に達していることが原因で、802.1X クライアントの MAC アドレスの 導入に失敗すると、ポート セキュリティ違反が引き起こされます。
- マルチ ホスト モードの場合にポートが許可されると、ポート セキュリティが限度に達していることが原因で導入できない追加 MAC アドレスにより、ポート セキュリティ違反が引き起こされます。
- 802.1X クライアントがログオフすると、ポートが無許可ステートに移行し、クライアントのエントリを含むセキュア ホスト テーブル内のすべてのダイナミック エントリが削除されます。 そのあと、通常の認証が行われます。
- ポートが管理上のシャットダウン状態になると、ポートは無許可ステートになり、すべてのダイナミック エントリがセキュア ホスト テーブルから削除されます。
- ポート セキュリティ テーブルからクライアントの MAC アドレスを削除できるのは、802.1X のみです。マルチ ホスト モードでは、クライアントの MAC アドレスを除き、ポート セキュリティによって学習されたすべての MAC アドレスを、ポート セキュリティ CLI(コマンドライン インターフェイス)を使用して削除できます。
- ポート セキュリティによって 802.1X クライアントの MAC アドレスが期限切れになると、802.1X はクライアントの再認証を試行します。ポート セキュリティ テーブル内でクライアントの MAC アドレスを維持できるのは、再認証に成功した場合のみです。
- CLI を使用してポート セキュリティ テーブルを表示すると、802.1X クライアントのすべての MAC アドレスに [dot1x] というタグが付加されます。

RADIUS によるセッション タイムアウトを使用した 802.1X 認証の利用

スイッチで使用する再認証タイムアウトを、ローカルに設定されたものと RASIUD によるもののどちらにするかを指定できます。スイッチがローカル設定のタイムアウトを使用するように設定されている場合、タイマーが切れるとホストを再認証します。

スイッチがRADIUS によるセッションタイムアウトを使用するように設定されている場合、スイッチはRADIUS Access-Accept メッセージの Session-Timeout および任意の Termination-Action 属性を確認します。スイッチは、セッションの期間を判断するためには Session-Timeout 属性の値を使用し、セッションのタイマーが切れた際のスイッチのアクションを判断するためには Termination-Action 属性の値を使用します。

Termination-Action 属性が存在し、その値が [RADIUS-Request] である場合、スイッチはホストを再認証します。Termination-Action 属性が存在しないか、またはその値が [Default] である場合、スイッチはセッションを終了します。



(注)

ポート上のサプリカントは、そのセッションが終了され、新しいセッションを開始しようとすることを認識します。認証サーバがこの新しいセッションを別に処理しないかぎり、スイッチが新しいセッションを確立しても、クライアントはネットワーク接続に少しの割り込みしか確認しない可能性があります。

スイッチが RADIUS によるタイムアウトを使用するように設定されているが、Access-Accept メッセージに Session-Timeout 属性が含まれない場合、スイッチはサプリカントを再認証しません。これは、シスコのワイヤレス アクセス ポイントに一貫した動作です。

RADIUS によるセッション タイムアウトを設定する方法については、「RADIUS によるセッション タイムアウトの設定」(p.37-31) を参照してください。

RADIUS アカウンティングを使用した 802.1X 認証の利用



(注)

Supervisor Engine 6-E は、この機能をサポートして*いません*。



(注)

システム全体にアカウンティングを実装する場合は、802.1X アカウンティングも設定する必要があります。さらに、システムのリロード時にシステム リロード イベントをアカウンティング サーバに通知する必要もあります。これにより、アカウンティング サーバは、このシステム上のすべての未処理 802.1X セッションが終了していることを確認できます。



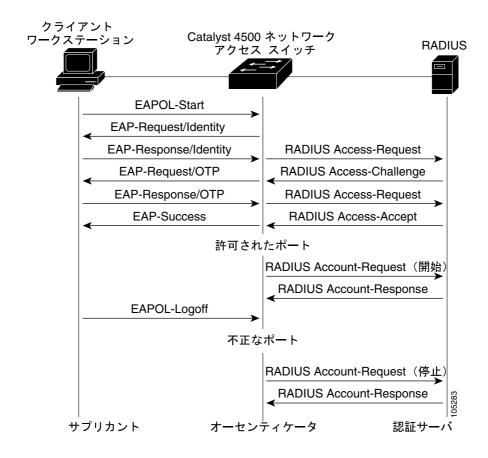
(注)

802.1X アカウンティングをイネーブルにするには、最初に 802.1X 認証を設定し、スイッチから RADIUS サーバへの通信を設定する必要があります。

802.1X RADIUS アカウンティングは重要なイベント (クライアントの接続セッションなど)を RADIUS サーバにリレーします。このセッションは、クライアントがポートの使用を許可された時点から、クライアントがポートの使用を停止した時点までの間隔として定義されます。

図 37-6 に RADIUS アカウンティング プロセスを示します。

図 37-6 RADIUS アカウンティング





ユーザがログオフしたときに、EAP-Logoff (Stop) メッセージをスイッチに送信するように 802.1X クライアントを設定する必要があります。このように 802.1X クライアントを設定しないと、EAP-Logoff メッセージはスイッチに送信されず、付随する Stop メッセージが認証サーバに送信されません。次の URL で「Microsoft Knowledge Base Article」の資料を参照してください。 http://support.microsoft.com

また、次の URL の Microsoft の資料も参照してください。 http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/cableguy/cg0703.asp

そして SupplicantMode レジストリを 3 に、AuthMode レジストリを 1 に設定してください。

クライアントが認証されると、スイッチはアカウンティング要求パケットを RADIUS サーバに送信します。RADIUS サーバはアカウンティング応答パケットで応答して、要求受領に確認応答を行います。

RADIUS アカウンティング要求パケットには、各種イベントおよび関連情報を RADIUS サーバにレポートするための Attribute/Value ペアが 1 つ以上格納されます。追跡されるイベントは、次のとおりです。

- ユーザの正常な認証
- ユーザのログオフ
- 802.1X ポートで発生したリンクダウン
- 再認証の成功
- 再認証の失敗

ポートが許可ステートから無許可ステートに移行すると、RADIUS メッセージが RADIUS サーバに送信されます。

スイッチはアカウンティング情報を記録しないで、RADIUS サーバに送信します。RADIUS サーバは、アカウンティング メッセージを記録するように設定する必要があります。

802.1X の認証、許可、およびアカウンティング プロセスは、次のとおりです。

- **ステップ1** ユーザがスイッチのポートに接続します。
- **ステップ2** ユーザ名 / パスワード方式などを使用して、認証が実行されます。
- ステップ3 必要に応じて、RADIUS サーバ設定ごとに、VLAN 割り当てがイネーブルになります。
- **ステップ4** スイッチがアカウンティング サーバに Start メッセージを送信します。
- ステップ 5 必要に応じて、再認証が実行されます。
- **ステップ6** スイッチが、再認証の結果に基づく内部アカウンティング アップデートをアカウンティング サーバに送信します。
- **ステップ7** ユーザがポートから切断します。
- ステップ8 スイッチがアカウンティング サーバに Stop メッセージを送信します。

802.1X アカウンティングを設定するには、次の作業を実行する必要があります。

- RADIUS サーバの Network Configuration タブで、[Update/Watchdog packets from this AAA client] のロギングをイネーブルにします。
- RADIUS サーバの System Configuration タブで、[Logging>CVS RADIUS Accounting] をイネーブルにします。
- スイッチ上で 802.1X アカウンティングをイネーブルにします。
- aaa system accounting コマンドを使用して、AAA アカウンティングをイネーブルにします。「802.1X RADIUS アカウンティングのイネーブル化」(p.37-32)を参照してください。

802.1X アカウンティングとともに AAA システム アカウンティングをイネーブルにすると、システム リロード イベントをアカウンティング RADIUS サーバに送信して、記録できます。これにより、アカウンティング RADIUS サーバは、すべてのアクティブな 802.1X セッションが適切に終了すると推測します。

RADIUS は信頼性のないトランスポート プロトコルである UDP を使用するため、ネットワーク状態が悪い場合は、アカウンティング メッセージが失われることがあります。設定可能な回数だけアカウンティング要求を再送信しても、スイッチが RADIUS サーバからアカウンティング応答メッセージを受信しない場合は、次のシステム メッセージが表示されます。

Accounting message %s for session %s failed to receive Accounting Response.

Stop メッセージが正常に送信されない場合は、次のメッセージが表示されます。

00:09:55: %RADIUS-3-NOACCOUNTINGRESPONSE: Accounting message Start for session 172.20.50.145 sam 11/06/03 07:01:16 11000002 failed to receive Accounting Response.

アカウンティング応答メッセージを受信しない RADIUS メッセージ数を表示するには、show radius statistics コマンドを使用します。

音声 VLAN ポートを使用した 802.1X 認証の利用

音声 VLAN ポートは、次の2つの VLAN 識別子で関連付けられる特殊なアクセス ポートです。

- IP Phone へ、または IP Phone から音声トラフィックを伝送するための Voice VLAN ID(VVID)。 VVID は、ポートに接続された IP Phone を設定するのに使用します。
- IP Phone 経由でスイッチに接続されたワークステーションへ、またはワークステーションから データ トラフィックを伝送する Port VLAN ID (PVID)。PVID はポートのネイティブ VLAN です。

音声 VLAN に設定する各ポートは、VVID および PVID に関連付けられています。この設定により、 音声トラフィックとデータ トラフィックを異なる VLAN に分離できます。

ポートが AUTHORIZED か UNAUTHORIZED かにかかわらずリンクがある場合、音声 VLAN ポートはアクティブになります。音声 VLAN を介するすべてのトラフィックは正常に認識され、MAC アドレス テーブルに表示されます。Cisco IP Phone は他のデバイスから Cisco Discovery Protocol (CDP; シスコ検出プロトコル) メッセージをリレーしません。その結果、いくつかの Cisco IP Phone がシリーズで接続されている場合、スイッチは直接接続している IP Phone のみを認識します。802.1X が音声 VLAN ポートでイネーブルの場合、スイッチは複数のホップの認識されていない Cisco IP Phone からのパケットをドロップします。

802.1X がポートでイネーブルの場合、VVID と同じ PVID を設定できません。音声 VLAN については、第 35 章「音声インターフェイスの設定」を参照してください。

次の機能の相互作用に注意してください。

- 802.1X VLAN 割り当ては、音声 VLAN と同じ VLAN のポートに割り当てることができません。 割り当てると 802.1X 認証が失敗します。
- 802.1X ゲスト VLAN は、802.1X 音声 VLAN ポート機能と連動します。ただし、同一 VLAN を ゲスト VLAN と音声 VLAN には設定できません。
- 802.1X ポート セキュリティは 802.1X 音声 VLAN ポート機能と連動し、ポート単位で設定されます。2 つの MAC アドレスを設定する必要があります。1 つは VVID の Cisco IP Phone MAC アドレス、もう 1 つは PVID の PC MAC アドレスです。

ただし、 $802.1~\rm X$ ポート セキュリティのスティッキ MAC アドレス設定および $802.1\rm X$ ポート セキュリティのスタティックに設定された MAC アドレス設定と一緒に、 $802.1\rm X$ 音声 VLAN ポート機能を使用することはできません。

- 802.1X アカウンティングは、802.1X 音声 VLAN ポート機能による影響を受けません。
- 802.1X がポート上で設定されている場合、ハブを介して複数の IP Phone を Catalyst 4500 シリーズ スイッチに接続することはできません。

• 音声 VLAN は PVLAN のホスト ポートとして設定できず、PVLAN のホスト ポートに割り当てられるのは PVLAN だけであるため、VLAN 割り当てでは音声 VLAN が設定されたポートに PVLAN を割り当てることができません。

音声 VLAN に 802.1X を設定する方法については、「音声 VLAN に対する 802.1X 認証の設定」 (p.37-43) を参照してください。

複数ドメイン認証の使用

MDA は、データ デバイスと IP Phone(Cisco または Cisco 以外)などの音声デバイスの両方が、データ ドメインと音声ドメインに分割される同一スイッチ ポートで認証できるようにします。

MDA は、デバイス認証の順番を強制しません。ただし、最適な結果を得るには、MDA 対応ポートで、データ デバイスを認証する前に音声デバイスを認証する必要があります。

MDA の設定には、次の注意事項を参考にしてください。

- DoS 攻撃 (サービス拒絶攻撃)を防ぐために MDA 対応ポートで CoPP をイネーブルにすることを強く推奨します。第 39 章「コントロール プレーン ポリシングの設定」を参照してください。
- MDA に対してスイッチ ポートを設定するには、「複数ドメイン認証の設定」(p.37-28)を参照してください。
- ホスト モードがマルチドメインに設定されているときは、IP Phone の音声 VLAN を設定する必要があります。詳細については、第 35 章 「音声インターフェイスの設定」を参照してください。



(注)

ダイナミック VLAN を使用して MDA 対応スイッチ ポートに音声 VLAN を割り当てると、音声デバイスは認証に失敗します。

- 音声デバイスを許可するには、AAA サーバが Cisco Attribute-Value (AV) ペア属性を device-traffic-class=voice にして送信するように設定する必要があります。この値がない と、スイッチは音声デバイスをデータ デバイスとして扱います。
- ゲスト VLAN および制限された VLAN 機能は、MDA 対応ポートのデータ デバイスにのみ適用 されます。 スイッチは、 認証に失敗した音声デバイスをデータ デバイスとして扱います。
- 複数のデバイスが、ポートの音声ドメインまたはデータドメインのいずれかで認証を試行する場合、errdisableです。
- デバイスが認証されるまで、ポートはそのトラフィックをドロップします。Cisco 以外の IP 電話または音声デバイスは、データ VLAN と音声 VLAN の両方で許可されます。データ VLAN により、音声デバイスは DHCP サーバに接続し、IP アドレスを取得して音声 VLAN 情報を入手できます。音声デバイスが音声 VLAN での送信を開始したあと、データ VLAN へのアクセスはブロックされます。
- RADIUS サーバからのダイナミック VLAN 割り当ては、データ デバイスに対してのみ使用できます。
- MDA はフォールバック メカニズムとして MAC 認証バイパスを使用して、スイッチ ポートが 802.1X 認証をサポートしないデバイスに接続できるようにします。これは特に 802.1X サプリカントのないサードパーティ電話で役立ちます。詳細については、「MAC 認証バイパスを使用した 802.1X 認証の利用」(p.37-10) を参照してください。
- *データ*または*音声*デバイスがポート上で検出されると、その MAC アドレスは認証が正常に完了するまでブロックされます。認証が失敗した場合、MAC アドレスは 5 分間ブロックされたままになります。
- データVLAN で複数のデバイスが検出された場合、またはポートが許可されていないときに*音* 声VLAN で複数の音声デバイスが検出された場合、そのポートは errdisable になります。

- ポートのホスト モードが単一モードからマルチドメイン モードに変更されると、許可された データ デバイスはポート上で許可されたままとなります。ただし、音声 VLAN のポートで許 可されている Cisco IP Phone は自動的に削除されるので、そのポート上で再認証される必要が あります。
- ゲスト VLAN および制限 VLAN などのアクティブ フォールバック メカニズムは、ポートが単一またはマルチホスト モードからマルチドメイン モードに変更されたあとも設定済みのままになります。
- ポートのホスト モードをマルチドメイン モードから単一またはマルチホスト モードに切り替えると、許可されたすべてのデバイスがポートから削除されます。
- データドメインが最初に許可され、ゲスト VLAN に設定された場合、非 802.1X 対応音声デバイスは音声 VLAN のパケットにタグを付け、認証をトリガーする必要があります。
- MDA 対応ポートを使用したユーザ単位の ACL は推奨しません。ユーザ単位 ACL ポリシーを 持つ許可されたデバイスは、ポートの音声 VLAN およびデータ VLAN の両方のトラフィック に影響を与えることがあります。使用する場合、ポート上の 1 つのデバイスだけが、ユーザ単 位 ACL を強制する必要があります。

サポート対象トポロジ

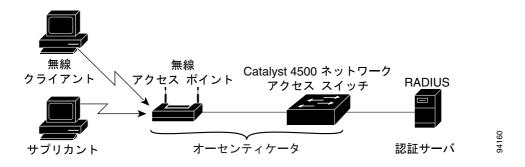
802.1X ポートベースの認証は、次の 2 つのトポロジをサポートします。

- ポイントツーポイント
- 無線 LAN

ポイントツーポイント構成(図 37-1 [p.37-3] を参照)では、マルチホスト モードがイネーブルでない場合(デフォルト) 802.1X 対応スイッチ ポートに接続できるクライアントは1台だけです。スイッチは、ポートのリンク ステートがアップ ステートに変化すると、クライアントを検出します。クライアントが脱退するか、別のクライアントに交換されると、スイッチはポートのリンク ステートをダウンに変更し、ポートは無許可ステートに戻ります。

ワイヤレス LAN の 802.1X ポートベース認証(図 37-7)では、クライアントが認証されるとすぐに ワイヤレス アクセス ポイントとして認証される 802.1X ポートを複数ホスト ポートとして設定します(「802.1X 設定をデフォルト値にリセットする方法」[p.37-50]を参照)。ポートが許可される と、ポートに間接的に接続されたホストを除くすべてのホストに対して、ネットワーク アクセスが 許可されます。ポートが無許可になると(再認証が失敗するか、EAPOL-Logoff メッセージを受信すると)、スイッチは、無線アクセス ポイントに接続されたすべてのクライアントに対してネット ワーク アクセスを拒否します。このトポロジでは、無線アクセス ポイントは、接続しているクライアントを認証する役割があり、スイッチに対してクライアントとして機能します。

図 37-7 無線 LAN の例



802.1X の設定

802.1X を設定する手順は次のとおりです。

- ステップ 1 802.1X 認証をイネーブルにします「802.1X 認証のイネーブル化」(p.37-24) を参照してください。
- ステップ2 スイッチ /RADIUS サーバ通信を設定します。「スイッチ /RADIUS サーバ通信の設定」(p.37-26)を 参照してください。
- ステップ3 802.1X タイマー値を調整します。「待機時間の変更」(p.37-46)を参照してください。
- **ステップ4** 任意の機能を設定します。「RADIUS によるセッション タイムアウトの設定」(p.37-31)を参照してください。

ここでは、802.1Xを設定する方法について説明します。

- 802.1X のデフォルト設定 (p.37-23)
- 802.1X 設定時の注意事項(p.37-23)
- 802.1X 認証のイネーブル化 (p.37-24)(必須)
- スイッチ /RADIUS サーバ通信の設定 (p.37-26)(必須)
- 複数ドメイン認証の設定 (p.37-28)
- RADIUS によるセッション タイムアウトの設定 (p.37-31)(任意)
- 802.1X RADIUS アカウンティングのイネーブル化 (p.37-32)(任意)
- ゲスト VLAN を使用した 802.1X 認証の設定 (p.37-33)(任意)
- MAC 認証バイパスを使用した 802.1X 認証の設定 (p.37-36)(任意)
- アクセス不能認証バイパスを使用した 802.1X 認証の設定 (p.37-37)(任意)
- 単方向制御ポートを使用した 802.1X 認証の設定 (p.37-40)(任意)
- 認証失敗 VLAN 割り当てを使用した 802.1X 認証の設定 (p.37-41)(任意)
- 音声 VLAN に対する 802.1X 認証の設定 (p.37-43)(任意)
- 定期的再認証のイネーブル化 (p.37-44)(任意)
- 複数ホストのイネーブル化 (p.37-45)(任意)
- 待機時間の変更 (p.37-46)(任意)
- スイッチ / クライアント間の再送信時間の変更 (p.37-47)(任意)
- スイッチ / クライアント間のフレーム再送信回数の設定 (p.37-48)(任意)
- 手動によるポート接続クライアントの再認証 (p.37-49)(任意)
- 802.1X 認証ステートの初期化 (p.37-50)
- 802.1X クライアント情報の削除 (p.37-50)
- 802.1X 設定をデフォルト値にリセットする方法 (p.37-50)(任意)

802.1X のデフォルト設定

表 37-1 に、802.1X のデフォルト設定を示します。

表 37-1 802.1X のデフォルト設定

機能	プフォルト設定
AAA	ディセーブル
RADIUS サーバ	
IP アドレス	指定なし
UDP 認証ポート	• 1812
• +-	指定なし
インターフェイス単位の 802.1X プロトコル	強制認証
イネーブル ステート	ポートは、クライアントの 802.1X ベース認証なしで通常のトラフィックを送受信します。
定期的再認証	ディセーブル
再認証の試行間隔	3600 秒
待機時間	60 秒
	クライアントとの認証交換が失敗したあと、スイッチが待機ステートに ある秒数です。
再送信時間	30 秒
	要求を再送信するまでに、スイッチがクライアントからの
	EAP-Request/Identity フレームに対する応答を待機する秒数です。
最大再送信回数	2
	認証プロセスを再開するまでにスイッチが EAP-Request/Identity フレームを送信する回数です。
複数ホストのサポート	ディセーブル
クライアントのタイムアウト時間	30 秒
	認証サーバからの要求をクライアントにリレーするとき、クライアント に要求を再送信するまでにスイッチが応答を待機する時間です。
認証サーバのタイムアウト時間	30 秒
	クライアントの応答を認証サーバにリレーするとき、サーバに応答を再送信するまでにスイッチが応答を待機する時間です。この値は設定不可能です。

802.1X 設定時の注意事項

802.1X 認証を設定する場合の注意事項は次のとおりです。

- 802.1X プロトコルは、レイヤ 2 スタティック アクセス、プライベート LAN ホスト ポート、およびレイヤ 3 ルーテッド ポートでのみサポートされます。その他のポート モードには 802.1X を設定できません。
- 802.1X アカウンティングまたは VLAN 割り当てのどちらかを使用する場合は、両方の機能で 一般的な AAA コマンドが利用されることに留意してください。AAA の設定については、「802.1X 認証のイネーブル化」(p.37-24)を参照してください。または、Cisco IOS セキュリティ に関する次のマニュアルを参照してください。
 - http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/fsecur_c/index.htm
 - http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/fsecur_r/index.htm

802.1X 認証のイネーブル化

802.1X ポート ベース認証をイネーブルにするには、まずスイッチ上で 802.1X をグローバルにイネーブルにしてから、AAA をイネーブルにし、認証方式リストを指定する必要があります。方式リストは、ユーザ認証のためクエリー送信を行う手順と認証方式を記述したものです。

ソフトウェアは、方式リスト内の最初の方式を使用してユーザを認証します。その方式で応答が得られなかった場合、ソフトウェアはそのリスト内の次の認証方式を選択します。このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式を使い果たすまで続きます。このサイクルのどこかのポイントで認証が失敗すると、認証プロセスは停止し、他の認証方式は試行されません。



VLAN 割り当てを可能にするには、AAA 許可をイネーブルにして、ネットワーク関連のすべてのサービス要求に対応するようにスイッチを設定する必要があります。

802.1X ポートベース認証を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<pre>Switch(config)# dot1x system-auth-control</pre>	スイッチ上で 802.1X をイネーブルにします。
		スイッチ上で 802.1X をグローバルにディセーブルにする には、no dot1x system-auth-control コマンドを使用します。
ステップ 3	Switch(config)# aaa new-model	AAA をイネーブルにします。
		AAA をディセーブルにするには、no aaa new-model コマンドを使用します。
ステップ 4	Switch(config)# aaa authentication dot1x {default} method1 [method2]	802.1X AAA 認証方式リストを作成します。
		authentication コマンドに名前付きリストが指定されない場合に使用されるデフォルトのリストを作成するには、defaultキーワードの後ろにデフォルトの状況で使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのインターフェイスに適用されます。
		次のキーワードを少なくとも1つ入力します。
		• group radius すべての RADIUS サーバのリストを認証に使用します。
		• none 認証を使用しません。クライアントは、クライアントが提供する情報を使用しないで、スイッチによって自動的に認証されます。
		802.1X AAA 認証をディセーブルにするには、 no aaa authentication dot1x { default <i>list-name</i> } <i>method1</i> [<i>method2</i>] グローバル コンフィギュレーション コマンドを使用します。
ステップ 5	<pre>Switch(config)# aaa authorization network {default} group radius</pre>	(任意)ネットワーク関連のすべてのサービス要求 (VLAN割り当てなど)に対するユーザ RADIUS 許可を、スイッチに設定します。

	コマンド	目的
ステップ 6	Switch(config)# interface interface-id	インターフェイス コンフィギュレーション モードを開始し、802.1X 認証をイネーブルにするインターフェイスを 指定します。
ステップ 7	Switch(config-if)# switchport mode access	非トランキング、タグなし単一 VLAN レイヤ 2 インターフェイスを指定します。
ステップ 8	<pre>Switch(config-if)# dot1x pae authenticator</pre>	ポート上でデフォルト設定の 802.1X 認証をイネーブルに します。 「802.1X のデフォルト設定」(p.37-23)を参照してください。
ステップ 9	Switch(config-if)# dot1x port-control auto	インターフェイス上で、802.1X 認証をイネーブルにします。
ステップ 10	Switch(config-if)# end	特権 EXEC モードに戻ります。
ステップ 11	Switch # show dot1x interface interface-id details	入力を確認します。 この出力の 802.1X ポート サマリー セクションの PortControl 行を調べます。PortControl 値は auto に設定され ています。
ステップ 12	Switch# show running-config	入力を確認します。
ステップ 13	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。



スパニング ツリー PortFast をイネーブルにすると、許可直後にポートが必ずアップになります。



(注)

ポートに任意の802.1X パラメータを設定すると、ポート上に802.1X 認証が自動的に作成されます。 結果的に、設定に dot1x pae authenticator が表示されます。手動での操作を行わずに、802.1X 認証 をレガシー コンフィギュレーション上でそのまま実行することができます。これは、今後のリリー スで変更される可能性があります。 次に、ポート FastEthernet 2/1 で 802.1X と AAA をイネーブルにし、設定を確認する例を示します。

```
Switch# configure terminal
Switch(config) # dot1x system-auth-control
Switch(config)# aaa new-model
Switch(config) # aaa authentication dot1x default group radius
Switch(config) # interface fastethernet2/1
Switch(config-if) # switchport mode access
Switch(config-if) # dot1x pae authenticator
Switch(config-if) # dot1x port-control auto
Switch(config-if)# end
Switch# show dot1x interface f7/1 details
Dot1x Info for FastEthernet7/1
______
PAE
                        = AUTHENTICATOR
Port.Cont.rol
                        = AUTO
                       = Both
= SINGLE_HOST
ControlDirection
HostMode
                       = Disabled
ReAuthentication
OuietPeriod
                        = 60
ServerTimeout
                        = 30
SuppTimeout
                        = 30
                       = 3600 (Locally configured)
ReAuthPeriod
ReAuthMax
                        = 2
MaxReq
                        = 2.
TxPeriod
RateLimitPeriod
Dot1x Authenticator Client List
Supplicant
                        = 1000.0000.2e00
       Auth SM State = AUTHENTICATED
       Auth BEND SM Stat = IDLE
Port Status
                        = AUTHORIZED
Authentication Method
                        = Dot1x
Authorized By
                       = Authentication Server
Vlan Policy
                        = N/A
```

スイッチ/RADIUS サーバ通信の設定

RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と各 UDP ポート番号、あるいは IP アドレスと各 UDP ポート番号で識別します。IP アドレスと UDP ポート番号の組み合わせにより、一意の識別子が作成され、これにより、RADIUS 要求を同一 IP アドレスのサーバ上にある複数の UDP ポートに送信できます。同じ RADIUS サーバ上の 2 つの異なるホスト エントリが同じサービス (認証など)に対して設定されている場合、2 番めに設定されたホスト エントリは、最初のエントリのフェールオーバー時のバックアップとして機能します。RADIUS のホストエントリは、設定された順序で試行されます。

スイッチ上で RADIUS サーバ パラメータを設定するには、次の作業を行います。

コマンド 目的 ステップ 1 Switch# configure terminal グローバル コンフィギュレーション モードを開始します。 ステップ 2 Switch(config)# radius-server host スイッチ上に RADIUS サーバ パラメータを設定します。 {hostname | ip-address} auth-port port-number [acct-port port-number] hostname | ip-address には、リモート RADIUS サーバのホス [test username name] [ignore-auth-port] ト名または IP アドレスを指定します。 [ignore-acct-port] [idle-time min] key strina 指定された RADIUS サーバを削除するには、 **no radius-server host** {hostname | ip-address} グローバル コン フィギュレーション コマンドを使用します。 auth-port port-number には、認証要求のための UDP 宛先 ポートを指定します。デフォルトは 1812 です。 acct-port port-number には、アカウンティング要求の UDP 宛先ポートを指定します。デフォルトは 1813 です。 RADIUS サーバの自動テストをイネーブルにし、RADIUS サーバのアップとダウンを検出するには、test username name を使用します。name パラメータはテスト アクセス要 求で使用するユーザ名で、RADIUS サーバに送信されます。 サーバに設定されている有効なユーザである必要はありま せん。ignore-auth-port オプションと ignore-acct-port オプ ションを使用すると、認証ポートとアカウンティング ポー トのテストをそれぞれディセーブルにします。 idle-time min パラメータには、アイドル状態の RADIUS サーバがまだアップであることを確認するまでの時間を分 単位で指定します。デフォルトは60分です。 key string には、スイッチと RADIUS サーバ上で稼働する RADIUS デーモンとの間で使用する認証および暗号化キー を指定します。キーは、RADIUS サーバ上で使用する暗号 化キーと一致する必要のある文字列です。 (注) キーの先行スペースは無視されますが、キーの内部 および終わりのスペースは有効であるため、キーは 必ず radius-server host コマンド構文の最後の項目 として設定してください。キーにスペースを使用す る場合は、キーの一部として引用符を使用する場合 を除いて、キーを引用符で囲まないでください。こ のキーは、RADIUS デーモン上で使用する暗号と一 致する必要があります。 RADIUS サーバを複数使用する場合は、このコマンドを繰 り返し使用してください。 ステップ 3 Switch(config-if)# radius deadtime min (任意)ダウンしていた RADIUS サーバがアップしたかど うかをテストするまでの時間を分単位で指定します。デ フォルトは1分です。

	コマンド	目的
ステップ 4	Switch(config-if)# radius dead-criteria time seconds tries num	(任意)RADIUS サーバがダウンしているかどうかを判断する基準を設定します。time パラメータには、サーバへの要求に応答がなくなってからサーバがダウンと判断されるまでの時間を秒単位で指定します。tries パラメータには、サーバがダウンと判断されるまでにサーバへの要求に応答がない回数を指定します。 これらのパラメータの推奨値は、radius-server retransmitに等しい tries および radius-server retransmit x
		radius-server timeout に等しい time です。
ステップ 5	<pre>Switch(config-if)# ip radius source-interface m/p</pre>	すべての発信 RADIUS パケットの送信元アドレスとして使用する IP アドレスを確立します。
ステップ 6	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 7	Switch# show running-config	入力を確認します。
ステップ 8	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

次に、IP アドレスが 172.120.39.46 であるサーバを RADIUS サーバとして指定する例を示します。最初のコマンドはポート 1612 を認証ポートとして指定し、暗号化キーを rad123 に設定します。

2番めのコマンドは、RADIUSサーバ上でキーを照合するように指定します。

Switch# configure terminal

Switch(config) # radius-server host 172.120.39.46 auth-port 1612 key rad123

Switch(config)# ip radius source-interface m/p

Switch(config)# end

Switch#

radius-server host グローバル コンフィギュレーション コマンドを使用すると、すべての RADIUS サーバに対してタイムアウト、再送信、および暗号化キーの値をグローバルに設定できます。サーバ単位でこれらのオプションを設定する場合は、radius-server timeout、radius-server retransmit、および radius-server key グローバル コンフィギュレーション コマンドを使用します。

さらに、RADIUS サーバでいくつかの設定を行う必要があります。この設定には、スイッチの IP アドレス、およびサーバとスイッチで共用するキー文字列などがあります。

複数ドメイン認証の設定

MDA を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# radius-server vsa send authentication	ネットワーク アクセス サーバが、ベンダー固有の属性 (VSA) を認識して使用するように設定します。
ステップ 3	Switch(config)# interface interface-id	複数ホストが間接的に接続されているポートを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 4	<pre>Switch(config-if)# [no] dot1x host-mode {single-host multi-host multi-domain}</pre>	キーワードの意味は次のとおりです。
		• single-host IEEE 802.1X 許可ポートの単一ホスト(クライアント)を許可します。
		• multi-host 単一ホストの認証後に 802.1X 許可ポート の複数ホストを許可します。
	• multi-domain ホストおよび IP Phone (Cisco または Cisco 以外)などの音声デバイスの両方が、IEEE 802.1X 許可ポートで認証されるようにします。	
		(注) ホスト モードがマルチドメインに設定されているときは、IP Phone の音声 VLAN を設定する必要があります。詳細については、第 35 章 「音声インターフェイスの設定」を参照してください。
		指定されたインターフェイスについて、dot1x port-control
		インターフェイス コンフィギュレーション コマンドが auto に設定されていることを確認します。
		ポート上の複数のホストをディセーブルにするには、no dot1x multiple-hosts インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 5	Switch(config-if)# switchport voice vlan vlan-id	(任意)音声 VLAN を設定します。
ステップ 6	Switch(config-if)# end	特権 EXEC モードに戻ります。
ステップ 7	Switch# show dot1x interface interface-id [detail]	入力を確認します。
ステップ 8	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

次に、802.1X 認証をイネーブルにし、複数ホストを許可する例を示します。

```
Switch(config) # interface gigabitethernet2/1
Switch(config-if) # dot1x port-control auto
Switch(config-if) # dot1x host-mode multi-host
Switch(config-if) # end
```

次に、MDA をイネーブルにし、ポート上でホストと 802.1X 音声デバイス (802.1X サプリカントを持つ Cisco またはサードパーティ電話など) の両方を許可する例を示します。

```
Switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface FastEthernet3/1
Switch(config-if)# shut
Switch(config-if)# switchport access vlan 12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 10
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-domain
Switch(config-if)# no shut
Switch(config-if)# end
```

次に、MDA をイネーブルにし、ポート上でホストと 802.1X 以外の音声デバイスを許可する例を示します。

```
Switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface FastEthernet3/1
Switch(config-if)# shut
Switch(config-if)# switchport access vlan 12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 10
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-domain
Switch(config-if)# dot1x mac-auth-bypass
Switch(config-if)# no shut
Switch(config-if)# end
```

次に、インターフェイス FastEthernet6/1 での dot1x MDA 設定を確認する例を示します。

Switch# show dot1x interface FastEthernet3/1 detail

```
Dot1x Info for FastEthernet3/1
PAE
                        = AUTHENTICATOR
                        = AUTO
= Both
PortControl
ControlDirection
                        = MULTI_DOMAIN
HostMode
                        = Disabled
ReAuthentication
OuietPeriod
                        = 60
ServerTimeout
                         = 30
SuppTimeout
                         = 30
                        = 3600 (Locally configured)
ReAuthPeriod
ReAuthMax
                        = 2
MaxReq
TxPeriod
RateLimitPeriod
Dot1x Authenticator Client List
Domain
       ant = 0000.0000.ab01
Auth SM State = AUTHENTICATED
Supplicant
       Auth BEND SM Stat = IDLE
Port Status
                        = AUTHORIZED
Authentication Method
                        = Dot1x
                        = Authentication Server
Authorized By
Vlan Policy
                        = 12
                         = VOICE
                        = 0060.b057.4687
Supplicant
       Auth SM State = AUTHENTICATED
       Auth BEND SM Stat = IDLE
                        = AUTHORIZED
Port Status
Authentication Method
                        = Dot1x
                        = Authentication Server
Authorized By
Switch#
```

RADIUS によるセッション タイムアウトの設定

Catalyst 4500 シリーズ スイッチでは、RADIUS による再認証タイムアウトを使用するように設定できます。

RADIUS によるタイムアウトを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	Switch(config)# interface interface-id	インターフェイス コンフィギュレーション モー ドを開始します。
ステップ 3	Switch(config-if)# switchport mode access	非トランキング、タグなし単一 VLAN レイヤ 2 インターフェイスを指定します。
ステップ 4	Switch(config-if)# dot1x pae authenticator	ポート上でデフォルト設定の 802.1X 認証をイネー ブルにします。 「802.1X のデフォルト設定」(p.37-23)を参照してく
		ださい。
ステップ 5	Switch(config-if)# dot1x timeout reauth-period {interface/server}	再認証時間(秒)を設定します。
ステップ 6	Switch(config-if)# end	特権 EXEC モードに戻ります。
ステップ 7	Switch# show dot1x interface interface-id details	入力を確認します。
ステップ 8	Switch # copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を 保存します。

次に、スイッチがサーバから再認証時間を取得するように設定し、設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# interface f7/1
Switch(config-if) # switchport mode access
Switch(config-if) # dot1x pae authenticator
Switch(config-if)# dot1x timeout reauth-period server
Switch(config-if)# end
Switch# show dot1x interface f7/1 det
Dot1x Info for FastEthernet7/11
                        = AUTHENTICATOR
PortControl
                        = FORCE_AUTHORIZED
ControlDirection
                        = Both
HostMode
                         = SINGLE_HOST
                        = Disabled
ReAuthentication
QuietPeriod
                        = 60
                        = 30
ServerTimeout
SuppTimeout
                         = 30
                        = (From Authentication Server)
ReAuthPeriod
ReAuthMax
MaxReq
                         = 2
TxPeriod
                         = 30
RateLimitPeriod
Dot1x Authenticator Client List Empty
Port Status
                         = AUTHORIZED
Switch#
```

802.1X RADIUS アカウンティングのイネーブル化



Supervisor Engine 6-E は、この機能をサポートして*いません*。

802.1X アカウンティングを設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	Switch(config)# aaa accounting dot1x default start-stop group radius	全 RADIUS サーバのリストを使用して、802.1X アカウンティングをイネーブルにします。
ステップ 3	Switch(config)# clock timezone PST -8	アカウンティングのイベントタイム スタンプ フィールドで使用するタイム ゾーンを設定します。
ステップ 4	Switch(config)# clock calendar-valid	アカウンティングのイベントタイム スタンプ フィールドの日付をイネーブルにします。
ステップ 5	Switch(config)# aaa accounting system default start-stop group radius	(任意)システム アカウンティングをイネーブルに して (全 RADIUS サーバのリストを使用)、スイッ チのリロード時にシステム アカウンティング リ ロード イベント メッセージを生成します。
ステップ 6	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 7	Switch# show running-config	入力を確認します。
ステップ 8	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を 保存します。

次に、IP アドレスが 172.120.39.46 であるサーバを RADIUS サーバとして指定する例を示します。 最 初のコマンドは RADIUS サーバを設定し、ポート 1612 を認証ポートに、1813 をアカウンティング 用の UDP ポートに、rad123 を暗号キーに指定します。

Switch# configure terminal

Switch(config) # radius-server host 172.120.39.46 auth-port 1812 acct-port 1813 key rad123

Switch(config) # aaa accounting dot1x default start-stop group radius Switch(config)# aaa accounting system default start-stop group radius Switch(config) # end

Switch#



ロギングの開始、停止、および暫定更新メッセージとタイムスタンプなどのアカウンティング動作 を実行するように、RADIUS サーバを設定する必要があります。これらの機能を有効にするには、 RADIUS サーバの Network Configuration タブで、[Update/Watchdog packets from this AAA client] のロ ギングをイネーブルにします。次に、RADIUS サーバの System Configuration タブで、[CVS RADIUS Accounting] をイネーブルにします。

ゲスト VLAN を使用した 802.1X 認証の設定



(注) Supervisor Engine 6-E は、この機能をサポートしていません。

Catalyst 4500 シリーズ スイッチの各 802.1X ポートにゲスト VLAN を設定して、クライアントに限定されたサービス (802.1X クライアントのダウンロードなど)を提供できます。これらのクライアントは 802.1X 認証用にシステムをアップグレードできる場合もありますが、一部のホストには (Windows 98 システムなど) 802.1X 対応でないものもあります。

802.1X ポート上でゲスト VLAN をイネーブルにすると、(1) 認証サーバが EAPOL request/identity フレームに対する応答を受信しない場合、または (2) EAPOL パケットがクライアントにより送信されない場合、Catalyst 4500 シリーズ スイッチはクライアントをゲスト VLAN に割り当てます。

Cisco IOS Release 12.2(25)EWA 以降では、Catalyst 4500 シリーズ スイッチでは EAPOL パケット履歴が保持されます。リンクの存続期間中に他の EAPOL パケットがインターフェイス上で検出された場合、ネットワーク アクセスは拒否されます。EAPOL 履歴は、リンクの消失時にリセットされます。

スイッチ ポートがゲスト VLAN に移されると、許可される 802.1X 非対応クライアントの許容数に制限がなくなります。 802.1X 対応クライアントが、ゲスト VLAN が設定されたのと同じポートに参加する場合、ポートはユーザ設定のアクセス VLAN 内で無許可ステートになり、認証が再開されます。

ゲスト VLAN は、シングルホスト モードまたはマルチホスト モードの 802.1X ポートでサポートされます。



(注)

ポートがゲスト VLAN に追加されると、自動的にマルチホスト モードになり、このポートを介してポートを無制限に接続できるようになります。マルチホスト設定を変更しても、ゲスト VLAN 内のポートには影響しません。



(注)

RSPAN VLAN または音声 VLAN 以外の任意のアクティブな VLAN を、802.1X ゲスト VLAN として設定できます。

ポート上のゲスト VLAN に 802.1X を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始
		します。
ステップ 2		インターフェイス コンフィギュレーション モードを開始し、802.1X 認証をイネーブルにするインターフェイスを指定します。

	コマンド	目的
ステップ 3	Switch(config-if)# switchport mode access または Switch(config-if)# switchport mode	非トランキング、タグなし単一 VLAN レイヤ 2 インターフェイスを指定します。
	private-vlan host	有効な PVLAN トランクの関連付けを持つポートが、アクティブ ホストの PVLAN トランク ポートになることを指定します。
ステップ 4	Switch(config-if)# dot1x pae authenticator	ポート上でデフォルト設定の 802.1X 認証をイネーブルにします。
		「802.1X のデフォルト設定」(p.37-23)を参照してく ださい。
ステップ 5	Switch(config-if)# dot1x guest-vlan vlan-id	特定のインターフェイス上でゲスト VLAN をイネーブルにします。
		特定のポートでゲスト VLAN 機能をディセーブル にするには、no dot1x guest-vlan インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 6	Switch(config-if)# dot1x port-control auto	インターフェイス上で、802.1X 認証をイネーブルに します。
ステップ 7	Switch(config-if)# end	コンフィギュレーション モードに戻ります。
ステップ 8	Switch(config)# end	特権 EXEC モードに戻ります。

次に、FastEthernet 4/3 上の通常の VLAN 50 をスタティックなアクセス ポート上のゲスト VLAN としてイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# interface fa4/3
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x guest-vlan 50
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
Switch#
```

次に、セカンダリ PVLAN 100 を PVLAN ホスト ポート上のゲスト VLAN としてイネーブルにする 例を示します。

```
Switch# configure terminal
Switch(config)# interface fa4/3
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x guest-vlan 100
Switch(config-if)# end
Switch#
```

サプリカントがスイッチ上のゲスト VLAN で許容されるようにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	Switch# dot1x guest-vlan supplicant	(任意)サプリカントがスイッチ上のゲスト VLAN にグローバルに許容されるようにします。
		(注) Cisco IOS Release 12.3(31)SG の CLI では表示されませんが、dot1x guest-vlan supplicant コマンドを含むレガシー コンフィギュレーションは現在も動作します。ただし、認証失敗 VLAN オプションによってこのコマンドの必要性がなくなったため、推奨しません。
		スイッチ上でサプリカント ゲスト VLAN 機能を ディセーブルにするには、no dot1x guest-vlan supplicant グローバル コンフィギュレーション コマ ンドを使用します。
ステップ 3	Switch(config)# interface interface-id	インターフェイス コンフィギュレーション モードを開始し、802.1X 認証をイネーブルにするインターフェイスを指定します。
ステップ 4	Switch(config-if)# switchport mode access または Switch(config-if)# switchport mode	非トランキング、タグなし単一 VLAN レイヤ 2 インターフェイスを指定します。
	private-vlan host	有効な PVLAN トランクの関連付けを持つポートが、アクティブ ホストの PVLAN トランク ポートになることを指定します。
ステップ 5	Switch(config-if)# dot1x pae authenticator	ポート上でデフォルト設定の 802.1X 認証をイネーブルにします。
		「802.1X のデフォルト設定」(p.37-23)を参照してく ださい。
ステップ 6	Switch(config-if)# dot1x guest-vlan vlan-id	アクティブ VLAN を 802.1X ゲスト VLAN として指定します。有効範囲は 1 ~ 4094 です。
ステップ 7	Switch(config-if)# dot1x port-control auto	インターフェイス上で、802.1X 認証をイネーブルに します。
ステップ 8	Switch(config-if)# end	特権 EXEC モードに戻ります。
ステップ 9	Switch# show dot1x interface interface-id	入力を確認します。
ステップ 10	Switch# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を 保存します。

次に、ゲスト VLAN 機能をイネーブルにし、ゲスト VLAN として VLAN 5 を指定する例を示します。

```
Switch# configure terminal
Switch(config)# dot1x guest-vlan supplicant
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x guest-vlan 5
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
Switch#
```

MAC 認証バイパスを使用した 802.1X 認証の設定

MAB をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	Switch(config)# interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	Switch(config-if)# switchport mode access または Switch(config-if)# switchport mode private-vlan host	非トランキング、タグなし単一 VLAN レイヤ 2 インターフェイスを指定します。 有効な PVLAN トランクの関連付けを持つポートが、アクティブ ホストの PVLAN トランク ポートになることを指定します。
ステップ 4	Switch(config-if)# dot1x pae authenticator	ポート上でデフォルト設定の 802.1X 認証をイネーブルにします。 「802.1X のデフォルト設定」(p.37-23)を参照してください。
ステップ 5	Switch(config-if)# dot1x port-control auto	インターフェイス上で、802.1X 認証をイネーブルに します。
ステップ 6	Switch(config-if)# dot1x mac-auth-bypass [eap]	スイッチの MAB をイネーブルにします。
ステップ 7	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 8	Switch# show dot1x interface interface-id details	(任意)入力を確認します。
ステップ 9	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を 保存します。



(注)

ポートの 802.1X MAB 設定を削除しても、ポートの許可ステートおよび認証ステートには影響がありません。ポートが無許可ステートであれば、そのステートのまま残ります。 MAB のためにポートが認証ステートであれば、スイッチは 802.1X オーセンティケータに戻ります。 MAC アドレスによりポートがすでに許可されている場合に、MAB 設定が削除されると、再認証されるまでポートは許可ステートのままになります。そのとき 802.1X サプリカントがライン上で検出されれば、MAC アドレスは削除されます。

次に、インターフェイス GigabitEthernet 3/3 で MAB をイネーブルにし、設定を確認する例を示します。

```
Switch# configure terminal
Switch(config) # interface gigabitethernet3/3
Switch(config-if)# switchport mode access
Switch(config-if) # dot1x pae authenticator
Switch(config-if)# dot1x port-control auto
Switch(config-if) # dot1x mac-auth-bypass
Switch(config-if)# end
Switch# show dot1x int g3/3 details
Dot1x Info for GigabitEthernet3/3
                         = AUTHENTICATOR
PortControl
                         = AUTO
ControlDirection
                         = Both
HostMode
                         = SINGLE_HOST
ReAuthentication
                        = Disabled
QuietPeriod
                        = 60
ServerTimeout
                         = 30
                         = 30
SuppTimeout
                         = 3600 (Locally configured)
ReAuthPeriod
ReAuthMax
MaxReq
                         = 2.
TxPeriod
RateLimitPeriod
Mac-Auth-Bypass
                         = Enabled
Dot1x Authenticator Client List
Supplicant
                         = 0000.0000.0001
Auth SM State = AUTHENTICATED
Auth BEND SM Stat = IDLE
Port Status
                         = AUTHORIZED
Authentication Method
                         = MAB
                       = Authentication Server
Authorized By
Vlan Policy
                        = N/A
Switch#
```

アクセス不能認証バイパスを使用した 802.1X 認証の設定



Supervisor Engine 6-E は、この機能をサポートして*いません*。



注意

アクセス不能認証バイパスを正しく機能させるには、スイッチ/RADIUS サーバ通信の設定(p.37-26) で説明されているようにスイッチを設定して RADIUS サーバのステートを監視する必要があります。特に、RADIUS テスト ユーザ名、アイドル時間、ダウン時間、およびダウン基準を設定する必要があります。設定しない場合、スイッチは RADIUS サーバがダウンしても検出できなかったり、動作しない RADIUS サーバを動作していると早まってマーキングしてしまったりします。

ポートをクリティカル ポートとして設定し、アクセス不能認証バイパス機能をイネーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	Switch(config)# dot1x critical eapol	(任意)EAP交換を通じてポートが部分的にクリティカル許可されているとき EAPOL-Success パケットを送信するかどうかを設定します。
		(注) 一部のサプリカントでは必須です。 デフォルトでは、ポートがクリティカル許可されている場合は EAPOL-Success パケットは送信しません。
ステップ 3	Switch(config)# dot1x critical recovery delay msec	(任意)RADIUS サーバが使用可能になったとき、クリティカル許可されたポートの再初期化スロットルレートを指定します。デフォルトのスロットルレートは 100 ミリ秒です。これは、1 秒 に 10 ポートが再初期化されることを表します。
ステップ 4	Switch(config)# interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	Switch(config-if)# switchport mode access \$\frac{t}{c}\tag{t}\$ Switch(config-if)# switchport mode private-vlan host	非トランキング、タグなし単一 VLAN レイヤ 2 インターフェイスを指定します。
		有効な PVLAN トランクの関連付けを持つポートが、アクティブ ホストの PVLAN トランク ポートになることを指定します。
ステップ 6	Switch(config-if)# dot1x pae authenticator	ポート上でデフォルト設定の 802.1X 認証をイネーブルにします。
		「802.1X のデフォルト設定」(p.37-23)を参照してく ださい。
ステップ 7	Switch(config-if)# dot1x port-control auto	インターフェイス上で、802.1X 認証をイネーブルに します。
ステップ 8	Switch(config-if)# dot1x critical	ポートのアクセス不能認証バイパス機能をイネーブ ルにします。
		この機能をディセーブルにするには、no dot1x critical コンフィギュレーション コマンドを使用します。
ステップ 9	Switch(config-if)# dot1x critical vlan vlan	(任意)ポートがクリティカル許可されている場合に割り当てられる VLAN を指定します。 (注) Supervisor Engine 6-E は、この機能をサポートしません。
		デフォルトでは、ポートで設定された VLAN を使用 します。

	コマンド	目的
ステップ 10	Switch(config-if)# dot1x critical recovery action reinitialize	(任意)ポートがクリティカル許可されており RADIUS が使用可能であれば、ポートを再初期化す ることを指定します。
		デフォルトでは、ポートを再初期化しません。
ステップ 11	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 12	Switch# show dot1x interface interface-id details	(任意)入力を確認します。
ステップ 13	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を 保存します。

次に、アクセス不能認証バイパスを使用した 802.1X 認証の完全な設定例を示します。これには、「802.1X 認証のイネーブル化」(p.37-24) および「スイッチ/RADIUS サーバ通信の設定」(p.37-26) で指定した必須 の AAA および RADIUS 設定が含まれます。

設定された RADIUS サーバの IP アドレスは 10.1.2.3 で、認証にはポート 1812 を、アカウンティングには 1813 を使用します。RADIUS 秘密キーは mykey です。テスト サーバ プローブに使用するユーザ名は randomuser です。アップとダウンの両方のサーバに対するテスト プローブは 1 分間に 1 回生成されます。インターフェイス FastEthernet 3/1 は、AAA の応答がなくなると VLAN でクリティカル認証され、AAA が再び使用可能になると自動的に再初期化するように設定されます。

```
Switch# configure terminal
Switch(config) # aaa new-model
Switch(config) # aaa authentication dot1x default group radius
Switch(config) # dot1x system-auth-control
Switch(config) # radius-server host 10.1.2.3 auth-port 1812 acct-port 1813 test
username randomuser idle-time 1 key mykey
Switch(config) # radius deadtime 1
Switch(config) # radius dead-criteria time 15 tries 3
Switch(config) # interface f3/1
Switch(config-if) # switchport mode access
Switch(config-if) # dot1x pae authenticator
Switch(config-if) # dot1x port-control auto
Switch(config-if)# dot1x critical
Switch(config-if) # dot1x critical vlan 17
Switch(config-if) # dot1x critical recovery action reinitialize
Switch(config-if)# end
Switch# show dot1x int fastethernet 3/1 det
Dot1x Info for FastEthernet3/1
_____
                        = AUTHENTICATOR
                       = AUTO
PortControl
ControlDirection
                        = Both
HostMode
                        = SINGLE HOST
                       = Disabled
ReAuthentication
QuietPeriod
                       = 60
                        = 30
ServerTimeout
SuppTimeout
ReAuthPeriod
                        = 3600 (Locally configured)
                        = 2
ReAuthMax
MaxReq
                        = 2
TxPeriod
                        = 30
RateLimitPeriod
                        = Enabled
Critical-Auth
Critical Recovery Action = Reinitialize
Critical-Auth VLAN
Dot1x Authenticator Client List
______
Supplicant
                        = 0000.0000.0001
```

Auth SM State = AUTHENTICATING

Auth BEND SM Stat = RESPONSE

Port Status = AUTHORIZED

Authentication Method = Dot1x

Authorized By = Critical-Auth

Operational HostMode = SINGLE_HOST

Vlan Policy = 17

Switch#

単方向制御ポートを使用した 802.1X 認証の設定



Supervisor Engine 6-E は、この機能をサポートして*いません*。

単方向制御ポートを設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	Switch(config)# interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	Switch(config-if)# switchport mode access または Switch(config-if)# switchport mode private-vlan host	非トランキング、タグなし単一 VLAN レイヤ 2 インターフェイスを指定します。
		有効な PVLAN トランクの関連付けを持つポートが、アクティブ ホストの PVLAN トランク ポートになることを指定します。
ステップ 4	Switch(config-if)# dot1x pae authenticator	ポート上でデフォルト設定の 802.1X 認証をイネーブルにします。
		「802.1X のデフォルト設定」(p.37-23)を参照してく ださい。
ステップ 5	Switch(config-if)# dot1x control-direction {in both}	ポート ベースごとに単方向ポート制御をイネーブルにします。
ステップ 6	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 7	Switch# show dot1x interface interface-id details	(任意)入力を確認します。
ステップ 8	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を 保存します。

次に、単方向ポート制御をイネーブルにする例を示します。

Switch# configure terminal

 ${\tt Switch(config)\#\ interface\ gigabitethernet3/3}$

Switch(config-if)# switchport mode access

Switch(config-if) # dot1x pae authenticator

Switch(config-if)# dot1x control-direction in

Switch(config-if)# end

Switch# show dot1x int g3/3

Dot1x Info for GigabitEthernet3/3

PAE = AUTHENTICATOR

PortControl = AUTO

ControlDirection = In (Inactive) HostMode = SINGLE_HOST ReAuthentication = Disabled

QuietPeriod = 60 ServerTimeout = 30 SuppTimeout = 30

ReAuthPeriod = 3600 (Locally configured)

 ReAuthMax
 = 2

 MaxReq
 = 2

 TxPeriod
 = 30

 RateLimitPeriod
 = 0

Switch#

認証失敗 VLAN 割り当てを使用した 802.1X 認証の設定



(注)

Supervisor Engine 6-E は、この機能をサポートして*いません*。

Catalyst 4500 シリーズ スイッチのレイヤ 2 ポートに認証失敗 VLAN アライメントを設定すると、認証プロセスに失敗するクライアントに限定的なネットワーク サービスを提供できます。



(注)

認証失敗 VLAN 割り当ては、他のセキュリティ機能 (Dynamic ARP Inspection [DAI; ダイナミック ARP インスペクション] DHCP スヌーピング、および IP ソース ガードなど) と併用できます。認証失敗 VLAN 上では、これらの機能を個別にイネーブルおよびディセーブルにできます。



(注)

同一ポート上に、認証失敗 VLAN と音声 VLAN の両方は設定できません。これら 2 つの機能を同じポート上で設定しようとすると、Syslog メッセージが生成されます。

認証失敗 VLAN 割り当てを使用した 802.1X を設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始
		します。
ステップ 2	Switch(config)# interface interface-id	インターフェイス コンフィギュレーション モードを開始し、802.1X 認証をイネーブルにするインターフェイスを指定します。

	コマンド	目的
ステップ 3	Switch(config-if)# switchport mode access	非トランキング、タグなし単一 VLAN レイヤ 2 インターフェイスを指定します。
ステップ 4	Switch(config-if)# dot1x port-control auto	インターフェイス上で、802.1X 認証をイネーブルに します。
ステップ 5	Switch(config-if)# dot1x auth-fail vlan vlan-id	特定のインターフェイス上で認証失敗 VLAN をイネーブルにします。
		特定のポートで認証失敗 VLAN 機能をディセーブルにするには、no dot1x auth-fail vlan インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 6	Switch(config-if)# dot1x auth-fail max-attempts max-attemtps	ポートが認証失敗 VLAN に移される前の、最大試行回数を設定します。 デフォルトの試行回数は 3 です。
ステップ 7	Switch(config-if)# end	コンフィギュレーション モードに戻ります。
ステップ 8	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 9	Switch# show dot1x interface interface-id details	(任意)入力を確認します。
ステップ 10	Switch# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を 保存します。

次に、スタティック アクセス ポート上の認証失敗 VLAN としてインターフェイス FastEthernet 4/3 上の通常の VLAN 40 をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet3/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x port-control auto
Switch(config-if) # dot1x auth-fail vlan 40
Switch(config-if) # dot1x auth-fail max-attempts 5
Switch(config-if)# end
Switch(config)# end
Switch# show dot1x all
Dot1x Info for interface GigabitEthernet3/1
           = AUTHORIZED (AUTH-FAIL-VLAN)
               = 2
MaxReq
MaxAuthReq
               = 2
HostMode
                = Single(AUTH-FAIL-VLAN)
             = Auto
= 60 Seconds
PortControl
QuietPeriod
Re-authentication = Disabled
ReAuthPeriod
                = 3600 Seconds
                = 30 Seconds
ServerTimeout
SuppTimeout
                 = 30 Seconds
                = 30 Seconds
TxPeriod
Guest-Vlan
                = 6
Switch
```

音声 VLAN に対する 802.1X 認証の設定



(注)

802.1X と音声 VLAN を同時に設定する必要があります。



(注)

同一ポート上に、認証失敗 VLAN と音声 VLAN の両方は設定できません。これら 2 つの機能を同じポート上で設定しようとすると、Syslog メッセージが生成されます。

音声 VLAN で 802.1X をイネーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	Switch(config)# interface interface-id	インターフェイス コンフィギュレーション モー ドを開始します。
ステップ 3	Switch(config-if)# switchport access vlan vlan-id	VLAN をアクセス モードのスイッチド インター フェイスに設定します。
ステップ 4	Switch(config-if)# switchport mode access	非トランキング、タグなし単一 VLAN レイヤ 2 インターフェイスを指定します。
ステップ 5	Switch(config-if)# switchport voice vlan vlan-id	音声 VLAN をインターフェイスに設定します。
ステップ 6	Switch(config-if)# dot1x pae authenticator	ポート上でデフォルト設定の 802.1X 認証をイネーブルにします。 「802.1X のデフォルト設定」(p.37-23)を参照してく
		802.1A の
ステップ 7	Switch(config-if)# dot1x port-control auto	インターフェイス上で、802.1X 認証をイネーブルに します。
ステップ 8	Switch(config-if)# end	コンフィギュレーション モードに戻ります。
ステップ 9	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 10	Switch# show dot1x interface interface-id details	(任意)入力を確認します。
ステップ 11	Switch# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を 保存します。

次に、インターフェイス FastEthernet 5/9 上の音声 VLAN 機能で 802.1X をイネーブルにする例を示します。

 ${\tt Switch\#} \ \ \textbf{configure terminal}$

Switch(config) # interface fastethernet5/9
Switch(config-if) # switchport access vlan 2
Switch(config-if) # switchport mode access
Switch(config-if) # switchport voice vlan 10
Switch(config-if) # dot1x pae authenticator
Switch(config-if) # dot1x port-control auto
Switch(config-if) # end
Switch(config + end
Switch#

定期的再認証のイネーブル化

定期的な 802.1X クライアント再認証をイネーブルにして、その発生間隔を指定できます。再認証をイネーブルにする前に時間の間隔を指定しなかった場合、再認証を試行する間隔は 3600 秒になります。

自動 802.1X クライアント再認証はインターフェイス単位の設定で、個々のポートに接続しているクライアントに対して設定できます。特定のポートに接続しているクライアントを手動で再認証する方法については、「待機時間の変更」(p.37-46)を参照してください。

クライアントの定期的再認証をイネーブルにして、再認証を試行する間隔を秒数で設定するには、 次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	Switch(config)# interface interface-id	インターフェイス コンフィギュレーション モードを開始し、定期的再認証をイネーブルにするインターフェイスを指定します。
ステップ 3	Switch(config-if)# switchport mode access	非トランキング、タグなし単一 VLAN レイヤ 2 インターフェイスを指定します。
ステップ 4	Switch(config-if)# dot1x pae authenticator	ポート上でデフォルト設定の 802.1X 認証をイネー ブルにします。 「802.1X のデフォルト設定」(p.37-23)を参照してく ださい。
ステップ 5	Switch(config-if)# dot1x re-authentication	クライアントの定期的再認証をイネーブルにします (デフォルトではディセーブル)。
		定期的再認証をディセーブルにするには、no dot1x re-authentication インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 6	Switch(config-if)# dot1x timeout reauth-period {seconds server}	再認証を試行する間隔(秒)を指定するか、または スイッチが RADIUS によるセッション タイムアウ トを使用するようにします。
		指定できる範囲は 1 ~ 65,535 秒です。デフォルトは 3600 秒です。
		再認証を試行する間隔をデフォルトの秒数に戻すには、no dot1x timeout reauth-period グローバル コンフィギュレーション コマンドを使用します。
		このコマンドがスイッチの動作に影響を与えるのは、定期的再認証がイネーブルに設定されている場合だけです。
ステップ 7	Switch(config-if)# dot1x port-control auto	インターフェイス上で、802.1X 認証をイネーブルに します。
ステップ 8	Switch(config-if)# end	特権 EXEC モードに戻ります。

次に、定期的な再認証をイネーブルにし、再認証を試行する間隔を 4000 秒に設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface fastethernet5/9
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x re-authentication
Switch(config-if)# dot1x timeout reauth-period 4000
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
Switch#
```

複数ホストのイネーブル化

図 37-7 (p.37-21) のように、複数のホスト (クライアント) を 1 つの 802.1X 対応ポートに接続できます。このモードでは、ポートが許可されると、ポートに間接的に接続された他のすべてのホストに対して、ネットワーク アクセスが許可されます。ポートが無許可になると (再認証が失敗するか、EAPOL-Logoff メッセージを受信すると) スイッチは、無線アクセス ポイントに接続されたすべてのクライアントに対してネットワーク アクセスを拒否します。

dot1x port-control インターフェイス コンフィギュレーション コマンドが auto に設定されている 802.1X 許可ポート上で、複数のホスト (クライアント) を許容するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	Switch(config)# interface interface-id	インターフェイス コンフィギュレーション モード を開始し、複数のホストを間接的に接続するインターフェイスを指定します。
ステップ 3	Switch(config-if)# switchport mode access	非トランキング、タグなし単一 VLAN レイヤ 2 インターフェイスを指定します。
ステップ 4	Switch(config-if)# dot1x pae authenticator	ポート上でデフォルト設定の 802.1X 認証をイネーブルにします。 「802.1X のデフォルト設定」(p.37-23)を参照してください。
ステップ 5	Switch(config-if)# dot1x host-mode multiple-hosts	802.1X 許可ポート上で、複数のホスト(クライアント)を許容します。 (注) 指定されたインターフェイスについて、dot1x port-control インターフェイス コンフィギュレーション コマンドが auto に設定されていることを確認します。 ポート上の複数のホストをディセーブルにするには、no dot1x multiple-hosts インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 6	Switch(config-if)# dot1x port-control auto	インターフェイス上で、802.1X 認証をイネーブルに します。
ステップ 7	Switch(config-if)# end	特権 EXEC モードに戻ります。
ステップ 8	Switch# show dot1x all interface interface-id	入力を確認します。
ステップ 9	Switch# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を 保存します。

次に、インターフェイス FastEthernet 0/1 上で 802.1X をイネーブルにし、複数のホストを許容する 例を示します。

Switch# configure terminal
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x host-mode multiple-hosts
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
Switch#

待機時間の変更

スイッチがクライアントを再認証できないとき、スイッチは一定時間アイドルのままになり、そのあと再試行します。アイドル時間は、quiet-periodの値によって決まります。クライアントが無効なパスワードを提供したことにより、クライアントの認証失敗が起こる可能性があります。デフォルトより小さい数値を入力すると、ユーザに応答するまでの時間を短縮できます。

待機時間を変更するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	Switch(config)# interface interface-id	インターフェイス コンフィギュレーション モード を 開 始 し て、タ イ ム ア ウ ト の 待 機 時 間 (quiet-period) をイネーブルにするインターフェイスを指定します。
ステップ 3	Switch(config-if)# switchport mode access	非トランキング、タグなし単一 VLAN レイヤ 2 インターフェイスを指定します。
ステップ 4	Switch(config-if)# dot1x pae authenticator	ポート上でデフォルト設定の 802.1X 認証をイネーブルにします。
		「802.1X のデフォルト設定」(p.37-23)を参照してく ださい。
ステップ 5	<pre>Switch(config-if)# dot1x timeout quiet-period seconds</pre>	クライアントとの認証交換が失敗したあと、スイッチが待機する秒数(quiet-period)を設定します。
		デフォルトの待機時間に戻すには、no dot1x timeout quiet-period グローバル コンフィギュレーション コマンドを使用します。
		指定できる範囲は 0 ~ 65,535 秒です。デフォルトは 60 秒です。
ステップ 6	Switch(config-if)# dot1x port-control auto	インターフェイス上で、802.1X 認証をイネーブルに します。
ステップ 7	Switch(config-if)# end	特権 EXEC モードに戻ります。
ステップ 8	Switch# show dot1x all	入力を確認します。
ステップ 9	Switch# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を 保存します。

次に、スイッチ上の待機時間 (quiet-period)を 30 秒に設定する例を示します。

Switch# configure terminal
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x timeout quiet-period 30
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
Switch#

スイッチ / クライアント間の再送信時間の変更

クライアントは、スイッチからの EAP-Request/Identity フレームに、EAP-Response/Identity フレーム で応答します。この応答を受信しなかった場合、スイッチは一定時間(再送信時間といいます)待機してから、フレームを再送信します。



このコマンドのデフォルト値の変更は、信頼性のないリンクや特定のクライアントおよび認証サーバの特殊な動作問題など、異常な状況を調整する場合だけ行うようにしてください。

スイッチがクライアントの通知を待機する時間を変更するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	Switch(config)# interface interface-id	インターフェイス コンフィギュレーション モード を開始して、タイムアウトの再送信時間をイネーブ ルにするインターフェイスを指定します。
ステップ 3	Switch(config-if)# switchport mode access	非トランキング、タグなし単一 VLAN レイヤ 2 イン ターフェイスを指定します。
ステップ 4	Switch(config-if)# dot1x pae authenticator	ポート上でデフォルト設定の 802.1X 認証をイネーブルにします。
		「802.1X のデフォルト設定」(p.37-23)を参照してく ださい。
ステップ 5	Switch(config-if)# dot1x timeout tx-period seconds	要求を再送信するまでに、スイッチがクライアントからの EAP-Request/Identity フレームに対する応答を待機する秒数を設定します。
		指定できる範囲は1~65,535 秒です。デフォルトは30 秒です。
		デフォルトの再送信時間に戻すには、no dot1x timeout tx-period インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 6	Switch(config-if)# dot1x port-control auto	インターフェイス上で、802.1X 認証をイネーブルに します。
ステップァ	Switch(config-if)# end	特権 EXEC モードに戻ります。
ステップ 8	Switch# show dot1x all	入力を確認します。
ステップ 9	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を 保存します。

次に、再送信時間を60秒に設定する例を示します。

Switch# configure terminal
Switch(config) # interface fastethernet0/1
Switch(config-if) # switchport mode access
Switch(config-if) # dot1x pae authenticator
Switch(config-if) # dot1x timeout tx-period 60
Switch(config-if) # dot1x port-control auto
Switch(config-if) # end
Switch#

スイッチ/クライアント間のフレーム再送信回数の設定

スイッチ / クライアント間の再送信回数の変更以外に、認証プロセスを再開するまでに、スイッチがクライアントに EAP-Request/Identity フレームおよびその他の EAP-Request フレームを送信する回数を変更できます。EAP-Request/Identity 再送信の回数は、dot1x max-reauth-req コマンドによって制御され、その他の EAP-Request フレームの再送信回数は dot1x max-req コマンドによって制御されます。



このコマンドのデフォルト値の変更は、信頼性のないリンクや特定のクライアントおよび認証サーバの特殊な動作問題など、異常な状況を調整する場合だけ行うようにしてください。

スイッチ/クライアント間のフレーム再送信回数を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	Switch(config)# interface interface-id	インターフェイス コンフィギュレーション モードを開始し、max-reauth-req および max-req またはどちらか一方に対してイネーブルにするインターフェイスを指定します。
ステップ 3	Switch(config-if)# switchport mode access	非トランキング、タグなし単一 VLAN レイヤ 2 インターフェイスを指定します。
ステップ 4	Switch(config-if)# dot1x pae authenticator	ポート上でデフォルト設定の 802.1X 認証をイネー ブルにします。 「802.1X のデフォルト設定」(p.37-23)を参照してく ださい。

	コマンド	目的
ステップ 5	Switch(config-if)# dot1x max-req count	(消失したり応答がない場合に) EAPOL DATA パケットが再送信される回数を指定します。たとえば、
	または	認証の途中にサプリカントがあってそこで問題が発
	Switch(config-if)#	生した場合、オーセンティケータは認証要求を中止
	dot1x max-reauth-req count	する前にデータ要求を3回再送信します。countの範
		囲は1~10回です。デフォルトは2回です。
		EAPOL-Identity-Request フレーム(のみ)のタイマー
		を指定します。802.1X に対応していないデバイスを
		接続した場合、ステート マシンがリセットされる前
		に3つのEAPOL-Id-Reqフレームが送信されます。代
		わりに、ゲスト VLAN を設定している場合、この
		ポートがイネーブルになる前に3フレームが送信さ
		れます。このパラメータのデフォルト値は2です。
		再送信回数をデフォルトに戻すには、no dot1x max-req および no dot1x max-reauth-req グローバル コンフィギュレーション コマンドを使用します。
ステップ 6	Switch(config-if)# dot1x port-control auto	インターフェイス上で、802.1X 認証をイネーブルに
		します。
ステップ 7	Switch(config-if)# end	特権 EXEC モードに戻ります。
ステップ 8	Switch# show dot1x all	入力を確認します。
ステップ 9	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を
		保存します。

次に、認証プロセスを再開するまでに、スイッチが EAP-Request/Identity フレームを再送信する回数を 5 に設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x max-reauth-req 5
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
Switch#
```

手動によるポート接続クライアントの再認証

dot1x re-authenticate interface 特権 EXEC コマンドを使用すると、特定のポートに接続しているクライアントを手動でいつでも再認証できます。定期的再認証をイネーブルまたはディセーブルにする場合は、「定期的再認証のイネーブル化」(p.37-44)を参照してください。

次に、FastEthernet 1/1 ポートに接続したクライアントを手動で再認証する例を示します。

Switch# dot1x re-authenticate interface fastethernet1/1 Starting reauthentication on FastEthernet1/1

802.1X 認証ステートの初期化

dot1x initialize コマンドを実行すると、現在のステートにかかわらず認証プロセスが再開されます。

次に、ポート FastEthernet 1/1 で認証プロセスを再開する例を示します。

Switch# dot1x initialize interface fastethernet1/1

次に、スイッチの全ポートで認証プロセスを再開する例を示します。

Switch# dot1x initialize

802.1X クライアント情報の削除

clear dot1x コマンドを実行すると、既存の全サプリカントを 1 つのインターフェイスまたはスイッチの全インターフェイスから完全に削除します。

次に、ポート FastEthernet 1/1 の 802.1X クライアント情報を削除する例を示します。

Switch# clear dot1x interface fastethernet1/1

次に、スイッチの全ポートの802.1Xクライアント情報を削除する例を示します。

Switch# clear dot1x all

802.1X 設定をデフォルト値にリセットする方法

802.1X 設定をデフォルト値にリセットするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# dot1x default	設定可能な 802.1X パラメータをデフォルト値にリセット します。
ステップ 3	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 4	Switch# show dot1x all	入力を確認します。
ステップ 5	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

802.1X 統計情報およびステータスの表示

すべてのインターフェイスの 802.1X 統計情報を表示するには、show dot1x all statistics 特権 EXEC コマンドを使用します。

スイッチの 802.1X 管理および動作ステータスを表示するには、show dot1x all details 特権 EXEC コマンドを使用します。特定のインターフェイスの 802.1X 管理および動作ステータスを表示するには、show dot1x interface details 特権 EXEC コマンドを使用します。

■ 802.1X 統計情報およびステータスの表示



CHAPTER

38

ポート セキュリティの設定

この章では、Catalyst 4500 シリーズ スイッチ上で、ポート セキュリティを設定する方法について説明します。Catalyst 4500 シリーズ スイッチのポート セキュリティの概要と、アクセス、音声、トランク、プライベート VLAN (PVLAN) など各種ポートの設定について説明します。

この章の内容は、次のとおりです。

- コマンドリスト(p.38-2)
- ポート セキュリティの概要 (p.38-4)
- アクセス ポート上のポート セキュリティ (p.38-8)
- PVLAN ポートのポート セキュリティ (p.38-16)
- トランク ポートのポート セキュリティ (p.38-19)
- 音声ポート上のポート セキュリティ (p.38-25)
- ポート セキュリティ設定の表示 (p.38-31)
- 他の機能/環境でのポート セキュリティの設定 (p.38-35)
- ポート セキュリティの注意事項および制約事項 (p.38-38)



この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/cr/index.htm

コマンド リスト

この表には、主にポート セキュリティで共通に使用されるコマンドを示します。

コマンド	目的	参照先
errdisable recovery cause	セキュア ポートの errdisable ステートを解	違反処理 (p.38-7)
psecure-violation	除します。	
errdisable recovery interval	指定したエラー ディセーブル理由から回 復する時間をカスタマイズします。	違反処理 (p.38-7)
port-security mac-address	それぞれの VLAN にセキュアなすべての MAC アドレスを設定します。	セキュア MAC アドレス (p.38-4)
port-security maximum	インターフェイスに MAC アドレスの最大 数を設定します。	アクセス ポート上のポート セキュ リティの設定 (p.38-8)
private-vlan association add	セカンダリ VLAN とプライマリ VLAN の アソシエーションを作成します。	独立 PVLAN ホスト ポートでの ポートセキュリティの例(p.38-17)
private-vlan isolated	VLAN を PVLAN として指定します。	独立 プライベート VLAN ホスト ポートでのポート セキュリティの 設定 (p.38-16)
private-vlan primary	VLAN をプライマリ プライベート VLAN として指定します。	独立 プライベート VLAN ホストポートでのポート セキュリティの設定 (p.38-16)
switchport mode private-vlan host	有効な PVLAN トランクのアソシエーションを持つポートが、アクティブ ホストの PVLAN トランク ポートになるように指定します。	独立 プライベート VLAN ホストポートでのポート セキュリティの設定 (p.38-16)
switchport private-vlan host-association	独立ホスト ポート上でホスト アソシエーションを定義します。	独立 プライベート VLAN ホスト ポートでのポート セキュリティの 設定 (p.38-16)
switchport private-vlan mapping	混合モード ポートに対して PVLAN を定 義します。	独立 プライベート VLAN ホスト ポートでのポート セキュリティの 設定 (p.38-16)
switchport port-security	ポート セキュリティをイネーブルにします。	アクセス ポート上のポート セキュ リティの設定 (p.38-8)
switchport port-security aging static	MAC アドレスのスタティック エージング を設定します。	セキュア MAC アドレスのエージン グ (p.38-5)
switchport port-security aging time	ポートに対してエージング タイムを指定 します。	例 3: エージング タイマーの設定 (p.38-12)
switchport port-security limit rate invalid-source-mac	不良パケットに対してレート制限を設定 します。	例 7: 不良パケットに対するレート 制限の設定 (p.38-14)
switchport port-security mac-address	インターフェイスに対してセキュア MAC アドレスを設定します。	例 5: セキュア MAC アドレスの設 定 (p.38-13)
switchport port-security mac-address <mac_address> sticky</mac_address>	インターフェイスに対してスティッキ MAC アドレスを指定します。	アクセス ポート上のポート セキュ リティの設定 (p.38-8)
switchport port-security mac-address sticky	スティッキ ポート セキュリティをイネー ブルにします。	ポートのスティッキ アドレス (p.38-6)
no switchport port-security mac-address sticky	スティッキ セキュア MAC アドレスをダ イナミック MAC セキュア アドレスに変 換します。	アクセス ポート上のポート セキュ リティの設定 (p.38-8)

コマンド	目的	参照先
switchport port-security maximum	インターフェイスに対して最大セキュア	例 1:最大セキュア アドレス数の設
	MAC アドレス数を設定します。	定 (p.38-12)
switchport port-security violation	違反モードを設定します。	例 2: 違反モードの設定 (p.38-12)
no switchport port-security violation	違反モードを設定します。	アクセス ポート上のポート セキュ
		リティの設定 (p.38-8)
switchport trunk encapsulation dot1q	カプセル化モードを dot1q に設定します。	例 1: すべての VLAN での最大セ
		キュア MAC アドレス制限の設定
		(p.38-22)

ポート セキュリティの概要

ポート セキュリティを使用すると、ポート上で MAC アドレス(セキュア MAC アドレス)の数を制限し、未認証 MAC アドレスによるアクセスを防ぐことができます。また、指定したポートにセキュア MAC アドレスの最大数を設定することもできます(トランク ポートの VLAN に対しても任意で設定できます)。セキュア ポートが最大数を超えるとセキュリティ違反がトリガーされ、そのポートに設定された違反処理モードに基づいて違反アクションが実行されます。

そのポートの最大セキュア MAC アドレス数を 1 に設定すると、そのセキュア ポートに接続された 装置だけがそのポートにアクセスできるようになります。

ポート上でセキュア MAC アドレスがセキュアな場合、その MAC アドレスはその VLAN 以外のポートでは受信されません。他の VLAN のポートに送信すると、パケットは通知されないままハードウェアでドロップされます。インターフェイスまたはポート カウンタを使用する場合は別として、ドロップされたことを知らせるログ メッセージが表示されることはありません。これにより違反がトリガーされることに注意する必要があります。このようなパケットはハードウェアでドロップする方が効率的であり、CPU に余分な負荷がかかることはありません。

ポートセキュリティには次のような特性があります。

- セキュア MAC アドレスをエージング アウトできます。サポートされているエージングは、非アクティブと絶対の 2 種類です。
- スティッキ機能をサポートします。この機能により、ポート上のセキュア MAC アドレスがスイッチのリブートとリンク フラップを通じて保持されます。
- アクセス、音声、トランク、EtherChannel、PVLAN など、さまざまな種類のポート上で設定できます。

ここでは、次の内容について説明します。

- セキュア MAC アドレス (p.38-4)
- セキュア MAC アドレスの最大数 (p.38-5)
- セキュア MAC アドレスのエージング (p.38-5)
- ポートのスティッキ アドレス (p.38-6)
- 違反処理(p.38-7)

セキュア MAC アドレス

ポート セキュリティは、次のタイプのセキュア MAC アドレスをサポートします。

- ダイナミックまたは学習済み セキュア ポートのホストからパケットを受信すると、ダイナミック セキュア MAC アドレスが学習されます。このタイプは、ユーザの MAC アドレスが固定されていない場合 (たとえばノート型パソコンの場合)に使用します。
- スタティックまたは設定済み ユーザは、CLI または SNMP を通じてスタティック セキュア MAC アドレスを設定します。このタイプは、MAC アドレスが固定されている場合 (たとえば PC の場合) に使用します。
- スティッキ スティッキ アドレスはダイナミック セキュア MAC アドレスと同じように学習 されますが、スタティック セキュア MAC アドレスと同じようにスイッチの再起動やリンク フラップを通じて継続されます。このタイプは、固定 MAC アドレスが多数あって手動で MAC アドレスを設定しない場合 (たとえば 100 台の PC がそれぞれのポートでセキュアになっている場合)に使用します。

ポートのセキュア MAC アドレスが最大数を超過しているときにスタティック セキュア MAC アドレスを設定しようとすると、設定が拒否されエラー メッセージが表示されます。ポートのセキュア MAC アドレスが最大数を超過しているときにダイナミック セキュア MAC アドレスが新しく追加されると、違反処理がトリガーされます。

ダイナミック セキュア MAC アドレスをクリアするには、clear port-security コマンドを使用します。スティッキ セキュア MAC アドレスとスタティック セキュア MAC アドレスを同時にクリアするには、switchport port-security mac-address コマンドの no 形式を使用します。

セキュア MAC アドレスの最大数

セキュア ポートの MAC アドレスは、デフォルトで 1 つです。このデフォルト値は、1 ~ 3,000 の任意の値に変更できます。上限の 3,000 を指定すると、各ポートに MAC アドレスが 1 つ設定され、さらにシステムのポート全体で 3,000 の MAC アドレスが設定されます。

ポートに最大セキュア MAC アドレス数を設定すると、セキュア アドレスを次のいずれかの方法でアドレス テーブルに含めることができます。

- セキュア MAC アドレスを設定するには、switchport port-security mac-address mac_address インターフェイス コンフィギュレーション コマンドを使用します。
- トランクポートの VLAN 範囲にすべてのセキュア MAC アドレスを設定するには、port-security mac-address VLAN 範囲コンフィギュレーション コマンドを使用します。
- ポートは、接続デバイスの MAC アドレスを使用してセキュア MAC アドレスをダイナミック に設定します。
- いくつかのアドレスを手動で設定し、残りはダイナミックに設定されるようにすることも可能です。



- **(注)** ポートのリンクがダウンした場合、そのポート上のダイナミック セキュア アドレスはすべてセキュアではなくなります。
 - MAC アドレスをスティッキに設定できます。MAC アドレスはダイナミックに学習されるか、または手動で設定され、アドレス テーブル内に格納され、実行コンフィギュレーションに追加されます。これらのアドレスをコンフィギュレーション ファイルに保存した後は、スイッチを再起動しても、インターフェイスはダイナミックにこれらのアドレスを再学習する必要がありません。スティッキ セキュア アドレスを手動で設定することは可能ですが、推奨しません。



(注)

トランク ポートでは、セキュア MAC アドレスの最大数をポートとポート VLAN の両方に設定できます。ポートでの最大数をポート VLAN での最大数と同じかそれ以上にすることはできますが、ポート VLAN での最大数よりも少なくすることはできません。ポートの最大数がいずれかのポート VLAN の最大数よりも小さい場合(VLAN 10 の最大数を 3 に設定し、「スイッチ ポートの最大数」を設定しない場合 [デフォルトは 1])、VLAN 10 のダイナミック アドレスが 2 つになるとポートはシャットダウンします(「ポート セキュリティの注意事項および制約事項」 [p.38-38] を参照)、ポート VLAN の最大数により、指定した VLAN の指定したポートに最大数が設定されます。指定した VLAN で最大数を超過しポートの最大数は超過していない場合でも、ポートはシャットダウンします。ポートのどれか 1 つの VLAN が違反した場合でも、ポート全体がシャットダウンします。

セキュア MAC アドレスのエージング

スイッチが 3,000 件より多くの入力アドレスを受信する場合、セキュア MAC アドレスをエージン グさせることができます。



(注)

スティッキ アドレスのエージングはサポートされません。

デフォルトでは、ポートセキュリティはセキュア MAC アドレスをエージング アウトしません。学習された MAC アドレスは、スイッチがリブートするかリンクがダウンするまでポートに残ります (スティッキ機能がイネーブルでないかぎり)。ただしポート セキュリティでは、絶対モードまたは 非アクティビティ モードおよびエージング間隔 ($1 \sim n$ 、分単位)に基づいてエージングを設定できます。

- 絶対モード n と n+1 の間のエージング
- 非アクティビティ モード n+1 と n+2 の間のエージング

この機能を使用すると、既存のセキュア MAC アドレスを手動で削除しなくても、ポートのセキュア アドレス数を制限しながら、セキュア ポート上の PC の取り外しを削除および追加ができます。

switchport port-security aging static コマンドを使用してスタティック エージングを明示的に設定しないかぎり、ポートでエージングが設定されていてもスタティック アドレスがエージングすること はありません。



(注)

エージングは1分ごとに増加します。

ポートのスティッキ アドレス

スティッキポート セキュリティをイネーブルにすると、ダイナミック MAC アドレスをスティッキ セキュア MAC アドレスに変換し、それらを実行コンフィギュレーションに追加するように、イン ターフェイスを設定できます。この作業は、ユーザが他のポートに移動しないことがわかっている 場合や各ポートに MAC アドレスをスタティックに設定しない場合に行います。



<u>~</u>

別のシャーシを使用する場合は、別の MAC アドレスが必要です。

スティッキ ポート セキュリティをイネーブルにするには、switchport port-security mac-address sticky コマンドを入力します。このコマンドを入力すると、インターフェイスはすべてのダイナミック セキュア MAC アドレス(スティッキ ラーニングがイネーブルになる前にダイナミックに学習されたアドレスを含む)を、スティッキ セキュア MAC アドレスに変換します。

スティッキ セキュア MAC アドレスは、コンフィギュレーション ファイル(スイッチを再起動する たびに使用されるスタートアップ コンフィギュレーション)には、自動的には反映されません。コンフィギュレーション ファイルに実行コンフィギュレーション ファイルをユーザが保存した場合は、スイッチを再起動するときに、インターフェイスはこれらのアドレスを再学習する必要がありません。この設定は保存しないと失われます。

スティッキ ポート セキュリティをディセーブルにした場合、スティッキ セキュア MAC アドレス はダイナミック セキュア アドレスに変換され、実行コンフィギュレーションから削除されます。

最大数のセキュア MAC アドレスが設定されると、それらはアドレス テーブルに保存されます。接続デバイスがポートに唯一アクセスできるようにする場合は、接続デバイスの MAC アドレスを設定し、最大アドレス数を 1 に設定します (デフォルト設定)。

ポートに対する最大数のセキュア MAC アドレスがアドレス テーブルに追加されている場合に、アドレス テーブルにない MAC アドレスを持つワークステーションがインターフェイスにアクセスしようとすると、セキュリティ違反が発生します。

違反処理

ポートのセキュア MAC アドレス数がそのポートで許容されている最大セキュア MAC アドレス数を超過した場合、セキュリティ違反がトリガーされます。



(注)

あるポートでセキュアなホストが別のポートで認識された場合は、セキュア違反はトリガーされません。Catalyst 4500 シリーズ スイッチはハードウェア上で、そのようなパケットを新しいポートで自動的にドロップし、CPU に余分な負荷をかけません。

次のいずれかの違反モードをインターフェイスに設定できます。違反に対する応答に基づいています。

restrict (制限) ポート セキュリティ違反によりデータが制限され(つまり、ソフトウェアでパケットがドロップされ) セキュリティ違反カウンタが増加し、SNMP(簡易ネットワーク管理プロトコル)通知が生成されます。このモードは、セキュアポートのサービスやアクセスを中断しないために設定します。

SNMP トラップが生成される頻度は、snmp-server enable traps port-security trap-rate コマンド で制御できます。デフォルト値 (0) の場合、SNMP トラップはセキュリティ違反が発生する たびに生成されます。

• shutdown(シャットダウン) ポート セキュリティ違反が発生すると、インターフェイスがただちにシャットダウンします。このモードは非常にセキュアな環境で使用します。セキュアではない MAC アドレスがソフトウェアで拒否されることを回避し、サービスが中断しても問題ではない場合です。

errdisable recovery cause psecure-violation グローバル コンフィギュレーション コマンドを設定すると、セキュア ポートが errdisable ステートの場合に実行してこのステートを自動的に解除できます。また、shutdown および no shutdown インターフェイス コンフィギュレーション コマンドを入力すると、手動で再びイネーブルにできます。これがデフォルト設定です。

また、**errdisable recovery interval** *interval* コマンドを入力して、指定したエラー ディセーブル 理由から回復する時間 (デフォルトは 300 秒)をカスタマイズすることも可能です。

無効なパケット操作

デバイスが無効なパケットを送信すると思われる場合(トラフィック ジェネレータ、スニッファ、不良な NIC など) セキュア ポート上で無効な送信元 MAC アドレス パケットのレート制限をする ことができます。ポート セキュリティにより、すべてゼロの MAC アドレスを持つパケットと、マルチキャストまたはブロードキャスト送信元 MAC アドレスを持つパケットは、無効なパケットと 見なされます。これらのパケットのレート制限を選択し、レートを超過した場合はポートに対する 違反処理をトリガーすることができます。

アクセス ポート上のポート セキュリティ

ここでは、ポート セキュリティを設定する方法について説明します。

- アクセス ポート上のポート セキュリティの設定 (p.38-8)
- 例 (p.38-11)



(注)

アクセス モードに設定されたレイヤ 2 ポート チャネル インターフェイスのポート セキュリティは イネーブルにすることができます。EtherChannel のポート セキュリティ設定は、物理メンバ ポートの設定とは別に保持されます。

アクセス ポート上のポート セキュリティの設定

ポートで許容されたステーションの MAC アドレスを制限および識別することにより、ポートのトラフィックを制限するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# interface interface_id interface port-channel port_channel_number	インターフェイス コンフィギュレーション モード を開始し、設定するインターフェイスを指定します。
		(注) レイヤ 2 ポート チャネル論理インターフェ イスを指定することができます。
ステップ 2	Switch(config-if)# switchport mode access	インターフェイス モードを設定します。
		(注) デフォルト モード(dynamic desirable)のインターフェイスは、セキュア ポートとして設定できません。
ステップ 3	Switch(config-if)# [no] switchport port-security	インターフェイス上でポート セキュリティをイ ネーブルにします。
		インターフェイスをセキュア ポートでないデフォルトの状態に戻すには、no switchport port-securityコマンドを使用します。
ステップ 4	Switch(config-if)# [no] switchport port-security maximum value	(任意)インターフェイスの最大セキュア MAC アドレス数を設定します。指定できる範囲は 1 ~ 3072 です。デフォルトは 1 です。
		インターフェイスをデフォルトのセキュア MAC アドレス数に戻すには、no switchport port-security maximum <i>value</i> を使用します。

コマンド 目的 ステップ 5 Switch(config-if)# switchport port-security ポート上のすべてのセキュア アドレスに対して、 [aging {static | time aging_time | type エージング タイムとエージング タイプを設定しま {absolute | inactivity}] この機能を使用すると、既存のセキュア MAC アド レスを手動で削除しなくても、ポートのセキュア ア ドレス数を制限しながら、セキュア ポート上の PC の取り外しおよび追加ができます。 static キーワードは、このポートにスタティックに設 定されたセキュア アドレスのエージングをイネー ブルにします。 time aging_time キーワードは、このポートのエージ ング タイムを指定します。aging_time の有効範囲は 0~1440分です。時間が0の場合、このポートの エージングはディセーブルになります。 type キーワードは、エージング タイプを absolute ま たは inactive に設定します。 • absolute このポートのすべてのセキュア アド レスは指定した時間(分)が経過したあとに期 限切れとなり、セキュア アドレス リストから削 除されます。 指定された時間内にセキュア送信元 アドレスからのデータ トラフィックがない場合 のみ、このポートのセキュア アドレスが期限切 れとなります。 ポート上のすべてのセキュア アドレスに対して ポート セキュリティ エージングをディセーブルに するには、no switchport port-security aging time イン ターフェイス コンフィギュレーション コマンドを 使用します。

	コマンド	目的
ステップ 6	Switch(config-if)# [no] switchport port-security violation {restrict shutdown}	(任意)違反モードを設定します。セキュリティ違反が発生した場合に、次のいずれかのアクションを実行します。
		• restrict ポート セキュリティ違反によりデータが制限され、セキュリティ違反カウンタが増加して、SNMPトラップ通知が送信されます。
		• shutdown セキュリティ違反が発生すると、インターフェイスが errdisable になります。
		(注) セキュア ポートが errdisable ステートの場合、errdisable recovery cause psecure-violation グローバル コンフィギュレーション コマンドを入力してこのステートを解除したり、shutdown および no shutdown インターフェイス コンフィギュレーション コマンドを入力して手動で再びイネーブルにしたりできます。
		違反モードをデフォルトの状態(シャットダウンモード)に戻すには、no switchport port-security violation shutdown コマンドを使用します。
ステップィ	Switch(config-if)# switchport port-security	不良パケットに対してレート制限を設定します。
	limit rate invalid-source-mac packets_per_sec	デフォルトは 10 pps です。
ステップ 8	Switch(config-if)# [no] switchport port-security mac-address mac_address	(任意)インターフェイスのセキュア MAC アドレスを入力します。このコマンドを使用するとセキュア MAC アドレスが設定できます。設定したセキュア MAC アドレスが最大数より少ない場合、残りの MAC アドレスは動的に学習されます。
		MAC アドレスをアドレス テーブルから削除するには、no switchport port-security mac-address mac_address コマンドを使用します。
		(注) このコマンドは、アクセス、PVLAN ホスト、および PVLAN 無差別モードに対してのみ適用できます。PVLAN、トランク、または通常のトランク モードの詳細については、「トランク ポートのポート セキュリティ」(p.38-19)を参照してください。
ステップ 9	Switch(config-if)# [no] switchport port-security mac-address sticky	(任意)インターフェイス上でスティッキ ラーニン グをイネーブルにします。
		インターフェイス上でスティッキ ラーニングを ディセーブルにするには、no switchport port-security mac-address sticky コマンドを使用します。インター フェイスはスティッキ セキュア MAC アドレスをダ イナミック セキュア アドレスに変換します。

	コマンド	目的	
ステップ 10	Switch(config-if)# [no] switchport port-security mac-address mac_address sticky [vlan [voice access]]	インターフェイスにスティッキ MAC アドレスを指定します。	
		vlan キーワードを指定すると、指定した VLAN の MAC アドレスがスティッキになります。	
		アドレス テーブルからスティッキ セキュア MAC アドレスを削除するには、no switchport port-security mac-address mac_address sticky コマンドを使用します。スティッキ アドレスをダイナミック アドレスに変換するには、no switchport port-security mac-address sticky コマンドを使用します。	
		(注) このコマンドは、アクセス、PVLAN ホスト、および PVLAN 無差別モードに対してのみ適用できます。PVLAN、トランク、または通常のトランク モードの詳細については、「トランク ポートのポート セキュリティ」(p.38-19)を参照してください。	
ステップ 11	Switch(config-if)# end	特権 EXEC モードに戻ります。	
ステップ 12	Switch# show port-security address interface interface_id Switch# show port-security address	入力を確認します。	



(注)

ダイナミックに学習されたポート セキュリティ MAC アドレスを CAM テーブルから削除するには、clear port-security dynamic コマンドを使用します。address キーワードを指定すると、セキュア MAC アドレスを削除できます。interface キーワードを指定すると、各種のインターフェイス上の(ポート チャネル インターフェイスを含む)すべてのセキュア アドレスを削除できるようになります。VLAN キーワードにより、per-VLAN per-Port 単位でポート セキュリティ MAC アドレスをクリアできます。

例

ここでは、次の例を示します。

- 例 1:最大セキュア アドレス数の設定 (p.38-12)
- 例 2: 違反モードの設定 (p.38-12)
- 例 3: エージング タイマーの設定 (p.38-12)
- 例 4: エージング タイマーのタイプの設定 (p.38-13)
- 例 5: セキュア MAC アドレスの設定 (p.38-13)
- 例 6: スティッキ ポート セキュリティの設定 (p.38-14)
- 例7:不良パケットに対するレート制限の設定(p.38-14)
- 例 8:ダイナミック セキュア MAC アドレスの削除 (p.38-15)

例1:最大セキュア アドレス数の設定

次に、インターフェイス FastEthernet 3/12 でポート セキュリティをイネーブルにし、セキュア アドレスの最大数を 5 に設定する例を示します。違反モードはデフォルトで、セキュア MAC アドレスは設定されていません。

```
Switch# configure terminal
Enter configuration commands, one per line. End with {\tt CNTL/Z.}
Switch(config) # interface fastethernet 3/12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# end
Switch# show port-security interface fastethernet 3/12
Port Security
                          : Enabled
Port Status
                          : Secure-up
Violation Mode
                          : Shutdown
Aging Time
                           : 0 mins
Aging Type
                          : Absolute
SecureStatic Address Aging : Enabled
                         : 5
Maximum MAC Addresses
Total MAC Addresses
                         : 0
Configured MAC Addresses
Sticky MAC Addresses
                          : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0
```

例2:違反モードの設定

この例では、インターフェイス FastEthernet 3/12 の違反モードを restrict に設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 3/12
Switch(config-if)# switchport port-security violation restrict
Switch(config-if)# end
Switch#
```

レート制限を使用することによって SNMP トラップをイネーブルにし、制限モードによるポートセキュリティ違反を検出します。次に、1 秒間に 5 回のポート セキュリティのトラップをイネーブルにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# snmp-server enable traps port-security trap-rate 5
Switch(config)# end
Switch#
```

例 3:エージング タイマーの設定

次に、インターフェイス FastEthernet 5/1 のセキュア アドレスのエージング タイムを 2 時間 (120 分) に設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 5/1
Switch(config-if)# switchport port-security aging time 120
Switch(config-if)# end
Switch#
```

次に、エージング タイムを 2 分に設定する例を示します。

Switch(config-if) # switchport port-security aging time 2

上記のコマンドを確認するには、show port-security interface コマンドを使用します。

例 4: エージング タイマーのタイプの設定

次に、インターフェイス ファスト イーサネット 3/5 のセキュア アドレスでエージング タイム タイプを inactivity に設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config) # interface fastethernet 3/5
Switch(config-if) # switch port-security aging type inactivity
Switch(config-if)# end
Switch# show port-security interface fastethernet 3/5
Port Security
                          : Enabled
Port Status
                         : Secure-up
Violation Mode
                         : Shutdown
                         : 0 mins
Aging Time
Aging Type
                          : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses
                         : 0
Configured MAC Addresses : 0
Sticky MAC Addresses
                          : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0
```

例 5: セキュア MAC アドレスの設定

次に、インターフェイス FastEthernet 5/1 にセキュア MAC アドレスを設定し、設定を確認する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config) # interface fastethernet 5/1
Switch(config-if)# switchport mode access
Switch(config-if) # switchport port-security
Switch(config-if)# switchport port-security maximum 10
Switch(config-if)# switchport port-security mac-address 0000.0000.0003 (Static secure
MAC)
Switch(config-if)# end
Switch#show port address
Secure Mac Address Table
______
Vlan
     Mac Address
                      Type
                                            Ports Remaining Age
                                                     (mins)
       _____
     0000.0000.0003 SecureConfigured
                                            Fa5/1
Total Addresses in System (excluding one mac per port) : 2
Max Addresses limit in System (excluding one mac per port) : 3072
```

例 6:スティッキ ポート セキュリティの設定

次に、インターフェイス FastEthernet 5/1 にスティッキ MAC アドレスを設定し、設定を確認する例を示します。

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fa5/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)# end



ポートにトラフィックを送信すると、ポートにスティッキ セキュア アドレスが設定されます。

Switch# show port-security address

Secure Mac Address Table

Vlan	Mac Address	Type		Ports	Remaining	Age
					(mins)	
1	0000.0000.0001	SecureSticky		Fa5/1	_	
1	0000.0000.0002	SecureSticky		Fa5/1	-	
1	0000.0000.0003	SecureSticky		Fa5/1	-	
Total	Addresses in Syste	m (excluding one	e mac per p	 ort)	: 2	
	ldresses limit in S	· ·				
	# show running-con		-	_	. 3072	
	ng configuration	-	ab chemernee	37 1		
Darrar	ing confriguration.	•				
Curren	t configuration :	344 bytes				
1	· · · · · · · · · · · · · · · · · · ·	311 27 005				
interf	ace FastEthernet5/	1				
	switchport mode access					
	switchport port-security					
	hport port-securit	-				
	hport port-securit	-	ticky			
	hport port-securit		_	0000.0001		
	hport port-securit		_			
	hport port-securit	-	-			
SWILL	TIPOTE POTE-SECULTE	y mac-address s	LICKY 0000.	0000.0003		

Switch#

end

例7:不良パケットに対するレート制限の設定

次に、インターフェイス FastEthernet 5/1 の無効な送信元パケットにレート制限を設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 5/1
Switch(config-if)# switchport port-security limit rate invalid-source-mac 100
Switch(config-if)# end
Switch#
```

次に、インターフェイス FastEthernet 5/1 の無効な送信元パケットにレート制限を設定する例を示します。

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 5/1

Switch(config-if)# switchport port-security limit rate invalid-source-mac none Switch(config-if)# end

Switch#

例 8:ダイナミック セキュア MAC アドレスの削除

次に、ダイナミック セキュア MAC アドレスを削除する例を示します。

Switch# clear port-security dynamic address 0000.0001.0001

次に、インターフェイス fa 2/1 のすべてのダイナミック セキュア MAC アドレスを削除する例を示します。

 ${\tt Switch\#\ clear\ port-security\ dynamic\ interface\ fa2/1}$

次に、システムのすべてのダイナミック セキュア MAC アドレスを削除する例を示します。

Switch# clear port-security dynamic

PVLAN ポートのポート セキュリティ

PVLAN ポート上でポート セキュリティを設定すると、PVLAN 機能を利用しながら MAC アドレス の数を制限することができます。



ここでは、アクセスポートで説明したものと同じ設定モデルを使用します。

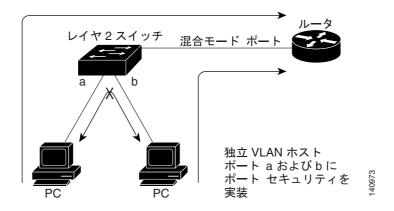
ここでは、ホストと混合モード ポート上でトランク ポート セキュリティを設定する方法を説明し ます。

- 独立 プライベート VLAN ホスト ポートでのポート セキュリティの設定 (p.38-16)
- 独立 PVLAN ホスト ポートでのポート セキュリティの例 (p.38-17)
- PVLAN 混合モード ポートでのポート セキュリティの設定 (p.38-18)
- PVLAN 混合モード ポートでのポート セキュリティの例 (p.38-18)

独立 プライベート VLAN ホスト ポートでのポート セキュリティの設定

図 38-1 に、PVLAN ホスト ポートに実装されている代表的なポート セキュリティのトポロジを示 します。このトポロジでは、スイッチのポート a で接続する PC は、混合モード ポートで接続する ルータだけと通信できます。ポート a で接続する PC はポート b で接続する PC とは通信できませ h.

図 38-1 独立 PVLAN ホスト ポートのポート セキュリティ





PVLAN 上の独立 PVLAN ホスト ポートでセキュアなダイナミック アドレスはセカンダリ VLAN 上でセキュアであり、プライマリ VLAN 上ではセキュアではありません。

独立 PVLAN ホスト ポート上でポート セキュリティを設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	Switch(config)# vlan sec_vlan_id	セカンダリ VLAN を指定します。
ステップ 3	Switch(config-vlan)# private-vlan isolated	PVLAN モードを isolated に設定します。
ステップ 4	Switch(config-vlan)# exit	グローバル コンフィギュレーション モードに戻り ます。
ステップ 5	Switch(config)# vlan pri_vlan_id	プライマリ VLAN を指定します。
ステップ 6	Switch(config-vlan)# private-vlan primary	VLAN をプライマリ PVLAN として指定します。
ステップ 7	$\label{eq:switch} $	セカンダリ VLAN とプライマリ VLAN のアソシ エーションを作成します。
ステップ 8	Switch(config-vlan)# exit	グローバル コンフィギュレーション モードに戻り ます。
ステップ 9	Switch(config)# interface interface_id	インターフェイス コンフィギュレーション モード を開始し、設定する物理インターフェイスを指定します。
ステップ 10	Switch(config-if)# switchport mode private-vlan host	有効な PVLAN トランクのアソシエーションを持つ ポートが、アクティブ ホストの PVLAN トランク ポートになるように指定します。
ステップ 11	Switch(config-if)# switchport private-vlan host-association primary_vlan secondary_vlan	独立ホスト ポート上でホスト アソシエーションを 設定します。
ステップ 12	<pre>Switch(config-if)# [no] switchport port-security</pre>	インターフェイス上でポート セキュリティをイ ネーブルにします。
ステップ 13	Switch(config-if)# end	特権 EXEC モードに戻ります。
ステップ 14	Switch# show port-security address interface interface_id Switch# show port-security address	入力を確認します。

独立 PVLAN ホスト ポートでのポート セキュリティの例

次に、独立 PVLAN ホスト ポートであるインターフェイス FastEthernet 3/12 上でポート セキュリティを設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# vlan 6
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit
Switch(config)# vlan 3
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# private-vlan association add 6
Switch(config-vlan)# exit
Switch(config)# interface fastethernet 3/12
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan association host 3 6
Switch(config-if)# switchport port-security
Switch(config-if)# end
```

PVLAN 混合モード ポートでのポート セキュリティの設定

独立 PVLAN 混合モード ポート上でポート セキュリティを設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	Switch(config)# vlan sec_vlan_id	VLAN を設定します。
ステップ 3	Switch(config-vlan)# private-vlan isolated	PVLAN モードを isolated に設定します。
ステップ 4	Switch(config-vlan)# exit	グローバル コンフィギュレーション モードに戻り ます。
ステップ 5	Switch(config)# vlan pri_vlan_id	VLAN を設定します。
ステップ 6	Switch(config-vlan)# private-vlan primary	VLAN をプライマリ PVLAN として指定します。
ステップ 7	Switch(config-vlan)# private-vlan association add sec_vlan_id	セカンダリ VLAN とプライマリ VLAN のアソシ エーションを作成します。
ステップ 8	Switch(config-vlan)# exit	グローバル コンフィギュレーション モードに戻り ます。
ステップ 9	Switch(config)# interface interface_id	インターフェイス コンフィギュレーション モード を開始し、設定する物理インターフェイスを指定します。
ステップ 10	Switch(config-if)# switchport mode private-vlan promiscuous	有効な PVLAN マッピングのあるポートがアクティ ブ混合モード ポートになるように指定します。
ステップ 11	Switch(config-if)# switchport private-vlan mapping primary_vlan secondary_vlan	混合モード ポートに対して PVLAN を設定します。
ステップ 12	Switch(config-if)# switchport port-security	インターフェイス上でポート セキュリティをイ ネーブルにします。
ステップ 13	Switch(config-if)# end	特権 EXEC モードに戻ります。
ステップ 14	Switch# show port-security address interface interface_id Switch# show port-security address	入力を確認します。

PVLAN 混合モード ポートでのポート セキュリティの例

次に、PVLAN 混合モード ポートであるインターフェイス FastEthernet 3/12 上でポート セキュリティを設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# vlan 6
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit
Switch(config)# vlan 3
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# private-vlan association add 6
Switch(config-vlan)# exit
Switch(config)# interface fastethernet 3/12
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport mode private-vlan mapping 3 6
Switch(config-if)# switchport port-security
Switch(config-if)# end
```

トランク ポートのポート セキュリティ

メトロ集約のトランク ポート上にポート セキュリティを設定すると、VLAN ごとに MAC アドレス の数を制限することができます。トランク ポート セキュリティにより、ポート セキュリティがトランク ポートにまで拡張されます。許容される MAC アドレスまたは MAC アドレスの最大数は、トランク ポート上の個々の VLAN ごとに制限されます。トランク ポート セキュリティにより、サービス プロバイダーはそのトランク ポートの VLAN に指定されたものとは異なる MAC アドレスを持つステーションからのアクセスをブロックできるようになります。また、トランク ポート セキュリティは PVLAN のトランク ポートでもサポートされます。



(注)

アクセス モードに設定されたレイヤ 2 ポート チャネル インターフェイスのポート セキュリティは イネーブルにすることができます。 EtherChannel のポート セキュリティ設定は、物理メンバ ポートの設定とは別に保持されます。

ここでは、トランク ポート セキュリティを設定する方法について説明します。

- トランク ポート セキュリティの設定 (p.38-19)
- トランク ポート セキュリティの例 (p.38-21)
- トランク ポート セキュリティの注意事項および制約事項 (p.38-23)

トランク ポート セキュリティの設定

Catalyst 4500 シリーズスイッチの 802.1q または ISL トランクが近接するレイヤ 2 スイッチに接続されている場合は、ポート セキュリティが使用されます。たとえば、メトロ集約ネットワーク (図 38-2) で使用されます。

SVI 2 SVI 3 SVI

図 38-2 トランク ポート セキュリティ

さまざまなポート セキュリティ関連パラメータをポート単位 /VLAN 単位で設定できます。



ポート セキュリティ パラメータを設定する手順はアクセス ポートの場合と似ています。トランクポートの場合は、これらの手順に加えて次のポート単位 /VLAN 単位設定を行います。

ポート セキュリティ関連パラメータをポート単位 /VLAN 単位で設定するには、次の作業を行います。

	コマンド	目的	
ステップ 1	Switch(config)# interface interface_id interface port-channel port_channel_number	インターフェイス コンフィギュレーション モード を開始し、設定するインターフェイスを指定します。	
		(注) レイヤ 2 ポート チャネル論理インターフェ イスを指定することができます。	
ステップ 2	Switch(config-if)# switchport trunk encapsulation dot1q	トランク カプセル化形式を 802.1Q に設定します。	

	コマンド	目的(続き)
ステップ 3	Switch(config-if)# switchport mode trunk	インターフェイス モードを設定します。
		<u> </u>
		(注) デフォルト モード(dynamic desirable)のインターフェイスは、セキュア ポートとして設定できません。
ステップ 4	Switch(config-if)# switchport port-security maximum value vlan	最大 MAC アドレス制限が明示的に設定されていない VLAN ごとに、最大セキュア MAC アドレス数を設定します(「セキュア MAC アドレスの最大数」[p.38-5]を参照)。
ステップ 5	Switch(config-if)# vlan-range range	VLAN 範囲サブモードを開始します。 <u>▲</u> (注) 単一または複数の VLAN を指定できます。
ステップ 6	Switch(config-if-vlan-range)# port-security maximum value	最大セキュア MAC アドレス数を VLAN ごとに設定 します。
ステップ 7	Switch(config-if-vlan-range)# no port-security maximum	すべての VLAN の最大セキュア MAC アドレス数の 設定を削除します。そのあと、ポートに設定された 最大値がすべての VLAN で使用されます。
ステップ 8	Switch(config-if-vlan-range)# [no] port-security mac-address mac_address	VLAN 範囲にセキュア MAC アドレスを設定します。
ステップ 9	Switch(config-if-vlan-range)# [no] port-security mac-address sticky mac_address	VLAN 範囲にスティッキ MAC アドレスを設定します。
ステップ 10	Switch(config-if-vlan-range)# end	インターフェイス コンフィギュレーション モード に戻ります。
ステップ 11	Switch(config-if)# end	特権 EXEC モードに戻ります。

トランク ポート セキュリティの例

ここでは、次の例を示します。

- 例 1: すべての VLAN での最大セキュア MAC アドレス制限の設定 (p.38-22)
- 例 2:特定の VLAN での最大セキュア MAC アドレス制限の設定 (p.38-22)
- 例 3: VLAN 範囲でのセキュア MAC アドレスの設定 (p.38-23)

例 1: すべての VLAN での最大セキュア MAC アドレス制限の設定

次に、すべての VLAN のインターフェイス g1/1 上でセキュア MAC アドレスおよび最大セキュア MAC アドレス制限を設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config) # interface g1/1
Switch(config-if) # switchport trunk encapsulation dot1q
Switch(config-if)# sw mode trunk
Switch(config-if) # switchport port-security
Switch(config-if) # switchport port-security maximum 3
Switch# show port-security in gil/1 vlan
Default maximum: 3
VLAN Maximum
              Current
                          0
   1
    2
              3
   3
                         Ω
              3
    4
              3
    5
              3
                         Ω
    6
              3
Switch#
Switch# show running interface gi1/1
Building configuration...
Current configuration: 161 bytes
interface GigabitEthernet1/1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport port-security
switchport port-security maximum 3 vlan
6nd
```

例 2:特定の VLAN での最大セキュア MAC アドレス制限の設定

次に、特定の VLAN または VLAN 範囲のインターフェイス $\rm g1/1$ にセキュア MAC アドレスを設定 する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface g1/1
Switch(config-if) # switchport trunk encapsulation dot1q
Switch(config-if) # sw mode trunk
Switch(config-if)# switchport port-security
Switch(config-if) # vlan-range 2-6
Switch(config-if-vlan-range)# port-security maximum 3
Switch(config-if)# exit
Switch# show port-security interface g1/1 vlan
Default maximum: not set, using 3072
VLAN Maximum Current
  2
             3
                        0
  3
             3
                        0
   4
             3
                        0
  5
             3
                        Ω
  6
Switch#
```

例3: VLAN 範囲でのセキュア MAC アドレスの設定

次に、インターフェイス g1/1 上の VLAN でセキュア MAC アドレスを設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface g1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# sw mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# vlan-range 2-6
Switch(config-if-vlan-range)# port-security mac-address 1.1.1
Switch(config-if-vlan-range)# port-security mac-address sticky 1.1.2
Switch(config-if-vlan-range)# port-security mac-address sticky 1.1.3
Switch(config-if-vlan-range)# port-security mac-address sticky 1.1.3
Switch(config-if-vlan-range)# exit
Switch# show port-security interface g1/1 address vlan 2-4
Secure Mac Address Table
```

Vlan Mac Address Type Ports Remaining Age (mins)

2 0001.0001.0001 SecureConfigured Gi1/1 2 0001.0001.0002 SecureSticky Gi1/1 2 0001.0001.0003 SecureSticky Gi1/1 -

0001.0001.0003 SecureSticky Gi1/1 0001.0001.0001 SecureConfigured 0001.0001.0002 SecureSticky Gi1/1 3 Gi1/1 3 0001.0001.0003 SecureSticky Gi1/1 3 0001.0001.0001 SecureConfigured Gi1/1 0001.0001.0002 SecureSticky 4 Gi 1 / 1 0001.0001.0003 SecureSticky Gi1/1

_

Total Addresses: 9

Switch#

トランク ポート セキュリティの注意事項および制約事項

ポート単位 /VLAN 単位でポート セキュリティ関連パラメータを設定する場合は、次の注意事項に 従ってください。

- セキュア MAC アドレスは、通常のトランク ポートで許容されていない VLAN では設定できません。
- PVLAN トランク上のプライマリ VLAN の設定はできません。CLI は拒否され、エラー メッセージが表示されます。
- ポート上の特定の VLAN で最大値が設定されていない場合(直接的または間接的) この VLAN にはポートに設定された最大値が使用されます。この場合、この VLAN 上のセキュア アドレスの最大数はポートに設定された最大値に制限されます。

各 VLAN は、ポートで設定された値よりも大きい最大数を設定できます。また、すべての VLAN に設定される最大値の合計は、ポートに設定される最大値を上回ることができます。いずれの場合でも、各 VLAN のセキュア MAC アドレス数は、VLAN の設定最大値とポートの設定最大値の小さい方の数に制限されます。また、すべての VLAN のポートでのセキュア アドレス数は、ポートに設定された最大数を超えることはできません。

• PVLAN のトランク ポートでは、設定が実行される VLAN は、PVLAN トランクの許容 VLAN リストか、またはアソシエーション ペアのセカンダリ VLAN リスト内にある必要があります (この条件が満たされていない場合、CLI は拒否されます)。PVLAN トランク上の許容 VLAN リストでは、PVLAN トランクで許可されたすべての通常の VLAN の VLAN ID が保持されます。

• PVLAN トランクからアソシエーション ペアを削除すると、ペアのセカンダリ VLAN に関連付けられたすべてのスタティックおよびスティッキ アドレスが実行コンフィギュレーションから削除されます。セカンダリ VLAN に関連付けられているダイナミック アドレスはシステムから削除されます。

同様に、許容された PVLAN トランクのリストから VLAN を削除すると、その VLAN に関連付けられているアドレスが削除されます。



(注)

通常の VLAN または PVLAN のトランク ポートでは、VLAN が許容 VLAN リストから削除されると、その VLAN に関連付けられたすべてのアドレスが削除されます。

ポート モードの変更

一般的にポート モードが変更されると、そのポートに関連付けられたすべてのダイナミック アドレスは削除されます。すべてのスタティックまたはスティッキ アドレス、およびネイティブ VLAN で設定されたその他のポート セキュリティ パラメータは、新しいモードのポートのネイティブ VLAN に移されます。非ネイティブ VLAN のすべてのアドレスは削除されます。

ネイティブ VLAN とは、次のポート タイプの VLAN です。

ポート タイプ	ネイティブ VLAN
アクセス	アクセス VLAN
トランク	ネイティブ VLAN
独立	セカンダリ VLAN(ホスト アソシエーションから)
混合モード	プライマリ VLAN(マッピングから)
PVLAN トランク	PVLAN トランク ネイティブ VLAN
802.1Q トンネル	アクセス VLAN

たとえば、モードがアクセスから PVLAN トランクに変わると、アクセス ポートのアクセス VLAN に設定されているすべてのスタティックおよびスティッキ アドレスは、PVLAN トランク ポートの PVLAN ネイティブ VLAN に移動します。その他のアドレスはすべて削除されます。

同様に、PVLAN トランク モードからアクセス モードに変わると、PVLAN ネイティブ VLAN に設定されているすべてのスタティックおよびスティッキ アドレスは、アクセス ポートのアクセス VLAN に移動します。その他のアドレスはすべて削除されます。

ポートがトランクから PVLAN トランクに変わる場合は、許容されている PVLAN トランクのリストにその VLAN がある場合、または PVLAN トランクで関連付けられているセカンダリ VLAN にある場合は、トランクの VLAN に関連付けられているアドレスはそのまま残ります。VLAN がいずれにもない場合は、実行コンフィギュレーションからアドレスが削除されます。

ポートが PVLAN トランクからトランクに変わる場合は、アドレスに関連付けられている VLAN がトランクの許容 VLAN リストにあれば、スタティックまたはスティッキ アドレスはそのまま残ります。 VLAN が許容されているリストにない場合、実行コンフィギュレーションからアドレスが削除されます。

音声ポート上のポート セキュリティ

ポートにデータ VLAN (PC 用) と音声 VLAN (Cisco IP Phone 用) が設定されている場合、IP テレフォニー環境にポート セキュリティを設定できます。

ここでは、音声ポート上にポート セキュリティを設定する方法について説明します。

- 音声ポート上のポート セキュリティの設定 (p.38-25)
- 音声ポート セキュリティの例 (p.38-27)
- 音声ポート セキュリティの注意事項および制約事項 (p.38-30)

音声ポート上のポート セキュリティの設定

音声ポート上でポート セキュリティを設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	Switch(config)# interface interface_id	インターフェイス コンフィギュレーション モードを開始し、設定する物理インターフェイスを指定します。
ステップ 2	Switch(config-if)# switchport mode access	インターフェイス モードを設定します。
		(注) デフォルト モード(dynamic desirable)のインターフェイスは、セキュア ポートとして設定できません。
ステップ 3	Switch(config-if)# [no] switchport port-security	インターフェイス上でポート セキュリティをイネーブル にします。
		インターフェイスをセキュア ポートでないデフォルトの 状態に戻すには、no switchport port-security コマンドを使 用します。
ステップ 4	<pre>Switch(config-if)# [no] switchport port-security violation {restrict shutdown}</pre>	(任意)違反モードを設定します。セキュリティ違反が発生 した場合に、次のいずれかのアクションを実行します。
		 restrict ポート セキュリティ違反によりデータが制限され、セキュリティ違反カウンタが増加して、SNMPトラップ通知が送信されます。
		• shutdown セキュリティ違反が発生すると、インターフェイスが errdisable になります。
		(注) セキュア ポートが errdisable ステートの場合、errdisable recovery cause psecure-violation グローバル コンフィギュレーション コマンドを入力してこのステートを解除したり、shutdown および no shutdown インターフェイス コンフィギュレーション コマンドを入力して手動で再びイネーブルにしたりできます。
		違反モードをデフォルトの状態(シャットダウン モード) に戻すには、no switchport port-security violation shutdown コマンドを使用します。
ステップ 5	Switch(config-if)# switchport port-security limit rate	不良パケットに対してレート制限を設定します。
	invalid-source-mac packets_per_sec	デフォルトは 10 pps です。

	コマンド	目的(続き)	
ステップ 6	Switch(config-if)# [no] switchport port-security mac-address mac_address [vlan {voice access}]	(任意)インターフェイスのセキュア MAC アドレスを指定 します。	
		vlan キーワードを指定すると、指定した VLAN にアドレス が設定されます。	
		• voice 音声 VLAN に MAC アドレスが設定されます。	
		• access アクセス VLAN に MAC アドレスが設定されます。	
		このコマンドを使用するとセキュア MAC アドレスが設定 できます。設定したセキュア MAC アドレスが最大数より 少ない場合、残りの MAC アドレスは動的に学習されます。	
		MAC アドレスをアドレス テーブルから削除するには、no switchport port-security mac-address mac_address コマンドを使用します。	
		(注) このコマンドは、アクセス、PVLANホスト、および PVLAN 無差別モードに対してのみ適用できます。PVLAN、トランク、または通常のトランク モードの詳細については、「トランクポートのポートセキュリティ」(p.38-19)を参照してください。	
ステップ 7	Switch(config-if)# [no] switchport port-security mac-address sticky	(任意)インターフェイス上でスティッキ ラーニングをイ ネーブルにします。	
		インターフェイス上でスティッキ ラーニングをディセーブルにするには、no switchport port-security mac-address sticky コマンドを使用します。インターフェイスはスティッキ セキュア MAC アドレスをダイナミック セキュアアドレスに変換します。	

	コマンド	目的(続き)	
ステップ 8	Switch(config-if)# [no] switchport port-security mac-address mac_address sticky [vlan {voice access}]	インターフェイスにスティッキ MAC アドレスを指定します。	
		vlan キーワードを指定すると、指定した VLAN の MAC アドレスがスティッキになります。	
		• voice 音声 VLAN の MAC アドレスがスティッキになります。	
		• access アクセス VLAN の MAC アドレスがスティッキになります。	
		アドレス テーブルからスティッキ セキュア MAC アドレス を削除するには、no switchport port-security mac-address mac_address sticky コマンドを使用します。スティッキ アドレスをダイナミック アドレスに変換するには、no switchport port-security mac-address sticky コマンドを使用します。	
		(注) このコマンドは、アクセス、PVLAN ホスト、および PVLAN 無差別モードに対してのみ適用できます。PVLAN、トランク、または通常のトランク モードの詳細については、「トランク ポートのポート セキュリティ」(p.38-19)を参照してください。	
ステップ 9	Switch(config-if)# end	特権 EXEC モードに戻ります。	
ステップ 10	Switch# show port-security address interface interface_id Switch# show port-security address	入力を確認します。	



(注)

ダイナミックに学習されたポート セキュリティ MAC アドレスを CAM テーブルから削除するには、clear port-security dynamic コマンドを使用します。address キーワードを指定すると、セキュア MAC アドレスを削除できます。interface キーワードを指定すると、インターフェイス上の(ポート チャネル インターフェイスを含む) すべてのセキュア アドレスを削除できます。VLAN キーワードにより、per-VLAN per-Port 単位でポート セキュリティ MAC アドレスをクリアできます。



(注)

ポートセキュリティを設定した各インターフェイスは、デフォルトで1つの MAC アドレスを受け入れます。ポートセキュリティでは、ポート レベルのポートセキュリティ設定が VLAN レベルのポートセキュリティ設定よりも優先されます。したがって、1つの MAC アドレスをそれぞれ音声およびデータ VLAN で許可するために、最大で2アドレス以上でポートを設定します。

音声ポート セキュリティの例

ここでは、次の例を示します。

- 例 1:音声 VLAN およびデータ VLAN への最大 MAC アドレスの設定 (p.38-28)
- 例 2:音声 VLAN およびデータ VLAN へのスティッキ MAC アドレスの設定 (p.38-29)

例 1:音声 VLAN およびデータ VLAN への最大 MAC アドレスの設定

次に、インターフェイス fa5/1 上で Cisco IP Phone などの音声 VLAN と PC などのデータ VLAN に MAC アドレスをそれぞれ最大 1 つ設定して、設定を確認する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fa5/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 2
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security maximum 1 vlan voice
Switch(config-if)# switchport port-security maximum 1 vlan access
Switch(config-if)# end
```



ポートにトラフィックを送信すると、ポートにスティッキ セキュア アドレスが設定されます。

Switch# show port-security address

Secure Mac Address Table

Vlan	Mac Address	Type	Ports	Remaining Age (mins)
1	0000.0000.0001	SecureSticky	Fa5/1	
3	0000.0000.0004	SecureSticky	Fa5/1	=

Total Addresses in System (excluding one mac per port) : 1 Max Addresses limit in System (excluding one mac per port) : 3072

${\tt Switch\#} \ \ \textbf{show running-config interface fastEthernet 5/1}$

Building configuration...

```
Current configuration : 344 bytes !
interface FastEthernet5/1
switchport mode access
switchport voice vlan 3
switchport port-security
switchport port-security maximum 1 vlan voice
switchport port-security maximum 3072
switchport port-security maximum 1 vlan access
switchport port-security maximum 1 vlan access
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0000.0000.0001
switchport port-security mac-address sticky 0000.0000.0004 vlan voice
end
```

Switch#

例 2:音声 VLAN およびデータ VLAN へのスティッキ MAC アドレスの設定

次に、インターフェイス fa5/1 上で音声 VLAN およびデータ VLAN に対してスティッキ MAC アドレスを設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fa5/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 3072
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.obob vlan voice
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.0005 vlan access
Switch(config-if)# end
```



ポートにトラフィックを送信すると、ポートにスティッキ セキュア アドレスが設定されます。

Switch# show port-security address

Secure Mac Address Table

Vlan	Mac Address	Type	Ports	Remaining Age (mins)
1	0000.0000.0001	SecureSticky	Fa5/1	=
1	0000.0000.0002	SecureSticky	Fa5/1	=
1	0000.0000.0003	SecureSticky	Fa5/1	=
3	0000.0000.0004	SecureSticky	Fa5/1	_
1	0000.0000.0005	SecureSticky	Fa5/1	=
3	0000.0000.0b0b	SecureSticky	Fa5/1	_

Total Addresses in System (excluding one mac per port) : 5
Max Addresses limit in System (excluding one mac per port) : 3072

${\tt Switch\#\ show\ running-config\ interface\ fastEthernet\ 5/1}$

Building configuration...

Switch#

```
Current configuration: 344 bytes!

interface FastEthernet5/1
switchport mode access
switchport voice vlan 3
switchport port-security
switchport port-security maximum 3072
switchport port-security maximum 5 vlan voice
switchport port-security mac-address sticky
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0000.0000.0001
switchport port-security mac-address sticky 0000.0000.0002
switchport port-security mac-address sticky 0000.0000.0003
switchport port-security mac-address sticky 0000.0000.0004 vlan voice
switchport port-security mac-address sticky 0000.0000.0005
switchport port-security mac-address sticky 0000.0000.000b vlan voice
end
```

音声ポート セキュリティの注意事項および制約事項

音声ポートに実装されたポート セキュリティの動作は、アクセス ポート上のポート セキュリティと同じです。

- 音声ポートにスティッキ ポート セキュリティを設定できます。音声ポートのスティッキ ポート セキュリティがイネーブルの場合、データ VLAN および音声 VLAN 上でセキュアなアドレスはスティッキ アドレスとしてセキュアです。
- 最大セキュア アドレスは VLAN 単位で設定できます。最大数は、データ VLAN または音声 VLAN のいずれかに設定できます。また、アクセス ポートの場合と同様、ポート単位でも設定できます。
- ポート セキュリティ MAC アドレスは、データ VLAN または音声 VLAN 上で VLAN 単位で設定できます。
- Cisco IOS Release 12.2(31)SG より前のリリースでは、IP Phone と PC をサポートするために3つの MAC アドレスが最大パラメータとして必要でした。Cisco IOS Release 12.2(31)SG 以降のリリースでは、最大数パラメータは2(IP Phone と PC に1つずつ)に設定する必要があります。

ポート セキュリティ設定の表示

show port-security コマンドを使用すると、インターフェイスまたはスイッチのポート セキュリティ 設定が表示されます。

トラフィック制御情報を表示するには、次の作業を1つまたは複数行います。

コマンド	目的
Switch# show interface status err-disable	errdisable となったインターフェイスを、ディセーブルの理由とともに表示します。
Switch# show port-security [interface interface_id interface port_channel port_channel_number]	スイッチまたは指定したインターフェイスのポート セキュリティ設定を表示します。表示される内容は、各インターフェイスで許容される最大セキュア MAC アドレス数、インターフェイスのセキュア MAC アドレス数、発生したセキュリティ違反数、および違反モードです。ポート チャネル論理インターフェイスを指定することができます。
Switch# show port-security [interface interface_id interface port_channel port_channel_number] address	すべてのスイッチ インターフェイスまたは指定したインターフェイスに設定されたすべてのセキュア MAC アドレス、および各アドレスのエージング情報を表示します。
Switch# show port-security [interface interface_id interface port_channel port_channel_number] vlan vlan_list	特定の VLAN リストおよび特定のインターフェイス上で、 許容される最大セキュア MAC アドレス数および現在のセ キュア MAC アドレス数を表示します。
Switch# show port-security [interface interface_id interface port_channel port_channel_number] [address [vlan vlan_list]]	特定の VLAN リストおよび特定のインターフェイスで設定されたすべてのセキュア MAC アドレスを表示します。

例

ここでは、次の例を示します。

- 例 1:スイッチ全体のセキュリティ設定の表示 (p.38-32)
- 例 2: インターフェイスのセキュリティ設定の表示 (p.38-32)
- 例 3: スイッチ全体のすべてのセキュア アドレスの表示 (p.38-33)
- 例 4: インターフェイス上の最大 MAC アドレス数の表示 (p.38-33)
- 例 5: VLAN 範囲に対するインターフェイス上のセキュリティ設定の表示 (p.38-33)
- 例 6: インターフェイスのセキュア MAC アドレスおよびエージング情報の表示 (p.38-34)
- 例7: インターフェイスの VLAN 範囲でのセキュア MAC アドレスの表示 (p.38-34)

例 1:スイッチ全体のセキュリティ設定の表示

次に、スイッチ全体のポート セキュリティの設定を表示する例を示します。

Switch# show Secure Port	port-security MaxSecureAddr	CurrentAddr	SecurityViolation	Security Action
	(Count)	(Count)	(Count)	
Fa3/1		2	0	Restrict
Fa3/2	2	2	0	Restrict
Fa3/3	2	2	0	Shutdown
Fa3/4	2	2	0	Shutdown
Fa3/5	2	2	0	Shutdown
Fa3/6	2	2	0	Shutdown
Fa3/7	2	2	0	Shutdown
Fa3/8	2	2	0	Shutdown
Fa3/10	1	0	0	Shutdown
Fa3/11	1	0	0	Shutdown
Fa3/12	1	0	0	Restrict
Fa3/13	1	0	0	Shutdown
Fa3/14	1	0	0	Shutdown
Fa3/15	1	0	0	Shutdown
Fa3/16	1	0	0	Shutdown
Po2	3	0	0	Shutdown

Total Addresses in System (excluding one mac per port) :8 Max Addresses limit in System (excluding one mac per port) :3072

Global SNMP trap control for port-security :20 (traps per second)

例2:インターフェイスのセキュリティ設定の表示

次に、インターフェイス FastEthernet 5/1 のポート セキュリティの設定を表示する例を示します。

Switch# show port-security interface fastethernet 5/1

Port Security : Enabled Port Status : Secure-up : Shutdown Violation Mode Aging Time : 0 mins Aging Type : Absolute SecureStatic Address Aging : Disabled

Maximum MAC Addresses Total MAC Addresses : 1 Configured MAC Addresses : 0

Sticky MAC Addresses : 1
Last Source Address:Vlan : 0000.0001.001a:1
Security Violation Count : 0

例3:スイッチ全体のすべてのセキュア アドレスの表示

次に、スイッチのすべてのインターフェイスで設定されたすべてのセキュア MAC アドレスを表示する例を示します。

Switch# show port-security address

Secure Mac Address Table

Vlan	Mac Address	Туре	Ports	Remaining Age (mins)
				15 (+)
1	0000.0001.0000	SecureConfigure		15 (I)
1	0000.0001.0001	SecureConfigure	d Fa3/1	14 (I)
1	0000.0001.0100	SecureConfigure	d Fa3/2	_
1	0000.0001.0101	SecureConfigure	d Fa3/2	=
1	0000.0001.0200	SecureConfigure	fa3/3	=
1	0000.0001.0201	SecureConfigure	d Fa3/3	=
1	0000.0001.0300	SecureConfigure	d Fa3/4	=
1	0000.0001.0301	SecureConfigure	d Fa3/4	=
1	0000.0001.1000	SecureDynamic	Fa3/5	_
1	0000.0001.1001	SecureDynamic	Fa3/5	=
1	0000.0001.1100	SecureDynamic	Fa3/6	=
1	0000.0001.1101	SecureDynamic	Fa3/6	=
1	0000.0001.1200	SecureSticky	Fa3/7	-
1	0000.0001.1201	SecureSticky	Fa3/7	=
1	0000.0001.1300	SecureSticky	Fa3/8	=
1	0000.0001.1301	SecureSticky	Fa3/8	=
1	0000.0001.2000	SecureSticky	Po2	-

Total Addresses in System (excluding one mac per port) :8
Max Addresses limit in System (excluding one mac per port) :3072

例 4: インターフェイス上の最大 MAC アドレス数の表示

次に、インターフェイス g1/1 上で許容される最大セキュア MAC アドレス数および現在のセキュア MAC アドレス数を表示する例を示します。

Switch# show port-security interface g1/1 vlan

Defau	It maximum:	22
VLAN	Maximum	Current
2	22	3
3	22	3
4	22	3
5	22	1
6	22	2

例 5: VLAN 範囲に対するインターフェイス上のセキュリティ設定の表示

次に、VLAN~2 および VLAN~3 のインターフェイス g1/1 上のポート セキュリティの設定を表示する 例を示します。

Switch# show port-security interface g1/1 vlan 2-3

Default maximum: 22
VLAN Maximum Current
2 22 3
3 22 3

例 6: インターフェイスのセキュア MAC アドレスおよびエージング情報の表示

次に、インターフェイス g1/1 上で設定されたすべてのセキュア MAC アドレスおよび各アドレスのエージング情報を表示する例を示します。

Switch# show port-security interface g1/1 address

Secure Mac Address Table

Vlan	Mac Address	Туре	Ports Remaining Age(mins)	
2	0001.0001.0001	SecureConfigured	Gi1/1 -	
2	0001.0001.0002	SecureSticky	Gi1/1 -	
2	0001.0001.0003	SecureSticky	Gi1/1 -	
3	0001.0001.0001	SecureConfigured	Gi1/1 -	
3	0001.0001.0002	SecureSticky	Gi1/1 -	
3	0001.0001.0003	SecureSticky	Gi1/1 -	
4	0001.0001.0001	SecureConfigured	Gi1/1 -	
4	0001.0001.0002	SecureSticky	Gi1/1 -	
4	0001.0001.0003	SecureSticky	Gi1/1 -	
5	0001.0001.0001	SecureConfigured	Gi1/1 -	
6	0001.0001.0001	SecureConfigured	Gi1/1 -	
6	0001.0001.0002	SecureConfigured	Gi1/1 -	

Total Addresses: 12

例7: インターフェイスの VLAN 範囲でのセキュア MAC アドレスの表示

次に、インターフェイス g1/1 の VLAN 2 および VLAN 3 上で設定されたすべてのセキュア MAC アドレスおよび各アドレスのエージング情報を表示する例を示します。

Switch# show port-security interface g1/1 address vlan 2-3

Secure Mac Address Table

Vlan	Mac Address	Туре	Ports	Remaining Age(mins)
2	0001.0001.0001	SecureConfigured	Gi1/1	_
2	0001.0001.0002	SecureSticky	Gi1/1	=
2	0001.0001.0003	SecureSticky	Gi1/1	_
3	0001.0001.0001	SecureConfigured	Gi1/1	=
3	0001.0001.0002	SecureSticky	Gi1/1	=
3	0001.0001.0003	SecureSticky	Gi1/1	_

Total Addresses: 12

Switch#

38-34

他の機能/環境でのポート セキュリティの設定

ここでは、次の内容について説明します。

- DHCP および IP ソース ガード (p.38-35)
- 802.1X 認証 (p.38-36)
- ワイヤレス環境でのポート セキュリティの設定(p.38-36)
- レイヤ 2 EtherChannel でのポート セキュリティの設定 (p.38-37)

DHCP および IP ソース ガード

DHCP および IP ソース ガードを使用してポート セキュリティを設定し、セキュアではない MAC アドレスによる IP スプーフィングを防ぐことができます。IP ソース ガードは次の 2 つのレベルの IP トラフィック フィルタリングをサポートします。

- 送信元 IP アドレス フィルタリング
- 送信元 IP および MAC アドレス フィルタリング

IP ソース ガードをソース IP および MAC アドレス フィルタリングで使用する場合、送信元 IP アドレスに基づいてトラフィックをフィルタリングする場合はプライベート ACL (アクセス コントロール リスト)が、送信元 MAC アドレスに基づいてトラフィックをフィルタリングする場合はポート セキュリティが使用されます。このため、このモードではアクセス ポートのポート セキュリティをイネーブルにする必要があります。

両方の機能がイネーブルの場合の制約事項は次のとおりです。

- DHCP パケットは、ポート セキュリティのダイナミック学習の対象になりません。
- 複数の IP クライアントが 1 つのアクセス ポートに接続されている場合、ポート セキュリティ では各クライアントの送信元 IP アドレスと MAC アドレスを正確にバインディングすることは できません。

たとえば、クライアントのアクセス ポートが次の IP/MAC アドレスであるとします。

- クライアント1: MAC1 <---> IP1
- クライアント2: MAC2 <---> IP2

この場合、トラフィックの送信元 MAC アドレスと IP アドレス トラフィックの組み合わせが次のいずれでも許容されます。

- MAC1 <---> IP1、有効
- MAC2 <---> IP2、有効
- MAC1 <---> IP2、無効
- MAC2 <---> IP1、無効

送信元 IP/MAC アドレス バインディングが正しい IP トラフィックだけが許可され、ポート セキュリティはこのトラフィックの MAC アドレスをダイナミックに学習します。バインディングされていない送信元アドレスの IP トラフィックは、ポート セキュリティによって無効なパケットとして処理され、ドロップされます。DoS 攻撃(サービス拒絶攻撃)を防ぐには、無効な送信元 MAC アドレスに対してポート セキュリティ レート制限を設定する必要があります。

802.1X 認証

MAC スプーフィングを防ぐために、802.1X 認証を使用したポート セキュリティを設定できます。802.1X は、通常の VLAN トランクおよび PVLAN トランクではサポートされません。アクセス ポート、および PVLAN ホストまたは混合モード ポートでは、ポート セキュリティと 802.1X を同時に設定できます。両方とも設定する場合、ホストが 802.1X 認証されたあとでポート セキュリティによってホストの MAC アドレスをセキュアにする必要があります。802.1X とポート セキュリティの両方がホストを承認する必要があります。一方がホストを認証しない場合、セキュリティ違反がトリガーされます。セキュリティ違反の種類は、ポートを拒否する機能がどちらであるかによって異なります。ホストが 802.1X では許可されても(たとえばポートがマルチホスト モードであるため)ポート セキュリティでは許可されない場合、ポートセキュリティ違反アクションがトリガーされます。ホストがポート セキュリティでは許可されても 802.1X では拒否される場合(たとえば、ホストがシングルホスト モード ポートでは未許可であるため) 802.1X セキュリティ違反アクションがトリガーされます。



802.1X、ポートセキュリティ、および VVID は、すべて同じポートに設定できます。

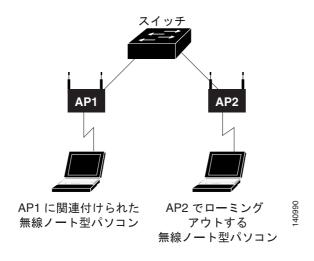
802.1X とポート セキュリティの相互作用の詳細については、「ポート セキュリティを使用した802.1X 認証の利用」(p.37-15)を参照してください。

ワイヤレス環境でのポート セキュリティの設定

アクセス ポイントをセキュア ポートに接続する場合、ユーザのスタティック MAC アドレスを設定 しないでください。 MAC アドレスは 1 つのアクセス ポイントから別のアクセス ポイントに移動することがあり、 両方のアクセス ポイントが同じスイッチに接続されるとセキュリティ違反になります。

図 38-3 に、ワイヤレス環境でのポート セキュリティの代表的なトポロジを示します。

図 38-3 ワイヤレス環境でのポート セキュリティ



レイヤ 2 EtherChannel でのポート セキュリティの設定



Supervisor Engine 6-E は、この機能をサポートしません。

ポート セキュリティは、トランク モードまたはアクセス モードのいずれかの EtherChannel でイネーブルにできます (設定手順については、「アクセス ポート上のポート セキュリティ」[p.38-8] および「トランク ポートのポート セキュリティ」[p.38-19] を参照してください)。トランキングモードで設定するときは、MAC アドレスの制限が、VLAN 単位でポートチャネル全体に適用されます。

一般的に、次の点に注意してください。

- レイヤ 2 EtherChannel でのポート セキュリティはアクセス モードまたはトランク モード上で のみ有効で、物理メンバ ポートでの設定からは独立しています。
- 少なくともメンバ ポートが 1 つセキュアであれば、チャネル インターフェイスのポート セキュリティはディセーブルにできず、CLI によって拒否されます。
- セキュア ポートは非セキュア EtherChannel に加入できません。CLI によって拒否されます。
- EtherChannel でのポート セキュリティは、PAgP モードと LACP モードの両方でサポートされています。レイヤ 3 EtherChannel には適用されません。

ポート セキュリティの注意事項および制約事項

ポート セキュリティの設定時には、次の注意事項に従ってください。

- セキュア ポートを Switched Port Analyzer (SPAN; スイッチド ポート アナライザ) の宛先ポートにすることはできません。
- インターフェイスのセキュア ポートおよびスタティック MAC アドレス設定は、相互に排他的です。
- インターフェイスの最大セキュア アドレス値を入力する際に新しい値が以前の値より大きい場合、新しい値は以前に設定された値を上書きします。新しい値が以前の値よりも小さく、インターフェイスで設定されたセキュアアドレス数が新しい値を上回る場合、コマンドは拒否されます。
- トランク ポートでトランク ポート セキュリティを設定しているときは、プロトコル パケット (CDP や BPDU) を考慮する必要はありません。これらは学習されることも、セキュアにされることもありません。
- スティッキ セキュア MAC アドレスのポート セキュリティ エージングをイネーブルにすることはできません。
- ポート セキュリティを使用して MAC スプーフィングを制限するには、802.1X 認証をイネーブルにする必要があります。
- ダイナミック ポートにはポート セキュリティを設定できません。ポート セキュリティをイネーブルにする前にモードをアクセスに変更する必要があります。
- EtherChannel のポート セキュリティがイネーブルの場合、802.1X はイネーブルにすることはできません。
- セキュア EtherChannel は PVLAN モードでは動作しません。



CHAPTER 39

コントロール プレーン ポリシングの 設定



コントロール プレーン ポリシングは、スーパーバイザ エンジン 6-E ではサポートされて*いません*。

この章では、Control Plane Policing (CoPP; コントロール プレーン ポリシング)を使用して Catalyst 4000 ファミリスイッチを保護する方法を説明します。この章の内容は Catalyst 4500 シリーズ スイッチに固有であり、第 42 章「ACL によるネットワーク セキュリティの設定」で説明する ネットワーク セキュリティ情報や手順を補足するものです。また、次のマニュアルのネットワーク セキュリティ情報や手順の補足にもなります。

- 次の URL の 『Cisco IOS Security Configuration Guide』 Cisco IOS Release 12.4
 http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_book09186a008043360a.html
- ・ 次の URL の 『Cisco IOS Security Command Reference』 Cisco IOS Release 12.4 http://www.cisco.com/en/US/products/ps6350/products_command_reference_book09186a008042df75.h tml



この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univered/cc/td/doc/product/software/ios122sr/cr/index.htm

この章の主な内容は、次のとおりです。

- CoPP 機能の概要 (p.39-2)
- コントロール プレーン ポリシングの注意事項 (p.39-4)
- CoPP のデフォルト設定 (p.39-5)
- CoPP の設定 (p.39-5)
- CoPP 設定時の注意事項および制約事項 (p.39-9)
- CoPP のモニタリング (p.39-10)

CoPP 機能の概要

CoPP 機能は、不要なトラフィックまたは DoS トラフィックから CPU を保護し、重要なコントロール プレーンおよび管理トラフィックを優先させることにより Catalyst 4000 ファミリ スイッチのセキュリティを向上させます。 分類 TCAM および QoS (Quality Of Service) ポリサーは、CoPP へのハードウェア サポートを提供します。 CoPP は、Cisco IOS Release 12.2(31)SG がサポートするすべてのスーパーバイザ エンジンで動作します。

CPU が管理するトラフィックは、次の3つの機能コンポーネント(プレーン)に分割されます。

- データ プレーン
- 管理プレーン
- コントロール プレーン

CoPP を使用することで、大半の CPU 行きトラフィックを保護し、ルーティングの安定性と信頼性を確保し、パケットを確実に配信することができます。特に重要なのは、CoPP を使用して CPU を DoS 攻撃 (サービス拒絶攻撃)から保護する場合が多いことです。レイヤ 2 およびレイヤ 3 コントロール プレーン パケットの選択済みセットに一致する、定義済み ACL のリストがあります。必要なポリシング パラメータをこれらのコントロール パケットに定義することはできますが、定義済み ACL の一致基準を変更することはできません。次に、定義済み ACL のリストを示します。

定義済み名前付き ACL	説明
system-cpp-dot1x	MacDA = 0180.C200.0003
system-cpp-bpdu-range	MacDA = 0180.C200.0000 - 0180.C200.000F
system-cpp-cdp	MacDA = 0100.0CCC.CCCC (UDLD/DTP/VTP/PAgP)
system-cpp-sstp	MacDA = 0100.0CCC.CCCD
system-cpp-cgmp	Mac DA = 01-00-0C-DD-DD
system-cpp-ospf	IP プロトコル = OSPF、IPDA は 224.0.0.0/24 に一致
system-cpp-igmp	IP プロトコル = IGMP、IPDA は 224.0.0.0/3 に一致
system-cpp-pim	IP プロトコル = PIM、IPDA は 224.0.0.0/24 に一致
system-cpp-all-systems-on-subnet	IPDA = 224.0.0.1
system-cpp-all-routers-on-subnet	IPDA = 224.0.0.2
system-cpp-ripv2	IPDA = 224.0.0.9
system-cpp-ip-mcast-linklocal	IP DA = 224.0.0.0/24
system-cpp-dhcp-cs	IP Protocol = UDP、L4SrcPort = 68、L4DstPort = 67
system-cpp-dhcp-sc	IP Protocol = UDP、L4SrcPort = 67、L4DstPort = 68
system-cpp-dhcp-ss	IP Protocol = UDP、L4SrcPort = 67、L4DstPort = 67

データ プレーンおよび管理プレーン トラフィックの場合、ポリシングするトラフィック クラスと 一致するようにユーザの ACL を定義できます。

CoPP では Modular Qulality of Service Command Line Interface (MQC; モジュラ QoS コマンドラインインターフェイス)を使用してトラフィック分類基準を定義し、分類されたトラフィックに対して実行する設定可能なポリシー アクションを指定します。MQC ではクラス マップを使用して特定のトラフィック クラスに対するパケットを定義します。トラフィックを分類したら、指定したトラフィックに対してポリシーを実行するためのポリシー マップを作成できます。コントロール プレーン グローバル コンフィギュレーション コマンドを使用すると、CoPP サービス ポリシーをコントロール プレーンに直接付加できます。

コントロール プレーンに付加できるポリシー マップは system-cpp-policy だけです。ポリシー マップの冒頭には事前に定義されたクラスマップが事前に定義された順番で含まれていることが必要です。system-cpp-policy ポリシー マップを作成するのに最善の方法は、グローバル マクロ system-cpp を使用する方法です。

system-cpp-policy には、コントロール プレーン トラフィックに対する定義済みクラス マップが含まれています。システムで定義されたすべての CoPP クラス マップの名前と、それらの一致 ACL には [system-cpp-] というプレフィクスが付いています。デフォルトでは、トラフィック クラスに対するアクションは指定されていません。CPU 行きデータ プレーンおよび管理プレーン トラフィックに一致するクラス マップを独自に定義できます。定義したクラス マップは system-cpp-policy ポリシーマップに追加できます。

コントロール プレーン ポリシングの注意事項

• ポート セキュリティは、非 IP コントロール パケットに対する効果をキャンセルすることがあります。

Catalyst 4500 シリーズ スイッチでの送信元 MAC ラーニングはソフトウェアで実行されますが、コントロール パケット(例、IEEE BPDU/CDP/SSTP BPDU/GARP/ など)からの送信元 MAC アドレスのラーニングは許可されません。このような(範囲から外れた可能性のある)高いレートのコントロール パケットを受信するとみなされるポートでポート セキュリティを設定すると、システムはパケットを転送するのではなく、(送信元アドレスが学習されるまで、ポート セキュリティがどのように実装されるか)パケットのコピーを CPU に生成します。

Catalyst 4500 スイッチング エンジンの現在のアーキテクチャでは、CPU に送信されたパケットのコピーにポリシングを適用できません。ポリシングを適用できるのは、CPU に転送されたパケットに対してだけです。したがって、パケットのコピーは、パケットが到着するレートでCPU に送信され、コントロール パケットからのラーニングが許可されないため、ポート セキュリティはトリガーされません。さらに、元のパケットではなくパケットのコピーが CPU に送信されるため、ポリシングも適用されません。

Cisco IOS Release 12.2 (31) SGA1 と同様に、GARP クラスは、CoPP の一部ではなくなりました(CSCsg08775 に伴う修正のため、system-cpp-garp-range エントリが CPP 設定に引き続き表示されていても、単にアイドリングになっているだけで、その後のリリースでは削除される予定です)。これ以降、ユーザ ACL および QoS で GARP トラフィックを操作できます。GARP パケットに対して CPU を保護したい場合、GARP パケットのユーザ クラスを定義したあとで、CoPP を使用して GARP パケットを下方ポリシングすることも可能です(GARP がスタティック CAM 領域の一部ではなくなったため、下方ポリシングが可能になりました)。

IOS とプラットフォーム コードの間での CPP 実装の統合が強固になったため、起動時には常にエラー メッセージが表示され、この注意事項が以前のリリースに統合されている(この修正が存在しない)バージョンから IOS ソフトウェアをダウングレードするときには、CPP が適用されません。

%Invalid control plane policy-map; Please unconfigure policy-map attached to control-plane, and associated class-maps, and execute config command "macro global apply system-cpp" error: failed to install policy map system-cpp-policy

次善策として、次の手順を実行します。

- 1. ソフトウェアのダウングレードを実行するときは、コンフィギュレーションをバックアップ します。
- 2. コンフィギュレーションからすべての CPP を手動で削除し、macro global apply system-cpp コマンドを再度適用します。

リリース間でアップグレードするときは、この注意事項に関連する問題は発生しないはずです。

CoPP のデフォルト設定

CoPP はデフォルトでディセーブルです。

CoPP の設定

ここでは、次の作業について説明します。

- コントロール プレーン トラフィックの CoPP を設定 (p.39-5)
- データ プレーンおよび管理プレーン トラフィックの CoPP の設定 (p.39-6)

コントロール プレーン トラフィックの CoPP を設定

コントロール プレーン トラフィックの CoPP を設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	Switch# config terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	Switch(config)# qos	(任意) QoS をグローバルにイネーブルにします。
ステップ 3	Switch(config)# macro global apply system-cpp	(任意)system-cpp-policy ポリシー マップを作成して コントロール プレーンに付加します。
ステップ 4	Switch(config)# policy-map system-cpp-policy Switch(config-pmap)# class {system-cpp-dot1x system-cpp-bpdu-range system-cpp-cdp service system-cpp-sstp system-cpp-cgmp system-cpp-ospf system-cpp-igmp system-cpp-pim system-cpp-pim system-cpp-all-systems-on-subnet system-cpp-all-routers-on-subnet system-cpp-ip-mcast-linklocal system-cpp-dhcp-cs system-cpp-dhcp-sc system-cpp-dhcp-ss} Switch(config-pmap-c)# police [aggregate name] rate burst [conform-action {drop transmit}] [{exceed-action {drop transmit}}]	サービス ポリシー マップで 1 つまたは複数のシステム定義のコントロール プレーン トラフィックにアクションを関連付けます。必要に応じてこのステップを繰り返します。
ステップ 5	Switch# show policy-map system-cpp-policy	(任意)コンフィギュレーションを確認します。

次に、CDP パケットをポリシングする例を示します。

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# qos
Switch(config) # macro global apply system-cpp
Switch(config)# policy-map system-cpp-policy
Switch(config-pmap)# class system-cpp-cdp
Switch(config-pmap-c)# police 32000 1000 conform-action transmit exceed-action drop
Switch(config-pmap-c)# end
Switch# show policy-map system-cpp-policy
 Policy Map system-cpp-policy
   Class system-cpp-dot1x
    Class system-cpp-bpdu-range
    Class system-cpp-cdp
     police 32000 bps 1000 byte conform-action transmit exceed-action drop *
    {\tt Class\ system-cpp-sstp}
    Class system-cpp-cgmp
   Class system-cpp-ospf
   Class system-cpp-igmp
   Class system-cpp-pim
   Class system-cpp-all-systems-on-subnet
    Class system-cpp-all-routers-on-subnet
   Class system-cpp-ripv2
   Class system-cpp-ip-mcast-linklocal
   Class system-cpp-dhcp-cs
    Class system-cpp-dhcp-sc
    Class system-cpp-dhcp-ss
Switch#
```

データ プレーンおよび管理プレーン トラフィックの CoPP の設定

データ プレーンおよび管理プレーン トラフィックの CoPP を設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	Switch(config)# qos	(任意) QoS をグローバルにイネーブルにします。
ステップ 2	magna glabal apple greaten gpp	(任意) system-cpp-policy ポリシー マップをコント ロール プレーンに付加します。

コマンド 目的 ステップ 3 Switch(config)# {ip | mac} access-list トラフィックに一致する ACL を定義します。 extended {access-list-name} パケットが名前付き ACL をパスする permit For an ip access list, issue 条件を指定します。 Switch(config-ext-nacl) #{permit | deny} パケットが名前付き ACL をパスしない denv {protocol} source {source-wildcard} **destination** { destination-wildcard} 条件を指定します。 For a mac access list, issue Switch(config-ext-macl) #{permit | deny} source (注) トラフィックの重要性を判断するために、 {source-wildcard} destination ACL をほとんどの場合について設定する必 {destination-wildcard} [protocol-family] 要があります。 または **type-code** 0x で始まる 16 進のビット数(0x6000 Switch(config) # access-list など)。802 カプセル化パケットの場合は Link {access-list-name} {permit | deny} {type-code Service Access Point(LSAP: リンク サービス アク wild-mask | address mask} セス ポイント)タイプ コードを、SNAP カプセ ル化パケットの場合は SNAP タイプ コードを指 定します(LSAPはSAP「サービスアクセスポ イント]とも呼ばれ、802 ヘッダーの DSAP [宛 先サービス アクセス ポイント] フィールドおよ び SSAP [送信元サービス アクセス ポイント] フィールドのタイプ コードのことです)。 • wild-mask 1のビットが type-code 引数のビッ トに対応する 16 進数。wild-mask は、比較時に 無視する type-code 引数のビットです (DSAP/SSAP のペアのマスクでは、2 つのビット がSAPコードの識別以外の目的で使用されるた め、常に 0x0101 です)。 48 ビットのトークン リング アドレ address ス。16 進の数字を 4 桁ずつドットで 3 つに区 切って表します。このフィールドはベンダー コードでのフィルタリングに使用されます。 48 ビットのトークン リング アドレス。 16 進の数字を 4 桁ずつドットで 3 つに区切って 表します。マスクの1ビットはアドレスでは無 視されます。このフィールドはベンダー コード でのフィルタリングに使用されます。 ステップ 4 Switch(config)# class-map パケット分類基準を定義します。クラスに関連付け {traffic-class-name} られたトラフィックを識別するには、match 文を使 用します。 Switch(config-cmap) # match access-group {access-list-number | name {access-list-name}} ステップ 5 Switch(config-cmap)# exit グローバル コンフィギュレーション モードに戻り ます。 ステップ 6 Switch(config) # policy-map system-cpp-policy CoPP ポリシー マップにトラフィック クラスを追加 します。トラフィック クラスにアクションを関連付 Switch(config-pmap) # class < class-map-name> けるには、police 文を使用します。 Switch(config-pmap-c)# police [aggregate name] rate burst [conform-action {drop | transmit}] [{exceed-action {drop transmit}}] ステップ 7 Switch(config)# end 特権 EXEC モードに戻ります。 ステップ 8 Switch# show policy-map system-cpp-policy 入力を確認します。

次に、信頼されるホストの送信元アドレスに 10.1.1.1 および 10.1.1.2 を設定して Telnet パケットを 制約なしにコントロール プレーンに転送し、残りの Telnet パケットはすべて一定のレートでポリシングする例を示します (この例ではグローバル QoS がイネーブルであり、system-cpp-policy ポリシー マップが作成されていると仮定します)。

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config) # qos
Switch(config) # macro global apply system-cpp
! Allow 10.1.1.1 trusted host traffic.
Switch(config) # access-list 140 deny tcp host 10.1.1.1 any eq telnet
! Allow 10.1.1.2 trusted host traffic.
Switch(config)# access-list 140 deny tcp host 10.1.1.2 any eq telnet
! Rate limit all other Telnet traffic.
Switch(config) # access-list 140 permit tcp any any eq telnet
! Define class-map "telnet-class."
Switch(config) # class-map telnet-class
Switch(config-cmap) # match access-group 140
Switch(config-cmap)# exit
! Add the class-map "telnet-class" to "system-cpp-policy" and define ! the proper
action Switch(config)# policy-map system-cpp-policy
Switch(config-pmap)# class telnet-class
Switch(config-pmap-c) # police 80000 1000 conform transmit exceed drop
Switch(config-pmap-c)# exit
Switch(config-pmap) # exit
! Verify the above configuration steps
Switch# show policy-map system-cpp-policy
 Policy Map system-cpp-policy
   Class system-cpp-dot1x
    Class system-cpp-bpdu-range
   Class system-cpp-cdp
     police 32000 bps 1000 byte conform-action transmit exceed-action drop
   Class system-cpp-sstp
    Class system-cpp-cgmp
   Class system-cpp-ospf
   Class system-cpp-igmp
   Class system-cpp-pim
   Class system-cpp-all-systems-on-subnet
    Class system-cpp-all-routers-on-subnet
   Class system-cpp-ripv2
   Class system-cpp-ip-mcast-linklocal
    Class system-cpp-dhcp-cs
    Class system-cpp-dhcp-sc
    Class system-cpp-dhcp-ss
    Class telnet-class
```

police 8000 bps 1000 byte conform-action drop exceed-action drop

CoPP 設定時の注意事項および制約事項

CoPP を設定する際は、次の注意事項と制約事項に従います。

- 入力 CoPP だけがサポートされます。つまり、コントロール パネルに関連する CLI では input キーワードだけがサポートされます。
- コントロール プレーン トラフィックをポリシングする場合はシステム定義クラス マップを使用します。
- コントロール プレーン トラフィックは、CoPP を使用する場合にだけポリシングできます。ポリシー マップをインターフェイスまたは VLAN に付加するとき、コントロール プレーン トラフィックを含むポリシー マップが受け付けられても、入力インターフェイスまたは VLAN のトラフィックはポリシングできません。
- システム定義クラス マップは、通常の OoS のポリシー マップでは使用できません。
- CPU が処理するデータ プレーンおよび管理プレーン トラフィックを識別するには、ACL とクラスマップを使用します。ユーザー定義クラス マップは、CoPP の system-cpp-policy ポリシーマップに追加する必要があります。
- system-cpp-policy という名前のポリシー マップは CoPP 専用です。いったん control-plane に付加すると削除できません。
- デフォルトの system-cpp-policy マップはシステム定義クラス マップのアクションを定義しません。つまり no policing です。
- system-cpp-policy ポリシー マップがサポートするアクションは police だけです。
- CoPP ポリシー ACL では log キーワードは使用できません。
- データ プレーンおよび管理プレーン トラフィック クラスは、MAC ACL と IP ACL のどちらでも定義できます。パケットがコントロール プレーン トラフィックの事前に定義された ACL にも一致する場合は、コントロール プレーン クラスがサービス ポリシーのユーザ定義クラスの上にあるため、コントロール プレーン クラスの police アクション (または no police アクション)が実行されます。これは同じ MQC セマンティックです。
- 超過アクション policed-dscp-transmit は CoPP ではサポートされません。
- グローバル QoS がイネーブルで、police アクションが指定されないかぎり、CoPP はイネーブルになりません。

CoPP のモニタリング

show policy-map control-plane コマンドを実行すると、サイト固有のポリシーの開発、コントロール プレーン ポリシーの統計情報のモニタリング、および CoPP のトラブルシューティングができます。このコマンドは、実際に適用されるポリシーのダイナミック情報を表示します。このダイナミック情報には、レート情報と、ハードウェアおよびソフトウェアに設定したポリシーに準拠または超過するバイト数(およびパケット数)が含まれます。

次に、show policy-map control-plane コマンドの出力例を示します。

```
Switch# show policy-map control-plane
Control Plane
Service-policy input: system-cpp-policy
   Class-map: system-cpp-dot1x (match-all)
      0 packets
     Match: access-group name system-cpp-dot1x
    Class-map: system-cpp-bpdu-range (match-all)
     Match: access-group name system-cpp-bpdu-range
    Class-map: system-cpp-cdp (match-all)
     160 packets
      Match: access-group name system-cpp-cdp
       police: Per-interface
        Conform: 22960 bytes Exceed: 0 bytes
   Class-map: system-cpp-sstp (match-all)
      0 packets
     Match: access-group name system-cpp-sstp
    Class-map: system-cpp-cgmp (match-all)
     Match: access-group name system-cpp-cgmp
    Class-map: system-cpp-ospf (match-all)
      0 packets
     Match: access-group name system-cpp-ospf
    Class-map: system-cpp-igmp (match-all)
      0 packets
     Match: access-group name system-cpp-igmp
    Class-map: system-cpp-pim (match-all)
      0 packets
      Match: access-group name system-cpp-pim
    Class-map: system-cpp-all-systems-on-subnet (match-all)
     Match: access-group name system-cpp-all-systems-on-subnet
    Class-map: system-cpp-all-routers-on-subnet (match-all)
      0 packets
     Match: access-group name system-cpp-all-routers-on-subnet
   Class-map: system-cpp-ripv2 (match-all)
      0 packets
     Match: access-group name system-cpp-ripv2
    Class-map: system-cpp-ip-mcast-linklocal (match-all)
      0 packets
      Match: access-group name system-cpp-ip-mcast-linklocal
    Class-map: system-cpp-dhcp-cs (match-all)
      83 packets
      Match: access-group name system-cpp-dhcp-cs
```

```
Class-map: system-cpp-dhcp-sc (match-all)
      0 packets
     Match: access-group name system-cpp-dhcp-sc
    Class-map: system-cpp-dhcp-ss (match-all)
      0 packets
     Match: access-group name system-cpp-dhcp-ss
    Class-map: telnet-class (match-all)
      0 packets
     Match: access-group 140
       police: Per-interface
        Conform: 0 bytes Exceed: 0 bytes*
    Class-map: class-default (match-any)
      0 packets
     Match: any
       0 packets
Switch#
```

コントロール プレーンのカウンタをクリアするには、clear control-plane * コマンドを実行します。

Switch# clear control-plane *
Switch#

すべての CoPP アクセス リスト情報を表示するには、show access-lists コマンドを実行します。

```
Switch# show access-lists
Extended IP access list system-cpp-all-routers-on-subnet
10 permit ip any host 224.0.0.2
Extended IP access list system-cpp-all-systems-on-subnet
10 permit ip any host 224.0.0.1
Extended IP access list system-cpp-dhcp-cs
10 permit udp any eq bootpc any eq bootps Extended IP access list
system-cpp-dhcp-sc
10 permit udp any eq bootps any eq bootpc Extended IP access list
system-cpp-dhcp-ss
10 permit udp any eq bootps any eq bootps Extended IP access list
system-cpp-igmp
10 permit igmp any 224.0.0.0 31.255.255.255 Extended IP access list
system-cpp-ip-mcast-linklocal
10 permit ip any 224.0.0.0 0.0.0.255 Extended IP access list
system-cpp-ospf
10 permit ospf any 224.0.0.0 0.0.0.255 Extended IP access list
system-cpp-pim
10 permit pim any 224.0.0.0 0.0.0.255 Extended IP access list
system-cpp-ripv2
10 permit ip any host 224.0.0.9
Extended MAC access list system-cpp-bpdu-range
permit any 0180.c200.0000 0000.0000.000f Extended MAC access list
system-cpp-cdp
permit any host 0100.0ccc.ccc
Extended MAC access list system-cpp-cgmp
permit any host 0100.0cdd.dddd
Extended MAC access list system-cpp-dot1x
permit any host 0180.c200.0003
system-cpp-sstp
permit any host 0100.0ccc.cccd
```

CoPP アクセス リストを 1 つだけ表示するには、show access-lists system-cpp-cdp コマンドを実行します。

```
Switch# show access-list system-cpp-cdp
Extended MAC access list system-cpp-cdp
permit any host 0100.0ccc.cccc
Switch#
```

■ CoPP のモニタリング



CHAPTER

40

DHCP スヌーピング、IP ソース ガード、およびスタティック ホストの IPSG の設定

この章では、Catalyst 4500 シリーズ スイッチ上で Dynamic Host Configuration Protocol (DHCP) スヌーピングと IP ソース ガード、およびスタティック ホストの IPSG を設定する手順について説明します。設定上の注意事項、設定手順、および設定例も示します。

この章の主な内容は、次のとおりです。

- DHCP スヌーピングの概要 (p.40-2)
- スイッチ上での DHCP スヌーピングの設定 (p.40-8)
- DHCP スヌーピング情報の表示 (p.40-18)
- IP ソース ガードの概要 (p.40-19)
- スイッチ上での IP ソース ガードの設定 (p.40-20)
- IP 送信元バインディング情報の表示 (p.40-24)
- スタティック ホストの IP ソース ガードの設定 (p.40-25)



(注)

この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/cr/index.htm

DHCP スヌーピングの概要

DHCP スヌーピングは、信頼できない DHCP メッセージをフィルタリングし、DHCP スヌーピング バインディング テーブルを構築およびメンテナンスすることで安全性を持たせる DHCP セキュリティ機能です。信頼できないメッセージとは、ネットワークまたはファイアウォール外部からの受信メッセージのうち、ネットワーク内でトラフィック攻撃を引き起こす可能性のあるメッセージです。

DHCP スヌーピング バインディング テーブルには、MAC (メディア アクセス制御) アドレス、IP アドレス、リース期間、バインディング タイプ、VLAN (仮想 LAN)番号、およびスイッチの信頼できないローカル インターフェイスに対応するインターフェイス情報が格納されます。信頼できるインターフェイスに相互接続するホストに関する情報は収められていません。信頼できないインターフェイスとは、ネットワークまたはファイアウォール外部からのメッセージを受信するように設定されたインターフェイスです。信頼できるインターフェイスとは、ネットワーク内からのメッセージのみを受信するように設定されたインターフェイスです。

DHCP スヌーピングは、信頼できないホストと DHCP サーバ間でファイアウォールのように機能します。また、DHCP スヌーピングはエンドユーザに接続する信頼できないインターフェイスと、DHCP サーバまたは別のスイッチに接続する信頼できるインターフェイスとを差異化する方法を提供します。



VLAN 上で DHCP スヌーピングをイネーブルにするには、スイッチ上で DHCP スヌーピングをイネーブルにする必要があります。

DHCP スヌーピングはスイッチと VLAN に対して設定できます。スイッチ上で DHCP スヌーピングをイネーブルにする場合、インターフェイスはレイヤ 2 ブリッジとして動作し、レイヤ 2 VLAN に送信される DHCP メッセージを代行受信および保護します。 VLAN 上で DHCP スヌーピングをイネーブルにする場合、スイッチは VLAN ドメイン内のレイヤ 2 ブリッジとして動作します。

次の内容について説明します。

- 信頼送信元と信頼できない送信元 (p.40-2)
- DHCP スヌーピング データベース エージェントの概要 (p.40-3)
- オプション82データ挿入(p.40-4)

信頼送信元と信頼できない送信元

DHCP スヌーピング機能は、トラフィックの送信元が信頼できるかまたは信頼できないかを判別します。信頼できない送信元は、トラフィック攻撃または他の敵対的アクションを起こすことがあります。これらの攻撃を回避するために、DHCP スヌーピング機能は、信頼できない送信元からのメッセージおよびレート制限トラフィックをフィルタします。

エンタープライズ ネットワークでは、管理制御下のデバイスは信頼できる送信元です。これらのデバイスには、使用ネットワークのスイッチ、ルータ、およびサーバが含まれます。ファイアウォール外またはネットワーク外のデバイスは、信頼できない送信元です。一般的に、ホスト ポートは信頼できない送信元として扱われます。

サービス プロバイダ環境では、サービス プロバイダ ネットワーク内にないデバイス(顧客のスイッチなど)は、信頼できない送信元です。 ホスト ポートは、信頼できない送信元です。

Catalyst 4500 シリーズ スイッチでは、接続しているインターフェイスの信頼状態を設定して、送信元が信頼できることを示します。

すべてのインターフェイスのデフォルトは、信頼できない状態です。DHCP サーバ インターフェイスは、信頼できる送信元として設定する必要があります。また、ネットワーク内のデバイス(スイッチまたはルータなど)に接続している場合、他のインターフェイスも信頼できる送信元として設定できます。通常は、ホスト ポート インターフェイスは信頼できる送信元としては設定しません。



DHCP スヌーピングが正常に機能するには、すべての DHCP サーバを信頼できるインターフェイスを介してスイッチに接続し、信頼できない DHCP メッセージが信頼できるインターフェイスにのみ転送されるようにする必要があります。

DHCP スヌーピング データベース エージェントの概要

スイッチのリロード時にバインディングが失われないようにするには、DHCP スヌーピング データベース エージェントを使用する必要があります。このエージェントがないと、DHCP スヌーピングによって確立されたバインディングがスイッチのリロード時に失われます。接続も同様に失われます。

データベース エージェントのメカニズムでは、設定されたロケーションのファイルにバインディングを格納します。 リロード時に、スイッチはファイルを読み取り、バインディングのデータベースを作成します。スイッチは、データベースが変更されるとファイルを書き込み、ファイルを最新の状態に保ちます。

バインディングを含むファイルの形式は、次のようになります。

```
<initial-checksum>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<entry-1> <checksum-1>
<entry-2> <checksum-1-2>
...
...
<entry-n> <checksum-1-2-..-n>
END
```

ファイルの各エントリは、ファイルが読み取られるたびにエントリの確認に使用されるチェックサムでタグ付けされています。最初の行の <initial-checksum> エントリは、以前の書き込みに関連付けられたエントリと最新の書き込みに関連付けられたエントリを区別するのに役立ちます。

次に、バインディングファイルの例を示します。

```
3ebe1518

TYPE DHCP-SNOOPING

VERSION 1

BEGIN

1.1.1.1 512 0001.0001.0005 3EBE2881 Gi1/1 e5e1e733

1.1.1.1 512 0001.0001.0002 3EBE2881 Gi1/1 4b3486ec

1.1.1.1 1536 0001.0001.0004 3EBE2881 Gi1/1 f0e02872

1.1.1.1 1024 0001.0001.0003 3EBE2881 Gi1/1 ac41adf9

1.1.1.1 1 0001.0001.0001 3EBE2881 Gi1/1 34b3273e
```

各エントリには、IP アドレス、VLAN、MAC アドレス、リース期間(16 進法) およびバインディングに関連付けられたインターフェイスが含まれます。各エントリの最後には、ファイルの開始からエントリに関連付けられたすべてのバイトの合計を計上するチェックサムがあります。各エントリは、72 バイトのデータで構成され、スペースおよびチェックサムがあとに続きます。

起動時に、算出されたチェックサムが格納されたチェックサムに合致すると、スイッチはファイルからエントリを読み取り、バインディングを DHCP スヌーピング データベースに追加します。算出されたチェックサムが格納されたチェックサムに合致しない場合、ファイルから読み取られたエントリが無視され、失敗したエントリに続くすべてのエントリも無視されます。また、スイッチは、リース時間が期限切れになったファイルのすべてのエントリを無視します(この状況が可能なのは、リース時間が期限切れになった時間を示す場合があるからです)。また、エントリ内で指定されたインターフェイスがシステムにすでに存在しない場合、またはインターフェイスがルータ ポート、または DHCP スヌーピングで信頼されたインターフェイスである場合、ファイルのエントリが無視されます。

スイッチが新しいバインディングを学習した場合、または一部のバインディングを失った場合、スイッチはスヌーピング データベースから修正した一連のエントリをファイルに書き込みます。書き込みでは、実際の書き込みが行われるまで、バッチに対して設定可能な遅延時間内で、可能な限り多くの変更を行うことができます。各転送に関連付けられるのは、完了しない場合に、その後転送が中断されるタイムアウトです。これらのタイマーは、書き込み遅延および中断タイムアウトと呼ばれます。

オプション 82 データ挿入

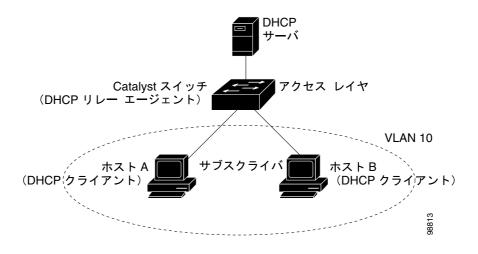
居住、メトロポリタン イーサネット アクセス環境では、DHCP が多数のサブスクライバの IP アドレス割り当てを集中的に管理できます。DHCP オプション 82 機能がスイッチでイネーブルのとき、サブスクライバ デバイスは、(MAC アドレスのほかに) ネットワークへの接続に使用しているスイッチ ポートによって識別されます。サブスクライバ LAN の複数ホストは、アクセス スイッチにある同じポートに接続でき、一意に識別されます。



DHCP オプション 82 機能は、DHCP スヌーピングがグローバルにイネーブルで、この機能を使用しているサブスクライバ デバイスが割り当てられている VLAN 上にある場合にのみサポートされます。

図40-1 に、アクセス レイヤーでスイッチに接続しているサブスクライバに IP アドレスを集中 DHCP サーバが割り当てる、メトロポリタン イーサネット ネットワークの例を示します。 DHCP クライアントとその関連 DHCP サーバが同じ IP ネットワークまたはサブネット上にないため、 DHCP リレー エージェント (Catalyst スイッチ) は、ブロードキャスト転送をイネーブルにし、クライアントとサーバ間で DHCP メッセージを転送するようにヘルパー アドレスで設定されています。

図 40-1 メトロポリタン イーサネット ネットワークの DHCP リレー エージェント



スイッチでの DHCP スヌーピング情報オプション 82 をイネーブルにすると、次のイベントが順に 発生します。

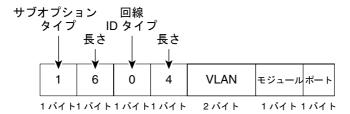
- ホスト(DHCP クライアント)はDHCP 要求を生成し、ネットワーク上でブロードキャストします。
- スイッチが DHCP 要求を受信すると、オプション 82 情報をパケットに追加します。デフォルトでは、リモート ID サブオプションはスイッチの MAC アドレスで、回線 ID サブオプションは、パケットが受信されるポートの識別子 vlan-mod-port です。Cisco IOS Release 12.2(40)SG 以降では、リモート ID および回線 ID を設定できます。これらのサブオプションの設定手順については、「DHCP スヌーピングとオプション 82 のイネーブル化」(p.40-11)を参照してください。
- リレー エージェントの IP アドレスが設定されている場合、スイッチはこの IP アドレスを DHCP パケットに追加します。
- スイッチは、オプション 82 フィールドを含む DHCP 要求を DHCP サーバに転送します。
- DHCP サーバがパケットを受信します。サーバがオプション 82 対応である場合、リモート ID、回線 ID、またはその両方を使用して IP アドレスを割り当て、単一リモート ID または回線 ID に割り当て可能な多数の IP アドレスを制限するようなポリシーを実装できます。DHCP サーバは、DHCP 応答内にオプション 82 フィールドをエコーします。
- 要求がスイッチによってサーバにリレーされた場合、DHCP サーバは応答をスイッチにユニキャストします。スイッチは、リモート ID および場合によっては回線 ID フィールドを検査して、元からオプション 82 データが挿入されたのかどうかを確認します。スイッチはオプション 82 フィールドを削除し、DHCP 要求を送信した DHCP クライアントに接続しているスイッチポートにパケットを転送します。

- 回線 ID サブオプション フィールド
 - サブオプション タイプ
 - サブオプション タイプの長さ
 - 回線 ID タイプ
 - 回線 ID タイプの長さ
- リモート ID サブオプション フィールド
 - サブオプション タイプ
 - サブオプション タイプの長さ
 - リモート ID タイプ
 - リモート ID タイプの長さ

図 40-2 に、デフォルトのサブオプション設定が使用されたときの、リモート ID サブオプションおよび回線 ID サブオプションのパケット形式を示します。回線 ID サブオプションの場合、モジュール番号はスイッチ モジュール番号に対応します。DHCP スヌーピングをグローバルにイネーブルにして、ip dhcp snooping information option グローバル コンフィギュレーション コマンドを開始すると、スイッチはパケット形式を使用します。

図 40-2 サブオプション パケット形式

回線 ID サブオプション フレームの形式



リモート ID サブオプション フレームの形式

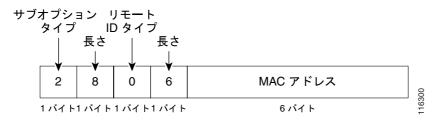


図 40-3 に、ユーザ設定のリモート ID および回線 ID サブオプションのパケット形式を示します。 DHCP スヌーピングがグローバルにイネーブルで、ip dhcp snooping information option format remote-id グローバル コンフィギュレーション コマンドおよび ip dhcp snooping vlan information option format-type circuit-id string インターフェイス コンフィギュレーション コマンドが開始されると、スイッチはこれらのパケット形式を使用します。

パケット内のこれらのフィールドの値は、リモート ID および回線 ID サブオプションを設定すると、デフォルト値から変更されます。

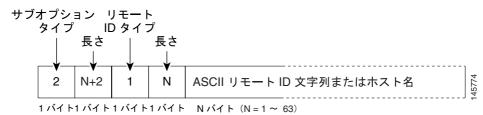
- 回線 ID サブオプション フィールド
 - 回線 ID タイプは 1 です。
 - 長さの値は変数で、設定した文字列の長さによって変わります。
- リモート ID サブオプション フィールド
 - リモート ID タイプは 1 です。
 - 長さの値は変数で、設定した文字列の長さによって変わります。

図 40-3 ユーザ設定サブオプションのパケット形式

回線 ID サブオプション フレームの形式 (ユーザ設定文字列用)



リモート ID サブオプション フレームの形式 (ユーザ設定文字列用)



スイッチ上での DHCP スヌーピングの設定

スイッチ上で DHCP スヌーピングを設定する場合、信頼できるインターフェイスと信頼できないインターフェイスを区別できるようにスイッチを設定します。VLAN で DHCP スヌーピングを使用する前に、DHCP スヌーピングをグローバルにイネーブルにする必要があります。他の DHCP 機能から切り離して DHCP スヌーピングをイネーブルにできます。

DHCP スヌーピングをイネーブルにしたあと、すべての DHCP リレー情報オプション コンフィギュレーション コマンドはディセーブルになります。次のコマンドがあります。

- ip dhcp relay information check
- ip dhcp relay information policy
- ip dhcp relay information trusted
- ip dhcp relay information trust-all

ここでは、DHCP スヌーピングを設定する手順について説明します。

- DHCP スヌーピングのデフォルト設定 (p.40-8)
- DHCP スヌーピングのイネーブル化 (p.40-9)
- 集約スイッチ上での DHCP スヌーピングの設定 (p.40-11)
- DHCP スヌーピングとオプション 82 のイネーブル化 (p.40-11)
- PVLAN 上での DHCP スヌーピングのイネーブル化 (p.40-13)
- DHCP スヌーピング データベース エージェントのイネーブル化 (p.40-13)
- データベース エージェントの設定例(p.40-14)



DHCP サーバの設定については、次の URL の『Cisco IOS IP and IP Routing Configuration Guide』の「Configuring DHCP」を参照してください。

http://www.cisco.com/univered/ec/td/doc/product/software/ios122/122cgcr/ip c/ipcprt1/1cddhcp.htm

DHCP スヌーピングのデフォルト設定

DHCP スヌーピングは、デフォルトでディセーブルに設定されています。表 40-1 に DHCP スヌーピングの各オプションのデフォルト設定値を示します。

表 40-1 DHCP スヌーピングのデフォルト設定値

オプション	デフォルト値 / ステート
DHCP スヌーピング	ディセーブル
dhcp snooping information option	イネーブル
dhcp snooping information option allow-untrusted	ディセーブル
dhcp snooping limit rate	infinite (レート制限のディセーブルと同じよう
	に機能)
dhcp snooping trust	untrusted(信頼性がない)
dhcp snooping vlan	ディセーブル

デフォルト設定値を変更する場合は、「DHCP スヌーピングのイネーブル化」を参照してください。

DHCP スヌーピングのイネーブル化



(注)

DHCP スヌーピングがグローバルにイネーブルに設定されている場合、ポートが設定されるまで DHCP 要求がドロップされます。そのため、作成時ではなく、メンテナンス ウィンドウの間に、この機能を設定する必要がある場合があります。

DHCP スヌーピングをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# ip dhcp snooping	DHCP スヌーピングをグローバルにイネーブルにします。
		DHCP スヌーピングをディセーブルにする場合は、 no キーワードを使用します。
ステップ 2	Switch(config)# ip dhcp snooping vlan number [number] vlan {vlan range}]	VLAN または VLAN 範囲上の DHCP スヌーピング をイネーブルにします。
ステップ 3	Switch(config-if)# ip dhcp snooping trust	インターフェイスの信頼性を trusted または untrusted に設定します。
		信頼できないクライアントからのメッセージを受信するようにインターフェイスを設定する場合は、noキーワードを使用します。
ステップ 4	Switch(config-if)# ip dhcp snooping limit rate rate	インターフェイスが受信できる 1 秒あたりの DHCP パケット数(pps)を設定します。 ¹
ステップ 5	Switch(config)# end	コンフィギュレーション モードを終了します。
ステップ 6	Switch# show ip dhcp snooping	設定を確認します。

^{1.} 信頼できないインターフェイスのレート制限を 101 pps 以上に設定しないことを推奨します。信頼できない各クライアントの 推奨レート制限は、15 pps です。通常、このレート制限が信頼できないインターフェイスに適用されます。信頼できるイン ターフェイスのレート制限を設定する場合、信頼できるインターフェイスはスイッチのすべての DHCP トラフィックを収束 するため、レート制限を高い値に調整する必要があることに注意してください。ネットワーク構成に応じてこのしきい値を調 整する必要があります。CPU が、DHCP パケットを平均速度 1001 pps 以上で受信しないようにしてください。

DHCP スヌーピングは、単一の VLAN または複数の VLAN に設定できます。単一の VLAN を設定するには、VLAN 番号を 1 つ入力します。VLAN の範囲を設定するには、最初と最後の VLAN 番号、またはダッシュと VLAN 範囲を入力します。

次に、VLAN 500 ~ 555 の DHCP スヌーピングをイネーブルにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config) # ip dhcp snooping
Switch(config) # ip dhcp snooping vlan 500 555
Switch(config)# ip dhcp snooping information option format remote-id string switch123
Switch(config) # interface GigabitEthernet 5/1
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)# ip dhcp snooping limit rate 100
Switch(config-if)# ip dhcp snooping vlan 555 information option format-type circuit-id
string customer-555
Switch(config-if)# interface FastEthernet 2/1
Switch(config-if)# ip dhcp snooping vlan 555 information option format-type circuit-id
string customer-500
Switch(config)# end
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
DHCP snooping is operational on following VLANs:
500,555
DHCP snooping is configured on the following L3 Interfaces:
Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
    remote-id: switch123 (string)
Option 82 on untrusted port is not allowed Verification of hwaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:
Interface
                            Trusted
                                        Rate limit (pps)
                              -----
FastEthernet5/1
                                        100
                             ves
 Custom circuit-ids:
   VLAN 555: customer-555
FastEthernet2/1
                            no
                                       unlimited
 Custom circuit-ids:
    VLAN 500: customer-500
Switch#
```

次の設定では、ルーティングが別の Catalyst スイッチ (たとえば、Catalyst 6500 シリーズ スイッチ) で定義された場合の DHCP スヌーピング設定手順について説明しています。

```
// Trust the uplink gigabit Ethernet trunk port
interface range GigabitEthernet 1/1 ñ 2
switchport mode trunk
switchport trunk encapsulation dot1q
ip dhcp snooping trust
!
interface VLAN 14
ip address 10.33.234.1 255.255.254.0
ip helper-address 10.5.1.2
```



アップリンク ギガビット インターフェイスでトランキングがイネーブルであり、Catalyst 6500 シリーズ スイッチに上記ルーティング設定が定義されている場合は、Option 82 を追加する (Catalyst 4500 シリーズ スイッチ上の) ダウンストリーム DHCP スヌーピングとの「信頼」関係を設定する必要があります。Catalyst 6500 シリーズ スイッチでこの作業を実行するには、ip dhcp relay information trusted VLAN コンフィギュレーション コマンドを使用します。

集約スイッチ上での DHCP スヌーピングの設定

集約スイッチ上で DHCP スヌーピングをイネーブルにするには、信頼できないスヌーピング ポートとしてダウンストリーム スイッチに接続するインターフェイスを設定します。ダウンストリーム スイッチ(または集約スイッチと DHCP クライアント間のパスにある DSLAM などのデバイス)が、DHCP パケットに DHCP Option 82 情報を追加すると、信頼できないスヌーピング ポート上に着信した DHCP パケットはドロップされます。 ip dhcp snooping information option allow-untrusted グローバル コンフィギュレーション コマンドが設定された集約スイッチは、任意の信頼できないスヌーピング ポートからの Option 82 情報を持つ DHCP 要求を受け入れることができます。

DHCP スヌーピングとオプション 82 のイネーブル化

スイッチで DHCP スヌーピングとオプション 82 をイネーブルにするには、次の手順を実行します。

	コマンド	目的			
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。			
ステップ 2	Switch(config)# ip dhcp snooping	DHCP スヌーピングをグローバルにイネーブルにします。			
ステップ 3	Switch(config)# ip dhcp snooping vlan vlan-range	VLAN または VLAN 範囲で DHCP スヌーピングをイネーブルにします。有効範囲は $1 \sim 4094$ です。			
		入力できるのは、VLAN ID 番号で識別される VLAN ID、カンマで区切られた一連の VLAN ID、ハイフンで区切られた VLAN ID の範囲、またはスペースで区切られた開始 VLAN ID と終了 VLAN ID を入力して区切られた VLAN ID の範囲です。			
ステップ 4	Switch(config)# ip dhcp snooping information option	スイッチが、転送された DHCP 要求メッセージにある DHCP リレー情報(オプション 82 フィールド)を DHCI サーバに挿入したり削除したりできるようにイネーブルにします。これはデフォルト設定です。 (任意)リモート ID サブオプションを設定します。			
ステップ 5	Switch(config)# ip dhcp snooping information option format remote-id	(任意)リモート ID サブオプションを設定します。			
	[string ASCII-string hostname]	次になるようにリモート ID を設定できます。			
		63 文字までの ASCII 文字 (スペースなし) の文字列			
		スイッチの設定済みホスト名			
		(注) ホスト名が 63 文字以上の場合、リモート ID 設定では 63 文字に切り捨てられます。			
		デフォルトのリモート ID は、スイッチの MAC アドレスです。			
ステップ 6	Switch(config)# ip dhcp snooping information option allow-untrusted	(任意)スイッチが、エッジスイッチに接続された集約スイッチである場合、エッジスイッチからのオプション 82情報付き着信 DHCP スヌーピングパケットを受け入れるようにスイッチ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。			
		(注) このコマンドは、信頼できるデバイスに接続されて いる集約スイッチにのみ入力します。			

	コマンド	目的		
ステップ 7	Switch(config)# interface interface-id	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。		
ステップ 8	Switch(config-if)# ip dhcp snooping vlan vlan information option format-type circuit-id string ASCII-string	(任意)指定したインターフェイスの回線 ID サブオプションを設定します。		
	ibeli beling	1 ~ 4094 の範囲内の VLAN ID を使用して、VLAN およびポート識別子を指定します。デフォルトの回線 ID はポートID で、形式は vlan-mod-port です。		
		回線 ID が 3 ~ 63 文字の ASCII 文字 (スペースなし) の文字列になるように設定できます。		
ステップ 9	<pre>Switch(config-if)# ip dhcp snooping trust</pre>	(任意) インターフェイスの信頼性を trusted または untrusted に設定します。信頼できないクライアントからのメッセージを受信するようにインターフェイスを設定する場合は、no キーワードを使用します。デフォルト設定は信頼できない状態です。		
ステップ 10	<pre>Switch(config-if)# ip dhcp snooping limit rate rate</pre>	(任意)インターフェイスが受信できる 1 秒あたりの DHCP パケット数を設定します。指定できる範囲は 1 ~ 2048 です。デフォルトでは、レート制限は設定されていません。		
		(注) 信頼できないレート制限は、最高で毎秒 100 パケットを推奨します。信頼できるインターフェイスのレート制限を設定する場合、ポートが、DHCP スヌーピングがイネーブルになっている複数のVLAN に割り当てられたトランク ポートであると、レート制限を増やす必要があります。		
ステップ 11	Switch(config-if)# exit	グローバル コンフィギュレーション モードに戻ります。		
	Switch(config)# ip dhcp snooping verify mac-address	(任意)信頼できないポートで受信される DHCP パケットにある送信元 MAC アドレスが、パケット内のクライアント ハードウェア アドレスに一致するかどうかを、スイッチが確認するように設定します。 デフォルトでは、送信元MAC アドレスがパケット内のクライアント ハードウェアアドレスに一致することを確認します。		
	Switch(config)# end	特権 EXEC モードに戻ります。		
	Switch# show running-config	入力を確認します。		
ステップ 15	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。		

DHCP スヌーピングをディセーブルにするには、no ip dhcp snooping グローバル コンフィギュレーション コマンドを使用します。VLAN または VLAN 範囲で DHCP スヌーピングをディセーブルに するには、no ip dhcp snooping vlan vlan-range グローバル コンフィギュレーション コマンドを使用します。オプション 82 フィールドの挿入および削除をディセーブルにするには、no ip dhcp snooping information option グローバル コンフィギュレーション コマンドを使用します。集約スイッチがエッジスイッチからのオプション 82 情報付き着信 DHCP スヌーピング パケットをドロップするように設定するには、no ip dhcp snooping information option allow-untrusted グローバル コンフィギュレーション コマンドを使用します。

次に、DHCP スヌーピングをグローバルにおよび VLAN 10 でイネーブルにし、ポートで毎秒 100 パケットのレート制限を設定する例を示します。

Switch(config) # ip dhcp snooping
Switch(config) # ip dhcp snooping vlan 10
Switch(config) # ip dhcp snooping information option
Switch(config) # interface gigabitethernet2/0/1
Switch(config-if) # ip dhcp snooping limit rate 100

PVLAN 上での DHCP スヌーピングのイネーブル化

DHCP スヌーピングを Private VLAN (PVLAN)でイネーブルにして、同一 VLAN 内のレイヤ 2 ポートを分離できます。 DHCP スヌーピングがイネーブル (ディセーブル) の場合、設定はプライマリ VLAN および関連付けられたセカンダリ VLAN の両方に伝播します。この設定変更をセカンダリ VLAN に反映させずに、プライマリ VLAN の DHCP スヌーピングをイネーブル (ディセーブル)にすることはできません。

セカンダリ VLAN で DHCP スヌーピングを設定することは可能ですが、関連付けられたプライマリ VLAN で DHCP スヌーピングを設定しないと有効になりません。関連付けられたプライマリ VLAN が設定されている場合、対応するプライマリ VLAN によってセカンダリ VLAN の DHCP スヌーピング モードが有効になります。セカンダリ VLAN で DHCP スヌーピングを手動で設定すると、スイッチで次の警告メッセージが発行されます。

DHCP Snooping configuration may not take effect on secondary vlan XXX

show ip dhcp snooping コマンドは、DHCP スヌーピングがイネーブルのすべての VLAN (プライマリおよびセカンダリの両方)を表示します。

DHCP スヌーピング データベース エージェントのイネーブル化

データベース エージェントを設定するには、次の作業を1つまたは複数行います。

コマンド	目的
Switch(config)# ip dhcp snooping database { url write-delay seconds timeout seconds }	(必須)データベース エージェント (またはファイル)の URL および関連付けられたタイムアウト値を設定します。
<pre>Switch(config)# no ip dhcp snooping database [write-delay timeout]</pre>	
Switch# show ip dhcp snooping database [detail]	(任意)データベース エージェントの現在の動作ステート および転送に関連付けられた統計情報を表示します。
Switch# clear ip dhcp snooping database statistics	(任意)データベース エージェントに関連付けられた統計 情報をクリアします。
Switch# renew ip dhcp snooping database [validation none] $[ur1]$	(任意)所定の URL のファイルからの読み取りエントリを要求します。
Switch# ip dhcp snooping binding mac-addr vlan vlan ipaddr interface ifname expiry lease-in-seconds	(任意)スヌーピング データベースのバインディングを追加または削除します。
Switch# no ip dhcp snooping binding mac-addr vlan vlan ipaddr interface ifname	



(注)

NVRAM(不揮発性 RAM)およびブートフラッシュの保存容量は限られているので、TFTP またはネットワークベースのファイルを使用してください。フラッシュにデータベース ファイルを保存する場合は、エージェントによって新しく更新されると新しいファイルが作成されます(フラッシュがすぐにいっぱいになります)。さらに、フラッシュで使用するファイルシステムの性質上、ファイル数が多いとアクセスが遅くなります。TFTP からアクセス可能なリモート ロケーションにファイルが格納されている場合、RPR/SSO スタンバイ スーパーバイザ エンジンはスイッチオーバーが発生したときにバインディング リストを引き継ぐことができます。



(注)

ネットワークベースの URL (TFTP および FTP [ファイル転送プロトコル] など) では、スイッチが最初に一連のバインディングを書き込む前に、設定された URL に空のファイルを作成することが必要です。

データベース エージェントの設定例

次に、前述のコマンドを使用する例を示します。

例1: データベース エージェントのイネーブル化

Switch#

次に、DHCP スヌーピング データベース エージェントを設定して、所定のロケーションにバインディングを格納し、設定および動作ステートを表示する例を示します。

```
Switch# configure terminal
Switch(config) # ip dhcp snooping database tftp://10.1.1.1/directory/file
Switch(config)# end
Switch# show ip dhcp snooping database detail
Agent URL: tftp://10.1.1.1/directory/file
Write delay Timer: 300 seconds
Abort Timer: 300 seconds
Agent Running: No
Delay Timer Expiry : 7 (00:00:07)
Abort Timer Expiry : Not Running
Last Succeded Time : None
Last Failed Time: 17:14:25 UTC Sat Jul 7 2001
Last Failed Reason : Unable to access URL.
                          21 Startup Failures:
Total Attempts
                :
                          0 Failed Transfers:
Successful Transfers :
                                                      21
Successful Reads :
                          0 Failed Reads :
                          O Failed Writes :
Successful Writes
                                                       2.1
Media Failures
First successful access: Read
Last ignored bindings counters :
Binding Collisions : 0
                                Expired leases
                           0
Tnvalid interfaces
                                Unsupported vlans:
Parse failures
                    :
Last Ignored Time : None
Total ignored bindings counters:
Binding Collisions : 0 Expired leases
Invalid interfaces
                           0 Unsupported vlans :
Parse failures
                           0
                   :
```

出力の最初の3行は、設定されたURLおよび関連付けられたタイマー設定値を表示します。次の3行は、動作ステートおよび書き込み遅延時間および中断タイマーの残りの時間を表示します。

出力に表示される統計情報のうち、Startup Failures は起動時のファイル読み込みまたは作成に失敗した試行回数を示します。



(注)

ロケーションはネットワークに基づいているので、TFTP サーバに一時ファイルを作成する必要があります。TFTP サーバデーモンが参照できるようにディレクトリ [directory] に 0 バイトのファイル [file] を作成して、標準的な UNIX ワークステーション上に一時ファイルを作成できます。UNIX ワークステーションのサーバ実装の一部では、ファイルへの書き込みに対して完全な (777) 許可がファイルに必要です。

DHCP スヌーピング バインディングは、MAC アドレスおよび VLAN の組み合わせに適合しています。したがって、スイッチがすでにバインディングを所有する、所定の MAC アドレスと VLAN の組み合わせのエントリがリモート ファイルにある場合、ファイルが読み取られるときにリモートファイルからのエントリは無視されます。この状態をバインディング コリジョンといいます。

エントリに指定されたリースが読み取られた時間によって期限切れになった可能性があるので、ファイルのエントリが無効になる可能性があります。Expired leases カウンタは、この状態によって無視されたバインディング数を示します。Invalid interfaces カウンタは読み取りの際に、エントリで指定されたインターフェイスがシステムに存在しない場合、またはインターフェイスが存在する場合は、それがルータ、または DHCP スヌーピングで信頼されたインターフェイスのどちらかであるために無視されたバインディング数を示します。Unsupported vlans は、指定された VLAN がシステムによってサポートされないために無視されたエントリ数を示します。Parse failures カウンタは、スイッチがファイルのエントリの意味を解釈できなかった場合に無視されたエントリ数を示します。

スイッチは、このような無視されたバインディングに対して2組のカウンタを維持します。1つは、このような状態の少なくとも1つによって無視されたバインディングを、少なくとも1つ持つ読み取りのカウンタを提供します。このようなカウンタは[Last ignored bindings counters] として表示されます。[Total ignored bindings counters] は、スイッチの起動後、すべての読み取りによって無視されたバインディングの総数を提供します。この2組のカウンタは、clear コマンドによってクリアされます。したがって、総数カウンタは、最後にクリアが行われてから無視されたバインディング数を示す場合があります。

例2:TFTP ファイルからのパインディング エントリの読み取り

手動で TFTP ファイルのエントリを読み取るには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# show ip dhcp snooping database	DHCP スヌーピング データベース エージェントの統計情
		報を表示します。
ステップ 2	Switch# renew ip dhcp snoop data url	所定の URL からファイルを読み取るようにスイッチに指
		示します。
ステップ 3	Switch# show ip dhcp snoop data	読み取りステータスを表示します。
ステップ 4	Switch# show ip dhcp snoop bind	バインディングが正常に読み取られたことを確認します。

次に、手動で tftp://10.1.1.1/directory/file からエントリを読み取る例を示します。

```
Switch# showb ip dhcp snooping database
Agent URL :
Write delay Timer : 300 seconds
Abort Timer: 300 seconds
Agent Running: No
Delay Timer Expiry : Not Running
Abort Timer Expiry : Not Running
Last Succeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.
Total Attempts : U Scarcap :...

Successful Transfers : 0 Failed Transfers :

Successful Reads : 0 Failed Writes :
Successful Reads : Successful Writes :
                            0 Failed Writes
Media Failures
Switch#
Switch# renew ip dhcp snoop data tftp://10.1.1.1/directory/file
Loading directory/file from 10.1.1.1 (via GigabitEthernet1/1): !
[OK - 457 bytes]
Database downloaded successfully.
00:01:29: %DHCP_SNOOPING-6-AGENT_OPERATION_SUCCEEDED: DHCP snooping database Read
succeeded.
Switch#
Switch# show ip dhcp snoop data
Agent URL :
Write delay Timer: 300 seconds
Abort Timer: 300 seconds
Agent Running : No
Delay Timer Expiry : Not Running
Abort Timer Expiry: Not Running
Last Succeded Time: 15:24:34 UTC Sun Jul 8 2001
Last Failed Time : None
Last Failed Reason: No failure recorded.
                  :
Total Attempts
                             1 Startup Failures :
Successful Reads
                             1 Failed Transfers:
1 Failed Reads:
Successful Reads :
                   :
                             0 Failed Writes :
Successful Writes
Media Failures
Switch#
Switch# show ip dhcp snoop bind
MacAddress IpAddress
                                    Lease(sec) Type
                                                               VLAN Interface
00:01:00:01:00:05 1.1.1.1 49810 dhcp-snooping 512 GigabitEthernet1/1
                                 49810 dhcp-snooping 512 GigabitEthernet1/1
49810 dhcp-snooping 1536 GigabitEthernet1/1
49810 dhcp-snooping 1024 GigabitEthernet1/1
49810 dhcp-snooping 1 GigabitEthernet1/1
00:01:00:01:00:02 1.1.1.1
00:01:00:01:00:04 1.1.1.1
00:01:00:01:00:03 1.1.1.1
00:01:00:01:00:01 1.1.1.1
Switch#
Switch# clear ip dhcp snoop bind
Switch# show ip dhcp snoop bind
                                                                VLAN Interface
MacAddress IpAddress
                                   Lease(sec) Type
Switch#
```

例3:DHCP スヌーピング データベースへの情報の追加

手動で DHCP スヌーピング データベースにバインディングを追加するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# show ip dhcp snooping binding	DHCP スヌーピング データベースを表示します。
ステップ 2	Switch# ip dhcp snooping binding binding-id vlan vlan-id interface interface expiry lease-time	ip dhcp snooping EXEC コマンドを使用してバイン ディングを追加します。
ステップ 3	Switch# show ip dhcp snooping binding	DHCP スヌーピング データベースを確認します。

次に、手動で DHCP スヌーピング データベースにバインディングを追加する例を示します。

Switch# show ip dho MacAddress	p snooping binding IpAddress	ng Lease(sec)	Туре	VLAN	Interface
Switch# Switch# ip dhcp sno	ooping binding 1.1	.1 vlan 1 1.	1.1.1 interface	gi1/1	expiry 1000
Switch# show ip dho MacAddress	p snooping bindin	ng Lease(sec)	Туре	VLAN	Interface
00:01:00:01:00:01 Switch#	1.1.1.1	992	dhcp-snooping	1	GigabitEthernet1/1

DHCP スヌーピング情報の表示

スイッチ上のすべてのインターフェイスについて、DHCP スヌーピング バインディング テーブル および設定情報を表示できます。

バインディング テーブルの表示

各スイッチの DHCP スヌーピング バインディング テーブルには、信頼できないポートに関連した バインティング エントリが格納されています。テーブルには、trusted ポートに相互接続するホスト に関する情報は収められていません。相互接続した各スイッチは、独自の DHCP スヌーピング バインディング テーブルを持つためです。

次に、スイッチの DHCP スヌーピング バインディング情報を表示する例を示します。

Switch# show ip dhcp snooping binding

MacAddress	IpAddress	Lease(sec)	Туре	VLAN	Interface
	55.5.5.2	6943	dhcp-snooping	10	FastEthernet6/10
Switch#					

表 40-2 で show ip dhcp snooping binding コマンド出力のフィールドを説明します。

表 40-2 show ip dhcp snooping binding コマンド出力

フィールド	説明
MAC Address	クライアント ハードウェア MAC アドレス
IP Address	DHCP サーバから割り当てられたクライアント IP アドレス
Lease(sec)	IP アドレス リース時間 (秒)
タイプ	バインディング タイプ (DHCP スヌーピングによって学習されたダイナミック バインディングまたはスタティックに設定されたバインディング)
VLAN	クライアント インターフェイスの VLAN 番号
インターフェイス	DHCP クライアント ホストに接続したインターフェイス

DHCP スヌーピング設定の表示

次に、スイッチの DHCP スヌーピング設定を表示する例を示します。

Switch# show ip dhcp snooping

Switch DHCP snooping is enabled.

DHCP Snooping is configured on the following VLANs:

10 30-40 100 200-220

Insertion of option 82 is enabled

Option82 on untrusted port is not allowed

Verification of hwaddr field is enabled

Switch#

IP ソース ガードの概要

この機能は、DHCP スヌーピングと同様、DHCP スヌーピングの信頼できないレイヤ 2 ポート上でイネーブルに設定されています。最初に、ポートのすべての IP トラフィックが、DHCP スヌーピング処理によってキャプチャされた DHCP パケットを除いてブロックされます。クライアントがDHCP サーバから有効な IP アドレスを受信する場合、またはユーザがスタティック IP 送信元バインディングを設定した場合に、Per-Port and VLAN Access Control List (PVACL)がポート上にインストールされます。この処理は、クライアント IP トラフィックをバインディングに設定された送信元 IP アドレスに制限するので、IP 送信元バインディングにない送信元 IP アドレスを持つ IP トラフィックが排除されます。このフィルタリングは、ホストがネイバー ホストの IP アドレスを名乗ってネットワークを攻撃することを制限します。



(注)

DHCP スヌーピングがイネーブルにされた大量の VLAN のトランク ポート上で IP ソース ガードが イネーブルにされている場合、ACL ハードウェア リソースが不足し、代わりにパケットの一部が ソフトウェアでスイッチングされる可能性があります。



(注)

IP ソース ガードがイネーブルの場合、ACL ハードウェア プログラミングの代替方式を指定する場合があります。詳細については、第 33 章「ACL によるネットワーク セキュリティの設定」の「TCAM プログラミングおよび ACL」を参照してください。

IP ソース ガードは、アクセスおよびトランクの両方を含むレイヤ 2 ポートだけをサポートしています。それぞれの信頼できないレイヤ 2 ポートには、2 つのレベルの IP トラフィック セキュリティフィルタリングがあります。

送信元 IP アドレス フィルタ

スから削除されます。

フィックだけが許可されます。

IP トラフィックは、送信元 IP アドレスに基づいてフィルタリングされます。IP 送信元バインディング エントリに一致する送信元 IP アドレスを持つ IP トラフィックだけが許可されます。新しい IP 送信元エントリ バインディングがポートで作成または削除されると、IP 送信元アドレス フィルタが変更されます。IP 送信元バインディングの変更を反映するために、ポートPVACL がハードウェアで再計算および再適用されます。デフォルトでは、ポートに IP 送信元バインディングがない状態で IP フィルタがイネーブルにされている場合、すべての IP トラフィックを拒否するデフォルトの PVACL がポートにインストールされます。同様に、IP フィルタがディセーブルにされている場合、すべての IP 送信元フィルタ PVACL がインターフェイ

送信元 IP および MAC アドレス フィルタ
 IP トラフィックは送信元 IP アドレスと MAC アドレスに基づいてフィルタリングされます。IP 送信元バインディング エントリに一致する送信元 IP アドレスと MAC アドレスを持つ IP トラ



(注)

IP ソース ガードが IP と MAC フィルタリング モードでイネーブルに設定されている場合、DHCP プロトコルが正常に稼働するように、DHCP スヌーピング Option 82 がイネーブルに設定されている必要があります。Option 82 データがないと、スイッチは DHCP サーバ応答を転送するようにクライアント ホスト ポートを設置できません。そして、DHCP サーバ応答がドロップされ、クライアントは IP アドレスを取得できなくなります。

スイッチ上での IP ソース ガードの設定

IP ソース ガードをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# ip dhcp snooping	DHCP スヌーピングをグローバルにイネーブルにします。
		DHCP スヌーピングをディセーブルにする場合は、 no キーワードを使用します。
ステップ 2	Switch(config)# ip dhcp snooping vlan number [number]	VLAN 上で DHCP スヌーピングをイネーブルにします。
ステップ 3	Switch(config-if)# no ip dhcp snooping trust	インターフェイスの信頼性を trusted または untrusted に設定します。
		ネットワーク内からのメッセージのみを受信するようにインターフェイスを設定する場合は、no キーワードを使用します。
ステップ 4	Switch(config-if)# ip verify source vlan dhcp-snooping port-security	ポート上の IP ソース ガード、送信元 IP、および送信元 MAC アドレス フィルタリングをイネーブルにします。
ステップ 5	Switch(config-if)# switchport port-security limit rate invalid-source-mac N	ポート上の学習済み送信元 MAC アドレスに対してセキュリティ レート制限をイネーブルにします。
		(注) この制限は、IP および MAC アドレスの両方をフィルタリングするように IP ソース ガードがイネーブルにされたポートにのみ適用されます。
ステップ 6	Switch(config)# ip source binding mac-address Vlan vlan-id ip-address interface interface-name	ポート上にスタティック IP バインディングを設定します。
ステップ 7	Switch(config)# end	コンフィギュレーション モードを終了します。
ステップ 8	Switch# show ip verify source interface interface-name	設定を確認します。

インターフェイス上のスタティック ホストを使用して IP ソース ガードを停止したい場合、インターフェイス コンフィギュレーション サブモードで次のコマンドを使用します。

Switch(config-if)# no ip verify source
Switch(config-if)# no ip device tracking max"

インターフェイス コンフィギュレーション サブモードで「no ip device tracking」が使用されている場合、このコマンドは変換され、実際にグローバル コンフィギュレーション モードで実行されて、IP デバイス トラッキングがグローバルにディセーブルになります。「ip verify source tracking [port-security]」というコマンドを使用するすべてのインターフェイスでは、IP デバイス トラッキングがグローバルにディセーブルになると、スタティックホストを使用する IP ソース ガードが、これらのインターフェイスからのすべての IP トラフィックを拒否するようになります。



(注)

スタティック IP 送信元バインディングが設定できるのは、スイッチ ポート上だけです。レイヤ 3 ポートで ip source binding vlan interface コマンドを実行すると、次のエラーメッセージが表示されます。Static IP source binding can only be configured on switch port.

次に、VLAN 10~20 上でレイヤ 2 ポートごとの IP ソース ガードをイネーブルにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config) # ip dhcp snooping
Switch(config) # ip dhcp snooping vlan 10 20
Switch(config)# interface fa6/1
Switch(config-if) # switchport trunk encapsulation dot1q
Switch(config-if) # switchport mode trunk
Switch(config-if) # switchport trunk native vlan 10
Switch(config-if) # switchport trunk allowed vlan 11-20
Switch(config-if) # no ip dhcp snooping trust
Switch(config-if) # ip verify source vlan dhcp-snooping
Switch(config)# end
Switch# show ip verify source interface f6/1
Interface Filter-type Filter-mode IP-address
                                                   Mac-address
                                                                       Vlan
                      active
                                    10.0.0.1
          ip-mac
                                                                        10
         ip-mac
Fa6/1
                                                                       11 - 20
                       active
                                   deny-all
Switch#
```

この出力は、VLAN 10 に有効な DHCP バインディングが 1 つあることを示します。

PVLAN 上での IP ソース ガードの設定

PVLAN ポートでは、IP ソース ガードを有効にするためにプライマリ VLAN 上で DHCP スヌーピングをイネーブルにする必要があります。プライマリ VLAN 上の IP ソース ガードは、自動的にセカンダリ VLAN に伝播されます。セカンダリ VLAN 上にスタティック IP 送信元バインディングを設定することはできますが、有効ではありません。手動でセカンダリ VLAN 上にスタティック IP 送信元バインディングを設定すると、次の意味の警告が表示されます。



IP 送信元フィルタは、IP 送信元バインディングが設定されたセカンダリ VLAN では有効にならない可能性があります。PVLAN 機能がイネーブルにされている場合、プライマリ VLAN 上の IP 送信元フィルタがすべてのセカンダリ VLAN に自動的に伝播されます。

IP ソース ガード情報の表示

スイッチ上のすべてのインターフェイスの IP ソース ガード PVACL 情報を表示するには、show ip verify source コマンドを使用します。

• 次に、VLAN 10 ~ 20 で DHCP スヌーピングがイネーブルにされていて、IP フィルタリングに 対してインターフェイス fa6/1 が設定されていて、VLAN 10 に既存の IP アドレス バインディ ング 10.0.01 が存在する場合に表示される PVACL の例を示します。

Interface	Filter-type	Filter-mode	IP-address	Mac-address	Vlan
fa6/1	ip	active	10.0.0.1		10
fa6/1	ip	active	deny-all		11-20



2番めのエントリは、デフォルト PVACL (すべての IP トラフィックを拒否)が、有効な IP 送信元 バインディングを持たず、スヌーピングがイネーブルにされた VLAN のポート上にインストール されていることを示します。

• 次に、trusted ポートに対して表示される PVACL の例を示します。

Interface	Filter-type	Filter-mode	IP-address	Mac-address	Vlan
fa6/2	ip	inactive-tru			

• 次に、DHCP スヌーピングが設定されていない VLAN のポートに対して表示される PVACL の 例を示します。

Interface	Filter-type	Filter-mode	IP-address	Mac-address	Vlan
fa6/3	ip	inactive-no-			

• 次に、複数のバインディングが IP/MAC フィルタリングに設定されているポートに対して表示 される PVACL の例を示します。

Interface	Filter-type	Filter-mode	IP-address	Mac-address	Vlan
fa6/4	ip-mac	active	10.0.0.2	aaaa.bbbb.cccc	10
fa6/4	ip-mac	active	11.0.0.1	aaaa.bbbb.cccd	11
fa6/4	ip-mac	active	deny-all	deny-all	12-20

次に、ポートセキュリティが設定されておらず、IP/MACフィルタリングが設定されているポー トに対して表示される PVACL の例を示します。

Interface	Filter-type	Filter-mode	IP-address	Mac-address	Vlan
fa6/5	ip-mac	active	10.0.0.3	permit-all	10
fa6/5	ip-mac	active	deny-all	permit-all	11-20



(注) MAC フィルタで permit-all が表示されるのは、ポート セキュリティがイネーブルにさ れていないためです。MAC フィルタはポート /VLAN に適用できず、事実上ディセー ブルの状態です。常にポート セキュリティを最初にイネーブルにしてください。

• 次に、IP 送信元フィルタ モードが設定されていないポートに show ip verify source コマンドを 入力した場合に表示されるエラー メッセージの例を示します。

IP Source Guard is not configured on the interface fa6/6.

また、show ip verify source コマンドを使用して、IP ソース ガードがイネーブルにされたスイッチ上のすべてのインターフェイスを表示できます。

Interface	Filter-type	Filter-mode	IP-address	Mac-address	Vlan
fa6/1	ip	active	10.0.0.1		10
fa6/1	ip	active	deny-all		11-20
fa6/2	ip	inactive-tru	st-port		
fa6/3	ip	inactive-no-	snooping-vlan		
fa6/4	ip-mac	active	10.0.0.2	aaaa.bbbb.cccc	10
fa6/4	ip-mac	active	11.0.0.1	aaaa.bbbb.cccd	11
fa6/4	ip-mac	active	deny-all	deny-all	12-20
fa6/5	ip-mac	active	10.0.0.3	permit-all	10
fa6/5	ip-mac	active	deny-all	permit-all	11-20

IP 送信元パインディング情報の表示

スイッチ上のすべてのインターフェイス上に設定された IP 送信元バインディングを表示するには、 show ip source binding コマンドを使用します。

Switch#	show	ip	source	binding
---------	------	----	--------	---------

MacAddress	IpAddress	Lease(sec)	Туре	VLAN	Interface
00:02:B3:3F:3B:99 00:00:00:0A:00:0B	55.5.5.2 11.0.0.1	6522 infinite	dhcp-snooping static	10 10	FastEthernet6/10 FastEthernet6/10

表 40-3 で show ip source binding コマンド出力のフィールドについて説明します。

表 40-3 show ip source binding コマンド出力

フィールド	説明
MAC Address	クライアント ハードウェア MAC アドレス
IP Address	DHCP サーバから割り当てられたクライアント IP アドレス
Lease(sec) IP アドレス リース時間 (秒)	
タイプ	バインディング タイプ (CLI [コマンドライン インターフェイス] から設定されたスタティック バインディング、および DHCP スヌーピングによって学習されたダイナミック バインディング)
VLAN	クライアント インターフェイスの VLAN 番号
インターフェイス	DHCP クライアント ホストに接続したインターフェイス

スタティック ホストの IP ソース ガードの設定



Supervisor Engine 6-E は、この機能をサポートして*いません*。



スタティック ホストの IPSG は、アップリンク ポートでは使用しないでください。

スタティック ホストの IP ソース ガード (IPSG) は、IPSG 機能を非 DHCP およびスタティック環境に拡張します。既存の IPSG 機能は、DHCP スヌーピング機能により作成されたエントリを使用して、スイッチに接続されたホストを検証します。有効な DHCP バインディング エントリを持たないホストから受信されたトラフィックは、ドロップされます。基本的に、DHCP 環境は IPSG が機能するための前提条件になります。スタティック ホストの IPSG 機能は、DHCP に対する IPSG の依存性を削除します。スイッチは、ARP 要求または他の IP パケットに基づいてスタティック エントリを作成し、このエントリを使用して指定ポートの有効なホストのリストを保持します。さらに、ユーザは、指定ポートにトラフィックを送信できるホスト数を指定できます。これは、レイヤー3 でのポート セキュリティに相当します。



(注)

複数ネットワーク インターフェイスを持つ一部の IP ホストは、一部の無効パケットをネットワーク インターフェイスに投入することがあります。これらの無効パケットには、送信元アドレスとしてのホストの別のネットワーク インターフェイスの IP/MAC アドレスを含みます。これにより、ホストに接続しているスイッチにあるスタティック ホストの IIPSG が、無効な IP/MAC アドレスバインディングを学習し、有効なバインディングを拒否します。無効パケットの投入を回避するには、対応する OS またはそのホストのネットワーク デバイスのベンダーに相談する必要があります。

スタティック ホストの IPSG は、最初に ACL ベースのスヌーピング メカニズムを介して動的に IP・MAC バインディングを学習します。IP/MAC バインディングは、ARP および IP パケットを経由してスタティック ホストから学習され、デバイス トラッキング データベースを使用して保存されます。指定ポートでダイナミックに学習された、またはスタティックに設定された IP アドレスの数が最大限度に達すると、新しい IP アドレスを持つパケットはハードウェアでドロップされます。何らかの理由で移動されたまたは消去されたホストを扱うために、スタティック ホストの IPSG 機能は IP デバイス トラッキング機能を強化し、ダイナミックに学習した IP アドレス バインディングをエージング アウトします。この機能は、DHCP スヌーピングと同時に使用できます。複数バインディングが、DHCP とスタティック ホストの両方に接続されているポート上で確立されます(つまり、バインディングは、デバイス トラッキング データベースだけでなく、DHCP スヌーピング バインディング データベースにも保存されます)。

次の内容について説明します。

- レイヤ 2 アクセス ポート上のスタティック ホストの IPSG (p.40-26)
- PVLAN ホスト ポート上のスタティック ホストの IPSG (p.40-29)

レイヤ 2 アクセス ポート上のスタティック ホストの IPSG

レイヤ 2 アクセス ポート上でスタティック ホストの IPSG を設定できます。

レイヤ 2 アクセス ポート上で IP フィルタを使用してスタティック ホストの IPSG をイネーブルに するには、次の作業を実行します。

	コマンド	目的
ステップ 1	Switch(config)# ip device tracking	IP ホスト テーブルをオンにします。
ステップ 2	Switch(config)# interface fastEthernet 	IP コンフィギュレーション モードを開始します。
ステップ 3	Switch(config-if)# switchport mode access	アクセスとしてポートを設定します。
ステップ 4	Switch(config-if)# switchport access vlan <n></n>	このポートに VLAN を設定します。
ステップ 5	<pre>Switch(config-if)# ip device tracking maximum <n></n></pre>	このポート上でバインディングの最大限度を確立します。
		最大限度は 10 です。
ステップ 6	Switch(config-if)# switchport port-security	(任意)このポートのポート セキュリティをアク ティブにします。
ステップ 7	<pre>Switch(config-if)# switchport port-security maximum <n></n></pre>	(任意) このポートの MAC アドレスの最大数を確立 します。
ステップ 8	<pre>Switch(config-if)# ip verify source tracking [port-security]</pre>	このポート上でスタティック ホストの IPSG をアク ティブにします。
ステップ 9	Switch(config-if)# end	インターフェイス コンフィギュレーション モード を終了します。
ステップ 10	Switch# show ip verify source interface-name	設定を確認します。
ステップ 11	Switch# show ip device track all [active inactive] count	スイッチ インターフェイス上の指定ホストの IP/MAC バインディングを表示して、設定を確認し ます。
		• all active アクティブな IP/MAC バインディング エントリだけを表示します。
		• all inactive 非アクティブな IP/MAC バイン ディング エントリだけを表示します。
		• all アクティブおよび非アクティブの IP/MAC バインディング エントリを表示します。

インターフェイス上でスタティック ホストの IPSG を停止するには、インターフェイス コンフィギュレーション サブモードで次のコマンドを使用します。

Switch(config-if)# no ip verify source
Switch(config-if)# no ip device tracking max"

ポート上でスタティック ホストの IPSG をイネーブルにするには、次のコマンドを実行します。

Switch(config)# ip device tracking ****enable IP device tracking globally Switch(config)# ip device tracking max <n> ****set an IP device tracking maximum on int Switch(config-if)# ip verify source tracking [port-security] ****activate IPSG on the port



IP デバイス トラッキングをグローバルにイネーブルにせずに、またはそのインターフェイス上の IP デバイス トラッキングの最大値を設定せずに、ポートで ip verify source tracking [port-security] インターフェイス コンフィギュレーション コマンドだけを設定した場合、スタティック ホストの IPSG は、そのインターフェイスからのすべての IP トラフィックを拒否します。



上記の問題は、PVLAN ホスト ポート上のスタティック ホストの IPSG にも適用されます。

次に、レイヤ 2 アクセス ポートでの IP フィルタを使用したスタティック ホストの IPSG をイネーブルにし、インターフェイス Fa4/3 上で 3 つの有効 IP バインディングを確認する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface fastEthernet 4/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# ip verify source tracking
```

Switch# show ip verify source

Switch(config-if)# end

Interface	Filter-type	Filter-mode	IP-address	Mac-address	Vlan
Fa4/3	ip trk	active	40.1.1.24		10
Fa4/3	ip trk	active	40.1.1.20		10
Fa4/3	ip trk	active	40.1.1.21		10

次に、レイヤ 2 アクセス ポートで IP/MAC フィルタを使用してスタティック ホストの IPSG をイネーブルにし、インターフェイス Fa4/3 上の 5 つの有効 IP/MAC バインディングを確認して、このインターフェイス上のバインディング数が最大限度に達したかどうかを確認する例を示します。

Switch# configure terminal

```
Enter configuration commands, one per line. End with CNTL/Z. Switch(config)# ip device tracking
Switch(config)# interface fastEthernet 4/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)# ip verify source tracking port-security
Switch(config-if)# end
```

Switch# show ip verify source

Interface	Filter-type	Filter-mode	IP-address	Mac-address	Vlan
Fa4/3	ip-mac trk	active	40.1.1.24	00:00:00:00:03:04	1
Fa4/3	ip-mac trk	active	40.1.1.20	00:00:00:00:03:05	1
Fa4/3	ip-mac trk	active	40.1.1.21	00:00:00:00:03:06	1
Fa4/3	ip-mac trk	active	40.1.1.22	00:00:00:00:03:07	1
Fa4/3	ip-mac trk	active	40.1.1.23	00:00:00:00:03:08	1

次に、すべてのインターフェイスのすべての IP/MAC バインディングを表示する例を示します。CLI で非アクティブ エントリと一緒にすべてのアクティブ エントリが表示されていることを確認します。インターフェイス上でホストが学習されるとき、新しいエントリにアクティブのマークが付けられます。同じホストが現在のインターフェイスから切断され、別のインターフェイスの接続され

ると、ホストが検出され次第、新しい IP/MAC バインディング エントリがアクティブとして表示されます。ここで、前のインターフェイス上のこのホストの古いエントリは、非アクティブとしてマークが付けられます。

Switch# show ip device tracking all

- IP Device Tracking = Enabled
- IP Device Tracking Probe Count = 3
- IP Device Tracking Probe Interval = 30

IP Address	MAC Address	Vlan	Interface	STATE
200.1.1.8	0001.0600.0000	8	GigabitEthernet3/1	INACTIVE
200.1.1.9	0001.0600.0000	8	GigabitEthernet3/1	INACTIVE
200.1.1.10	0001.0600.0000	8	GigabitEthernet3/1	INACTIVE
200.1.1.1	0001.0600.0000	9	GigabitEthernet4/1	ACTIVE
200.1.1.1	0001.0600.0000	8	GigabitEthernet3/1	INACTIVE
200.1.1.2	0001.0600.0000	9	GigabitEthernet4/1	ACTIVE
200.1.1.2	0001.0600.0000	8	GigabitEthernet3/1	INACTIVE
200.1.1.3	0001.0600.0000	9	GigabitEthernet4/1	ACTIVE
200.1.1.3	0001.0600.0000	8	GigabitEthernet3/1	INACTIVE
200.1.1.4	0001.0600.0000	9	GigabitEthernet4/1	ACTIVE
200.1.1.4	0001.0600.0000	8	GigabitEthernet3/1	INACTIVE
200.1.1.5	0001.0600.0000	9	GigabitEthernet4/1	ACTIVE
200.1.1.5	0001.0600.0000	8	GigabitEthernet3/1	INACTIVE
200.1.1.6	0001.0600.0000	8	GigabitEthernet3/1	INACTIVE
200.1.1.7	0001.0600.0000	8	GigabitEthernet3/1	INACTIVE

次に、すべてのインターフェイスのすべてのアクティブ IP/MAC バインディングを表示する例を示します。

Switch# show ip device tracking all active

- IP Device Tracking = Enabled
- IP Device Tracking Probe Count = 3
- IP Device Tracking Probe Interval = 30

IP Address	MAC Address	Vlan	Interface	STATE
200.1.1.1	0001.0600.0000	9	GigabitEthernet4/1	ACTIVE
200.1.1.1	0001.0600.0000	9	GigabicEchernet4/i	ACTIVE
200.1.1.2	0001.0600.0000	9	GigabitEthernet4/1	ACTIVE
200.1.1.3	0001.0600.0000	9	GigabitEthernet4/1	ACTIVE
200.1.1.4	0001.0600.0000	9	GigabitEthernet4/1	ACTIVE
200.1.1.5	0001.0600.0000	9	GigabitEthernet4/1	ACTIVE

次に、すべてのインターフェイスのすべての非アクティブ IP/MAC バインディングを表示する例を示します。ホストは、最初に $GigabitEthernet\ 3/1$ で学習されてから、 $GigabitEthernet\ 4/1$ に移動されました。したがって、 $GigabitEthernet\ 3/1$ で学習された IP/MAC バインディング エントリが非アクティブとしてマークが付けられます。

Switch# show ip device tracking all inactive

- IP Device Tracking = Enabled
- IP Device Tracking Probe Count = 3
- IP Device Tracking Probe Interval = 30

IP Address	MAC Address	Vlan	Interface	STATE
200.1.1.8	0001.0600.0000	8	GigabitEthernet3/1	INACTIVE
200.1.1.9	0001.0600.0000	8	GigabitEthernet3/1	INACTIVE
200.1.1.10	0001.0600.0000	8	GigabitEthernet3/1	INACTIVE
200.1.1.1	0001.0600.0000	8	GigabitEthernet3/1	INACTIVE
200.1.1.2	0001.0600.0000	8	GigabitEthernet3/1	INACTIVE
200.1.1.3	0001.0600.0000	8	GigabitEthernet3/1	INACTIVE
200.1.1.4	0001.0600.0000	8	GigabitEthernet3/1	INACTIVE
200.1.1.5	0001.0600.0000	8	GigabitEthernet3/1	INACTIVE
200.1.1.6	0001.0600.0000	8	GigabitEthernet3/1	INACTIVE
200.1.1.7	0001.0600.0000	8	GigabitEthernet3/1	INACTIVE

次に、 すべてのインターフェイスのすべての IP デバイス トラッキング ホスト エントリのカウント を表示する例を示します。

Switch# show ip device tracking all count

Total IP Device Tracking Host entries: 5

Interface	Maximum Limit	Number of Entries
Fa4/3	 5	

PVLAN ホスト ポート上のスタティック ホストの IPSG

PVLAN ホスト ポート上でスタティック ホストの IPSG を設定できます。

PVLAN ホスト ポート上で IP フィルタを使用してスタティック ホストの IPSG をイネーブルにするには、次の作業を実行します。

コマンド 目的 Switch(config) ** vlan < ni> コンフィギュレーション VLAN モードを開始します。			
す。			目的
Aデップ 3 Switch(config-vlan)# exit	ステップ 1	Switch(config)# vlan <n1></n1>	
大子ツブ 1 Switch(config) # vlan <n2></n2>	ステップ 2	Switch(config-vlan)# private-vlan primary	PVLAN ポートにプライマリ VLAN を確立します。
### Switch(config-vlan)# private-vlan isolated pvLAN ポートに独立 VLAN を確立します。 ***********************************	ステップ 3	Switch(config-vlan)# exit	
Switch(config-vlan)# exit	ステップ 4	Switch(config)# vlan <n2></n2>	
ステップ 7 Switch(config)# vlan <ni>ステップ 7 Switch(config-vlan)# private-vlan association 201 ステップ 8 Switch(config-vlan)# exit VLAN コンフィギュレーション モードを終了します。 ステップ 10 Switch(config-if)# switchport mode private-vlan host ステップ 12 Switch(config-if)# switchport private-vlan host-association </ni>			

次に、PVLAN ホスト ポート上で IP フィルタを使用し、スタティック ホストの IPSG をイネーブル にする例を示します。

```
Switch(config) # vlan 200
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit
Switch(config)# vlan 201
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit
Switch(config) # vlan 200
Switch(config-vlan) # private-vlan association 201
Switch(config-vlan) # exit
Switch(config)# int fastEthernet 4/3
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 200 201
Switch(config-if)# ip device tracking maximum 8
Switch(config-if)# ip verify source tracking
Switch# show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
 IP Address MAC Address Vlan Interface
                                                           STATE
40.1.1.24 0000.0000.0304 200 FastEthernet4/3 40.1.1.20 0000.0000.0305 200 FastEthernet4/3
                                                           ACTIVE
40.1.1.20
                                                           ACTIVE
40.1.1.21
              0000.0000.0306 200 FastEthernet4/3
40.1.1.22
              0000.0000.0307 200 FastEthernet4/3
                                                           ACTIVE
               0000.0000.0308 200 FastEthernet4/3
```

出力では、インターフェイス Fa4/3 で学習された 5 つの有効 IP/MAC バインディングを示しています。PVLAN の場合、バインディングはプライマリ VLAN ID と関連付けられます。しがって、この例では、プライマリ VLAN ID の 200 がテーブル内に表示されます。

Switch# show ip verify source				
Filter-type	Filter-mode	IP-address	Mac-address	Vlan
ip trk	active	40.1.1.23		200
ip trk	active	40.1.1.24		200
ip trk	active	40.1.1.20		200
ip trk	active	40.1.1.21		200
ip trk	active	40.1.1.22		200
ip trk	active	40.1.1.23		201
ip trk	active	40.1.1.24		201
ip trk	active	40.1.1.20		201
ip trk	active	40.1.1.21		201
ip trk	active	40.1.1.22		201
	Filter-type ip trk	Filter-type Filter-mode	Filter-type Filter-mode IP-address ip trk active 40.1.1.23 ip trk active 40.1.1.20 ip trk active 40.1.1.21 ip trk active 40.1.1.21 ip trk active 40.1.1.22 ip trk active 40.1.1.22 ip trk active 40.1.1.23 ip trk active 40.1.1.23 ip trk active 40.1.1.24 ip trk active 40.1.1.20 ip trk active 40.1.1.20 ip trk active 40.1.1.20 ip trk active 40.1.1.21	Filter-type Filter-mode IP-address Mac-address ip trk active 40.1.1.23 ip trk active 40.1.1.20 ip trk active 40.1.1.21 ip trk active 40.1.1.22 ip trk active 40.1.1.22 ip trk active 40.1.1.22 ip trk active 40.1.1.23 ip trk active 40.1.1.23 ip trk active 40.1.1.24 ip trk active 40.1.1.24 ip trk active 40.1.1.20 ip trk active 40.1.1.20 ip trk active 40.1.1.21

出力では、5 つの有効 IP/MAC バインディングが、プライマリとセカンダリ両方の VLAN 上にあることを示しています。



CHAPTER

41

DAI の設定

この章では、Catalyst 4000 ファミリ スイッチ上で Dynamic ARP Inspection (DAI; ダイナミック ARP インスペクション)を設定する方法について説明します。

この章の主な内容は、次のとおりです。

- DAIの概要 (p.41-2)
- DAI の設定 (p.41-6)



この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/cr/index.htm

DAIの概要

DAI は、ネットワークの Address Resolution Protocol (ARP; アドレス解決プロトコル) パケットを確認するセキュリティ機能です。DAI によって、ネットワーク管理者は、無効な MAC (メディア アクセス制御) /IP アドレスのペアを持つ ARP パケットを代行受信、記録、およびドロップすることができます。この機能は、特定の [man-in-the-middle] 攻撃からネットワークを保護します。

ここでは、次の内容について説明します。

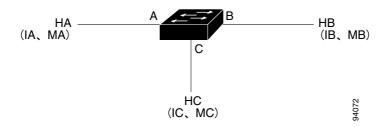
- ARP キャッシュのポイズニング (p.41-2)
- DAI の目的 (p.41-3)
- インターフェイスの信頼状態、セキュリティ適用範囲、およびネットワークの構成 (p.41-3)
- スタティック バインディング DHCP スヌーピングのエントリの相対的なプライオリティ (p.41-4)
- ドロップされたパケットのロギング(p.41-4)
- ARP パケットのレート制限 (p.41-5)
- ポート チャネルとその動作 (p.41-5)

ARP キャッシュのポイズニング

ARP キャッシュを「ポイズニング (汚染)」することによって、レイヤ 2 ネットワークに接続されたホスト、スイッチおよびルータを攻撃できます。たとえば、悪意のあるユーザが、サブネットに接続されたシステムの ARP キャッシュをポイズニングすることによって、サブネットの他のホストに向けられたトラフィックを代行受信する可能性があります。

次の構成を考えてみます。

図 41-1 ARP キャッシュのポイズニング



ホスト HA、HB、HC は、スイッチのインターフェイス A、B、C に接続されており、すべてが同一のサブネット上にあります。それぞれの IP アドレスと MAC アドレスは、カッコ内に表示されています。たとえば、ホスト HA は、IP アドレス IA と MAC アドレス IA を使用します。IA が IP レイヤの IB と通信する必要がある場合、IA は IB に対応付けられた IB の IB の IB の IB の IB の IB の IB が IB の IB の IB の IB の IB が IB の IB が IB の IB の IB の IB か IB が IB の IB の IB か IB が IB の IB の IB か IB が IB の IB の IB の IB か IB か IB の IB の IB か IB の IB の IB の IB の IB か IB の IB の IB の IB か IB の IB の IB の IB の IB か IB の IB の

ホスト HC は、IP アドレス IA (または IB) と MAC アドレス (MC) のホストのバインディングを持つ偽造された ARP 応答をブロードキャストすることによって、HA と HB の ARP キャッシュを「ポイズニング」できます。ポイズニングされた ARP キャッシュを持つホストは、IA または IB に向けられたトラフィックの宛先 MAC アドレスとして MAC アドレス MC を使用します。つまり、

HC はこのトラフィックを代行受信します。HC は IA と IB に対応付けられた正しい MAC アドレスを知っているため、正しい MAC アドレスを宛先として使用するこれらのホストに代行受信されたトラフィックを転送できます。HC は、HA から HB へのトラフィック ストリームに自分自身を割り込ませたことになります。これは典型的な [man in the middle] 攻撃です。

DAI の目的

ARP のポイズニング攻撃を防止するには、スイッチは有効な ARP 要求および応答のみがリレーされることを確認する必要があります。DAI は、すべての ARP 要求と応答を代行受信することによってこれらの攻撃を防ぎます。代行受信された各パケットは、ローカル ARP キャッシュが更新される前、またはパケットが適切な宛先に転送される前に、有効な MAC/IP アドレスのバインディングと照合されます。無効な ARP パケットはドロップされます。

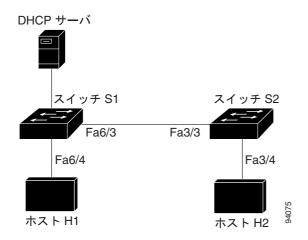
DAI は、ARP パケットの有効性を、信頼性のあるデータベースに格納された有効な MAC/IP アドレスのバインディングに基づいて判別します。このデータベースは、Dynamic Host Configuration Protocol (DHCP) スヌーピングが VLAN (仮想 LAN) および該当するスイッチでイネーブルにされている場合に、DHCP スヌーピングの実行時に作成されます。さらに、DAI は、スタティックに設定された IP アドレスを使用するホストを処理するために、ユーザが設定した ARP Access Control List (ACL; アクセス コントロール リスト) と ARP パケットを照合できます。

パケットの IP アドレスが無効である場合、または ARP パケットの本体にある MAC アドレスがイー サネット ヘッダーに指定されたアドレスと一致しない場合に、 ARP パケットをドロップするように DAI を設定することもできます。

インターフェイスの信頼状態、セキュリティ適用範囲、およびネットワークの構成

DAI は、システム上の各インターフェイスに信頼状態を対応付けます。信頼できるインターフェイスに着信するパケットは、すべての DAI 確認検査を迂回します。信頼できないインターフェイスに着信するパケットは、DAI 確認処理を受けます。DAI の一般的なネットワーク構成では、ホストポートに接続されたすべてのポートは、untrusted(信頼できない)に設定されます。スイッチに接続されたすべてのポートは、trusted(信頼できる)に設定されています。この設定では、所定のスイッチからネットワークに入ったすべての ARP パケットはセキュリティ チェックを通過します。

図 41-2 DAI 対応 VLAN における ARP パケットの確認



実際には untrusted の場合に、インターフェイスを trusted に設定すると、ネットワークにセキュリティ ホールが残ります。S1 が DAI を実行していない場合は、H1 は簡単に S2 の ARP (および ISL [スイッチ間リンク] が trusted に設定されている場合の H2)をポイズニングできます。この状態は、S2 が DAI を実行していても発生します。

DAI は、DAI を実行するスイッチに接続された(信頼できないインターフェイス上の)ホストが、ネットワークのその他のホストの ARP キャッシュをポイズニングしないようにします。ただし、ネットワークのその他の部分からのホストが、接続されているホストのキャッシュをポイズニングしないとは限りません。

VLAN の一部のスイッチが DAI を実行して、残りのスイッチが DAI を実行しないケースに対処するには、このようなスイッチを接続するインターフェイスを untrusted に設定する必要があります。ただし、DAI 非対応スイッチからのパケットのバインディングを確認するには、DAI を実行するスイッチに ARP ACL が設定されている必要があります。このようなバインディングを判別できない場合は、DAI を実行するスイッチを DAI 非対応スイッチからレイヤ 3 で分離する必要があります。



(注)

DHCP サーバおよびネットワークの設定によって、VLAN 内のすべてのスイッチ上で所定の ARP パケットの確認が実行できない場合があります。

スタティック バインディング DHCP スヌーピングのエントリの相対的なプライオリティ

前述したように、DAI は DHCP スヌーピングを通じて、有効な MAC/IP アドレスのバインディングのデータベースを入力します。また、ARP パケットをスタティックに設定された ARP ACL と照合します。ここで注意する必要があるのは、ARP ACL が DHCP スヌーピング データベースのエントリより優先されるということです。ARP パケットは最初に、ユーザが設定した ARP ACL と比較されます。ARP ACL が ARP パケットを拒否した場合、DHCP スヌーピングによって入力されたデータベースに有効なバインディングが存在する場合でも、パケットが拒否されます。

ドロップされたパケットのロギング

スイッチがパケットをドロップすると、ログ バッファにエントリが入力され、次にレート制御単位でシステム メッセージが生成されます。メッセージの生成後、スイッチはログ バッファからエントリをクリアします。各ログ エントリには、フロー情報 (受信 VLAN、ポート番号、送信元と宛先IP アドレス、および送信元と宛先 MAC アドレスなど)が含まれます。

バッファ内のエントリ数およびシステム メッセージを生成するのに指定間隔で必要となるエントリ数を設定するには、ip arp inspection log-buffer グローバル コンフィギュレーション コマンドを使用します。記録されるパケット タイプを指定するには、ip arp inspection vlan logging グローバルコンフィギュレーション コマンドを使用します。詳しい設定手順については、「ログ バッファの設定」(p.41-15) を参照してください。

ARP パケットのレート制限

DAI は CPU で確認検査を行うので、DoS 攻撃(サービス拒絶攻撃)を防ぐために着信 ARP パケット数がレート制限されています。デフォルトでは、信頼できないインターフェイスのレートは 15 pps に設定されており、信頼できるインターフェイスにはレート制限がありません。着信 ARP パケットのレートが設定された制限を超える場合は、ポートが errdisable ステートに置かれます。管理者が介入するまで、ポートはそのままの状態です。errdisable recovery グローバル コンフィギュレーション コマンドにより、errdisable 回復をイネーブルにして、ポートが指定のタイムアウト時間の経過後自動的にこのステートから回復できるようにします。

インターフェイスに着信する ARP 要求および ARP 応答のレートを制限するには、ip arp inspection limit グローバル コンフィギュレーション コマンドを使用します。レート制限がインターフェイス上に明示的に設定されていないかぎり、インターフェイスの信頼状態を変更すると、その信頼状態のデフォルト値のレート制限に変更されます。つまり、信頼できないインターフェイスは 15 pps で、信頼できるインターフェイスは無制限になります。レート制限が明示的に設定されると、信頼状態が変更されてもインターフェイスはそのレート制限を保持します。 rate limit コマンドの no 形式が適用されると、インターフェイスはいつでもデフォルトのレート制限値に戻ります。詳しい設定手順については、「着信 ARP パケットのレート制限」(p.41-18) を参照してください。

ポート チャネルとその動作

所定の物理ポートは、物理ポートとチャネルの信頼状態が一致した場合にだけチャネルに加入できます。一致しなければ、物理ポートがチャネルで中断されたままの状態になります。チャネルは、チャネルに加入した最初の物理ポートの信頼状態を継承します。そのため、最初の物理ポートの信頼状態は、チャネルの信頼状態に一致する必要がありません。

反対に、信頼状態がチャネル上で変更された場合は、新しい信頼状態がチャネルを構成するすべての物理ポート上に設定されます。

ポート チャネル上のレート制限確認は、ほかとは異なります。物理ポート上の着信パケットのレートは、物理ポートの設定ではなく、ポート チャネルの設定と比較確認されます。

ポート チャネル上のレート制限設定は、物理ポートの設定に依存しません。

レート制限は、すべての物理ポートで累積されます。つまり、ポート チャネル上の着信パケットのレートは、すべての物理ポートにおけるレートの合計と等しくなります。

トランク上の ARP パケットにレート制限を設定する場合、1 つの VLAN 上の高いレート制限によって、ポートがソフトウェアによって errdisable にされたときに、その他の VLAN に DoS 攻撃が行われる原因になる可能性があるので、VLAN 集約を計上する必要があります。同様に、ポート チャネルが errdisable の場合、1 つの物理ポート上の高いレート制限は、チャネル内の他のポートを停止させる原因になります。

DAI の設定

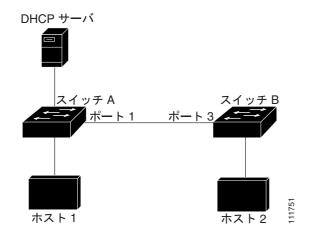
ここでは、スイッチ上で DAI を設定する手順について説明します。

- DHCP 環境での DAI の設定 (p.41-6)(必須)
- 非 DHCP 環境に対する ARP ACL の設定 (p.41-11)(任意)
- ログ バッファの設定 (p.41-15)(任意)
- 着信 ARP パケットのレート制限 (p.41-18)(任意)
- 確認検査の実行 (p.41-20)(任意)

DHCP 環境での DAI の設定

次の手順は、2 つのスイッチがこの機能をサポートする場合の DAI の設定方法を示しています。ホスト 1 はスイッチ A に、ホスト 2 はスイッチ B に接続されます(2 41-3 を参照)。両方のスイッチは、ホストが存在する VLAN 100 上で DAI を実行しています。DHCP サーバはスイッチ A に接続されます。両方のホストは同じ DHCP サーバから A IP アドレスを取得します。つまり、スイッチ A にはホスト A のバインディングがあり、スイッチ A にはホスト A のバインディングがあります。

図 41-3 DAI がイネーブルな VLAN 上での ARP パケットの確認





着信 ARP 要求および ARP 応答の IP/MAC アドレス バインディングを確認する場合、DAI は DHCP スヌーピング バインディング データベースのエントリに基づきます。 IP アドレスにダイナミック に割り当てられた ARP パケットを許可するために、DHCP スヌーピングがイネーブルであること を確認してください。設定情報については、第 40 章「DHCP スヌーピング、IP ソース ガード、およびスタティック ホストの IPSG の設定」を参照してください。

1 つのスイッチだけが DAI 機能をサポートする場合の DAI の設定方法については、「非 DHCP 環境に対する ARP ACL の設定」(p.41-11) を参照してください。

DAIを設定するには、両方のスイッチ上で次の作業を行います。

	コマンド	目的		
ステップ 1	Switch# show cdp neighbors	スイッチ間の接続を確認します。		
ステップ 2	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。		
ステップ 3	Switch(config)# [no] ip arp inspection vlan vlan-range	VLAN 単位で DAI をイネーブルにします。デフォルトでは、 DAI はすべての VLAN でディセーブルです。		
		DAI をディセーブルにするには、 no ip arp inspection vlan <i>vlan-range</i> グローバル コンフィギュレーション コマンドを使用します。		
		vlan- $range$ には、 $VLAN$ ID 番号で識別される単一の $VLAN$ 、 N H		
		両方のスイッチに同じ VLAN ID を指定します。		
ステップ 4	Switch(config)# interface interface-id	他のスイッチに接続されるインターフェイスを指定して、 インターフェイス コンフィギュレーション モードを開始 します。		
ステップ 5	Switch(config-if)# ip arp inspection trust	スイッチ間の接続を trusted に設定します。		
	trust	インターフェイスを untrusted ステートに戻すには、 no ip arp inspection trust インターフェイス コンフィギュレーション コマンドを使用します。		
		デフォルトでは、すべてのインターフェイスが untrusted です。		
		スイッチは、信頼できるインターフェイス上の他のスイッチから受信した ARP パケットの確認を行いません。単にパケットを転送します。		
		信頼できないインターフェイスの場合、スイッチはすべての ARP 要求および ARP 応答を代行受信します。代行受信されたパケットに有効な IP/MAC アドレス バインディングが含まれることを確認してから、ローカル キャッシュを更新し、適切な宛先にパケットを転送します。スイッチは、ip arp inspection vlan logging グローバル コンフィギュレーション コマンドで指定されたロギング設定に従って、無効なパケットをドロップし、ログ バッファに記録します。詳細については、「ログ バッファの設定」(p.41-15)を参照してください。		
ステップ 6	Switch(config-if)# end	特権 EXEC モードに戻ります。		
ステップ 7	Switch# show ip arp inspection interfaces Switch# show ip arp inspection vlan vlan-range	DAI の設定を確認します。		
ステップ 8	Switch# show ip dhcp snooping binding	DHCP バインディングを確認します。		
ステップ 9	Switch# show ip arp inspection statistics vlan vlan-range	DAI の統計情報を確認します。		
ステップ 10	Switch# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。		

次に、VLAN 100 のスイッチ A 上で DAI を設定する例を示します。スイッチ B でも同様の手順を実行します。

スイッチ A

SwitchA# show cdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID Local Intrfce Holdtme Capability Platform Port ID SwitchB Gig 3/48 179 R S I WS-C4506 Gig 3/46

SwitchA# configure terminal

SwitchA(config)# ip arp inspection vlan 100

SwitchA(config)# interface g3/48

SwitchA(config-if)# ip arp inspection trust

SwitchA(config-if)# end

SwitchA# show ip arp inspection interfaces

Interface	Trust State	Rate (pps)	Burst Interval
Gi1/1	Untrusted	15	1
Gi1/2	Untrusted	15	1
Gi3/1	Untrusted	15	1
Gi3/2	Untrusted	15	1
Gi3/3	Untrusted	15	1
Gi3/4	Untrusted	15	1
Gi3/5	Untrusted	15	1
Gi3/6	Untrusted	15	1
Gi3/7	Untrusted	15	1
Gi3/8	Untrusted	15	1
Gi3/9	Untrusted	15	1
Gi3/10	Untrusted	15	1
Gi3/11	Untrusted	15	1
Gi3/12	Untrusted	15	1
Gi3/13	Untrusted	15	1
Gi3/14	Untrusted	15	1
Gi3/15	Untrusted	15	1
Gi3/16	Untrusted	15	1
Gi3/17	Untrusted	15	1
Gi3/18	Untrusted	15	1
Gi3/19	Untrusted	15	1
Gi3/20	Untrusted	15	1
Gi3/21	Untrusted	15	1
Gi3/22	Untrusted	15	1
Gi3/23	Untrusted	15	1
Gi3/24	Untrusted	15	1
Gi3/25	Untrusted	15	1
Gi3/26	Untrusted	15	1
Gi3/27	Untrusted	15	1
Gi3/28	Untrusted	15	1
Gi3/29	Untrusted	15	1
Gi3/30	Untrusted	15	1
Gi3/31	Untrusted	15	1
Gi3/32	Untrusted	15	1
Gi3/33	Untrusted	15	1
Gi3/34	Untrusted	15	1
Gi3/35	Untrusted	15	1
Gi3/36	Untrusted	15	1
Gi3/37	Untrusted	15	1
Gi3/38	Untrusted	15	1
Gi3/39	Untrusted	15	1
Gi3/40	Untrusted	15	1
Gi3/41	Untrusted	15	1
Gi3/42	Untrusted	15	1
Gi3/43	Untrusted	15	1
Gi3/44	Untrusted	15	1
Gi3/45	Untrusted	15	1

1

Gi3/47 Untrusted	đ	15	1
Gi3/48 Trusted		None	N/A
SwitchA# show ip arp inspec	ction vlan 1	00	
Source Mac Validation	: Disabled		
Destination Mac Validation	: Disabled		
IP Address Validation	: Disabled		
Vlan Configuration	Operation	ACL Match	Static ACL

15

100 Enabled Active

Vlan ACL Logging DHCP Logging
---- -----100 Deny Deny

Gi3/46 Untrusted

SwitchA# show ip dhcp snooping binding

${\tt SwitchA\#}$ show ip arp inspection statistics vlan 100

Vlan	Forwarded	Dropped	DHCP Drops	ACL Drops	
100	15	0	0	0	
Vlan	DHCP Permits	ACL Permits	Source MAC Fa:	ilures	
100	0	0		0	
Vlan	Dest MAC Failu	res IP Valid	ation Failures	Invalid Protocol Data	
100		0	0	0	
Switch	\ #				

スイッチ B

SwitchB# show cdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID Local Intrfce Holdtme Capability Platform Port ID SwitchA Gig 3/46 163 R S I WS-C4507R Gig 3/48

SwitchB#

SwitchB# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

SwitchB(config)# ip arp inspection vlan 100

SwitchB(config) # interface g3/46

SwitchB(config-if)# ip arp inspection trust

SwitchB(config-if)# end

SwitchB#

SwitchB# show ip arp inspection interfaces

Interface	Trust State	Rate (pps)	Burst Interval
Gi1/1	Untrusted	15	1
Gi1/2	Untrusted	15	1
Gi3/1	Untrusted	15	1
Gi3/2	Untrusted	15	1
Gi3/3	Untrusted	15	1
Gi3/4	Untrusted	15	1
Gi3/5	Untrusted	15	1
Gi3/6	Untrusted	15	1
Gi3/7	Untrusted	15	1
Gi3/8	Untrusted	15	1
Gi3/9	Untrusted	15	1
Gi3/10	Untrusted	15	1
Gi3/11	Untrusted	15	1
Gi3/12	Untrusted	15	1
Gi3/13	Untrusted	15	1
Gi3/14	Untrusted	15	1
Gi3/15	Untrusted	15	1
Gi3/16	Untrusted	15	1
Gi3/17	Untrusted	15	1
Gi3/18	Untrusted	15	1
Gi3/19	Untrusted	15	1
Gi3/20	Untrusted	15	1
Gi3/21	Untrusted	15	1
Gi3/22	Untrusted	15	1
Gi3/23	Untrusted	15	1
Gi3/24	Untrusted	15	1
Gi3/25	Untrusted	15	1
Gi3/26	Untrusted	15	1
Gi3/27	Untrusted	15	1
Gi3/28	Untrusted	15	1
Gi3/29	Untrusted	15	1
Gi3/30	Untrusted	15	1
Gi3/31	Untrusted	15	1
Gi3/32	Untrusted	15	1
Gi3/33	Untrusted	15	1
Gi3/34	Untrusted	15	1
Gi3/35	Untrusted	15	1
Gi3/36	Untrusted	15	1
Gi3/37	Untrusted	15	1
Gi3/38	Untrusted	15	1
Gi3/39	Untrusted	15	1
Gi3/40	Untrusted	15	1
Gi3/41	Untrusted	15	1
Gi3/42	Untrusted	15	1
Gi3/43	Untrusted	15	1
Gi3/44	Untrusted	15	1
Gi3/45	Untrusted	15	1
Gi3/46	Trusted	None	N/A
Gi3/47	Untrusted	15	1
-,			_

Gi3/48	3 Untrus	ted	15		1	
Source Destina	B# show ip arp ins Mac Validation ation Mac Validati cess Validation	: Disabledon : Disabled	l l			
Vlan	Configuration	Operation		Sta	atic ACL	
100	Enabled					
Vlan	ACL Logging					
100	Deny	Deny#	· 			
MacAddr	_	ldress	Lease(sec)			Interface
Gigabit	Ethernet3/31 number of bindings		3492	dhcp-snoopi	ig 100	
SwitchE	# show ip arp ins	p statistics	vlan 100			
Vlan			DHCP Drop		-	
100	2398	0		0	0	
	DHCP Permits					
100	2398	0		0		
Vlan			tion Failure	es Invalid	Protocol	Data
100		0		0		0

非 DHCP 環境に対する ARP ACL の設定

SwitchB#

次の手順は、スイッチ B (図 41-3 [p.41-6] を参照) が DAI または DHCP スヌーピングをサポート しない場合の DAI の設定方法を示しています。

スイッチ A のポート 1 を trusted に設定した場合、スイッチ A およびホスト 1 はスイッチ B またはホスト 2 により攻撃される可能性があるため、セキュリティホールが発生します。この可能性を防止するには、スイッチ A のポート 1 を untrusted に設定する必要があります。ホスト 2 からの ARP パケットを許可するには、ARP ACL を設定し、VLAN 100 に適用する必要があります。ホスト 2 の IP アドレスがスタティックでなく、スイッチ A の ACL 設定を適用できない場合は、レイヤ 3 でスイッチ A とスイッチ B を分離し、これらのスイッチ間のパケット ルーティングにはルータを使用する必要があります。

(非 DHCP 環境のスイッチ A 上で) ARP ACL を設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# arp access-list acl-name	ARP ACL を定義して、ARP アクセスリスト コンフィギュレーション モードを開始します。デフォルトでは、ARP アクセス リストは定義されていません。 (注) ARP アクセス リストの末尾には、暗黙の deny ip
		any mac any コマンドがあります。
ステップ 3	Switch(config-arp-nac)# permit ip host sender-ip mac host sender-mac[log]	指定されたホスト (ホスト 2) からの ARP パケットを許可します。
		• sender-ip には、ホスト2のIPアドレスを入力します。
		• sender-mac には、ホスト2のMACアドレスを入力します。
		 (任意) log を指定して、Access Control Entry (ACE; アクセスコントロールエントリ)に一致するパケットをログ バッファに記録します。ip arp inspection vlan logging グローバルコンフィギュレーション コマンドで matchlog キーワードを設定した場合も、一致するパケットが記録されます。詳細については、「ログ バッファの設定」(p.41-15)を参照してください。
ステップ 4	Switch(config-arp-nac)# exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	Switch(config)# ip arp inspection filter arp-acl-name vlan vlan-range [static]	VLAN に ARP ACL を適用します。デフォルトでは、いずれの VLAN にも ARP ACL は定義されていません。
		 arp-acl-name には、ステップ 2 で作成された ACL 名を 指定します。
		 vlan-range には、スイッチおよびホストが存在する VLAN を指定します。VLAN ID 番号で識別される単一 の VLAN、ハイフンで区切られた VLAN 範囲、または カンマで区切られた一連の VLAN を指定できます。有 効範囲は 1 ~ 4094 です。
		 (任意)static を指定して、ARP ACL の暗黙の deny (拒否)を明示的な deny として処理し、ACL 内のそれより前の句に一致しないパケットをドロップします。DHCP バインディングは使用されません。
		このキーワードを指定しない場合は、ACL 内にパケットを拒否する明示的な deny が存在しないことを意味し、パケットが ACL 内の句と一致しない場合は、DHCPバインディングがパケットを許可するか拒否するかを決定します。
		IP/MAC アドレス バインディングのみを含む ARP パケットは、ACL と比較されます。アクセス リストが許可したパケットのみが許可されます。
ステップ 6	Switch(config)# interface interface-id	スイッチ B に接続されたスイッチ A のインターフェイス を指定し、インターフェイス コンフィギュレーション モー ドを開始します。

	コマンド	目的
ステップ 7	Switch(config-if)# no ip arp inspection trust	スイッチ B に接続されたスイッチ A のインターフェイス を untrusted として設定します。
		デフォルトでは、すべてのインターフェイスが untrusted です。
		信頼できないインターフェイスの場合、スイッチはすべての ARP 要求および ARP 応答を代行受信します。代行受信されたパケットに有効な IP/MAC アドレス バインディングが含まれることを確認してから、ローカル キャッシュを更新し、適切な宛先にパケットを転送します。スイッチは、ip arp inspection vlan logging グローバル コンフィギュレーション コマンドで指定されたロギング設定に従って、無効なパケットをドロップし、ログ バッファに記録します。詳細については、「ログ バッファの設定」(p.41-15)を参照してください。
ステップ 8	Switch(config-if)# end	特権 EXEC モードに戻ります。
ステップ 9	Switch# show arp access-list [acl-name] Switch# show ip arp inspection vlan vlan-range Switch# show ip arp inspection interfaces	DAI の設定を確認します。
ステップ 10	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

ARP ACL を削除するには、**no arp access-list** グローバル コンフィギュレーション コマンドを使用します。VLAN に対応付けられた ARP ACL を削除するには、**no ip arp inspection filter** *arp-acl-name* **vlan** *vlan-range* グローバル コンフィギュレーション コマンドを使用します。

次に、スイッチ A 上の host B という名前の ARP ACL を設定し、ホスト B からの ARP パケット (IP アドレス 170.1.1.2、MAC アドレス 2.2.2)を許可し、VLAN 100 に ACL を適用し、スイッチ A 上のポート 1 を untrusted に設定する例を示します。

SwitchA# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SwitchA(config)# arp access-list hostB
SwitchA(config-arp-nacl)# permit ip host 170.1.1.2 mac host 2.2.2 log
SwitchA(config-arp-nacl)# exit
SwitchA(config)# ip arp inspection filter hostB vlan 100 static
SwitchA(config)# interface g3/48
SwitchA(config-if)# no ip arp inspection trust
SwitchA(config-if)# end
SwitchA# show arp access-list hostB
ARP access list hostB
permit ip host 170.1.1.2 mac host 0002.0002.0002 log

SwitchA# show ip arp inspection interfaces

Interface	Trust State	Rate (pps)	Burst Interval
Gi1/1	Untrusted	15	1
Gi1/2	Untrusted	15	1
Gi3/1	Untrusted	15	1
Gi3/2	Untrusted	15	1
Gi3/3	Untrusted	15	1
Gi3/4	Untrusted	15	1
Gi3/5	Untrusted	15	1
Gi3/6	Untrusted	15	1
Gi3/7	Untrusted	15	1
Gi3/8	Untrusted	15	1
Gi3/9	Untrusted	15	1
Gi3/10	Untrusted	15	1
Gi3/11	Untrusted	15	1
Gi3/12	Untrusted	15	1
Gi3/13	Untrusted	15	1
Gi3/14	Untrusted	15	1
Gi3/15	Untrusted	15	1
Gi3/16	Untrusted	15	1
Gi3/17	Untrusted	15	1
Gi3/18	Untrusted	15	1
Gi3/19	Untrusted	15	1
Gi3/20	Untrusted	15	1
Gi3/21	Untrusted	15	1
Gi3/22	Untrusted	15	1
Gi3/23	Untrusted	15	1
Gi3/24	Untrusted	15	1
Gi3/25	Untrusted	15	1
Gi3/26	Untrusted	15	1
Gi3/27	Untrusted	15	1
Gi3/28	Untrusted	15	1
Gi3/29	Untrusted	15	1
Gi3/30	Untrusted	15	1
Gi3/31	Untrusted	15	1
Gi3/32	Untrusted	15	1
Gi3/33 Gi3/34	Untrusted	15 15	1
	Untrusted	15	1
Gi3/35 Gi3/36	Untrusted	15	1
Gi3/37	Untrusted Untrusted	15	1
Gi3/38	Untrusted	15	1
Gi3/39	Untrusted	15	1
Gi3/40	Untrusted	15	1
Gi3/41	Untrusted	15	1
Gi3/42	Untrusted	15	1
Gi3/43	Untrusted	15	1
Gi3/44	Untrusted	15	1
Gi3/45	Untrusted	15	1
013/43	JIICI US CEU	13	1

	Untrusto Untrusto Untrusto	ed	15 15 15	1 1 1	
SwitchA	show ip arp inspe	ection stati	istics vlan 100		
Vlan	Forwarded	Dropped	DHCP Drops	ACL Drops	
100	15	169	160	9	
Vlan	DHCP Permits A	CL Permits	Source MAC Fai	lures	
100	0	0		0	
Vlan	Dest MAC Failures	IP Valida	ation Failures	Invalid Protocol	Data
100 SwitchA	0		0		0

ログ バッファの設定

スイッチがパケットをドロップすると、ログ バッファにエントリが入力され、次にレート制御単位でシステム メッセージが生成されます。メッセージの生成後、スイッチはログ バッファからエントリをクリアします。各ログ エントリには、フロー情報(受信 VLAN、ポート番号、送信元と宛先IP アドレス、および送信元と宛先 MAC アドレスなど)が含まれます。

ログバッファ エントリは、複数のパケットを表すことができます。たとえば、インターフェイスが同一 VLAN 上で同じ ARP パラメータを持つ多数のパケットを受信した場合、スイッチはログ バッファでこれらのパケットを 1 つのエントリとして結合し、エントリに単一のシステム メッセージを生成します。

ログ バッファがオーバーフローになる (つまり、ログ イベントがログ バッファに収まらない)場合は、show ip arp inspection log 特権 EXEC コマンドの表示に影響します。エントリには、その他の統計情報は提供されません。

ログ バッファを設定するには、特権 EXEC モードを開始して次の作業を行います。

	コマンド	目的			
	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。			
	Switch(config)# ip arp inspection log-buffer {entries number logs number	DAI のロギング バッファを設定します。			
	<pre>interval seconds}</pre>	デフォルトでは、DAI がイネーブルの場合、拒否またはドロップされた ARP パケットが記録されます。ログ エントリ数は 32 です。システム メッセージ数は、 1 秒あたり 5 に制限されます。ロギングレート間隔は 1 秒です。			
		キーワードの意味は次のとおりです。			
		• entries <i>number</i> には、バッファに記録されるエントリ数を指定します。有効範囲は 0 ~ 1024 です。			
		• logs number interval seconds には、指定の間隔でシステム メッセージを生成するエントリ数を指定します。			
		logs number では、範囲は 0 ~ 1024 です。値が 0 の場合 はログ バッファにエントリは存在しますが、システム メッセージは生成されないことを意味します。			
	interval $seconds$ では、範囲は $0 \sim 86400$ 秒 $(1 \ H)$ です。値が 0 の場合はシステム メッセージがすぐに生成されることを意味します $($ また、ログ バッファは常に空です $)$				
		0 の間隔設定は、 0 のログ設定を上書きします。			
		logs および interval 設定は相互に作用します。logs number X が interval $seconds$ Y よりも大きい場合、 X を Y で除算した (X/Y) 数のシステム メッセージが毎秒送信されます。そうでない場合は、 Y を X で除算した (Y/X) 秒ごとに 1 つのシステム メッセージが送信されます。			

	コマンド	目的
ステップ 3	<pre>vlan vlan-range logging {acl-match {matchlog none } dhcp-bindings {all none permit}}</pre>	記録されるパケット タイプを VLAN 単位で制御します。デフォルトでは、拒否またはドロップされたパケットがすべて記録されます。logged という用語は、エントリがログ バッファ内に存在し、システム メッセージが生成されることを意味します。
		キーワードの意味は次のとおりです。
		• vlan-range には、VLAN ID 番号で識別される単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカ ンマで区切られた一連の VLAN を指定します。有効範 囲は 1 ~ 4094 です。
		• acl-match matchlog では、ACE ロギング設定に基づいてパケットを記録します。このコマンドで matchlog キーワードを指定し、permit または deny ARP アクセスリスト コンフィギュレーション コマンドで log キーワードを指定した場合、ログ キーワードを持つ ACE で許可または拒否された ARP パケットが記録されます。
		• acl-match none では、ACL に一致するパケットを記録しません。
		• dhcp-bindings all では、DHCP バインディングに一致するすべてのパケットを記録します。
		• dhcp-bindings none では、DHCP バインディングに一致 するパケットを記録しません。
		• dhcp-bindings permit では、DHCP バインディングが許可したパケットを記録します。
ステップ 4	Switch(config)# exit	特権 EXEC モードに戻ります。
ステップ 5	Switch# show ip arp inspection log	設定を確認します。
ステップ 6	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

デフォルトのログ バッファ設定に戻すには、no ip arp inspection log-buffer グローバル コンフィギュレーション コマンドを使用します。 デフォルトの VLAN ログ設定に戻すには、

no ip arp inspection vlan *vlan-range* logging {acl-match | dhcp-bindings} グローバル コンフィギュレーション コマンドを使用します。ログ バッファをクリアするには、clear ip arp inspection log 特権 EXEC コマンドを使用します。

次に、ログ バッファのエントリ数を 1024 に設定する例を示します。また、ログが 100/10 秒のレートで生成されるよう Catalyst 4500 シリーズ スイッチを設定する例も示します。

SwitchB# configure terminal

Enter configuration commands, one per line. End with CNTL/Z. SwitchB(config)# ip arp inspection log-buffer entries 1024
SwitchB(config)# ip arp inspection log-buffer logs 100 interval 10
SwitchB(config)# end
SwitchB# show ip arp inspection log
Total Log Buffer Size : 1024
Syslog rate : 100 entries per 10 seconds.

Interface	Vlan	Sender MAC	Sender IP	Num Pkts	Reason	Time
Gi3/31	100	0002.0002.0003	170.1.1.2	5	DHCP Deny	02:05:45
UTC Fri Feb 4 2005						
SwitchB#						

着信 ARP パケットのレート制限

スイッチの CPU が DAI の確認検査を行うので、DoS 攻撃を防ぐために着信 ARP パケット数がレート制限されています。

着信 ARP パケットのレートが設定された制限を超える場合は、ポートが errdisable ステートに置かれます。ユーザが介入するか、または errdisable 回復をイネーブルにして、指定されたタイムアウト時間の経過後自動的にこのステートから回復するまで、ポートはこの状態のままです。



レート制限がインターフェイス上で明示的に設定されていないかぎり、インターフェイスの信頼状態を変更すると、レート制限はその信頼状態のデフォルト値に変更されます。レート制限の設定後は、インターフェイスの信頼状態が変更されてもそのレート制限を保持します。no ip arp inspection limit インターフェイス コンフィギュレーション コマンドを入力した場合、インターフェイスはデフォルトのレート制限に戻ります。

着信 ARP パケットのレートを制限するには、特権 EXEC モードを開始して次の作業を行います。

	コマンド	目的
1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
2	Switch(config)# interface interface-id	レート制限されるインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。
3	Switch(config-if)# [no] ip arp inspection limit {rate pps [burst interval seconds] none}	インターフェイス上の着信 ARP 要求および ARP 応答のレートを制限します。
		デフォルトのレートは、信頼できないインターフェイスでは 15 pps 、信頼できるインターフェイスでは無制限です。バースト間隔は 1 秒です。
		キーワードの意味は次のとおりです。
		• rate pps には、1 秒間に処理される着信パケット数の上限 を指定します。有効範囲は 0 ~ 2048 pps です。
		 (任意) burst interval seconds には、高いレートの ARP パケットに関してインターフェイスを監視する連続した間隔を秒数で指定します。有効範囲は1~15秒です。
		• rate none では、処理できる着信 ARP パケットのレートに 上限を指定しません。
	Switch(config-if)# exit	グローバル コンフィギュレーション モードに戻ります。
j	Switch(config)# errdisable recovery {cause arp-inspection interval interval}	(任意)DAI の errdisable ステートからのエラー回復をイネーブ ルにします。
	,	デフォルトでは、回復はディセーブルで、回復間隔は 300 秒です。
		interval <i>interval</i> には、errdisable ステートから回復する時間を 秒単位で指定します。有効範囲は 30 ~ 86400 です。
i	Switch(config)# exit	特権 EXEC モードに戻ります。
•	Switch# show ip arp inspection interfaces	設定を確認します。
	Switch# show errdisable recovery	設定を確認します。
	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

デフォルトのレート制限設定に戻すには、no ip arp inspection limit インターフェイス コンフィギュレーション コマンドを使用します。DAI のエラー回復をディセーブルにするには、no errdisable recovery cause arp-inspection グローバル コンフィギュレーション コマンドを使用します。

次に、着信パケット数の上限(100 pps)を設定し、バースト間隔(1秒)を指定する例を示します。

SwitchB# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

SwitchB(config)# interface g3/31

SwitchB(config-if)# ip arp inspection limit rate 100 burst interval 1

SwitchB(config-if)# exit

SwitchB(config)# errdisable recovery cause arp-inspection

SwitchB(config)# exit

SwitchB# show ip arp inspection interfaces

Gil/1 Untrusted 15 1 Gil/2 Untrusted 15 1 Gil/2 Untrusted 15 1 Gil/2 Untrusted 15 1 Gil/3 Untrusted 15 1 Gil/3 Untrusted 15 1 Gil/3 Untrusted 15 1 Gil/3 Untrusted 15 1 Gil/4 Untrusted 15 1 Gil/5 Untrusted 15 1 Gil/6 Untrusted 15 1 Gil/7 Untrusted 15 1 Gil/8 Untrusted 15 1 Gil/8 Untrusted 15 1 Gil/9 Untrusted 15 1 Gil/9 Untrusted 15 1 Gil/10 Untrusted 15 1 Gil/11 Untrusted 15 1 Gil/11 Untrusted 15 1 Gil/12 Untrusted 15 1 Gil/12 Untrusted 15 1 Gil/13 Untrusted 15 1 Gil/14 Untrusted 15 1 Gil/17 Untrusted 15 1 Gil/18 Untrusted 15 1 Gil/19 Untrusted 15 1 Gil/19 Untrusted 15 1 Gil/10 Untrusted	Interface		Rate (pps)	Burst Interval
Gi1/2 Untrusted 15 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1				
Gi3/1 Untrusted 15 1 Gi3/2 Untrusted 15 1 Gi3/3 Untrusted 15 1 Gi3/4 Untrusted 15 1 Gi3/4 Untrusted 15 1 Gi3/5 Untrusted 15 1 Gi3/6 Untrusted 15 1 Gi3/7 Untrusted 15 1 Gi3/7 Untrusted 15 1 Gi3/8 Untrusted 15 1 Gi3/9 Untrusted 15 1 Gi3/10 Untrusted 15 1 Gi3/11 Untrusted 15 1 Gi3/11 Untrusted 15 1 Gi3/12 Untrusted 15 1 Gi3/13 Untrusted 15 1 Gi3/14 Untrusted 15 1 Gi3/15 Untrusted 15 1 Gi3/16 Untrusted 15 1 Gi3/17 Untrusted 15 1 Gi3/17 Untrusted 15 1 Gi3/18 Untrusted 15 1 Gi3/19 Untrusted 15 1 Gi3/17 Untrusted 15 1 Gi3/18 Untrusted 15 1 Gi3/19 Untrusted 15 1 Gi3/19 Untrusted 15 1 Gi3/19 Untrusted 15 1 Gi3/20 Untrusted 15 1 Gi3/20 Untrusted 15 1 Gi3/21 Untrusted 15 1 Gi3/22 Untrusted 15 1 Gi3/23 Untrusted 15 1 Gi3/24 Untrusted 15 1 Gi3/25 Untrusted 15 1 Gi3/26 Untrusted 15 1 Gi3/27 Untrusted 15 1 Gi3/28 Untrusted 15 1 Gi3/28 Untrusted 15 1 Gi3/29 Untrusted 15 1 Gi3/28 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/34 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/34 Untrusted 15 1 Gi3/34 Untrusted 15 1 Gi3/44 Untrusted 15 1 Gi3/44 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/46 Untrusted 15 1 Gi3/46 Untrusted 15 1 Gi3/47 Untrusted 15 1				
Gi3/2 Untrusted 15 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1				
Gi3/4 Untrusted 15 1 1 Gi3/4 Untrusted 15 1 1 Gi3/4 Untrusted 15 1 1 Gi3/6 Untrusted 15 1 1 Gi3/6 Untrusted 15 1 1 Gi3/6 Untrusted 15 1 1 Gi3/7 Untrusted 15 1 1 Gi3/7 Untrusted 15 1 1 Gi3/9 Untrusted 15 1 1 Gi3/9 Untrusted 15 1 1 Gi3/9 Untrusted 15 1 1 Gi3/10 Untrusted 15 1 1 Gi3/11 Untrusted 15 1 1 Gi3/11 Untrusted 15 1 Gi3/12 Untrusted 15 1 Gi3/13 Untrusted 15 1 Gi3/13 Untrusted 15 1 Gi3/14 Untrusted 15 1 Gi3/15 Untrusted 15 1 Gi3/16 Untrusted 15 1 Gi3/16 Untrusted 15 1 Gi3/17 Untrusted 15 1 Gi3/18 Untrusted 15 1 Gi3/18 Untrusted 15 1 Gi3/19 Untrusted 15 1 Gi3/19 Untrusted 15 1 Gi3/20 Untrusted 15 1 Gi3/20 Untrusted 15 1 Gi3/21 Untrusted 15 1 Gi3/22 Untrusted 15 1 Gi3/23 Untrusted 15 1 Gi3/23 Untrusted 15 1 Gi3/24 Untrusted 15 1 Gi3/25 Untrusted 15 1 Gi3/26 Untrusted 15 1 Gi3/27 Untrusted 15 1 Gi3/27 Untrusted 15 1 Gi3/27 Untrusted 15 1 Gi3/28 Untrusted 15 1 Gi3/29 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/34				1
Gi3/4 Untrusted 15 1 1 Gi3/5 Untrusted 15 1 1 Gi3/6 Untrusted 15 1 1 Gi3/7 Untrusted 15 1 1 Gi3/7 Untrusted 15 1 1 Gi3/7 Untrusted 15 1 1 Gi3/8 Untrusted 15 1 1 Gi3/9 Untrusted 15 1 1 Gi3/9 Untrusted 15 1 Gi3/10 Untrusted 15 1 Gi3/11 Untrusted 15 1 Gi3/11 Untrusted 15 1 Gi3/11 Untrusted 15 1 Gi3/12 Untrusted 15 1 Gi3/13 Untrusted 15 1 Gi3/14 Untrusted 15 1 Gi3/15 Untrusted 15 1 Gi3/15 Untrusted 15 1 Gi3/16 Untrusted 15 1 Gi3/17 Untrusted 15 1 Gi3/17 Untrusted 15 1 Gi3/18 Untrusted 15 1 Gi3/19 Untrusted 15 1 Gi3/19 Untrusted 15 1 Gi3/20 Untrusted 15 1 Gi3/20 Untrusted 15 1 Gi3/21 Untrusted 15 1 Gi3/22 Untrusted 15 1 Gi3/23 Untrusted 15 1 Gi3/23 Untrusted 15 1 Gi3/24 Untrusted 15 1 Gi3/25 Untrusted 15 1 Gi3/26 Untrusted 15 1 Gi3/27 Untrusted 15 1 Gi3/28 Untrusted 15 1 Gi3/29 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/34 Untrusted 15 1 Gi3/44 Untruste				
Gi3/5 Untrusted 15 1 1 6i3/6 Untrusted 15 1 1 6i3/6 Untrusted 15 1 1 6i3/7 Untrusted 15 1 1 6i3/8 Untrusted 15 1 1 6i3/8 Untrusted 15 1 1 6i3/9 Untrusted 15 1 1 6i3/9 Untrusted 15 1 1 6i3/10 Untrusted 15 1 1 6i3/11 Untrusted 15 1 1 6i3/11 Untrusted 15 1 6i3/12 Untrusted 15 1 1 6i3/13 Untrusted 15 1 1 6i3/13 Untrusted 15 1 1 6i3/14 Untrusted 15 1 1 6i3/15 Untrusted 15 1 1 6i3/15 Untrusted 15 1 1 6i3/16 Untrusted 15 1 1 6i3/17 Untrusted 15 1 1 6i3/17 Untrusted 15 1 1 6i3/18 Untrusted 15 1 1 6i3/19 Untrusted 15 1 1 6i3/19 Untrusted 15 1 1 6i3/19 Untrusted 15 1 1 6i3/20 Untrusted 15 1 1 6i3/21 Untrusted 15 1 1 6i3/22 Untrusted 15 1 1 6i3/22 Untrusted 15 1 1 6i3/23 Untrusted 15 1 1 6i3/24 Untrusted 15 1 1 6i3/25 Untrusted 15 1 1 6i3/25 Untrusted 15 1 1 6i3/26 Untrusted 15 1 1 6i3/27 Untrusted 15 1 1 6i3/28 Untrusted 15 1 1 6i3/28 Untrusted 15 1 1 6i3/29 Untrusted 15 1 1 6i3/29 Untrusted 15 1 1 6i3/30 Untrusted 15 1 1 6i3/40 Untrusted				
Gi3/6 Untrusted 15 1 1 6 6 3 1 7 Untrusted 15 1 1 6 3 1 7 Untrusted 15 1 1 6 3 1 1 6 3 3 7 Untrusted 15 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1				1
Gi3/7 Untrusted 15 1 1 6 6 3 / 8 Untrusted 15 1 1 6 6 3 / 9 Untrusted 15 1 1 6 6 3 / 10 Untrusted 15 1 1 6 6 3 / 10 Untrusted 15 1 1 6 6 3 / 11 Untrusted 15 1 1 6 6 3 / 11 Untrusted 15 1 1 6 6 3 / 12 Untrusted 15 1 1 6 6 3 / 12 Untrusted 15 1 1 6 6 3 / 13 Untrusted 15 1 1 6 6 3 / 13 Untrusted 15 1 1 6 6 3 / 14 Untrusted 15 1 1 6 6 3 / 14 Untrusted 15 1 1 6 6 3 / 15 Untrusted 15 1 1 6 6 3 / 15 Untrusted 15 1 1 6 6 3 / 15 Untrusted 15 1 1 6 6 3 / 15 Untrusted 15 1 1 6 6 3 / 17 Untrusted 15 1 1 6 6 3 / 17 Untrusted 15 1 1 6 6 3 / 19 Untrusted 15 1 1 6 6 3 / 19 Untrusted 15 1 1 6 6 3 / 19 Untrusted 15 1 1 6 6 3 / 19 Untrusted 15 1 1 6 6 3 / 19 Untrusted 15 1 1 6 6 3 / 19 Untrusted 15 1 1 6 6 3 / 12 Untrusted 15 1 1 6 1 6 3 / 12 Untrusted 15 1 1 6 1 6 3 / 12 Untrusted 15 1 1 6 1 6 3 / 12 Untrusted 15 1 1 6 1 6 3 / 12 Untrusted 15 1 1 6 1 6 3 / 12 Untrusted 15 1 1 6 1 6 3 / 12 Untrusted 15 1 1 6 1 6 3 / 12 Untrusted 15 1 1 6 1 6 3 / 12 Untrusted 15 1 1 6 1 6 3 / 12 Untrusted 15 1 1 6 1 6 3 / 12 Untrusted 15 1 1 6 1 6 3 / 12 Untrusted 15 1 1 6 1 6 3 / 12 Untrus		Untrusted	15	1
Gi3/8 Untrusted 15 1 1 Gi3/9 Untrusted 15 1 1 Gi3/10 Untrusted 15 1 1 Gi3/10 Untrusted 15 1 1 Gi3/11 Untrusted 15 1 1 Gi3/11 Untrusted 15 1 Gi3/12 Untrusted 15 1 Gi3/12 Untrusted 15 1 Gi3/14 Untrusted 15 1 1 Gi3/14 Untrusted 15 1 Gi3/15 Untrusted 15 1 Gi3/15 Untrusted 15 1 Gi3/16 Untrusted 15 1 Gi3/17 Untrusted 15 1 Gi3/18 Untrusted 15 1 Gi3/19 Untrusted 15 1 Gi3/19 Untrusted 15 1 Gi3/19 Untrusted 15 1 Gi3/20 Untrusted 15 1 Gi3/21 Untrusted 15 1 Gi3/22 Untrusted 15 1 Gi3/23 Untrusted 15 1 Gi3/23 Untrusted 15 1 Gi3/24 Untrusted 15 1 Gi3/25 Untrusted 15 1 Gi3/26 Untrusted 15 1 Gi3/27 Untrusted 15 1 Gi3/28 Untrusted 15 1 Gi3/28 Untrusted 15 1 Gi3/28 Untrusted 15 1 Gi3/29 Untrusted 15 1 Gi3/29 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/44 Untru				
Gi3/10 Untrusted 15 1 Gi3/11 Untrusted 15 1 Gi3/12 Untrusted 15 1 Gi3/13 Untrusted 15 1 Gi3/13 Untrusted 15 1 Gi3/14 Untrusted 15 1 Gi3/15 Untrusted 15 1 Gi3/16 Untrusted 15 1 Gi3/17 Untrusted 15 1 Gi3/18 Untrusted 15 1 Gi3/19 Untrusted 15 1 Gi3/20 Untrusted 15 1 Gi3/21 Untrusted 15 1 Gi3/22 Untrusted 15 1 Gi3/23 Untrusted 15 1 Gi3/24 Untrusted 15 1 Gi3/25 Untrusted 15 1 Gi3/26 Untrusted 15 1 Gi3/27 Untrusted 15 1 Gi3/27 Untrusted 15 1 Gi3/28 Untrusted 15 1 Gi3/29 Untrusted 15 1 Gi3/29 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/32 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/33 Untrusted 15 1 Gi3/34 Untrusted 15 1 Gi3/35 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/34 Untrusted 15 1 Gi3/35 Untrusted 15 1 Gi3/36 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/41 Untrusted 15 1 Gi3/42 Untrusted 15 1 Gi3/44 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/46 Trusted 15 1 Gi3/46 Trusted 15 1 Gi3/47 Untrusted 15 1			15	1
Gi3/10 Untrusted 15 1 Gi3/11 Untrusted 15 1 Gi3/12 Untrusted 15 1 Gi3/13 Untrusted 15 1 Gi3/13 Untrusted 15 1 Gi3/14 Untrusted 15 1 Gi3/15 Untrusted 15 1 Gi3/16 Untrusted 15 1 Gi3/17 Untrusted 15 1 Gi3/18 Untrusted 15 1 Gi3/19 Untrusted 15 1 Gi3/20 Untrusted 15 1 Gi3/21 Untrusted 15 1 Gi3/22 Untrusted 15 1 Gi3/23 Untrusted 15 1 Gi3/24 Untrusted 15 1 Gi3/25 Untrusted 15 1 Gi3/26 Untrusted 15 1 Gi3/27 Untrusted 15 1 Gi3/27 Untrusted 15 1 Gi3/28 Untrusted 15 1 Gi3/29 Untrusted 15 1 Gi3/29 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/32 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/33 Untrusted 15 1 Gi3/34 Untrusted 15 1 Gi3/35 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/34 Untrusted 15 1 Gi3/35 Untrusted 15 1 Gi3/36 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/41 Untrusted 15 1 Gi3/42 Untrusted 15 1 Gi3/44 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/46 Trusted 15 1 Gi3/46 Trusted 15 1 Gi3/47 Untrusted 15 1	Gi3/9	Untrusted	15	1
Gi3/11 Untrusted 15 1 Gi3/12 Untrusted 15 1 Gi3/13 Untrusted 15 1 Gi3/14 Untrusted 15 1 Gi3/15 Untrusted 15 1 Gi3/16 Untrusted 15 1 Gi3/17 Untrusted 15 1 Gi3/18 Untrusted 15 1 Gi3/18 Untrusted 15 1 Gi3/19 Untrusted 15 1 Gi3/20 Untrusted 15 1 Gi3/21 Untrusted 15 1 Gi3/22 Untrusted 15 1 Gi3/22 Untrusted 15 1 Gi3/23 Untrusted 15 1 Gi3/24 Untrusted 15 1 Gi3/25 Untrusted 15 1 Gi3/26 Untrusted 15 1 Gi3/27 Untrusted 15 1 Gi3/28 Untrusted 15 1 Gi3/28 Untrusted 15 1 Gi3/29 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/32 Untrusted 15 1 Gi3/34 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/33 Untrusted 15 1 Gi3/34 Untrusted 15 1 Gi3/35 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/34 Untrusted 15 1 Gi3/35 Untrusted 15 1 Gi3/36 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/34 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/41 Untrusted 15 1 Gi3/42 Untrusted 15 1 Gi3/44 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/46 Trusted 15 1 Gi3/46 Trusted 15 1 Gi3/47 Untrusted 15 1				
Gi3/12 Untrusted 15 1 Gi3/13 Untrusted 15 1 Gi3/14 Untrusted 15 1 Gi3/15 Untrusted 15 1 Gi3/15 Untrusted 15 1 Gi3/16 Untrusted 15 1 Gi3/17 Untrusted 15 1 Gi3/18 Untrusted 15 1 Gi3/19 Untrusted 15 1 Gi3/20 Untrusted 15 1 Gi3/20 Untrusted 15 1 Gi3/21 Untrusted 15 1 Gi3/22 Untrusted 15 1 Gi3/22 Untrusted 15 1 Gi3/24 Untrusted 15 1 Gi3/25 Untrusted 15 1 Gi3/26 Untrusted 15 1 Gi3/27 Untrusted 15 1 Gi3/28 Untrusted 15 1 Gi3/28 Untrusted 15 1 Gi3/29 Untrusted 15 1 Gi3/29 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/32 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/32 Untrusted 15 1 Gi3/33 Untrusted 15 1 Gi3/34 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/41 Untrusted 15 1 Gi3/42 Untrusted 15 1 Gi3/44 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/46 Trusted None N/A Gi3/47 Untrusted 15 1 Gi3/47 Untrusted 15 1 Gi3/46 Trusted None N/A				1
Gi3/13 Untrusted 15 1 Gi3/14 Untrusted 15 1 Gi3/15 Untrusted 15 1 Gi3/16 Untrusted 15 1 Gi3/16 Untrusted 15 1 Gi3/17 Untrusted 15 1 Gi3/18 Untrusted 15 1 Gi3/19 Untrusted 15 1 Gi3/20 Untrusted 15 1 Gi3/21 Untrusted 15 1 Gi3/22 Untrusted 15 1 Gi3/22 Untrusted 15 1 Gi3/23 Untrusted 15 1 Gi3/24 Untrusted 15 1 Gi3/25 Untrusted 15 1 Gi3/26 Untrusted 15 1 Gi3/27 Untrusted 15 1 Gi3/28 Untrusted 15 1 Gi3/29 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/32 Untrusted 15 1 Gi3/33 Untrusted 15 1 Gi3/34 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/34 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/36 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/41 Untrusted 15 1 Gi3/42 Untrusted 15 1 Gi3/44 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/46 Trusted None N/A Gi3/47 Untrusted None N/A		Untrusted	15	1
Gi3/14 Untrusted 15 1 Gi3/15 Untrusted 15 1 Gi3/16 Untrusted 15 1 Gi3/17 Untrusted 15 1 Gi3/18 Untrusted 15 1 Gi3/18 Untrusted 15 1 Gi3/19 Untrusted 15 1 Gi3/20 Untrusted 15 1 Gi3/21 Untrusted 15 1 Gi3/22 Untrusted 15 1 Gi3/22 Untrusted 15 1 Gi3/23 Untrusted 15 1 Gi3/24 Untrusted 15 1 Gi3/25 Untrusted 15 1 Gi3/26 Untrusted 15 1 Gi3/27 Untrusted 15 1 Gi3/28 Untrusted 15 1 Gi3/29 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/32 Untrusted 15 1 Gi3/33 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/32 Untrusted 15 1 Gi3/33 Untrusted 15 1 Gi3/34 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/41 Untrusted 15 1 Gi3/42 Untrusted 15 1 Gi3/44 Untrusted 15 1 Gi3/44 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/46 Trusted None N/A Gi3/47 Untrusted None N/A				
Gi3/15 Untrusted 15 1 Gi3/16 Untrusted 15 1 Gi3/17 Untrusted 15 1 Gi3/18 Untrusted 15 1 Gi3/19 Untrusted 15 1 Gi3/20 Untrusted 15 1 Gi3/21 Untrusted 15 1 Gi3/22 Untrusted 15 1 Gi3/23 Untrusted 15 1 Gi3/24 Untrusted 15 1 Gi3/25 Untrusted 15 1 Gi3/26 Untrusted 15 1 Gi3/27 Untrusted 15 1 Gi3/28 Untrusted 15 1 Gi3/29 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/32 Untrusted 15 1 Gi3/33 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/32 Untrusted 15 1 Gi3/33 Untrusted 15 1 Gi3/34 Untrusted 15 1 Gi3/35 Untrusted 15 1 Gi3/36 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/36 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/41 Untrusted 15 1 Gi3/42 Untrusted 15 1 Gi3/44 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/46 Trusted 15 1 Gi3/46 Trusted 15 1 Gi3/46 Trusted None N/A Gi3/47 Untrusted None N/A				
Gi3/16 Untrusted 15 1 Gi3/17 Untrusted 15 1 Gi3/18 Untrusted 15 1 Gi3/19 Untrusted 15 1 Gi3/20 Untrusted 15 1 Gi3/20 Untrusted 15 1 Gi3/21 Untrusted 15 1 Gi3/22 Untrusted 15 1 Gi3/23 Untrusted 15 1 Gi3/24 Untrusted 15 1 Gi3/25 Untrusted 15 1 Gi3/26 Untrusted 15 1 Gi3/27 Untrusted 15 1 Gi3/28 Untrusted 15 1 Gi3/29 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/32 Untrusted 15 1 Gi3/33 Untrusted 15 1 Gi3/34 Untrusted 15 1 Gi3/35 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/34 Untrusted 15 1 Gi3/35 Untrusted 15 1 Gi3/36 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/41 Untrusted 15 1 Gi3/44 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/46 Trusted 15 1 Gi3/46 Trusted 15 1 Gi3/46 Trusted None N/A Gi3/47 Untrusted None N/A				
Gi3/17 Untrusted 15 1 Gi3/18 Untrusted 15 1 Gi3/19 Untrusted 15 1 Gi3/20 Untrusted 15 1 Gi3/20 Untrusted 15 1 Gi3/21 Untrusted 15 1 Gi3/22 Untrusted 15 1 Gi3/22 Untrusted 15 1 Gi3/23 Untrusted 15 1 Gi3/24 Untrusted 15 1 Gi3/25 Untrusted 15 1 Gi3/26 Untrusted 15 1 Gi3/27 Untrusted 15 1 Gi3/28 Untrusted 15 1 Gi3/29 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/32 Untrusted 15 1 Gi3/33 Untrusted 15 1 Gi3/34 Untrusted 15 1 Gi3/35 Untrusted 15 1 Gi3/36 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/34 Untrusted 15 1 Gi3/35 Untrusted 15 1 Gi3/36 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/41 Untrusted 15 1 Gi3/42 Untrusted 15 1 Gi3/43 Untrusted 15 1 Gi3/44 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/46 Trusted None N/A Gi3/47 Untrusted 15 1				
Gi3/18 Untrusted 15 1 Gi3/19 Untrusted 15 1 Gi3/20 Untrusted 15 1 Gi3/21 Untrusted 15 1 Gi3/21 Untrusted 15 1 Gi3/22 Untrusted 15 1 Gi3/23 Untrusted 15 1 Gi3/24 Untrusted 15 1 Gi3/25 Untrusted 15 1 Gi3/26 Untrusted 15 1 Gi3/27 Untrusted 15 1 Gi3/28 Untrusted 15 1 Gi3/29 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/32 Untrusted 15 1 Gi3/33 Untrusted 15 1 Gi3/34 Untrusted 15 1 Gi3/35 Untrusted 15 1 Gi3/36 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/36 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/41 Untrusted 15 1 Gi3/42 Untrusted 15 1 Gi3/43 Untrusted 15 1 Gi3/44 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/46 Trusted 15 1 Gi3/46 Trusted 15 1 Gi3/47 Untrusted 15 1				
Gi3/19 Untrusted 15 1 Gi3/20 Untrusted 15 1 Gi3/21 Untrusted 15 1 Gi3/22 Untrusted 15 1 Gi3/22 Untrusted 15 1 Gi3/23 Untrusted 15 1 Gi3/24 Untrusted 15 1 Gi3/25 Untrusted 15 1 Gi3/26 Untrusted 15 1 Gi3/27 Untrusted 15 1 Gi3/28 Untrusted 15 1 Gi3/29 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/32 Untrusted 15 1 Gi3/33 Untrusted 15 1 Gi3/33 Untrusted 15 1 Gi3/34 Untrusted 15 1 Gi3/35 Untrusted 15 1 Gi3/36 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/41 Untrusted 15 1 Gi3/42 Untrusted 15 1 Gi3/43 Untrusted 15 1 Gi3/44 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/46 Trusted 15 1 Gi3/46 Trusted 15 1 Gi3/47 Untrusted 15 1 Gi3/47 Untrusted 15 1 Gi3/46 Trusted None N/A Gi3/47 Untrusted 15 1				
Gi3/20 Untrusted 15 1 Gi3/21 Untrusted 15 1 Gi3/22 Untrusted 15 1 Gi3/23 Untrusted 15 1 Gi3/24 Untrusted 15 1 Gi3/25 Untrusted 15 1 Gi3/26 Untrusted 15 1 Gi3/27 Untrusted 15 1 Gi3/28 Untrusted 15 1 Gi3/29 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/32 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/32 Untrusted 15 1 Gi3/33 Untrusted 15 1 Gi3/34 Untrusted 15 1 Gi3/35 Untrusted 15 1 Gi3/36 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/36 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/41 Untrusted 15 1 Gi3/42 Untrusted 15 1 Gi3/43 Untrusted 15 1 Gi3/44 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/46 Trusted None N/A Gi3/47 Untrusted 15 1				
Gi3/21 Untrusted 15 1 Gi3/22 Untrusted 15 1 Gi3/23 Untrusted 15 1 Gi3/24 Untrusted 15 1 Gi3/25 Untrusted 15 1 Gi3/26 Untrusted 15 1 Gi3/27 Untrusted 15 1 Gi3/28 Untrusted 15 1 Gi3/29 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/32 Untrusted 15 1 Gi3/32 Untrusted 15 1 Gi3/33 Untrusted 15 1 Gi3/34 Untrusted 15 1 Gi3/35 Untrusted 15 1 Gi3/36 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/34 Untrusted 15 1 Gi3/35 Untrusted 15 1 Gi3/36 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/41 Untrusted 15 1 Gi3/42 Untrusted 15 1 Gi3/43 Untrusted 15 1 Gi3/44 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/46 Trusted None N/A Gi3/47 Untrusted 15 1				
Gi3/22 Untrusted 15 1 Gi3/23 Untrusted 15 1 Gi3/24 Untrusted 15 1 Gi3/25 Untrusted 15 1 Gi3/26 Untrusted 15 1 Gi3/27 Untrusted 15 1 Gi3/28 Untrusted 15 1 Gi3/29 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/32 Untrusted 15 1 Gi3/33 Untrusted 15 1 Gi3/34 Untrusted 15 1 Gi3/35 Untrusted 15 1 Gi3/36 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/36 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/41 Untrusted 15 1 Gi3/42 Untrusted 15 1 Gi3/44 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/46 Trusted 15 1 Gi3/46 Trusted 15 1 Gi3/46 Trusted None N/A Gi3/47 Untrusted 15 1				
Gi3/23 Untrusted 15 1 Gi3/24 Untrusted 15 1 Gi3/25 Untrusted 15 1 Gi3/26 Untrusted 15 1 Gi3/27 Untrusted 15 1 Gi3/28 Untrusted 15 1 Gi3/29 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/31 Untrusted 100 1 Gi3/32 Untrusted 15 1 Gi3/32 Untrusted 15 1 Gi3/33 Untrusted 15 1 Gi3/34 Untrusted 15 1 Gi3/35 Untrusted 15 1 Gi3/36 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/41 Untrusted 15 1 Gi3/44 Untrusted 15 1 Gi3/44 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/46 Trusted 15 1 Gi3/47 Untrusted 15 1 Gi3/46 Trusted 15 1 Gi3/47 Untrusted 15 1 Gi3/47 Untrusted 15 1 Gi3/47 Untrusted 15 1 Gi3/46 Trusted None N/A Gi3/47 Untrusted 15 1				
Gi3/24 Untrusted 15 1 Gi3/25 Untrusted 15 1 Gi3/26 Untrusted 15 1 Gi3/27 Untrusted 15 1 Gi3/28 Untrusted 15 1 Gi3/29 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/32 Untrusted 15 1 Gi3/32 Untrusted 15 1 Gi3/33 Untrusted 15 1 Gi3/34 Untrusted 15 1 Gi3/35 Untrusted 15 1 Gi3/36 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/41 Untrusted 15 1 Gi3/42 Untrusted 15 1 Gi3/44 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/46 Trusted 15 1 Gi3/46 Trusted 15 1 Gi3/46 Trusted 15 1 Gi3/47 Untrusted 15 1 Gi3/47 Untrusted 15 1 Gi3/46 Trusted 15 1 Gi3/47 Untrusted 15 1 Gi3/47 Untrusted 15 1 Gi3/47 Untrusted 15 1 Gi3/46 Trusted None N/A Gi3/47 Untrusted 15 1				
Gi3/25 Untrusted 15 1 Gi3/26 Untrusted 15 1 Gi3/27 Untrusted 15 1 Gi3/28 Untrusted 15 1 Gi3/29 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/31 Untrusted 15 1 Gi3/32 Untrusted 15 1 Gi3/33 Untrusted 15 1 Gi3/34 Untrusted 15 1 Gi3/35 Untrusted 15 1 Gi3/36 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/41 Untrusted 15 1 Gi3/42 Untrusted 15 1 Gi3/42 Untrusted 15 1 Gi3/43 Untrusted 15 1 Gi3/44 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/46 Trusted 15 1 Gi3/47 Untrusted 15 1 Gi3/47 Untrusted 15 1 Gi3/47 Untrusted 15 1 Gi3/46 Trusted None N/A Gi3/47 Untrusted 15 1				
Gi3/26 Untrusted 15 1 Gi3/27 Untrusted 15 1 Gi3/28 Untrusted 15 1 Gi3/29 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/31 Untrusted 100 1 Gi3/32 Untrusted 15 1 Gi3/33 Untrusted 15 1 Gi3/34 Untrusted 15 1 Gi3/35 Untrusted 15 1 Gi3/36 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/41 Untrusted 15 1 Gi3/42 Untrusted 15 1 Gi3/44 Untrusted 15 1 Gi3/45 Untrusted 15				
Gi3/27 Untrusted 15 1 Gi3/28 Untrusted 15 1 Gi3/29 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/31 Untrusted 100 1 Gi3/32 Untrusted 15 1 Gi3/33 Untrusted 15 1 Gi3/34 Untrusted 15 1 Gi3/35 Untrusted 15 1 Gi3/36 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/41 Untrusted 15 1 Gi3/42 Untrusted 15 1 Gi3/43 Untrusted 15 1 Gi3/44 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/46 Trusted None N/A				1
Gi3/28 Untrusted 15 1 Gi3/29 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/31 Untrusted 100 1 Gi3/32 Untrusted 15 1 Gi3/33 Untrusted 15 1 Gi3/34 Untrusted 15 1 Gi3/35 Untrusted 15 1 Gi3/36 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/41 Untrusted 15 1 Gi3/42 Untrusted 15 1 Gi3/43 Untrusted 15 1 Gi3/44 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/46 Trusted None N/A Gi3/47 Untrusted 15 1			15	1
Gi3/29 Untrusted 15 1 Gi3/30 Untrusted 15 1 Gi3/31 Untrusted 100 1 Gi3/32 Untrusted 15 1 Gi3/33 Untrusted 15 1 Gi3/34 Untrusted 15 1 Gi3/35 Untrusted 15 1 Gi3/36 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/41 Untrusted 15 1 Gi3/42 Untrusted 15 1 Gi3/43 Untrusted 15 1 Gi3/44 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/46 Trusted None N/A Gi3/47 Untrusted 15 1				1
Gi3/31 Untrusted 100 1 Gi3/32 Untrusted 15 1 Gi3/33 Untrusted 15 1 Gi3/34 Untrusted 15 1 Gi3/35 Untrusted 15 1 Gi3/36 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/41 Untrusted 15 1 Gi3/42 Untrusted 15 1 Gi3/42 Untrusted 15 1 Gi3/43 Untrusted 15 1 Gi3/44 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/46 Trusted None N/A Gi3/47 Untrusted 15 1			15	1
Gi3/32 Untrusted 15 1 Gi3/33 Untrusted 15 1 Gi3/34 Untrusted 15 1 Gi3/35 Untrusted 15 1 Gi3/36 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/41 Untrusted 15 1 Gi3/41 Untrusted 15 1 Gi3/42 Untrusted 15 1 Gi3/43 Untrusted 15 1 Gi3/44 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/46 Trusted None N/A Gi3/47 Untrusted 15 1	Gi3/30	Untrusted	15	1
Gi3/33 Untrusted 15 1 Gi3/34 Untrusted 15 1 Gi3/35 Untrusted 15 1 Gi3/36 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/41 Untrusted 15 1 Gi3/42 Untrusted 15 1 Gi3/42 Untrusted 15 1 Gi3/43 Untrusted 15 1 Gi3/44 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/46 Trusted None N/A Gi3/47 Untrusted 15 1	Gi3/31	Untrusted	100	1
Gi3/34 Untrusted 15 1 Gi3/35 Untrusted 15 1 Gi3/36 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/41 Untrusted 15 1 Gi3/42 Untrusted 15 1 Gi3/42 Untrusted 15 1 Gi3/43 Untrusted 15 1 Gi3/44 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/46 Trusted None N/A Gi3/47 Untrusted 15 1	Gi3/32	Untrusted	15	1
Gi3/35 Untrusted 15 1 Gi3/36 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/41 Untrusted 15 1 Gi3/42 Untrusted 15 1 Gi3/42 Untrusted 15 1 Gi3/43 Untrusted 15 1 Gi3/44 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/46 Trusted None N/A Gi3/47 Untrusted 15 1	Gi3/33	Untrusted	15	1
Gi3/36 Untrusted 15 1 Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/41 Untrusted 15 1 Gi3/42 Untrusted 15 1 Gi3/43 Untrusted 15 1 Gi3/44 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/46 Trusted None N/A Gi3/47 Untrusted 15 1	Gi3/34	Untrusted	15	1
Gi3/37 Untrusted 15 1 Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/41 Untrusted 15 1 Gi3/42 Untrusted 15 1 Gi3/43 Untrusted 15 1 Gi3/44 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/46 Trusted None N/A Gi3/47 Untrusted 15 1	Gi3/35	Untrusted	15	1
Gi3/38 Untrusted 15 1 Gi3/39 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/41 Untrusted 15 1 Gi3/42 Untrusted 15 1 Gi3/43 Untrusted 15 1 Gi3/44 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/46 Trusted None N/A Gi3/47 Untrusted 15 1	Gi3/36	Untrusted	15	1
Gi3/39 Untrusted 15 1 Gi3/40 Untrusted 15 1 Gi3/41 Untrusted 15 1 Gi3/42 Untrusted 15 1 Gi3/43 Untrusted 15 1 Gi3/44 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/46 Trusted None N/A Gi3/47 Untrusted 15 1	Gi3/37	Untrusted	15	1
Gi3/40 Untrusted 15 1 Gi3/41 Untrusted 15 1 Gi3/42 Untrusted 15 1 Gi3/43 Untrusted 15 1 Gi3/44 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/46 Trusted None N/A Gi3/47 Untrusted 15 1	Gi3/38	Untrusted	15	1
Gi3/41 Untrusted 15 1 Gi3/42 Untrusted 15 1 Gi3/43 Untrusted 15 1 Gi3/44 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/46 Trusted None N/A Gi3/47 Untrusted 15 1	Gi3/39	Untrusted	15	1
Gi3/42 Untrusted 15 1 Gi3/43 Untrusted 15 1 Gi3/44 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/46 Trusted None N/A Gi3/47 Untrusted 15 1		Untrusted	15	1
Gi3/42 Untrusted 15 1 Gi3/43 Untrusted 15 1 Gi3/44 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/46 Trusted None N/A Gi3/47 Untrusted 15 1	Gi3/41	Untrusted	15	1
Gi3/44 Untrusted 15 1 Gi3/45 Untrusted 15 1 Gi3/46 Trusted None N/A Gi3/47 Untrusted 15 1		Untrusted	15	1
Gi3/45 Untrusted 15 1 Gi3/46 Trusted None N/A Gi3/47 Untrusted 15 1	Gi3/43	Untrusted	15	1
Gi3/46 Trusted None N/A Gi3/47 Untrusted 15 1	Gi3/44	Untrusted	15	1
Gi3/47 Untrusted 15 1	Gi3/45	Untrusted	15	1
	Gi3/46	Trusted	None	N/A
Gi3/48 Untrusted 15 1	Gi3/47	Untrusted	15	1
	Gi3/48	Untrusted	15	1

SwitchB# show errdisable recovery

ErrDisable Reason	Timer Status
udld	Disabled
bpduguard	Disabled
security-violatio	Disabled
channel-misconfig	Disabled
vmps	Disabled
pagp-flap	Disabled
dtp-flap	Disabled
link-flap	Disabled
12ptguard	Disabled
psecure-violation	Disabled
gbic-invalid	Disabled
dhcp-rate-limit	Disabled
unicast-flood	Disabled
storm-control	Disabled
arp-inspection	Enabled

Timer interval: 300 seconds

Interfaces that will be enabled at the next timeout:

SwitchB#

1w2d: %SW_DAI-4-PACKET_RATE_EXCEEDED: 101 packets received in 739 milliseconds on Gi3/31.

1w2d: %PM-4-ERR_DISABLE: arp-inspection error detected on Gi3/31, putting Gi3/31 in err-disable state

SwitchB# show clock

*02:21:43.556 UTC Fri Feb 4 2005

SwitchB#

SwitchB# show interface g3/31 status

Port Name Status Vlan Duplex Speed Type Gi3/31 err-disabled 100 auto 10/100/1000-TX

SwitchB#

SwitchB#

1w2d: %PM-4-ERR_RECOVER: Attempting to recover from arp-inspection err-disable state on Gi3/31

SwitchB# show interface g3/31 status

Port Name Status Vlan Duplex Speed Type

Gi3/31 connected 100 a-full a-100 10/100/1000-TX

SwitchB# show clock

*02:27:40.336 UTC Fri Feb 4 2005

SwitchB#

確認検査の実行

DAI では、無効な IP/MAC アドレスバインディングを持つ ARP パケットを代行受信し、記録して、ドロップします。スイッチが宛先 MAC アドレス、送信側とターゲット IP アドレス、および送信元 MAC アドレスで追加の検査を実行するよう設定できます。

着信 ARP パケットで特定の検査を実行するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config) # ip arp inspection validate {[src-mac][dst-mac][ip]}	着信 ARP パケットで特定の検査を実行します。デフォルトでは、追加の検査は実行されません。
		キーワードの意味は次のとおりです。
		• src-mac では、ARP の本体内の送信側 MAC アドレスに対してイーサネット ヘッダー内の送信元 MAC アドレスを検査します。この検査は、ARP 要求および ARP 応答の両方で実行されます。イネーブルの場合、異なるMAC アドレスを持つパケットは無効として分類されてドロップされます。
		• dst-mac では、ARP の本体内のターゲット MAC アドレスに対してイーサネット ヘッダー内の宛先 MAC アドレスを検査します。この検査は、ARP 応答に対して実行されます。イネーブルの場合、異なる MAC アドレスを持つパケットは無効として分類されてドロップされます。
		• ip では、無効で予期しない IP アドレスに関して ARP の 本 体 を 検 査 し ま す。ア ド レ ス に は、0.0.0.0、255.255.255.255、およびすべての IP マルチキャスト ア ドレスが含まれます。送信側 IP アドレスはすべての ARP 要求および ARP 応答で検査され、ターゲット IP アドレスは、ARP 応答でのみ検査されます。
		キーワードは、少なくとも 1 つ指定する必要があります。 各コマンドは、以前のコマンドの設定を上書きします。つ まり、コマンドが src および dst mac 確認をイネーブルに し、2 番めのコマンドが IP 確認のみをイネーブルにした場 合、src および dst mac 確認は 2 番めのコマンドによりディ セーブルになります。
ステップ 3	Switch(config)# exit	特権 EXEC モードに戻ります。
ステップ 4	Switch# show ip arp inspection vlan vlan-range	設定を確認します。
ステップ 5	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

検査をディセーブルにするには、no ip arp inspection validate [src-mac] [dst-mac] [ip] グローバル コンフィギュレーション コマンドを使用します。転送、ドロップ、MAC 確認の失敗、および IP 確認の失敗パケットの統計情報を表示するには、show ip arp inspection statistics 特権 EXEC コマンドを使用します。

次に、送信元 MAC 確認を設定する例を示します。イーサネット ヘッダー内の送信元アドレスが ARP ボディ内の送信側ハードウェア アドレスに一致しない場合、パケットはドロップされ、エラー メッセージが生成される可能性があります。

SwitchB# configure terminal

Enter configuration commands, one per line. End with ${\tt CNTL/Z.}$

SwitchB(config)# ip arp inspection validate src-mac

SwitchB(config)# exit

SwitchB# show ip arp inspection vlan 100

Source Mac Validation : Enabled Destination Mac Validation : Disabled IP Address Validation : Disabled

Vlan	Configuration	Operation	ACL Match	Static ACL

100 Enabled Active

Vlan ACL Logging DHCP Logging -----100

Deny Deny

SwitchB#

1w2d: %SW_DAI-4-INVALID_ARP: 9 Invalid ARPs (Req) on Gi3/31, vlan 100.([0002.0002.0002/170.1.1.2/0001.0001.0001/170.1.1.1/02:30:24 UTC Fri Feb 4 2005])



CHAPTER

42

ACL によるネットワーク セキュリティ の設定

この章では、Access Control List (ACL; アクセス コントロール リスト)を使用して Catalyst 4500 シリーズ スイッチ上でネットワーク セキュリティを設定する方法について説明します。



この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univered/cc/td/doc/product/software/ios122sr/cr/index.htm

この章の主な内容は、次のとおりです。

- ACL の概要 (p.42-2)
- ハードウェアおよびソフトウェア ACL のサポート (p.42-6)
- TCAM プログラミングと Supervisor Engine II-Plus、Supervisor Engine IV、Supervisor Engine V、および Supervisor Engine V-10GE の ACL (p.42-7)
- Supervisor Engine 6-E の TCAM プログラミングと ACL (p.42-16)
- ACL のレイヤ 4 演算 (p.42-16)
- ユニキャスト MAC アドレス フィルタリングの設定 (p.42-20)
- 名前付き MAC 拡張 ACL の設定 (p.42-20)
- 名前付き IPv6 ACL の設定 (p.42-22)
- レイヤ 3 インターフェイスへの IPv6 ACL の適用 (p.42-23)
- VLAN マップの設定 (p.42-24)
- VLAN アクセス マップ情報の表示 (p.42-31)
- ルータ ACL を VLAN マップと併用する方法 (p.42-32)
- PACL の設定 (p.42-34)
- VLAN マップおよびルータを PACL と併用する方法 (p.42-38)



(注)

次の説明は、特に記述がないかぎり、Supervisor Engine 6-E の設定と Supervisor Engine 6-E 以外の設定の両方に該当します。

ACL の概要

ここでは、次の内容について説明します。

- ACL の概要 (p.42-2)
- ACL を使用するサポート対象機能 (p.42-3)
- ルータ ACL (p.42-3)
- PACL (p.42-4)
- VLAN マップ (p.42-5)

ACL の概要

ACL は、パケットに適用される許可条件および拒否条件を集めて順番に並べたものです。パケットがインターフェイスに着信すると、スイッチはパケットのフィールドと適用される ACL を比較し、アクセス リストに指定されている条件に基づいて、転送に必要な許可がパケットに与えられているかどうかを調べます。スイッチはパケットをアクセス リストの条件と1つ1つ突き合わせます。最初に一致した条件によって、スイッチがパケットを許可するかまたは拒否するかが決まります。スイッチは最初に一致した時点で条件のテストを中止するため、リストに条件を指定する順序が重要です。いずれの条件とも一致しなかった場合、スイッチはパケットを拒否します。制限がない場合、スイッチはパケットを転送し、制限がある場合はパケットをドロップします。

従来、スイッチはレイヤ 2 で稼働し、VLAN (仮想 LAN) 内でトラフィックをスイッチングしていました。一方、ルータはレイヤ 3 の VLAN 間でトラフィックをルーティングしていました。Catalyst 4500 シリーズ スイッチは、レイヤ 3 スイッチングを使用して、VLAN 間のパケット ルーティングの速度を向上させます。レイヤ 3 スイッチでブリッジングされたパケットは、外部ルータに送信されずに内部でルーティングされます。そのあと、再度ブリッジングされて宛先に送信されます。スイッチはこのプロセス中に、VLAN 内でブリッジングされるパケットを含めて、すべてのパケットを制御します。

トラフィックをフィルタリングし、ネットワークに基本的なセキュリティを導入するには、ルータまたはスイッチにアクセスリストを設定します。ACLを設定しないと、スイッチを通過するすべてのパケットが、ネットワーク内のすべての場所に転送されることがあります。ACLを使用すると、ネットワークの場所ごとにアクセス可能なホストを制御したり、ルータインターフェイスで転送またはブロックされるトラフィックの種類を決定できます。たとえば、電子メールトラフィックの転送を許可して、Telnetトラフィックの転送を禁止できます。ACLは着信トラフィック、発信トラフィック、またはその両方をブロックするように設定できます。ただし、レイヤ2インターフェイスでは、ACLを適用できるのは着信方向だけです。

ACL には、Access Control Entry (ACE; アクセス コントロール エントリ)が順番に記述されています。各 ACE では、許可 (permit) または拒否 (deny) および ACE と一致するためのパケットの必須条件のセットを指定します。許可または拒否の意味は、ACL の使用状況に応じて変わります。

Catalyst 4500 シリーズ スイッチでは、次の3つの ACL タイプがサポートされています。

- TCP、UDP、Internet Group Management Protocol(IGMP) Internet Control Message Protocol(ICMP)
 などの IP トラフィックをフィルタリングする IP ACL
- IPv6 ACL (Supervisor Engine 6-E にのみ該当)

ACL を使用するサポート対象機能

スイッチは、トラフィックをフィルタリングするため、次に示す 3 種類の ACL をサポートしています。

- ルータ ACL は、レイヤ 3 インターフェイスに適用されます。この ACL は、VLAN 間でルーティングされたトラフィックのアクセスを制御します。すべての Catalyst 4500 シリーズ スイッチでルータ ACL を作成できますが、レイヤ 3 インターフェイスに ACL を適用して、VLAN 間でルーティングされたパケットをフィルタリングするには、スイッチに Cisco IOS ソフトウェア イメージをインストールする必要があります。
- Port ACL (PACL; ポート ACL) は、レイヤ 2 インターフェイスに入るトラフィックのアクセスを制御します。ハードウェアの CAM (連想メモリ) エントリが十分でない場合、出力 PACL がポートに適用されず、警告メッセージがユーザに送られます (この制限は、出力 PACL のすべてのアクセス グループ モードに適用します)。CAM エントリが十分な場合、出力ポート ACL は再適用されます。

レイヤ 2 ポートに出力 PACL が設定されている場合、レイヤ 2 ポートが属する VLAN に VACL またはルータ ACL を設定できません。その逆の場合も同じです。つまり、PACL および VLAN ベースの ACL (VACL およびルータ ACL) は、レイヤ 2 ポート上では相互に排他的です。この制限はすべてのアクセス グループ モードに適用されます。入力方向では、ポート ACL、VLAN ベース ACL、およびルータ ACL が共存できます。

1 つのレイヤ 2 インターフェイスに適用できるのは、IP アクセス リスト 1 つと MAC (メディア アクセス制御) アクセス リスト 1 つです。

• VLAN ACL または VLAN マップは、すべてのパケット(ブリッジドパケットおよびルーテッドパケット)のアクセスを制御します。VLAN マップを使用すると、同じ VLAN 内のデバイス間で転送されるトラフィックをフィルタリングできます。VLAN マップを作成または適用するために、拡張イメージをインストールする必要はありません。VLAN マップは、IP のレイヤ3 アドレスに基づいてアクセス コントロールするように設定されています。イーサネット ACEを使用する MAC アドレスにより、サポートされていないプロトコルがアクセス コントロールされます。VLAN マップを VLAN に適用すると、VLAN に入るすべてのパケット(ルーテッドパケットまたはブリッジドパケット)が VLAN マップと照合されます。パケットはスイッチポートを介して VLAN に入ることができます。ルーティングされたパケットの場合は、ルーテッドポートを介して VLAN に入ることができます。

同じスイッチ上でルータ ACL と VLAN マップを両方使用できます。

ルータ ACL

サポートされる各タイプのアクセス リスト1 つをインターフェイスに適用できます。



(注)

Cisco IOS Release 12.2(40)SG を実行している Catalyst 4500 シリーズ スイッチは、IPv6 Port ACL (PACL)をサポート*しません*。

1 つの ACL を特定のインターフェイスの複数の機能に使用できます。また、1 つの機能に複数の ACL を使用することもできます。1 つのルータ ACL を複数の機能で使用する場合、そのルータ ACL は複数回テストされます。アクセス リストのタイプによって、一致処理に対する入力が決まります。

- 標準 IP アクセス リストは、送信元アドレスを使用して一致処理を行います。
- 拡張 IP アクセス リストは、送信元アドレス、宛先アドレス、およびオプションのプロトコルタイプ情報を使用して一致処理を行います。

スイッチは、特定のインターフェイスおよび方向に対する設定機能に関連付けられている ACL をテストします。パケットがスイッチのインターフェイスに着信すると、そのインターフェイスに設定されているすべての着信機能に対応する ACL がテストされます。パケットがルーティングされてからネクスト ホップに転送されるまでの間に、出力インターフェイスに設定された発信機能に対応するすべての ACL がテストされます。

ACL は、ACL 内のエントリとの一致結果に基づいて、転送を許可または拒否します。たとえば、アクセスリストを使用すると、ネットワークの特定の場所へのアクセスを特定のホストに許可し、別のホストに対しては禁止できます。図 42-1 の例では、ルータへの入力に適用されている ACL に基づき、ホスト A は人事部ネットワークへのアクセスを許可されますが、ホスト B は拒否されます。

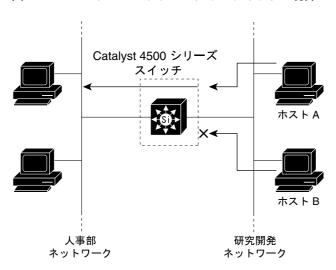


図 42-1 ACL によるネットワーク トラフィックの制御

 X = ACL はホスト B からのトラフィックを拒否 し、ホスト A からのトラフィックを許可
 → = パケット

PACL

スイッチ上のレイヤ 2 インターフェイスにも ACL を適用できます。PACL は、物理インターフェイスおよび EtherChannel インターフェイス上でサポートされています。

レイヤ2インターフェイス上では、次のアクセスリストがサポートされています。

- 送信元アドレスを使用する標準 IP アクセス リスト
- 送信元アドレス、宛先アドレス、およびオプションのプロトコル タイプ情報を使用する拡張 IP アクセス リスト
- 送信元 MAC アドレス、宛先 MAC アドレス、およびオプションのプロトコル タイプ情報を使用する MAC 拡張アクセス リスト

ルータ ACL と同様、スイッチは所定のインターフェイスに設定されている機能に関連付けられている ACL をテストし、パケットが ACL 内のエントリと一致するかどうかによって、パケットの転送を許可または拒否します。図 42-1 の例では、すべてのワークステーションが同じ VLAN 内にある場合、レイヤ 2 の入力に適用されている ACL によって、ホスト A は人事部ネットワークへのアクセスが許可されますが、ホスト B は同じネットワークへのアクセスを拒否されます。

PACL をトランク ポートに適用すると、そのトランク ポートにあるすべての VLAN 上で ACL によるトラフィックのフィルタリングが行われます。音声 VLAN があるポートに PACL を適用すると、データ VLAN と音声 VLAN の両方でその ACL によるトラフィックのフィルタリングが行われます。

PACL を使用すると、IP アクセス リストを使用して IP トラフィックをフィルタリングし、MAC アドレスを使用して IP 以外のトラフィックをフィルタリングできます。 インターフェイスに IP アクセス リストと MAC アクセス リストの両方を適用することにより、同一のレイヤ 2 インターフェイス上で IP トラフィックと IP 以外のトラフィックをフィルタリングできます。



1 つのレイヤ 2 インターフェイスに、IP アクセス リストと MAC アクセス リストのそれぞれを 2 つ以上適用できません。すでに IP アクセス リストまたは MAC アクセス リストが 1 つずつ設定されているレイヤ 2 インターフェイスに、新しい IP アクセス リストまたは MAC アクセス リストを適用すると、前に設定した ACL が新しい ACL に置き換わります。

VLAN マップ

VLAN マップを使用すると、VLAN のすべてのトラフィックのアクセスを制御できます。VLAN の内外でルーティングされる、または VLAN 内でブリッジングされるすべてのパケットに対して、スイッチの VLAN マップを適用できます。ルータ ACL と異なり、VLAN マップでは方向(着信または発信)は定義されません。

VLAN マップを設定すると、IP トラフィックのレイヤ 3 アドレスを照合できます。すべての IP 以外のプロトコルは、VLAN マップの MAC ACL を使用して、MAC アドレスおよび EtherType によってアクセス コントロールされます (IP トラフィックには、VLAN マップの MAC ACL によるアクセス コントロールが行われません)。VLAN マップはスイッチを通過するパケットにのみ適用できます。ハブのホスト間、またはこのスイッチに接続された別のスイッチのホスト間を通過するトラフィックには、VLAN マップを適用できません。

VLAN マップを使用すると、パケットの転送は、マップに指定されたアクションに基づいて許可または拒否されます。図 42-2 に、VLAN マップを適用して、特定タイプのトラフィックを VLAN 10のホスト A から転送できないように設定する例を示します。

図 42-2 VLAN マップによるトラフィックの制御



X = VLAN マップはホスト A からの 特定タイプのトラフィックを拒否 → = パケット

94153

ハードウェアおよびソフトウェア ACL のサポート

ここでは、ACL をハードウェア、ソフトウェアのどちらで処理するかを決定する方法について説明します。

- 標準および拡張 ACL の拒否 (deny) 文と一致するフローは、ICMP 到達不能メッセージがディセーブルの場合、ハードウェアでドロップされます。
- 標準 ACL の (permit)文に一致するフローは、ハードウェアで処理されます。
- ソフトウェアでは、次の ACL タイプはサポートされていません。
 - 標準 Xerox Network Systems (XNS) プロトコル アクセス リスト
 - 拡張 XNS アクセス リスト
 - DECnet アクセス リスト
 - プロトコル タイプコード アクセス リスト
 - 標準 Internet Packet Exchange (IPX) アクセス リスト
 - 拡張 IPX アクセス リスト



ロギングが必要なパケットは、ソフトウェアで処理されます。ロギング用にパケットのコピーが CPU に送信され、実際のパケットはハードウェアで転送されるので、ロギング対象外のパケットの 処理は影響を受けません。

デフォルトでは、アクセス リストによりパケットが拒否されると、ICMP 到達不能メッセージが Catalyst 4500 シリーズ スイッチ スイッチによって送信されます。

入力インターフェイス上でハードウェア内のアクセス リスト拒否パケットをドロップするには、no ip unreachables インターフェイス コンフィギュレーション コマンドを使用して ICMP 到達不能 メッセージをディセーブルにする必要があります。ip unreachables コマンドはデフォルトでイネーブルに設定されています。



(注)

Cisco IOS Release 12.2(40)SG は、IPv6 トラフィックをルーティングするインターフェイス上での ip unreachables のディセーブル化をサポートしません。



(注)

すべてのレイヤ 3 インターフェイスで no ip unreachable コマンドを設定する場合、出力 ACL 拒否 パケットは、CPU に届きません。

Catalyst 4500 シリーズ スイッチでの TCAM エントリおよびマスク利用率は、次の要素に基づきます。

- ACL 設定
- スーパーバイザ モデル
- IOS ソフトウェアのバージョン

Supervisor Engine II-Plus-10GE、Supervisor Engine V-10GE、および Catalyst 4948-10GE スイッチの場合、エントリおよびマスク利用率は、IOS ソフトウェア バージョンに関係なく、TCAM リージョンのエントリ数で割った ACL 設定の ACE 数と等しくなります。最適化された TCAM 利用率は、必要ありません。

Supervisor Engine II-Plus-TS、Supervisor Engines IV、Supervisor Engines V、および Catalyst 4948 スイッチの場合、IOS ソフトウェアのリリースに関係なく、8 つまでのエントリが TCAM の 1 つのマスクを共有します。したがって、TCAM 利用率は、ACL の設定によって変わります。また、各 ACL の設定順によっても変わります。ある ACL が別の ACL の前に設定された場合と、その逆の順で設定された場合では、TCAM 利用率は異なります。同じ ACL 設定を実行コンフィギュレーションにコピーしても、TCAM 利用率が変わります。

Supervisor II-Plus-TS、IV、V、および Catalyst 4948 スイッチでの TCAM 利用率は、ACL 設定および IOS ソフトウェア バージョンに従って最適化されます。たとえば、Cisco IOS Release 12.2(31)SGA 以降のリリースでは、マスクを保持するために、順番に依存しない ACL エントリの順序を自動的 に付け直します。単一パケットが ACL の 1 つにのみ一致する場合、2 つの ACE は順番に依存しません。たとえば、次の 2 つの ACE は順番に依存しません。

```
permit ip host 10.1.1.10 any permit ip host 10.1.1.20 any
```

最初の ACE に一致するパケットは、2 番めの ACE には一致せず、その逆も同様です。これに対して、次の 2 つの ACE は順番に依存します。

```
permit ip host 10.1.1.10 any permit ip any host 10.1.1.20
```

送信元 IP アドレスが 10.1.1.10、宛先 IP アドレスが 10.1.1.20 のパケットは、両方の ACE に一致することができるため、その順番が問題になります。

展開する前に Supervisor Engine II-Plus-TS、IV、V、および Catalyst 4948 スイッチの TCAM 利用率を見積もるときは、デフォルトの設定から開始します。マスクを共有する ACE をプログラミングするときのダイナミックな性質により、ACL がすでにプログラミングされているときの TCAM 利用率の見積もりは、予想できません。

Cisco IOS Release 12.2(31)SGA 以降では、TCAM が空である場合、IP ACL の TCAM 利用率を見積もることができます。各 IP ACL では、4 つの ACE が自動的に ACL に追加されます。4 つの ACE とは、2 つのスタティック ACE、追加された IP 全拒否 ACE、および追加された全許可 ACE です。したがって、1 つの IP ACL のマスクの最少数は5 です。残りの ACE で利用されるマスクの数を調べるには、8 つを超える ACE を持つ別々のマスクに対して1 つを追加して、異なるマスクの数をカウントします。

12.2(31)SGA より前のリリースの IOS ソフトウェアを実行している Supervisor Engine II-Plus-TS、IV、 V、および Catalyst 4948 スイッチの場合、ACL は TCAM のプログラミング前には自動的に最適化 されません。ACLの設定前に同様のマスクを持つACEをグループ化すると、マスクの利用率が向 上する場合があります。



Supervisor Engine II-Plus-TS、IV、V、および Catalyst 4948 スイッチで Cisco IOS Release 12.2(31)SGA 以上にアップグレードしたあと、TCAM ACL 利用率は、独立した ACE の再順番付けのために低下 することがあります。逆に、Cisco IOS Release 12.2(31)SG 以下にダウングレードすると、TCAM 利 用率は上がることがあります。

TCAM プログラミング アルゴリズム



Supervisor Engine 6-E では、TCAM プログラミング アルゴリズムは使用 できません。

Cisco IOS Release 12.2(25)EWA 以降では、packed と scattered の 2 つの TCAM プログラミング アル ゴリズムが Catalyst 4500 および 4900 シリーズ スイッチでサポートされます。packed モード アルゴ リズムは、エントリのマスクが一致する場合、同じ8エントリ TCAM ブロックのエントリをプロ グラムします。現在のエントリのマスクが前のエントリのマスクと異なる場合、スイッチ ソフト ウェアは、新しい8エントリ ブロックにエントリをプログラムします。マスクが変わらない場合、 または設定の開始から終了まで ACL で 8 エントリごとにマスクが変わる場合、Supervisor Engine II-Plus-TS、IV、V、および Catalyst 4948 シリーズ スイッチでは、TCAM が packed モードで完全に 利用されます。

scattered モードでは、単一 ACL のエントリは、ACL が完全にプログラムされるまで、異なる8エ ントリ ブロックに分散されます。連続した ACL に最初の ACL と同じマスク パターンがある場合、 Supervisor Engine II-Plus-TS、IV、V、および Catalyst 4948 シリーズ スイッチの TCAM は、完全に利 用されます。

Supervisor Engine II-Plus-TS、IV、V、および Catalyst 4948 スイッチでの IP ソース ガードの設定に は、scattered モードを推奨します。これは、VLAN 単位の ACL のマスク パターンが、IP ソース ガー ドに対して設定されたすべてのポートで同じためです。つまり、ARPパケットを許可し、ポート セ キュリティが設定されていない場合はレイヤ2トラフィックを許可し、32ビットマスクを持つ特 定の送信元 IP アドレスからの IP トラフィックを許可し、不明を拒否し、さらにすべてを許可しま す。



TCAM プログラミング アルゴリズムは、Cisco IOS Release 12.2(25)EWA または後続のメンテナンス リリースを実行している Supervisor Engine V-10GE および Catalyst 4948-10GE スイッチで設定でき ます。ただし、Supervisor Engine V-10GE および Catalyst 4948-10GE スイッチでは、ACL マスクが ACE 間で共有されていないため、プログラミング アルゴリズムが設定されているかどうかに関係 なく、TCAM 利用率は同じになります。



(注)

TCAM プログラミング アルゴリズムは、Supervisor Engine II-Plus-10GE または Cisco IOS Release 12.2(25)SG 以降を実行している Catalyst 4948-10GE スイッチでは設定できません。



TCAM 利用率は、同じ TCAM プログラミング アルゴリズムを正常に設定したあとには変更しないでください。たとえば、2 回パックされたアクセスリスト ハードウェア エントリの設定は、TCAM 利用率に影響を与えません。ただし、同じ TCAM プログラミング アルゴリズムの連続する設定間に 1 つまたは複数のコマンドが実行された場合、TCAM 利用率は変化することがあります。

TCAM 利用率を変化させるのは、次のような場合です。

- 実行コンフィギュレーションでの ACL または ACE の追加または削除
- ブートフラッシュ、TFTP サーバ、またはコンパクト フラッシュ メモリから実行コンフィギュレーションへの ACL 設定のコピーまたは再コピー
- TCAM プログラミング アルゴリズムの変更
- 実行コンフィギュレーションの NVRAM への保存とスイッチのリロード
- Cisco IOS Release 12.2(31)SGA 以上での access-list hardware region <feature | qos> <input | output> balance <percent> コマンドを使用した、TCAM の機能 ACL または QoS リージョンのサイズ変更
- Cisco IOS Release 12.2(25)EWA に基づくイメージから Cisco IOS Release 12.2(31)SGA に基づくイメージへのアップグレード

これまでに述べたように、ACL をプログラムする際は、エントリおよびマスクの 2 種類のハードウェア リソースが消費されます。これらのリソースのいずれかが使い果たされると、ACL をそれ以上ハードウェアにプログラムすることはできません。

リソースを使い果たした場合は、次を参照します。

- プログラミング アルゴリズムの変更 (p.42-9)
- TCAM リージョンのサイズ変更 (p.42-11)
- 制御パケットのキャプチャのモード選択 (p.42-13)

プログラミング アルゴリズムの変更

システム上のマスクが使い果たされても、エントリは使用できる場合、プログラミング方式を packed から scattered に変更すると、マスクが使用可能になり、ACL をハードウェアにさらにプログラムできるようになります。



ACL プログラミング アルゴリズムを変更したり TCAM リージョンのサイズを変更したりすると、すべての ACL が一時的にハードウェアからアンロードされ、新しい TCAM パラメータに従って再びロードされます。再ロード プロセスが終了するまでは ACL は動作できません。

目的は、ACL エントリごとのマスク数を最小化することにより、TCAM リソースをさらに有効に使用することです。

目的	コマンド
scattered または packed アルゴリズム採用時の TCAM 利用状況を比較	Switch# show platform hardware acl statistics utilization brief
アルゴリズムを packed から scattered に変更	Switch(config)# access-list hardware entries scattered
アルゴリズムを scattered から packed に変更	Switch(config)# access-list hardware entries packed



<u>一</u> (注)

scattered アルゴリズムが設定されているかどうかを判別するには、show running-config コマンドを使用します。scattered が設定されている場合は、access-list hardware entries scattered が表示されます。



(注)

TCAM プログラミング アルゴリズムのデフォルト設定は、packed です。

次の出力は、packed モードで稼働するスイッチで収集したものです。ACL エントリの 49 %だけを プログラムするために、89 %のマスクが必要であることがわかります。

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# access-list hardware entries packed
Switch(config)# end
Switch#
01:15:34: %SYS-5-CONFIG_I: Configured from console by console
Switch#
Switch# show platform hardware acl statistics utilization brief

Entries/Total(%) Masks/Total(%)

		EI	161	iles/1	.01	_a⊥(₀)	Mai	SKS.	/ 10 Lc	11 ((6)
Input	Acl(PortAndVlan)	2016	/	4096	(49)	460	/	512	(89)
Input	Acl(PortOrVlan)	6	/	4096	(0)	4	/	512	(0)
Input	Qos(PortAndVlan)	0	/	4096	(0)	0	/	512	(0)
Input	Qos(PortOrVlan)	0	/	4096	(0)	0	/	512	(0)
Output	Acl(PortAndVlan)	0	/	4096	(0)	0	/	512	(0)
Output	Acl(PortOrVlan)	0	/	4096	(0)	0	/	512	(0)
Output	Qos(PortAndVlan)	0	/	4096	(0)	0	/	512	(0)
Output	Qos(PortOrVlan)	0	/	4096	(0)	0	/	512	(0)

L4Ops: used 2 out of 64

次の出力は、アルゴリズムを scattered に変更したあとに収集したものです。エントリの 49% をプログラムするのに必要なマスク数が 49% に減少したことがわかります。



(注)

シャーシ上のすべてのポートで DHCP スヌーピングおよび IP ソース ガードがイネーブルの場合は、scattered キーワードを使用する必要があります。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# access-list hardware entries scattered
Switch(config)# end
Switch#
01:39:37: %SYS-5-CONFIG_I: Configured from console by console
Switch#
Switch# show platform hardware acl statistics utilization brief
Entries/Total(%) Masks/Total(%)
```

Input	Acl(PortAndVlan)	2016	/	4096	(49)	252	/	512	(49)
Input	Acl(PortOrVlan)	6	/	4096	(0)	5	/	512	(0)
Input	Qos(PortAndVlan)	0	/	4096	(0)	0	/	512	(0)
Input	Qos(PortOrVlan)	0	/	4096	(0)	0	/	512	(0)
Output	Acl(PortAndVlan)	0	/	4096	(0)	0	/	512	(0)
Output	Acl(PortOrVlan)	0	/	4096	(0)	0	/	512	(0)
Output	Qos(PortAndVlan)	0	/	4096	(0)	0	/	512	(0)
Output	Qos(PortOrVlan)	0	/	4096	(0)	0	/	512	(0)

L40ps: used 2 out of 64

Switch#

TCAM リージョンのサイズ変更

TCAM は、異なる種類のエントリを保持するリージョンに分割されます。TCAM には、入力 ACL、出力 ACL、入力 QoS (Quality Of Service) 出力 QoS の 4 種類があります。それぞれが PortAndVlan リージョンと PortOrVlan リージョンに分割されます。デフォルトでは、PortAndVlan リージョンと PortOrVlan リージョンのサイズは同じです。

次の表に、エントリおよびマスク数をサポート対象のスーパーバイザ エンジンごとに示します。スーパーバイザ エンジンのエントリおよびマスク数が、それぞれの TCAM の種類について示されています。たとえば、入力機能 TCAM には 16,000 エントリが、出力機能 TCAM には 16,000 エントリがあります。

スーパーパイザ エンジン	エントリ	マスク
Supervisor Engine III	16,000	2,000
Supervisor Engine IV	16,000	2,000
Supervisor Engine V	16,000	2,000
Supervisor Engine II-Plus	8,000	1,000
Supervisor Engine II-Plus-TS	8,000	1,000
Supervisor Engine V-10GE	16,000	16,000
Supervisor Engine II-Plus-10GE	TBP	TBP



(注)

Supervisor Engine II-Plus-TS、IV、V、および Catalyst 4948 スイッチのマスクに対するエントリの比率が 8:1 であるため、マスク用の TCAM スペースは、エントリ用のスペースが消費される前に消費されることがあります。



(注)

TCAM タイプのあるリージョンは満杯でも他のリージョンは空いていることがあります。このような場合、リージョンの空きエントリをエントリが必要な他のリージョンに移動することによって、リージョンのサイズを変更できます。リージョンのサイズを変更するには access-list hardware region { feature | qos } { input | output } balance コマンドを使用します。それぞれの TCAM には固有のリージョン バランスがあります。



(注)

バランス値を高くすると、PortAndVlan リージョンのエントリが増え、PortOrVlan リージョンのエントリは減ります。バランス値を低くすると、PortAndVlan リージョンのエントリが減り、PortOrVlan リージョンのエントリは増えます。バランス値を 50 にすると、PortAndVlan リージョンと PortOrVlan リージョンの割り当ては同じになります。



(注)

特定の TCAM タイプでは PortAndVlan リージョンと PortOrVlan リージョンのエントリをシフトさせることができます(たとえば、入力 ACL TCAM PortOrVlan リージョンから入力 ACL TCAM PortAndVlan リージョンへ交換できます)。 TCAM タイプでは、エントリをシフトすることはできません。

リージョンのサイズ変更による効果があるかどうかを調べるには、show platform hardware acl statistics utilization brief コマンドを使用します。

Switch# show platform hardware acl statistics utilization brief

Input	Acl(PortAndVlan)	2346	/	8112	(29)	1014	/	1014	(1	00)
Input	Acl(PortOrVlan)	0	/	8112	(0)	0	/	1014	(0)
Input	Qos(PortOrVlan)	0	/	8128	(0)	0	/	1016	(0)
Input	Qos(PortOrVlan)	0	/	8128	(0)	0	/	1016	(0)
Output	Acl(PortOrVlan)	0	/	8112	(0)	0	/	1014	(0)
Output	Acl(PortOrVlan)	0	/	8112	(0)	0	/	1014	(0)
Output	Qos(PortOrVlan)	0	/	8128	(0)	0	/	1016	(0)
Output	Qos(PortOrVlan)	0	/	8128	(0)	0	/	1016	(0)

L4Ops: used 2 out of 64

上の出力は、入力 ACL PortAndVlan リージョンのマスクがなくなったものの入力 ACL PortOrVlan リージョンに空き容量があり、別の用途で利用できることを示しています。次に、PortAndVlan リージョンにエントリの 75% を割り当て、PortOrVlan リージョンに 25% を割り当てるように入力 ACL TCAM のリージョン バランスを変更する例を示します。

Switch# configure terminal

Switch(config)# access-list hardware region feature input balance 75

リージョン バランスの調整後は、PortAndVlan リージョンに割り当てられたリソースは増え、PortOrVlan リージョンのリソースは少なくなります。

Switch# show platform hardware acl statistics utilization brief

Acl(PortAndVlan)	2346 /	12160 (19)	1014 / 1520 (67	')
Acl(PortOrVlan)	0 /	4064 (0)	0 / 508 (0)	
Qos(PortOrVlan)	0 /	8128 (0)	0 / 1016 (0)	
Qos(PortOrVlan)	0 /	8128 (0)	0 / 1016 (0)	
Acl(PortOrVlan)	0 /	8112 (0)	0 / 1014 (0)	
Acl(PortOrVlan)	0 /	8112 (0)	0 / 1014 (0)	
Qos(PortOrVlan)	0 /	8128 (0)	0 / 1016 (0)	
Qos(PortOrVlan)	0 /	8128 (0)	0 / 1016 (0)	
	Acl(PortAndVlan) Acl(PortOrVlan) Qos(PortOrVlan) Qos(PortOrVlan) Acl(PortOrVlan) Acl(PortOrVlan) Qos(PortOrVlan) Qos(PortOrVlan) Qos(PortOrVlan)	Acl(PortOrVlan) 0 / Qos(PortOrVlan) 0 / Qos(PortOrVlan) 0 / Acl(PortOrVlan) 0 / Acl(PortOrVlan) 0 / Qos(PortOrVlan) 0 /	Acl(PortOrVlan) 0 / 4064 (Qos(PortOrVlan) 0 / 8128 (Qos(PortOrVlan) 0 / 8128 (Acl(PortOrVlan) 0 / 8112 (Acl(PortOrVlan) 0 / 8112 (Qos(PortOrVlan) 0 / 8128 (Acl(PortOrVlan) 0 / 4064 (0) Qos(PortOrVlan) 0 / 8128 (0) Qos(PortOrVlan) 0 / 8128 (0) Acl(PortOrVlan) 0 / 8112 (0) Acl(PortOrVlan) 0 / 8112 (0) Qos(PortOrVlan) 0 / 8128 (0)	Acl(PortOrVlan) 0 / 4064 (0) 0 / 508 (0) Qos(PortOrVlan) 0 / 8128 (0) 0 / 1016 (0) Qos(PortOrVlan) 0 / 8128 (0) 0 / 1016 (0) Acl(PortOrVlan) 0 / 8112 (0) 0 / 1014 (0) Acl(PortOrVlan) 0 / 8112 (0) 0 / 1014 (0) Qos(PortOrVlan) 0 / 8128 (0) 0 / 1016 (0)

L40ps: used 2 out of 64

Switch#



デフォルト値に戻すには、access-list hardware region {feature | qos} {input | output} balance コマンドの no 形式を使用するか、バランスを 50 にします。同様の設定は QoS についても実行できます。

ACL による高 CPU のトラブルシューティング

完全にプログラムされた ACL のエントリに一致するパケットは、ハードウェアで処理されます。ただし、大型 ACL および IPSG の設定は、ACL が完全にプログラムされる前に、Supervisor Engine II-Plus-TS、IV、V、および Catalyst 4948 スイッチの TCAM マスクを消費することがあります。

部分的にプログラムされた ACL のエントリに一致するパケットは、CPU を使用してソフトウェアで処理されます。これにより、高 CPU 利用率が高くなったりパケットがドロップされることがあります。パケットが高 CPU 利用率のためにドロップされているかどうかを判別するには、次の URL を参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps663/products_tech_note09186a00804cef15.shtml

ACL または IPSG 設定がハードウェアで部分的にプログラムされている場合、Cisco IOS Release 12.2(31)SGA 以上にアップグレードし、TCAM リージョンのサイズを変更すると、ACL の完全プログラムが可能になることがあります。



(注)

使用されていない TCAM エントリの削除を完了するには、何回かの CPU プロセス レビュー サイクルがかかります。これにより、TCAM エントリまたはマスク利用率が 100% に近い場合、一部のパケットがソフトウェアで切り替えられます。

制御パケットのキャプチャのモード選択



(注)

Supervisor Engine 6-E は、この機能をサポートして*いません*。

展開によっては、(CPU を犠牲にして)制御パケットをグローバルにキャプチャしてソフトウェアで転送するのではなく、ハードウェアでブリッジします。VLAN 単位のキャプチャ モード機能により、Catalyst 4500 シリーズ スイッチは、選択した VLAN でのみ制御パケットをキャプチャし、他のすべての VLAN についてはハードウェアでトラフィックをブリッジできます。

スイッチで VLAN 単位キャプチャ モードを採用すると、内部でグローバル TCAM キャプチャ エントリを部分的にディセーブルにし、スヌーピング機能またはルーティング機能のためにイネーブルになっている VLAN 上の機能固有キャプチャ ACL を付加します (すべての IP キャプチャ エントリ、CGMP、および他の IP 以外のエントリは、引き続きグローバル TCAM を介してキャプチャされます)。この機能は、特定の制御パケットを制御するので、内部 ACL がインストールされた VLANでのみキャプチャされます。他のすべての VLAN では、制御トラフィックは CPU に転送されるのではなく、ハードウェアでブリッジされます。

VLAN 単位のキャプチャ モードにより、制御パケットにユーザ定義 ACL および QoS ポリサー(ハードウェア内) を適用できます。 さらに、CPU に入力する集約制御トラフィックをコントロール プレーン ポリシングの対象にできます。

VLAN 単位キャプチャ モードを使用するとき、次の 4 つのプロトコル グループを VLAN 単位で選択できます。各グループで代行受信されたプロトコルの詳細を参考にしてください。

- IGMP スヌーピング CGMP、OSPF、IGMP、PIM、224.0.0.1、224.0.0.2、224.0.0.*
- DHCP スヌーピング クライアントからサーバへ、サーバからクライアントへ、サーバから サーバへ
- ユニキャストルーティング OSPF、RIP v2、224.0.0.1、224.0.0.2、224.0.0.*
- マルチキャストルーティング OSPF、RIP v2、IGMP、PIM、224.0.0.1、224.0.0.2、224.0.0.*

グループの一部には複数の重複 ACE があるため (たとえば、224.0.0.* は、DHCP スヌーピング以外のすべてのグループに存在します)、特定のグループをオンにすると、他のグループからの一部のプロトコルの代行受信もトリガーされます。

VLAN 単位の 4 つのプロトコル グループのプログラミング トリガーは、次のとおりです。

- IGMP スヌーピングは、指定 VLAN でグローバルにイネーブルにする必要があります。
- DHCP スヌーピングは、指定 VLAN でグローバルにイネーブルにする必要があります。
- ユニキャスト ルーティングはイネーブルに、SVI(またはレイヤ3物理)インターフェイスはアップになり、IPプロトコル アドレスで設定されている必要があります。これは、SVIインターフェイスがアップになり、プロトコルファミリアドレスが設定されると、インターフェイスはすぐにルーティングプロセスの一部になるためです。

• マルチキャスト ルーティングはイネーブルにされ、マルチキャスト ルーティング プロトコルの 1 つがインターフェイスで設定されている必要があります (IGMP、PIMv1、PIMv2、MBGP、MOSPF、DVMRP、および IGMP スヌーピング)。

注意事項および制限事項



(注)

VLAN 単位キャプチャ モードを設定する前に設定を調べ、目的の VLAN で必要な機能だけがイネーブルになっていることを確認する必要があります。

VLAN 単位キャプチャ モードには、次の注意事項および制限事項が適用されます。

• VLAN 単位キャプチャ モードをイネーブルにすると、ACL/ 機能 TCAM のエントリがさらに消費されます。

使用可能な TCAM エントリ数は、スーパーバイザ エンジンの種類によって変わります。エントリ/マスク数により、ACL/機能 TCAM の利用率はさらに制限されます。

• ある種の設定では、グローバル キャプチャ モードよりも早く VLAN 単位キャプチャ モードで TCAM リソースを消費することがあります (IP ソース ガードがいくつかのインターフェイス 上、またはユーザ設定 PACL 上でイネーブルにされるなど)。

TCAM リージョンのサイズを変更し、設定に基づいて PortAndVlan または PortOrVlan リージョンに対してより多くのエントリを使用可能にできます。これにより、制限に達する前により多くのエントリをハードウェア内でプログラムできるようになります。TCAM リソースが消費されてしまうと、パケットはソフトウェア内で転送されます。

• VLAN 単位キャプチャ モードでは、ACL が VLAN またはポート上で制御トラフィックを許可または拒否するように設定できます。

セキュリティ ACL は*暗黙の拒否*で終了されるため、機能(プロトコル)が動作するために必要な制御パケットを許可するように ACL が設定されていることを確認する必要があります。ただし、この規則はデフォルトの動作と同じです。

設定

制御パケットのキャプチャ モードを選択するには、次の作業を実行します。

	コマンド	目的
ステップ 1	Switch# conf terminal	コンフィギュレーション モードを開始します。
ステップ 2	<pre>Switch(config)# [no] access-list hardware capture mode [vlan global]</pre>	制御パケットのキャプチャ モードを選択します。
		access-list hardware capture mode コマンドの no 形式
		は、キャプチャ モードをデフォルトのグローバルに戻しま
		す。
ステップ 3	Switch(config)# end	イネーブル モードに戻ります。

次に、Catalyst 4500 シリーズ スイッチが、機能がイネーブルになっている VLAN でのみ制御パケットをキャプチャするように設定する例を示します。

Switch# configure terminal

Enter configuration commands, one per line. End with \mathtt{CNTL}/\mathtt{Z} .

Switch(config)# access-list hardware capture mode vlan

Switch(config)# end

Switch#

次に、Catalyst 4500 シリーズ スイッチが、すべての VLAN で(デフォルト モードのスタティック ACL を使用して)制御パケットをグローバルにキャプチャするように設定する例を示します。

Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config) # access-list hardware capture mode global
Switch(config) # end
Switch#

キャプチャ モードがグローバルからパス管理に変更されると、スタティック CAM エントリは無効になります。これにより、制御パケットが代行受信されずに Catalyst 4500 シリーズ スイッチを通過して CPU に達するウィンドウ (時間)が儲けられます。この一時的な状況は、新しい VLAN 単位のキャプチャ エントリがハードウェアでプログラムされ次第復元されます。

VLAN キャプチャ モードを設定したら、個々の機能の show コマンドを調べ、適切な動作になっていることを確認する必要があります。VLAN 単位キャプチャ モードでは、無効になった CAM エントリは、show platform hardware acl entries static all コマンドの出力で非アクティブ (inactive) として表示されます。たとえば、非アクティブ エントリのヒット数は、無効になって機能がイネーブルになっている VLAN ごとに適用されているので、凍結されたままになります。

Camindex エントリの種類	アクティブ	ヒット数	CamRegion
50 PermitSharedStp	Y	3344	ControlPktsTwo
51 PermitLoopbackTest	Y	0	ControlPktsTwo
52 PermitProtTunnel	Y	0	ControlPktsTwo
53 CaptureCgmp	N	440	ControlPktsTwo
54 CaptureOspf	N	4321	ControlPktsTwo
55 CaptureIgmp	N	0	ControlPktsTwo

Supervisor Engine 6-E の TCAM プログラミングと ACL

Supervisor Engine 6-E の ACL および ACL ベースの機能をプログラムするときは、Mapping Table Entry (MTE)、プロファイル、TCAM 値 / マスク エントリの 3 種類のハードウェア リソースを適用します。これらのリソースのいずれかが消費されてしまうと、ソフトウェア ベースの処理のために、パケットが CPU に送信されます。



Supervisor Engine II-Plus から V-10GE までとは異なり、Supervisor Engine 6-E は、使用可能リソース を自動的に管理します。Supervisor Engine 6-E ではマスクが共有されないため、プログラミング アルゴリズムは 1 つだけです。リージョンが存在しないので、リージョンのサイズ変更は必要ありません。VLAN 単位パケット キャプチャ モードは違うように実装されるので、ディセーブルにはできません。

Supervisor Engine 6-E でリソースが消費されてしまった場合、設定の複雑さを軽減する必要があります。

ACL のレイヤ4演算

ここでは、レイヤ 4 ポート演算を含む ACL を設定する場合の注意事項および制約事項について説明します。

- レイヤ4演算の制約事項(p.42-16)
- レイヤ 4 演算設定時の注意事項 (p.42-17)
- ACL 処理が CPU に与える影響 (p.42-18)

レイヤ4演算の制約事項

次のタイプの演算子を指定できます。いずれも、ハードウェアのレイヤ4演算が1つ使用されます。

- gt (geater than:より大きい)
- It (less than:より小さい)
- neq (not equal: 等しくない)
- range (inclusive range:包含範囲)

Supervisor Engine 2-Plus から V-10GE までの場合、同じ ACL で異なる演算を 7 つ以上指定しないでください。この数を超えると、超過した各演算の影響を受ける ACE が、ハードウェアで複数の ACE に変換されることがあります。また、影響を受ける ACE がソフトウェアで処理される可能性があります。

Supervisor Engine 6-E では、レイヤ 4 演算数の制限は、それぞれの ACL の種類によって異なり、他の要素によっても変わることがあります。変更する要素としては、ACL が着信または発信トラフィックに適用されているかどうか、ACL がセキュリティ ACL かまたは QoS ポリシーの一致条件として使用されているかどうか、IPv6 ACL が圧縮フローラベル形式を使用してプログラムされているかどうか、などがあります。



IPv6 圧縮フローラベル形式では、レイヤ 2 アドレス テーブルを使用して、ACL にある各 ACE の IPv6 送信元アドレスの一部を圧縮します。フローラベルで解放された余分なスペースは、さらに多くのレイヤ 4 演算をサポートするために使用可能です。この圧縮を使用するには、IPv6 ACL に、送信元 IPv6 アドレスの下位の 48 ビットの部分でのみマスクする ACE を含めることはできません。

一般的に、同じ ACL に含めることができるレイヤ 4 演算の最大数は次のようになります。

Direction	Prot	ocol	Туре	Operations
Input	IPv4		Security	16
Input	IPv6	Compressed	Security	16
Input	IPv6	Uncompressed	Security	7
Input	IPv4		QoS	5
Input	IPv6	Compressed	QoS	12
Input	IPv6	Uncompressed	QoS	8
Output	IPv4		Security	17
Output	IPv6	Compressed	Security	17
Output	IPv6	Uncompressed	Security	8
Output	IPv4		QoS	5
Output	IPv6	Compressed	QoS	12
Output	IPv6	Uncompressed	QoS	8



16の演算がサポートされる場合、17番めの演算によって、拡張がトリガーされます。

使用可能なレイヤ4演算数を超えた場合、超過した各演算により、影響を受ける ACE がハードウェアで複数 ACE に変換されることがあります。このような変換ミスにより、パケットはソフトウェアの処理のために、CPU に送信されます。

レイヤ4演算設定時の注意事項

レイヤ4演算子を使用するときは、次の注意事項に従ってください。

- レイヤ4演算は、演算子またはオペランドが異なっていると、異なる演算であるとみなされます。たとえば、次の ACL には3つの異なるレイヤ4演算が定義されています。gt 10 と gt 11 は2つの異なるレイヤ4演算とみなされるためです。
 - ... gt 10 permit ... lt 9 deny ... gt 11 deny



____ (注)

eq 演算子は、ハードウェアのレイヤ 4 演算を使用しないので、何回でも無制限に使用できます。

- 次の例のように、レイヤ 4 演算は、同じ演算子またはオペランドの組み合わせでも、送信元ポートに適用するか宛先ポートに適用するかによって異なる演算になります。
 - ... Src gt 10.... ... Dst gt 10

以下は、より詳細な例です。

```
access-list 101
... (dst port) gt 10 permit
... (dst port) lt 9 deny
... (dst port) gt 11 deny
... (dst port) neq 6 permit
... (src port) neq 6 deny
... (dst port) gt 10 deny
access-list 102
... (dst port) gt 20 deny
... (src port) lt 9 deny
... (src port) range 11 13 deny
... (dst port) neq 6 permit
```

アクセス リスト 101 および 102 で使用しているレイヤ 4 演算は、次のとおりです。

- アクセス リスト 101 のレイヤ 4 演算:5
 - gt 10 permit および gt 10 deny は、どちらも同じ演算です。まったく同じで、どちらも宛先ポートに適用されます。
- アクセス リスト 102 のレイヤ 4 演算:4
- レイヤ4演算の合計:8(2つのアクセスリスト間で共用されるため)
 - neq6 permit は 2 つの ACL 間で共用されます。まったく同じで、どちらも同じ宛先ポートに 適用されます。
- 使用しているレイヤ4演算について説明します。
 - レイヤ4演算1は、ACL101からgt 10 permit およびgt 10 deny を格納します。
 - レイヤ4演算2は、ACL101からlt9denyを格納します。
 - レイヤ4演算3は、ACL101からgt11denyを格納します。
 - レイヤ 4 演算 4 は、ACL101 および 102 から neq 6 permit を格納します。
 - レイヤ4演算5は、ACL101から neq6denyを格納します。
 - レイヤ4演算6は、ACL1021からgt20denyを格納します。
 - レイヤ4演算7は、ACL102からlt9denyを格納します。
 - レイヤ4演算8は、ACL102から range 11 13 deny を格納します。

ACL 処理が CPU に与える影響

ACL 処理は、次の2つの形でCPUに影響を与える可能性があります。

- 一部のパケットで、ハードウェア リソースを使い果たした場合、ACL との照合をソフトウェアで実行する必要があります。
 - 「rst ack」と「syn fin rst」、「urq」、および「psh」以外の TCP フラグの組み合わせは、ハードウェアで処理されます。*rst ack* はキーワード **established** に相当します。他の TCP フラグの組み合わせは、ソフトウェアでサポートされます。
 - Supervisor Engine 2-Plus から V-10GE の場合、すべての演算をハードウェアで処理するには、ACL に指定するレイヤ 4 演算(lt、gt、neq、および range)を6つまでにする必要があります。7以上のレイヤ 4 演算では、超過分の演算についてハードウェアで複数の ACE に変換しようとします。ハードウェアで変換できなかった場合、パケットはソフトウェアで処理されます。変換プロセスは、大量のレイヤ 4 演算のある大規模 ACL や、大量の ACL が設定されたスイッチで成功の可能性が低くなります。正確な限度は、その他に設定されている ACL の数や変換対象の ACL が使用する特定のレイヤ 4 演算によって異なります。eq 演算子は、レイヤ 4 演算を必要としないので、何回でも使用できます。
 - Supervisor Engine 6-E については、「レイヤ4演算の制約事項」(p.42-16)を参照してください。

- ACL 内のレイヤ4演算の合計数が6に満たない場合、任意の形で処理を分散させることができます。

次に例を示します。

次のアクセス リストは、すべてハードウェアで処理されます。

```
access-list 104 permit tcp any any established access-list 105 permit tcp any any rst ack access-list 107 permit tcp any synfin rst
```

アクセス リスト 104 および 105 は同じです。established は rst および ack の省略形です。

次のアクセス リスト 101 は、すべてソフトウェアで処理されます。

```
access-list 101 permit tcp any any syn
```

次のアクセス リスト 106 は、送信元演算が 4、宛先演算が 2 なので、ハードウェアで処理されます。

```
access-list 106 permit tcp any range 100 120 any range 120 140 access-list 106 permit tcp any range 140 160 any range 180 200 access-list 106 permit tcp any range 200 220 access-list 106 deny tcp any range 220 240
```

次のコードの場合、送信元演算と宛先演算が 3 つずつあるので、3 番めの ACE に対するレイヤ 4 演算は dst lt 1023 をハードウェアで複数の ACE に変換しようとします。変換できなかった場合、3 番めの ACE はソフトウェアで処理されます。

```
access-list 102 permit tcp any lt 80 any gt 100 access-list 102 permit tcp any range 100 120 any range 120 1024 access-list 102 permit tcp any gt 1024 any lt 1023
```

次のアクセス リスト 103 の場合も同様に、3 番めの ACE は dst gt 1023 をハードウェアで複数の ACE に変換しようとします。変換できなかった場合、3 番めの ACE はソフトウェアで処理されます。送信元ポートおよび宛先ポートの演算は同じように見えますが、異なるレイヤ 4 演算とみなされます。

```
access-list 103 permit tcp any lt 80 any lt 80 access-list 103 permit tcp any range 100 120 any range 100 120 access-list 103 permit tcp any gt 1024 any gt 1023 \,
```



source port lt 80 と destination port lt 80 は、異なる演算とみなされるので注意してください。

- 一部のパケットはアカウンティング目的で CPU に送信する必要がありますが、アクションはそのままハードウェアで実行されます。たとえば、パケットのログが必要な場合、ログ収集のためにコピーが CPU に送信されますが、転送(またはドロップ)はハードウェアで実行されます。ロギングによって CPU の処理速度が低下しますが、転送速度は影響を受けません。この状況が発生するのは、次のような場合です。
 - log キーワードが使用されている場合
 - 出力 ACL でパケットが拒否された場合
 - 入力 ACL でパケットが拒否され、ACL が適用されたインターフェイス上で ip unreachable がイネーブルの場合 (ip unreachable は、すべてのインターフェイスにおいてデフォルトでイネーブル)

ユニキャスト MAC アドレス フィルタリングの設定

特定の VLAN にある MAC アドレスのユニキャスト トラフィックをすべてブロックするには、次の作業を行います。

コマンド	目的
Switch(config)# mac-address-table static mac_address vlan vlan_ID drop	特定の VLAN にある MAC アドレスのユニキャスト トラフィックをすべてブロックします。
	MAC アドレスベースのブロッキングをクリアするには、このコマンドの no 形式を drop キーワードなしで使用します。

次に、VLAN~12~にある MAC アドレス 0050.3e8d.6400~のユニキャスト トラフィックをすべてブロックする例を示します。

Router# configure terminal

Router(config) # mac-address-table static 0050.3e8d.6400 vlan 12 drop

名前付き MAC 拡張 ACL の設定



ここでの説明は、Supervisor Engine II-Plus から 6-E までに該当します。

VLAN および物理レイヤ 2 インターフェイスで IP 以外のトラフィックをフィルタリングするには、MAC アドレスおよび名前付き MAC 拡張 ACL を使用します。手順については、他の名前付き拡張 ACL の場合と同様です。アクセス リストの名前として番号を使用することもできますが、700~~799~の MAC アクセス リスト番号はサポートされません。



名前付き MAC 拡張 ACL は、レイヤ 3 インターフェイスに適用できません。

mac access-list extended コマンドでサポートされている IP 以外のプロトコルの詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』を参照してください。

名前付きの MAC 拡張 ACL を作成するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# mac access-list extended name	名前を使用して MAC 拡張アクセス リストを定義します。

	コマンド	目的
ステップ 3	Switch(config-ext-macl)# {deny permit} {any host source MAC address source MAC address mask} {any host destination MAC address destination MAC address mask} [protocol-family {appletalk arp-non-ipv4 decnet ipx ipv6 rarp-ipv4 rarp-non-ipv4 vines xns}]	拡張 MAC アクセス リスト コンフィギュレーション モードでは、あらゆる (any) 送信元 MAC アドレス、マスク付きの送信元 MAC アドレス、または特定の (host) 送信元 MAC アドレス、およびあらゆる (any) 宛先 MAC アドレス、マスク付き宛先 MAC アドレス、または特定の宛先 MAC アドレスに、permit または deny を指定します。
		(任意)
		• [protocol-family {appletalk arp-non-ipv4 decnet ipx ipv6 rarp-ipv4 rarp-non-ipv4 vines xns }]
		(注) Supervisor Engine 6-E では、IPv6 パケットはレイヤ 2 ACL 検索キーを生成 しないため、Supervisor Engine II-Plus から V-10GE の MAC ACL に対して IPv4 パケットが一致しないのと同様に、MAC ACL で一致しません。したがって、ipv6 キーワードは Supervisor Engine II-Plus から V-10GE の MAC ACL では使用可能ですが、Supervisor Engine 6-E では使 用できません。
ステップ 4	Switch(config-ext-macl)# end	特権 EXEC モードに戻ります。
ステップ 5	Switch# show access-lists [number name]	アクセスリストの設定を表示します。
ステップ 6	<pre>Switch(config) # copy running-config startup-config</pre>	(任意)コンフィギュレーション ファイルに設定を保存します。

ACL 全体を削除するには、**no mac access-list extended** *name* グローバル コンフィギュレーション コマンドを使用します。名前付き MAC 拡張 ACL から ACE を個別に削除することもできます。

次に、DECnet Phase IV という EtherType のトラフィックのみを拒否し、その他のすべてのタイプのトラフィックを許可する、mac1 という名前のアクセス リストを作成、表示する例を示します。

```
Switch(config) # mac access-list extended mac1
Switch(config-ext-macl) # deny any any decnet-iv (old) protocol-family decnet (new)
Switch(config-ext-macl) # permit any any
Switch(config-ext-macl) # end
Switch # show access-lists
Extended MAC access list macl
    deny any any decnet-iv (old) protocol-family decnet (new)
    permit any any
```

ハードウェア統計をイネーブルまたはディセーブルにするには、アクセス リストの ACE を設定する際に次のコマンドを入力します。

```
Switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# mac access-list extended mac1
Switch(config-ext-nacl)# hardware statistics
Switch(config-ext-nacl)# end
```

名前付き IPv6 ACL の設定



注) ここでの説明は、Supervisor Engine 6-E に該当します。

Supervisor Engine 6-E は、ハードウェア ベースの IPv6 ACL をサポートし、レイヤ 3 インターフェイス上のユニキャスト、マルチキャスト、およびブロードキャスト IPv6 トラフィックをフィルタリングします。こういったアクセス リストは、IPv6 アドレスが設定されたレイヤ 3 インターフェイスでのみ設定できます。

名前付き IPv6 ACL を作成するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# ipv6 access-list name	名前を使用して IPv6 アクセス リストを定義します。
ステップ 3	Switch(config-ipv6-acl)# {deny permit} {any proto} {host ipv6-addr ipv6-prefix} host ipv6-addr ipv6-prefix}	各 IPv6 ACE を指定します。 (注) このステップは、ACL の複数 ACE を定義するときに繰り返すことがあります。
ステップ 4	<pre>Switch(config-ipv6-acl)# hardware statistics</pre>	(任意) IPv6 ACL のハードウェア統計をイネーブルにします。
ステップ 5	Switch(config-ipv6-acl)# end	特権 EXEC モードに戻ります。
ステップ 6	Switch# show ipv6 access-list	IPv6 アクセス リストの設定を表示します。

IPv6 ACL を削除するには、**no ipv6 access-list name** グローバル コンフィギュレーション コマンドを使用します。また、IPv6 アクセス リストから個々の ACE を削除することもできます。

次に、1 つの特定送信元 / 宛先アドレスを持つ 1 つの IPv6 トラフィックのみを拒否するが、他のすべての種類の IPv6 トラフィックは許可する *v6test* という名前の IPv6 アクセス リストを作成および表示する例を示します。

```
Switch(config)# ipv6 access-list v6test
Switch(config-ipv6-acl)# deny ipv6 host 2020::10 host 2040::10
Switch(config-ipv6-acl)# permit any any
Switch(config-ipv6-acl)# end
Switch# show ipv6 access-list
IPv6 access list v6test
   deny ipv6 host 2020::10 host 2040::10 sequence 10
   permit ipv6 any any sequence 20
```

ハードウェア統計をイネーブルにするには、アクセス リスト ACE を設定するときに、次のコマンドを入力します。

```
Switch(config)# ipv6 access-list v6test
Switch(config-ipv6-acl)# hardware statistics
Switch(config-ipv6-acl)# end
```



*ハードウェア統計*は、デフォルトではディセーブルです。

レイヤ 3 インターフェイスへの IPv6 ACL の適用

IPv6 ACL をレイヤ 3 インターフェイスに適用するには、次の作業を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# interface interface-type slot/interface	設定するインターフェイスを指定します。
		(注) interface-type は、レイヤ 3 インターフェイスである 必要があります。
ステップ 3	Switch(config-if)# ipv6 traffic-filter ipv6-acl {in out}	IPv6 ACL をレイヤ 3 インターフェイスに適用します。





IPv6 ACL は、Supervisor VI-E のハードウェアでのみサポートされます。



IPv6 ACL は、レイヤ 3 インターフェイスでのみサポートされます。

次の例は、拡張名前付き IPv6 ACL simple-ipv6-acl を SVI 300 ルーテッド入力トラフィックに適用します。

Switch# configure terminal
Switch(config)# interface vlan 300
Switch(config-if)# ipv6 traffic-filter simple-ipv6-acl in

VLAN マップの設定

ここでは、次の内容について説明します。

- VLAN マップ設定時の注意事項 (p.42-25)
- VLAN マップの作成および削除 (p.42-25)
- VLAN への VLAN マップの適用 (p.42-28)
- ネットワークでの VLAN マップの使用方法 (p.42-28)

ここでは、VLAN マップを設定する方法について説明します。この方法は、VLAN 内でフィルタリングを制御する唯一の方法です。VLAN マップには方向がありません。VLAN マップを使用して、特定の方向のトラフィックをフィルタリングするには、特定の送信元または宛先アドレスが指定された ACL を追加する必要があります。VLAN マップ内に該当タイプのパケット(IP または MAC)に対する match コマンドがある場合、デフォルトでは、マップ内のどのエントリにも一致しないパケットはドロップされます。該当タイプのパケットに対する match コマンドがない場合、デフォルトでは、パケットが転送されます。

VLAN マップを作成して、1 つまたは複数の VLAN に適用するには、次の作業を行います。

- ステップ1 VLAN に適用する標準 IP ACL または拡張 IP ACL、または名前付き MAC 拡張 ACL を作成します。
- ステップ2 VLAN ACL マップ エントリを作成するには、vlan access-map グローバル コンフィギュレーションコマンドを入力します。
- ステップ3 アクセス マップ コンフィギュレーション モードでは、action として、forward (デフォルト)または drop を任意で入力できます。また、match コマンドを入力して、既知の MAC アドレスのみが格納された IP パケットまたは IP 以外のパケットを指定したり、1 つまたは複数の ACL (標準または拡張)とパケットを照合することもできます。match コマンドが指定されていない場合は、すべてのパケットにアクションが適用されます。match コマンドを使用すると、パケットを複数の ACL と照合できます。指定された ACL のいずれかにパケットが一致すると、アクションが適用されます。



(注)

該当タイプのパケット (IP または MAC) に対する match コマンドが VLAN マップにある場合でも、パケットがそのタイプに一致しない場合、デフォルトでは、パケットがドロップされます。該当タイプのパケットに対する match コマンドが VLAN マップ内になく、それに対するアクションが指定されていない場合、パケットは転送されます。

ステップ4 VLAN マップを 1 つまたは複数の VLAN に適用するには、vlan filter グローバル コンフィギュレーション コマンドを使用します。



<u>~</u>

レイヤ 2 インターフェイスに ACL (PACL) が適用されているスイッチ上の VLAN には、VLAN マップを適用できません。

VLAN マップ設定時の注意事項

VLAN マップを設定する際は、次の注意事項に従ってください。

- VLAN マップは IPv4 Address Resolution Protocol (ARP; アドレス解決プロトコル) パケットをフィルタリングしません。
- ルーテッド VLAN インターフェイス (入力または出力) でトラフィックを拒否するように設定 されたルータ ACL が存在せず、VLAN マップが設定されていない場合は、すべてのトラフィックが許可されます。
- 各 VLAN マップは一連のエントリで構成されます。VLAN マップのエントリの順序は重要です。スイッチに着信したパケットは、VLAN マップの最初のエントリに対してテストされます。一致した場合は、VLAN マップで指定されたアクションが実行されます。一致しなかった場合、パケットはマップ内の次のエントリに対してテストされます。
- 該当タイプのパケット (IP または MAC) に対する match コマンドが VLAN マップに 1 つまた は複数ある場合でも、パケットがそれらの match コマンドに一致しないと、デフォルトでは、パケットがドロップされます。該当タイプのパケットに対する match コマンドが VLAN マップ 内にない場合、デフォルトでは、パケットが転送されます。
- 多数の ACL が設定されている場合は、システムの起動に時間がかかることがあります。

VLAN マップの作成および削除

各 VLAN マップは順番に並べられた一連のエントリで構成されます。 VLAN マップ エントリを作成、追加、または削除するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# vlan access-map name [number]	VLAN マップを作成し、名前と、任意で番号を付けます。 番号は、マップ内のエントリの順序を表す数字です。
		同じ名前の VLAN マップを作成すると、10 ずつ増分する番号が順に割り当てられます。マップを変更または削除するときは、目的のマップ エントリの番号を入力します。
		このコマンドを入力すると、アクセスマップ コンフィギュ レーション モードに変わります。
ステップ 3	<pre>Switch(config-access-map)# action {drop forward}</pre>	(任意)マップエントリに対するアクションを設定します。 デフォルトは転送です。
ステップ 4	Switch(config-access-map) # match {ip mac} address {name number} [name number]	1 つまたは複数の標準または拡張アクセス リストに対してパケットを比較します (IP または MAC アドレスを使用)。パケットの比較は、対応するプロトコル タイプのアクセスリストに対してのみ行われます。IP パケットは、標準または拡張 IP アクセス リストに対して比較されます。IP 以外のパケットは、名前付き MAC 拡張アクセス リストに対してのみ比較されます。match コマンドが指定されていない場合は、すべてのパケットにアクションが実行されます。
ステップ 5	Switch(config-access-map)# end	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	Switch(config)# show running-config	アクセス リストの設定を表示します。
ステップ 7	Switch(config)# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

マップを削除するには、no vlan access-map name グローバル コンフィギュレーション コマンドを使用します。マップ内の単一のシーケンス エントリを削除するには、no vlan access-map name number グローバル コンフィギュレーション コマンドを使用します。デフォルトのアクションである転送を行うには、no action アクセスマップ コンフィギュレーション コマンドを使用します。

VLAN マップでは、特定の permit または deny キーワードは使用されません。VLAN マップを使用してパケットを拒否するには、パケットと比較する ACL を作成して、アクションをドロップに設定します。ACL に permit を指定すると、一致とみなされます。ACL に deny を指定すると、一致しないという意味になります。

ACL および VLAN マップの例

特定の目的のための ACL および VLAN マップを作成する例を示します。

例 1

ここでは、パケットを拒否する ACL および VLAN マップを作成する例を示します。最初のマップでは、ip1 ACL (TCP パケット) に一致するすべてのパケットがドロップされます。最初に、すべての TCP パケットを許可し、それ以外のパケットをすべて拒否する ip1 ACL を作成します。VLANマップには IP パケットに対する match コマンドが存在するので、デフォルトでは、どの match コマンドとも一致しないすべての IP パケットがドロップされます。

```
Switch(config)# ip access-list extended ip1
Switch(config-ext-nacl)# permit tcp any any
Switch(config-ext-nacl)# exit

Switch(config)# vlan access-map map_1 10
Switch(config-access-map)# match ip address ip1
Switch(config-access-map)# action drop
```

次に、パケットを許可する VLAN マップを作成する例を示します。ACL~ip2~dL~UDP~ll. がいます。ip2~ACL~e一致するすべてのパケットが転送されます。

```
Switch(config) # ip access-list extended ip2
Switch(config-ext-nacl) # permit udp any any
Switch(config-ext-nacl) # exit
Switch(config) # vlan access-map map_1 20
Switch(config-access-map) # match ip address ip2
Switch(config-access-map) # action forward
```

このマップでは、これ以前のどの ACL とも一致しないすべての IP パケット (TCP でも UDP でもないパケット) がドロップされます。

例 2

次の例の VLAN マップでは、デフォルトで IP パケットがドロップされ、MAC パケットが転送されるように設定されています。 標準の ACL 101、名前付き拡張アクセス リスト igmp-match および tcp-match を適用して、次のように VLAN マップを設定します。

- すべての UDP パケットが転送されます。
- すべての IGMP パケットがドロップされます。
- すべての TCP パケットが転送されます。
- その他のすべての IP パケットがドロップされます。
- すべての非 IP パケットが転送されます。

```
Switch(config) # access-list 101 permit udp anv anv
Switch(config) # ip access-list extended igmp-match
Switch(config-ext-nacl)# permit igmp any any
Switch(config)# ip access-list extended tcp-match
Switch(config-ext-nacl)# permit tcp any any
Switch(config-ext-nacl)# exit
Switch(config) # vlan access-map drop-ip-default 10
Switch(config-access-map) # match ip address 101
Switch(config-access-map) # action forward
Switch(config-access-map)# exit
Switch(config) # vlan access-map drop-ip-default 20
Switch(config-access-map) # match ip address igmp-match
Switch(config-access-map) # action drop
Switch(config-access-map)# exit
Switch(config) # vlan access-map drop-ip-default 30
Switch(config-access-map)# match ip address tcp-match
Switch(config-access-map)# action forward
```

例3

次の例の VLAN マップでは、デフォルトで MAC パケットがドロップされ、IP パケットが転送されるように設定されています。 MAC 拡張アクセス リスト good-hosts および good-protocols を適用して、次のように VLAN マップを設定します。

- ホスト 0000.0c00.0111 および 0000.0c00.0211 からの MAC パケットが転送されます。
- DECnet または Virtual Integrated Network Service (VINES)プロトコルファミリの MAC パケットが転送されます。
- その他のすべての IP 以外のパケットがドロップされます。
- すべての IP パケットが転送されます。

```
Switch(config) # mac access-list extended good-hosts
Switch(config-ext-macl) # permit host 000.0c00.0111 any
Switch(config-ext-macl) # permit host 000.0c00.0211 any
Switch(config-ext-nacl) # exit
Switch(config) # mac access-list extended good-protocols
Switch(config-ext-macl) # permit any any protocol-family decnet
Switch(config-ext-macl) # permit any any protocol-family vines
Switch(config-ext-nacl) # exit
Switch(config) # vlan access-map drop-mac-default 10
Switch(config-access-map) # match mac address good-hosts
Switch(config-access-map) # exit
Switch(config-access-map) # exit
Switch(config-access-map) # match mac address good-protocols
Switch(config-access-map) # match mac address good-protocols
Switch(config-access-map) # match mac address good-protocols
Switch(config-access-map) # action forward
```

例 4

次の例の VLAN マップでは、すべてのパケット (IP および IP 以外) がドロップされるように設定されています。アクセス リスト tcp-match および good-hosts を適用して、次のように VLAN マップを設定します。

- すべての TCP パケットが転送されます。
- ホスト 0000.0c00.0111 および 0000.0c00.0211 からの MAC パケットが転送されます。
- その他のすべての IP パケットがドロップされます。
- その他のすべての MAC パケットがドロップされます。

```
Switch(config) # vlan access-map drop-all-default 10
Switch(config-access-map) # match ip address tcp-match
Switch(config-access-map) # action forward
Switch(config-access-map) # exit
Switch(config) # vlan access-map drop-all-default 20
Switch(config-access-map) # match mac address good-hosts
Switch(config-access-map) # action forward
```

VLAN への VLAN マップの適用

1つの VLAN マップを1つまたは複数の VLAN に適用するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# vlan filter mapname vlan-list list	VLAN マップを 1 つまたは複数の VLAN に適用します。
		list には単一の VLAN ID (22)、連続した範囲(10 ~ 22)、
		または VLAN ID から構成されるストリング (12、22、30)
		を指定できます。カンマやハイフンの前後にスペースを挿
		入することもできます。
ステップ 3	Switch(config)# show running-config	アクセスリストの設定を表示します。
ステップ 4	<pre>cSwitch(config) # copy running-config startup-config</pre>	(任意)コンフィギュレーション ファイルに設定を保存します。



レイヤ 2 インターフェイスに ACL (PACL) が適用されているスイッチ上の VLAN には、VLAN マップを適用できません。

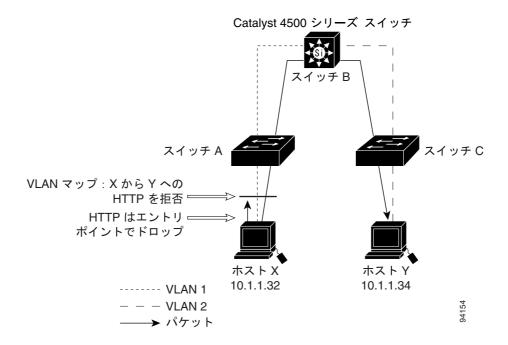
次に、VLAN マップ 1 を VLAN 20 ~ 22 に適用する例を示します。

Switch(config) # vlan filter map 1 vlan-list 20-22

ネットワークでの VLAN マップの使用方法

図 42-3 に、一般的なワイヤリングクローゼットの構成を示します。ホスト X およびホスト Y は異なる VLAN 内にあり、ワイヤリング クローゼット スイッチ A およびスイッチ C に接続されています。ホスト X からホスト Y へのトラフィックは、スイッチ B によってルーティングされます。ホスト X からホスト Y へのトラフィックは、トラフィックのエントリ ポイントであるスイッチ A でアクセス コントロールできます。次の構成では、スイッチは VLAN マップと QoS 分類 ACL をサポートします。

図 42-3 ワイヤリング クローゼットの構成



たとえば、HTTP トラフィックをホスト X からホスト Y へスイッチングしない場合は、スイッチ A に VLAN マップを適用し、ホスト X (IP アドレス 10.1.1.32) からホスト Y (IP アドレス 10.1.1.34) への HTTP トラフィックがスイッチ B にブリッジングされずに、すべてスイッチ A でドロップされるようにすることもできます。

最初に、HTTP ポートですべての TCP トラフィックを許可(一致)する IP アクセス リスト http を定義します。

```
Switch(config)# ip access-list extended http
Switch(config-ext-nacl)# permit tcp host 10.1.1.32 host 10.1.1.34 eq www
Switch(config-ext-nacl)# exit
```

次に、VLAN アクセス マップ map2 を作成し、http アクセス リストと一致するトラフィックがドロップされ、その他すべての IP トラフィックが転送されるようにします。

```
Switch(config)# vlan access-map map2 10
Switch(config-access-map)# match ip address http
Switch(config-access-map)# action drop
Switch(config-access-map)# exit

Switch(config)# ip access-list extended match_all
Switch(config-ext-nacl)# permit ip any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map map2 20
Switch(config-access-map)# match ip address match_all
Switch(config-access-map)# action forward
```

次に、VLAN アクセス マップ map2 を VLAN 1 に適用します。

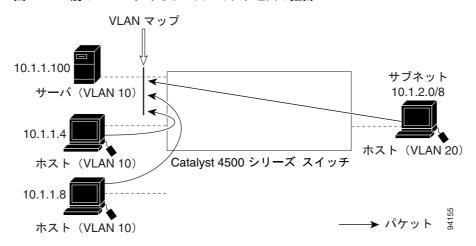
Switch(config) # vlan filter map2 vlan 1

別の VLAN にあるサーバへのアクセスの拒否

図 42-4 に、別の VLAN にあるサーバへのアクセスを制限する方法を示します。この例では、VLAN 10 内のサーバ 10.1.1.100 に対しては、次のようにアクセスが制限されています。

- VLAN 20 内のサブネット 10.1.2.0/8 にあるホストのアクセスが禁止されています。
- VLAN 10 内のホスト 10.1.1.4 および 10.1.1.8 のアクセスが禁止されています。

図 42-4 別の VLAN にあるサーバへのアクセスの拒否



この手順では、別の VLAN にあるサーバへのアクセスを拒否するように VLAN マップを使用して ACL を設定します。 VLAN マップ SERVER 1_ACL は、サブネット 10.1.2.0/8 内のホスト、ホスト 10.1.1.4、およびホスト 10.1.1.8 のアクセスを拒否します。一方、その他すべての IP トラフィック を許可します。 ステップ 3 では、VLAN 10 に VLAN マップ SERVER1 を適用します。

このように設定するには次の手順を実行します。

ステップ1 対応するパケットと照合し、許可する IP ACL を定義します。

```
Switch(config)# ip access-list extended SERVER1_ACL
Switch(config-ext-nacl))# permit ip 10.1.2.0 0.0.0.255 host 10.1.1.100
Switch(config-ext-nacl))# permit ip host 10.1.1.4 host 10.1.1.100
Switch(config-ext-nacl))# permit ip host 10.1.1.8 host 10.1.1.100
Switch(config-ext-nacl))# exit
```

ステップ2 SERVER1_ACL と一致する IP パケットをドロップして、一致しない IP パケットを転送するこの ACL を使用して、VLAN マップを定義します。

```
Switch(config) # vlan access-map SERVER1_MAP
Switch(config-access-map) # match ip address SERVER1_ACL
Switch(config-access-map) # action drop
Switch(config) # vlan access-map SERVER1_MAP 20
Switch(config-access-map) # action forward
Switch(config-access-map) # exit
```

ステップ3 VLAN 10 に VLAN マップを適用します。

Switch(config) # vlan filter SERVER1_MAP vlan-list 10.

VLAN アクセス マップ情報の表示

VLAN アクセス マップまたは VLAN フィルタに関する情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
Switch# show vlan access-map [mapname]	すべての VLAN アクセス マップまたは指定されたアクセス マップに関する情報を表示します。
Switch# show vlan filter [access-map name vlan vlan-id]	すべての VLAN フィルタ、または指定された VLAN や VLAN アクセス マップに関する情報を表示します。

次に、show vlan access-map コマンドの出力例を示します。

```
Switch# show vlan access-map
Vlan access-map "map_1" 10
Match clauses:
    ip address: ip1
Action:
    drop
Vlan access-map "map_1" 20
Match clauses:
    mac address: mac1
Action:
    forward
Vlan access-map "map_1" 30
Match clauses:
Action:
    drop
```



シーケンス 30 には match コマンドがありません。すべてのパケット (IP および IP 以外) はこれと 照合されてドロップされます。

次に、show vlan filter コマンドの出力例を示します。

```
Switch# show vlan filter
VLAN Map map_1 is filtering VLANs:
20-22
```

ルータ ACL を VLAN マップと併用する方法

該当タイプのパケット(IP または MAC)に対する match コマンドが VLAN マップにある場合でも、パケットがそのタイプに一致しない場合、デフォルトでは、パケットがドロップされます。VLAN マップ内に match コマンドがなく、アクションが指定されていない場合、どの VLAN マップ エントリとも一致しないパケットは転送されます。



1 つのスイッチ上で、VLAN マップまたは入力ルータ ACL を組み合わせて使用することはできません。

ルータ ACL を VLAN マップと併用する場合の注意事項

ルータ ACL と VLAN マップを同じ VLAN 上に設定する必要がある場合は、次の注意事項に従ってください。

スイッチ ハードウェアは、方向(入力および出力)ごとに、1 回の検索を実行するので、ルータ ACL および VLAN マップを同じ VLAN に設定する場合は、これらを統合する必要があります。ルータ ACL を VLAN マップと統合すると、ACE の数が急激に増加することがあります。

できるだけ末尾のデフォルト アクションを除くすべてのエントリのアクションが同一となるように、ACL を記述します。次のいずれかの形式を使用して ACL を記述します。

permit...
permit...
permit...
deny ip any any

または

deny...

deny...

deny...

permit ip any any

ACL 内で複数の許可または拒否アクションを定義する場合は、それぞれのアクション タイプをまとめて、エントリ数を削減します。

レイヤ 4 情報を含む IP ACE と TCP/UDP/ICMP ACE がともに ACL 内に存在する場合に、フルフローモードを指定する必要があるときは、レイヤ 4 ACE をリストの末尾に配置します。この結果、IP アドレスに基づくトラフィックのフィルタリングが優先されます。

VLAN に適用されるルータ ACL と VLAN マップの例

以下の例では、ルータ ACL および VLAN マップを VLAN に適用して、スイッチド パケット、ブリッジド パケット、ルーテッド パケット、およびマルチキャスト パケットへのアクセスを制御します。次の図では、それぞれの宛先に転送されるパケットを示します。ただし、パケットのパスが VLAN マップや ACL を示す回線と交差するポイントごとで、パケットを転送しないでドロップすることもできます。

ACL およびスイッチド パケット

図 42-5 に、VLAN 内でスイッチングされるパケットを ACL が処理する方法を示します。VLAN 内でスイッチングされるパケットは、ルータ ACL では処理されません。

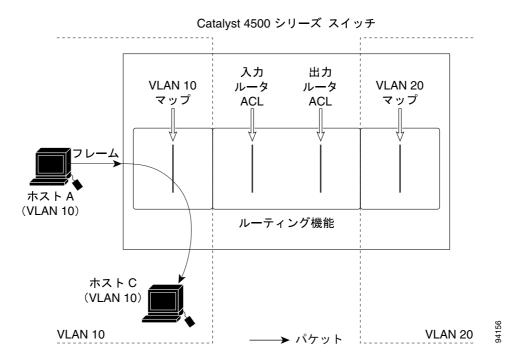


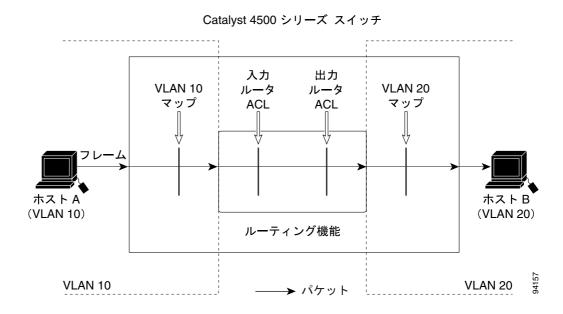
図 42-5 スイッチド パケットへの ACL の適用

ACL およびルーテッド パケット

図 42-6 に、ルーテッド パケットに ACL を適用する方法を示します。ルーテッド パケットの場合、ACL は次の順に適用されます。

- 1. 入力 VLAN の VLAN マップ
- 入力ルータ ACL
- **3.** 出力ルータ ACL
- **4.** 出力 VLAN の VLAN マップ

図 42-6 ルーテッド パケットへの ACL の適用



PACL の設定

ここでは、PACL を設定する方法について説明します。PACL は、レイヤ 2 インターフェイス上のフィルタリングを制御するのに使用されます。PACL は、レイヤ 3 情報、レイヤ 4 ヘッダー情報または IP 以外のレイヤ 2 情報に基づいて、レイヤ 2 インターフェイスのトラフィックをフィルタリングできます。

ここでは、次の内容について説明します。

- PACL の作成 (p.42-34)
- PACL 設定時の注意事項 (p.42-34)
- レイヤ 2 インターフェイス上での IP ACL と MAC ACL の設定 (p.42-35)
- アクセス グループ モードを PACL と併用する方法 (p.42-35)
- レイヤ 2 インターフェイス上でのアクセス グループ モードの設定 (p.42-36)
- レイヤ 2 インターフェイスへの ACL の適用 (p.42-36)
- レイヤ 2 インターフェイス上の ACL 設定の表示 (p.42-37)

PACL の作成

PACL を作成して、1 つまたは複数のインターフェイスに適用するには、次の作業を行います。

- ステップ 1 インターフェイスに適用する標準 IP ACL または拡張 IP ACL、または名前付き MAC 拡張 ACL を作成します。
- **ステップ2** ip access-group または mac access-group interface コマンドを使用して、IP ACL または MAC ACL を 1 つまたは複数のレイヤ 2 インターフェイスに適用します。

PACL 設定時の注意事項

PACL を設定する場合は、次の注意事項に留意してください。

- 各方向に対して同一のレイヤ 2 インターフェイスに適用できるのは、多くても 1 つの IP アクセス リストと 1 つの MAC アクセス リストだけです。
- IP アクセス リストは、IP パケットだけをフィルタリングします。MAC アクセス リストは、IP 以外のパケットだけをフィルタリングします。
- PACL の一部として設定できる ACL と ACE の数は、スイッチのハードウェア リソースにより 制限されます。これらのハードウェア リソースは、システムに設定された各 ACL 機能(RACL、VACL など)で共有されます。ハードウェアに PACL をプログラミングするのに十分なハード ウェア リソースがない場合、入力 PACL と出力 PACL のアクションが異なります。
 - 入力 PACL では、一部のパケットがソフトウェア転送のために CPU に転送されます。
 - 出力 PACL では、PACL がポート上でディセーブルに設定されます。
- 次の制限は、出力 PACL だけに関連します。
 - ハードウェアに PACL をプログラミングするのに十分なハードウェア リソースがない場合、出力 PACL はポートに適用されず、警告メッセージが表示されます。
 - 出力 PACL がレイヤ 2 ポート上に設定されている場合、レイヤ 2 ポートが属する VLAN に VACL またはルータ ACL は設定できません。

レイヤ 2 ポートが属する VLAN 上に VACL またはルータ ACL が設定されている場合、出力 PACL はレイヤ 2 ポート上に設定できません。つまり、PACL と VLAN ベースの ACL (VACL およびルータ ACL) は、レイヤ 2 ポート上では相互に排他的です。

- 出力 IP ACL と MAC ACL ではロギングがサポートされていませんが、入力 IP ACL のロギング オプションはサポートされています。
- アクセス グループ モードを使用して、その他の ACL との PACL の対話形式を変更できます。 シスコのプラットフォームにおいて動作の一貫性を保つためには、デフォルトのアクセス グ ループ モードを使用します。

レイヤ 2 インターフェイス上での IP ACL と MAC ACL の設定

レイヤ 2 物理インターフェイスに適用できるのは、IP ACL または MAC ACL だけです。(番号付き、名前付き)標準 IP ACL、(番号付き、名前付き)拡張 IP ACL、および名前付き拡張 MAC ACL がサポートされています。

レイヤ2インターフェイス上に IP ACL または MAC ACL を適用するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure t	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# interface interface	インターフェイス コンフィギュレーション モードを開 始します。
ステップ 3	<pre>Switch(config-if)# [no] {ip mac } access-group {name number in out}</pre>	レイヤ 2 インターフェイス上にアクセス グループ モード を設定します。no プレフィクスは、レイヤ 2 インターフェ イスから IP ACL または MAC ACL を削除します。
ステップ 4	Switch(config)# show running-config	アクセスリストの設定を表示します。

次に、すべての TCP トラフィックを許可し、暗黙的にその他すべての IP トラフィックを拒否する 名前付き拡張 IP ACL simple-ip-acl を設定する例を示します。

Switch(config)# ip access-list extended simple-ip-acl
Switch(config-ext-nacl)# permit tcp any any
Switch(config-ext-nacl)# end

次に、送信元ホスト 000.000.011 をすべての宛先ホストで許可する、名前付き拡張 MACL simple-mac-acl を設定する例を示します。

Switch(config)# mac access-list extended simple-mac-acl
Switch(config-ext-macl)# permit host 000.000.011 any
Switch(config-ext-macl)# end

アクセス グループ モードを PACL と併用する方法

次のモードが定義されています。

prefer port モード PACL がレイヤ2インターフェイス上に設定されている場合、PACL が有効になり、その他の ACL (ルータ ACL と VACL) を無効にします。レイヤ2インターフェイス上に PACL 機能が設定されていない場合、その他の適用可能な機能がこのインターフェイスに統合され、インターフェイス上に適用されます。これがデフォルトのアクセスグループモードです。

- prefer vlan モード ポートに VLAN ベースの ACL 機能が適用され、PACL が無効の場合は、 VLAN ベースの ACL 機能が有効になります。レイヤ 2 インターフェイスに VLAN ベースの ACL 機能が適用できない場合、インターフェイス上の既存の PACL 機能が適用されます。
- merge モード ハードウェアにプログラミングされる前に、適用可能な ACL 機能を統合します。



(注)

出力 PACL と、VACL およびルータ ACL は相互に排他的なので、アクセス グループ モードは出力トラフィック フィルタリングの動作を変更しません。

レイヤ 2 インターフェイス上でのアクセス グループ モードの設定

レイヤ2インターフェイス上にアクセス モードを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure t	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# interface interface	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	Switch(config-if)# [no] access-group mode {prefer {port vlan} merge}	レイヤ 2 インターフェイス上にアクセス グループ モード を設定します。no プレフィクスは、レイヤ 2 インターフェ イスからアクセス グループ モードを解除します。
ステップ 4	Switch(config)# show running-config	アクセス リストの設定を表示します。

次に、PACL 以外の機能を統合して、インターフェイス上に適用する例を示します。

Switch# configure t
Switch(config)# interface interface
Switch(config-if)# access-group mode prefer port

次に、ハードウェアにプログラミングされる前に、適用可能な ACL 機能を統合する例を示します。

Switch# configure t
Switch(config)# interface interface
Switch(config-if)# access-group mode merge

レイヤ 2 インターフェイスへの ACL の適用

レイヤ 2 インターフェイスに IP ACL および MAC ACL を適用するには、次のいずれかの作業を行います。

コマンド	目的
Switch(config-if)# ip access-group ip-acl {in out}	レイヤ2インターフェイスに IP ACL を適用します。
Switch(config-if)# mac access-group mac-acl {in out}	レイヤ 2 インターフェイスに MAC ACL を適用します。



Catalyst 4500 シリーズ スイッチ上で稼働する Supervisor Engine III および Supervisor Engine IV は、インターフェイス上の入力 PACL および出力 PACL の両方をサポートしています。

次に、名前付き拡張 IP ACL simple-ip-acl をインターフェイス FastEthernet 6/1 の入力トラフィックに 適用する例を示します。

Switch# configure t
Switch(config)# interface fastEthernet 6/1
Switch(config-if)# ip access-group simple-ip-acl in

次に、名前付き拡張 MAC ACL simple-mac-acl をインターフェイス FastEthernet 6/1 の出力トラフィックに適用する例を示します。

Switch# configure t
Switch(config) # interface fastEthernet 6/1
Switch(config-if) # mac access-group simple-mac-acl out

レイヤ2インターフェイス上の ACL 設定の表示

レイヤ 2 インターフェイス上の ACL 設定に関する情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
Switch# show ip interface [interface-name]	インターフェイス上の IP アクセス グループ設定を
	表示します。
Switch# show mac access-group interface [interface-name]	インターフェイス上の MAC アクセス グループ設定
	を表示します。
Switch# show access-group mode interface [interface-name]	インターフェイス上のアクセス グループ モード設
	定を表示します。

次に、IP アクセス グループ simple-ip-acl がインターフェイス fa6/1 の着信方向に設定されている例 を示します。

Switch# show ip interface fast 6/1
FastEthernet6/1 is up, line protocol is up
Inbound access list is simple-ip-acl
Outgoing access list is not set

次に、MAC アクセス グループ simple-mac-acl がインターフェイス fa6/1 の着信方向に設定されている例を示します。

Switch# show mac access-group interface fast 6/1
Interface FastEthernet6/1:
 Inbound access-list is simple-mac-acl
Outbound access-list is not set

次に、アクセス グループ統合がインターフェイス fa6/1 に設定されている例を示します。

Switch# show access-group mode interface fast 6/1
Interface FastEthernet6/1:
 Access group mode is: merge

VLAN マップおよびルータを PACL と併用する方法

出力 PACL は、VACL または出力ルータ ACL との相互作用がありません(「PACL 設定時の注意事項」[p.42-34] で説明した制限を参照)。 ただし、入力 PACL のルータ ACL および VACL との相互作用は、表 42-1 に示されるアクセス グループ モードによって決まります。

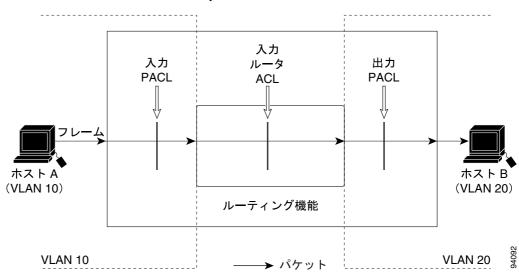
表 42-1	PACL,	VACL,	およびルータ	ACL	の相互作用
--------	-------	-------	--------	------------	-------

ACL タイプ	入力 PACL			
	prefer port モード	prefer vlan モード	merge モード	
 入力ルータ ACL 	PACL が適用される		PACL、入力ルータ ACL (統合)の順で適用される (入力側)	
2. VACL	PACL が適用される	VACL が適用される	PACL、VACL(統合)の 順で適用される(入力側)	
3. VACL と入力ルー タ ACL	PACL が適用される	VACL+ 入力ルータ ACL が適用される	PACL、VACL、入力ルータ ACL(統合)の順で適用される(入力側)	

表 42-1 に示される各 ACL タイプは、次に説明する別のシナリオで同様に使用されます。

シナリオ 1: ホスト A は、SVI が設定された VLAN 20 のインターフェイスに接続されています。図 42-7 で示すように、インターフェイスには入力 PACL が設定され、SVI には入力ルータ ACL が設定されています。

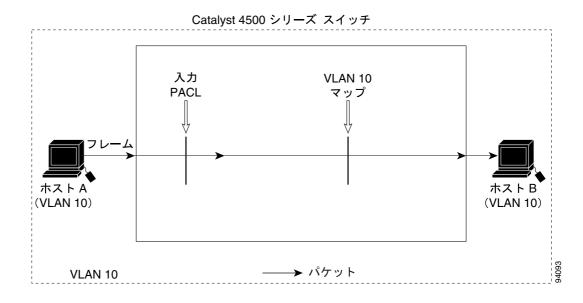
図 42-7 シナリオ 1: 入力ルータ ACL との PACL の相互作用



Catalyst 4500 シリーズ スイッチ

インターフェイス アクセス グループ モードが prefer port の場合、ホスト A からの入力トラフィックに適用されるのは入力 PACL のみです。モードが prefer vlan の場合、ルーティングを必要とするホスト A からの入力トラフィックに適用されるのは入力ルータ ACL のみです。モードが merge である場合、入力 PACL が最初にホスト A からの入力トラフィックに適用され、次に入力ルータ ACL がルーティングを必要とするトラフィックに適用されます。

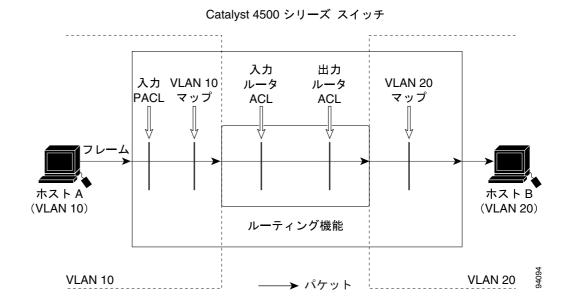
図 42-8 シナリオ 2: VACL との PACL の相互作用



インターフェイス アクセス グループ モードが prefer port の場合、ホスト A からの入力トラフィックに適用されるのは入力 PACL のみです。モードが prefer vlan の場合、ホスト A からの入力トラフィックに適用されるのは VACL のみです。モードが merge の場合、入力 PACL が最初にホスト A からの入力トラフィックに適用され、次に VACL がトラフィックに適用されます。

シナリオ 3: ホスト A は、VACL と SVI が設定された VLAN 20 のインターフェイスに接続されています。図 42-9 で示すように、SVI には入力ルータ ACL が設定されていて、インターフェイスには入力 PACL が設定されています。

図 42-9 シナリオ 3: VACL と入力ルータ ACL



インターフェイス アクセス グループ モードが prefer port の場合、ホスト A からの入力トラフィックに適用されるのは入力 PACL のみです。モードが prefer vlan の場合、VACL と入力ルータ ACL の 統合結果がホスト A からの入力トラフィックに適用されます。モードが merge の場合、入力 PACL が最初にホスト A からの入力トラフィックに適用され、次に VACL がトラフィックに適用され、最後に入力ルータ ACL がルーティングを必要とするトラフィックに適用されます(つまり、入力 PACL、VACL、および入力ルータ ACL の統合結果がトラフィックに適用されます)。



CHAPTER

43

ポート ユニキャストおよびマルチキャスト フラッディング ブロック

この章では、Catalyst 4000 ファミリ スイッチ上でマルチキャストおよびユニキャスト フラッディング ブロックを設定する方法について説明します。この章の内容は、次のとおりです。

- フラッディング ブロックの概要 (p.43-1)
- ポート ブロックの設定 (p.43-2)



この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/cr/index.htm

フラッディング ブロックの概要

MAC (メディア アクセス制御) アドレスが期限切れになるか、スイッチによって学習されなかったために、不明のユニキャストまたはマルチキャスト トラフィックがスイッチ ポートにフラッディングすることがあります (この状態は、特に Private VLAN [PVLAN] 独立ポートでは望ましくありません)。ポートにユニキャストおよびマルチキャスト トラフィックがフラッディングしないようにするには、switchport block unicast および switchport block multicast コマンドを使用して、スイッチでのフラッディング ブロックをイネーブルにします。



(注)

フラッディング ブロック機能は、すべてのスイッチド ポート(PVLAN ポートを含む)でサポートされ、ポートが転送するすべての VLAN (仮想 LAN)に適用されます。

ポート ブロックの設定

デフォルトでは、スイッチは不明の宛先 MAC アドレスを持つパケットをすべてのポートにフラッディングします。不明のユニキャストおよびマルチキャスト トラフィックがスイッチ ポートに転送される場合、セキュリティ問題が生じる可能性があります。このようなトラフィックの転送を防ぐために、不明のユニキャストまたはマルチキャスト パケットをブロックするようにポートを設定できます。



(注)

ユニキャストまたはマルチキャスト トラフィックのブロックは、スイッチ ポート上で自動的には イネーブルになりません。明示的に設定する必要があります。

インターフェイス上でのフラッディングするトラフィックのブロック



(注)

有効なインターフェイスは、物理インターフェイス(たとえば、GigabitEthernet 1/1)または EtherChannel グループ (port-channel 5 など) です。ポート チャネルのマルチキャストまたはユニキャストトラフィックをブロックする場合、ポート チャネル グループのすべてのポートでブロックされます。

インターフェイスへのマルチキャストおよびユニキャスト パケットのフラッディングをディセーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	Switch(config)# interface interface-id	インターフェイス コンフィギュレーション モードを開始し、スイッチポート インターフェイスのタイプおよび番号を入力します(たとえば、GigabitEthernet 1/1)。
ステップ 3	Switch(config-if)# switchport block multicast	ポートへの不明マルチキャストの転送をブロックします。
ステップ 4	Switch(config-if)# switchport block unicast	ポートへの不明ユニキャストの転送をブロックします。
ステップ 5	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 6	Switch# show interface interface-id switchport	入力を確認します。
ステップ 7	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を 保存します。

次に、インターフェイス GigabitEthernet 1/1 上でユニキャストおよびマルチキャスト フラッディングをブロックし、設定を確認する例を示します。

Switch# configure terminal

Enter configuration commands, one per line. End with ${\tt CNTL/Z.}$

Switch(config)# interface gigabitethernet1/1

 ${\tt Switch(config-if)\#\ \textbf{switchport\ block\ multicast}}$

Switch(config-if)# switchport block unicast

Switch(config-if)# end

Switch# show interface gigabitethernet1/1 switchport

Name: Gi1/3

Switchport: Enabled

<テキスト出力は省略>

Port Protected: On

Unknown Unicast Traffic: Not Allowed Unknown Multicast Traffic: Not Allowed

Broadcast Suppression Level: 100 Multicast Suppression Level: 100 Unicast Suppression Level: 100

ポート上での通常の転送の再開

ポート上で通常の転送を再開するには、次の作業を行います。

コマンド	目的
Switch# configure terminal	グローバル コンフィギュレーション モードを開始 します。
Switch(config)# interface interface-id	インターフェイス コンフィギュレーション モードを開始し、スイッチポート インターフェイスのタイプおよび番号を入力します(たとえば、GigabitEthernet 1/1)。
<pre>Switch(config-if)# no switchport block multicast</pre>	ポートへの不明マルチキャストのフラッディングを イネーブルにします。
Switch(config-if)# no switchport block unicast	ポートへの不明ユニキャストのフラッディングをイ ネーブルにします。
Switch(config)# end	特権 EXEC モードに戻ります。
Switch# show interface interface-id switchport	入力を確認します。
Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を 保存します。

■ ポート ブロックの設定



CHAPTER

44

ストーム制御の設定

この章では、Catalyst 4500 シリーズ スイッチ上でポートベースのトラフィック制御を設定する方法 について説明します。



この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univered/cc/td/doc/product/software/ios122sr/cr/index.htm

この章の内容は、次のとおりです。

- ストーム制御の概要 (p.44-2)
- ブロードキャスト ストーム制御のイネーブル化 (p.44-4)
- マルチキャスト ストーム制御のイネーブル化 (p.44-6)
- ブロードキャスト ストーム制御のディセーブル化 (p.44-8)
- マルチキャスト ストーム制御のディセーブル化 (p.44-9)
- ストーム制御の表示 (p.44-10)

ストーム制御の概要

ここでは、次の内容について説明します。

- ハードウェアベースのストーム制御実装 (p.44-2)
- ソフトウェアベースのストーム制御実装 (p.44-3)

ストーム制御は、LAN インターフェイスがブロードキャスト ストームによって混乱しないようにします。ブロードキャスト ストームは、ブロードキャスト パケットがサブネットにフラッディングすると発生し、過剰なトラフィックが生み出され、ネットワーク パフォーマンスを低下させます。プロトコルスタック実装またはネットワーク設定のエラーが、ブロードキャスト ストームの原因になります。



(注)

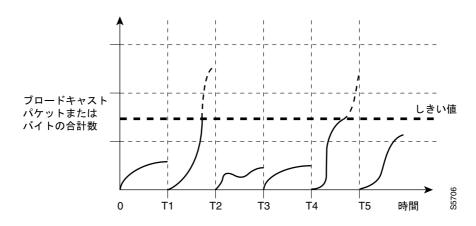
ストーム制御は、WS-X4516 スーパーバイザ エンジンおよびスーパーバイザ エンジン 6-E 上の全ポートにあるハードウェアでサポートされます。これに対して、スーパーバイザ エンジン WS-X4515、WS-X4014、および WS-X4013+ は、非ブロッキング ギガビット ポート上のハードウェアおよび他のすべてのポート上のソフトウェアでサポートされ、これらのインターフェイスのカウンタが概算で算出されます。マルチキャスト ストーム制御がサポートされるのは、WS-X4516 スーパーバイザ エンジンおよびスーパーバイザ エンジン 6-E のみです。

ハードウェアベースのストーム制御実装

ブロードキャスト抑制は、サブネット上でのブロードキャスト アクティビティを 1 秒のインターバルで測定し、その測定結果をあらかじめ定義されたしきい値と比較するフィルタリングを使用します。 しきい値に達した場合、以降のブロードキャスト アクティビティが一定時間だけ抑制されます。 ブロードキャスト抑制は、デフォルトではディセーブル設定にされています。

図 44-1 は、一定時間における LAN インターフェイスのブロードキャスト トラフィック パターンを示しています。この例では、T1 と T2、および T4 と T5 の間にブロードキャスト抑制が行われています。これらのインターバル中に、ブロードキャスト トラフィックの量が設定済みのしきい値を超過したためです。





ブロードキャスト抑制しきい値とタイム インターバルの組み合わせによって、ブロードキャスト抑制アルゴリズムをさまざまなレベルで機能させることができます。しきい値が高いほど、通過できるブロードキャスト パケット数が多くなります。

Catalyst 4500 シリーズ スイッチ (スーパーバイザ エンジン 6-E を含む)でのブロードキャスト抑制 は、ハードウェアに実装されます。LAN インターフェイスからスイッチング バスへ流れるパケットは抑制回路で監視されます。パケットの宛先アドレスがブロードキャストの場合、ブロードキャスト抑制回路は、1 秒のインターバル内の現在のブロードキャスト数を追跡します。この値がしきい値に達すると、以降のブロードキャスト パケットは排除されます。

ハードウェアによるブロードキャスト抑制では、ブロードキャスト アクティビティの測定に帯域幅 ベースの方式が使用されるので、ブロードキャスト トラフィックが使用できる総帯域幅に対する割合の設定が、実装上の最も重要な要素になります。パケットは均等な間隔で着信するわけではないので、ブロードキャスト アクティビティが測定される 1 秒のインターバルによって、ブロードキャスト抑制の動作が影響を受ける場合があります。

ソフトウェアベースのストーム制御実装

ストーム制御がインターフェイス上でイネーブルに設定されている場合、スイッチはインターフェイス上で受信されるパケットをモニタし、パケットがブロードキャストかどうかを判別します。スイッチは、1秒のインターバルで受信されるブロードキャスト パケット数を監視します。インターフェイスしきい値に達した場合、インターフェイス上のすべての着信データ トラフィックがドロップされます。このしきい値は、ブロードキャスト トラフィックが使用できる総帯域に対する割合として指定されます。下限しきい値が指定されている場合、着信トラフィックがそのしきい値を下回るとすぐにすべてのデータ トラフィックが転送されます。

ブロードキャスト ストーム制御のイネーブル化

ストーム制御をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するポートを入力します。
ステップ 3	Switch(config-if)# storm-control	ブロードキャスト ストーム制御を設定します。
	broadcast level [high level] [lower level]	ブロードキャスト トラフィックの上限しきい値レベルを 指定します。ストーム制御のアクションは、トラフィック 使用率がこのレベルに達すると実行されます。
		(任意)下限しきい値レベルを指定します。ソフトウェアベースの抑制をサポートするインターフェイスのトラフィックがこのレベルを下回ると、(アクションがフィルタリングの場合)通常の伝送が再開されます。
		(注) 低レベルのキーワードは、スーパーバイザ エンジン 6-E の実装には適用されません。
		(注) ハードウェアベースの抑制を実行するポートでは、 下限しきい値が無視されます。
ステップ 4	Switch(config-if)# storm-control	ストーム検出時に実行するアクションを指定します。
	action {shutdown trap}	デフォルトでは、ブロードキャスト トラフィックが排除され、トラップは送信されません。
		shutdown キーワードは、ストーム時にポートを errdisable ステートにします。回復インターバルが設定されていない 場合、ポートはシャットダウン ステートのままです。
		(注) trap キーワードは、ストーム検出時に SNMP(簡易 ネットワーク管理プロトコル)トラップを生成します。このキーワードは使用可能ですが、Cisco IOS Release 12.1(19)EW ではサポートされていません。
ステップ 5	Switch(config-if)# exit	コンフィギュレーション モードに戻ります。
ステップ 6	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 7	Switch# show storm-control [interface] broadcast	抑制されたパケット数を表示します。
ステップ 8	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

次に、インターフェイス上でストーム制御をイネーブルにする例を示します。

Diagnostic Monitoring: N/A

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fa3/1
Switch(config-if) # storm-control broadcast level 50
Switch(config-if)# end
Switch# show storm-control //Supervisor Engine 6-E
Interface Filter State Broadcast Multicast Level
Fi3/1
        Forwarding Enabled Disabled 50.00%
Switch# show int fa2/1 capabilities //Supervisor Engine 6-E
FastEthernet2/1
 Model:
                      WS-X4148-RJ45V-RJ-45
 Type:
                      10/100BaseTX
 Speed:
                       10,100,auto
                      half,full,auto
 Duplex:
 Auto-MDIX:
                     no
 Trunk encap. type: 802.1Q
 Trunk mode:
                      on, off, desirable, nonegotiate
 Channel:
                      yes
 Broadcast suppression: percentage(0-100), hw
 Multicast suppression: percentage(0-100), hw <===== unique to Sup Engine 6-E systems
                   rx-(none),tx-(none)
 Flowcontrol:
 VLAN Membership:
                      static, dynamic
 Fast Start:
                      yes
 CoS rewrite:
                      ves
                      yes
 ToS rewrite:
                     yes (Cisco Voice Protocol)
 Inline power:
 SPAN:
                      source/destination
 IIDI D:
                      ves
 Link Debounce:
 Link Debounce Time: no
 Port Security:
                      yes
                      yes
 Dot1x:
 Maximum MTU:
                     1552 bytes (Baby Giants)
 Multiple Media Types: no
```

マルチキャスト ストーム制御のイネーブル化

次の内容について説明します。

- スーパーバイザ エンジン 6-E でのマルチキャスト抑制 (p.44-6)
- WS-X4516 スーパーバイザ エンジンでのマルチキャスト抑制 (p.44-7)
- WS-X4515、WS-X4014、および WS-X4013+ スーパーバイザ エンジンでのマルチキャスト抑制 (p.44-7)



(注)

Cisco IOS Release 12.2(18)EW 以降、**show interface counters storm-control** コマンドで出力されるカウンタには、ドロップされたマルチキャスト パケットも含まれます。

スーパーバイザ エンジン 6-E でのマルチキャスト抑制

スーパーバイザ エンジン 6-E は、インターフェイス単位のマルチキャスト抑制をサポートします。これにより、ユーザは着信マルチキャストおよびインターフェイス上のプロードキャスト トラフィックを抑制できます。



<u>—</u> (注)

マルチキャスト抑制およびブロードキャスト抑制は、インターフェイスごとに共通のしきい値を共有します。マルチキャスト抑制は、ブロードキャスト抑制がイネーブルになっている場合*のみ*有効になります。

インターフェイスでブロードキャスト抑制をディセーブルにすると、マルチキャスト抑制もディセーブルになります。

スーパーバイザ エンジン 6-E のマルチキャスト抑制をイネーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するポートを入力します。
ステップ 3	<pre>Switch(config-if)# storm-control broadcast include multicast</pre>	マルチキャスト抑制をイネーブルにします。
ステップ 4	Switch(config-if)# exit	コンフィギュレーション モードに戻ります。
ステップ 5	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 6	Switch# show storm-control	設定を確認します。

次に、ブロードキャスト抑制がイネーブルであるポート上で、マルチキャスト抑制をイネーブルに する例を示します。

Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config) # int fa3/1

Switch(config-if) # storm-control broadcast include multicast

Switch(config-if)# end

Switch#

Switch# show storm-control

Interface Filter State Broadcast Multicast Level _____ Fi3/1 Forwarding Enabled Enabled 50.00%

WS-X4516 スーパーバイザ エンジンでのマルチキャスト抑制

WS-X4516 スーパーバイザ エンジンでは、ストーム制御がイネーブルであるすべてのポートに対し て、マルチキャスト抑制をイネーブルにできます。マルチキャスト抑制は、ブロードキャスト抑制 が設定されたすべてのポートに適用されます。また、将来ブロードキャスト ストーム制御用に設定 するポートにも適用されます。マルチキャストトラフィックのみを抑制することはできません。

ブロードキャストまたはマルチキャスト トラフィックのしきい値を個別に指定することはできま せん。ブロードキャスト抑制用に設定したしきい値は、着信マルチキャスト トラフィックと着信ブ ロードキャストトラフィックの両方に適用されます。

WS-X4516 スーパーバイザ エンジンのマルチキャスト抑制をイネーブルにするには、次の作業を実 行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するポートを入力します。
ステップ 3	<pre>Switch(config-if)# storm-control broadcast include multicast</pre>	マルチキャスト抑制をイネーブルにします。
ステップ 4	Switch(config-if)# exit	コンフィギュレーション モードに戻ります。
ステップ 5	Switch(config)# end	特権 EXEC モードに戻ります。

次に、ブロードキャスト抑制がイネーブルであるポート上で、マルチキャスト抑制をイネーブルに する例を示します。

Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z. Switch(config) # storm-control broadcast include multicast Switch(config)# end

Switch#

WS-X4515、WS-X4014、および WS-X4013+ スーパーバイザ エンジンでのマルチキャ スト抑制

WS-X4515、WS-X4014、および WS-X4013+ スーパーバイザ エンジンでは、マルチキャスト抑制が ハードウェアでサポートされません。これらのモジュールでソフトウェアベースのブロードキャス ト抑制が使用されると、着信したすべてのデータ パケットはドロップされます。 ブロードキャスト 抑制のみを設定したかどうかに関係なく、マルチキャスト パケットはスタブおよびブロッキング ギガビット ボートの場合と同様に排除されます。 ブロードキャスト抑制をハードウェアで実行する ノンブロッキング ギガビット ポートでも、マルチキャスト パケットは排除されません。

Switch#

ブロードキャスト ストーム制御のディセーブル化

ストーム制御をディセーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するポートを入力します。
ステップ 3	Switch(config-if)# no storm-control broadcast level	ポートのストーム制御をディセーブルにします。
ステップ 4	Switch(config-if)# no storm-control action {shutdown trap}	指定されたストーム制御のアクションをディセーブルに し、デフォルトのフィルタ アクションに戻します。
ステップ 5	Switch(config-if)# exit	コンフィギュレーション モードに戻ります。
ステップ 6	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 7	Switch# show storm-control broadcast	入力を確認します。
ステップ 8	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

次に、インターフェイス上でストーム制御をディセーブルにする例を示します。

マルチキャスト ストーム制御のディセーブル化

WS-X4516、WS-X4515、WS-X4014、および WS-X4013+ スーパーバイザ エンジンのマルチキャスト抑制をディセーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するポートを入力します。
ステップ 3	Switch(config-if)# [no] storm-control broadcast include multicast	マルチキャスト抑制をイネーブルにします。
ステップ 4	Switch(config-if)# end	コンフィギュレーション モードに戻ります。
ステップ 5	Switch(config)# end	特権 EXEC モードに戻ります。

スーパーバイザ エンジン 6-E のマルチキャスト抑制をディセーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# [no] storm-control broadcast include multicast	マルチキャスト抑制をイネーブルまたはディセーブルにし ます。
ステップ 3	<pre>Switch(config-if)# no storm-control broadcast level</pre>	ポート ストーム制御 (ブロードキャストおよびマルチキャスト) をディセーブルにします。
ステップ 4	Switch(config-if)# end	コンフィギュレーション モードに戻ります。
ステップ 5	Switch(config)# end	特権 EXEC モードに戻ります。

ストーム制御の表示



インターフェイス上でサポートされているストーム制御のモードを確認するには、show interface capabilities コマンドを使用します。

次に、ソフトウェア(sw)でブロードキャスト抑制をサポートするインターフェイスの例を示します。

Switch# show int fa2/1 capabilities

FastEthernet2/1

Model: WS-X4148-RJ45V-RJ-45

10/100BaseTX Type: Speed: 10,100,auto Duplex: half, full, auto

Auto-MDIX: no

Auto-MDIA.

Trunk encap. type: 802.10
on,off,desirable,nonegotiate

yes

Broadcast suppression: percentage(0-100), hw

Multicast suppression: percentage(0-100), hw <=====unique to Sup Engine 6-E

Flowcontrol: rx-(none),tx-(none) VLAN Membership: static, dynamic

Fast Start: yes CoS rewrite: yes ToS rewrite: ves

yes (Cisco Voice Protocol) Inline power:

SPAN: source/destination

UDLD: yes Link Debounce: no Link Debounce Time: Port Security: ves Dot1x: yes

1552 bytes (Baby Giants) Maximum MTU:

Multiple Media Types: no Diagnostic Monitoring: N/A



廃棄パケット数を表示するには、show interfaces counters storm-control コマンドを使用します。

Switch# show interfaces counters storm-control

TotalSuppressedPackets Port Broadcast Multicast Level Fa2/1 Enabled Disabled 10.00% 46516510 Enabled Gi3/1 Enabled 50.00%

次に、show storm-control コマンドの出力の例を示します。

Switch# show storm-control //Supervisor Engine 2+ to V-10GE

Interface Filter State Upper Lower Current 2.00% Gi 4/4 Forwarding 2.00% Switch



前述の例では、[current] が所定の瞬間に抑制されたトラフィックの割合を表し、ハードウェアで抑 制を実行するポートでは値が N/A (該当しない)になります。

Switch# show storm-control //Supervisor Engine 6-E Interface Filter State Broadcast Multicast Level Fa2/1 Blocking Enabled Disabled 10.00% Gi3/1 Link Down Enabled Enabled 50.00%



CHAPTER

45

SPAN と RSPAN の設定

この章では、Catalyst 4500 シリーズ スイッチ上で Switched Port Analyzer (SPAN; スイッチド ポートアナライザ)と Remote SPAN (RSPAN)を設定する方法について説明します。SPAN は、SwitchProbe デバイスまたはその他の Remote Monitoring (RMON) プローブなどのネットワーク アナライザによる解析用に、ネットワーク トラフィックを選択します。

この章の内容は、次のとおりです。

- SPAN と RSPAN の概要 (p.45-2)
- SPAN の設定 (p.45-8)
- CPU ポートのスニッフィング (p.45-12)
- カプセル化の設定 (p.45-14)
- 入力パケット (p.45-14)
- アクセス リスト フィルタリング (p.45-16)
- パケット タイプ フィルタリング (p.45-18)
- 設定例 (p.45-19)
- RSPAN の設定 (p.45-20)
- SPAN および RSPAN ステータスの表示 (p.45-30)



この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cr/index.htm

SPAN と RSPAN の概要

ここでは、次の内容について説明します。

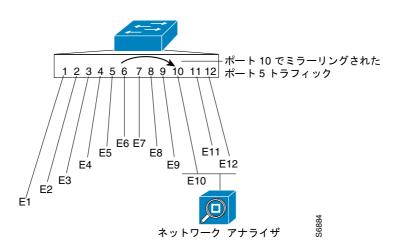
- SPAN と RSPAN の概念と用語 (p.45-3)
- SPAN と RSPAN のセッション限度 (p.45-6)
- SPAN と RSPAN のデフォルト設定 (p.45-7)

SPAN は、任意の VLAN (仮想 LAN)上の1つまたは複数の送信元インターフェイスからのトラフィック、または1つまたは複数の VLAN から宛先インターフェイスへのトラフィックを解析するためにミラーリングします。図 45-1では、イーサネットインターフェイス 5(送信元インターフェイス)上のすべてのトラフィックが、イーサネットインターフェイス 10 にミラーリングされます。イーサネットインターフェイス 10 のネットワーク アナライザは、イーサネットインターフェイス 5 に物理的に接続していなくても、このインターフェイスからのすべてのネットワーク トラフィックを受信できます。

SPAN を設定する場合、送信元インターフェイスと宛先インターフェイスは同一スイッチ上に存在している必要があります。

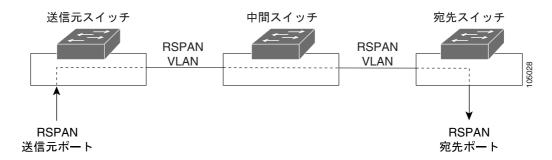
SPAN は、送信元インターフェイス上のネットワーク トラフィックのスイッチングに影響を与えません。送信元インターフェイスが送受信したパケットのコピーは宛先インターフェイスに送信されます。

図 45-1 SPAN の設定例



RSPAN は、ネットワーク内の複数のスイッチの RMON 機能をイネーブルにすることによって、SPAN を拡張します。各 RSPAN セッションのトラフィックは、関与するすべてのスイッチ上のその RSPAN セッション専用のユーザ指定 RSPAN VLAN を介して伝送されます。送信元からの SPAN トラフィックは、RSPAN VLAN にコピーされてから、トランク ポートを介して転送されます。トランク ポートは、RSPAN VLAN を監視する RSPAN 宛先セッションに RSPAN VLAN を伝送します(図 45-2 を参照)。

図 45-2 RSPAN の設定例



SPAN と RSPAN は、送信元ポートまたは送信元 VLAN 上でのネットワーク トラフィックのスイッチングに影響しません。送信元によって送受信されたパケットのコピーは、宛先に送信されます。デフォルトでは、SPAN または RSPAN セッションによって必要とされるトラフィックを除いて、宛先ポートはトラフィックの送受信を行いません。

SPAN または RSPAN 宛先ポートを使用して、ネットワーク セキュリティ デバイスから送信されたトラフィックを転送できます。たとえば、Cisco Intrusion Detection System (IDS; 侵入検知システム) センサー装置を宛先ポートに接続した場合、IDS デバイスは TCP リセット パケットを送信して、疑わしい攻撃者の TCP セッションを停止させることができます。

SPAN と RSPAN の概念と用語

ここでは、SPAN と RSPAN の設定に関連する概念と用語について説明します。ここでは、次の内容について説明します。

- SPAN セッション (p.45-3)
- トラフィック タイプ (p.45-4)
- 送信元ポート (p.45-5)
- 宛先ポート (p.45-5)
- VSPAN (p.45-6)
- SPAN トラフィック (p.45-6)

SPAN セッション

ローカル SPAN セッションは、宛先ポートを送信元ポートに対応付けます。一連のまたは一定範囲のポートおよび送信元 VLAN の着信または発信トラフィックを監視できます。RSPAN セッションは、送信元ポートと送信元 VLAN をネットワーク上の RSPAN VLAN に対応付けます。宛先の送信元は RSPAN VLAN です。

モニタ対象のネットワーク トラフィックの送信元を指定するパラメータを使用して、SPAN セッションを設定します。

個別のまたは重複する一連の SPAN 送信元を使用して、複数の SPAN または RSPAN セッションを設定できます。スイッチド ポートおよびルーテッド ポートはいずれも、SPAN 送信元または宛先ポートとして設定できます。

RSPAN 送信元セッションは、SPAN 送信元ポートまたは VLAN を宛先 RSPAN VLAN に対応付けます。 RSPAN 宛先セッションは、RSPAN VLAN を宛先ポートに対応付けます。

SPAN セッションは、スイッチの正常な動作を妨げません。ただし、SPAN の宛先がオーバーサブスクライブ型ポート(たとえば 100~Mbps ポートを監視する 10~Mbps ポート)では、パケットがドロップされるか、失われる可能性があります。

ディセーブルに設定されたポート上でも SPAN セッションを設定できます。ただし、そのセッションに対して宛先ポートと、少なくとも 1 つの送信元ポートまたは VLAN をイネーブルにしないかぎり、SPAN セッションはアクティブになりません。

SPAN セッションは、システムの起動後に、宛先ポートが動作可能になるまでアクティブになりません。

トラフィック タイプ

SPAN セッションには、次のトラフィック タイプがあります。

• 受信(Rx)SPAN 受信(または入力)SPANの目的は、スイッチが変更または処理を行う前に、送信元インターフェイスまたは VLAN が受信したすべてのパケットをできるかぎり多く監視することです。送信元が受信した各パケットのコピーは、その SPAN セッションの宛先ポートに送信されます。1 つの SPAN セッションで、一連のまたは一定範囲の入力ポートまたは VLAN を監視できます。

タグ付きパケット (ISL [スイッチ間リンク] たは IEEE 802.1Q) では、タギングは入力ポートで削除されます。宛先ポートでは、タギングがイネーブルの場合、パケットは ISL または 802.1Q ヘッダー付きで表示されます。 タギングが指定されていない場合、パケットはネイティブ形式で表示されます。

ルーティングが原因で変更されたパケットは、Rx SPAN 用に変更されることなくコピーされます。つまり、元のパケットがコピーされます。QoS (Quality Of Service)が原因で変更されたパケット (たとえば、変更済み Differentiated Services Code Point [DSCP; DiffServ コード ポイント]) は、Rx SPAN 用に変更されてコピーされます。

受信処理中にパケットをドロップする可能性のある機能は、SPAN では無効です。実際の着信パケットがドロップされた場合でも、宛先ポートはパケットのコピーを受信します。これらの機能には、標準および拡張 IP 入力 Access Control List (ACL; アクセス コントロール リスト)、ユニキャストおよび入力側 QoS ポリシング用の標準および拡張 IP 出力 ACL、VLAN マップ、入力側 QoS ポリシング、Policy-Based Routing (PBR; ポリシーベース ルーティング) などがあります。パケットのドロップを引き起こすスイッチ輻輳も、SPAN には影響しません。

• 送信(Tx)SPAN 送信(または出力)SPANの目的は、スイッチによる変更または処理がすべて実行されたあとに、送信元インターフェイスから送信されたすべてのパケットをできるかぎり多く監視することです。パケットが変更されたあと、送信元から各パケットのコピーがそのSPANセッションに対応する宛先ポートに送信されます。1つのSPANセッションで一定範囲の出力ポートを監視できます。

ルーティングにより変更されたパケット (Time to Live [TTL; 存続可能時間] または MAC [メディア アクセス制御] による変更など) は、宛先ポートでも変更されます。 QoS が原因で変更されたパケットは、SPAN 送信元とは異なる DSCP (IP パケット) または Class of Service (CoS; サービス クラス) (IP 以外のパケット) を設定されることがあります。

送信処理中にパケットをドロップする可能性のある機能は、SPAN 用のコピーにも影響を与えることがあります。このような機能には、VLAN マップ、マルチキャスト パケットに対応する標準および拡張 IP 出力 ACL、出力側 QoS ポリシングがあります。出力 ACL の場合は、SPAN 送信元がパケットをドロップすると、SPAN の宛先もパケットをドロップします。出力側 QoS ポリシングの場合は、SPAN 送信元がパケットをドロップしても、SPAN 宛先はパケットをドロップするとは限りません。送信元ポートがオーバーサブスクライブ型である場合、宛先ポートは別の廃棄動作を行います。

双方向 1つの SPAN セッションで、一連の単一ポートまたは一定範囲のポートの受信パケットと送信パケットを両方監視できます。

送信元ポート

送信元ポート(別名モニタ対象ポート)は、ネットワーク トラフィック解析のために監視するスイッチド ポートまたはルーテッド ポートです。単一のローカル SPAN セッションまたは RSPAN 送信元セッションで、受信(Rx) 送信(Tx) または双方向(both)の送信元ポートトラフィックを監視できます。スイッチは、任意の数の送信元ポート(スイッチで使用可能なポートの最大数まで)および任意の数の送信元 VLAN をサポートしています。

送信元ポートには、次の特性があります。

- すべてのポート タイプ (EtherChannel、ファスト イーサネット、ギガビット イーサネットなど)が可能です。
- 複数の SPAN セッションで監視できます。
- 宛先ポートに指定することはできません。
- 各送信元ポートに、監視する方向(入力、出力、または両方)を設定できます。EtherChannel の送信元に設定する場合、監視する方向はグループ内のすべての物理ポートに適用されます。
- 送信元ポートは同じ VLAN 内にあっても異なる VLAN にあってもかまいません。
- VLAN SPAN 送信元の場合、送信元 VLAN 内のすべてのアクティブ ポートは、送信元ポートとして組み入れられます。

トランク ポートを、送信元ポートとして設定できます。デフォルトでは、トランク上でアクティブ なすべての VLAN が監視されます。VLAN フィルタリングを使用することにより、トランク送信元 ポート上の SPAN トラフィックの監視を特定の VLAN に制限できます。選択された VLAN のスイッチドトラフィックのみが宛先ポートに送信されます。この機能は、宛先 SPAN ポートに転送されたトラフィックのみに影響し、通常のトラフィックのスイッチングには影響を与えません。この機能は、VLAN 送信元によるセッションでは許可されません。

宛先ポート

各ローカル SPAN セッションまたは RSPAN 宛先セッションには、送信元ポートおよび VLAN からのトラフィックのコピーを受信する宛先ポート(別名モニタリング ポート)を設定する必要があります。

宛先ポートには、次の特性があります。

- 送信元ポートと同じスイッチ上になければなりません (ローカル SPAN セッションの場合)。
- 任意のイーサネット物理ポートに指定できます。
- 同時に1つの SPAN セッションにしか参加できません(ある SPAN セッションの宛先ポートは、 別の SPAN セッションの宛先ポートになることはできません)。
- 送信元ポートに指定することはできません。
- EtherChannel グループに指定することはできません。
- EtherChannel グループが SPAN 送信元として指定されている場合でも、EtherChannel グループ に割り当てられた物理ポートに指定できます。ポートは、SPAN 宛先ポートとして設定されて いる間は、グループから削除されます。
- ラーニングがイネーブルに設定されていないかぎり、ポートは SPAN セッションが必要とする ものを除いて、トラフィックの転送を行いません。ラーニングがイネーブルに設定されている 場合、ポートは、宛先ポート上で学習されたホストに向けられたトラフィックも伝送します。
- 入力トラフィックの転送がネットワーク セキュリティ デバイスでイネーブルの場合、宛先ポートはレイヤ2でトラフィックを転送します。
- SPAN セッションがアクティブな間は、スパニングツリーに参加しません。

- 宛先ポートである場合は、どのレイヤ 2 プロトコル (Spanning-Tree Protocol [STP; スパニング ツリー プロトコル] VLAN Trunking Protocol [VTP; VLAN トランキング プロトコル] Cisco Discovery Protocol [CDP; シスコ検出プロトコル]、Dynamic Trunking Protocol [DTP]、Port Aggregation Protocol [PAgP]) にも参加しません。
- SPAN セッションの送信元 VLAN に所属する宛先ポートは、送信元リストから除外され、監視されません。
- すべての監視された送信元ポートの送受信されたトラフィックのコピーを受信します。宛先ポートがオーバーサブスクライブ型である場合、輻輳を起こす可能性があります。この輻輳は、1つまたは複数の送信元ポートにおいてトラフィック転送に影響を与えます。

VSPAN

VLAN-based SPAN (VSPAN) は、1 つまたは複数の VLAN でのネットワーク トラフィックを監視します。

VSPAN セッションでは、次の注意事項に従ってください。

- RSPAN VLAN 上のトラフィックは、VSPAN セッションでは監視されません。
- モニタ対象の VLAN 上のトラフィックのみが宛先ポートに送信されます。
- 宛先ポートが送信元 VLAN に所属する場合は、送信元リストから除外され、監視されません。
- ポートが送信元 VLAN に追加または送信元 VLAN から削除されると、これらのポートで受信された送信元 VLAN 上のトラフィックは、監視中の送信元に追加または送信元から削除されます。
- VLAN プルーニングと VLAN 許可リストは、SPAN モニタでは無効です。
- VSPAN が監視するのはスイッチに入るトラフィックに限られ、VLAN 間でルーティングされるトラフィックは監視しません。たとえば、VLAN が受信で監視され、マルチレイヤ スイッチが別の VLAN からのトラフィックをモニタ対象の VLAN にルーティングする場合、そのトラフィックはモニタ対象とはならず、SPAN 宛先ポート上で受信されません。
- 同じセッション内のフィルタ VLAN を VLAN 送信元と併用することはできません。
- 監視できるのは、イーサネット VLAN だけです。

SPAN トラフィック

ローカル SPAN を使用すれば、マルチキャストパケットおよび Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) パケットをはじめ、CDP、VTP、DTP、STP、PAgP の各パケットを含む、すべてのネットワーク トラフィックを監視できます。RSPAN を使用して、レイヤ 2 プロトコルを監視することはできません (詳細については、「RSPAN 設定時の注意事項」[p.45-20] を参照)。

SPAN の設定によっては、同じ送信元パケットの複数のコピーが SPAN 宛先ポートに送信される場合があります。たとえば、送信元 a1 受信モニタおよび a2 受信 / 送信モニタから宛先ポート d1 まで、双方向(受信と送信の両方) SPAN セッションが設定されているとします。パケットが a1 からスイッチに入り、a2 へスイッチングされると、着信パケットおよび発信パケットの両方が宛先ポート d1 に送信されます。このため、両方のパケットは同じものになります(レイヤ 3 書き換えが行われた場合には、付加されたレイヤ 3 情報のため異なるパケットになります)。

SPAN と RSPAN のセッション限度

入力側送信元を含む同時 SPAN セッションを最大 2 つ設定できます。また、出力側送信元を含む同時セッションを最大 4 つ設定できます。双方向送信元は、入力と出力の両方として数えます。RSPAN 宛先セッションは、入力側送信元を含むセッションとして数えます。

SPAN と RSPAN のデフォルト設定

表 45-1 に、SPAN と RSPAN のデフォルト設定を示します。

表 45-1 SPAN と RSPAN のデフォルト設定

機能	デフォルト設定
SPAN ステート	ディセーブル。
監視する送信元ポートのトラフィック	受信トラフィックと送信トラフィックの両方 (both)
フィルタ	すべての VLAN、すべてのパケット タイプ、すべてのア
	ドレス タイプ
カプセル化タイプ(宛先ポート)	ネイティブ形式 (カプセル化タイプ ヘッダーなし)
入力転送 (宛先ポート)	ディセーブル。
ホスト学習 (宛先ポート)	ディセーブル。

SPAN の設定

ここでは、SPAN を設定する方法について説明します。

- SPAN 設定時の注意事項および制約事項 (p.45-8)
- SPAN 送信元の設定 (p.45-9)
- SPAN 宛先の設定 (p.45-10)
- トランク インターフェイス上の送信元 VLAN のモニタリング (p.45-10)
- 設定例 (p.45-11)
- SPAN の設定の確認 (p.45-11)



(注)

SPAN コンフィギュレーション コマンドを入力しても、すでに設定された SPAN パラメータはクリアされません。設定済みの SPAN パラメータをクリアするには、no monitor session コマンドを使用する必要があります。

SPAN 設定時の注意事項および制約事項

SPAN を設定する際、次の注意事項および制約事項に従ってください。

- ネットワーク アナライザを使用して、インターフェイスを監視する必要があります。
- SPAN セッションでは、送信元 VLAN とフィルタ VLAN を混在させることはできません。送信元 VLAN またはフィルタ VLAN を使用することはできますが、両方を同時には使用できません。
- EtherChannel インターフェイスを、SPAN 送信元インターフェイスにできますが、SPAN 宛先インターフェイスにできません。
- 送信元インターフェイスを指定し、トラフィック タイプ(tx、rx、または both)を指定しなかった場合、デフォルトで [both] が使用されます。
- 複数の SPAN 送信元インターフェイスを指定する場合、各インターフェイスはそれぞれ異なる VLAN に属していてもかまいません。
- **no monitor session** *number* コマンドを他のパラメータを指定せずに入力して、SPAN のセッション *番号*をクリアする必要があります。
- no monitor コマンドを実行すると、すべての SPAN セッションがクリアされます。
- SPAN 宛先は、スパニングツリー インスタンスに参加しません。SPAN はモニタ対象トラフィックに BPDU を含みます。 したがって、SPAN 宛先上で検出される BPDU は、SPAN 送信元からのものです。
- SPAN 宛先ポートは 1 セッションにつき 1 つに制限されています。

SPAN 送信元の設定

SPAN セッションの送信元を設定するには、次の作業を行います。

コマンド

Switch(config)# [no] monitor session {session_number} {source {interface} <interface_list> | {vlan vlan_IDs | cpu [queue queue_ids] } [rx | tx | both]

目的

SPAN セッション番号 ($1 \sim 6$)、送信元インターフェイス (FastEthernet または GigabitEthernet)、VLAN ($1 \sim 4094$)、CPU から送受信されたトラフィックがセッションの宛先にコピーされるか否か、および監視するトラフィックの方向を指定します。

 $session_number$ には、この RSPAN セッションで識別されるセッション番号を指定します(1 ~ 6)。

interface-list には、監視する送信元ポートを指定します。有効なインターフェイスには、物理インターフェイスとポート チャネル論理インターフェイス(port-channel port-channel-number) があります。

vlan_IDsには、送信元 VLAN を指定します。

queue_ids には、関連するキューを指定します。

(任意)[, | -] には、一連のまたは一定範囲のインターフェイスを指定します。カンマのあとにはスペースを入れます。ハイフンの前後にはスペースを1つ入れます。

(任意) 監視するトラフィックの方向を指定します。トラフィックの方向を指定しない場合、送信元インターフェイスは、送信(tx)と受信(rx)の両方のトラフィックを送信します。追加の送信元ポートは、受信トラフィックだけを監視します。

- rx 受信トラフィックを監視します。
- tx 送信トラフィックを監視します。
- both 送受信両方のトラフィック(双方向) を監視します。

キューは、番号または名前のどちらかによって識別されます。キュー名には、便宜上、複数の番号付けキューを組み入れることができます。

デフォルトの設定に戻すには、no キーワードを使用します。

次に、SPAN セッション 1 で、送信元インターフェイス FastEthernet 5/1 からの双方向トラフィックを監視するように設定する例を示します。

Switch(config) # monitor session 1 source interface fastethernet 5/1

次に、SPAN セッション内で送信元を異なる方向に設定する例を示します。

Switch(config)# monitor session 1 source interface fa2/3 rx
Switch(config)# monitor session 1 source interface fa2/2 tx
Switch(config)#

SPAN 宛先の設定

SPAN セッションの宛先を設定するには、次の作業を行います。

コマンド	目的
<pre>Switch(config)# [no] monitor session <session_number> destination interface <interface> [encapsulation {isl </interface></session_number></pre>	SPAN セッション番号(1 ~ 6)および宛先インターフェイスまたは VLAN を指定します。
<pre>dot1q}] [ingress [vlan vlan_IDs] [learning}]</pre>	$session_number$ には、この RSPAN セッションで識別されるセッション番号を指定します ($1 \sim 6$)。
	interface には、宛先インターフェイスを指定します。
	vlan_IDs には、宛先 VLAN を指定します。
	デフォルトの設定に戻すには、no キーワードを使用します。



SPAN 宛先ポートは1セッションにつき1つに制限されています。

次に、SPAN セッション 1 の宛先として、インターフェイス FastEthernet 5/48 を設定する例を示します。

Switch(config)# monitor session 1 destination interface fastethernet 5/48

トランク インターフェイス上の送信元 VLAN のモニタリング

SPAN 送信元がトランク インターフェイスである場合、特定の VLAN を監視するには、次の作業を行います。

コマンド	目的
<pre>Switch(config)# [no] monitor session {session_number} filter {vlan vlan_IDs [, -]} {packet-type {good bad}} {address-type {unicast multicast broadcast} [rx tx both]}</pre>	SPAN 送信元がトランク インターフェイスである 場合に、特定の VLAN を監視します。filter キー ワードで、指定された VLAN 上のトラフィックに モニタを限定します。これは通常、トランク イン ターフェイスを監視する場合に使用します。
	$session_number$ には、この RSPAN セッションで識別されるセッション番号を指定します ($1 \sim 6$)。
	vlan_IDs には、VLAN を指定します。
	指定された VLAN のすべてのポートを介したモニタが設定されます。
	デフォルトの設定に戻すには、no キーワードを使用します。

次に、SPAN 送信元がトランク インターフェイスである場合に、VLAN $1\sim5$ および 9 をモニタする例を示します。

 $\label{eq:switch} {\tt Switch(config)\,\#\,\,monitor\,\,session\,\,2\,\,\,filter\,\,vlan\,\,1\,\,-\,\,5\,\,\,,\,\,9}$

設定例

この章で説明したコマンドを使用して SPAN セッションを完全に設定する例、および設定を解除する例を示します。送信元インターフェイス FastEthernet 4/10 からの双方向トラフィックを監視すると想定します。このインターフェイスは、VLAN $1\sim4094$ を伝送するトランク インターフェイスとして設定されています。さらに、そのトランク上の VLAN 57 のトラフィックだけを監視するものとします。宛先インターフェイスとして FastEthernet 4/15 を使用し、次のコマンドを入力します。

```
Switch(config)# monitor session 1 source interface fastethernet 4/10
Switch(config)# monitor session 1 filter vlan 57
Switch(config)# monitor session 1 destination interface fastethernet 4/15
```

これで、VLAN 57 上のインターフェイス FastEthernet 4/10 からのトラフィックが、インターフェイス FastEthernet 4/15 で監視されます。SPAN セッションをディセーブルにする場合は、次のコマンドを入力します。

Switch(config) # no monitor session 1

SPAN の設定の確認

次に、SPAN セッション 2 の設定を確認する例を示します。

```
Switch# show monitor session 2
Session 2
Source Ports:
   RX Only:
                  Fa5/12
   TX Only:
                  None
   Both:
                  None
Source VLANs:
   RX Only:
                  None
   TX Only:
                  None
   Both:
                  None
Destination Ports: Fa5/45
Filter VLANs:
                 1-5.9
Switch#
```

CPU ポートのスニッフィング

SPAN セッションを設定する場合は、CPU(または CPU キューのサブセット)を SPAN 送信元として指定できます。キューは、番号または名前のどちらかで指定されます。このような送信元が指定されると、指定された 1 つのキューを介して CPU に送信されるトラフィックはミラーリングされ、セッションの SPAN 宛先ポートから送信されます。このトラフィックには、(ソフトウェア転送による) CPU で送受信される制御パケットと通常のデータ パケットの両方が含まれます。

CPU 送信元を通常のポート送信元または VLAN 送信元と組み合わせることができます。

CPU 送信元のスニッフィングを設定するには、次の作業を行います。

コマンド

Switch(config)# [no] monitor session {session_number} {source {interface} interface_list | {vlan vlan_IDs | cpu [queue queue_ids] } [rx | tx | both]

目的

CPU に送受信されたトラフィックを CPU がセッションの宛先にコピーするように指定します。 queue 識別子は、指定された CPU キューで受信されたスニッフィングだけのトラフィックを任意で許可します。

 $session_number$ には、この SPAN セッションで識別されるセッション番号を指定します(1 ~ 6)。

interface-list には、監視する送信元ポートを指定します。有効なインターフェイスには、物理インターフェイスとポート チャネル論理インターフェイス(port-channel port-channel-number) があります。

vlan_IDs には、送信元 VLAN を指定します。

queue_ids には、関連するキューを指定します。

(任意)[, | -] には、一連のまたは一定範囲のインターフェイスを指定します。カンマのあとにはスペースを入れます。ハイフンの前後にはスペースを1つ入れます。

(任意) 監視するトラフィックの方向を指定します。トラフィックの方向を指定しない場合、送信元インターフェイスは、送信(tx)と受信(rx)の両方のトラフィックを送信します。追加の送信元ポートは、受信トラフィックだけを監視します。

- rx 受信トラフィックを監視します。
- tx 送信トラフィックを監視します。
- both 送受信両方のトラフィック(双方向) をモニタします。

キューは、番号または名前のどちらかによって識別されます。キュー名には、便宜上、複数の番号付けキューを組み入れることができます。

デフォルトの設定に戻すには、no キーワードを使用します。

次に、CPU によって受信されたすべてのパケットをスニッフィングする CPU 送信元を設定する例を示します。

Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z. Switch(config) # monitor session 1 source cpu rx

次に、Supervisor Engine 2+ から V 10-GE で、SPAN 送信元として CPU のキュー名およびキュー番号 の範囲を使用する例を示します。

次に、Supervisor Engine 6-E で SPAN 送信元として CPU のキュー名およびキュー番号の範囲を使用する例を示します。

```
Switch(config)# monitor session 2 source cpu queue control-packet rx Switch(config)# monitor session 3 source cpu queue 10 rx
```



Supervisor Engine 6-E の場合、 control-packet はキュー 10 にマップされます。

カプセル化の設定

SPAN 宛先ポートを設定する場合、ポートで使用するカプセル化タイプを明示的に指定できます。ポートに送信されるパケットは、指定されたモードに基づいてタグ付けされます(また、入力パケット オプションがイネーブルにされている場合、カプセル化モードは、タグ付けされたパケットが処理される方法を制御します)。Catalyst 4500 シリーズ スイッチのスーパーバイザ エンジンは、ISL カプセル化、802.1Q カプセル化、およびタグなしパケットをサポートしています。



Superviso Engine 6-E は、802.1q カプセル化のみをサポートします。

「複製」カプセル化タイプはサポートされていません(このタイプでは、元のパケットに適用されたカプセル化を使用してパケットが宛先ポートから送信されます)。カプセル化モードが指定されていない場合、ポートのデフォルトはタグなしです。カプセル化設定の動作については、下記のコマンドの表を参照してください。

入力パケット

入力がイネーブルにされている場合、SPAN 宛先ポートは(指定されたカプセル化モードによって タグ付けされている可能性のある)着信パケットを受け入れ、通常どおりスイッチングします。 SPAN 宛先ポートを設定する場合、入力機能がイネーブルにされているか否か、およびタグなし入 カパケットをスイッチングするのに使用する VLAN について指定できます(すべての ISL カプセル 化パケットに VLAN タグが付加されている場合は、入力 VLAN を指定する必要がありません)。ポートは STP フォワーディング ステートですが、 STP には参加しないため、スパニングツリー ループ がネットワークに生じないように、この機能を設定する場合は注意してください。入力およびトランク カプセル化の両方が SPAN 宛先ポート上で指定されている場合、すべてのアクティブ VLANでポートが転送を行います。存在しない VLAN を入力 VLAN として設定することはできません。

デフォルトでは、ホスト学習は入力がイネーブルに設定された SPAN 宛先ポート上でディセーブルに設定されています。また、このポートは VLAN のフラッディング セットから削除されるので、通常のトラフィックは宛先ポートからスイッチングされません。ただし、学習がイネーブルに設定されている場合は、宛先ポート上で学習されたホストのトラフィックが宛先ポートからスイッチングされます。SPAN 宛先ポートに接続されているホストは、ブロードキャスト ARP 要求を受信しないため、応答しません。また、SPAN 宛先ポート上にスタティック ホスト エントリ(スタティックARP エントリおよび MAC アドレス テーブルのスタティック エントリを含む)を設定することもできます。



(注)

設定は、SPAN セッションに送信元が設定されていない場合は機能しません。このセッションは、SPAN 宛先ポートだけでは、半分しか設定されていないことになります。

入力パケットとカプセル化を設定するには、次の作業を行います。

コマンド	目的
<pre>Switch(config)# [no] monitor session <session_number> destination interface <interface> [encapsulation {isl dotlq}] [ingress [vlan vlan_IDs] [learning]]</interface></session_number></pre>	入力パケットの設定と宛先ポートのカプセル化タ イプを指定します。 ◆
	(注) isl キーワードは、Supervisor Engine 6-E ではサポート されません。 session_number には、この SPAN セッションで識別されるセッション番号を指定します (1 ~ 6)。
	interface には、宛先インターフェイスを指定します。 vlan_IDs には、宛先 VLAN を指定します。
	デフォルトの設定に戻すには、no キーワードを使用します。

次に、ネイティブ VLAN 7 を使用して、宛先ポートに 802.1Q カプセル化と入力パケットを設定する例を示します。

Switch(config) # monitor session 1 destination interface fastethernet 5/48 encapsulation dot1q ingress vlan 7

この設定では、セッション 1 に対応付けられた SPAN 送信元からのトラフィックは、802.1Q カプセル化を使用して、インターフェイス FastEthernet 5/48 からコピーされます。着信トラフィックは、タグなしパケットが VLAN 7 に分類されてから、受け入れられてスイッチングされます。

アクセス リスト フィルタリング

SPAN セッションを設定する場合、アクセス リスト フィルタリングを適用できます。アクセス リスト フィルタリングは、出力方向または入力方向でスニッフィングされた SPAN 宛先ポートを通過するすべてのパケットに適用されます。アクセス リスト フィルタは、ローカル SPAN セッションでのみ許可されます。SPAN の宛先が RSPAN VLAN である場合、アクセス リスト フィルタは拒否されます。



アクセス リスト フィルタリングは、Cisco IOS Release 12.2(20)EW 以降で使用できます。

ACL 設定時の注意事項

SPAN セッション上で ACL を設定できます。ACL/SPAN セッションでは、次の注意事項に従ってください。

- ACL が SPAN セッションに関連付けられている場合、ACL に関連付けられるルールは、SPAN 宛先インターフェイスに存在するすべてのパケットに対して適用されます。それまで SPAN 宛 先インターフェイスに関連付けられていた他の VACL または RACL に関連するルールは、適用されません。
- SPAN セッションに関連付けできる ACL は1つだけです。
- SPAN 宛先インターフェイスに存在するパケットに ACL が適用されていない場合、それまで宛 先インターフェイスまたは SPAN 宛先インターフェイスが所属する VLAN に適用されていた PACL、VACL、または RACL に関係なく、すべてのトラフィックが許可されます。
- ACL が SPAN セッションから削除されると、すべてのトラフィックが再び許可されます。
- SPAN セッションから SPAN 設定が削除されると、SPAN 宛先インターフェイスに関連付けられたすべてのルールが、再び適用されます。
- SPAN 宛先ポートが、トランクポートとして設定され、所属する VLAN に関連付けられた ACL が設定されている場合、トラフィックは VACL の対象となりません。
- ACL 設定は通常、RSPAN VLAN、および RSPAN VLAN を伝送するトランク ポートに適用されます。この設定により、ユーザは RSPAN VLAN 上の VACL を適用できるようになります。 ユーザが、宛先ポートを RSPAN VLAN として、SPAN セッション上で ACL の設定を試みる場合、この設定は拒否されます。
- CAM(連想メモリ)が過負荷状態で、パケットが検索のために CPU に引き渡される場合、SPAN セッションに関連付けられた出力ポートの ACL はいずれも、適用されません。
- ACL が作成される前に、名前つき IP ACL が SPAN セッション上で設定される場合、この設定は受け入れられ、ソフトウェアは Access Control Entry (ACE; アクセス コントロール エントリ)なしで空の ACL を作成します (空の ACL は、すべてのパケットを許可します)。その後、ACLにルールを追加できます。
- SPAN セッションに関連付けられた ACL は、出力宛先インターフェイス上で適用されます。
- SPAN ポートに存在するトラフィックでは、ポリシングが許可されません。
- SPAN セッションでは、IP ACL のみがサポートされます。

アクセス リスト フィルタリングの設定

アクセス リスト フィルタリングを設定するには、次の作業を行います。

コマンド	目的
Switch(config)# [no] monitor session {session_number} filter {ip access-group [name id] }{vlan}	アクセス リストに基づいて、フィルタ スニッフィ ングを指定します。
<pre>vlan_IDs [, -] } {packet-type {good bad}} {address-type {unicast multicast broadcast} [rx tx </pre>	session_number には、この SPAN セッションで識別されるセッション番号を指定します(1 ~ 6)。
both]}	アクセス リストには、名前または数値の ID のいずれかを指定できます。
	name には、IP アクセス リスト名を指定します。
	id には、標準の <1 ~ 199> または拡張の <1300 ~ 2699> の IP アクセス リストを指定します。



IP アクセス リストは、コンフィギュレーション モードで作成される必要があります(第 33 章「ACL によるネットワークセキュリティの設定」を参照)。

次に、SPAN セッション上で IP アクセス グループ 10 を設定し、アクセス リストが設定されたこと を確認する例を示します。

```
Switch# configure terminal
```

```
Enter configuration commands, one per line. End with {\tt CNTL/Z.}
Switch(config) # monitor session 1 source interface fa6/1 both
Switch(config) # monitor session 1 destination interface fa6/2
{\tt Switch(config)\#\ monitor\ session\ 1\ filter\ vlan\ 1}
Switch(config) # monitor session 1 filter ip access-group 10
Switch(config)# exit
Switch# show monitor
Session 1
Type
                  : Local Session
Source Ports
  Both
                 : Fa6/1
Destination Ports : Fa6/2
   Encapsulation : Native
         Ingress : Disabled
         Learning : Disabled
Filter VLANs
                 : 1
IP Access-group : 10
```

パケット タイプ フィルタリング

SPAN セッションを設定する場合、VLAN フィルタに類似したパケット フィルタ パラメータを指定できます。パケット フィルタを指定した場合、パケット フィルタはスニッフィングされるパケットのタイプを表示します。パケット フィルタが指定されていない場合、すべてのタイプのパケットがスニッフィングされます。別のタイプのパケット フィルタが入力および出力トラフィックに指定される場合もあります。

パケット フィルタリングは、パケットベース (good、error) またはアドレスベース (unicast/multicast/broadcast) の 2 つのカテゴリに分類されます。パケットベースのフィルタは、入 カ方向だけに適用できます。パケットは、宛先アドレスに基づいたハードウェアによって、ブロードキャスト、マルチキャスト、またはユニキャストに分類されます。



両方のタイプのフィルタが設定されると、両方のフィルタを通過するパケットだけがスパニングされます。たとえば、[error] および [multicast] の両方を設定すると、エラーのあるマルチキャスト パケットだけがスパニングされます。

パケットタイプフィルタリングを設定するには、次の作業を行います。

コマンド	目的
Switch(config)# [no] monitor session {session_number} filter {vlan vlan_IDs [, -] } {packet-type {good bad}}}	指定された方向による指定されたパケット タイプ のフィルタ スニッフィングを指定します。
{address-type {unicast multicast broadcast} [rx tx both]}	session_number には、この SPAN セッションで識別されるセッション番号を指定します(1 ~ 6)。
	vlan_IDs には、VLAN を指定します。
	rx とtx タイプの両方のフィルタ設定をすると同時に、複数のタイプのフィルタを設定できます(たとえば、good と unicast を設定して、エラーがないユニキャスト フレームだけをスニッフィングします)。VLAN フィルタでは、タイプまたはフィルタが指定されていない場合、すべてのパケットタイプがスニッフィングされます。
	デフォルトの設定に戻すには、no キーワードを使用します。

次に、入力方向のユニキャスト パケットだけを受け入れるようにセッションを設定する例を示します。

Switch(config) # monitor session 1 filter address-type unicast rx

RX Only

: Unicast

設定例

次に、SPAN 拡張機能の一部を使用した SPAN の設定例を示します。

次の例では、インターフェイス Gi1/1 上に着信するユニキャスト トラフィックをスニッフィングするようにセッションを設定します。トラフィックは、ISL カプセル化を使用して、インターフェイス Gi1/2 からミラーリングされます。入力トラフィックが許可されます。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config) # monitor session 1 source interface gil/1 rx
Switch(config) # monitor session 1 destination interface gi1/2 encapsulation is1
ingress
{\tt Switch(config)\,\#\,\,monitor\,\,session\,\,1\,\,filter\,\,address-type\,\,unicast\,\,rx}
Switch(config)# exit
Switch# show monitor
Session 1
Type
                  : Local Session
               :
: Gi1/1
Source Ports
  RX Only
Destination Ports : Gi1/2
   Encapsulation : ISL
         Ingress : Enabled
         Learning : Disabled
Filter Addr Type :
```

RSPAN の設定



(注)

この機能は、Supervisor Engine 6-E ではサポートされていません。

ここでは、スイッチ上で RSPAN を設定する手順について説明します。具体的な設定情報は次のとおりです。

- RSPAN 設定時の注意事項 (p.45-20)
- RSPAN セッションの作成 (p.45-21)
- RSPAN 宛先セッションの作成 (p.45-23)
- RSPAN 宛先セッションの作成および入力トラフィックのイネーブル化 (p.45-24)
- RSPAN セッションからのポートの削除 (p.45-25)
- 監視する VLAN の指定 (p.45-26)
- フィルタリングする VLAN の指定 (p.45-28)

RSPAN 設定時の注意事項

RSPAN の設定時には、次の注意事項に従ってください。



(注)

RSPAN VLAN には特殊なプロパティがあるので、RSPAN VLAN として使用する VLAN をネット ワーク上に一部確保します。これらの VLAN にはアクセス ポートを割り当てないでください。



(注)

RSPAN トラフィックに出力 ACL を適用して、特定のパケットを選択的にフィルタリングまたはモニタできます。 これらの ACL は、RSPAN 送信元スイッチ内の RSPAN VLAN 上で指定します。

- RSPAN セッションは、「SPAN と RSPAN のセッション限度」(p.45-6) に記載された限度内であれば、SPAN セッションと共存できます。
- RSPAN の設定では、送信元ポートと宛先ポートをネットワーク内の複数のスイッチに分散させることができます。
- RSPAN は、BPDU パケット モニタリングまたはその他のレイヤ2 スイッチ プロトコルをサポートしていません。
- RSPAN VLAN はトランク ポート上にのみ設定されており、アクセス ポート上には設定されて いません。不要なトラフィックが RSPAN VLAN に発生するのを防ぐため、参加しているすべ てのスイッチで RSPAN VLAN 機能がサポートされていることを確認してください。RSPAN VLAN 上のアクセス ポートは自動的にディセーブルになります。
- RSPAN VLAN を作成してから、RSPAN 送信元または宛先セッションを設定します。
- VTP および VTP プルーニングがイネーブルの場合、RSPAN トラフィックはトランクでプルーニングされ、ネットワーク上で 1005 未満の VLAN ID が RSPAN トラフィックの不要なフラッディングを防止できます。
- RSPAN トラフィックは RSPAN VLAN のネットワーク上で伝送されるため、ミラーリングされたパケットの元の VLAN アソシエーションは失われます。したがって、RSPAN では、IDS デバイスからユーザが指定した単一 VLAN へのトラフィック転送のみをサポートしています。

RSPAN セッションの作成

最初に、RSPAN に参加させる予定のスイッチのいずれにおいても、RSPAN セッション用として存在していない RSPAN VLAN を作成します。ネットワークで VTP がイネーブルになっている場合、1 つのスイッチで RSPAN VLAN を作成して、VTP がその RSPAN VLAN を、VLAN ID が 1005 未満の、VTP ドメイン内の他のスイッチに伝播させることができます。

VTP プルーニングを使用して、RSPAN トラフィックのフローを効率化するか、または RSPAN トラフィックを伝送する必要のないすべてのトランクから、RSPAN VLAN を手動で削除します。

RSPAN 送信元セッションを開始し、送信元(モニタ対象)ポートおよび宛先 RSPAN VLAN を指定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config) # no monitor session { session_number all local remote}	セッションの既存の RSPAN 設定をクリアします。
		$session_number$ には、この RSPAN セッションで識別されるセッション番号を指定します($1\sim6$)。
		すべての RSPAN セッションを削除するには all を、すべてのローカル セッションを削除するには local を、すべてのリモート SPAN セッションを削除するには remote を指定します。
ステップ 3	<pre>Switch(config)# vlan {remote_vlan_ID}</pre>	リモート VLAN ID を指定します。 この VLAN ID がユーザ トラフィックで使用されていない ことを確認してください。
ステップ 4	Switch(config-vlan)# remote-span	VLAN ID をリモート VLAN ID に変換します。
ステップ 5	Switch(config-vlan)# exit	グローバル コンフィギュレーション モードに戻ります。

	コマンド	目的
Switch(config)# [no] monitor session {session_number} {source {interface <interface_list> {vlan vlan_IDs cpu [queue queue_ids]} [rx tx both]</interface_list>	RSPAN セッションおよび送信元ポート(モニタ対象ポート)を指定します。 session_number には、この RSPAN セッションで識別される セッション番号を指定します($1 \sim 6$)。	
		interface-list には、監視する送信元ポートを指定します。有効なインターフェイスには、物理インターフェイスとポート チャネル論理インターフェイス (port-channel port-channel-number) があります。
		$vlan ext{-}IDs$ には、 1 つまたは複数のモニタ対象送信元 VLAN を指定します。有効な VLAN の範囲は、 $1\sim4094$ です。
		<i>queue_ids</i> には、一連の CPU キュー識別番号 (1 ~ 32) または名前指定のキューのどちらかを指定します。
		(任意)[, -] には、一連のまたは一定範囲のインターフェイスを指定します。カンマのあとにはスペースを入れます。 ハイフンの前後にはスペースを 1 つ入れます。
		(任意)監視するトラフィックの方向を指定します。トラフィックの方向を指定しない場合、送信元インターフェイスは、送信(tx)と受信(rx)の両方のトラフィックを送信します。追加の送信元ポートは、受信トラフィックだけをモニタします。
		• rx 受信トラフィックを監視します。
		tx 送信トラフィックを監視します。both 送受信両方のトラフィック(双方向)をモニタします。
ステップ 7	Switch(config)# monitor session session_number destination remote vlan vlan-ID	RSPAN セッションと宛先リモート VLAN を指定します。 session_number には、この RSPAN セッションで識別される セッション番号を指定します (1 ~ 6)。
		<i>vlan-ID</i> には、モニタ対象トラフィックを宛先ポートに伝送 する RSPAN VLAN を指定します。
ステップ 8	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 9	Switch# show monitor [session session_number]	入力を確認します。
ステップ 10	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

次に、セッション 1 の既存の RSPAN 設定をクリアし、複数の送信元インターフェイスをモニタする RSPAN セッション 1 を設定し、宛先 RSPAN VLAN を設定する例を示します。

```
Switch# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.

Switch(config) # no monitor session 1

Switch(config) # monitor session 1 source interface fastEthernet3/10 tx

Switch(config) # monitor session 1 source interface fastEthernet3/2 rx

Switch(config) # monitor session 1 source interface fastEthernet3/3 rx

Switch(config) # monitor session 1 source interface port-channel 102 rx

Switch(config) # monitor session 1 destination remote vlan 901

Switch(config) # end
```

RSPAN 宛先セッションの作成

RSPAN 宛先セッションを作成し、送信元 RSPAN VLAN および宛先ポートを指定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# monitor session session_number source remote vlan	RSPAN セッションと送信元 RSPAN VLAN を指定します。
	vlan-ID	session_number には、この RSPAN セッションで識別される セッション番号を指定します ($1 \sim 6$)。
		<i>vlan-IDs</i> には、監視する送信元 RSPAN VLAN を指定します。
ステップ 3	Switch(config) # [no] monitor session <session_number> destination interface</session_number>	RSPAN セッションと宛先インターフェイスを指定します。
	<pre><interface> [encapsulation {isl dot1q}] [ingress [vlan vlan_IDs] [learning]]</interface></pre>	$session_number$ には、この RSPAN セッションで識別されるセッション番号を指定します(1 ~ 6)。
		interface には、宛先インターフェイスを指定します。
		vlan_IDs には、必要に応じて、入力 VLAN を指定します。
		(任意)[, -] には、一連のまたは一定範囲のインターフェイスを指定します。カンマのあとにはスペースを入れます。 ハイフンの前後にはスペースを1つ入れます。
		(任意)監視するトラフィックの方向を指定します。トラフィックの方向を指定しない場合、送信元インターフェイスは、送受信両方のトラフィックを送信します。追加の送信元ポートは、受信(rx)トラフィックだけを監視します。
		isl ISL カプセル化を使用します。dot1q 802.1Q カプセル化を使用します。
ステップ 4	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 5	Switch# show monitor [session session_number]	入力を確認します。
ステップ 6	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存し ます。

次に、VLAN 901 を送信元リモート VLAN に、ポート 5 を宛先インターフェイスに設定する例を示します。

Switch# configure terminal

Enter configuration commands, one per line. End with ${\tt CNTL/Z.}$

 ${\tt Switch(config)\#\ monitor\ session\ 1\ source\ remote\ vlan\ 901}$

Switch(config) # monitor session 1 destination interface gigabitEthernet1/2

Switch(config)# end

RSPAN 宛先セッションの作成および入力トラフィックのイネーブル化

RSPAN 宛先セッションを作成して、送信元 RSPAN VLAN を指定し、ネットワーク セキュリティデバイス (Cisco IDS センサー装置など) 用に宛先ポート上の入力トラフィックをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# monitor session {session_number} source vlan vlan_IDs	RSPAN セッションと送信元 RSPAN VLAN を指定します。
		$session_number$ には、この RSPAN セッションで識別されるセッション番号を指定します(1 \sim 6)。
		<i>vlan_IDs</i> には、1 つまたは複数のモニタ対象送信元 VLAN を指定します。有効な VLAN の範囲は、1 ~ 4094 です。
ステップ 3	Switch(config)# [monitor session session_number destination interface interface-id [encapsulation {dot1q	RSPAN セッション、宛先ポート、パケット カプセル化、および入力側 VLAN を指定します。
	<pre>[ingress vlan vlan id] ISL [ingress]} ingress vlan vlan id] [learning]]</pre>	$session_number$ には、この RSPAN セッションで識別されるセッション番号を指定します($1 \sim 6$)。
		interface-id には、宛先ポートを指定します。有効なインターフェイスは物理インターフェイスなどです。
		(任意)RSPAN 宛先ポート上で送信されるパケットのカプセル化を指定します。カプセル化タイプが指定されていない場合、すべての送信パケットはネイティブ形式(タグなし)で送信されます。
		 タグなしのネイティブ VLAN パケットと、他のすべての dot1q タグ付き VLAN tx パケットを送信する場合は、encapsulation dot1q と入力します。
		• ISL を使用してカプセル化されたすべての tx パケット を送信する場合は、encapsulation isl を入力します。
		(任意)RSPAN 宛先ポート上で入力トラフィックの転送を イネーブルにするか否かを指定します。
		• ネイティブ(タグなし)および dot1q カプセル化の場合、ingress vlan vlan id を指定し、vlan id をネイティブ VLAN として入力転送をイネーブルにします。また、vlan id は、送信パケット用のネイティブ VLAN としても使用されます。
		• ISL カプセル化を使用する場合、ingress を指定して入 力転送をイネーブルにします。
		• 入力がイネーブルの場合、learning を指定して学習を イネーブルにします。
ステップ 4	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 5	Switch# show monitor [session session_number]	入力を確認します。
ステップ 6	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

次に、送信元リモート VLAN として VLAN 901 を設定し、802.1Q カプセル化をサポートするセキュリティ デバイスを使用して VLAN 5 上の入力トラフィック用の宛先ポートを設定する例を示します。

Switch# configure terminal

Enter configuration commands, one per line. End with $\mathtt{CNTL}/\mathtt{Z}\text{.}$

Switch(config)# monitor session 1 source remote vlan 901

 ${\tt Switch}(\texttt{config}) \ \# \ \textbf{monitor session 1 destination interface gigabitEthernet1/2 ingress}$

vlan 5

Switch(config)# end

RSPAN セッションからのポートの削除

セッションの RSPAN 送信元としてのポートを削除するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
{	Switch(config) # [no] monitor session {session_number} {source {interface interface_list {vlan_vlan_IDs cpu	削除する RSPAN 送信元ポート(モニタ対象ポート)の特性を指定します。
	[queue queue_ids]} [rx tx both]	$session_number$ には、この RSPAN セッションで識別されるセッション番号を指定します($1\sim6$)。
	interface-list には、モニタを中止する送信元ポートを指定します。 有効なインターフェイスには、物理インターフェイスとポートチャネル論理インターフェイス (port-channel port-channel-number) があります。	
		vlan_IDsには、1 つまたは複数のモニタ対象送信元 VLANを指定します。有効な VLAN の範囲は、1 ~ 4094 です。
		$queue_ids$ には、一連の CPU キュー識別番号 $(1 \sim 32)$ または名前指定のキューのどちらかを指定します。
		(任意)[, -] には、一連のまたは一定範囲のインターフェイスを指定します。カンマのあとにはスペースを入れます。 ハイフンの前後にはスペースを1つ入れます。
		(任意)監視するトラフィックの方向を指定します。トラフィックの方向を指定しない場合、送信元インターフェイスは、送信(tx)と受信(rx)の両方のトラフィックを送信します。追加の送信元ポートは、受信トラフィックだけをモニタします。
		• rx 受信トラフィックを監視します。
		• tx 送信トラフィックを監視します。
		• both 送受信両方のトラフィック(双方向)をモニタ します。
ステップ 3	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 4	Switch# show monitor [session session_number]	入力を確認します。
ステップ 5	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

次に、RSPAN セッション 1 の RSPAN 送信元としてのポート 1 を削除する例を示します。

Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config) # no monitor session 1 source interface gigabitEthernet1/1
Switch(config) # end

次に、双方向モニタ用に設定されたポート 1 上での受信トラフィック モニタをディセーブルにする 例を示します。

 ${\tt Switch(config)\#\ no\ monitor\ session\ 1\ source\ interface\ gigabitEthernet1/1\ rx}$

ポート 1 上での受信トラフィックのモニタはディセーブルになりますが、このポートから送信されたトラフィックは引き続きモニタされます。

監視する VLAN の指定

VLAN のモニタは、ポートのモニタと類似しています。監視する VLAN を指定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# no monitor session {session_number all local remote}	セッションの既存の SPAN 設定をすべてクリアします。
		$session_number$ には、この RSPAN セッションで識別されるセッション番号を指定します($1 \sim 6$)。
		すべての SPAN セッションを削除するには all を、すべての ローカル セッションを削除するには local を、すべての RSPAN セッションを削除するには remote を指定します。

	コマンド	目的
ステップ 3	Switch(config)# [no] monitor session {session_number} {source {interface interface_list {vlan vlan_IDs cpu [queue queue_ids]} [rx tx both]	RSPAN セッションおよび送信元 VLAN(モニタ対象ポート)を指定します。監視できるのは、VLAN 上の受信(rx)トラフィックだけです session_number には、この RSPAN セッションで識別される セッション番号を指定します(1 ~ 6)。
		interface-list には、モニタを中止する送信元ポートを指定します。有効なインターフェイスには、物理インターフェイスとポートチャネル論理インターフェイス(port-channel port-channel-number)があります。
		vlan-IDs の範囲は 1 ~ 4094 です。先行 0 は入力しないでください。
		queue_ids には、送信元キューを指定します。
		(任意)[, -] には、一連のまたは一定範囲のインターフェイスを指定します。カンマのあとにはスペースを入れます。 ハイフンの前後にはスペースを 1 つ入れます。
		(任意)監視するトラフィックの方向を指定します。トラフィックの方向を指定しない場合、送信元インターフェイスは、送信(tx)と受信(rx)の両方のトラフィックを送信します。追加の送信元ポートは、受信トラフィックだけをモニタします。
		• rx 受信トラフィックを監視します。
		• tx 送信トラフィックを監視します。
		both 送受信両方のトラフィック(双方向)を監視します。
ステップ 4	Switch(config)# monitor session	RSPAN セッションと宛先リモート VLAN を指定します。
	session_number destination remote vlan vlan-id	$session_number$ には、この RSPAN セッションで識別されるセッション番号を指定します(1 ~ 6)。
		<i>vlan-id</i> には、モニタ対象トラフィックを宛先ポートに伝送 する RSPAN VLAN を指定します。
ステップ 5	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 6	Switch# show monitor [session session_number]	入力を確認します。
ステップ 7	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

RSPAN セッションから 1 つまたは複数の送信元 VLAN を削除するには、no monitor session session_number source vlan vlan-id rx グローバル コンフィギュレーション コマンドを使用します。

次に、RSPAN セッション 2 の既存の設定をすべてクリアし、VLAN 1 ~ 3 に所属するすべてのポート上で受信トラフィックを監視する RSPAN セッション 2 を設定し、宛先リモート VLAN 902 に送信する例を示します。この設定は次に、VLAN 10 に所属するすべてのポートで受信トラフィックを監視するように変更されています。

Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)# no monitor session 2

Switch(config)# monitor session 2 source vlan 1 - 3 rx

Switch(config) # monitor session 2 destination remote vlan 902

Switch(config)# monitor session 2 source vlan 10 rx

Switch(config)# end

フィルタリングする VLAN の指定

RSPAN 送信元トラフィックを特定の VLAN に制限するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config) # no monitor session {session_number all local remote}	セッションの既存の SPAN 設定をすべてクリアします。 $session_number$ には、この RSPAN セッションで識別されるセッション番号を指定します (1 ~ 6)。
		すべての SPAN セッションを削除するには all を、すべてのローカル セッションを削除するには local を、すべてのRSPAN セッションを削除するには remote を指定します。
ステップ 3	Switch(config) # [no] monitor session {session_number} {source {interface interface_list {vlan vlan_IDs cpu [queue queue_ids]} [rx tx both]	送信元ポート(モニタ対象ポート)と RSPAN セッション の特性を指定します。
		$session_number$ には、この RSPAN セッションで識別されるセッション番号を指定します(1 ~ 6)。
		interface-list には、監視する送信元ポートを指定します。指定されたインターフェイスは、常にトランク ポートとして設定されている必要があります。
		vlan-IDs の範囲は 1 ~ 4094 です。先行 0 は入力しないでく ださい。
		queue_ids には、送信元キューを指定します。
		(任意)[, -] には、一連のまたは一定範囲のインターフェイスを指定します。カンマのあとにはスペースを入れます。 ハイフンの前後にはスペースを 1 つ入れます。
		(任意)監視するトラフィックの方向を指定します。トラフィックの方向を指定しない場合、送信元インターフェイスは、送信(tx)と受信(rx)の両方のトラフィックを送信します。追加の送信元ポートは、受信トラフィックだけを監視します。
		• rx 受信トラフィックを監視します。
		tx 送信トラフィックを監視します。both 送受信両方のトラフィック(双方向)を監視し
		ます。

	コマンド	目的
ステップ 4	Switch(config)# monitor session session_number filter vlan vlan-id [,	RSPAN 送信元トラフィックを特定の VLAN に制限します。
	-]	$session_number$ には、この RSPAN セッションで識別されるセッション番号を指定します($1\sim6$)。
		vlan-id の範囲は 1 ~ 4094 です。先行 0 は入力しないでください。
		(任意)カンマ(,)を使用して一連の VLAN を指定するか、 ハイフン(-)を使用して一定範囲の VLAN を指定します。 カンマのあとにはスペースを入れます。ハイフンの前後に はスペースを I つ入れます。
ステップ 5	Switch(config)# monitor session session_number destination remote vlan	RSPAN セッションと宛先リモート VLAN を指定します。
	vlan-id	$session_number$ には、この RSPAN セッションで識別されるセッション番号を指定します($1\sim6$)。
		vlan-id には、モニタ対象トラフィックを宛先ポートに伝送 する RSPAN VLAN を指定します。
ステップ 6	Switch(config)# end	特権 EXEC モードに戻ります。
ステップァ	Switch# show monitor [session session_number]	入力を確認します。
ステップ 8	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

トランク ポート上のすべての VLAN を監視するには、**no monitor session** session_number **filter vlan** グローバル コンフィギュレーション コマンドを使用します。

次に、RSPAN セッション 2 の既存の設定をすべてクリアし、トランク ポート 4 上での受信したトラフィックを監視する RSPAN セッション 2 を設定し、VLAN 1 ~ 5 および 9 のトラフィックのみを、宛先リモート VLAN 902 に送信する例を示します。

Switch# configure terminal

```
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source interface gigabitethernet1/1 rx
Switch(config)# monitor session 2 filter vlan 1 - 5 , 9
Switch(config)# monitor session 2 destination remote vlan 902
Switch(config)# end
```

SPAN および RSPAN ステータスの表示

現在の SPAN または RSPAN 設定のステータスを表示するには、show monitor 特権 EXEC コマンドを使用します。

次に、SPAN 送信元セッション 1 の show monitor コマンドの出力例を示します。

```
Switch# show monitor session 1
Session 1
Type: Local Source Session
Source Ports:
   RX Only:
                 Fa3/13
   TX Only:
                None
   Both:
Source VLANs:
   RX Only:
                None
   TX Only:
                 None
   Both:
                  None
Source RSPAN VLAN: None
Destination Ports: None
   Encapsulation: DOT1Q
              Enabled, default VLAN=5
   Ingress:
Filter VLANs:
                 None
Dest RSPAN VLAN: None
Ingress: Enabled, default VLAN=2
Learning : Disabled
```



CHAPTER

46

システム メッセージ ロギングの設定

この章では、Catalyst 4500 シリーズ スイッチにシステム メッセージ ロギングを設定する方法を説明します。



ここで使用するコマンドの構文および使用方法の詳細については、次の URL にある『Cisco IOS Configuration Fundamentals Command Reference』Release 12.4 を参照してください。

 $http://www.cisco.com/univered/cc/td/doc/product/software/ios124/124tcr/tcf_r/index.htm$

この章の内容は、次のとおりです。

- システム メッセージ ロギングの概要 (p.46-2)
- システム メッセージ ロギングの設定 (p.46-3)
- ロギング設定の表示 (p.46-13)

システム メッセージ ロギングの概要

デフォルトでは、システムはシステム メッセージと debug 特権 EXEC コマンドの出力をロギング プロセスに送ります。ロギング プロセスは、ロギング バッファ、端末回線、UNIX Syslog サーバな ど、構成に応じたさまざまな宛先へのロギング メッセージの配信を制御します。 プロセスはコンソールにもメッセージを送信します。



Syslog は 4.3 BSD UNIX 互換形式です。

ロギング プロセスがディセーブルの場合、メッセージはコンソールだけに送信されます。メッセージは生成と同時に送信されるので、メッセージとデバッグ出力は、プロンプトや他のコマンドの出力に紛れ込んでいます。メッセージは、そのメッセージの生成プロセスが終了するとコンソールに表示されます。

メッセージの重大度を設定すると、コンソールとそれぞれの宛先に表示されるメッセージの種類を制御できます。ログ メッセージにタイムスタンプを設定したり、リアルタイム デバッギングおよび管理を強化するために Syslog 送信元アドレスを設定したりできます。表示される可能性があるメッセージについては、このリリースのシステム メッセージ ガイドを参照してください。

記録されたシステム メッセージにアクセスするには、スイッチの CLI (コマンドライン インターフェイス)を使用するか、正しく設定された Syslog サーバに保存します。スイッチ ソフトウェアは、syslog メッセージをスイッチの内部バッファに保存します。スイッチに障害が発生した場合、フラッシュ メモリに保存していないかぎり、ログは失われます。

Syslog サーバのログを確認するか、Telnet またはコンソール ポート経由でスイッチにアクセスすれば、システム メッセージをリモートでモニタできます。

システム メッセージ ロギングの設定

ここでは、システム メッセージ ロギングの設定方法を説明します。

- システム ログ メッセージの形式 (p.46-3)
- システム メッセージ ロギングのデフォルト設定 (p.46-4)
- メッセージ ロギングのディセーブル化 (p.46-4)(任意)
- メッセージ表示先装置の設定 (p.46-5)(任意)
- ログメッセージの同期化 (p.46-6)(任意)
- ログ メッセージのタイムスタンプのイネーブル化およびディセーブル化 (p.46-8)(任意)
- ログメッセージのシーケンス番号のイネーブル化およびディセーブル化(p.46-8)(任意)
- メッセージの重大度の定義 (p.46-9)(任意)
- 履歴テーブルおよび SNMP への Syslog メッセージの送信制限 (p.46-10)(任意)
- UNIX Syslog サーバの設定 (p.46-11)(任意)

システム ログ メッセージの形式

システム ログ メッセージには最大 80 文字とパーセント記号 (%)を1つ含めることができ、任意でシーケンス番号またはタイムスタンプ情報(設定されている場合)を続けることもできます。メッセージの表示形式は次のとおりです。

seq no:timestamp: %facility-severity-MNEMONIC:description

パーセント記号よりも前の部分のメッセージは、service sequence-numbers、service timestamps log datetime、service timestamps log datetime [localtime] [msec] [show-timezone]、または service timestamps log uptime グローバル コンフィギュレーション コマンドの設定によって異なります。

表 46-1 で Syslog メッセージの要素を説明します。

表 46-1 システム ログ メッセージの要素

要素	説明
seq no:	service sequence-numbers グローバル コンフィギュレーション コマンドが設定されている場合、ログ メッセージにシーケンス番号を追加します。
	詳細については、「ログ メッセージのシーケンス番号のイネーブル化およびディセーブル化」(p.46-8)を参照してください。
timestamp の形式:	メッセージまたはイベントの日時。service timestamps log [datetime log] グローバル
mm/dd hh:mm:ss	コンフィギュレーション コマンドが設定されている場合にだけ表示されます。
または	詳細については、「ログ メッセージのタイムスタンプのイネーブル化およびディセーブル化」(p.46-8)を参照してください。
hh:mm:ss(短い動作期間)	
または	
d h (長い動作期間)	
facility	メッセージが関係するファシリティ (SNMP、SYS など)。サポートされるファシリティのリストは、表 $46-4$ ($p.46-13$) を参照してください。
severity	メッセージの重大度を表す 0 ~ 7 の 1 桁のコード。重大度については表 46-3(p.46-10) を参照してください。
MNEMONIC	メッセージを一意に表す文字列
description	レポートされるイベントの内容を説明する文字列

次に、スイッチ システム メッセージの例の一部を示します。

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/2, changed state to up
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1,
changed state to down 2

*Mar 1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
18:47:02: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)

*Mar 1 18:48:50.483 UTC: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

システム メッセージ ロギングのデフォルト設定

表 46-2 に、システム メッセージ ロギングのデフォルト設定を示します。

表 46-2 システム メッセージ ロギングのデフォルト設定

機能	デフォルト設定
コンソールへのシステム メッセージ ロギング	イネーブル
コンソールの重大度	デバッグ(および数値がさらに小さいレベル。
	表 46-3 [p.46-10] を参照)
ロギング ファイル設定	ファイル名は指定されていない
ロギング バッファ サイズ	4096 バイト
ロギング履歴サイズ	メッセージ 1 件
タイムスタンプ	ディセーブル
同期ロギング	ディセーブル
ログ収集サーバ	ディセーブル
Syslog サーバ IP アドレス	設定なし
サーバ ファシリティ	Local7 (表 46-4 [p.46-13] を参照)
サーバの重大度	情報(および数値がさらに小さいレベル。表 46-3
	[p.46-10] を参照)

メッセージ ロギングのディセーブル化

メッセージ ロギングはデフォルトでイネーブルです。コンソール以外の宛先にメッセージを送信する場合はイネーブルにしておく必要があります。 イネーブルの場合はログ メッセージがロギング プロセスに送られます。 ロギング プロセスでメッセージは、生成したプロセスとは非同期で、指定した場所に保存されます。

メッセージロギングをディセーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# no logging on	メッセージ ロギングをディセーブルにします。
ステップ 3	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 4	Switch# show running-config または show logging	入力を確認します。
ステップ 5	Switch# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存し ます。

ロギング プロセスをディセーブルにするとスイッチのパフォーマンスが低下します。メッセージが コンソールに書き込まれるのを待ってからプロセスを継続する必要があるからです。 ロギング プロセスがディセーブルになると、メッセージは作成されるとすぐにコンソールに表示され、コマンド出力の途中で表示されることが多くなります。

logging synchronous グローバル コンフィギュレーション コマンドも、コンソールでのメッセージ の表示に影響を与えます。このコマンドをイネーブルにすると、改行キーを押した場合にのみメッセージが表示されます。詳細については、「ログ メッセージの同期化」(p.46-6)を参照してください。

ディセーブルにしたメッセージ ロギングを再びイネーブルにするには、logging on グローバル コンフィギュレーション コマンドを使用します。

メッセージ表示先装置の設定

メッセージ ロギングがイネーブルの場合、コンソール以外にも指定した場所にメッセージを送信できます。

メッセージの受信先を指定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# logging buffered[size]	スイッチの内部バッファにメッセージを保存します。デフォルト バッファ サイズは 4096 で、範囲は 4096 ~ 2147483647 バイトです。 スイッチで障害が発生すると、あらかじめフラッシュ メモリに保存していないかぎりログ ファイルは失われます。ステップ 4 を参照してください。 (注) バッファサイズは大きくしすぎないようにします。スイッチが他の作業の分のメモリを使い果たしてしまう可能性があるからです。スイッチのプロセッサメモリの空き容量を表示するには、show memory 特権 EXEC コマンドを使用します。ただしこれは最大空き容量なので、バッファサイズをこの値に設定しないでください。
ステップ 3	Switch(config)# logging host	UNIX Syslog サーバ ホストにメッセージを保存します。 host には、Syslog サーバとして使用するホストの名前また
		は IP アドレスを指定します。
		ロギング メッセージを受信する Syslog サーバのリストを作成するには、このコマンドを複数回入力します。
		詳細な Syslog サーバの設定手順については、「UNIX Syslog サーバの設定」(p.46-11)を参照してください。
ステップ 4	Switch(config)# end	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 5	Switch# terminal monitor	現在のセッション間、非コンソール端末にメッセージを保存します。
		端末パラメータ設定コマンドはローカルに設定され、セッションが終了後は無効になります。デバッギング メッセージを表示するには、この手順を各セッションで実行する必要があります。
ステップ 6	Switch# show running-config	入力を確認します。
ステップ 7	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

logging buffered グローバル コンフィギュレーション コマンドは、ロギング メッセージを内部バッファにコピーします。バッファはサーキュラ方式なので、バッファが満杯になると新しいメッセージが古いメッセージを上書きします。バッファに保存されたメッセージを表示するには、show logging 特権 EXEC コマンドを使用します。最初に表示されるメッセージは、バッファで一番古いメッセージです。バッファの内容をクリアするには、clear logging 特権 EXEC コマンドを使用します。

コンソールへのロギングをディセーブルにするには、no logging console グローバル コンフィギュレーション コマンドを使用します。ファイルへのロギングをディセーブルにするには、no logging file [severity-level-number | type] グローバル コンフィギュレーション コマンドを使用します。

ログ メッセージの同期化

割り込みメッセージと debug 特権 EXEC コマンド出力を、特定のコンソール ポート回線または仮想端末回線の送信請求装置出力およびプロンプトと同期させることができます。非同期で出力するメッセージの種類を重大度に基づいて特定することができます。端末に非同期メッセージ保存するバッファの最大数を設定することもできます。最大数を超えたあとのメッセージはドロップされます。

割り込みメッセージと debug コマンド出力の同期ロギングがイネーブルの場合、送信請求装置出力が表示またはプリンタ出力されたあとに割り込み装置出力がコンソールに表示またはプリンタ出力されます。割り込みメッセージと debug コマンド出力は、ユーザ入力のプロンプトが戻ったあとにコンソールに表示されます。このため、割り込みメッセージと debug コマンド出力が送信請求装置出力およびプロンプトに紛れ込むことはありません。割り込みメッセージが表示されると、コンソールは再びユーザ プロンプトを表示します。

同期ロギングを設定にするには、次の作業を行います。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	line [console vty] line-number	メッセージの同期ロギングを設定する回線を指定します。
	[ending-line-number]	• スイッチ コンソール ポートで発生する設定の場合、 console キーワードを使用します。
		 同期ロギングをイネーブルにする VTY 回線を指定するには、line vty line-number コマンドを使用します。 Telnet セッションで発生する設定には VTY 接続を使用します。回線番号の範囲は 0 ~ 15 です。
		16 の VTY 回線全部の設定を変更するには、次のように入力します。
		line vty 0 15
		または、現在の接続で使用している 1 つの VTY 回線の設定 だけを変更することができます。たとえば、VTY 回線 2 を 変更する場合は次のように入力します。
		line vty 2
		このコマンドを入力するとライン コンフィギュレーション モードになります。
ステップ 3	logging synchronous [level [severity-level all] limit number-of-buffers]	メッセージの同期ロギングをイネーブルにします。
		• (任意) level severity-level には、メッセージの重大度を 指定します。この値以上の重大度のメッセージは同期 的にプリンタに出力されます。値が小さいほど重大度 が大きく、値が大きいほど重大度は小さくなります。 デフォルトは2です。
		• (任意) level all を指定すると、重大度にかかわらずす べてのメッセージがプリンタ出力されます。
		• (任意) limit number-of-buffers には、端末にキューイン グされるバッファ数を指定します。これ以降の新しい メッセージはドロップされます。指定できる範囲は 0 ~ 2147483647 です。デフォルトは 20 です。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	入力を確認します。
ステップ 6	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

割り込みメッセージとデバッグ出力の同期をディセーブルにするには、no logging synchronous [level severity-level | all] [limit number-of-buffers] ライン コンフィギュレーション コマンドを使用します。

ログ メッセージのタイムスタンプのイネーブル化およびディセーブル化



(注)

デフォルトでは、ログメッセージにはタイムスタンプは含まれません。

ログ メッセージのタイムスタンプをイネーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	service timestamps log uptime	ログのタイムスタンプをイネーブルにします。
	または service timestamps log datetime [msec] [localtime] [show-timezone]	最初のコマンドはログ メッセージのタイムスタンプをイネーブルにし、システムがリブートされてからの時間が示されます。
		2番めのコマンドはログ メッセージのタイムスタンプをイネーブルにします。指定したオプションによっては、タイムスタンプに日付、現地時間による時刻(ミリ秒) および時間帯の名前が含まれます。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	入力を確認します。
ステップ 5	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

デバッグおよびログ メッセージのタイムスタンプをディセーブルにするには、no service timestamps グローバル コンフィギュレーション コマンドを使用します。

次に、service timestamps log datetime グローバル コンフィギュレーション コマンドをイネーブルに した場合のロギング表示 (一部)の例を示します。

*Mar 1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)

次に、service timestamps log uptime グローバル コンフィギュレーション コマンドをイネーブルに した場合のロギング表示 (一部)の例を示します。

00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up

ログ メッセージのシーケンス番号のイネーブル化およびディセーブル化

複数のメッセージに同じタイムスタンプが表示される可能性があるので、シーケンス番号を使用してメッセージを表示することにより参照するメッセージを明確にすることができます。デフォルトでは、ログ メッセージのシーケンス番号は表示されません。

ログ メッセージのシーケンス番号をイネーブルにするには、次の作業を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	service sequence-numbers	シーケンス番号をイネーブルにします。
ステップ 3	end	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	show running-config	入力を確認します。
ステップ 5	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存し
		ます。

シーケンス番号をディセーブルにするには、no service sequence-numbers グローバル コンフィギュレーション コマンドを使用します。

次に、シーケンス番号をイネーブルにしてログ画面の一部を表示する例を示します。

000019: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)

メッセージの重大度の定義

メッセージの重大度を定義することによって、選択した装置に表示するメッセージを制限することができます (メッセージの重大度については表 46-3 を参照)。

メッセージの重大度を定義するには、次の作業を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	logging console level	コンソールに保存するメッセージを制限します。
		デフォルトでは、コンソールはデバッギング メッセージと、これよりも数値が小さいレベルのメッセージを受信します (表46-3 [p.46-10] を参照)。
ステップ 3	logging monitor level	端末回線に出力するメッセージを制限します。
		デフォルトでは、端末はデバッギング メッセージと、これよりも数値が小さいレベルのメッセージを受信します (表 46-3 [p.46-10] を参照)。
ステップ 4	logging trap level	Syslog サーバに保存するメッセージを制限します。
		デフォルトでは、Syslog サーバは情報メッセージと、これよりも数値が小さいレベルのメッセージを受信します (表 $46-3$ [p. $46-10$] を参照)。
		詳細な Syslog サーバの設定手順については、「UNIX Syslog サーバの設定」(p.46-11)を参照してください。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show running-config	入力を確認します。
	または	
	show logging	
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。



level を指定すると、この数値以下のレベルのメッセージが出力先に表示されます。

コンソールへのロギングをディセーブルにするには、no logging console グローバル コンフィギュレーション コマンドを使用します。コンソール以外の端末へのロギングをディセーブルにするには、no logging monitor グローバル コンフィギュレーション コマンドを使用します。Syslog サーバへのロギングをディセーブルにするには、no logging trap グローバル コンフィギュレーション コマンドを使用します。

表 46-3 では、level キーワードについて説明します。また、対応する UNIX Syslog 定義についても、重大度の順(最も大きい重大度から最も小さい重大度へ)に示します。

レベル キーワード	レベル	説明	Syslog 定義
emergencies	0	システムが不安定	LOG_EMERG
alerts	1	すぐに対応する必要あり	LOG_ALERT
critical	2	クリティカルな状態	LOG_CRIT
errors	3	エラー状態	LOG_ERR
varnings	4	警告状態	LOG_WARNING
otifications	5	正常だが重大な状態	LOG_NOTICE
nformational	6	情報メッセージのみ	LOG_INFO
ebugging	7	デバッグ メッセージ	LOG_DEBUG

表 46-3 メッセージ ログレベル キーワード

このほかにも、ソフトウェアには次の4つのメッセージカテゴリがあります。

- ソフトウェアまたはハードウェアの誤動作に関するエラー メッセージ。warnings から emergencies のレベルで表示されます。スイッチの機能が影響を受けることを意味します。この状態から回復する方法については、このリリースのシステム メッセージ ガイドを参照してください。
- **debug** コマンドの出力。 **debugging** レベルで表示されます。 通常、デバッグ コマンドは Technical Assistance Center (TAC) だけが使用します。
- インターフェイスのアップまたはダウン移行メッセージおよびシステム再起動メッセージ。 notifications レベルで表示されます。これは情報メッセージで、スイッチ機能に影響はありません。
- リロード要求および低プロセス スタック メッセージ。informational レベルで表示されます。これは情報メッセージで、スイッチ機能に影響はありません。

履歴テーブルおよび SNMP への Syslog メッセージの送信制限

snmp-server enable trap グローバル コンフィギュレーション コマンドを使用して、Syslog メッセージ トラップの SNMP ネットワーク管理ステーションへの送信をイネーブルにした場合、送信する メッセージやスイッチ履歴テーブルに保存するメッセージのレベルを変更できます。また、履歴 テーブルに保存するメッセージの数も変更できます。

SNMP トラップが宛先に届く保証はないので、メッセージは履歴テーブルに保存されます。デフォルトでは、warning レベルおよびこれよりも数値が小さいレベルの 1 つのメッセージ (表 46-3 [p.46-10] を参照)が、Syslog トラップがイネーブルではない場合でも履歴テーブルに保存されます。

レベルおよび履歴テーブルのサイズのデフォルトを変更するには、次の作業を実行します。この手順は任意です。

	コマンド	目的			
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。			
ステップ 2	logging history level ¹	履歴ファイルに保存し SNMP サーバに送信する Syslog メッセージのデフォルト レベルを変更します。			
		level キーワードのリストについては、表 46-3 (p.46-10)を 参照してください。			
		デフォルトで送信されるメッセージのレベルは、warnings、errors、critical、alerts、および emergencies です。			
ステップ 3	logging history size number	履歴テーブルに保存できる Syslog メッセージの数を指定します。			
		デフォルトでは 1 件のメッセージが保存されます。有効範囲は 0 ~ 500 件です。			
ステップ 4	end	特権 EXEC モードに戻ります。			
ステップ 5	show running-config	入力を確認します。			
ステップ 6	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。			

^{1.} 表 46-3 に、レベル キーワードと重大度を示します。SNMP を使用する場合は、重大度の値は 1 つずつ大きくなります。たとえば、emergencies は 1 に、critical は 3 になります。

履歴テーブルが満杯の場合(logging history size グローバル コンフィギュレーション コマンドで指定した最大件数が保存されている場合)、最も古いメッセージ エントリがテーブルから削除され、新しいメッセージ エントリが保存されます。

Syslog メッセージのロギングをデフォルト レベルに戻すには、no logging history グローバル コンフィギュレーション コマンドを使用します。履歴テーブルのメッセージ件数をデフォルト値に戻すには、no logging history size グローバル コンフィギュレーション コマンドを使用します。

UNIX Syslog サーバの設定

次のセクションでは、UNIX サーバ Syslog デーモンを設定する方法と UNIX システム ロギング ファシリティを定義する方法を説明します。

UNIX Syslog デーモンへのメッセージ ロギング

UNIX Syslog サーバにシステム ログ メッセージを送信するには、UNIX サーバに Syslog デーモンを 設定する必要があります。この手順は任意です。

ルートとしてログインし、次の手順を実行します。



(注)

UNIX Syslog デーモンの一部の最新バージョンのデフォルトでは、ネットワークからの Syslog パケットを受け付けません。該当するシステムを使用する場合、リモート Syslog メッセージのロギングをイネーブルにするために Syslog コマンドラインに追加または削除するオプションを判断するには、UNIX man syslogd コマンドを使用します。

ステップ1 ファイル /etc/syslog.conf に、次のような行を追加します。

local7.debug /usr/adm/logs/cisco.log

local7 キーワードは使用するロギング ファシリティを指定します。ファシリティについては、表 46-4 (p.46-13) を参照してください。debug キーワードは Syslog レベルを指定します。重大度については、表 46-3 (p.46-10) を参照してください。Syslog デーモンは、次のフィールドで指定するファイルに、このレベル以上の重大度のメッセージを送信します。ファイルが存在しており Syslog デーモンに書き込み権限があることが必要です。

ステップ2 UNIX シェル プロンプトで次のコマンドを入力し、ログ ファイルを作成します。

- \$ touch /var/log/cisco.log
- \$ chmod 666 /var/log/cisco.log

ステップ3 Syslog デーモンが新しい変更内容を読み取るようにします。

\$ kill -HUP `cat /etc/syslog.pid`

詳細については、UNIX システムの man syslog.conf および man syslogd コマンドを参照してください。

UNIX システム ロギング ファシリティの設定

外部装置にシステム ログ メッセージを送信する場合、任意の UNIX Syslog ファシリティで作成されたメッセージをスイッチで識別させることができます。

特権 EXEC モードで次の手順を実行し、UNIX システム ファシリティ メッセージ ロギングを設定します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	logging host	IP アドレスを入力することにより、メッセージを UNIX Syslog サーバ ホストに保存するようにします。
		ロギング メッセージを受信する Syslog サーバのリストを作成するには、このコマンドを複数回入力します。
ステップ 3	logging trap level	Syslog サーバに保存するメッセージを制限します。
		デフォルトでは、Syslog サーバは情報メッセージとそれ以下のレベルのメッセージを受信します。 <i>level</i> キーワードについては、表46-3 (p.46-10)を参照してください。
ステップ 4	logging facility facility-type	Syslog ファシリティを設定します。 $facility$ - $type$ キーワードについては、表 46-4 (p.46-13)を参照してください。
		デフォルトは local7 です。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show running-config	入力を確認します。
ステップ 7	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

Syslog サーバを削除するには、**no logging** host グローバル コンフィギュレーション コマンドを実行し、Syslog サーバ IP アドレスを指定します。Syslog サーバへのロギングをディセーブルにするには、**no logging trap** グローバル コンフィギュレーション コマンドを実行します。

表 46-4 に、ソフトウェアでサポートされる UNIX システム ファシリティを示します。ファシリティの詳細については、使用する UNIX オペレーティング システムのオペレータ マニュアルを参照してください。

表 46-4 ロギング ファシリティ タイプ キーワード

ファシリティ タイプ キーワード	説明
auth	認可システム
cron	cron ファシリティ
daemon	システム デーモン
kern	カーネル
local0-7	ローカル定義メッセージ
lpr	ライン プリンタ システム
mail	メール システム
news	USENET = ¬ - Z
sys9-14	システム使用
syslog	システム ログ
user	ユーザ プロセス
uucp	UNIX 同士のコピー システム

ロギング設定の表示

ロギング設定およびログ バッファの内容を表示するには、show logging 特権 EXEC コマンドを使用します。この出力のフィールドについては、『Cisco IOS Configuration Fundamentals Command Reference』Release 12.3 を参照してください。

■ ロギング設定の表示



CHAPTER

47

SNMP の設定

この章では、Catalyst 4500 シリーズ スイッチに SNMP (簡易ネットワーク管理プロトコル)を設定する方法を説明します。



ここで使用するコマンドの構文および使用方法の詳細については、次の URL にある『Cisco IOS Configuration Fundamentals Command Reference』Release 12.4 を参照してください。

 $http://www.cisco.com/univered/cc/td/doc/product/software/ios124/124tcr/tcf_r/index.htm$

この章の内容は、次のとおりです。

- SNMPの概要 (p.47-2)
- SNMP の設定 (p.47-6)
- SNMP ステータスの表示 (p.47-18)

SNMP の概要

SNMP は、マネージャとエージェント間の通信にメッセージ形式を提供するアプリケーションレイヤ プロトコルです。SNMP は、SNMP マネージャ、SNMP エージェント、および MIB (管理情報ベース)で構成されています。SNMP マネージャは、Cisco Works などの NMS (Network Management System; ネットワーク管理システム)の一部になることができます。エージェントと MIB はスイッチに常駐します。スイッチに SNMP を設定するには、マネージャとエージェントの関係を定義する必要があります。

SNMP エージェントには、SNMP マネージャが値を要求または変更できる MIB 変数が含まれています。マネージャはエージェントから値を取得することも、エージェントに値を保存することもできます。エージェントは、デバイス パラメータおよびネットワーク データに関する情報のリポジトリである MIB からデータを収集します。エージェントは、マネージャの要求に応じてデータを取得または設定できます。

エージェントはマネージャに非送信請求トラップを送信できます。トラップとは、そのネットワークの状態を SNMP マネージャに通知するメッセージです。トラップには、間違ったユーザ認証、再起動、リンク状態(アップまたはダウン)、MAC アドレスの追跡、Transmission Control Protocol (TCP) 接続の終了、ネイバーへの接続の消失、その他の重要なイベントがあります。

ここでは、次の内容について説明します。

- SNMP のバージョン (p.47-2)
- SNMP マネージャの機能 (p.47-4)
- SNMP エージェントの機能 (p.47-4)
- SNMP コミュニティ ストリング (p.47-4)
- SNMP を使用した MIB 変数へのアクセス (p.47-5)
- SNMP 通知 (p.47-5)

SNMP のバージョン

Catalyst 4500 シリーズ スイッチは、次の SNMP バージョンをサポートします。

- SNMPv1 完全インターネット標準の SNMP で、RFC 1157 で定義されています。
- SNMPv2C SNMPv2Classic のパーティベース管理およびセキュリティ フレームワークが SNMPv2C のコミュニティストリングベース管理フレームワークに置き換えられていますが、 SNMPv2Classic のバルク検索は引き継がれ、エラー処理は改良されています。 SNMPv2C には 次の機能があります。
 - SNMPv2 SNMP のバージョン 2 で、RFC 1902 ~ 1907 で定義されているドラフト インターネット標準です。
 - SNMPv2C SNMPv2 のコミュニティストリングベース管理フレームワークで、RFC 1901 で定義されている実験的インターネット プロトコルです。
- SNMPv3 SNMPのバージョン 3 で、RFC 2273 ~ 2275 で定義されている相互運用可能な標準ベースのプロトコルです。SNMPv3 はネットワークのパケットを認証して暗号化することによってデバイスへのセキュアなアクセスを提供し、次のセキュリティ機能があります。
 - メッセージ完全性 送信中にパケットが改ざんされないようにします。
 - 認証 有効な送信元からのメッセージであることを判断します。
 - 暗号化 パッケージの内容を混ぜ合わせ、不正なソースによって読み取られることを防ぎます。



(注)

暗号化を選択するには、priv キーワードを入力します。このキーワードは、暗号(暗号化)ソフトウェアイメージがインストールされている場合にのみ指定できます。

SNMPv1 と SNMPv2C はどちらもコミュニティスベースのセキュリティ形式を使用します。エージェントの MIB にアクセスできるマネージャのコミュニティは、IP アドレス Access Control List (ACL; アクセス コントロール リスト) とパスワードによって定義されます。

SNMPv2C には、バルク検索メカニズムと、詳細なエラー メッセージを管理ステーションに報告する機能が備わっています。バルク検索メカニズムはテーブルおよび大量の情報を検索し、必要な往復回数を最小限に抑えます。SNMPv2C の改良されたエラー処理には多様なエラー状態を区別する拡張型エラー コードがあります。これらの状態は、SNMPv1 では 1 つのエラー コードで報告されます。SNMPv2C ではエラー戻りコードがエラーの種類を報告します。

SNMPv3 は、セキュリティ モデルとセキュリティ レベルの両方を提供します。セキュリティ モデルは、ユーザおよびユーザが存在するグループに設定された認証方法です。セキュリティ レベルは、セキュリティ モデルで許可されたセキュリティのレベルです。セキュリティ レベルとセキュリティ モデルの組み合わせにより、SNMP パケットを処理する場合に使用するセキュリティ メカニズムが決まります。利用可能なセキュリティ モデルは、SNMPv1、SNMPv2C、および SNMPv3です。

表 47-1 に、セキュリティ モデルとセキュリティ レベルの組み合わせの特性を示します。

表 47-1 SNMP のセキュリティ モデルとセキュリティ レベル

モデル	レベル	認証	暗号化	結果
SNMPv1	noAuthNoPriv	コミュニティ ストリング	含まれない	コミュニティ ストリングの照合を認証に 使用
SNMPv2C	noAuthNoPriv	コミュニティ ストリング	含まれない	コミュニティ ストリングの照合を認証に 使用
SNMPv3	noAuthNoPriv	ユーザ名	含まれない	ユーザ名の照合を認証に使用
SNMPv3	authNoPriv	MD5 または SHA	含まれない	HMAC-MD5 または HMAC-SHA アルゴリ ズムに基づく認証を行う
SNMPv3	authPriv(暗号化ソフトウェアイメージが必要)	MD5 または SHA	DES	HMAC-MD5 または HMAC-SHA アルゴリ ズムに基づく認証を行う CBC-DES (DES-56) 標準に基づく認証の ほか、DES 56 ビット暗号化を行う

管理ステーションがサポートする SNMP バージョンを使用するには SNMP エージェントを設定する必要があります。エージェントは複数のマネージャと通信できるため、ソフトウェアを設定して SNMPv1、SNMPv2C、および SNMPv3 プロトコルを使用する通信をサポートすることができます。

SNMP マネージャの機能

SNMP マネージャは MIB の情報を使用して、表 47-2 に示す動作を行います。

表 47-2 SNMP の動作

動作	説明
get-request	指定した変数の値を取得します。
get-next-request	テーブル内の変数の値を取得します。1
get-bulk-request ²	テーブル内の複数行のような大きなデータ ブロックを取得します。多数の小
	さなデータ ブロックの送信が必要になります。
get-response	NMS が送信した get-request、get-next-request、および set-request に応答します。
set-request	指定した変数に値を保存します。
trap	イベント発生時に SNMP エージェントから SNMP マネージャに送信される
	割り込みメッセージ

^{1.} この動作では、SNMPマネージャが正しい変数名を知る必要はありません。必要な変数が見つかるまでテーブル内でのシーケンシャルな検索が実行されます。

SNMP エージェントの機能

SNMP エージェントは、次のような SNMP マネージャ要求に応答します。

- MIB 変数の取得 SNMP エージェントは、NMS の要求に応じてこの機能を開始します。エージェントは要求された MIB 変数の値を取得して NMS にその値を返します。
- MIB 変数の設定 SNMP エージェントは、NMS のメッセージに応じてこの機能を開始します。 SNMP エージェントは MIB 変数の値を NMS が要求する値に変更します。

SNMP エージェントは、重要なイベントがエージェントで発生したことを NMS に知らせる割り込みトラップ メッセージも送信します。トラップ条件の例には、ポートまたはモジュールがアップまたはダウンになった場合、スパニングツリートポロジが変更された場合、認証に失敗した場合などがありますが、これだけに限定されることはありません。

SNMP コミュニティ ストリング

SNMP コミュニティ ストリングは MIB オブジェクトへのアクセスを認証し、埋め込みパスワード として機能します。NMS がスイッチにアクセスできるためには、NMS のコミュニティ ストリング 定義がスイッチに定義された 3 つのコミュニティ ストリングの少なくとも 1 つと一致する必要が あります。

コミュニティ ストリングには次のいずれかの属性があります。

- Read-only (RO) 認可された管理ステーションに、コミュニティ ストリングを除く MIB の全 オブジェクトに対する読み取りアクセス権を与えますが、書き込みアクセス権は与えません。
- Read-write(RW) 認可された管理ステーションに、MIBの全オブジェクトに対する読み取り および書き込みアクセス権を与えますが、コミュニティストリングへのアクセス権は与えません。
- Read-write-all 認可された管理ステーションに、コミュニティ ストリングを含む MIB の全オブジェクトに対する読み取りおよび書き込みアクセス権を与えます。

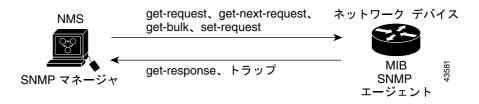
^{2.} get-bulk コマンドは SNMPv2 以降でのみ動作します。

SNMP を使用した MIB 変数へのアクセス

NMS の1つに CiscoWorks ネットワーク管理ソフトウェアがあります。CiscoWorks 2000 はスイッチ MIB 変数を使用してデバイス変数を設定し、ネットワーク上のデバイスの特定の情報をポーリング します。ポーリングした結果をグラフなどで表示して分析し、インターネットワーキングのトラブ ルシューティング、ネットワーク パフォーマンスの向上、デバイスの設定確認、トラフィック負荷 のモニタリングなどを行うことができます。

図 47-1 で示すように、SNMP エージェントは MIB のデータを収集します。エージェントは SNMP マネージャにトラップや特定イベントの通知を送信し、SNMP マネージャはトラップを受信して処理します。トラップは SNMP マネージャにネットワークの状態を通知します。不適切なユーザ認証、再起動、リンクの状態(アップまたはダウン)、MAC アドレスの追跡などが通知されます。SNMP エージェントは、SNMP マネージャから get-request、get-next-request、および set-request 形式で送信される MIB 関連のクエリーにも応答します。

図 47-1 SNMP ネットワーク



SNMP 通知

SNMPでは、特定のイベントが発生した場合にスイッチから SNMPマネージャに通知を送信できます。SNMP通知はトラップまたはインフォーム要求として送信されます。コマンド構文では、コマンドでトラップとインフォームのどちらかを任意で選択できないかぎり、traps キーワードは、トラップとインフォームのどちらか一方または両方を意味します。SNMP通知をトラップまたはインフォームとして送信するには、snmp-server host コマンドを使用します。



SNMPv1 はインフォームをサポートしません。

受信側はトラップを受信しても acknowledgment (ACK; 確認応答)を送信しないのでトラップが受信されたかどうかを送信側で判断することができないため、トラップには信頼性があるとは言えません。SNMP マネージャがインフォーム要求を受信すると、SNMP 応答 Protocol Data Unit (PDU; プロトコル データ ユニット)を使用してメッセージに確認応答します。送信側が応答を受信しなかった場合、インフォーム要求が再送信されます。このため、インフォームは、指定した宛先に到着する可能性がトラップよりも高くなります。

インフォームにはトラップよりも信頼性が高いという特性がありますが、より多くのスイッチおよびネットワークのリソースを消費します。送信後すぐに廃棄されるトラップとは異なり、インフォーム要求は、応答を受信するか要求期限が過ぎるまでメモリに保存されます。トラップは1回しか送信されませんが、インフォームは何度か再送信されます。再送信によってトラフィックが増し、ネットワークのオーバーヘッドにつながります。このため、トラップとインフォームには信頼性とリソースの間で妥協が必要になります。SNMPマネージャがすべての通知を受け取ることが重要であれば、インフォーム要求を使用します。ネットワークのトラフィックやスイッチのメモリが問題であり通知が不要であれば、トラップを使用します。

SNMP の設定

ここでは、スイッチに SNMP を設定する方法を説明します。内容は次のとおりです。

- SNMP のデフォルト設定 (p.47-6)
- SNMP 設定時の注意事項 (p.47-6)
- SNMP エージェントのディセーブル化 (p.47-7)
- コミュニティ ストリングの設定 (p.47-7)
- SNMP グループおよびユーザの設定 (p.47-9)
- SNMP 通知の設定 (p.47-11)
- エージェントの連絡先および設置場所の設定 (p.47-15)
- SNMP で使用する TFTP サーバの限定 (p.47-15)
- SNMPの例 (p.47-16)

SNMP のデフォルト設定

表 47-3 に、SNMP のデフォルト設定を示します。

表 47-3 SNMP のデフォルト設定

機能	デフォルト設定
SNMP エージェント	イネーブル
SNMP トラップ レシーバ	設定なし
SNMP トラップ	TCP 接続へのトラップ(tty)以外はイネーブルになっていません。
SNMP のバージョン	version キーワードがない場合、デフォルトはバージョン 1
SNMPv3 認証	キーワードを指定しない場合、デフォルトは noauth
	(noAuthNoPriv) セキュリティ レベル
SNMP 通知の種類	種類が指定されていない場合、すべての通知が送信されます。

SNMP 設定時の注意事項

SNMP group は、SNMP ユーザを SNMP ビューにマッピングするテーブルです。SNMP user は、SNMP グループのメンバです。SNMP host は、SNMP トラップ動作のレシーバです。SNMP $engine\ ID$ は、ローカルまたはリモート SNMP エンジンの名前です。

SNMP を設定する場合は、以下の注意事項に従ってください。

- SNMP グループを設定する場合、通知ビューを設定しないようにします。snmp-server host グローバル コンフィギュレーション コマンドはユーザの通知ビューを自動的に生成し、そのユーザに関連付けられているグループに追加します。グループの通知ビューを変更すると、そのグループに関連付けられているすべてのユーザが影響を受けます。通知ビューを設定するタイミングについては、『Cisco IOS Configuration Fundamentals Command Reference』Release 12.2 を参照してください。
- リモート ユーザを設定するには、ユーザが存在するデバイスのリモート SNMP エージェント の IP アドレスまたはポート番号を指定します。
- 特定のエージェントにリモート ユーザを設定する前に、snmp-server engineID グローバル コンフィギュレーション コマンドに remote オプションを使用して SNMP エンジン ID を設定します。リモート エージェントの SNMP エンジン ID とユーザ パスワードは、認証およびプライバシー ダイジェストを計算するために使用されます。最初にリモート エンジン ID を設定しなかった場合、コンフィギュレーション コマンドは失敗します。

- SNMP インフォームを設定する場合、まず SNMP データベースにリモート エージェントの SNMP エンジン ID を設定し、それからプロキシ要求やインフォームを送信します。
- ローカル ユーザがリモート ホストに関連付けられていない場合、スイッチは auth(authNoPriv) および priv (authPriv) 認証レベルのインフォームを送信しません。
- SNMP エンジン ID の値を変更すると大きな影響が発生します。ユーザのパスワード(コマンドラインで入力)は、パスワードとローカル エンジン ID に基づいて MD5 または SHA セキュリティ ダイジェストに変換されます。その後、RFC 2274 に従ってコマンドライン パスワードは破棄されます。このため、エンジン ID の値を変更すると SNMPv3 ユーザのセキュリティ ダイジェストが無効になり、snmp-server user username グローバル コンフィギュレーション コマンドを使用して SNMP ユーザを再設定する必要があります。エンジン ID を変更した場合にも、同様の制約によってコミュニティ ストリングの再設定が必要になります。

SNMP エージェントのディセーブル化

SNMP エージェントをディセーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始しま
		す。
ステップ 2	Switch(config)# no snmp-server	SNMP エージェント動作をディセーブルにします。
ステップ 3	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 4	Switch# show running-config	入力を確認します。
ステップ 5	Switch# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存 します。

no snmp-server グローバル コンフィギュレーション コマンドは、デバイスで実行するすべてのバージョン (バージョン 1、バージョン 2C、およびバージョン 3) をディセーブルにします。 SNMP をイネーブルにするための特別な IOS コマンドはありません。 最初に **snmp-server** グローバル コンフィギュレーション コマンドを入力すると、 SNMP の全バージョンがイネーブルになります。

コミュニティ ストリングの設定

SNMP マネージャとエージェントの関係を定義するには、SNMP コミュニティ ストリングを使用します。コミュニティ ストリングは、スイッチのエージェントへのアクセスを許可するパスワードのように機能します。オプションとして、コミュニティ ストリングに関連付けられた次の特性のうち1 つまたは複数を指定できます。

- エージェントへのアクセスを取得するためにコミュニティ ストリングを使用することを許可された SNMP マネージャの IP アドレスのアクセス リスト
- MIB ビュー。指定したコミュニティがアクセス可能なすべての MIB オブジェクトのサブセットを定義します。
- コミュニティがアクセス可能な MIB オブジェクトの読み取りおよび書き込み、または読み取り アクセス権

スイッチにコミュニティ ストリング設定するには、次の作業を行います。

	コマンド	目的
	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
co	Switch(config)# [no] snmp-server community string [view view-name] [ro rw] [access-list-number]	コミュニティ ストリングを設定します。 • string には、パスワードのように機能する、SNMP プロトコルへのアクセスを許可する文字列を設定します。
		最大 117 文字までの 1 つまたは複数のコミュニティ ストリングを設定できます。
		• (任意) view には、コミュニティがアクセスできる ビュー レコードを指定します。
		• (任意) 許可された管理ステーションに MIB オブジェクトを取得させる場合は読み取り(ro)を、許可された管理ステーションに MIB オブジェクトの取得を変更させる場合は読み取りおよび書き込み(rw)を指定します。デフォルトでは、コミュニティストリングは全オブジェクトに対する読み取りアクセスを許可します。
		 (任意) access-list-number には、番号が1~99 および 1300~1999 の IP 標準アクセス リストを入力します。
		特定のコミュニティ ストリングを削除するには、no
		snmp-server community string グローバル コンフィギュ
		レーション コマンドを使用します。
	<pre>witch(config)# access-list access-list-number {deny permit} source source-wildcard]</pre>	(任意)ステップ2のIP標準アクセスリストの番号を指定した場合、必要な回数だけコマンドを実行してリストを作成します。
		• access-list-number には、ステップ 2 で指定したアクセス リストの番号を入力します。
		• deny キーワードは、条件が一致した場合にアクセスを 拒否します。permit キーワードは、条件が一致した場 合にアクセスを許可します。
		• source には、エージェントへのアクセスを取得するためにコミュニティ ストリングを使用することを許可されている SNMP マネージャの IP アドレスを指定します。
		• (任意) source-wildcard には、送信元に適用するワイル ドカード ビットをドット付き 10 進表記で指定します。 無視するビットの位置に 1 を入力します。
		アクセス リストは、すべてに対する黙示的な拒否 (deny) 文によって常に終了します。
	Switch(config)# end	特権 EXEC モードに戻ります。
	Switch# show running-config	入力を確認します。
	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。



SNMP コミュニティへのアクセスをディセーブルにするには、そのコミュニティのコミュニティ ストリングをヌル ストリングに設定します (コミュニティ ストリングに値を入力しません)。



snmp-server enable informs コマンドはサポートされません。SNMP 応答要求型通知の送信をイネーブルにするには、snmp-server enable traps コマンドを snmp-server host host-addr informs コマンドとともに使用します。

次に、SNMP に文字列 comaccess を割り当てて読み取りアクセス権を設定し、IP アクセス リスト 4 でコミュニティ ストリングを使用してスイッチ SNMP エージェントへのアクセスを取得する例を示します。

Switch(config) # snmp-server community comaccess ro 4

SNMP グループおよびユーザの設定

スイッチのローカルまたはリモート SNMP サーバ エンジンに ID 名(エンジン ID)を指定できます。 SNMP ユーザを SNMP ビューにマッピングする SNMP サーバ グループを設定し、SNMP グループに新しいユーザを追加することができます。

スイッチに SNMP を設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[logal engineid-string remote	SNMP のローカル コピーまたはリモート コピーに名前を 設定します。
		• engineid-string は SNMP のコピー名を持つ 24 文字の ID 文字列です。末尾にゼロが続いている場合は、エンジン ID を 24 文字全部指定する必要はありません。エンジン ID の値がゼロばかりになるところまでを指定すれば十分です。たとえば、エンジン ID 1234000000000000000000000000000000000000
		• remote を選択する場合、SNMP のリモート コピーを含むデバイスの <i>ip-address</i> と、任意でリモート デバイスの UDP ポートを指定します。デフォルトは 162 です。

コマンド

_ _ = ---

ステップ 3 Switch(config)# snmp-server group groupname {v1 | v2c | v3 [auth | noauth | priv]} [read readview] [write writeview] [notify notifyview] [access access-list]

目的

リモート デバイス上で新しい SNMP グループを設定します。

- groupname には、グループ名を指定します。
- 次のセキュリティ モデルを指定します。
 - v1 は、セキュリティが最も低いセキュリティ モデルです。
 - v2c は、2番めに低いセキュリティモデルです。通常の2倍の幅でインフォームと整数を送信します。
 - v3 は、最もセキュアなセキュリティ モデルです。 次の認証レベルを選択する必要があります。

auth MD5 および Secure Hash Algorithm (SHA) パケット認証をイネーブルにします。

noauth noAuthNoPriv セキュリティ レベル。 キーワードが指定されていない場合は、これがデ フォルトです。

priv Data Encryption Standard (DES; データ暗号 規格)パケット暗号化 (*プライバシー*ともいう) をイネーブルにします。



(注)

priv キーワードは、暗号イメージがインストールされている場合にのみ指定できます。

- (任意) **read** readview は、エージェントの内容が表示されるだけのビューの名前(64文字以内の文字列)とともに指定します。
- (任意) write writeview は、データを入力しエージェントの内容を設定できるビューの名前(64文字以内の文字列)とともに指定します。
- (任意) **notify** *notifyview* は、通知、インフォーム、トラップを指定できるビューの名前(64 文字以内の文字列) とともに指定します。
- (任意) **access** *access-list* は、アクセスリストの名前(64 文字以内の文字列) とともに指定します。

	コマンド	目的
ステップ 4	Switch(config)# snmp-server user username groupname [remote host	SNMP グループに新しいユーザを設定します。
	<pre>[udp-port port]] {v1 v2c v3 [auth {md5 sha} auth-password]} [encrypted] [access access-list]</pre>	• username は、エージェントに接続するホストのユーザ 名です。
		• groupname は、ユーザが関連付けられるグループの名前です。
		• (任意) remote を入力して、ユーザが所属するリモート SNMP エンティティと、そのエンティティのホスト名または IP アドレスを UDP ポート番号 (任意)とともに指定します。デフォルトは 162 です。
		• SNMP バージョン番号を指定します (v1、v2c、または v3)。v3 を指定した場合は、次のオプションも設定できます。
		- auth 。認証レベル設定セッションです。 HMAC-MD5-96 と HMAC-SHA-96 のどちらかを指 定でき、64 文字以内のパスワード文字列が必要で す。
		- encrypted。パスワードが暗号形式で表示されます。
		 (任意) access access-list は、アクセス リストの名前(64 文字以内の文字列)とともに指定します。
ステップ 5	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 6	Switch# show running-config	入力を確認します。
ステップ 7	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

SNMP 通知の設定

トラップ マネージャは、トラップを受信して処理する管理ステーションです。トラップはシステム の警報で、特定のイベントが発生した場合にスイッチが生成します。デフォルトでは、トラップマ ネージャは定義されておらず、トラップは送信されません。IOS Cisco IOS Release 12.2(31)SG を実 行するスイッチで使用できるトラップマネージャの数には制限がありません。



コマンド構文で traps という単語を使用するコマンドは多数あります。トラップとインフォームの どちらかを選択するオプションがコマンドにないかぎり、traps キーワードは、トラップとイン フォームのどちらか一方または両方を意味します。SNMP 通知をトラップまたはインフォームとし て送信するには、snmp-server host コマンドを使用します。

表 47-4 に、サポートされるスイッチ トラップを示します (通知の種類)。 これらのトラップの一部 または全部をイネーブルにし、受信するためのトラップマネージャを設定できます。

表 47-4 スイッチの通知の種類

通知の種類の キーワード	説明		
bgp	BGPステート変更トラップを生成します。		
	(注) 拡張マルチレイヤ イメージがインストールされている場合にだけ指定できます。		
bridge	STP ブリッジ MIB トラップを生成します。		
config	SNMP 設定変更に対するトラップを生成します。		
config-copy	SNMP コピー設定変更に対するトラップを生成します。		
сри	CPU 関連トラップを許可します。		
eigrp	EIGRP トラップをイネーブルにします。		
	(注) 拡張マルチレイヤ イメージがインストールされている場合にだけ指定できます。		
entity	SNMP エンティティ変更に対するトラップを生成します。		
envmon	環境モニタ トラップを生成します。環境トラップの fan、shutdown、supply、temperature の一部またはすべてをイネーブルにできます。		
flash	SNMP FLASH 通知を生成します。		
fru-ctrl	SNMP エンティティ FRU 制御トラップをイネーブルにします。		
hsrp	Hot Standby Router Protocol(HSRP; ホットスタンバイ ルータ プロトコル)変更に対するトラップを生成します。		
ipmulticast	IP マルチキャスト ルーティング変更に対するトラップを生成します。		
isis	IS-IS トラップをネーブルにします。		
	(注) 拡張マルチレイヤ イメージがインストールされている場合にだけ指定できます。		
mac-notification	MAC アドレス通知に対するトラップを生成します。		
msdp	Multicast Source Discovery Protocol(MSDP)変更に対するトラップを生成します。		
	(注) 拡張マルチレイヤ イメージがインストールされている場合にだけ指 定できます。		
ospf	OSPF変更に対するトラップを生成します。Cisco 固有、エラー、リンクステートアドバタイズ、レート制限、再送信、およびステート変化トラップのいずれかまたはすべてを指定できます。		
	(注) 拡張マルチレイヤ イメージがインストールされている場合にだけ指定できます。		
pim	PIM 変更に対するトラップを生成します。無効 PIM メッセージ、ネイバー変更、およびランデブー ポイント (RP) マッピング変更トラップのいずれかまたはすべてを指定できます。		

表 47-4 スイッチの通知の種類 (続き)

通知の種類の キーワード	説明
port-security	SNMP ポート セキュリティ トラップを生成します。最大トラップ レートを 秒単位で設定することもできます。範囲は $0 \sim 1000$ で、デフォルトは 0 (レート制限なし) です。
rf	Cisco-RF-MIB で定義したすべての SNMP トラップをイネーブルにします。
snmp	認証、コールド スタート、ウォーム スタート、リンク アップまたはリンク ダウンの SNMP タイプの通知に対するトラップを生成します。
storm-control	SNMP ストーム制御に対するトラップを生成します。最大トラップ レートを 秒単位で設定することもできます。範囲は 0 ~ 1000 で、デフォルトは 0 (制限なし、発生するたびにトラップが送信される) です。
stpx	SNMP STP 拡張 MIB トラップを生成します。
syslog	SNMP Syslog トラップを生成します。
tty	TCP 接続に対するトラップを生成します。このトラップは、デフォルトでイネーブルに設定されています。
vlan-membership	SNMP VLAN メンバシップ変更に対するトラップを生成します。
vlancreate	SNMP VLAN 作成トラップを生成します。
vlandelete	SNMP VLAN 削除トラップを生成します。
vtp	VLAN Trunking Protocol(VTP; VLAN トランキング プロトコル)変更に対するトラップを生成します。

特定のホストに snmp-server host グローバル コンフィギュレーション コマンドを使用して、表 47-4 に示した通知の種類を受信することができます。

ホストにトラップまたはインフォームを送信するようにスイッチを設定するには、次の作業を実行 します。

目的
グローバル コンフィギュレーション モードを開始します。
リモート ホストのエンジン ID を指定します。
SNMP ユーザを設定し、ステップ 2 で作成したリモート ホストに関連付けます。 (注) リモート ユーザのアドレスを設定するには、最初にリモート ホストにエンジン ID を設定する必要があります。リモート エンジン ID を設定する前にユーザを設定しようとするとエラー メッセージが表示され、コマンドは実行されません。

	コマンド	目的
ステップ 4	Switch(config)# snmp-server host	SNMP トラップ動作の受信先を指定します。
	<pre>host-addr[traps informs] [version {1 2c 3 [auth noauth priv]}] community-string [udp-port port] [notification-type]</pre>	 host-addr には、ホスト(受信対象)の名前またはインターネットアドレスを指定します。
	[notification type]	● (任意)traps を入力すると、ホストに SNMP トラップ が送信されます(デフォルト)。
		• (任意) informs を入力すると、ホストに SNMP インフォームが送信されます。
		• (任意)SNMP バージョン (1、2c、または3)を指定します。SNMPv1 はインフォームをサポートしません。
		• (任意)バージョン3の場合、認証レベル auth、noauth、 または priv を選択します。
		(注) priv キーワードは、暗号イメージがインストールされている場合にのみ指定できます。
		• community-string には、通知動作とともに送信される、 パスワードに似たコミュニティ ストリングを指定しま す。
		• (任意)udp-port port には、リモート デバイス UDP ポートを指定します。
		• (任意) notification-type には、表 47-4 (p.47-12)に示す キーワードを指定します。種類が指定されていない場合、すべての通知が送信されます。
ステップ 5	Switch(config)# snmp-server enable traps notification-types	スイッチでのトラップまたはインフォームの送信をイネーブルにし、送信する通知の種類を指定します。通知の種類については表 47-4 (p.47-12)を参照するか、次のように入力します。snmp-server enable traps?
		複数の種類のトラップをイネーブルにするには、トラップ の種類ごとに snmp-server enable traps コマンドを個別に入 力する必要があります。
ステップ 6	Switch(config)# snmp-server trap-source interface-id	(任意)発信元インターフェイスを指定します。このインターフェイスによってトラップ メッセージの IP アドレスが提供されます。このコマンドはインフォームの発信元 IP アドレスも設定します。
ステップ 7	Switch(config)# snmp-server queue-length length	(任意) 各トラップ ホストのメッセージ キューの長さを指定します。指定できる範囲は 1 ~ 1000 です。デフォルトは 10 です。
ステップ 8	Switch(config)# snmp-server trap-timeout seconds	(任意)トラップ メッセージを再送信する頻度を指定します。指定できる範囲は $1\sim 1000$ です。デフォルトは 30 秒です。
ステップ 9	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 10	Switch# show running-config	入力を確認します。
ステップ 11	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

snmp-server host コマンドは、通知を受信するホストを指定します。snmp-server enable trap コマンドは、指定した通知(トラップおよびインフォーム)のメカニズムをグローバルにイネーブルにします。ホストにインフォームを受信させるには、ホストに snmp-server host informs コマンドを設定し、snmp-server enable traps コマンドを使用してインフォームをグローバルにイネーブルにする必要があります。

受信トラップから指定したホストを削除するには、no snmp-server host host グローバル コンフィギュレーション コマンドを使用します。no snmp-server host コマンドにキーワードを使用しなかった場合、トラップはディセーブルになりますがインフォームはディセーブルになりません。インフォームをディセーブルにするには、no snmp-server host informs グローバル コンフィギュレーション コマンドを使用します。特定の種類のトラップをディセーブルにするには、no snmp-server enable traps notification-types グローバル コンフィギュレーション コマンドを使用します。

エージェントの連絡先および設置場所の設定

システムの連絡先および SNMP エージェントの設置場所を設定してコンフィギュレーション ファイルを通じてアクセスできるようにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 Switch(config)# snmp-server contact text		システムの連絡先の文字列を設定します。
		次に例を示します。
		snmp-server contact Dial System Operator at beeper 21555.
ステップ 3	Switch(config)# snmp-server location text	システムの設置場所の文字列を設定します。
		次に例を示します。
		snmp-server location Building 3/Room 222
ステップ 4	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 5	Switch# show running-config	入力を確認します。
ステップ 6	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

SNMP で使用する TFTP サーバの限定

SNMP を介したコンフィギュレーション ファイルの保存とロードに使用する TFTP サーバを、アクセス リストで指定したサーバに限定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2		SNMP を介したコンフィギュレーション ファイルのコピー に使用する TFTP サーバを、アクセス リストのサーバに限定します。 access-list-number には、1 ~ 99 および 1300 ~ 1999 の番号の IP 標準アクセス リストを入力します。

	コマンド	目的
ステップ 3	Switch(config) # access-list access-list-number {deny permit} source [source-wildcard]	標準アクセス リストを作成し、コマンドを必要な回数だけ 実行します。
		• access-list-number には、ステップ 2 で指定したアクセス リストの番号を入力します。
		• deny キーワードは、条件が一致した場合にアクセスを 拒否します。permit キーワードは、条件が一致した場 合にアクセスを許可します。
		 source には、スイッチにアクセスできる TFTP サーバの IP アドレスを指定します。
		● (任意)source-wildcard には、送信元に適用するワイル ドカード ビットをドット付き 10 進表記で指定します。 無視するビットの位置に 1 を入力します。
		アクセス リストは、すべてに対する黙示的な拒否(deny) 文によって常に終了します。
ステップ 4	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 5	Switch# show running-config	入力を確認します。
ステップ 6	Switch# copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

SNMP の例

次に、SNMP の全バージョンをイネーブルにする例を示します。コミュニティ ストリング public を使用して、SNMP マネージャからすべてのオブジェクトへの読み取りアクセスを許可します。この設定によりスイッチがトラップを送信することはありません。

Switch(config)# snmp-server community public

次に、コミュニティ ストリング public を使用して、SNMP マネージャからすべてのオブジェクトへの読み取りアクセスを許可する例を示します。スイッチはまた、SNMPv1 を使用した場合はホスト 192.180.1.111 および 192.180.1.33 に、SNMPv2C を使用した場合はホスト 192.180.1.27 に、VTP トラップを送信します。コミュニティ ストリング public はトラップとともに送信されます。

```
Switch(config)# snmp-server community public
Switch(config)# snmp-server enable traps vtp
Switch(config)# snmp-server host 192.180.1.27 version 2c public
Switch(config)# snmp-server host 192.180.1.111 version 1 public
Switch(config)# snmp-server host 192.180.1.33 public
```

次に、comaccess コミュニティ ストリングを使用するアクセス リスト 4 のメンバに対してすべての オブジェクトへの読み取りアクセスを許可する例を示します。他の SNMP マネージャはどのオブ ジェクトにもアクセスできません。SNMP Authentication Failure トラップは、コミュニティ ストリング public を使用して SNMPv2C によってホスト cisco.com に送信されます。

```
Switch(config) # snmp-server community comaccess ro 4
Switch(config) # snmp-server enable traps snmp authentication
Switch(config) # snmp-server host cisco.com version 2c public
```

次に、Entity MIB トラップをホスト cisco.com に送信する例を示します。コミュニティ ストリング は restricted です。最初の行では、それまでにイネーブルになったトラップのほかに Entity MIB トラップをスイッチで送信できるようにします。2 番めの行ではこれらのトラップの宛先が指定され、ホスト cisco.com についての以前の snmp-server host コマンドを上書きします。

```
Switch(config)# snmp-server enable traps entity
Switch(config)# snmp-server host cisco.com restricted entity
```

次に、コミュニティ ストリング *public* を使用して、スイッチですべてのトラップをホスト *myhost.cisco.com* に送信できるようにする例を示します。

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com public
```

次に、ユーザをリモート ホストに関連付け、ユーザがグローバル コンフィギュレーション モード を開始したとき **auth** (authNoPriv) 認証レベルのインフォームを送信する例を示します。

```
Switch(config) # snmp-server engineID remote 192.180.1.27 00000063000100a1c0b4011b
Switch(config) # snmp-server group authgroup v3 auth
Switch(config) # snmp-server user authuser authgroup remote 192.180.1.27 v3 auth md5
mypassword
Switch(config) # snmp-server user authuser authgroup v3 auth md5 mypassword
Switch(config) # snmp-server host 192.180.1.27 informs version 3 auth authuser config
Switch(config) # snmp-server enable traps
Switch(config) # snmp-server inform retries 0
```

SNMP ステータスの表示

SNMP の出入力統計情報を、不正なコミュニティ ストリング エントリの数、エラー、および要求 された変数を含めて表示するには、show snmp 特権 EXEC コマンドを使用します。表 47-5 の他の 特権 EXEC コマンドを使用して SNMP 情報を表示することもできます。出力のフィールドについて は、『Cisco IOS Configuration Fundamentals Command Reference』 Release 12.4 を参照してください。

表 47-5 SNMP 情報の表示コマンド

機能	デフォルト設定
show snmp	SNMP 統計情報を表示します。
show snmp engineID デバイスに設定されたローカル SNMP エンジンおよびすべてのモート エンジンの情報を表示します。	
show snmp group	ネットワークの各 SNMP グループの情報を表示します。
show snmp pending	保留中の SNMP 要求に関する情報を表示します。
show snmp sessions	現在の SNMP セッションに関する情報を表示します。
show snmp user	SNMP ユーザ テーブル内の SNMP ユーザ名別の情報を表示します。



snmp-server enable informs コマンドはサポートされません。SNMP 応答要求型通知の送信をイネーブルにするには、snmp-server enable traps コマンドを snmp-server host host-addr informs コマンドとともに使用します。



CHAPTER

48

NetFlow の設定



注) Netflow は、Supervisor Engine 6-E ではサポートされて*いません*。

この章では、Catalyst 4500 シリーズ スイッチ上で、NetFlow 統計情報を設定する方法について説明します。設定上の注意事項、設定手順、および設定例についても示します。



E) NetFlow 機能を使用するには、Supervisor Engine V-10GE (機能はスーパーバイザ エンジンに組み込まれている) または NetFlow Services Card (WS-F4531) および Supervisor Engine IV か Supervisor Engine V が必要です。



【注) この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/cr/index.htm



(注)

NetFlow の使用および管理の詳細については、『NetFlow Solutions Guide』を参照してください。

ここでは、次の内容について説明します。

- NetFlow 統計情報収集機能の概要(p.48-2)
- NetFlow 統計情報収集機能の設定 (p.48-7)
- NetFlow 統計情報収集機能の設定例 (p.48-14)
- NetFlow の設定例 (p.48-15)

NetFlow 統計情報収集機能の概要

ネットワーク フローは、特定の送信元と宛先(両方ともネットワークレイヤ IP アドレスおよびトランスポートレイヤ ポート番号で定義)の間における、パケットの単方向ストリームとして定義されます。 具体的にフローは、送信元 IP アドレス、宛先 IP アドレス、送信元ポート番号、宛先ポート番号、プロトコル タイプ、サービス タイプ、入力インターフェイスというフィールドの組み合わせとして識別されます。

NetFlow 統計情報は、グローバル トラフィックのモニタ機能であり、これにより、NetFlow Data Export (NDE; NetFlow データ エクスポート)を使用して、スイッチを通過するすべての IPv4 ルーテッド トラフィックをフローレベルで監視できるようになります。収集された統計情報は、外部デバイス (NetFlow Collector/Analyzer)にエクスポートしてさらに処理できます。ネットワーク プランナーは、NetFlow 統計情報 (および NDE)をデバイス単位で選択的にイネーブルにして、特定のネットワーク領域のトラフィック パフォーマンス、制御、または課金情報を得ることができます。

NetFlow は、2 つのフォーマットのうちどちらかにより、UDP データグラムでフロー情報をエクスポートします。バージョン 1 フォーマットは最初にリリースされたバージョンであり、バージョン 5 は、Border Gateway Protocol (BGP) Autonomous System (AS; 自律システム)情報およびフローシーケンス番号を追加した強化機能です。バージョン 1 フォーマットおよびバージョン 5 フォーマットでは、ヘッダーおよび 1 つ以上のフロー レコードからデータグラムが構成されます。ヘッダーの先頭フィールドには、エクスポート データグラムのバージョン番号が含まれます。

ここでは、次の内容について説明します。

- ハードウェアから取得する情報 (p.48-4)
- ソフトウェアから取得する情報 (p.48-4)
- 入力および出力インターフェイス番号と AS 番号の割り当て (p.48-4)
- UBRL およびマイクロフロー ポリシングと Netflow 統計情報の機能の相互作用 (p.48-5)
- VLAN の統計情報 (p.48-6)

NDE バージョン

Catalyst 4500 シリーズ スイッチでは、収集された統計情報用に NDE バージョン 1 および 5 がサポートされます。 NetFlow 集計では NDE バージョン 8 が必要です。

現在のフロー マスクによっては、フロー レコードの一部のフィールドには値が含まれないことがあります。サポートされていないフィールドにはゼロ(0)が含まれます。

次の表では、NDE バージョン 5 でサポートされているフィールドについて説明します。

- 表 48-1 バージョン 5 のヘッダー フォーマット
- 表 48-2 バージョン 5 のフロー レコード フォーマット

表 48-1 ND	Eバージョン	5 のヘッダー	フォーマット
-----------	--------	---------	--------

パイト	内容	説明
0 ~ 1	version	NetFlow エクスポート フォーマットのバージョン番号
2 ~ 3	count	このパケットでエクスポートされるフローの数(1 ~ 30)
4 ~ 7	SysUptime	ルータをブートしてから経過したミリ秒単位の時間
8 ~ 11	unix_secs	0000 UTC(世界標準時)1970 から経過した秒数
12 ~ 15	unix_nsecs	0000 UTC 1970 から経過したナノ秒
16 ~ 19	flow_sequence	確認された合計フローのシーケンス カウンタ
20 ~ 21	engine_type	フロー スイッチング エンジンのタイプ
21 ~ 23	engine_id	フロー スイッチング エンジンのスロット番号

表 48-2 NDE パージョン 5 のフロー レコード フォーマット

			• X =	- マス 入力あ 追加フ		, ド		
パイト	内容	説明	送信元	宛先	宛先送信元	宛先送信元 インターフェイス	金	完全 インターフェイス
0 ~ 3	srcaddr	送信元 IP アドレス	X		X	X	X	X
4 ~ 7	dstaddr	宛先 IP アドレス		X	X	X	X	X
8 ~ 11	nexthop	ネクスト ホップ ルータの IP アドレス		\mathbf{A}^{1}	A	A	A	A
12 ~ 13	input	入力インターフェイス SNMP ifIndex				X		X
14 ~ 15	output	出力インターフェイス SNMP ifIndex		\mathbf{A}^1	A	A	A	A
16 ~ 19	dPkts	フローのパケット	X	X	X	X	X	X
20 ~ 23	dOctets	フローのオクテット (バイト)	X	X	X	X	X	X
24 ~ 27	first	フロー開始時の SysUptime	X	X	X	X	X	X
28 ~ 31	last	フローの最終パケットを受信したときの SysUptime	X	X	X	X	X	X
32 ~ 33	srcport	レイヤ4送信元ポート番号またはそれと同等のもの					\mathbf{X}^2	\mathbf{X}^2
34 ~ 35	dstport	レイヤ 4 宛先ポート番号またはそれと同等のもの					X	X
36	pad1	未使用(ゼロ)バイト						
37	tcp_flags	TCP フラグの累積 OR						
38	prot	レイヤ4プロトコル (6=TCP、17=UDP など)					X	X
39	tos	IP サービス タイプ バイト						
40 ~ 41	src_as	送信元の AS 番号 (始点またはピア)	X		X	X	X	X
42 ~ 43	dst_as	宛先の AS 番号(始点またはピア)		X	X	X	X	X
44 ~ 45	src_mask	送信元アドレス プレフィクス マスク ビット	X		X	X	X	X
46 ~ 47	dst_mask	宛先アドレス プレフィクス マスク ビット		X	X	X	X	X
48	pad2	未使用(ゼロ)バイト						

^{1.} 宛先フロー マスクの場合、「ネクスト ホップ ルータの IP アドレス」フィールドおよび「出力インターフェイスの SNMP ifIndex」フィールドには、すべてのフローで正確な情報が含まれないことがあります。

^{2.} PFC3BXL モードまたは PFC3B モードでは、Internet Control Message Protocol (ICMP) トラフィックに ICMP コードとタイプの値が含まれます。

ハードウェアから取得する情報

ハードウェアからの一般的な NetFlow レコードで入手できる情報には、次の内容が含まれます。

- パケットおよびバイト数
- 開始タイムスタンプおよび終了タイムスタンプ
- 送信元 IP アドレスおよび宛先 IP アドレス
- IP プロトコル
- 送信元ポート番号および宛先ポート番号

ソフトウェアから取得する情報

ソフトウェアからの一般的な NetFlow レコードで入手できる情報には、次の内容が含まれます。

- 入力識別子および出力識別子
- ネクストホップ アドレス、始点およびピア AS、送信元および宛先プレフィクス マスクを含む ルーティング情報

入力および出力インターフェイス番号と AS 番号の割り当て

ここでは、次の内容について説明します。

- 予測フィールドの割り当て (p.48-4)
- 出力インターフェイスおよび出力関連予測フィールドの割り当て(p.48-4)
- 入力インターフェイスおよび入力関連予測フィールドの割り当て(p.48-5)

予測フィールドの割り当て

Catalyst 4500 シリーズ スイッチでは、ハードウェアで NetFlow フローが収集されます。ハードウェアでは、すべての NetFlow フロー フィールドのサブセットが収集されます。残りのフィールドは、ソフトウェアによってルーティング状態が調査されたとき、ソフトウェアによって入力されます。

Netflow Services Card には、NetFlow Flows に関連する入力インターフェイス、出力インターフェイス、その他のルーティング情報を正確にかつ一貫して判別する情報が十分にありません。Catalyst 4500 シリーズ スイッチには、これを補うソフトウェア メカニズムがあります。このメカニズムについて、次の段落で説明します。

出力インターフェイスおよび出力関連予測フィールドの割り当て

ソフトウェアは、(宛先 IP アドレスに基づいた)デフォルトの Forwarding Information Base (FIB; 転送情報ベース)テーブルの FIB エントリを検索して出力インターフェイス情報を判別します。この FIB エントリから、ソフトウェアはこの宛先 IP アドレスの宛先 AS 番号およびインターフェイス情報を格納する適切な隣接装置へのアクセスができるようになります。したがって、出力インターフェイスは単に宛先 IP アドレスに基づいています。スイッチ上でロード バランシングがイネーブルにされている場合、FIB エントリで隣接装置を検索する代わりに、ロード バランシング ハッシュが適切な FIB パスにアクセスするように適用され、適切な隣接装置にアクセスします。このプロセスは、通常、正しい結果を生成しますが、デフォルトの FIB テーブルで IP アドレスを共有する Policy-Based Routing (PBR; ポリシーベース ルーティング)が使用されている場合、正しい結果が得られない場合があります。このような環境では、同一の宛先 IP アドレスに FIB テーブル エントリおよび関連付けられた隣接装置が複数存在するようになります。

入力インターフェイスおよび入力関連予測フィールドの割り当て

同様に、入力インターフェイスと送信元 IP アドレスの送信元 AS 番号は、送信元 IP アドレスに基づいたデフォルトの FIB テーブルの FIB エントリを検索することによって判別されます。したがって、入力インターフェイスは単に送信元 IP アドレスに基づいており、逆ルックアップが行われて、この IP 宛先アドレスを持つパケットがルーティングされる必要があるインターフェイスが判別されます。このプロセスは、転送パスが対称であると仮定します。ただし、このプロセスが複数の入力インターフェイスを生成する場合、最小の IP アドレスを持つインターフェイスを 1 つ選択するように決定論的なアルゴリズムが適用されます。このプロセスは通常正しい値を生成しますが、値が正確でない場合もあります。

- ロード バランシングがアップストリーム隣接スイッチによって適用されている場合、使用可能な複数の入力インターフェイスから任意の1つの入力インターフェイスが選択される必要があります。このアクションが必要とされるのは、使用される入力インターフェイスが、隣接アップストリーム スイッチによって適用されるロード バランシング アルゴリズムのタイプに左右されるためです。そのアルゴリズムを常に知ることができるとは限りません。したがって、すべてのフロー統計情報は、1つの入力インターフェイスによるものとなります。ソフトウェアは、最小の IP サブネット番号を持つインターフェイスを選択します。
- 非対称ルーティング方式では、IP サブネットのトラフィックが、この IP サブネットにパケットを送信するインターフェイスとは別のインターフェイスで受信されることがありますが、逆ルックアップに基づいて入力インターフェイスを選択した予測が、不正確で確認できない可能性があります。
- スイッチ上で PBR または VPN Routing/Forwarding (VRF; VPN ルーティング/転送)がイネーブルに設定されており、フローが PBR 範囲または VRF 範囲にあるアドレスに送られる場合、または PBR 範囲または VRF 範囲にあるアドレスから送信される場合、この情報は正しくありません。この場合、入力および出力インターフェイスは、デフォルトのルート(設定されている場合)を指定する可能性が高く、そうでない場合は値が得られずヌルの状態となります。
- 一部のインターフェイスのスイッチで VRF がイネーブルになっており、フローが VRF インターフェイスから送信される場合、情報は正しくありません。この場合、入力および出力インターフェイスは、デフォルトのルート(設定されている場合)を指定する可能性が高く、そうでない場合は値が得られずヌルの状態となります。



Supervisor Engine V-10GE はハードウェアからの入力インターフェイス情報を提供して、NetFlow 情報の精度を向上させます。

UBRL およびマイクロフロー ポリシングと Netflow 統計情報の機能の相互作用

Supervisor Engine V-10GE を含むシステムでは、Netfow 統計情報および User Based Rate Limiting (UBRL)の間に機能の相互作用があります。特定インターフェイスで正しく設定している UBRL の一部として、クラスマップではフローマスクを指定する必要があります。このフローマスクは、フローのハードウェアベース NetFlow 統計情報の作成に使用されます。デフォルトの場合、従来の full flow NetFlow 統計情報には、full flow マスクが使用されます。しかし UBRL では、マスクが異なることがあります。特定インターフェイスで UBRL を設定している場合、統計情報は、UBRL 用に設定したマスクに基づいて収集されます。その結果、UBRL で設定されたインターフェイスを通過するトラフィックの full flow 統計情報がシステムで収集されません。詳細については、「UBRL の設定」(p.34-45)を参照してください。

VLAN の統計情報

NetFlow がサポートされている場合は、レイヤ 2 出力 VLAN 統計、および VLAN を出入りするルーティング済みトラフィックの VLAN 統計をレポートできます。

次の例は、特定 VLAN の CLI (コマンドライン インターフェイス)出力を示しています。

Switch# show vlan counters or show vlan id 22 count

:22
:38
:2432
:14344621
:659852566
:8983050
:413220300
:0
:0
:0
:0
:340
:21760



NetFlow のサポートには、プラットフォームのサポートをすべての NetFlow フィールドのサブセットに限定するハードウェア制限があります。具体的には、TCP フラグおよび Type of Service (ToS; タイプ オブ サービス) バイト (DSCP) がサポートされません。

NetFlow 統計情報収集機能の設定

NetFlow スイッチングを設定するには、次の作業を行います。

- 必要なハードウェアの確認 (p.48-7)
- NetFlow 統計情報収集機能のイネーブル化(p.48-8)
- スイッチド / ブリッジド IP フローの設定 (p.48-8)
- NetFlow 統計情報のエクスポート (p.48-10)
- NetFlow 統計情報収集機能の管理 (p.48-10)
- 集約キャッシュの設定 (p.48-10)
- ルータベース集約の NetFlow 最小プレフィクス マスクの設定 (p.48-11)
- NetFlow エージング パラメータの設定 (p.48-13)

必要なハードウェアの確認

必要なハードウェアがイネーブルであることを確認するためには、次のように show module コマンドを入力します。

```
Switch# show module all
Chassis Type: WS-C4507R
Power consumed by backplane : 40 Watts
Mod Ports Card Type
                                                    Model
Serial No.
1 2 1000BaseX (GBIC) Supervisor(active)
                                                   WS-X4515
TAB062604KB
2 1000BaseX (GBIC) Supervisor(standby) WS-X4515
JAB062408CB
6 48 10/100BaseTX (RJ45)
                                                   WS-X4148
JAB032305UH
M MAC addresses
                                    Hw Fw
__+____
1 0001.6442.2c00 to 0001.6442.2c01 0.4 12.1(14r)EW( 12.1(20030513:00 Ok
2 0001.6442.2c02 to 0001.6442.2c03 0.4 12.1(14r)EW( 12.1(20030513:00 Ok
6 0050.3ed8.6780 to 0050.3ed8.67af 1.6 12.1(14r)EW( 12.1(20030513:00 Ok
Mod Submodule
                              Model
                                                 Serial No. Hw
                                                                    Status

        1
        Netflow Services Card
        WS-F4531
        JAB062209CG
        0.2
        0k

        2
        Netflow Services Card
        WS-F4531
        JAB062209AG
        0.2
        0k

                                                JAB062209CG 0.2 Ok
Switch#
```



この機能をイネーブルにしても、スイッチのハードウェア転送パフォーマンスには影響しません。

ハードウェアのフロー キャッシュ テーブルの有効サイズは 65,000 フローです。Supervisor Engine V-10GE のハードウェア フロー キャッシュは、85,000 フローです。85,000 フローより多いフローが同時にアクティブになると、一部のフローの統計情報が失われます。

ソフトウェアのフロー テーブルの有効サイズは 256,000 フローです。NetFlow ソフトウェアは、ハードウェア テーブルとソフトウェア テーブル間の一貫性を管理します。 ソフトウェア テーブルへの 非アクティブのハードウェア フローを削除することで、ハードウェア テーブルをオープンのまま にします。

ユーザが設定するタイムアウト設定は、フローが削除され、ソフトウェア キャッシュから NDE を通じてエクスポートされる時間を指定します。ハードウェア フロー管理は、ハードウェア フロー削除とユーザが設定するタイムアウト設定との一貫性を保ちます。

また、ソフトウェア転送フローもモニタされます。さらに、いずれかのフローが 2 Gbps を超える 平均速度でトラフィックを受信すると統計情報がオーバーフローになります。ただし、一般的に ポートは 2 Gbps 以上の速度で伝送できないため、このような状態は発生しません。



設計上、タイムアウト設定が高い場合でも、統計情報の制限に近づくとフローは自動的に「期限切れ」となります。

NetFlow 統計情報収集機能のイネーブル化



(注)

デフォルトでは、NetFlow 統計情報はディセーブルです。

NetFlow スイッチングをイネーブルにするには、最初に『Cisco IOS IP and IP Routing Configuration Guide』の「IP configuration」にある IP ルーティング用のスイッチ設定を実行してください。IP ルーティングを設定したあと、次のいずれかの作業を行ってください。

コマンド	目的			
Switch(config)# ip flow ingress	IP ルーティング用の NetFlow をイネーブルにします。			
Switch(config)# ip flow ingress infer-fields	情報として予測入力/出力インターフェイスおよび送信元/宛先 BGP を持つ NetFlow をイネーブルにします。			
	AS 情報が判別されるようにするには、inter-fields オプションを設定する必要があります。			

スイッチド/ブリッジド IP フローの設定

Netflow は、すべてのルーテッド IP トラフィック用に作成および追跡されるルーテッド IP フローの 収集として定義されます。スイッチング環境では、多量の IP トラフィックが VLAN 内でスイッチングされるため、ルーティングはされません。このトラフィックは、スイッチド/ブリッジド IP トラフィックといいます。これに関連するフローをスイッチド/ブリッジド IP フローといいます。NetFlow ハードウェアには、このタイプのフローを作成および追跡する機能があります。NetFlow スイッチド IP フロー機能により、スイッチド IP フローを作成、追跡、およびエクスポートできます(つまり、スイッチングされ、ルーティングされない IP トラフィックのフローを作成および追跡します)。

次の点に注意してください。

- Catalyst 4500 シリーズ スイッチでは、スイッチド IP フロー収集を単独でイネーブルにできません。 スイッチド IP フローの収集を開始するには、 ルーテッド フロー収集およびスイッチド フロー収集の両方をイネーブルにする必要があります。
- 一般的に、入力および出力インターフェイスの情報はヌルになります。トラフィックが Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) に関連付けられた VLAN 上でスイッチングされる場合、入力および出力インターフェイス情報は同じレイヤ 3 インターフェイスをポイントします。

48-8

- スイッチド フローは通常のエクスポート設定に従ってエクスポートされます。個別のエクスポート CLI は存在しません。
- メイン キャッシュでは、ハードウェア制限によりスイッチド IP フローおよびルーテッド IP フローの区別ができません。



(注)

すべてのインターフェイス上でスイッチド IP フロー収集をイネーブルにするには、ip flow ingress および ip flow ingress layer2-switched コマンドの両方を入力する必要があります。



(注)

スイッチド IP フロー トラフィック上で UBRL ポリシーをイネーブルにするには、ip flow ingress コマンドではなく ip flow ingress layer2-switched コマンドを入力する必要があります (「UBRL の設定」[p.34-45] を参照)。

NetFlow キャッシュを設定し、スイッチド IP フロー収集をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# conf terminal	コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# ip flow ingress	ルーテッド フロー収集をイネーブルにします。
ステップ 3	Switch(config)# ip flow ingress layer2-switched	スイッチドフロー収集をイネーブルにします。

次に、スイッチ IP フローを含む IP フロー キャッシュの内容を表示する例を示します。

Switch# show ip cache flow

IP Flow Switching Cache, 17826816 bytes

2 active, 262142 inactive, 2 added

6 ager polls, 0 flow alloc failures

Active flows timeout in 30 minutes

Inactive flows timeout in 15 seconds

IP Sub Flow Cache, 1081480 bytes 2 active, 65534 inactive, 2 added, 2 added to flow

 ${\tt 0}$ alloc failures, ${\tt 0}$ force free

1 chunk, 1 chunk added

last clearing of statistics never

Protocol	Total	Flows	Packets	Bytes	Packets	Active	e(Sec)	Idle	(Sec)
	Flows	/Sec	/Flow	/Pkt	/Sec	/ I	71ow	/F	low
SrcIf	SrcIPaddress	s DstI	f	DstI	Paddress	Pr	SrcP	DstP	Pkts
Fa1	150.1.1.1	Fa1		13.1	.1.1	11	003F	003F	425K
Fa1	13.1.1.1	Fa1		150.	1.1.1	11	003F	003F	425K
Switch#									

NetFlow 統計情報のエクスポート

フローの有効期限が切れたときに NetFlow 統計情報をワークステーションにエクスポートするようにスイッチを設定するには、次のいずれかの作業を行います。

コマンド	目的				
Switch(config)# ip flow-export destination {hostname ip-address} udp-port	(必須)NetFlow キャッシュ エントリを特定の宛先(ワークステーションなど)にエクスポートするようにスイッチを設定します。 ◇ (注) 複数の宛先を指定できます。				
<pre>Switch(config)# ip flow-export version {1 {5 [origin-as peer-as]}}</pre>	(任意)バージョン1または5が必要な受信ソフトウェアを使用している場合に、ワークステーションに NetFlow キャッシュ エントリをエクスポートするようにスイッチを設定します。バージョン1がデフォルトです。				
	origin-as によって、NetFlow は、フローの送信元と宛先ホスト両方の始点 BGP AS を判別します。 peer-as によって、NetFlow は、フローの入力および出力インターフェイス両方のピア BGP AS を判別します。				
Switch(config)# ip flow-export source <interface></interface>	(任意) IP アドレスが NDE パケットの IP ヘッダー内で送信元 IP アドレスとして使用されるインターフェイスを指定します。デフォルトは、NDE 出力インターフェイスです。				

NetFlow 統計情報収集機能の管理

IP フロー スイッチング キャッシュ情報やフロー情報(プロトコル、フロー合計、秒あたりのフローなど) などの NetFlow 統計情報を表示し、クリアできます。また、結果情報を使用してスイッチ トラフィックの情報を得ることもできます。

NetFlow スイッチング統計情報を管理するには、次のいずれかの作業、または両方の作業を行います。

コマンド	目的	
Switch# show ip cache flow	NetFlow スイッチング統計情報を表示します。	
Switch# clear ip flow stats	NetFlow スイッチング統計情報をクリアします。	

集約キャッシュの設定

NetFlow 統計情報の集約は、通常、管理ワークステーション上の NetFlow 収集ツールによって実行されます。このサポートを Catalyst 4500 シリーズ スイッチに拡張することによって、次のことが可能になります。

- エクスポートされる NDE パケットが少なくなるため、スイッチとワークステーション間で必要な帯域幅が削減されます。
- 必要な収集ワークステーション数が削減されます。
- CLI で集約されたフローの統計情報を表示できます。

集約キャッシュを設定するには、集約キャッシュ コンフィギュレーション モードを開始し、設定する集約方式のタイプ (as、destination prefix、protocol prefix、または source prefix aggregation cache)を決定する必要があります。集約方式を定義したら、その方式の動作パラメータを定義します。同時に複数の集約キャッシュを設定できます。

集約キャッシュを設定にするには、次の作業を行います。

	コマンド	目的	
ステップ 1	Router(config)# ip flow-aggregation cache as	集約キャッシュ コンフィギュレーション モードを 開始し、集約キャッシュ方式 (as、destination-prefix、 prefix、protocol-port、または source-prefix) をイネー ブルにします。	
ステップ 2	Router(config-flow-cache)# cache timeout inactive 199	非アクティブのエントリが削除されるまで集約 キャッシュに保持される秒数(ここでは、199)を指 定します。	
ステップ 3	Router(config-flow-cache)# cache timeout active 45	アクティブ エントリがアクティブの状態である分数(ここでは、45)を指定します。	
ステップ 4	<pre>Router(config-flow-cache)# export destination 10.42.41.1 9991</pre>	データ エクスポートをイネーブルにします。	
ステップ 5	Router(config-flow-cache)# enabled	集約キャッシュの作成をイネーブルにします。	

集約キャッシュ設定およびデータ エクスポートの確認

集約キャッシュ情報を確認するには、次の作業を行います。

コマンド	目的
Router# show ip cache flow aggregation destination-prefix	指定された集約キャッシュ情報を表示します。

データエクスポートを確認するには、次の作業を行います。

コマンド	目的
Router# show ip flow export	メイン キャッシュおよびその他のすべてのイネーブルに設定されたキャッシュを含むデータ エクスポートの統計情報を表示します。

ルータベース集約の NetFlow 最小プレフィクス マスクの設定

最小プレフィクス マスクは、1 つの IP アドレス ベースの集約キャッシュ (source-prefix、destination-prefix、prefix など)内の集約フローに使用される最短のサブネット マスクを指定します。このようなキャッシュでは、フローは IP アドレス (送信元、宛先、またはその両方のそれぞれ)に基づいて集約され、最小プレフィクス マスク、およびスイッチのルーティング テーブルで見つかったフローの送信元 / 宛先ホストへのルートのサブネット マスクのうち長い方によってマスクされます。



最小マスクのデフォルト値は 0 です。最小マスクの設定可能範囲は、1 ~ 32 です。トラフィックに応じて適切な値を選択する必要があります。最小マスクの値が高いと、より詳細なネットワークアドレスが提供できますが、集約キャッシュのフローの数が増加する可能性もあります。

ルータベース集約機能の最小プレフィクス マスクを設定するには、次のセクションで説明する作業を行います。 これらの作業は任意です。

- prefix 集約方式の最小マスクの設定
- destination-prefix 集約方式の最小マスクの設定
- source-prefix 集約方式の最小マスクの設定
- 集約方式の最小マスクのモニタおよび保守

prefix 集約方式の最小マスクの設定

prefix 集約方式の最小マスクを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# ip flow-aggregation cache prefix	prefix 集約キャッシュを設定します。
ステップ 2	Router(config-flow-cache)# mask source minimum value	送信元マスクの最小値を指定します。
ステップ 3	Router(config-flow-cache)# mask destination minimum value	宛先マスクの最小値を指定します。

destination-prefix 集約方式の最小マスクの設定

destination-prefix 集約方式の最小マスクを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# ip flow-aggregation cache destination-prefix	宛先集約キャッシュを設定します。
ステップ 2	Router(config-flow-cache)# mask destination minimum value	宛先マスクの最小値を指定します。

source-prefix 集約方式の最小マスクの設定

source-prefix 集約方式の最小マスクを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# ip flow-aggregation cache source-prefix	source-prefix 集約キャッシュを設定し
		ます。
ステップ 2	Router(config-flow-cache)# mask source minimum value	送信元マスクの最小値を指定します。

集約方式の最小マスクのモニタおよび保守

設定された最小マスクの値を表示するには、必要に応じて各集約方式に対して次のコマンドを使用 します。

コマンド	目的
Router# show ip cache flow aggregation prefix	prefix 集約方式の設定された最小マスクの値を表示します。
Router# show ip cache flow aggregation destination-prefix	destination-prefix 集約方式の設定された最小マスクの値を表示します。
Router# show ip cache flow aggregation source-prefix	source-prefix 集約方式の設定された最小マスク の値を表示します。

NetFlow エージング パラメータの設定

フローをソフトウェア フロー キャッシュから削除する (また、設定されている場合、NDE を通じてレポートする)時期を、ip flow-cache timeout コマンドの設定エージング パラメータ Active および Inactive を使用して制御できます。

アクティブ エージングは、フローが作成されたあとにフローがソフトウェア フロー キャッシュから削除される時間を指定します。一般的に、このパラメータは外部収集デバイスへアクティブ フローについて定期的に通知するために使用します。このパラメータは、フローの既存のトラフィックから独立して動作します。アクティブ タイムアウト設定は通常、分単位で設定されます(デフォルト設定は 30 分)。

非アクティブ エージングは、最後のパケットが確認されてからフローを削除するまでの時間を指定します。非アクティブ パラメータは、「失効した」フローのフロー キャッシュをクリアして、(リソース不足により)新しいフローが長時間停止しないようにします。非アクティブ タイムアウト設定は通常、秒単位で設定されます(デフォルト設定は 15 秒)。

NetFlow 統計情報収集機能の設定例

Switch# config t

次に、設定を変更して NetFlow スイッチングをイネーブルにする例を示します。また、フロー統計情報をエクスポートして、IP アドレスが 40.0.0.2 のワークステーションの UDP ポート 9991 で処理する例を示します。この例では、既存の NetFlow 統計情報がクリアされるため、show ip cache flow コマンドで NetFlow スイッチング統計情報の正確なサマリーが確実に表示されます。

```
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config) # ip route-cache flow
Switch(config) # ip flow-export destination 40.0.0.2 9991
Switch(config) # ip flow-export version 5
Switch(config)# end
Switch# show ip flow export
Flow export is enabled
 Exporting flows to 40.0.0.2 (9991)
 Exporting using source IP address 40.0.0.1
 Version 5 flow records
 2 flows exported in 1 udp datagrams
 0 flows failed due to lack of export packet
 O export packets were sent up to process level
 0 export packets were dropped due to no fib
 O export packets were dropped due to adjacency issues
 O export packets were dropped due to fragmentation failures
 0 export packets were dropped due to encapsulation fixup failures
Switch#
Switch# show ip cache flow
IP Flow Switching Cache, 17826816 bytes
 69 active, 262075 inactive, 15087 added
 4293455 ager polls, 0 flow alloc failures
 Active flows timeout in 30 minutes
 Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 1081480 bytes
 0 active, 65536 inactive, 0 added, 0 added to flow
 O alloc failures, O force free
 1 chunk, 1 chunk added
 last clearing of statistics never
Protocol
              Total Flows Packets Bytes Packets Active(Sec) Idle(Sec)
                             167 40
2 40
                       /Sec
                              /Flow /Pkt /Sec /Flow
                                                              /Flow
              Flows
                                      40 0.0
48 0.0
                                                      20.9
                                                               11.9
TCP-Telnet
                28
                       0.0
                                                      6.2
                                                                15.4
TCP-other
               185
                        0.0
UDP-DNS
                 4
                         0.0
                                    1
                                               0.0
                                                        0.0
                                                                15.5
                        0.0 3396586
                                      46 91831.3
                                                                15.9
                                                     139.3
              13466
IIDP-other
               97
                                                      2.3
                       0.0 2 95 0.0
                                                               15.1
                 1
                       0.0
                                   2 40
                                               0.0
TGMP
                                                        0.9
IP-other
                     0.0 38890838
0.0 5992629
                                       46 87453.0 1354.5
46 179284.3 227.8
                1120
                                                                24.0
Total:
              14901
                                        46 179284.3
                                                      227.8
SrcIf
           SrcIPaddress DstIf
                                       DstIPaddress Pr SrcP DstP Pkts
                                       DstIPaddress
                                                     Pr SrcP DstP Pkts
            SrcIPaddress DstIf
                          Gi6/1
                                                     11 4001 4001
Gi 6/2
            30.20.1.18
                                       30.10.1.18
                                                                  537K
                        Gi6/1
                                                   11 4001 4001
Gi6/2
           30.20.1.19
                                      30.10.1.19
                                      30.10.1.16
Gi6/2
           30.20.1.16
                         Gi6/1
                                                     11 4001 4001 537K
                         Gi6/1
Gi6/2
            30.20.1.17
                                       30.10.1.17
                                                     11 4001 4001
                                                                   537K
                                                     11 4001 4001
                                                                  537K
                                       30.10.1.20
Gi6/2
            30.20.1.20
                          Gi6/1
                         Gi6/1
                                      30.10.1.10
                                                     11 4001 4001
                                                                  539K
Gi 6/2
            30.20.1.10
Gi6/2
           30.20.1.11
                         Gi6/1
                                      30.10.1.11
                                                     11 4001 4001 539K
                                                     11 4001 4001
                                                                  539K
Gi6/2
            30.20.1.14
                         Gi6/1
                                      30.10.1.14
Gi6/2
            30.20.1.15
                          Gi6/1
                                       30.10.1.15
                                                      11 4001 4001
                         Gi6/1
                                                     11 4001 4001
                                                                  539K
                                       30.10.1.12
Gi 6/2
            30.20.1.12
           30.20.1.13
                                      30.10.1.13
Gi6/2
                         Gi6/1
                                                     11 4001 4001
Gi5/48
           171.69.23.149 Local
                                      172.20.64.200 06 8214 0017
                                                                  759
Gi6/1
            30.10.1.12 Gi6/2
                                       30.20.1.12 11 4001 4001
                                                                   539K
                                                      11 4001 4001
Gi6/1
            30.10.1.13
                          Gi6/2
                                       30.20.1.13
                                                                    539K
                                      30.20.1.14 11 4001 4001
           30.10.1.14 Gi6/2
                                                                  539K
Gi 6/1
```

Gi6/1	30.10.1.15	Gi6/2	30.20.1.15	11 4001 4001 539K
Gi6/1	30.10.1.10	Gi6/2	30.20.1.10	11 4001 4001 539K
Gi6/1	30.10.1.11	Gi6/2	30.20.1.11	11 4001 4001 539K
Gi6/1	30.10.1.20	Gi6/2	30.20.1.20	11 4001 4001 537K
Gi6/1	30.10.1.16	Gi6/2	30.20.1.16	11 4001 4001 537K
Gi6/1	30.10.1.17	Gi6/2	30.20.1.17	11 4001 4001 537K
Gi6/1	30.10.1.18	Gi6/2	30.20.1.18	11 4001 4001 537K
Gi6/1	30.10.1.19	Gi6/2	30.20.1.19	11 4001 4001 537K
Switch#				

NetFlow の設定例

ここでは、次の基本的な設定例を提供します。

- NetFlow イネーブル化方式のサンプル (p.48-15)
- NetFlow 集約設定のサンプル (p.48-15)
- ルータベース集約方式の NetFlow 最小プレフィクス マスクのサンプル (p.48-17)

NetFlow イネーブル化方式のサンプル



(注)

Catalyst 4500 スイッチ上では、インターフェイス単位の NetFlow のイネーブル化がサポートされていません。

次に、NetFlow をグローバルにイネーブルにする例を示します。

Switch# configure terminal
Switch(config)# ip flow ingress

次に、予測フィールドをサポートする NetFlow をイネーブルにする例を示します。

Switch# configure terminal
Switch(config)# ip flow ingress infer-fields

NetFlow 集約設定のサンプル

ここでは、次の集約キャッシュ設定例を示します。

- AS の設定 (p.48-16)
- 宛先プレフィクスの設定 (p.48-16)
- プレフィクスの設定 (p.48-16)
- プロトコル ポートの設定 (p.48-16)
- 送信元プレフィクスの設定 (p.48-16)

AS の設定

次に、AS の集約キャッシュに、200 秒の非アクティブ タイムアウト、45 分のキャッシュ アクティブ タイムアウト、エクスポート宛先 IP アドレス 10.42.42.1、および宛先ポート 9992 を設定する例を示します。

```
Switch(config)# ip flow-aggregation cache as
Switch(config-flow-cache)# cache timeout inactive 200
Switch(config-flow-cache)# cache timeout active 45
Switch(config-flow-cache)# export destination 10.42.42.1 9992
Switch(config-flow-cache)# enabled
```

宛先プレフィクスの設定

次に、宛先プレフィクスの集約キャッシュに、200 秒の非アクティブ タイムアウト、45 分のキャッシュ アクティブ タイムアウト、エクスポート宛先 IP アドレス 10.42.42.1、および宛先ポート 9992 を設定する例を示します。

```
Switch(config)# ip flow-aggregation cache destination-prefix
Switch(config-flow-cache)# cache timeout inactive 200
Switch(config-flow-cache)# cache timeout active 45
Switch(config-flow-cache)# export destination 10.42.42.1 9992
Switch(config-flow-cache)# enabled
```

プレフィクスの設定

次に、プレフィクスの集約キャッシュに、200 秒の非アクティブ タイムアウト、45 分のキャッシュ アクティブ タイムアウト、エクスポート宛先 IP アドレス 10.42.42.1、および宛先ポート 9992 を設定する例を示します。

```
Switch(config)# ip flow-aggregation cache prefix
Switch(config-flow-cache)# cache timeout inactive 200
Switch(config-flow-cache)# cache timeout active 45
Switch(config-flow-cache)# export destination 10.42.42.1 9992
Switch(config-flow-cache)# enabled
```

プロトコル ポートの設定

次に、プロトコル ポートの集約キャッシュに、200 秒の非アクティブ タイムアウト、45 分のキャッシュ アクティブ タイムアウト、エクスポート宛先 IP アドレス 10.42.42.1、および宛先ポート 9992 を設定する例を示します。

```
Switch(config)# ip flow-aggregation cache protocol-port
Switch(config-flow-cache)# cache timeout inactive 200
Switch(config-flow-cache)# cache timeout active 45
Switch(config-flow-cache)# export destination 10.42.42.1 9992
Switch(config-flow-cache)# enabled
```

送信元プレフィクスの設定

次に、送信元プレフィクスの集約キャッシュに、200 秒の非アクティブ タイムアウト、45 分のキャッシュ アクティブ タイムアウト、エクスポート宛先 IP アドレス 10.42.42.1、および宛先ポート 9992 を設定する例を示します。

```
Switch(config)# ip flow-aggregation cache source-prefix
Switch(config-flow-cache)# cache timeout inactive 200
Switch(config-flow-cache)# cache timeout active 45
Switch(config-flow-cache)# export destination 10.42.42.1 9992
Switch(config-flow-cache)# enabled
```

ルータベース集約方式の NetFlow 最小プレフィクス マスクのサンプル

ここでは、NetFlow 最小プレフィクス マスク集約キャッシュの設定例を示します。

- prefix 集約方式
- destination-prefix 集約方式
- source-prefix 集約方式

prefix 集約方式

次に、prefix 集約キャッシュの設定例を示します。

```
!
ip flow-aggregation cache prefix
mask source minimum 24
mask destination minimum 28
```

この例では、次の設定が前提になっています。

```
ip route 118.42.20.160 255.255.255.224 110.42.13.2 ip route 122.16.93.160 255.255.255.224 111.22.21.2
```

両方のルートがスイッチ上のルーティング テーブルに 27 ビットのサブネット マスクを持ちます。

118.42.20.160 サブネットから、送信元 IP アドレスが 27 ビットのマスクに一致し、宛先 IP アドレスが 28 ビットのマスクに一致する 122.16.93.160 サブネットに移動するフローは、キャッシュ統計情報で一緒に集約されます。

destination-prefix 集約方式

```
次に、destination-prefix 集約キャッシュの設定例を示します。
```

```
!
ip flow-aggregation cache destination-prefix
mask destination minimum 32
```

source-prefix 集約方式

次に、source-prefix 集約キャッシュの設定例を示します。

```
ip flow-aggregation cache source-prefix mask source minimum 30\,
```

NetFlow の設定例



CHAPTER

49

RMON の設定

この章では、Catalyst 4500 シリーズ スイッチにリモート ネットワーク モニタリング (RMON) を設定する方法を説明します。RMON は、RMON 適合コンソール システムとネットワーク プローブ 間で交換可能な統計情報と機能のセットを定義する標準モニタリング仕様です。RMON は、総合的なネットワーク障害診断、計画、およびパフォーマンス調整情報を提供します。



ここで使用するコマンドの構文および使用方法の詳細については、次の URL にある『Cisco IOS Configuration Fundamentals Command Reference』Release 12.4 を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124tcr/tcf_r/index.htm

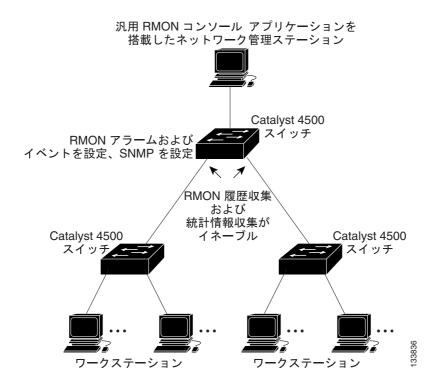
この章の内容は、次のとおりです。

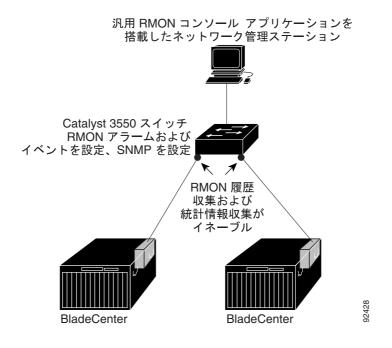
- RMON の概要 (p.49-2)
- RMON の設定 (p.49-4)
- RMON ステータスの表示 (p.49-7)

RMON の概要

RMON は、さまざまなネットワーク エージェントとコンソール システムでネットワーク モニタリング情報を交換できる Internet Engineering Task Force (IETF; インターネット技術特別調査委員会)の標準モニタリング仕様です。スイッチで RMON 機能を Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル)エージェントとともに使用して、接続しているすべての LAN セグメントでスイッチ間のすべてのトラフィック フローを監視できます。

図 49-1 リモート モニタリングの例





スイッチは次の RMON グループ (RFC 1757 で定義)をサポートします。

- 統計情報 (RMON グループ 1) インターフェイス上のイーサネット、ファスト イーサネット、およびギガビット イーサネットの統計情報を収集
- 履歴 (RMON グループ 2) イーサネット、ファスト イーサネット、およびギガビット イーサネット インターフェイスについて、指定したポーリング間隔で、統計情報の履歴グループを収集
- アラーム (RMON グループ 3) 特定の MIB (管理情報ベース)オブジェクトを指定した間隔で監視し、指定した値 (上昇しきい値)でアラームをトリガーし、別の値 (下限しきい値)でアラームをリセットします。アラームはイベントとともに使用できます。アラームがトリガーしたイベントによってログ エントリや SNMP トラップを生成できます。
- イベント(RMON グループ9) アラームによってイベントがトリガーされたときのアクションを指定します。ログ エントリや SNMP トラップの生成があります。

Cisco IOS Release 12.2(31)SG でサポートされるスイッチはハードウェア カウンタを使用して RMON データを処理します。このため、効率的なモニタリングが可能で、処理パワーは少なくて済みます。

RMON の設定

ここでは、スイッチに RMON を設定する方法を説明します。内容は次のとおりです。

- デフォルトの RMON 設定 (p.49-4)
- RMON アラームとイベントの設定 (p.49-4)
- インターフェイス設定する RMON 収集 (p.49-5)

デフォルトの RMON 設定

デフォルトでは RMON はディセーブルです。アラームやイベントは設定されていません。 RMON だけがスイッチでサポートされています。

RMON アラームとイベントの設定

CLI(コマンドライン インターフェイス) または SNMP 適合の NMS(ネットワーク管理ステーション)を使用すると、スイッチに RMON を設定できます。 NMS で汎用 RMON コンソール アプリケーションを使用して RMON のネットワーク管理機能を利用することを推奨します。 スイッチで SNMPを設定して、RMON MIB オブジェクトにアクセスできるようにする必要もあります。 詳細については、第 47 章「SNMP の設定」を参照してください。

RMON アラームおよびイベントをイネーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	rmon alarm number variable interval {absolute	MIB オブジェクトにアラームを設定します。
	delta} rising-threshold value [event-number] falling-threshold value [event-number] [owner string]	 number には、アラーム番号を指定します。有効範囲は 1 ~ 65535 です。
		• variable には、監視する MIB オブジェクトを指定します。
		• <i>interval</i> には、アラームが MIB 変数をモニタする時間 を秒単位で指定します。有効範囲は 1 ~ 4294967295 秒 です。
		• それぞれの MIB 変数を直接テストするには absolute キーワードを指定します。MIB 変数のサンプルの変化 をテストするには delta キーワードを指定します。
		 value には、アラームがトリガーする値とリセットする値を指定します。value の上昇しきい値と下限しきい値の有効範囲は、-2147483648 ~ 2147483647 です。
		• (任意) event-number には、上昇しきい値または下限し きい値を超過する際にトリガーするイベント番号を指 定します。
		• (任意) owner string には、アラームのオーナーを指定します。

	コマンド	目的
ステップ 3	rmon event number [description string] [log]	RMON イベント テーブルで RMON イベント番号に関連付
	[owner string] [trap community]	けられたイベントを追加します。
		number には、イベント番号を指定します。有効範囲は 1 ~ 65535 です。
		• (任意) description <i>string</i> には、イベントの説明を指定します。
		• (任意)イベントがトリガーされた際に RMON ログ エントリを生成するには、log キーワードを使用します。
		• (任意)owner string には、このイベントのオーナーを 指定します。
		• (任意) community には、このとラップに使用する SNMP コミュニティ ストリングを指定します。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	入力を確認します。
ステップ 6	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存し
		ます。

アラームをディセーブルにするには、設定したアラームごとに no rmon alarm number グローバルコンフィギュレーション コマンドを使用します。設定したすべてのアラームを一度にディセーブルにすることはできません。 イベントをディセーブルにするには、no rmon event number グローバルコンフィギュレーション コマンドを使用します。アラームおよびイベントの詳細と相互作用については、RFC 1757 を参照してください。

任意の MIB オブジェクトにアラームを設定できます。次に、rmon alarm コマンドを使用して RMON アラーム番号 10 を設定する例を示します。このアラームはディセーブルになるまで MIB 変数 ifEntry.20.1 を 20 秒ごとに監視し、変数の上昇または下降の変化をチェックします。ifEntry.20.1 の 値が MIB カウンタにおいて 15 以上増加すると(たとえば 100000 から 100015 になると)、アラームがトリガーされます。次にアラームはイベント番号 1 をトリガーします。このイベント番号は rmon event コマンドで設定します。ログ エントリや rmon rmo

 ${\tt Switch(config)\#\ rmon\ alarm\ 10\ ifEntry.20.1\ 20\ delta\ rising-threshold\ 15\ 1} \\ {\tt falling-threshold\ 0\ owner\ jjohnson}$

次に、 $rmon\ event\$ コマンドを使用して $RMON\$ イベント番号 1 を作成する例を示します。イベントは $High\ ifOutErrors\$ として定義され、イベントがアラームによってトリガーされるとログ エントリが生成されます。ユーザ $ijones\$ は、このコマンドでイベント テーブルに作成された列のオーナーです。次も、イベントがトリガーされると $SNMP\$ トラップを生成する例です。

Switch(config) # rmon event 1 log trap eventtrap description "High ifOutErrors" owner jjones

インターフェイス設定する RMON 収集

収集情報を表示するには、まず RMON アラームおよびイベントを設定する必要があります。 インターフェイスのグループ履歴統計情報を収集するには、次の作業を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	履歴を収集するインターフェイスを指定して、インターフェイスコンフィギュレーション モードを開始します。
ステップ 3	rmon collection history index [buckets bucket-number] [interval seconds] [owner ownername]	指定したバケット数と期間での履歴収集をイネーブルにします。 • index には、統計情報の RMON グループを指定します。有効範囲は 1 ~ 65535 です。 • (任意) buckets bucket-number には、RMON 統計情報収集履歴グループに必要なバケットの最大数を指定します。指定できる範囲は 1 ~ 65535 です。デフォルトは50 バケットです。 • (任意) interval seconds には、ポーリング サイクルの時間を秒単位で指定します。 • (任意) owner ownername には、RMON 統計情報グループのオーナー名を指定します。 履歴収集をディセーブルにするには、no rmon collection history index インターフェイス コンフィギュレーションコマンドを使用します。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	入力を確認します。
ステップ 6	show rmon history	スイッチの履歴テーブルの内容を表示します。
ステップ 7	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

インターフェイスのグループイーサネット統計情報を収集するには、次の作業を実行します。

コマンド		目的
configure terminal		グローバル コンフィギュレーション モードを開始します。
interface interface-id		統計情報を収集するインターフェイスを指定して、インターフェイスコンフィギュレーション モードを開始します。
rmon collection stats ind	lex [owner ownername]	インターフェイスの RMON 統計情報収集をイネーブルに します。
		 index には、RMON 統計情報グループを指定します。有 効範囲は1~65535です。
		 (任意) owner ownername には、RMON 統計情報グループのオーナー名を指定します。
		グループ イーサネット統計情報の収集をディセーブルにするには、no rmon collection stats <i>index</i> インターフェイスコンフィギュレーション コマンドを使用します。
end		特権 EXEC モードに戻ります。
show running-config		入力を確認します。
show rmon statistics		スイッチの統計情報テーブルの内容を表示します。
copy running-config star	rtup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

RMON ステータスの表示

RMON ステータスを表示するには、表 49-1 に示す特権 EXEC コマンドのいずれかを使用します。

表 49-1 RMON ステータスの表示コマンド

コマンド	目的
show rmon	一般的な RMON 統計情報を表示します。
show rmon alarms	RMON アラーム テーブルを表示します。
show rmon events	RMON イベント テーブルを表示します。
show rmon history	RMON 履歴テーブルを表示します。
show rmon statistics	RMON 統計情報テーブルを表示します。

■ RMON ステータスの表示



CHAPTER

50

診断の実行

Catalyst 4500 シリーズ スイッチの診断では、ライブ ネットワークに接続しながら、ご使用のシステムのハードウェア コンポーネント (シャーシ、スーパーバイザ エンジン、モジュール、および Application Specific Integrated Circuit [ASIC; 特定用途向け集積回路]) の機能をテストし、検証します。診断では、ハードウェア コンポーネントをテストして、データ パスおよび制御信号を検証するパケット スイッチング テストが行われます。診断テストは、中断を伴わないテストで(Power-on Self-Test [POST; 電源投入時自己診断テスト] を除く)、さまざまな時点で行われます。テストには、システムのステータスをモニタするのにバックグラウンドで継続して実行されるもの(スイッチング モジュールのテストなど)もありますが、一度だけ実行されるものもあります。

この章では、Catalyst 4500 シリーズ スイッチ上の次のタイプの診断について説明します。

- オンライン診断 (p.50-1)
- POST診断 (p.50-3)



この章のスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univered/cc/td/doc/product/software/ios122sr/cr/index.htm

オンライン診断

オンライン診断テストでは、ラインカード上のすべてのポートが正常に稼働していることを確認します。このテストにより、ラインカードの前面パネルポートへのパスに障害があるかどうかは検出できますが、パス上のどこで問題が発生したのかは解明できません。

このテストは、システムの稼働中に実行されるためオンラインと呼ばれます。



このテストは、スタブチップを持つラインカードに対してのみ実行されます。

オンライン診断は、ラインカードの起動時に一度だけ実行されます。 ラインカードの挿入時、またはシャーシの電源投入時に実行できます。 オンライン診断は、CPU からラインカードのすべてのポートにパケットを送信することによって実行されます。このパケットは *loopback* とマークされているため、CPU はパケットがポートから戻されることを予測します。パケットは、まずスーパーバイザ エンジン上の ASIC に送信され、次にシャーシのバックプレーンおよびラインカード上のスタブ チップを経由して、Physical Sublayer (PHY: 物理サブレイヤ)に送信されます。PHY は、同じパスでパケットを返送します。



前面パネルポートでは、パケットの着信および送信は行われません。

オンライン診断によるトラブルシューティング

ラインカードに障害が発生する条件は、次のとおりです。

- すべてのポートに障害がある。
- スタブチップ上のすべてのポートに障害がある。
- 1 つのポートだけに障害がある。

上記のすべての状況で、ラインカードのステータスは show module コマンド出力に障害として表示されます。

Switch# show mod Chassis Type : WS-C4507R Power consumed by backplane : 40 Watts Mod Ports Card Type

		Card Type				del 	Serial No.
1 2 3 4 5 6 7	6 6 48 48 48	Sup II+10GE 10G Sup II+10GE 10G 100BaseX (SFP) 10/100BaseTX (R 10/100BaseTX (R 10/100BaseTX (R	E (X2), 10 E (X2), 10 J45)V J45)V J45)V	00BaseX (;	SFP) WS SFP) WS WS WS WS	-X4013+10GE -X4013+10GE -X4248-FE-SFP -X4148-RJ45V -X4148-RJ45V -X4148-RJ45V -X4524-GB-RJ45V	JAB091502G0 JAB091502FC JAB093305RP JAE070717E5 JAE061303U3 JAE061303WJ
						Sw -+	
2 0 3 0 4 0 5 0 6 0	000b.5i 0005.9a 000c.30 0008.a3	E27.8b80 to 000b E27.8b86 to 000b a80.6810 to 0005 016.aae0 to 000c Ba3.4e70 to 0008 Ba3.3fa0 to 0008 50e.3e78 to 0030	.5f27.8b8b .9a80.683f .3016.ab0f .a3a3.4e9f .a3a3.3fcf	0.2 12.2 0.4 2.6 1.6	. ,	, , ,	Ok Ok Ok Faulty Ok
		ndancy role	_			ancy status	
	Activ	ve Supervisor Iby Supervisor	SSO		Active Standb		

障害のあるラインカードをトラブルシューティングするには、次の作業を実行します。

ステップ 1 show diagnostic result module 3 コマンドを入力します。

障害のあるラインカードがシャーシに挿入された場合、診断は失敗し、次のような出力が表示されます。

ラインカードの Return Materials Authorization (RMA)を入手し、TAC に連絡します。ステップ 2 および 3 は省略します。

ただし、出力が次のような場合は、

```
module 3:
   Overall diagnostic result: PASS

Test results: (. = Pass, F = Fail, U = Untested)

1) linecard-online-diag -----> .
```

1)ラインカードが最後にシャーシに挿入されたとき、または2)スイッチの電源が投入されたときのいずれかで、ラインカードがオンライン診断に合格しました([.] としてレポートされる)。詳細な検査が必要となります。

ステップ2 別のスーパーバイザエンジンカードを挿入し、ラインカードを再度挿入します。

ラインカードがテストに合格する場合、スーパーバイザ エンジン カードに不具合があります。

スーパーバイザ エンジンの RMA を入手し、TAC に連絡します。ステップ 3 は省略します。

スーパーバイザ エンジン カードではオンライン診断が実行されないため、スーパーバイザ エンジン カードに障害があるかどうかをテストするのに #show diagnostic module 1 コマンドを使用できません。

ステップ3 ラインカードを別のシャーシに再度挿入します。

ラインカードがテストに合格する場合、問題はシャーシに関連しています。

シャーシの RMA を入手して、TAC に連絡します。

POST 診断

ここでは、次の内容について説明します。

- 概要 (p.50-4)
- POST 結果のサンプル (p.50-4)
- Supervisor Engine V-10GE の POST 結果 (p.50-9)
- 障害の原因およびトラブルシューティング(p.50-14)

概要

すべての Catalyst 4500 シリーズ スイッチでは、スーパーバイザ エンジンが起動すると必ず POST が実行されます。POST は、スーパーバイザ スイッチング エンジン、それに対応するパケット メモリ、およびその他のオンボードのハードウェア コンポーネントの基本的なハードウェア機能についてテストします。スイッチの動作にとってスーパーバイザ エンジンのヘルスは特に重要であるため、POST の結果はスイッチの起動方法に影響を与えます。スイッチは、marginal ステートまたはfaulty ステートで起動する可能性があります。

現在 POST をサポートしているのは、次のスーパーバイザ エンジンです。

- WS-X4014
- WS-X4515
- WS-X4516
- WS-X4516-10GE
- WS-X4013+
- WS-X4013+TS
- WS-X4013+10GE
- WS-C4948G
- WS-C4948G-10GE
- ME-4924-10GE
- WS-X45-SUP6-E

POST 結果は、成功の場合は [.] または [Pass]、失敗の場合は [F]、テストされていない場合は [U] と表示されます。

POST 結果のサンプル

すべてのスーパーバイザ エンジンに対して、POST は CPU、トラフィック、システム、システム メモリ、および機能についてのテストを実行します。

CPU テストでは、POST は使用中のスーパーバイザ SEEPROM、温度センサ、および Ethernet-end-of-band channel (eobc) の適切なアクティビティを検証します。

次に、WS-X4013+TS 以外のすべてのスーパーバイザ エンジン上での CPU サブシステム テストの 出力例を示します。

```
[..]
Cpu Subsystem Tests ...
seeprom: . temperature_sensor: . eobc: .
[..]
```

次に、WS-X4013+TS スーパーバイザ エンジン上での CPU サブシステム テストの出力例を示します。

```
[..]
Cpu Subsystem Tests ...
seeprom: .temperature_sensor: .
[..]
```

トラフィック テストでは、POST は CPU からスイッチにパケットを送信します。これらのパケットはスイッチ コア内を数回ループして、スイッチング、およびレイヤ 2 とレイヤ 3 の機能を検証します。ハードウェア障害を的確に切り離すため、ループ バックはスイッチ ポートの内部と外部の両方で行われます。

次に、スーパーバイザ エンジン WS-X4516、WS-X4516-10GE、WS-X4013+10GE、WS-C4948G-10GE 上でのスイッチ ポートのレイヤ 2 トラフィック テストの出力例を示します。

```
Port Traffic: L2 Serdes Loopback ...

0: . 1: . 2: . 3: . 4: . 5: . 6: . 7: . 8: . 9: . 10: . 11: .

12: . 13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: . 22: . 23: .

24: . 25: . 26: . 27: . 28: . 29: . 30: . 31: . 32: . 33: . 34: . 35: .

36: . 37: . 38: . 39: . 40: . 41: . 42: . 43: . 44: . 45: . 46: . 47: .
```

次に、スーパーバイザ エンジン WS-X4013+TS、WS-X4515、WS-X4013+、WS-X4014、WS-C4948G 上でのスイッチ ポートのレイヤ 2 トラフィック テストの出力例を示します。

```
Port Traffic: L2 Serdes Loopback ...

0: . 1: . 2: . 3: . 4: . 5: . 6: . 7: . 8: . 9: . 10: . 11: .

12: . 13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: . 22: . 23: .

24: . 25: . 26: . 27: . 28: . 29: . 30: . 31:
```

POST は、スイッチのパケット メモリおよびシステム メモリ上でもテストを行います。これらのテストは、1 から昇順で動的に番号が付けられ、それぞれ別のメモリを表します。

次に、システム メモリ テストの出力例を示します。

```
Switch Subsystem Memory ...

1: . 2: . 3: . 4: . 5: . 6: . 7: . 8: . 9: . 10: . 11: . 12: .

13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: . 22: . 23: . 24: .

25: . 26: . 27: . 28: . 29: . 30: . 31: . 32: . 33: . 34: . 35: . 36: .

37: . 38: . 39: . 40: . 41: . 42: . 43: . 44: . 45: . 46: . 47: . 48: .

49: . 50: . 51: . 52: . 53: . 54: . 55: .
```

また、POST は Netflow サービス カード(Supervisor Engine IV と Supervisor Engine V)および Netflow サービス機能(Supervisor Engine V-10GE)についてもテストします。これらのテストによる障害は、スイッチの機能には影響しないため(Netflow 機能が使用できなくなること以外) 重要度の低いものとして扱われます。

```
Netflow Services Feature ...
se: . cf: . 52: . 53: . 54: . 55: . 56: . 57: . 58: . 59: . 60: . 61: .
62: . 63: . 64: . 65: .
```



Superbisor Engine VI-E は、CPU サブシステム テスト、レイヤ 3 およびレイヤ 2 トラフィック テスト、メモリ テストなど、以前のスーパーバイザの POST 機能のほとんどを保持します。冗長システムの冗長ポートはテストされません。すべての POST 診断は、テストを実行しているスーパーバイザに対してローカルです。

次に、WS-X4516 スーパーバイザエンジンに関する出力例を示します。

Switch# show diagnostic result module 2 detail

```
module 2:
  Overall diagnostic result: PASS
  Test results: (. = Pass, F = Fail, U = Untested)
    1) supervisor-bootup ----> .
           Error code -----> 0 (DIAG_SUCCESS)
          Total run count -----> 1
           Last test execution time -----> Jul 20 2005 14:15:52
          First test failure time -----> n/a
          Last test failure time -----> n/a
           Last test pass time -----> Jul 20 2005 14:15:52
           Total failure count -----> 0
           Consecutive failure count -----> 0
Power-On-Self-Test Results for ACTIVE Supervisor
Power-on-self-test for Module 2: WS-X4516
 Port/Test Status: (. = Pass, F = Fail, U = Untested)
 Reset Reason: PowerUp RemoteDebug
Cpu Subsystem Tests ...
seeprom: . temperature_sensor: . eobc: .
Port Traffic: L2 Serdes Loopback ...
0: . 1: . 2: . 3: . 4: . 5: . 6: . 7: . 8: . 9: . 10: . 11: .
12: . 13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: . 22: . 23: .
24: . 25: . 26: . 27: . 28: . 29: . 30: . 31: . 32: . 33: . 34: . 35: . 36: . 37: . 38: . 39: . 40: . 41: . 42: . 43: . 44: . 45: . 46: . 47: .
Port Traffic: L2 Asic Loopback ...
0: . 1: . 2: . 3: . 4: . 5: . 6: . 7: . 8: . 9: . 10: . 11: .
12: . 13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: . 22: . 23: .
24: . 25: . 26: . 27: . 28: . 29: . 30: . 31: . 32: . 33: . 34: . 35: . 36: . 37: . 38: . 39: . 40: . 41: . 42: . 43: . 44: . 45: . 46: . 47: .
Port Traffic: L3 Asic Loopback ...
 0: . 1: . 2: . 3: . 4: . 5: . 6: . 7: . 8: . 9: . 10: . 11: .
12: . 13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: . 22: . 23: . 24: . 25: . 26: . 27: . 28: . 29: . 30: . 31: . 32: . 33: . 34: . 35: .
36: . 37: . 38: . 39: . 40: . 41: . 42: . 43: . 44: . 45: . 46: . 47: .
Switch Subsystem Memory \dots
1: . 2: . 3: . 4: . 5: . 6: . 7: . 8: . 9: . 10: . 11: . 12: .
13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: . 22: . 23: . 24: . 25: . 26: . 27: . 28: . 29: . 30: . 31: . 32: . 33: . 34: . 35: . 36: .
37: . 38: . 39: . 40: . 41: . 42: . 43: . 44: . 45: . 46: . 47: . 48: .
49: . 50: . 51: . 52: . 53: . 54: . 55: .
Module 2 Passed
    2) packet-memory-bootup -----> U
           Error code -----> 0 (DIAG_SUCCESS)
```

■ Catalyst 4500 シリーズ スイッチ Cisco IOS ソフトウェア コンフィギュレーション ガイド

Total run count -----> 0

```
Last test execution time ----> n/a
         First test failure time ----> n/a
         Last test failure time -----> n/a
         Last test pass time -----> n/a
         Total failure count -----> 0
         Consecutive failure count -----> 0
packet buffers on free list: 64557 bad: 0 used for ongoing tests: 979
Exhaustive packet memory tests did not run at bootup.
Bootup test results:5
No errors.
   3) packet-memory-ongoing ----> U
         Error code -----> 0 (DIAG_SUCCESS)
         Total run count -----> 0
         Last test execution time -----> n/a
         First test failure time -----> n/a
         Last test failure time -----> n/a
         Last test pass time -----> n/a
         Total failure count -----> 0
         Consecutive failure count -----> 0
packet buffers on free list: 64557 bad: 0 used for ongoing tests: 979
Packet memory errors: 0 0
Current alert level: green
Per 5 seconds in the last minute:
   0 0 0 0 0 0 0 0 0 0
   0 0
Per minute in the last hour:
   0 0 0 0 0 0 0 0 0
   0 0 0 0 0 0 0 0 0 0
   0 0 0 0 0 0 0 0 0 0
   0 0 0 0 0 0 0 0 0
   0 0 0 0 0 0 0 0 0 0
   0 0 0 0 0 0 0 0 0 0
Per hour in the last day:
   0 0 0 0 0 0 0 0 0 0
   0 0 0 0 0 0 0 0 0 0
   0 0 0 0
Per day in the last 30 days:
   0 0 0 0 0 0 0 0 0
   0 0 0 0 0 0 0 0 0 0
   0 0 0 0 0 0 0 0 0 0
Direct memory test failures per minute in the last hour:
   0 0 0 0 0 0 0 0 0 0
   0 0 0 0 0 0 0 0 0 0
   0 0 0 0 0 0 0 0 0
   0 0 0 0 0 0 0 0 0
   0 0 0 0 0 0 0 0 0 0
   0 0 0 0 0 0 0 0 0 0
Potential false positives: 0 0
 Ignored because of rx errors: 0 0
 Ignored because of cdm fifo overrun: 0 0
 Ignored because of oir: 0 0
 Ignored because isl frames received: 0 0
 Ignored during boot: 0 0
 Ignored after writing hw stats: 0 0
 Ignored on high gigaport: 0
Ongoing diag action mode: Normal
Last 1000 Memory Test Failures:
Last 1000 Packet Memory errors:
First 1000 Packet Memory errors:
```

Switch#

次に、WS-X45-SUP6-E スーパーバイザエンジンに関する出力例を示します。

```
Switch# show diagnostic result module 3 detail
module 3: SerialNo : XXXXXXXXXX
 Overall diagnostic result: PASS
 Test results: (. = Pass, F = Fail, U = Untested)
   1) supervisor-bootup ---->
        Error code -----> 0 (DIAG_SUCCESS)
        Total run count ----> 1
        Last test execution time ----> Oct 01 2007 17:37:04
        First test failure time ----> n/a
        Last test failure time -----> n/a
        Last test pass time -----> Oct 01 2007 17:37:04
        Total failure count ----> 0
        Consecutive failure count ---> 0
Power-On-Self-Test Results for ACTIVE Supervisor
prod: WS-X45-SUP6-E part: XXXXXXXXX serial: XXXXXXXXX
Power-on-self-test for Module 3: WS-X45-SUP6-E
Test Status: (. = Pass, F = Fail, U = Untested)
CPU Subsystem Tests ...
seeprom: Pass
Traffic: L3 Loopback ...
Test Results: Pass
Traffic: L2 Loopback ...
Test Results: Pass
Switching Subsystem Memory \dots
Packet Memory Test Results: Pass
Module 3 Passed
   2) linecard-online-diag ----->
        Error code -----> 0 (DIAG_SUCCESS)
        Total run count -----> 1
        Last test execution time ----> Oct 01 2007 17:37:04
        First test failure time ----> n/a
        Last test failure time ----> n/a
        Last test pass time -----> Oct 01 2007 17:37:04
        Total failure count ----> 0
        Consecutive failure count ---> 0
Slot Ports Card Type
                                           Diag Status
                                                         Diag Details
3 6 Sup 6-E 10GE (X2), 1000BaseX (SFP) Skipped
                                                         Packet memory
Detailed Status
_____
. = Pass
                  U = Unknown
L = Loopback failure S = Stub failure
P = Port failure
E = SEEPROM failure
                  G = GBIC integrity check failure
Ports 1 2 3 4 5 6
```

Switch#

Supervisor Engine V-10GE の POST 結果

Supervisor Engine V-10GE (WS-X4516-10GE) では、POST は 10 ギガビット ポートの特別な冗長機能についてテストします。

ここでは、次の内容について説明します。

- アクティブ スーパーバイザ エンジン上での POST (p.50-9)
- アクティブ スーパーバイザ エンジンの POST 結果のサンプル (p.50-9)
- スタンバイ スーパーバイザ エンジン上での POST (p.50-11)
- スタンバイ スーパーバイザ エンジンの POST 表示のサンプル (p.50-12)

アクティブ スーパーバイザ エンジン上での POST

アクティブ スーパーバイザ エンジンは、起動時にスタンバイ スーパーバイザ エンジン (存在する場合)上のリモートの冗長 10 ギガビット ポートについてテストします。ポートのステータスは、[Remote TenGigabit Port Status] と表示されます。スタンバイ スーパーバイザ エンジンが存在しない場合は、リモートのポート ステータスは常に [Untested] と表示されます。これは新しいスタンバイスーパーバイザ エンジンが挿入されたあとも継続します。残りのテストは、ギガビット ポートの設定のみを使用して実施されます。

アクティブ スーパーバイザ エンジンで起動時の診断が完了したあとで、スタンバイ スーパーバイザ エンジンが取り外された場合、総合診断結果内のリモートのポート ステータスは [Untested] に変更されます。

アクティブ スーパーバイザ エンジンの POST 結果のサンプル

```
Switch# show diagnostic result module 1 detail
module 1:
 Overall diagnostic result: PASS
 Test results: (. = Pass, F = Fail, U = Untested)
   1) supervisor-bootup ----->
        Error code -----> 0 (DIAG_SUCCESS)
        Total run count -----> 1
        Last test execution time -----> Jul 19 2005 13:28:16
        First test failure time ----> n/a
        Last test failure time ----> n/a
        Last test pass time -----> Jul 19 2005 13:28:16
        Total failure count ----> 0
        Consecutive failure count ----> 0
Power-On-Self-Test Results for ACTIVE Supervisor
Power-on-self-test for Module 1: WS-X4516-10GE
Port/Test Status: (. = Pass, F = Fail, U = Untested)
Reset Reason: Software/User
Cpu Subsystem Tests ...
seeprom: . temperature_sensor: . eobc: .
```

```
Port Traffic: L3 Serdes Loopback ...
0: . 1: . 2: . 3: . 4: . 5: . 6: . 7: . 8: . 9: . 10: . 11: .
12: . 13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: . 22: . 23: .
24: . 25: . 26: . 27: . 28: . 29: . 30: . 31: . 32: . 33: . 34: . 35: .
36: . 37: . 38: . 39: . 40: . 41: . 42: . 43: . 44: . 45: . 46: . 47: .
Local 10GE Port 62: .
Local 10GE Port 63: .
Port Traffic: L2 Serdes Loopback ...
0: . 1: . 2: . 3: . 4: . 5: . 6: . 7: . 8: . 9: . 10: . 11: .
12: . 13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: . 22: . 23: .
24: . 25: . 26: . 27: . 28: . 29: . 30: . 31: . 32: . 33: . 34: . 35: .
36: . 37: . 38: . 39: . 40: . 41: . 42: . 43: . 44: . 45: . 46: . 47: .
48: . 49: . 50: . 51: .
Port Traffic: L2 Asic Loopback ...
0: . 1: . 2: . 3: . 4: . 5: . 6: . 7: . 8: . 9: . 10: . 11: .
12: . 13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: . 22: . 23: .
24: . 25: . 26: . 27: . 28: . 29: . 30: . 31: . 32: . 33: . 34: . 35: .
36: . 37: . 38: . 39: . 40: . 41: . 42: . 43: . 44: . 45: . 46: . 47: .
48: . 49: . 50: . 51: .
Switch Subsystem Memory ...
1: . 2: . 3: . 4: . 5: . 6: . 7: . 8: . 9: . 10: . 11: . 12: .
13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: . 22: . 23: . 24: .
25: . 26: . 27: . 28: . 29: . 30: . 31: . 32: . 33: . 34: . 35: . 36: .
37: . 38: . 39: . 40: . 41: . 42: . 43: . 44: . 45: . 46: . 47: . 48: .
49: . 50: . 51: .
Netflow Services Feature ...
se: . cf: . 52: . 53: . 54: . 55: . 56: . 57: . 58: . 59: . 60: . 61: .
62: . 63: . 64: . 65: .
Module 1 Passed
Remote TenGigabitPort status: Passed
   2) packet-memory-bootup -----> U
         Error code -----> 0 (DIAG_SUCCESS)
         Total run count -----> 0
         Last test execution time -----> n/a
         First test failure time -----> n/a
         Last test failure time -----> n/a
         Last test pass time -----> n/a
         Total failure count ----> 0
         Consecutive failure count -----> 0
packet buffers on free list: 64557 bad: 0 used for ongoing tests: 979
Exhaustive packet memory tests did not run at bootup.
Bootup test results:5
No errors.
   3) packet-memory-ongoing ----> U
         Error code -----> 0 (DIAG_SUCCESS)
         Total run count -----> 0
         Last test execution time -----> n/a
```

```
First test failure time -----> n/a
         Last test failure time -----> n/a
         Last test pass time -----> n/a
         Total failure count ----> 0
         Consecutive failure count ----> 0
packet buffers on free list: 64557 bad: 0 used for ongoing tests: 979
Packet memory errors: 0 0
Current alert level: green
Per 5 seconds in the last minute:
   0 0 0 0 0 0 0 0 0 0
Per minute in the last hour:
   0 0 0 0 0 0 0 0 0 0
   0 0 0 0 0 0 0 0 0 0
   0 0 0 0 0 0 0 0 0 0
   0 0 0 0 0 0 0 0 0 0
   0 0 0 0 0 0 0 0 0
   0 0 0 0 0 0 0 0 0 0
Per hour in the last day:
   0 0 0 0 0 0 0 0 0 0
   0 0 0 0 0 0 0 0 0 0
   0 0 0 0
Per day in the last 30 days:
   0 0 0 0 0 0 0 0 0 0
   0 0 0 0 0 0 0 0 0 0
   0 0 0 0 0 0 0 0 0
Direct memory test failures per minute in the last hour:
   0 0 0 0 0 0 0 0 0
   0 0 0 0 0 0 0 0 0 0
   0 0 0 0 0 0 0 0 0 0
   0 0 0 0 0 0 0 0 0
   0 0 0 0 0 0 0 0 0 0
   Potential false positives: 0 0
 Ignored because of rx errors: 0 0
 Ignored because of cdm fifo overrun: 0 0
 Ignored because of oir: 0 0
 Ignored because isl frames received: 0 0
 Ignored during boot: 0 0
 Ignored after writing hw stats: 0 0
 Ignored on high gigaport: 0
Ongoing diag action mode: Normal
Last 1000 Memory Test Failures:
Last 1000 Packet Memory errors:
First 1000 Packet Memory errors:
```

Switch#

スタンパイ スーパーパイザ エンジン上での POST

スーパーバイザ エンジンのポート 62 および 63 は、常に [Untested] または [U] のままです。スタンバイ スーパーバイザ エンジンでは、アクティブ スーパーバイザ エンジン上のリモートの 10 ギガビット ポートについてテストしないため、スタンバイ スーパーバイザ エンジン上のリモートの 10 ギガビット ポート ステータスは常に [Untested] です。スーパーバイザ エンジンは、ギガビット ポートの設定を使用して残りのテストを実行します。



冗長シャーシでは、すでに挿入されているスーパーバイザ エンジンでの並列 POST がサポートされます。ただし、最初のスーパーバイザ エンジンをロード中に 2 番めのスーパーバイザ エンジンを挿入すると、最初のスーパーバイザ エンジンは faulty IOS ステートでブートします (POST が打ち切られ、一部の POST テストがバイパスされます)。これは、複数のスーパーバイザ エンジンを同時起動した場合だけに発生します。先に装着したスーパーバイザ エンジンが POST を実行している間は、空のスーパーバイザ エンジン スロットに追加のスーパーバイザ エンジンを装着しないでください。POST シーケンスが終了すると、[Exiting to ios...] メッセージが表示されます。

スタンパイ スーパーパイザ エンジンの POST 表示のサンプル

```
Switch# show diagnostic result module 2 detail
module 2:
 Overall diagnostic result: PASS
 Test results: (. = Pass, F = Fail, U = Untested)
   1) supervisor-bootup -----> .
         Error code -----> 0 (DIAG SUCCESS)
         Total run count -----> 1
         Last test execution time -----> Jul 19 2005 13:29:44
         First test failure time -----> n/a
         Last test failure time -----> n/a
         Last test pass time -----> Jul 19 2005 13:29:44
         Total failure count ----> 0
         Consecutive failure count -----> 0
Power-On-Self-Test Results for ACTIVE Supervisor
Power-on-self-test for Module 2: WS-X4516-10GE
Port/Test Status: (. = Pass, F = Fail, U = Untested)
Reset Reason: OtherSupervisor Software/User
Cpu Subsystem Tests ...
seeprom: . temperature_sensor: . eobc: .
Port Traffic: L3 Serdes Loopback ...
0: . 1: . 2: . 3: . 4: . 5: . 6: . 7: . 8: . 9: . 10: . 11: .
12: . 13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: . 22: . 23: .
24: . 25: . 26: . 27: . 28: . 29: . 30: . 31: . 32: . 33: . 34: . 35: .
36: . 37: . 38: . 39: . 40: . 41: . 42: . 43: . 44: . 45: . 46: . 47: .
Local 10GE Port 62: U
Local 10GE Port 63: U
Port Traffic: L2 Serdes Loopback ...
0: . 1: . 2: . 3: . 4: . 5: . 6: . 7: . 8: . 9: . 10: . 11: .
12: . 13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: . 22: . 23: .
24: . 25: . 26: . 27: . 28: . 29: . 30: . 31: . 32: . 33: . 34: . 35: .
36: . 37: . 38: . 39: . 40: . 41: . 42: . 43: . 44: . 45: . 46: . 47: .
48: . 49: . 50: . 51: .
Port Traffic: L2 Asic Loopback ...
0: . 1: . 2: . 3: . 4: . 5: . 6: . 7: . 8: . 9: . 10: . 11: .
```

```
12: . 13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: . 22: . 23: .
24: . 25: . 26: . 27: . 28: . 29: . 30: . 31: . 32: . 33: . 34: . 35: .
36: . 37: . 38: . 39: . 40: . 41: . 42: . 43: . 44: . 45: . 46: . 47: .
48: . 49: . 50: . 51: .
Switch Subsystem Memory ...
1: . 2: . 3: . 4: . 5: . 6: . 7: . 8: . 9: . 10: . 11: . 12: . 13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: . 22: . 23: . 24: .
25: . 26: . 27: . 28: . 29: . 30: . 31: . 32: . 33: . 34: . 35: . 36: .
37: . 38: . 39: . 40: . 41: . 42: . 43: . 44: . 45: . 46: . 47: . 48: .
49: . 50: . 51: .
Netflow Services Feature ...
se: . cf: . 52: . 53: . 54: . 55: . 56: . 57: . 58: . 59: . 60: . 61: .
62: . 63: . 64: . 65: .
Module 2 Passed
Remote TenGigabitPort status: Untested
   2) packet-memory-bootup ----> U
         Error code -----> 0 (DIAG_SUCCESS)
         Total run count -----> 0
         Last test execution time ----> n/a
         First test failure time ----> n/a
         Last test failure time -----> n/a
         Last test pass time -----> n/a
         Total failure count ----> 0
         Consecutive failure count -----> 0
packet buffers on free list: 64557 bad: 0 used for ongoing tests: 979
Exhaustive packet memory tests did not run at bootup.
Bootup test results:5
No errors.
   3) packet-memory-ongoing ----> U
         Error code -----> 0 (DIAG_SUCCESS)
         Total run count -----> 0
         Last test execution time -----> n/a
         First test failure time -----> n/a
         Last test failure time -----> n/a
         Last test pass time -----> n/a
         Total failure count -----> 0
         Consecutive failure count ----> 0
packet buffers on free list: 64557 bad: 0 used for ongoing tests: 979
Packet memory errors: 0 0
Current alert level: green
Per 5 seconds in the last minute:
   0 0 0 0 0 0 0 0 0 0
   0 0
Per minute in the last hour:
   0 0 0 0 0 0 0 0 0 0
   0 0 0 0 0 0 0 0 0
   0 0 0 0 0 0 0 0 0 0
   0 0 0 0 0 0 0 0 0 0
   0 0 0 0 0 0 0 0 0
   0 0 0 0 0 0 0 0 0 0
```

```
Per hour in the last day:
   0 0 0 0 0 0 0 0 0 0
   0 0 0 0 0 0 0 0 0 0
   0 0 0 0
Per day in the last 30 days:
   0 0 0 0 0 0 0 0 0 0
Direct memory test failures per minute in the last hour:
   0 0 0 0 0 0 0 0 0
   0 0 0 0 0 0 0 0 0 0
   0 0 0 0 0 0 0 0 0
   0 0 0 0 0 0 0 0 0 0
   0 0 0 0 0 0 0 0 0 0
   0 0 0 0 0 0 0 0 0 0
Potential false positives: 0 0
 Ignored because of rx errors: 0 0
 Ignored because of cdm fifo overrun: 0 0
 Ignored because of oir: 0 0
 Ignored because isl frames received: 0 0
 Ignored during boot: 0 0
 Ignored after writing hw stats: 0 0
 Ignored on high gigaport: 0
Ongoing diag action mode: Normal
Last 1000 Memory Test Failures:
Last 1000 Packet Memory errors:
First 1000 Packet Memory errors:
```

Switch#



(注) ポートの最大数がテストされたことを確認するには、電源投入時に両方のスーパーバイザ エンジンが存在することを確認します。

障害の原因およびトラブルシューティング

すべての POST テストの障害は、スーパーバイザ エンジン上のハードウェアに関する問題を示します。 IOS が限定された機能を使用してスーパーバイザ エンジンを起動することで、ユーザは診断テストの結果を評価および表示できます。

ハードウェア障害が継続しているかどうか見極めるには、スーパーバイザ エンジンの電源をオフ/オンし、POST テストに戻ります。

また、シャーシでスーパーバイザ エンジンを取り外し、再度挿入しても、装着が正しいことを確認 できます。詳細は、シスコのカスタマー サポート チームにご連絡ください。



(注)

冗長シャーシでは、すでに挿入されているスーパーバイザ エンジンでの並列 POST がサポートされます。ただし、最初のスーパーバイザ エンジンをロード中に 2 番めのスーパーバイザ エンジンを挿入すると、最初のスーパーバイザ エンジンは faulty IOS ステートでブートします (POST が打ち切られ、一部の POST テストがバイパスされます)。 これは、複数のスーパーバイザ エンジンを同時起動した場合だけに発生します。先に装着したスーパーバイザ エンジンが POST を実行している間は、空のスーパーバイザ エンジン スロットに追加のスーパーバイザ エンジンを装着しないでください。POST シーケンスが終了すると、[Exiting to ios...] メッセージが表示されます。



CHAPTER 51

WCCP バージョン 2 サービスの設定



WCCP v2 は、Supervisor Engine 6-E ではサポートされていません。

この章では、Catalyst 4500 シリーズ スイッチを設定し、Web Cache Communication Protocol (WCCP) バージョン 2 を使用してコンテント エンジン (Web キャッシュ)にトラフィックをリダイレクトする方法を説明します。



この章の WCCP は WCCP バージョン 2 を表します。WCCP バージョン 1 はサポートされません。

この章の内容は、次のとおりです。

- WCCP の概要 (p.51-2)
- WCCP の制約事項 (p.51-6)
- WCCP の設定 (p.51-7)
- WCCP 設定値の確認およびモニタリング (p.51-10)
- WCCP の設定例 (p.51-11)



<u>—</u> (注)

この章の作業は、コンテント エンジンがネットワークに設定されていることを前提にしています。 Cisco Content Engine および WCCP に関連するハードウェアおよびネットワーク計画の詳細につい ては、次の URL の Cisco.com Web Scaling サイトから Product Literature Documentation リンクにアク セスしてください。

http://www.cisco.com/warp/public/cc/pd/cxsr/ces/index.shtml

WCCP の概要

ここでは、WCCPの次の内容について説明します。

- WCCP の概要 (p.51-2)
- ハードウェア アクセラレーション (p.51-2)
- WCCP 構成の概要 (p.51-3)
- WCCP の機能 (p.51-4)

WCCP の概要

WCCP はシスコが開発したコンテンツ ルーティング技術で、ネットワーク インフラストラクチャ にコンテント エンジンを統合することができます。

Cisco IOS WCCP 機能を使用すると、Cisco Content Engine (または WCCP を実行する他のコンテント エンジン)を使用してネットワークの Web トラフィック パターンをローカライズし、コンテンツ要求をローカルで処理できます。トラフィックをローカライズすると、送信コストとダウンロード時間が減少します。

WCCP により、Cisco IOS ルーティング プラットフォームはコンテンツ要求を透過的にリダイレクトできるようになります。HTTP 要求の透過的なリダイレクトの主な利点は、ユーザが自分のブラウザを Web プロキシを使用するように設定しないですむことです。ユーザは代わりにターゲット URL を使用してコンテンツを要求し、コンテント エンジンへ自動的にリダイレクトされるようにすることができます。この場合の「透過的」とは、要求したファイル(Webページなど)がコンテント エンジンから送信されたものであり、指定したサーバから送信されたものではないことがユーザにはわからないという意味です。

要求を受信したコンテント エンジンは、自分のローカル コンテンツを使用して要求に応じようとします。要求された情報が存在しない場合、コンテント エンジンは要求された情報を得るため最初に、ターゲットとされたサーバに自身の要求を送信します。コンテント エンジンは要求された情報を受け取ると、その情報を要求元のクライアントに転送し、さらに、今後の要求に備えてキャッシュに保存します。その結果、ダウンロードパフォーマンスが最大になり、送信コストが大幅に減少します。

WCCP により、一連のコンテント エンジン(コンテント エンジン クラスタと呼ぶ)が 1 つまたは 複数のルータにコンテンツを提供できます。ネットワーク管理者は、このようなクラスタ処理機能 を通じて使用するコンテント エンジンを簡単に拡張して、トラフィック負荷が重い場合でも処理することができます。シスコのクラスタ処理技術により、それぞれのコンテンツ メンバの同時動作が 可能になり、直線的なスケーラビリティが実現します。コンテント エンジンをクラスタ処理する と、キャッシング ソリューションのスケーラビリティ、冗長性、およびアベイラビリティが大きく 向上します。最大 32 のコンテント エンジンをクラスタ処理して、必要な容量まで拡張することが できます。

ハードウェア アクセラレーション

Catalyst 4500 シリーズ スイッチに Cisco Content Engine が直接接続されているとハードウェアが加速されます。これは、ソフトウェアのレイヤ 3 リダイレクションよりも効率的です。

直接接続されたコンテント エンジンを設定して、WCCP レイヤ 2 リダイレクション機能をマスク割り当てテーブルに基づいたロード バランシングとともに使用するようにネゴシエーションできるようにする必要があります。 show ip wccp web-cache detail コマンドを実行すると、それぞれのキャッシュで使用されるリダイレクション方法が表示されます。



WCCP レイヤ 2 リダイレクション機能をマスク割り当てテーブルとともに使用するように設定できるのは、Cisco Content Engine ソフトウェア リリース 2.2 以上のリリースです。

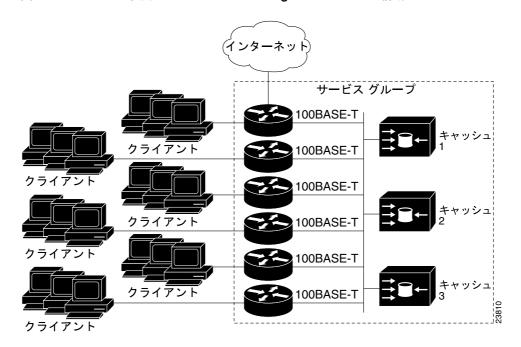
WCCP 構成の概要



WCCPv1 はサポートされません。

1 つのキャッシュ クラスタにサービスを提供するために複数のルータで WCCP を使用できます。図 51-1 に、複数のルータを使用する場合の構成例を示します。

図 51-1 WCCP を使用した Cisco Content Engine ネットワーク構成



クラスタ内のコンテント エンジンと、同じサービスを実行しているクラスタに接続するルータのサブセットを、サービス グループと呼びます。利用可能なサービスには TCP および User Datagram Protocol (UDP; ユーザ データグラム プロトコル) リダイレクションがあります。

WCCP では、それぞれのコンテント エンジンは、サービス グループ内のすべてのルータを認識する必要があります。サービス グループのすべてのルータのアドレスを指定するには、次のいずれかの方法を選択します。

- ユニキャスト 各コンテント エンジンに、グループの各ルータのアドレスをリストで設定します。この場合、グループの各ルータのアドレスをコンテント エンジンごとに設定時に明示的に指定する必要があります。
- マルチキャスト コンテント エンジンごとに単一のマルチキャスト アドレスを設定します。 マルチキャスト アドレスを設定すると、コンテント エンジンはサービス グループの全ルータ を対象とした単一アドレス通知を送信します。たとえば、マルチキャスト アドレス 224.0.0.100

にパケットを送信するようにコンテント エンジンで示すことができます。この場合、WCCP を使用してグループ リスニングが設定されているサービス グループのすべてのルータにマルチキャスト パケットが送信されます (詳細については ip wccp group-listen インターフェイス コンフィギュレーション コマンドを参照)。

各コンテント エンジンに単一のアドレスを指定すればいいだけなので、マルチキャスト方式の方が 簡単に設定できます。またこの方法では、コンテント エンジンに毎回異なるアドレスのリストを再 設定せずに、サービス グループにダイナミックにルータを追加したり削除したりすることができま す。

次のような流れで、WCCP 設定は機能します。

- 1. 各コンテント エンジンにルータのリストが設定されます。
- 2. 各コンテント エンジンが自身の存在と、自身が接続を確立した全ルータのリストをアナウンスします。ルータは、グループのコンテントエンジンの自身のビュー(リスト)で応答します。
- 3. クラスタのすべてのコンテント エンジンのビューが同じであれば、1 つのコンテント エンジン が先頭として指定され、パケットのリダイレクション時にルータで適用する必要があるポリシーを設定します。

次のセクションでは、ルータに WCCP を設定してサービス グループに参加させる方法を説明します。

WCCP の機能

ここでは、WCCPの次の機能について説明します。

- HTTP および非 HTTP サービスのサポート
- 複数ルータのサポート
- MD5 セキュリティ
- ウェブ コンテンツ パケットの返送

HTTP および非 HTTP サービスのサポート

WCCP は HTTP トラフィック (TCP ポート 80 のトラフィック)および非 HTTP トラフィック (TCP および UDP)のリダイレクションを可能にします。WCCP は他のポート向けパケットのリダイレクションもサポートします。これには、プロキシ Web キャッシュ処理、FTP (ファイル転送プロトコル) キャッシング、FTP プロキシ処理、ポートの Web キャッシング (ポート 80 を除く)、および Real Audio、Video、テレフォニー アプリケーション用のパケットが含まれます。

さまざまなタイプのサービスが利用できるようにするために、WCCP には複数のサービスグループという考え方が導入されています。サービス情報は、ダイナミック サービス ID 番号([98] など)または事前に定義されたサービスキーワード([web-cache] など)を使用して、WCCP コンフィギュレーション コマンドで指定されます。この情報は、サービスグループのメンバがすべて同じサービスを使用または提供していることを確認するために使用されます。



Catalyst 4500 シリーズ スイッチは、最大 8 つのサービス グループをサポートします。

ACNS バージョン 5.2 ソフトウェアでサポートされている WCCP バージョン 2 サービスについては、『Release Notes for Cisco ACNS Software』 Release 5.2.3 を参照してください。

サービス グループのコンテント エンジンは、プロトコル (TCP または UDP) およびポート (送信元または宛先)によってリダイレクトされるトラフィックを指定します。それぞれのサービス グループにはプライオリティ レベルが割り当てられています。パケットは、サービス グループに対してプライオリティ順に照合され、トラフィック特性に一致する最高のプライオリティのサービスグループによってリダイレクトされます。

複数ルータのサポート

WCCP では、複数のルータをキャッシュ エンジンのクラスタに追加できます。サービス グループ で複数のルータを使用すると、冗長化、インターフェイス集約、およびリダイレクション負荷の分散が可能になります。

MD5 セキュリティ

WCCP には任意の認証機能があり、パスワードおよび HMAC MD5 標準を使用して、どのルータおよびコンテント エンジンがサービス グループの一部になるかを制御できます。共有秘密 MD5 ワンタイム認証 (ip wccp [password [0-7] password] グローバル コンフィギュレーション コマンドで設定)により、メッセージを代行受信、検閲、および再生から保護することができます。

ウェブ コンテンツ パケットの返送

エラーや過負荷のために、コンテント エンジンがキャッシュした要求オブジェクトを提供できない場合、コンテント エンジンは本来の宛先であるサーバに転送するように要求をルータに返します。WCCP は、どの要求がサービスを実行されずにコンテント エンジンから返されたかを確認します。ルータは、この情報を使用して、要求を本来の宛先サーバに転送します(コンテンツ クラスタに要求を再送信しません)。これにより、エラー処理がクライアントに透過的に行われることになります。

コンテント エンジンがパケットを拒否してパケットを返送する主な理由は次のとおりです。

- コンテント エンジンが過負荷でパケットを処理する余裕がない
- コンテント エンジンに一定のフィルタリングがあり、パケットのキャッシングは逆効果である (IP 認証がオンの場合など)

WCCP の制約事項

WCCP には次のような制約事項があります。

- WCCP は IP ネットワークだけで動作します。
- マルチキャスト クラスタにサービスを提供するルータの場合、Time To Live (TTL; 存続可能時間)値は 15 秒以下にする必要があります。
- ほとんどの場合、メッセージは IP マルチキャストのため、メンバは関係のないメッセージや重複メッセージを受信することがあります。 適切なフィルタリングを実行する必要があります。
- 1 つのサービス グループは最大 32 のコンテント エンジンと 32 のルータで構成できます。
- クラスタのすべてのコンテント エンジンは、クラスタ サービスを行うすべてのルータと通信できるように設定する必要があります。
- 最大 8 つのサービス グループがクライアントの同一インターフェイス上で同時にサポートされます。
- L2 再書き込み転送方式はサポートされていますが、GRE カプセル化はサポートされていません。
- コンテント エンジンには L3 で直接接続する必要があります。1 つまたは複数のホップを経た L3 接続はサポートされません。
- レイヤ 2 リダイレクションでは、コンテント エンジンおよびクライアント インターフェイス はルータに直接接続し、異なる IP サブネットワークに存在することが必要です。
- TCAM と親和性の高いマスクベース割り当てはサポートされていますが、ハッシュ バケット ベース方式はサポートされません。
- クライアント インターフェイスでの WCCP のリダイレクト ACL(アクセス コントロール リスト) はサポートされません。
- インターフェイスでの着信トラフィックのリダイレクションはサポートされますが、発信トラフィックのリダイレクションはサポートされません。
- TCAM スペースを使い果たした場合はトラフィックはリダイレクトされず、通常どおりに転送されます。
- WCCP バージョン 2 標準では最大 256 の個別マスクをサポートします。ただし、Catalyst 4500 シリーズ スイッチは、単一マスクを持つマスク割り当てテーブルだけをサポートします。

WCCP の設定

次の設定作業は、ネットワークに含めるコンテント エンジンの設置および設定が完了していることを前提にしています。 クラスタにコンテント エンジンを設定してから、ルータで WCCP 機能を設定する必要があります。 コンテント エンジンの構成およびセットアップについては、『Cisco Content Engine User Guide』を参照してください。

キャッシュ エンジンに接続されているルータ インターフェイスに IP を設定する必要があります。 ルータの設定作業の例は次のセクションで示します。コマンド構文の詳細については、『 $Cisco\ IOS$ $Configuration\ Fundamentals\ Command\ Reference$ 』 Cisco IOS Release 12.3 を参照してください。

ここでは、WCCP の設定手順について説明します。

- WCCP を使用したサービス グループの設定 (p.51-7)(必須)
- WCCP サービス グループに対するアクセス リストの使用 (p.51-9)(任意)
- ルータおよびキャッシュ エンジンへのパスワードの設定 (p.51-9)(任意)

WCCP を使用したサービス グループの設定

WCCP は、トラフィックの代行受信およびリダイレクトを行うために導入された論理リダイレクション サービスに基づいてサービス グループを使用します。標準サービスはコンテント エンジンで、TCP ポート 80 (HTTP) トラフィックを代行受信してコンテント エンジンにリダイレクトします。このサービスは well-known サービスとも呼ばれます。ルータとコンテント エンジンの両方がWeb キャッシュ サービスの特性をよく知っているからです。よく知られたサービスの説明は、サービス ID 以外には要求されることはありません(この例では、CLI [コマンドライン インターフェイス] によりコマンド構文で web-cache キーワードが提供されます)。

ACNS バージョン 5.2 ソフトウェアでサポートされる WCCP サービスについては、『Release Notes for Cisco ACNS Software 』 Release 5.2.3 を参照してください。

Web キャッシュ サービス以外にも、最大 7 つのダイナミック サービスをスイッチで同時に実行できます。



(注)

スイッチでは同時に複数のサービスが実行できます。また、ルータおよびコンテント エンジンは、同時に複数のサービス グループの一部になることができます。

ダイナミック サービスはコンテント エンジンによって定義されます。コンテント エンジンがルータにどのプロトコルやポートを代行受信してどのようにトラフィックを配信するかを指示します。ルータ自身はダイナミック サービス グループのトラフィック特性に関する情報を持っていません。この情報はグループに最初に加入したコンテント エンジンが提供します。ダイナミック サービスでは、1 つのプロトコル (TCP または UDP) に最大 8 つのポートを指定できます。

たとえば Cisco Content Engine は ダイナミック サービス 99 を使用してリバース プロキシ サービス を指定します。ただし、このサービス番号は、他のコンテント エンジンでは他のサービスに使用されることがあります。次に、シスコルータで一般サービスをイネーブルにする手順を説明します。 コンテント エンジンにサービスを設定する場合の詳細については、コンテント エンジンのマニュアルを参照してください。

Catalyst 4500 シリーズ スイッチでサービスをイネーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	Switch(config)# ip wccp {web-cache service-number} [group-address groupaddress] [group-list access-list] [password password]	スイッチでイネーブルにするダイナミック サービス、サービス グループで使用する IP マルチキャスト アドレス (任意)、コンテント エンジン メンバシップに使用するグループ リスト (任意)、MD5 認証の使用の有無 (任意)を指定し、WCCP サービスをイネーブルにします。
ステップ 2	Switch(config)# interface type number	設定するクライアント インターフェイスを指定し、 インターフェイスコンフィギュレーション モード を開始します。
ステップ 3	<pre>Switch(config-if)# ip wccp {web-cache service-number} redirect in</pre>	指定したクライアント インターフェイスで、入トラフィックの WCCP リダイレクションをイネーブルにします。
ステップ 4	Switch(config)# interface type number	(マルチキャスト機能を実行する場合にのみ必要)マルチキャストを受信するように設定するコンテントエンジン インターフェイスを指定します。
ステップ 5	Switch(config-if)# ip wccp {web-cache service-number} group-listen	(マルチキャスト機能を実行する場合にのみ必要)ステップ 4 で指定したインターフェイスで IP マルチキャスト パケット(コンテント エンジンから送信される WCCP プロトコル パケット)の受信をイネーブルにします。

Web キャッシュ サービスの指定

Web キャッシュ サービスを設定するには、次の作業を実行します。

	コマンド	目的
1	Switch(config)# ip wccp web-cache	スイッチで Web キャッシュ サービスをイネーブル
		にします。
	Switch(config)# interface type number	Web キャッシュ サービスを実行するクライアント
		インターフェイス番号を指定し、インターフェイス
		設定モードを開始します。
	Switch(config-if)# ip wccp web-cache redirect	ステップ 2 で指定したクライアント インターフェイ
	in	スを使用して、コンテント エンジンにリダイレクト
		できるパケットかどうかのチェックをイネーブルに
		します。

WCCP サービス グループに対するアクセス リストの使用

Catalyst 4500 シリーズ スイッチは、アクセス リストを使用して、サービス グループに加入するコンテント エンジンを制限できます。

コンテントエンジンを制限するには、次の作業を実行します。

	コマンド	目的
ステップ 1	Switch(config)# access-list access-list permit ip host host-address [destination-address destination-host any]	コンテント エンジンのユニキャスト アドレスに基づいたアクセス リストを作成します。
ステップ 2	Switch(config)# ip wccp web-cache group-list access-list	スイッチに、どのコンテント エンジンのサービス グループへの加入が許可または不許可であるかを示します。

ルータおよびキャッシュ エンジンへのパスワードの設定

MD5 パスワード セキュリティでは、サービス グループに加入するコンテント エンジンおよび Catalyst 4500 シリーズ スイッチごとにサービス グループ パスワードを設定する必要があります。パスワードは 7 文字以内で指定します。 サービス グループのコンテント エンジンまたは Catalyst 4500 シリーズ スイッチは、WCCP メッセージ ヘッダーを確認した直後に、受信した WCCP パケットの セキュリティ コンポーネントを認証します。 認証に失敗したパケットは廃棄されます。

WCCP 通信で Catalyst 4500 シリーズ スイッチが使用する MD5 パスワードを設定するには、次の作業を実行します。

コマンド	目的
	Catalyst 4500 シリーズ スイッチに MD5 パスワードを設定します。

WCCP 設定値の確認およびモニタリング

WCCP の設定値を確認および監視するには、次のコマンドを EXEC モードで使用します。

コマンド	目的
Switch# show ip wccp [web-cache service-number]	WCCP に関連するグローバル情報を表示します。この情報には、実行中のプロトコルのバージョン、ルータ サービスグループのコンテント エンジンの数、ルータに接続可能なコンテント エンジン グループ、使用中のアクセス リストが含まれます。
Switch# show ip wccp {web-cache service-number} detail	ルータが検出した、サービス グループのコンテント エンジンの情報を問い合わせます。 Web キャッシュ サービスまたは指定したダイナミック サービスのいずれかの情報を表示できます。
Switch# show ip interface	ip wccp リダイレクション コマンドがクライアント インターフェイスで設定されているかどうかを表示します。たとえば、[Web Cache Redirect is enabled / disabled] と表示されます。
Switch# show ip wccp {web-cache service-number} view	特定のサービス グループで検出された装置、トラブルが発生しているコンテント エンジン、現在のスイッチに接続されているその他のすべてのスイッチで認識可能なコンテント エンジンを表示します。
	view キーワードは、サービス グループのアドレスのリストを表します。 Web キャッシュ サービスまたは指定したダイナミック サービスのいずれかの情報を表示できます。
	詳細なトラブルシューティング情報を表示するには、 show ip wccp {web-cache service number} service コマンドを 使用します。

WCCP の設定例

ここでは、次の設定例を示します。

- 一般的な WCCP 設定の実行例 (p.51-11)
- Web キャッシュ サービスの実行例 (p.51-11)
- リバース プロキシ サービスの実行例 (p.51-11)
- アクセス リストの使用例 (p.51-11)
- スイッチおよびコンテント エンジンへのパスワードの設定例 (p.51-12)
- WCCP 設定の確認例 (p.51-12)

一般的な WCCP 設定の実行例

次に、一般的な WCCP 設定セッションの例を示します。VLAN 20 はクライアント インターフェイスです。VLAN 50 はコンテント エンジン インターフェイスです。

```
Switch# configure terminal
Switch(config)# ip wccp web-cache group-address 224.1.1.100 password alaska1
Switch(config)# interface vlan 20
Switch(config-if)# ip wccp web-cache redirect in
Switch(config)# interface vlan 50
Switch(config-if)# ip wccp web cache group-listen
```

Web キャッシュ サービスの実行例

次に、Web キャッシュ サービスの設定セッション例を示します。

```
Switch# configure terminal
Switch(config)# ip wccp web-cache
Switch(config)# interface vlan 20
Switch(config-if)# ip wccp web-cache redirect in
Switch(config-if)# ^Z
Switch# copy running-config startup-config
Switch# show ip interface vlan 20 | include WCCP Redirect
WCCP Redirect inbound is enabled
WCCP Redirect exclude is disabled
```

リバース プロキシ サービスの実行例

次に、リバース プロキシ サービスの実行にダイナミック サービス 99 を使用する Cisco Content Engine を使用してサービス グループを設定する例を示します。

```
Switch# configure terminal
router(config)# ip wccp 99
router(config)# interface vlan 40
router(config-if)# ip wccp 99 redirect in
```

アクセス リストの使用例

セキュリティを向上させるには、現在のスイッチで登録するコンテント エンジンのものとして有効な IP アドレスを、標準のアクセス リストを使用して Catalyst 4500 シリーズ スイッチに通知します。 次に、標準のアクセス リスト設定セッションの例を示します。 サンプル ホストのアクセス リスト番号は 10 です。

```
router(config)# access-list 10 permit host 11.1.1.1
router(config)# access-list 10 permit host 11.1.1.2
router(config)# access-list 10 permit host 11.1.1.3
router(config)# ip wccp web-cache group-list 10
```

スイッチおよびコンテント エンジンへのパスワードの設定例

次に、WCCP パスワード設定セッションの例を示します。パスワードは alaska1 です。

Switch# configure terminal router(config)# ip wccp web-cache password alaska1

WCCP 設定の確認例

設定の変更を確認するには、**more system:running-config** EXEC コマンドを使用します。次に、Catalyst 4500 シリーズ スイッチの Web キャッシュ サービスとダイナミック サービス 99 がどちらもイネーブルである場合の例を示します。

Switch# more system:running-config

```
Building configuration...
Current configuration:
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service udp-small-servers
service tcp-small-servers
hostname router4
enable secret 5 $1$nSVy$faliJsVQXVPW.KuCxZNTh1
enable password alabama1
ip subnet-zero
ip wccp web-cache
ip wccp 99
ip domain-name cisco.com
ip name-server 10.1.1.1
ip name-server 10.1.1.2
ip name-server 10.1.1.3
interface Vlan200
ip address 10.3.1.2 255.255.255.0
no ip directed-broadcast
ip wccp web-cache redirect in
ip wccp 99 redirect in
no ip route-cache
no ip mroute-cache
interface Vlan300
ip address 10.4.1.1 255.255.255.0
interface Serial0
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown
interface Serial1
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown
ip default-gateway 10.3.1.1
ip classless
```

```
ip route 0.0.0.0 0.0.0.0 10.3.1.1
no ip http server
!
!!!
line con 0
transport input none
line aux 0
transport input all
line vty 0 4
password alaska1
login
!
end
```

■ WCCP の設定例



CHAPTER

52

MIB サポートの設定

この章では、Cisco 4500 シリーズ スイッチに SNMP (簡易ネットワーク管理プロトコル) および MIB (管理情報ベース) サポートを設定する方法を説明します。ここでは、次の内容について説明します。

- Cisco IOS リリースの MIB サポートの判断 (p.52-1)
- Cisco IOS MIB ツールの使用 (p.52-2)
- MIB のダウンロードおよびコンパイル (p.52-3)
- SNMP サポートのイネーブル化 (p.52-5)

Cisco IOS リリースの MIB サポートの判断

Cisco 4500 シリーズ スイッチで動作する Cisco IOS リリースに含まれている MIB を調べるには、次の手順を実行します。

ステップ1 次の URL の Cisco MIB サポート ページにアクセスします。

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

- **ステップ2** Cisco Access Products で **Cisco 4500 switch** を選択すると、Cisco 4500 スイッチでサポートされる MIB のリストが表示されます。
- ステップ3 リスト内をスクロールして目的のリリースを探します。

Cisco IOS MIB ツールの使用

ここでは、Cisco MIB ツール ページにアクセスする方法を説明します。MIB Locator を使用すると、Cisco IOS ソフトウェア リリースの MIB がわかります。MIB の一般情報、SNMP Object Navigator を使用して SNMP Object Identifier (OID; オブジェクト ID) を SNMP 名に変換する方法、および Cisco MIB をロードする方法もわかります。

Cisco IOS MIB ツールのサイトには次の手順でアクセスできます。

ステップ1 次の URL の Cisco Products and Services ページにアクセスします。

http://tools.cisco.com/ITDIT/MIBS/servlet/index

ステップ2 MIB Locator をクリックしてアプリケーションを起動します。MIB Locator を使用して MIB を探すには、3 つの方法があります。

MIB Locator ページを利用する方法

- a. ドロップダウン メニューをクリックし、目的の Cisco IOS ソフトウェア リリースを選択します。
- b. Platform Family メニューに表示されたフィーチャ セット(CAT4500-SUP2-PLUS、CAT4500-SUP2-PLUS、CAT4500-SUP3、CAT4500-SUP4、CAT4500-SUP5、CAT4500-SUP5、CAT4500-SUP5-10gGE2、CAT4948)から、適切なフィーチャ セットを選択します。最初にプラットフォームを選択すると、Cisco 4500 シリーズ スイッチに適用されるリリースおよびフィーチャ セットだけが表示されます。
- c. Feature Set メニューで、Service Provider W/VIP を選択します。
- **ステップ3** MIB Locator ページではイメージ名で検索できます。たとえば、次のように入力して **Submit** ボタンをクリックします。

c7200-js56i-mz.12.0-1

ステップ4 MIB Locator ページでは、メニューに表示された MIB のリストから MIB を検索することもできます。 MIB を選択することも、CTRL キーを押したままクリックすることによって複数の MIB を選択することもできます。そのあと、Submit ボタンをクリックします。



(注) MIB を選択したら、リンクおよび指示に従います。

MIB のダウンロードおよびコンパイル

次のセクションで、Cisco 4500 シリーズ スイッチの MIB をダウンロードしてコンパイルする方法 を説明します。

- MIB を扱う際の考慮事項
- MIB のダウンロード
- MIB のコンパイル

MIB を扱う際の考慮事項

MIB を扱う際は以下の点を考慮してください。

データタイプ定義のミスマッチ

データタイプ定義のミスマッチにより、コンパイラ エラーが発生したり警告メッセージが表示 されることがあります。Cisco MIB データタイプ定義にはミスマッチはありませんが、一部の 標準 RFC MIB にはミスマッチがあります。次に例を示します。

```
MIB A defines: SomeDatatype ::= INTEGER(0..100)
MIB B defines: SomeDatatype ::= INTEGER(1..50)
```

この例は小さなエラーとみなされ、MIB は警告メッセージが表示されますが正しくロードされ ます。

次の例は小さなエラーとはみなされず(どちらの定義も本質的に同じですが)、MIB は正しく 解析されません。

```
MIB A defines: SomeDatatype ::= DisplayString
MIB B defines: SomeDatatype ::= OCTET STRING (SIZE(0..255))
```

MIB コンパイラがこれらをエラーとして扱う場合、または警告メッセージを消したい場合は、 定義が一致するようにこれと同じデータタイプを定義するいずれかの MIB を編集します。

• MIB の多くは他の MIB から定義をインポートします。使用する管理アプリケーションに MIB をロードする必要があり、未定義オブジェクトに関する問題が発生する場合は、次の MIB を記 載順にロードします。

SNMPv2-SMI.my SNMPv2-TC.my SNMPv2-MIB.my RFC1213-MIB.my IF-MIB.my CISCO-SMI.my CISCO-PRODUCTS-MIB.my

CISCO-TC.my

• その他の情報や SNMP テクニカル ティップスを入手するには、Locator ページで SNMP MIB Technical Tips をクリックしてリンクをクリックするか、次の URL にアクセスします。

http://www.cisco.com/pcgi-bin/Support/browse/psp_view.plp=Internetworking:SNMP&s=Implementati on_and_Configuration#Samples_and_Tips

• MIB オブジェクトに割り当てられている SNMP OID のリストを入手するには、次の URL で SNMP Object Navigator をクリックし、リンクを参照します。

http://tools.cisco.com/ITDIT/MIBS/servlet/index



MIB Locator にアクセスするには、Cisco COO 名とパスワードが必要です。

 Cisco MIB をダウンロードしてコンパイルする方法については、次の URL を参照してください。 http://www.cisco.com/warp/public/477/SNMP/mibcompilers.html

MIB のダウンロード

システムに MIB がない場合は、次の手順でダウンロードします。

- ステップ 1 前のセクションの考慮事項を参照してください (「MIB を扱う際の考慮事項」)。
- ステップ2 次の URL のどちらかにアクセスします。 ダウンロードする MIB がない場合は、もう一方の URL にアクセスします。 どちらにもない場合は、ステップ 5 の URL のどちらかにアクセスします。

ftp://ftp.cisco.com/pub/mibs/v2

ftp://ftp.cisco.com/pub/mibs/v1

- ステップ3 システムにダウンロードする MIB のリンクをクリックします。
- **ステップ4** File > Save または File > Save As の順に選択し、システムに MIB を保存します。
- ステップ 5 次の URL では、業界標準の MIB をダウンロードできます。
 - http://www.ietf.org
 - http://www.atmforum.com

MIB のコンパイル

Cisco 4500 シリーズ スイッチを SNMP ベースの管理アプリケーションと統合する場合は、そのプラットフォーム用に MIB をコンパイルする必要があります。たとえば、HP Open View を UNIX オペレーティング システム上で実行する場合は、Cisco 4500 シリーズ スイッチ MIB を HP Open View NMS (network management system; ネットワーク管理システム) でコンパイルする必要があります。手順については、NMS のマニュアルを参照してください。

SNMP サポートのイネーブル化

次に、Cisco 4500 シリーズ スイッチに SNMP サポートを設定する手順の概要を説明します。

SNMP コマンドの詳細については、次のシスコ マニュアルを参照してください。

- 次の URL でアクセスできる『Cisco IOS Release 12.3 Configuration Fundamentals Configuration Guide』の「Monitoring the Router and Network」の章
 - http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ffun_c/index.htm
- ・ 次の URL でアクセスできる『Cisco IOS Release 12.3 Configuration Fundamentals Command Reference』の Part 3「System Management Commands」の「Router and Network Configuration Commands」

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ffun_r/index.htm

Cisco 4500 シリーズ スイッチに SNMP サポートを設定するには、次のステップを実行します。

- **ステップ1** ルータの CLI (コマンドライン インターフェイス)を使用し、SNMP の基本設定を行います。これらの基本設定コマンドは SNMPv2c に対して実行されます。SNMPv3 では SNMP ユーザおよびグループも設定する必要があります (コマンドおよび設定情報については前述のマニュアルを参照)。
 - a. SNMP リード(read)コミュニティおよびリード/ライト(read/write)コミュニティを定義します。

```
Router (config)# snmp-server community Read_Only_Community_Name ro
Router (config)# snmp-server community Read_Write_Community_Name rw
```

b. SNMP ビューを設定します(他の SNMP ユーザ グループにアクセス可能にするオブジェクトの 範囲を制限するため)。

Router (config)# snmp-server view view_name oid-tree {included | excluded}

ステップ2 ルータから SNMP 通知を受信するホストを (IP アドレスで)指定します。

```
Router (config) # snmp-server host host
```

ステップ3 ルータで通知を生成できるように設定します。キーワードを使用すると、生成するメッセージの数および種類を制限できます。

```
Router (config)# snmp-server enable traps [notification-type] [notification-option]
```

ステップ 4 (任意) Field Replaceable Unit (FRU; 現場交換可能ユニット) に関する SNMP 通知をルータで生成するように設定します。

```
Router (config) # snmp-server enable traps fru-ctrl
```

ステップ 5 (任意)環境モニタリングに関する SNMP 通知をルータで生成するように設定します。

```
Router (config) # snmp-server enable traps envmon
```

■ SNMP サポートのイネープル化



CHAPTER

53

ROM モニタ

この章では、Cisco 806 ルータの ROM モニタ(ブートストラップ プログラムとも呼ぶ)について説明します。ROM モニタ ファームウェアは、ルータの電源投入時またはリセット時に起動します。ファームウェアは、プロセッサ ハードウェアの初期化とオペレーティング システムの起動を助けます。ROM モニタを使用して、忘れてしまったパスワードの回復やコンソール ポートでのソフトウェアのダウンロードなど、特定の設定作業を実行できます。ルータに Cisco IOS ソフトウェア イメージがロードされていない場合、ROM モニタがルータを実行します。

この章の内容は、次のとおりです。

- ROM モニタの設置
- ROM モニタ コマンド
- コマンドの説明
- コンフィギュレーション レジスタ
- コンソール ダウンロード
- デバッグ コマンド
- ROM モニタの終了

ROM モニタの設置

ROM モニタを使用するには、端末または PC をコンソール ポート経由でルータに接続している必要があります。ルータに付属の『Cisco 806 Router Hardware Installation Guide』のインストレーションの章を参照して、ルータと PC または端末を接続します。

次に再起動する場合は ROM モニタ モードで起動するようにルータを設定するには、次のステップを実行します。

	コマンド	作業
ステップ 1	enable	イネーブル パスワードが設定されている場合、イネーブル コマンドとイネーブル パスワードを入力して特権 EXEC モードを開始します。
ステップ 2	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	config-reg 0x0	コンフィギュレーション レジスタをリセットします。
ステップ 4	exit	グローバル コンフィギュレーション モードを終了します。
ステップ 5	eload	新しいコンフィギュレーション レジスタ値をルータを使用して起動します。ルータは ROM モニタ モードのままで、Cisco IOS ソフトウェアを起動しません。
		設定値が 0x0 であるかぎり、コンソールから手動でオペレーティング システムを起動する必要があります。この章の「コマンドの説明」の bootコマンドを参照してください。
		再起動したルータは ROM モニタ モードになります。新しく行が増える ごとにプロンプトの数字が増加します。

ROM モニタ コマンド

利用できるコマンドおよびオプションのリストを表示するには、ROM プロンプトで?または help を入力します。次に例を示します。

rommon 1 > ?	
alias	set and display aliases command
boot	boot up an external process
confreg	configuration register utility
dev	list the device table
dir	list files in file system
help	monitor builtin command help
history	monitor command history
meminfo	main memory information
repeat	repeat a monitor command
reset	system reset
set	display the monitor variables
sysret	print out info from last system return
unalias	unset an alias
unset	unset a monitor variable

コマンドの大文字と小文字を区別は区別されます。端末上で Break キーを押すとコマンドを停止できます。PC を使用している場合、Ctrl キーと Break キーを同時に押すと、ほとんどのターミナル エミュレーション プログラムはコマンドを停止します。別のタイプのターミナル エミュレータや ターミナル エミュレーション ソフトウェアを使用している場合に Break コマンドを送信する方法については、その製品のマニュアルを参照してください。

コマンドの説明

表 53-1 に、一般的に使用される ROM モニタ コマンドを示します。

表 53-1 一般的に使用される ROM モニタ コマンド

コマンド	説明	
reset または i	ルータをリセットまたは初期化します。電源投入に似ています。	
dev	ルータの起動装置の ID を表示します。次に例を示します。	
	rommon 10> dev Devices in device table: id name flash: flash	
dir device:	指定した装置のファイルを表示します。次に例を示します。 rommon 4 > dir flash: File size Checksum File name	
	2835276 bytes (0x2b434c) 0x2073 c806-oy6-mz	
ブート コマンド	ROM モニタのブート コマンドの詳細については、『Cisco IOS Configuration Guide』および『Cisco IOS Command Reference』を参照してください。	
b	フラッシュ メモリの最初のイメージを起動します。	
b flash:[filename]	フラッシュ メモリの最初のパーティションからイメージを直接起動しようとします。ファイル名を入力しなかった場合、フラッシュの最初のイメージが起動されます。	

コンフィギュレーション レジスタ

仮想コンフィギュレーション レジスタは Nonvolatile RAM (NVRAM; 不揮発性 RAM) にあり、他の Cisco ルータと同じ機能を持っています。仮想コンフィギュレーション レジスタは、ROM モニタまたはオペレーティング システムで表示または変更できます。ROM モニタで 16 進形式のレジスタ値を入力するか、ROM モニタのプロンプトに従って各ビットを指定すると、コンフィギュレーション レジスタを変更できます。

コンフィギュレーション レジスタの手動での変更

仮想コンフィギュレーション レジスタを ROM モニタから手動で変更するには、confreg コマンド に続けて新しいレジスタ値を 16 進数で入力します。次に例を示します。

rommon 1 > confreg 0x2101

You must reset or power cycle for new config to take effect rommon 2 $\!\!\!\!>$

値は常に 16 進数とみなされます。新しい仮想コンフィギュレーション レジスタ値は NVRAM に書き込まれますが、ルータをリセットまたは再起動するまでは有効になりません。

コンフィギュレーション レジスタのプロンプトでの変更

confreg コマンドを引数なしで入力すると、仮想コンフィギュレーション レジスタの内容とプロンプトが表示されます。プロンプトに各ビットの意味を指定すると、内容が変更できます。

いずれの場合も、新しい仮想コンフィギュレーション レジスタ値は NVRAM に書き込まれますが、 ルータをリセットまたは再起動するまでは有効になりません。

次に、confreg コマンドの入力例を示します。

```
rommon 7> confreg
     Configuration Summary
enabled are:
console baud: 9600
boot: the ROM Monitor
do you wish to change the configuration? y/n [n]: y
enable "diagnostic mode"? y/n [n]: y
enable "use net in IP bcast address"? y/n = [n]:
enable "load rom after netboot fails"? y/n [n]:
enable "use all zero broadcast"? y/n [n]:
enable "break/abort has effect"? y/n [n]:
enable "ignore system config info"? y/n = [n]:
change console baud rate? y/n [n]: y
enter rate: 0 = 9600, 1 = 4800, 2 = 1200, 3 = 2400 [0]: 0
change the boot characteristics? y/n [n]: y
enter to boot:
0 = ROM Monitor
 1 = the boot helper image
2-15 = boot system
    [0]: 0
Configuration Summary
enabled are:
diagnostic mode
console baud: 9600
boot: the ROM Monitor
do you wish to change the configuration? y/n [n]:
You must reset or power cycle for new config to take effect
```

コンソール ダウンロード

ROM モニタのコンソール ダウンロード機能を使用し、ルータのコンソール ポートを通じてソフトウェア イメージまたはコンフィギュレーション ファイルをダウンロードできます。ダウンロードしたファイルはミニフラッシュ メモリ モジュールまたはメイン メモリに保存され、実行されます(イメージファイルのみ)。

Trivial File Transfer Protocol (TFTP) サーバにアクセスできない場合は、コンソール ダウンロードを使用します。



(注)

コンソール ポートを通じてルータにソフトウェア イメージまたはコンフィギュレーション ファイルをダウンロードする場合は、ROM monitor コマンドを使用します。



(注)

PC を使用し Cisco IOS イメージをルータ コンソール ポート経由で 115,200 bps でダウンロードする場合は、PC シリアル ポートで 16550 Universal Asynchronous Receiver/Transmitter (UART; 汎用非同期送受信器)が使用されていることを確認します。PC シリアル ポートで 16550 UART が使用されていない場合、コンソール ポート経由で Cisco IOS イメージをダウンロードするには 38,400 bps 以下の速度を使用することを推奨します。

エラー レポート

ROM モニタ コンソール ダウンロードではデータの転送にコンソールが使用されるため、エラーメッセージはデータ転送が終了した場合にのみコンソールに表示されます。

データ転送中にエラーが発生すると転送が中止され、エラー メッセージが表示されます。デフォルトのボー レートを変更した場合は、端末のボー レートをコンフィギュレーション レジスタに指定されたボー レートに戻すことを指示するメッセージがエラー メッセージに続いて表示されます。

デバッグ コマンド

ROM モニタのほとんどのデバッグ コマンドは、Cisco IOS ソフトウェアがクラッシュまたは停止した場合にのみ機能します。

次に、ROM モニタのデバッグ コマンドを示します。

- frame 個別のスタック フレームを表示します。
- sysret 最後に起動したシステム イメージから返された情報を表示します。この情報には、イメージを中止した理由、最大 8 フレームのスタック ダンプ、および例外が発生したアドレス (例外がある場合)などが含まれます。

```
rommon 8> sysret
System Return Info:
count: 19,    reason: user break
pc:0x801111b0,    error address: 0x801111b0
Stack Trace:
FP: 0x80005ea8, PC: 0x801111b0
FP: 0x80005eb4, PC: 0x80113694
FP: 0x80005f74, PC: 0x8010eb44
FP: 0x80005f9c, PC: 0x80008118
FP: 0x80005fac, PC: 0x80008064
FP: 0x80005fc4, PC: 0xfff03d70
FP: 0x80005ffc, PC: 0x00000000
FP: 0x00000000, PC: 0x00000000
```

meminfo サイズ(バイト) 開始アドレス、使用可能なメインメモリの範囲、パケットメモリの開始点およびサイズ、NVRAMのサイズなどを表示します。

```
rommon 9> meminfo

Main memory size: 40 MB.

Available main memory starts at 0x10000, size 40896KB

IO (packet) memory size: 5 percent of main memory.

NVRAM size: 32KB
```

ROM モニタの終了

起動時またはリロード時にフラッシュ メモリから Cisco IOS イメージを起動するには、ルータのコンフィギュレーション レジスタに $0x2 \sim 0xF$ の値を設定する必要があります。

次に、コンフィギュレーション レジスタをリセットし、フラッシュ メモリに保存した Cisco IOS イメージをルータが起動する例を示します。

```
rommon 1 > confreg \ 0x2101
You must reset or power cycle for new config to take effect rommon 2 > boot
```

ルータは、フラッシュ メモリの Cisco IOS イメージを起動します。ルータの次のリセット時または電源の再投入時に、コンフィギュレーション レジスタの値は 0x2101 になります。

■ ROM モニタの終了



APPENDIX



略語

表 A-1 に、このマニュアルで使用されている略語の定義を示します。

表 A-1 略語

略語	説明
ACE	Access Control Entry: アクセス コントロール エントリ
ACL	Access Control List: アクセス コントロール リスト
AFI	Authority and Format Identifier
Agport	集約ポート
ALPS	Airline Protocol Support
AMP	Active Monitor Present
APaRT	Automated Packet Recognition and Translation:自動パケット認識および 変換
ARP	Address Resolution Protocol:アドレス解決プロトコル
AV	Attribute Value
AVVID	Architecture for Voice, Video and Integrated Data
BDD	Binary Decision Diagrams
BECN	Backward Explicit Congestion Notification:逆方向明示的輻輳通知
BGP	Border Gateway Protocol:ボーダー ゲートウェイ プロトコル
BPDU	Bridge Protocol Data Unit: ブリッジ プロトコル データ ユニット
BRF	Bridge Relay Function:ブリッジ リレー機能
BSC	Bisync:バイナリ同期
BSTUN	Block Serial Tunnel: ブロック シリアル トンネル
BUS	Broadcast and Unknown Server
BVI	Bridge-group Virtual Interface : ブリッジ グループ仮想インターフェイス
CAM	Content-Addressable Memory:連想メモリ
CAR	Committed Access Rate:専用アクセス レート
CCA	Circuit Card Assembly
Cisco Discovery Protocol	Cisco Discovery Protocol:シスコ検出プロトコル
(CDP; シスコ検出プロト	
コル)	
CEF	Cisco Express Forwarding
CGMP	Cisco Group Management Protocol

略語	説明
СНАР	Challenge Handshake Authentication Protocol: チャレンジ ハンドシェイク認証プロトコル
CIR	Committed Information Rate:認定情報レート
CIST	Common and Internal Spanning-Tree
CLI	Command-Line Interface: コマンドライン インターフェイス
CLNS	Connection-Less Network Service:コネクションレス型ネットワークサービス
CMNS	Connection-Mode Network Service: コネクション モード ネットワークサービス
COPS	Common Open Policy Server
COPS-DS	Common Open Policy Server Differentiated Services
CoS	Class Of Service: サービス クラス
CPLD	Complex Programmable Logic Device
CRC	Cyclic Redundancy Check:巡回冗長検査
CRF	Concentrator Relay Function: コンセントレータ リレー機能
CST	Common Spanning-Tree
CUDD	University of Colorado Decision Diagram
DBL	Dynamic Buffer Limiting
DCC	Data Country Code: データ カントリ コード
dCEF	distributed Cisco Express Forwarding
DDR	Dial-on-Demand Routing: ダイヤル オンデマンド ルーティング
DE	Discard Eligibility:廃棄適性
DEC	Digital Equipment Corporation
DFI	Domain-Specific Part Format Identifier
DFP	Dynamic Feedback Protocol
DISL	Dynamic Inter-Switch Link
DLC	Data Link Control:データ リンク制御
DLSw	Data Link Switching: データ リンク スイッチング
DMP	Data Movement Processor
DNS	Domain Name System: ドメイン ネーム システム
DoD	Department of Defense:米国国防総省
DoS	Denial of Service: サービス拒絶
DRAM	Dynamic RAM
DSAP	Destination Service Access Point: 宛先サービス アクセス ポイント
DSCP	Differentiated Services Code Point: DiffServ コード ポイント
DSPU	Downstream SNA Physical Units
DTP	Dynamic Trunking Protocol: ダイナミック トランキング プロトコル
DTR	Data Terminal Ready: データ ターミナル レディ
DXI	Data Exchange Interface:データ交換インターフェイス
EAP	Extensible Authentication Protocol
EARL	Enhanced Address Recognition Logic

略語	説明
EEPROM	Electrically Erasable Programmable Read-Only Memory:電気的に消去可能でプログラミング可能な ROM
EHSA	Enhanced High System Availability: 拡張高システム可用性
ЕНТ	EHT
EIA	Electronic Industries Association:米国電子工業会
ELAN	Emulated Local Area Network: エミュレート LAN
EOBC	Ethernet Out-of-Band Channel
ESI	End-System Identifier: エンド システム識別子
FECN	Forward Explicit Congestion Notification:順方向明示的輻輳通知
FM	Feature Manager
FRU	Field-Replaceable Unit:現場交換可能ユニット
FSM	Feasible Successor Metrics
GARP	General Attribute Registration Protocol
GMRP	GARP Multicast Registration Protocol
GVRP	GARP VLAN Registration Protocol
HSRP	Hot Standby Router Protocol
ICC	Inter-card Communication
ICD	International Code Designator
ICMP	Internet Control Message Protocol:インターネット制御メッセージ プロトコル
IDB	Interface Descriptor Block: インターフェイス デスクリプション ブロック
IDP	Initial Domain Part または Internet Datagram Protocol
IFS	IOS File System
IGMP	IGMP
IGRP	Interior Gateway Routing Protocol
ILMI	Integrated Local Management Interface: 統合ローカル管理インターフェイス
IP	Internet Protocol: インターネット プロトコル
IPC	Interprocessor Communication:プロセッサ間通信
IPX	Internetwork Packet Exchange
IS-IS	Intermediate System-to-Intermediate System
ISL	Inter-Switch Link:スイッチ間リンク
ISO	International Organization for Standardization: 国際標準化機構
LAN	Local Area Network: ローカルエリア ネットワーク
LANE	LAN Emulation: LAN エミュレーション
LAPB	Link Access Procedure, Balanced: 平衡型リンク アクセス手順
LDA	Local Director Acceleration
LCP	Link Control Protocol: リンク コントロール プロトコル
LEC	LAN Emulation Client: LAN エミュレーション クライアント
LECS	LAN Emulation Configuration Server: LAN エミュレーション コンフィギュレーション サーバ
	オュレーション リーハ

略語	説明
LEM	Link Error Monitor: リンク エラー モニタ
LER	Link Error Rate: リンク エラー レート
LES	LAN Emulation Server:LAN エミュレーション サーバ
LLC	Logical Link Control:論理リンク制御
LTL	Local Target Logic
MAC	Media Access Control:メディア アクセス制御
MACL	MAC Access Control
MD5	Message Digest 5
MFD	Multicast Fast Drop
MIB	Management Information Base:管理情報ベース
MII	Media-Independent Interface:メディア独立型インターフェイス
MLS	Multilayer Switching: マルチレイヤ スイッチング
MLSE	Maintenance Loop Signaling Entity
MOP	Maintenance Operation Protocol : メンテナンス オペレーション プロトコル
MOTD	Message-of-The-Day : ログイン バナー
MLSE	Maintenance Loop Signaling Entity
MRM	Multicast Routing Monitor
MSDP	Multicast Source Discovery Protocol
MST	Multiple Spanning-Tree
MSTI	MST Instance: MST インスタンス
MTU	Maximum Transmission Unit:最大伝送ユニット
MVAP	Multiple VLAN Access Port
NBP	Name Binding Protocol: ネーム バインディング プロトコル
NCIA	Native Client Interface Architecture: ネイティブ クライアント インターフェイス アーキテクチャ
NDE	NetFlow Data Export: NetFlow データ エクスポート
NET	Network Entity Title
NetBIOS	Network Basic Input/Output System
NFFC	NetFlow Feature Card: NetFlow フィーチャ カード
NMP	Network Management Processor:ネットワーク管理プロセッサ
NSAP	Network Service Access Point:ネットワーク サービス アクセス ポイント
NTP	Network Time Protocol: ネットワーク タイム プロトコル
NVRAM	Nonvolatile RAM:不揮発性 RAM
OAM	Operation, Administration, and Maintenance:運用管理および保守
ODM	Order Dependent Merge
OSI	Open Systems Interconnection: オープン システム インターコネクション
OSPF	Open Shortest Path First
PACL	Port Access Control List
PAE	Port Access Entity
PAgP	Port Aggregation Protocol

表 A-1 略語 (続き)

略語	説明
PBD	Packet Buffer Daughterboard
PBR	Policy Based Routing: ポリシー ベース ルーティング
PC	Personal Computer: パーソナル コンピュータ
PCM	Pulse Code Modulation:パルス符号変調
PCR	Peak Cell Rate: ピーク セル レート
PDP	Policy Decision Point: ポリシー デシジョン ポイント
PDU	Protocol Data Unit: プロトコル データ ユニット
PEP	Policy Enforcement Point
PGM	Pragmatic General Multicast
PHY	Physical Sublayer:物理サブレイヤ
PIB	Policy Information Base
PIM	Protocol Independent Multicast
PoE	Power over Ethernet
PPP	Point-to-Point Protocol: ポイントツーポイント プロトコル
PRID	Policy Rule Identifiers
PVST+	Per VLAN Spanning Tree Plus
QM	QoS Manager
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RAM	Random-Access Memory : ランダム アクセス メモリ
RCP	Remote Copy Protocol: リモート コピー プロトコル
RGMP	Router-Ports Group Management Protocol
RIB	Routing Information Base
RIF	Routing Information Field:ルーティング情報フィールド
RMON	Remote Monitoring: リモート モニタリング
ROM	Read-Only Memory
ROMMON	ROM Monitor: ROM モニタ
RP	Route Processor:ルート プロセッサ、または Rendezvous Point: ランデブー ポイント
RPC	Remote Procedure Call: リモート プロシージャ コール
RPF	Reverse Path Forwarding
RPR	Route Processor Redundancy
RSPAN	Remote SPAN
RST	リセット
RSVP	ReSerVation Protocol
SAID	Security Association Identifier
SAP	Service Access Point: サービス アクセス ポイント
SCM	Service Connection Manager
SCP	Switch-Module Configuration Protocol
SDLC	Synchronous Data Link Control
SGBP	Stack Group Bidding Protocol

 略語	説明
SIMM	Single In-Line Memory Module: シングル インライン メモリ モジュール
SLB	Server Load Balancing
SLCP	Supervisor Line-Card Processor
SLIP	Serial Line Internet Protocol:シリアル ライン インターネット プロトコル
SMDS	Software Management and Delivery Systems
SMF	Software MAC Filter: ソフトウェア MAC フィルタ
SMP	Standby Monitor Present
SMRP	Simple Multicast Routing Protocol : シンプル マルチキャスト ルーティング プロトコル
SMT	Station Management:ステーション管理
SNAP	Subnetwork Access Protocol: サブネットワーク アクセス プロトコル
SNMP	Simple Network Management Protocol: 簡易ネットワーク管理プロトコル
SPAN	Switched Port Analyzer : スイッチド ポート アナライザ
SSTP	Cisco Shared Spanning-Tree
STP	Spanning-Tree Protocol: スパニングツリー プロトコル
SVC	Switched Virtual Circuit:相手先選択接続
SVI	Switched Virtual Interface: スイッチ仮想インターフェイス
TACACS+	Terminal Access Controller Access Control System Plus
TARP	Target Identifier Address Resolution Protocol
TCAM	Ternary Content Addressable Memory
TCL	Table Contention Level
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
TIA	Telecommunications Industry Association:電気通信工業会
TopN	ユーザがレポートを使用してポート トラフィックを分析するための ユーティリティ
ToS	Type of Service: タイプ オブ サービス
TLV	Type-Length-Value
TTL	Time To Live:存続可能時間
TVX	有効な伝送
UDLD	UniDirectional Link Detection Protocol:単一方向リンク検出プロトコル
UDP	User Datagram Protocol: ユーザ データグラム プロトコル
UNI	User-Network Interface
UTC	Coordinated Universal Time:世界標準時
VACL	VLAN Access Control List: VLAN アクセス コントロール リスト
VCC	Virtual Channel Circuit:仮想チャネル回線
VCI	Virtual Circuit Identifier:仮想回線識別子
VCR	Virtual Configuration Register: 仮想コンフィギュレーション レジスタ
VINES	Virtual Network System
VLAN	Virtual LAN

略語	説明
VMPS	VLAN Membership Policy Server: VLAN メンバシップ ポリシー サーバ
VPN	Virtual Private Network: バーチャル プライベート ネットワーク
VRF	VPN Routing/Forwarding: VPN ルーティングおよび転送
VTP	VLAN Trunking Protocol
VVID	Voice VLAN ID
WFQ	Weighted Fair Queuing:重み付け均等化キューイング
WRED	Weighted Random Early Detection:重み付けランダム早期検出
WRR	Weighted Round-Robin: 重み付けラウンドロビン
XNS	Xerox Network System



INDEX

Numerics	WoL 37-12
10 ギガビット イーサネット ポート ギガビット イーサネット SFP ポートの配置 6-8 10 ギガビット イーサネット ポートおよびギガビット イーサネット SFP ポートの配置 6-8	音声 VLAN ポート 37-19 クリティカル認証に対する 37-12 ゲスト VLAN 37-9 ポート セキュリティ 37-15 802.3ad
10 ギガビット イーサネット ポートおよびギガビット イーサネット ポートの WS-X4606-10GE-E および Supervisor Engine 6-E への配置 6-10 10 ギガビット イーサネット ポートまたはギガビット イーサネット ポート WS-X4606-10GE-E および Supervisor 6-E 6-10 10/100 自動ネゴシエーション機能、強制 6-15	AAA 39-1 ACE ACL 42-2
1400 W DC SP トリプル入力電力装置 特記事項 10-18 1400 W DC 電力装置 特記事項 10-17 802.10 SAID (デフォルト) 13-5	IP 42-2 レイヤ4演算の制約事項 42-16 ACE と ACL 39-1 ACL ACE 42-2
802.1Q 他の機能を備えたトンネル ポート 23-6 トランク 17-6 トンネリング 説明 23-2 他の機能との互換性 23-5 デフォルト 23-4	CPU への影響 42-18 IP、ポート ACL の一致基準 42-4 MAC 拡張 42-20 SPAN 45-6 Sup 6-E の TCAM プログラミング 42-16 Sup II-Plus から V-10GE の TCAM プログラミンク
802.1Q VLAN カプセル化 15-4 トランクの制約事項 15-6	42-7 TCAM プログラミング アルゴリズム 42-8 TCAM プログラミング アルゴリズムの変更 42-9
802.1s MST を参照 802.1w MST を参照 802.1X	TCAM リージョンのサイズ変更 42-11 VLAN マップ 42-5 VLAN マップでの設定 42-32 同じスイッチでの互換性 42-3
ポートベースの認証を参照 802.1X で許可ステートのポート 37-5 802.1X で無許可ステートのポート 37-5 802.1X 認証 MAC 認証バイパスに対する 37-10	概要 42-2 高 CPU のトラブルシューティング 42-12 サポートされるタイプ 42-3 処理 42-18 スイッチド パケットへの適用 42-32 制御パケットのキャプチャのモード選択
RADIUS アカウンティング 37-16	42-13

VLAN 割り当て 37-7

ハードウェアおよびソフトウェアのサポート	BPDU
42-6	擬似ブリッジ 17-28
ポート	内容 17-3
音声 VLAN 42-5	メディア速度 17-2
制限 42-5	BPDU ガード
定義 42-3	MST 17-26
ルータ ACL の一致基準 42-3	概要 19-9
ルーテッド パケットへの適用 42-33	設定 19-19
レイヤ 3 インターフェイスへの IPv6 ACL の適用	BSR
42-23	
ACL および VLAN マップ、例 42-26	設定例 31-24
ACL による高 CPU のトラブルシューティング	
42-12	С
ACL による高 CPU、トラブルシューティング	
42-12	Catalyst 4500 スイッチでの電源管理の制限事項
ARP	10-9
定義 4-31	Catalyst 4500 スイッチの電源管理
テーブル	冗長モード 10-8
アドレス解決 4-31	複合モード 10-8
管理 4-31	CDP
Automatic QoS	LLDP で定義 25-2
QoS を参照	インターフェイス上でのイネーブル化 24-3
Auto-QoS	概要 1-2, 24-2
設定 34-19	コミュニティ内の自動検出 12-7
auto-sync コマンド 8-8	信頼境界 34-28
	設定 24-2
	設定の表示 24-3
В	メンテナンス 24-4
	モニタリング 24-4
b flash コマンド 53-3	レイヤ 2 プロトコル トンネリング 23-8
b コマンド 53-3	cdp enable コマンド 24-3
BackboneFast	CE デバイス 33-2
MST 17-26	CEF
STP も参照	イネーブル化 28-7
概要 19-16	サポーフルル 26-7 および NSF/SSO 9-6
サポートされていない MST 17-26	
スイッチの追加(図) 19-4	概要 28-2 ソフトウェア スイッチング 28-4
設定 19-19	
リンク障害(図) 19-17, 19-18	統計情報の表示 28-9
BGP 1-9	ハードウェア スイッチング 28-4
Multi-VRF CE のルーティング セッション 33-7	隣接関係テーブル 28-2
boot bootldr コマンド 3-33	ロード バランシング 28-6
boot system flash コマンド 3-30	ロード バランシングの設定 28-7
boot system コマンド 3-28, 3-33	CGMP
boot コマンド 3-29	概要 21-2
Border Gateway Protocol	channel-group group コマンド 20-8, 20-10
・ ボーダー ゲートウェイ プロトコル	Cisco 7600 シリーズ インターネット ルータ
BGP を参照	SNMP のイネーブル化 52-5
····	

Cisco Discovery Protocol	コントロール プレーンに QoS サービス ポリシー
シスコ検出プロトコル	を適用 39-5
CDP を参照	設定
Cisco Express Forwarding	MLS QoS のイネーブル化 39-5
CEF を参照	サービス ポリシー マップ 39-5
Cisco Group Management Protocol	トラフィックに一致する ACL 39-5
CGMP を参照	パケット分類基準 39-5
Cisco IOS NSF 対応サポート 9-2	統計情報のモニタリング 39-10
Cisco IOS NSF 認識	表示
サポート 9-2	ダイナミック情報 39-10
Cisco IP Phone	適合するバイトとパケットの数 39-10
音質 35-2	比率情報 39-10
設定 35-4	copy running-config startup-config コマンド 3-10
CiscoWorks 2000 47-5	copy system:running-config nvram:startup-config コマンド
CIST	3-33
=	CoS
	Cisco IP Phone での変更 35-7
class-map コマンド 34-35	図 34-2
clear cdp counters コマンド 24-4	定義 34-4
clear cdp table コマンド 24-4	プライオリティ 35-7
clear counters コマンド 6-31	CoS 値、インターフェイス用の設定 34-57
clear ip eigrp neighbors コマンド 27-21	CoS 転換
clear ip flow stats コマンド 48-10	設定 34-44
CLI	CoS/DSCP マップ 34-61
1 レベル後退 2-6	CPU ポートのスニッフィング 45-12
ROM モニタ 2-9	CPU、ACL 処理の影響 42-18
アクセス 2-2	CST 42-16
環境のモニタ 45-1	
クラスタの管理 12-14	IST 17-25
コマンドの取得 2-7	MST 17-25 ⇒8 □ 17-20
ソフトウェアの基礎知識 2-5	説明 17-29
ヒストリ置換 2-4	
モード 2-6	D
Common and Internal Spanning-Tree	
CIST を参照	DBL
Common Spanning-Tree	グローバルに 34-30
CST を参照	特定 CoS 值 34-32
config-register コマンド 3-30	特定 IP DSCP 值 34-31
configure terminal コマンド 3-9, 3-30, 6-3	DBL 経由の AQM、Supervisor Engine 6-E での QoS
confreg コマンド 53-4	34-93
CoPP	DBL 経由のアクティブ キュー管理、Supervisor Engine
概要 39-2	6-E での QoS 34-93
コントロール プレーン コンフィギュレーション	description コマンド 6-18
エード	dev コマンド 53-3
設置 39 <i>-</i> 5	DHCP オプション 82
コントロール プレーン コンフィギュレーション	概要 40-4
モードの開始 39-5	DHCP スヌーピング
	イネーブル化 40-9

イネーブル化、およびオブション 82 40-11	デフォルト設定 4-16
エッジ スイッチからの信頼できないパケットの受	Domain Name System
け入れ 40-11	DNS を参照
オプション 82 データ挿入 40-4	DoS 攻撃
概要 40-2	IP アドレス スプーフィング、軽減 29-5
集約スイッチ上でのイネーブル化 40-11	ユニキャスト RPF、展開 29-5
情報の表示 40-18	DSCP 値
スヌーピング データベース エージェント 40-3	
設定 40-8	IP precedence 34-2 送信キューへのマッピング 34-59
設定の表示 40-18	
データベース エージェントのイネーブル化	定義 34-4
40-13	マークダウンのマッピング 34-26
デフォルト設定 40-8	マップの設定 34-61
バインディング テーブルの表示 40-18	DSCP 値、ポート値の設定 34-58
プライベート VLAN 上でのイネーブル化	DSCP マップ 34-61
40-13	DSCP/CoS マップ
メッセージの交換プロセス 40-5	設定 34-63
DHCP スヌーピング データベース エージェント	DTP
TFTP ファイルからの読み取り(例) 40-15	VLAN トランク 15-4
イネーブル化 (例) 40-14	duplex コマンド 6-17
概要 40-3	Dynamic ARP Inspection
データベースへの追加(例) 40-17	ARP キャッシュのポイズニング 41-2
DHCP ベースの自動設定	ARP パケットのレート制限 41-5
BOOTP に対する関係 3-3	設定 41-18
	DoS 攻撃、防止 41-18
	インターフェイスの信頼状態、セキュリティ適用
クライアントの要求メッセージの交換 3-3	範囲 41-3
設定	概要 41-2
DNS 3-5	確認検査、実行 41-20
TFTP サーバ 3-5	スタティック バインディングのプライオリティ
クライアント側 3-3	41-4
サーバ側 3-4	設定
リレー装置 3-6	DHCP 環境 41-6
リース オプション	着信 ARP パケットのレート制限 41-18
IP アドレス情報 3-4	非 DHCP 環境の ACL 41-11
コンフィギュレーション ファイルの受信	ログ バッファ 41-15
3-4	ドロップされたパケットのロギング 41-4
例 3-7	ポート チャネル、その動作 41-5
DiffServ アーキテクチャ、QoS 34-2	目的 41-3
DiffServ コード ポイント値	ログ バッファ
DSCP 値を参照	設定 41-15
dir device コマンド 53-3	Dynamic Host Configuration Protocol スヌーピング
disconnect コマンド 7-8	DHCP スヌーピングを参照
DNS	Dynamic Trunking Protocol
DHCP ベースの自動設定 3-5	ダイナミック トランキング プロトコル
概要 4-15	ウイナミック ドラフィブグ フロドコル DTP を参照
設定 4-16	ロロでの流
設定の表示 4-17	

E	物理インターフェイスの設定 20-8
	ポートチャネル インターフェイス 20-2
E シリーズでの Enhanced PoE サポート 11-15	モード 20-3
EAPフレーム	レイヤ 2 の設定 20-10
Request/Identity 37-4	レイヤ 3 の設定 20-7
Response/Identity 37-4	Explicit Host Tracking
交換(図) 37-5, 37-6, 37-11	イネーブル化 21-10
再送信回数の設定 37-48	Extensible Authentication Protocol over LAN 37-2
再送信時間の変更 37-47	Exterior Gateway Protocol
EAPOL フレーム	EGP を参照 1-9
802.1X 認証 37-3	
OTP 認証、例(図) 37-5, 37-11	F
開始 37-4	г
EGP	FIB
概要 1-9	MFIB も参照
EIGRP	説明 28-2
設定例 27-21	frame コマンド 53-7
モニタリングおよびメンテナンス 27-21	
eigrp stub コマンド 27-20	
EIGRP スタブ ルーティング、設定 27-15	G
EIGRP (Enhanced IGRP)	
スタブ ルーティング	get-bulk-request 動作 47-4
概要 27-16	get-next-request 動作 47-4, 47-5
確認 27-20	get-request 動作 47-4, 47-5
制約事項 27-20	get-response 動作 47-4
設定 27-16	
設定作業 27-20	н
利点 27-20	
EIGRP (拡張 IGRP)	hello タイム (STP)
概要 1-9	設定 17-20
enable コマンド 3-9, 3-30	Hot Standby Router Protocol
Enhanced Interior Gateway Routing Protocol	HSRP を参照
EIGRP を参照	HSRP
EtherChannel	説明 1-8
channel-group group コマンド 20-8, 20-10	http
interface port-channel コマンド 20-7	//www.cisco.com/univercd/cc/td/doc/product/software/
lacp system-priority	ios124/124tcr/tcf_r/index.htm 24-1, 46-1,
コマンド例 20-13	47-1, 49-1
PAgP	hw-module module num power コマンド 10-20
概要 20-4	
port-channel load-balance コマンド 20-14	1
インターフェイスの削除 20-15	ı
概要 20-2	i コマンド 53-3
削除 20-15	ICMP
設定 20-7 20-15	IP traceroute の実行 7-10
設定時の注意事項 20-6	ping 7-9
300 C	1 0

Time-Exceeded メッセージ 7-10	interface range コマンド 6-5
イネーブル化 7-13	interface コマンド 3-9, 6-2
IDS	Interior Gateway Routing Protocol
SPAN と RSPAN で使用 45-3	IGRP を参照
IEEE 802.1s	Internet Control Message Protocol
MST を参照	ICMP を参照
IEEE 802.1w	IP
MST を参照	スタティック ルートの設定 3-12
IEEE 802.3ad	デフォルト ゲートウェイの設定 3-11
LACP を参照	統計情報の表示 28-9
IGMP	フロー スイッチング キャッシュ 48-10
Explicit Host Tracking 21-4, 21-10	ip cef コマンド 28-7
IGMP を参照	IP Enhanced IGRP
Leave タイマーの設定	インターフェイス、表示 27-21
イネーブル化 21-9	ip flow-aggregation cache destination-prefix コマンド
イネーブル化 31-15	48-12
概要 21-2	ip flow-aggregation cache prefix コマンド 48-12
設定可能な Leave タイマー 21-4 説明 31-3	ip flow-aggregation cache source-prefix コマンド 48-12
即時脱退処理 21-3	ip flow-export コマンド 48-10
脱退処理、イネーブル化 22-10	ip icmp rate-limit unreachable コマンド 7-13
レポート抑制	ip igmp profile コマンド 21-20
ディセーブル化 22-12	ip igmp snooping tcn flood query count コマンド 21-13
IGMP グループ	ip igmp snooping ten flood コマンド 21-12
最大数の設定 21-23	ip igmp snooping ten query solicit コマンド 21-14
IGMP スヌーピング	ip load-sharing per-destination コマンド 28-8
IP マルチキャスト 31-4	ip local policy route-map コマンド 32-5
イネーブル化 21-5, 21-6	ip mask-reply コマンド 7-14
イネーブル化およびディセーブル化 22-7	IP MTU サイズ、設定 27-10
概要 21-2	ip multicast-routing コマンド 31-15
設定時の注意事項 21-5	IP Phone
デフォルト設定 22-6, 22-7	Cisco IP Phone を参照 35-2
IGMP 即時脱退	QoS の信頼境界 34-28
設定時の注意事項 21-9	音声ポートの設定 35-5
IGMP フィルタリング	自動分類およびキューイング 34-19
設定 21-20	ip pim dense-mode コマンド 31-15
説明 21-20	ip pim sparse-dense-mode コマンド 31-16
デフォルト設定 21-20	ip pim コマンド 31-16
IGMP プロファイル	ip policy route-map コマンド 32-5
コンフィギュレーション モード 21-20	ip redirects コマンド 7-14
設定 21-21	ip route-cache flow コマンド 48-8
適用 21-22	IP traceroute
IGRP	概要 7-10
説明 1-10	実行 7-10
interface port-channel コマンド 20-7	ip unreachables コマンド 7-13
interface range macro コマンド 6-7	IP アドレス
	クラスタ コマンド スイッチ 12-12

クラスタの候補またはメンバ 12-13	IPX
検出 4-31	EIGRP によるルート情報の再配布 1-9
IP アンナンバード サポート	ISL
DHCP オプション 82 14-2	802.1Q トンネリングによるトランキング 23-4
DHCP サーバとリレー エージェントでの 14-2	カプセル化 15-4
LAN および VLAN インターフェイスに対する設	ISSU
定 14-4	Cisco Feature Navigator を使用した互換性の検証
イーサネット VLAN 範囲に対する設定 14-5	5-13
エージェント リモート ID サブオプションの形式	NSF の概要 5-3
14-3	SNMP サポート 5-13
接続したホストのポーリングでの 14-3	SSO の概要 5-3
接続したホストのポーリングでの設定 14-6	互換性マトリクス 5-12
設定の表示 14-8	サポートするソフトウェアのバージョン許容範囲
トラブルシューティング 14-9	5-11
IP 以外のトラフィックのフィルタリング 42-20	制約事項 5-2
IP 情報	前提条件 5-2
割り当て	プロセスの概要 5-6
DHCP ベースの自動設定 3-3	プロセスの実行
IP ソース ガード	ISSU ステートの確認 5-17
概要 40-19	新しくスタンバイになったスーパーバイザ エ
設定 40-20	ンジンへの新しいソフトウェアの
表示 40-22, 40-24	ロード 5-24
プライベート VLAN 上での設定 40-21	互換性マトリクスの表示 5-28
IP 統計情報	冗長モードの確認 5-15
表示 28-9	スタンバイ スーパーバイザ エンジンへの新し
IP マルチキャスト	いソフトウェアのロード 5-17
Auto-RP、IGMP、PIM、RP、RPF も参照	スタンバイ スーパーバイザ エンジンへの切り 替え 5-20
IGMP スヌーピング 21-5, 31-4	ョル - 3-20 セーフガードとしてのロールバック タイマー
PIM 情報の表示 31-17	の設定 5-27
イネーブル化 31-15	ソフトウェア アップグレードの中断 5-26
概要 31-2	ソフトウェア インストレーションの確認
希薄モードのイネーブル化 31-16	5-14
サポートされない機能 31-13	ロールバック タイマーの停止 5-23
稠密モード PIM のイネーブル化 31-15	IST
設定 31-14	MST リージョンを参照 17-25
ソフトウェアによる転送 31-9	説明 17-25
テーブル エントリの削除 31-23	マスター 17-30
デフォルト設定 31-14	
ハードウェアによる転送 31-9 モニタリング 31-17	L
	10 11 1 7 1 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1
ルーティング テーブル情報の表示 31-18	12protocol-tunnel コマンド 23-12
ルーティング プロトコル 31-3	LACP
IP ユニキャスト	システム ID 20-5
統計情報の表示 28-9	Link Layer Discovery Protocol
IP ルーティング テーブル	CDP を参照
エントリの削除 31-23	

LLDP	テーブルの作成 4-20, 15-3
イネーブルおよびディセーブル	デフォルト設定 4-21
インターフェイス上 25-6	表示 4-30,7-4
グローバルに 25-5	割り当て 17-6
概要 25-2	MAC アドレスの限定 17-2
設定 25-4	MAC 拡張アクセス リスト 42-20
デフォルト設定 25-4	MAC 認証バイパス
特性 25-4	802.1X による設定 37-36
送信タイマーおよびホールドタイム、設定 25-4	MAC/PHY コンフィギュレーション ステータス TLV 25-2
モニタリングおよびメンテナンス 25-8	main-cpu コマンド 8-8
LLDP Media Endpoint Discovery	mask destination コマンド 48-12
LLDP-MED も参照	mask source コマンド 48-12
LLDP-MED	match ip address コマンド 32-4
概要 25-2	MDA
サポートされる TLV 25-2 設定	設定時の注意事項 37-20 37-21 説明 37-20
TLV 25-7	meminfo コマンド 53-7
手順 25-4	MFIB
モニタリングおよびメンテナンス 25-8	CEF 31-6
logoutwarning コマンド 7-7	概要 31-12
	表示 31-21
N 4	MIB
M	SNMP の相互作用 47-5
M ツリー 17-26	概要 47-2
M レコード 17-26	関連情報 52-3
MAC アドレス	コンパイル 52-4
ACL 42-20	ダウンロード 52-3,52-4
DHCP スヌーピング バインディング テーブルでの	MIB のコンパイル 52-4
表示 40-18	MIB のダウンロード 52-3, 52-4
VLAN アソシエーション 4-21	MLD Done メッセージおよび即時脱退 22-4
エージング タイム 4-21	MLD クエリー 22-3
検出 4-31	MLD スヌーピング
スタティック	MLD Done メッセージおよび即時脱退 22-4
削除 4-28	MLD クエリー 22-3
追加 4-28	MLD メッセージ 22-3
特性 4-27	MLD レポート 22-4
ドロップ 4-29	概要 22-2
認可 4-30	マルチキャスト クライアント エージングの堅牢
スティッキ 38-5	性 22-3
スティッキ セキュア、追加 38-6	マルチキャスト ルータ検出 22-4
ダイナミック	MLD メッセージ 22-3
学習 4-20	MLD レポート 22-4
削除 4-22	MST
ダイナミックからスティッキ セキュアへの変換	BPDU 17-26
38-6	PVST+ とのインターオペラビリティ 17-26
	SST とのインターオペラビリティ 17-28

イネーブル化 17-33	設定(例) 48-15
インスタンス	source-prefix 集約
サポートされる数 17-29	最小マスク、設定 48-12
説明 17-26	集約
パラメータの設定 17-36	最小マスク、デフォルト値 48-11
エッジ ポート 17-30	スイッチング
境界ポート 17-30	キャッシュ エントリのエクスポート
コンフィギュレーション パラメータ 17-29	48-10
制約事項 17-32	収集のイネーブル化 48-8
設定 17-33	スイッチド IP フローの設定 48-8
設定の表示 17-37	設定(例) 48-14
複数のスパニングツリー 1-3, 17-25	統計情報 48-10
ホップ カウント 17-31	必要なハードウェアの確認 48-7
マスター 17-30	NetFlow 統計情報
メッセージ エージ 17-31	キャッシュ エントリのエクスポート 48-10
リージョン 17-29	収集機能の概要 48-2
リンク タ イプ 17-31	収集機能の設定 48-7
MSTP	収集のイネーブル化 48-8
M ツリー 17-26	スイッチド / ブリッジド IP フロー 48-8
M レコード 17-26	スーパーバイザの注意事項 48-7
MTU	必要なハードウェアの確認 48-7
概要 6-23	Network Assistant
MTU サイズ	CLI コマンドの概要 12-3
設定 6-25, 6-26, 6-33, 6-34	VTY 12-13
デフォルト 13-5	設定する
Multiple Spanning-Tree	スイッチとの通信を可能にする 12-14,
MST を参照	12-18
Multi-VRF CE	デフォルト設定 12-2
コンポーネント 33-3	Network Time Protocol
設定例 33-8	NTP を参照
定義 33-1	Next Hop Resolution Protocol
デフォルト設定 33-4	NHRP を参照
ネットワーク コンポーネント 33-3	NFFC/NFFC II
パケット転送プロセス 33-3	IGMP スヌーピング 21-5
表示 33-12	NHRP
	サポート 1-10
N I	Nonstop Forwarding
N	NSF を参照
NetFlow	NSF
destination-prefix 集約	注意事項および制約事項 9-10
Gestination-pichx 来版 最小マスク、設定 48-12	定義 9-1
設定(例) 48-17	動作 9-5
IP	NSF 対応
 フロー スイッチング キャッシュ 48-10	サポート 9-2
prefix 集約	スーパーバイザ エンジン 9-4
prenx 集約 最小マスク、設定 48-12	NSF 認識
HX'1' \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \	サポート 9-2

スーパーバイザ エンジン 9-3	概要 32-2
NSF/SSO スーパーバイザ エンジンの冗長構成	機能 32-2
SSO の動作 9-5	使用 32-3
および CEF 9-6	設定(例) 32-6
概要 9-4	ルートマップ 32-2
NTP	PE から CE のルーティング、設定 33-7
アクセスの制限	PE デバイス 33-2
アクセス グループの作成 4-9	per-Port per-VLAN QoS
インターフェイス単位での NTP サービスの	イネーブル化 34-52
ディセーブル化 4-10	概要 34-17
アソシエーション	Per-VLAN Rapid Spanning-Tree 17-7
サーバ 4-6	イネーブル化 17-22
定義 4-3	概要 17-7
認証 4-4	PIM
ピア 4-6	概要 31-3
ブロードキャスト メッセージのイネーブル化	希薄 / 稠密モードのイネーブル化 31-16
4-7	希薄モードの設定 31-16
概要 4-2	稠密モードの設定 31-15
時刻	情報の表示 31-17
サービス 4-3	
同期化 4-2	
ストラタム 4-2	PIM-DM 31-4
設定の表示 4-11	PIM-SM 31-4
送信元 IP アドレス、設定 4-10	ping
デバイスの同期化 4-6	概要 7-9
デフォルト設定 4-4	実行 7-9
NVRAM	ping コマンド 7-9, 31-17
設定値の保存 3-10	PoE
	E シリーズでの拡張サポート 11-15
	インターフェイス ステータスの表示 11-9
0	受電装置の電力消費量
OIR	インテリジェントな電源管理 11-5
	概要 11-6
概要 6-30	サポートされているケーブル接続トポロジ
Open Shortest Path First	11-8
OSPF を参照	スイッチの電力消費量の設定 11-6
OSPF	単一デバイスの電力消費量の設定 11-6
エリア概念 1-11	電源管理モード 11-3
説明 1-11	モジュールで消費される PoE の表示 11-11
	モジュールの電源切断 10-20
P	police コマンド 34-40
	policy-map コマンド 34-36, 34-38
PACL、アクセス グループ モードとの併用 42-35	Port Aggregation Protocol
PAgP	PAgP を参照
概要 20-4	port-channel load-balance
PBR(ポリシーベース ルーティング)	コマンド 20-13
イネーブル化 32-4	コマンド例 20-13

port-channel load-balance コマンド 20-14	設定およびデフォルトの表示 34-22
PortFast	設定時の注意事項 34-21
BPDU フィルタ、設定 19-11	説明 34-19
MST 17-26	表示 34-22
概要 19-7	CoS、DSCP 値、送信キューも参照
設定またはイネーブル化 19-19	IP Phone
PortFast BPDU フィルタリング	検出および trusted 設定 34-19, 34-28
MST 17-26	自動分類およびキューイング 34-19
イネーブル化 19-11	PVQoS のイネーブル化 34-52
概要 19-10	PVQoS の概要 34-17
power dc input コマンド 10-17	UBRL の設定 34-45
power inline consumption コマンド 11-6, 11-7	VLANベース 34-55
power inline コマンド 11-4	イネーブル化およびディセーブル化 34-55
power redundancy-mode コマンド 10-11	インターフェイス上でのイネーブル化 34-43
PVACL 40-19	インターフェイス上でのディセーブル化
PVID (ポート VLAN ID)	34-43
音声 VLAN ポートを使用した 802.1X 37-19	階層型ポリサーのイネーブル化 34-50
PVLAN	概要 34-2
802.1Q サポート 36-12	基本モデル 34-6
VLAN の設定 36-13	信頼状態
概要 36-1	信頼できるデバイス 34-28
混合モード ポートの設定 36-15	設定
設定 36-10	Auto-QoS 34-19
インターフェイス モード 36-22	DBL 34-29
設定時の注意事項 36-11	DSCP マップ 34-61
複数のスイッチ 36-5	信頼境界 34-28
ポート セキュリティを設定 38-16, 38-18, 38-20	トラフィック シェーピング 34-60
ホストポート	設定時の注意事項 34-27
設定 36-22	Auto-QoS 34-21
レイヤ 2 インターフェイスの設定 36-16	送信レート 34-60
無差別モード	ソフトウェア処理されるパケット 34-17
無差別に一下 設定 36-22	帯域幅の割り当て 34-60
設定 30-22 ルーティングの許可、例 36-21	定義 34-4
レイヤ 2 EtherChannel でのポート セキュリティの	デフォルト設定 34-26
シャド 2 Editer Chainler Cのホード ビーエッティの 設定 38-37	デフォルトの自動設定 34-19
ワイヤレス環境でポート セキュリティを設定	トラフィック シェーピング 34-17
38-36	名前付き集約ポリサーの作成 34-33
PVLAN 混合モード トランク ポート	バーストサイズ 34-34
設定 36-2, 36-15, 36-19	パケットの変更 34-17
	プライオリティ 34-16
•	フローチャート 34-8, 34-13
Q	分類 34-7 34-10
QoS	ポートベース 34-55
Auto-QoS	ポリシング ルールの作成 34-35
	レイヤ 2 インターフェイス上での VLAN ベースの
NVRAM 設定の影響 34-20	シャンテーフェイスエ CO VLAN ペースの 設定 34-55
VoIP に対するイネーブル化 34-21	

レイヤ2制御パケット OoS の設定、概要 range macro 34-64 定義 6-7 レイヤ2制御パケット QoS の設定、機能の相互作 range コマンド 6-5 34-69 Rapid Spanning-Tree レイヤ2制御パケット OoS の設定、注意事項 RSTP を参照 rcommand コマンド 12-14 QoS アクティブ キュー管理 Release 7.7 の新しいソフトウェア機能 キュー長の追跡 TDR 7-5 QoS サービス ポリシー reload コマンド 3-30, 3-31 前提条件 34-75 **REP** 適用に関する制約事項 34-75 MST 18-6 QoS の信頼境界 34-28 SNMP トラップ、設定 18-14 QoS の送信キュー VLAN ブロッキング 18-13 DHCP 値のマッピング 34-59 VLAN ロード バランシング 18-4 概要 34-15 VLAN ロード バランシングのトリガー 18-5 最大速度 34-17 インターフェイスの設定 18-9 帯域幅の割り当て 34-60 オープン セグメント 18-2 トラフィック シェーピングの設定 34-60 管理 VLAN 18-8 バースト 34-17 管理 VLAN、設定 18-8 リンク帯域幅の共有 34-16 コンバージェンス 18-4 QoS の送信キュー、設定 34-59 サポートされているインターフェイス 18-2 OoS のマーキング 手動によるプリエンプション、設定 18-13 説明 34-5 セカンダリ エッジ ポート 18-4 QoS のマッピング テーブル セグメント 18-2 CoS/DSCP 34-61 特性 18-3 DSCP/CoS 34-63 設定時の注意事項 18-7 タイプ 34-15 デフォルト設定 18-7 ポリシング済み DSCP 34-62 ネイバー オフセット番号 18-4 QoS ポリサー プライマリ エッジ ポート 18-4 種類 34-10 プリエンプト遅延時間 18-5 バースト サイズ 34-34 ポート 18-6 QoS ポリシー モニタリング 18-15 インターフェイスへの付加 34-12 リング セグメント 18-2 設定の概要 34-35 リンク完全性の確認 18-3 QoS ポリシング reset コマンド 53-3 説明 34-6, 34-10 Resilient Ethernet Protocol。REP を参照 定義 34-5 **RFC** OoS ラベル 1157, SNMPv1 47-2 定義 34-4 1901、SNMPv2C 47-2 1305, NTP 4-2 R 1757、RMON 49-3 1902 ~ 1907, SNMPv2 47-2 RADIUS サーバ 2273 ~ 2275, SNMPv3 47-2 スイッチ上のパラメータ 37-26 RIP スイッチとの通信設定 37-26 説明 1-11 設定値の設定 37-28

RMON	S
アラームとイベントのイネーブル化 49-4	
概要 49-2	SAID
サポートされるグループ 49-3	802.10 SAID を参照
ステータスの表示 49-7	Security Association Identifier
デフォルト設定 49-4	802.10 SAID を参照
ROM モニタ	service-policy input コマンド 30-2, 34-43
CLI 2-9	service-policy コマンド 34-36
概要 53-1	set default interface コマンド 32-4, 32-5
コマンド 53-2 53-3	set interface コマンド 32-4
終了 53-7	set ip default next-hop コマンド 32-4
設置 53-2	set ip next-hop コマンド 32-4
デバッグ コマンド 53-7	set-request 動作 47-5
ブートプロセス 3-27	show adjacency コマンド 28-10
route-map (IP) コマンド 32-4	show boot コマンド 3-33
Routing Information Protocol	show catalyst4000 chassis-mac-address コマンド 17-3
RIP を参照	show cdp entry コマンド 24-4
RPF	show cdp interface コマンド 24-3
IP ユニキャストを <i>参照</i>	show cdp neighbors コマンド 24-4
RSPAN	show cdp traffic コマンド 24-4
IDS 45-3	show cdp コマンド 24-2, 24-4
VLAN ベース 45-6	show ciscoview package コマンド 4-34
宛先ポート 45-5	show ciscoview version コマンド 4-34
受信したトラフィック 45-4	show cluster members コマンド 12-14
セッション	show configuration コマンド 6-18
VLAN のモニタリング 45-26	show debugging コマンド 24-4
作成 45-21	show environment コマンド 10-2
送信元(モニタ対象)ポートの削除 45-25	show history コマンド 2-4
定義 45-3	show interfaces status コマンド 7-3
特定の VLAN に送信元トラフィックを制限	show interfaces コマンド 6-25, 6-26, 6-31, 6-33, 6-34
45-28 モニタ対象ポートの指定 45-21	show ip cache flow aggregation destination-prefix コマンド 48-12
設定時の注意事項 45-20	show ip cache flow aggregation prefix コマンド 48-12
送信されたトラフィック 45-4	show ip cache flow aggregation source-prefix コマンド 48-12
送信元ポート 45-5	show ip cache flow コマンド 48-10
モニタ対象ポート 45-5	show ip cef コマンド 28-8
モニタリング ポート 45-5	show ip eigrp interfaces コマンド 27-21
RSTP	show ip eigrp neighbors コマンド 27-21
互換性 17-26	show ip eigrp topology コマンド 27-21
説明 17-25	show ip eigrp traffic コマンド 27-21
ポートステート 17-27 ポートの(2.*) 17-27	show ip interface コマンド 31-17
ポートの役割 17-27	show ip local policy コマンド 32-5
	show ip mroute コマンド 31-17
	show ip pim interface コマンド 31-17
	show l2protocol コマンド 23-13
	show lldn traffic コマンド 25-9

show mac-address-table address コマンド 7-4	概要 47-4
show mac-address-table interface コマンド 7-4	設定 47-7
show mls entry コマンド 28-9	サポートされるバージョン 47-2
show module コマンド 7-2, 17-6	システム ログ メッセージを NMS に限定 46-10
show power inline consumption コマンド 11-6	システムの連絡先と設置場所 47-15
show power inline コマンド 11-9	ステータス、表示 47-18
show power supplies コマンド 10-11	設定時の注意事項 47-6
show protocols コマンド 6-31	設定例 47-16
show running-config コマンド	通知 47-5
ACL の表示 42-25, 42-28, 42-35, 42-36	デフォルト設定 47-6
インターフェイスの記述の追加 6-18	トラップ
設定の確認 3-10	MAC アドレス通知のイネーブル化 4-22
show startup-config コマンド 3-11	MAC 移動通知のイネーブル化 4-25
show users コマンド 7-8	MAC しきい値通知のイネーブル化 4-26
show version コマンド 3-31	イネーブル化 47-11
shutdown、コマンド 6-32	概要 47-2, 47-5
Single Spanning-Tree	種類 47-11
SST を参照	情報との違い 47-5
SmartPort マクロ	説明 47-4, 47-5
Web サイト 16-2	トラップ マネージャ、設定 47-13
グローバル パラメータ値の適用 16-9	認証レベル 47-10
アローバルバングー ア ii の ii	ホスト 47-6
設定時の注意事項 16-6	ユーザ 47-6, 47-9
定義 16-2	SNMP コマンド 52-5
デフォルト設定 16-4	SNMP トラップ
トレース 16-7	REP 18-14
パラメータ値の適用 16-9	SNMP のイネーブル化 52-5
表示 16-15	SNMPv1 47-3
マクロの適用 16-9	SNMPv2C 47-3
SNMP	SNMPv3 47-3
MIB 変数にアクセス 47-5	SPAN
TFTP サーバによるアクセスの限定 47-15	ACL 45-6
イネーブル化 52-5	IDS 45-3
インフォーム	VLANベース 45-6
inform および trap キーワード 47-11	宛先ポート 45-5
イネーブル化 47-15	受信したトラフィック 45-4
説明 47-5	セッション
トラップとの違い 47-5	定義 45-3
エージェント	設定 45-8 45-11
説明 47-4	設定時の注意事項 45-8
ディセーブル化 47-7	送信されたトラフィック 45-4
エンジン ID 47-6	送信元ポート 45-5
概要 47-2, 47-5	モニタ対象ポート、定義 45-5
グループ 47-6, 47-9	モニタリング ポート、定義 45-5
コミュニティ ストリング	

SPAN 拡張機能	拡張システム ID のイネーブル化 17-10
CPU ポートのスニッフィング 45-12	最大エージング タイム 17-20
アクセス リスト フィルタリング 45-16	設定 17-9 17-22
カプセル化の設定 45-14	ディセーブル化 17-22
設定例 45-19	デフォルト 17-8
入力パケット 45-14	転送遅延時間 17-21
パケット タイプ フィルタリング 45-18	トポロジの作成 17-5
SPAN ← RSPAN	ブリッジ ID 17-2
概念と用語 45-3	ポートコスト 17-17
概要 45-2	ポート プライオリティ 17-15
ステータスの表示 45-30	ルート ブリッジ 17-11
セッション限度 45-6	レイヤ 2 プロトコル トンネリング 23-8
デフォルト設定 45-7	Sup 6-E の TCAM プログラミングと ACL 42-16
spanning-tree backbonefast コマンド 19-19	Supervisor Engine 6-E システムの緊急アラーム 10-3
spanning-tree cost コマンド 17-18	Supervisor Engine 6-E での QoS
spanning-tree guard root コマンド 19-3	DBL 経由の AQM 34-93
spanning-tree portfast bpdu-guard コマンド 19-9	DBL 経由のアクティブ キュー管理 34-86,
spanning-tree portfast コマンド 19-8	34-93
spanning-tree port-priority コマンド 17-15	MQC ベースの QoS の設定 34-72
spanning-tree uplinkfast コマンド 19-14	アクション ドライバのマーキング 34-80
spanning-tree vlan	階層型ポリシー 34-95
コマンド 17-10	キュー制限 34-91
コマンド例 17-11	共有(帯域幅) 34-86
spanning-tree vlan cost コマンド 17-18	共有(帯域幅) シェーピング、およびプライオ
spanning-tree vlan forward-time コマンド 17-21	リティキュー 34-84
spanning-tree vlan hello-time コマンド 17-20	高レベル モデル 34-73
spanning-tree vlan max-age コマンド 17-21	サービス ポリシーの適用に関する制約事項 34-75
spanning-tree vlan port-priority コマンド 17-15	サービス ポリシーを適用するための前提条件
spanning-tree vlan priority コマンド 17-19	34-75
spanning-tree vlan root primary コマンド 17-12	シェーピング 34-84
spanning-tree vlan root secondary コマンド 17-14	設定 34-72
spanning-tree vlan コマンド 17-9	ソフトウェア QoS 34-98
speed コマンド 6-16	トラフィック マーキング手順のフローチャート
SSO	34-80
設定 9-11	ネットワーク トラフィックのマーキング
SSO の動作 9-5	34-77
SST	プライオリティ キュー 34-89
インターオペラビリティ 17-28	プラットフォーム ハードウェアの機能 34-75
説明 17-25	プラットフォームでサポートされる分類基準およ
STP	び QoS 機能 34-72, 34-74
hello タイム 17-20	プラットフォームの制約事項 34-77
Per-VLAN Rapid Spanning-Tree 17-7	分類 34-75 ポルン・フェーン・0部ウ
PVRST のイネーブル化 17-22	ポリシー マップ マーキング アクションの設定 34-82
REP 18-6	ポリシーの関連付け 34-97
イネーブル化 17-9	ポリシング 34-76
概要 17-2, 17-3	ポリシングの実装方法 34-77
	かりとととめ大公川は コサー//

マーキング用のハードウェア機能 34-82	TCAM プログラミング アルゴリズム
マルチ属性マーキングのサポート 34-81	変更 42-9
Supervisor Engine II-TS	TCAM プログラミング アルゴリズム、概要 42-8
- 不十分なインライン パワーの処理 10-18, 11-14	TCAM プログラミングおよび ACL 42-11, 42-13
Supervisor Engine II-TS に対する電力処理 11-14	Sup II-Plus から V-10GE 42-7
Supervisor Engine II-TS に対する不十分なインライン パ	TCAM リージョン、アルゴリズムの変更 42-9
ワーの処理 10-18	TCAM リージョン、サイズ変更 42-11
Supervisor Engine V-10GE O POST 50-9	TCN 処理
SVI 自動ステート除外	MLD スヌーピング
概要 27-3	TCN 処理 22-5
設定 27-9	TDR
switchport access vlan コマンド 15-8, 15-10	ケーブル接続の確認 7-5
switchport block multicast コマンド 43-2	注意事項 7-5
switchport block unicast コマンド 43-2	テストのイネーブル化およびディセーブル化
switchport mode access コマンド 15-10	7-5
switchport mode dot1q-tunnel コマンド 23-6	Telnet
switchport mode dynamic コマンド 15-7	CLI アクセス 2-2
switchport mode trunk コマンド 15-7	実行 7-7
switchport trunk allowed vlan コマンド 15-8	ユーザ セッションの切断 7-8
switchport trunk encapsulation dot1q コマンド 15-4	ユーザ セッションのモニタリング 7-8
switchport trunk encapsulation isl コマンド 15-4	telnet コマンド 7-7
switchport trunk encapsulation negotiate コマンド 15-4	Terminal Access Controller Access Control System Plus
switchport trunk encapsulation コマンド 15-7	TACACS+ を参照
switchport trunk native vlan コマンド 15-8	TFTP
switchport trunk pruning vlan コマンド 15-8	サーバによるアクセスの限定 47-15
sysret コマンド 53-7	自動設定の設定 3-5
	ベース ディレクトリのコンフィギュレーション
Т	ファイル 3-5
I	TFTP ダウンロード
TACACS+ 39-1	コンソール ダウンロードも参照
アカウンティング、定義 3-17	Time Domain Reflectometer
概要 3-16	TDR を参照
サーバの特定 3-19	Time-Exceeded メッセージ 7-10
設定	TLV
アカウンティング 3-23	LLDP-MED 25-2
ixi 3-22	定義 1-3, 25-2
認証 キー 3-19	ToS
ログイン認証 3-20	説明 34-4
設定の表示 3-23	trace コマンド 7-10
設定の役が 3-23 デフォルト設定 3-19	traceroute
動作 3-18	IP traceroute を参照
認可、定義 3-17	レイヤ 2 traceroute を参照
認可、定義 3-17 認証、定義 3-17	traceroute mac ip コマンド 7-12
認証、圧義 3-17 ユーザがアクセスしたサービスの追跡 3-23	traceroute mac コマンド 7-12
ユーザルのサービスの制限 3-22	TwinGig コンバータ
ユ シ NO ク こ人の向ibx 3-77	X2/TwinGig コンバータ モードの選択 6-11
	使用時の制限事項 6-11

ポート番号設定 6-10	標準範囲 13-4
TwinGig コンバータ使用時の制限事項 6-11	予約範囲 13-4
TwinGig コンバータによるポート番号設定 6-10	VLAN ACL
	VLAN マップを参照
	vlan dot1q tag native コマンド 23-4
U	VLAN ID、検出 4-31
UDLD	VLAN Trunking Protocol
イネーブル化 26-3	VTP を参照
概要 26-2	vlan コマンド 13-7
100女 20-2 ディセーブル化 26-4	VLAN トランク
デフォルト設定 26-3	概要 15-3
UniDirectional Link Detection Protocol	VLAN ブロッキング、REP 18-13
UDLD を参照	VLAN マップ
	VLAN への適用 42-28
UNIX Syslog サーバ サポートされるファシリティ 46-13	アクセス拒否の例 42-30
	エントリの作成および削除 42-25
デーモンの設定 46-11 メッセージ ロギング情報 46-12	エントリの順序 42-25
メッセージ ロギング情報 46-12 UplinkFast	使用(図) 42-5
-	設定 42-24
MST 17-26	設定時の注意事項 42-25
イネーブル化 19-19 概要 10.12	設定例 42-29
概要 19-13 User Based Rate Limiting	定義 42-3
_	ネットワークの使用 42-28
概要 34-45	パケットの許可 42-26
設定 34-46	パケットの拒否 42-26
	表示 42-31
V	ルータ ACL 42-32
	VLAN マップおよびルータ ACL との PACL 42-38
VACL	VLAN マップの設定 42-24
レイヤ 4 ポート演算 42-16	VLAN マップ、PACL およびルータ ACL 42-38
VLAN	VLAN メンバシップ ポリシー サーバ
ID (デフォルト) 13-5	VMPS を参照
PVLAN も参照	VLAN ロード バランシング
RSPAN による送信元トラフィックの制限	REP 18-4
45-28	VLAN ロード バランシング、トリガー 18-5
RSPAN によるモニタ 45-26	VMPS
インターフェイスの割り当て 13-8	クライアントでのダイナミック アクセス ポート
概要 13-2	の設定 13-24
拡張範囲 13-4	コンフィギュレーション ファイルの例 13-31
サービス プロバイダー ネットワークのカスタ	サーバの概要 13-19
マー番号 23-3	再試行間隔の設定 13-25
設定 13-6	ダイナミック ポート メンバシップ
設定時の注意事項 13-4	再確認 13-24, 13-25
説明 1-6	例 13-27
デフォルト設定 13-5 トランクトで15-8	データベース コンフィギュレーション ファイル
トランク上で許容 15-8	13-31
名前(デフォルト) 13-5	メンバシップの再確認間隔 13-25

割り当ての再確認 13-24	VTP サーバ
VMPS クライアント	設定 13-15
管理およびモニタリング 13-26	VTP 統計情報
スイッチの設定	表示 13-18
IP VMPS アドレスの入力 13-23	VTP ドメイン
VLAN メンバシップの再確認 13-24	説明 13-9
再確認間隔 13-25	VTP バージョン 2
再確認間隔の設定 13-25	VTP も参照
ダイナミック ポート 13-24	イネーブル化 13-15
ダイナミック VLAN メンバシップの概要	概要 13-11
13-22	VTP プルーニング
ダイナミック ポート VLAN メンバシップのトラ	イネーブル化 13-14
ブルシューティング 13-27	概要 13-11
デフォルト設定 13-22	VTP モード 13-10
VMPS サーバ	VTY & Network Assistant 12-13
概要 13-19	VVID(音声 VLAN ID)
セキュリティ モード	802.1X 認証 37-19
multiple 13-21	設定 35-5
open 13-20	1XAC 33-3
セキュア 13-20	
代替 VLAN 13-21	W
不正な VMPS クライアント要求 13-21	Waan
Voice over IP	WCCP
設定 35-2	機能 51-4
VPN	サービス グループ 51-7
サービス プロバイダー ネットワーク内 33-1	制約事項 51-6
転送 33-3	設定例 51-11
ルーティング / 転送テーブル	ルータに設定 51-2,51-12
VRF を参照	Web Cache Communication Protocol
ルーティングの設定 33-6	WCCP を参照 51-1
ルート 33-2	WoL
VRF	802.1X による設定 37-40
定義 33-3	
テ ー ブル 33-1	X
VTP	
VTP バージョン 2 も参照	X2/TwinGig コンバータ モードの選択 6-11
概要 13-9	
設定 13-14 13-18	_
設定時の注意事項 13-13	あ
ディセーブル化 13-17	アカウンティング
デフォルト設定 13-13	802.1X の設定 37-32
トランスペアレント モードの設定 13-17	TACACS+ 3-17, 3-23
レイヤ 2 プロトコル トンネリング 23-8	アクション ドライバのマーキング 34-80
VTP アドバタイズ	アクション ドライバ、マーキング 34-80
説明 13-10	アクセス VLAN 15-8
VTP クライアント	アクセス グループ モードの PACL との併用 42-35
設定 13-16	

アクセス グループ モード、PACL との併用 42-35	記述名の追加 6-18
アクセス グループ モード、レイヤ 2 インターフェイ	再起動 6-32
ス上での設定 42-36	情報の表示 6-31
アクセス コントロール エントリ	設定 6-3
ACE を参照	範囲設定 6-5
アクセス コントロール エントリとリスト 39-1	番号 6-2
アクセス ポート	命名 6-18
設定 15-10	メンテナンス 6-31
ポート セキュリティを設定 38-8, 38-25	モニタリング 6-31
レイヤ 2 プロトコル トンネリング 23-10	レイヤ 2 インターフェイスも参照
アクセス リスト	レイヤ2モード 15-4
WCCP での使用 51-9	インターフェイス コンフィギュレーション
アクセス リスト フィルタリング拡張機能 45-16	REP 18-9
アクセスの制限 NTP サービス 4-8	インターフェイス リンクおよびトランク ステータス イベント
TACACS+ 3-16	設定 6-33
アクティブ キュー管理 34-15	インターフェイス リンクおよびトランク ステータス
アドバタイズメント	イベントの設定 6-33
LLDP 1-3, 25-2	インターフェイス上での QoS のイネーブル化または
アドバタイズ、VTP	ディセーブル化 34-55
VTP アドバタイズを参照	インターフェイスの信頼状態、設定
アドレス	インターフェイスのデフォルト設定へのリセット
MAC アドレス テーブルの表示 4-30	6-35
MAC アドレスを参照	インターフェイスの範囲
MAC、検出 4-31	設定 6-5
スタティック	インテリジェントな電源管理 11-5
追加および削除 4-27	インライン パワー
定義 4-20	Cisco IP Phone での設定 35-7
ダイナミック	
エージング タイムの変更 4-21	う
学習 4-20	
削除 4-22	ウェブ キャッシュ
定義 4-20	キャッシュ エンジンを参照
アドレス解決 4-31	ウェブ キャッシュ サービス
7 I V X NT X T S I	説明 51-4
	ウェブ キャッシング
l l	WCCP も参照 51-4
A.,	ウェブ キャッシュ サービスを参照
イネーブル	ウェブ スケーリング 51-1
終了 3-25	
デフォルトの変更 3-25	_
レベルの設定 3-24	え
ログイン 3-25	エージング タイム
イネーブル モード 2-6	MAC アドレス テーブル 4-21
インターフェイス	MAC アトレス テーフル 4-21 エッジ ポート
概要 6-2	
カウンタのクリア 6-31	説明 17-30

お	き
オプション 82 DHCP スヌーピングのイネーブル化 40-11 オペレーティング システム イメージ	キーボード ショートカット 2-4 ギガビット イーサネット SFP ポート 10 ギガビット イーサネットの配置 6-8
システム イメージを参照	擬似ブリッジ
音声 VLAN	説明 17-28
IP Phone の音声トラフィック、説明 35-2	キャッシュ エンジン 51-1
IP Phone のデータ トラフィック、説明 35-3	キャッシュ エンジン クラスタ 51-1
音声 VLAN ポート	キャッシュ ファーム
802.1X を使用する 37-19	キャッシュ エンジン クラスタを参照
音声インターフェイス	キューイング 34-6, 34-15
設定 35-1	キュー制限、Supervisor Engine 6-E での QoS 34-91
音声トラフィック 11-2,35-7	境界ポート
音声ポート	説明 17-30
VVID の設定 35-5 オンライン診断 50-1	共有(帯域幅) Supervisor Engine 6-E での QoS 34-86
	許可ステートおよび無許可ステートのポート 37-5
か	
	<
階層型ポリサー、設定 34-50	(F. 1) - G. 11
階層型ポリシー、Supervisor Engine 6-E での QoS	組み込み CiscoView
34-95	インストールおよび設定 4-32
カウンタ	概要 4-31
MFIB の削除 31-23	情報の表示 4-34
インターフェイスのクリア 6-31	クライアント 000 1X 初末 07.2
拡張範囲 VLAN	802.1X 認証 37-3
VLAN を参照 仮想 LAN	クライアントの再認証
仮想 LAN VLAN を参照	手動による設定 37-49 定期的なイネーブル化 37-44
VLAN を参照 仮想コンフィギュレーション レジスタ 53-4	定期的なイネーブル化 37-44 クラスタリング スイッチ
D プセル化タイプ 15-4	サンステラング スキック 概要 12-12
ガラビルピッパラー 13-4 簡易ネットワーク管理プロトコル	(M.安 12-12 管理
SNMP を参照	E CLI を使用した 12-14
環境状態	計画の考慮事項
Supervisor Engine 6-E 10-3	CLI 12-14
Supervisor Engine II-Plus から V-10GE 10-2	パスワード 12-8
環境のモニタリング	コマンド スイッチの特性 12-12, 12-13
CLI コマンドの使用 10-2	VTY 12-13
管理 VLAN	コミュニティへの変換 12-10
REP、設定 18-8	クラスレベル、サービス ポリシー内の設定 34-91
管理 VLAN、REP 18-8	クリティカル認証
管理アドレス TLV 25-2	802.1X による設定 37-37
管理オプション	グローバル コンフィギュレーション モード 2-6
SNMP 47-2	クロック
	システム クロックを参照

け	設定 47-7
	コミュニティ ポート 36-4
ゲートウェイ	コミュニティへのメンバの追加 12-9
デフォルト ゲートウェイを参照	混合モード ポート
ゲスト VLAN	PVLAN の設定 36-15
802.1X による設定 37-33, 37-43	設定モード 36-22
検出、クラスタ	定義 36-5
自動検出を参照	コンソール コンフィギュレーション モード 2-6
	コンソール ダウンロード 53-6
_	コンソール ポート
こ	ユーザ セッションの切断 7-8
高速ドロップ	ユーザ セッションのモニタリング 7-8
エントリの削除 31-23	コントロール プレーン ポリシング
エントリの表示 31-22	CoPP も参照
概要 31-11	コンバージェンス
候補	REP 18-4
自動検出 12-7	コンフィギュレーション ファイル
日勤1950 12-7 候補スイッチ、クラスタ	コンフィヤコレーション ファイル DHCP による入手 3-6
定義 12-13	TFTP サーバ アクセスを限定 47-15
要件 12-13	システムの連絡先と設置場所の情報 47-15
コマンド	保存 3-10
b 53-3	コンフィギュレーション レジスタ
b flash 53-3	ROM モニタから変更 53-4
confreg 53-4	起動時の設定 3-29
dev 53-3	設定 3-28
dir device 53-3	設定の変更 3-30 3-31
frame 53-7	ブート フィールド
i 53-3	値の表示 3-31
meminfo 53-7	変更 3-30
reset 53-3	コンポーネント管理 TLV 25-3, 25-7
ROM モニタ 53-2 53-3	
ROM モニタのデバッグ 53-7	ਰੇ
SNMP 52-5	
sysret 53-7	サーバ、VTP
ブート 53-3	VTP サーバを参照
リスト 2-7	サービス クラス
コマンド スイッチ、クラスタ	CoS を参照
要件 12-12	サービス プロバイダー ネットワーク
コマンドモード 2-6	カスタマー VLAN 23-2
コマンドの省略 2-6	サービス ポリシーでのクラスレベル キュー制限の設
コマンドライン処理 2-4	定 34-91
コミュニティ VLAN 36-3, 36-4	サービス ポリシー、クラスレベル キュー制限の設定
PVLAN としての設定 36-13	34-91
SPAN 機能 36-11	サービス品質
コミュニティ ストリング	QoS を参照
概要 47-4	

再送信回数	エラー メッセージの重大度の定義 46-9
802.1X 認証の設定 37-48	概要 46-2
再送信時間	シーケンス番号、イネーブル化およびディセーフ
802.1X 認証の変更 37-47	ル化 46-8
最大エージング タイム (STP)	設定の表示 46-13
設定 17-20	タイムスタンプ、イネーブル化およびディセーフ
削除	ル化 46-8
IP マルチキャスト テーブル エントリ 31-23	ディセーブル化 46-4
サブドメイン、プライベート VLAN 36-3	デフォルト設定 46-4
	表示先装置の設定 46-5
	ファシリティ キーワード、説明 46-13
U	メッセージの形式 46-3
SIT — VIII Supervisor Engine 6 E 700 Oct	メッセージの制限 46-10
シェーピング、Supervisor Engine 6-E での QoS 34-84	レベル キーワード、説明 46-10
時間帯 4-12	ログ メッセージの同期化 46-6
時刻	システム機能 TLV 25-2
NTP およびシステム クロックを参照	システム説明 TLV 25-2
システム	システム名
起動時の設定 3-29	DNS も参照
設定の確認 3-11	手動の設定 4-15
システム MTU	デフォルト設定 4-15
802.1Q トンネリング 23-5	システム名 TLV 25-2
最大許容システム 23-5	自動検出
システムアラーム	考慮事項 12-7
Supervisor 6-E 10-5	自動設定 3-2
Supervisor Engine II-Plus から V-10GE 10-5	自動ネゴシエーション機能
概要 10-4	強制 10/100 Mbps 6-15
システム イメージ	シャットダウン
指定 3-32	インターフェイス 6-32
プート フィールドの修正 3-29	ジャンボ フレーム
フラッシュ メモリからの起動 3-32	MTU サイズの 設定 6-25
システム クロック	MTU の概要 6-23
NTP も参照	VLAN インターフェイス 6-24
概要 4-2	イーサネット ポート 6-24
設定	サポートするポートおよびラインカード 6-22
時間帯 4-12	サポートの概要 6-23
手動での設定 4-11	重大度、システム メッセージに定義 46-9
夏時間 4-13	集約スイッチ、DHCP スヌーピングのイネーブル化
日時の表示 4-12	40-11
システム プロンプト、デフォルト設定 4-15	手動によるプリエンプション、REP、設定 18-13
システム メッセージ ロギング	冗長性
UNIX Syslog サーバ	NSF 対応サポート 9-2
サポートされるファシリティ 46-13	NSF 認識サポート 9-2
デーモンの設定 46-11	概要 8-2
ロギング ファシリティの設定 46-12	冗長コマンド 8-8
イネーブル化 46-5	設定 8-8
ויו איט דיין דיין דיין דיין דיין דיין דיין	注意事項および制約事項 8-6

SNMP による変更 8-12	候補の特性 12-7
同期化の概要 8-5	コミュニティ名 12-8
冗長性(NSF) 9-1	設定情報 12-9
設定	通信プロトコル 12-8
BGP 9-13	デバイスの追加 12-9
CEF 9-12	パスワード 12-8
EIGRP 9-18	ホスト名 12-8
IS-IS 9-15	スイッチのデフォルトへのリセット 3-34
OSPF 9-14	スイッチポート
ルーティング プロトコル 9-6	show interfaces 6-25, 6-26, 6-33, 6-34
冗長性 (RPR)	スイッチング、NetFlow
同期化 8-5	キャッシュ エントリのエクスポート 48-10
ルート プロセッサ冗長性 8-3	収集のイネーブル化 48-8
冗長性 (SSO)	スイッチド IP フローの設定 48-8
冗長コマンド 9-11	設定(例) 48-14
同期化 8-5	必要なハードウェアの確認 48-7
ルート プロセッサ冗長性 8-3	スーパーバイザ エンジン
診断	ROM モニタ 3-27
Supervisor Engine V-10GE \mathcal{O} POST 50-9	環境のモニタリング 10-2
オンライン 50-1	冗長へのアクセス 8-17
トラブルシューティング 50-2	冗長性 9-1
電源投入時自己診断テスト	スタートアップ コンフィギュレーション 3-27
概要 50-3	スタティック ルート 3-12
機能 50-4	スタンバイへのファイルのコピー 8-17
障害の原因 50-14	設定 3-9 3-13
侵入検知システム	設定の同期化 8-12
IDS を参照	デフォルト ゲートウェイ 3-11
信頼状態	デフォルト設定 3-2
設定 34-56	スケジューリング 34-15
信頼できる時刻源、説明 4-2	概要 34-6
	定義 34-5
*	スタティック アドレス
す ·	アドレスを参照
スイッチ ポート	スタティック ホストの IP ポート セキュリティ
アクセス ポートを参照	PVLAN ホスト ポート上 40-29
スイッチ /RADIUS サーバ通信	概要 40-25
設定 37-26	レイヤ 2 アクセス ポート上 40-26
スイッチ間リンク カプセル化方式	スタティック ルート
ISL カプセル化を参照	確認 3-13
スイッチド パケット	設定 3-12
ACL 42-32	スタブ ルーティング (EIGRP)
スイッチド ポート アナライザ	概要 27-15, 27-16
SPAN を参照	確認 27-20
スイッチのコミュニティ	制約事項 27-20
Network Assistant のアクセス モード 12-8	設定 27-16
クラスタからの変換 12-10	設定作業 27-20

利点 27-20	そ
スティッキ MAC アドレス	
設定 38-8	送信キュー
定義 38-5	QoS の送信キューを参照
スティッキ ラーニング	送信レート 34-60
アドレスの保存 38-6	即時脱退処理
イネーブル化 38-6	IGMP
コンフィギュレーション ファイル 38-6	即時脱退処理を参照
定義 38-6	イネーブル化 21-8
ディセーブル化 38-6	即時脱退、IGMP
ストーム制御	イネーブル化 22-10
概要 44-2	速度
ソフトウェアベース、実装 44-3	インターフェイスの設定 6-15
ハードウェアベース、実装 44-2	ソフトウェア
表示 44-10	アップグレード 8-15
ブロードキャストのイネーブル化 44-4	ソフトウェア QoS、Supervisor Engine 6-E で 34-98
マルチキャストのイネーブル化 44-6	ソフトウェア コンフィギュレーション レジスタ
ストーム制御の表示 44-10	3-28
ストラタム、NTP 4-2	ソフトウェア スイッチング
スロット番号、説明 6-2	インターフェイス 28-6
	使用する主なデータ構造 31-8
	説明 28-5
t	
	+ -
制御パケットのキャプチャ	た
モードの選択 42-13	ダイナミック ポート VLAN メンバシップ
制御パケットのキャプチャのモード、選択 42-13	再確認 13-24, 13-25
セカンダリ VLAN 36-3	トラブルシューティング 13-27
プライマリとの関連付け 36-14	ホスト上の制限 13-27
ルーティングの許可 36-21	例 13-27
セカンダリ エッジ ポート、REP 18-4	タイプ オブ サービス
セカンダリ ルート スイッチ 17-13	ToS を参照
セキュリティ	タイマー
IP	・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
DoS 攻擊 29-10	タグ付きパケット
TCP SYN フラッディング攻撃 29-10	802.1Q 23-3
設定 39-1	レイヤ 2 プロトコル 23-8
設定可能な Leave タイマー、IGMP 21-4	単一方向イーサネット
設定時の注意事項	イネーブル化 30-2
REP 18-7	概要 30-2
SNMP 47-6	127.12.
設定例	Mark Andrews and Adult
SNMP 47-16	単一方向リンク検出 26-1

ち	Catalyst 4500 シリーズ 10-6
	Catalyst 4948 シリーズ 10-21
注意	概要 10-2
ユニキャスト RPF	冗長性 10-6
オプションの BGP 属性 29-5	冗長モードの設定 10-11
	複合モードの設定 10-12
τ	電源管理 TLV 25-3, 25-7
	電源管理モード
ディセーブル ステート	選択 10-8
RSTP の比較 (表) 17-27	電源管理モードの選択 10-8
ディセーブル化	電源装置
ブロードキャスト ストーム制御 44-8	Catalyst 4500 スイッチで利用可能な電力 10-13
データベース エージェント	可变 10-7, 10-21
DHCP スヌーピングのイネーブル化 40-13	固定 10-7
設定例 40-14	電源投入時自己診断テスト診断 50-3,50-14
デバイス検出プロトコル 25-2	転送情報ベース
デバッグ コマンド、ROM モニタ 53-7	FIB を参照
デフォルト ゲートウェイ	転送遅延時間(STP)
設定 3-11	設定 17-21
設定の確認 3-12	
デフォルト設定	T.
802.1X 37-23	ح
Auto-QoS 34-19	統計情報
DNS 4-16	802.1X の表示 37-51
IGMP スヌーピング 22-6, 22-7	LLDP 25-8
IGMP フィルタリング 21-20	LLDP-MED 25-8
LLDP 25-4	NetFlow 課金 48-10
MAC アドレス テーブル 4-21	PIM の表示 31-22
Multi-VRF CE 33-4	SNMP 出入力 47-18
NTP 4-4	トークンリング
REP 18-7	サポートされていないメディア 13-6, 13-11
RMON 49-4	独立 VLAN 36-3, 36-4, 36-5
SNMP 47-6	独立ポート 36-4
SPAN ∠ RSPAN 45-7	特権 EXEC モード 2-6
TACACS+ 3-19	ドメイン名
インターフェイスのリセット 6-35	DNS 4-16
システム メッセージ ロギング 46-4	トラップ
システム名とプロンプト 4-15	MAC アドレス通知の設定 4-22
バナー 4-18	MAC 移動通知の設定 4-25
プライベート VLAN 36-11	MAC しきい値通知の設定 4-26
レイヤ 2 プロトコル トンネリング 23-11	イネーブル化 4-22, 4-25, 4-26, 47-11
デフォルト設定、erase コマンド 3-34	概要 47-2, 47-5
デュプレックス モード	通知の種類 47-11
インターフェイスの設定 6-15	定義 47-4
電源管理	マネージャの設定 47-11
Catalyst 4500 スイッチの電源装置 10-13	TO TOPHANE TO TE

トラフィック	名前付き MAC 拡張 ACL の設定 42-20
フラッディングのブロック 43-2	名前付き集約ポリサー、作成 34-33
トラフィック シェーピング 34-17	
トラフィック マーキング手順のフローチャート 34-80	IC
トラフィックの制御 ACL の使用(図) 42-4 VLAN マップの使用(図) 42-5	二重タグ付きパケット 802.1Q トンネリング 23-2
トラブルシューティング Cisco Works を使用 47-5 traceroute 7-10 システム メッセージ ロギングを使用 46-2 トランク 802.1Q の制限事項 15-6 DTP をサポートしない装置のイネーブル化 15-5 アクセス VLAN の設定 15-8	レイヤ 2 プロトコル トンネリング 23-10 入力パケット、SPAN 拡張機能 45-14 認可 TACACS+ 3-17, 3-22 認証 NTP アソシエーション 4-4 TACACS+ キー 3-19 定義 3-17 ログイン 3-20
インターフェイスのデフォルト設定 15-7 概要 15-3 カプセル化 15-4 許容される VLAN の設定 15-8 異なる VTP ドメイン 15-4 設定 15-7 ネイティブ VLAN の指定 15-8	ポートベースの認証も参照 認証サーバ RADIUS サーバ 37-3 定義 37-3 認証失敗 VLAN 割り当て 802.1X による設定 37-41
トランク ポート	認証、認可、アカウンティング 39-1
PVLAN の設定 36-17 36-19	
ポート セキュリティを設定 38-19	ね
トランスレーショナル ブリッジ番号(デフォルト)	10.
13-5	ネイティブ VLAN
トンネリング	802.1Q トンネリング 23-4
定義 23-1	指定 15-8
トンネル ポート	ネイバー オフセット番号、REP 18-4
802.1Q、設定 23-6	ネットワーク トラフィックのマーキング 34-77
説明 23-2	ネットワーク トラフィック、マーキング 34-77
他の機能との互換性 23-5	ネットワーク ポリシー TLV 25-3, 25-7
	ネットワーク管理
な	RMON 49-1 SNMP 47-1
夏時間 4-13	設定 24-1
名前付き IPv6 ACL の設定 42-22	ネットワーク耐障害性 1-3,17-25
名前付き IPv6 ACL、設定 ACL	
名前付き IPv6 ACL の設定 42-22	は
名前付き MAC 拡張 ACL	バースト サイズ 34-34
ACL	バースト リイス 34-34 バースト レート 34-60
 名前付き MAC 拡張の設定 42-20	// VI. N I. 24-00

バーチャル プライベート ネットワーク	131
VPN を参照	
ハードウェア スイッチング 28-5	フィルタリング
ハードウェアおよびソフトウェア ACL のサポート	IP 以外のトラフィック 42-20
42-6	VLAN 42-24
パケット	ブート コマンド 53-3
ソフトウェア処理	ブート フィールド
QoS 34-17	コンフィギュレーション レジスタ、ブート
変更 34-17	フィールドを参照
パケット タイプ フィルタリング	ブートストラップ プログラム
SPAN 拡張機能 45-18	ROM モニタを参照
概要 45-18	不揮発性ランダム アクセス メモリ
パケットのブロック 43-2	NVRAM を参照
パスワード	複数ドメイン認証
暗号化 3-23	MDA を参照
イネーブル シークレット パスワードの設定	複数の VRF
3-14	Multi-VRF CE を参照
イネーブル パスワードの設定 3-14	複数の転送パス 1-3, 17-25
イネーブル パスワードを忘れた場合の回復方法	複製
3-26	説明 31-9
回線パスワードの設定 3-15	物理レイヤ 3 インターフェイス、設定 27-14
クラスタ内 12-8	プライオリティ
パスワードに関する注意	着信フレームの CoS の変更 35-7
暗号化 3-24	プライオリティ キュー、Supervisor Engine 6-E での
バナー	QoS 34-89
設定	プライベート VLAN
MoTD ログイン 4-18	DHCP スヌーピングのイネーブル化 40-13
ログイン 4-19	SVI 36-9
デフォルト設定 4-18	コミュニティ VLAN 36-3, 36-4
表示される場合 4-18	コミュニティ ポート 36-4
パワー	混合モード ポート 36-5
インライン 35-7	サブドメイン 36-3
	セカンダリ VLAN 36-3
₩.	端末アクセス 36-4
· ·	デフォルト設定 36-11
非 IPv4 トラフィックの一致 CoS	独立 VLAN 36-3, 36-4, 36-5
設定 34-38	独立ポート 36-4
非 RPF トラフィック	トラフィック 36-8
冗長構成(図) 31-11	複数のスイッチ 36-5
説明 31-10	プライマリ VLAN 36-3, 36-5
光デジタル モニタ トランシーバのサポート 6-14	ポート
ヒストリ	コミュニティ 36-4
CLI 2-4	混合モード 36-5
非対称リンクと 802.1Q トンネリング 23-4	独立 36-4
標準範囲 VLAN	ポート セキュリティを設定 38-16
VLANを参照	利点 36-3
, Dan C 2 /m	プライマリ VLAN 36-3, 36-5

PVLAN としての設定 36-13 13-27 セカンダリ VLAN との関連付け 36-14 転送の再開 43-3 プライマリ エッジ ポート、REP 18-4 ブロック 43-2 フラグ 31-12 ポートACL 音声 VLAN フラッシュ メモリ 42-5 システム ソフトウェア イメージのロード 制限 3-32 42-5 セキュリティ上の注意 3-32 定義 42-3 ルータの起動元としての設定 3-32 ポート VLAN ID TLV 25-2 フラッディングしたトラフィックをブロック ポート コスト (STP) 43-2 プリエンプト遅延時間、REP 設定 17-17 ブリッジID ポート ステート STP、ブリッジ ID を参照 説明 17-6 ブリッジ プライオリティ(STP) 17-19 ポート セキュリティ ブリッジ プロトコル データ ユニット 802.1X 認証を使用 38-36 BPDU を参照 802.1X を使用 37-15 プルーニング、VTP DHCP と IP ソース ガードを使用 38-35 VTP プルーニングを参照 OoS 信頼境界 34-28 フロー制御の設定 RADIUS アカウンティング 6-18 37-16 フロー制御、設定 6-18 アクセス ポート上 38-8, 38-25 フローチャート、トラフィック マーキング手順 違反 38-6 34-80 エージング 38-5 ブロードキャスト ストーム制御 音声ポート上 38-25 イネーブル化 44-4 スティッキ ラーニング 38-6 ディセーブル化 44-8 設定 38-8 ブロッキング ステート(STP) 他の機能 38-38 RSTP の比較(表) 17-27 注意事項および制約事項 38-38 プロトコル タイマー 17-5 トランク ポート上 38-19 注意事項および制約事項 38-16, 38-20, 38-23, 38-36 ポート モードの変更 38-24 表示 38-31 別の VLAN にあるサーバへのアクセスの拒否 42-30 プライベート VLAN 上 38-16 混合モード ベビー ジャイアント 38-18 トポロジ 38-16, 38-20, 38-36 対話 6-25 ホスト 38-16 ベビー ジャイアント機能との対話 6-25 レイヤ 2 EtherChannel 38-37 ポート プライオリティ ΙŦ MSTI の設定 17-36 STP の設定 17-15 ポイントツーポイント ポート ベースの OoS 機能 802.1X 認証(図) 37-3, 37-17 QoS を参照 ポート ポート上の Auto-MDIX REP 18-6 概要 6-27 インターフェイスも参照 設定 6-28 ステータスの確認 7-3 設定の表示 6-28 ダイナミック VLAN メンバシップ ポート説明 TLV 25-2 再確認 13-24, 13-25

ポートチャネル インターフェイス ポート セキュリティ 複数ホスト モード EtherChannel も参照 37-7 概要 ポート セキュリティの使用 20-2 37-15 ホストモード 37-7 作成 20-7ポートの信頼状態 ホスト ダイナミック ポート上の制限 信頼状態を参照 13-27 ポートベースの認証 ホストを静的に設定 21-11 802.1X アカウンティングの設定 37-32 ホスト ポート MAC 認証バイパスによる 37-10 種類 36-4 MAC 認証バイパスを使用した設定 37-36 ホットスワップ VLAN 割り当て 37-7 OIR を参照 WoL を使用した設定 ホップ カウント 37-40 イネーブル化 37-24 MST ブリッジの設定 17-31 ポリサー 音声 VLAN ポートを使用した 802.1X 37-19 開始とメッセージ交換 37-4 種類 34-10 カプセル化 37-3 説明 34-6 許可ステートの制御 37-5 ポリシー クライアント、定義 37-3 QoS ポリシーを参照 クリティカル認証による 37-12 ポリシー アソシエーション、Supervisor Engine 6-E で の QoS 34-97 クリティカル認証による設定 37-37 ポリシー マップ ゲスト VLAN に対する設定 37-33, 37-43 インターフェイスへの付加 34-43 ゲスト VLAN による 設定 34-38 ゲスト VLAN の設定 37-26 ポリシー マップ マーキング アクション、設定 再送信回数の設定 37-48 34-82 再送信時間の設定 37-47 ポリシング サポートされないポート 37-5 OoS ポリシングを参照 手動によるクライアントの再認証の設定 実装方法 34-77 ポリシング済み DSCP マップ 34-62 スイッチ/RADIUS サーバ通信の設定 37-26 設定 マルチドメイン認証 37-28 恚 設定時の注意事項 37-23 説明 37-2 マーキング 装置の役割 37-3 ハードウェア機能 34-82 待機時間の変更 37-46 マーキングのサポート、マルチ属性 34-81 定期的再認証のイネーブル化 37-44 マクロ デフォルト設定 37-23 SmartPort マクロを参照 デフォルト値へのリセット 37-50 マッピング 統計情報の表示 37-51 DSCP 値から送信キュー 34-59 トポロジ、サポート対象 37-21 DSCP マークダウン値 34-26 認証失敗 VLAN 割り当てを使用した設定 マッピング テーブル 37-41 DSCP の設定 34-61 複数ドメイン認証 37-20 説明 34-15 複数ホスト モード、説明 37-7 マルチキャスト 複数ホストのイネーブル化 37-45 IP マルチキャストを参照 方式リスト 37-24

マルチキャスト クライアント エージングの堅牢性 モニタリング 22 - 3802.1Q トンネリング 23-14 マルチキャスト グループ REP 18-15 スタティックに加入 22-8 スイッチのトラフィック フロー 49-2 マルチキャスト ストーム制御 トンネリング 23-14 レイヤ 2 プロトコル トンネリング 23-14 イネーブル化 44-6 WS-X4014 での抑制 44-7 ゅ WS-X4016 での抑制 44-7 WS-X4515、WS-X4014、およびWS-X4013+スー ユーザ EXEC モード 2-6 パーバイザ エンジン 44-7 ユーザ セッション WS-X4516 スーパーバイザ エンジン 44-7 切断 7-8 スーパーバイザ 6-E での抑制 モニタリング 7-8 ディセーブル化 44-9 ユニキャスト マルチキャスト ストーム制御のディセーブル化 IP ユニキャストを参照 44-9 ユニキャスト MAC アドレス フィルタリング マルチキャスト パケット および CPU パケット 4-29 ブロック 43-2 およびスタティック アドレスの追加 4-29 マルチキャスト ルータ およびブロードキャスト MAC アドレス 4-29 フラッディングの抑制 21-11 およびマルチキャスト アドレス 4-29 ルーティング テーブルの表示 31-18 およびルータ MAC アドレス 4-29 マルチキャスト ルータ インターフェイス 22-13 設定時の注意事項 4-29 マルチキャスト ルータ ポート、追加 22-9 説明 4-29 マルチキャスト ルータ検出 22-4 ユニキャスト MAC アドレス フィルタリングの設定 マルチドメイン認証 42-20 設定 37-28 ユニキャスト MAC アドレス フィルタリング、設定 ホスト モードの概要 37-7 ACL ユニキャスト MAC アドレス フィルタリング の設定 42-20 め ユニキャスト RPF (ユニキャスト Reverse Path メッセージ、バナーを介したユーザ 4-18 Forwarding) メトロ タグ 23-2 BGP 属性 メンバ 注意 29-5 自動検出 12-7 **CEF** メンバ スイッチ テーブル 29-8 管理 要件 12-14 29-2 メンバ スイッチ、クラスタ FIB 29-2 定義 12-12 エンタープライズ ネットワーク(図) 29-6 要件 12-13 確認 29-12 失敗 29-4 送信元アドレス も パケット、ドロップ 29-4 29-4 実装 モジュール 集約ルータ(図) 29-8 ステータスの確認 7-2 制約事項 電源切断 10-20 基本 29-9 モジュール、消費される PoE の表示 11-11

ルーティングの非対称性 29-8	ı)
ルーティングの 非対称性(図) 29-9	
セキュリティ ポリシー	リスニング ステート (STP)
攻撃、軽減 29-5	RSTP の比較 (表) 17-27
適用 29-5	リモート ネットワーク モニタリング
展開 29-5	RMON を参照
トンネリング 29-5	略語リスト A-1
設定 29-11	履歴テーブル、Syslog メッセージのレベルと数 46-10
BOOTP 29-9	リンクおよびトランク ステータス イベント
DHCP 29-9	インターフェイスの設定 6-33
エンタープライズ ネットワーク(図) 29-6	リンク完全性、REP による確認 18-3
確認 29-12	隣接関係テーブル
作業 29-11	説明 28-2
集約ルータ(図) 29-8	統計情報の表示 28-10
前提条件 29-10	
ルーティング テーブルの要件 29-8	7
(例) 29-15	న
説明 29-2	ルータ ACL
前提条件 29-10	VLAN マップとの併用 42-32
送信元アドレス、確認 29-3	説明 42-3
失敗 29-4	ルータ ACL、PACL の VLAN マップとの併用 42-38
(図) 29-3, 29-4	ルーテッド パケット
ディセーブル化 29-13	ACL 42-33
適用 29-5	ルートガード
展開 29-5	MST 17-26
トラフィック フィルタリング 29-6	イネーブル化 19-3
トンネリング 29-5	概要 19-2
パケット、ドロップ(図) 29-4	ルート ターゲット
メンテナンス 29-13	VPN 33-3
モニタリング 29-13	ルート ブリッジ
ルーティング テーブルの要件 29-8	MST での選択 17-25
ユニキャスト トラフィック	設定 17-11
ブロック 43-2	ルート マップ
ユニキャスト フラッディング ブロック	PBR 32-2
設定 43-1	定義 32-4
	ループ ガード
L	MST 17-26
\$	概要 19-4
予約範囲 VLAN	設定 19-6
VLAN を参照	
, 12/11 C 2/m	
	ħ
5	レイヤ 2 traceroute
ラベル、定義 34-4	1 ポートに複数のデバイス 7-12
	ARP 7-11

CDP 7-11 概要 27-2 IP アドレスおよびサブネット 7-11 物理 27-3 MAC アドレスおよび VLAN 論理 27-2 7-11 使用上の注意事項 7-11 設定時の注意事項 27-6 レイヤ3インターフェイス カウンタ、概要 ホスト間パス 7-11 27-4 マルチキャスト トラフィック レイヤ3インターフェイス カウンタ、設定 27-12 7-11 ユニキャスト トラフィック レイヤ3インターフェイスへの IPv6 ACL の適用 1-24, 7-11 42-23 レイヤ 2 アクセス ポート 15-10 レイヤ3インターフェイス、IPv6 ACL の適用 42-23 レイヤ2インターフェイス レイヤ3パケット PVLAN 混合モード ポートとしての設定 36-15 分類方式 34-2 PVLAN トランク ポートとしての設定 36-17 レイヤ4ポート演算 PVLAN ホスト ポートとしての設定 36-16 制約事項 42-16 show interfaces コマンド 設定時の注意事項 42-17 VLAN の割り当て 13-8 レポート抑制、IGMP 設定 15-7 ディセーブル化 22-12 設定のディセーブル化 15-11 デフォルト 15-6 モード 15-4 3 レイヤ2インターフェイス上での VLAN ベース OoS、 設定 34-55 ロード バランシング レイヤ2インターフェイス上でのアクセス グループ CEF の設定 28-7 モードの設定 42-36 EtherChannel の設定 20-14 レイヤ2インターフェイスのタイプ 宛先別 28-7 設定 36-22 概要 20-5, 28-6 リセット 36-22 ログ メッセージのシーケンス番号 46-8 レイヤ2インターフェイス、アクセス グループ モー ログ メッセージのタイムスタンプ 46-8 ドの設定 42-36 ログイン タイマー レイヤ2スイッチング 变更 7-7 概要 15-2 ログイン バナー 4-18 レイヤ2制御パケット OoS ログイン認証 概要 34-64 TACACS+ 3-20 機能の相互作用 34-69 ロケーション TLV 25-7 使用上の注意事項 34-68 論理レイヤ3インターフェイス レイヤ2トランク 設定 27-7 概要 15-3 設定 15-7 レイヤ2フレーム CoS による分類 34-2 レイヤ 2 プロトコル トンネリング 注意事項 23-11 デフォルト設定 23-11 レイヤ2プロトコルパケットのシャットダウンしきい レイヤ2プロトコルパケットのドロップしきい値 23-11 レイヤ3インターフェイス

27-9

インターフェイスとしての VLAN