Cisco IOS ソフトウェア コンフィギュレーション ガイド

Cisco IOS Release 15.1SY

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

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

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system.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。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、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、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned 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. (1110R)

Supervisor Engine 2T ソフトウェア コンフィギュレーション ガイド リリース 15.1SY
© 2013 年 5 月 20 日 Cisco Systems, Inc. All rights reserved.

CONTENTS

はじめに

ここでは、『*Supervisor Engine 2T ソフトウェア コンフィギュレーション ガイド リリース 15.1SY*』の対象読者および手順や情報を記述するための表記法について説明します。

対象読者

このマニュアルは、Cisco IOS Release 15.1SY でサポートされるスイッチの設定およびメンテナンスを担当する、経験豊富なネットワーク管理者を対象としています。

関連資料

次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

管理情報ベースについては、次の URL を参照してください。

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

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
太字	コマンド、コマンド オプションおよびキーワードは**太字**で示しています。
イタリック体	ユーザが値を指定する引数は、*イタリック体*で表記されています。
[ ]	角カッコの中の要素は、省略可能です。
{ x | y | z }	必ずどれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。

表記法	説明
screen フォント	システムが表示する端末セッションおよび情報は、screen フォントで示しています。
太字の screen フォント	ユーザが入力しなければならない情報は、**太字の screen** フォントで示しています。
イタリック体の screen フォント	ユーザが値を指定する引数は、*イタリック体の screen* フォントで示しています。
——→	このポインタは、例の中の重要な行を強調しています。
^	^ 記号は、Ctrl キーを表します。たとえば、画面に表示される ^D というキーの組み合わせは、Ctrl キーを押しながら D キーを押すことを意味します。
< >	パスワードのように出力されない文字は、山カッコ（<>）で囲んで示しています。

（注）は、次のように表しています。

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

注意は、次のように表しています。

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

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

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

PART 1

製品概要

製品概要

（注）

- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。
- サポートされるシャーシ、モジュール、およびソフトウェア機能の詳細については、『*Release Notes for Cisco IOS Release 15.1SY*』を参照してください。

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/15.1SY/release_notes.html

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

Supervisor Engine 2T-10GE のフラッシュ メモリ デバイス

- **disk0:**（アクティブ）および **slavedisk0:**（スタンバイ）：
  - 外部 CompactFlash Type II スロット
  - 米国シスコで販売されている CompactFlash Type II フラッシュ PC カードをサポート
- **bootdisk:**（アクティブ）および **slavebootdisk:**（スタンバイ）：1 GB 内部フラッシュ メモリ

Supervisor Engine 2T-10GE ポート

- コンソール ポート：
  - RJ-45 コネクタを備えた EIA/TIA-232（RS-232）ポート
  - USB ポート

  デフォルト（コンソール 0 インターフェイスに **no media-type rj45** を設定）では、いずれのコネクタも使用でき、アクティブな USB 接続が検出されると、RJ-45 コネクタが非アクティブになります。コンソール 0 インターフェイスに **no media-type rj45** コマンドが設定されている場合、RJ-45 コネクタは、アクティブな USB 接続がない場合にのみ使用できます。コンソール 0 インターフェイスに **media-type rj45** コマンドが設定されている場合は、RJ-45 コネクタのみを使用できます。USB ドライバについては、次の資料を参照してください。

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Module_Installation/Sup_Eng_Guide/03instal.html#USB_Console_Port_Driver_Installation

  （注）　リリース 15.1(1) SY には、デフォルトでイネーブルになっている、コンソール切断機能があります。

- ポート 1、2、および 3：ギガビット イーサネット SFP（ファイバまたは 10/100/1000 Mbps RJ-45）
- ポート 4 およびポート 5：10 ギガビット イーサネット× 2

（注）
- **platform qos 10g-only** グローバル コンフィギュレーション コマンドで 1 ギガビット イーサネット ポートをディセーブルにした場合を除き、1 ギガビット イーサネット ポートと 10 ギガビット イーサネット ポートの QoS ポート アーキテクチャは同じです（2q4t/1p3q4t）。1 ギガビット イーサネット ポートをディセーブルにした場合、10 ギガビット イーサネット ポートの QoS ポート アーキテクチャは 8q4t/1p7q4t です。
- 10/100/1000 Mbps RJ-45 ポートについては、『*Supervisor Engine 2T-10GE Connectivity Management Processor Configuration Guide*』を参照してください。

ポート設定の詳細については、「オプションのインターフェイス機能の設定方法」（P.10-3）を参照してください。

Supervisor Engine 2T-10GE 接続管理プロセッサ（CMP）

次の資料を参照してください。

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/cmp_configuration/guide/sup2T_10GEcmp.html

システムのハードウェア容量の判別

show platform hardware capacity コマンドを入力することで、システムのハードウェア容量を判別できます。このコマンドは、ハードウェア リソースの現在のシステム利用率を表示し、現在使用可能なハードウェア容量を一覧表示します。この内容は次のとおりです。

- ハードウェア転送テーブルの使用率
- スイッチ ファブリックの使用率
- CPU（1 つまたは複数）の使用率
- メモリ デバイス（フラッシュ、DRAM、NVRAM）の使用率

次に、ルート プロセッサ、スイッチ プロセッサ、およびスイッチング モジュールに対する CPU 容量とその利用率情報を表示する例を示します。

```
Router# show platform hardware capacity cpu
CPU Resources
  CPU utilization: Module             5 seconds       1 minute       5 minutes
                   3                   0% /  0%             1%              1%
                   7  RP               2% /  0%             1%              1%
  Processor memory: Module   Bytes:       Total           Used           %Used
                    3                 1612928756      164136704             10%
                    7  RP             1569347520      242739196             15%
  I/O memory: Module         Bytes:       Total           Used           %Used
              3                         268435456       21163672              8%
              7  RP                     268435456      110324056             41%

Router#
```

次に、ルート プロセッサ、スイッチ プロセッサ、および DFC に対する EOBC 関連の統計情報を表示する例を示します。

```
Router# show platform hardware capacity eobc
EOBC Resources
  Module                      Packets/sec     Total packets     Dropped packets
  3          Rx:                       25             57626                   0
             Tx:                       19             45490                   0
  7  RP      Rx:              36456689392             54747                   0
             Tx:                       25             66898                   0
```

次に、現在、およびピーク時のスイッチング使用率を表示する例を示します。

```
Router# show platform hardware capacity fabric
  Bus utilization: current is 100%, peak was 100% at 12:34 12mar45
  Fabric utilization:      ingress                      egress
      Module channel speed current peak                current peak
       1      0        20G   100%  100% 12:34 12mar45  100%    100% 12:34 12mar45
       1      1        20G   12%    80% 12:34 12mar45   12%     80% 12:34 12mar45
       4      0        20G   12%    80% 12:34 12mar45   12%     80% 12:34 12mar45
      13      0         8G   12%    80% 12:34 12mar45   12%     80% 12:34 12mar45
```

次に、システム内のフラッシュおよび NVRAM リソースに対する合計容量、使用バイト数、および割合（%）を表示する例を示します。

```
Router# show platform hardware capacity flash
Flash/NVRAM Resources
  Usage: Module Device              Bytes:      Total          Used     %Used
         3      dfc#3-bootflash:              15990784             0        0%
         7  RP  nvram:                         2552192         40640        2%
         7  RP  const_nvram:                   1048556           676        1%
         7  RP  bootdisk:                   1024196608      99713024       10%
         7  RP  disk0:                      1024655360      77824000        8%
```

次に、システム内の PFC および DFC の容量および使用率を表示する例を示します。

```
Router# show platform hardware capacity forwarding
L2 Forwarding Resources
           MAC Table usage:   Module  Collisions  Total       Used     %Used
                              6                0  65536         11        1%
             VPN CAM usage:                        Total       Used     %Used
                                                     512          0        0%
L3 Forwarding Resources
             FIB TCAM usage:                       Total       Used     %Used
                  72 bits (IPv4, MPLS, EoM)       196608         36        1%
                 144 bits (IP mcast, IPv6)         32768          7        1%

                     detail:      Protocol                     Used     %Used
                                  IPv4                           36        1%
                                  MPLS                            0        0%
                                  EoM                             0        0%

                                  IPv6                            4        1%
                                  IPv4 mcast                      3        1%
                                  IPv6 mcast                      0        0%

            Adjacency usage:                       Total       Used     %Used
                                                  1048576         175        1%

     Forwarding engine load:
                     Module       pps   peak-pps  peak-time
                     6              8       1972  02:02:17 UTC Thu Apr 21 2005

Netflow Resources
          TCAM utilization:       Module       Created      Failed     %Used
                                  6                  1           0        0%
          ICAM utilization:       Module       Created      Failed     %Used
                                  6                  0           0        0%

                Flowmasks:   Mask#   Type        Features
                       IPv4:     0   reserved    none
                       IPv4:     1   Intf FulNAT_INGRESS NAT_EGRESS FM_GUARDIAN
                       IPv4:     2   unused      none
                       IPv4:     3   reserved    none

                       IPv6:     0   reserved    none
                       IPv6:     1   unused      none
                       IPv6:     2   unused      none
                       IPv6:     3   reserved    none

CPU Rate Limiters Resources
             Rate limiters:       Total         Used      Reserved     %Used
                    Layer 3           9            4             1       44%
                    Layer 2           4            2             2       50%

ACL/QoS TCAM Resources
```

```
  Key: ACLent - ACL TCAM entries, ACLmsk - ACL TCAM masks, AND - ANDOR,
       QoSent - QoS TCAM entries, QOSmsk - QoS TCAM masks, OR - ORAND,
       Lbl-in - ingress label, Lbl-eg - egress label, LOUsrc - LOU source,
       LOUdst - LOU destination, ADJ - ACL adjacency

  Module ACLent ACLmsk QoSent QoSmsk Lbl-in Lbl-eg LOUsrc LOUdst  AND OR  ADJ
  6          1%     1%     1%     1%     1%     1%     0%     0%   0% 0%   1%

Router#
```

次に、インターフェイス リソースを表示する例を示します。

```
Router# show platform hardware capacity interface
  Interface drops:
    Module    Total drops:    Tx            Rx      Highest drop port: Tx  Rx
    9                          0             2                           0  48

  Interface buffer sizes:
    Module                              Bytes:     Tx buffer           Rx buffer
         1                                            12345               12345
         5                                            12345               12345
Router#
```

次に、SPAN 情報を表示する例を示します。

```
Router# show platform hardware capacity monitor
  Source sessions: 2 maximum, 0 used
    Type                                    Used
    Local                                      0
    RSPAN source                               0
    ERSPAN source                              0
    Service module                             0
  Destination sessions: 64 maximum, 0 used
    Type                                    Used
    RSPAN destination                          0
    ERSPAN destination (max  24)               0
Router#
```

次に、レイヤ 3 マルチキャスト機能の各リソースの容量および使用率を表示する例を示します。

```
Router# show platform hardware capacity multicast
L3 Multicast Resources
  IPv4 replication mode: ingress
  IPv6 replication mode: ingress
  Bi-directional PIM Designated Forwarder Table usage: 4 total, 0 (0%) used
  Replication capability: Module                                IPv4     IPv6
                          5                                   egress   egress
                          9                                  ingress  ingress
  MET table Entries: Module                                Total    Used    %Used
                     5                                     65526       6       0%
Router#
```

次に、システム電源の容量および使用率情報を表示する例を示します。

```
Router# show platform hardware capacity power
Power Resources
  Power supply redundancy mode: administratively redundant
                                operationally non-redundant (single power supply)
  System power: 3795W, 0W (0%) inline, 865W (23%) total allocated
  Powered devices: 0 total, 0 Class3, 0 Class2, 0 Class1, 0 Class0, 0 Cisco
Router#
```

次に、各 PFC および DFC に対する QoS ポリサー リソースの容量および利用率を表示する例を示します。

```
Router# show platform hardware capacity qos
QoS Policer Resources
  Aggregate policers: Module                      Total         Used     %Used
                      6                           16384           16        1%
  Microflow policer configurations: Module        Total         Used     %Used
                                    6               128            1        1%
Netflow policer configurations: Module          Total         Used     %Used
                                    6               384            0        0%
  Aggregate policer configs:    Module            Total         Used     %Used
                                6                  1024            8        1%
  Distributed policers: Total          Used     %Used
                          4096            1         1%
  QoS Tcam Entries: Module                        Total         Used     %Used
                    1                             16384         1171        7%
                    2                             16384         1171        7%
                    3                             16384         1171        7%

Router#
```

次に、重要なシステム リソースについての情報を表示する例を示します。

```
Router# show platform hardware capacity system
System Resources
PFC operating mode: PFC4
  Supervisor redundancy mode: administratively sso, operationally sso
  Switching resources: Module   Part number              Series      CEF mode
                       6        VS-SUP2T-10G          supervisor           CEF
Router#
```

次に、VLAN 情報を表示する例を示します。

```
Router# show platform hardware capacity vlan
  VLANs: 4094 total, 10 VTP, 0 extended, 0 internal, 4084 free
Router#
```

モジュール ステータスのモニタリング

スーパーバイザ エンジンは、スイッチ通信プロトコル（SCP）メッセージを使用して、インストールされたモジュールをポーリングして、モジュールのステータスをモニタします。

SCP では、各モジュールにメッセージが 2 秒ごとに送信されます。3 個のメッセージ（6 秒）の後のモジュールの無応答は障害として分類されます。CPU_MONITOR システム メッセージは 30 秒ごとに送信されます。25 回の順次障害（150 秒）の後、スーパーバイザ エンジンはモジュールの電源を再投入し、CPU_MONITOR TIMED_OUT システム メッセージおよび OIR PWRCYCLE システム メッセージを送信します。

モジュールまたはポートの目視確認のイネーブル化

モジュールを視覚的に識別しやすくするために、対象のモジュールで青い ID LED（青色のビーコン LED とも呼ぶ）が点滅するように設定できます。

- Supervisor Engine 2T-10GE
- WS-X6908-10GE の 10 ギガビット イーサネット スイッチング モジュール

モジュールで点滅をイネーブルにするコマンドを次に示します。

```
Router(config)# hw-module slot slot_number led beacon
```

モジュールで点滅をディセーブルにするコマンドを次に示します。

```
Router(config)# no hw-module slot slot_number led beacon
```

ポートを視覚的に識別しやすいさせるために、対象のモジュールでリンク LED が点滅するように設定できます。

- Supervisor Engine 2T-10GE
- WS-X6908-10GE の 10 ギガビット イーサネット スイッチング モジュール

ポートで点滅をイネーブルにするコマンドを次に示します。

```
Router(config-if)# led beacon
```

点滅をディセーブルにするコマンドを次に示します。

```
Router(config-if)# no led beacon
```

ユーザ インターフェイス

- CLI：第 2 章「コマンドライン インターフェイス」を参照してください。
- SNMP：次の URL で『*SNMP Configuration Guide*』（Cisco IOS Release 15.1SY）を参照してください。

  http://www.cisco.com/en/US/docs/ios-xml/ios/snmp/configuration/15sy/snmp-15-sy-book.html
- Cisco IOS Web ブラウザ インターフェイス：次の URL で『*HTTP Services Configuration Guide*』（Cisco IOS Release 15.1SY）を参照してください。

  http://www.cisco.com/en/US/docs/ios-xml/ios/https/configuration/15-sy/https-15-sy-book.html

PFC および DFC がハードウェアでサポートするソフトウェア機能

- レイヤ 3 ポートおよび VLAN インターフェイスのアクセス コントロール リスト（ACL）
  - 入 / 出力標準 ACL および拡張 ACL の許可アクションおよび拒否アクション

    （注）　ACL ロギングを必要とするフローはルート プロセッサ（RP）のソフトウェアで処理されます。
  - マルチプロトコル ラベル スイッチング（MPLS）インターフェイス以外でのリフレクシブ ACL フロー（セッション内の最初のパケットが RP のソフトウェアで処理されたあとのフロー）
  - ダイナミック ACL フロー

    （注）　アイドル タイムアウトは RP のソフトウェアで処理されます。

ACL の PFC および DFC サポートの詳細については、第 69 章「Cisco IOS ACL のサポート」を参照してください。

- ハードウェアの双方向 Protocol Independent Multicast（PIM）：「IPv4 双方向 PIM」（P.43-9）を参照してください。
- ダイナミック アドレス解決プロトコル（ARP）インスペクション（DAI）：第 80 章「ダイナミック ARP インスペクション（DAI）」を参照
- 複数パスによるユニキャスト リバース パス転送（RPF）チェック：ユニキャスト RPF チェックを設定するには、「ユニキャスト リバース パス転送（uRPF）チェック」（P.76-7）を参照してください。
- MPLS インターフェイスを除く、IPv4 ユニキャストおよびマルチキャスト トラフィックのネットワーク アドレス変換（NAT）

  ハードウェアが処理する NAT については、次の点に注意してください。

  - PFC および DFC は、マルチキャスト トラフィックの NAT をサポートしません。（CSCtd18777）。
  - PFC および DFC は、長さを指定するルート マップが設定された NAT をサポートしません。
  - インターフェイスで NAT および NDE を設定する場合、RP は、ソフトウェアの断片化されたパケットのすべてのトラフィックを処理します。
  - DoS 攻撃または設定ミスが原因で莫大な量の NAT トラフィックが RP に送信されないようにするには、**platform rate-limit unicast acl** {**ingress** | **egress**} コマンドを入力します。
- NetFlow：第 52 章「NetFlow ハードウェア サポート」を参照してください
- ポリシー ベース ルーティング（PBR）：第 33 章「Policy-Based Routing（PBR）」を参照してください。

（注）　PFC および DFC は、**tunnel key** コマンドで設定されるトンネル用にハードウェアを加速しません。

- ポイントツーポイント総称ルーティングカプセル化（GRE）トンネル上での IPv4 マルチキャスト。
- GRE トンネリングおよび IP-in-IP トンネリング：PFC および DFC は次の **tunnel** コマンドをサポートします。
  - **tunnel destination**
  - **tunnel mode gre**
  - **tunnel mode ipip**
  - **tunnel source**
  - **tunnel ttl**
  - **tunnel tos**

  ソフトウェアで実行されるその他のサポート対象トンネリング タイプ。

  tunnel ttl コマンド（デフォルトは 255）は、カプセル化パケットの TTL を設定します。

  tunnel tos コマンドが存在する場合は、パケットがカプセル化されるときの Type of Service（ToS; タイプ オブ サービス）バイトを設定します。**tunnel tos** コマンドが存在せず、QoS がイネーブルでない場合、パケットがカプセル化される際にパケットの ToS バイトには、元のパケットの ToS バイトが設定されます。**tunnel tos** コマンドが存在せず、QoS がイネーブルである場合、パケットがカプセル化される際にパケットの ToS バイトには、PFC QoS によって変更されたパケットの ToS バイトが設定されます。

GRE トンネリングおよび IP-in-IP トンネリングを設定するには、次のマニュアルを参照してください。

http://www.cisco.com/en/US/docs/ios-xml/ios/interface/configuration/15-sy/ir-impl-tun.html

tunnel tos および **tunnel ttl** コマンドを設定するには、次のマニュアルを参照してください。

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/12s_tos.html

トンネルについては、次の点に注意してください。

- PFC4 および DFC4 では、最大 8 個のマルチキャスト ランデブー ポイント（RP）をサポートしています。
- ハードウェアが処理する各トンネルには固有の送信元が必要です。ハードウェアが処理するトンネルは宛先が異なる場合でも送信元を共有できません。ループバック インターフェイス上のセカンダリ アドレスを使用するか、複数のループバック インターフェイスを作成します (CSCdy72539)。
- 各トンネル インターフェイスは、内部 VLAN を 1 つ使用します。
- 各トンネル インターフェイスは、ルータ MAC アドレスごとに追加ルータ MAC アドレス エントリを 1 つ使用します。
- PFC と DFC は、トンネル インターフェイス上で PFC QoS 機能をサポートしています。
- トンネル インターフェイスの出力機能で設定されたトンネルは、ソフトウェアでサポートされます。出力機能例として、出力 Cisco IOS ACL、NAT（内部から外部への変換）、TCP 代行受信、暗号化が挙げられます。

- VLAN ACL（VACL）：VACL を設定するには、第 74 章「VLAN ACL（VACL）」を参照してください。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

PART 2

設定の基礎

コマンドライン インターフェイス

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CLI のアクセス

EIA/TIA-232 コンソール インターフェイス経由で 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。

EIA/TIA-232 コンソール インターフェイスの接続を使用して、初期設定を行います。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 6500 Series Switch Module Installation Guide*』を参照してください。

コンソールを接続するには、次の作業を行います。

	コマンド	目的
ステップ 1	Return キーを押します。	プロンプトを表示します。
ステップ 2	`Router> enable`	イネーブル モードを開始します。
ステップ 3	`Password: password` `Router#`	イネーブル モードの開始を完了します。
ステップ 4	`Router# quit`	終了したらセッションを終了します。

コンソールに接続すると、次のように表示されます。

```
Press Return for Console prompt

Router> enable
Password:
Router#
```

Telnet を使用して CLI にアクセスする場合

（注）　スイッチに telnet で接続するには、事前に IP アドレスを設定する必要があります。

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** コマンドに指定されている時間が経過すると、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*}	アクセス対象のスイッチに、リモート ホストから telnet 接続します。
ステップ 2	`Password: password` `Router#`	認証を開始します。 （注）　パスワードが設定されていない場合は、Return を押します。
ステップ 3	`Router> enable`	イネーブル モードを開始します。
ステップ 4	`Password: password` `Router#`	イネーブル モードの開始を完了します。
ステップ 5	`Router# quit`	終了したら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 Router_1
Trying 172.20.52.40...
Connected to 172.20.52.40.
Escape character is '^]'.

User Access Verification

Password:
Router_1> enable
Password:
Router_1#
```

コマンドラインの処理

コマンドには、大文字と小文字の区別はありません。また、コマンドおよびパラメータは、現在使用可能な他のコマンド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。直前に入力した 20 のコマンドは、履歴バッファに保存されます。これらのコマンドをスクロールして、プロンプトに対するコマンドを入力したり、編集したりできます 表 2-1 に、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	目的
Ctrl+B または ←キーを押す	カーソルを 1 文字分だけ後退させます。 **（注）** 矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。
Ctrl+F または →キーを押す	カーソルを 1 文字分だけ進めます。 **（注）** 矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。
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	カーソルをコマンドラインの末尾に移動します。
Esc B	1 文字分だけカーソルを後退させます。
Esc F	カーソルを 1 文字分だけ進めます。

ヒストリ置換

履歴バッファには、直前に入力した 20 のコマンドが保存されます。特別な省略コマンドを使用して、再入力せずに保存されているコマンド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↑キー	履歴バッファ内のコマンドを呼び出します。最後に実行したコマンドが最初に呼び出されます。キーを押すたびに、より古いコマンドが順次表示されます。 **（注）** 矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。
Ctrl+N または↓キー	Ctrl+P または↑キーでコマンドを呼び出してから、履歴バッファ内のより新しいコマンドに戻ります。キーを押すたびに、より新しいコマンドが順次表示されます。 **（注）** 矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。
`Router# show history`	EXEC モードで、直前に入力したいくつかのコマンドを表示します。

Cisco IOS コマンド モード

（注） Cisco IOS コマンド モードの詳細については、次の URL にある『*Cisco IOS Configuration Fundamentals Configuration Guide*』を参照してください。

http://www.cisco.com/en/US/docs/ios-xml/ios/fundamentals/configuration/15_sy/fundamentals-15-sy-book.html

Cisco IOS ユーザ インターフェイスは、いくつかのモードに分かれています。使用できるコマンドの種類は、現在のモードによって異なります。特定のモードで使用できるコマンドのリストを表示するには、システム プロンプトで疑問符（?）を入力します。「Cisco IOS コマンド リストおよび構文の表示」（P.2-6）を参照してください。

スイッチとのセッションを開始するときは、ユーザ モード（別名ユーザ EXEC モード）が有効です。EXEC モードでは、一部のコマンドしか使用できません。すべてのコマンドにアクセスするには、特権 EXEC モードを開始する必要があります。特権 EXEC モードにアクセスするには、通常、パスワードの入力が必要です。特権 EXEC モードでは、任意の EXEC コマンドを入力できるほか、グローバル コンフィギュレーション モードにアクセスできます。

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、再起動後もそれらのコマンドが保存されます。最初にグローバル コンフィギュレーション モードを開始する必要があります。グローバル コンフィギュレーション モードから、インターフェイス コンフィギュレーション モード、サブインターフェイス コンフィギュレーション モード、および各種プロトコル固有のモードを開始できます。

（注）　EXEC モード コマンドを入力するには、コマンドの前に **do** キーワードを入力します。

ROM モニタ モードは、スイッチが適切にブートできない場合に使用される別のモードです。たとえば、スイッチの起動時に有効なシステム イメージが見つからない場合、またはスイッチのコンフィギュレーション ファイルが壊れている場合に、スイッチで ROM モニタ モードが開始される場合があります。「ROM モニタの CLI」（P.2-7）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	開始方法	プロンプト
ユーザ EXEC	リモート装置への接続、端末の一時的な設定変更、基本的なテストの実行、およびシステム情報の表示。	ログイン。	`Router>`
特権 EXEC（イネーブル）	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。このコマンドを使用して、別のコマンド モードにアクセスします。	ユーザ EXEC モードで、**enable** コマンドおよびイネーブル パスワードを入力します。	`Router#`
グローバル設定	システム全体に影響を及ぼす機能の設定。	特権 EXEC モードで、**configure terminal** コマンドを入力します。	`Router(config)#`
インターフェイス コンフィギュレーション	インターフェイス別の多岐にわたる機能があります。インターフェイス コマンドを実行すると、インターフェイスの動作がイネーブルになるか、または変更されます。	グローバル コンフィギュレーション モードで、**interface** *type slot/port* コマンドを入力します。	`Router(config-if)#`
コンソール コンフィギュレーション	直接接続されたコンソールまたは Telnet 接続による仮想端末から、このコンフィギュレーション モードを使用してコンソール インターフェイスを設定します。	グローバル コンフィギュレーション モードから **line console 0** コマンドを入力します。	`Router(config-line)#`

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

exit 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。

Cisco IOS コマンド リストおよび構文の表示

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

```
Router> ?
```

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

```
Router# co?
collect  configure  connect  copy
```

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

次に例を示します。

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

前に入力したコマンドを再表示するには、↑キーまたは Ctrl+P を押します。↑キーを続けて押すことにより、直前に入力したコマンドを 20 まで表示できます。

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

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。

CLI のセキュリティ保護

CLI へのアクセスをセキュリティ保護することにより、無許可のユーザは、コンフィギュレーションの設定を見たりコンフィギュレーションを変更したりできなくなります。それにより、ネットワークの安定性や安全性を守ることができます。次のセキュリティ機能を 1 つ以上設定することにより、強力で柔軟なセキュリティ スキームをスイッチに構築できます。

- 特権 EXEC コマンドへのアクセスの保護：最低限、ユーザ EXEC と特権 EXEC（イネーブル）IOS コマンド モードには、別々のパスワードを設定する必要があります。CLI セッションへのアクセスが特定のユーザに限定されるようにユーザ名とパスワードのペアを設定することにより、セキュリティのレベルをさらに強化できます。詳細については、以下のマニュアルを参照してください。

  http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_cfg_sec_4cli.html

- RADIUS、TACACS+、または Kerberos によるスイッチのアクセス コントロール：集中型かつスケーラブルなセキュリティ スキームにするには、Remote Authentication Dial-In User Service（RADIUS）、Terminal Access Controller Access-Control System Plus（TACACS+）、または Kerberos を外部セキュリティ サーバで稼働してユーザの認証と許可を行う必要があります。詳細については、以下のマニュアルを参照してください。

  http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/15-sy/secdata-15-sy-library.html

- SSH または HTTPS によるセキュア接続の設定：コンフィギュレーション セッションの盗聴を防ぐために、セキュア シェル（SSH）クライアント、あるいは HTTP over Secure Socket Layer（HTTPS）をサポートするブラウザを使用して、に暗号化接続できます。詳細については、以下のマニュアルを参照してください。

  http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/15-sy/secdata-15-sy-library.html

  HTTPS についての詳細は、次の URL にある『HTTPS - HTTP Server and Client with SSL 3.0』を参照してください。

  http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_cfg_sec_4cli.html

- SCP によるコンフィギュレーション ファイルのセキュアなコピー：スイッチとの間でコンフィギュレーション ファイルやイメージ ファイルをコピーするときに盗聴されるのを防ぐために、セキュア コピー プロトコル（SCP）を使用して暗号化ファイル転送を実行できます。SCP についての詳細は、次の URL にある『Secure Copy』を参照してください。

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_ssh/configuration/15-sy/sec-usr-ssh-sec-copy.html

ROM モニタの CLI

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

スイッチを再起動し、起動から 60 秒以内に Break キーを押して、ROM モニタ モードを開始することもできます。

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

端末サーバから ROM モニタ モードにアクセスするには、エスケープによって Telnet プロンプトを表示し、端末エミュレーション プログラムで **send break** コマンドを入力し、ROM モニタ モードを開始します。

ROM モニタ モードが開始されると、プロンプトが rommon 1> になります。疑問符（**?**）を入力すると、使用できる ROM モニタ コマンドが表示されます。

ヒント　Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

SmartPort マクロ

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

SmartPort マクロの前提条件

なし。

SmartPort マクロの制約事項

- 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 name** *macro-name* ユーザ EXEC コマンドを使用します。
- マクロは編集できません。**macro name** コマンドで既存のマクロ名を指定した場合、既存のマクロは新しいマクロに置換されます。
- マクロにすでに説明が設定済みの状態で **macro description** コマンドを使用して何らかの説明を入力すると、既存の説明を置換するのではなく、既存の説明に追加されます。入力された説明はパイプ文字（|）で区切られます。
- マクロの説明は、256 文字以内です。説明のための文字列が 256 文字を超えると、新しい説明を保存するために最も古い説明が削除されます。
- 再帰的なユーザ作成マクロはサポートされていません。他のマクロを呼び出すようなマクロは定義できません。
- 各ユーザ作成マクロには、キーワード/値のペアを最大 3 つ含むことができます。
- マクロの定義は、3,000 文字以内です。改行文字は 2 文字として数えます。
- マクロを作成する際に、**exit** や **end** コマンド、または **interface** *interface-id* コマンド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* に続くコマンドが異なるコマンド モードで実行されることがあります。マクロを作成するときは、すべての CLI コマンドを同じコンフィギュレーション モードにします。
- 一意の値の割り当てを必要とするマクロを作成する場合、**parameter** *value* キーワードを使用して、その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。キーワードで一致が見られると、すべて対応する値に置き換えられます。キーワードが完全に一致すると、それが長い文字列の一部であったとしても一致と見なされて、対応する値に置き換えられます。
- マクロ名では、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、2 つの別個のマクロとなります。
- 一部のマクロには、パラメータ値が必要なキーワードが含まれます。**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、マクロで必要な値を一覧表示できます。キーワード値を入力せずにマクロを適用した場合、コマンドは無効となり、マクロは適用されません。
- マクロがスイッチまたはスイッチ インターフェイスに対してグローバルに適用される場合は、インターフェイス上の既存の設定が保持されます。これは、差分設定に適用する場合に役立ちます。
- コマンドを追加または削除してマクロ定義を変更する場合、元のマクロを適用したインターフェイスに変更は反映されません。新規または変更済みのコマンドを適用するには、インターフェイスにアップデート済みマクロを再適用する必要があります。
- マクロを適用およびデバッグして、構文エラーまたは設定エラーを検出するには、**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 コマンドを使用できます。構文エラーまたは設定エラーが原因でコマンドが失敗した場合でも、マクロは引き続き残りのコマンドを適用します。
- 特定のインターフェイス タイプ固有の CLI コマンドもあります。設定を受け入れないインターフェイスにマクロを適用すると、マクロは構文チェックまたは設定チェックに失敗し、スイッチはエラー メッセージを返します。

- インターフェイス範囲へのマクロの適用は、単一インターフェイスへのマクロの適用と同じです。インターフェイスの範囲を使用する場合、マクロはその範囲内の各インターフェイスに順番に適用されます。1 つのインターフェイスでマクロ コマンドの実行に失敗しても、マクロは残りのインターフェイス上に適用されます。
- スイッチまたはスイッチ インターフェイスにマクロを適用すると、マクロ名が自動的にスイッチまたはインターフェイスに追加されます。**show running-config** ユーザ EXEC コマンドを使用して、適用されたコマンドおよびマクロ名を表示できます。

SmartPort マクロについて

シスコ提供の SmartPort マクロについて

シスコ提供の SmartPort マクロおよびそれに含まれるコマンドを表示するには、**show parser macro** ユーザ EXEC コマンドを使用します。

表 3-1　シスコ提供の SmartPort マクロ

マクロ名	説明
cisco-global	VLAN 間でのロード バランシングをイネーブルにする場合、スパニングツリー インスタンスの高速コンバージェンスを実行する場合、およびポート エラー回復をイネーブルにする場合、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 のようなデスクトップ 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 セキュリティと信頼性を高めるために、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 を搭載した 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** マクロの拡張機能で、同じセキュリティ機能と復元力機能を提供します。ただし、遅延に影響されやすい音声トラフィックを適切に処理するために、専用音声 VLAN が追加されています。
cisco-switch	スイッチやルータなどのデバイス間でレイヤ 2 接続を実行する場合、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	スイッチやルータなどのデバイス間でレイヤ 3 接続を実行する場合、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。

Catalyst スイッチ向けには、シスコが推奨するテスト済みのベースライン コンフィギュレーション テンプレートも提供されています。オンライン リファレンス ガイドのテンプレートには、ポート使用に応じて SmartPort マクロが作成できる CLI コマンドが含まれています。このコンフィギュレーション テンプレートを使用して SmartPort マクロを作成することにより、シスコ推奨のネットワーク設計および設定を構築し、導入できます。

ユーザ作成の SmartPort マクロについて

SmartPort マクロは、共通の設定を保存して共有するのに便利な方法です。SmartPort マクロを使用すると、ネットワーク内でのスイッチの場所に基づいて機能や設定をイネーブルにしたり、ネットワーク全体にわたる大規模な設定導入を行ったりすることができます。

各 SmartPort マクロは、ユーザ定義による Cisco IOS CLI コマンドの集まりです。SmartPort マクロをインターフェイスに適用すると、そのマクロに含まれる CLI コマンドがインターフェイス上に設定されます。インターフェイスに SmartPort マクロを適用しても、インターフェイスの既存の設定は失われません。新しいコマンドがインターフェイスに追加され、実行コンフィギュレーション ファイルに保存されます。

SmartPort マクロのデフォルト設定

次に、デフォルトで提供されるシスコ提供の SmartPort マクロをリストで表示する例を示します。

```
Router# show parser macro brief
    default global   : cisco-global
    default interface: cisco-desktop
    default interface: cisco-phone
    default interface: cisco-switch
    default interface: cisco-router
```

SmartPort マクロの設定方法

- 「シスコ提供の SmartPort マクロの使用」（P.3-4）
- 「SmartPort マクロの作成」（P.3-13）

シスコ提供の SmartPort マクロの使用

- 「cisco-global SmartPort マクロの使用」（P.3-4）
- 「cisco-desktop SmartPort マクロの使用」（P.3-5）
- 「cisco-phone SmartPort マクロの使用」（P.3-7）
- 「cisco-switch SmartPort マクロの使用」（P.3-9）
- 「cisco-router SmartPort マクロの使用」（P.3-11）

cisco-global SmartPort マクロの使用

- 「cisco-global SmartPort マクロの内容の表示」（P.3-4）
- 「cisco-global SmartPort マクロの適用」（P.3-5）

cisco-global SmartPort マクロの内容の表示

```
Router# 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

# Config Cos to DSCP mappings
platform qos map cos-dscp 0 8 16 26 32 46 48 56

# 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-global SmartPort マクロの適用

cisco-global SmartPort マクロを適用するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# 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	`Router(config)# macro global apply cisco-global`	cisco-global SmartPort マクロを適用します。
ステップ 3	`Router(config)# end`	特権 EXEC モードに戻ります。

次に、cisco-global SmartPort マクロを適用して、適用したマクロ名を表示する例を示します。

```
Router# configure terminal
Router(config)# macro global apply cisco-global
Changing VTP domain name from previous_domain_name to [smartports]
Setting device to VTP TRANSPARENT mode.
Router(config)# end
Router# show parser macro description
Global Macro(s): cisco-global

Interface    Macro Description(s)
-----------------------------------------------------------------
-----------------------------------------------------------------
Router#
```

cisco-desktop SmartPort マクロの使用

- 「cisco-desktop SmartPort マクロの内容の表示」（P.3-6）
- 「cisco-desktop SmartPort マクロの適用」（P.3-6）

cisco-desktop SmartPort マクロの内容の表示

```
Router# show parser macro name cisco-desktop
Macro name : cisco-desktop
Macro type : default interface
# macro keywords $AVID
# Basic interface - Enable data VLAN only
# Recommended value for access vlan (AVID) should not be 1
switchport
switchport access vlan $AVID
switchport mode access

# Enable port security limiting port to a single
# MAC address -- that of desktop
switchport port-security
switchport port-security maximum 1

# Ensure port-security age is greater than one minute
# and use inactivity timer
switchport port-security violation restrict
switchport port-security aging time 2
# Configure port as an edge network port
spanning-tree portfast
spanning-tree bpduguard enable
```

cisco-desktop SmartPort マクロの適用

cisco-desktop SmartPort マクロを適用するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# 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	`Router(config)# interface` *type slot/port*	設定するインターフェイスを選択します。
ステップ 3	`Router(config-if)# macro apply cisco-desktop $AVID` *access_vlan_ID*	cisco-desktop SmartPort マクロを適用します。*access_vlan_ID* の値として推奨される範囲は 2 ～ 4094 です。
ステップ 4	`Router(config-if)# end`	特権 EXEC モードに戻ります。

次に、アクセス VLAN として VLAN 2 を指定して、cisco-desktop SmartPort マクロをポート GigabitEthernet 1/1 に適用し、その結果を確認する例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 1/1
Router(config-if)# macro apply cisco-desktop $AVID 2
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION

%Portfast has been configured on GigabitEthernet1/1 but will only
 have effect when the interface is in a non-trunking mode.
Router(config)# end
Router# show parser macro description interface gigabitethernet 1/1
Global Macro(s): cisco-global

Interface    Macro Description(s)
---------------------------------------------------------------
Gi1/1        cisco-desktop
```

```
------------------------------------------------------------
Router# show running-config interface gigabitethernet 1/1
Building configuration...

Current configuration : 307 bytes
!
interface GigabitEthernet1/1
 switchport
 switchport access vlan 2
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 shutdown
 macro description cisco-desktop
 spanning-tree portfast
 spanning-tree bpduguard enable
end

Router#
```

cisco-phone SmartPort マクロの使用

cisco-phone SmartPort マクロの内容の表示

```
Router# show parser macro name cisco-phone
Macro name : cisco-phone
Macro type : default interface
# macro keywords $AVID $VVID
# VoIP enabled interface - Enable data VLAN
# and voice VLAN (VVID)
# Recommended value for access vlan (AVID) should not be 1
switchport
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 3 MAC
# addressess -- One for desktop and two for phone
switchport port-security
switchport port-security maximum 3

# Ensure port-security age is greater than one minute
# and use inactivity timer
switchport port-security violation restrict
switchport port-security aging time 2
# 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
```

cisco-phone SmartPort マクロの適用

cisco-phone SmartPort マクロを適用するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# 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	`Router(config)# interface` *type slot/port*	設定するインターフェイスを選択します。
ステップ 3	`Router(config-if)# macro apply cisco-phone $AVID` *access_vlan_ID* `$VVID` *voice_vlan_ID*	cisco-phone SmartPort マクロを適用します。*access_vlan_ID* の値として推奨される範囲は 2 ～ 4094 です。*voice_vlan_ID* の値として推奨される範囲は 2 ～ 4094 です。
ステップ 4	`Router(config-if)# end`	特権 EXEC モードに戻ります。

cisco-phone SmartPort マクロを適用する場合は、次の点に注意してください。

- 生成されるコマンドの中には、PFC QoS コマンドに分類されるものもあります。PFC QoS コマンドはポート ASIC で制御されるすべてのポートに適用されます。生成されたこれらのコマンドのいずれかが適用されると、PFC QoS では、コマンド適用の結果生成されたメッセージをポート ASIC で制御されるすべてのポートに表示します。これらのコマンドは、モジュールに応じて 48 ものポートに適用されます。『*Release Notes for Cisco IOS Release 15.1SY*』の各モジュールの説明を参照し、ポート グループの数およびポート グループごとのポート範囲を確認してください。

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/15.1SY/release_notes.html

- 他のポートに trust CoS を設定するよう指示するメッセージが表示される場合があります。生成された QoS コマンドをイネーブルにするには、そのように設定する必要があります。
- ポート信頼状態の要件が矛盾するため、同じポート ASIC で制御されるポート上で cisco-phone SmartPort マクロおよび他のマクロを適用できない場合があります。

次に、アクセス VLAN として VLAN 2 を指定して、cisco-phone SmartPort マクロをポート GigabitEthernet 2/2 に適用し、その結果を確認する例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 2/2
Router(config-if)# macro apply cisco-phone $AVID 2 $VVID 3
Hardware QoS is enabled
Propagating cos-map to inband port
Propagating cos-map configuration to: [ポート　リストは省略]
```

（同じポート ASIC で制御されるその他のポートに関するテキスト出力は省略）

```
Warning: rcv cosmap will not be applied in hardware.
  To modify rcv cosmap in hardware, all of the interfaces below
  must be put into 'trust cos' state:
    [ポート　リストは省略]
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION

%Portfast has been configured on GigabitEthernet1/2 but will only
 have effect when the interface is in a non-trunking mode.
Router(config)# end

Router# show parser macro description interface gigabitethernet 2/2
Global Macro(s): cisco-global
```

```
Interface    Macro Description(s)
-------------------------------------------------------------
Gi2/2        cisco-phone
-------------------------------------------------------------

Router# show running-config interface gigabitethernet 2/2
Building configuration...

Building configuration...

Current configuration : 307 bytes
!
interface GigabitEthernet1/2
Building configuration...

Current configuration : 1336 bytes
!
interface GigabitEthernet2/2
 switchport
 switchport access vlan 2
 switchport mode access
 switchport voice vlan 3
 switchport port-security
 switchport port-security maximum 3
 switchport port-security aging time 2
 switchport port-security violation restrict
 shutdown
```

（QoS キューイング コマンドに関するテキスト出力は省略。ポート タイプによって異なる）

```
 platform qos trust cos
 auto qos voip cisco-phone
 macro description cisco-phone
 spanning-tree portfast
 spanning-tree bpduguard enable
end

Router#
```

cisco-switch SmartPort マクロの使用

- 「cisco-switch SmartPort マクロの内容の表示」（P.3-9）
- 「cisco-switch SmartPort マクロの適用」（P.3-10）

cisco-switch SmartPort マクロの内容の表示

```
Router# show parser macro name cisco-switch
Macro name : cisco-switch
Macro type : default interface
# macro keywords $NVID
# Do not apply to EtherChannel/Port Group
# Access Uplink to Distribution

# Define unique Native VLAN on trunk ports
# Recommended value for native vlan (NVID) should not be 1
switchport
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 trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate

# 802.1w defines the link as pt-pt for rapid convergence
spanning-tree link-type point-to-point

Router#
```

cisco-switch SmartPort マクロの適用

cisco-switch SmartPort マクロを適用するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# 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	`Router(config)# interface` *type slot/port*	設定するインターフェイスを選択します。
ステップ 3	`Router(config-if)# macro apply cisco-switch $NVID` *native_vlan_ID*	cisco-switch SmartPort マクロを適用します。*native_vlan_ID* の値として推奨される範囲は 2 ～ 4094 です。
ステップ 4	`Router(config-if)# end`	特権 EXEC モードに戻ります。

次に、ネイティブ VLAN として VLAN 4 を指定して、cisco-switch SmartPort マクロをポート GigabitEthernet 1/4 に適用し、その結果を確認する例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 1/4
Router(config-if)# macro apply cisco-switch $NVID 4
Router(config-if)# end
Router# show parser macro description interface gigabitethernet 1/4
Interface    Macro Description(s)
-------------------------------------------------------------
Gi1/4        cisco-switch
-------------------------------------------------------------
Router# show running-config interface gigabitethernet 1/4
Building configuration...

Current configuration : 247 bytes
!
interface GigabitEthernet1/4
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4
 switchport mode trunk
 switchport nonegotiate
 shutdown
 macro description cisco-switch
 spanning-tree link-type point-to-point
end

Router#
```

cisco-router SmartPort マクロの使用

cisco-router SmartPort マクロの内容の表示

```
Router# show parser macro name cisco-router
Macro name : cisco-router
Macro type : default interface
# macro keywords $NVID
# Do not apply to EtherChannel/Port Group
# Access Uplink to Distribution
switchport

# 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 trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate

# Configure qos to trust this interface
auto qos voip trust
platform 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

Router#
```

cisco-router SmartPort マクロの適用

cisco-router SmartPort マクロを適用するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# 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	`Router(config)# interface` *type slot/port*	設定するインターフェイスを選択します。
ステップ 3	`Router(config-if)# macro apply cisco-router $NVID` *native_vlan_ID*	cisco-router SmartPort マクロを適用します。*native_vlan_ID* の値として推奨される範囲は 2 ～ 4094 です。
ステップ 4	`Router(config-if)# end`	特権 EXEC モードに戻ります。

（注）　cisco-router SmartPort マクロには、auto qos voip trust コマンドが含まれています。**switchport** コマンドで設定したポートに対して **auto qos voip trust** コマンドを入力すると、**platform qos trust cos** コマンドが生成され、このポートに適用されます。ただし、cisco-router SmartPort マクロでは **platform qos trust dscp** コマンドを使用して、DSCP を信頼するようにポート信頼状態を変更します。cisco-router SmartPort マクロを適用する場合、ポート ASIC で制御されるその他のポートに対して **platform qos trust cos** コマンドを入力するよう求めるメッセージは無視してください。

次に、cisco-router SmartPort マクロをポート GigabitEthernet 1/5 に適用し、その結果を確認する例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 1/5
Router(config-if)# macro apply cisco-router $NVID 5
Hardware QoS is enabled
Propagating cos-map to inband port
Propagating cos-map configuration to: [ポート　リストは省略]
```

（同じポート ASIC で制御されるその他のポートに関するテキスト出力は省略）

（一時的に適用された trust CoS コマンドに関するテキスト出力は省略）

```
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION

%Portfast has been configured on GigabitEthernet1/5 but will only
 have effect when the interface is in a non-trunking mode.
Router(config-if)# end
Router# show parser macro description interface gigabitethernet 1/5
Interface    Macro Description(s)
-------------------------------------------------------------
Gi1/5        cisco-router
-------------------------------------------------------------
Router# show running-config interface gigabitethernet 1/5
Building configuration...

Current configuration : 1228 bytes
!
interface GigabitEthernet1/5
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 5
 switchport mode trunk
 switchport nonegotiate
 shutdown
 wrr-queue bandwidth 20 100 200
```

（QoS キューイング コマンドに関するテキスト出力は省略。ポート タイプによって異なる）

```
 platform qos trust dscp
 auto qos voip trust
 macro description cisco-router
 spanning-tree portfast
 spanning-tree bpduguard enable
end

Router#
```

SmartPort マクロの作成

SmartPort マクロの作成

SmartPort マクロを作成するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# 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	`Router(config)# macro name macro-name`	マクロを作成します。 マクロ名では、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、2 つの別個のマクロとなります。 マクロの定義は、3,000 文字以内です。改行文字は 2 文字として数えます。 マクロ作成モードではプロンプトは表示されません。 1 行ごとに 1 つのマクロ コマンドを指定します。 マクロ内にコメントを入力する場合は、行頭に # 文字を指定します。 マクロを終了するには、@ 文字を使用します。 マクロ内では、**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。**exit** または **end**、または **interface** *interface-id* 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るためです。最良の結果を出すには、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。 各ユーザ作成マクロには、キーワード/値のペアを最大 3 つ含むことができます。
ステップ 3	`# macro keywords keyword1 keyword2 keyword3`	（任意）マクロに定義したキーワードを説明するためのヘルプ ストリングを作成できます。1 つのマクロには最大 3 つのヘルプ ストリング コメントを入力できます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show parser macro name** *macro-name*	マクロが作成されたことを確認します。

（注）　**no** 形式の **macro name** グローバル コンフィギュレーション コマンドでは、マクロ定義だけが削除されます。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、影響はありません。

次に、レイヤ 2 アクセス VLAN および送信元メディア アクセス コントロール（MAC）アドレス数を定義し、さらに **# macro keywords** の使用によって 2 つのヘルプ ストリング キーワードを含むマクロを作成する例を示します。

```
Router(config)# macro name test
#macro keywords $VLANID $MAX
switchport access vlan $VLANID
switchport port-security maximum $MAX
@
```

ユーザ作成の SmartPort マクロの適用

SmartPort マクロを適用するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# 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	`Router(config)# 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 3	`Router(config)# interface` *interface_id*	（インターフェイス マクロの場合に必要）マクロを適用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 4	`Router(config)# macro` [**global**] {**apply** | **trace**} *macro-name* [*keyword value*] [*keyword value*] [*keyword value*]	マクロで定義された個々のコマンドを適用、または適用し追跡します。 グローバル マクロの場合： • 構文エラーや設定エラーを検出するには、**macro global trace** *macro-name* コマンドを入力して、マクロを適用しデバッグします。 • マクロに定義されているキーワード/値のペアの一覧を表示するには、**macro global apply macro-name ?** コマンドを使用します。 インターフェイス マクロの場合： • 構文エラーや設定エラーを検出するには、**macro trace** *macro-name* コマンドを入力して、マクロを適用しデバッグします。 • マクロに定義されているキーワード/値のペアの一覧を表示するには、**macro apply macro-name ?** コマンドを使用します。 マクロを適切に適用するには、必要なキーワード/値のペアをすべて入力してください。 キーワードの照合では、大文字と小文字が区別されます。 マクロにより適用されたコマンドでは、一致するすべてのキーワードが、対応する値に置換されます。
ステップ 5	`Router(config)# end`	特権 EXEC モードに戻ります。

スイッチ上のグローバル マクロ適用済みの設定を削除するには、マクロ内にある各コマンドの **no** バージョンだけを入力します。インターフェイスの設定すべてを削除するには、**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。

次に、snmp という名前のユーザ作成マクロを適用し、ホスト名アドレスを **test-server**、IP precedence 値を 7 に設定する例を示します。

```
Router(config)# macro global apply snmp ADDRESS test-server VALUE 7
```

次に、**macro global trace** 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 という名前のユーザ作成マクロをデバッグし、スイッチへの適用時にマクロの構文エラーまたは設定エラーを検出する例を示します。

```
Router(config)# macro global trace snmp VALUE 7
Applying command...'snmp-server enable traps port-security'
Applying command...'snmp-server enable traps linkup'
Applying command...'snmp-server enable traps linkdown'
Applying command...'snmp-server host'
%Error Unknown error.
Applying command...'snmp-server ip precedence 7'
```

次に、desktop-config という名前のユーザ作成マクロを適用し、設定を確認する例を示します。

```
Router(config)# interface gigabitethernet1/2
Router(config-if)# macro apply desktop-config
Router(config-if)# end
Router# show parser macro description
Interface    Macro Description
---------------------------------------------------------------
Gi1/2      desktop-config
---------------------------------------------------------------
```

次に、desktop-config という名前のユーザ作成マクロを適用し、キーワード *vlan* をいずれも VLAN ID 25 に置換する例を示します。

```
Router(config-if)# macro apply desktop-config vlan 25
```

SmartPort マクロの設定の確認

表 3-2　SmartPort マクロの表示コマンド

コマンド	目的
show parser macro	設定されている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	設定されているマクロ名を表示します。
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説明を表示します。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

PART 3

仮想スイッチング システム（VSS）

仮想スイッチング システム

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

VSS の前提条件

startup-config ファイルの VSS の設定が、両方のシャーシで一致している必要があります。

VSS の制約事項

一般的な VSS の制約事項

- VSS モードは 1 つのシャーシ内でのスーパーバイザ エンジンの冗長性をサポートしていません。
- スイッチ プライオリティの新しい値を設定した場合、変更内容は、コンフィギュレーション ファイルを保存して、再起動を実行した後に有効になります。
- DFC 搭載スイッチング モジュール間のアウトオブバンド MAC アドレス テーブルの同期（**mac address-table synchronize** コマンド）は、VSS モードで自動的にイネーブルになります。これは推奨設定です。
- ICS スーパーバイザ エンジンは、**show** コマンドをサポートしていません。トレースバックを避けるため、ICS スーパーバイザ エンジンでは **show** コマンドを発行しないでください。

VSL の制約事項

- 回線の冗長性については、VSL のため、スイッチごとに少なくとも 2 つのポートを設定することを推奨します。モジュールの冗長性については、2 つのポートを各シャーシの別のスイッチング モジュールで設定できます。
- VSL を設定すると、**no platform qos channel-consistency** コマンドが自動的に適用されます。このコマンドを削除しないでください。
- VSL ポートはミニ プロトコル アナライザの送信元に設定できません（**monitor ... capture** コマンド）。送信元がスタンバイ スイッチのポート チャネル上の VSL の場合、モニタ キャプチャ セッションは開始できません。スタンバイ スイッチ上のリモート VSL ポート チャネルが指定されている場合にモニタ キャプチャを開始しようとすると、次のメッセージが表示されます。

  ```
  % remote VSL port is not allowed as capture source
  ```

  送信元がリモート VSL ポート チャネルであるためにスケジュールされたモニタ キャプチャの起動に失敗した場合は、次のメッセージが表示されます。

  ```
  Packet capture session 1 failed to start. A source port is a remote VSL.
  ```

マルチシャーシ EtherChannel（MEC）の制約事項

- MEC のすべてのリンクは、同じ仮想ドメインのアクティブまたはスタンバイ シャーシでローカルに終端している必要があります。
- LACP 制御プロトコルを使用する MEC の場合、*minlinks* コマンド引数に、MEC が動作する各シャーシ内の物理リンクの最小数を定義します。
- LACP 制御プロトコルを使用する MEC の場合、*maxbundle* のコマンド引数に、VSS 全体の MEC 内の最大リンク数を定義します。

- MEC では、LACP 1:1 冗長性がサポートされています。LACP 1:1 冗長性の詳細については、「LACP 1:1 冗長性に関する情報」（P.22-7）を参照してください。
- MEC は、異なる VSS ドメイン内の別の MEC に接続できます。

デュアル アクティブ検出の制約事項

- Flex Link が VSS で設定されている場合、PAgP デュアル アクティブ検出を使用します。
- デュアル アクティブ検出のリンク冗長性を維持するには、デュアル アクティブ検出用にスイッチごとに少なくとも 2 つのポートを設定します。モジュールの冗長性を維持するために、2 つのポートを、各シャーシ内の異なるスイッチング モジュール上に配置できます。可能であれば、VSL 以外の異なるモジュールに配置してください。
- dual-active fast hello モードを設定すると、次のコマンドを除いて、既存のすべての設定がインターフェイスから自動的に除外されます。
  - **description**
  - **logging event**
  - **load-interval**
  - **rcv-queue cos-map**
  - **rcv-queue queue-limit**
  - **rcv-queue random-detect**
  - **rcv-queue threshold**
  - **wrr-queue bandwidth**
  - **wrr-queue cos-map**
  - **wrr-queue queue-limit**
  - **wrr-queue random-detect**
  - **wrr-queue threshold**
  - **priority-queue cos-map**
- デュアル アクティブ検出の fast hello ポートで使用できるのは、次のコンフィギュレーション コマンドだけです。
  - **default**
  - **description**
  - **dual-active**
  - **exit**
  - **load-interval**
  - **logging**
  - **no**
  - **shutdown**
- ASIC 固有の QoS コマンドは、デュアル アクティブ検出の fast hello ポートで直接設定されませんが、同じ ASIC グループ内の別の非 fast hello ポートでコマンドが設定された場合、fast hello ポート上で使用することができます。これらのコマンドの一覧については、第 62 章「PFC QoS に関する制約事項」を参照してください。

VSS モードのサービス モジュールの制約事項

- VLAN グループをサービス モジュール インターフェイスに設定および接続する場合は、**switch** {**1** | **2**} コマンド キーワードを使用します。たとえば **firewall vlan-group** コマンドは、**firewall switch** *num* **slot** *slot* **vlan-group** コマンドになります。
- サービス モジュールのソフトウェア イメージをアップグレードする場合は、**switch** {**1** | **2**} コマンド キーワードを使用します。
- アクティブ シャーシの IDSM-2 とスタンバイ シャーシの IDSM-2 の間では、EtherChannel ロード バランシング（ECLB）はサポートされていません。
- VSS 内の別個のシャーシにある 2 つのサービス モジュール間で行われるスイッチオーバーは、シャーシ間のスイッチオーバーと見なされます。

（注）　VSS モードのサービス モジュールの説明、制約事項、および注意事項の詳細については、サービス モジュールのコンフィギュレーション ガイドとコマンド リファレンスを参照してください。

仮想スイッチング システムについて

VSS の概要

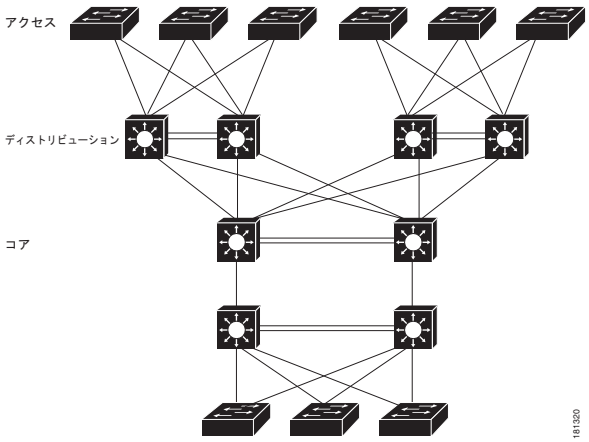
VSS トポロジ

スイッチを冗長ペアとして構成し、冗長ペアの両方のスイッチにリンクをプロビジョニングすることにより、ネットワークの信頼性を高めることができます。図 4-1 に、一般的なネットワーク構成を示します。冗長ネットワーク要素や冗長リンクにより、ネットワークの設計や操作が複雑になることがあります。仮想スイッチングを使用すると、ネットワーク要素の数が減り、複雑な冗長スイッチおよびリンクの管理が隠され、ネットワークが単純化されます。

VSS モードは、一対の Catalyst 6500 シリーズ スイッチを結合して、1 つのネットワーク要素にします。VSS モードによって管理される冗長リンクは、外部的には 1 つのポート チャネルとして機能します。

VSS モードは、レイヤ 3 のルーティング ネイバーの数を減らし、ループのないレイヤ 2 トポロジを構成することにより、ネットワークの構成と操作を単純化します。

図 4-1　　一般的なネットワーク設計



主要概念

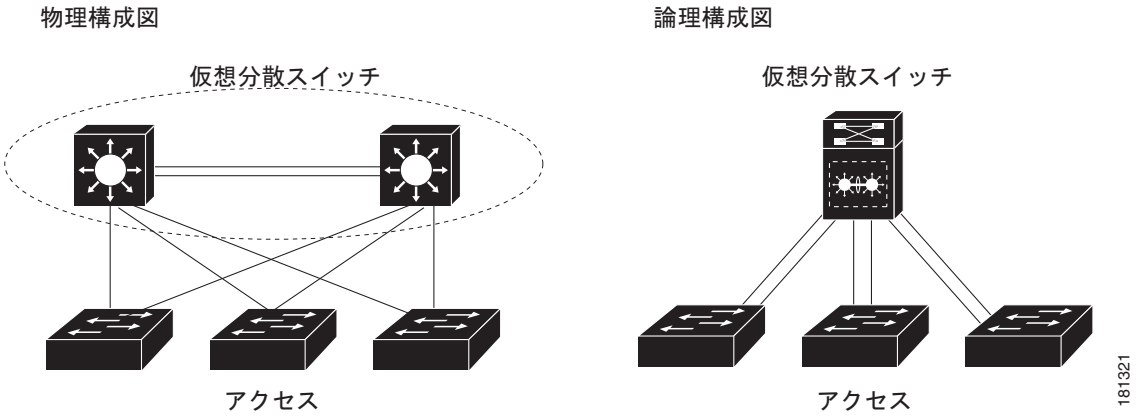
- 「仮想スイッチング システム」（P.4-5）
- 「アクティブ シャーシとスタンバイ シャーシ」（P.4-6）
- 「仮想スイッチ リンク」（P.4-7）
- 「マルチシャーシ EtherChannel（MEC）」（P.4-7）

仮想スイッチング システム

VSS は、一対のスイッチを結合して 1 つのネットワーク要素にします。たとえば、ネットワークのディストリビューション レイヤの VSS は、1 つのスイッチであるかのようにアクセス ネットワークおよびコア ネットワークとの通信を行います。図 4-2 を参照してください。

アクセス スイッチは、論理ポート チャネルを使用して、VSS の両方のシャーシと接続されます。VSS モードは、ポート チャネル上で冗長性とロード バランシングを管理します。この機能により、ループのないレイヤ 2 ネットワーク トポロジが構成可能になります。また、VSS モードでは、ネットワーク内のルーティング ピアの数も減らせるため、レイヤ 3 ネットワーク トポロジを単純化することもできます。

図 4-2　ディストリビューション ネットワークの VSS



アクティブ シャーシとスタンバイ シャーシ

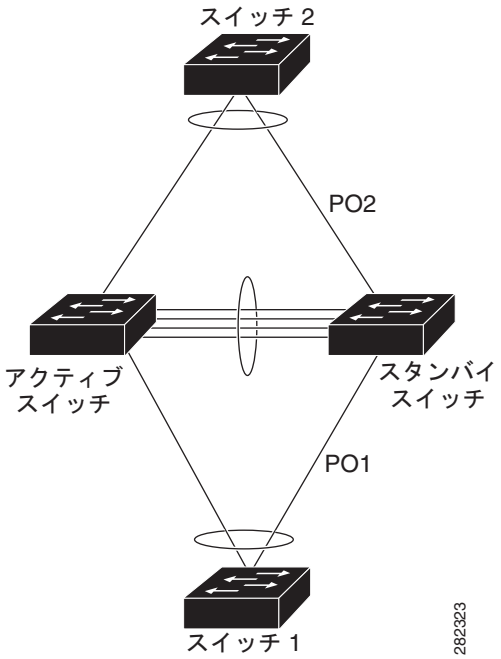
VSS の作成または再起動時、ピア シャーシ間でそのロールがネゴシエーションされます。一方のシャーシがアクティブ シャーシになり、他方のシャーシがスタンバイ シャーシになります。

アクティブ シャーシの方が、VSS の制御を行います。アクティブ シャーシで、両方のシャーシのスイッチング モジュールのためのレイヤ 2 およびレイヤ 3 制御プロトコルが実行されます。アクティブ シャーシは、モジュールの活性挿抜（OIR）やコンソール インターフェイスなど、VSS の管理機能も備えています。

アクティブ シャーシとスタンバイ シャーシは、ローカルにホスティングされたインターフェイス上で入力データ トラフィックのパケット転送を行います。ただし、スタンバイ シャーシは、処理のための制御トラフィックをアクティブ シャーシに送信します。

スタンバイ シャーシの起動中にトラフィックのリカバリ パフォーマンスに対処するために、マルチシャーシ EtherChannel（MEC）シャーシのトラフィック ロードを延期できます。たとえば、図 4-3 は、VSS（アクティブおよびスタンバイ スイッチ）がアップストリーム スイッチ（スイッチ 2）およびダウンストリーム スイッチ（スイッチ 1）と相互に動作しているネットワーク レイアウトを表します。

図 4-3　VSS によって相互接続されたスイッチ

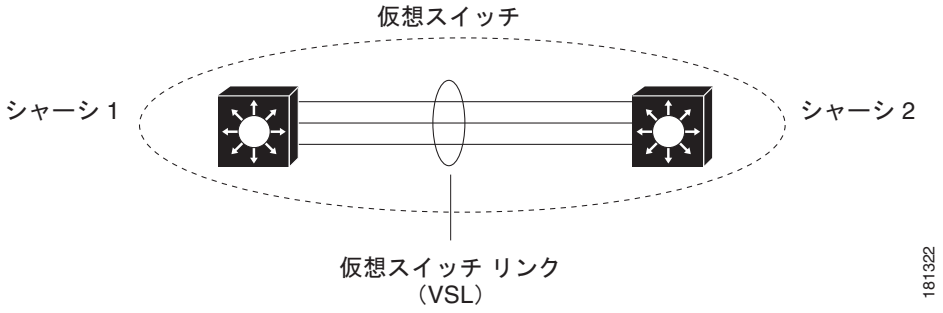


仮想スイッチ リンク

VSS の 2 つのシャーシが 1 つのネットワーク要素として機能するには、制御情報とデータ トラフィックを共有する必要があります。

仮想スイッチ リンク（VSL）は、VSS の 2 つのシャーシ間で制御トラフィックおよびデータ トラフィックをやりとりする特別なリンクです。図 4-4 を参照してください。VSL は、最大 8 つのリンクを持つ EtherChannel として実装されます。VSL では、制御メッセージが廃棄されないように、制御トラフィックにデータ トラフィックよりも高いプライオリティが割り当てられます。データ トラフィックは、EtherChannel ロードバランシング アルゴリズムにより、VSL リンク間でロードバランシングが行われます。

図 4-4　仮想スイッチ リンク



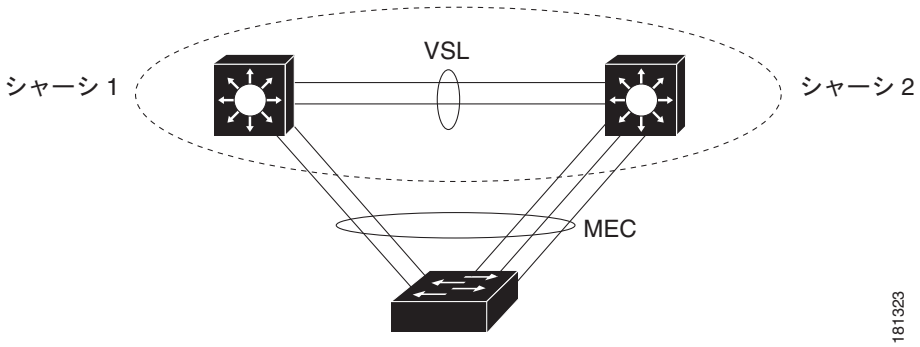
マルチシャーシ EtherChannel（MEC）

ポート チャネル インターフェイスで設定された EtherChannel は、1 つの論理リンクを形成するために結合する複数の物理的リンクです。レイヤ 2 プロトコルは、EtherChannel 上で 1 つの論理エンティティとして動作します。

MEC は、VSS の両方のシャーシのメンバ ポートがあるポート チャネルです。接続された非 VSS デバイスは、MEC を標準 EtherChannel として見なします。図 4-5 を参照してください。

VSS モードは最大 512 個の EtherChannel をサポートします。この制限値は、正規の EtherChannel と MEC を合わせた合計の数にも適用されます。VSL には 2 つの EtherChannel 番号（各シャーシに 1 つずつ）が必要であるため、ユーザが設定できる EtherChannel の数は 510 になります。内部 EtherChannel を使用するサービス モジュールも合計数に含まれます。

図 4-5　VSS と MEC



VSS の機能

冗長性とハイ アベイラビリティ

VSS モードでは、ステートフル スイッチオーバー（SSO）およびノンストップ フォワーディング（NSF）を使用して、アクティブ シャーシとスタンバイ シャーシの間でスーパーバイザ エンジンの冗長性が機能します。ピア シャーシは、VSL 全体で設定情報とステート情報を交換し、スタンバイ スーパーバイザ エンジンはホット スタンバイ モードで動作します。

スタンバイ シャーシは、VSL を使用してアクティブ シャーシをモニタします。障害を検出すると、スタンバイ シャーシがスイッチオーバーを開始し、アクティブ ロールを代行します。故障したシャーシが回復すると、スタンバイ ロールに戻ります。

VSL が完全に障害となると、スタンバイ シャーシはアクティブ シャーシが故障したと判断し、スイッチオーバーを開始します。スイッチオーバーのあと、両方のシャーシがアクティブになると、デュアル アクティブ検出機能によりこの状態が検出され、回復アクションが開始されます。デュアル アクティブ検出の詳細については、「デュアル アクティブ検出」（P.4-25）を参照してください。

パケット処理

アクティブ スーパーバイザ エンジンは、レイヤ 2 プロトコルおよびレイヤ 3 プロトコルと、VSS のための機能を実行し、両方のシャーシのためのドーター フィーチャ カード（DFC）モジュールを管理します。

VSS では、VSL を使用してピア シャーシ間でプロトコルおよびシステム情報を通信し、必要に応じてシャーシ間でデータ トラフィックをやりとりします。

両方のシャーシは、インターフェイス上で入力トラフィックのパケット転送を行います。可能であれば、VSL を通過するデータ トラフィックを低減するため、入力トラフィックが同じシャーシの出力インターフェイスに転送されます。

スタンバイ シャーシはアクティブにトラフィックを転送しているため、アクティブ スーパーバイザ エンジンはスタンバイ スーパーバイザ エンジン PFC とすべてのスタンバイ シャーシ DFC に更新情報を配信します。

システム管理

アクティブ スーパーバイザ エンジンは、VSS 制御のシングル ポイントとして機能します。たとえば、アクティブ スーパーバイザ エンジンは両方のシャーシのスイッチング モジュールの OIR を処理します。アクティブ スーパーバイザ エンジンは、VSL を使用して、スタンバイ シャーシのローカル ポートとの間で、メッセージの送受信を行います。

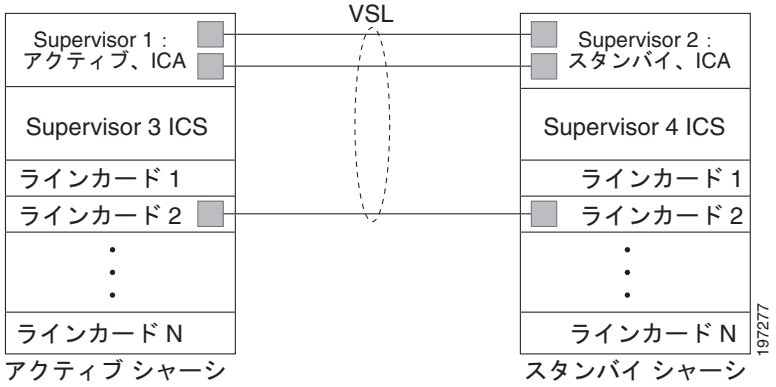
両方のシャーシを制御するため、アクティブ スーパーバイザ エンジンのコマンド コンソールが使用されます。仮想スイッチ モードでは、スタンバイ スーパーバイザ エンジン ブロックのコマンド コンソールがコンフィギュレーション モードの開始を試みます。

スタンバイ シャーシでは、システム管理タスクのサブセットが実行されます。たとえば、スタンバイ シャーシでは、それ自身の電源管理が行われます。

VSS Quad-Sup SSO（VS4O）

リリース 15.1(1) SY1 以降のリリースでは、VSS Quad-Sup SSO（VS4O）機能 をサポートしています。

図 4-6　　一般的な VSS クアッドスーパーバイザの設定



クアッドスーパーバイザ VSS には、次の役割があります。

- インシャーシ アクティブ（ICA）スーパーバイザ エンジン：1 台のシャーシに VSS アクティブ スーパーバイザ エンジンがあり、もう 1 台のシャーシに VSS スタンバイ スーパーバイザ エンジンがあるのが ICA スーパーバイザ エンジンです。

  ICA VSS アクティブ スーパーバイザ エンジンがクラッシュすると、もう 1 台のシャーシにあるスタンバイ ICA 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。両方の VSS シャーシが、アクティブなままです。すべてのスイッチング モジュールが、アクティブなままです。

これまでのアクティブ ICA スーパーバイザ エンジンを搭載したシャーシでは、これまでのアクティブ ICA スーパーバイザ エンジンから ICS スタンバイ スーパーバイザ エンジンへの SSO スイッチオーバーが発生し、ICS が ICA を引き継ぎます。故障した ICA がリロードされ、ICS 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 モードを確認するには、**show module** コマンドを入力します。

- インシャーシ スタンバイ（ICS）スーパーバイザ エンジン：もう 1 つのスーパーバイザ エンジンは、ICS スーパーバイザ エンジンです。このスーパーバイザ エンジンのアップリンク ポートは、トラフィック転送に使用できます。

（注） ICS スーパーバイザ エンジンは、**show** コマンドをサポートしていません。トレースバックを避けるため、ICS スーパーバイザ エンジンでは **show** コマンドを発行しないでください。

スーパーバイザ エンジンの PFC モードが一致しない場合は、ICS スーパーバイザ エンジンが ROMMON にリセットされます。同じ PFC モードで動作するように、両方のシャーシを設定します。

ICS スーパーバイザ エンジンは、SSO スタンバイ モードで起動します。これにより、ICS が完全に初期化および設定され、ステートフル機能とユーザ セッション情報が維持されます。

スーパーバイザ エンジンのスイッチオーバー モードを確認するには、**show module** コマンドを入力します。

VSS クアッド スーパーバイザ エンジン モードでないときに ICS となるスーパーバイザ エンジンを挿入すると、スーパーバイザ エンジン番号を更新するためにスーパーバイザ エンジンがリセットされ、リブートしてからオンラインになります。

クアッドスーパーバイザ SSO（VS4O）では、eFSU アップグレードをサポートしています。ISSU を使用して、VSS システムをアップグレードまたはダウングレードできます。eFSU アップグレードの詳細については、「VSS のアップグレード方法」（P.4-55）を参照してください。

インターフェイスの命名規則

VSS モードでは、両方のシャーシで同じスロット番号が使用されるため、インターフェイスは（スロットとポートのほかに）スイッチ番号を使用して指定されます。たとえば、**interface 1/5/4** コマンドは、スイッチ 1 のスロット 5 にあるスイッチング モジュールのポート 4 を指定しています。**interface 2/5/4** コマンドは、スイッチ 2 のスロット 5 にあるスイッチング モジュールのポート 4 を指定しています。

ソフトウェア機能

一部の例外はありますが、VSS モードには非 VSS モードとの機能パリティがあります。主要な例外は、次のとおりです。

- VSS モードは 1 つのシャーシ内でのスーパーバイザ エンジンの冗長性をサポートしていません。
- ポートベースの QoS および PACL は、VSL ポートを除くすべての物理ポートに適用できます。PACL は最大 2,046 ポートに適用できます。

ハードウェア要件

- 「シャーシとモジュール」（P.4-11）
- 「VSL のハードウェア要件」（P.4-11）

- 「PFC、DFC、および CFC の要件」（P.4-12）
- 「マルチシャーシ EtherChannel の要件」（P.4-12）
- 「サービス モジュールのサポート」（P.4-12）

シャーシとモジュール

表 4-1　VSS のハードウェア要件

ハードウェア	数	要件
シャーシ	2	Supervisor Engine 2T に対応しているすべてのシャーシは、Cisco IOS Release 15.1SY で VSS モードをサポートしています。 **（注）**　2 台のシャーシは、同じ機種である必要はありません。
スーパーバイザ エンジン	2	2 台の VS-SUP2T-10G または 2 台の VS-SUP2T-10G-XL スーパーバイザ エンジンのいずれか。 2 台のスーパーバイザ エンジンは、同一機種である必要があります。
スイッチング モジュール	2+	リリース ノートに示されている VSS モードのサポート。 VSS モードでは、サポートされていないスイッチング モジュールは電源がオフのままとなります。

VSL のハードウェア要件

VSL EtherChannel は、40 ギガビットおよび 10 ギガビット イーサネット ポートに限りサポートします。ポートは、スーパーバイザ エンジン（推奨）または次のいずれかのスイッチング モジュールに配置できます。

- WS-X6904-40G-2T
- WS-X6908-10GE
- WS-X6816-10T-2T、WS-X6716-10T
- WS-X6816-10G-2T、WS-X6716-10G

スーパーバイザ エンジンの両方の 10 ギガビット イーサネット ポートを使用して、2 つのシャーシ間で VSL を構成することを推奨します。

VSL をサポートするスイッチング モジュールの 40 ギガビットまたは 10 ギガビット イーサネット ポートを使用して、VSL EtherChannel に物理リンクを追加できます。

（注）

- VSL リンクとしてオーバーサブスクライブ モードで動作可能なスイッチング モジュールのポートを使用する場合、オーバーサブスクリプション モードではなく、パフォーマンス モードでポートを動作させる必要があります。スイッチング モジュールを設定する場合は、**no hw-module switch x slot y oversubscription port-group** *num* コマンドを入力してください。非オーバーサブスクリプション モード（パフォーマンス モード）を設定するために **no hw-module switch** *switch_number* **slot** *slot_number* **oversubscription** コマンドを入力する場合、ポート 1、5、9、および 13 だけが設定可能です。モジュール上のその他のポートはディセーブルになります。
- ポートグループは相互に独立しています。未使用ポートが管理上の理由でシャットダウンされているときに VSL の非オーバーサブスクライブ モードで 1 つ以上のポートグループが動作でき、その他のポートグループはそのままオーバーサブスクライブ モードで動作できます。

PFC、DFC、および CFC の要件

CFC、DFC4、または DFC4XL を搭載したスイッチング モジュールは、VSS モードをサポートします。

PFC4 を使用すると、一部のモジュールに DFC4XL が搭載されていても、VSS は PFC4 モードで自動的に動作します。PFC4XL を使用する場合、一部のモジュールに DFC4 が搭載されていると、PFC4 モードで動作するように VSS を設定する必要があります。**platform hardware vsl pfc mode non-xl** コンフィギュレーション コマンドを実行すると、次の再起動後に、システムが PFC4 モードで動作するよう設定されます。このコマンドの詳細については、「SSO の依存関係」（P.4-27）を参照してください。

マルチシャーシ EtherChannel の要件

CFC、DFC4、または DFC4XL を搭載したモジュールからの物理リンクは、マルチシャーシ EtherChannel（MEC）を実装するために使用できます。

サービス モジュールのサポート

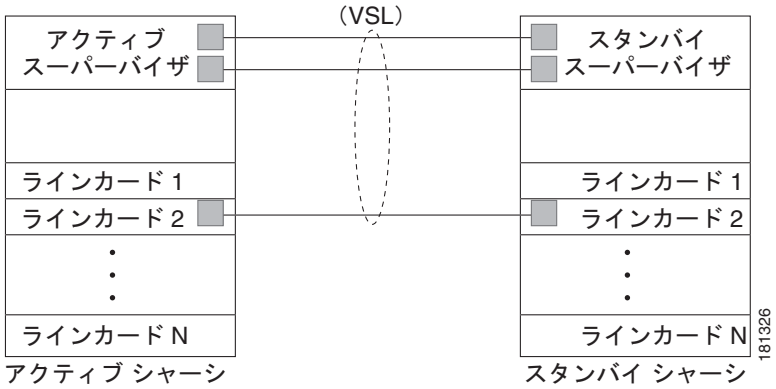
- Application Control Engine（ACE）：
  - ACE20-MOD-K9
  - ACE30-MOD-K9
- ASA サービス モジュール：WS-SVC-ASA-SM1-K9
- ファイアウォール サービス モジュール（FWSM）：WS-SVC-FWM-1-K9
- ネットワーク解析モジュール（NAM）：
  - WS-SVC-NAM-1
  - WS-SVC-NAM-2
  - WS-SVC-NAM3-6G-K9
- ワイヤレス サービス モジュール（WiSM）：
  - WS-SVC-WISM-1-K9
  - WS-SVC-WISM2

（注） サービス モジュールを VSS モードで導入する前に、そのモジュールを、最低限サポートされるリリースにスタンドアロン モードでアップデートしてください。最低限必要なサービス モジュールのソフトウェア バージョンについては、サービス モジュールのリリース ノートを参照してください。

VSL トポロジについて

VSS は、特殊なポート グループである VSL を使用して通信する 2 つのシャーシです。スーパーバイザ エンジンの両方の 10 ギガビット イーサネット ポートを VSL ポートとして設定します。または、任意でスイッチング モジュールの 40 または 10 ギガビット イーサネット ポートを含むように VSL ポート グループを構成することもできます。この構成では、VSL の能力が拡張されます。設定例のトポロジについては、図 4-7 を参照してください。

図 4-7　　VSL のトポロジ例



VSS の冗長性

概要

VSS では、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 エンジンの間でステートフル スイッチオーバー（SSO）が実行されます。スタンドアロン モードと比べた場合、VSS モードは冗長性モデルに次のような重要な違いがあります。

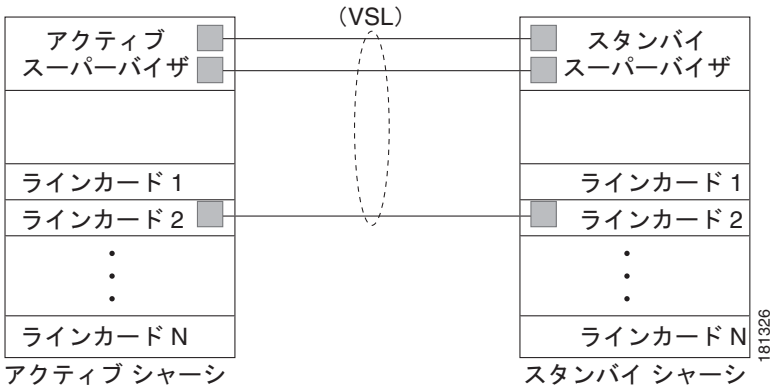
- アクティブ スーパーバイザ エンジンとスタンバイ スーパーバイザ エンジンは別のシャーシに配置され、VSL を使用して情報交換を行います。
- アクティブ スーパーバイザ エンジンが VSS の両方のシャーシの制御を行います。アクティブ スーパーバイザ エンジンで、レイヤ 2 およびレイヤ 3 制御プロトコルが実行され、両方のシャーシのスイッチング モジュールが管理されます。
- アクティブ シャーシとスタンバイ シャーシの両方がデータ トラフィックの転送を行います。

アクティブ スーパーバイザ エンジンが障害になると、スタンバイ スーパーバイザ エンジンがスイッチオーバーを開始し、アクティブ ロールを代行します。

RPR と SSO の冗長性

通常、VSS では、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 エンジンの間でステートフル スイッチオーバー（SSO）が実行されます（図 4-8 を参照）。初期化中に、VSS によって各スーパーバイザ エンジンのロールが決定されます。

図 4-8　VSS モード内のシャーシのロール



VSS は、VSL リンクを使用して、設定データをアクティブ 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 エンジンに同期させます。また、ハイ アベイラビリティをサポートしているプロトコルと機能により、スタンバイ スーパーバイザ エンジンに対してイベントやステート情報が同期されます。

VSS モードでは、次の要件を満たしている場合に、ステートフル スイッチオーバー（SSO）冗長性が機能します。

- 両方のスーパーバイザ エンジンで同じソフトウェア バージョンを実行していること。
- 2 台のシャーシ間で VSL 関連の設定が一致していること。
- PFC モードが一致していること。
- SSO とノンストップ フォワーディング（NSF）が両方のシャーシで設定されていること。

VSS での SSO 冗長性の要件に関する詳細については、「SSO の依存関係」（P.4-27）を参照してください。SSO および NSF の設定については、第 8 章「Nonstop Forwarding（NSF）」を参照してください。

SSO 冗長性では、スタンバイ シャーシのスーパーバイザ エンジンは、ホット スタンバイ ステートで実行され、アクティブ スーパーバイザ エンジンで障害が発生した場合に、制御を代行できるよう常にスタンバイ状態になっています。設定情報、転送情報、ステート情報は、起動時やアクティブ スーパーバイザ エンジンの設定が変更されたときに、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。スイッチオーバー発生時のトラフィックの中断は最小限に抑えられます。

VSS が SSO 冗長性の要件を満たしていない場合、その VSS では Route Processor Redundancy（RPR）が使用されます。RPR モードでは、アクティブ スーパーバイザ エンジンは、設定変更やステート情報をスタンバイ スーパーバイザ エンジンと同期しません。スタンバイ スーパーバイザ エンジンは一部だけが初期化され、スタンバイ スーパーバイザ エンジンのスイッチング モジュールは起動されません。スイッチオーバーが発生すると、スタンバイ スーパーバイザ エンジンの初期化が最後まで行われ、スイッチング モジュールが起動されます。トラフィックは、約 2 分間中断します。

障害が発生したシャーシの回復

アクティブ シャーシまたはスーパーバイザ エンジンが障害になると、VSS はステートフル スイッチオーバー（SSO）を開始し、スタンバイ状態であったスーパーバイザ エンジンがアクティブ ロールを代行します。障害が発生したシャーシは、スーパーバイザ エンジンをリロードすることにより、回復アクションを実行します。

スタンバイ シャーシまたはスーパーバイザ エンジンが障害となった場合、スイッチオーバーは不要です。障害が発生したシャーシは、スーパーバイザ エンジンをリロードすることにより、回復アクションを実行します。

障害が発生したシャーシの回復処理中は、VSL は利用できません。リロードを完了したシャーシは新しいスタンバイ シャーシとなり、VSS は 2 台のシャーシ間で VSL の再初期化を行います。

回復処理中は、障害となったシャーシのスイッチング モジュールを使用できないため、VSS はアクティブ シャーシで終端する MEC リンクだけで動作します。VSS の帯域幅は、障害が発生したシャーシの回復処理が完了して動作可能となるまで、縮小されます。障害が発生したシャーシだけに接続されているデバイスは、停止します。

（注）　SSO 後にスタンバイ シャーシのスイッチング モジュールが動作可能になったとき、VSS で一時的にデータ パスの中断が発生することがあります。

SSO のあと、アクティブ スーパーバイザ エンジンの処理能力の大半は、スタンバイ シャーシの多くのポートを同時に起動することに消費されます。その結果、スーパーバイザ エンジンがリンクの転送を設定する前に、一部のリンクが起動することがあります。これにより、これらのリンクへのトラフィックは、設定が完了するまで消失します。リンクが MEC リンクの場合、この状態は特に混乱を招きます。SSO のあとに起こるデータの中断は、次の 2 つの方法で低減できます。

- 同時にすべてのポートをアクティブにするのではなく、小さいグループの非 VSL ポートを一定時間アクティブにするように VSS を設定できます。ポートのアクティブ化の遅延については、「スタンバイ回復時のポートのアクティブ化遅延の設定」（P.4-46）を参照してください。
- ポート接続の再確立中は、ピア スイッチの MEC メンバ ポートのロード シェアリングを延期することができます。ロード シェアリングの延期については、「障害が発生したシャーシ MEC の回復」（P.4-18）を参照してください。

VSL の障害

VLS 障害からの迅速な回復を保証するために、ハードウェアが高速リンク通知をサポートしているすべてのポート チャネル メンバ（VSL ポートを含む）上で、仮想スイッチ モードの高速リンク通知がイネーブルになります。

（注）　高速リンク通知は、リンク デバウンス メカニズムとの互換性はありません。仮想スイッチ モードでは、リンク デバウンスは、すべてのポート チャネル メンバ上でディセーブルです。

1 つの VSL 物理リンクがダウンした場合、VSS はポート グループを調整し、障害となったリンクが選択されないようにします。

スタンバイ シャーシで完全な VSL リンク障害が検出された場合、ステートフル スイッチオーバー（SSO）が開始されます。アクティブ シャーシが障害となっている場合（VSL リンクのダウンが発生）は、前のセクションで説明したように、シャーシの障害時の処理が行われます。

VSL だけが障害となって、アクティブ シャーシは正常に動作している場合、デュアル アクティブ シナリオとなります。VSS で、両方のシャーシがアクティブ モードで動作していることが検出され、回復アクションが実行されます。デュアル アクティブ シナリオの詳細については、「デュアル アクティブ検出」（P.4-25）を参照してください。

ユーザ アクション

アクティブ シャーシのコマンド コンソールから、VSS のスイッチオーバーまたはリロードを開始できます。

コマンド コンソールで **reload** コマンドを入力すると、VSS 全体のリロードが実行されます。

スタンバイ シャーシだけのリロードを行う場合は、**redundancy reload peer** コマンドを使用します。

スーパーバイザ エンジンをアクティブからスタンバイに強制的に切り替えるには、**redundancy force-switchover** コマンドを使用します。

VSS スタンバイ スーパーバイザ エンジンをリセットするか、VSS アクティブ スーパーバイザ エンジンと VSS スタンバイ スーパーバイザ エンジンの両方をリセットするには、**redundancy reload shelf** コマンドを使用します。

マルチシャーシ EtherChannel

概要

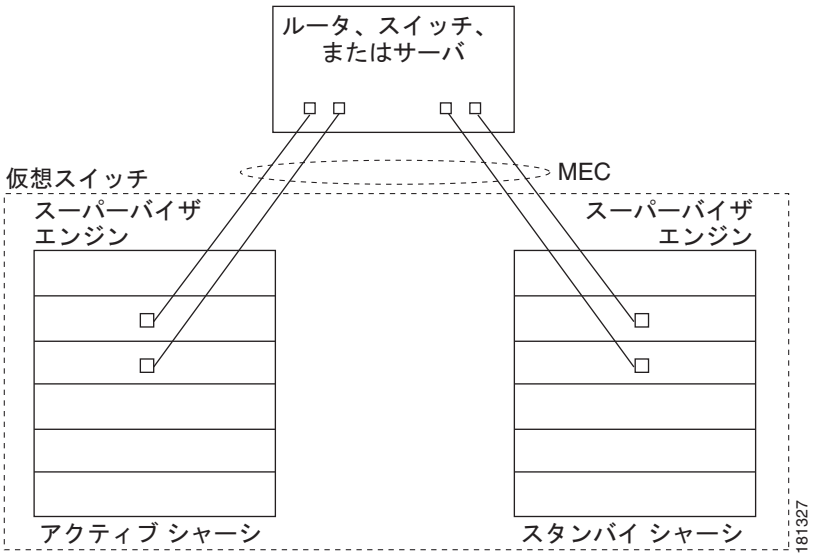
マルチシャーシ EtherChannel は、VSS の両方のシャーシで終端するポートが搭載された EtherChannel です（図 4-9 を参照）。VSS MEC は、EtherChannel をサポートしているネットワーク要素（ホスト、サーバ、ルータ、スイッチなど）に接続できます。

VSS では、MEC は追加機能を持った EtherChannel であり、VSS は独立して各シャーシのポート全体のロードバランシングを行います。たとえば、アクティブ シャーシにトラフィックが到着すると、VSS はアクティブ シャーシの中から MEC リンクを選択します。MEC 機能により、データ トラフィックが不必要に VSL を通過しないよう制御できます。

Port Aggregation Protocol（PAgP）または Link Aggregation Control Protocol（LACP）をサポートするように各 MEC を設定することもできます。これらのプロトコルは、アクティブ シャーシ上でだけ動作します。スタンバイ シャーシの MEC リンクを宛先とする PAgP または LACP 制御パケットは、VSL を通って送信されます。

MEC では、最大 8 つのアクティブ物理リンクをサポートでき、これらのリンクをアクティブ シャーシとスタンバイ シャーシに任意の比率で分散させることができます。

図 4-9　MEC トポロジ



MEC 障害シナリオ

（注）　各シャーシに少なくとも 1 個のリンクを MEC に設定します。この構成により、VSL 帯域幅が確保され（トラフィックの出力リンクが入力リンクと同じシャーシ上に存在）、ネットワークの信頼性が向上します（一方の VSS スーパーバイザ エンジンに障害が発生しても、MEC は動作可能）。

単一 MEC リンクの障害

MEC 内のリンクに障害が発生した（そして MEC 内の別のリンクは動作している）場合、通常のポートと同様に、MEC は動作しているリンク間でロード バランシングを再調整します。

アクティブ シャーシへのすべての MEC リンクの障害

アクティブ シャーシへのすべてのリンクが障害となった場合、MEC はスタンバイ シャーシへの動作可能なリンクを持つ通常の EtherChannel となります。

アクティブ シャーシで終端するデータ トラフィックは、スタンバイ シャーシへの VSL を通って MEC に到達します。制御プロトコルは、アクティブ シャーシで動作を続行します。プロトコル メッセージは、VSL を通って MEC に到達します。

スタンバイ シャーシへのすべての MEC リンクの障害

スタンバイ シャーシへのすべてのリンクが障害となった場合、MEC はアクティブ シャーシへの動作可能なリンクを持つ通常の EtherChannel となります。

制御プロトコルは、アクティブ シャーシで動作を続行します。スタンバイ シャーシからのすべての制御トラフィックおよびデータ トラフィックは、アクティブ シャーシへの VSL を通って MEC に到達します。

すべての MEC リンクの障害

MEC 内のすべてのリンクに障害が発生した場合、EtherChannel の論理インターフェイスが unavailable に設定されます。レイヤ 2 制御プロトコルは、通常の EtherChannel のリンク ダウン イベントと同様の修正措置を実行します。

隣接スイッチでは、ルーティング プロトコルとスパニングツリー プロトコル（STP）により、通常の EtherChannel と同様の修正措置が実行されます。

スタンバイ シャーシの障害

スタンバイ シャーシが障害となった場合、MEC はアクティブ シャーシ上の動作可能なリンクを持つ通常の EtherChannel となります。接続されているピア スイッチにより、リンクの障害が検出され、アクティブ シャーシへのリンクだけを使用するようにロード バランシング アルゴリズムが調整されます。

アクティブ シャーシの障害

アクティブ シャーシが障害となった場合、ステートフル スイッチオーバー（SSO）が実行されます。VSS での SSO の詳細については、「VSS の冗長性」（P.4-13）を参照してください。スイッチオーバーの完了後、MEC は新しいアクティブ シャーシで動作可能になります。接続されているピア スイッチにより、（障害となったシャーシへの）リンクの障害が検出され、新しいアクティブ シャーシへのリンクだけを使用するようにロード バランシング アルゴリズムが調整されます。

障害が発生したシャーシ MEC の回復

障害となったシャーシが新しいスタンバイ シャーシとして動作状態に戻る場合、プロトコル メッセージによって、回復したシャーシと接続先ピア スイッチ間の MEC リンクが確立されます。

回復したシャーシの MEC リンクは、ただちにピア スイッチからユニキャスト トラフィックを受信できる状態になりますが、受信したマルチキャスト トラフィックは、数秒～数分間消失する場合があります。こうしたトラフィックの消失を低減するには、ピア スイッチの MEC ポート チャネルでポートのロード シェアリング延期機能を設定します。ロード シェアリング延期が設定されると、ピアの延期された MEC ポート チャネルは、最初のロード シェアリング 0 を使用して確立されます。設定された延期期間中、ピアの延期されたポート チャネルは、データの受信、トラフィックの制御、および制御トラフィックの送信はできますが、VSS にデータ トラフィックを転送できません。ポートのロード シェアリング延期の設定については、「ピア スイッチでのロード シェアリング延期の設定」（P.4-47）を参照してください。

パケット処理

パケット処理の概要

VSS モードでは、アクティブ スーパーバイザ エンジンは、レイヤ 2 プロトコルおよびレイヤ 3 プロトコルと、VSS のための機能を実行し、両方のシャーシのための DFC モジュールを管理します。

VSS では、VSL を使用してピア シャーシ間でシステムおよびプロトコル情報を通信し、2 台のシャーシ間でデータ トラフィックを伝送します。

両方のシャーシは、ローカル インターフェイス上で入力トラフィックのパケット転送を行います。VSS モードでは、VSL を通過するデータ トラフィックの量が最小限に抑えられます。

VSL のトラフィック

VSL では、2 台のシャーシ間のデータ トラフィックとインバンド制御トラフィックが送信されます。VSL リンク上を送信されるすべてのフレームは、特殊な 32 バイトのヘッダーでカプセル化されます。このヘッダーには、VSS でピア シャーシ上のパケット転送を行うための情報が記述されます。

VSL は、2 台のシャーシの間の制御メッセージを送信します。メッセージには、処理はアクティブ スーパーバイザ エンジンで行われますが、スタンバイ シャーシのインターフェイスで送受信されるプロトコル メッセージも含まれます。制御トラフィックには、アクティブ スーパーバイザ エンジンとスタンバイ シャーシのスイッチング モジュールの間のモジュール プログラミングも含まれます。

VSS は、次の状況のとき、VSL 上でデータ トラフィックを送信する必要があります。

- VLAN 上でレイヤ 2 トラフィックのフラッディングが発生しているとき（デュアル ホーム リンクの場合でも）
- 入力インターフェイスがスタンバイ シャーシ上にあるアクティブ スーパーバイザ エンジンのソフトウェアでパケットが処理されているとき
- 次のように、パケットの宛先がピア シャーシ上にあるとき
  - 既知の宛先インターフェイスがピア シャーシ上にある VLAN 内のトラフィック
  - マルチキャスト グループおよびマルチキャスト レシーバのために複製されたトラフィックがピア シャーシ上にある場合
  - 既知のユニキャスト宛先 MAC アドレスがピア シャーシ上にある場合
  - パケットが、ピア シャーシ上のポートを宛先とする MAC 通知フレームである場合

VSL では、NetFlow エクスポート データや SNMP データなどのシステム データも、スタンバイ シャーシからアクティブ スーパーバイザ エンジンに送信されます。

重要な機能のために VSL 帯域幅を確保するため、VSS では、VSL を必ず通過するユーザ データのトラフィックを最小限に抑えるよう規定されています。たとえば、アクセス スイッチがデュアル ホームである（両方の VSS シャーシに MEC 終端が設置されている）場合、VSS は、同じシャーシ上のリンクを入力リンクとして使用して、パケットをアクセス スイッチに送信します。

VSL のトラフィックは、EtherChannel で利用できるのと同じグローバル ハッシュ アルゴリズム（デフォルトのアルゴリズムは送信元/宛先 IP）に基づいてロード バランシングされます。

レイヤ 2 プロトコル

レイヤ 2 プロトコルの概要

アクティブ スーパーバイザ エンジンはで、両方のシャーシのスイッチング モジュールを管理するため、レイヤ 2 プロトコル（STP や VTP など）が実行されます。スタンバイ シャーシのスイッチング モジュールで送受信されるプロトコル メッセージは、VSL を通してアクティブ スーパーバイザ エンジンに到達する必要があります。

スパニングツリー プロトコル

アクティブ シャーシでは、スパニングツリー プロトコル（STP）が実行されます。スタンバイ シャーシは、VSL を通して STP BPDU をアクティブ シャーシにリダイレクトします。

通常、STP ブリッジ ID はシャーシの MAC アドレスから導出されます。スイッチオーバー後もブリッジ ID が変わらないように、VSS は元のシャーシの MAC アドレスを STP ブリッジ ID として使い続けます。

仮想トランク プロトコル

仮想トランク プロトコル（VTP）では、アドバタイズメントのバージョン制御用に、スイッチの IP アドレスとローカルの現在時刻を使用します。スイッチオーバーの完了後、VTP は新しいアクティブ シャーシの IP アドレスを使用します。

EtherChannel 制御プロトコル

Link Aggregation Control Protocol（LACP）パケットとポート集約プロトコル（PAgP）パケットには、デバイス ID が組み込まれます。VSS では、両方のシャーシで使用する共通のデバイス ID が定義されます。

デュアル アクティブ シナリオ検出をサポートするため、新しい PAgP 拡張が定義されています。詳細は、「デュアル アクティブ検出」（P.4-25）を参照してください。

マルチキャスト プロトコル

リリース 15.1(1)SY1 以降のリリースでは、Fast-redirect 最適化により、メンバー ポート リンクの障害と回復の場合に、レイヤ 2 トランクおよびレイヤ 3 マルチシャーシ EtherChannel または分散 EtherChannel についてシャーシ間またはシャーシ内ラインカードの間のマルチキャスト トラフィック リダイレクションが高速になります。これが行われるのは、主にメンバ ポート リンクがダウンした場合（ポートが EtherChannel を脱退した場合）と、メンバ ポート リンクがアップした場合（ポートが EtherChannel に加入または再加入した場合）です。Fast-redirect は、設定の変更のため、またはシステム起動時にメンバー ポートの追加または取り外しを行った場合には有効になりません。

レイヤ 3 プロトコル

レイヤ 3 プロトコルの概要

アクティブ スーパーバイザ エンジンの RP では、レイヤ 3 プロトコルと VSS 用の機能が実行されます。両方のシャーシは、インターフェイス上で入力トラフィックのパケット転送を行います。可能であれば、VSL を必ず通過するデータ トラフィックを低減するため、入力トラフィックが同じシャーシの出力インターフェイスに転送されます。

スタンバイ シャーシはアクティブにトラフィックを転送しているため、アクティブ スーパーバイザ エンジンはスタンバイ スーパーバイザ エンジン PFC とすべてのスタンバイ シャーシ DFC に更新情報を配信します。

IPv4

アクティブ シャーシのスーパーバイザ エンジンでは、IPv4 ルーティング プロトコルが実行され、必要なソフトウェア転送が行われます。

スタンバイ シャーシで受信したルーティング アップデートは、VSL を通してアクティブ シャーシにリダイレクトされます。

ハードウェア転送は、VSS のすべての DFC に配信されます。アクティブ シャーシのスーパーバイザ エンジンは、FIB アップデートを、すべてのローカル DFC、リモート DFC、およびスタンバイ スーパーバイザ エンジン PFC に送信します。

すべてのハードウェア ルーティングでは、アクティブ スーパーバイザ エンジンによって割り当てられたルータ MAC アドレスが使用されます。スイッチオーバー後も、元の MAC アドレスが使用されます。

（IPX などのプロトコルの）ソフトウェア転送と（フラグメンテーションや TTL 超過などの）機能実行はすべて、アクティブ シャーシのスーパーバイザで行われます。スイッチオーバーが発生すると、新しいアクティブ スーパーバイザ エンジンが最新の CEF 情報や他の転送情報などを取得するまで、ソフトウェア転送は中断します。

仮想スイッチ モードで Non-Stop Forwarding（NSF）をサポートするための要件は、スタンドアロン モードの場合と同様です。第 8 章「Nonstop Forwarding（NSF）」を参照してください。

ルーティング ピアの観点では、EtherChannel はスイッチオーバーの処理中も動作可能です（障害となったシャーシへのリンクがダウンするだけ）。

VSS では、FIB エントリにローカル パス（VSL を通らないパス）だけを保存することにより、パス フィルタリングを実装します。そのため、IP 転送は、ローカル パス間でロード シェアリングを実行します。所定の宛先への利用可能なローカル パスがない場合、VSS はリモート パス（VSL を通って到達可能）を追加するよう FIB エントリをアップデートします。

IPv6、MPLS、および VPLS

VSS は IPv6 ユニキャスト、MPLS、および VPLS をサポートします。

IPv4 マルチキャスト

IPv4 マルチキャスト プロトコルは、アクティブ スーパーバイザ エンジン上で実行されます。スタンバイ スーパーバイザ エンジンで受信したインターネット グループ管理プロトコル（IGMP）および Protocol Independent Multicast（PIM）プロトコル パケットは、VSL を通してアクティブ シャーシに送信されます。

アクティブ スーパーバイザ エンジンは、ステートフル スイッチオーバー（SSO）のためのレイヤ 2 情報を維持するために、スタンバイ スーパーバイザ エンジンに IGMP および PIM プロトコル パケットを送信します。

アクティブ スーパーバイザ エンジンは、スタンバイ スーパーバイザ エンジンとスイッチング モジュール DFC に、マルチキャスト FIB と隣接関係テーブルのアップデートを配信します。

VSS のレイヤ 3 マルチキャストの場合、学習されたマルチキャスト ルートはスタンバイ スーパーバイザ エンジンのハードウェアに保存されます。スイッチオーバー後、マルチキャスト転送は既存のハードウェア エントリを使用して継続されます。

（注）　スイッチオーバーによってマルチキャスト ルートが変更されるのを避けるために、マルチキャスト トラフィックを伝送するすべてのリンクは Equal Cost Multipath（ECMP）ではなく MEC として設定することを推奨します。

仮想スイッチ モードでは、アクティブ シャーシはスタンバイ シャーシのマルチキャスト拡張テーブル（MET）をプログラムしません。スタンバイ スーパーバイザ エンジンが、すべてのローカル マルチキャスト レシーバの出力インターフェイスのハードウェア エントリをプログラムします。

アクティブ シャーシとスタンバイ シャーシのすべてのスイッチング モジュールが出力可能である場合、マルチキャスト複製モードが出力モードに設定されます。そうでない場合、モードは入力モードに設定されます。

出力レプリケーション モードでは、複製は、特定のフローのための出力 VLAN ポートを持つ DFC に配信されます。入力モードでは、すべての発信 VLAN のための複製が、入力 DFC で行われます。

VSL を通るパケットのために、入力シャーシですべてのレイヤ 3 マルチキャストの複製が行われます。出力シャーシに複数のレシーバがある場合、複製されたパケットが VSL 上で転送されます。

ソフトウェア機能

ソフトウェア機能は、アクティブ スーパーバイザ エンジン上だけで実行されます。ソフトウェア処理の必要なスタンバイ シャーシへの着信パケットは、VSL を通して送信されます。

ハードウェアでサポートされる機能のために、ACL 設定がアクティブ スーパーバイザ エンジン、スタンバイ スーパーバイザ エンジン、およびすべての DFC 上の TCAM マネージャに送信されます。

VSS での SPAN のサポート

VSS では、VSL 以外のインターフェイス用に、すべての SPAN 機能がサポートされます。VSS では、VSL インターフェイスでの SPAN 機能もサポートされていますが、次の制限があります。

- VSL ポートは、SPAN 宛先に設定できません。
- VSL ポートは、RSPAN、ERSPAN、または出力専用 SPAN 送信元に設定できません。
- VSL ポートがローカル SPAN 送信元として設定されている場合、SPAN 宛先インターフェイスは送信元インターフェイスと同じシャーシ上になければなりません。
- SPAN のコピーは、常に入力ポートが配置されているシャーシで作成されます。
- 2 つの VSL が同じ SPAN セッションを共有できません。

- LTL インデックスのペアは、VSL インターフェイス上の重複した SPAN のコピーを回避するために使用されます。

VSS で利用可能な SPAN セッションの数は、スタンドアロン モードで動作するシングル シャーシの場合と同様です。

SPAN 送信元としての VSL ポートでは、次の制約事項が適用されます。

- SPAN 宛先は、同じシャーシにある必要があります。
- ポート チャネル インターフェイスは、SPAN 宛先に設定できません。

システム モニタリング

電源管理

アクティブ シャーシからスタンバイ シャーシの電源関連の機能を制御できます。たとえば、**(no) power enable switch** コマンドを使用すると、スタンバイ シャーシのモジュールおよびスロットの電源を管理できます。**show power switch** コマンドを使用すると、現在の電源の設定およびステータスを確認できます。

環境モニタ

環境モニタリングは、両方のスーパーバイザ エンジンで実行されます。スタンバイ シャーシは、アクティブ スーパーバイザ エンジンに通知をレポートします。アクティブ シャーシは、両方のシャーシのログ メッセージを収集します。アクティブ シャーシは、カレンダーとシステム クロックをスタンバイ シャーシと同期させます。

ファイル システムへのアクセス

アクティブ シャーシから、両方のシャーシのファイル システムにアクセスできます。スタンバイ シャーシのディレクトリにアクセスするには、デバイス名の先頭にスイッチ番号とスロット番号を付加します。たとえば、**dir sw2-slot6-disk0** コマンドを使用すると、スタンバイ シャーシの disk0 の内容が表示されます（スイッチ 2 をスタンバイ シャーシと仮定）。スタンバイ シャーシのファイル システムへのアクセスは、VSL が動作可能状態である場合だけ可能です。

診断

VSS で **diagnostic schedule** コマンドと **diagnostic start** コマンドを使用できます。仮想スイッチ モードでこれらのコマンドを使用するには、パラメータとして、コマンドの適用先となるシャーシを指定する必要があります。

スイッチング モジュールまたはスーパーバイザ エンジン モジュールの VSL ポートを設定するとき、診断スイートに VSL ポートのための追加テストが組み込まれます。

モジュール用の診断テスト スイートを表示するには、**show diagnostic content** コマンドを使用します。

VSL の診断

次の VSL 固有の診断テストは中断を伴います。

- TestVSActiveToStandbyLoopback
- TestVslBridgeLink
- TestVslLocalLoopback

スイッチング モジュールまたはスーパーバイザ エンジンの VSL ポートでは、次の VSL 固有の診断テストが利用できます。これは中断を伴わないテストです。

- TestVslStatus

サービス モジュール

次のシステム モニタリングおよびシステム管理の注意事項が、VSS モードでサポートされるサービス モジュールに適用されます。

- サービス モジュールと同じシャーシのスーパーバイザ エンジンが、サービス モジュールの電源投入を制御します。サービス モジュールがオンラインになったあと、アクティブ スーパーバイザ エンジンからサービス モジュールへのセッションを開始できます。
- サービス モジュールに接続するには、**session** コマンドを使用します。サービス モジュールがスタンバイ シャーシにある場合、セッションは VSL を通して行われます。
- アクティブ シャーシは、スタンバイ シャーシを含むすべてのサービス モジュールのグレースフル シャットダウンを実行します。

ネットワーク管理

- 「Telnet over SSH セッションおよびブラウザ ユーザ インターフェイス」（P.4-24）
- 「SNMP」（P.4-24）
- 「コンソール接続」（P.4-25）

Telnet over SSH セッションおよびブラウザ ユーザ インターフェイス

VSS モードでは、Telnet over SSH セッションおよび Cisco Web ブラウザ ユーザ インターフェイスを使用したリモート アクセスがサポートされています。

リモート アクセスはすべてアクティブ スーパーバイザ エンジンに向けられ、ここで VSS が管理されます。

VSS のスイッチオーバーは、Telnet over SSH セッションおよび Web ブラウザ セッションを切断します。

SNMP

SNMP エージェントは、アクティブ スーパーバイザ エンジン上で実行されます。
CISCO-VIRTUAL-SWITCH-MIB は VSS モードの MIB で、次の主要コンポーネントで構成されています。

- cvsGlobalObjects：ドメイン番号、スイッチ番号、スイッチ モード
- cvsCoreSwitchConfig：スイッチのプライオリティ
- cvsChassisTable：シャーシのロールと動作ステート
- cvsVSLConnectionTable：VSL ポート カウント、動作ステート
- cvsVSLStatsTable：総パケット数、総エラー パケット数
- cvsVSLPortStatsTable：TX/RX 正常、不正、双方向および単一方向パケット

コンソール接続

両方のスーパーバイザ エンジンのコンソール ポートにケーブル接続します。スタンバイ シャーシのコンソールは、文字「-stdby」をコマンドライン プロンプトに追加して、シャーシがスタンバイ モードで動作していることを示します。スタンバイ シャーシのコンソールは、コンフィギュレーション モードにできません。

次に、スタンバイ コンソールのプロンプトの例を示します。

```
Router-stdby> show switch virtual

Switch mode                  : Virtual Switch
Virtual switch domain number : 100
Local switch number          : 1
Local switch operational role: Virtual Switch Standby
Peer switch number           : 2
Peer switch operational role : Virtual Switch Active
```

デュアル アクティブ検出

デュアル アクティブ検出の概要

VSL が障害となると、スタンバイ シャーシでは、アクティブ シャーシの状態を検出できません。スイッチオーバーが遅延なく行われるように、スタンバイ シャーシはアクティブ シャーシが障害になったと判断し、スイッチオーバーを開始してアクティブ ロールを代行します。

元のアクティブ シャーシも正常に動作している場合、両方のシャーシがアクティブ状態になります。この状況を、*デュアル アクティブ シナリオ*と呼びます。デュアル アクティブ シナリオでは、両方のシャーシで同じ IP アドレス、SSH キー、および STP ブリッジ ID が使用されるため、ネットワークの安定性に悪影響を及ぼすことがあります。VSS は、デュアル アクティブ シナリオを検出し、回復アクションを実行する必要があります。

VSS では、デュアル アクティブ シナリオを検出するために、次の 2 種類の方法がサポートされています。

- Enhanced PAgP：MEC リンク上で PAgP メッセージングを使用し、ネイバー スイッチを通して 2 台のシャーシ間の通信を行います。
- dual-active fast-hello：バックアップ イーサネット接続で特殊な hello メッセージを使用します。

両方の検出方法を同時にアクティブにするように設定できます。

回線の冗長性を維持するには、スイッチごとに少なくとも 2 つのポートをデュアル アクティブ検出用に設定することを推奨します。モジュールの冗長性を維持するために、2 つのポートを、各シャーシ内の異なるスイッチング モジュール上に配置できます。可能であれば、VSL リンク以外の異なるモジュールに配置してください。

拡張 PAgP を使用したデュアル アクティブ検出

VSS MEC が Cisco スイッチで終端する場合、MEC のポート集約プロトコル（PAgP）を実行できます。拡張 PAgP が VSS と Release 12.2(33)SXH1 以降のリリースを実行する別のスイッチの間の MEC で実行されている場合、VSS は拡張 PAgP を使用してデュアル アクティブ シナリオを検出できます。

MEC は、VSS の各シャーシに少なくとも 1 つのポートを持っている必要があります。VSS モードでは、PAgP メッセージには、VSS アクティブ スイッチの ID を含む新しい Type Length Value（TLV）が記述されます。VSS モードのスイッチだけが新しい TLV を送信します。

VSS スタンバイ シャーシで VSL の障害が検出された場合、SSO が開始され、そのシャーシは VSS アクティブになります。それ以降、新しく VSS アクティブになったシャーシから接続先スイッチに送信される PAgP メッセージには、新しい VSS アクティブ ID が記述されます。接続先スイッチは、新しい VSS アクティブ ID が記述された PAgP メッセージを、両方の VSS シャーシに送信します。

前にアクティブであったシャーシが動作可能な状態である場合、PAgP メッセージ内のアクティブ ID が変更されているため、デュアル アクティブ シナリオを検出します。このシャーシは、「回復アクション」（P.4-26）に示す要領で、回復アクションを開始します。

dual-active fast hello パケットを使用したデュアル アクティブ検出

dual-active fast hello パケット検出方式を使用するには、2 台の VSS シャーシ間の直接イーサネット接続をプロビジョニングする必要があります。最大 4 つの非 VSL リンクをこの目的に使用できます。

2 台のシャーシは、スイッチ ステートに関する情報が記述された、特殊なレイヤ 2 dual-active hello メッセージを定期的に交換します。VSL が障害となり、デュアル アクティブ シナリオが発生すると、各スイッチはピアのメッセージから、デュアル アクティブ シナリオがあることを認識し、「回復アクション」（P.4-26）に示すリカバリ アクションを開始します。タイマーの期限が満了するまでに、予想していた dual-active fast hello メッセージをピアから受信しなかった場合、スイッチはリンクがデュアル アクティブ検出を実行できる状態にないと見なします。詳細については、「拡張 PAgP デュアル アクティブ検出の設定」（P.4-48）を参照してください。

回復アクション

デュアル アクティブ状態を検出するアクティブ シャーシは、自身をネットワークから削除するためにすべての非 VSL インターフェイス（シャットダウンから除外するよう設定されたインターフェイスを除く）をシャットダウンし、VSL リンクが回復するまで回復モードで待機します。VSL の障害を物理的に修理する必要がある場合があります。シャットダウン シャーシで VSL が再び動作可能であることが検出されると、そのシャーシはリロードを実行し、スタンバイ シャーシとして動作状態に戻ります。

ループバック インターフェイスも、回復モードでシャットダウンされます。回復モードで設定された新しいループバック インターフェイスはシャット ダウンされないため、回復モードでループバック インターフェイスを設定しないでください。

（注）　回復モードのシャーシの実行コンフィギュレーションが保存せずに変更されると、そのシャーシはリロードを自動的に実行しません。この場合、実行コンフィギュレーションを保存し、手動でリロードする必要があります。

VSS の初期化

VSS の初期化の概要

VSS は、2 台のシャーシと、その間の VSL リンクが動作可能になったときに実体化します。ピア シャーシは、VSL を通して通信し、シャーシのロールをネゴシエーションします。

一方のシャーシだけが動作可能になった場合、そちらがアクティブ ロールを担います。VSS は、2 台めのシャーシが動作可能になり、両方のシャーシで VSL インターフェイスが起動されたときに実体化します。

仮想スイッチ リンク プロトコル

仮想スイッチ リンク プロトコル（VSLP）は、仮想スイッチの初期化に使用される複数のプロトコルからなります。VSLP を構成するプロトコルは、次のとおりです。

- ロール解決プロトコル：ピア シャーシは、ロール解決プロトコル（RRP）を使用して、各シャーシのロール（アクティブまたはスタンバイ）をネゴシエーションします。
- リンク管理プロトコル：リンク管理プロトコル（LMP）はすべての VSL リンクで実行され、2 台のシャーシ間の通信を確立するために必要な情報を交換します。LMP は単一方向リンクを識別および拒否します。LMP で単一方向リンクが検出されると、この状態を検出したシャーシはリンクをダウンさせ、VSLP のネゴシエーションを再開します。VSL は、必要に応じて、制御トラフィックを別のポートに移動させます。

SSO の依存関係

VSS を SSO 冗長性と合わせて機能させるには、VSS が次の条件を満たしている必要があります。

- 同じソフトウェア バージョン：VSS の両方のスーパーバイザ エンジン モジュールで、同じソフトウェア バージョンが稼働していなければなりません。
- VSL 設定の整合性：起動シーケンスでは、スタンバイ シャーシがアクティブ シャーシに対して、startup-config ファイルの仮想スイッチ情報を送信します。アクティブ シャーシでは、両方のシャーシで次の情報が完全に一致していることを確認します。
  - スイッチの仮想ドメイン
  - スイッチの仮想ノード
  - スイッチ プライオリティ
  - VSL ポート チャネル：スイッチ仮想リンク ID
  - VSL ポート：チャネルグループ番号、シャットダウン、VSL ポートの総数
  - 電源の冗長モード
  - VSL モジュールで有効な電源

  VSS で不一致が検出されると、アクティブ シャーシのコンソールにエラー メッセージが出力され、スタンバイ シャーシが RPR モードに切り替えられます。

コンフィギュレーション ファイルを修正したあと、アクティブ シャーシで **copy running-config startup-config** コマンドを入力してファイルを保存してから、スタンバイ シャーシを再起動します。

- PFC モード チェック：両方のスーパーバイザ エンジンが PFC4 を使用してプロビジョニングされると、一部のスイッチング モジュールに DFC4XL が搭載されていても、VSS は自動的に PFC4 モードで動作します。

  ただし、スーパーバイザ エンジンが PFC4XL を使用してプロビジョニングされていて、DFC4 と DFC4XL のスイッチング モジュールが混在している場合、システムの PFC モードは、2 台のシャーシ間で DFC4XL と DFC4XL のスイッチング モジュールがどのように分布しているかによって変わります。

  VSS の各シャーシによってそのシステムの PFC モードが決まります。所定のシャーシのスーパーバイザ エンジンが PFC4XL を使用してプロビジョニングされ、そのシャーシ内のすべてのスイッチング モジュールが DFC4XL を使用してプロビジョニングされている場合、そのシャーシの PFC モードは PFC4XL になります。ただし、DFC4 を使用してプロビジョニングされたスイッチング モジュールが 1 台でもある場合、シャーシの PFC モードは PFC4 に設定されます。2 台のシャーシの PFC モードに違いがある場合、VSS は SSO モードではなく、RPR モードで起動されます。この状況を回避するには、**platform hardware vsl pfc mode non-xl** コマンドを実行して、次のリロード後に VSS を強制的に PFC4 モードで動作させます。

- SSO および NSF のイネーブル化：SSO および NSF は両方のシャーシで設定し、イネーブルにする必要があります。SSO および NSF の設定および確認については、第 8 章「Nonstop Forwarding（NSF）」を参照してください。

これらの条件が満たされない場合、VSS は RPR 冗長モードで動作します。SSO と RPR の詳細については、「VSS の冗長性」（P.4-13）を参照してください。

初期化手順

VSL の初期化

VSS は、2 台のシャーシと、その間の VSL リンクが動作可能になったときに実体化します。初期化が完了する前に両方のシャーシにロール（アクティブまたはスタンバイ）を割り当てる必要があるため、VSL は、システムの残りの部分が初期化される前にオンラインになります。初期化のシーケンスは、次のとおりです。

1. VSS により、VSL ポートを搭載したすべてのカードが初期化されてから、VSL ポートが初期化されます。
2. 2 台のシャーシが VSL を通して通信し、それぞれのロール（アクティブまたはスタンバイ）をネゴシエーションします。
3. アクティブ シャーシのブート シーケンスが最後まで行われます。これには、「SSO の依存関係」（P.4-27）で説明する整合性検査も行われます。
4. 整合性検査で問題がなければ、スタンバイ シャーシが SSO スタンバイ モードで起動します。整合性検査で問題があった場合、スタンバイ シャーシは RPR モードで起動されます。
5. アクティブ シャーシは、設定データとアプリケーション データを、スタンバイ シャーシと同期させます。

システムの初期化

両方のシャーシを同時にブートすると、VSL ポートがアクティブになり、シャーシはアクティブおよびスタンバイとして起動します。プライオリティが設定されている場合、プライオリティの高いスイッチがアクティブになります。

1 台のシャーシだけをブートすると、VSL ポートは非アクティブのままで、シャーシはアクティブとして起動します。あとからもう 1 台のシャーシをブートすると、VSL リンクがアクティブになり、そのシャーシはスタンバイとして起動します。

VSL のダウン

両方のシャーシのブート時に VSL がダウンしていると、デュアル アクティブ シナリオと同じ状態になります。

一方のシャーシがアクティブになり、もう一方のシャーシはデュアル アクティブ シナリオからの回復を開始します。詳細については、「デュアル アクティブ検出の設定」（P.4-48）を参照してください。

VSS のデフォルト設定

なし。

VSS の設定方法

- 「VSS への変換」（P.4-29）
- 「VSS 情報の表示」（P.4-36）
- 「VSS をスタンドアロン シャーシに変換」（P.4-37）
- 「VSS パラメータの変換」（P.4-38）
- 「マルチシャーシ EtherChannel（MEC）の設定」（P.4-47）
- 「ピア スイッチでのロード シェアリング延期の設定」（P.4-47）
- 「デュアル アクティブ検出の設定」（P.4-48）
- 「VSS でのサービス モジュールの設定」（P.4-53）
- 「VSS のシャーシ ステータスとモジュール情報の表示」（P.4-55）

VSS への変換

- 「VSS への変換の概要」（P.4-30）
- 「スタンドアロン構成のバックアップ」（P.4-30）
- 「SSO および NSF の設定」（P.4-31）
- 「仮想スイッチ ドメインおよびスイッチ番号の割り当て」（P.4-32）
- 「VSL ポート チャネルの設定」（P.4-32）
- 「VSL ポートの設定」（P.4-33）
- 「PFC 動作モードの確認」（P.4-34）
- 「シャーシを仮想スイッチ モードに変換」（P.4-34）

- 「スタンバイ VSL 情報の自動設定」（P.4-35）
- 「（任意）スタンバイ シャーシ モジュールの設定」（P.4-36）

VSS への変換の概要

スタンドアロン モードがデフォルトの動作モード（単一シャーシのスイッチ）です。VSS モードは、2 台のスタンドアロン スイッチを結合して、VSS モードで動作する 1 つの仮想スイッチング システム（VSS）にします。

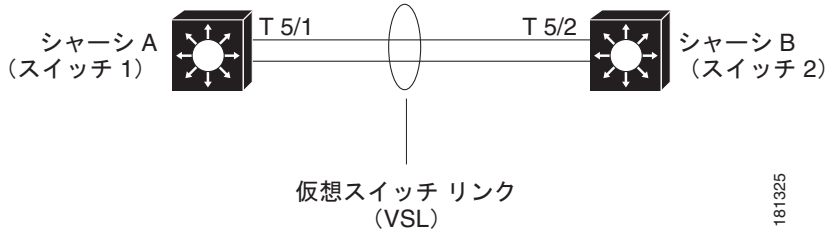
（注）　2 台のスタンドアロン スイッチを 1 つの VSS に変換すると、スタンバイ シャーシの非 VSL コンフィギュレーション設定は、すべてデフォルト設定に戻ります。

2 台のスタンドアロン シャーシを VSS に変換するには、次の作業を行います。

- スタンドアロンのコンフィギュレーション ファイルを保存します。
- SSO および NSF を各シャーシに設定します。
- 各シャーシを VSS として設定します。
- VSS への変換を実行します。
- ピア VSL 情報を設定します。

次の手順で使用するコマンドの例は、図 4-10 のような構成を想定しています。

図 4-10　VSS の例



2 台のシャーシ A と B は、仮想スイッチ ドメイン 100 によって VSS に変換されます。スイッチ 1 の 10 ギガビット イーサネット ポート 5/1 が、スイッチ 2 の 10 ギガビット イーサネット ポート 5/2 に接続されて、VSL を構成します。

スタンドアロン構成のバックアップ

両方のシャーシのコンフィギュレーション ファイルを保存します。これらのファイルは、仮想スイッチ モードからスタンドアロン モードに戻すために必要です。

スイッチ 1 での作業

	コマンド	目的
ステップ 1	`Switch-1# copy running-config startup-config`	（任意）実行コンフィギュレーションを、スタートアップ コンフィギュレーションに保存します。
ステップ 2	`Switch-1# copy startup-config disk0:old-startup-config`	スタートアップ コンフィギュレーションをバックアップ ファイルにコピーします。

スイッチ 2 での作業

	コマンド	目的
ステップ 1	`Switch-2# copy running-config startup-config`	（任意）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 ファイルに保存します。
ステップ 2	`Switch-2# copy startup-config disk0:old-startup-config`	スタートアップ コンフィギュレーションをバックアップ ファイルにコピーします。

SSO および NSF の設定

SSO および NSF は両方のシャーシで設定し、イネーブルにする必要があります。

スイッチ 1 での作業

	コマンド	目的
ステップ 1	`Switch-1(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-1(config-red)# mode sso`	SSO を設定します。このコマンドが入力されると、冗長スーパーバイザ エンジンがリロードされ、SSO モードで動作を開始します。
ステップ 3	`Switch-1(config-red)# exit`	冗長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-1(config)# router ospf processID`	OSPF ルーティング プロセスをイネーブルにし、ルータをルータ コンフィギュレーション モードにします。
ステップ 5	`Switch-1(config-router)# nsf`	OSPF 用に NSF 動作をイネーブルにします。
ステップ 6	`Switch-1(config-router)# end`	特権 EXEC モードに戻ります。
ステップ 7	`Switch-1# show running-config`	SSO および NSF が設定され、イネーブルになっていることを確認します。
ステップ 8	`Switch-1# show redundancy states`	動作中の冗長モードを表示します。

スイッチ 2 での作業

	コマンド	目的
ステップ 1	`Switch-2(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-2(config-red)# mode sso`	SSO を設定します。このコマンドが入力されると、冗長スーパーバイザ エンジンがリロードされ、SSO モードで動作を開始します。
ステップ 3	`Switch-2(config-red)# exit`	冗長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-2(config)# router ospf processID`	OSPF ルーティング プロセスをイネーブルにし、ルータをルータ コンフィギュレーション モードにします。
ステップ 5	`Switch-2(config-router)# nsf`	OSPF 用に NSF 動作をイネーブルにします。
ステップ 6	`Switch-2(config-router)# end`	特権 EXEC モードに戻ります。
ステップ 7	`Switch-2# show running-config`	SSO および NSF が設定され、イネーブルになっていることを確認します。
ステップ 8	`Switch-2# show redundancy states`	動作中の冗長モードを表示します。

SSO および NSF の設定および確認については、第 8 章「Nonstop Forwarding（NSF）」を参照してください。

仮想スイッチ ドメインおよびスイッチ番号の割り当て

両方のシャーシに同じ仮想スイッチ ドメイン番号を設定します。仮想スイッチ ドメインは、1 ～ 255 の数値で、ネットワーク内の各 VSS で一意とします（ドメイン番号は、各種 ID に組み込まれ、これらの ID がネットワーク内で一意であることが確認されます）。VSS では、一方のシャーシをスイッチ番号 1、もう一方のシャーシをスイッチ番号 2 に設定する必要があります。

スイッチ 1 での作業

	コマンド	目的
ステップ 1	`Switch-1(config)# switch virtual domain 100`	シャーシ A で仮想スイッチ ドメインを設定します。
ステップ 2	`Switch-1(config-vs-domain)# switch 1`	シャーシ A を仮想スイッチの 1 番として設定します。
ステップ 3	`Switch-1(config-vs-domain)# exit`	config-vs-domain を終了します。

スイッチ 2 での作業

	コマンド	目的
ステップ 1	`Switch-2(config)# switch virtual domain 100`	シャーシ B で仮想スイッチ ドメインを設定します。
ステップ 2	`Switch-2(config-vs-domain)# switch 2`	シャーシ B を仮想スイッチの 2 番として設定します。
ステップ 3	`Switch-2(config-vs-domain)# exit`	config-vs-domain を終了します。

（注）　両方のシャーシで同じコンフィギュレーション ファイルが使用されるため、スイッチ番号はスタートアップ コンフィギュレーションおよび実行コンフィギュレーションに保存されません（ただし、同じスイッチ番号を設定しないでください）。

VSL ポート チャネルの設定

VSL は、各シャーシで一意のポート チャネルによって設定されます。変換中に、VSS はアクティブ シャーシ上で両方のポート チャネルを設定します。スタンバイ シャーシの VSL ポート チャネル番号に、他方で使用されているのと同じ数値が設定されている場合、VSS は RPR モードで起動します。この状況を避けるため、両方のシャーシで両方のポート チャネル番号が利用できるかどうか確認してください。

ポート チャネル番号を確認するには、**show running-config interface port-channel** コマンドを使用します。このコマンドを実行すると、ポート チャネルが VSL で利用できる場合、エラー メッセージが表示されます。たとえば、次のコマンドを実行すると、スイッチ 1 でポート チャネル 20 を利用できることが示されます。

```
Switch-1 # show running-config interface port-channel 20
% Invalid input detected at '^' marker.
```

スイッチ 1 での作業

	コマンド	目的
ステップ 1	`Switch-1(config)# interface port-channel 10`	スイッチ 1 でポート チャネル 10 を設定します。
ステップ 2	`Switch-1(config-if)# switch virtual link 1`	スイッチ 1 をポート チャネル 10 のオーナーとして関連付けます。
ステップ 3	`Switch-1(config-if)# no shutdown`	ポート チャネルをアクティブにします。
ステップ 4	`Switch-1(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。

スイッチ 2 での作業

	コマンド	目的
ステップ 1	`Switch-2(config)# interface port-channel 20`	スイッチ 2 でポート チャネル 20 を設定します。
ステップ 2	`Switch-2(config-if)# switch virtual link 2`	スイッチ 2 をポート チャネル 20 のオーナーとして関連付けます。
ステップ 3	`Switch-2(config-if)# no shutdown`	ポート チャネルをアクティブにします。
ステップ 4	`Switch-2(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。

VSL ポートの設定

ポート チャネルに VSL 物理ポートを追加する必要があります。次の例では、スイッチ 1 上の 10 ギガビット イーサネット ポート 3/1 および 3/2 がスイッチ 2 の 10 ギガビット イーサネット ポート 5/2 および 5/3 に接続されています。VSL の回線の冗長性を維持するには、シャーシごとに少なくとも 2 つのポートを VSL に設定します。モジュールの冗長性については、2 つのポートを各シャーシの別のスイッチング モジュールで設定できます。

スイッチ 1 での作業

	コマンド	目的
ステップ 1	`Switch-1(config)# interface range tengigabitethernet 3/1-2`	スイッチ 1 で、インターフェイス範囲 tengigabitethernet 3/1 ～ 2 に対して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-1(config-if)# channel-group 10 mode on`	このインターフェイスをチャネル グループ 10 に追加します。
ステップ 3	`Switch-1(config-if)# no shutdown`	ポートをアクティブにします。

スイッチ 2 での作業

	コマンド	目的
ステップ 1	`Switch-2(config)# interface range tengigabitethernet 5/2-3`	スイッチ 2 で、インターフェイス範囲 tengigabitethernet 5/2 ～ 3 に対して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-2(config-if)# channel-group 20 mode on`	このインターフェイスをチャネル グループ 20 に追加します。
ステップ 3	`Switch-2(config-if)# no shutdown`	ポートをアクティブにします。

PFC 動作モードの確認

PFC 動作モードが両方のシャーシで一致することを確認します。現在の PFC モードを表示するには、各シャーシで **show platform hardware pfc mode** コマンドを入力します。一方のシャーシだけが PFC4XL モードの場合、**platform hardware vsl pfc mode non-xl** コマンドによって、PFC4 モードを使用するよう設定できます。

スイッチ 1 での作業

	コマンド	目的
ステップ 1	`Switch-1# show platform hardware pfc mode`	両方のシャーシで PFC の動作モードが一致していて、VSS が SSO 冗長モードで起動していることを確認します。
ステップ 2	`Switch-1(config)# platform hardware vsl pfc mode non-xl`	（任意）シャーシ A で PFC 動作モードを PFC4 に設定します。

スイッチ 2 での作業

	コマンド	目的
ステップ 3	`Switch-2# show platform hardware pfc mode`	両方のシャーシで PFC の動作モードが一致していて、VSS が SSO 冗長モードで起動していることを確認します。
ステップ 4	`Switch-2(config)# platform hardware vsl pfc mode non-xl`	（任意）シャーシ B で PFC 動作モードを PFC4 に設定します。

シャーシを仮想スイッチ モードに変換

VSS モードへの変換は、両方のシャーシで再起動が必要です。リブート後は、インターフェイスと *module_#/port_#* を指定するコマンドにスイッチ番号を追加します。たとえば、スイッチング モジュールのポートは *switch_#/module_#/port_#* として指定します。

再起動前に、VSS は *switch_#/module_#/port_#* 表記法を使用するようにスタートアップ コンフィギュレーションを変換します。スタートアップ コンフィギュレーション ファイルのバックアップ コピーは、RP に保存されます。このファイルにはデフォルトの名前が割り当てられますが、必要に応じて名前を上書きして変更するように指示されます。

スイッチ 1 での作業

コマンド	目的
`Switch-1# switch convert mode virtual`	スイッチ 1 を仮想スイッチ モードに変換します。 コマンドを入力すると、処理内容を確認するよう指示されます。**yes** と入力します。 変換後のコンフィギュレーション ファイルが作成され、RP ブートフラッシュに保存されます。

スイッチ 2 での作業

コマンド	目的
`Switch-2# switch convert mode virtual`	スイッチ 2 を仮想スイッチ モードに変換します。 コマンドを入力すると、処理内容を確認するよう指示されます。**yes** と入力します。 変換後のコンフィギュレーション ファイルが作成され、RP ブートフラッシュに保存されます。

（プロンプトで **yes** を入力して）コマンドを確定すると、自動的に実行コンフィギュレーションがスタートアップ コンフィギュレーションとして保存され、シャーシが再起動されます。再起動後は、シャーシは仮想スイッチ モードとなるため、インターフェイスの指定時に 3 つの ID（*switch_#/module_#/port_#*）を使用することになります。

スタンバイ VSL 情報の自動設定

2 台のシャーシが VSS を構成し、システムはスタンバイ VSL を自動的に設定します。マージが正常に完了したあと、アクティブ シャーシの VSS に対してすべてのコンフィギュレーション コマンドを入力します。スタートアップ コンフィギュレーション ファイルは、スタンバイ シャーシが ready ステートに達すると自動的にスタンバイ シャーシに同期されます。VSS モードでは、自動的にスタンバイ シャーシのコンフィギュレーション情報がマージされます。

スタンバイ シャーシのすべての非 VSL インターフェイス設定はデフォルト設定に戻り、非 VSL 関連の設定はマージされません。必要な設定を実行しなかった場合、アクティブ シャーシで設定を繰り返す必要があります。自動設定は、スタンバイ シャーシに対して次のコマンドをマージします。

- **hw-module switch** *number* **slot** *number*
- **switch virtual domain** *number*
- **switch** *number* **priority** *priority*
- **power redundancy-mode combined switch** *number*
- **no power enable switch** *num* **module** *number*
- **interface port-channel** *num* **switch virtual link** *number*
- **interface** *type switch_#/slot_#/port_#* **channel-group** *number* **mode on**

（任意）スタンバイ シャーシ モジュールの設定

リブート後、各シャーシにはそれ自身のスロット用にプロビジョニングするモジュールが含まれています。また、スタンバイ シャーシのモジュールは、アクティブ シャーシでデフォルト設定により自動的にプロビジョニングされます。

スタンバイ シャーシ モジュールの設定は、デフォルト設定に戻ります（たとえば、IP アドレスなし）。

コンフィギュレーション ファイルのモジュール プロビジョニング情報を表示するには、設定を保存したあとに **show startup-config** コマンドを入力します。

（注）　コンフィギュレーション ファイルのこのセクションは、削除したり修正したりしないでください。Cisco IOS Release 12.2(50)SY 以降では、**module provision** CLI コマンドを使用したモジュール プロビジョニング エントリの追加はできません。モジュールが存在しない場合、**no slot** コマンドと **module provision** CLI コマンドを使用して、そのモジュールのプロビジョニング エントリを消去できます。VSS セットアップは **module clear-config** コマンドをサポートしていないことに注意してください。

次に、コンフィギュレーション ファイルのモジュール プロビジョニング情報の例を示します。

```
module provision switch 1
 slot 1 slot-type 148 port-type 60 number 4  virtual-slot 17
 slot 2 slot-type 137 port-type 31 number 16  virtual-slot 18
 slot 3 slot-type 227 port-type 60 number 8  virtual-slot 19
 slot 4 slot-type 225 port-type 61 number 48  virtual-slot 20
 slot 5 slot-type 82 port-type 31 number 2  virtual-slot 21
module provision switch 2
 slot 1 slot-type 148 port-type 60 number 4  virtual-slot 33
 slot 2 slot-type 227 port-type 60 number 8  virtual-slot 34
 slot 3 slot-type 137 port-type 31 number 16  virtual-slot 35
 slot 4 slot-type 225 port-type 61 number 48  virtual-slot 36
 slot 5 slot-type 82 port-type 31 number 2  virtual-slot 37
```

VSS 情報の表示

次のコマンドは、VSS の基本情報を表示します。

コマンド	目的
show switch virtual	仮想スイッチのドメイン番号と、各シャーシのスイッチ番号およびロールを表示します。
show switch virtual role	VSS 内の各シャーシのロール、スイッチ番号、プライオリティを表示します。
show switch virtual link	VSL のステータスを表示します。

次に、これらのコマンドの情報出力の例を示します。

```
Router# show switch virtual
Switch mode                  : Virtual Switch
Virtual switch domain number : 100
Local switch number          : 1
Local switch operational role: Virtual Switch Active
Peer switch number           : 2
Peer switch operational role : Virtual Switch Standby

Router# show switch virtual role
Switch  Switch Status  Preempt    Priority  Role     Session ID
        Number         Oper(Conf) Oper(Conf)         Local  Remote
```

```
-------------------------------------------------------------------
LOCAL    1      UP       FALSE(N)    100(100)  ACTIVE   0       0
REMOTE   2      UP       FALSE(N)    100(100)  STANDBY  8158    1991

In dual-active recovery mode: No

Router# show switch virtual link
VSL Status: UP
VSL Uptime: 4 hours, 26 minutes
VSL SCP Ping: Pass OK
VSL ICC (Ping): Pass
VSL Control Link: Te 1/5/1
```

VSS をスタンドアロン シャーシに変換

VSS 設定をバックアップ ファイルにコピー

アクティブ シャーシのコンフィギュレーション ファイルを保存します。このファイルは、仮想スイッチ モードに再度変換する場合に必要となります。スタンバイ シャーシのコンフィギュレーション ファイルはアクティブ シャーシのコンフィギュレーション ファイルと同じなので、アクティブ シャーシのコンフィギュレーション ファイルだけを保存すれば十分です。

	コマンド	目的
ステップ 1	`Switch-1# copy running-config startup-config`	（任意）実行コンフィギュレーションを、スタートアップ コンフィギュレーションに保存します。この手順は、保存しておく実行コンフィギュレーションに未保存の変更点がある場合だけ必要となります。
ステップ 2	`Switch-1# copy startup-config disk0:vs-startup-config`	スタートアップ コンフィギュレーションをバックアップ ファイルにコピーします。

アクティブ シャーシをスタンドアロンに変換

アクティブ シャーシをスタンドアロン モードに変換するとき、アクティブ シャーシは VSL リンクとピア シャーシ モジュールに関連するプロビジョニング情報および設定情報を削除し、コンフィギュレーション ファイルを保存し、リロードを実行します。シャーシは、スタンドアロン システムに関連するプロビジョニング データおよび設定データだけを使用して、スタンドアロン モードで起動します。

VSS のスタンバイ シャーシの方がアクティブになります。ピアは利用不可になっているため、このシャーシの VSL リンクはダウンします。

アクティブ シャーシをスタンドアロン モードに変換するには、アクティブ シャーシで次の作業を行います。

コマンド	目的
Switch-1# **switch convert mode stand-alone**	スイッチ 1 をスタンドアロン モードに変換します。 コマンドを入力すると、処理内容を確認するよう指示されます。**yes** と入力します。

ピア シャーシをスタンドアロンに変換

新しくアクティブになったシャーシをスタンドアロン モードに変換するとき、シャーシは VSL リンクとピア シャーシ モジュールに関連するプロビジョニング情報および設定情報を削除し、コンフィギュレーション ファイルを保存し、リロードを実行します。シャーシは、そのシャーシ用のプロビジョニング データおよび設定データだけを使用して、スタンドアロン モードで起動されます。

ピア シャーシをスタンドアロン モードに変換するには、スタンバイ シャーシで次の作業を行います。

コマンド	目的
Switch-2# **switch convert mode stand-alone**	スイッチ 2 をスタンドアロン モードに変換します。 コマンドを入力すると、処理内容を確認するよう指示されます。**yes** と入力します。

VSS パラメータの変換

VSL のスイッチ プライオリティの設定

スイッチ 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	`Router(config)# switch virtual domain 100`	仮想スイッチ ドメインに対して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	`Router(config-vs-domain)# switch [1 | 2] priority [priority_num]`	シャーシのプライオリティを設定します。プライオリティの高いスイッチが、アクティブ ロールを担います。範囲は 1（最小プライオリティ）～ 255（最大プライオリティ）で、デフォルトは 100 です。 **（注）** • 新しく設定したプライオリティ値が反映されるのは、設定を保存して VSS のリロードを実行したあとです。 • プライオリティの高いスイッチが現在スタンバイ状態になっている場合、スイッチオーバーを開始することにより、アクティブ スイッチに切り替えることができます。**redundancy force-switchover** コマンドを入力します。 • **show switch virtual role** コマンドを実行すると、VSS の各スイッチの動作プライオリティと設定プライオリティが表示されます。 • このコマンドの **no** 形式を使用すると、プライオリティ値がデフォルト プライオリティ値の 100 にリセットされます。設定を保存してリロードを実行すると、新しい値が有効になります。

（注） スイッチのプライオリティの設定値を変更した場合、変更内容が反映されるのは、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 ファイルに保存してリロードを実行したあとです。**show switch virtual role** コマンドを実行すると、動作値および設定されたプライオリティ値が表示されます。スタンバイ スイッチを手動でアクティブ スイッチに設定するには、**redundancy force-switchover** コマンドを使用します。

次に、仮想スイッチのプライオリティを設定する例を示します。

```
Router(config)# switch virtual domain 100
Router(config-vs-domain)# switch 1 priority 200
Router(config-vs-domain)# exit
```

次に、VSS のプライオリティ情報を表示する例を示します。

```
Router# show switch virtual role
Switch  Switch Status  Preempt    Priority  Role     Session ID
        Number         Oper(Conf) Oper(Conf)         Local  Remote
------------------------------------------------------------------
LOCAL    1     UP      FALSE(N)   100(200)  ACTIVE   0      0
REMOTE   2     UP      FALSE(N)   100(100)  STANDBY  8158   1991

In dual-active recovery mode: No
```

PFC モードの設定

VSS 内に DFC4 と DFC4XL スイッチング モジュールが混在している場合、次の手順で PFC モードを設定します。

コマンド	目的
Router(config)# **platform hardware vsl pfc mode non-xl**	VSS の PFC コンフィギュレーション モードを PFC4 に設定します。 **（注）** このコマンドの設定を反映させるには、システムをリロードする必要があります。

次に、VSS の PFC コンフィギュレーション モードを PFC4 に設定する例を示します。次のメンテナンス ウィンドウで **reload** コマンドが実行されるのを待ちます。

```
Router(config)# platform hardware vsl pfc mode non-xl
Router(config)# end
Router# reload
```

VSS のすべてのスーパーバイザ エンジンとスイッチング モジュールが XL の場合、PFC モードを PFC4 に設定しようとすると、次の警告が表示されます。

```
Router(config)# platform hardware vsl pfc mode non-xl
PFC Preferred Mode: PFC4XL. The discrepancy between Operating Mode and
Preferred Mode could be due to PFC mode config. Your System has all PFC4XL modules.
Remove ' platform hardware vsl pfc mode non-xl ' from global config.
```

次に、PFC の動作モードとコンフィギュレーション モードを表示する例を示します。

```
Router# show platform hardware pfc mode
PFC operating mode : PFC4
Configured PFC operating mode : PFC4
```

VSL の設定

ポート チャネルを VSL 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	Router(config)# **interface port-channel** *channel_num*	特定のポート チャネルに対して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	Router(config-if)# **switch virtual link** *switch_num*	指定のスイッチの仮想リンクに、ポート チャネルを割り当てます。

（注） VSL の設定は、シャーシを VSS に変換する前に行うことを推奨します。

次に、VSL を設定する例を示します。

```
Switch-1(config)# interface port-channel 10
Switch-1(config-if)# switch virtual link 1
Switch-1(config-if)# no shutdown
Switch-1(config)# interface tenGigabitEthernet 5/1
Switch-1(config-if)# channel-group 10 mode on
Switch-1(config-if)# no shutdown
```

```
Switch-2(config)# interface port-channel 25
Switch-2(config-if)# switch virtual link 2
Switch-2(config-if)# no shutdown
Switch-2(config-if)# interface tenGigabitEthernet 5/2
Switch-2(config-if)# channel-group 25 mode on
Switch-2(config-if)# no shutdown
```

VSL の暗号化の設定

VSL の暗号化の概要

Cisco IOS Release 15.1SY は、スーパーバイザ エンジン 2T または WS-X6908-10GE スイッチング モジュールで設定された VSL の HW ベースの暗号化をサポートします。VSL の暗号化では、手動で設定する暗号キーを使用します。暗号キーは安全に保存されます。

VSL の暗号化の制約事項

- VSL の暗号化では、各シャーシに MACSec ライセンスが必要です。
- シャーシは暗号キーを設定したり、VSL の暗号化を有効にするためにリブートする必要があります。
- アクティブ シャーシに暗号キーを入力します。スタンバイ シャーシには暗号キーを入力することはできません。
- 一方のシャーシに VSL を介してプレーン テキストとしてキーを送信することが許容される場合は、一方のシャーシから他方のシャーシにキーを送信することができます。最大限のセキュリティを確保するために、各シャーシに暗号キーを設定します。
- 暗号キーを表示する **show** コマンドはありません。
- VSL の暗号化が有効な間は、暗号キーは削除できません。
- 次のコマンドは、リブート後に有効になります。
  - 暗号キーを削除するには、**clear switch pmk** EXEC モード コマンドを入力します。
  - VSL の暗号化をディセーブルにするには、**no vsl-encryption** 仮想スイッチ ドメイン コンフィギュレーション サブモード コマンドを入力します。
- 2 台のシャーシの暗号キーおよび VSL の暗号化ステートが一致しない場合、VSL はリンクアップ ステートに移行しません。

- VSS モードでは、VSL の暗号化を行わずに FIPS 暗号化モードを設定することはできません。システムのシャットダウンを避けるには、FIPS の暗号化モードをイネーブルにする前に VSL の暗号化をイネーブルにします。（CSCts96040、CSCtx58304）

VSL の暗号キーの設定

VSL の暗号キーを設定するには、次の作業を行います。

コマンド	目的
`Router# switch pmk encryption_key`	VSL の暗号キーを設定します。 • *encryption_key* は 32 文字（256 ビット）までの 16 進数の文字列です。 • 自動的に暗号キーを同期するかどうかを尋ねられます。自動的に暗号キーを同期していない場合は、もう一方のシャーシに同じ暗号キーを設定します。

次に、VSL の暗号キーを設定する例を示します。

```
Router# switch pmk encryption_key
Key effective only upon reboot and will override old VSL PMK.
Key needs to be provisioned on both VSS switches.
Warning - Sending the key to standby will cause the key to be sent over an unencrypted VSL
link.
Do you want to automatically synchronize the key [yes/no]?
```

VSL の暗号化のイネーブル化

VSL の暗号化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	`Router(config)# switch virtual domain domain_id`	VSS 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	`Router(config-vs-domain)# vsl-encryption`	VSL の暗号化をイネーブルにします。

次に、VSL の暗号化をイネーブルにする例を示します。

```
Router(config)# switch virtual domain domain_id
Router(config-vs-domain)# vsl-encryption
```

（注）
- 各シャーシに暗号キーを手動で設定する場合、次の作業を行います。
  - アクティブ シャーシを再起動します。スタンバイ シャーシがアクティブになります。
  - 新しいアクティブ シャーシに暗号キーを設定します。
  - 新しいアクティブ シャーシをリブートします。
- 暗号キーがスタンバイ シャーシに送信されるようにした場合、アクティブ シャーシをリブートします。

VSL の暗号化ステートの表示

次に、VSL の暗号化ステートを表示する例を示します。

```
Router# show switch virtual link | include Encryption
VSL Encryption : Configured Mode - On, Operational Mode - On
```

VSL 情報の表示

VSL の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
Router# **show switch virtual link**	VSL に関する情報を表示します。
Router# **show switch virtual link port-channel**	VSL ポート チャネルに関する情報を表示します。
Router# **show switch virtual link port**	VSL ポートに関する情報を表示します。

次に、VSL 情報を表示する例を示します。

```
Router# show switch virtual link
VSL Status : UP
VSL Uptime : 1 day, 3 hours, 39 minutes
VSL SCP Ping : Pass
VSL ICC Ping : Pass
VSL Control Link : Te 1/5/1

Router# show switch virtual link port-channel
VSL Port Channel Information

Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator

        M - not in use, no aggregation due to minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
10     Po10(RU)         -        Te1/5/4(P) Te1/5/5(P)
20     Po20(RU)         -        Te2/5/4(P) Te2/5/5(P)

Router# show switch virtual link port
VSL Link Info          : Configured: 2 Operational: 1


                          Peer         Peer    Peer
Interface   State         MAC          Switch  Interface
------------------------------------------------------------------------
Te1/5/4   operational   0013.5fcb.1480  2    Te2/5/4
Te1/5/5   link_down     -               -     -

            Last operational         Current packet       Last Diag   Time since
Interface   Failure state            State                Result      Last Diag
------------------------------------------------------------------------------
Te1/5/4 No failure               Hello bidir           Never ran   7M:51S
```

```
Te1/5/5 No failure               No failure             Never ran   7M:51S


                            Hello Tx (T4) ms        Hello Rx (T5*) ms
 Interface  State         Cfg     Cur     Rem     Cfg     Cur     Rem
-------------------------------------------------------------------------
Te1/5/4 operational  500     500     404     5000    5000    4916
Te1/5/5 link_down    500     -       -       500000  -       -
Te2/5/4 operational  500     500     404     500000  500000  499916
Te2/5/5 link_down    500     -       -       500000  -       -
 *T5 = min_rx * multiplier
```

VSL QoS の設定

VSS では、デフォルトの CoS マッピングを使用して、信頼できる CoS のために VSL ポートを自動的に設定します（VSL ポートのマッピングは変更できません）。

ASIC 単位の設定をサポートしているスイッチング モジュールでは、VSL 設定が同じ ASIC 上のすべてのポートに適用されます（VSL 以外のポートも含む）。

VSS は、VSL ポート（および同じ ASIC 上の非 VSL ポート）の QoS コマンドをディセーブルにします。たとえば、VSL ポートでは QoS キューイングまたはマップ コマンドは使用できません。

スーパーバイザ エンジン上の 10 ギガビット イーサネット ポートに対して 8 つの QoS 受信キューをすべてイネーブルにするには、**platform qos 10g-only** 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。

Cisco IOS Release 12.2(50)SY 以降のリリースでは、**platform qos 10g-only** コマンドが入力され、スーパーバイザ エンジン上の 2 つの 10 ギガビット イーサネット ポートのうち 1 つだけが VSL ポートの場合、非 VSL の 10 ギガビット イーサネット ポートを QoS 用に設定できます。

VSL ポート チャネルのサブコマンド

VSL ポート チャネルでは、インターフェイス サブコマンドのサブセットだけをコマンド コンソールで利用できます。表 4-2 に、使用可能なインターフェイス サブコマンドを示します。

表 4-2　VSL ポート チャネルのインターフェイス サブコマンド

サブコマンド	説明
default	コマンドをデフォルト値に設定します。
description	インターフェイスの説明文を入力します。
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。
load-interval	インターフェイスのロード計算の間隔を指定します。
logging	インターフェイスのロギングを設定します。
platform	プラットフォーム固有のコマンドを指定します。
no	コマンドをディセーブルにします。または、コマンドをデフォルトに設定します。
shutdown	選択したインターフェイスをシャットダウンします。

表 4-2　VSL ポート チャネルのインターフェイス サブコマンド （続き）

サブコマンド	説明
switch virtual link	このポート チャネルに関連付けられたスイッチを指定します。
vslp	VSLP インターフェイス コンフィギュレーション コマンドを指定します。

VSL ポートのサブコマンド

VSL ポート チャネルにポートがある場合、コマンド コンソールでは、インターフェイス サブコマンドのサブセットだけを利用できます。表 4-3 に、使用可能なインターフェイス サブコマンドを示します。

表 4-3　VSL ポートのインターフェイス サブコマンド

サブコマンド	説明
channel-group	指定したチャネル グループにインターフェイスを追加します。
default	コマンドをデフォルト値に設定します。
description	インターフェイスに説明を追加します。
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。
load-interval	インターフェイスのロード計算の間隔を指定します。
logging	インターフェイスのロギングを設定します。
no	コマンドをディセーブルにします。または、コマンドをデフォルトに設定します。
shutdown	選択したインターフェイスをシャットダウンします。

ルータ MAC アドレス割り当ての設定

VSS を初めて起動したとき、最初のアクティブ スーパーバイザ エンジンは VSS にルータ MAC アドレスを割り当てます。デフォルトでは、スーパーバイザ エンジンはユーザのシャーシから MAC アドレスを割り当てます。2 番めのシャーシにスイッチオーバーしたあと、VSS は前のアクティブ シャーシからの MAC アドレスをルータ MAC アドレスとして使用し続けます。

まれなケースとして、両方のシャーシがあとで非アクティブになってから、最初のアクティブ スーパーバイザ エンジンになる 2 番めのスーパーバイザ エンジンを起動する場合があります。この場合、VSS は 2 番めのシャーシのルータ MAC アドレスで起動します。GARP に応答せず、VSS に直接接続されていない他のレイヤ 2 ホストは、VSS の以前のルータ MAC アドレスを維持し、VSS とは通信できません。この状態を回避するには、MAC アドレスの最後のオクテットで符号化されたドメイン ID を持ったアドレスの専用プールからルータ MAC アドレスを割り当てるように VSS を設定するか、または、MAC アドレスを指定します。

（注）　ルータ MAC アドレスを変更する場合、新しいルータ MAC アドレスを有効にするには、新しいルータ MAC アドレスの仮想スイッチをリロードする必要があります。

ドメインベースのアドレスの専用プールからルータ MAC アドレスを割り当てられ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
ステップ 1	`Router(config)# switch virtual domain domain_id`	VSS 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	`Router(config-vs-domain)# mac address use-virtual`	ルータ MAC アドレスはドメインベースのアドレスの専用プールから割り当てられます。 **（注）** このコマンドの **no** 形式は、最初のアクティブ シャーシのバックプレーンから MAC アドレスを使用して、デフォルト設定に戻ります。

ルータ MAC アドレスを指定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# switch virtual domain domain_id`	VSS 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	`Router(config-vs-domain)# mac address mac_address`	ルータ MAC アドレスは、2 バイトの 16 進数の番号 3 つで指定されます。

次に、ドメインベースのアドレスの専用プールからルータ MAC アドレスの割り当てを設定する例を示します。

```
Router(config)# switch virtual domain 255
Router(config-vs-domain)# mac address use-virtual
```

次に、ルータ MAC アドレスを 16 進数形式で指定する例を示します。

```
Router(config)# switch virtual domain 255
Router(config-vs-domain)# mac address 0123.4567.89ab
```

スタンバイ回復時のポートのアクティブ化遅延の設定

障害となったシャーシをスタンバイ シャーシとして再起動するときにすべてのポートを同時にアクティブ化する代わりに、非 VSL ポートのアクティブ化を遅らせ、グループ内のポートを一定の期間アクティブ化するようにシステムを設定できます。

ポートのアクティブ化遅延を指定するには、次の作業を行います。

コマンド	目的
`Router(config)# switch virtual domain 1`	VSS 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
`Router(config-vs-domain)# standby port delay` *delay-time*	まずポートのアクティブ化を遅らせてから、サイクルごとに実行するよう指定します。 *delay-time* では、ポートのアクティブ化が開始するまでの時間（秒）を指定します。範囲は 30 ～ 3600 です。
`Router(config-vs-domain)# standby port bringup` *number cycle-time*	サイクルごとにアクティブ化するポートの数と、サイクルの間の待ち時間を指定します。 *number* では、サイクルごとにアクティブ化するポートの数を指定します。指定できる範囲は 1 ～ 100 です。デフォルト値は 1 ポートです。 *cycle-time* では、サイクルの間の待ち時間を指定します。指定できる範囲は 1 ～ 10 です。デフォルト値は 1 秒です。

次に、ポートのアクティブ化を 120 秒遅らせ、20 のポートのグループ単位で 5 秒ごとにアクティブ化するよう設定する例を示します。

```
Router(config)# switch virtual domain 1
Router(config-vs-domain)# standby port delay 120
Router(config-vs-domain)# standby port bringup 20 5
```

マルチシャーシ EtherChannel（MEC）の設定

マルチシャーシ EtherChannel（MEC）を、通常の EtherChannel と同様に設定します。VSS は、両方のシャーシのポートが EtherChannel に追加されると、その EtherChannel が MEC であると認識します。MEC の設定を確認するには、**show etherchannel** コマンドを入力します。

1 つの VSS で最大 512 のポート チャネルがサポートされます。

（注）　Cisco IOS Release 12.2(50)SY よりも前のリリースでは、最大 128 のポート チャネルがサポートされます。

ピア スイッチでのロード シェアリング延期の設定

ポート チャネルにロード シェアリング延期機能を設定するには、VSS の MEC ピアであるスイッチで次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# port-channel load-defer` *time*	（任意）すべてのポート チャネルに対し、ポートのロード シェアリング延期間隔を設定します。 • *time* : 遅延するポート チャネルのロード シェアリングが最初に 0 である時間。指定できる範囲は 1 ～ 1800 秒です。デフォルトは 120 秒です。

	コマンド	目的
ステップ 2	`Router(config)# interface port-channel channel-num`	ポート チャネル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。
ステップ 3	`Router(config-if)# port-channel port load-defer`	ポート チャネルでポートのロード シェアリング延期をイネーブルにします。

次に、VSS の MEC ピアであるスイッチ上のポート チャネル 10 でロード シェアリング延期機能を設定する例を示します。

```
Router(config)# port-channel load-defer 60
Router(config)# interface port-channel 10
Router(config-if)# port-channel port load-defer
This will enable the load share deferral feature on this port-channel.
```

（注）　マルチキャスト トラフィックに最適なサポートを提供するために、複数のモジュールのメンバ ポートがあるすべての EtherChannel でロード シェアリング延期機能を設定します。

デュアル アクティブ検出の設定

拡張 PAgP デュアル アクティブ検出の設定

拡張 PAgP が VSS とそのアクセス スイッチの間の MEC 上で実行されている場合、VSS は拡張 PAgP メッセージングを使用してデュアル アクティブ シナリオを検出できます。

デフォルトでは、PAgP デュアル アクティブ検出はイネーブルです。ただし、拡張メッセージは、信頼モードがイネーブルになっている場合だけ、ポート チャネル上で送信されます（信頼モードについては下記を参照してください）。

（注）　PAgP デュアル アクティブ検出の設定を変更する前に、信頼モードがイネーブルになったすべてのポート チャネルが管理ダウン ステートになっていることを確認してください。ポート チャネルのインターフェイス コンフィギュレーション モードで、**shutdown** コマンドを使用します。デュアル アクティブ検出の設定が完了してポート チャネルを再アクティブ化するときは、忘れずに **no shutdown** コマンドを使用してください。

PAgP デュアル アクティブ検出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	`Router(config)# switch virtual domain domain_id`	仮想スイッチ サブモードを開始します。
ステップ 2	`Router(config-vs-domain)# dual-active detection pagp`	拡張 PAgP メッセージの送信をイネーブルにします。

PAgP デュアル アクティブ検出を行うポート チャネルに信頼モードを設定する必要があります。デフォルトでは、信頼モードはディセーブルです。

（注）　PAgP デュアル アクティブ検出をイネーブルにする場合、信頼モードを変更する前に、ポート チャネルを管理ダウン ステートに設定する必要があります。ポート チャネルのインターフェイス コンフィギュレーション モードで、**shutdown** コマンドを使用します。ポート チャネルの信頼モードの設定が完了してポート チャネルを再アクティブ化するときは、忘れずに **no shutdown** コマンドを使用してください。

ポート チャネルで信頼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	`Router(config)# switch virtual domain domain_id`	仮想スイッチ サブモードを開始します。
ステップ 2	`Router(config-vs-domain)# dual-active detection pagp trust channel-group group_number`	指定したポート チャネルの信頼モードをイネーブルにします。

次に、PAgP デュアル アクティブ検出をイネーブルにする例を示します。

```
Router(config)# interface port-channel 20
Router(config-if)# shutdown
Router(config-if)# exit
Router(config)# switch virtual domain 100
Router(config-vs-domain)# dual-active detection pagp
Router(config-vs-domain)# dual-active detection pagp trust channel-group 20
Router(config-vs-domain)# exit
Router(config)# interface port-channel 20
Router(config-if)# no shutdown
Router(config-if)# exit
```

次に、信頼できるポート チャネルがシャットダウンされていない状態で PAgP デュアル アクティブ検出をイネーブルにしようとしたときに表示されるエラー メッセージの例を示します。

```
Router(config)# switch virtual domain 100
Router(config-vs-domain)# dual-active detection pagp
Trusted port-channel 20 is not administratively down.
To change the pagp dual-active configuration, "shutdown" these port-channels first.
Remember to "no shutdown" these port-channels afterwards.
```

次に、シャットダウンされていないポート チャネルに信頼モードを設定しようとしたときに表示されるエラー メッセージの例を示します。

```
Router(config)# switch virtual domain 100
Router(config-vs-domain)# dual-active detection pagp trust channel-group 20
Trusted port-channel 20 is not administratively down. To change the pagp dual-active trust
configuration, "shutdown" the port-channel first. Remember to "no shutdown" the
port-channel afterwards.
```

fast hello デュアル アクティブ検出の設定

fast hello デュアル アクティブ検出は、デフォルトでイネーブルになっていますが、デュアル アクティブ インターフェイス ペアを、fast hello デュアル アクティブ メッセージング リンクとして動作するように設定する必要があります。

fast hello デュアル アクティブ検出を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# switch virtual domain domain_id`	仮想スイッチ サブモードを開始します。
ステップ 2	`Router(config-vs-domain)# dual-active detection fast-hello`	fast hello デュアル アクティブ検出方式をイネーブルにします。fast hello デュアル アクティブ検出は、デフォルトでイネーブルになっています。
ステップ 3	`Router(config-vs-domain)# exit`	仮想スイッチ サブモードを終了します。
ステップ 4	`Router(config)# interface type switch/slot/port`	設定するインターフェイスを選択します。このインターフェイスは、もう一方のシャーシと直接接続されている必要があります。また、VSL リンクをインターフェイスとすることはできません。
ステップ 5	`Router(config-if)# dual-active fast-hello`	インターフェイス上で fast hello デュアル アクティブ検出をイネーブルにし、他のすべての設定をそのインターフェイスから自動的に削除し、インターフェイスをデュアル アクティブ コンフィギュレーション コマンドに制限します。
ステップ 6	`Router(config-if)# no shutdown`	インターフェイスをアクティブにします。

fast hello デュアル アクティブ インターフェイス ペアを設定する際、次の点に注意してください。

- デュアル アクティブ インターフェイス ペアのもう一方のシャーシと接続するために、各シャーシには最大 4 つのインターフェイスを設定できます。
- 各インターフェイスは、もう一方のシャーシと直接接続されている必要があります。また、VSL リンクをインターフェイスとすることはできません。VSL によって使用されていないスイッチング モジュールからリンクを使用することを推奨します。
- 各インターフェイスは、物理ポートでなければなりません。SVI などのローカル ポートはサポートされません。
- fast hello デュアル アクティブ モードを設定すると、インターフェイスからすべての既存設定が自動的に削除され、インターフェイスは fast hello デュアル アクティブ コンフィギュレーション コマンドに制限されます。
- fast hello デュアル アクティブ インターフェイス ペアでは、単方向リンク検出（UDLD）はディセーブルになります。

次に、fast hello デュアル アクティブ検出用のインターフェイスを設定する例を示します。

```
Router(config)# switch virtual domain 255
Router(config-vs-domain)# dual-active detection fast-hello
Router(config-vs-domain)# exit
Router(config)# interface fastethernet 1/2/40
Router(config-if)# dual-active fast-hello
WARNING: Interface FastEthernet1/2/40 placed in restricted config mode. All extraneous
configs removed!

Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# exit
Router# show run interface fastethernet 1/2/40
interface FastEthernet1/2/40
 no switchport
 no ip address
 dual-active fast-hello
end
```

除外リストの設定

デュアル アクティブ シナリオが検出された場合、回復アクションの一部として、シャーシで VSL 以外のすべてのインターフェイスをシャットダウンします。このアクションから除外する 1 つまたは複数のインターフェイスを指定できます（たとえば、シャーシへのリモート アクセスのために使用するインターフェイスを除外）。

デュアル アクティブ回復によるシャットダウンの対象外とするインターフェイスを指定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# switch virtual domain` *domain_id*	仮想スイッチ サブモードを開始します。
ステップ 2	`Router(config-vs-domain)# dual-active exclude interface` *type switch/slot/port*	デュアル アクティブ回復によるシャットダウンの対象から除外するインターフェイスを指定します。

除外リストを設定する際、次の点に注意してください。

- インターフェイスは、IP アドレスによって設定された物理ポートとします。
- VSL ポートをインターフェイスとすることはできません。
- インターフェイスは fast hello デュアル アクティブ検出に使用できません。

次に、インターフェイスを除外項目として設定する例を示します。

```
Router(config)# switch virtual domain 100
Router(config-vs-domain)# dual-active exclude interface gigabitethernet 1/5/5
```

デュアル アクティブ検出の表示

デュアル アクティブ検出の情報を表示するには、次の作業を行います。

コマンド	目的
`Router# show switch virtual dual-active [pagp | fast-hello | summary]`	デュアル アクティブ検出の設定とステータスに関する情報を表示します。

次に、デュアル アクティブ検出のためのサマリー ステータスを表示する例を示します。

```
Router# show switch virtual dual-active summary
Pagp dual-active detection enabled: Yes
Fast-hello dual-active detection enabled: Yes

No interfaces excluded from shutdown in recovery mode

In dual-active recovery mode: No
```

次に、fast-hello デュアル アクティブ検出のための情報を表示する例を示します。

```
Router# show switch virtual dual-active fast-hello
Fast-hello dual-active detection enabled: Yes

Fast-hello dual-active interfaces:
Port       State (local only)
```

```
------------------------------
Gi1/4/47   Link dn
Gi2/4/47   -
```

次に、PAgP ステータスと、信頼モードがイネーブルに設定されたチャネル グループを表示する例を示します。

```
Router# show pagp dual-active
PAgP dual-active detection enabled: Yes
PAgP dual-active version: 1.1

Channel group 3 dual-active detect capability w/nbrs Dual-Active trusted group: No
          Dual-Active     Partner              Partner   Partner
Port      Detect Capable  Name                 Port      Version
Fa1/2/33  No              None                 None      N/A

Channel group 4
Dual-Active trusted group: Yes
No interfaces configured in the channel group

Channel group 5
Dual-Active trusted group: Yes
Channel group 5 is not participating in PAGP

Channel group 10 dual-active detect capability w/nbrs Dual-Active trusted group: Yes
          Dual-Active     Partner              Partner   Partner
Port      Detect Capable  Name                 Port      Version
Gi1/6/1   Yes             partner-1            Gi1/5/1   1.1
Gi2/5/1   Yes             partner-1            Gi1/5/2   1.1

Channel group 11 dual-active detect capability w/nbrs Dual-Active trusted group: No
          Dual-Active     Partner              Partner   Partner
Port      Detect Capable  Name                 Port      Version
Gi1/6/2   Yes             partner-1            Gi1/3/1   1.1
Gi2/5/2   Yes             partner-1            Gi1/3/2   1.1

Channel group 12 dual-active detect capability w/nbrs Dual-Active trusted group: Yes
          Dual-Active     Partner              Partner   Partner
Port      Detect Capable  Name                 Port      Version
Fa1/2/13  Yes             partner-1            Fa1/2/13  1.1
Fa1/2/14  Yes             partner-1            Fa1/2/14  1.1
Gi2/1/15  Yes             partner-1            Fa1/2/15  1.1
Gi2/1/16  Yes             partner-1            Fa1/2/16  1.1
```

（注）　**show switch virtual dual-active pagp** コマンドの出力内容は、**show pagp dual-active** コマンドの出力内容と同じです。

VSS でのサービス モジュールの設定

（注）　VSS でのサービス モジュール設定の詳細については、サービス モジュールのコンフィギュレーション ガイドとコマンド リファレンスを参照してください。

VSS のサービス モジュールでのセッションの開始

セッションの開始を必要とするサービス モジュールを設定するには、次の作業を行います。

コマンド	目的
Router# **session switch** *num* **slot** *slot* **processor** *processor-id*	指定されたモジュールでセッションを開始します。 • *num*：アクセスするスイッチを指定します。有効な値は 1 と 2 です。 • *slot*：モジュールのスロット番号を指定します。 • *processor-id*：プロセッサ ID 番号を指定します。範囲は 0 ～ 9 です。

次に、VSS でファイアウォール サービス モジュールへのセッションを開始する例を示します。

```
Router# session switch 1 slot 4 processor 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.41 ... Open
```

VSS のファイアウォール サービス モジュールへの VLAN グループの割り当て

VLAN グループを FWSM に割り当てるには、次の作業を実行します。

コマンド	目的
Router(config)# **firewall switch** *num* **slot** *slot* **vlan-group** [*vlan_group* | *vlan_range*]	VLAN を指定されたモジュール内のファイアウォール グループに割り当てます。 • *num*：アクセスするスイッチを指定します。有効な値は 1 と 2 です。 • *slot*：モジュールのスロット番号を指定します。 • *vlan_group*：グループ ID を整数で指定します。 • *vlan_range*：グループに割り当てられる VLAN を指定します。

次に、VSS のファイアウォール サービス モジュールに VLAN グループを割り当てる例を示します。

```
Router(config)# firewall switch 1 slot 4 vlan-group 100,200
```

VSS の ACE サービス モジュールへの VLAN グループの割り当て

VLAN グループを ACE に割り当てるには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# svclc multiple-vlan-interfaces`	サービス モジュールに対して複数 VLAN インターフェイス モードをイネーブルにします。
ステップ 2	`Router(config)# svclc switch num slot slot vlan-group [vlan_group | vlan_range]`	VLAN を指定されたモジュール内のファイアウォール グループに割り当てます。 • *num*：アクセスするスイッチを指定します。有効な値は 1 と 2 です。 • *slot*：モジュールのスロット番号を指定します。 • *vlan_group*：グループ ID を整数で指定します。 • *vlan_range*：グループに割り当てられる VLAN を指定します。

次に、VSS の ACE サービス モジュールに複数の VLAN グループを割り当てる例を示します。

```
Router(config)# svclc multiple-vlan-interfaces
Router(config)# svclc switch 1 slot 4 vlan-group 100,200
```

VSS のサービス モジュールに挿入されたルートの表示

Route Health Injection（RHI）ルートを表示するには、次の作業を行います。

コマンド	目的
`Router# show svclc rhi-routes switch num slot slot`	指定されたサービス モジュールに挿入された RHI ルートを表示します。 • *num*：アクセスするスイッチを指定します。有効な値は 1 と 2 です。 • *slot*：モジュールのスロット番号を指定します。

次に、VSS のサービス モジュールに挿入されたルートを表示する例を示します。

```
Router# show svclc rhi-routes switch 1 slot 4
RHI routes added by slot 34
        ip              mask            nexthop       vlan  weight tableid
  --------------- --------------- --------------- ------ ------ -------
A 23.1.1.4        255.255.255.252 20.1.1.1        20     1      0
```

VSS のシャーシ ステータスとモジュール情報の表示

VSS のシャーシ ステータスと一方または両方のシャーシに搭載されたモジュール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
Router# **show module switch** { **1** | **2** | **all** }	指定されたシャーシ（**1** または **2**）または両方のシャーシ（**all**）のモジュールに関する情報を表示します。

次に、VSS のシャーシ番号 1 のシャーシ ステータスとモジュール情報を表示する例を示します。

```
module switch 1
 Switch Number:     1   Role:   Virtual Switch Active
---------------------  -----------------------------

Mod Ports Card Type                                Model              Serial No.
--- ----- ---------------------------------------- ------------------ -----------
  1    48  CEF720 48 port 10/100/1000mb Ethernet  WS-X6748-GE-TX     SAL1215M2YA
  2    16  CEF720 16 port 10GE with DFC            WS-X6716-10GE      SAL1215M55F
  3     1  Application Control Engine Module       ACE20-MOD-K9       SAD120603SU
.
.
.
```

VSS のアップグレード方法

- 「VSS の Fast Software Upgrade の実行」（P.4-55）
- 「VSS の enhanced Fast Software Upgrade の実行」（P.4-56）

VSS の Fast Software Upgrade の実行

VSS の FSU は、第 6 章「高速ソフトウェア アップグレード」で説明する RPR ベース スタンドアロン シャーシ FSU に似ています。スタンドアロン シャーシのアップグレードは、スタンバイ スーパーバイザ エンジンをリロードすることで開始されますが、VSS のアップグレードは、スタンバイ シャーシのリロードによって開始されます。FSU 手順の実行中、アクティブ シャーシとスタンバイ シャーシ間にソフトウェア バージョンの不一致があると、システムがステートレスな RPR 冗長モードでブートされ、すべてのモジュールがハード リセットされる原因になります。その結果、FSU 手順では、RPR のスイッチオーバーの時間に対応するシステム ダウンタイムが必要になります。

（注）　VSS モードは、各シャーシでスーパーバイザ エンジンを 1 つだけサポートしています。

VSS の FSU 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	`Router# copy tftp disk_name`	TFTP を使用して新しいソフトウェア イメージをアクティブ シャーシとスタンバイ シャーシのフラッシュ メモリ（disk0: および slavedisk0:）にコピーします。プロンプトで、新しいソフトウェア イメージの名前と場所を指定します。
ステップ 2	`Router# 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 3	`Router(config)# no boot system`	以前に割り当てられたブート変数を削除します。
ステップ 4	`Router(config)# config-register 0x2102`	コンフィギュレーション レジスタを設定します。
ステップ 5	`Router(config)# boot system flash device:file_name`	新しいイメージをブートするように、シャーシを設定します。
ステップ 6	`Router(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	`Router# copy running-config startup-config`	設定を保存します。
ステップ 8	`Router# redundancy reload peer`	スタンバイ シャーシをリロードして、再びオンライン状態に戻します（新しいバージョンの Cisco IOS ソフトウェアを実行します）。2 台のシャーシのソフトウェア バージョンが違っていると、スタンバイ シャーシは RPR 冗長モードになります。 **（注）** スタンバイ シャーシをリロードする前に、すべての設定の同期変更が完了するまで、十分に待機してください。
ステップ 9	`Router# redundancy force-switchover`	スタンバイ シャーシに、新しい Cisco IOS イメージを実行するアクティブ シャーシのロールを強制的に代行させます。モジュールがリロードされ、モジュール ソフトウェアが新しいアクティブ シャーシからダウンロードされます。 古いアクティブ シャーシは、新しいイメージを使用してリブートされ、スタンバイ シャーシになります。

次に、FSU の実行例を示します。

```
Router# config terminal
Router(config)# no boot system
Router(config)# config-register 0x2102
Router(config)# boot system flash disk0:image_name
Router(config)# end
Router# copy running-config startup-config
Router# redundancy reload peer
Router# redundancy force-switchover
```

VSS の enhanced Fast Software Upgrade の実行

eFSU では、In-Service Software Upgrade（ISSU）と同じコマンドとソフトウェア インフラストラクチャを使用します。eFSU と ISSU の違いは、FSU ではモジュールをリセットするため、トラフィックが短時間中断されることです。VSS の eFSU シーケンスは、第 5 章「Enhanced Fast Software Upgrade」で説明する単一シャーシの eFSU と同じ論理手順で実行されます。ただし、この手順は、1

台のシャーシにある 2 つのスーパーバイザ エンジンではなく、各シャーシの VSS アクティブ スーパーバイザ エンジンと VSS スタンバイ スーパーバイザ エンジンに適用されます。eFSU の実行中、スーパーバイザ エンジンおよびモジュールを含む VSS スタンバイ シャーシがアップグレードされ、ステートフル スイッチオーバー（SSO）モードになります。次に、eFSU プロセスはスイッチオーバーを実行して、もう一方のシャーシに対して同じアップグレードを行い、このシャーシは新しい VSS スタンバイ シャーシになります。

（注）　VSS モードは、各シャーシでスーパーバイザ エンジンを 1 つだけサポートしています。シャーシに別のスーパーバイザがある場合は、DFC として動作します。

ここでは、次の内容について説明します。

eFSU の制約事項および注意事項

eFSU を実行する際、次の注意事項と制約事項に従ってください。

- リリースに関係なく、異なる機能セットで生成されたイメージに eFSU 互換性チェックを実行すると、エラーになります。
- eFSU を開始する前に、新しいイメージ ファイルが各シャーシのスーパーバイザ エンジンのファイル システム内に配置されている必要があります。**issu** コマンドは、グローバルなファイル システム名（disk0:、bootdisk: など）だけを受け入れます。**issu** コマンドは、スイッチ番号固有のファイル システム名（sw1-slot5-disk0: など）を受け入れません。
- eFSU の準備をする際、ブート変数を変更しないでください。FSU（RPR）手順ではブート変数の変更が必要ですが、eFSU 手順でブート変数を変更すると、CurrentVersion 変数の一貫性がなくなり、eFSU を実行できなくなります。
- VSS eFSU アップグレードに使用する **issu** コマンドは、第 5 章「Enhanced Fast Software Upgrade」で説明する単一シャーシ（スタンドアロン）eFSU のコマンドと似ていますが、次のような相違点があります。
  - スタンドアロンの **issu** コマンドがスロット番号の引数を受け入れるのに対し、VSS の **issu** コマンドは *switch/slot* 形式（たとえば、1/5 はスイッチ 1、スロット 5）のスイッチおよびスロット番号を受け入れます。
  - 通常の VSS eFSU では、VSS **issu** コマンドの入力時にスイッチまたはスロット番号を指定する必要はありません。
- eFSU プロセスの実行中、ロールバック タイマーの期間は変更できません。
- eFSU プロセスの実行中、**issu** コマンドによって実行されるものを除き、手動のスイッチオーバーは行わないでください。
- eFSU プロセスの実行中、どのモジュールでも活性挿抜（OIR）を行わないでください。
- eFSU ダウングレード時、**loadversion** コマンドを実行した直後に（MCL エラーまたは **abortversion** コマンドを入力したことによって）プロセスが強制終了した場合、SSO VSS スタンバイは元のイメージでリロードされます。ただし、SSO VSS スタンバイの ICS の bootvar は、**loadversion** コマンドのあとに実行された強制終了時に変更されないため、SSO VSS スタンバイの ICS はリロードされません。

VSS アップグレードの eFSU ステージ

eFSU シーケンスは複数のステージで構成され、各ステージは CLI に個々の **issu** コマンドを入力することで明示的に開始されます。各ステージでは、次のステージに進む前に、システム ステータスを確認したり、アップグレードをロールバックしたりすることができます。

ここでは、VSS アップグレードの eFSU ステージについて、次の順序で説明します。

準備

eFSU プロセスを開始する前に、アップグレード イメージが各シャーシのスーパーバイザ エンジンのファイル システム内に配置されている必要があります。そうでない場合、最初のコマンドは拒否されます。VSS が安定した動作状態にあり、一方のシャーシは VSS アクティブ ステート、もう一方のシャーシはホット VSS スタンバイ ステートである必要があります。

loadversion ステージ

VSS アクティブ シャーシと VSS スタンバイ シャーシの新しいアップグレード イメージのメモリでの場所を指定して、**issu loadversion** コマンドを入力すると、eFSU プロセスが開始されます。**issu loadversion** コマンドでは、VSS アクティブ シャーシと VSS スタンバイ シャーシのスイッチおよびスロット番号を指定できますが、その必要はありません。**issu loadversion** コマンドを入力すると、スーパーバイザ エンジンおよびモジュールを含む VSS スタンバイ シャーシ全体が、新しいアップグレード イメージを使用してリロードされます。リロード中は VSS スタンバイ シャーシのモジュールを使用できないので、このステージでは VSS のスループットが一時的に 50% 低下します。リロード後、VSS スタンバイ シャーシは新しいイメージでブートされ、SSO モードで初期化され、トラフィックのスループットは回復します。このステージでは、VSS スタンバイ シャーシは VSS アクティブ シャーシとは異なるソフトウェア バージョンを実行します。したがって、VSS アクティブ シャーシは、2 台のシャーシ間で異なるイメージ バージョンを実行するモジュールと通信する必要があります。

runversion ステージ

VSS スタンバイ シャーシが SSO モードで新しいイメージを正常に実行している場合、**issu runversion** コマンドを入力できます。このコマンドは、アップグレードされた VSS スタンバイ シャーシを新しい VSS アクティブ シャーシにするスイッチオーバーを実行します。前に VSS アクティブだったシャーシはリロードされ、新しい VSS スタンバイ シャーシとして SSO モードで初期化され、古いイメージを実行します。loadversion ステージと同様、VSS スタンバイ シャーシのリロード中、VSS のスループットは一時的に低下し、VSS スタンバイ シャーシは VSS アクティブ シャーシとは異なるソフトウェア バージョンを実行します。

acceptversion ステージ（任意）

issu runversion コマンドを入力すると、新しいイメージを実行するシャーシへのスイッチオーバーが実行され、アップグレード プロセスによって VSS が非稼働にならないよう、保護措置として自動ロールバック タイマーが起動します。ロールバック タイマーが切れる前に、新しいソフトウェア イメージを受け入れまたは確定する必要があります。ロールバック タイマーが切れると、アップグレードされ

たシャーシがリロードされ、前のソフトウェア バージョンに戻ります。ロールバック タイマーを停止するには、**issu acceptversion** コマンドを入力します。eFSU プロセスを開始する前に、ロールバック タイマーをディセーブルにしたり、タイマーに最大 2 時間までの値（デフォルトは 45 分）を設定したりすることができます。

アップグレードされた VSS アクティブ シャーシで操作するこのステージでは、新しいソフトウェア イメージの機能を調べることができます。新しいイメージが受け入れ可能であることが確認できたら、**issu commitversion** コマンドを入力してアップグレード プロセスを終了します。

commitversion ステージ

アップグレード イメージを 2 台めのシャーシに適用するには、eFSU を完了して **issu commitversion** コマンドを入力します。VSS スタンバイ シャーシはリロードされ、新しいアップグレード イメージでブートされ、再び VSS スタンバイ シャーシとして初期化されます。loadversion ステージの場合と同様に、モジュールのリロードおよび初期化中は、VSS のスループットが一時的に低下します。VSS スタンバイ シャーシのリロードとリブートが正常に実行されたら、VSS アップグレード プロセスは完了です。

abortversion（任意）

issu commitversion コマンドを入力する前に **issu abortversion** コマンドを入力すると、いつでもアップグレードをロールバックできます。ソフトウェアが障害を検知すると、アップグレード プロセスは自動的に終了します。ロールバックのプロセスは、現在のステートによって異なります。**issu runversion** コマンドを入力する前に FSU が強制終了した場合、VSS スタンバイ シャーシは古いイメージを使用してリロードされます。**issu runversion** コマンドの入力後に FSU が強制終了した場合は、スイッチ オーバーが実行されます。古いイメージを実行している VSS スタンバイ シャーシは、VSS アクティブ シャーシになります。前に VSS アクティブだったシャーシは古いイメージでリロードされ、ロールバックが完了します。

eFSU アップグレードの設定と実行

ここでは、eFSU アップグレードの設定および実行方法について、次の順序で説明します。

- 「eFSU ロールバック タイマーの変更」（P.4-60）
- 「eFSU アップグレードの実行」（P.4-60）
- 「eFSU アップグレードの強制終了」（P.4-61）

eFSU ロールバック タイマーの変更

eFSU ロールバック タイマーの変更を表示するには、アップグレードの前に次の作業を行います。

	コマンド	目的
ステップ 1	`Router# config 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	`Router(config)# issu set rollback-timer {seconds | hh:mm:ss}`	（任意）アップグレード プロセスによって VSS が非稼働にならないよう、ロールバック タイマーを設定します。タイマーが切れると、ソフトウェア イメージは前のソフトウェア イメージに戻ります。タイマーを停止するには、新しいソフトウェア イメージを受け入れまたは確定する必要があります。 タイマーの時間は、秒数を表す 1 つの数値（*秒*）、またはコロンで区切られた秒、分、および時間（*hh:mm:ss*）を使用して設定できます。範囲は 0 ～ 7200 秒（2 時間）、デフォルトは 2700 秒（45 分）です。0 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。
ステップ 3	`Router(config)# exit`	特権 EXEC モードに戻ります。
ステップ 4	`Router# show issu rollback timer`	現在のロールバック タイマー値を表示します。

次に、両方のコマンド形式を使用して eFSU ロールバック タイマーを 1 時間に設定する例を示します。

```
Router# config terminal
Router(config)# issu set rollback-timer 3600
% Rollback timer value set to [ 3600 ] seconds
Router(config)# issu set rollback-timer 01:00:00
% Rollback timer value set to [ 3600 ] seconds
Router(config)#
```

eFSU アップグレードの実行

VSS の eFSU アップグレード（またはダウングレード）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	`Router# copy tftp disk_name`	TFTP を使用して、新しいソフトウェア イメージを VSS アクティブ シャーシおよび VSS スタンバイ シャーシ（disk0: および slavedisk0:）のフラッシュ メモリと ICS（存在する場合）にコピーします。プロンプトで、新しいソフトウェア イメージの名前と場所を指定します。
ステップ 2	`Router# show issu state [switch/slot] [detail]`	（任意）VSS で eFSU を実行する準備ができていることを確認します。 **（注）** アップグレードでは、任意のステージで **show issu state** コマンドを使用して、アップグレードの進捗とステータスを確認できます。

	コマンド	目的
ステップ 3	Router# **issu loadversion** [*active_switch/slot*] *active-image* [*standby_switch/slot*] *standby-image*	新しいソフトウェア イメージを VSS スタンバイ シャーシにロードして、アップグレード プロセスを開始します。イメージ名には、ロード対象のイメージのパスが *devicename:filename* という形式で含まれています。 新しいイメージをロードし、VSS スタンバイ シャーシが SSO モードに移行するには、数分かかる場合があります。
ステップ 4	Router# **issu runversion**	スイッチオーバーを実行します。VSS スタンバイ シャーシは VSS アクティブ シャーシになり、新しいソフトウェアを実行します。前に VSS アクティブだったシャーシは VSS スタンバイ シャーシになり、古いイメージでブートされます。
ステップ 5	Router# **issu acceptversion**	（任意）ロールバック タイマーを停止して、アップグレード プロセス中に新しいソフトウェア イメージが自動的に中断されないようにします。
ステップ 6	Router# **issu commitversion**	新しいソフトウェア イメージを VSS スタンバイ シャーシにロードします。
ステップ 7	Router# **show issu state** [*switch/slot*][**detail**]	アップグレード プロセスのステータスを確認します。アップグレードが正常に実行された場合、VSS アクティブ シャーシと VSS スタンバイ シャーシはどちらも新しいソフトウェア バージョンを実行しています。

eFSU アップグレード シーケンスの例については、「eFSU アップグレードの例」（P.4-61）を参照してください。

eFSU アップグレードの強制終了

eFSU を手動で強制終了してアップグレードをロールバックするには、次の作業を行います。

コマンド	目的
Router# **issu abortversion**	アップグレード プロセスを中止し、前のソフトウェア イメージへのロールバックを実行します。

次に、VSS の eFSU アップグレードを強制終了する例を示します。

```
Router# issu abortversion
```

eFSU アップグレードの例

次に、VSS の eFSU アップグレードを実行および確認する例を示します。

システムの準備状態の確認

新しいイメージ ファイルをアクティブおよび VSS スタンバイ シャーシのファイル システムにコピーしたら、**show issu state detail** コマンドと **show redundancy status** コマンドを入力し、VSS が eFSU を実行する準備ができていることを確認します。一方のシャーシはアクティブ ステート、もう一方は

ホット VSS スタンバイ ステートである必要があります。両方のシャーシが ISSU Init ステートで、かつ SSO 冗長ステートでなければなりません。次の例では、両方のシャーシは「oldversion」イメージを実行しています。

```
Router# show issu state detail
                         Slot = 1/2
                   RP State = Active
                 ISSU State = Init
                Boot Variable = disk0:s72033-oldversion.v1,12;
              Operating Mode = sso
            Primary Version = N/A
          Secondary Version = N/A
            Current Version = disk0:s72033-oldversion.v1
             Variable Store = PrstVbl

                         Slot = 2/7
                   RP State = Standby
                 ISSU State = Init
                Boot Variable = disk0:s72033-oldversion.v1,12;
              Operating Mode = sso
            Primary Version = N/A
          Secondary Version = N/A
            Current Version = disk0:s72033-oldversion.v1

Router# show redundancy status
       my state = 13 -ACTIVE
     peer state = 8  -STANDBY HOT
           Mode = Duplex
           Unit = Secondary
        Unit ID = 18

Redundancy Mode (Operational) = sso
Redundancy Mode (Configured)  = sso
Redundancy State              = sso
     Maintenance Mode = Disabled
 Communications = Up

   client count = 132
 client_notification_TMR = 30000 milliseconds
          keep_alive TMR = 9000 milliseconds
        keep_alive count = 0
    keep_alive threshold = 18
           RF debug mask = 0x0
```

VSS スタンバイ シャーシへの新しいイメージのロード

issu loadversion コマンドを入力して、アップグレード プロセスを開始します。この手順では、VSS スタンバイ シャーシがリブートされ、新しいイメージでリロードされ、VSS スタンバイ シャーシとして SSO 冗長モードで初期化され、新しいイメージを実行します。「Bulk sync succeeded」メッセージが表示されてシャーシの設定が同期すると、この手順は完了します。

```
Router# issu loadversion disk0:s72033-newversion.v2

000133: Aug  6 16:17:44.486 PST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet1/2/4, changed state to down
000134: Aug  6 16:17:43.507 PST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet2/7/4, changed state to down
000135: Aug  6 16:17:43.563 PST: %LINK-3-UPDOWN: Interface TenGigabitEthernet2/7/4,
changed state to down
000136: Aug  6 16:17:44.919 PST: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/2/4,
changed state to down
```

（複数のインターフェイスおよびプロトコルのダウン メッセージを省略）

```
%issu loadversion executed successfully, Standby is being reloaded
```

（複数のインターフェイスおよびプロトコルのダウン メッセージ、続いてインターフェイスおよびプロトコルのアップ メッセージを省略）

```
0000148: Aug  6 16:27:54.154 PST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet1/2/5, changed state to up
000149: Aug  6 16:27:54.174 PST: %LINK-3-UPDOWN: Interface TenGigabitEthernet2/7/5,
changed state to up
000150: Aug  6 16:27:54.186 PST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet2/7/5, changed state to up
000151: Aug  6 16:32:58.030 PST: %HA_CONFIG_SYNC-6-BULK_CFGSYNC_SUCCEED: Bulk Sync
succeeded
```

VSS スタンバイ シャーシの新しいイメージの確認

show issu state detail コマンドと **show redundancy** コマンドを入力して、両方のシャーシが ISSU Load Version ステートおよび SSO 冗長ステートであることを確認できます。次の例では、VSS スタンバイ シャーシは、「newversion」イメージを実行しています。

```
Router# show issu state detail
                        Slot = 1/2
                   RP State = Active
                  ISSU State = Load Version
                Boot Variable = disk0:s72033-oldversion.v1,12
               Operating Mode = sso
             Primary Version = disk0:s72033-oldversion.v1
           Secondary Version = disk0:s72033-newversion.v2
             Current Version = disk0:s72033-oldversion.v1
              Variable Store = PrstVbl

                        Slot = 2/7
                   RP State = Standby
                  ISSU State = Load Version
                Boot Variable =
disk0:s72033-newversion.v2,12;disk0:s72033-oldversion.v1,12
               Operating Mode = sso
             Primary Version = disk0:s72033-oldversion.v1
           Secondary Version = disk0:s72033-newversion.v2
             Current Version = disk0:s72033-newversion.v2

Router# show redundancy status
       my state = 13 -ACTIVE
     peer state = 8  -STANDBY HOT
           Mode = Duplex
           Unit = Secondary
        Unit ID = 18

Redundancy Mode (Operational) = sso
Redundancy Mode (Configured)  = sso
Redundancy State              = sso
     Maintenance Mode = Disabled
 Communications = Up

   client count = 132
 client_notification_TMR = 30000 milliseconds
          keep_alive TMR = 9000 milliseconds
        keep_alive count = 1
    keep_alive threshold = 18
           RF debug mask = 0x0
```

新しいイメージへのスイッチオーバーの実行

VSS スタンバイ シャーシが SSO 冗長モードで新しいイメージを正常に実行している場合は、**issu runversion** コマンドを入力してスイッチオーバーを実行します。アップグレードされた VSS スタンバイ シャーシは、新しいアクティブ シャーシとしてロールを代行し、新しいイメージを実行します。前にアクティブだったシャーシは、新しい SSO モードの VSS スタンバイ シャーシとしてリロードおよびリブートされ、（ソフトウェア アップグレードを終了して古いイメージを復元する必要がある場合は）古いイメージを実行します。「Bulk sync succeeded」メッセージが表示されてシャーシの設定が同期すると、この手順は完了します。

```
Router# issu runversion
This command will reload the Active unit.Proceed ?[confirm]
```
（複数の行を省略）

```
Download Start
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
(複数の行を省略)
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Download Completed!Booting the image.
Self decompressing the image :
##########################################################################################
(複数の行を省略)
################################################################################## [OK]
running startup....

(複数の行を省略)

000147: Aug  6 16:53:43.199 PST: %HA_CONFIG_SYNC-6-BULK_CFGSYNC_SUCCEED: Bulk Sync
succeeded
```

スイッチオーバーの確認

show issu state detail コマンドと **show redundancy** コマンドを入力して、両方のシャーシが ISSU Run Version ステートおよび SSO 冗長ステートであることを確認できます。次の例では、アクティブ シャーシは、「newversion」イメージを実行しています。

```
Router# show issu state detail
                          Slot = 2/7
                      RP State = Active
                    ISSU State = Run Version
                 Boot Variable =
disk0:s72033-newversion.v2,12;disk0:s72033-oldversion.v1,12
                Operating Mode = sso
               Primary Version = disk0:s72033-newversion.v2
             Secondary Version = disk0:s72033-oldversion.v1
               Current Version = disk0:s72033-newversion.v2
                Variable Store = PrstVbl

                          Slot = 1/2
                      RP State = Standby
                    ISSU State = Run Version
                 Boot Variable = disk0:s72033-oldversion.v1,12
                Operating Mode = sso
               Primary Version = disk0:s72033-newversion.v2
             Secondary Version = disk0:s72033-oldversion.v1
               Current Version = disk0:s72033-oldversion.v1

Router# show redundancy status
       my state = 13 -ACTIVE
     peer state = 8  -STANDBY HOT
           Mode = Duplex
           Unit = Primary
        Unit ID = 39

Redundancy Mode (Operational) = sso
Redundancy Mode (Configured)  = sso
Redundancy State              = sso
     Maintenance Mode = Disabled
 Communications = Up

   client count = 134
 client_notification_TMR = 30000 milliseconds
          keep_alive TMR = 9000 milliseconds
        keep_alive count = 1
    keep_alive threshold = 18
           RF debug mask = 0x0
```

VSS スタンバイ シャーシへの新しいイメージの確定

アクティブ シャーシが新しいイメージを SSO モードで正常に実行している場合は、**issu acceptversion** コマンドを入力すると、ロールバック タイマーを停止し、このステートを無制限に保留できます。**issu commitversion** コマンドを入力すると、eFSU を続行できます。続行するには、**issu commitversion** コマンドを入力して VSS スタンバイ シャーシをアップグレードし、eFSU シーケンスを完了します。VSS スタンバイ シャーシはリブートされ、新しいイメージでリロードされ、VSS スタンバイ シャーシとして SSO 冗長ステートで初期化され、新しいイメージを実行します。「Bulk sync succeeded」メッセージが表示されてシャーシの設定が同期すると、この手順は完了します。

```
Router# issu commitversion
Building configuration...
[OK]
000148: Aug  6 17:17:28.267 PST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet2/7/4, changed state to down
000149: Aug  6 17:17:28.287 PST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet1/2/4, changed state to down
```

（複数のインターフェイスおよびプロトコルのダウン メッセージを省略）

```
%issu commitversion executed successfully
```

（複数のインターフェイスおよびプロトコルのダウン メッセージ、続いてインターフェイスおよびプロトコルのアップ メッセージを省略）

```
000181: Aug  6 17:41:51.086 PST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet1/2/5, changed state to up
000182: Aug  6 17:42:52.290 PST: %HA_CONFIG_SYNC-6-BULK_CFGSYNC_SUCCEED: Bulk Sync
succeeded
```

アップグレードの完了確認

show issu state detail コマンドと **show redundancy** コマンドを入力して、eFSU の結果を確認できます。この例では、両方のシャーシは「newversion」イメージを実行しており、eFSU が成功したことを意味しています。eFSU が完了したため、2 台のシャーシは eFSU 開始前のように再び ISSU Init Version ステートになります。

```
Router# show issu state detail
                           Slot = 2/7
                     RP State = Active
                   ISSU State = Init
                Boot Variable =
disk0:s72033-newversion.v2,12;disk0:s72033-oldversion.v1,12
              Operating Mode = sso
             Primary Version = N/A
           Secondary Version = N/A
             Current Version = disk0:s72033-newversion.v2
              Variable Store = PrstVbl

                           Slot = 1/2
                     RP State = Standby
                   ISSU State = Init
                Boot Variable =
disk0:s72033-newversion.v2,12;disk0:s72033-oldversion.v1,12
              Operating Mode = sso
             Primary Version = N/A
```

```
              Secondary Version = N/A
                Current Version = disk0:s72033-newversion.v2

Router# show redundancy status
       my state = 13 -ACTIVE
     peer state = 8  -STANDBY HOT
           Mode = Duplex
           Unit = Primary
        Unit ID = 39

Redundancy Mode (Operational) = sso
Redundancy Mode (Configured)  = sso
Redundancy State              = sso
     Maintenance Mode = Disabled
 Communications = Up

   client count = 134
 client_notification_TMR = 30000 milliseconds
          keep_alive TMR = 9000 milliseconds
        keep_alive count = 1
    keep_alive threshold = 18
           RF debug mask = 0x0
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

PART 4

ハイ アベイラビリティ

CHAPTER 5

Enhanced Fast Software Upgrade

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

eFSU の前提条件

なし。

eFSU の制約事項

- Release 15.0(1)SY のペイロード暗号化なし（NPE）イメージでは、中断のない ACL アップデート機能または [**no**] **platform hardware acl update-mode hitless** コマンドはサポートされません。

  Release 15.0(1)SY1 以降のペイロード暗号化なし（NPE）イメージでは、中断のない ACL アップデートがサポートされ、および**platform hardware acl update-mode hitless** コマンドがデフォルトで設定されます（これがデフォルトになるため、コマンドはコンフィギュレーション ファイルには表示されません）。

  中断のない ACL アップデート機能をサポートする他のリリースおよびイメージでは、**platform hardware acl update-mode hitless** コマンドがデフォルトで設定されます。

  NPE イメージを使用する場合に、Release 15.0(1)SY1 以降から Release 15.0(1)SY へのダウングレードの実行中の問題を回避するため、中断のない ACL アップデート機能をディセーブル（**no platform hardware acl update-mode hitless**）にしないでください。その理由は、CLI は Release 15.0(1)SY の NPE イメージに存在せず、デフォルト以外の条件を設定すると、CLI が Release 15.0(1)SY1 のコンフィギュレーション ファイルに表示され、サポートされないコマンドにより Release 15.0(1)SY に問題が発生するためです。

  中断のない ACL アップデート機能は TCAM リソースを消費します。TCAM 使用率が高い場合は、ダウングレードをサポートするために中断のない ACL アップデート機能をイネーブルにすると、その他の設定済み機能との TCAM の競合が発生する可能性があります。
- eFSU には、アクティブとスタンバイの 2 つのスーパーバイザ エンジンが必要です。
- 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 エンジンには、アップグレード プロセスの前に新旧のソフトウェア イメージを格納する十分なフラッシュ メモリが必要です。
- リリースに関係なく、異なる機能セットで生成されたイメージに eFSU 互換性チェックを実行すると、エラーになります。
- Cisco IOS ソフトウェアの旧バージョンに eFSU でダウングレードした場合、プロセスを開始する前に以前のバージョンでサポートされていない機能をすべてディセーブルにしない限り、コンフィギュレーション ファイルは同期せず、スタンバイ スーパーバイザ エンジンがリロードされます。以前のバージョンでは使用できないコンフィギュレーション コマンドをすべて削除します。
- eFSU アップグレード時に、モジュールは再起動されます。
- スイッチは既存のソフトウェア イメージと新規のソフトウェア イメージを確認し、次のように自動的に適切なプロセス（eFSU）を実行して、ソフトウェア イメージをアップグレードします。
  - パッチ アップグレードの場合、モジュール ソフトウェアが既存のソフトウェア イメージと新規のソフトウェア イメージの両方で同じである場合、モジュール ソフトウェアのアップグレードは必要ないので、eFSU によってスーパーバイザ エンジンのソフトウェアだけがアップグレードされます。システムのダウンタイムは、0 ～ 3 秒です。
  - イメージのモジュール ソフトウェアが異なる場合、アップグレード プロセス時にモジュールが再起動またはリセットされます。システムのダウンタイムは、モジュールが eFSU をサポートするかどうかによって異なります（詳細については、「停止時間とサポートに関する考慮事項」（P.5-4）を参照してください）。
- eFSU アップグレード機能は、ノンストップ フォワーディング（NSF）/SSO とともに動作します。NSF/SSO をサポートしないソフトウェア機能は、ソフトウェア アップグレード時に発生するスイッチオーバーの後にオンラインに戻るまで、動作が停止します。
- eFSU プリロードをサポートするすべてのモジュールには、新規のソフトウェア イメージを保持するための十分な空き容量がある 512 MB 以上のメモリが必要です。メモリの空き容量が不十分であると、eFSU はプリロードを試行せず、スイッチオーバー時にモジュールをリセットします。

- Online Insertion and Replacement（OIR; 活性挿抜）は、eFSU の実行時にはサポートされません。アップグレードがアクティブであるときに、新規のモジュールをスイッチに挿入しようとしても、スイッチからそのモジュールに電源は供給されません。アップグレードが終了すると、スイッチは新規に挿入されたモジュールをリセットします。
- アップグレード時には、スーパーバイザ エンジン間の手動によるスイッチオーバーを実行できません。
- コンフィギュレーション レジスタが自動起動できるよう設定されていることを確認します（レジスタの最低バイトは 2 に設定する必要があります）。
- **issu abortversion** コマンドを入力する前に（ソフトウェア アップグレードを打ち切るため）、スタンバイ スーパーバイザ エンジンがアップ（STANDBY HOT（SSO モード）または COLD（RPR モード））であることを確認します。
- Fast Software Upgrade（FSU）プロセスは、以前のリリースからのアップグレードをサポートしています。このプロセス時には、eFSU をサポートするモジュールでもモジュール ソフトウェア イメージがアップグレードされます。

eFSU に関する情報

（注）　eFSU は、仮想スイッチング システム（VSS）モードでサポートされています。詳細については、「VSS の制約事項」（P.4-2）を参照してください。

eFSU の動作

eFSU は、拡張型のソフトウェア アップグレード手順です。eFSU（FSU）以外のソフトウェア アップグレードには、システムのダウンタイムが必要です。なぜなら、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 エンジンとのソフトウェア バージョンの不一致により、システムが強制的にステートレスな Route Processor Redundancy（RPR）冗長モードを起動し、すべてのモジュールのハード リセットを引き起こすためです。

eFSU では、ソフトウェアのアップグレードによるダウンタイムを減らし、ネットワークのアベイラビリティが向上します。eFSU は、次の方法でこれを実現します。

- 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 エンジンのソフトウェア バージョンが異なる場合、または VSS が設定されている場合に、2 つのシャーシ内のスーパーバイザ エンジンにそれぞれ異なるソフトウェア バージョンが搭載されている場合でも、スタンバイ スーパーバイザ エンジンをステートフル スイッチオーバー（SSO）モードにします。

  eFSU の実行中は、新規のソフトウェアがスタンバイ スーパーバイザ エンジンにロードされる一方、アクティブ スーパーバイザ エンジンは既存のソフトウェアを使用して動作し続けます。アップグレードの一環として、スタンバイ プロセッサが SSO Standby Hot のステージに到達し、スイッチオーバーが発生し、スタンバイがアクティブになって新規のソフトウェアが実行されます。以前のリリースでは、別のソフトウェア バージョンを実行するスーパーバイザ エンジンが Route Processor Redundancy モードで動作していました。

アップグレードを続行して新しいソフトウェアを別のプロセッサにロードすることも、アップグレードを中断して古いソフトウェアで動作を再開することもできます。

- サポートされているモジュールのメモリに新規のモジュール ソフトウェアをプリロードして、ハードウェア リセットを回避します。

  新規のソフトウェア リリースに新規のモジュール ソフトウェアが含まれている場合、eFSU によって新規のモジュール ソフトウェアが、eFSU プリロードをサポートするスイッチのすべてのモジュールにプリロードされます。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 エンジンの間でスイッチオーバーが発生すると、モジュールは新規のソフトウェア イメージを使用して再起動します。

  eFSU プリロードは、次のモジュールでサポートされています。

  - WS-X67*xx* モジュール
  - SIP-400 および SIP-600

  その他のすべてのモジュールでは、スイッチオーバーの発生時にハードウェア リセットが行われ、モジュールの再起動後にソフトウェア イメージがロードされます。

  ソフトウェア アップグレード時に、スイッチは eFSU プリロードをサポートするモジュールに対して自動的に次の手順を実行します。

  - 各モジュールで、新規の Cisco IOS ソフトウェア イメージに必要なメモリを予約します。
  - **issu loadversion** コマンドの一環として、新規のソフトウェア イメージをモジュールにプリロードします。
  - スイッチオーバーが発生したときに、新規のソフトウェア イメージを使用してモジュールを再起動します（**ssu runversion**）。
  - 再起動中は、ソフトウェア機能とルーティング プロトコルを使用できません。
  - ロールバックまたは打ち切りが行われた場合は、中断を最小限にするため、スイッチは元のソフトウェア バージョンをモジュールにプリロードします。ロールバックまたは打ち切りが完了すると、元のソフトウェア バージョンを使用してモジュールが再起動します。

（注）　eFSU プリロードをサポートするすべてのモジュールには、新規のソフトウェア イメージを保持するための十分な空き容量がある 512 MB 以上のメモリが必要です。メモリの空き容量が不十分であると、eFSU はプリロードを試行せず、スイッチオーバー時にモジュールをリセットします。

停止時間とサポートに関する考慮事項

eFSU アップグレード時は、スーパーバイザ エンジン間で発生するスイッチオーバー後にモジュールが再起動またはリセットされます。モジュールが再起動またはリセットされるため、プロトコルおよびソフトウェア機能がオンラインに戻るまで、モジュールに接続するリンクがアップからダウンになり、トラフィック処理が中断します。モジュール処理が中断される時間の長さ（停止時間）は、eFSU プロセスが新規のソフトウェア イメージをモジュールにプリロードできたかどうかによって異なります。

- eFSU プリロードをサポートするモジュールの場合、eFSU モジュールのウォーム リロードによる停止時間のほうが RPR モードのモジュール リロードより速くなります。
- eFSU プリロードをサポートしないモジュールの場合、モジュール リロードによる停止時間は RPR モードのモジュール リロードと同様です。

新規のソフトウェアがロードされた後は（**issu loadversion**）、**show issu outage slot all** コマンドを使用して、搭載されているモジュールの最大停止時間を表示できます。コマンドの例については、「搭載されているモジュールの最大停止時間の表示（任意）」（P.5-10）を参照してください。

モジュール メモリの予約

eFSU をサポートするモジュールでは、新規のソフトウェア イメージ（非圧縮形式）を格納するため、スーパーバイザ エンジンが自動的にモジュールのメモリを予約します。必要なメモリの容量は、モジュールのタイプによって異なります。

推奨されませんが、次のコマンドを入力して、スイッチによるソフトウェア プリロード用のメモリの予約を抑止することができます（*slot-num* にはモジュールが搭載されているスロットを指定します）。

```
no mdr download reserve memory image slot slot-num
```

（注）　eFSU プリロードをサポートするすべてのモジュールには、新規のソフトウェア イメージを保持するための十分な空き容量がある 512 MB 以上のメモリが必要です。メモリの空き容量が不十分であると、eFSU はプリロードを試行せず、スイッチオーバー時にモジュールをリセットします。

モジュールでのメモリの予約に成功したかどうかを表示するには、**show issu outage slot all** コマンドを使用します。コマンドの例については、「搭載されているモジュールの最大停止時間の表示（任意）」（P.5-10）を参照してください。

eFSU プリロードのエラー処理

eFSU プリロード時に問題が発生した場合、スイッチでは次の処理が行われます。

- loadversion の実行中にモジュールがクラッシュした場合：スイッチオーバーが発生した時点でモジュールがリセットされます。
- eFSU の起動時にモジュールがアクティブでない場合：ソフトウェア アップグレード中はモジュールに電源が供給されず、プロセスが終了した時点でモジュールがリセットされます。ソフトウェア アップグレード プロセスが開始された後、スイッチに挿入されているモジュールにも同じ処理が適用されます。
- runversion の実行中またはロールバック中にモジュールがクラッシュした場合：モジュールは、アクティブ スーパーバイザ エンジンに存在するソフトウェア イメージに対応するソフトウェア イメージ バージョンを使って起動します。

eFSU のデフォルト設定

なし。

eFSU の実行方法

- 「eFSU の概要手順」（P.5-6）
- 「アップグレードの準備」（P.5-7）
- 「新しいソフトウェア イメージのコピー」（P.5-9）
- 「スタンバイ スーパーバイザ エンジンへの新規ソフトウェアのロード」（P.5-9）
- 「搭載されているモジュールの最大停止時間の表示（任意）」（P.5-10）
- 「スイッチオーバーのアクティブからスタンバイへの強制切り替え」（P.5-11）
- 「新しいソフトウェア バージョンの許可とロールバック プロセスの停止（任意）」（P.5-12）

- 「スタンバイに対する新しいソフトウェアの認定」（P.5-13）
- 「ソフトウェア インストレーションの確認」（P.5-13）
- 「アップグレード プロセスの中断」（P.5-14）

eFSU の概要手順

この作業は、eFSU の概要手順です。

	コマンド	目的
ステップ 1	Router> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	Router# **copy tftp** *disk_name*	TFTP を使用して、新規のソフトウェア イメージをアクティブ スーパーバイザ エンジンおよびスタンバイ スーパーバイザ エンジンのフラッシュ メモリ（disk0: および slavedisk0:）にコピーします。プロンプトで、新しいソフトウェア イメージの名前と場所を指定します。
ステップ 3	Router# **show version | in image** Router# **show bootvar** Router# **show redundancy** Router# **show issu state** [**detail**]	これらの **show** コマンドを実行すると、スイッチが eFSU を実行できる状態にあることを確認できます。**show version** および **show bootvar** コマンドでは、ブート イメージの設定を確認します。 **show redundancy** および **show issu state** コマンドでは、冗長モードがイネーブルになっていることと、SSO と NSF が設定されていることを確認します。 **（注）** アップグレードのステータスを確認するためにアップグレード中に **show redundancy** コマンドおよび **show issu state** コマンドを使用します。
ステップ 4	Router# **issu loadversion** *active-slot active-image standby-slot standby-image*	アップグレード プロセスを開始し、新規のソフトウェア イメージをスタンバイ スーパーバイザ エンジンにロードします。新規のイメージをロードし、スタンバイ スーパーバイザ エンジンを SSO モードに移行するには、数秒かかる場合があります。
ステップ 5	Router# **show issu outage slot all**	（任意）搭載されているモジュールの最大停止時間を表示します。スーパーバイザ エンジンのスイッチ プロセッサに対してコマンドを入力します。
ステップ 6	Router# **issu runversion**	スイッチオーバーを強制的に実施します。それによって、スタンバイ スーパーバイザ エンジンがアクティブになり、新規のソフトウェアの実行が開始されます。それまでアクティブだったプロセッサはスタンバイ状態となり、古いイメージを使用して起動します。
ステップ 7	Router# **issu acceptversion**	（任意）ロールバック タイマーを停止して、アップグレード プロセス中に新しいソフトウェア イメージが自動的に中断されないようにします。

	コマンド	目的
ステップ 8	`Router# issu commitversion`	新規のソフトウェア イメージを指定のスロットのスタンバイ スーパーバイザ エンジンにロードします。
ステップ 9	`Router# show redundancy` `Router# show issu state [detail]`	アップグレード プロセスのステータスを確認します。アップグレードに成功すると、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 エンジンの両方で新規のソフトウェア バージョンが実行されます。

アップグレードの準備

- 「ブート イメージのバージョンとブート変数の確認」（P.5-7）
- 「冗長モードの確認」（P.5-7）
- 「eFSU ステートの確認」（P.5-8）

（注）　ソフトウェア アップグレードを実行する前に、必ず「eFSU の制約事項」（P.5-2）を確認してください。

ブート イメージのバージョンとブート変数の確認

始める前に、次の例のとおりに **show version** コマンドおよび **show bootvar** コマンドを入力して、ブート イメージ バージョンと BOOT 環境変数を確認します。

```
Router# show version | in image
BOOT variable = disk0:image_name;
CONFIG_FILE variable =
BOOTLDR variable =
Configuration register is 0x2002

Standby is up
Standby has 1048576K/65536K bytes of memory.

Standby BOOT variable = disk0:image_name;
Standby CONFIG_FILE variable =
Standby BOOTLDR variable =
```

冗長モードの確認

冗長モードがイネーブルであること、および NSF と SSO が設定されていることを確認します。次のコマンド例に冗長性の確認方法を示します。

```
Router# show redundancy
Redundant System Information :
------------------------------
       Available system uptime = 45 minutes
Switchovers system experienced = 0
              Standby failures = 0
        Last switchover reason = none

                  Hardware Mode = Duplex
    Configured Redundancy Mode = sso
     Operating Redundancy Mode = sso
              Maintenance Mode = Disabled
                Communications = Up
```

```
Current Processor Information :
-------------------------------
               Active Location = slot 6
        Current Software state = ACTIVE
       Uptime in current state = 44 minutes
                 Image Version = Cisco IOS Software, image_details
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 18-Feb-09 12:48 by kchristi
                         BOOT = disk0:image_name;
                   CONFIG_FILE =
                       BOOTLDR =
        Configuration register = 0x2002

Peer Processor Information :
----------------------------
              Standby Location = slot 5
        Current Software state = STANDBY HOT
       Uptime in current state = 28 minutes
                 Image Version = Cisco IOS Software, image_details
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled image_details
                         BOOT = disk0:image_name ;
                   CONFIG_FILE =
                       BOOTLDR =
        Configuration register = 0x2002
```

eFSU ステートの確認

インサービス ソフトウェア アップグレード（ISSU）ステートが、eFSU アップグレードの中間ステートではなく **Init** であることを確認します。次のコマンドを入力します。

```
Router# show issu state detail
                         Slot = 6
                    RP State = Active
                   ISSU State = Load Version
                  Boot Variable = disk0:image_name
                 Operating Mode = sso
                Primary Version = disk0:sierra.0217
              Secondary Version = disk0:sierra.0217
                Current Version = disk0:sierra.0217
                 Variable Store = PrstVbl
                      ROMMON CV = [disk0:image_name]

                         Slot = 5
                    RP State = Standby
                   ISSU State = Load Version
                  Boot Variable = disk0:image_name
                 Operating Mode = sso
                Primary Version = disk0:image_name
              Secondary Version = disk0:image_name
                Current Version = disk0:image_name
```

新しいソフトウェア イメージのコピー

eFSU プロセスを開始する前に、新規のソフトウェア イメージをアクティブ スーパーバイザ エンジンおよびスタンバイ スーパーバイザ エンジンのフラッシュ メモリ（disk0: および slavedisk0:）にコピーします。

スタンバイ スーパーバイザ エンジンへの新規ソフトウェアのロード

issu loadversion コマンドを入力して、アップグレード プロセスを開始します。このコマンドによってスタンバイ スーパーバイザ エンジンが再起動し、新規のソフトウェア 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ます。ダウンロードが完了すると、**runversion** コマンドの入力を求めるプロンプトが表示されます。

（注）　自動的に両方のイメージに共通しない機能をディセーブルにしないでください。**issu loadversion** コマンドを入力してスタンバイの初期化が実行されているときに、スタンバイ スーパーバイザ エンジンでサポートされていない機能がイネーブルであると、この機能がイネーブルである間はスタンバイ スーパーバイザ エンジンを初期化できず、スタンバイ スーパーバイザ エンジンは強制的に RPR モード（load-version ステート）になることを示すメッセージが表示されます。

```
Router# issu loadversion device:filename
%issu loadversion executed successfully, Standby is being reloaded
```

issu loadversion コマンドの実行が完了すると、スタンバイ スーパーバイザ エンジンに新しいソフトウェア イメージがロードされ、スーパーバイザ エンジンは SSO モードになります。**issu loadversion** コマンドの完了までには、数秒かかる場合があります。**show** コマンドの入力が早すぎると、必要な情報が表示されない場合があります。

次に、**show redundancy** コマンドおよび **show issu state detail** コマンドを使用してアップグレードのステータスを確認する例を示します。

```
Router# show redundancy
Redundant System Information :
------------------------------
       Available system uptime = 1 hour, 0 minutes
Switchovers system experienced = 0
              Standby failures = 1
        Last switchover reason = none

                 Hardware Mode = Duplex
    Configured Redundancy Mode = sso
     Operating Redundancy Mode = sso
              Maintenance Mode = Disabled
                Communications = Up

Current Processor Information :
-------------------------------
               Active Location = slot 6
        Current Software state = ACTIVE
       Uptime in current state = 59 minutes
                 Image Version = Cisco IOS Software, image_details
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled ...
                         BOOT = disk0:image_name
                   CONFIG_FILE =
                      BOOTLDR =
        Configuration register = 0x2002
```

```
Peer Processor Information :
----------------------------
              Standby Location = slot 5
        Current Software state = STANDBY HOT
       Uptime in current state = 3 minutes
                 Image Version = Cisco IOS Software, image_name
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled ...
                         BOOT = disk0:image_name
                   CONFIG_FILE =
                       BOOTLDR =
        Configuration register = 0x2002

Router# show issu state detail
                         Slot = 6
                     RP State = Active
                    ISSU State = Load Version
                  Boot Variable = disk0:image_name
                 Operating Mode = sso
                Primary Version = disk0:image_name
              Secondary Version = disk0:image_name
                Current Version = disk0:image_name
                 Variable Store = PrstVbl
                      ROMMON CV = [disk0:image_name]

                         Slot = 5
                     RP State = Standby
                    ISSU State = Load Version
                  Boot Variable = disk0:image_name
                 Operating Mode = sso
                Primary Version = disk0:image_name
              Secondary Version = disk0:image_name
                Current Version = disk0:image_name
```

搭載されているモジュールの最大停止時間の表示（任意）

新規のソフトウェアがダウンロードされた後は、スイッチ プロセッサに対して **show issu outage slot all** コマンドを入力し、搭載されているモジュールの最大停止時間を表示することができます。

```
Router# show issu outage slot all
Slot # Card Type                                    MDR Mode    Max Outage Time
------ -------------------------------------------- ----------- ---------------
     1 CEF720 8 port 10GE with DFC                  WARM_RELOAD        300 secs
     2 96-port 10/100 Mbps RJ45                     RELOAD             360 secs
     4 CEF720 48 port 1000mb SFP                    RELOAD             360 secs

Slot # Reason                                       Error Number
------ -------------------------------------------- ------------
     1 PLATFORM_INIT                                           3
     2 PLATFORM_INIT                                           3
     4 PREDOWNLOAD_LC_MIMIMUM_MEMORY_FAILURE                   5
Router#
```

スイッチオーバーのアクティブからスタンバイへの強制切り替え

issu runversion コマンドを入力して、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 エンジンとのスイッチオーバーを強制的に実施します。新規のソフトウェア イメージがロードされたスタンバイ スーパーバイザ エンジンがアクティブになります。以前のアクティブ スーパーバイザ エンジンはスタンバイになり、既存のソフトウェア イメージを使用して起動します（ソフトウェア アップグレードを打ち切り、既存のイメージを復元する必要がある場合）。

```
Router# issu runversion

This command will reload the Active unit.  Proceed ? [confirm] y
```

この時点で、スーパーバイザ エンジン間のスイッチオーバーが発生します。以前のスタンバイ スーパーバイザ エンジンがアクティブになり、新規のソフトウェア バージョンが実行されます。以前のアクティブ スーパーバイザ エンジンで、現在のスタンバイ スーパーバイザ エンジンは既存のソフトウェアを使用して起動します。

（注） この時点で、新規のアクティブ スーパーバイザ エンジンが新規のソフトウェア イメージを実行し、スタンバイ スーパーバイザ エンジンが既存のソフトウェア イメージを実行しています。次の例（**show redundancy** および **show issu state detail**）のとおりに、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 エンジンの状態を確認します。

```
Router# show redundancy
------------------------------
       Available system uptime = 1 hour, 9 minutes
Switchovers system experienced = 1
              Standby failures = 0
        Last switchover reason = user forced

                 Hardware Mode = Duplex
    Configured Redundancy Mode = sso
     Operating Redundancy Mode = sso
              Maintenance Mode = Disabled
                Communications = Up

Current Processor Information :
------------------------------
                Active Location = slot 5
        Current Software state = ACTIVE
       Uptime in current state = 7 minutes
                 Image Version = Cisco IOS Software, image_details
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled ...
                          BOOT = disk0:image_name
                   CONFIG_FILE =
                       BOOTLDR =
        Configuration register = 0x2002

Peer Processor Information :
------------------------------
              Standby Location = slot 6
        Current Software state = STANDBY HOT
       Uptime in current state = 0 minutes
                 Image Version = Cisco IOS Software, image_details
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 18-Feb-09 12:48 by kchristi
                          BOOT = disk0:image_name
```

```
                    CONFIG_FILE =
                        BOOTLDR =
        Configuration register = 0x2002

Router# show issu state detail
                            Slot = 5
                      RP State = Active
                     ISSU State = Run Version
                  Boot Variable = disk0:image_name
                 Operating Mode = sso
               Primary Version = disk0:image_name
             Secondary Version = disk0:image_name
               Current Version = disk0:image_name
                Variable Store = PrstVbl
                     ROMMON CV = [disk0:image_name]

                            Slot = 6
                      RP State = Standby
                     ISSU State = Run Version
                  Boot Variable = disk0:image_name
                 Operating Mode = sso
               Primary Version = disk0:image_name
             Secondary Version = disk0:image_name
               Current Version = disk0:image_name
```

（注）　アップグレード プロセスを完了するには、**issu acceptversion** コマンド（任意）および **issu commitversion** コマンドを入力します（以降のセクションを参照）。

新しいソフトウェア バージョンの許可とロールバック プロセスの停止（任意）

新しいソフトウェア イメージは、許可または認定する必要があります。そうでなければ、ロールバック タイマーが期限切れになり、アップグレード プロセスが停止されます。この状況が発生した場合、ソフトウェア イメージは前回のソフトウェア バージョンに戻ります。ロールバック タイマーは、アップグレード プロセスによってスイッチの動作が停止しないようにするためのセーフガードとして機能します。

（注）　以前のイメージでサポートされていない新規機能は、**issu commitversion** コマンドを入力した後に限り、イネーブルにすることができます。

次に、**issu acceptversion** コマンドによってロールバック タイマーを停止して、新規のソフトウェア イメージの機能性を確認するコマンド シーケンスを示します。新規のイメージの受け入れに問題がないことを確認したら、**issu commitversion** コマンドを入力してアップグレード プロセスを終了します。

```
Router# show issu rollback-timer
        Rollback Process State = In progress
      Configured Rollback Time = 00:45:00
       Automatic Rollback Time = 00:37:28

Router# issu acceptversion
% Rollback timer stopped. Please issue the commitversion command.
```

ロールバック プロセスが停止されていることを確認するには、次のコマンドを使用してロールバック タイマーを表示します。

```
Router# show issu rollback-timer
        Rollback Process State = Not in progress
      Configured Rollback Time = 00:45:00
```

スタンバイに対する新しいソフトウェアの認定

issu commitversion コマンドを入力して新規のソフトウェア イメージをスタンバイ スーパーバイザ エンジンにロードし、ソフトウェア アップグレード プロセスを完了します。次の例では、新規のイメージがスロット 5 のスタンバイ スーパーバイザ エンジンにロードされます。

```
Router# issu commitversion
Building configuration...
[OK]
%issu commitversion executed successfully
```

（注）　以上で、ソフトウェア アップグレード プロセスが完了しました。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 エンジンの両方とも、新規のソフトウェア バージョンを実行しています。

ソフトウェア インストレーションの確認

ソフトウェア アップグレードのステータスを確認する必要があります。アップグレードに成功すると、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 エンジンの両方で新規のソフトウェア バージョンが実行されます。

```
Router# show redundancy
Redundant System Information :
------------------------------
       Available system uptime = 1 hour, 17 minutes
Switchovers system experienced = 1
              Standby failures = 1
        Last switchover reason = user forced

                 Hardware Mode = Duplex
    Configured Redundancy Mode = sso
     Operating Redundancy Mode = sso
              Maintenance Mode = Disabled
                Communications = Up

Current Processor Information :
-------------------------------
               Active Location = slot 5
        Current Software state = ACTIVE
       Uptime in current state = 15 minutes
                 Image Version = Cisco IOS Software, image_name
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled ...
                         BOOT = disk0:image_name
                  CONFIG_FILE =
                      BOOTLDR =
        Configuration register = 0x2002

Peer Processor Information :
----------------------------
              Standby Location = slot 6
        Current Software state = STANDBY HOT
```

```
       Uptime in current state = 0 minutes
                 Image Version = Cisco IOS Software, image_details
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled ...
                         BOOT = disk0:image_name
                   CONFIG_FILE =
                       BOOTLDR =
        Configuration register = 0x2002

Router# show issu state detail

                         Slot = 5
                   RP State = Active
                  ISSU State = Init
                Boot Variable = disk0:image_name
               Operating Mode = sso
             Primary Version = N/A
           Secondary Version = N/A
             Current Version = disk0:image_name
              Variable Store = PrstVbl
                   ROMMON CV = [disk0:simage_name ]

                         Slot = 6
                   RP State = Standby
                  ISSU State = Init
                Boot Variable = disk0:image_name
               Operating Mode = sso
             Primary Version = N/A
           Secondary Version = N/A
             Current Version = disk0:image_name
```

アップグレード プロセスの中断

issu abortversion コマンドを入力することにより、ソフトウェア アップグレードをどの段階でも手動で打ち切ることができます。またソフトウェアが障害を検出した場合、アップグレード プロセス自体が中断します。

issu loadversion コマンドを入力した後にプロセスを打ち切ると、スタンバイ スーパーバイザ エンジンがリセットされ、元のソフトウェアと一緒に再ロードされます。

次に、**issu abortversion** *slot image* コマンドを使用して、ソフトウェア アップグレード プロセスを中断する例を示します。

```
Router# issu abortversion 6 c7600s72033
```

（注）　**issu abortversion** コマンドを入力する前に、スタンバイ スーパーバイザ エンジンがアップ（STANDBY HOT（SSO モード）または COLD（RPR モード））であることを確認します。

eFSU イメージへの非 eFSU イメージのアップグレード方法

新しい Cisco IOS ソフトウェア イメージが eFSU をサポートしていない場合、ソフトウェア イメージを手動でアップグレードする必要があります。それには、スタンバイ スーパーバイザ エンジンのソフトウェア イメージをアップグレードしてから、手動によるスイッチオーバーを実行して、スタンバイ

が新規のイメージによる処理を引き継ぐようにする必要があります。その後で、以前アクティブであり、現在スタンバイであるスーパーバイザ エンジンのソフトウェア イメージをアップグレードできます。詳細については、「eFSU の概要手順」（P.5-6）を参照してください。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CHAPTER 6

高速ソフトウェア アップグレード

（注）

- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。
- 冗長スーパーバイザ エンジンだけでサポートされます。Cisco IOS ソフトウェアがスタンバイ RP でアップグレードされ、手動によるスイッチオーバーが実行されます。次に、もう一方の RP で新しい Cisco IOS イメージをアップグレードできます。
- アップグレード プロセスでは、さまざまなイメージが非常に短い期間、RP にロードされます。この間にスイッチオーバーが発生すると、デバイスは RPR モードで回復します。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

Cisco IOS イメージをアップグレードまたはダウングレードするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router> 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	`Router# copy {ftp: | http:// | https:// | rcp: | scp: | tftp:} device:filename`	Cisco IOS イメージをアクティブ RP のフラッシュ デバイスにコピーします。
ステップ 3	`Router# copy {ftp: | http:// | https:// | rcp: | scp: | tftp:} slavedevice:filename`	Cisco IOS イメージをスタンバイ RP のフラッシュ デバイスにコピーします。
ステップ 4	`Router# 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 5	`Router(config)# no boot system flash [flash-fs:][partition-number:][filename]`	（任意）既存のシステム フラッシュ ブート イメージの指定内容をすべてクリアします。

	コマンド	目的
ステップ 6	`Router(config)# boot system flash [flash-fs:][partition-number:][filename]`	フラッシュ メモリに保存されたイメージのファイル名を指定します。
ステップ 7	`Router(config)# config-register 0x2102`	コンフィギュレーション レジスタの設定をデフォルト値に設定します。
ステップ 8	`Router(config)# exit`	グローバル コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 9	`Router# copy running-config startup-config`	コンフィギュレーションの変更をスタートアップ コンフィギュレーション ファイルに保存します。
ステップ 10	`hw-module {module standby_slot} reset`	指定した Cisco IOS イメージを使用してスタンバイ プロセッサのリセットとリロードを行い、イメージを実行します。
ステップ 11	`redundancy force-switchover`	スタンバイ RP へのスイッチオーバーを強制します。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

ステートフル スイッチオーバー（SSO）

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。
- SSO および NSF は IPv6 マルチキャスト トラフィックをサポートしません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

SSO の前提条件

なし。

SSO の制約事項

一般的な制約事項

- 2 つの RP をシャーシに設置し、それぞれが同じバージョンの Cisco IOS ソフトウェアを実行している必要があります。
- 両方の RP は、同じ Cisco IOS イメージを実行する必要があります。2 つの RP が、異なる Cisco IOS イメージを実行している場合、SSO が設定されていても、システムは RPR モードに戻ります。
- SNMP 経由で行った設定変更が、スイッチオーバーの実行後、自動的にスタンバイ RP に設定されないことがあります。
- デュアル プロセッサ間のロード シェアリングはサポートされていません。
- ホット スタンバイ ルーティング プロトコル（HSRP）は、Cisco NSF/SSO でサポートされていません。HSRP を Cisco NSF/SSO で使用しないでください。
- 拡張オブジェクト トラッキング（EOT）は、SSO 認識ではないので、SSO モードで HSRP 仮想ルータ冗長プロトコル（VRRP）、ゲートウェイ ロード バランシング プロトコル（GLBP）とともには使用できません。
- マルチキャストは SSO を認識しないため、スイッチオーバー後に再起動されません。したがって、マルチキャスト テーブルおよびデータ構造は、スイッチオーバー時にクリアされます。

コンフィギュレーション モードに関する制約事項

- 両方の RP のコンフィギュレーション レジスタを同一に設定する必要があります。これにより、いずれか一方の RP がリブートされても、ネットワーキング デバイスの動作が同一に維持されます。
- 起動時の（一括）同期の際、設定の変更はできません。設定を変更する場合は、次のような内容のメッセージが表示するまで待ってください。

```
%HA-5-MODE:Operating mode is sso, configured mode is sso.
```

スイッチオーバー プロセスに関する制約事項

- ファブリックのコンフィギュレーションに対する変更と RP スイッチオーバーが同時に発生した場合、シャーシおよびすべてのラインカードがリセットされます。
- スイッチが SSO モードに設定されていて、スタンバイの準備が完了する前にアクティブ RP に障害が発生した場合、スイッチはフル システム リセットによって回復します。
- アクティブ RP とスタンバイ RP の間での SSO の同期中は、設定されたモードは RPR になります。同期が完了すると、動作モードが SSO になります。同期が完了する前にスイッチオーバーが発生すると、スイッチオーバーが RPR モードになります。
- 一括同期処理が完了する前にスイッチオーバーが発生した場合、新しくアクティブになった RP が不整合な状態になることがあります。この場合、スイッチが再度読み込まれます。

- SSO モードでスイッチオーバーが実行されても、ラインカードはリセットされません。
- RP 自体のインターフェイスはステートフルではなく、スイッチオーバーごとにリセットされます。特に、RP 上の GE インターフェイスは、スイッチ オーバーごとにリセットされ、SSO をサポートしません。
- スイッチオーバーの時点でオンラインでないすべてのラインカードは、リセットされ、スイッチオーバー時にリロードされます。

SSO について

SSO の概要

Catalyst 6500 シリーズ スイッチでは、プライマリのスーパーバイザ エンジンに障害が発生した場合、冗長スーパーバイザ エンジンに切り替えることができることで、障害に対する耐久性が提供されています。シスコ SSO（一般に NSF と使用）は、スイッチオーバー後、IP パケットの転送を継続する一方で、ユーザのネットワーク使用不能時間を最小限に抑えます。Catalyst 6500 シリーズ スイッチは、冗長性のため、Route Processor Redundancy（RPR）をサポートします。詳細については、第 9 章「Route Processor Redundancy（RPR）」を参照してください。

SSO は特にネットワーク エッジで役立ちます。従来から、コア ルータはルータの冗長化とメッシュ接続を使用して、障害ネットワーク要素を迂回したトラフィック伝送を可能にすることにより、ネットワーク障害からシステムを保護します。SSO は、ネットワーク設計内のシングル ポイント障害であり、障害時には顧客に対するサービス提供が中断する可能性があるネットワーク エッジ デバイスを、デュアル ルート プロセッサ（RP）によって保護します。

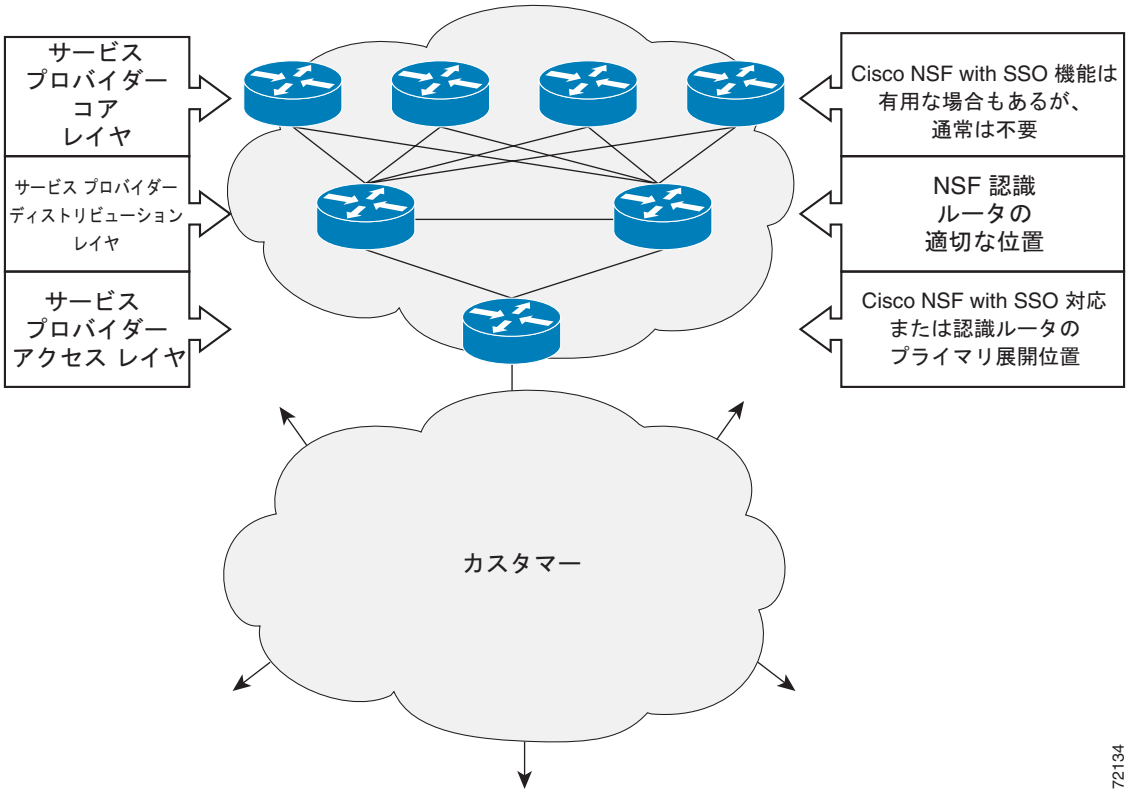
SSO には次のような多くの利点があります。SSO 機能は、ステートフル機能情報を保守するため、ユーザ セッション情報は、スイッチオーバー中に保守され、ラインカードは、引き続き、セッションを損失することなくネットワーク トラフィックを転送します。これにより、ネットワーク アベイラビリティが改善されます。また SSO では、RPR よりもスイッチオーバーが高速で実行されます。これは 1 つにはスタンバイ RP を完全に初期化して完全に設定するからであり、もう 1 つには、ステート情報を同期することによってルーティング プロトコルのコンバージェンスに要する時間を短縮できるからです。ネットワークの安定性は、ネットワーク内でルータに障害が発生し、ルーティング テーブルが失われたときに作成されるルート フラップの数を減らすことで改善できます。

Cisco Nonstop Forwarding（NSF）機能には SSO が必要です（第 8 章「Nonstop Forwarding（NSF）」を参照）。

図 7-1 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、CiscoNSF/SSO が主にサービス プロバイダー ネットワークのアクセス レイヤ（エッジ）に配置されています。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。

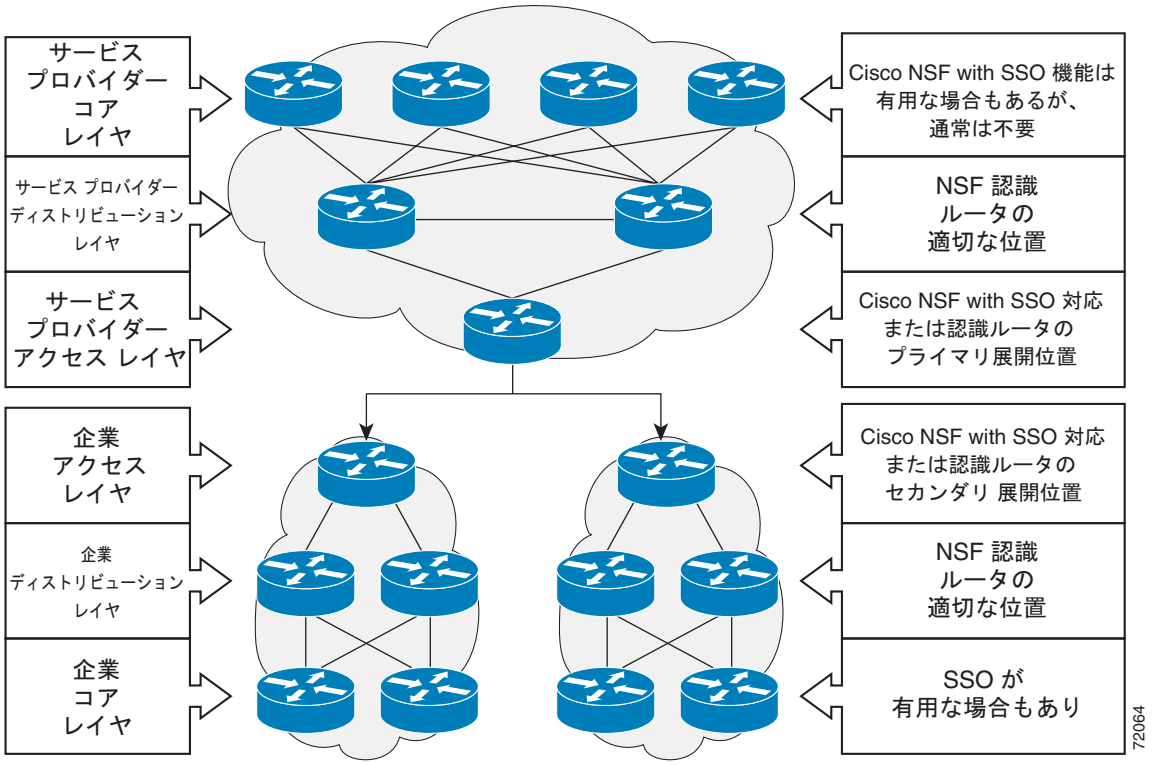
Cisco NSF プロトコルは、ネイバー デバイスが Cisco NSF に参加している必要があるので、それらのネイバー ディストリビューション レイヤ デバイスに Cisco NSF 対応のソフトウェア イメージをインストールする必要があります。その他に、ネットワークのコア レイヤに Cisco NSF と SSO 機能を適用することで、ネットワーク アベイラビリティの利点が得られる可能性もありますが、ネットワーク設計エンジニアと相談して、具体的なサイトの要件を評価してください。

図 7-1　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 7-2 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。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、企業顧客の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 7-2　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 の動作

SSO は RP の 1 つをアクティブ プロセッサ、もう一方の RP をスタンバイ プロセッサとして設定します。SSO は完全にスタンバイ RP を初期化し、アクティブ RP とスタンバイ RP 間で重要なステート情報を同期します。

SSO スイッチオーバー時に、ラインカードではリセットされません。これにより、プロセッサ間のスイッチオーバーが高速化されます。次のイベントが発生すると、スイッチオーバーが行われます。

- アクティブ スーパーバイザ エンジンでのハードウェア障害
- スーパーバイザ エンジン間のクロック同期損失
- 手動スイッチオーバーまたはシャットダウン

SSO スイッチオーバーでは、レイヤ 2 トラフィックは中断されません。SSO スイッチオーバーは FIB と隣接エントリを保護し、スイッチオーバーの後にレイヤ 3 トラフィックを転送できます。SSO スイッチオーバー時間は 0 ～ 3 秒です。

ルート プロセッサの同期

同期化の概要

SSO が動作するネットワーキング デバイスでは、アクティブ RP に障害が発生したときに、スタンバイ RP がいつでも制御を引き継げるように、両方の RP で同じコンフィギュレーションを実行する必要があります。起動時およびアクティブ RP のコンフィギュレーションに変更が生じるたびに、SSO はアクティブ RP からスタンバイ RP にコンフィギュレーション情報を同期します。この同期は、次の 2 段階で行われます。

- スタンバイ RP の起動時に、アクティブ RP からスタンバイ RP にコンフィギュレーション情報が同期されます。
- コンフィギュレーションまたはステートに変更が生じたときに、アクティブ RP からスタンバイ RP へのインクリメンタル同期が実行されます。

初期化時の一括同期

SSO を備えたシステムの初期化時に、アクティブ RP はシャーシ探索（システムにあるラインカードの数とタイプ、およびファブリック カードが装着されている場合は、その数とタイプ）を実行し、スタートアップ コンフィギュレーション ファイルを解析します。

アクティブ RP は次に、このデータをスタンバイ RP に同期し、スタンバイ RP に対して初期化を完了するように指示します。この方法により、両方の RP に同じコンフィギュレーション情報が設定されます。

スタンバイ RP は、完全に初期化されていても、アクティブ RP とのみやり取りし、コンフィギュレーション ファイルに変更が生じたときにその増分を受け取ります。スタンバイ RP に対する CLI の実行はサポートされていません。

スタートアップ コンフィギュレーションの同期

システムの起動時に、スタートアップ コンフィギュレーション ファイルがアクティブ RP からスタンバイ RP にコピーされます。スタンバイ RP にある既存のスタートアップ コンフィギュレーション ファイルは上書きされます。

スタートアップ コンフィギュレーションは、RP の NVRAM に保存されたテキスト ファイルです。このファイルは、次の操作を実行するたびに同期されます。

- CLI コマンド **copy system:running-config nvram:startup-config** を使用したとき
- CLI コマンド **copy running-config startup-config** を使用したとき
- CLI コマンド **write memory** を使用したとき
- CLI コマンド **copy** *filename* **nvram:startup-config** を使用したとき
- CISCO_CONFIG_COPY MIB で、MIB 変数 ccCopyEntry の SNMP SET を使用したとき
- **reload** コマンドを使用してシステム コンフィギュレーションを保存したとき
- 強制スイッチオーバー CLI コマンドの入力後に、ステム コンフィギュレーションを保存したとき

インクリメンタル同期

インクリメンタル同期の概要

両方の RP が完全に初期化された後、実行コンフィギュレーションまたはアクティブ RP ステートに対して行われた変更は、発生したときにスタンバイ RP に同期されます。アクティブ RP ステートは、機能情報処理、外部イベント（インターフェイスがアップ状態またはダウン状態になるなど）、またはユーザ コンフィギュレーション コマンド（CLI コマンドや簡易ネットワーク管理プロトコル（SNMP）を使用）やその他の内部イベントの結果として更新されます。

CLI コマンド

CLI による実行コンフィギュレーションの変更は、アクティブ RP からスタンバイ RP に同期されます。実際には、CLI コマンドがアクティブとスタンバイの両方の RP に対して実行されます。

SNMP SET コマンド

SNMP set 操作によるコンフィギュレーション変更は、ケースバイケースで同期されます。現在、次の 2 つの SNMP コンフィギュレーション設定操作のみがサポートされています。

- （インターフェイスの）**shut** および **no-shut**
- **link** *up/down* **trap** *enable/disable*

情報のルーティングおよび転送

情報のルーティングおよび転送は、RP に同期されます。

- SSO 認識機能（SNMP など）のステート変更は、スタンバイ RP へ同期されます。
- シスコ エクスプレス フォワーディングによる転送情報ベース（FIB）の更新は、スタンバイ RP に同期されます。

シャーシのステート

ラインカードの抜き挿しによるシャーシ ステートの変更は、スタンバイ RP に同期されます。

ラインカードのステート

ラインカードのステートの変更は、スタンバイ RP に同期されます。ラインカードのステート情報は、最初、スタンバイ RP の一括同期によって取得されます。一括同期の後、アクティブ プロセッサで受信されたラインカード イベント（インターフェイスのアップ/ダウン状態など）は、スタンバイ RP に同期されます。

カウンタおよび統計情報

アクティブ RP で維持されているさまざまなカウンタおよび統計情報は、頻繁に変更されるうえ、必要とされる同期の程度が大きいため同期されません。統計情報に関連付けられている情報量が非常に大きいため、同期は実際的ではありません。

（注）　RP 間でカウンタと統計情報が同期されないために、この情報をモニタする外部ネットワーク管理システムで問題が生じることがあります。

SSO の動作

SSO 条件

自動または手動スイッチオーバーは、次の条件で実行される可能性があります。

- アクティブ RP のクラッシュまたはリブートを引き起こす原因となる障害状態：自動スイッチオーバー
- アクティブ RP の機能停止が宣言された場合（応答なし）：自動スイッチオーバー
- CLI が呼び出された場合：手動スイッチオーバー

ユーザは CLI コマンドを使用して、アクティブ RP からスタンバイ RP へのスイッチオーバーを強制できます。この手動の手順により、アクティブな RP の「通常の」制御されたシャットダウンが行われ、スタンバイ RP に切り替えられます。この通常シャットダウンにより、不可欠なクリーンアップが行われます。

（注）　この手順を、コア ルータのルーティング プロトコルについてのグレースフル シャットダウン手順と混同しないでください。これらは別個のメカニズムです。

注意　SSO 機能では、手動でスイッチオーバーを実行するコマンドなど、いくつかの新しいコマンドが導入されるとともに、既存のコマンドが変更されています。**reload** コマンドでは、スイッチオーバーは発生しません。**reload** コマンドを実行すると、ボックスが完全にリロードされ、すべてのテーブル エントリが削除され、すべてのラインカードがリセットされて、ノンストップ フォワーディングが中断されます。

スイッチオーバー時間

アクティブ RP からスタンバイ RP に切り替えるためにデバイスに必要な時間は、0 ～ 3 秒です。

新しくアクティブになったプロセッサは、スイッチオーバーの直後に処理を引き継ぎますが、デバイスが完全冗長（SSO）モードで動作を再開するまでには、プラットフォームによっては、数分かかることもあります。スイッチオーバー時間の長さは、複数の要因に左右されます。たとえば、前にアクティブだったプロセッサがクラッシュ情報を取得する時間、コードおよびマイクロコードをロードする時間、およびプロセッサ間のコンフィギュレーションの同期に必要な時間などが要因として挙げられます。

DFC 搭載のスイッチング モジュールでは、転送情報が配信され、同じラインカードから転送されるパケットは、転送遅延がほとんどありません。ただし、ラインカード間でパケットを転送すると、スイッチオーバー時間の間、パケット転送が待機する必要がある可能性があるため、RP との対話が必要です。

アクティブ RP の活性挿抜

アクティブ RP の活性挿抜は、スタンバイ RP へのステートフル スイッチオーバーを自動的に強制します。

高速ソフトウェア アップグレード

Fast Software Upgrade（FSU）を使用して、予定されているダウンタイムを短縮することができます。FSU を使用すると、アップグレードされた Cisco IOS ソフトウェア イメージがあらかじめロードされたスタンバイ RP にシステムをスイッチオーバーできます。FSU は、アップグレードされた Cisco IOS ソフトウェアがあらかじめインストールされているスタンバイ RP に機能を転送することにより、ソフトウェア アップグレード時のダウンタイムを短縮します。また、古いバージョンの Cisco OS にシステムをダウングレードしたり、アップグレードの直後に、前のイメージにダウングレードするためにバックアップ システムをロードしたりするためにも FSU を使用できます。

FSU を実行する前に、ネットワーキング デバイスで SSO を設定する必要があります。

（注） アップグレード プロセスでは、さまざまなイメージが、短時間だけ RP にロードされます。この間、デバイスは RPR モードで動作します。

コア ダンプ処理

SSO をサポートするネットワーキング デバイスでは、スイッチオーバーが行われた後、新しくアクティブになったプライマリ プロセッサが、コア ダンプ処理を実行します。ダンプ処理を待つ必要がないので、プロセッサ間のスイッチオーバー時間が効果的に短縮されます。

スイッチオーバーの後、新しいアクティブ RP は、コア ダンプが完了するまで一定時間待った後、以前のアクティブ RP のリロードを試みます。この待ち時間は設定可能です。たとえば、プラットフォームによっては、以前のアクティブ RP がコア ダンプを実行するのに 1 時間またはそれ以上必要なことがありますが、サイト ポリシーによっては、それほど長い時間待機せずに、以前のアクティブ RP のリセットとリロードを行うことがあります。指定された時間内にコア ダンプが完了しない場合、コア ダンプがまだ実行中であるかどうかとは無関係に、スタンバイがリセットされてリロードされます。

コア ダンプ プロセスは、ファイルの内容を生成したプロセッサを識別するためのスロット番号をコア ダンプ ファイルに追加します。

（注） コア ダンプは、一般的にテクニカルサポート担当者にだけ役立ちます。コア ダンプ ファイルは、非常に大きなバイナリ ファイルであり、TFTP、FTP、またはリモート コピー プロトコル（RCP）サーバを使用して転送した後、ソース コードと詳細なメモリ マップにアクセスできる Cisco Technical Assistance Center（TAC）の担当者に分析してもらう必要があります。

SSO 認識機能

機能が、RP スイッチオーバーを経ても、一部または全体が問題なく動作し続ける場合、その機能やプロトコルは SSO 認識です。SSO 認識機能のステート情報は、これらの機能のステートフル スイッチオーバーを実現するために、アクティブからスタンバイへ同期されます。

SSO 非認識の機能の場合、ステートをダイナミックに作成しても、スイッチオーバー時に失われるため、スイッチオーバーの際に再初期化と再起動が必要になります。

show redundancy clients コマンドの出力には、SSO 認識機能が表示されます（「SSO 機能の確認」（P.7-14）を参照）。

SSO のデフォルト設定

なし。

SSO の設定方法

（注） スイッチにイメージをコピーする方法については、第 6 章「高速ソフトウェア アップグレード」を参照してください。アップグレード プロセスでは、さまざまなイメージが非常に短い期間、RP にロードされます。この間にスイッチオーバーが発生すると、デバイスは RPR モードで回復します。

SSO または RPR 冗長モードが常に設定されます。SSO 冗長モードはデフォルトで設定されます。RPR 冗長モードからデフォルト SSO 冗長モードに戻すには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router> 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	`Router# 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	`Router(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 4	`Router(config)# mode sso`	アクティブとスタンバイの両方の RP で、冗長コンフィギュレーション モードを SSO に設定します。 **（注）** SSO モードを設定した後、スタンバイ RP が自動的にリセットされます。
ステップ 5	`Router(config-red)# end`	冗長コンフィギュレーション モードを終了して、スイッチを特権 EXEC モードに戻します。
ステップ 6	`Router# copy running-config startup-config`	コンフィギュレーションの変更をスタートアップ コンフィギュレーション ファイルに保存します。

次に、SSO 冗長モードを設定する例を示します。

```
Router> enable
Router# configure terminal
```

```
Router(config)# redundancy
Router(config)# mode sso
Router(config-red)# end
Router# copy running-config startup-config
Router#
```

SSO のトラブルシューティング

考えられる SSO の問題状況

- スタンバイ RP をリセットしたが、生じた問題を説明するメッセージが表示されない：SSO イベントのログなど、スイッチオーバーやその他のイベントが発生した理由を探る鍵となるものを表示するには、新しくアクティブになった RP で **show redundancy history** コマンドを実行します。

  ```
  Router# show redundancy history
  ```

- **show redundancy states** コマンドを実行すると、ネットワーキング デバイスでの設定内容と異なる動作モードが表示される：特定のプラットフォームで **show redundancy states** コマンドを使用すると、プラットフォームごとに設定されたコンフィギュレーション モードではなく、デバイスで実行されている実際の動作冗長モードが出力表示されることがあります。システムの動作モードは、システム イベントに応じて変化する可能性があります。たとえば、SSO を使用するためには、ネットワーキング デバイス上の両方の RP が同じソフトウェア イメージを実行する必要があります。イメージが異なる場合、デバイスはそのコンフィギュレーションに関係なく、SSO モードでは動作しなくなります。

  たとえば、アップグレード プロセス中にごく短時間、さまざまなイメージが RP にロードされます。この間にスイッチオーバーが発生すると、デバイスは RPR モードで回復します。

- デバイスをリロードすると、SSO の動作が中断する：SSO の機能によって新しいコマンドが導入されましたが、その中に、手動でスイッチオーバーを発生させるコマンドがあります。reload コマンドは SSO コマンドではありません。このコマンドを実行すると、ボックスが完全にリロードされ、すべてのテーブル エントリが削除され、すべてのラインカードがリセットされるので、ネットワーク トラフィック転送が中断されます。誤ってボックスをリロードしないようにするには、**redundancy force-switchover** コマンドを使用します。

- ソフトウェア アップグレードの際、ネットワーキング デバイスが SSO ではないモードで表示される：ソフトウェア アップグレード プロセス中は、show redundancy コマンドを使用するとデバイスが SSO ではないモードで動作していることを示します。

  これは正常な動作です。FSU 手順が完了するまで、各 RP では異なるソフトウェア バージョンが実行されています。RP が異なるソフトウェア バージョンを実行している間、モードはいずれかの RPR に変更されます。アップグレードが完了すれば、デバイスは SSO モードに変更されます。

- コア ダンプが完了する前に以前のアクティブ プロセッサのリセットとリロードが実行される：以前のアクティブ プロセッサのリセットとリロードを実行するまでの新しいアクティブ プロセッサの最大待機時間を設定するには、**crashdump-timeout** コマンドを使用します。

- 「send break」コマンドを発行してもシステムのスイッチオーバーが実行されない：これは通常の動作です。「send break」コマンドを使用して、システムをブレークまたは一時停止することは推奨できません。予期しない結果が生じるおそれがあります。手動のスイッチオーバーを開始するには、**redundancy force-switchover** コマンドを使用します。

Cisco IOS ソフトウェアでは、スイッチを再起動し、起動開始から 60 秒以内に Break キーを押すか Telnet セッションから「send break」コマンドを実行すると、ROM モニタ モードを開始できます。send break 機能は、経験豊富なユーザまたは Cisco Technical Assistance Center（TAC）の担当者の指示によって操作しているユーザが、特定のシステム障害の回復やシステム障害の原因の解明を行うのに役立ちます。

SSO のトラブルシューティング

次の各コマンドは、必要に応じて SSO 機能のトラブルシューティングに使用できます。これらのコマンドには、決まった入力順序はありません。

コマンド	目的
`Router(config-red)# crashdump-timeout [mm | hh:mm]`	新しいアクティブ RP が、それまでアクティブだった RP をリロードするまでに待つ最長時間を設定します。
`Router# debug redundancy {all | ui | clk | hub}`	ネットワーキング デバイスで、冗長をデバッグします。
`Router# show diag [slot-number | chassis | subslot slot/subslot] [details | summary]`	ハードウェア情報を表示します。
`Router# show redundancy [clients | counters | debug-log | handover | history | switchover history | states | inter-device]`	RP の冗長コンフィギュレーション モードを表示します。スイッチオーバーの回数、システム稼働時間、プロセッサ稼働時間、冗長ステート、およびスイッチオーバーの理由に関する情報もあわせて表示します。
`Router# show version`	各 RP に関するイメージ情報を表示します。

SSO 設定の確認

- SSO が設定されていることを確認する
- デバイス上での SSO の動作の確認
- SSO 機能の確認

SSO が設定されていることを確認する

次の例では、**show redundancy** コマンドを使用して、デバイス上に SSO が設定されていることを確認します。

```
Router> enable
Router# show redundancy
Redundant System Information :
------------------------------
       Available system uptime = 3 days, 4 hours, 35 minutes
Switchovers system experienced = 0
              Standby failures = 1
        Last switchover reason = none

                  Hardware Mode = Duplex
    Configured Redundancy Mode = sso
     Operating Redundancy Mode = sso
              Maintenance Mode = Disabled
                Communications = Up
```

```
Current Processor Information :
-------------------------------
               Active Location = slot 5
        Current Software state = ACTIVE
       Uptime in current state = 3 days, 4 hours, 35 minutes
                 Image Version = Cisco IOS Software, s2t54 Software ...
Synced to ...
Copyright (c) 1986-2011 by Cisco Systems, Inc.
Compiled ...
                         BOOT = disk0:0726_c4,12
                  CONFIG_FILE =
                      BOOTLDR =
        Configuration register = 0x2102

Peer Processor Information :
----------------------------
              Standby Location = slot 6
        Current Software state = STANDBY HOT
       Uptime in current state = 3 hours, 55 minutes
                 Image Version = Cisco IOS Software, s2t54 Software ...
Synced to ...
Copyright (c) 1986-2011 by Cisco Systems, Inc.
Compiled ...
                         BOOT = disk0:0726_c4,12
                  CONFIG_FILE =
                      BOOTLDR =
        Configuration register = 0x2102

Router#
```

デバイス上での SSO の動作の確認

次の例では、**show redundancy** コマンドと **states** キーワードを使用して、デバイス上に SSO が設定されていることを確認します。

```
Router# show redundancy states
my state = 13 -ACTIVE
     peer state = 8  -STANDBY HOT
           Mode = Duplex
           Unit = Primary
        Unit ID = 5

Redundancy Mode (Operational) = sso
Redundancy Mode (Configured)  = sso
Redundancy State              = sso
     Maintenance Mode = Disabled
    Manual Swact = enabled
 Communications = Up

   client count = 135
 client_notification_TMR = 30000 milliseconds
          keep_alive TMR = 9000 milliseconds
        keep_alive count = 1
    keep_alive threshold = 18
           RF debug mask = 0x0

Router#
```

SSO 機能の確認

SSO 機能として登録された機能のリストを表示するには、**show redundancy clients** コマンドを入力します。

```
Router# show redundancy clients
 clientID = 0       clientSeq = 0       RF_INTERNAL_MSG
 clientID = 1319    clientSeq = 1       Cat6k Platform First
 clientID = 29      clientSeq = 60      Redundancy Mode RF
 clientID = 139     clientSeq = 61      IfIndex
 clientID = 3300    clientSeq = 62      Persistent Variable
 clientID = 25      clientSeq = 68      CHKPT RF
 clientID = 1515    clientSeq = 69      HAL RF
 clientID = 3100    clientSeq = 73      MCM
 clientID = 77      clientSeq = 80      Event Manager
 clientID = 1328    clientSeq = 81      Cat6k Asic API RF Cl
 clientID = 1334    clientSeq = 82      Cat6k AUTOSHUT RF Cl
 clientID = 1333    clientSeq = 83      Cat6k OVERSUB RF Cli
 clientID = 1302    clientSeq = 84      Cat6k Fabric Manager
 clientID = 1331    clientSeq = 86      Cat6k Inline Power
 clientID = 1303    clientSeq = 88      Cat6k OIR
 clientID = 518     clientSeq = 89      PM Port Data
 clientID = 1306    clientSeq = 93      Cat6k QoS Manager
 clientID = 1501    clientSeq = 98      Cat6k CWAN HA
 clientID = 1503    clientSeq = 99      CWAN VLAN RF Client
 clientID = 1310    clientSeq = 100     Cat6k Feature Manage
 clientID = 1700    clientSeq = 101     Cat6k L3 Lif
 clientID = 78      clientSeq = 102     TSPTUN HA
 clientID = 305     clientSeq = 103     Multicast ISSU Conso
 clientID = 304     clientSeq = 104     IP multicast RF Clie
 clientID = 22      clientSeq = 105     Network RF Client
 clientID = 88      clientSeq = 106     HSRP
 clientID = 114     clientSeq = 107     GLBP
 clientID = 225     clientSeq = 108     VRRP
 clientID = 1505    clientSeq = 111     Cat6k SPA TSM
 clientID = 1509    clientSeq = 114     Cat6k Online Diag HA
 clientID = 1337    clientSeq = 116     Cat6k MPLS RF Client
 clientID = 75      clientSeq = 120     Tableid HA
 clientID = 1338    clientSeq = 124     Cat6k CTS Manager
 clientID = 512     clientSeq = 126     LAN-Switch BD Manage
 clientID = 501     clientSeq = 127     LAN-Switch VTP VLAN
 clientID = 513     clientSeq = 128     LAN-Switch IDBHAL
 clientID = 71      clientSeq = 129     XDR RRP RF Client
 clientID = 24      clientSeq = 130     CEF RRP RF Client
 clientID = 146     clientSeq = 132     BFD RF Client
 clientID = 301     clientSeq = 135     MRIB RP RF Client
 clientID = 306     clientSeq = 139     MFIB RRP RF Client
 clientID = 1504    clientSeq = 146     Cat6k CWAN Interface
 clientID = 1507    clientSeq = 147     CWAN LTL Mgr HA RF C
 clientID = 520     clientSeq = 151     RFS RF
 clientID = 210     clientSeq = 152     Auth Mgr
 clientID = 5       clientSeq = 153     Config Sync RF clien
 clientID = 138     clientSeq = 155     MDR SM
 clientID = 1308    clientSeq = 156     Cat6k Local Target L
 clientID = 1351    clientSeq = 157     RF VS Client
 clientID = 1358    clientSeq = 158     Cat6k VSlot
 clientID = 502     clientSeq = 162     LAN-Switch Port Mana
 clientID = 514     clientSeq = 163     SWITCH_VLAN_HA
 clientID = 1313    clientSeq = 165     Cat6k Platform
 clientID = 1318    clientSeq = 166     Cat6k Power
 clientID = 23      clientSeq = 171     Frame Relay
 clientID = 49      clientSeq = 172     HDLC
 clientID = 72      clientSeq = 173     LSD HA Proc
```

```
clientID = 113     clientSeq = 174      MFI STATIC HA Proc
clientID = 1335    clientSeq = 180      C6K EFP RF client
clientID = 200     clientSeq = 181      ETHERNET OAM RF
clientID = 207     clientSeq = 183      ECFM RF
clientID = 202     clientSeq = 184      ETHERNET LMI RF
clientID = 208     clientSeq = 186      LLDP
clientID = 20      clientSeq = 193      IPROUTING NSF RF cli
clientID = 21      clientSeq = 197      PPP RF
clientID = 1352    clientSeq = 201      C6K_provision_rf_cli
clientID = 1307    clientSeq = 202      Cat6k IDPROM
clientID = 74      clientSeq = 206      MPLS VPN HA Client
clientID = 34      clientSeq = 208      SNMP RF Client
clientID = 1502    clientSeq = 209      CWAN APS HA RF Clien
clientID = 52      clientSeq = 210      ATM
clientID = 35      clientSeq = 219      History RF Client
clientID = 90      clientSeq = 231      RSVP HA Services
clientID = 250     clientSeq = 243      EEM Server RF CLIENT
clientID = 252     clientSeq = 245      EEM POLICY-DIR RF CL
clientID = 54      clientSeq = 247      SNMP HA RF Client
clientID = 73      clientSeq = 248      LDP HA
clientID = 76      clientSeq = 249      IPRM
clientID = 57      clientSeq = 250      ARP
clientID = 50      clientSeq = 257      FH_RF_Event_Detector
clientID = 1508    clientSeq = 263      CWAN LTL SP RF Clien
clientID = 1304    clientSeq = 267      Cat6k Ehc
clientID = 1305    clientSeq = 271      Cat6k PAgP/LACP
clientID = 503     clientSeq = 272      Spanning-Tree Protoc
clientID = 1309    clientSeq = 273      CMRP RF Client
clientID = 1311    clientSeq = 275      Cat6k L3 Manager
clientID = 1317    clientSeq = 276      Cat6k CAPI
clientID = 1506    clientSeq = 277      CWAN SRP RF Client
clientID = 83      clientSeq = 284      AC RF Client
clientID = 145     clientSeq = 285      VFI Mgr
clientID = 84      clientSeq = 286      AToM manager
clientID = 85      clientSeq = 287      SSM
clientID = 87      clientSeq = 291      SLB RF Client
clientID = 504     clientSeq = 294      Switch SPAN client
clientID = 507     clientSeq = 295      Switch Backup Interf
clientID = 105     clientSeq = 298      DHCP Snooping
clientID = 1510    clientSeq = 304      Call-Home RF
clientID = 203     clientSeq = 307      MVRP RF
clientID = 151     clientSeq = 310      IP Tunnel RF
clientID = 94      clientSeq = 311      Config Verify RF cli
clientID = 516     clientSeq = 314      EnergyWise rf client
clientID = 508     clientSeq = 316      Port Security Client
clientID = 509     clientSeq = 317      LAN-Switch IP Host T
clientID = 515     clientSeq = 318      SISF table
clientID = 135     clientSeq = 322      IKE RF Client
clientID = 136     clientSeq = 323      IPSEC RF Client
clientID = 130     clientSeq = 324      CRYPTO RSA
clientID = 400     clientSeq = 326      IP Admission RF Clie
clientID = 3099    clientSeq = 335      ISSU process
clientID = 4005    clientSeq = 338      ISSU Test Client
clientID = 93      clientSeq = 342      Network RF 2 Client
clientID = 1320    clientSeq = 343      Cat6k PF_ML_RP
clientID = 510     clientSeq = 345      LAN-Switch PAgP/LACP
clientID = 511     clientSeq = 346      LAN-Switch Private V
clientID = 1321    clientSeq = 347      PM SP client
clientID = 1322    clientSeq = 348      VLAN Mapping
clientID = 1315    clientSeq = 350      Cat6k Clear Counter
clientID = 141     clientSeq = 352      DATA DESCRIPTOR RF C
clientID = 1000    clientSeq = 361      CTS HA
clientID = 1001    clientSeq = 362      Keystore
clientID = 3150    clientSeq = 363      SIA SD RF CLIENT
```

```
clientID = 3151    clientSeq = 364      SIA SB RF CLIENT
clientID = 3152    clientSeq = 365      SIA SCL RF CLIENT
clientID = 3153    clientSeq = 366      SIA SVE RF CLIENT
clientID = 3154    clientSeq = 367      SIA TCP RF CLIENT
clientID = 1332    clientSeq = 373      PCLC
clientID = 1367    clientSeq = 375      Cat6k ITASCA_RP
clientID = 4032    clientSeq = 379      ACL handle RF Client
clientID = 4020    clientSeq = 381      IOS Config ARCHIVE
clientID = 4021    clientSeq = 382      IOS Config ROLLBACK
clientID = 1339    clientSeq = 404      Cat6k blue beacon RF
clientID = 1362    clientSeq = 405      VS HA
clientID = 517     clientSeq = 406      LAN-Switch IDBHAL2
clientID = 1336    clientSeq = 415      Cat6k NTI SUP SI swi
clientID = 65000   clientSeq = 416      RF_LAST_CLIENT
```

SSO の設定例

次に、SSO 冗長モードを設定する例を示します。

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# mode sso
Router(config-red)# exit
Router# copy running-config startup-config
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CHAPTER 8

Nonstop Forwarding（NSF）

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。
- ステートフル スイッチオーバー（SSO）およびノンストップ フォワーディング（NSF）は IPv6 マルチキャスト トラフィックをサポートしません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

NSF の前提条件

なし。

NSF の制約事項

一般的な制約事項

- NSF には SSO が必要です（第 7 章「ステートフル スイッチオーバー（SSO）」を参照）。
- ホット スタンバイ ルーティング プロトコル（HSRP）は、Cisco NSF/SSO でサポートされていません。HSRP を Cisco NSF/SSO で使用しないでください。

BGP NSF の制限

- BGP NSF に参加するすべてのネイバー デバイスが NSF 対応である必要があり、「NSF の BGP の設定および検証」（P.8-9）で説明されているように、BGP グレースフル リスタートが設定されます。

EIGRP NSF の制約事項

- EIGRP NSF 稼働に関与しているすべての隣接デバイスが NSF に対応または NSF を認識する必要があります。
- NSF 認識ルータは、2 台の NSF 対応ピアが 1 つの NSF の再起動処理を同時に実行することはサポートしません。ただし、NSF 再起動処理が完了した後で、両方のネイバーがピアリング セッションを確立します。

OSPF NSF の制約事項

- 仮想リンク用 OSPF NSF はサポートされません。
- 同じネットワーク セグメント上のすべての OSPF ネットワーキング デバイスは、NSF 認識（NSF ソフトウェア イメージを稼働）である必要があります。
- シャム リンクの OSPF NSF はサポートされていません。

IS-IS NSF の制約事項

- IETF IS-IS の場合、ネイバー デバイスはすべて NSF 認識ソフトウェア イメージを稼働する必要があります。

IPv6 NSF の制限

- IPv6 NSF をサポートするため、ルータで IPv6 をイネーブルにする必要があります。

NSF について

NSF の概要

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 の主な目的は、ルート プロセッサ（RP）のスイッチオーバー後に、引き続き IP パケットを転送することです。

通常、ネットワーキング 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したルーティング フラップによって、ルーティングが不安定になります。これは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。データ トラフィックはインテリジェント ラインカードを介して転送されますが、スタンバイ RP では、スイッチオーバー中に障害が発生したアクティブな RP からの制御と見なされます。ラインカードの機能はスイッチオーバーの前後で維持され、アクティブな RP の転送情報ベース（FIB）が Cisco NSF 動作で最新状態が維持されます。

Cisco NSF 機能には、次のような複数の利点があります。

- 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。
- ネットワーク全体の安定性：ネットワークの安定性は、ネットワーク内でルータに障害が発生し、ルーティング テーブルが失われたときに作成されるルート フラップの数を減らすことで改善できます。
- 隣接ルータによるリンクのフラッピングの検出防止：インターフェイスが、スイッチオーバー中もアップ状態を維持するので、隣接ルータはリンク フラップを検出しません（つまり、リンクがダウンして、再度アップするということが起こりません）。
- ルーティング フラップの防止：SSO はスイッチオーバーの際もネットワーク トラフィックの転送を続けるので、ルーティング フラップが回避されます。
- ユーザ セッションの維持：スイッチオーバーの前に確立されたユーザセッションは、スイッチオーバを経ても維持されます。

ネットワーキング デバイスが NSF 互換ソフトウェアを実行している場合、このデバイスは NSF 認識です。デバイスが NSF をサポートするように設定されている場合、デバイスは NSF 対応で、NSF 認識または NSF 対応ネイバーからルーティング情報を再構築します。

CEF は、Catalyst 6500 シリーズ スイッチで常にイネーブルにされ、ディセーブルにできません。ルーティング プロトコルは、スイッチオーバー中にルーティング情報ベース（RIB）テーブルを再構築している間、CEF に依存してパケット フォワーディングを行います。ルーティング プロトコルのコンバージェンスが完了すると、CEF は FIB テーブルを更新し、失効したルート エントリを削除し、CEF はラインカードを新しい FIB 情報で更新します。

NSF による相互作用機能

シスコ エクスプレス フォワーディング

NSF の重要な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、パケットの転送は CEF によって行われます。CEF は、Catalyst 6500 シリーズ スイッチで常にイネーブルにされ、ディセーブルにできません。CEF は FIB を維持し、スイッチオーバー時の FIB 情報を使用してスイッチオーバー中にパケットを転送し続けます。この機能により、スイッチオーバー中のトラフィックの中断を短くします。

通常の NSF 操作中に、アクティブなルート プロセッサ（RP）上の CEF は、現在の FIB と隣接データベースを、スタンバイ RP 上の FIB と隣接データベースと同期させます。アクティブな RP のスイッチオーバー時に、スタンバイ RP には最初、アクティブな RP 上で最新だったもののミラー イメージである FIB と隣接データベースがあります。インテリジェント ラインカードを備えたプラットフォームでは、ラインカードはスイッチオーバーの前後で現行の転送情報を維持します。フォワーディング エンジンを備えたプラットフォームでは、CEF は、アクティブな RP の CEF によって送信される変更を使用して、スタンバイ RP のフォワーディング エンジンを最新の状態に保ちます。この方法では、フォワーディング エンジンのラインカードは、インターフェイスとデータ パスが使用可能になるとすぐに、スイッチオーバー後に転送を続行できます。

ルーティング プロトコルがプレフィックスごとに RIB を再び読み込み始めるため、CEF に対してプレフィックスごとの更新が行われます。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。既存または新規エントリは、リフレッシュされたことを示す新しいバージョン（「エポック」）番号を受信します。転送情報はラインカードまたは収束中のフォワーディング エンジンで更新されます。RIB が収束すると、RP が信号通知を行います。ソフトウェアは、現在のスイッチオーバー エポックよりも前のエポックを持った FIB および隣接エントリをすべて削除します。これで FIB は最新のルーティング プロトコル転送情報を表示するようになります。

ルーティング プロトコルの動作

ルーティング プロトコルは、アクティブな RP だけで実行され、隣接ルータからルーティングの更新を受信します。ルーティング プロトコルは、スタンバイ RP では実行されません。スイッチオーバーのあとルーティング プロトコルは、NSF 認識ネイバー デバイスがルーティング テーブルを再構築するス

テート情報を送信するよう要求します。またこの代わりに、ネイバー 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 RP のステート情報をスタンバイ RP と同期させるように、IS-IS プロトコルを設定できます。

NSF 動作の場合、ルーティング プロトコルは、ルーティング情報を再構築している間にパケットを転送し続ける CEF によって異なります。

BGP の動作

NSF 対応ルータは、BGP ピアと BGP セッションを開始すると、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」があることを示す宣言が含まれています。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 ピアがこの機能を受信した場合、メッセージを送信するデバイスが NSF 対応であることを認識しています。NSF 対応ルータ ピアおよび BGP ピアは両方ともセッションの確立時に、OPEN メッセージ内でグレースフル リスタート機能を交換する必要があります。両方のピアがグレースフル リスタート機能を交換しない場合、セッションはグレースフル リスタート対応になりません。

RP 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 対応ルータに関連付けられ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 RP 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ぐことができます。

RP のスイッチオーバーが発生した後、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時に、NSF 対応ルータが再起動したことを識別する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 ピアの間で交換されます。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ます。この後 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 セッションは確立されます。この機能により、非 NSF 認識 BGP ピアとのインターオペラビリティ（および NSF 機能が無いインターオペラビリティ）を可能にしますが、非 NSF 認識 BGP ピアでの BGP セッションはグレースフル リスタート対応になりません。

（注） NSF の BGP サポートでは、ネイバー ネットワーキング デバイスが NSF 認識である必要があります。つまり、デバイスにはグレースフル リスタート機能があり、セッション確立中に OPEN メッセージ内でこ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した場合、そのネイバーとの NSF 対応セッションを確立しません。グレースフル リスタート機能のある他のネイバーはすべて、NSF 対応ネットワーキング デバイスとの NSF 対応セッションを維持し続けます。

EIGRP の動作

EIGRP NSF 機能は、hello パケットで EIGRP ピアと交換されます。NSF 対応ルータは、hello パケットで再起動（RS）ビットを設定したことによって NSF の再起動処理が開始されたことをネイバーに通知します。NSF 認識ルータが NSF 対応ネイバーから、NSF の再起動処理が進行中であるという通知を受け取ると、NSF 対応ルータと NSF 認識ルータは、即座にそれぞれのトポロジ テーブルを交換しま

す。トポロジ テーブルの送信が完了すると、NSF 認識ルータは end-of-table（EOT）アップデート パケットを送信します。次に NSF 認識ルータは、NSF 対応ルータを支援するために次のアクションを実行します。

- EIGRP hello ホールド タイマーの期限を終了し、hello パケットの生成および送信の間隔を短くします。これにより、NSF 認識ルータは NSF 対応ルータにより早く応答し、NSF 対応ルータがネイバーを再検出し、トポロジ テーブルを再構築するために必要な時間を短縮します。
- ルート ホールド タイマーが開始されます。このタイマーを使用して、NSF 認識ルータが NSF 対応ネイバーに対する既知のルートを保持している期間を設定します。このタイマーは、**timers nsf route-hold** コマンドで設定されます。デフォルトの期間は 240 秒です。
- NSF 認識ルータは、ピア リストに、NSF 対応のネイバーが再起動していることを記録するとともに、このネイバーからトポロジ テーブルを送信するように信号通知されるか、またはルート ホールド タイマーが期限切れになるまで、隣接関係を維持し、NSF 対応のネイバーの既知のルートを保持します。NSF 認識ルータでルート ホールド タイマーが期限切れになった場合、NSF 認識ルータは保留中のルートを廃棄し、NSF 対応ルータをネットワークに参加した新しいルータとして扱って、新しいルータに対して行うように隣接関係を再度確立します。
- NSF 認識ルータは、スイッチオーバーの後なおコンバージェンスしている NSF 対応ルータにクエリーを送信し続けることによって、Stuck In Active（SIA）状態が発生するまでの時間を効果的に延長します。

スイッチオーバー処理が完了すると、NSF 対応ルータは、サポートしているルータに対して EOT アップデート パケットを送信することによって、再コンバージェンスされたこと、およびすべてのトポロジ テーブルを受信したことをネイバーに通知します。その後、NSF 対応ルータは通常の処理に戻ります。NSF 認識ルータは、（再起動中の）NSF 対応ルータでリフレッシュされないルートに対して、（アクティブな）別のパスを探します。その後、NSF 認識ルータは通常の処理に戻ります。NSF 対応ルータによってすべてのパスがリフレッシュされると、NSF 認識ルータはすぐに通常の処理に戻ります。

（注）　NSF 認識ルータは、EIGRP ネットワーク内で NSF 非認識ネイバーまたは NSF 非対応ネイバーと完全に共存できます。NSF 非認識ネイバーは、NSF 対応を無視し、隣接関係をリセットするか、そうでなければピア セッションを正常に維持します。

IS-IS の動作

ピア デバイスから受信した情報の代わりに、アクティブおよびスタンバイの RP 間で同期されているステート情報を使用して、スイッチオーバー以降のルート情報を回復するよう IS-IS プロトコルを設定できます。

IS-IS NSF 対応ルータが RP 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 2 つの処理を実行する必要があります。まず、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。次に、ネットワークに関するリンク ステート データベースの内容を再度取得します。

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

ネットワーク セグメント上の隣接ルータが NSF 認識の場合、つまり隣接ルータが、ルータの再起動可能性についての 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、それらのルータは、再起動中の IETF NSF ルータをサポートします。IETF を使用する場合、隣接ルータはスイッチオーバー後のルーティング情報を再構築する隣接情報およびリンク ステート情報を提供します。IETF IS-IS コンフィギュレーションの利点は、提案された標準に基づいたピア デバイスの間の動作であることです。

（注）　ネットワーキング デバイスに IETF を設定する場合で隣接ルータが IETF と互換性がないとき、NSF はスイッチオーバー後に中断します。

ネットワーク セグメント上の隣接ルータが NSF 認識でない場合、シスコのコンフィギュレーション 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 RP からスタンバイ RP に転送します。シスコのコンフィギュレーションの利点は、NSF 認識ネイバーに依存していないことです。

IETF IS-IS コンフィギュレーション

NSF 対応ルータは、IETF IS-IS コンフィギュレーションを使用して、RP スイッチオーバーの後できるだけ迅速に、ネイバー NSF 認識デバイスに IS-IS NSF 再起動要求を送信します。ネイバー 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指示として認識します。再起動するルータがネットワーク上のルータから再起動要求を受信すると、ネイバー リストの再構築を始めます。

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 が完全にコンバージェンスされます。

あるスーパーバイザ エンジンから別の RP へのスイッチオーバーは、数秒間以内に発生します。IS-IS はルーティング テーブルを再構築し、数秒以内にネットワークと同期化します。この時点で IS-IS は次の NSF 再起動を実行する前に、指定された時間の間、待機します。この間に、新しいスタンバイ RP が起動し、そのコンフィギュレーションをアクティブ RP に同期します。IS-IS NSF を再起動しようとする前に接続を安定させるため、IS-IS NSF 動作は指定された時間の間、待機します。この機能は、IS-IS が失効情報で back-to-back NSF を再起動しないようにします。

Cisco IS-IS コンフィギュレーション

Cisco コンフィギュレーション オプションを使用することで、すべての隣接および LSP 情報を保存するか、スタンバイ RP に「チェックポイント」として設定されます。スイッチオーバーのあと、新しくアクティブになった RP はチェックポイント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アップ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アップにならない場合、これらのネイバー 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アップ状態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 RP へのスイッチオーバーは、数秒間以内に発生します。IS-IS はルーティング テーブルを再構築し、数秒以内にネットワークと同期化します。この時点で IS-IS は次の NSF 再起動を実行する前に、指定された時間の間、待機します。この間に、新しいスタンバイ RP が起動し、そのコンフィギュレーションをアクティブ RP に同期します。この同期が完了したあと、IS-IS 隣接および LSP データにスタンバイ RP のチェックポイントが設定されます。ただし、新しい NSF 再起動は、この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 がバックツーバック NSF 再起動を試行しないようにします。

OSPF の動作

OSPF NSF 対応ルータが RP 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 2 つの処理を実行する必要があります。まず、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。次に、ネットワークに関するリンク ステート データベースの内容を再度取得します。

NSF 対応ルータは、RP スイッチオーバーの後できるだけ迅速に、ネイバー NSF 認識デバイスに OSPF NSF 信号を送信します。ネイバー 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指示として認識します。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、ネイバー リストの再構築を始めます。

ネイバー関係が再構築されると、NSF 対応ルータはすべての NSF 認識ネイバーとデータベースの再同期化を始めます。この時点でルーティング情報は OSPF ネイバーの間で交換されます。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、失効ルートを削除し、RIB を更新して、新しい転送情報で FIB を更新します。その後、OSPF プロトコルは完全に収束されます。

（注）　OSPF NSF では、すべてのネイバー ネットワーク デバイスが NSF 認識である必要があります。NSF 対応ルータが特定のネットワーク セグメント上に NSF 認識ネイバーがないことを検出した場合、ルータはそのセグメントの NSF 機能をディセーブルにします。全体が NSF 対応または NSF 認識ルータで構成された他のネットワーク セグメントは、NSF 機能を提供し続けます。

OSPF RFC 3623 のグレースフル リスタート機能を使用すると、マルチベンダー ネットワークにおいて IETF NSF を設定できます。詳細については、『*OSPF RFC 3623 Graceful Restart*』マニュアルを参照してください。

IPv6 ルーティング プロトコルの動作

NSF の IPv6 サポートには、次の機能があります。

- 「MP-BGP IPv6 アドレス ファミリのノンストップ フォワーディングおよびグレースフル リスタート」（P.8-8）
- 「IPv6 RIP のノンストップ フォワーディング」（P.8-9）
- 「IPv6 スタティック ルートでのノンストップ フォワーディング」（P.8-9）

MP-BGP IPv6 アドレス ファミリのノンストップ フォワーディングおよびグレースフル リスタート

グレースフル リスタート機能は、IPv6 BGP ユニキャスト、および VPNv6 アドレス ファミリでサポートされ、BGP IPv6 で Cisco NSF 機能を実現しています。BGP グレースフル リスタート機能を使用すると、TCP 状態を維持することなく、BGP ルーティング テーブルをピアから回復できます。

NSF では、ルーティング プロトコルのコンバージェンス時にも引き続きパケットが転送されるため、スイッチオーバー時のルート フラップが回避されます。転送は、アクティブ RP とスタンバイ RP 間で FIB を同期することで維持されます。スイッチオーバー時、転送は FIB を使用して維持されます。RIB の同期は維持されないため、RIB はスイッチオーバー時に空になります。RIB は、ルーティング プロトコルによって再入力され、次に、NSF_RIB_CONVERGED レジストリ コールを使用して RIB コンバージェンスに関する情報を FIB に伝えます FIB テーブルは、RIB から更新され、古いエントリが削除されます。RIB は、ルーティング プロトコルが RIB のコンバージェンスの通知に失敗した場合、RP スイッチオーバー時にフェールセーフ タイマーを開始します。

Cisco BGP Address Family Identifier（AFI）モデルは、モジュラ式で拡張性に優れ、複数の AFI 設定および Subsequent Address Family Identifier（SAFI）設定をサポートします。

IPv6 BGP グレースフル リスタート機能を設定する方法については『*Implementing Multiprotocol BGP for IPv6*』マニュアルを参照してください。

IPv6 RIP のノンストップ フォワーディング

RIP は IPv6 NSF クライアントとして登録されます。これにより、RIP がスタンバイ上で収束を完了するまで、シスコ エクスプレス フォワーディング テーブルにインストールされている RIP ルートを使用できるという利点が得られます。

IPv6 スタティック ルートでのノンストップ フォワーディング

Cisco NSF は IPv6 スタティック ルートをサポートしています。

NSF のデフォルト設定

なし。

NSF の設定方法

- 「NSF の BGP の設定および検証」（P.8-9）（任意）
- 「EIGRP NSF の設定および検証」（P.8-10）（任意）
- 「OSPF NSF の設定および検証」（P.8-12）（任意）
- 「IS-IS NSF の設定および検証」（P.8-13）（任意）
- 「Cisco Nonstop Forwarding のトラブルシューティング」（P.8-15）（任意）

NSF の BGP の設定および検証

- 「NSF の BGP の設定」（P.8-9）
- 「BGP での NSF の確認」（P.8-10）

NSF の BGP の設定

NSF の BGP を設定するには、次の作業を実行します。この作業は各 BGP NSF ピア デバイスで繰り返します。

	コマンド	目的
ステップ 1	`Router> 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	`Router# 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。

	コマンド	目的
ステップ 3	`Router(config)# router bgp autonomous-system-number`	BGP ルーティング プロセスをイネーブルにし、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 4	`Router(config-router)# bgp graceful-restart [restart-time seconds | stalepath-time seconds]`	BGP 対応の NSF を開始する BGP グレースフル リスタート機能をイネーブルにします。

次に、NSF の BGP を設定する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# router bgp 120
Router(config-router)# bgp graceful-restart
```

BGP での NSF の確認

グレースフル リスタート機能が SSO 対応ネットワーキング デバイスおよびネイバー デバイス上で設定されているか確認するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router> 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	`Router# show running-config`	現在実行されているコンフィギュレーション ファイルの内容を表示します 「bgp graceful-restart」のフレーズが SSO 対応ルータの BGP コンフィギュレーションに表示されていることを確認します。 各 BGP ネイバーでこの手順を繰り返します。
ステップ 3	`Router# show ip bgp neighbors [ip-address [advertised-routes | dampened-routes | flap-statistics | paths [reg-exp] | received prefix-filter | received-routes | routes | policy [detail]]]`	ネイバーに対する BGP 接続と TCP 接続に関する情報を表示します。 SSO デバイスおよびネイバー デバイスで、このコマンドはグレースフル リスタート機能がアドバタイズおよび受信されたことを示していることを検証し、グレースフル リスタート機能を備えたアドレス ファミリであることを確認します。アドレス ファミリが表示されない場合、BGP NSF も発生しません。

次に、BGP の NSF を確認する例を示します。

```
Router> enable
Router# configure terminal
Router# show running-config
Router# show ip bgp neighbors
```

EIGRP NSF の設定および検証

NSF の EIGRP の設定

（注）
- NSF 認識ルータがネットワークと完全にコンバージェンスされて、NSF 再起動処理で NSF 対応ルータを支援できる状態になっている必要があります。
- サポートされているバージョンの Cisco IOS ソフトウェアが動作する分散プラットフォームは、完全な NSF 機能をサポートできます。このようなルータは、再起動処理を実行するとともに、他の NSF 対応のピアをサポートできます。
- サポートされているバージョンの Cisco IOS ソフトウェアが動作するシングル プロセッサ プラットフォームは、NSF 認識のみをサポートします。サポートされている NSF 認識ルータは、NSF 対応ルータからトポロジ テーブルの送信を指示するか信号が届くか、またはルート ホールド タイマーが期限切れになるまで、隣接関係を維持し、NSF 対応のネイバーへの既知のルートを保持します。

NSF の EIGRP を設定するには、次の作業を実行します。この作業は各 EIGRP NSF ピア デバイスで繰り返します。

	コマンド	目的
ステップ 1	`Router> 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	`Router# 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	`Router(config)# router eigrp` *as-number*	EIGRP ルーティング プロセスをイネーブルにして、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 4	`Router(config-router)# nsf` [{**cisco** | **ietf**} | **interface wait** *seconds* | **interval** *minutes* | **t3** [**adjacency** | **manual** *seconds*]	（任意）NSF 対応ルータで EIGRP NSF サポートをイネーブルにします。このコマンドは、NSF 対応ルータでのみ入力します。サポートする Cisco IOS ソフトウェアバージョンが、NSF 対応または NSF 認識をサポートするルータにインストールされている場合は、NSF 認識はデフォルトでイネーブルになっています。
ステップ 5	`Router(config-router)# timers nsf converge` *seconds*	再起動しているルータが NSF 対応または NSF 認識ピアから EOT 通知を待機する最大時間を調整します。
ステップ 6	`Router(config-router)# timers nsf route-hold` *seconds*	EIGRP を実行している NSF 認識ルータが、非アクティブなピア用のルートを保持する期間を決定するために、ルート ホールド タイマーを設定します。
ステップ 7	`Router(config-router)# timers nsf signal` *seconds*	初期再起動期間の最大時間を調整します。

次に、NSF の EIGRP を設定する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# router eigrp 109
Router(config-router)# nsf
Router(config-router)# timers nsf converge 60
Router(config-router)# timers nsf route-hold 120
```

```
Router(config-router)# timers nsf signal seconds
```

NSF での EIGRP の確認

NSF 認識または NSF 対応、またはその両方が SSO 対応ネットワーキング デバイスおよびネイバー デバイス上で設定されているか確認するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router> 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	`Router# show ip protocols`	アクティブ ルーティング プロトコル プロセスのパラメータと現在の状態を表示します。 各 EIGRP ネイバーでこの手順を繰り返します。

次に、NSF の EIGRP を確認する例を示します。

```
Router> enable
Router# show ip protocols
```

OSPF NSF の設定および検証

- 「NSF OSPF の設定」（P.8-12）
- 「NSF での OSPF の確認」（P.8-13）

NSF OSPF の設定

（注）　OSPF NSF に参加するすべてのピア デバイスは、OSPF NSF 認識にされなければなりません。サポートする Cisco IOS ソフトウェアのバージョンが NSF 対応または NSF 認識をサポートするルータにインストールされている場合は、NSF 認識はデフォルトでイネーブルになっています。

NSF の OSPF 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	`Router> 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	`Router# 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	`Router(config)# router ospf process-id [vrf vpn-name]`	OSPF ルーティング プロセスをイネーブルにし、ルータをルータ コンフィギュレーション モードにします。
ステップ 4	`Router(config-router)# nsf [{cisco | ietf} | interface wait seconds | interval minutes | t3 [adjacency | manual seconds]`	NSF 対応ルータで EIGRP NSF サポートをイネーブルにします。 • このコマンドは、NSF 対応ルータでのみ入力します。

次に、NSF の OSPF を設定する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# router ospf 12
Router(config-router)# nsf
```

NSF での OSPF の確認

NSF の OSPF を確認するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router> 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	`Router# show ip ospf [process-id]`	OSPF ルーティング プロセスに関する一般情報を表示します。

次に、NSF の OSPF を確認する例を示します。

```
Router> enable
Router# show ip ospf
```

IS-IS NSF の設定および検証

IS-IS の NSF の設定

IS-IS の NSF 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	`Router> 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	`Router# 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	`Router(config)# router isis area-tag`	IS-IS ルーティング プロトコルをイネーブルにして IS-IS プロセスを指定し、ルータをルータ コンフィギュレーション モードにします。

	コマンド	目的
ステップ 4	Router(config-router)# **nsf** [{**cisco** | **ietf**} | **interface wait** *seconds* | **interval** *minutes* | **t3** [**adjacency** | **manual** *seconds*]	IS-IS 用 NSF をイネーブルにします。 • **ietf** : IETF ドラフトベースの再起動をサポートするネットワーキング デバイスとの隣接関係がサポートしている同種ネットワークで IS-IS をイネーブルにする。 • **cisco** : NSF 認識ネットワーキング デバイスとの隣接関係がない同種ネットワークで IS-IS を実行する。
ステップ 5	Router(config-router)# **nsf interval** *minutes*	Cisco NSF 再起動試行の間隔の最小時間を設定します。
ステップ 6	Router(config-router)# **nsf t3** {**manual** *seconds* | **adjacency**}	IETF NSF が過負荷になっているリンクのステート情報を生成して、その情報をネイバーにフラッディングする前に、リンク ステート パケット（LSP）データベースが同期するまで IETF Cisco NSF が待機する時間の決定に使用される方法を指定します。
ステップ 7	Router(config-router)# **nsf interface wait** *seconds*	Cisco NSF 再起動時に、再起動が完了する前に IS-IS 隣接関係を持つすべてのインターフェイスがアップするまで待機する時間を指定します。

次に、IS-IS の NSF を設定する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# router isis cisco1
Router(config-router)# nsf ietf
Router(config-router)# nsf interval 2
Router(config-router)# nsf t3 manual 40
Router(config-router)# nsf interface wait 15
```

IS-IS の NSF の確認

IS-IS の NSF 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	Router> **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	Router# **show running-config**	現在実行されているコンフィギュレーション ファイルの内容を表示します
ステップ 3	Router# **show isis nsf**	IS-IS NSF に関する現在のステート情報を表示します。

次に、IS-IS の NSF を確認する例を示します。

```
Router> enable
Router# show running-config
Router# show isis nsf
```

Cisco Nonstop Forwarding のトラブルシューティング

Cisco Nonstop Forwarding をトラブルシューティングするには、必要に応じて次のコマンドを使用します。

コマンド	目的
Router# **debug eigrp nsf**	EIGRP ルーティング プロセスの NSF イベントに関する通知と情報を表示します。
Router# **debug ip eigrp notifications**	EIGRP ルーティング プロセスの情報と通知を表示します。この出力には、NSF 通知とイベントが含まれています。
Router# **debug isis nsf** [**detail**]	Cisco NSF の再起動時の IS-IS ステートに関する情報を表示します。
Router# **debug ospf nsf** [**detail**]	OSPF Cisco NSF コマンドに関するデバッグ メッセージが表示されます。
Router# **show cef nsf**	アクティブ RP とスタンバイ RP の両方における CEF の現在の NSF ステートを表示します。
Router# **show cef state**	ネットワーキング デバイスでの CEF ステートを表示します。
Router# **show clns neighbors**	エンド システムと中継システムの両方のネイバーを表示します。
Router# **show ip bgp**	BGP ルーティング テーブル内のエントリを表示します。
Router# **show ip bgp neighbor**	ネイバー デバイスへの TCP 接続および BGP 接続についての情報を表示します。
Router# **show ip cef**	未解決の FIB エントリを表示するか、FIB の要約を表示します。
Router# **show ip eigrp neighbors** [*interface-type* | *as-number* | **static** | **detail**]	EIGRP によって検出されたネイバーについての詳細情報を表示します。
Router# **show ip ospf**	OSPF ルーティング プロセスに関する一般情報を表示します。
Router# **show ip ospf neighbor** [**detail**]	OSPF のネイバー情報をインターフェイス単位で表示します。
Router# **show ip protocols**	アクティブ ルーティング プロトコル プロセスのパラメータと現在の状態を表示します。EIGRP NSF 設定のステータスとサポートが出力に表示されます。
Router# **show isis database** [**detail**]	IS-IS リンクステート データベースを表示します。
Router# **show isis nsf**	IS-IS Cisco NSF に関する現在のステート情報を表示します。

NSF の設定例

- 「例：BGP NSF の設定」（P.8-16）
- 「例：BGP NSF の隣接デバイスの設定」（P.8-16）
- 「例：BGP NSF の確認」（P.8-16）
- 「例：EIGRP NSF の収束タイマーの設定」（P.8-17）
- 「例：EIGRP グレースフル リスタート パージ時間タイマーの設定」（P.8-17）

例：BGP NSF の設定

次の例に、BGP NSF をネットワーキング デバイスで設定する方法を示します。

```
Router# configure terminal
Router(config)# router bgp 590
Router(config-router)# bgp graceful-restart
```

例：BGP NSF の隣接デバイスの設定

次に、隣接ルータで BGP NSF を設定する例を示します。BGP NSF をサポートするすべてのデバイスは、NSF 認識であることが必要です。これは、これらのデバイスがグレースフル リスタート機能を認識し、アドバタイズすることを意味します。

```
Router# configure terminal
Router(config)# router bgp 770
Router(config-router)# bgp graceful-restart
```

例：BGP NSF の確認

show running-config コマンドを入力して、「bgp graceful-restart」が SSO 対応ルータの BGP コンフィギュレーションに表示されているか確認します。

```
Router# show running-config

router bgp 120
bgp graceful-restart
 neighbor 10.2.2.2 remote-as 300
```

SSO デバイスおよびネイバー デバイスで、グレースフル リスタート機能がアドバタイズおよび受信されたことを示していることを確認し、グレースフル リスタート機能を備えたアドレス ファミリであることを確認します。アドレス ファミリが表示されない場合、BGP NSF も発生しません。

```
Router# show ip bgp neighbors x.x.x.x

BGP neighbor is 192.168.2.2,  remote AS YY, external link
  BGP version 4, remote router ID 192.168.2.2
  BGP state = Established, up for 00:01:18
  Last read 00:00:17, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh:advertised and received(new)
Address family IPv4 Unicast:advertised and received
    Address 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
```

例：EIGRP NSF の収束タイマーの設定

timers nsf converge コマンドを使用して、再起動しているルータが NSF 対応または NSF 認識ピアから EOT 通知を待機する最大時間を調整します。次に、収束タイマーを 1 分に設定する例を示します。

```
Router# configure terminal
Router(config)# router eigrp 101
Router(config-router)# timers nsf converge 60
```

例：EIGRP グレースフル リスタート パージ時間タイマーの設定

timers graceful-restart purge-time コマンドを使用して、ルートホールド タイマーを設定します。これにより、EIGRP を実行している NSF 認識ルータが、非アクティブなピアに対してルートを保持する期間を設定します。次の例は、ルートホールド タイマーを 2 分に設定する方法を示しています。

```
Router(config-router)# timers graceful-restart purge-time 120
```

例：EIGRP NSF のルート ホールド タイマーの設定

timers nsf route-hold コマンドを使用して、スイッチオーバーの実行中に NSF 認識ルータが NSF 対応ネイバーに対する既知のルートを保持する最大期間を設定します。次の例は、ルートホールド タイマーを 2 分に設定する方法を示しています。

```
Router# configure terminal
Router(config)# router eigrp 101
Router(config-router)# timers nsf route-hold 120
```

例：EIGRP NSF の信号タイマーの設定

timers nsf signal コマンドを使用して、初期再起動期間の最大時間を調整します。次に、信号タイマーを 10 秒に設定する例を示します。

```
Router# configure terminal
Router(config)# router eigrp 101
Router(config-router)# timers nsf signal 10
```

例：EIGRP NSF の確認

show ip protocols コマンドを入力して、インストールされている Cisco IOS ソフトウェア イメージに EIGRP NSF サポートが存在することを確認します。NSF 認識または対応がルータでサポートされている場合に、「EIGRP NSF-aware route hold timer is...」が出力に表示されます。この行に、ルートホールド タイマーのデフォルト値またはユーザ定義の値が表示されます。NSF 対応がルータでサポートされている場合にのみ、「EIGRP NSF...」が出力に表示されます。この行には、EIGRP NSF 機能のステータスによって、「disabled」または「enabled」が表示されます。

```
Router# show ip protocols

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:
    10.4.9.0/24
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: internal 90 external 170
```

例：EIGRP NSF サポートのディセーブル化

EIGRP NSF 機能は、Cisco IOS ソフトウェアのサポート バージョンを実行している分散プラットフォームにおいてデフォルトでイネーブルです。EIGRP NSF 対応をイネーブルまたはディセーブルにするには **nsf** コマンドを使用します。次に、NSF 対応をディセーブルにする例を示します。

```
Router# configure terminal
Router(config)# router eigrp 101
Router(config-router)# no nsf
```

例：OSPF NSF の設定

次の例に、OSPF NSF をネットワーキング デバイスで設定する方法を示します。

```
Router# configure terminal
Router(config)# router ospf 400
Router(config-router)# nsf
```

例：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 デバイス上で設定されていることを確認する必要があります。**show running-config** コマンドを入力して、「nsf」が SSO 対応デバイスの OSPF コンフィギュレーションに表示されていることを確認します。

```
Router# show running-config

router ospf 120
log-adjacency-changes
nsf
network 192.168.20.0 0.0.0.255 area 0
network 192.168.30.0 0.0.0.255 area 1
network 192.168.40.0 0.0.0.255 area 2
```

次に、NSF がデバイス上でイネーブルであることを確認するには、**show ip ospf** コマンドを入力します。

```
Router> show ip ospf

Routing Process "ospf 1" with ID 192.168.2.1 and Domain ID 0.0.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x0
Number of opaque AS LSA 0. Checksum Sum 0x0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
Non-Stop Forwarding enabled, last NSF restart 00:02:06 ago (took 44 secs)
Area BACKBONE(0)
Number of interfaces in this area is 1 (0 loopback)
 Area has no authentication
 SPF algorithm executed 3 times
```

例：IS-IS NSF の設定

次の例に、シスコ独自の IS-IS NSF 動作をネットワーキング デバイスで設定する方法を示します。

```
Router# configure terminal
Router(config)# router isis
Router(config-router)# nsf cisco
```

次の例に、IETF の IS-IS NSF 動作をネットワーキング デバイスで設定する方法を示します。

```
Router# configure terminal
Router(config)# router isis
Router(config-router)# nsf ietf
```

例：IS-IS NSF の確認

show running-config コマンドを入力して、「NSF」が SSO 対応デバイスの IS-IS コンフィギュレーションに表示されているか確認します。表示は、Cisco IS-IS または IETF IS-IS コンフィギュレーションを示しています。次の例は、デバイスが IS-IS NSF のシスコ実装を使用していることを示します。

```
Router# show running-config

router isis
nsf cisco
```

NSF コンフィギュレーションが **cisco** に設定されている場合、NSF がデバイス上でイネーブルかを確認するには **show isis nsf** コマンドを使用します。シスコのコンフィギュレーションを使用すると、コマンドの出力はアクティブ RP およびスタンバイ RP で異なります。次に、アクティブ RP 上のシスココンフィギュレーションの出力例を示します。この例では、「NSF restart enabled」のフレーズがあることに注意してください。

```
Router# show isis nsf

NSF is ENABLED, mode 'cisco'

RP is ACTIVE, standby ready, bulk sync complete
NSF interval timer expired (NSF restart enabled)
Checkpointing enabled, no errors
```

```
Local state:ACTIVE,  Peer state:STANDBY HOT,  Mode:SSO
```

次に、スタンバイ RP 上のシスコ コンフィギュレーションの出力例を示します。この例では、「NSF restart enabled」のフレーズがあることに注意してください。

```
Router# show isis nsf

NSF enabled, mode 'cisco'
RP is STANDBY, chkpt msg receive count:ADJ 2, LSP 7
NSF interval timer notification received (NSF restart enabled)
Checkpointing enabled, no errors
Local state:STANDBY HOT,  Peer state:ACTIVE,  Mode:SSO
```

次に、ネットワーキング デバイス上の IETF IS-IS コンフィギュレーションの出力例を示します。

```
Router# show isis nsf

NSF is ENABLED, mode IETF
NSF pdb state:Inactive
NSF L1 active interfaces:0
NSF L1 active LSPs:0
NSF interfaces awaiting L1 CSNP:0
Awaiting L1 LSPs:
NSF L2 active interfaces:0
NSF L2 active LSPs:0
NSF interfaces awaiting L2 CSNP:0
Awaiting L2 LSPs:
Interface:Serial3/0/2
    NSF L1 Restart state:Running
    NSF p2p Restart retransmissions:0
    Maximum L1 NSF Restart retransmissions:3
    L1 NSF ACK requested:FALSE
    L1 NSF CSNP requested:FALSE
    NSF L2 Restart state:Running
    NSF p2p Restart retransmissions:0
    Maximum L2 NSF Restart retransmissions:3
    L2 NSF ACK requested:FALSE
Interface:GigabitEthernet2/0/0
    NSF L1 Restart state:Running
    NSF L1 Restart retransmissions:0
    Maximum L1 NSF Restart retransmissions:3
    L1 NSF ACK requested:FALSE
    L1 NSF CSNP requested:FALSE
    NSF L2 Restart state:Running
    NSF L2 Restart retransmissions:0
    Maximum L2 NSF Restart retransmissions:3
    L2 NSF ACK requested:FALSE
    L2 NSF CSNP requested:FALSE
Interface:Loopback1
    NSF L1 Restart state:Running
    NSF L1 Restart retransmissions:0
    Maximum L1 NSF Restart retransmissions:3
    L1 NSF ACK requested:FALSE
    L1 NSF CSNP requested:FALSE
    NSF L2 Restart state:Running
    NSF L2 Restart retransmissions:0
    Maximum L2 NSF Restart retransmissions:3
    L2 NSF ACK requested:FALSE
    L2 NSF CSNP requested:FALSE
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CHAPTER 9

Route Processor Redundancy（RPR）

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。
- Route Processor Redundancy（RPR）冗長モードでは、スタンバイ モードのスーパーバイザ エンジン上のポートはディセーブルです。
- RPR は IPv6 マルチキャスト トラフィックをサポートしています。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

RPR の前提条件

なし。

RPR の制約事項

- 「RPR のハードウェア制限」（P.9-2）

一般的な RPR の制約事項

- 冗長スーパーバイザ エンジンがスタンバイ モードの場合、スタンバイ スーパーバイザ エンジン上の 2 つのギガビット イーサネット インターフェイスは常にアクティブです。
- スーパーバイザ エンジンを冗長構成にしても、スーパーバイザ エンジンのミラーリングやロードバランスは行われません。スーパーバイザ エンジンのうちの 1 台だけがアクティブになります。
- SNMP を通じて行われた設定変更は、スタンバイ スーパーバイザ エンジンと同期化されません。SNMP を通じてスイッチを設定したあと、running-config ファイルをアクティブ スーパーバイザ エンジンの startup-config ファイルにコピーして、スタンバイ スーパーバイザ エンジンの startup-config ファイルの同期化を引き起こします。
- スーパーバイザ エンジンのスイッチオーバーは、障害のあるスーパーバイザ エンジンがコア ダンプを完了したあとに行われます。コア ダンプには最大で 15 分間かかります。スイッチオーバー時間を短縮するには、スーパーバイザ エンジンでコア ダンプをディセーブルにします。
- 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
  ```

- スーパーバイザ エンジンのスイッチオーバー時に設定を変更した場合、その変更内容は失われます。

RPR のハードウェア制限

- Cisco IOS は、スーパーバイザ エンジンが同一である冗長構成をサポートします。スーパーバイザ エンジンが同一でない場合、片方が最初に起動されてアクティブになり、もう一方がリセット状態で保留されます。
- 各スーパーバイザ エンジンが単独でスイッチを稼働させるためのリソースを備えている必要があります。つまり、スーパーバイザ エンジンのすべてのリソース（すべてのフラッシュ装置を含む）が重複している必要があります。
- スーパーバイザ エンジンごとに個別のコンソール接続を行ってください。コンソール ポートに Y 字ケーブルを接続しないでください。
- FSU 時を除いて、両方のスーパーバイザ エンジンのシステム イメージを同じにする必要があります（「RP へのファイルのコピー」（P.9-6）を参照）。
- コンフィギュレーション レジスタを 0x2102（**config-register 0x2102**）に設定する必要があります。

（注） ネットワークからの起動はサポートされていません。

RPR について

- 「スーパーバイザ エンジンの冗長構成の概要」（P.9-3）
- 「RPR 動作」（P.9-3）

スーパーバイザ エンジンの冗長構成の概要

Catalyst 6500 シリーズ スイッチでは、プライマリのスーパーバイザ エンジンに障害が発生した場合、スタンバイ スーパーバイザ エンジンに切り替えることができることで、障害に対する耐久性が提供されています。RPR は 2 分以上のスイッチオーバー時間をサポートします。

次のイベントが発生すると、スイッチオーバーが行われます。

- アクティブ スーパーバイザ エンジンでのハードウェア障害
- スーパーバイザ エンジン間のクロック同期損失
- 手動スイッチオーバー

RPR 動作

RPR は次の機能をサポートします。

- 自動スタートアップおよびアクティブ スーパーバイザ エンジンとスタンバイ スーパーバイザ エンジン間の bootvar の同期化
- スーパーバイザ エンジンのアクティブ ステータスまたはスタンバイ ステータスを検出および決定するハードウェア信号
- 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、60 秒間隔でクロック同期化を実行
- スタンバイ スーパーバイザ エンジンはブートされるが、すべてのサブシステムはアップしていない。アクティブ スーパーバイザ エンジンが故障した場合に、完全に動作可能になります。
- 故障した装置の代わりに動作可能なスーパーバイザ 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。
- Fast Software Upgrade（FSU）のサポート（第 6 章「高速ソフトウェア アップグレード」を参照）

スイッチの電源投入時に、2 つのスーパーバイザ エンジン間で RPR が稼働します。最初に起動するスーパーバイザ エンジンは、RPR アクティブスーパーバイザ エンジンになります。ルート プロセッサ（RP）およびポリシー フィーチャ カード（PFC）が完全に動作可能になります。スタンバイ スーパーバイザ エンジン上の RP および PFC はリセットされますが、動作可能にはなりません。

スイッチオーバーが行われると、スタンバイ スーパーバイザ エンジンが完全に動作可能になり、次の動作が行われます。

- すべてのスイッチ モジュールの電源が再びオンになります。
- RP 上の残りのサブシステム（レイヤ 2 およびレイヤ 3 プロトコルを含む）が起動されます。
- アクセス コントロール リスト（ACL）がスーパーバイザ エンジンのハードウェアに再度プログラミングされます。

（注）　スイッチオーバー時には、一部のアドレス ステートが失われ、ダイナミックに再確認したあとで復元されるので、トラフィックが一時中断されます。

スーパーバイザ エンジンの設定の同期化

（注）　SNMP を通じて行われた設定変更は、スタンバイ スーパーバイザ エンジンと同期化されません。SNMP を通じてスイッチを設定したあと、running-config ファイルをアクティブ スーパーバイザ エンジンの startup-config ファイルにコピーして、スタンバイ スーパーバイザ エンジンの startup-config ファイルの同期化を引き起こします。

RPR モードの動作時には、2 つのスーパーバイザ エンジン間で startup-config ファイルおよび config-register コンフィギュレーションが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。

RPR のデフォルト設定

なし。

RPR の設定方法

RPR モードの設定

RPR モ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
ステップ 1	`Router(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	`Router(config-red)# mode rpr`	RPR を設定します。このコマンドを入力すると、スタンバイ スーパーバイザ エンジンがリロードされ、RPR モードでの処理が開始されます。

次に、RPR のシステムを設定する例を示します。

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# redundancy
Router(config-red)# mode rpr
Router(config-red)# end
Router# show running-config
Router# show redundancy states
```

スーパーバイザ エンジンの設定の同期化

通常の動作時には、2 つのスーパーバイザ エンジン間で startup-config および config-register 設定が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）　デフォルトの自動同期設定を変更しないでください。

冗長ステートの表示

冗長ステートを表示するには、次の作業を行います。

コマンド	目的
Router# **show redundancy states**	冗長ステートを表示します。

次に、冗長ステートを表示する例を示します。

```
Router# show redundancy states
my state = 13 -ACTIVE
     peer state = 8  -STANDBY HOT
           Mode = Duplex
           Unit = Primary
        Unit ID = 1

Redundancy Mode (Operational) = Route Processor Redundancy
Redundancy Mode (Configured)  = Route Processor Redundancy
     Split Mode = Disabled
   Manual Swact = Enabled
 Communications = Up

   client count = 11
 client_notification_TMR = 30000 milliseconds
          keep_alive TMR = 9000 milliseconds
        keep_alive count = 0
    keep_alive threshold = 18
           RF debug mask = 0x0
```

次の例では、2 番めのスーパーバイザ エンジンがディセーブルになっているか、見つからないため、冗長ステートに入ることができません。

```
Router# show redundancy states
       my state = 13 -ACTIVE
     peer state = 1  -DISABLED
           Mode = Simplex
           Unit = Primary
        Unit ID = 1

Redundancy Mode (Operational) = rpr
Redundancy Mode (Configured)  = rpr
Redundancy State              = Non Redundant
     Maintenance Mode = Disabled
 Communications = Down      Reason: Simplex mode

   client count = 11
 client_notification_TMR = 30000 milliseconds
          keep_alive TMR = 4000 milliseconds
```

```
    keep_alive count = 0
keep_alive threshold = 7
       RF debug mask = 0x0
```

RP へのファイルのコピー

次のコマンドを使用して、アクティブ RP 上の **bootflash:** 装置にファイルをコピーします。

```
Router# copy source_device:source_filename bootflash:target_filename
```

次のコマンドを使用して、スタンバイ RP 上の **bootflash:** 装置にファイルをコピーします。

```
Router# copy source_device:source_filename slavebootflash:target_filename
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

PART 5

インターフェイスおよびハードウェア コンポーネント

CHAPTER 10

インターフェイス コンフィギュレーション

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

インターフェイスの設定に関する情報

ソフトウェアの多くの機能は、インターフェイス単位でイネーブルになります。**interface** コマンドを入力する場合、次の情報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：モジュールの搭載先スロットです。Cisco IOS Release 15.1SY でサポートされるスイッチの各スロットには、上から下へ、1 から始まる通し番号が付けられています。
- ポート番号：モジュールの物理的なポート番号です。Cisco IOS Release 15.1SY でサポートされるスイッチのポート番号は、常に 1 から始まります。スイッチ背面の、左から右へ通し番号が付けられています。

各ポートは、物理的な位置によって識別できます。また、**show** コマンドを使用して、特定のポートまたはすべてのポートに関する情報を表示することもできます。

interface コマンドについては、次のドキュメントを参照してください。

http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-i1.html#GUID-0D6BDFCD-3FBB-4D26-A274-C1221F8592DF

インターフェイスの範囲を設定する方法

インターフェイス範囲コンフィギュレーション 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コンフィギュレーション 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、その範囲内の全インターフェイスに適用されます。**interface range** コマンドの詳細については、次のドキュメントを参照してください。

http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-i1.html#GUID-8EC4EF91-F929-45F8-95CA-E4C9A9724FFF

インターフェイス範囲マクロの定義および使用方法

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 ストリングで **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
`Router(config)# define interface-range` *macro_name* {**vlan** *vlan_ID - vlan_ID*} | {*type slot/port - port*} [, {*type slot/port - port*}]	インターフェイス範囲マクロを定義して、NVRAM に保存します。

次に、ギガビット イーサネット ポート 1/1 ～ 1/4 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。

```
Router(config)# define interface-range enet_list gigabitethernet 1/1 - 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
`Router# 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。

```
Router# show running-config | include define
define interface-range enet_list GigabitEthernet1/1 - 4
Router#
```

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
`Router(config)# interface range macro` *macro_name*	定義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コンフィギュレーション モードに切り替える例を示します。

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

オプションのインターフェイス機能の設定方法

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 モード設定上のガイドライン

通常、イーサネット ポート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、ポート間で速度およびデュプレックス モードをネゴシエーションできるようにします。ポート速度およびデュプレックス モードを手動で設定する場合には、次の点について考慮してください。

- デュプレックス モードが自動（**no duplex** コマンド）に設定されていない場合、イーサネット ポート速度を自動（**no speed** コマンド）に設定できません。
- イーサネット ポート速度を auto 以外の値（10 Mbps、100 Mbps、1000 Mbps など）に設定する場合は、それに合わせて接続先ポートを設定してください。接続先ポートが速度をネゴシエーションするように設定しないでください。
- イーサネット ポート速度を 10 Mbps または 100 Mbps のいずれかに手動で設定すると、ポートにデュプレックス モードを設定するように求めるプロンプトが表示されます。

（注） 接続先ポートが auto 以外の値に設定されている場合、LAN ポートはイーサネット ポート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ません。

注意 イーサネット ポート速度およびデュプレックス モードの設定を変更すると、再設定時にインターフェイスがシャットダウンされてから再びイネーブルになる場合があります。

イーサネット インターフェイス速度の設定

（注） 10/100/1000 Mbps イーサネット ポートでイーサネット ポート速度を **auto** に設定すると、速度とデュプレックスの両方が自動ネゴシエートされます。10 ギガビット イーサネット ポートは自動ネゴシエーションをサポートしません。

10/100/1000 Mbps イーサネット ポートのポート速度を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface gigabitethernet` *slot/port*	設定するイーサネット ポートを選択します。
ステップ 2	`Router(config-if)# speed {10 | 100 | 1000 | {auto [10 100 [1000]]}}`	イーサネット インターフェイス速度を設定します。

10/100/1000 Mbps イーサネット ポートのポート速度を設定する場合は、以下に注意してください。

- ネゴシエーション速度を 10 Mbps または 100 Mbps に制限するには、**auto 10 100** キーワードを入力します。
- **auto 10 100 1000** キーワードには、**auto** キーワードと同じ効果があります。

次に、ギガビット イーサネット ポート 1/4 の速度を 100 Mbps に設定する例を示します。

```
Router(config)# interface gigabitethernet 1/4
Router(config-if)# speed 100
```

インターフェイスのデュプレックス モードの設定

（注）
- 10 ギガビット イーサネットおよびギガビット イーサネットは全二重通信専用です。ギガビット イーサネット用に設定された 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 ポート、または 10/100/1000 Mbps ポート上では、デュプレックス モードを変更できません。
- 10/100/1000 Mbps イーサネット ポートでポート速度を auto に設定すると、速度とデュプレックスの両方が自動ネゴシエートされます。自動ネゴシエーション ポートのデュプレックス モードは変更できません。

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	`Router(config)# interface gigabitethernet` *slot/port*	設定するイーサネット ポートを選択します。
ステップ 2	`Router(config-if)# duplex [auto | full | half]`	イーサネット ポートのデュプレックス モードを設定します。

次に、ギガビット イーサネット ポート 1/4 のデュプレックス モードを full に設定する例を示します。

```
Router(config)# interface gigabitethernet 1/4
Router(config-if)# duplex full
```

ギガビット イーサネット ポート上のリンク ネゴシエーションの設定

（注）　リンク ネゴシエーションでは、ポート速度のネゴシエーションは行われません。

ギガビット イーサネット ポートでは、リンク ネゴシエーションによってフロー制御パラメータ、リモート障害情報、およびデュプレックス情報が交換されます。リンク ネゴシエーションはデフォルトでイネーブルです。

リンクの両端のポートは同じ設定にする必要があります。リンクの両端で設定が矛盾している場合（一方のポートでリンク ネゴシエーションがイネーブルで、他方のポートではディセーブルの場合）、リンクはアクティブになりません。

表 10-1 に、設定可能な 4 種類のリンク ネゴシエーションと各設定のリンク ステータスを示します。

表 10-1　リンク ネゴシエーションの設定および可能なリンク ステータス

リンク ネゴシエーションのステート		リンク ステータス	
ローカル ポート	リモート ポート	ローカル ポート	リモート ポート
Off	Off	Up	Up
On	On	Up	Up
Off	On	Up	Down
On	Off	Down	Up

特定のポート上でリンク ネゴシエーションを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface gigabitethernet slot/port`	設定するポートを選択します。
ステップ 2	`Router(config-if)# speed nonegotiate`	リンク ネゴシエーションをディセーブルにします。

次に、ギガビット イーサネット ポート 1/4 上でリンク ネゴシエーションをイネーブルにする例を示します。

```
Router(config)# interface gigabitethernet 1/4
Router(config-if)# no speed nonegotiate
```

速度およびデュプレックス モードの設定の表示

ポート速度およびデュプレックス モード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
`Router# show interfaces type slot/port [transceiver properties]`	速度およびデュプレックス モードの設定を表示します。速度およびデュプレックスの自動ネゴシエーション ステータスを表示するには、**transceiver properties** オプションを追加します。

ジャンボ フレーム サポートの設定

ジャンボ フレーム サポートに関する情報

ジャンボ フレーム サポートの概要

ジャンボ フレームは、デフォルトのイーサネット サイズよりも大きなフレームです。ポートや VLAN インターフェイスにデフォルト値よりも大きい最大伝送単位（MTU）サイズを設定し、グローバル LAN ポート MTU サイズを設定することにより、ジャンボ フレームのサポートをイネーブルにします。

（注）
- ジャンボ フレームのサポートは、ルート プロセッサ（RP）上のソフトウェアのルーテッド トラフィックをフラグメント化します。
- ジャンボ フレームのサポートは、ブリッジド トラフィックをフラグメント化しません。

入力 10/100 Mbps、100 Mbps イーサネットおよび 10 ギガビット イーサネット ポートでのブリッジドおよびルーテッド トラフィック サイズのチェック

ジャンボ フレームのサポートは、デフォルト値以外の MTU サイズが設定された入力 10/100 Mbps、100 Mbps イーサネットおよび 10 ギガビット イーサネット LAN ポートで、入力トラフィック サイズとグローバルな LAN ポート MTU サイズを比較します。ポートでは、サイズを超えているトラフィックがドロップされます。グローバルな LAN ポートの MTU サイズを設定できます（「グローバルな出力 LAN ポート MTU サイズの設定」（P.10-9）を参照）。

入力ギガビット イーサネット ポートでのブリッジドおよびルーテッド トラフィック サイズのチェック

ギガビット イーサネット LAN ポートにデフォルト値以外の MTU サイズを設定すると、パケット サイズが 64 バイトよりも大きい場合に、フレームを許可します。デフォルト値以外の MTU サイズが設定されている場合、ギガビット イーサネット LAN ポートはサイズを越えている入力フレームを調べません。

PFC でのルーテッド トラフィック サイズのチェック

ルーティングする必要があるトラフィックの場合、PFC のジャンボ フレームのサポートは設定された MTU サイズとトラフィック サイズを比較し、そのトラフィックに対応できる MTU サイズが設定されたインターフェイス間のジャンボ トラフィックに、レイヤ 3 スイッチングを行います。MTU サイズが十分な大きさに設定されていないインターフェイス間では、「do not fragment」ビットが設定されていない場合、PFC はトラフィックを RP に送信して、フラグメント化およびソフトウェアでのルーティングを行います。「do not fragment」ビットが設定されていれば、PFC はトラフィックをドロップします。

出力 10 Mbps、10/100 Mbps、100 Mbps イーサネット ポートでのブリッジドおよびルーテッド トラフィック サイズのチェック

10 Mbps、10/100 Mbps、100 Mbps イーサネット LAN ポートにデフォルト値以外の MTU サイズを設定すると、パケット サイズが 64 バイトよりも大きいフレームが送信されます。デフォルト値以外の MTU サイズが設定されている場合、10 Mbps、10/100 Mbps、100 Mbps イーサネット LAN ポートはサイズが大きい出力フレームを調べません。

出力ギガビット イーサネットおよび 10 ギガビット イーサネット ポートでのブリッジドおよびルーテッド トラフィック サイズのチェック

ジャンボ フレームのサポートは、デフォルト値以外の MTU サイズが設定されたギガビット イーサネットおよび 10 ギガビット イーサネット出力 LAN ポート上で、出力トラフィック サイズとグローバルな出力 LAN ポート MTU サイズを比較します。ポートでは、サイズを超えているトラフィックがドロップされます。グローバルな LAN ポートの MTU サイズを設定できます（「グローバルな出力 LAN ポート MTU サイズの設定」（P.10-9）を参照）。

イーサネット ポートのデフォルト以外の MTU サイズ

イーサネット ポートの概要

デフォルト値以外の MTU サイズを 10 Mbps、10/100 Mbps、または 100 Mbps イーサネット ポートに設定すると、入力パケットはグローバルな LAN ポートの MTU サイズに制限され、64 バイトよりも大きいサイズの出力トラフィックが許可されます。

ギガビット イーサネット ポートでデフォルト値以外の MTU サイズを設定すると、64 バイトよりも大きいすべてのサイズの入力パケットが許可され、出力トラフィックはグローバルな LAN ポートの MTU サイズに制限されます。

デフォルト値以外の MTU サイズを 10 ギガビット イーサネット ポートに設定すると、入出力パケットはグローバルな LAN ポートの MTU サイズに制限されます。

いずれのイーサネット ポートでも MTU サイズを設定できます。

レイヤ 3 イーサネット ポート

レイヤ 3 ポートでは、レイヤ 3 イーサネット ポートごとにグローバルな LAN ポート MTU サイズとは異なる MTU サイズを設定できます。

（注）　デフォルト値以外の MTU サイズが設定されているレイヤ 3 イーサネット LAN ポートを経由するトラフィックは、グローバルな LAN ポートの MTU サイズにも影響を受けます（「グローバルな出力 LAN ポート MTU サイズの設定」（P.10-9）を参照）。

レイヤ 2 イーサネット ポート

レイヤ 2 ポートでは、グローバルな LAN ポート MTU サイズと一致する MTU サイズだけを設定できます（「グローバルな出力 LAN ポート MTU サイズの設定」（P.10-9）を参照）。

VLAN インターフェイス

レイヤ 3 VLAN インターフェイスごとに異なる MTU サイズを設定できます。VLAN インターフェイスにデフォルト値以外の MTU サイズを設定すると、トラフィックはデフォルト値以外の MTU サイズに制限されます。ジャンボ フレームをサポートするように VLAN インターフェイスに MTU サイズを設定できます。

MTU サイズの設定

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	`Router(config)# interface {{vlan vlan_ID} | {type 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	`Router(config-if)# mtu mtu_size`	MTU サイズを設定します。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。

MTU サイズを設定するときは、以下に注意してください。

- VLAN インターフェイスとレイヤ 3 イーサネット ポートについては、サポートされている MTU 値は 64 ～ 9216 バイトです。
- レイヤ 2 イーサネット ポートについては、グローバルな出力 LAN ポート MTU サイズだけ設定可能です（「グローバルな出力 LAN ポート MTU サイズの設定」（P.10-9）を参照）。

次に、ギガビット イーサネット ポート 1/2 上で MTU サイズを設定する例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 1/2
Router(config-if)# mtu 9216
Router(config-if)# end
```

次に、設定を確認する例を示します。

```
Router# 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,
<...Output Truncated...>
Router#
```

グローバルな出力 LAN ポート MTU サイズの設定

グローバルな出力 LAN ポート 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	`Router(config)# system jumbomtu mtu_size`	グローバルな出力 LAN ポートの MTU サイズを設定します。 **（注）** すべてのインターフェイス MTU サイズが設定されているデフォルト以外のインターフェイス MTU サイズではなく、デフォルト（1500）に変更されるため、system jumbomtu コマンドを使用して MTU サイズを 1500 に設定しないでください。（CSCtq52016）。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

IEEE 802.3x フロー制御の設定

ギガビット イーサネット ポートおよび 10 ギガビット イーサネット ポートは、指定時間のあいだポートへのフレーム送信を停止するためにフロー制御を使用します。他のイーサネット ポートは、フロー制御要求に応答す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 ポートまたは 10 ギガビット イーサネット ポートの受信バッファがいっぱいになると、指定時間のあいだフレーム送信処理を遅らせるようにリモート ポートに要求する IEEE802.3x ポーズ フレームを送信するように、ポートを設定できます。すべてのイーサネット ポートは他の装置からの IEEE 802.3x ポーズ フレームに応答するように設定できます。

イーサネット ポート上でフロー制御を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface type slot/port`	設定するポートを選択します。
ステップ 2	`Router(config-if)# flowcontrol {receive | send} {desired | off | on}`	ポーズ フレームを送信またはポーズ フレームに応答するように、ポートを設定します。

フロー制御を設定するときは、以下に注意してください。

- 10 ギガビット イーサネット光ファイバ ポートでは自動ネゴシエーションが機能しないため、デフォルトでポーズ フレームに応答します。10 ギガビット イーサネット光ファイバ ポートでは、フロー制御動作モードは常に管理モードと同じです。
- ポートがポーズ フレームに応答する方法を設定する場合、次の情報に注意してください。
  - ギガビット イーサネット ポートでは、リモート ポートの設定が不明な場合は、**receive desired** キーワードを使用して、受信したポーズ フレームに応答するようにギガビット イーサネット ポートを設定できます （ギガビット イーサネット ポートだけでサポートされます）。
  - **receive on** キーワードを使用すると、受信したポーズ フレームに応答するようにポートが設定されます。
  - **receive off** キーワードを使用すると、受信したポーズ フレームを無視するようにポートが設定されます。
- ポート上のポーズ フレームの送信を設定する場合は、次の情報に注意してください。
  - ギガビット イーサネット ポートでは、リモート ポートの設定が不明な場合は、**send desired** キーワードを使用して、ポーズ フレームを送信するようにギガビット イーサネット ポートを設定できます （ギガビット イーサネット ポートだけでサポートされます）。
  - **send on** キーワードを使用すると、ポーズ フレームを送信するようにポートが設定されます。
  - **send off** キーワードを使用すると、ポーズ フレームを送信しないようにポートが設定されます。

次に、フロー制御の受信を有効にし、フロー制御設定を確認する例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 1/2
Router(config-if)# flowcontrol receive on
Router(config-if)# end
Router# show interfaces flowcontrol

Interface Send         Receive
Gi1/1     Desired      OFF
Gi1/2     Desired      ON
<output truncated>
```

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、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 ポートに、個別に設定できます。

注意　ポート デバウンス タイマーをイネーブルにすると、リンク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	`Router(config)# interface type slot/port`	設定するポートを選択します。
ステップ 2	`Router(config-if)# link debounce [time debounce_time]`	デバウンス タイマーを設定します。

ポートにデバウンス タイマーを設定する場合、次の点に注意してください。

- **time** キーワードは、光ファイバ 1000 Mpbs よりも高速なイーサネット ポート上だけでサポートされます。
- 銅製メディア上で 1000Mpbs で動作するポートでは、ポート デバウンス タイマー値を 5000 ミリ秒まで 100 ミリ秒単位で増やすことができます。
- デバウンス タイマーは 10 Gbps 銅製メディアを認識し、メディアだけの変更を検出します。

表 10-2 は、リンク変更の通知前に発生する時間遅延を一覧表示します。

表 10-2　デフォルトのポート デバウンス タイマー遅延時間

ポート タイプ	デバウンス タイマーがディセーブルの場合	デバウンス タイマーがイネーブルの場合
10 Mpbs または 100 Mbps で動作するポート：	300 ミリ秒	3100 ミリ秒
銅製メディア上で 1000 Mpbs または 10 Gbps で動作するポート：	300 ミリ秒	3100 ミリ秒
ファイバ メディアを通じて 1000 Mbps または 10 Gbps で動作するポート：	10 ミリ秒	100 ミリ秒

（注）　show interfaces debounce コマンドは、ポート デバウンス タイマーがディセーブルの場合 10 ギガビット イーサネット ポートのデフォルト値を表示しません。

（注）　すべての 10 ギガビット イーサネット ポートで、デバウンス タイマーがディセーブル値の場合は 10 ミリ秒、デバウンス タイマーがイネーブル値の場合は 100 ミリ秒になります。

次に、ギガビット イーサネット ポート 1/12 のポート デバウンス タイマーをイネーブルにする例を示します。

```
Router(config)# interface gigabitethernet 1/12
Router(config-if)# link debounce
Router(config-if)# end
```

次に、ポート デバウンス タイマーの設定を表示する例を示します。

```
Router# show interfaces debounce | include enable
Gi1/12  enable          3100
```

活性挿抜に関する情報

Catalyst 6500 シリーズ スイッチでは活性挿抜（OIR）機能がサポートされており、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。モジュールを取り外す前にシャットダウンし、取り付けた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。

（注）　取り外しおよび取り付けを行うモジュールは、一度に 1 つだけにしてください。モジュールの取り外しおよび取り付け後に、LED を確認してから次の作業を始めます。モジュールの LED については、『*Catalyst 6500 Series Switch Installation Guide*』を参照してください。

モジュールの取り外しおよび取り付けを行うと、Catalyst 6500 シリーズ スイッチはモジュールのトラフィック処理を停止し、設定の変更がないかどうかシステムを走査します。各インターフェイス タイプがシステム コンフィギュレーションと照らし合わせてチェックされます。そのあと、システムは新しいモジュールに関して診断を実行します。モジュールの取り付けおよび取り外し中に、通常の動作が中断されることはありません。

スイッチがオンラインにできるのは、同等の交換モジュール 1 つだけです。同一モジュールの OIR をサポートするために、モジュールを取り外すときにモジュールの設定は running-config ファイルから削除されません。

交換モジュールと取り外したモジュールが異なる場合は、交換モジュールを設定してからでないと、スイッチはモジュールをオンラインにできません。

レイヤ 2 MAC アドレスは Electrically Erasable Programmable Read-Only Memory（EEPROM; 電気的消去再書き込み可能 ROM）上に保存され、システムがスイッチング テーブルおよびデータ構造を更新しなくても、モジュールをオンラインで交換できます。レイヤ 2 MAC アドレスは、インストールされているモジュールのタイプとは関係なく、スーパーバイザ エンジンを交換しない限り変更されません。スーパーバイザ エンジンを交換すると、すべてのポートのレイヤ 2 MAC アドレスが、新しいスーパーバイザ エンジン上のアドレス アロケータで指定されるアドレスに変更されます。

インターフェイスのモニタ方法およびメンテナンス方法

インターフェイス ステータスのモニタ

インターフェイスに関する情報（ソフトウェア/ハードウェアのバージョン、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モニタリング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、『*Cisco IOS 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
`Router# show ibc`	現在の内部ステータス情報を表示します。
`Router# show eobc`	現在の内部帯域外情報を表示します。
`Router# show interfaces [type slot/port]`	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。

コマンド	目的
Router# **show running-config**	現在の実行コンフィギュレーションを表示します。
Router# **show rif**	現在の Routing Information Field（RIF; ルーティング情報フィールド）キャッシュの内容を表示します。
Router# **show protocols** [*type slot/port*]	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。
Router# **show version**	ハードウェア設定、ソフトウェア バージョン、コンフィギュレーション ファイルの名前と送信元、およびブート イメージを表示します。

インターフェイスのカウンタのクリア

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、次の作業を行います。

コマンド	目的
Router# **clear counters** {{**vlan** *vlan_ID*} | {*type slot/port*} | {**port-channel** *channel_ID*}}	インターフェイス カウンタをクリアします。

次に、ギガビット イーサネット ポート 1/5 のカウンタをクリアしてリセットする例を示します。

```
Router# clear counters gigabitethernet 1/5
Clear "show interface" counters on this interface [confirm] y
*Sep 30 08:42:55: %CLEAR-5-COUNTERS: Clear counter on interface GigabitEthernet1/5
```

clear counters コマンドを実行すると、オプションの引数を使用して特定のインターフェイスを指定しない限り、現在のすべてのインターフェイス カウンタがクリアされます。

（注）　**clear counters** コマンドでは、SNMP を使用して取得したカウンタはクリアされず、**show interfaces** EXEC コマンドで表示されるカウンタだけがクリアされます。

インターフェイスのリセット

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
Router# **clear interface** *type slot/port*	インターフェイスをリセットします。

次に、ギガビット イーサネット ポート 1/5 をリセットする例を示します。

```
Router# clear interface gigabitethernet 1/5
```

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シャットダウンすると、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 サーバに伝達されます。そのインターフェイスは、あらゆるルーティング 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	`Router(config)# interface {{vlan vlan_ID} | {type slot/port} | {port-channel channel_ID}}`	設定するインターフェイスを選択します。
ステップ 2	`Router(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	`Router(config-if)# no shutdown`	インターフェイスを再びイネーブルにします。

次に、ギガビット イーサネット ポート 1/5 をシャットダウンする例を示します。

```
Router(config)# interface gigabitethernet 1/5
Router(config-if)# shutdown
Router(config-if)#
```

（注）　リンク ステート メッセージ（LINK-3-UPDOWN および LINEPROTO-5-UPDOWN）は、デフォルトではディセーブルに設定されています。このメッセージをイネーブルにするには、対象となる各インターフェイスに対して **logging event link status** コマンドを使用します。

次に、ギガビット イーサネット ポート 1/5 を再びイネーブルにする例を示します。

```
Router(config-if)# no shutdown
Router(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 コマンドを使用します。シャットダウンされたインターフェイスは、**show interfaces** コマンドの出力では [administratively down] と表示されます。

TDR を使用してケーブルのステータスを確認する方法

Time Domain Reflectometer（TDR; タイム ドメイン リフレクトメータ）を使用して、銅製ケーブルのステータスを確認できます。TDR はケーブルを介して信号を送信し、反射され戻ってきた信号を読み取ることで、ケーブル障害を検出します。信号のすべてまたは一部は、ケーブル不良の数によって、またはケーブルの終端によって反射されて戻ってきます。

TDR を使用して、リンクを確立できない場合にケーブル配置に障害が発生しているかどうかを判断します。特に既存のスイッチを交換する、ギガビット イーサネットにアップグレードする、または新しいケーブルを敷く場合に、このテストは重要です。

（注）

- TDR では、最大で 115 m の長さのケーブルをテストできます。
- TDR の結果は、正常に動作しているリンクには意味がありません。
- TDR テストを実行する前に、ポートはアップである必要があります。ポートがダウンしている場合、**test cable-diagnostics tdr** コマンドを入力できず、次のメッセージが表示されます。

  ```
  Router# test cable-diagnostics tdr interface gigabitethernet2/12
  ```

```
% Interface Gi2/12 is administratively down
% Use 'no shutdown' to enable interface before TDR test start.
```

TDR テストを開始または中止するには、次の作業を行います。

コマンド	目的
test cable-diagnostics tdr interface {**interface** *interface_number*}	TDR テストを開始または中止します。

次に、TDR ケーブル診断を実行する例を示します。

```
Router # test cable-diagnostics tdr interface gigabitethernet2/1
TDR test started on interface Gi2/1
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
Router #
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CHAPTER 11

単一方向リンク検出（UDLD）

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

UDLD の前提条件

なし。

UDLD の制約事項

なし。

UDLD について

UDLD の概要

シスコ独自の UDLD プロトコルにより、LAN ポートに接続された光ファイバまたは銅製（カテゴリ 5 ケーブルなど）イーサネット ケーブルを使用して接続されたデバイスで、ケーブルの物理構成をモニタし、単一方向リンクの存在を検出することができます。単一方向リンクが検出されると、UDLD が関係のある LAN ポート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 プロトコルと連動し、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、ネイバーの ID の検知、誤って接続された LAN ポートのシャットダウンなど、自動ネゴシエーションでは実行不可能な処理を実行します。自動ネゴシエーションと UDLD の両方をイネーブルにすると、レイヤ 1 とレイヤ 2 の検知機能が連動し、物理的および論理的な単一方向接続、および他のプロトコルの誤動作を防止します。

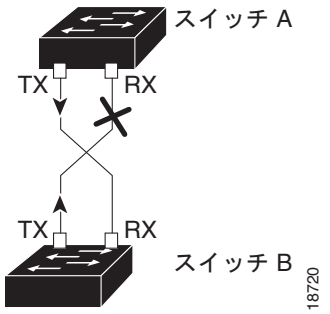
リンク上でローカル デバイスが送信したトラフィックはネイバーで受信されるけれども、ネイバーから送信されたトラフィックはローカル デバイスで受信されない場合に、単方向リンクが発生します。対になっているファイバ ケーブルのいずれかの接続が切断された場合、自動ネゴシエーションがアクティブである限り、そのリンクは存続できません。この場合、論理リンクは不定であり、UDLD は何の処理も行いません。レイヤ 1 で両方のファイバが正常に動作していれば、レイヤ 2 の UDLD はそれらのファイバが正しく接続しているかどうか、また、トラフィックが適切なネイバー間で双方向に流れているかどうかを判別します。自動ネゴシエーションはレイヤ 1 で行われるので、このチェックは自動ネゴシエーションでは実行されません。

UDLD をイネーブルに設定した LAN ポートは、ネイバー デバイスに定期的に UDLD パケットを送信します。このパケットが一定時間内にエコー バックされ、かつ特定の確認応答（エコー）がない場合には、そのリンクは単一方向リンクとしてフラグ付けされ、LAN ポート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てディセーブルにするには、リンクの両端のデバイスで 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 LAN ポート上ではローカルにディセーブルに設定されています。このタイプのメディアは、アクセス ポートに使用されることが多いので、メディアに不要な制御トラフィックを送信しません。

図 11-1 に、単一方向リンク条件の例を示します。スイッチ B は、ポート上でスイッチ A から正常にトラフィックを受信しますが、スイッチ A は、同じポート上でスイッチ B からのトラフィックを受信しません。UDLD によって問題が検出され、ポートがディセーブルにされます。

図 11-1　単方向リンク



UDLD アグレッシブ モード

UDLD アグレッシブ モードはデフォルトではディセーブルに設定されています。UDLD アグレッシブ モードは、そのモードをサポートするネットワーク デバイス間のポイントツーポイントのリンク上に限って設定してください。UDLD アグレッシブ モードをイネーブルに設定した場合、UDLD ネイバー関係が設定されている双方向リンク上のポートが UDLD パケットを受信しなくなったとき、UDLD はネイバーとの接続を再確立しようとします。この試行に 8 回失敗すると、ポートはディセーブルになります。

スパニングツリー ループを防止するために、デフォルトの 15 秒間隔を使用する非アグレッシブな UDLD により、（デフォルトのスパニングツリー パラメータを使用している場合）ブロッキング ポートがフォワーディング ステートに移行する前に、すみやかに単方向リンクをシャットダウンすることができます。

UDLD アグレッシブ モードをイネーブルにすると、次のような状況でさらに利点をもたらします。

- リンクの一方の側でポート スタック（TX および RX 両方）を使用している場合
- リンクの一方の側がダウンしているにもかかわらず、もう一方の側がアップしたままの場合

このような状況では、UDLD アグレッシブ モードにより、リンク上のポートの 1 つがディセーブルになり、トラフィックの廃棄が防止されます。

（注）　UDLD ノーマル モードでは、単一方向エラーが検出されても、ポートはディセーブルになりません。UDLD アグレッシブ モードでは、単一方向エラーが検出されると、ポートはディセーブルになります。

Fast UDLD

Fast UDLD は Release 15.0(1)SY1 以降のリリースでサポートされます。

Fast UDLD はポート単位の設定オプションで、200 ～ 1000 ミリ秒の UDLD メッセージ時間間隔をサポートします。Fast UDLD は、サブセカンド単一方向リンク検出を提供するように設定できます（Fast UDLD がない場合、メッセージ時間間隔は 7 ～ 90 秒です）。

Fast UDLD を設定する際、次の注意事項と制約事項に従ってください。

- Fast UDLD は、デフォルトではディセーブルに設定されています。
- ノーマル モードとアグレッシブ モードは、両方とも Fast UDLD をサポートしています。
- Fast UDLD ポートは、**link debounce** コマンドをサポートしていません。
- Fast UDLD がサポートするのは、Fast UDLD をサポートするネットワーク デバイス間のポイントツーポイント リンクだけです。
- 互いに接続されたネットワーク デバイス間の少なくとも 2 つのリンクで Fast UDLD を設定します。Fast UDLD は、ネイバー デバイスへの単一リンク接続をサポートしません。
- 同じネイバー デバイスに対する複数のリンクで同じエラーが同時に発生した場合、Fast UDLD は単一方向リンクを報告しません。
- CPU 使用率が 60 パーセントを超えた場合、Fast UDLD は単一方向リンクを検出できません。
- Fast UDLD は、スーパーバイザ エンジン 2T を使用する 60 個のポートでサポートされます。

UDLD のデフォルト設定

機能	デフォルト値
UDLD グローバル イネーブル ステート	グローバルにディセーブル
UDLD アグレッシブ モード	ディセーブル
ポート別の UDLD イネーブル ステート（光ファイバ メディア用）	すべてのイーサネット光ファイバ LAN ポートでイネーブル
ポート別の UDLD イネーブル ステート（ツイストペア（銅製）メディア用）	すべてのイーサネット 10/100 および 1000BASE-TX LAN ポートでディセーブル
Fast UDLD	ディセーブル
Fast UDLD エラー通知機能	ディセーブル

UDLD の設定方法

- 「UDLD のグローバルなイネーブル化」（P.11-5）
- 「LAN インターフェイスでの UDLD のイネーブル化」（P.11-5）
- 「光ファイバ以外の LAN インターフェイス上での UDLD のディセーブル化」（P.11-5）
- 「光ファイバ LAN インターフェイス上での UDLD のディセーブル化」（P.11-6）
- 「UDLD プローブ メッセージ間隔の設定」（P.11-6）
- 「Fast UDLD の設定」（P.11-6）

- 「ディセーブルになった LAN インターフェイスのリセット」（P.11-7）

UDLD のグローバルなイネーブル化

すべての光ファイバ LAN ポートで 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
`Router(config)# udld {enable | aggressive}`	光ファイバ LAN ポート上で UDLD をグローバルにイネーブルにします。 **（注）** このコマンドで設定できるのは、光ファイバ LAN ポートだけです。このコマンドによる設定は、個々の LAN ポートの設定によって上書きされます。

LAN インターフェイスでの UDLD のイネーブル化

LAN ポート上で 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	`Router(config)# interface type slot/port`	設定する LAN ポートを選択します。
ステップ 2	`Router(config-if)# udld port [aggressive]`	LAN ポートで UDLD をイネーブルにします。 • **aggressive** キーワードを入力して、アグレッシブ モードをイネーブルにします。 • 光ファイバ LAN ポートの場合、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。 • 光ファイバ LAN ポートの場合、**no udld port** コマンドを使用すると、LAN ポートの設定は **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。

光ファイバ以外の LAN インターフェイス上での UDLD のディセーブル化

光ファイバ以外の LAN ポート上で 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	`Router(config)# interface type slot/port`	設定する LAN ポートを選択します。
ステップ 2	`Router(config-if)# no udld port [aggressive]`	光ファイバ以外の LAN ポート上で UDLD をディセーブルにします。

光ファイバ LAN インターフェイス上での UDLD のディセーブル化

個別の光ファイバ LAN ポート上で 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
`Router(config)# interface type slot/port`	設定する LAN ポートを選択します。
`Router(config-if)# udld port disable`	光ファイバの LAN ポート上で UDLD をディセーブルにします。 **（注）** このコマンドの no 形式を使用すると、**udld enable** グローバル コンフィギュレーション コマンド設定に戻ります。この形式は、光ファイバ LAN ポートだけでサポートされています。

UDLD プローブ メッセージ間隔の設定

アドバタイズ モードにあり、現在双方向に設定されているポートで、UDLD プローブ メッセージの間隔を設定するには、次の作業を行います。

コマンド	目的
`Router(config)# udld message time interval`	アドバタイズ モードにあり、現在双方向に設定されているポートで、UDLD プローブ メッセージの間隔を設定します。有効値の範囲は 7 ～ 90 秒です。

Fast UDLD の設定

Fast UDLD は Release 15.0(1)SY1 以降のリリースでサポートされます。ここでは、Fast UDLD の設定手順について説明します。

- 「ポート上の Fast UDLD の設定」（P.11-7）
- 「Fast UDLD エラー通知機能のイネーブル化」（P.11-7）

（注） UDLD がイネーブルになっていないポートで Fast UDLD を設定することはできますが、Fast UDLD がアクティブになるのは、UDLD がそのポートでイネーブルになっている場合だけです。

ポート上の Fast UDLD の設定

特定のポート上で Fast UDLD 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)# udld fast-hello` *interval*	ポート上で Fast UDLD プローブ メッセージ間隔を設定します。 • 「Fast UDLD」（P.11-4）の注意事項と制約事項を参照してください。 • 値を選択する場合は、次の注意事項に従ってください。 – 有効値の範囲は 200 ～ 1000 ミリ秒です。 – Fast UDLD プローブ メッセージ間隔は、必要なリンク障害検出時間を確保できる最大値に調整します。メッセージ間隔が短いと、負荷が大きい場合に UDLD が誤ってリンク障害を通知する可能性が増加します。
ステップ 2	`Router# show udld fast-hello`	Fast UDLD の設定および動作状態を表示します。
ステップ 3	`Router# show udld fast-hello` *type*[1] *slot/number*	ポート単位の Fast UDLD の設定および動作状態を確認します。

1. *type* = **fastethernet**、**gigabitethernet**、または **tengigabitethernet**

Fast UDLD エラー通知機能のイネーブル化

デフォルトでは、Fast UDLD によって、単一方向リンクのポートはエラー ディセーブルになります。単一方向リンクのポートをエラー ディセーブルにする代わりに、Fast UDLD をグローバルにイネーブル化して、単一方向リンクを通知し、コンソールにメッセージを表示することができます。

（注）　Fast UDLD エラー通知機能をイネーブルにする場合、リンクの状態について手動で適切に対処する必要があります。

Fast UDLD エラー通知機能をグローバルにイネーブル化するには、次の作業を行います。

コマンド	目的
`Router(config)# udld fast-hello error-reporting`	Fast UDLD エラー通知機能をイネーブルにします。

ディセーブルになった LAN 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 LAN ポートをリセットするには、次の作業を行います。

コマンド	目的
`Router# udld reset`	UDLD によってシャットダウンされたすべての LAN ポートをリセットします。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CHAPTER 12

EnergyWise の設定

EnergyWise は、Cisco スイッチおよび接続されたデバイスで消費される電力について、設定、レポート、および管理を行う共通のアプローチを提供するシスコのエネルギー管理アーキテクチャです。Cisco EnergyWise では、ネットワーク レベル、サブネットワーク レベル、またはネットワーク エレメント レベルで電力を管理できます。

リリース	機能の変更内容
12.2(33)SXI4	Catalyst 6500 シリーズ スイッチで導入された EnergyWise Phase2
15.0(1)SY1	Catalyst 6500 シリーズ スイッチで導入された EnergyWise Phase 2.6
15.1(1)SY1	Catalyst 6500 シリーズ スイッチで導入された EnergyWise Phase 2.7

ハードウェア互換性マトリクス、新機能の情報、および EnergyWise のリリース番号の詳細については、Cisco EnergyWise リリース ノート（http://www.cisco.com/en/US/products/ps10195/prod_release_notes_list.html）を参照してください。

EnergyWise コンフィギュレーション ガイドおよび EnergyWise Orchestrator コンフィギュレーション ガイドは、次の URL にあります。

http://www.cisco.com/en/US/products/ps10195/products_installation_and_configuration_guides_list.html

その他の Cisco EnergyWise のドキュメント（ホワイト ペーパー、データ シート、FAQ など）については、次の URL を参照してください。

http://www.cisco.com/en/US/products/ps10195/

CHAPTER 13

電源管理

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

電源管理の概要

システムの電源装置を冗長構成にする場合は、両方の電源装置のワット数が同じでなければなりません。Catalyst 6500 シリーズ スイッチでは、同じシャーシ内に AC 入力および DC 入力電源装置の両方を使用できます。サポートされている電源構成の詳細については、『*Catalyst 6500 Series Switch Installation Guide*』を参照してください。

モジュールは、所要電力がそれぞれ異なります。構成によっては、必要とされる電力が 1 台の電源装置では足りない場合があります。電源管理機能を使用すると、電源装置 2 台で搭載されたモジュールすべてに電力供給できます。ただし、両方の電源装置から供給される合計電力が 1 台の電源装置の電力容量よりも大きくなることはないので、冗長構成はこの構成ではサポートされません。ここでは、冗長および非冗長の電源構成について説明します。

電源の冗長性をイネーブルまたはディセーブルにする方法

冗長構成をディセーブルまたは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 **power redundancy-mode combined** | **redundant** コマンドを入力します。電源装置の構成は、いつでも冗長または非冗長に変更できます。

冗長構成をディセーブルにするには、**combined** キーワードを使用します。非冗長構成では、システムで使用できる電力量は、2 台の電源装置で供給できる合計電力です。システムは合計電力量の許容範囲以内であれば、何個でもモジュールに電力を供給できます。ただし、1 台の電源装置が故障し、それまでに電力が供給されていた全モジュールに供給できる十分な電力がない場合、システムは十分な電力を供給できないモジュールの電源を切断します。

冗長構成をイネーブルにするには、**redundant** キーワードを使用します。冗長構成では、両方の電源装置から供給される合計電力が、1 台の電源装置の電力容量よりも大きくなることはありません。1 台の電源装置が故障した場合、もう 1 台がシステムの負荷全体を引き継ぎます。2 台の電源装置を搭載して電源をオンにすると、それぞれの電源装置がシステムに必要な電力の約半分を同時に供給します。負荷分散と冗長構成は自動的にイネーブルになるので、ソフトウェアの設定は必要ありません。

各モジュールの現在のステートおよび使用できる総電力量を表示するには、**show power** コマンドを入力します（「システムの電力ステータスの表示方法」（P.13-3）を参照）。

表 13-1 に、電源装置の構成を変更した場合のシステムへの影響について説明します。

表 13-1　電源装置の構成を変更した場合の影響

構成の変更内容	影響
冗長から非冗長へ	• システム ログと、Syslog メッセージが表示されます。 • システムの電力が、両方の電源装置の合計電力量に増加します。 • 十分な電力がある場合、*show power* コマンド出力の oper state フィールドで **power-deny** と表示されていたモジュールに電源が入ります。
非冗長から冗長へ（両方の電源装置でワット数が同じであるものとします）	• システム ログと、Syslog メッセージが表示されます。 • システムの電力が、一方の電源装置の電力量に減少します。 • それまでに電力が供給されていた全モジュールに供給できる十分な電力がない場合は、一部のモジュールの電源が切断され、そのモジュールについては *show power* コマンド出力の oper state フィールドで **power-deny** と表示されます。
冗長構成がイネーブルで、同じワット数の電源装置を取り付けた場合	• システム ログと、Syslog メッセージが表示されます。 • システムの電力が、一方の電源装置の電力量と等しくなります。 • 供給できる電力量には変化がないので、モジュールのステータスは変化しません。
冗長構成がディセーブルで、同じワット数の電源装置を取り付けた場合	• システム ログと、Syslog メッセージが表示されます。 • システムの電力が、両方の電源装置の合計電力量に増加します。 • 十分な電力がある場合、*show power* コマンド出力の oper state フィールドで **power-deny** と表示されていたモジュールに電源が入ります。
冗長構成がイネーブルで、ワット数がより大きいまたは小さい電源装置を取り付けた場合	• システム ログと、Syslog メッセージが表示されます。 • システムは非冗長連結モードで動作します。
冗長構成がディセーブルで、ワット数がより大きいまたは小さい電源装置を取り付けた場合	• システム ログと、Syslog メッセージが表示されます。 • システムの電力が、両方の電源装置の合計電力量に増加します。 • 十分な電力がある場合、*show power* コマンド出力の oper state フィールドで **power-deny** と表示されていたモジュールに電源が入ります。

表 13-1　電源装置の構成を変更した場合の影響 （続き）

構成の変更内容	影響
冗長構成がイネーブルの電源装置を取り外した場合	• システム ログと、Syslog メッセージが表示されます。 • 供給できる電力量には変化がないので、モジュールのステータスは変化しません。
冗長構成がディセーブルの電源装置を取り外した場合	• システム ログと、Syslog メッセージが表示されます。 • システムの電力が、一方の電源装置の電力量に減少します。 • それまでに電力が供給されていた全モジュールに供給できる十分な電力がない場合は、一部のモジュールの電源が切断され、そのモジュールについては *show power* コマンド出力の oper state フィールドで **power-deny** と表示されます。
ワット数が異なり冗長構成がイネーブルの電源装置を取り付けてシステムを起動した場合	• システム ログと、Syslog メッセージが表示されます。 • システムは、冗長構成ではワット数の異なる電源装置の使用を認めません。ワット数の小さい方の電源装置がシャットダウンされます。
ワット数が等しいかまたは異なり、冗長構成がディセーブルの電源装置を取り付け、システムを起動した場合	• システム ログと、Syslog メッセージが表示されます。 • システムの電力が、両方の電源装置の合計電力と等しくなります。 • システムは合計電力量の許容範囲以内であれば、何個でもモジュールに電力を供給できます。

モジュールの電源切断および電源投入の方法

モジュールの電源を CLI から切断および投入するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# 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	`Router(config)# power enable module slot_number`	モジュールの電源を投入します。
ステップ 3	`Router(config)# no power enable module slot_number`	モジュールの電源を切断します。

（注）　**no power enable module** *slot* コマンドを使用してモジュールの電源を切断した場合、そのモジュールの設定は保存されません。

次に、スロット 3 のモジュールに電源投入する例を示します。

```
Router# configure terminal
Router(config)# power enable module 3
```

システムの電力ステータスの表示方法

show power コマンドはシステム コンポーネントの現在の電力ステータスを表示します。

```
Router# show power
system power redundancy mode = redundant
system power redundancy operationally = non-redundant
system power total =     3795.12 Watts (90.36 Amps @ 42V)
system power used =       864.78 Watts (20.59 Amps @ 42V)
```

```
system power available = 2930.34 Watts (69.77 Amps @ 42V)
                         Power-Capacity PS-Fan Output Oper
PS   Type                Watts   A @42V Status Status State
---- ------------------ ------- ------ ------ ------ -----
1    none
2    WS-CAC-4000W-US    3795.12 90.36  OK     OK     on
                         Pwr-Allocated  Oper
Fan  Type                Watts   A @42V State
---- ------------------ ------- ------ -----
1    WS-C6506-E-FAN      140.70  3.35  OK
                         Pwr-Requested  Pwr-Allocated  Admin Oper
Slot Card-Type           Watts   A @42V Watts   A @42V State State
---- ------------------ ------- ------ ------- ------ ----- -----
5    (Redundant Sup)       -      -      362.04  8.62  -     -
6    VS-SUP2T-10G        362.04  8.62   362.04  8.62  on    on
system auxiliary power mode = off
system auxiliary power redundancy operationally = non-redundant
system primary connector power limit =   7266.00 Watts (173.00 Amps @ 42V)
system auxiliary connector power limit = 10500.00 Watts (250.00 Amps @ 42V)
system primary power used =               864.78 Watts (20.59 Amps @ 42V)
system auxiliary power used =            0 Watt

Router#
```

show power コマンドは特定の電源装置の現在の電力ステータスを表示します。

```
Router# show power status power-supply 2
Power-Capacity PS-Fan Output Oper
PS   Type                Watts   A @42V Status Status State
---- ------------------ ------- ------ ------ ------ -----
2    WS-CAC-4000W-US    3795.12 90.36  OK     OK     on
Router#
```

コマンドに電源番号を指定して、電源の入力フィールドを表示できます。複数の出力モードを持つ電源に対し、新規の電源出力フィールド、および動作モードが表示されます。次のように **show environment status power-supply** コマンドを入力します。

```
Router# show environment status power-supply 1
power-supply 1:
  power-supply 1 fan-fail: OK
  power-supply 1 power-input 1: AC low
  power-supply 1 power-output-fail: OK
Router# show environment status power-supply 2
power-supply 2:
  power-supply 2 fan-fail: OK
  power-supply 2 power-input 1: none
  power-supply 2 power-input 2: AC low
  power-supply 2 power-input 3: AC high
  power-supply 2 power-output: low (mode 1)<<< high for highest mode only
  power-supply 2 power-output-fail: OK
```

モジュールの電源をオフ/オンする方法

モジュールの電源をオフ/オン（リセット）するには、グローバル コンフィギュレーション モードで **power cycle module** *slot* コマンドを入力します。モジュールの電源は 5 秒間オフになり、それからオンになります。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CHAPTER 14

環境モニタリング

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

環境モニタリングの概要

シャーシ コンポーネントの環境をモニタすることにより、コンポーネント障害の兆候を早期に発見し、安全で信頼性の高いシステム運用を実現するとともに、ネットワーク障害を防止することができます。ここでは、これらの重要なシステム コンポーネントをモニタし、システム内でハードウェア関連の問題点を特定し、すみやかに修正する方法を説明します。

センサーの温度しきい値の特定方法

システム センサーは、さまざまな温度しきい値設定に基づいてアラームを発行します。センサーの温度しきい値を表示するには、**show environment alarm threshold** コマンドを使用します。

```
Router> show environment alarm threshold
environmental alarm thresholds:
```

```
power-supply 1 fan-fail: OK
  threshold #1 for power-supply 1 fan-fail:
    (sensor value != 0) is system minor alarm power-supply 1 power-output-fail: OK
  threshold #1 for power-supply 1 power-output-fail:
    (sensor value != 0) is system minor alarm fantray fan operation sensor: OK
  threshold #1 for fantray fan operation sensor:
    (sensor value != 0) is system minor alarm operating clock count: 2
  threshold #1 for operating clock count:
    (sensor value < 2) is system minor alarm
  threshold #2 for operating clock count:
    (sensor value < 1) is system major alarm operating VTT count: 3
  threshold #1 for operating VTT count:
    (sensor value < 3) is system minor alarm
  threshold #2 for operating VTT count:
    (sensor value < 2) is system major alarm VTT 1 OK: OK
  threshold #1 for VTT 1 OK:
    (sensor value != 0) is system minor alarm VTT 2 OK: OK
  threshold #1 for VTT 2 OK:
    (sensor value != 0) is system minor alarm VTT 3 OK: OK
  threshold #1 for VTT 3 OK:
    (sensor value != 0) is system minor alarm clock 1 OK: OK
  threshold #1 for clock 1 OK:
    (sensor value != 0) is system minor alarm clock 2 OK: OK
  threshold #1 for clock 2 OK:
    (sensor value != 0) is system minor alarm module 1 power-output-fail: OK
  threshold #1 for module 1 power-output-fail:
    (sensor value != 0) is system major alarm module 1 outlet temperature: 21C
  threshold #1 for module 1 outlet temperature:
    (sensor value > 60) is system minor alarm
  threshold #2 for module 1 outlet temperature:
    (sensor value > 70) is system major alarm module 1 inlet temperature: 25C
  threshold #1 for module 1 inlet temperature:
    (sensor value > 60) is system minor alarm
  threshold #2 for module 1 inlet temperature:
    (sensor value > 70) is system major alarm module 1 device-1 temperature: 30C
  threshold #1 for module 1 device-1 temperature:
    (sensor value > 60) is system minor alarm
  threshold #2 for module 1 device-1 temperature:
    (sensor value > 70) is system major alarm module 1 device-2 temperature: 29C
  threshold #1 for module 1 device-2 temperature:
    (sensor value > 60) is system minor alarm
  threshold #2 for module 1 device-2 temperature:
    (sensor value > 70) is system major alarm module 5 power-output-fail: OK
  threshold #1 for module 5 power-output-fail:
    (sensor value != 0) is system major alarm module 5 outlet temperature: 26C
  threshold #1 for module 5 outlet temperature:
    (sensor value > 60) is system minor alarm
  threshold #2 for module 5 outlet temperature:
    (sensor value > 75) is system major alarm module 5 inlet temperature: 23C
  threshold #1 for module 5 inlet temperature:
    (sensor value > 50) is system minor alarm
  threshold #2 for module 5 inlet temperature:
    (sensor value > 65) is system major alarm EARL 1 outlet temperature: N/O
  threshold #1 for EARL 1 outlet temperature:
    (sensor value > 60) is system minor alarm
  threshold #2 for EARL 1 outlet temperature:
    (sensor value > 75) is system major alarm EARL 1 inlet temperature: N/O
  threshold #1 for EARL 1 inlet temperature:
    (sensor value > 50) is system minor alarm
  threshold #2 for EARL 1 inlet temperature:
    (sensor value > 65) is system major alarm
```

システム環境ステータスのモニタ方法

システム ステータス情報を表示するには、**show environment** [**alarm** | **cooling** | **status** | **temperature**] コマンドを入力します。キーワードを指定することで、次の情報が表示されます。

- **alarm**：環境アラームを表示します。
  - **status**：アラーム ステータスを表示します。
  - **thresholds**：アラームしきい値を表示します。
- **cooling**：ファン トレイ ステータス、シャーシの冷却容量、周囲温度、およびスロット単位の冷却容量を表示します。
- **status**：現場交換可能ユニット（FRU）の動作ステータスおよび電源と温度の情報を表示します。
- **temperature**：FRU の温度情報を表示します。

システム ステータス情報を表示するには、**show environment** コマンドを入力します。

```
Router# show environment
environmental alarms:
  no alarms

Router# show environment alarm
environmental alarms:
  no alarms

Router# show environment cooling
fan-tray 1:
  fan-tray 1 type: WS-C6513-E-FAN
  fan-tray 1 mode: High-power
  fan-tray 1 fan-fail: OK
chassis per slot cooling capacity: 94 cfm
ambient temperature: < 55C
  module 3 cooling requirement: 84 cfm
  module 7 cooling requirement: 35 cfm

Router# show environment status
backplane:
  operating clock count: 2
  operating VTT count: 3
  operating fan count: 1

fan-tray 1:
  fan-tray 1 type: WS-C6513-E-FAN
  fan-tray 1 mode: High-power
  fan-tray 1 fan-fail: OK
VTT 1:
  VTT 1 OK: OK
  VTT 1 outlet temperature: 30C
VTT 2:
  VTT 2 OK: OK
  VTT 2 outlet temperature: 28C
VTT 3:
  VTT 3 OK: OK
  VTT 3 outlet temperature: 29C
clock 1:
  clock 1 OK: OK, clock 1 clock-inuse: in-use
clock 2:
  clock 2 OK: OK, clock 2 clock-inuse: not-in-use
power-supply 1:
  power-supply 1 fan-fail: OK
  power-supply 1 power-input: AC low
  power-supply 1 power-output-mode: low
```

```
  power-supply 1 power-output-fail: OK
power-supply 2:
  power-supply 2 fan-fail: OK
  power-supply 2 power-input: AC low
  power-supply 2 power-output-mode: low
  power-supply 2 power-output-fail: OK
module 3:
  module 3 power-output-fail: OK
  module 3 outlet temperature: N/O
  module 3 inlet temperature: N/O
  module 3 asic-1 temperature: 72C
  module 3 asic-2 temperature: 81C
  module 3 EARL outlet temperature: 43C
  module 3 EARL inlet temperature: 33C
module 7:
  module 7 power-output-fail: OK
  module 7 outlet temperature: 44C
  module 7 inlet temperature: 27C
  module 7 device-1 temperature: 39C
  module 7 device-2 temperature: 41C
  module 7 asic-1 temperature: 69C
  module 7 asic-2 temperature: 68C
  module 7 asic-3 temperature: 50C
  module 7 asic-4 temperature: 72C
  module 7 asic-5 temperature: 55C
  module 7 asic-6 temperature: 60C
  module 7 asic-7 temperature: 63C
  module 7 asic-8 temperature: 59C
  module 7 RP outlet temperature: 39C
  module 7 RP inlet temperature: 34C
  module 7 RP device-1 temperature: 42C
  module 7 EARL outlet temperature: 42C
  module 7 EARL inlet temperature: 30C

Router#
```

LED 環境表示に関する情報

LED は、メジャーとマイナーの 2 種類のアラームを示します。メジャー アラームは、システムのシャットダウンを引き起こす可能性のある重大な問題を表します。マイナー アラームは、解消されなければ重大な問題に発展する可能性のある問題を表すメッセージです。

過熱状態により、システムが（メジャーまたはマイナー）アラームを表示した場合、5 分間アラームは取り消されず、いかなる（モジュールのリセットまたはシャットダウンなどの）措置も行われません。この間に温度がアラームしきい値より 5 °C（41 °F）下がると、アラームは取り消されます。

表 14-1 に、スーパーバイザ エンジンおよびスイッチング モジュールに関する環境インジケータを示します。

（注） スーパーバイザ エンジンの SYSTEM LED を含む、LED の詳細については、『*Catalyst 6500 Series Switch Module Installation Guide*』を参照してください。

表 14-1　スーパーバイザ エンジンおよびスイッチング モジュールの環境モニタリング

コンポーネント	アラームの種類	LED 表示	アクション
スーパーバイザ エンジンの温度センサーがメジャーしきい値を超過	メジャー	STATUS LED レッド	Syslog メッセージおよび SNMP トラップを生成します。 冗長構成の場合、システムは冗長スーパーバイザ エンジンに切り替え、アクティブなスーパーバイザ エンジンはシャットダウンします。 冗長構成ではなく、過熱状態が改善されない場合、システムは 5 分後にシャットダウンします。
（注） • 温度センサーは、主要なスーパーバイザ エンジン コンポーネント（ドーター カードも含む）をモニタします。 • STATUS LED は、スーパーバイザ エンジンの前面パネルおよびすべてのモジュールの前面パネルにあります。 • STATUS LED は、スーパーバイザ エンジンが故障するとレッドになります。冗長構成のスーパーバイザがない場合は、SYSTEM LED もレッドになります。			
スーパーバイザ エンジンの温度センサーが、マイナーしきい値を超過	マイナー	STATUS LED オレンジ	Syslog メッセージおよび SNMP トラップを生成します。 状態をモニタします。
冗長スーパーバイザ エンジンの温度センサーがメジャーまたはマイナーしきい値を超過			Syslog メッセージおよび SNMP トラップを生成します。
	メジャー	STATUS LED レッド	メジャー アラームが発生し過熱状態が改善されない場合、システムは 5 分後にシャットダウンします。
	マイナー	STATUS LED オレンジ	マイナー アラームが生成された場合、状態をモニタします。
スイッチング モジュールの温度センサーがメジャーしきい値を超過	メジャー	STATUS LED レッド	Syslog メッセージおよび SNMP を生成します。 モジュールの電源を切断します（手順については、「モジュールの電源切断および電源投入の方法」（P.13-3）を参照してください）。
スイッチング モジュールの温度センサーがマイナーしきい値を超過	マイナー	STATUS LED オレンジ	Syslog メッセージおよび SNMP トラップを生成します。 状態をモニタします。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CHAPTER 15

オンライン診断

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

オンライン診断機能の前提条件

なし。

オンライン診断の制約事項

なし。

オンライン診断について

オンライン診断では、動作中のネットワークにスイッチが接続されている間に、スイッチのハードウェア機能についてテストし、確認することができます。

オンライン診断には、個別のハードウェア コンポーネントを確認して、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 テストが含まれます。これには、中断を伴うオンライン診断テスト（Built In Self Test（BIST）や破壊モードのループバック テストなど）と中断を伴わないオンライン診断テスト（パケット スイッチング、ブートアップ中の実行、モジュールの活性挿抜（OIR）、システム リセット）があります。中断を伴わないオンライン診断テストは、バックグラウンド ヘルス モニタリングの一部として実行されます。中断を伴うテストまたは中断を伴わないテストは、ユーザ要求により（オンデマンドで）実行できます。

オンライン診断では、次の分野の問題が検出されます。

- ハードウェア コンポーネント
- インターフェイス（GBIC、イーサネット ポートなど）
- コネクタ（コネクタのゆるみ、曲がったピンなど）
- はんだ接合
- メモリ（年数経過による故障）

オンライン診断は、ハイ アベイラビリティ機能要件の 1 つです。ハイ アベイラビリティは、装置の故障によるネットワークへの影響を制限しようとする、一連の品質規格です。ハイ アベイラビリティの重要な要素は、アクティブ ネットワークでスイッチが動作しているときに、ハードウェア障害を検出して対策をとることです。ハイ アベイラビリティのオンライン診断では、ハードウェア障害を検出して、スイッチオーバーを判断するためにハイ アベイラビリティ ソフトウェアにフィードバックします。

オンライン診断はブートアップ、オンデマンド、スケジュール、またはヘルス モニタリング診断に分類されます。ブートアップ診断は、ブートアップ中に実行します。オンデマンド診断は CLI から実行します。スケジュール診断は、スイッチが稼働中のネットワークに接続している状態で、ユーザが指定した間隔や指定した時間に実行します。ヘルス モニタリング診断はバックグラウンドで実行します。

オンライン診断のデフォルト設定

付録 A「オンライン診断テスト」の各テストのデフォルト情報を参照してください。

オンライン診断の設定方法

- 「起動オンライン診断レベルの設定」（P.15-3）
- 「オンデマンド オンライン診断の設定」（P.15-3）
- 「オンライン診断のスケジューリング」（P.15-5）

起動オンライン診断レベルの設定

起動診断レベルは最小または完全として設定できます。または起動オンライン診断をまったく実行しないこともできます。すべての診断テストを実行するには、**complete** キーワードを入力します。スイッチのすべてのポートに対し、EARL テストとループバック テストだけを実行するには、**minimal** キーワードを入力します。すべての診断テストを省略するには、コマンドの **no** 形式を入力します。起動診断レベルのデフォルトは最小です。

起動診断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
Router(config)# **diagnostic bootup level** {**minimal** | **complete**}	起動診断レベルを設定します。

次に、起動オンライン診断レベルを設定する例を示します。

```
Router(config)# diagnostic bootup level complete
Router(config)#
```

次に、起動オンライン診断レベルを表示する例を示します。

```
Router(config)# show diagnostic bootup level
Current bootup diagnostic level: complete

Router(config)#
```

オンデマンド オンライン診断の設定

CLI からオンデマンド オンライン診断テストを実行できます。障害が検出された場合にテストを停止または継続するように、あるいは障害カウントを使用して特定の障害数に達した場合にテストを停止するように、実行アクションを設定できます。反復設定を使用して、複数回テストを実行するように設定できます。

メモリ テストの前にパケット スイッチング テストを実行してください。

（注） 次に示すすべてのステップを完了するまで、**diagnostic start all** コマンドは使用しないでください。

一部のオンデマンド オンライン診断テストは、他のテストの結果に影響を及ぼすことがあります。したがって、各テストは次の順序で実行する必要があります。

1. 中断を伴わないテストを実行します。
2. 関連する機能分野に含まれるすべてのテストを実行します。
3. TestTrafficStress テストを実行します。
4. TestEobcStressPing テストを実行します。
5. 完全メモリ テストを実行します。

オンデマンド オンライン診断テストを実行するには、次の作業を行います。

ステップ 1　中断を伴わないテストを実行します。

使用可能なテストとその属性を表示し、中断を伴わないカテゴリに属するコマンドを判別するには、**show diagnostic content** コマンドを使用します。

ステップ 2　関連する機能分野に含まれるすべてのテストを実行します。

パケット スイッチング テストは、それぞれ特定の機能分野に分類されます。特定の機能分野で問題の発生が疑われる場合は、この機能分野に含まれるすべてのテストを実行します。テストに必要な機能分野を明確に特定できない場合、または使用可能なすべてのテストを実行するには、**complete** キーワードを入力します。

ステップ 3　TestTrafficStress テストを実行します。

これは、中断を伴うパケット スイッチング テストです。このテストでは、ストレス テストとして、一組のポート間でパケットをラインレートでスイッチングします。このテストの実行中、すべてのポートはシャットダウンされ、リンク フラップが生じることもあります。リンク フラップは、テストの完了後に回復します。このテストの完了には数分かかります。

このテストを実行する前に、**no diagnostic monitor module** *number* **test all** コマンドを使用して、すべてのヘルス モニタリング テストをディセーブルにします。

ステップ 4　TestEobcStressPing テストを実行します。

これはディスラプティブ テストであり、モジュールの Ethernet over Backplane Channel（EOBC）接続をテストします。このテストの完了には数分かかります。このテストの実行後は、上記の各ステップに示したすべてのパケット スイッチング テストが実行できなくなります。ただし、このテストの実行後も、これ以降に説明する各テストは実行できます。

このテストを実行する前に、**no diagnostic monitor module** *number* **test all** コマンドを使用して、すべてのヘルス モニタリング テストをディセーブルにします。このテスト中は EOBC 接続が中断されるため、ヘルス モニタリング テストが失敗し、回復アクションが実行されます。

ステップ 5　完全メモリ テストを実行します。

完全メモリ テストを実行する前に、すべてのヘルス モニタリング テストをディセーブルにする必要があります。これは、ヘルス モニタリングがイネーブルになっているとテストが失敗し、回復アクションが実行されてしまうためです。ヘルス モニタリング診断テストをディセーブルにするには、**no diagnostic monitor module** *number* **test all** コマンドを使用します。

完全メモリ テストは、次の順序で実行します。

1. TestFibTcamSSRAM
2. TestAclQosTcam
3. TestNetFlowTcam
4. TestAsicMemory
5. TestAsicMemory

完全メモリ テストの実行後はスイッチを再起動して、動作可能な状態に戻す必要があります。完全メモリ テストの実行後は、スイッチ上で他のテストをすべて実行できなくなります。設定値はテスト中に変更されているため、再起動時に設定を保存しないでください。リブート後は、**diagnostic monitor module** *number* **test all** コマンドを使用して、ヘルス モニタリング テストを再度イネーブルにします。

起動診断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
Router# **diagnostic ondemand** {**iteration** *iteration_count*} | {**action-on-error {continue** | **stop**} [*error_count*]}	実行するオンデマンド診断テスト、実行回数（反復）、エラーを検出したときに実行する処置を設定します。

次に、オンデマンド テスト反復カウントを設定する例を示します。

```
Router# diagnostic ondemand iteration 3
Router#
```

次に、エラーを検出したときに実行する処置を設定する例を示します。

```
Router# diagnostic ondemand action-on-error continue 2
Router#
```

オンライン診断のスケジューリング

オンライン診断は、1 日のうち指定した時間、毎日、毎週、または毎月実行するよう、スケジューリングできます。あるインターバルで 1 回だけ、または繰り返しテストを実行するようスケジューリングできます。スケジューリングを削除するには、コマンドの **no** 形式を入力します。

オンライン診断をスケジューリングするには、次の作業を行います。

コマンド	目的
Router(config)# **diagnostic schedule module** *number* **test** {*test_id* | *test_id_range* | **all**} [**port** {*num* | *num_range* | **all**}] {**on** *mm dd yyyy hh*:*mm*} | {**daily** *hh*:*mm*} | {**weekly** *day_of_week hh*:*mm*}	特定の日時に特定のモジュールでオンデマンド診断テストを実行すること、および、その実行（反復）回数と、エラー検出時に行われるアクションについて、スケジューリングします。

次に、モジュール 1 の特定のポートについて、特定の日時に診断テストを実行するようにスケジューリングする例を示します。

```
Router(config)# diagnostic schedule module 1 test 1,2,5-9 port 3 on january 3 2003 23:32
Router(config)#
```

次に、特定のポートについて、毎日一定の時間に診断テストを実行するようにスケジューリングする例を示します。

```
Router(config)# diagnostic schedule module 1 test 1,2,5-9 port 3 daily 12:34
Router(config)#
```

次に、特定のポートについて、毎週一定の曜日に診断テストを実行するようにスケジューリングする例を示します。

```
Router(config)# diagnostic schedule module 1 test 1,2,5-9 port 3 weekly friday 09:23
Router(config)#
```

ヘルス モニタリング診断の設定

スイッチが稼働中のネットワークに接続している間に、ヘルス モニタリング診断テストを設定できます。ヘルス モニタリング診断テストの実行間隔と、テストに障害が発生したときにシステム メッセージを生成する、あるいは各テストをイネーブルまたはディセーブルにするように設定できます。テストをディセーブルにするには、コマンドの **no** 形式を入力します。

ヘルス モニタリング診断テ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	`Router(config)# diagnostic monitor interval module number test {test_id | test_id_range | all} [hour hh] [min mm] [second ss] [millisec ms] [day day]`	指定のテストに対し、ヘルス モニタリングの実行間隔を設定します。このコマンドの **no** 形式は、間隔をデフォルトまたは 0 に変更します。
ステップ 2	`Router(config)#[no] diagnostic monitor module number test {test_id | test_id_range | all}`	ヘルス モニタリング診断テストをイネーブルまたはディセーブルにします。

次に、モジュール 1 で 2 分ごとに指定されたテストを実行するように設定する例を示します。

```
Router(config)# diagnostic monitor interval module 1 test 1 min 2
Router(config)#
```

次に、ヘルス モニタリングがそれまでイネーブル状態でない場合に、テストを実行する例を示します。

```
Router(config)# diagnostic monitor module 1 test 1
```

次に、ヘルス モニタリング テストが失敗したときに Syslog メッセージを生成する例を示します。

```
Router(config)# diagnostic monitor syslog
Router(config)#
```

オンライン診断テストの実行方法

診断テストの実行の概要

オンライン診断を設定したあと、診断テストを開始または停止したり、またはテスト結果を表示したりできます。どのテストが設定され、どの診断テストがすでに実行されたかも、参照できます。

- オンライン診断テストをイネーブルにする前に、ロギング コンソール/モニタをイネーブルにして、すべての警告メッセージを確認します。
- 中断を伴うテストを実行している場合、コンソールを介して接続されたらテストを実行します。中断を伴うテストが完了すると、コンソールにシステムをリロードして通常の動作に戻すよう指示するメッセージが表示されます。この警告に従ってください。
- テストの実行中、すべてのポートはシャットダウンされます。負荷テストが内部でループするよう設定されたポートを使用して行われるためです。外部トラフィックによってテスト結果が変わることがあります。スイッチを正常な稼働に戻すために、スイッチをリロードしなければなりません。スイッチをリロードするコマンドを入力すると、コンフィギュレーションを保存するかどうかを聞かれます。コンフィギュレーションは保存しないでください。
- スーパーバイザ エンジン上でテストを実行している場合、テストの開始および終了後に、システム全体のリロードまたは電源のオフ/オンを行う必要があります。
- スイッチング モジュール（スーパーバイザ エンジンではなく）上でテストを実行している場合、テストの開始および終了後に、スイッチング モジュールをリセットする必要があります。

オンライン診断テストの開始または停止

実行する診断テストを設定したあと、診断テストを開始または停止するには **start** および **stop** を使用します。オンライン診断コマンドを開始または停止するには、次の作業を行います。

コマンド	目的
Router# **diagnostic start module** *number* **test** {*test_id* | *test_id_range* | **minimal** | **complete** | **basic** | **per-port** | **non-disruptive** | **all**} [**port** {*num* | *port#_range* | **all**}]	指定したモジュールのポートまたはポート範囲で、診断テストを開始します。
Router# **diagnostic stop module** *number*	指定したモジュールで診断テストを停止します。

次に、モジュール 1 で診断テストを開始する例を示します。

```
Router# diagnostic start module 1 test 5
Module 1:Running test(s) 5 may disrupt normal system operation
Do you want to run disruptive tests? [no]yes
00:48:14:Running OnDemand Diagnostics [Iteration #1] ...
00:48:14:%DIAG-SP-6-TEST_RUNNING:Module 1:Running TestNewLearn{ID=5} ...
00:48:14:%DIAG-SP-6-TEST_OK:Module 1:TestNewLearn{ID=5} has completed successfully
00:48:14:Running OnDemand Diagnostics [Iteration #2] ...
00:48:14:%DIAG-SP-6-TEST_RUNNING:Module 1:Running TestNewLearn{ID=5} ...
00:48:14:%DIAG-SP-6-TEST_OK:Module 1:TestNewLearn{ID=5} has completed successfully
Router#
```

次に、診断テストを停止する例を示します。

```
Router# diagnostic stop module 1
Router#
```

すべてのオンライン診断テストの実行

すべての診断テスト（中断を伴う診断テストおよび中断を伴わない診断テスト）を 1 つのコマンドで同時に実行できます。この場合、すべてのテストの依存関係は自動的に処理されます。

（注）

- オンライン診断テストを実行すると通常のシステム動作が中断されます。**diagnostic start system test all** コマンドを完了したあと、システムをリセットします。
- システム テストの実行中は、モジュールやスーパーバイザの挿入、取り外し、電源切断を行わないでください。
- システム テストの実行中は、**diagnostic stop system test all** コマンド以外の診断コマンドを実行しないでください。
- トラフィックがバックグラウンドで実行されていないことを確認します。

すべてのオンライン診断テストを開始または停止するには、次の作業を行います。

コマンド	目的
Router# **diagnostic start system test all**	すべてのオンライン診断テストを実行します。
Router# **diagnostic stop system test all**	すべてのオンライン診断テストの実行を停止します。

次に、すべてのオンライン診断テストを開始する例を示します。

```
Router# diagnostic start system test all
**************************************************************************
* WARNING:                                                               *
*   'diagnostic start system test all' will disrupt normal system        *
*   operation. The system requires RESET after the command               *
*   'diagnostic start system test all' has completed prior to            *
*   normal use.                                                          *
*                                                                        *
* IMPORTANT:                                                             *
*   1. DO NOT INSERT, OIR, or POWER DOWN Linecards or                    *
*      Supervisor while system test is running.                          *
*                                                                        *
*   2. DO NOT ISSUE ANY DIAGNOSTIC COMMAND except                        *
*      "diagnostic stop system test all" while system test               *
*      is running.                                                       *
*                                                                        *
*   3. PLEASE MAKE SURE no traffic is running in background.             *
**************************************************************************
Do you want to continue? [no]:
```

オンライン診断テストおよびテスト結果の表示

次の **show** コマンドを使用すると、設定されたオンライン診断テストを表示し、テスト結果を確認できます。

- **show diagnostic content**
- **show diagnostic health**

設定された診断テストを表示するには、次の作業を行います。

コマンド	目的
show diagnostic {**bootup level** | **content** [**module** *num*] | **events** [**module** *num*] [**event-type** *event-type*] | **health** | **ondemand settings** | **result** [**module** *num*] [**detail**] | **schedule** [**module** *num*]}	オンライン診断のテスト結果を表示し、サポートされるテスト スイートを一覧します。

次に、モジュール 6 に設定されたオンライン診断を表示する 例を示します。

```
Router# show diagnostic content module 6

Module 6: Supervisor Engine 2T 10GE w/ CTS (Active)

  Diagnostics test suite attributes:
    M/C/* - Minimal bootup level test / Complete bootup level test / NA
      B/* - Basic ondemand test / NA
    P/V/* - Per port test / Per device test / NA
    D/N/* - Disruptive test / Non-disruptive test / NA
      S/* - Only applicable to standby unit / NA
      X/* - Not a health monitoring test / NA
      F/* - Fixed monitoring interval test / NA
      E/* - Always enabled monitoring test / NA
      A/I - Monitoring is active / Monitoring is inactive
      R/* - Power-down line cards and need reload supervisor / NA
      K/* - Require resetting the line card after the test has completed / NA
      T/* - Shut down all ports and need reload supervisor / NA

                                                        Test Interval   Thre-
  ID   Test Name                           Attributes     day hh:mm:ss.ms shold
  ==== ================================== ============   =============== =====
    1) TestTransceiverIntegrity --------> **PD*X**I***    not configured  n/a
    2) TestLoopback --------------------> M*PD*X**I***    not configured  n/a
    3) TestActiveToStandbyLoopback -----> M*PDSX**I***    not configured  n/a
    4) TestL2CTSLoopback ---------------> M*PD*X**I***    not configured  n/a
    5) TestL3CTSLoopback ---------------> M*PD*X**I***    not configured  n/a
    6) TestScratchRegister -------------> ***N****A***    000 00:00:30.00 5
    7) TestNewIndexLearn ---------------> M**N****I***    000 00:00:15.00 10
    8) TestDontConditionalLearn --------> M**N****I***    000 00:00:15.00 10
    9) TestBpduTrap --------------------> M**D*X**I***    not configured  n/a
   10) TestMatchCapture ----------------> M**D*X**I***    not configured  n/a
   11) TestProtocolMatchChannel --------> M**D*X**I***    not configured  n/a
   12) TestMacNotification -------------> M**NS***A***    000 00:00:15.00 10
   13) TestPortSecurity ----------------> M**D*X**I***    not configured  n/a
   14) TestIPv4FibShortcut -------------> M**N****I***    000 00:00:15.00 10
   15) TestL3Capture2 ------------------> M**D*X**I***    not configured  n/a
   16) TestIPv6FibShortcut -------------> M**N****I***    000 00:00:15.00 10
   17) TestMPLSFibShortcut -------------> M**N****I***    000 00:00:15.00 10
   18) TestNATFibShortcut --------------> M**N****I***    000 00:00:15.00 10
   19) TestAclPermit -------------------> M**N****I***    000 00:00:15.00 10
   20) TestAclDeny ---------------------> M**D*X**I***    not configured  n/a
   21) TestAclRedirect -----------------> M**N****I***    not configured  n/a
   22) TestRBAcl -----------------------> M**N****I***    not configured  n/a
   23) TestQos -------------------------> M**D*X**I***    not configured  n/a
   24) TestDQUP ------------------------> M**D*X**I***    not configured  n/a
   25) TestL3VlanMet -------------------> M**D*X**I***    not configured  n/a
   26) TestIngressSpan -----------------> M**D*X**I***    not configured  n/a
   27) TestEgressSpan ------------------> M**D*X**I***    not configured  n/a
   28) TestNetflowShortcut -------------> M**D*X**I***    not configured  n/a
   29) TestInbandEdit ------------------> M**D*X**I***    not configured  n/a
```

```
  30) TestFabricInternalSnake ---------> M**D*X**I***    not configured  n/a
  31) TestFabricExternalSnake ---------> M**D*X**I***    not configured  n/a
  32) TestFabricVlanLoopback ----------> M**N*X**I***    not configured  n/a
  33) TestTrafficStress ---------------> ***D*X**I**T    not configured  n/a
  34) TestL3TcamMonitoring ------------> ***N****A***    000 00:00:15.00 10
  35) TestFibTcam ---------------------> ***D*X**IR**    not configured  n/a
  36) TestAclQosTcam ------------------> ***D*X**IR**    not configured  n/a
  37) TestEarlMemOnBootup -------------> M**N*X**I***    not configured  n/a
  38) TestAsicMemory ------------------> ***D*X**IR**    not configured  n/a
  39) ScheduleSwitchover --------------> ***D*X**I***    not configured  n/a
  40) TestFirmwareDiagStatus ----------> M**N****I***    000 00:00:15.00 10
  41) TestAsicSync --------------------> ***N****A***    000 00:00:15.00 10
  42) TestUnusedPortLoopback ----------> **PN****A***    000 00:01:00.00 10
  43) TestNonDisruptiveLoopback -------> **PN****A***    000 00:00:10.00 10
  44) TestFabricFlowControlStatus -----> ***N****I***    000 00:00:15.00 10
  45) TestPortTxMonitoring ------------> **PN****A***    000 00:01:15.00 5
  46) TestOBFL ------------------------> M**N****I***    000 00:00:15.00 10
  47) TestCFRW ------------------------> M*VN*X**I***    not configured  n/a
  48) TestLtlFpoeMemoryConsistency ----> ***N****A***    000 00:00:30.00 1
  49) TestErrorCounterMonitor ---------> ***N****A***    000 00:00:30.00 10
  50) TestEARLInternalTables ----------> ***N****A***    000 00:05:00.00 1

Router#
```

次に、モジュール 6 のオンライン診断結果を表示する例を示します。

```
Router# show diagnostic result module 6

Current bootup diagnostic level: minimal

Module 6: Supervisor Engine 2T 10GE w/ CTS (Active)  SerialNo : SAD132602A6

  Overall Diagnostic Result for Module 6 : PASS
  Diagnostic level at card bootup: minimal

  Test results: (. = Pass, F = Fail, U = Untested)

    1) TestTransceiverIntegrity:

      Port  1  2  3  4  5
      --------------------
            U  U  U  U  U


    2) TestLoopback:

      Port  1  2  3  4  5
      --------------------
            .  .  .  .  .


    3) TestActiveToStandbyLoopback:

      Port  1  2  3  4  5
      --------------------
            U  U  U  U  U


    4) TestL2CTSLoopback:

      Port  1  2  3  4  5
      --------------------
            .  .  .  .  .
```

```
 5) TestL3CTSLoopback:

   Port  1  2  3  4  5
   --------------------
         .  .  .  .  .


 6) TestScratchRegister -------------> .
 7) TestNewIndexLearn ---------------> .
 8) TestDontConditionalLearn --------> .
 9) TestBpduTrap --------------------> .
10) TestMatchCapture ----------------> .
11) TestProtocolMatchChannel --------> .
12) TestMacNotification -------------> U
13) TestPortSecurity ----------------> .
14) TestIPv4FibShortcut -------------> .
15) TestL3Capture2 ------------------> .
16) TestIPv6FibShortcut -------------> .
17) TestMPLSFibShortcut -------------> .
18) TestNATFibShortcut --------------> .
19) TestAclPermit -------------------> .
20) TestAclDeny ---------------------> .
21) TestAclRedirect -----------------> .
22) TestRBAcl -----------------------> .
23) TestQos -------------------------> .
24) TestDQUP ------------------------> .
25) TestL3VlanMet -------------------> .
26) TestIngressSpan -----------------> .
27) TestEgressSpan ------------------> .
28) TestNetflowShortcut -------------> .
29) TestInbandEdit ------------------> .
30) TestFabricInternalSnake ---------> .
31) TestFabricExternalSnake ---------> .
32) TestFabricVlanLoopback ----------> .
33) TestTrafficStress ---------------> U
34) TestL3TcamMonitoring ------------> .
35) TestFibTcam ---------------------> U
36) TestAclQosTcam ------------------> U
37) TestEarlMemOnBootup -------------> .
38) TestAsicMemory ------------------> U
39) ScheduleSwitchover --------------> U
40) TestFirmwareDiagStatus ----------> .
41) TestAsicSync --------------------> .
42) TestUnusedPortLoopback:

   Port  1  2  3  4  5
   --------------------
         U  U  U  .  .


43) TestNonDisruptiveLoopback:

   Port  1  2  3  4  5
   --------------------
         U  U  U  U  U


44) TestFabricFlowControlStatus -----> U
45) TestPortTxMonitoring:

   Port  1  2  3  4  5
   --------------------
         U  U  U  U  U
```

```
  46) TestOBFL ------------------------> .
  47) TestCFRW:

     Device  1
     ---------
             .


  48) TestLtlFpoeMemoryConsistency ----> .
  49) TestErrorCounterMonitor ---------> .
  50) TestEARLInternalTables ----------> .


Router#
```

次に、モジュール 6 のオンライン診断結果の詳細を表示する例を示します。

```
Router# show diagnostic result module 6 detail

Current bootup diagnostic level: minimal

Module 6: Supervisor Engine 2T 10GE w/ CTS (Active)  SerialNo : SAD132602A6

  Overall Diagnostic Result for Module 6 : PASS
  Diagnostic level at card bootup: minimal

  Test results: (. = Pass, F = Fail, U = Untested)

  ____________________________________________________________________________

    1) TestTransceiverIntegrity:

       Port  1  2  3  4  5
       -------------------
             U  U  U  U  U


           Error code ------------------> 3 (DIAG_SKIPPED)
           Total run count -------------> 0
           Last test testing type ------> n/a
           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
  ____________________________________________________________________________

    2) TestLoopback:

       Port  1  2  3  4  5
       -------------------
             .  .  .  .  .


           Error code ------------------> 0 (DIAG_SUCCESS)
           Total run count -------------> 1
           Last test testing type ------> Bootup
           Last test execution time ----> May 13 2011 21:59:25
           First test failure time -----> n/a
           Last test failure time ------> n/a
           Last test pass time ---------> May 13 2011 21:59:25
```

```
      Total failure count ---------> 0
      Consecutive failure count ---> 0
_____________________________________________________________________________

  3) TestActiveToStandbyLoopback:

    Port  1  2  3  4  5
    -------------------
          U  U  U  U  U


      Error code ------------------> 3 (DIAG_SKIPPED)
      Total run count -------------> 0
      Last test testing type ------> n/a
      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
_____________________________________________________________________________

  4) TestL2CTSLoopback:

    Port  1  2  3  4  5
    -------------------
          .  .  .  .  .


      Error code ------------------> 0 (DIAG_SUCCESS)
      Total run count -------------> 1
      Last test testing type ------> Bootup
      Last test execution time ----> May 13 2011 21:59:29
      First test failure time -----> n/a
      Last test failure time ------> n/a
      Last test pass time ---------> May 13 2011 21:59:29
      Total failure count ---------> 0
      Consecutive failure count ---> 0
_____________________________________________________________________________

  5) TestL3CTSLoopback:

    Port  1  2  3  4  5
    -------------------
          .  .  .  .  .


      Error code ------------------> 0 (DIAG_SUCCESS)
      Total run count -------------> 1
      Last test testing type ------> Bootup
      Last test execution time ----> May 13 2011 21:59:33
      First test failure time -----> n/a
      Last test failure time ------> n/a
      Last test pass time ---------> May 13 2011 21:59:33
      Total failure count ---------> 0
      Consecutive failure count ---> 0
_____________________________________________________________________________

  6) TestScratchRegister -------------> .

      Error code ------------------> 0 (DIAG_SUCCESS)
      Total run count -------------> 8191
      Last test testing type ------> Health Monitoring
      Last test execution time ----> May 16 2011 21:42:41
```

```
        First test failure time -----> n/a
        Last test failure time ------> n/a
        Last test pass time ---------> May 16 2011 21:42:41
        Total failure count ---------> 0
        Consecutive failure count ---> 0
_____________________________________________________________________________

  7) TestNewIndexLearn ---------------> .

        Error code ------------------> 0 (DIAG_SUCCESS)
        Total run count -------------> 1
        Last test testing type ------> Bootup
        Last test execution time ----> May 13 2011 21:59:37
        First test failure time -----> n/a
        Last test failure time ------> n/a
        Last test pass time ---------> May 13 2011 21:59:37
        Total failure count ---------> 0
        Consecutive failure count ---> 0
_____________________________________________________________________________

  8) TestDontConditionalLearn --------> .

        Error code ------------------> 0 (DIAG_SUCCESS)
        Total run count -------------> 1
        Last test testing type ------> Bootup
        Last test execution time ----> May 13 2011 21:59:37
        First test failure time -----> n/a
        Last test failure time ------> n/a
        Last test pass time ---------> May 13 2011 21:59:37
        Total failure count ---------> 0
        Consecutive failure count ---> 0
_____________________________________________________________________________

  9) TestBpduTrap --------------------> .

        Error code ------------------> 0 (DIAG_SUCCESS)
        Total run count -------------> 1
        Last test testing type ------> Bootup
        Last test execution time ----> May 13 2011 21:59:37
        First test failure time -----> n/a
        Last test failure time ------> n/a
        Last test pass time ---------> May 13 2011 21:59:37
        Total failure count ---------> 0
        Consecutive failure count ---> 0
_____________________________________________________________________________

 10) TestMatchCapture ----------------> .

        Error code ------------------> 0 (DIAG_SUCCESS)
        Total run count -------------> 1
        Last test testing type ------> Bootup
        Last test execution time ----> May 13 2011 21:59:37
        First test failure time -----> n/a
        Last test failure time ------> n/a
        Last test pass time ---------> May 13 2011 21:59:37
        Total failure count ---------> 0
        Consecutive failure count ---> 0
_____________________________________________________________________________

 11) TestProtocolMatchChannel --------> .

        Error code ------------------> 0 (DIAG_SUCCESS)
        Total run count -------------> 1
        Last test testing type ------> Bootup
```

```
        Last test execution time ----> May 13 2011 21:59:39
        First test failure time -----> n/a
        Last test failure time ------> n/a
        Last test pass time ---------> May 13 2011 21:59:39
        Total failure count ---------> 0
        Consecutive failure count ---> 0
_____________________________________________________________________________

 12) TestMacNotification -------------> U

        Error code ------------------> 3 (DIAG_SKIPPED)
        Total run count -------------> 0
        Last test testing type ------> n/a
        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
_____________________________________________________________________________

 13) TestPortSecurity ----------------> .

        Error code ------------------> 0 (DIAG_SUCCESS)
        Total run count -------------> 1
        Last test testing type ------> Bootup
        Last test execution time ----> May 13 2011 21:59:41
        First test failure time -----> n/a
        Last test failure time ------> n/a
        Last test pass time ---------> May 13 2011 21:59:41
        Total failure count ---------> 0
        Consecutive failure count ---> 0
_____________________________________________________________________________

 14) TestIPv4FibShortcut -------------> .

        Error code ------------------> 0 (DIAG_SUCCESS)
        Total run count -------------> 1
        Last test testing type ------> Bootup
        Last test execution time ----> May 13 2011 21:59:42
        First test failure time -----> n/a
        Last test failure time ------> n/a
        Last test pass time ---------> May 13 2011 21:59:42
        Total failure count ---------> 0
        Consecutive failure count ---> 0
_____________________________________________________________________________

 15) TestL3Capture2 ------------------> .

        Error code ------------------> 0 (DIAG_SUCCESS)
        Total run count -------------> 1
        Last test testing type ------> Bootup
        Last test execution time ----> May 13 2011 21:59:42
        First test failure time -----> n/a
        Last test failure time ------> n/a
        Last test pass time ---------> May 13 2011 21:59:42
        Total failure count ---------> 0
        Consecutive failure count ---> 0
_____________________________________________________________________________

 16) TestIPv6FibShortcut -------------> .

        Error code ------------------> 0 (DIAG_SUCCESS)
        Total run count -------------> 1
```

```
        Last test testing type ------> Bootup
        Last test execution time ----> May 13 2011 21:59:42
        First test failure time -----> n/a
        Last test failure time ------> n/a
        Last test pass time ---------> May 13 2011 21:59:42
        Total failure count ---------> 0
        Consecutive failure count ---> 0
_____________________________________________________________________________

 17) TestMPLSFibShortcut -------------> .

        Error code ------------------> 0 (DIAG_SUCCESS)
        Total run count -------------> 1
        Last test testing type ------> Bootup
        Last test execution time ----> May 13 2011 21:59:42
        First test failure time -----> n/a
        Last test failure time ------> n/a
        Last test pass time ---------> May 13 2011 21:59:42
        Total failure count ---------> 0
        Consecutive failure count ---> 0
_____________________________________________________________________________

 18) TestNATFibShortcut --------------> .

        Error code ------------------> 0 (DIAG_SUCCESS)
        Total run count -------------> 1
        Last test testing type ------> Bootup
        Last test execution time ----> May 13 2011 21:59:42
        First test failure time -----> n/a
        Last test failure time ------> n/a
        Last test pass time ---------> May 13 2011 21:59:42
        Total failure count ---------> 0
        Consecutive failure count ---> 0
_____________________________________________________________________________

 19) TestAclPermit -------------------> .

        Error code ------------------> 0 (DIAG_SUCCESS)
        Total run count -------------> 1
        Last test testing type ------> Bootup
        Last test execution time ----> May 13 2011 21:59:42
        First test failure time -----> n/a
        Last test failure time ------> n/a
        Last test pass time ---------> May 13 2011 21:59:42
        Total failure count ---------> 0
        Consecutive failure count ---> 0
_____________________________________________________________________________

 20) TestAclDeny ---------------------> .

        Error code ------------------> 0 (DIAG_SUCCESS)
        Total run count -------------> 1
        Last test testing type ------> Bootup
        Last test execution time ----> May 13 2011 21:59:42
        First test failure time -----> n/a
        Last test failure time ------> n/a
        Last test pass time ---------> May 13 2011 21:59:42
        Total failure count ---------> 0
        Consecutive failure count ---> 0
_____________________________________________________________________________

 21) TestAclRedirect -----------------> .

        Error code ------------------> 0 (DIAG_SUCCESS)
```

```
        Total run count -------------> 1
        Last test testing type ------> Bootup
        Last test execution time ----> May 13 2011 21:59:42
        First test failure time -----> n/a
        Last test failure time ------> n/a
        Last test pass time ---------> May 13 2011 21:59:42
        Total failure count ---------> 0
        Consecutive failure count ---> 0
_____________________________________________________________________________

 22) TestRBAcl ----------------------> .

        Error code ------------------> 0 (DIAG_SUCCESS)
        Total run count -------------> 1
        Last test testing type ------> Bootup
        Last test execution time ----> May 13 2011 21:59:42
        First test failure time -----> n/a
        Last test failure time ------> n/a
        Last test pass time ---------> May 13 2011 21:59:42
        Total failure count ---------> 0
        Consecutive failure count ---> 0
_____________________________________________________________________________

 23) TestQos ------------------------> .

        Error code ------------------> 0 (DIAG_SUCCESS)
        Total run count -------------> 1
        Last test testing type ------> Bootup
        Last test execution time ----> May 13 2011 21:59:42
        First test failure time -----> n/a
        Last test failure time ------> n/a
        Last test pass time ---------> May 13 2011 21:59:42
        Total failure count ---------> 0
        Consecutive failure count ---> 0
_____________________________________________________________________________

 24) TestDQUP ----------------------> .

        Error code ------------------> 0 (DIAG_SUCCESS)
        Total run count -------------> 1
        Last test testing type ------> Bootup
        Last test execution time ----> May 13 2011 21:59:42
        First test failure time -----> n/a
        Last test failure time ------> n/a
        Last test pass time ---------> May 13 2011 21:59:42
        Total failure count ---------> 0
        Consecutive failure count ---> 0
_____________________________________________________________________________

 25) TestL3VlanMet ------------------> .

        Error code ------------------> 0 (DIAG_SUCCESS)
        Total run count -------------> 1
        Last test testing type ------> Bootup
        Last test execution time ----> May 13 2011 21:59:42
        First test failure time -----> n/a
        Last test failure time ------> n/a
        Last test pass time ---------> May 13 2011 21:59:42
        Total failure count ---------> 0
        Consecutive failure count ---> 0
_____________________________________________________________________________

 26) TestIngressSpan ----------------> .
```

```
        Error code ------------------> 0 (DIAG_SUCCESS)
        Total run count -------------> 1
        Last test testing type ------> Bootup
        Last test execution time ----> May 13 2011 21:59:42
        First test failure time -----> n/a
        Last test failure time ------> n/a
        Last test pass time ---------> May 13 2011 21:59:42
        Total failure count ---------> 0
        Consecutive failure count ---> 0
_____________________________________________________________________________

 27) TestEgressSpan ------------------> .

        Error code ------------------> 0 (DIAG_SUCCESS)
        Total run count -------------> 1
        Last test testing type ------> Bootup
        Last test execution time ----> May 13 2011 21:59:43
        First test failure time -----> n/a
        Last test failure time ------> n/a
        Last test pass time ---------> May 13 2011 21:59:43
        Total failure count ---------> 0
        Consecutive failure count ---> 0
_____________________________________________________________________________

 28) TestNetflowShortcut -------------> .

        Error code ------------------> 0 (DIAG_SUCCESS)
        Total run count -------------> 1
        Last test testing type ------> Bootup
        Last test execution time ----> May 13 2011 21:59:43
        First test failure time -----> n/a
        Last test failure time ------> n/a
        Last test pass time ---------> May 13 2011 21:59:43
        Total failure count ---------> 0
        Consecutive failure count ---> 0
_____________________________________________________________________________

 29) TestInbandEdit ------------------> .

        Error code ------------------> 0 (DIAG_SUCCESS)
        Total run count -------------> 1
        Last test testing type ------> Bootup
        Last test execution time ----> May 13 2011 21:59:43
        First test failure time -----> n/a
        Last test failure time ------> n/a
        Last test pass time ---------> May 13 2011 21:59:43
        Total failure count ---------> 0
        Consecutive failure count ---> 0
_____________________________________________________________________________

 30) TestFabricInternalSnake ---------> .

        Error code ------------------> 0 (DIAG_SUCCESS)
        Total run count -------------> 1
        Last test testing type ------> Bootup
        Last test execution time ----> May 13 2011 21:59:43
        First test failure time -----> n/a
        Last test failure time ------> n/a
        Last test pass time ---------> May 13 2011 21:59:43
        Total failure count ---------> 0
        Consecutive failure count ---> 0
_____________________________________________________________________________

 31) TestFabricExternalSnake ---------> .
```

```
        Error code ------------------> 0 (DIAG_SUCCESS)
        Total run count -------------> 1
        Last test testing type ------> Bootup
        Last test execution time ----> May 13 2011 21:59:43
        First test failure time -----> n/a
        Last test failure time ------> n/a
        Last test pass time ---------> May 13 2011 21:59:43
        Total failure count ---------> 0
        Consecutive failure count ---> 0
_____________________________________________________________________________

 32) TestFabricVlanLoopback ----------> .

        Error code ------------------> 0 (DIAG_SUCCESS)
        Total run count -------------> 1
        Last test testing type ------> Bootup
        Last test execution time ----> May 13 2011 21:59:43
        First test failure time -----> n/a
        Last test failure time ------> n/a
        Last test pass time ---------> May 13 2011 21:59:43
        Total failure count ---------> 0
        Consecutive failure count ---> 0
_____________________________________________________________________________

 33) TestTrafficStress ---------------> U

        Error code ------------------> 3 (DIAG_SKIPPED)
        Total run count -------------> 0
        Last test testing type ------> n/a
        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
_____________________________________________________________________________

 34) TestL3TcamMonitoring ------------> .

        Error code ------------------> 0 (DIAG_SUCCESS)
        Total run count -------------> 16382
        Last test testing type ------> Health Monitoring
        Last test execution time ----> May 16 2011 21:42:42
        First test failure time -----> n/a
        Last test failure time ------> n/a
        Last test pass time ---------> May 16 2011 21:42:42
        Total failure count ---------> 0
        Consecutive failure count ---> 0
_____________________________________________________________________________

 35) TestFibTcam ----------------------> U

        Error code ------------------> 3 (DIAG_SKIPPED)
        Total run count -------------> 0
        Last test testing type ------> n/a
        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
_____________________________________________________________________________
```

```
36) TestAclQosTcam ------------------> U

       Error code ------------------> 3 (DIAG_SKIPPED)
       Total run count -------------> 0
       Last test testing type ------> n/a
       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
_____________________________________________________________________________

37) TestEarlMemOnBootup -------------> .

       Error code ------------------> 0 (DIAG_SUCCESS)
       Total run count -------------> 1
       Last test testing type ------> Bootup
       Last test execution time ----> May 13 2011 21:59:44
       First test failure time -----> n/a
       Last test failure time ------> n/a
       Last test pass time ---------> May 13 2011 21:59:44
       Total failure count ---------> 0
       Consecutive failure count ---> 0
_____________________________________________________________________________

38) TestAsicMemory ------------------> U

       Error code ------------------> 3 (DIAG_SKIPPED)
       Total run count -------------> 0
       Last test testing type ------> n/a
       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
_____________________________________________________________________________

39) ScheduleSwitchover --------------> U

       Error code ------------------> 3 (DIAG_SKIPPED)
       Total run count -------------> 0
       Last test testing type ------> n/a
       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
_____________________________________________________________________________

40) TestFirmwareDiagStatus ----------> .

       Error code ------------------> 0 (DIAG_SUCCESS)
       Total run count -------------> 1
       Last test testing type ------> Bootup
       Last test execution time ----> May 13 2011 21:59:44
       First test failure time -----> n/a
       Last test failure time ------> n/a
       Last test pass time ---------> May 13 2011 21:59:44
       Total failure count ---------> 0
       Consecutive failure count ---> 0
_____________________________________________________________________________
```

```
41) TestAsicSync --------------------> .

       Error code ------------------> 0 (DIAG_SUCCESS)
       Total run count -------------> 16382
       Last test testing type ------> Health Monitoring
       Last test execution time ----> May 16 2011 21:42:42
       First test failure time -----> n/a
       Last test failure time ------> n/a
       Last test pass time ---------> May 16 2011 21:42:42
       Total failure count ---------> 0
       Consecutive failure count ---> 0
```

```
42) TestUnusedPortLoopback:

   Port  1  2  3  4  5
   -------------------
         U  U  U  .  .


       Error code ------------------> 0 (DIAG_SUCCESS)
       Total run count -------------> 4261
       Last test testing type ------> Health Monitoring
       Last test execution time ----> May 16 2011 21:41:53
       First test failure time -----> n/a
       Last test failure time ------> n/a
       Last test pass time ---------> May 16 2011 21:41:53
       Total failure count ---------> 0
       Consecutive failure count ---> 0
```

```
43) TestNonDisruptiveLoopback:

   Port  1  2  3  4  5
   -------------------
         U  U  U  U  U


       Error code ------------------> 3 (DIAG_SKIPPED)
       Total run count -------------> 0
       Last test testing type ------> n/a
       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
```

```
44) TestFabricFlowControlStatus -----> U

       Error code ------------------> 3 (DIAG_SKIPPED)
       Total run count -------------> 0
       Last test testing type ------> n/a
       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
       Current run count ---------------->: 0
       First test execution time ------->:
       Last test execution time -------->:
```

```
        Total FPOE Rate0 Count ---------->: 0
        Total FPOE Reduced Rate Count --->: 0
_____________________________________________________________________________

45) TestPortTxMonitoring:

   Port  1  2  3  4  5
   -------------------
         U  U  U  U  U


        Error code ------------------> 0 (DIAG_SUCCESS)
        Total run count -------------> 3419
        Last test testing type ------> Health Monitoring
        Last test execution time ----> May 16 2011 21:42:25
        First test failure time -----> n/a
        Last test failure time ------> n/a
        Last test pass time ---------> May 16 2011 21:42:25
        Total failure count ---------> 0
        Consecutive failure count ---> 0
_____________________________________________________________________________

46) TestOBFL ------------------------> .

        Error code ------------------> 0 (DIAG_SUCCESS)
        Total run count -------------> 1
        Last test testing type ------> Bootup
        Last test execution time ----> May 13 2011 21:59:44
        First test failure time -----> n/a
        Last test failure time ------> n/a
        Last test pass time ---------> May 13 2011 21:59:44
        Total failure count ---------> 0
        Consecutive failure count ---> 0
_____________________________________________________________________________

47) TestCFRW:

   Device  1
   ---------
           .


        Error code ------------------> 0 (DIAG_SUCCESS)
        Total run count -------------> 1
        Last test testing type ------> Bootup
        Last test execution time ----> May 13 2011 21:59:44
        First test failure time -----> n/a
        Last test failure time ------> n/a
        Last test pass time ---------> May 13 2011 21:59:44
        Total failure count ---------> 0
        Consecutive failure count ---> 0
_____________________________________________________________________________

48) TestLtlFpoeMemoryConsistency ----> .

        Error code ------------------> 0 (DIAG_SUCCESS)
        Total run count -------------> 8191
        Last test testing type ------> Health Monitoring
        Last test execution time ----> May 16 2011 21:42:42
        First test failure time -----> n/a
        Last test failure time ------> n/a
        Last test pass time ---------> May 16 2011 21:42:42
        Total failure count ---------> 0
        Consecutive failure count ---> 0
```

```
    LTL PARITY
        Ltl index ------------------> 0
        Rbh value ------------------> 0

    FPOE DB
        Table size -----------------> 0
        Last entries checked --------> 0
        Total fail count ------------> 0
        Total correction count ------> 0
        Last detection time ---------> May 13 2011 21:58:47
        Last result -----------------> UNKNOWN
        Last fail count -------------> 0
        Last correction count -------> 0

_____________________________________________________________________________

 49) TestErrorCounterMonitor ---------> .

        Error code ------------------> 0 (DIAG_SUCCESS)
        Total run count -------------> 8191
        Last test testing type ------> Health Monitoring
        Last test execution time ----> May 16 2011 21:42:42
        First test failure time -----> n/a
        Last test failure time ------> n/a
        Last test pass time ---------> May 16 2011 21:42:42
        Total failure count ---------> 0
        Consecutive failure count ---> 0
        Error Records ---------------> n/a
_____________________________________________________________________________

 50) TestEARLInternalTables ----------> .

        Error code ------------------> 0 (DIAG_SUCCESS)
        Total run count -------------> 854
        Last test testing type ------> Health Monitoring
        Last test execution time ----> May 16 2011 21:38:38
        First test failure time -----> n/a
        Last test failure time ------> n/a
        Last test pass time ---------> May 16 2011 21:38:38
        Total failure count ---------> 0
        Consecutive failure count ---> 0

    AGE GROUP
        Total CC run count ----------> 860
        Table size ------------------> 16384
        Total fail count ------------> 0
        Total correction count ------> 0
        Last completion time --------> May 16 2011 21:39:30
        Last result -----------------> PASS
        Last fail count -------------> 0
        Last correction count -------> 0
        Last entries checked --------> 16384
        Consistency checker ---------> ON

    BUNDLE PORT MAP
        Total CC run count ----------> 860
        Table size ------------------> 512
        Total fail count ------------> 0
        Total correction count ------> 0
        Last completion time --------> May 16 2011 21:39:12
        Last result -----------------> PASS
        Last fail count -------------> 0
        Last correction count -------> 0
```

```
        Last entries checked --------> 512
        Consistency checker ---------> ON

    BUNDLE EXTENSION MAP
        Total CC run count ----------> 860
        Table size ------------------> 256
        Total fail count ------------> 0
        Total correction count ------> 0
        Last completion time --------> May 16 2011 21:39:12
        Last result -----------------> PASS
        Last fail count -------------> 0
        Last correction count -------> 0
        Last entries checked --------> 256
        Consistency checker ---------> ON

    VLAN ACCESS MODE MEMORY
        Total CC run count ----------> 860
        Table size ------------------> 512
        Total fail count ------------> 0
        Total correction count ------> 0
        Last completion time --------> May 16 2011 21:39:12
        Last result -----------------> PASS
        Last fail count -------------> 0
        Last correction count -------> 0
        Last entries checked --------> 512
        Consistency checker ---------> ON
_____________________________________________________________________________

Router#
```

次に、実行されたヘルス チェックの出力を表示する例を示します。

```
Router# show diagnostic health
Non-zero port counters for 6/4 -
13.                         linkChange = 8530

Non-zero port counters for 6/5 -
13.                         linkChange = 8530

Router#
```

メモリ テストの実行方法

大半のオンライン診断テストでは、特別なセットアップまたは設定は不要です。ただし、TestFibTcamSSRAM および TestLinecardMemory テストに付属のメモリ テストの場合、テストを実行する前に必須の作業や推奨される作業をいくつか行う必要があります。

オンライン診断メモリ テストを実行する前に、次の作業を行います。

- 必須作業
  - すべての接続ポートをディセーブルにして、ネットワーク トラフィックを分離します。
  - メモリ テスト中はテスト パケットを送信しないでください。
  - システムをユーザ動作モードに戻す前に、システムをリセットしてください。
- すべてのバックグラウンド ヘルス モニタリング テストをディセーブルにするには、**no diagnostic monitor module** *number* **test all** コマンドを使用します。

診断の健全性チェックの実行方法

ネットワーク内の潜在的な問題領域を検出するため、診断の健全性チェックを実行できます。健全性チェックでは、想定される特定のシステム状態の組み合わせを使用した設定に対し、既定の一連のチェックを実行して、警告状況の一覧をコンパイルします。このチェックの目的は、不適切な状態の要素がないかどうかを調べ、システムの健全性を維持するための支援を行うことです。

診断の健全性チェックを実行するには、次の作業を行います。

コマンド	目的
show diagnostic sanity	設定および特定のシステム状態で一連のテストを実行します。

次に、**show diagnostic sanity** コマンドの結果として表示される可能性があるメッセージの例を示します。

```
Router# show diagnostic sanity
Pinging default gateway 10.6.141.1 ....
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.6.141.1, timeout is 2 seconds:
..!!.
Success rate is 0 percent (0/5)

IGMP snooping disabled please enable it for optimum config.

IGMP snooping disabled but RGMP enabled on the following interfaces,
please enable IGMP for proper config :
Vlan1, Vlan2, GigabitEthernet1/1

Multicast routing is enabled globally but not enabled on the following
interfaces:
GigabitEthernet1/1, GigabitEthernet1/2

A programming algorithm mismatch was found on the device bootflash:
Formatting the device is recommended.

The bootflash: does not have enough free space to accomodate the crashinfo file.

Please check your confreg value : 0x0.

Please check your confreg value on standby: 0x0.

The boot string is empty. Please enter a valid boot string .
Could not verify boot image "disk0:" specified in the boot string on the
slave.

Invalid boot image "bootflash:asdasd" specified in the boot string on the
slave.

Please check your boot string on the slave.

UDLD has been disabled globally - port-level UDLD sanity checks are
being bypassed.
OR
[
The following ports have UDLD disabled. Please enable UDLD for optimum
config:
Gi1/22

The following ports have an unknown UDLD link state. Please enable UDLD
```

```
on both sides of the link:
Gi1/22
]

The following ports have portfast enabled:
Gi1/20, Gi1/22

The following ports have trunk mode set to on:
Gi1/1, Gi1/13

The following trunks have mode set to auto:
Gi1/2, Gi1/3

The following ports with mode set to desirable are not trunking:
Gi1/3, Gi1/4

The following trunk ports have negotiated to half-duplex:
Gi1/3, Gi1/4

The following ports are configured for channel mode on:
Gi1/1, Gi1/2, Gi1/3, Gi1/4

The following ports, not channeling are configured for channel mode
desirable:
Gi1/14

The following vlan(s) have a spanning tree root of 32768:
1

The following vlan(s) have max age on the spanning tree root different from
the default:
1-2

The following vlan(s) have forward delay on the spanning tree root different
from the default:
1-2

The following vlan(s) have hello time on the spanning tree root different
from the default:
1-2

The following vlan(s) have max age on the bridge different from the
default:
1-2

The following vlan(s) have fwd delay on the bridge different from the
default:
1-2

The following vlan(s) have hello time on the bridge different from the
default:
1-2

The following vlan(s) have a different port priority than the default
on the port gigabitEthernet1/1
1-2

The following ports have recieve flow control disabled:
Gi1/20, Gi1/22

The following inline power ports have power-deny/faulty status:
Gi1/1, Gi1/2

The following ports have negotiated to half-duplex:
Gi1/22

The following vlans have a duplex mismatch:
```

```
Gig 1/22

The following interafaces have a native vlan mismatch:
interface (native vlan - neighbor vlan)
Gig 1/22 (1 - 64)

The value for Community-Access on read-only operations for SNMP is the same
as default. Please verify that this is the best value from a security point
of view.

The value for Community-Access on write-only operations for SNMP is the same
as default. Please verify that this is the best value from a security point
of view.

The value for Community-Access on read-write operations for SNMP is the same
as default. Please verify that this is the best value from a security point
of view.
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CHAPTER 16

オンボード障害ロギング（OBFL）

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

OBFL の前提条件

なし。

OBFL の制約事項

- ソフトウェアの制約事項：デバイス（ルータやスイッチ）が OBFL ストレージ メディアとしてリニア フラッシュ メモリを使用する場合、Cisco IOS ソフトウェアは、OBFL 機能用に最小 2 つの物理セクター（または物理ブロック）を予約する必要があります。リニア フラッシュ デバイスの消去操作はセクターごと（またはブロックごと）に実行されるため、1 つの余分な物理セクターが必要です。それ以外の場合は、デバイス上で OBFL 機能用に予約するスペースの最小量は、少なくとも 8 KB である必要があります。
- ファームウェアの制約事項：ラインカードまたはポート アダプタが Cisco IOS オペレーティング システムと異なるオペレーティング システムまたはファームウェアを実行する場合、ラインカードまたはポート アダプタは、OBFL ファイル システムがラインカードまたはポート アダプタと通信できるデバイス ドライバ レベルのサポートまたはプロセッサ間通信（IPC）を提供する必要があります。この要件は、OBFL データをラインカードまたはポート アダプタに接続されたストレージ デバイスに記録できるようにするために適用されます。
- ハードウェアの制約事項：OBFL 機能をサポートするために、デバイスは OBFL データ ロギング用に予約された不揮発性メモリ スペースの少なくとも 8 KB が必要です。

OBFL について

OBFL の概要

オンボード障害ロギング（OBFL）機能は、Cisco ルータまたはスイッチにインストールされているシステム ハードウェアから動作温度、ハードウェアの稼働時間、割り込み、その他の重要なイベントやメッセージなどのデータを収集します。データは不揮発性メモリに保存され、技術担当者によるハードウェアの問題を診断に役立ちます。

OBFL によって収集されたデータについて

OBFL データの概要

OBFL 機能は、Cisco ルータまたはスイッチにインストールされているハードウェア カード（または*モジュール*）の問題の診断に役立つ動作温度、ハードウェア稼働時間、割り込み、その他の重要なイベントとメッセージを記録します。データのログは、不揮発性メモリに格納されるファイルに作成されます。オンボード ハードウェアが起動すると、モニタされている各領域で最初のレコードが作成され、後続のレコードの基準値となります。OBFL 機能は、継続的なレコードの収集と古い（履歴）レコードのアーカイブで循環更新スキームを提供し、システムに関する正確なデータを保証します。データは、

測定と継続ファイルのサンプルのスナップショットを表示する継続情報の形式、または収集したデータに関する詳細を提供する要約情報の形式で記録されます。データは、**show logging onboard** コマンドを使用して表示されます。履歴データが利用できない場合は、「No historical data to display」というメッセージが表示されます。

温度

ハードウェア モジュールの周囲の温度が推奨される安全な動作範囲を超え、パケット ドロップなどのシステムの問題を引き起こすことがあります。推奨される動作温度よりも高くなると、コンポーネントのパフォーマンス低下が加速し、装置の信頼性に影響する可能性があります。温度のモニタリングは、環境制御とシステムの信頼性を維持するために重要です。温度のサンプルが記録されると、そのサンプルが次のレコードの基準値となります。この時点から、前のレコードから変更がある場合、または最大格納時間を超えた場合に、温度が記録されます。温度は摂氏で測定され、記録されます。

温度の例：

```
--------------------------------------------------------------------------------
TEMPERATURE SUMMARY INFORMATION
--------------------------------------------------------------------------------
Number of sensors          : 12
Sampling frequency         : 5 minutes
Maximum time of storage    : 120 minutes
--------------------------------------------------------------------------------
Sensor                            |   ID   | Maximum Temperature 0C
--------------------------------------------------------------------------------
MB-Out                              980201     43
MB-In                               980202     28
MB                                  980203     29
MB                                  980204     38
EARL-Out                            910201     0
EARL-In                             910202     0
SSA 1                               980301     38
SSA 2                               980302     36
JANUS 1                             980303     36
JANUS 2                             980304     35
GEMINI 1                            980305     0
GEMINI 2                            980306     0
------------------------------------------------------------------
Temp                          Sensor ID
0C     1    2    3    4    5    6    7    8    9   10   11   12
------------------------------------------------------------------
No historical data to display
------------------------------------------------------------------
--------------------------------------------------------------------------------
TEMPERATURE CONTINUOUS INFORMATION
--------------------------------------------------------------------------------
Sensor                            |   ID   |
--------------------------------------------------------------------------------
MB-Out                              980201
MB-In                               980202
MB                                  980203
MB                                  980204
EARL-Out                            910201
EARL-In                             910202
SSA 1                               980301
SSA 2                               980302
JANUS 1                             980303
JANUS 2                             980304
GEMINI 1                            980305
GEMINI 2                            980306
```

```
-------------------------------------------------------------------------------
       Time Stamp   |Sensor Temperature 0C
MM/DD/YYYY HH:MM:SS |  1    2    3    4    5    6    7    8    9   10   11   12
-------------------------------------------------------------------------------
03/06/2007 22:32:51   31   26   27   27   NA   NA   33   32   30   29   NA   NA
03/06/2007 22:37:51   43   28   29   38   NA   NA   38   36   36   35   NA   NA
-------------------------------------------------------------------------------
```

このデータを解釈するには：

- [Number of sensors] は、記録される温度センサーの合計数です。各センサーのカラムで、該当する場合は各センサーの数の下に温度が表示されます。
- [Sampling frequency] は測定間隔です。
- [Maximum time of storage] は温度が変更されず、データがストレージ メディアに保存されていない状態で経過できる最大時間を分単位で決定します。この時間が経過すると、温度が変更されない場合でも、温度レコードが保存されます。
- [Sensor] カラムには、センサーの名前が表示されます。
- [ID] カラムには、センサーに割り当てられた ID がリストされています。
- [Maximum Temperature 0C] は、センサー 1 台あたりで記録された最高温度を示します。
- [Temp] は履歴レコードに記録された摂氏の温度を示します。以降のカラムは、各センサーでその温度を記録した合計時間を示します。
- [Sensor ID] は、割り当てられた番号であり、同じセンサーの温度をまとめて保存できます。

稼働時間

稼働時間のトラッキングはモジュールの電源投入時に開始され、情報はモジュールの寿命の間保持されます。

稼働時間の例

```
-------------------------------------------------------------------------------
UPTIME SUMMARY INFORMATION
-------------------------------------------------------------------------------
First customer power on : 03/06/2007 22:32:51
Total uptime            :   0 years   0 weeks   2 days  18 hours  10 minutes
Total downtime          :   0 years   0 weeks   0 days   8 hours   7 minutes
Number of resets        : 130
Number of slot changes  : 16
Current reset reason    : 0xA1
Current reset timestamp : 03/07/2007 13:29:07
Current slot            : 2
Current uptime          :   0 years   0 weeks   1 days   7 hours   0 minutes
-------------------------------------------------------------------------------
Reset  |        |
Reason | Count  |
-------------------------------------------------------------------------------
0x5         64
0x6         62
0xA1         4
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
UPTIME CONTINUOUS INFORMATION
-------------------------------------------------------------------------------
Time Stamp          | Reset  | Uptime
MM/DD/YYYY HH:MM:SS | Reason | years weeks days hours  minutes
-------------------------------------------------------------------------------
03/06/2007 22:32:51   0xA1      0     0     0     0     0
```

稼働時間アプリケーションは次のイベントを追跡します。

- カスタマーが最初にコンポーネントに電源を投入した日時。
- 年、週、日、時、分単位でのコンポーネントの合計稼働時間とダウンタイム。
- コンポーネントのリセットの総数。
- スロット（モジュール）変更の総数。
- 日時を含む現在のリセット タイムスタンプ。
- コンポーネントの現在のスロット（モジュール）番号。
- 年、週、日、時、分単位での現在の稼働時間。
- リセット理由。表示されている番号を解釈するには、表 16-1 を参照してください。
- [Count] は各リセット理由で発生したリセット回数です。

表 16-1　リセット理由コードと説明

リセット理由コード（16 進法）	コンポーネント / 説明
0x01	シャーシ
0x02	ラインカードのホット プラグ イン
0x03	スーパーバイザによるラインカードのオフ / オン要求
0x04	スーパーバイザによるラインカードのハード リセット要求
0x05	ラインカードによるスーパーバイザのオン / オフ要求
0x06	ラインカードによるスーパーバイザのハード リセット要求
0x07	内部システム レジスタを使用したラインカードの自己リセット
0x08	—
0x09	—
0x0A	ラインカードの一時的な停電
0x0B	—
0x0C	—
0x0D	—
0x0E	—
0x0F	—
0x10	—
0x11	スーパーバイザのマスク不能割り込み（NMI）後のオフ / オン
0x12	スーパーバイザの NMI 後のハード リセット
0x13	スーパーバイザの NMI 後のソフト リセット
0x14	—
0x15	ラインカードによるスーパーバイザ NMI 要求後のオフ / オン
0x16	ラインカードによるスーパーバイザ NMI 要求後のハード リセット
0x17	ラインカードによるスーパーバイザ NMI 要求後のソフト リセット
0x18	—

表 16-1　リセット理由コードと説明 （続き）

リセット理由コード（16 進法）	コンポーネント / 説明
0x19	ラインカードの自己 NMI 後のオフ / オン
0x1A	ラインカードの自己 NMI 後のハード リセット
0x1B	ラインカードの自己 NMI 後のソフト リセット
0x21	スプリアス NMI 後のオフ / オン
0x22	スプリアス NMI 後のハード リセット
0x23	スプリアス NMI 後のソフト リセット
0x24	—
0x25	ウォッチドッグ NMI 後のオフ / オン
0x26	ウォッチドッグ NMI 後のハード リセット
0x27	ウォッチドッグ NMI 後のソフト リセット
0x28	—
0x29	パリティ NMI 後のオフ / オン
0x2A	パリティ NMI 後のハード リセット
0x2B	パリティ NMI 後のソフト リセット
0x31	システムの重大な割り込み後のオフ / オン
0x32	システムの重大な割り込み後のハード リセット
0x33	システムの重大な割り込み後のソフト リセット
0x34	—
0x35	特定用途向け集積回路（ASIC）割り込み後のオフ / オン
0x36	ASIC 割り込み後のハード リセット
0x37	ASIC 割り込み後のソフト リセット
0x38	—
0x39	不明な割り込み後のオフ / オン
0x3A	不明な割り込み後のハード リセット
0x3B	不明な割り込み後のソフト リセット
0x41	CPU 例外後のオフ / オン
0x42	CPU 例外後のハード リセット
0x43	CPU 例外後のソフト リセット
0xA1	汎用データに変換されたリセット データ

割り込み

割り込みは、ASIC や NMI などの CPU からの注意が必要なシステム コンポーネントによって生成されます。割り込みは、修正する必要があるハードウェア制限条件またはエラーと一般に関連します。

コンポーネントが割り込まれるたびに連続形式が記録され、このレコードは後続のレコードの基本情報として保存および使用されます。リストが保存されるたびに、タイムスタンプが追加されます。前の割り込みからの時差がカウントされるため、エラーが発生すると技術担当者がコンポーネントの動作履歴の完全なレコードを取得できます。

割り込みの例

```
--------------------------------------------------------------------------------
INTERRUPT SUMMARY INFORMATION
--------------------------------------------------------------------------------
Name                                              |  ID | Offset | Bit |  Count
--------------------------------------------------------------------------------
No historical data to display
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
CONTINUOUS INTERRUPT INFORMATION
--------------------------------------------------------------------------------
MM/DD/YYYY HH:MM:SS mmm | Name                                |  ID | Offset | Bit
--------------------------------------------------------------------------------
03/06/2007 22:33:06 450   Port-ASIC #2                          9   0x00E7     6
--------------------------------------------------------------------------------
```

このデータを解釈するには：

- [Name] はデバイスの位置などのコンポーネント説明です。
- [ID] は、データ ストレージに割り当てられたフィールドです。
- [Offset] はコンポーネント レジスタのベース アドレスからのレジスタ オフセットです。
- [Bit] はコンポーネントの内部レジスタから記録された割り込みビット数です。
- タイムスタンプは割り込みが発生した日時がミリ秒まで表示されます。

メッセージ ロギング

OBFL 機能は標準のシステム メッセージを記録します。端末にメッセージを表示する代わりに、メッセージはファイルに書き込まれ、保存されます。そのため、メッセージはあとでアクセスしたり、読み取ることができます。システム メッセージは、レベル 1 のアラートからレベル 7 のデバッグ メッセージまでの範囲で、これらのレベルは、**hw module logging onboard** コマンドで指定できます。

エラー メッセージ ログの例

```
--------------------------------------------------------------------------------
ERROR MESSAGE SUMMARY INFORMATION
--------------------------------------------------------------------------------
Facility-Sev-Name       | Count | Persistence Flag
MM/DD/YYYY HH:MM:SS
--------------------------------------------------------------------------------
No historical data to display
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
ERROR MESSAGE CONTINUOUS INFORMATION
--------------------------------------------------------------------------------
MM/DD/YYYY HH:MM:SS Facility-Sev-Name
--------------------------------------------------------------------------------
03/06/2007 22:33:35  %GOLD_OBFL-3-GOLD : Diagnostic OBFL: Diagnostic OBFL testing
```

このデータを解釈するには：

- タイムスタンプは、メッセージが記録された日付と時刻を示します。
- [Facility-Sev-Name] は、システム メッセージのコーディングされた命名方式です。
  - [Facility] コードは、2 つ以上の大文字からなるコードで、メッセージによって参照されたハードウェア デバイス（ファシリティ）を示します。
  - [Sev] は、メッセージの重大度を表す 1 ～ 7 の 1 桁のコードです。
  - [Name] は 2 つのコード名をハイフンで区切ったもので、メッセージの送信元のシステム部分を説明します。
- エラー メッセージが [Facility-Sev-Name] コードに続きます。システム メッセージの詳細については、『*Cisco IOS System and Error Messages*』ガイドを参照してください。
- カウントは履歴ファイルに許可されるこのメッセージのインスタンスの数を示します。その数のインスタンスが記録されると、新しいインスタンスを保存するために最も古いインスタンスが履歴ファイルから削除されます。
- [Persistence Flag] はメッセージにフラグが設定されていないメッセージより高い優先順位を付けます。

OBFL のデフォルト設定

OBFL 機能はデフォルトでイネーブルです。この機能が技術担当者に有用な情報を提供するため、ディセーブルにしないでください。

OBFL のイネーブル化

OBFL をイネーブルにする手順は、次のとおりです。

	コマンドまたはアクション	目的
ステップ 1	`Router> 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	`Router# 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	`Router(config)# hw-module switch` *switch-number* `module` *module-number* `logging onboard [message level {1-7}]`	指定されたハードウェア モジュールの OBFL をイネーブルにします。 （注）　デフォルトでは、デバイスに送信されるすべてのシステム メッセージは、OBFL 機能によって記録されます。**message level** キーワードを使用して記録される特定のメッセージ レベル（例ではレベル 1 メッセージのみ）を定義できます。
ステップ 4	`Router(config)# end`	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。

OBFL の設定例

重要な OBFL 機能は、**show logging onboard module** 特権 EXEC コマンド表示される情報です。ここでは、OBFL レコードをイネーブルにして表示する例を示します。

- OBFL メッセージ ロギングのイネーブル化：例
- OBFL メッセージ ログ：例
- OBFL コンポーネント稼働時間レポート：例
- 特定の時間の OBFL レポート：例

OBFL メッセージ ロギングのイネーブル化：例

次に、レベル 3 の OBFL メッセージ ロギングを設定する例を示します。

```
Router(config)# hw-module switch 2 module 1 logging onboard message level 3
```

OBFL メッセージ ログ：例

次に、モジュール 2 について記録されているシステム メッセージを表示する例を示します。

```
Router# show logging onboard module 2 message continuous

--------------------------------------------------------------------------------
ERROR MESSAGE CONTINUOUS INFORMATION
--------------------------------------------------------------------------------
MM/DD/YYYY HH:MM:SS Facility-Sev-Name
--------------------------------------------------------------------------------
03/06/2007 22:33:35 %SWITCH_IF-3-CAMERR : [chars], for VCI [dec] VPI [dec] in stdby data
path check, status: [dec]
--------------------------------------------------------------------------------
```

OBFL コンポーネント稼働時間レポート：例

次に、モジュール 2 のコンポーネント稼働時間のサマリー レポートを表示する例を示します。

```
Router# show logging onboard module 2 uptime

--------------------------------------------------------------------------------
UPTIME SUMMARY INFORMATION
--------------------------------------------------------------------------------
First customer power on : 03/06/2007 22:32:51
Total uptime            :   0 years   0 weeks   0 days   0 hours  35 minutes
Total downtime          :   0 years   0 weeks   0 days   0 hours   0 minutes
Number of resets        : 1
Number of slot changes  : 0
Current reset reason    : 0xA1
Current reset timestamp : 03/06/2007 22:31:34
Current slot            : 2
Current uptime          :   0 years   0 weeks   0 days   0 hours  35 minutes
--------------------------------------------------------------------------------
Reset  |        |
Reason | Count  |
--------------------------------------------------------------------------------
No historical data to display
--------------------------------------------------------------------------------
```

特定の時間の OBFL レポート：例

次に、特定の期間におけるすべてのコンポーネントの連続したレポートを表示する例を示します。

```
Router# show logging onboard module 3 continuous start 15:01:57 1 Mar 2007 end 15:04:57 3
Mar 2007

PID: WS-X6748-GE-TX    , VID:    , SN: SAL09063B85

--------------------------------------------------------------------------------
UPTIME CONTINUOUS INFORMATION
--------------------------------------------------------------------------------
Time Stamp          | Reset  | Uptime
MM/DD/YYYY HH:MM:SS | Reason | years weeks days hours  minutes
--------------------------------------------------------------------------------
03/01/2007 15:01:57   0xA1      0     0     0    10     0
03/03/2007 02:29:29   0xA1      0     0     0     5     0
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
TEMPERATURE CONTINUOUS INFORMATION
--------------------------------------------------------------------------------
Sensor                              |   ID  |
--------------------------------------------------------------------------------
MB-Out                                930201
MB-In                                 930202
MB                                    930203
MB                                    930204
EARL-Out                              910201
EARL-In                               910202
SSA 1                                 930301
SSA 2                                 930302
JANUS 1                               930303
JANUS 2                               930304
GEMINI 1                              930305
GEMINI 2                              930306
--------------------------------------------------------------------------------
       Time Stamp   |Sensor Temperature 0C
MM/DD/YYYY HH:MM:SS |  1    2    3    4    5    6    7    8    9   10   11   12
--------------------------------------------------------------------------------
03/01/2007 15:01:57   26   26   NA   NA   NA   NA    0    0    0    0    0    0
03/01/2007 15:06:57   39   27   NA   NA   NA   NA   39   37   36   29   32   32
03/01/2007 15:11:02   40   27   NA   NA   NA   NA   40   38   37   30   32   32
03/01/2007 17:06:06   40   27   NA   NA   NA   NA   40   38   37   30   32   32
03/01/2007 19:01:09   40   27   NA   NA   NA   NA   40   38   37   30   32   32
03/03/2007 02:29:30   25   26   NA   NA   NA   NA    0    0    0    0    0    0
03/03/2007 02:34:30   38   26   NA   NA   NA   NA   39   37   36   29   31   31
03/03/2007 04:29:33   40   27   NA   NA   NA   NA   40   38   36   30   32   32
03/03/2007 06:24:37   40   27   NA   NA   NA   NA   40   38   36   29   32   32
03/03/2007 08:19:40   40   27   NA   NA   NA   NA   40   38   36   29   32   32
03/03/2007 10:14:44   40   27   NA   NA   NA   NA   40   38   36   30   32   32
03/03/2007 12:09:47   40   27   NA   NA   NA   NA   40   38   36   30   32   32
03/03/2007 14:04:51   40   27   NA   NA   NA   NA   40   38   36   30   32   32
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
CONTINUOUS INTERRUPT INFORMATION
--------------------------------------------------------------------------------
MM/DD/YYYY HH:MM:SS mmm | Name                                |  ID | Offset | Bit
--------------------------------------------------------------------------------
03/01/2007 15:01:59 350   Port-ASIC #0                         7   0x00E7     6
03/03/2007 02:29:34 650   Port-ASIC #0                         7   0x00E7     6
--------------------------------------------------------------------------------
```

```
------------------------------------------------------------------------------
ERROR MESSAGE CONTINUOUS INFORMATION
------------------------------------------------------------------------------
MM/DD/YYYY HH:MM:SS Facility-Sev-Name
------------------------------------------------------------------------------
03/01/2007 15:02:15  %GOLD_OBFL-3-GOLD : Diagnostic OBFL: Diagnostic OBFL testing
03/03/2007 02:29:51  %GOLD_OBFL-3-GOLD : Diagnostic OBFL: Diagnostic OBFL testing
------------------------------------------------------------------------------
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CHAPTER 17

スイッチ ファブリック機能

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

スイッチ ファブリック機能の前提条件

なし。

スイッチ ファブリック機能の制約事項

なし。

スイッチ ファブリック機能に関する情報

スイッチ ファブリック機能の概要

スイッチ ファブリック機能はスーパーバイザ エンジンに組み込まれ、ファブリック対応モジュール間に専用接続を確立し、これらのモジュール間で連続的なフレーム転送を行います。スイッチ ファブリック機能によって提供されるファブリック対応モジュール間の直接接続のほかに、ファブリック対応モジュールは、転送バスへの直接接続も行います。

レイヤ 3 スイッチド トラフィックの転送の決定

PFC または Distributed Feature Card は、次のようにレイヤ 3 スイッチド トラフィックの転送について決定します。

- PFC は、DFC が搭載されていないモジュールから入ってきた各パケットの転送判断をすべて行います。
- DFC は、次の状況で DFC が搭載されたモジュールに入ってきた各パケットの転送判断をすべて行います。
  - 出力ポートが入力ポートと同じモジュールにある場合、DFC はパケットをローカルに転送します（パケットはモジュールの外部に送信されません）。
  - 出力ポートが別のファブリック対応モジュール上にある場合、DFC はパケットを出力モジュールに送信し、出力ポートから送信します。
  - 出力ポートが別のファブリック非対応モジュール上にある場合、DFC はスーパーバイザ エンジンにパケットを送信します。スーパーバイザ エンジンのファブリック インターフェイスはスイッチング バスにパケットを送信します。スイッチング バスでは、パケットは出力モジュールで受信され、出力ポートから送信されます。

スイッチ ファブリック機能のデフォルト設定

モジュール間のトラフィック転送は、次のいずれかのモードで行われます。

- compact モード：スイッチにファブリック対応モジュールだけが搭載されている場合は、すべてのトラフィックに対してこのモードが使用されます。このモードでは、スイッチ ファブリック チャネルを通じて DBus ヘッダーのコンパクト版が転送され、最良のパフォーマンスが得られます。
- truncated モード：スイッチにファブリック対応モジュールとファブリック非対応モジュールが両方とも搭載されている場合は、ファブリック対応モジュール間のトラフィックに対して、このモードが使用されます。このモードでは、スイッチはスイッチ ファブリック チャネルを通じて、切り捨てた形のトラフィック（フレームの最初の 64 バイト）を送信します。
- bus モード（flow-through モード）：スイッチは、ファブリック非対応モジュール間のトラフィック、およびファブリック非対応モジュールとファブリック対応モジュール間のトラフィックにこのモードを使用します。このモードでは、すべてのトラフィックがローカル バスとスーパーバイザ エンジン バス間で送受信されます。

表 17-1 に、搭載されているファブリック対応モジュールおよび非対応モジュール別に、使用されるスイッチング モードを示します。

表 17-1　スイッチ ファブリック機能のスイッチング モード

モジュール	スイッチング モード
ファブリック対応モジュール間（ファブリック非対応モジュールが搭載されていない場合）	compact （注）　**show** コマンドを実行すると、DFC を装着したファブリック対応モジュールの場合は dcef モードとして表示され、それ以外のファブリック対応モジュールの場合は fabric モードとして表示されます。
ファブリック対応モジュール間（ファブリック非対応モジュールも搭載されている場合）	truncated （注）　**show** コマンドを実行すると、fabric モードとして表示されます。
ファブリック対応モジュールとファブリック非対応モジュール間	bus
ファブリック非対応モジュール間	bus

スイッチ ファブリック機能の設定方法

スイッチング 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
`Router(config)# [no] fabric switching-mode allow {bus-mode | {truncated [{threshold [number]}]}}`	スイッチング モードを設定します。

スイッチング モードを設定するときには、次の情報に注意してください。

- ファブリック非対応モジュールの使用、またはファブリック対応モジュールで bus モードの使用を可能にするには、**fabric switching-mode allow bus-mode** コマンドを入力します。
- ファブリック非対応モジュールの使用、またはファブリック対応モジュールで bus モードの使用を禁止するには、**no fabric switching-mode allow bus-mode** コマンドを入力します。

注意　**no fabric switching-mode allow bus-mode** コマンドを入力すると、スイッチに搭載されたファブリック非対応モジュールへの電力供給が停止します。

- ファブリック対応モジュールで truncated モードの使用を可能にするには、**fabric switching-mode allow truncated** コマンドを入力します。
- ファブリック対応モジュールで truncated モードの使用を禁止するには、**no fabric switching-mode allow truncated** コマンドを入力します。
- bus モードの代わりに truncated モードを使用する場合に、事前にインストールしなければならないファブリック対応モジュールの数を設定するには、**fabric switching-mode allow truncated threshold** *number* コマンドを入力します。
- デフォルトの truncated モードのしきい値に戻すには、**no fabric switching-mode allow truncated threshold** コマンドを入力します。

スイッチ ファブリック機能のモニタ

スイッチ ファブリック冗長ステータスの表示

スイッチ ファブリックの冗長ステータスを表示するには、次の作業を行います。

コマンド	目的
Router# **show fabric active**	スイッチ ファブリックの冗長ステータスを表示します。

```
Router# show fabric active
Active fabric card in slot 5
No backup fabric card in the system
Router#
```

ファブリック チャネルのスイッチング モードの表示

特定のモジュールまたは全モジュールについて、ファブリック チャネルのスイッチング モードを表示するには、次の作業を行います。

コマンド	目的
Router# **show fabric switching-mode** [**module** {*slot_number* | **all**]]	特定のモジュールまたは全モジュールについて、ファブリック チャネルのスイッチング モードを表示します。

次に、全モジュールについて、ファブリック チャネルのスイッチング モードを表示する例を示します。

```
Router# show fabric switching-mode module all
%Truncated mode is allowed
%System is allowed to operate in legacy mode

Module Slot     Switching Mode     Bus Mode
    5                     DCEF     Compact
    9                Crossbar      Compact
Router#
```

ファブリック ステータスの表示

特定のスイッチング モジュールまたは全スイッチング モジュールのファブリック ステータスを表示するには、次の作業を行います。

コマンド	目的
Router# **show fabric status** [*slot_number* | **all**]	ファブリック ステータスを表示します。

次に、全モジュールのファブリック ステータスを表示する例を示します。

```
Router# show fabric status
 slot    channel      speed               module               fabric
                                          status               status
    1          0         8G                   OK                   OK
    5          0         8G                   OK          Up- Timeout
    6          0        20G                   OK         Up- BufError
    8          0         8G                   OK                   OK
    8          1         8G                   OK                   OK
    9          0         8G        Down- DDRsync                   OK
Router#
```

ファブリック使用率の表示

特定のモジュールまたは全モジュールのファブリック使用率を表示するには、次の作業を行います。

コマンド	目的
Router# **show fabric utilization** [*slot_number* | **all**]	ファブリック使用率を表示します。

次に、全モジュールのファブリック使用率を表示する例を示します。

```
Router# show fabric utilization all
Lo% Percentage of Low-priority traffic.
Hi% Percentage of High-priority traffic.

 slot    channel      speed  Ingress Lo%   Egress Lo%  Ingress Hi% Egress Hi%
    5          0        20G            0            0            0          0
    9          0         8G            0            0            0          0
Router#
```

ファブリック エラーの表示

特定のモジュールまたは全モジュールのファブリック エラーを表示するには、次の作業を行います。

コマンド	目的
Router# **show fabric errors** [*slot_number* | **all**]	ファブリック エラーを表示します。

次に、全モジュールのファブリック エラーを表示する例を示します。

```
Router# show fabric errors

Module errors:
 slot    channel        crc       hbeat        sync   DDR sync
    1          0          0           0           0          0
    8          0          0           0           0          0
    8          1          0           0           0          0
    9          0          0           0           0          0

Fabric errors:
 slot    channel       sync     buffer    timeout
    1          0          0           0          0
    8          0          0           0          0
    8          1          0           0          0
    9          0          0           0          0
Router#
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

Cisco IP Phone のサポート

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

Cisco IP Phone サポートの前提条件

なし。

Cisco IP Phone サポートの制約事項

- このマニュアルの情報はシスコ製以外の IP Phone サポートの設定にも利用できますが、それらのデバイスに対しては、該当するメーカーのマニュアルを参照することを推奨します。
- 設定情報を Cisco IP Phone に送信するには、Cisco IP Phone に接続されているポートで Cisco Discovery Protocol（CDP）をイネーブルにしなければなりません。
- 音声 VLAN はレイヤ 2 LAN ポートだけに設定できます。

- 次に示す条件の場合、Cisco IP Phone および Cisco IP Phone に接続されているデバイスは同じ VLAN に存在し、必ず同じ IP サブネットに存在する必要があります。
  - 両方が 802.1p またはタグなしフレームを使用する場合
  - Cisco IP Phone が 802.1p フレームを使用し、デバイスはタグなしフレームを使用する場合
  - Cisco IP Phone がタグなしフレームを使用し、デバイスは 802.1p フレームを使用する場合
  - Cisco IP Phone は 802.1Q フレームを使用し、音声 VLAN がアクセス VLAN と同じである場合
- Cisco IP Phone と Cisco IP Phone に接続されているデバイスは、同じ VLAN とサブネット内に存在していても異なるフレーム タイプを使用する場合、通信できません。同じサブネット内にあるデバイス間のトラフィックがルーティングされないためです（フレーム タイプが違う場合ルーティングされません）。
- Cisco IOS ソフトウェア コマンドを使用して、Cisco IP Phone 上のアクセス ポートに接続されているデバイスから送信されるトラフィックが使用するフレームタイプを設定できません。
- 音声 VLAN が設定されているポートでポート セキュリティをイネーブルにし、Cisco IP Phone に接続されている PC がある場合、ポート上の最大許容セキュア アドレスを 2 つ以上に設定します。
- 音声 VLAN には、スタティック セキュア MAC アドレスを設定できません。
- 音声 VLAN に設定されているポートはセキュア ポートにすることができます（第 85 章「ポート セキュリティ」を参照）。
- すべての設定において、音声トラフィックはレイヤ 3 IP precedence 値を伝送します（デフォルト値は音声トラフィックについては 5、音声制御トラフィックについては 3）。

Cisco IP Phone サポートについて

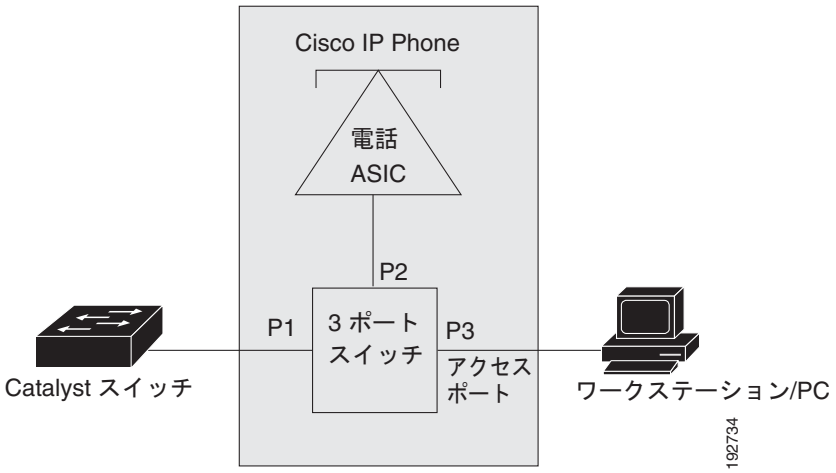
Cisco IP Phone の接続

Cisco IP Phone には、統合型 3 ポート 10/100 スイッチが搭載されています。各ポートは、次のデバイスとの接続専用です。

- ポート 1 は、スイッチに接続します。
- ポート 2 は、内蔵 10/100 インターフェイスで、Cisco IP Phone トラフィックを伝送します。
- ポート 3 は、PC またはその他のデバイスに接続します。

図 18-1 に、スイッチと PC 間に接続された Cisco IP Phone を示します。

図 18-1　スイッチに接続された Cisco IP Phone



Cisco IP Phone の音声トラフィック

Cisco IP Phone は、音声トラフィックをレイヤ 3 の IP precedence 値とレイヤ 2 の CoS 値と一緒に伝送します。この値は両方ともデフォルトで 5 に設定されています。Cisco IP Phone 通話の音質は、音声トラフィックが不均一に送信される場合、劣化する可能性があります。

スイッチ上のレイヤ 2 アクセス ポートについては、Cisco Discovery Protocol（CDP）パケットを送信するように設定することができます。接続された Cisco IP Phone では、これらの CDP パケットの設定に基づき、次のいずれかの方法により音声トラフィックがスイッチへ送信されます。

- レイヤ 2 CoS プライオリティ値によるタグ付きの音声 VLAN による送信
- レイヤ 2 CoS プライオリティ値によるタグ付きのアクセス VLAN による送信
- タグなしのアクセス VLAN（レイヤ 2 CoS プライオリティ値なし）による送信

（注）　すべての設定において、音声トラフィックはレイヤ 3 IP precedence 値を伝送します（デフォルト値は音声トラフィックについては 5、音声制御トラフィックについては 3）。

予測しやすい音声トラフィック フローを提供するために、受信したトラフィックのレイヤ 3 IP precedence 値またはレイヤ 2 CoS 値を信頼するようにスイッチの QoS を設定できます（第 61 章「PFC QoS の概要」を参照）。

デバイス検証による信頼境界機能では、ポートに接続されたデバイスが Cisco IP Phone であると Cisco Discovery Protocol（CDP）によって確認された場合だけ、設定済みの QoS ポート信頼コマンドを適用するように、スイッチのポートを設定できます。「シスコ デバイス検証による信頼境界を設定する方法」（P.65-10）を参照してください。

接続された Cisco IP Phone のレイヤ 2 アクセス ポートについては、1 つの VLAN を音声トラフィック用、もう 1 つの VLAN は Cisco IP Phone に接続しているデバイスからのデータ トラフィック用に使用するように設定できます。

Cisco IP Phone のデータ トラフィック

（注）

- Cisco IP Phone のアクセス ポートに接続されたデバイスからのタグ付きデータを信頼するまたはマーキングする機能を、「信頼境界（CDP デバイスに対する拡張された信頼）」機能といいます。
- Cisco IOS ソフトウェア コマンドを使用して、Cisco IP Phone 上のアクセス ポートに接続するデバイスから送信されるデータ トラフィックが使用するフレーム タイプを設定することはできません。
- Cisco IP Phone に接続されているデバイスからのタグなしトラフィックは、Cisco IP Phone のアクセス ポートの信頼状態にかかわらず、そのまま Cisco IP Phone を通過します。

Cisco IP Phone 上のアクセス ポートに接続するデバイスからのタグ付きデータ トラフィック（802.1Q または 802.1p フレーム タイプのトラフィック）を処理するには（図 18-1 を参照）、スイッチ上のレイヤ 2 アクセス ポートに CDP パケットの送信を設定して、接続された Cisco IP Phone が Cisco IP Phone 上のアクセス ポートを次のどちらかのモードに設定するように指定します。

- trusted（信頼性がある）モード：Cisco IP Phone 上のアクセス ポートから受信したすべてのトラフィックは、変化せずに Cisco IP Phone を通過します。
- untrusted（信頼性がない）モード：Cisco IP Phone 上のアクセス ポートから受信した 802.1Q または 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 値によってマーキングされます。デフォルトのレイヤ 2 CoS 値は 0 です。信頼できないモードがデフォルト設定です。

ほとんどの IP Phone には、IP Phone のアクセス ポートにおけるリンク ステートの変更をスイッチに通知する機能がありません。アクセス ポートに接続されたデバイスが管理上の理由で接続解除またはディセーブル化されても、スイッチはその変更を認識しません。一部の Cisco IP Phone は、ホスト存在 Type Length Value（TLV）が含まれた CDP メッセージを送信できます。TLV によって、アクセス ポート リンクの変更されたステートが通知されます。

Cisco IP Phone のその他の機能

Catalyst 6500 シリーズ スイッチは、第 83 章「IEEE 802.1X ポートベースの認証」で説明するように、Cisco IP Phone の認証、許可、アカウンティング（AAA）をサポートします。

Catalyst 6500 シリーズ スイッチは、Cisco Emergency Responder（Cisco ER）の自動トラッキングもサポートし、テレフォニー ネットワーク内の緊急事態コールの管理を支援します。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/sw/voicesw/ps842/tsd_products_support_series_home.html

Cisco IP Phone サポートのデフォルト設定

- Cisco IP Phone サポートはデフォルトではディセーブルに設定されています。
- 音声 VLAN 機能がイネーブルに設定されている場合、タグなしのすべてのトラフィックは、ポートのデフォルトの CoS プライオリティで送信されます。
- 802.1p または 802.1Q のタグ付きトラフィックでは、CoS 値が信頼されません。

Cisco IP Phone サポートの設定方法

音声トラフィックのサポートの設定

Cisco IP Phone が音声トラフィックを伝送する方法を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface gigabitethernet` *slot/port*	設定するポートを選択します。
ステップ 2	`Router(config-if)# switchport`	LAN ポートをレイヤ 2 スイッチング用に設定します。 （注）　LAN ポートをレイヤ 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 度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さらに **switchport** コマンドを入力してください。
ステップ 3	`Router(config-if)# switchport voice vlan` {*voice_vlan_ID* | **dot1p** | **none** | **untagged**}	Cisco IP Phone が音声トラフィックを伝送する方法を設定します。
ステップ 4	`Router(config)# end`	コンフィギュレーション モードを終了します。

Cisco IP Phone が音声トラフィックを伝送する方法を設定する際、次の情報に注意してください。

- 音声 VLAN ID を入力して、CDP パケットを送信します。CDP パケットは、音声トラフィックを音声 VLAN ID およびレイヤ 2 CoS 値（デフォルトは 5）によるタグ付き 802.1Q フレームで伝送するように Cisco IP Phone を設定します。指定できる VLAN ID は 1 ～ 4094 です。スイッチは 802.1Q 音声トラフィックを音声 VLAN に入れます。
- **dot1p** キーワードを入力して、CDP パケットを送信します。CDP パケットは、音声トラフィックを VLAN ID 0 およびレイヤ 2 の CoS 値（デフォルトは、音声トラフィックの場合 5、音声制御トラフィックの場合 3）によるタグ付き 802.1p フレームで伝送するように Cisco IP Phone を設定します。スイッチは 802.1p 音声トラフィックをアクセス VLAN に送ります。
- **untagged** キーワードを入力して、Cisco IP Phone が、タグなし音声トラフィックを伝送するように設定する CDP パケットを送信します。スイッチはタグなし音声トラフィックをアクセス VLAN に入れます。
- **none** キーワードを入力して、Cisco IP Phone が独自の設定を使用し、タグなし音声トラフィックを伝送できるようにします。スイッチはタグなし音声トラフィックをアクセス VLAN に入れます。
- すべての設定において、音声トラフィックはレイヤ 3 IP precedence 値（デフォルトは 5）を伝送します。
- QoS の設定方法の詳細については、第 61 章「PFC QoS の概要」を参照してください。
- ポートをレイヤ 2 アクセス ポートとして設定する方法、およびアクセス VLAN の設定方法の詳細については、「レイヤ 2 アクセス ポートとしての LAN インターフェイスの設定」（P.20-15）を参照してください。

次に、ギガビット イーサネット ポート 5/1 に対して、Cisco IP Phone が VLAN 101 を音声 VLAN として使用するように指示する CDP パケットを送信するように、設定する例を示します

```
Router# configure terminal
```

```
Router(config)# interface gigabitethernet 5/1
Router(config-if)# switchport voice vlan 101
Router(config-if)# exit
```

次に、ギガビット イーサネット ポート 5/1 の設定を確認する例を示します。

```
Router# show interfaces gigabitethernet 5/1 switchport
Name: Gi5/1
Switchport: Enabled
Administrative Mode: access
Operational Mode: access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: off
Access Mode VLAN: 100
Voice VLAN: 101
Trunking Native Mode VLAN: 1 (default)
Administrative private-vlan host-association: none
Administrative private-vlan mapping: 900 ((Inactive)) 901 ((Inactive))
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

データ トラフィックのサポートの設定

（注）　**platform qos trust extend** コマンドを使用して、信頼境界機能を実装します。

接続された Cisco IP Phone がデータ トラフィックを伝送する方法を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface gigabitethernet` *slot/port*	設定するポートを選択します。
ステップ 2	`Router(config-if)# platform qos trust extend` [**cos** *cos_value*]	接続された Cisco IP Phone がデータ トラフィックを伝送する方法を設定します。
ステップ 3	`Router(config)# end`	コンフィギュレーション モードを終了します。

接続された Cisco IP Phone がデータ トラフィックを伝送する方法を設定する際、次の点に注意してください。

- CDP パケットを送信して、接続された Cisco IP Phone 上のアクセス ポートに接続しているデバイスから受信したタグ付きトラフィックを Cisco IP Phone が信頼するように設定するには、**cos** キーワードおよび CoS 値を入力しないでください。
- CDP パケットを送信して、接続された Cisco IP Phone 上のアクセス ポートに接続しているデバイスから受信したタグ付き入力トラフィックを Cisco IP Phone がマーキングするように設定するには、**cos** キーワードおよび CoS 値を入力してください（有効値は 0 ～ 7 です）。
- Cisco IOS ソフトウェア コマンドを使用しても、Cisco IP Phone 上のアクセス ポートに接続するデバイスから送信されるデータ トラフィックへのタグの有無を設定できません。

次に、ギガビット イーサネット ポート 5/1 が CDP パケットを送信して、Cisco IP Phone にアクセス ポートを信頼できないポートとして設定すること、および CoS 3 を使用する Cisco IP Phone 上のアクセス ポートと接続しているデバイスから受信したすべてのタグ付きトラフィックをマーキングすることを通知するように設定する例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 5/1
Router(config-if)# platform qos trust extend cos 3
```

次に、ギガビット イーサネット ポート 5/1 が CDP パケットを送信して、Cisco IP Phone にアクセス ポートを信頼できるポートとして設定することを通知するように設定する例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 5/1
Router(config-if)# platform qos trust extend
```

次に、ギガビット イーサネット ポート 5/1 の設定を確認する例を示します。

```
Router# show queueing interface gigabitethernet 5/1 | include Extend
  Extend trust state: trusted
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

Power over Ethernet（PoE）のサポート

（注）
- PoE をサポートするスイッチング モジュールの詳細については、次の URL で『*Release Notes for Cisco IOS Release 15.1SY*』を参照してください。
  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/15.1SY/release_notes.html
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。
  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。
http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

PoE の前提条件

なし。

PoE の制約事項

PoE は、レイヤ 2 スイッチポートでのみサポートされます。

PoE について

デバイスの役割

- 給電側機器（PSE）：ツイストペア イーサネット接続を介して電力を供給するデバイス。Power over Ethernet（PoE）ドーターカードを搭載したスイッチング モジュールを使用するスイッチは、PSE ロールで機能します。
- 受電デバイス（PD）：PSE により電力が供給されるデバイス（IP Phone、IP カメラ、ワイヤレス アクセス ポイントなど）。

（注）　すべての PoE 対応デバイスがスイッチから電力供給されるわけではありません。PoE 対応デバイスのローカル電源には次の 2 種類があります。

- デバイスに接続されている電源装置。
- デバイスへのイーサネット接続を通じてパッチ パネルを経由する電源装置。

ローカルに電力供給されている PoE 対応デバイスがスイッチング モジュール ポート上にある場合、スイッチング モジュール自体はデバイスの存在を検出できません。デバイスが CDP をサポートしている場合、スーパーバイザ エンジンはデバイスとの CDP メッセージングを通じて、ローカルに電力供給されている PoE 対応デバイスを検出できます。ローカルに電源供給されている PoE 対応デバイスがローカル電源を失うと、インライン パワー モードが **auto** に設定されている場合、スイッチング モジュールは IP Phone を検出し、電力を供給できます。

PoE の概要

Cisco PoE ドーターカードは、次に示す 1 つ以上の PoE 実装をサポートします。

- Cisco Feature Navigator で「PoE Plus（PoE+、PoEP）サポート」として表示される IEEE 802.3at 標準。
  - WS-X6148E-GE-45AT スイッチング モジュールの PoE ドーターカードでのみサポートされています。
  - これらの機能は、IEEE 802.3at 準拠のクラス 4 PD でサポートされます。
    - PSE ではクラス 4：30.00 W（PD では 12.95 ～ 25.50 W）。
    - 任意で、PoE+ 用の LLDP インライン電力ネゴシエーション。
  - リリース 15.1(1)SY よりも前のリリースでは、PSE で最大 16.8 W（最大 45 ポートの ePoE）。

- IEEE 802.3af 標準。
  - WS-F6K-48-AF PoE ドーターカードおよび WS-X6148E-GE-45AT スイッチング モジュールの PoE ドーターカードでサポートされています。
  - PSE では、最大 16.80 W です。
  - IEEE 802.3af PoE 標準は、PD を検出し、ただちにその PD の所要電力を、PSE でのポートの電力範囲ごとに次のように分類する方式を定義しています。
    - クラス 0：最大 15.4 W（PD では 0.44 ～ 12.95 W。デフォルトの分類）
    - クラス 1：最大 4 W（PD では 0.44 ～ 3.84 W）
    - クラス 2：最大 7 W（PD では 3.84 ～ 6.49 W）
    - クラス 3：最大 15.4 W（PD では 6.49 ～ 12.95 W）
- シスコの先行標準インライン パワー：PSE では 10 W。

PoE ドーターカードが搭載されていると、スイッチング モジュールは、PoE ドーターカードでサポートされている PoE 実装に準拠した PoE 対応デバイスを自動的に検出し、プロビジョニングできます。スイッチング モジュールは、手動設定以外では他の PoE 実装をサポートするデバイスに電力を供給できません。

スイッチ ポートに直接接続されている PD だけが、スイッチから電力を供給されます。スイッチ ポートに接続された PD から 2 台めの PD がデイジーチェーン接続されている場合、2 台めの PD は、スイッチから電力を供給されません。

各 PD には、シャーシの電源バジェットから割り当てられる電力が必要です。それぞれの PD には固有の所要電力があるため、システムの電力管理ソフトウェアがポート単位で必要な電力をインテリジェントに割り当てることができれば、より多くのデバイスをサポートできます。

次に基づいたレベルで電力を割り当てるようにポートを設定できます。

- PD が検出されたときに、自動モードが設定されている場合：
  - デバイスから検出された情報
  - デフォルトのレベル
  - 設定されている最大レベル
- PD がポートに存在するかどうかにかかわらず、スタティック モードが設定されている場合：
  - デフォルトのレベル
  - 設定されているレベル

CPD-Based PoE 管理

スイッチング モジュール ポートが電力供給されていない PD を検出すると、デフォルトの電力割り当て量がそのポートに供給されます。PD との CDP メッセージ交換によって正確な電力量を判別すると、スーパーバイザ エンジンは、搭載されている PoE ドーターカードのハードウェア制限まで割り当て電力を加減します。

注意　ポートに PD ケーブルを差し込み、電源をオンにすると、スーパーバイザ エンジンは回線上でリンクが起動するまで、4 秒間待機します。この 4 秒の間に、IP Phone のケーブルを取り外し、ネットワーク デバイスを接続すると、そのネットワーク デバイスが損傷することがあります。ネットワーク デバイスを取り外し、別のネットワーク デバイスを接続する場合は、10 秒以上待機してから行うようにしてください。

インライン パワー IEEE 電力分類の無効化

IEEE 802.3af 標準には、電力割り当ての調整のプロビジョニングは含まれていません。CDP をサポートする 802.3af 準拠の PD は、CDP を使用して、IEEE 802.3af 電力分類を無効にすることができます。

WS-F6K-48-AF PoE ドーターカードまたは WS-X6148E-GE-45AT スイッチング モジュールの PoE ドーターカードは、インライン パワー IEEE 802.3af パワー電力分類の無効化機能をサポートします。

- 電力消費の測定：ポートにより受電デバイスに供給される正確な電力を測定する機能。
- 電力ポリシング：ポートの電力消費量をモニタする機能。

電力測定とポリシングを使用すると、IEEE 電力分類範囲内の最低電力レベルを必要とするデバイスの IEEE 802.3af 電力分類を安全に無効にできます。

PoE モニタリングおよびポリシングは、ポートの電力消費を管理上の最大値（設定された最大値またはポートのデフォルト値）と比較します。モニタ対象ポートの電力消費が管理上の最大値を超えると、次の処理が行われます。

- syslog メッセージが発行されます。
- モニタ対象ポートはシャットダウンされ、errdisable になります。
- 割り当てられた電力は解放されます。

PoE+ の LLDP インライン電力ネゴシエーション（IEEE 802.3at）

WS-X6148E-GE-45AT スイッチング モジュールの PoE ドーター カードは、電力消費量を減らすことができる追加のネゴシエーションをサポートする、IEEE 802.3at 準拠 LLDP PoE 電力ネゴシエーションをサポートしています。

（注）

- デフォルトでは、イネーブルです。
- 使用される LLDP TLV は DTE Power-via-MDI TLV です。
- 複数のプロトコル（CDP および LLDP 802.3at）を使用して電力ネゴシエーションを実行する PD がスイッチに接続されている場合、スイッチは電力ネゴシエーション TLV を含む最初のプロトコル パケット（CDP または LLDP）にロックされます。いずれか 1 つの電力ネゴシエーション プロトコルを毎回使用する必要がある場合は、スイッチ インターフェイスの他の電力ネゴシエーション プロトコルを管理上ディセーブルにする必要があります。
- その他のリンク層検出プロトコル（LLDP）設定手順については、次のマニュアルを参照してください。

  http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_lldp-med.html

PoE サポートの設定方法

PoE ステータスの表示

次に、スイッチでの PoE ステータスを表示する例を示します。

```
Router# show power auxiliary
system auxiliary power mode = on
system auxiliary power redundancy operationally = redundant
system primary connector power limit =   7266.00 Watts (173.00 Amps @ 42V)
system auxiliary connector power limit = 10500.00 Watts (250.00 Amps @ 42V)
system primary power used =              1407.00 Watts (33.50 Amps @ 42V)
system auxiliary power used =              22.68 Watts ( 0.54 Amps @ 42V)
                         Inline          Inline-Pwr     Inline-Pwr     VDB
                         Pwr-Limit       Used-Thru-Pri  Used-Thru-Aux  Aux-Pwr
Slot Card-Type           Watts   A @42V  Watts   A @42V Watts   A @42V Capable
---- ------------------- ------- ------ ------- ------ ------- ------ -------
2    WS-F6K-48-AT        1600.20 38.10    23.10  0.55    11.34  0.27  Yes
4    WS-F6K-48-AT        1600.20 38.10    23.10  0.55    11.34  0.27  Yes
---- ------------------- ------- ------ ------- ------ ------- ------ -------
Totals:                                    46.20  1.10    22.68  0.54
```

ポート単位の PoE サポートの設定

ポート単位の PoE 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	`Router(config-if)# power inline {auto | static | never}[max milliwatts]`	ポート単位の PoE サポートを設定し、任意でポートの最大インライン パワー レベル（ミリ W）を指定します。
ステップ 2	`Router# show power inline {type slot/port | module slot}[detail]`	設定を確認します。

power inline コマンドでインライン パワー サポートを設定する場合、次の点に注意してください。

- PD と PoE 自動割り当ての自動検出を設定するには、**auto** キーワードを入力します。
- PD の自動検出を設定するが、固定 PoE 割り当てを維持する場合は、**static** キーワードを入力します。
- ポートに割り当てる最大電力を指定するには、**auto** または **static** キーワードを入力してから、**max** キーワードを入力し、パワー レベル（ミリ W）を指定します。
- **auto** キーワードが入力され、CDP がポートでイネーブルになると、CDP をサポートする PD は別の電力レベルをネゴシエートできます。
- PD の自動検出をディセーブルにするには、**never** キーワードを入力します。

- WS-F6K-GE48-AF、WS-F6K-48-AF、または WS-X6148E-GE-45AT スイッチング モジュールの PoE ドーターカードの場合：
  - **max** キーワードを使用して設定可能な最大電力範囲は 4000 ～ 16800 ミリ W です。最大電力レベルが設定されていない場合、デフォルトの最大電力は 15400 ミリ W です。

（注）　インライン パワー カードで 15400 ミリ W を超える電力を使用して多くのインライン パワー ポートをサポートするには、電力バジェットを確定するために **static** キーワードを使用することを推奨します。

  - **auto** キーワードが入力され、CDP がポート上でイネーブルである場合、最大電力レベルが 16800 ミリ W より低く設定されていない限り、CDP をサポートするインライン パワー装置は最大で 16800 ミリ W の電力レベルをネゴシエーションできます。

次に、ポート GigabitEthernet 2/10 のインライン パワーをディセーブルにする例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 2/10
Router(config-if)# power inline never
```

次に、ポート GigabitEthernet 2/10 のインライン パワーをイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 2/10
Router(config-if)# power inline auto
```

次に、GigabitEthernet ポート 2/10 のインライン パワー設定を確認する例を示します。

```
Router# show power inline gigabitethernet 2/10
Interface Admin  Priority     Oper      Power(Watts)    Device             Class
                 (enabled )            From PS To PD
---------------- ---------- ---------- ------- ------- ------------------ -----

Gi2/10    auto   low        on            14.5    13.1 Cisco IP Phone 9971     4

Interface AdminPowerMax Police ActConsumption
             (ワット)
--------- ------------- ------ --------------

Gi2/10             30.0 on                6.7
```

PoE 電力プライオリティの設定

PoE を供給するポートのプライオリティの設定によって、電力が不足したときにスイッチがどのように対応するかを設定できます。このプライオリティによって、電力が不足したときにポートから削除される PoE の順序が決まります。つまり、低いプライオリティ、次に高いプライオリティ、そしてクリティカル プライオリティ ポートに関してはできる限り電力が維持されます。ここでは、PoE 電力プライオリティの設定方法について説明します。

- 「PoE 電力プライオリティのグローバル イネーブル ステートの設定」（P.19-7）
- 「PoE ポートの電力プライオリティの設定」（P.19-7）

PoE 電力プライオリティのグローバル イネーブル ステートの設定

PoE 電力プライオリティをグローバルに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	`Router(config)# no power inline priority enable`	PoE 電力プライオリティをグローバルにディセーブルにします（デフォルトはイネーブル）。
ステップ 2	`Router# show power inline`	設定を確認します。

次に、PoE 電力プライオリティをグローバルにディセーブルにする例を示します。

```
Router(config)# no power inline priority enable
```

すべての **show power inline** コマンドのカラム見出しに、PoE 電力プライオリティのグローバル ステートが表示されます（この例では「disabled」）。

```
Router# show power inline
Interface Admin  Priority     Oper      Power(Watts)    Device             Class
                 (disabled)            From PS To PD
---------------- ---------- ---------- ------- ------- ------------------ -----
...
```

PoE ポートの電力プライオリティの設定

PoE ポートの電力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	`Router(config-if)# power inline auto priority {critical | high | low}`	PoE ポートの電力プライオリティをイネーブルにします（電力プライオリティがグローバルにイネーブルの場合、デフォルトは低プライオリティ）。 電力不足が発生した場合、PoE は次の順序でポートから削除されます。 • 低プライオリティ ポート • 高プライオリティ ポート クリティカル プライオリティ ポートの PoE はできる限り維持されます。
ステップ 2	`Router# show power inline type slot/port [detail]`	設定を確認します。

次に、ポート GigabitEthernet 2/10 の PoE ポート電力プライオリティを高に設定する例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 2/10
Router(config-if)# power inline auto priority high
```

次に、ポート GigabitEthernet 2/10 の PoE ポート電力プライオリティ設定を確認する例を示します。

```
Router# show power inline gigabitethernet 2/10 detail | include Priority
  Priority: high
```

PoE モニタリングおよびポリシングの設定

WS-F6K-48-AF PoE ドーターカードまたは WS-X6148E-GE-45AT スイッチング モジュールの PoE ドーターカードによって、PoE モニタリングおよびポリ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	`Router(config-if)# power inline police`	PoE モニタリングおよびポリシングをイネーブルにします。
ステップ 2	`Router# show power inline {type slot/port | module slot}[detail]`	設定を確認します。

次に、ポート GigabitEthernet 1/9 でモニタリングおよびポリシングをイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 2/10
Router(config-if)# power inline police
```

次に、ポート GigabitEthernet 2/10 で電力モニタリングとポリシング設定を確認する例を示します。

```
Router# show power inline gigabitethernet 2/10 detail | include Police
Police: on
Router#
Router# show power inline gigabitethernet 2/10
Interface  Admin  Oper  Power (Watts)     Device   Class
                       From PS To Device
---------  -----  ---- ------- ---------  -------  -----
Gi2/10      auto   on   17.3    15.4        Ieee PD   3

Interface  AdminPowerMax (Watts) Police   ActualConsumption
---------  --------------------- ------   -----------------
 Gi2/10            15.4            on      5.7
Router#
```

LLDP 電力ネゴシエーションのディセーブル化（IEEE 802.3at）

WS-X6148E-GE-45AT スイッチング モジュールでは、LLDP 電力ネゴシエーションはデフォルトでイネーブルです。LLDP 電力ネゴシエーション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
`Router(config-if)# no lldp tlv-select power-management`	LLDP 電力ネゴシエーションをディセーブルにします（デフォルトはイネーブル）。

次に、LLDP 電力ネゴシエーションがイネーブルの場合にインターフェイス GigabitEthernet 3/1 での LLDP 電力ネゴシエーション設定を表示する例を示します。

```
Router# show power inline gigabitethernet 2/10 detail | begin LLDP
 LLDP Power Classification    -- Sent to PD --  -- Rcvd from PD --
   Power Type :               type 2 PSE        type 2 PD
   Power Source :             primary           PSE
   Power Priority :           low               high
   Requested Power (watts):   11.2              11.2
   Allocated Power (watts):   11.2              11.2
   Power class :              4                 4

 LLDP Legacy MDI TLV          -- Rcvd from PD --
```

```
   MDI power support :         0
   pse power pair :            0
   MDI power class :           0
```

次に、インターフェイス GigabitEthernet 2/10 で LLDP 電力ネゴシエーションをディセーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.End with CNTL/Z.
Router(config)# interface gigabitethernet 2/10
Router(config-if)# no lldp tlv-select power-management
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

PART 6

LAN スイッチング

レイヤ 2 スイッチング用 LAN ポート

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。
- レイヤ 3 インターフェイスの設定手順については、第 34 章「レイヤ 3 インターフェイス」を参照してください。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

レイヤ 2 LAN インターフェイスの前提条件

なし。

レイヤ 2 LAN インターフェイスの制約事項

- 802.1Q トランクを介して Cisco スイッチを接続するときは、802.1Q トランクのネイティブ VLAN がトランク リンクの両端で同じであることを確認してください。トランクの一端のネイティブ VLAN と反対側の端のネイティブ VLAN が異なると、スパニングツリー ループの原因になります。
- ネットワーク上の各 VLAN のスパニングツリーをディセーブルにせずに 802.1Q トランクのネイティブ VLAN のスパニングツリーをディセーブルにすると、スパニングツリー ループが発生することがあります。802.1Q トランクのネイティブ VLAN 上で、スパニングツリーをイネーブルのままにしておくことを推奨します。この設定ができない場合は、ネットワークのすべての VLAN 上でスパニングツリーをディセーブルにしてください。スパニングツリーをディセーブルにする場合には、事前にネットワークに物理的なループが存在しないことを確認してください。
- 802.1Q トランクを介して 2 台の Cisco スイッチを接続すると、トランク上で許容される VLAN ごとにスパニングツリー BPDU が交換されます。トランクのネイティブ VLAN 上の BPDU は、タグなしの状態で、予約済み IEEE 802.1d スパニングツリー マルチキャスト MAC アドレス（01-80-C2-00-00-00）に送信されます。トランクの他のすべての VLAN 上の BPDU は、タグ付きの状態で、予約済み Cisco Shared Spanning Tree（SSTP）マルチキャスト MAC アドレス（01-00-0c-cc-cc-cd）に送信されます。
- 他社製の 802.1Q スイッチでは、すべての VLAN に対してスパニングツリー トポロジーを定義するスパニングツリーのインスタンス（Mono Spanning Tree（MST））が 1 つしか維持されません。802.1Q トランクを介してシスコ製スイッチを他社製のスイッチに接続すると、他社製のスイッチの MST とシスコ製スイッチのネイティブ VLAN スパニングツリーが組み合わされて、Common Spanning Tree（CST）と呼ばれる単一のスパニングツリー トポロジが形成されます。
- Cisco スイッチは、トランクのネイティブ VLAN 以外の VLAN にある SSTP マルチキャスト MAC アドレスに BPDU を送信します。したがって、他社製のスイッチではこれらのフレームが BPDU として認識されず、対応する VLAN のすべてのポート上でフラッディングされます。他社製の 802.1Q クラウドに接続された他の Cisco スイッチは、フラッディングされたこれらの BPDU を受信します。このようにして、Cisco スイッチは、他社製の 802.1Q スイッチ クラウドにわたって、VLAN 別のスパニングツリー トポロジーを維持できます。Cisco スイッチを隔てている他社製の 802.1Q クラウドは、802.1Q トランクを介して他社製の 802.1Q クラウドに接続されたすべてのスイッチ間の単一のブロードキャスト セグメントとして処理されます。
- Cisco スイッチを他社製の 802.1Q クラウドに接続するすべての 802.1Q トランク上で、ネイティブ VLAN が同じであることを確認します。
- 他社製の特定の 802.1Q クラウドに複数の Cisco スイッチを接続する場合は、すべての接続に 802.1Q トランクを使用する必要があります。アクセス ポートを介して、Cisco スイッチを他社製の 802.1Q クラウドに接続できません。このように接続すると、スイッチはアクセス ポートのスパニングツリー ポート ステートを「一貫性のない」状態にし、ポートを介してトラフィックが送信されなくなります。

レイヤ 2 スイッチングについて

レイヤ 2 イーサネット スイッチングについて

レイヤ 2 イーサネット スイッチングの概要

Cisco スイッチ上のレイヤ 2 イーサネット ポートは、レイヤ 2 イーサネット セグメント間の同時パラレル接続をサポートしています。イーサネット セグメント間のスイッチド コネクションが維持されるのは、パケットの伝送時間の長さだけです。次のパケットには、別のセグメント間に新しい接続が確立されます。

レイヤ 2 LAN スイッチング（ハードウェアでサポートされるブリッジング）は、自身の衝突ドメインに接続されている各デバイスを割り当てることによって、輻輳を回避できます。各 LAN ポートは、それぞれ別のイーサネット衝突ドメイン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、接続されたデバイスはネットワークの全帯域幅にアクセスできます。

MAC アドレス テーブルの作成

MAC アドレス テーブルの概要

異なる LAN ポートに接続している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 LAN ポートから他方の LAN ポートにワイヤ速度でフレームを転送し、各セッションが全帯域幅を利用できるようにします。

LAN ポート間で効率的にフレームをスイッチングするために、スイッチは MAC アドレス テーブルを保持しています。フレームがスイッチに着信すると、ルータは送信元ネットワーク デバイスの MAC アドレスと、フレームを受信した LAN ポートを対応付けます。

MAC アドレス テーブルは、受信したフレームの送信元 MAC アドレスを使用して作成されます。MAC アドレス テーブルに宛先 MAC アドレスが登録されていないフレームをスイッチが受信すると、そのフレームを受信したポート以外の、同一 VLAN のすべての LAN ポートに、フレームをフラッディングします。宛先ステーションから応答があると、スイッチは関連する送信元 MAC アドレスおよびポート ID を MAC アドレス テーブルに追加します。その後、スイッチは、以降のフレームを、すべての LAN ポートにフラッディングするのではなく単一の LAN ポートへと転送します。

MAC 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 128,000 以上のアドレス エントリを保管できます。スイッチでは、**mac address-table aging-time** コマンドによって設定されたエージング メカニズムを使用するため、アドレスが非アクティブなまま指定した秒数が経過すると、そのアドレスはアドレス テーブルから削除されます。

アドレス テーブルの同期と共有

分散スイッチング環境で分散型フォワーディング カード（DFC）搭載の各スイッチング モジュールは MAC アドレスを学習し、アドレス テーブルを維持し、テーブル エントリを期限切れにします。Ethernet Out of Band Channel（EOBC）経由の MAC アドレス テーブルの同期は、PFC およびすべての DFC 間のアドレス テーブルを同期するため、DFC が別のモジュール上でアクティブなアドレスのためにフラッディングする必要がなくなります。MAC 同期はデフォルトでイネーブルです。

アドレス テーブル変更の通知

スイッチは、特定の LAN ポートに関連するアドレス テーブル エントリの動的な追加、および削除の履歴を保持するように設定できます。変更履歴は、SNMP トラップ通知として送信されるか、SNMP MIB から手動で読み取ることができます。

VLAN トランクについて

（注）　VLAN の詳細については、第 25 章「仮想ローカル エリア ネットワーク（VLAN）」を参照してください。

トランクとは、スイッチと他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することができます。

802.1Q（業界標準のトランキング カプセル化方式）が、すべてのイーサネット ポートで使用できます。

1 つのイーサネット ポートまたは EtherChannel に対してトランクを設定できます。EtherChannel の詳細については、第 22 章「EtherChannel」を参照してください。

イーサネット トランク ポートは、数種類のトランキング モードをサポートしています（表 20-1（P.20-4）を参照）。

Dynamic Trunking Protocol（DTP）は LAN ポート上のトランク自動ネゴシエーションを管理します。

トランキングを自動ネゴシエーションするには、LAN ポートが同じ VTP ドメインに存在する必要があります。異なるドメイン内の LAN ポートを強制的にトランクするには、**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、第 24 章「VLAN トランキング プロトコル（VTP）」を参照してください。

レイヤ 2 LAN ポート モード

表 20-1　　レイヤ 2 LAN ポート モード

モード	機能
switchport mode access	LAN ポートは永続的な非トランキング モードになり、リンクを非トランク リンクに変換するようにネゴシエーションを行います。ネイバー LAN ポートが変更に同意しなくても、LAN ポートは非トランク ポートになります。
switchport mode dynamic desirable	リンクからトランク リンクへの変換を LAN ポートにアクティブに試行させます。ネイバー LAN ポートが **trunk**、**desirable**、または **auto** モードに設定されていれば、LAN ポートはトランク ポートになります。このモードは、すべての LAN ポートのデフォルト モードです。
switchport mode dynamic auto	LAN ポートにリンクからトランク リンクへの変換を試行させます。ネイバー LAN ポートが **trunk** または **desirable** モードに設定されていれば、LAN ポートはトランク ポートになります。

表 20-1　レイヤ 2 LAN ポート モード （続き）

モード	機能
switchport mode trunk	LAN ポートは永続的なトランキング モードになり、リンクをトランク リンクに変換するようにネゴシエーションを行います。ネイバー ポートが変更に同意しなくても、LAN ポートはトランク ポートになります。
switchport nonegotiate	LAN ポートを永続的なトランキング モードにしますが、LAN ポートが DTP フレームを生成するのを防ぎます。トランク リンクを確立するには、ネイバー ポートを手動でトランク ポートとして設定する必要があります。

（注）　DTP はポイントツーポイント プロトコルです。ただし、インターネットワーキング 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 LAN ポートが、**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、LAN ポートをトランクにし、DTP フレームが生成されないようにします。

レイヤ 2 LAN インターフェイスのデフォルト設定

機能	デフォルト
インターフェイス モード： • **switchport** コマンドの入力前 • **switchport** コマンドの入力後	 レイヤ 3（未設定） **switchport mode dynamic desirable**
VLAN 許容範囲	VLAN 1 ～ 4094（予約済み VLAN を除く）（表 25-1 (P.25-3) を参照）
プルーニングに適格な VLAN 範囲	VLAN 2 ～ 1001
デフォルト アクセス VLAN	VLAN 1
ネイティブ VLAN（802.1Q トランク用）	VLAN 1
スパニングツリー プロトコル（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 LAN ポートでは 19 • 100 Mbps ファスト イーサネット LAN ポートでは 19 • 1,000 Mbps ギガビット イーサネット LAN 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

レイヤ 2 スイッチング用の LAN インターフェイスの設定方法

（注）　インターフェイスをデフォルト設定に戻すには、**default interface** {**fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port* コマンドを使用します。

レイヤ 2 スイッチング用の LAN ポートの設定

レイヤ 2 スイッチング用の LAN 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	`Router(config)# interface type slot/port`	設定する LAN ポートを選択します。
ステップ 2	`Router(config-if)# shutdown`	（任意）設定が完了するまでトラフィック フローを防止するために、インターフェイスをシャットダウンします。
ステップ 3	`Router(config-if)# switchport`	LAN ポートをレイヤ 2 スイッチング用に設定します。 （注）　LAN ポートをレイヤ 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 度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さらに **switchport** コマンドを入力してください。
ステップ 4	`Router(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ている場合に限り必要）。
ステップ 5	`Router(config-if)# end`	コンフィギュレーション モードを終了します。

switchport コマンドを入力したあとのデフォルト モードは、**switchport mode dynamic desirable** です。ネイバー ポートがトランキングをサポートし、かつトランキングを許可するように設定されている場合、**switchport** コマンドを入力すると、リンクはレイヤ 2 トランクになります。

（注）　**switchport** コマンドを使用する際に、レイヤ 3 に設定するポートが現在レイヤ 2 に設定されている場合、レイヤ 3 の設定はメモリには保持されますが、実行コンフィギュレーションには保持されず、ポートがレイヤ 3 にスイッチングされるたびにポートに適用されます。また、レイヤ 2 に設定するポートが現在レイヤ 3 に設定されている場合、レイヤ 2 の設定はメモリには保持されますが、実行コンフィギュレーションには保持されず、ポートがレイヤ 2 にスイッチングされるたびにポートに適用されます。メ

モリおよび実行コンフィグレーションでポートのデフォルト設定を復元するには、**default interface** コマンドを使用します。**switchport** コマンドを使用したポートの役割の変更に伴う潜在的な問題を回避するには、**switchport** コマンドを適用する前にインターフェイスをシャットダウンします。

アウトオブバンドの MAC アドレス テーブルの同期のイネーブル化

アウトオブバンドの MAC アドレス テーブルの同期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
`Router(config)# mac address-table synchronize [activity-time seconds]`	DFC 搭載のスイッチング モジュール間でアウトオブバンドの MAC アドレス テーブルの同期をイネーブルにします。 • **activity-time** *seconds*：（任意）アクティビティ タイマーの間隔を指定します。

アウトオブバンドの MAC アドレス テーブルの同期を設定する際は、次の点に注意してください。

- デフォルトでは、アウトオブバンドの MAC アドレス テーブルの同期はディセーブルになります。
- スイッチに WS-6708-10G スイッチング モジュールが搭載されている場合、アウトオブバンドの MAC アドレス テーブルの同期は自動的にイネーブルになります。
- アクティビティ タイマーの間隔は、160 秒、320 秒、および 640 秒として設定できます。デフォルトは 160 秒です。

次に、アウトオブバンドの MAC アドレス テーブルの同期をイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# mac address-table synchronize activity-time 320
```

MAC アドレス テーブル通知の設定

（注）
- ここに記載された作業を実行する前に、「レイヤ 2 スイッチング用の LAN ポートの設定」（P.20-6）の手順を実行します。
- この機能を使って SNMP トラップ通知を送信するには、**snmp-server enable mac-notification change** コマンドを使い、グローバル MAC トラップ フラグもイネーブルにする必要があります。

MAC アドレス テーブルの通知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	`Router(config)# mac address-table notification change [interval value]`	MAC アドレス テーブルにおける動的変更の通知送信をイネーブルにします。 （任意）変更を送信する最短の間隔を秒単位で指定します。 **（注）** このコマンドの **no** 形式を実行すると、変更情報は送信されずにデフォルトに戻ります。
ステップ 2	`Router(config)# mac address-table notification change [history size]`	MAC アドレス テーブルにおける動的変更の通知送信をイネーブルにします。 （任意）履歴バッファ内のエントリ数を設定します。 **（注）** このコマンドの **no** 形式を実行すると、変更情報は送信されずにデフォルトに戻ります。
ステップ 3	`Router(config)# interface type slot/port`	設定する LAN ポートを選択します。
ステップ 4	`Router(config-if)# snmp trap mac-notification change [added | removed]`	この LAN ポートに関連付けられている MAC アドレスで、MAC アドレスがアドレス テーブルに追加、またはアドレス テーブルから削除された場合に SNMP トラップ通知をイネーブルにします。 （任意）テーブルに MAC アドレスが追加された場合だけ通知する場合は、**added** オプションを使用します。テーブルから MAC アドレスが削除された場合だけ通知する場合は、**removed** オプションを使用します。
ステップ 5	`Router(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。

通知パラメータを設定する場合、次の情報に注意してください。

- **interval** *value* パラメータで指定できる値は、0 秒（即時）～ 2,147,483,647 秒です。デフォルトは 1 秒です。
- **history** *size* パラメータで設定できる値は、0 エントリから 500 エントリまでです。デフォルトは 1 エントリです。

次に、Gigabit Ethernet ポート 5/7 および 5/8 上のアドレスの MAC アドレス テーブルへの動的な追加に関する SNMP 通知を設定する方法の例を示します。変更の通知は、5 秒以下の間隔で送信されます。変更回数 25 回までが保存され、この間隔で送信されます。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# mac address-table notification change interval 5
Router(config)# mac address-table notification change history 25
Router(config)# interface gigabitethernet 5/7
Router(config-if)# snmp trap mac-notification change added
Router(config-if)# end
Router(config)# interface gigabitethernet 5/8
Router(config-if)# snmp trap mac-notification change added
Router(config-if)# end
Router# exit
```

トランクとしてのレイヤ 2 スイッチング ポートの設定

802.1Q トランクとしてのレイヤ 2 スイッチング ポートの設定

（注）
- ここに記載された作業を実行する前に、「レイヤ 2 スイッチング用の LAN ポートの設定」（P.20-6）の手順を実行します。
- キーワードを指定せずに **switchport** コマンドを入力する場合（前述のステップ 3）、デフォルト モードは **switchport mode dynamic desirable** です。

レイヤ 2 スイッチング ポートを 802.1Q 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
`Router(config-if)# switchport trunk encapsulation dot1q`	（任意）カプセル化を 802.1Q として設定します。

switchport mode trunk コマンドを使用できるようにするには、カプセル化を 802.1Q として設定する必要があります。

（注）　ここに記載された作業を実行したあとで、「トランクの設定の完了」（P.20-13）の手順を実行します。

DTP を使用するためのレイヤ 2 トランクの設定

（注）　ここに記載された作業を実行する前に、「レイヤ 2 スイッチング用の LAN ポートの設定」（P.20-6）の手順を実行します。

DTP を使用するようにレイヤ 2 トランクを設定するには、次の作業を行います。

コマンド	目的
`Router(config-if)# switchport mode dynamic {auto | desirable}`	（任意）DTP を使用するようにトランクを設定します。 **（注）** このコマンドの **no** 形式を実行すると、デフォルトのトランク トランキング モード（**switchport mode dynamic desirable**）に戻ります。

DTP を使用するようにレイヤ 2 トランクを設定する際、次の情報に注意してください。

- 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に限り必須です。
- トランキング モードの詳細については、表 20-1（P.20-4）を参照してください。

（注） ここに記載された作業を実行したあとで、「トランクの設定の完了」（P.20-13）の手順を実行します。

DTP を使用しないようにするためのレイヤ 2 トランクの設定

（注） ここに記載された作業を実行する前に、「レイヤ 2 スイッチング用の LAN ポートの設定」（P.20-6）の手順を実行します。

DTP を使用しないようにレイヤ 2 トランクを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config-if)# switchport mode trunk`	（任意）無条件にポートをトランクに設定します。
ステップ 2	`Router(config-if)# switchport nonegotiate`	（任意）DTP を使用しないようにトランクを設定します。 **（注）** このコマンドの **no** 形式を実行すると、ポートで DTP がイネーブルになります。

DTP を使用しないようにレイヤ 2 トランクを設定する際、次の点に注意してください。

- **switchport mode trunk** コマンドを入力する前に、カプセル化を設定する必要があります（「802.1Q トランクとしてのレイヤ 2 スイッチング ポートの設定」（P.20-9）を参照）。
- **switchport nonegotiate** コマンドを使用できるようにするには、**switchport mode trunk** コマンドを入力する必要があります。
- **switchport mode dynamic trunk** コマンドを入力します。トランキング モードの詳細については、表 20-1（P.20-4）を参照してください。
- **switchport nonegotiate** コマンドを入力する前にカプセル化を設定し（「802.1Q トランクとしてのレイヤ 2 スイッチング ポートの設定」（P.20-9）を参照）、**switchport mode trunk** コマンドを使用して無条件にポートをトランクに設定する必要があります（「DTP を使用するためのレイヤ 2 トランクの設定」（P.20-9）を参照）。

（注） ここに記載された作業を実行したあとで、「トランクの設定の完了」（P.20-13）の手順を実行します。

アクセス VLAN の設定

（注）　ここに記載された作業を実行する前に、「レイヤ 2 スイッチング用の LAN ポートの設定」（P.20-6）の手順を実行します。

アクセス VLAN を設定するには、次の作業を行います。

コマンド	目的
`Router(config-if)# switchport access vlan vlan_ID`	（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 を設定します。*vlan_ID* の値は 1 ～ 4094 です（予約済み VLAN は除く。表 25-1（P.25-3）を参照）。 **（注）** • VLAN のロックがイネーブルになっている場合は、VLAN の番号の代わりに VLAN の名前を入力します。詳細については、「VLAN ロック」（P.25-5）を参照してください。 • このコマンドの **no** 形式を実行すると、デフォルトの VLAN（VLAN 1）に戻ります。

（注）　ここに記載された作業を実行したあとで、「トランクの設定の完了」（P.20-13）の手順を実行します。

802.1Q ネイティブ VLAN の設定

（注）　ここに記載された作業を実行する前に、「レイヤ 2 スイッチング用の LAN ポートの設定」（P.20-6）の手順を実行します。

802.1Q ネイティブ VLAN を設定するには、次の作業を行います。

コマンド	目的
`Router(config-if)# switchport trunk native vlan vlan_ID`	（任意）802.1Q ネイティブ VLAN を設定します。 **（注）**　VLAN のロックがイネーブルになっている場合は、VLAN の番号の代わりに VLAN の名前を入力します。詳細については、「VLAN ロック」（P.25-5）を参照してください。

ネイティブ VLAN を設定する際、次の点に注意してください。

- *vlan_ID* の値は 1 ～ 4094 です（予約済み VLAN は除く。表 25-1（P.25-3）を参照）。
- アクセス VLAN がネイティブ VLAN として自動的に使用されることはありません。

（注）　ここに記載された作業を実行したあとで、「トランクの設定の完了」（P.20-13）の手順を実行します。

トランク上で許容される VLAN のリストの設定

（注）　ここに記載された作業を実行する前に、「レイヤ 2 スイッチング用の LAN ポートの設定」（P.20-6）の手順を実行します。

トランク上で許容される VLAN のリストを設定するには、次の作業を行います。

コマンド	目的
`Router(config-if)# switchport trunk allowed vlan [add | except | none | remove] vlan [,vlan[,vlan[,...]]]`	（任意）トランク上で許容される VLAN のリストを設定します。 **（注）** • VLAN のロックがイネーブルになっている場合は、VLAN の番号の代わりに VLAN の名前を入力します。詳細については、「VLAN ロック」（P.25-5）を参照してください。 • このコマンドの **no** 形式を実行すると、デフォルト値（すべての VLAN を許可）に戻ります。

トランク上で許容される VLAN のリストを設定する際、次の情報に注意してください。

- *vlan* パラメータは、1 ～ 4094 の間の 1 つの VLAN 番号、または 2 つの VLAN 番号で指定する（小さい方の数を先にして、間をダッシュで区切る）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。
- VLAN のロックがイネーブルになっている場合は、VLAN の番号の代わりに VLAN の名前を入力します。VLAN の名前の範囲を入力する場合は、VLAN の名前とダッシュの間にスペースを入力してください。
- デフォルトでは、すべての VLAN が許可されます。
- VLAN 1 を削除できます。トランクから VLAN 1 を削除した場合も、トランク インターフェイスは VLAN 1 の Cisco Discovery Protocol（CDP）、VLAN トランキング プロトコル（VTP）、ポート集約プロトコル（PAgP）、DTP などの管理トラフィックを引き続き送受信します。

（注）　ここに記載された作業を実行したあとで、「トランクの設定の完了」（P.20-13）の手順を実行します。

プルーニング適格 VLAN のリストの設定

（注）　ここに記載された作業を実行する前に、「レイヤ 2 スイッチング用の LAN ポートの設定」（P.20-6）の手順を実行します。

レイヤ 2 トランクでプルーニング適格 VLAN のリストを設定するには、次の作業を行います。

コマンド	目的
`Router(config-if)# switchport trunk pruning vlan {none |{{add | except | remove} vlan[,vlan[,vlan[,...]]]}}`	（任意）トランクでプルーニング適格 VLAN のリストを設定します（「VTP プルーニング」（P.24-7）を参照）。 **（注）** このコマンドの **no** 形式を実行すると、デフォルト値（すべての VLAN がプルーニング適格）に戻ります。

トランク上で許容されるプルーニング適格 VLAN のリストを設定する際、次の点に注意してください。

- *vlan* パラメータは、1 ～ 4094 の範囲の単一の VLAN 番号（予約済み VLAN を除く。表 25-1（P.25-3）を参照）、または 2 つの VLAN 番号（小さい番号が先、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。
- デフォルトでは、プルーニングが許容される VLAN のリストには、すべての VLAN が含まれます。
- VTP トランスペアレント モードのネットワーク デバイスは、VTP Join メッセージを送信しません。VTP トランスペアレント モードのネットワーク装置にトランク接続されている場合は、トランスペアレント モード ネットワーク装置によって使用される VLAN、またはプルーニング不適格としてトランスペアレント モード ネットワーク装置全体に伝送する必要がある VLAN を設定します。

（注） ここに記載された作業を実行したあとで、「トランクの設定の完了」（P.20-13）の手順を実行します。

トランクの設定の完了

レイヤ 2 トランクの設定を完了するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config-if)# 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ている場合に限り必要）。
ステップ 2	`Router(config-if)# end`	コンフィギュレーション モードを終了します。

レイヤ 2 トランクの設定の確認

レイヤ 2 トランク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
ステップ 1	`Router# show running-config interface type 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 2	`Router# show interfaces [type slot/port] switchport`	インターフェイスのスイッチ ポートの設定を表示します。
ステップ 3	`Router# show interfaces [type slot/port] trunk`	インターフェイスのトランクの設定を表示します。

設定および確認の例

次に、ギガビット イーサネット ポート 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、ネイバー ポートが 802.1Q トランキングをサポートするように設定されていることを前提としています。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 5/8
Router(config-if)# shutdown
Router(config-if)# switchport
Router(config-if)# switchport mode dynamic desirable
Router(config-if)# switchport trunk encapsulation dot1q
Router(config-if)# no shutdown
Router(config-if)# end
Router# exit
```

次に、設定を確認する例を示します。

```
Router# show running-config interface gigabitethernet 5/8
Building configuration...
Current configuration:
!
interface GigabitEthernet5/8
 no ip address
 switchport
 switchport trunk encapsulation dot1q
end

Router# show interfaces gigabitethernet 5/8 switchport
Name: Gi5/8
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
Pruning VLANs Enabled: ALL

Router# show interfaces gigabitethernet 5/8 trunk

Port      Mode         Encapsulation  Status        Native vlan
Gi5/8     desirable    n-802.1q       trunking      1

Port      Vlans allowed on trunk
Gi5/8 1-1005

Port      Vlans allowed and active in management domain
Gi5/8 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

Port      Vlans in spanning tree forwarding state and not pruned
Gi5/8 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

Router#
```

レイヤ 2 アクセス ポートとしての LAN インターフェイスの設定

（注）　存在しない VLAN に LAN ポートを割り当てると、VLAN データベースにその VLAN を作成するまで、LAN ポートはシャットダウンされます（「イーサネット VLAN の作成または変更」（P.25-5）を参照）。

LAN ポートをレイヤ 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	`Router(config)# interface type slot/port`	設定する LAN ポートを選択します。
ステップ 2	`Router(config-if)# shutdown`	（任意）設定が完了するまでトラフィック フローを防止するために、インターフェイスをシャットダウンします。
ステップ 3	`Router(config-if)# switchport`	LAN ポートをレイヤ 2 スイッチング用に設定します。 （注）　LAN ポートをレイヤ 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 度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さらに **switchport** コマンドを入力してください。
ステップ 4	`Router(config-if)# switchport mode access`	LAN ポートをレイヤ 2 アクセス ポートとして設定します。
ステップ 5	`Router(config-if)# switchport access vlan vlan_ID`	LAN ポートを VLAN に入れます。*vlan_ID* の値は 1 ～ 4094 です（予約済み VLAN は除く。表 25-1（P.25-3）を参照）。 （注）　VLAN のロックがイネーブルになっている場合は、VLAN の番号の代わりに VLAN の名前を入力します。詳細については、「VLAN ロック」（P.25-5）を参照してください。
ステップ 6	`Router(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ている場合に限り必要）。
ステップ 7	`Router(config-if)# end`	コンフィギュレーション モードを終了します。

次に、ギガビット イーサネット ポート 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。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 5/6
Router(config-if)# shutdown
Router(config-if)# switchport
Router(config-if)# switchport mode access
Router(config-if)# switchport access vlan 200
Router(config-if)# no shutdown
Router(config-if)# end
Router# exit
```

次に、設定を確認する例を示します。

```
Router# show running-config interface gigabitethernet 5/6
Building configuration...
!
```

```
Current configuration:
interface GigabitEthernet5/6
 no ip address
 switchport access vlan 200
 switchport mode access
end

Router# show interfaces gigabitethernet 5/6 switchport
Name: Gi5/6
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Enabled
Access Mode VLAN: 200 (VLAN0200)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: ALL

Router#
```

カスタム IEEE 802.1Q EtherType フィールド値の設定

802.1Q タグ付きまたは 802.1p タグ付きフレームの標準 0x8100 EtherType フィールド値を使用しないネットワーク デバイスをサポートするように、ポートでカスタム EtherType フィールド値を設定できます。

EtherType フィールドのカスタム値を設定するには、次の作業を行います。

コマンド	目的
`Router(config-if)# switchport dot1q ethertype value`	ポートの 802.1Q EtherType フィールド値を設定します。

カスタム EtherType フィールド値の設定時には、以下に注意してください。

- カスタム EtherType フィールド値を使用するには、ネットワーク上のトラフィック パス内のネットワーク デバイスすべてがカスタム EtherType フィールド値をサポートする必要があります。
- トランク ポート、アクセス ポート、トンネル ポート上のカスタム EtherType フィールド値を設定できます。
- EtherChannel のメンバ ポート上のカスタム EtherType フィールド値を設定できます。
- ポートチャネル インターフェイス上では、カスタム EtherType フィールド値を設定できません。
- ポートごとに、EtherType フィールド値 1 つだけをサポートします。カスタム EtherType フィールド値で設定されたポートでは、他の EtherType フィールド値を持つフレームはタグ付きフレームとして認識されません。たとえば、カスタム EtherType フィールド値で設定されたトランク ポートでは、802.1Q タグ付きフレームの標準 0x8100 EtherType フィールド値は認識されず、このフレームが属する VLAN にフレームを配置することができません。

注意　カスタム EtherType フィールド値で設定されたポートは、他の EtherType フィールド値を持つフレームをタグなしのフレームと見なします。カスタム EtherType フィールド値を持つトランク ポートは、他の EtherType フィールド値を持つフレームをネイティブ VLAN に配置します。カスタム

EtherType フィールド値を持つアクセス ポートまたはトンネル ポートは、他の EtherType フィールド値を持つフレームをアクセス VLAN に配置します。カスタム EtherType フィールド値を正しく設定しないと、フレームは間違った VLAN に配置される場合があります。

- カスタム IEEE802.1Q EtherType フィールド値をサポートするモジュールの一覧については、『*Release Notes for Cisco IOS Release 15.1SY*』を参照してください。

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/15.1SY/release_notes.html

次に、EtherType フィールド値を 0x1234 に設定する例を示します。

```
Router (config-if)# switchport dot1q ethertype 1234
Router (config-if)#
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CHAPTER 21

Flex Link

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

Flex Link の前提条件

なし。

Flex Link の制約事項

- アクティブ リンクには、Flex Link バックアップ リンクを 1 つだけ設定できます。バックアップ リンクは、アクティブ インターフェイスとは異なるインターフェイスにする必要があります。
- インターフェイスは 1 つの Flex Link ペアだけに属します。インターフェイスは、1 つだけのアクティブ リンクのバックアップ リンクにすることができます。アクティブ リンクは、別の Flex Link ペアに属することができません。
- どちらのリンクも、EtherChannel に属するポートには設定できません。ただし、2 つのポート チャネル（EtherChannel 論理インターフェイス）を Flex Link として設定でき、ポート チャネルおよび物理インターフェイスを Flex Link として設定して、ポート チャネルか物理インターフェイスのどちらかをアクティブ リンクにすることができます。
- バックアップ リンクを、アクティブ リンクと同じタイプにする必要はありません（ファスト イーサネット、ギガビット イーサネット、ポート チャネルのいずれか）。ただし同様の特性で両方の Flex Link を設定し、スタンバイ リンクがアクティブになった場合に、操作のループや変更が発生しないようにする必要があります。
- Flex Link ポートでは STP がディセーブルになります。スイッチで STP をディセーブルにする場合は、ネットワーク トポロジーにレイヤ 2 ループがないことを確認してください。
- Flex Link ポート、またはそのリンクの接続先ポートでは、STP 機能（PortFast、BPDU ガードなど）を設定しないでください。
- プリエンプションはリンク障害と見なされないため、ローカルで管理上のシャットダウンを行わないとリンクは再度フォワーディングを開始します。このような場合、この機能によりダイナミック ホストはフラッシュされ、移動されません。
- プライマリ リンクに設定されたスタティック MAC アドレスはスタンバイ リンクに移動されません。
- Flex Link ポートが再度フォワーディングとなった場合は、これに設定されているスタティック MAC アドレスを元に戻します。

Flex Link について

Flex Link は、レイヤ 2 インターフェイス（ポートまたはポート チャネル）のペアで、一方のインターフェイスが他方のインターフェイスのバックアップとして機能するように設定されています。Flex Link は、カスタマーが STP を実行しないサービス プロバイダー ネットワークまたはエンタープライズ ネットワークで一般的に設定します。Flex Link では、スパニングツリー プロトコル（STP）の代替手段であるリンクレベルの冗長性が提供されます。Flex Link インターフェイスでは、STP が自動的にディセーブルになります。

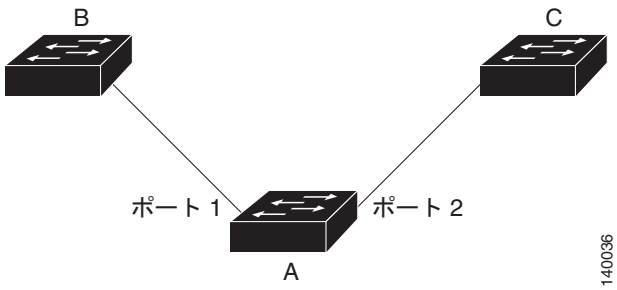
リリース 15.1SY は、最大 16 の Flex Link をサポートします。Flex Link はレイヤ 2 ポートおよびポート チャネルだけでサポートされ、VLAN またはレイヤ 3 ポートではサポートされません。

Flex Link 機能を設定するには、プライマリにするリンクのスタンバイ リンクとして、1 つのレイヤ 2 インターフェイスを設定します。インターフェイスのペアに Flex Link を設定すると、片方のインターフェイスだけがリンクアップ状態になり、トラフィックを転送します。プライマリ リンクがシャットダウンされると、スタンバイ リンクがトラフィックの転送を始めます。アクティブでないリンクがアップに戻ると、そのリンクはスタンバイ モードになります。

図 21-1 では、スイッチ A のポート 1 およびポート 2 がアップリンク スイッチ B およびアップリンク スイッチ C に接続されています。これは Flex Link として設定されているので、片方のインターフェイスだけがトラフィックを転送し、他方のインターフェイスはスタンバイ モードになります。ポート 1 がアクティブ リンクになる場合、ポート 1 とスイッチ B との間でトラフィックの転送を開始し、ポー

ト 2（バックアップ リンク）とスイッチ C との間のリンクでは、トラフィックは転送されません。ポート 1 がダウンした場合はポート 2 がアップし、トラフィックをスイッチ C に転送し始めます。ポート 1 は、アップに戻るとスタンバイ モードになり、トラフィックを転送しません。ポート 2 がトラフィックの転送を続けます。

図 21-1　　Flex Link の設定例



プライマリ（転送）リンクがダウンすると、トラップによってネットワーク管理ステーションが通知を受けます。スタンバイ リンクがダウンすると、トラップがユーザに通知します。プライマリ リンクに障害が発生すると、この機能は次のアクションを実行します。

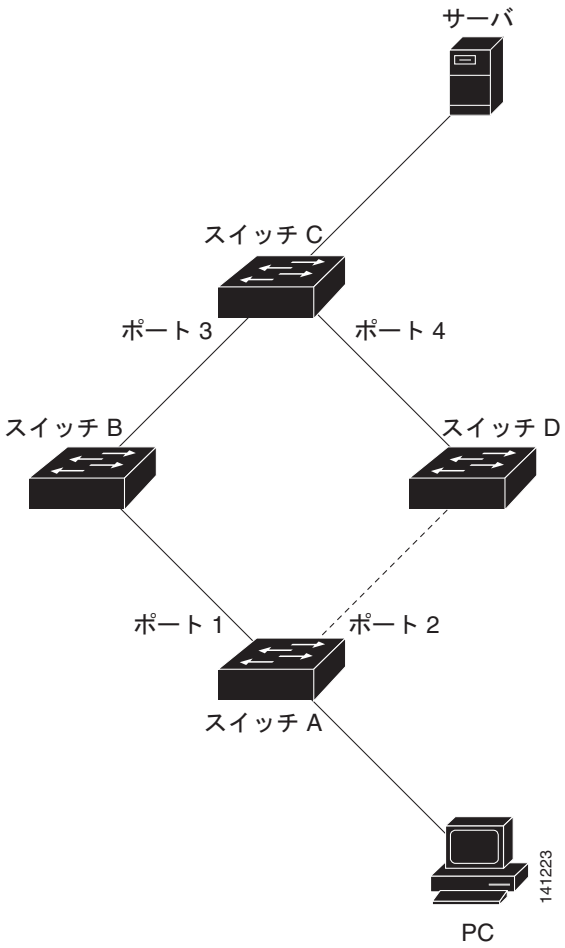
- 障害を検出します。
- プライマリ リンクで学習されたダイナミック ユニキャスト MAC アドレスをスタンバイ リンクに移行します。
- スタンバイ リンクをフォワーディング ステートに移行させます。
- 新しいアクティブ インターフェイス経由でダミーのマルチキャスト パケットを送信します。ダミーのマルチキャスト パケットのフォーマットは、次のとおりです。
  - 宛先：01:00:0c:cd:cd:cd
  - 送信元：新しいアクティブ Flex Link ポートのホストまたはポートの MAC アドレス。

  図 21-2 では、スイッチ A のポート 1 と 2 は Flex Link のペアを介してスイッチ B と D に接続しています。ポート 1 はトラフィックを転送していて、ポート 2 はブロッキング ステートです。PC からサーバへのトラフィックはポート 1 からポート 3 に転送されます。PC の MAC アドレスが、スイッチ C のポート 3 で学習されています。サーバから PC へのトラフィックはポート 3 からポート 1 に転送されます。

  ポート 1 がシャットダウンすると、ポート 2 がトラフィックの転送を開始します。ポート 2 へのフェールオーバー後に PC からサーバへのトラフィックがない場合、スイッチ C はポート 4 で PC の MAC アドレスを学習しません。このため、スイッチ C はポート 3 からサーバのトラフィックを PC に転送し続けます。ポート 1 がダウンしているため、サーバから PC へのトラフィックが消失します。この問題を軽減するため、この機能は、PC の送信元 MAC アドレスを持つダミーのマルチキャスト パケットをポート 2 経由で送信します。スイッチ C はポート 4 の PC の MAC アドレスを学習して、サーバから PC へのトラフィックの転送をポート 4 を経由して開始します。1 つのダミーのマルチキャスト パケットがすべての MAC アドレスに向けて送信されます。

Flex Link インターフェイスのプリエンプションでは、トラフィック転送に関する優先として、Flex Link のペアのいずれかのポートを指定します。プリファレンスは無条件とするか、または帯域幅の可用性に基づくようにできます。「Flex Link の設定方法」（P.21-4）を参照してください。

図 21-2　Flex Link のダミーのマルチキャスト パケットの例



Flex Link のデフォルト設定

- Flex Link：設定されません。
- Flex Link インターフェイスのプリエンプション：設定されません。
- Flex Link インターフェイスのプリエンプション遅延：35 秒。

Flex Link の設定方法

Flex Link 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# 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	`Router(conf)# interface {{type slot/port} | {port-channel number}}`	レイヤ 2 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	`Router(conf-if)# switchport backup interface interface_id`	Flex Link ペアの一部としてインターフェイスを設定します。 • *interface_id* では、物理ポートまたはポートチャネル インターフェイスを指定できます。 • バックアップ インターフェイスは、あらかじめレイヤ 2 ポートとして設定する必要があります。
ステップ 4	`Router(conf-if)# switchport backup interface interface_id preemption mode [forced | bandwidth | off]`	（任意）Flex Link ペアの優先 Flex Link インターフェイスのプリエンプション ポートを設定します。 • *interface_id* では、物理ポートまたはポートチャネル インターフェイスを指定できます。 • **forced**：アクティブ インターフェイスは常に、バックアップをプリエンプトします。 • **bandwidth**：より高い帯域幅を持つインターフェイスが常に、アクティブ インターフェイスとして動作します。 • **off**：アクティブからバックアップへのプリエンプトは発生しません。
ステップ 5	`Router(conf-if)# switchport backup interface interface_id preemption delay delay_time`	（任意）Flex Link ペアの Flex Link インターフェイスのプリエンプション遅延時間を設定します。 • *interface_id* では、物理ポートまたはポートチャネル インターフェイスを指定できます。 • delay_time の範囲は 1 ～ 300 秒です。
ステップ 6	`Router(conf-if)# exit`	コンフィギュレーション モードを終了します。

次に、Flex Link バックアップ インターフェイスでインターフェイスを設定して、設定を確認する例を示します。

```
Router# configure terminal
Router(conf)# interface tengigabitethernet 2/9
Router(conf-if)# switchport backup interface tengigabitethernet 2/12
Router(conf-if)# switchport backup interface tengigabitethernet 2/12 preemption mode
[forced | bandwidth | off]
Router(conf-if)# switchport backup interface tengigabitethernet 2/12 preemption delay 35
Router(conf-if)# exit
Router# show interface switchport backup detail

Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
Te2/9                   Te2/12                  Active Up/Backup Standby
Interface Pair   : Te2/9, Te2/12
Preemption Mode  : forced
Preemption Delay : 35 seconds (default)
Bandwidth : 10000000 Kbit (Te2/9), 10000000 Kbit (Te2/12)
```

Flex Link のモニタ

Flex Link の設定をモニタするには、次の作業を行います。

コマンド	目的
show interface [{*type slot/port*} | {**port-channel** *number*}] **switchport backup**	あるインターフェイス用に設定された Flex Link バックアップ インターフェイス、またはスイッチ上で設定されたすべての Flex Link と、各アクティブおよびバックアップ インターフェイスの状態（アップまたはスタンバイ モード）を表示します。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

EtherChannel

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

EtherChannel の前提条件

なし。

EtherChannel の制約事項

- LACP EtherChannel と 802.1ad プロバイダー ブリッジ モードは相互に排他的です。802.1ad プロバイダー ブリッジ モードがイネーブルの場合、LACP EtherChannel はトラフィックを送信できません。
- LACP EtherChannel の両端で LACP 1:1 冗長性をイネーブルにする必要があります。
- LACP は半二重リンクをサポートしていません。LACP EtherChannel 内の半二重リンクは中断ステートになります。

注意　手動モードと LACP モードが混在していたり、EtherChannel の一部として設定されていないポートに EtherChannel メンバ ポートを接続することにより、深刻なトラフィックの問題を引き起こす場合があります。たとえば、**on** モードで設定されたポートを、**desirable** モードで設定されたポート、または EtherChannel のメンバとして設定されていないポートに接続した場合、ブリッジ ループが発生し、ブロードキャスト ストームが起きる可能性があります。一方の端が **on** モードを使用する場合は、もう一方の端も同じモードを使用する必要があります。

- EtherChannel インターフェイスを正しく設定しないと、ネットワーク ループなどの問題を回避するために、一部の EtherChannel インターフェイスが自動的にディセーブルになることがあります。
- SAP/SNAP カプセル化を使用したフレームは、レイヤ 2 トラフィックとしてロード バランシングされます。
- この章で説明するコマンドは、スーパーバイザ エンジンおよび冗長スーパーバイザ エンジンのポートも含めて、すべてのレイヤ 2 イーサネット ポートに対して使用できます。
- 冗長スーパーバイザ エンジン上のポートも含め、すべてのモジュール上のすべてのレイヤ 2 イーサネット ポートが、EtherChannel（最大 8 つの LAN ポート）をサポートします。これらの LAN ポートは、物理的に隣接している LAN ポートでなくても、また同じモジュール上の LAN ポートでなくてもかまいません。
- 同じ EtherChannel プロトコルを使用するように EtherChannel 内のすべての LAN ポートを設定します。1 つの EtherChannel 内で 2 つの EtherChannel プロトコルの実行はできません。
- EtherChannel 内のすべての LAN ポートが、同じ速度および同じデュプレックス モードで動作するように設定してください。
- EtherChannel のすべての LAN ポートをイネーブルにしてください。EtherChannel 内の LAN ポートを 1 つシャットダウンすると、リンク障害として扱われ、そのポートのトラフィックが EtherChannel 内の残りのポートの 1 つに転送されます。
- いずれかの LAN ポートがスイッチド ポート アナライザ（SPAN）宛先ポートである場合には、EtherChannel は形成されません。
- レイヤ 3 EtherChannel の場合は、チャネル内の LAN ポートに対してではなく、ポート チャネル論理インターフェイスに対してレイヤ 3 アドレスを割り当ててください。
- レイヤ 2 EtherChannel の場合
  - EtherChannel 内のすべての LAN ポートを同じ 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。
  - トランキング LAN ポートから EtherChannel を設定する場合は、すべてのトランクでトランキング モードが同じであることを確認してください。EtherChannel 内の LAN ポートをそれぞれ異なるトランク モードに設定すると、予期しない結果が生じる可能性があります。
  - EtherChannel は、トランキング レイヤ 2 EtherChannel 内のすべての LAN ポートで同じ許容範囲の VLAN をサポートします。VLAN の許容範囲が異なる場合、LAN ポートは EtherChannel を形成しません。

  - STP ポート パス コストが異なる LAN ポートは、設定に互換性がある限り、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、LAN ポートが EtherChannel を形成できなくなるわけではありません。
  - プロトコル フィルタリングの設定が LAN ポートで異なっている場合には、EtherChannel を形成できません。
  - EtherChannel でだけスタティック MAC アドレスを設定し、EtherChannel の物理メンバ ポートでは設定しません。
- EtherChannel の設定後は、ポート チャネル インターフェイスに適用した設定が EtherChannel に作用します。LAN ポートに適用した設定は、設定を適用した LAN ポートだけに作用します。
- Cisco IOS Release 15.1SY は、ISL トランク カプセル化をサポートしません。非トランキング レイヤ 2 EtherChannel に、ISL トランク カプセル化に対応していないメンバ ポートが含まれている場合、**switchport trunk encapsulation dot1q** コマンドはポートチャネル インターフェイスに追加されます。switchport mode が「access」の場合、このコマンドによる影響はありません（CSCta45114）。
- QoS がイネーブルであれば、**no platform qos channel-consistency** ポートチャネル インターフェイス コマンドを入力し、完全プライオリティ キューのあるポートと完全プライオリティ キューのないポートを持つ EtherChannel をサポートします。

EtherChannel について

EtherChannel 機能の概要

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することによって、最大 8 つの物理リンクを合計した帯域幅を提供します。

Cisco IOS Release 15.1SY は、最大 128 の EtherChannel をサポートします。任意のスイッチング モジュール上の（設定に互換性のある）LAN ポートを 8 つまで使用して、1 つの EtherChannel を形成できます。各 EtherChannel の LAN ポートは、すべて同じ速度で、レイヤ 2 ポートまたはレイヤ 3 LAN ポートのどちらか一方として設定されている必要があります。

（注）　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 にバンドルできるポート数が制限される場合があります。

EtherChannel 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 EtherChannel 内の残りのセグメントに切り替えられます。障害が発生した場合、EtherChannel 機能はスイッチ、EtherChannel、および障害リンクを識別するトラップを送信します。EtherChannel の 1 つのセグメントに着信したブロードキャストおよびマルチキャスト パケットが、EtherChannel の別のセグメントに戻されることはありません。

EtherChannel の設定情報

EtherChannel の設定の概要

EtherChannel を形成するには、EtherChannel を手動で設定するか、Port Aggregation Control Protocol（PAgP）または Link Aggregation Control Protocol（LACP）を使用します。EtherChannel プロトコルを使用すると、接続先のネットワーク デバイスとダイナミックにネゴシエーションを行うことにより、同様な特性を持つポートが EtherChannel を形成できます。PAgP はシスコ システムズ独自のプロトコルであり、LACP は IEEE 802.3ad で定義されたプロトコルです。

PAgP および LACP はお互いに相互運用しません。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 を形成できません。LACP を使用するように設定されたポートは、PAgP を使用するように設定されたポートと EtherChannel を形成できません。どちらのポートも、手動で設定したポートとは相互運用しません。

表 22-1 に、ユーザ側で設定変更可能の EtherChannel モードを示します。

表 22-2 に、EtherChannel メンバ ポート ステートの一覧を示します。

表 22-1　EtherChannel のモード

モード	説明
on	LAN ポートを無条件かつ強制的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だけ、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、ポート間にネゴシエーション トラフィックは発生しません。EtherChannel プロトコルでは、**on** モードを設定できません。一方の端が **on** モードを使用する場合は、もう一方の端も同じモードを使用する必要があります。
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 （デフォルト）
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、LACP ネゴシエーションは開始しません （デフォルト）
active	ポートをアクティブ ネゴシエーション ステートにする LACP モード。この場合ポートでは LACP パケットを送信することにより、他のポートとのネゴシエーションが開始されます。

表 22-2　EtherChannel メンバ ポート ステート

ポート ステート	説明
bundled	ポートは EtherChannel の一部であり、BPDU およびデータ トラフィックを送受信できます。
suspended	ポートは EtherChannel の一部ではありません。ポートは BPDU を受信できますが、送信はできません。データ トラフィックはブロックされます。
standalone	ポートは EtherChannel にバンドルされていません。ポートはスタンドアロン データ ポートとして機能します。ポートは BPDU とデータ トラフィックを送受信できます。 （注）　EtherChannel の一方の終端に他方よりも多くのメンバがある場合、一致しないポートはスタンドアロン ステートになります。スパニングツリー プロトコル（STP）によるレイヤ 2 ループから保護されないトポロジでは、standalone ステートのポートが重大なネットワーク エラーを発生させることがあります。インターフェイス コンフィギュレーション モード コマンド **port-channel standalone-disable** を入力すると、ポートをスタンドアロン状態ではなく中断状態にすることができます。「LACP ポートチャネル スタンドアロン ディセーブルの設定」（P.22-17）を参照してください。

EtherChannel の手動設定に関する情報

手動設定された 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 の設定に関する情報

PAgP を使用すると、LAN ポート間で PAgP パケットを交換することにより、EtherChannel を自動的に作成できます。PAgP パケットが交換されるのは、**auto** モードおよび **desirable** モードのポート間に限られます。

このプロトコルは、LAN ポート グループの機能をダイナミックに学習し、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。作成された EtherChannel は、単一ブリッジ ポートとしてスパニングツリーに追加されます。

auto モードおよび **desirable** モードでは、PAgP は LAN ポート間でネゴシエーションを行い、ポート速度、トランキング ステートなどの一定の基準に従って EtherChannel を形成できるかどうかを判別します。レイヤ 2 EtherChannel は VLAN 番号も使用します。

LAN ポート間で PAgP モードが異なっていても、モードが矛盾しない限り EtherChannel を形成できます。たとえば、次のように入力します。

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

IEEE 802.3ad LACP EtherChannel の設定に関する情報

LACP では、LAN ポート間で LACP パケットを交換することによる、EtherChannel の自動作成をサポートしています。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 グループの機能をダイナミックに学習し、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。作成された EtherChannel は、単一ブリッジ ポートとしてスパニング ツリーに追加されます。

passive モードおよび **active** モードでは、LACP は LAN ポート間でネゴシエーションを行い、ポート速度、トランキング ステートなどの一定の基準に従って EtherChannel を形成できるかどうかを判別します。レイヤ 2 EtherChannel は VLAN 番号も使用します。

LAN ポート間で LACP モードが異なっていても、モードが矛盾しない限り EtherChannel を形成できます。たとえば、次のように入力します。

- **active** モードの LAN ポートは、**active** モードの別の LAN ポートと EtherChannel を形成できます。
- **active** モードの LAN ポートは、**passive** モードの別の LAN ポートと EtherChannel を形成できます。
- **passive** モードの LAN ポートは、どちらのポートもネゴシエーションを開始しないので、**passive** モードの別の LAN ポートとは EtherChannel を形成できません。

LACP では次のパラメータが使用されます。

- LACP システム プライオリティ：LACP を実行するスイッチごとに LACP システム プライオリティを設定する必要があります。システム プライオリティは自動設定、または CLI から設定できます（「LACP のシステム プライオリティおよびシステム ID の設定」（P.22-11）を参照）。LACP は、システム プライオリティとスイッチの MAC 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たポートごとに、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設定、または CLI から設定できます（「チャネル グループの設定」（P.22-9）を参照）。LACP では、ポート プライオリティおよびポート番号によりポート ID が構成されます。ハードウェアの制限により互換性のあるすべてのポートを集約できない場合、LACP はポート プライオリティを使用して、スタンバイ モードにする必要があるポートを決定します。
- LACP 管理キー：LACP は、LACP を使用するように設定されたポートごとに、チャネル グループ ID 番号と同じ管理キー値を自動的に設定します。管理キーにより、他のポートとともに集約されるポートの機能が定義されます。他のポートとの集約を行うポートの能力は、次の要因によって決まります。
  - データ レート、デュプレックス機能、ポイントツーポイント型や共有型メディアなどのポートの物理特性
  - ユーザが作成した設定に関する制約事項

LACP を使用するように設定されたポート上で、LACP は EtherChannel 内の互換性のあるポートの最大数を、ハードウェアで許容されている最大数（8 ポート）以下の値で設定しようとします。互換性のあるすべてのポートを LACP が集約できない場合（たとえば、リモート システムのハードウェア制限

が厳しい場合）、チャネルにアクティブに追加できないすべてのポートはホット スタンバイ ステートになり、チャネル ポートのいずれかに障害が発生した場合だけ使用されます。さらに 8 個のスタンバイ ポートを設定できます（EtherChannel には合計 16 個のポートが関連付けられます）。

LACP 1:1 冗長性に関する情報

LACP 1:1 冗長性機能では、ホットスタンバイ リンクへのファスト スイッチオーバーとアクティブ リンク 1 つによる EtherChannel 設定がサポートされます。ポート プライオリティ番号が小さい（つまり、プライオリティの高い）方のポートに接続されたリンクがアクティブ リンクになり、もう一方のリンクはホット スタンバイ ステートになります。アクティブ リンクがダウンした場合、LACP はホット スタンバイ リンクへのファスト スイッチオーバーを実行して、EtherChannel のアップ状態を維持します。障害が発生したリンクが再度動作可能になると、LACP は、もう一度ファスト スイッチオーバーを実行して元のアクティブ リンクに戻します。

高プライオリティ / 低プライオリティ スイッチオーバー後にポートが再度アクティブになった際に、プライオリティが高いポートを安定させるため、LACP の 1:1 のホット スタンバイ ダンプニング機能では、ポートがアクティブになった後のプライオリティが高いポートへのスイッチオーバーを遅らせるタイマーが設定されます。

「LACP 1:1 冗長性の設定」（P.22-15）を参照してください。

ポート チャネル インターフェイスに関する情報

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。1 ～ 256 の番号のポートチャネル インターフェイスを最大 128 個設定できます。ポート チャネル インターフェイスに適用した設定の内容は、そのポート チャネル インターフェイスに割り当てられたすべての LAN ポートに反映されます。

EtherChannel を設定すると、ポート チャネル インターフェイスに適用した設定は、EtherChannel に作用します。一方、LAN ポートに適用した設定は、適用先の LAN ポートだけに作用します。EtherChannel のすべてのポートのパラメータを変更する場合は、スパニングツリー プロトコル（STP）コマンドまたはレイヤ 2 EtherChannel をトランクとして設定するコマンドなどのコンフィギュレーション コマンドをポート チャネル インターフェイスに適用します。

ロード バランシングに関する情報

EtherChannel は、フレーム内のアドレスに基づいて形成されたバイナリ パターンの一部を、チャネル内の 1 つのリンクを選択する数値に変換することによって、EtherChannel 内のリンク間でトラフィックの負荷を分散させます。

EtherChannel のロードバランスには、MAC アドレスまたは IP アドレスを使用できます。EtherChannel のロードバランスにはレイヤ 4 ポート番号も使用できます。EtherChannel のロードバランスには、送信元と宛先のいずれか、または送信元と宛先の両方のアドレス、またはポートを使用できます。選択したモードは、スイッチ上で設定されているすべての EtherChannel に適用されます。EtherChannel のロードバランスは、MPLS レイヤ 2 情報を使用します。

使用している設定で最も多様なバランス基準を提供するオプションを使用してください。たとえば、EtherChannel 上のトラフィックが 1 つの MAC アドレスにだけ送信され、かつ EtherChannel ロードバランスの基準として宛先 MAC アドレスを使用している場合、EtherChannel は常に EtherChannel 内の同じリンクを選択します。IP アドレスの送信元アドレスを使用すると、ロードバランスが向上することがあります。

EtherChannel のデフォルト設定

なし。

EtherChannel の設定方法

- 「レイヤ 3 EtherChannel のポート チャネル論理インターフェイスの設定」（P.22-8）
- 「チャネル グループの設定」（P.22-9）
- 「LACP のシステム プライオリティおよびシステム ID の設定」（P.22-11）
- 「EtherChannel ロード バランシングの設定」（P.22-12）
- 「EtherChannel のハッシュ分散アルゴリズムの設定」（P.22-13）
- 「EtherChannel Min-Links 機能の設定」（P.22-14）
- 「LACP 1:1 冗長性の設定」（P.22-15）
- 「LACP ポート チャネルの自動インターリーブ ポート プライオリティの設定」（P.22-16）
- 「LACP ポートチャネル スタンドアロン ディセーブルの設定」（P.22-17）

（注）　LAN ポートが正しく設定されていることを確認してください（「EtherChannel の制約事項」（P.22-2）を参照）。

レイヤ 3 EtherChannel のポート チャネル論理インターフェイスの設定

（注）

- レイヤ 2 EtherChannel を設定する場合は、手動で作成したポート チャネル論理インターフェイスにレイヤ 2 LAN ポートを追加できません。レイヤ 2 EtherChannel を設定する場合、ここで説明する作業は行わないでください（「チャネル グループの設定」（P.22-9）を参照）。
- レイヤ 3 EtherChannel を設定する場合は、ここに記載されたポート チャネル論理インターフェイスを手動で作成し、レイヤ 3 LAN ポートをチャネル グループに追加する必要があります（「チャネル グループの設定」（P.22-9）を参照）。
- レイヤ 3 LAN ポートから EtherChannel に IP アドレスを移動するには、レイヤ 3 LAN ポートから IP アドレスを削除したあとで、その IP アドレスをポート チャネル論理インターフェイス上で設定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	`Router(config)# interface port-channel group_number`	ポート チャネル インターフェイスを作成します。
ステップ 2	`Router(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	`Router(config-if)# end`	コンフィギュレーション モードを終了します。

group_number は 1 ～ 256 を指定でき、最大 128 のポートチャネル インターフェイスを作成できます。次に、インターフェイス Port-channel 1 を作成する例を示します。

```
Router# configure terminal
Router(config)# interface port-channel 1
Router(config-if)# ip address 172.32.52.10 255.255.255.0
Router(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。

```
Router# 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
Router#
```

チャネル グループの設定

（注）

- レイヤ 3 EtherChannel を設定する場合は、ポート チャネル論理インターフェイスを手動で作成してから（「レイヤ 3 EtherChannel のポート チャネル論理インターフェイスの設定」（P.22-8）を参照）、ここに記載されているように、レイヤ 3 LAN ポートをチャネル グループに追加する必要があります。
- レイヤ 2 EtherChannel を設定するには、ここに記載されているように、ポート チャネル論理インターフェイスを自動作成する **channel-group** コマンドを使用して、LAN ポートを設定します。手動で作成したポート チャネル インターフェイスにレイヤ 2 LAN ポートを組み込むことはできません。
- Cisco IOS がレイヤ 2 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、レイヤ 2 LAN ポートが接続され、動作している必要があります。

チャネル グループを設定するには、LAN ポートごとに次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface` *type slot/port*	設定する LAN ポートを選択します。
ステップ 2	`Router(config-if)# no ip address`	この LAN ポートに 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 3	`Router(config-if)# channel-protocol {lacp | pagp}`	（任意）選択した LAN ポート上で、**channel-group** コマンドの適用範囲を、**channel-protocol** コマンドを使用して設定された EtherChannel プロトコルに制限します。
ステップ 4	`Router(config-if)# channel-group` *group_number* `mode {active | auto | desirable | on | passive}`	ポートチャネル内の LAN ポートを設定し、モードを指定します（表 22-1（P.22-4）を参照）。PAgP は、auto および desirable モードだけをサポートします。LACP は、active および passive モードだけをサポートします。

	コマンド	目的
ステップ 5	`Router(config-if)# lacp port-priority priority_value`	（任意：LACP 用）有効な値は 1 ～ 65535 です。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。
ステップ 6	`Router(config-if)# end`	コンフィギュレーション モードを終了します。

次に、ギガビット イーサネット ポート 5/6 および 5/7 を、PAgP モードが **desirable** のポートチャネル 2 に設定する例を示します。

```
Router# configure terminal
Router(config)# interface range gigabitethernet 5/6 -7
Router(config-if)# channel-group 2 mode desirable
Router(config-if)# end
```

（注）　**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を設定する方法」（P.10-2）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。

```
Router# show running-config interface port-channel 2
Building configuration...

Current configuration:
!
interface Port-channel2
 no ip address
 switchport
 switchport access vlan 10
 switchport mode access
end
Router#
```

次に、ギガビット イーサネット ポート 5/6 の設定を確認する例を示します。

```
Router# show running-config interface gigabitethernet 5/6
Building configuration...

Current configuration:
!
interface GigabitEthernet5/6
 no ip address
 switchport
 switchport access vlan 10
 switchport mode access
 channel-group 2 mode desirable
end
Router# show interfaces gigabitethernet 5/6 etherchannel
Port state    = Down Not-in-Bndl
Channel group = 12          Mode = Desirable-Sl     Gcchange = 0
Port-channel  = null        GC   = 0x00000000          Pseudo port-channel = Po1
2
Port index    = 0           Load = 0x00        Protocol =   PAgP

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
Port      Flags State   Timers  Interval Count   Priority   Method  Ifindex
Gi5/2     d     U1/S1           1s       0        128        Any      0

Age of the port in the current state: 04d:18h:57m:19s
```

次に、LAN ポートを設定したあとに、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。

```
Router# show etherchannel 12 port-channel
               Port-channels in the group:
               ----------------------

Port-channel: Po12
------------

Age of the Port-channel   = 04d:18h:58m:50s
Logical slot/port   = 14/1          Number of ports = 0
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel Ag-Not-Inuse
Protocol            =   PAgP

Router#
```

LACP のシステム 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	`Router(config)# lacp system-priority value`	（任意：LACP 用）有効な値は 1 ～ 65535 です。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。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

次に、LACP のシステム プライオリティを設定する例を示します。

```
Router# configure terminal
Router(config)# lacp system-priority 23456
Router(config)# end
Router(config)#
```

次に、設定を確認する例を示します。

```
Router# show lacp sys-id
23456,0050.3e8d.6400
Router#
```

システム プライオリティが最初に表示され、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

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	`Router(config)# port-channel per-module load-balance`	（任意）モジュール単位で、ロード バランシングの方式を指定する機能を有効にします。
ステップ 2	`Router(config)# port-channel load-balance {src-mac | dst-mac | src-dst-mac | src-ip | dst-ip | src-dst-ip | src-port | dst-port | src-dst-port} [module slot]`	EtherChannel ロード バランシングの方式を設定します。この方式はすべてのポート チャネルにグローバルに適用されます。任意で、特定のモジュールにロード バランシングの方式を設定することもできます。デフォルトの方式は src-dst-ip です。 **（注）** • VSS モードになっていないスイッチで EtherChannel ロード バランスを設定した場合、EtherChannel メンバー ポートがシャットダウン ステートに遷移し、次いで、非シャットダウン ステートに遷移する間、トラフィックは中断されます。 • VSS モードのスイッチに中断はありません。
ステップ 3	`Router(config)# end`	コンフィギュレーション モードを終了します。

ロード バランシング方式のキーワードの意味は、次のとおりです。

- **dst-ip**：宛先 IP アドレス
- **dst-mac**：宛先 MAC アドレス
- **dst-port**：宛先レイヤ 4 ポート
- **mpls**：MPLS パケットのロード バランシング
- **src-dst-ip**：（デフォルト）送信元および宛先 IP アドレス
- **src-dst-mac**：送信元および宛先の MAC アドレス
- **src-dst-port**：送信元および宛先のレイヤ 4 ポート
- **src-ip**：送信元の IP アドレス
- **src-mac**：送信元の MAC アドレス
- **src-port**：送信元のレイヤ 4 ポート

module キーワード（任意）を指定すると、ロード バランシング方式を特定のモジュールに対して指定できます。この機能は、DFC を装備したスイッチング モジュールでだけサポートされています。この機能をモジュールに設定する前に、モジュールごとのロード バランシングをグローバルに有効化する必要があります。

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。

```
Router# configure terminal
Router(config)# port-channel load-balance src-dst-ip
Router(config)# end
Router(config)#
```

次に、設定を確認する例を示します。

```
Router# show etherchannel load-balance
Source XOR Destination IP address
```

```
Router#
```

EtherChannel のハッシュ分散アルゴリズムの設定

EtherChannel にポートを追加したり、EtherChannel からポートを削除したりする場合、固定アルゴリズムにより、EtherChannel 内の各ポートのポート ASIC が更新されますが、更新時、各ポートが短時間停止します。

デフォルトの適合アルゴリズムでは、既存のメンバ ポートに対してポート ASIC を更新する必要がありません。適合アルゴリズムに対し、グローバルな値を設定できます。また、個々のポート チャネルにアルゴリズムを指定できます。

アルゴリズムを変更した場合、変更は次のメンバ リンク イベント（link down、link up、addition、deletion、no shutdown、および shutdown）から適用されます。アルゴリズムを変更するコマンドを入力すると、次のメンバ リンク イベントまでコマンドが反映されないという警告がコマンド コンソールで発行されます。

（注）
- 外部デバイスの中には、固定アルゴリズムが必要なものもあります。たとえば、Service Control Engine（SCE）では、着信パケットと発信パケットが同じポートを使用する必要があります。
- ロード バランシングの方式を変更した場合、DFC 搭載のスイッチング モジュールまたはデュアル スーパーバイザ エンジン設定のアクティブなスーパーバイザ エンジンにおいて、EtherChannel ポートのフラップが発生します。

ハッシュ分散アルゴリズムのグローバル設定

負荷分散型アルゴリズムをグローバルに設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# port-channel hash-distribution {adaptive | fixed}`	ハッシュ分散アルゴリズムを適合または固定に設定します。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

次に、ハッシュ分散アルゴリズムを、適合アルゴリズムにグローバルに設定する例を示します。

```
Router(config)# port-channel hash-distribution adaptive
```

ポート チャネルへのハッシュ分散アルゴリズムの設定

ハッシュ分散アルゴリズムを特定のポート チャネルに設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface port-channel channel-num`	ポート チャネル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 2	`Router(config-if)# port-channel port hash-distribution {adaptive | fixed}`	このインターフェイスにハッシュ分散アルゴリズムを設定します。
ステップ 3	`Router(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。

次に、ポート チャネル 10 に対して、ハッシュ分散アルゴリズムを適合として設定する例を示します。

```
Router (config)# interface port-channel 10
Router (config-if)# port-channel port hash-distribution adaptive
```

EtherChannel Min-Links 機能の設定

EtherChannel min-links 機能は、LACP EtherChannel でサポートされています。この機能では、ポート チャネル インターフェイスがリンクアップ状態に移行するために、リンクアップ状態になって EtherChannel でバンドルされている必要があるメンバ ポートの最低数を設定できます。EtherChannel min-links 機能を使用して低帯域幅の LACP EtherChannel をアクティブにしないようにできます。また LACP EtherChannel にアクティブ メンバ ポートが少なすぎて、必要な最低帯域幅を提供できない場合、この機能により LACP EtherChannel が非アクティブになります。また、LACP の max-bundle 値を min-links と同時に指定した場合、その設定は検証され、min-links 値が max-bundle 値と適合しない（min-links 値が max-bundle 値より大きい）と、エラー メッセージが返されます。

EtherChannel min-links 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	`Router(config)# interface port-channel group_number`	LACP ポート チャネル インターフェイスを選択します。
ステップ 2	`Router(config-if)# port-channel min-links number`	ポート チャネル インターフェイスがリンクアップ状態に移行するために、リンクアップ状態になって EtherChannel でバンドルされている必要があるメンバ ポートの最低数を設定します。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。

（注）　EtherChannel min-links 機能は、EtherChannel の一端にだけ設定した場合でも正常に機能しますが、最適な結果を得るために、同じ数の最小リンクを EtherChannel の両端に設定してください。

次に、EtherChannel でアクティブなメンバ ポートが 2 つ未満の場合に、ポート チャネル インターフェイス 1 を非アクティブに設定する例を示します。

```
Router# configure terminal
Router(config)# interface port-channel 1
Router(config-if)# port-channel min-links 2
Router(config-if)# end
```

LACP 1:1 冗長性の設定

LACP 1:1 冗長性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	`Router(config)# interface port-channel group_number`	LACP ポート チャネル インターフェイスを選択します。
ステップ 2	`Router(config-if)# lacp fast-switchover`	EtherChannel の LACP 1:1 冗長性機能をイネーブルにします。
ステップ 3	`Router(config-if)# lacp max-bundle 1`	アクティブ メンバ ポートの最大数を 1 に設定します。LACP 1:1 冗長性でサポートされる値は「1」だけです。
ステップ 4	`Router(config-if)# lacp fast-switchover dampening seconds`	（任意）この EtherChannel の LACP 1:1 のホット スタンバイ ダンプニング機能をイネーブルにします。time パラメータの範囲は 35 ～ 180 秒です。
ステップ 5	`Router(config-if)# end`	コンフィギュレーション モードを終了します。

（注）　LACP EtherChannel の両端で LACP 1:1 冗長性をイネーブルにする必要があります。

この例は、1:1 冗長性機能を備えた LACP EtherChannel を設定する方法を示しています。ギガビット イーサネット ポート 5/6 は、デフォルトの 32768 より大きいポート プライオリティ番号（つまり、低いプライオリティ）で設定されるため、スタンバイ ポートになります。

```
Router# configure terminal
Router(config)# lacp system-priority 33000
Router(config)# interface range gigabitethernet 5/6 -7
Router(config-if)# channel-protocol lacp
Router(config-if)# channel-group 1 mode active
Router(config)# interface gigabitethernet 5/6
Router(config-if)# lacp port-priority 33000
Router(config)# interface port-channel 1
Router(config-if)# lacp fast-switchover
Router(config-if)# lacp max-bundle 1
Router(config-if)# lacp fast-switchover dampening 30
Router(config-if)# end
```

LACP ポート チャネルの自動インターリーブ ポート プライオリティの設定

ポート チャネルで LACP の自動インターリーブ ポート プライオリティを設定するには、ポート チャネル 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	Router(config)# **interface port-channel** *channel-group*	設定するポート チャネル インターフェイスを選択します。
ステップ 2	Router(config-if)# **lacp active-port distribution automatic**	インターリーブ ポート プライオリティを使用するポート チャネルを設定します。 **（注）** インターリーブ ポート プライオリティをイネーブルにするには、shutdown および no shutdown を実行する必要があります。
ステップ 3	Router(config-if)# **shutdown**	インターフェイスをディセーブルにします。
ステップ 4	Router(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	Router(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	Router# **show etherchannel** *channel-group* **port-channel** Router# **show etherchannel** *channel-group* **summary**	設定を確認します。

次の例では、ポート チャネルの自動インターリーブ ポート プライオリティを設定する方法を示します。

```
Router(config)# interface port-channel23
Router(config-if)# lacp active-port distribution automatic
Please shut/no shut the port-channel for configuration to take effect immediately.
Router(config-if) #shutdown
Router(config-if)# no shutdown

Router(config-if)# end
```

次に、インターフェイス Port-channel 23 の設定を確認する例を示します。

```
Router# show running interfaces port-channel23
Building configuration...

Current configuration : 81 bytes
!
interface Port-channel23
 no switchport
 no ip address
 lacp max-bundle 4
 lacp active-port distribution automatic
end
```

次に、EtherChannel 23 の設定を確認する例を示します。

```
Router# show etherchannel 23 summary

Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
```

```
        f - failed to allocate aggregator

        M - not in use, no aggregation due to minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        d - default port

        w - waiting to be aggregated
Number of channel-groups in use: 9
Number of aggregators:           9

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------
23     Po23(RU)        LACP      Gi1/1/21(P)    Gi1/1/22(P)    Gi1/1/23(H)
                                 Gi1/1/24(H)    Gi2/1/17(P)    Gi2/1/18(P)
                                 Gi2/1/19(H)    Gi2/1/20(H)

Last applied Hash Distribution Algorithm: Fixed
```

（注）　上記の例では、4 つのバンドル ポートがシャーシおよびスロットごとに 2 つ分配されています。

LACP ポートチャネル スタンドアロン ディセーブルの設定

ポート チャネルのスタンドアロン EtherChannel メンバ ポート ステートをディセーブルにするには（表 22-2（P.22-5）を参照）、ポート チャネル 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	`Router(config)# interface port-channel channel-group`	設定するポート チャネル インターフェイスを選択します。
ステップ 2	`Router(config-if)# port-channel standalone-disable`	ポートチャネル インターフェイスのスタンドアロン モードをディセーブルにします。
ステップ 3	`Router(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	`Router# show etherchannel channel-group port-channel` `Router# show etherchannel channel-group detail`	設定を確認します。

次に、ポート チャネル 42 のスタンドアロン EtherChannel メンバ ポート ステートをディセーブルにする例を示します。

```
Router(config)# interface port-channel channel-group
Router(config-if)# port-channel standalone-disable
```

次に、設定を確認する例を示します。

```
Router# show etherchannel 42 port-channel | include Standalone
Standalone Disable  = enabled
Router# show etherchannel 42 detail | include Standalone
Standalone Disable  = enabled
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CHAPTER 23

IEEE 802.1ak MVRP および MRP

（注）
- この機能は、「IEEE 802.1ak - MVRP and MRP」として Cisco Feature Navigator に表示されます。
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

IEEE 802.1ak MVRP および MRP の前提条件

なし。

IEEE 802.1ak MVRP および MRP の制約事項

- CSCta96338 が解決されないリリースでは、MVRP 設定およびイネーブル ステートがポートチャネル インターフェイスに設定されているものと異なる物理ポートは、EtherChannel のアクティブ メンバになることはできません。
- CSCta96338 が解決されるリリースでは、MVRP 設定およびイネーブル ステートがポートチャネル インターフェイスに設定されているものと異なる物理ポートは、ポートチャネル インターフェイスの MVRP 設定とイネーブル ステートを使用するため、EtherChannel のアクティブ メンバになることができます。
- 他社製のデバイスは、802.1Q トランク経由でのみシスコ デバイスと相互運用できます。
- MVRP は、それがイネーブルになっているポートで動作します。VTP プルーニングは、MVRP がイネーブルになっていないポートで実行できます。
- MVRP は物理インターフェイスと EtherChannel インターフェイスの両方で設定できますが、EtherChannel メンバ ポートではサポートされません。
- MVRP ダイナミック VLAN 作成は、デバイスが VTP サーバまたはクライアント モードで動作している場合はサポートされません。
- MVRP と接続障害管理（CFM）は共存できますが、モジュールが両方のプロトコルをサポートするのに十分な MAC アドレスのマッチ レジスタがない場合、モジュールの MVRP ポートは errdisable ステートになります。シャット ダウンされたポートを使用するには、ポート上で MVRP をディセーブルにしてから、**shutdown** および **no shutdown** コマンドを入力します。
- MVRP がポートで稼働する前、ポートがアクティブになってからダイナミック トランキング プロトコル（DTP）のネゴシエーションが開始されるまでに、802.1X 認証および許可が行われます。
- アクセス ポートで設定されたエッジ スイッチ上では、MVRP の自動 MAC アドレス ラーニングをイネーブルにしないでください。すべてのトランク インターフェイスが MVRP を実行しているコア スイッチでだけ、MVRP の自動 MAC アドレス ラーニングをイネーブルにします。
- MVRP は、レイヤ 2 トランクでのみサポートされます。MVRP はサブインターフェイスではサポートされません。

IEEE 802.1ak MVRP および MRP に関する情報

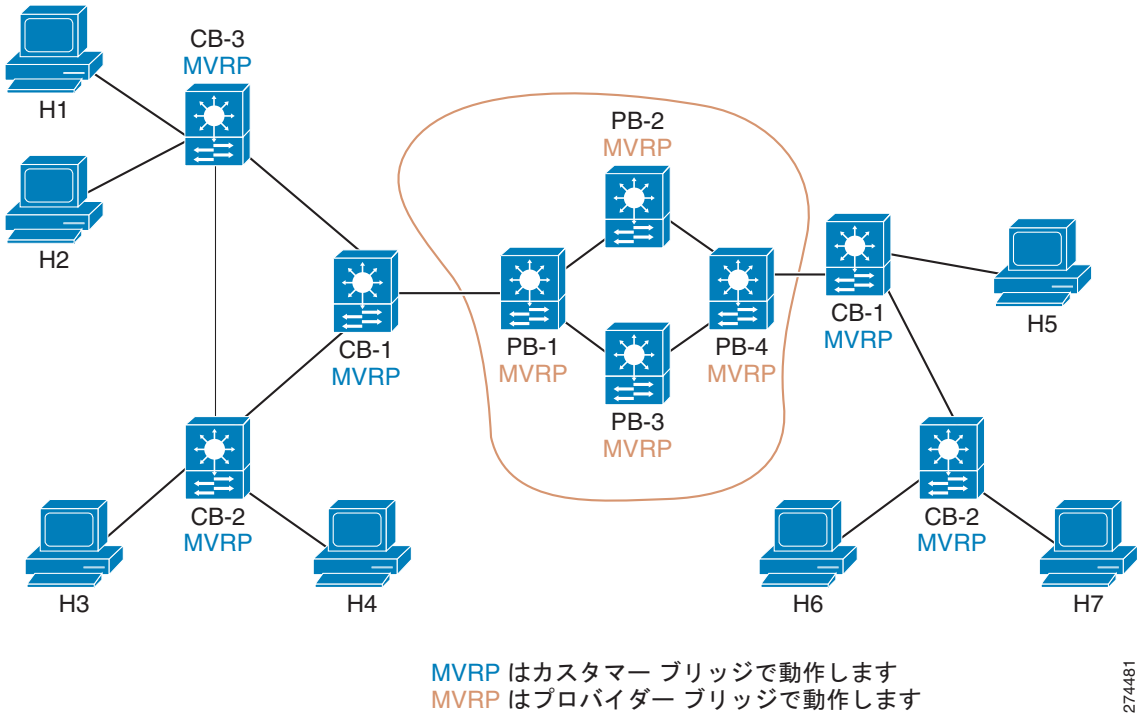
概要

IEEE 802.1ak Multiple VLAN Registration Protocol（MVRP）は、VLAN ブリッジ型ネットワークのポート上での VLAN の動的な登録および登録解除をサポートします。IEEE 802.1ak は効率的なプロトコル データ ユニット（PDU）とプロトコル設計を使用して、Generic VLAN Registration Protocol（GARP）VLAN Registration Protocol（GVRP）と GARP Multicast Registration Protocol（GMRP）プロトコルよりもパフォーマンスを向上させます。

VLAN ブリッジ型ネットワークは通常、適切なネットワーク デバイスにアクセスするためにトラフィックが使用するリンクに未知のユニキャスト、マルチキャスト、およびブロードキャスト トラフィックを制限します。大規模なネットワークでは、ローカライズされたトポロジ変更ははるかに大きいネットワーク部分上のサービスに影響を与えることがあります。IEEE 802.1ak は、GARP を Multiple Registration Protocol（MRP）に置き換えることで、リソースの使用率と帯域幅の節約を改善します。

802.1ak MRP 属性符号化方法では、MVRP はポート上のすべての 4094 VLAN のステートを含む、1 PDU のみを送信する必要があります。MVRP は、各 VLAN のトポロジ変更通知（TCN）も送信します。これは、トポロジの変更をローカライズできるため、サービス プロバイダーの重要な機能です。図 23-1 に、プロバイダー ネットワークのプロバイダー ブリッジとカスタマー ブリッジに配置された MVRP を示します。

図 23-1　プロバイダー ブリッジとカスタマー ブリッジに配置された MVRP

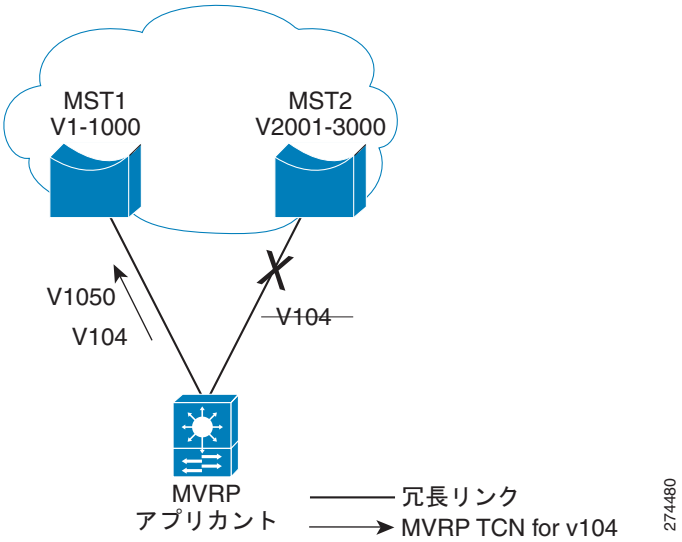


ほとんどのプロバイダーが宛先 MAC アドレスに基づいてトラフィックをフィルタリングしたくないため、頻繁に大量の VLAN を使用する Metro Ethernet ネットワークでは、MVRP のようなプルーニング プロトコルが重要になります。

図 23-2 に、クラウドのアクセス スイッチと 2 個のディストリビューション スイッチ間で設定されている冗長リンクを示します。VLAN 104 でリンク障害が発生した場合、MVRP は VLAN 104 の 1 TCN だけ送信する必要があります。MVRP がなければ、STP TCN を MST リージョン（VLANs1-1000）全体に送信する必要があり、不要なネットワーク割り込みが発生することがあります。

STP は、MVRP が MVRP TCN を送信するかどうかを決定する必要があることを MVRP に示す tcDetected 変数を設定します。MVRP はトポロジの変更後にフィルタリング データベース エントリを VLAN ごとに迅速にフラッシュできます。これは、ポートが新規としてマークされた属性宣言を受信すると、そのポートと VLAN のフィルタリング データベースのエントリが削除されるからです。

図 23-2　　MVRP TCN アプリケーション



ダイナミック VLAN 作成

Virtual Trunking Protocol（VTP）は、VTP ドメイン内の複数のデバイスに VLAN 設定情報を配信するシスコ独自のプロトコルです。VTP が MVRP 対応デバイスで動作している場合、Cisco ブリッジド LAN セグメントで許可される VLAN すべてが VTP によって決定されます。

VTP トランスペアレント モードだけで MVRP ダイナミック VLAN 作成をサポートします。ダイナミック VLAN 作成がディセーブルの場合、MVRP トランク ポートは、既存の VLAN のみの VLAN メッセージを登録し、送信できます。存在しない VLAN の MVRP PDU および MVRP メッセージは廃棄されます。

MVRP 規格に完全に準拠するようにスイッチを設定するには、スイッチ VTP モードをトランスペアレントにし、MVRP ダイナミック VLAN 作成をイネーブルにする必要があります。

MVRP と VTP の相互運用性

- 「サーバ モードまたはクライアント モードの VTP および VTP プルーニングがディセーブル」（P.23-5）
- 「サーバ モードまたはクライアント モードの VTP および VTP プルーニングがイネーブル」（P.23-5）

概要

VLAN トランキング プロトコル（VTP）は、VTP ドメイン内の複数のデバイスに VLAN 設定情報を配信するシスコ独自のプロトコルです。VTP プルーニングは VTP の拡張機能です。VTP プルーニングには、VTP PDU と交換可能な独自の Join メッセージがあります。VTP PDU は 802.1Q トランクと ISL トランクの両方で送信できます。VTP 対応デバイスはいずれかの VTP モード（サーバ、クライアント、またはオフ）です。

VTP プルーニングおよび MVRP を両方グローバルにイネーブルにすると、MVRP はイネーブル化されたトランクで動作し、VTP プルーニングはそれ以外のトランクで動作します。MVRP または VTP プルーニングをトランクでイネーブルにできますが、両方同時にはイネーブルにできません。

トランスペアレント モードまたはオフ モードの VTP

VTP がトランスペアレント モードまたはオフ モードの場合、VTP プルーニングはサポートされず、VTP PDU は処理されません。

ポートが VLAN に対する MVRP Join メッセージを受信すると、ポートはその VLAN でブロードキャスト、マルチキャスト、不明なユニキャスト フレームを送信して、その VLAN 用に設定された MRP Attribute Propagation（MAP）ポートにトラフィック定義を追加します。マッピングは VLAN がポートで登録されていないと削除されます。

各 VLAN で転送を行うインターフェイスごとに、MVRP は各 MRP 属性宣言（MAD）インスタンスに Join 要求を発行し、MVRP Join メッセージは対応する各 MVRP ポートに送信されます。

MVRP ダイナミック VLAN 作成は、VTP トランスペアレント モードまたはオフ モードでイネーブルにできます。この機能をイネーブルにし、Join メッセージで登録された VLAN がデバイスの VLAN データベースにない場合、VLAN が作成されます。

サーバ モードまたはクライアント モードの VTP および VTP プルーニングがディセーブル

MVRP はトランスペアレント モードとオフ モードで VTP と同様に機能しますが、MVRP ダイナミック VLAN 作成が許可されません。

サーバ モードまたはクライアント モードの VTP および VTP プルーニングがイネーブル

プルーニングがディセーブルの MVRP および VTP は同一のポートでサポートでき、この 2 つのプロトコルがプルーニング情報を通信し、交換する必要があります。

VTP が VTP Join メッセージを VTP トランクで受信すると、Join 要求を MVRP ポートの MAD インスタンスにポストできることが MVRP に通知され、MVRP Join メッセージが MVRP ポートから MVRP ネットワークに送信されます。

VTP プルーニングが VTP トランクから VLAN を削除すると、MVRP はすべての MAD インスタンスに脱退要求を送信し、MAD インスタンスは MVRP ポートから脱退メッセージまたは空のメッセージを送信して、VLAN がデバイスに設定されていないことを示します。

MVRP ポートが MVRP Join メッセージを受信すると、VTP プルーニングが VTP トランク ポートから VTP Join メッセージを送信できるように、MVRP は同じ MAP コンテキストの他の MVRP ポートにイベントを伝播し、VTP に通知します。

VLAN がネイバー デバイスで宣言されていないことを MVRP が学習すると、MVRP は VTP に回収イベントを送信し、VTP プルーニングは VTP Join メッセージを送信し続ける必要があるかどうかを確認します。

VTP トランクで非適格な VTP プルーニングとして設定された VLAN の場合、その VLAN に対して VTP プルーニングの状態変数が joined に設定されます。MVRP Join 要求は、MVRP ポートを使用してこれらの VLAN に送信されます。

MVRP と他社製のデバイスの相互運用性

他社製のデバイスは、802.1Q トランク経由でシスコ デバイスと相互運用できます。

他のソフトウェア機能およびプロトコルとの MVRP 相互運用性

802.1X とポート セキュリティ

802.1x は、リンクアップ ステートに移行してから DTP ネゴシエーションが実行されて MVRP がポートで稼働する前に、ポートを認証および許可します。ポート セキュリティは、MVRP とは無関係に動作します。

（注）　MVRP をグローバルにイネーブルにすると、MVRP の MAC アドレスの自動検出およびプロビジョニング機能がデフォルトでディセーブルになります（**mvrp mac-learning auto**）。状況によっては、MVRP の MAC アドレスの自動検出およびプロビジョニングによって、MAC アドレス ラーニングがディセーブルになり、正しいポート セキュリティ動作が行われなくなることがあります。たとえば、ポート セキュリティが設定されているポートで、ストリーム数が MAC アドレスの設定された最大数を超えると、MAC アドレス ラーニングがディセーブルになるためポート セキュリティ違反が発生せず、ポートに着信するストリームのポート セキュリティが更新されません。不適切なポート セキュリティ動作を防ぐために、ポート セキュリティが設定されているポートで MVRP の MAC アドレスの自動検出およびプロビジョニング機能をイネーブルにするときに注意してください。

DTP

リンクアップ ステートに移行してから、フォワーディング ステートに移行するまでに、DTP ネゴシエーションが実行されます。MVRP は、管理上グローバルにイネーブルにされ、ポートでイネーブルになっている場合、ポートがトランキングを開始すると稼働状態になります。

EtherChannel

EtherChannel のポートチャネル インターフェイスは、MVRP 参加者として設定できます。EtherChannel メンバ ポートは、MVRP 参加者にできません。MVRP は、EtherChannel のポートチャネル インターフェイスの STP ステートを学習します。MAP コンテキストは EtherChannel のポートチャネル インターフェイスに適用されますが、EtherChannel メンバ ポートに適用されません。

Flex Link

MVRP は STP フォワーディング ポートに対して VLAN を宣言しますが、ブロッキング ステートのポートに対しては宣言しません。Flex Link ポートで、MVRP はアクティブ ポートに対して VLAN を宣言しますが、スタンバイ ポートに対しては宣言しません。スタンバイ ポートが機能を引き継ぎ、アクティブ ポートがリンクダウン ステートに移行すると、MVRP は新しいアクティブ ポートに対して VLAN を宣言します。

ハイ アベイラビリティ

ステート スイッチオーバー（SSO）と ISSU は MVRP をサポートします。

ISSU および eFSU

Enhanced Fast Software Upgrade（EFSU）は、拡張ソフトウェア アップグレード手順です。MVRP は ISSU_MVRP_CLIENT_ID として特定された ISSU クライアントによって処理されます。

L2PT

レイヤ 2 プロトコル トンネリング（L2PT）は 802.1Q トンネル ポートの MVRP PDU をサポートしません。

SPAN

MVRP ポートはスイッチド ポート アナライザ（SPAN）の送信元または宛先として設定できます。

不明なユニキャストおよびマルチキャストのフラッディング コントロール

MVRP と不明なユニキャストおよびマルチキャストのフラッディング コントロール機能は、**switchport block** コマンドで設定し、同一ポート上に設定できません。

STP

STP が新規設定モードで再コンバージェンスするまで、STP モード変更によって、フォワーディング ポートはフォワーディング ステートを脱退します。異なるフォワーディング ポートで Join メッセージを受信し、他のポートで脱退タイマーが切れる可能性があるため、再コンバージェンスにより MVRP トポロジが変化する場合があります。

UDLR

MVRP および単方向リンク ルーティング（UDLR）は同一のポートに設定できません。

MVRP での VLAN

- 「VLAN 変換」（P.23-8）
- 「802.1Q ネイティブ VLAN タギング」（P.23-8）
- 「プライベート VLAN」（P.23-8）

VLAN 変換

VLAN 変換および MVRP は同一のポートに設定できません。

802.1Q ネイティブ VLAN タギング

その他の MVRP 参加者が 802.1Q ネイティブ VLAN 内のタグ付けされた MVRP PDU を受け付けられない場合があります。MVRP と 802.1Q ネイティブ VLAN タギングの互換性はネットワークの設定によって異なります。

プライベート VLAN

プライベート VLAN ポートは、MVRP をサポートできません。

IEEE 802.1ak MVRP および MRP のデフォルト設定

なし。

IEEE 802.1ak MVRP および MRP の設定方法

- 「MVRP のイネーブル化」（P.23-9）
- 「MAC アドレスの自動検出のイネーブル化」（P.23-9）
- 「MVRP ダイナミック VLAN 作成のイネーブル化」（P.23-10）
- 「MVRP レジストラの状態の変更」（P.23-10）

MVRP のイネーブル化

MVRP をグローバルおよびトランク ポートでイネーブルにする必要があります。MVRP をイネーブルにする手順は、次のとおりです。

	コマンドまたはアクション	目的
ステップ 1	`Router> 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	`Router# 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	`Router(config)# mvrp global`	MVRP をグローバルにイネーブルにします。
ステップ 4	`Router(config)# interface type number`	トランク 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	`Router(config-if)# mvrp`	インターフェイス上で MVRP をイネーブルにします。 （注）　MVRP がポートで正常にイネーブルにならない場合、ポートは errdisabled ステートになります。インターフェイス上で **no mvrp** コマンドまたは **no mvrp global** コマンドを入力して、errdisabled ステートを消去してください。

次に、インターフェイスで MVRP をグローバルにイネーブルにする例を示します。

```
Router> enable
Router# configure terminal
Router(config)# mvrp global
Router(config)# interface FastEthernet 2/1
Router(config-if)# mvrp
```

MAC アドレスの自動検出のイネーブル化

MAC アドレスの MVRP 自動検出はデフォルトでディセーブルです。VLAN の MAC アドレスの MVRP 自動検出をイネーブルにするには、次の作業を行います。

	コマンドまたはアクション	目的
ステップ 1	`Router> 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	`Router# 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	`Router(config)# mvrp mac-learning auto`	MAC アドレス ラーニングをイネーブルにします。

次に、自動 MAC アドレス ラーニングをイネーブルにする例を示します。

```
Router> enable
Router# configure terminal
Router(config)# mvrp mac-learning auto
```

MVRP ダイナミック VLAN 作成のイネーブル化

MVRP ダイナミック VLAN 作成をイネーブルにするには、次の作業を行います。

	コマンドまたはアクション	目的
ステップ 1	`Router> 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	`Router# 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	`Router(config)# vtp mode transparent`	VTP モードをトランスペアレントに設定します。 （注）　MVRP ダイナミック VLAN 作成で必要です。
ステップ 4	`Router(config)# mvrp vlan creation`	MRVP ダイナミック VLAN 作成をイネーブルにします。

次に、MVRP ダイナミック VLAN 作成をイネーブルにする例を示します。

```
Router> enable
Router# configure terminal
Router(config)# vtp mode transparent
Router(config)# mvrp vlan create
```

MVRP レジストラの状態の変更

MRP プロトコルはエンド ステーションのアプリケーションごとに 1 参加者、およびブリッジの各ポートでアプリケーションごとに 1 参加者を許可します。MVRP レジストラ ステートを設定するには、次の作業を行います。

	コマンドまたはアクション	目的
ステップ 1	`Router> 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	`Router# 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	`Router(config)# interface` *type number*	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 4	`Router(config-if)# mvrp registration` [**normal** | **fixed** | **forbidden**]	MAD インスタンスに MVRP を登録します。

次に、MVRP レジストラ ステートを通常に設定する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface FastEthernet 2/1
Router(config-if)# mvrp registration normal
```

MVRP 設定のトラブルシューティング

設定情報とインターフェイス ステートを表示するには **show mvrp summary** コマンドと **show mvrp interface** コマンドを使用し、インターフェイスに関するすべてまたは限定された出力メッセージをイネーブルにするには **debug mvrp** コマンドを使用します。

MVRP 設定をトラブルシューティングするには、次の作業を行います。

	コマンドまたはアクション	目的
ステップ 1	`Router> 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	`Router# show mvrp summary`	MVRP 設定を表示します。
ステップ 3	`Router# show mvrp interface` *interface-type port/slot*	指定したインターフェイスの MVRP インターフェイス ステートを表示します。
ステップ 4	`Router# debug mvrp`	MVRP デバッグ情報を表示します。
ステップ 5	`Router# clear mvrp statistics`	すべてのインターフェイスの MVRP 統計情報を消去します。

次に、**show mvrp summary** コマンドの出力例を示します。このコマンドをデバイス レベルの MVRP 設定の表示に使用できます。

```
Router# show mvrp summary

MVRP global state           : enabled
MVRP VLAN creation          : disabled
VLANs created via MVRP      : 20-45, 3001-3050
Learning disabled on VLANs  : none
```

次に、**show mvrp interface** コマンドの出力例を示します。このコマンドは、デバイスのすべてのまたは 1 個の特定のトランク ポートの管理および動作上の MVRP ステートの MVRP インターフェイス詳細を表示する場合に使用できます。

```
Router# show mvrp interface

Port      Status   Registrar State
Fa3/1     off      normal

Port      Join Timeout   Leave Timeout   Leaveall Timeout
Fa3/1     201  600       700             1000

Port      Vlans Declared
Fa3/1     none

Port      Vlans Registered
Fa3/1     none

Port      Vlans Registered and in Spanning Tree Forwarding State
Fa3/1     none
```

IEEE 802.1ak MVRP と MRP の設定例

- 「MVRP のイネーブル化」（P.23-12）
- 「MAC アドレスの MVRP 自動検出のイネーブル化」（P.23-12）
- 「ダイナミック VLAN 作成のイネーブル化」（P.23-12）
- 「MVRP レジストラの状態の変更」（P.23-12）

MVRP のイネーブル化

次に、MVRP をイネーブルにする例を示します。

```
Router> enable
Router# configure terminal
Router(config)# mvrp global
Router(config)# interface fastethernet2/1
Router(config-if)# mvrp
```

MAC アドレスの MVRP 自動検出のイネーブル化

次に、MAC アドレス ラーニングをイネーブルにする例を示します。

```
Router> enable
Router# configure terminal
Router(config)# mvrp mac-learning auto
```

ダイナミック VLAN 作成のイネーブル化

次に、ダイナミック VLAN 作成をイネーブルにする例を示します。

```
Router> enable
Router# configure terminal
Router(config)# vtp mode transparent
Router(config)# mvrp vlan create
```

MVRP レジストラの状態の変更

次に、MVRP レジストラの状態を変更する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# mvrp registration normal
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CHAPTER 24

VLAN トランキング プロトコル（VTP）

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

VTP の前提条件

なし。

VTP の制約事項

- スーパーバイザ エンジンの冗長構成は、デフォルト以外の VLAN データ ファイル名または場所をサポートしません。冗長スーパーバイザ エンジンを持つスイッチに対して、**vtp file** *file_name* コマンドは入力しないでください。
- 冗長スーパーバイザ エンジンを取り付ける前に、デフォルト設定に戻るには **no vtp file** コマンドを入力します。

- 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。
- 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ないと、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装置上で 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 対応ネットワーク装置は、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装置として動作できます（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。いずれかのネットワーク装置上で 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 対応ネットワーク装置上で VTP バージョン 2 がイネーブルになります。
- トークン リング環境では、トークン リング VLAN スイッチング機能を正常に動作させるために、VTP バージョン 2 をイネーブルにする必要があります。
- VTP サーバ上で VTP プルーニングをイネーブルまたはディセーブルにすると、管理ドメイン全体で VTP プルーニングがイネーブルまたはディセーブルになります。
- プルーニングの適格性の設定は、スイッチ上のすべてのトランクにグローバルに適用されます。プルーニングの適格性は、各トランクに個別に設定できません。
- 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なわけではありません。
- VTP バージョン 1 および VTP バージョン 2 は、設定情報を拡張範囲 VLAN（VLAN 番号 1006 ～ 4094）に伝播しません。VLAN 拡張範囲は、各ネットワーク デバイスで手作業で設定する必要があります。
- VTP バージョン 3 は拡張範囲 VLAN（VLAN 番号 1006 ～ 4094）をサポートします。VTP バージョン 3 から VTP バージョン 2 に変換する場合は、範囲 1006 ～ 4094 の VLAN が VTP の制御から削除されます。
- VTP バージョン 3 では、プライマリおよびセカンダリ サーバを設定でき、ドメイン内のデータベースの伝播がサポートされます。
- ネットワーク管理者は VTP バージョン 3 を実行する必要があるスイッチ上で VTP バージョン 3 を手動で設定する必要があります。
- VTP バージョン 3 はプライベート VLAN（PVLAN）ポートではサポートされません。
- VTP バージョン 3 を設定する前に **spanning-tree extend** *system-id* コマンドがイネーブルになっていることを確認してください。
- VTP が使用する利用可能な DRAM が不十分な場合、VTP のモードはトランスペアレントに変わります。
- VTP トランスペアレント モードのネットワーク デバイスは、VTP Join メッセージを送信しません。VTP トランスペアレント モードにおけるネットワーク装置へのトランク接続では、トランスペアレント モード ネットワーク装置によって使用される VLAN、またはプルーニング不適格としてトランク全体に伝送する必要がある VLAN を設定します。プルーニング適格性の設定については、「プルーニング適格 VLAN のリストの設定」（P.20-12）を参照してください。

VTP の概要

（注）　VLAN の詳しい設定手順については、第 25 章「仮想ローカル エリア ネットワーク（VLAN）」を参照してください。

VTP の概要

VTP はレイヤ 2 のメッセージング プロトコルであり、VTP ドメインでの VLAN の追加、削除、名前変更などを管理することにより、VLAN 設定の整合性を維持します。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 つ以上のネットワーク 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が最小限に抑えられます。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 デバイスに伝達することができます。

VTP ドメイン

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、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 つのネットワーク 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、コマンドライン インターフェイス（CLI）または簡易ネットワーク管理プロトコル（SNMP）を使用します。

VTP サーバ モードはデフォルトです。スイッチは、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メントを受信するか、またはユーザが管理ドメインを設定しない限り、非管理ドメイン ステートのままです。

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、スイッチは管理ドメイン名および VTP コンフィギュレーション リビジョン番号を継承します。スイッチは、別の管理ドメイン名または古いコンフィギュレーション リビジョン番号が指定されたアドバタイズメントについては、いっさい無視します。

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。有効な VLAN 範囲は次のとおりです。

- VTP バージョン 1 とバージョン 2 は VLAN 1 ～ 1000 だけをサポートします。
- VTP バージョン 3 は、VLAN 範囲全体（VLAN 1 ～ 4094）をサポートします。

- VLAN のプルーニングは VLAN 1 ～ 1000 にだけ適用されます。
- 拡張範囲 VLAN は VTP バージョン 3 だけでサポートされます。VTP バージョン 3 から VTP バージョン 2 に変換する場合は、範囲 1006 ～ 4094 の VLAN が VTP 制御から削除されます。

デフォルトでは、すべてのデバイスはセカンダリ サーバとして起動します。プライマリ サーバを指定するには **vtp primary** 特権 EXEC モード コマンドを入力します。

VTP バージョン 1 およびバージョン 2 を使用する場合、VTP サーバを使用してデータベースを NVRAM にバックアップし、データベース情報を変更できます。

VTP バージョン 3 では、VTP プライマリ サーバと VTP セカンダリ サーバが存在します。プライマリ サーバでは、データベース情報を変更でき、送信されたデータベース更新はシステム内のすべての装置で反映されます。セカンダリ サーバでは、プライマリ サーバから受け取った更新済み VTP 設定だけを NVRAM にバックアップできます。プライマリ サーバとセカンダリ サーバのステータスは実行時ステータスであり、設定不可能です。

VTP は、一意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 をダイナミック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がデバイスを管理するための作業負担が大幅に軽減されます。

VTP モード

次のいずれかの VTP モードを設定できます。

- 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 デバイスと同期化します。VTP サーバがデフォルトのモードです。
- クライアント : VTP クライアントは、VTP サーバと同様に動作しますが、VTP クライアント上で VLAN の作成、変更、または削除を行うことはできません。
- 透過的 : VTP 透過ネットワーク装置は、VTP に関与しません。VTP 透過ネットワーク装置は、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化することもありません。ただし VTP バージョン 2 では、透過ネットワーク装置は、トランキング LAN ポートから受信した VTP アドバタイズメントを転送します。VTP バージョン 3 では、1 つの透過ネットワーク装置は 1 つのインスタンスに固有です。
- オフ : VTP オフ モードでは、ネットワーク デバイス機能は、VTP 透過デバイスと同じ方法で動作します。ただし、VTP アドバタイズは転送されません。

（注）　VTP サーバ モードでは、NVRAM に設定を書き込むときにスイッチが障害を検出すると、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、スイッチは NVRAM が動作するまで VTP サーバ モードに戻ることができません。

VTP アドバタイズ

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 ポートからアドバタイズを定期的に送信します。VTP アドバタイズを受信したネイバー ネットワーク デバイスは、必要に応じて各自の VTP および VLAN 設定を更新します。

次のグローバル設定情報は、VTP バージョン 1 およびバージョン 2 アドバタイズメントで配布されます。

- VLAN ID
- エミュレート 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 設定のリビジョン番号
- 各 VLAN の最大伝送単位（MTU）サイズを含めた VLAN 設定
- フレーム形式

VTP バージョン 3 では、VTP バージョン 1 およびバージョン 2 アドバタイズメントで配布された情報と次の情報がサポートされます。

- プライマリ サーバ ID
- インスタンス番号
- 開始インデックス
- アドバタイズメント要求は、次の状況でクライアントまたはサーバによって送信されます。
  - 有効なデータベースとともにスイッチ上に現れるトランク
  - 設定変更または引継ぎメッセージの結果、スイッチのデータベースが無効になった場合のすべてのトランク
  - 上位のデータベースがアドバタイズされた特定のトランク
- VTP バージョン 3 は、サブセット アドバタイズメント要求に次のフィールドを追加します。
  - プライマリ サーバ ID
  - インスタンス番号
  - ウィンドウ サイズ
  - 開始インデックス

VTP 認証

VTP 認証が設定されていない場合、受信した VTP アップデートを検証するために使用される秘密キーは **show** コマンドおよび NVRAM ファイル（const_nvram:vlan.dat）のプレーン テキストに表示されます。VTP ドメインのセキュリティが損なわれた場合は、管理者が VTP ドメイン内のすべての装置に対して VTP 秘密キーを変更しなければなりませんでした。

VTP バージョン 3 では、**vtp password** コマンドを使用して認証パスワードを非表示にするよう設定できます。認証パスワードを非表示に設定した場合、設定のパスワードはプレーン テキストで表示されません。代わりに、使用されている設定でパスワードに関連付けられた秘密キーが 16 進数形式で保存されます。*password-string* 引数は、装置の管理ドメインを識別する 8 ～ 64 文字の ASCII 文字列です。

VTP バージョン 2

VTP バージョン 2 でサポートされる機能は、次のとおりです（バージョン 1 ではサポートされません）。

- 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 スイッチングおよび VLAN（Token Ring Bridge Relay Function（TrBRF; トークンリング ブリッジ リレー機能）および Token Ring Concentrator Relay Function（TrCRF; トークンリング コンセントレータ リレー機能））をサポートします。トークンリング VLAN の詳細については、「VLAN について」（P.25-2）を参照してください。
- 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。認識不能な 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 透過ネットワーク装置は、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。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 を介して新しい情報が入力された場合に限り、VLAN 整合性検査（VLAN 名、値など）を行います。VTP メッセージから新しい情報を取得した場合、または NVRAM から情報を読み込んだ場合には、整合性検査を行いません。受信した VTP メッセージのダイジェストが有効であれば、整合性検査を行わずに情報を受け入れます。

VTP バージョン 3

VTP バージョン 3 は、バージョン 1 およびバージョン 2 のすべての機能をサポートします。VTP バージョン 3 は、バージョン 1 およびバージョン 2 でサポートされていない次の機能もサポートします。

- 拡張認証：VTP バージョン 3 では、**vtp password** コマンドを使用して認証パスワードを非表示にするよう設定できます。認証パスワードを非表示に設定した場合、設定のパスワードはプレーンテキストで表示されません。代わりに、使用されている設定でパスワードに関連付けられた秘密キーが 16 進数形式で保存されます。*password-string* 引数は、装置の管理ドメインを識別する 8 ～ 64 文字の ASCII 文字列です。

  VTP パスワードに対する**非表示**で**秘密**のキーワードは VTP バージョン 3 だけでサポートされます。VTP バージョン 3 から VTP バージョン 2 へ変換する場合は、変換を行う前に**非表示**または**秘密**のキーワードを削除する必要があります。これらのキーワードは、Catalyst 6500 シリーズ スイッチでだけサポートされます。
- 拡張範囲 VLAN データベース伝播のサポート：VTP バージョン 1 およびバージョン 2 は VLAN 1 ～ 1000 だけをサポートします。VTP バージョン 3 では、VLAN 範囲全体（VLAN 1 ～ 4094）がサポートされます。VLAN のプルーニングは VLAN 1 ～ 1000 にだけ適用されます。拡張範囲 VLAN は VTP バージョン 3 だけでサポートされます。プライベート VLAN は VTP バージョン 3 でサポートされます。VTP バージョン 3 から VTP バージョン 2 に変換する場合は、範囲 1006 ～ 4094 の VLAN が VTP の制御から削除されます。
- VLAN 1002 ～ 1005 は、VTP バージョン 1、バージョン 2、およびバージョン 3 で予約済み VLAN です。
- ドメイン内にあるデータベースの伝播のサポート：VTP バージョン 1 およびバージョン 2 では、VTP サーバを使用してデータベースを NVRAM にバックアップし、データベース情報を変更できます。

（注）　VTP バージョン 3 は、VLAN データベースから独立したマルチ スパニングツリー（MST）（802.1s）データベース伝播のみをサポートします。MST データベース伝播では、VTP プライマ リサーバと VTP セカンダリ サーバが存在します。プライマリ サーバでは、データベース情報を変更でき、送信されたデータベース更新はシステム内のすべての装置で反映されます。セカンダリ サーバでは、プライマリ サーバから受け取った更新済み VTP 設定だけを NVRAM にバックアップできます。プライマリ サーバとセカンダリ サーバのステータスは実行時ステータスであり、設定不可能です。

デフォルトでは、すべてのデバイスはセカンダリ サーバとして起動します。プライマリ サーバを指定するには **vtp primary** 特権 EXEC モード コマンドを入力します。

プライマリ サーバ ステータスは、データベース変更を実行する必要がある場合だけ必要であり、管理者がドメイン内で引継ぎメッセージを発行した場合に取得されます。プライマリ サーバ ステータスは、リロードやスイッチオーバーを行ったとき、またはドメイン パラメータが変更したときに失われます。セカンダリ サーバは設定をバックアップし、データベースを伝播し続けます。プライマリ サーバなしで実用 VTP ドメインを持つことができます。ドメイン内の 1 つのインスタンスでプライマリ サーバとセカンダリ サーバは共存できます。

VTP バージョン 3 では、VLAN データベース情報だけを伝播できる制限がなくなりました。VTP バージョン 3 を使用して VTP ドメイン全体でデータベース情報を伝播できます。VTP を使用する各アプリケーションに対してプロトコルの個別インスタンスが実行されています。

2 つの VTP バージョン 3 領域は、トランスペアレント モードで VTP バージョン 1 または VTP バージョン 2 の領域を介してだけ通信できます。

- 1 つのトランクごとに VTP をディセーブルまたはイネーブルにする CLI : 1 つのトランクごとに VTP をイネーブルにするには **vtp** インターフェイス コンフィギュレーション モード コマンドを使用します。1 つのトランクごとに VTP をディセーブルにするにはこのコマンドの **no** 形式を使用します。トランキング ポートで VTP をディセーブルにすると、そのポートのすべての VTP インスタンスがディセーブルになります。VTP を MST データベースに対して OFF、VLAN データベースに対して ON に設定できません。

グローバルでの VTP : VTP モードをグローバルに OFF に設定すると、システム内のすべてのトランキング ポートに適用されます。ポートごとの設定とは異なり、1 つの VTP インスタンスごとに OFF オプションを指定できます。たとえば、システムは VLAN データベースに対する VTP-server として、または MST データベースに対する VTP-off として設定できます。この場合は、VLAN データベースが VTP によって伝播され、MST 更新がシステム内のトランク ポートに送信され、システムが受け取った MST 更新が破棄されます。

VTP プルーニング

VTP プルーニングは、ブロードキャスト パケット、マルチキャスト パケット、未知のパケット、フラッディング ユニキャスト パケットなど、不要なフラッディング トラフィックを削減することにより、ネットワークの帯域幅を拡張します。VTP プルーニングを使用すると、トラフィックがネットワーク 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えます。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 バージョン 1 および 2 では、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、ドメイン全体に伝播され、そのドメイン内のすべての装置によって受け入れられます。VTP バージョン 3 では、ドメイン管理者が装置ごとに手動で明示的に VTP プルーニングをイネーブルまたはディセーブルする必要があります。

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 24-1 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。ネットワーク スイッチ 1 のインターフェイス 1 およびスイッチ 4 のポート 2 は、Red という VLAN に割り当てられています。スイッチ 1 に接続されたホストから、ブロードキャストが送信されます。スイッチ 1 は、このブロードキャストをフラッディングします。Red VLAN にポートを持たないスイッチ 3、5、6 も含めて、ネットワーク内の全ネットワーク 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、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.24-13）を参照）。レイヤ 2 トランキング LAN ポートにプルーニングを設定します（「トランクとしてのレイヤ 2 スイッチング ポートの設定」（P.20-9）を参照）。

図 24-1　VTP プルーニングを使用しない場合のフラッディング トラフィック

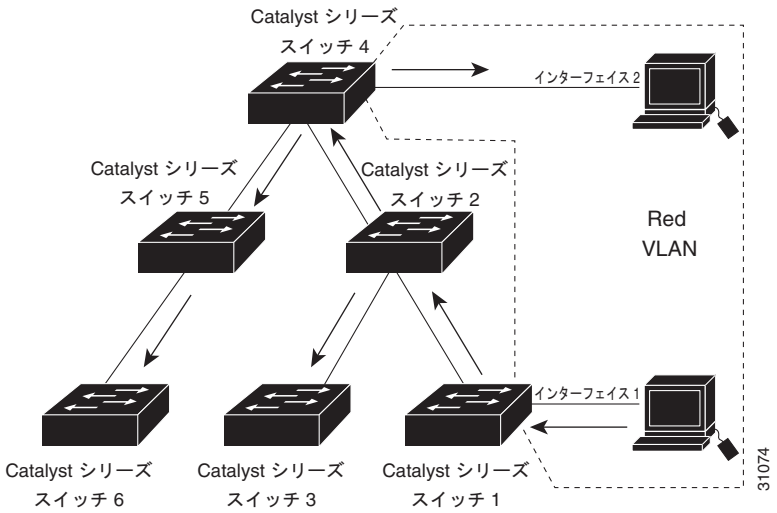
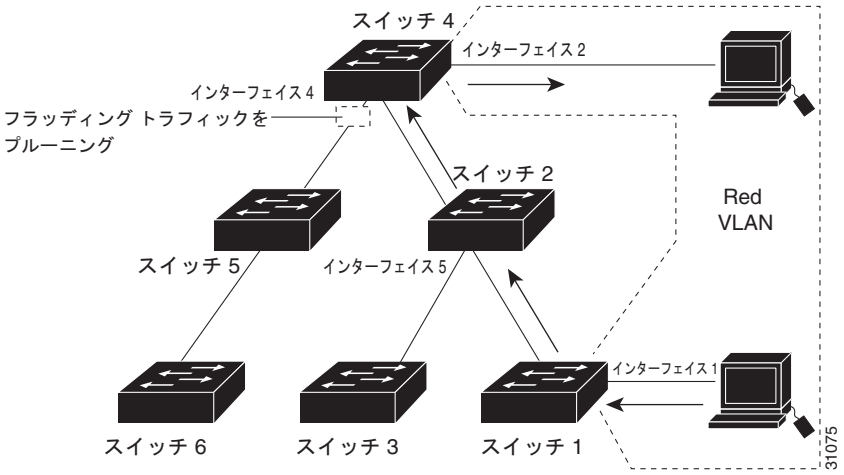


図 24-2 は、VTP プルーニングをイネーブルにした場合の同じスイッチド ネットワークを示しています。Red VLAN のトラフィックは指定されたリンク（スイッチ 2 のポート 5、スイッチ 4 のポート 4）でプルーニングされるので、スイッチ 1 からのブロードキャスト トラフィックは、スイッチ 3、5、6 には転送されません。

図 24-2　VTP プルーニングを使用した場合のフラッディング トラフィック



VTP 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イネーブルになります。VTP プルーニングは、イネーブルにしてから数秒後に有効になります。デフォルトでは、VLAN 2 ～ 1000 がプルーニング適格です。VTP プルーニング不適格の VLAN からのトラフィックは、プルーニングの対象になりません。VLAN 1 は常にプルーニング不適格であり、VLAN 1 からのトラフィックをプルーニングできません。

トランキング LAN ポートに 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（「トランクとしてのレイヤ 2 スイッチング ポートの設定」（P.20-9）を参照）。VTP プルーニングは、LAN ポートがトランキングを実行している場合に作用します。VLAN プルーニングの適格性は、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 ポート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、設定できます。

VLAN 対話

ここでは、VTP バージョンが異なる装置間の VLAN 対話について説明します。

- 「VTP バージョン 3 装置と VT バージョン 2 装置間の対話」（P.24-9）
- 「VTP バージョン 3 装置と VTP バージョン 1 装置間の対話」（P.24-10）

VTP バージョン 3 装置と VT バージョン 2 装置間の対話

トランク ポート上の VTP バージョン 3 装置が VTP バージョン 2 装置からメッセージを受け取ると、VTP バージョン 3 装置はその特定のトランク上にある VLAN データベースのスケールダウン バージョンを VTP バージョン 2 形式で送信します。VTP バージョン 3 装置は、トランクで最初に VTP バージョン 2 パケットを受信しない限り、そのトランク ポートで VTP バージョン 2 形式のパケットを送信しません。VTP バージョン 3 装置がトランク ポートで一定時間 VTP バージョン 2 パケットを受け取らないと、VTP バージョン 3 装置はそのトランク ポートで VTP バージョン 2 パケットの送信を中止します。

VTP バージョン 3 装置がトランク ポートで VTP バージョン 2 装置を検出した場合であっても、トランク上に 2 種類のネイバーが共存できるように VTP バージョン 3 装置は VTP バージョン 3 装置 2 パケット以外に VTP バージョン 3 パケットを送信し続けます。VTP バージョン 3 は、VTP バージョン 2 により検出されたトランクで VTP バージョン 3 と VTP バージョン 2 の更新を送信します。

VTP バージョン 3 装置は、VTP バージョン 2（または VTP バージョン 1）装置から設定を受け入れません。

VTP バージョン 2 とは異なり、VTP バージョンをバージョン 3 に設定した場合、バージョン 3 は、ドメイン内のすべての VTP バージョン 3 対応装置は VTP バージョン 3 システムのように動作するよう設定しません。

VTP バージョン 3 装置と VTP バージョン 1 装置間の対話

VTP バージョン 2 または VTP バージョン 3 に対応した VTP バージョン 1 装置が VTP バージョン 3 パケットを受信したときに VTP バージョン 2 の競合が発生しない場合、その装置は VTP バージョン 2 装置として設定されます。

VTP バージョン 1 にだけ対応した装置は VTP バージョン 3 装置と相互運用できません。

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 バージョン 1 およびバージョン 2 モード	サーバ
VTP バージョン 3 モード	VTP バージョン 1 または 2 から VTP バージョン 3 への変換後、VTP バージョン 3 VLAN データベース モードは VTP バージョン 1 または 2 の VLAN データベース モードと同じです。たとえば、VTP バージョン 1 または 2 VLAN データベース モードは VTP バージョン 3 VLAN データベース モードに引き継がれます。
MST データベース モード	透過
VTP バージョン 3 サーバ タイプ	セカンダリ
VTP バージョン 2 のステート	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

VTP の設定方法

- 「VTP グローバル パラメータの設定」（P.24-10）
- 「VTP モードの設定」（P.24-16）
- 「ポート単位の VTP モードの設定」（P.24-17）
- 「VTP 統計情報の表示」（P.24-18）

VTP グローバル パラメータの設定

- 「VTP バージョン 1 およびバージョン 2 パスワードの設定」（P.24-11）
- 「VTP バージョン 3 パスワードの設定」（P.24-11）

- 「VTP プルーニングのイネーブル化」（P.24-13）
- 「VTP バージョン 2 のイネーブル化」（P.24-13）
- 「VTP バージョン 3 のイネーブル化」（P.24-14）

（注）　VTP グローバル パラメータは、グローバル コンフィギュレーション モード、または EXEC モードで入力できます。

VTP バージョン 1 およびバージョン 2 パスワードの設定

VTP バージョン 1 およびバージョン 2 のグローバル 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
Router(config)# **vtp password** *password-string*	VTP ドメインのパスワード（8 ～ 64 文字）を設定します。
Router(config)# **no vtp password**	パスワードを消去します。

次に、グローバル コンフィギュレーション モードで VTP パスワードを設定する例を示します。

```
Router# configure terminal
Router(config)# vtp password WATER
Setting device VLAN database password to WATER.
Router#
```

次に、EXEC モードで VTP パスワードを設定する例を示します。

```
Router# vtp password WATER
Setting device VLAN database password to WATER.
Router#
```

（注）　パスワードは実行コンフィギュレーション ファイルには保存されません。

VTP バージョン 3 パスワードの設定

VTP バージョン 3 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
Router(config)# **vtp password** *password-string* [**hidden** | **secret**]	VTP ドメインのパスワード（8 ～ 64 文字または 32 桁の 16 進数）を設定します。 （注）　**秘密**のキーワードを入力する場合は、*password-string* を 32 桁の 16 進数で入力する必要があります。
Router(config)# **no vtp password**	パスワードを消去します。

次に、グローバル コンフィギュレーション モードで VTP パスワードを設定する例を示します。

```
Router# configure terminal
Router(config)# vtp password water
Setting device VTP database password to water.
```

```
Router#
```

（注）　EXEC モードで VTP パスワードを設定する場合、パスワードは、実行コンフィギュレーション ファイルに保存されません。

次に、実行コンフィギュレーションに 16 進表記で保存された非表示キーでパスワードを設定する例を示します。

```
Router# configure terminal
Router(config)# vtp password 82214640C5D90868B6A0D8103657A721 hidden
Setting device VTP password
Router#
```

次に、16 進表記でパスワード秘密キーを設定する例を示します。

```
Router# configure terminal
Router(config)# vtp password 300F060A2B060103530102010701020 1 secret
Setting device VTP password
Router#
```

VTP バージョン 3 サーバ タイプの設定

プライマリ サーバを指定するには、次の作業を行います。

コマンド	目的
Router# **vtp primary** [**vlan** | **mst**] [**force**]	この装置をプライマリ サーバとして設定します。

vtp primary コマンドには **no** 形式がありません。セカンダリ サーバ ステータスに戻るには、次のいずれかの条件を満たす必要があります。

- システム リロード
- 冗長スーパーバイザ間のスイッチオーバー
- 別のサーバからの引継ぎ
- モード設定の変更
- 任意のドメイン設定の変更（バージョン、ドメイン名、ドメイン パスワード）

次に、パスワード機能がディセーブルに設定されている場合にこの装置をプライマリ サーバとして設定する例を示します。

```
Router# vtp primary
This system is becoming primary server for feature vlan
No conflicting VTP version 3 devices found.
Do you want to continue? [confirm]y
Router#
```

次に、パスワード機能がディセーブルに設定されている場合にこの装置を VTP VLAN 機能のプライマリ サーバとして設定する例を示します。

```
Router# vtp primary vlan
This system is becoming primary server for feature vlan
No conflicting VTP version 3 devices found.
Do you want to continue? [confirm]y
Router#
```

次に、パスワード機能がディセーブルに設定されている場合にこの装置を VTP MST 機能のプライマリ サーバとして設定する例を示します。

```
Router# vtp primary mst force
This system is becoming primary server for feature MST
No conflicting VTP version 3 devices found.
Do you want to continue? [confirm]y
Router#
```

次に、ドメイン VTP パスワードが**非表示**または**秘密**のキーワードとともに設定されている場合にこの装置を VTP MST 機能のプライマリ サーバとして設定する例を示します。

```
Router# vtp primary mst force
Enter VTP password: water1
This switch is becoming Primary server for mst feature in the VTP domain
VTP Database Conf Switch ID      Primary Server Revision System Name
------------ ---- -------------- -------------- -------- --------------------
VLANDB       Yes  00d0.00b8.1400=00d0.00b8.1400 1        stp7
Do you want to continue (y/n) [n]? y
Router#
```

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
`Router(config)# 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。

次に、VTP プルーニングを管理ドメイン内でイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# vtp pruning
Pruning switched ON
```

次に、リリースに関係なく、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。

```
Router# vtp pruning
Pruning switched ON
```

次に、設定を確認する例を示します。

```
Router# show vtp status | include Pruning
VTP Pruning Mode: Enabled
Router#
```

プルーニング適格性の設定については、「プルーニング適格 VLAN のリストの設定」（P.20-12）を参照してください。

VTP バージョン 2 のイネーブル化

VTP バージョン 2 対応のネットワーク装置では、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。ネットワーク装置で 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 対応ネットワーク装置でバージョン 2 がイネーブルになります。

注意　同一 VTP ドメイン内のネットワーク デバイス上で、VTP バージョン 1 と VTP バージョン 2 は相互運用できません。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 デバイスがバージョン 2 をサポートしている場合以外では、VTP バージョン 2 をイネーブルにしないでください。

（注）　トークン リング環境では、トークン リング インターフェイスをサポートする装置上でトークン リング VLAN スイッチングを正常に動作させるために、VTP バージョン 2 をイネーブルにする必要があります。

VTP バージョン 2 をイネーブルにするには、次の作業を行います。

コマンド	目的
`Router(config)# vtp version 2`	VTP バージョン 2 をイネーブルにします。

次に VTP バージョン 2 をイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# vtp version 2
V2 mode enabled.
Router(config)#
```

次に、リリースに関係なく、VTP バージョン 2 をイネーブルにする例を示します。

```
Router# vtp version 2
V2 mode enabled.
Router#
```

次に、設定を確認する例を示します。

```
Router# show vtp status | include V2
VTP V2 Mode: Enabled
Router#
```

VTP バージョン 3 のイネーブル化

VTP バージョン 3 はデフォルトでディセーブルになります。バージョン 3 はグローバル コンフィギュレーション モードでだけイネーブルにできます。ネットワーク管理者は VTP バージョン 3 を実行する必要があるスイッチ上で VTP バージョン 3 を手動で設定する必要があります。

（注）　VTP バージョン 3 を設定する前に **spanning-tree extend** *system-id* コマンドがイネーブルになっていることを確認してください。

注意　VTP バージョン 3 では、ドメイン内の 1 つのインスタンス上にプライマリ サーバとセカンダリ サーバの両方を共存させることができます。

VTP バージョン 3 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
Router(config)# **vtp version 3**	VTP バージョン 3 をイネーブルにします。

次に VTP バージョン 3 をイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# vtp version 3
Router(config)#
```

次に、設定を確認する例を示します。

```
Router# show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 3
VTP Domain Name                 : lab_switch
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0015.c724.0040

Feature VLAN:
--------------
VTP Operating Mode                : Server
Number of existing VLANs          : 6
Number of existing extended VLANs : 0
Configuration Revision            : 0
Primary ID                        : 0000.0000.0000
Primary Description               :
MD5 digest                        : 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
                                    0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00


Feature MST:
--------------
VTP Operating Mode                : Transparent


Feature UNKNOWN:
--------------
VTP Operating Mode                : Transparent
Router#
```

VTP モードの設定

VTP 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	`Router(config)# vtp mode {client | server | transparent | off} {vlan | mst | unknown}`	VTP モードを設定します。
ステップ 2	`Router(config)# vtp domain domain-name`	（サーバ モードでは任意）VTP ドメイン名（最大 32 文字）を定義します。VTP サーバ モードではドメイン名が必要です。スイッチで VTP ドメインにトランクを接続している場合、スイッチはドメインの VTP サーバからドメイン名を学習します。 **（注）**　ドメイン名は消去できません。
ステップ 3	`Router(config)# end`	VLAN コンフィギュレーション モードを終了します。

（注）　VTP がディセーブルの場合は、VLAN データベース モードでなく、コンフィギュレーション モードで VLAN コンフィギュレーション コマンドを入力でき、VLAN 設定はスタートアップ コンフィギュレーション ファイルに保存されます。

次に、スイッチを VTP サーバとして設定する例を示します。

```
Router# configuration terminal
Router(config)# vtp mode server
Setting device to VTP SERVER mode.
Router(config)# vtp domain lab_network
Setting VTP domain name to lab_network
Router(config)# end
Router#
```

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。

```
Router# configuration terminal
Router(config)# vtp mode client
Setting device to VTP CLIENT mode.
Router(config)# exit
Router#
```

次に、スイッチ上で VTP をディセーブルにする例を示します。

```
Router# configuration terminal
Router(config)# vtp mode transparent
Setting device to VTP TRANSPARENT mode.
Router(config)# end
Router#
```

次に、スイッチ上で VTP をディセーブルにし、VTP アドバタイズメントの転送をディセーブルにする例を示します。

```
Router# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# vtp mode off
Setting device to VTP OFF mode.
Router(config)# exit
Router#
```

次に、設定を確認する例を示します。

```
Router# show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 3
VTP Domain Name                 : lab_network
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0015.c724.0040

Feature VLAN:
--------------
VTP Operating Mode                : Server
Number of existing VLANs          : 6
Number of existing extended VLANs : 0
Configuration Revision            : 0
Primary ID                        : 0000.0000.0000
Primary Description               :
MD5 digest                        : 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
                                    0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00

Feature MST:
--------------
VTP Operating Mode                : Transparent

Feature UNKNOWN:
--------------
VTP Operating Mode                : Transparent

Router#
```

ポート単位の VTP モードの設定

VTP モードは、ポートごとに設定できます。VTP イネーブル値は、ポートがトランク モードでスイッチド ポートになる場合にだけ適用されます。着信および発信 VTP PDU は、転送*されるのではなく*ブロックされます。VTP バージョン 3 では、トランク単位でも VTP モードを設定できます。VTP 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	`Router(config)# interface` *type 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	`Router(config-if)# vtp`	指定したポートの VTP をイネーブルにします。
ステップ 3	`Router(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。

次に、ポートで VTP モードを設定する例を示します。

```
Router# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 3/5
Router(config-if)# vtp
Router(config-if)# end
Router#
```

次に、ポートで VTP モードをディセーブルにする例を示します。

```
Router# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 3/5
Router(config-if)# no vtp
Router(config-if)# end
Router#
```

次に、設定の変更を確認する例を示します。

```
Router# show vtp interface gigabitethernet 3/5

 Interface               VTP Status
-------------------------------------
 GigabitEthernet3/5       disabled
Router#
```

次に、インターフェイスを確認する例を示します。

```
Router# show vtp interface

 Interface               VTP Status
-------------------------------------
 GigabitEthernet3/1       enabled
 GigabitEthernet3/2       enabled
 GigabitEthernet3/3       enabled
 GigabitEthernet3/4       enabled
 GigabitEthernet3/5       disabled
 GigabitEthernet3/6       enabled
 ...
```

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
Router# **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。

```
Router# 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 config digest errors     : 0
Number of V1 summary errors        : 0

VTP pruning statistics:

Trunk            Join Transmitted Join Received    Summary advts received from
                                                   non-pruning-capable device
---------------- ---------------- ---------------- ---------------------------
Gi5/8               43071            42766            5
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

仮想ローカル エリア ネットワーク（VLAN）

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

VLAN の前提条件

なし。

VLAN の制約事項

- 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 の設定方法」（P.24-10）を参照）、グローバル コンフィギュレーション モードまたは config-vlan コンフィギュレーション モードで VLAN を設定できます。グローバル コンフィギュレーション モードおよび config-vlan コンフィギュレーション モードで VLAN を設定すると、VLAN の設定は vlan.dat ファイルに保存されます。VLAN の設定を表示するには、**show vlan** コマンドを入力します。

  スイッチが VLAN トランスペアレント モードの場合、copy **running-config startup-config** コマンドを使用して、VLAN の設定を startup-config ファイルに保存します。実行コンフィギュレーションをスタートアップ コンフィギュレーションとして保存したあとに、**show running-config** および **show startup-config** コマンドを使用すると、VLAN の設定が表示されます。
- 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 ドメイン名および 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。
- 拡張範囲 VLAN が設定できるのはグローバル コンフィギュレーション モードだけです。
- スーパーバイザ エンジンの冗長構成は、デフォルト以外の VLAN データ ファイル名または場所をサポートしません。冗長スーパーバイザ エンジンを持つスイッチに対して、**vtp file** *file_name* コマンドは入力しないでください。
- 冗長スーパーバイザ エンジンを取り付ける前に、デフォルト設定に戻るには **no vtp file** コマンドを入力します。
- VLAN を作成する前に、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 モードにしておく必要があります。VTP の設定手順については、第 24 章「VLAN トランキング プロトコル（VTP）」を参照してください。
- 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。
- 設定を完全にバックアップする場合は、vlan.dat ファイルをバックアップに追加します。

VLAN について

VLAN の概要

VLAN は、物理的な位置にかかわりなく、共通の要件を持つエンド ステーションのグループです。VLAN は、物理 LAN と同じ属性をすべて備えていますが、物理的に同じ LAN セグメントに置かれていないエンド ステーションでもグループ化することができます。

VLAN は、通常 IP サブネットワークと関連付けます。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 に属させる場合などです。VLAN 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 ポートの VLAN メンバーシップは、ポートごとに手動で割り当てます。

VLAN の範囲

（注）　4096 個の 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 について」（P.30-3）を参照）。

Cisco IOS Release 15.1SY は、IEEE 802.1Q 規格に準拠した 4096 VLAN をサポートします。これらの VLAN はいくつかの範囲に分かれています。各範囲の使用法は少しずつ異なります。VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）を使用している場合、これらの VLAN の一部は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 は伝播されないため、ネットワーク デバイスごとに手動で設定する必要があります。

表 25-1 に VLAN の範囲を示します。

表 25-1　VLAN の範囲

VLAN	範囲	使用状況	VTP によって伝播される
0、4095	予約済み	システム専用です。これらの VLAN は参照または使用できません。	—
1	標準	シスコ システムズのデフォルトです。この VLAN は使用できますが、削除できません。	Yes
2 ～ 1001	標準	イーサネット VLAN に使用します。作成、使用、削除できます。	Yes
1002 ～ 1005	標準	FDDI およびトークンリング用のシスコ システムズのデフォルトです。VLAN 1002 ～ 1005 は削除できません。	Yes
1006 ～ 4094	拡張	イーサネット VLAN 専用です。	No

次の情報が VLAN の範囲に適用されます。

- レイヤ 3 LAN ポート、WAN インターフェイスとサブインターフェイス、および一部のソフトウェアの機能は、拡張範囲内の内部 VLAN を使用します。内部使用に割り当てられている拡張範囲 VLAN は使用できません。
- 内部で使用されている VLAN を表示するには、**show vlan internal usage** コマンドを入力します。旧リリースの場合は、**show vlan internal usage** および **show cwan vlans** コマンドを入力します。
- 昇順の内部 VLAN 割り当て（1006 から昇順）、または降順の内部 VLAN 割り当て（4094 から降順）を設定できます。
- 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（「ブリッジ ID について」（P.30-3）を参照）。

VLAN のデフォルト設定

- VLAN ID：1（範囲：1 ～ 4094）
- VLAN 名：
  - VLAN 1：「default」

  - その他の VLAN：「VLAN*vlan_ID*」
- 802.10 SAID：10*vlan_ID*（範囲：100001 ～ 104094）
- MTU サイズ：1500（範囲：1500 ～ 18190）
- トランスレーショナル ブリッジ 1：0（範囲：0 ～ 1005）
- トランスレーショナル ブリッジ 2：0（範囲：0 ～ 1005）
- VLAN ステート：active（active、suspend）
- プルーニング適格性：
  - VLAN 2 ～ 1001 はプルーニング適格です。
  - VLAN 1006 ～ 4094 はプルーニング不適格です。

VLAN の設定方法

設定可能な VLAN パラメータ

（注）
- イーサネット VLAN 1 はデフォルト値だけ使用します。
- VLAN 名を除き、イーサネット VLAN 1006 ～ 4094 はデフォルト値だけ使用します。
- 1006 ～ 4094 のイーサネット VLAN に対し、VLAN 名を設定できます。

VLAN 2 ～ 1001 では、次のパラメータを設定できます。

- VLAN 名
- VLAN タイプ（イーサネット、FDDI、FDDI Network Entity Title（NET）、TrBRF、または TrCRF）
- VLAN 状態（アクティブまたは中断）
- Security Association Identifier（SAID）
- TrBRF VLAN のブリッジ識別番号
- FDDI および TrCRF VLAN のリング番号
- TrCRF VLAN の親 VLAN 番号
- TrCRF VLAN のスパニングツリー プロトコル（STP）タイプ

VLAN ロック

VLAN ロック機能は、目的の VLAN が設定されていることを確認する、特別レベルの検証です。VLAN ロックがイネーブルの場合、ポートをある VLAN から別の VLAN に変更する際に VLAN の名前を指定する必要があります。この機能は、アクセス ポートおよびトランク ポート用の VLAN またはプライベート VLAN を指定する **switchport** コマンド（インターフェイス コンフィギュレーション モード時）に影響します。

VLAN ロックがイネーブルの場合に、アクセス ポートおよびトランク ポートを設定する方法については、「レイヤ 2 スイッチング用の LAN インターフェイスの設定方法」（P.20-6）を参照してください。

VLAN ロックがイネーブルの場合に、プライベート VLAN 上でポートを設定する方法については、「プライベート VLAN の設定方法」（P.26-10）を参照してください。

デフォルトでは、VLAN ロックはディセーブルです。VLAN ロ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
`Router(config)# vlan port provisioning`	VLAN ロックをイネーブルにします。

イーサネット VLAN の作成または変更

ユーザ定義 VLAN には、予約済み VLAN を除く 1 ～ 4094 の一意の ID があります（表 25-1（P.25-3）を参照）。VLAN を作成するには、**vlan** コマンドを入力して、未使用 ID を指定します。既存の VLAN を変更するには、その VLAN に対して **vlan** コマンドを入力します（レイヤ 3 ポートまたはソフトウェア機能が使用している既存 VLAN は変更できません）。

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.25-3）を参照してください。**media** キーワードを使用して VLAN タイプを指定しない場合、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	`Router# 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	`Router(config)# vlan vlan_ID{[-vlan_ID]|[,vlan_ID]}`	単独のイーサネット VLAN、イーサネット VLAN の範囲、またはカンマで区切ったリストで複数のイーサネット VLAN を作成または変更します（スペースは挿入しないでください）。
ステップ 3	`Router(config-vlan)# end`	VLAN データベースを更新して、特権 EXEC モードに戻ります。

イーサネット VLAN を作成または変更する場合は、次の情報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を使用するには、1006 以降が割り当てられた内部 VLAN が必要であるため、4094 から始まる拡張範囲 VLAN を設定します。
- 拡張範囲 VLAN が設定できるのはグローバル コンフィギュレーション モードだけです。VLAN データベース モードでは拡張範囲 VLAN を設定できません。
- 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 を使用しています。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。

VLAN を削除する場合は、次の情報に注意してください。

- イーサネット VLAN 1 および FDDI、またはトークンリング VLAN 1002 ～ 1005 の、メディア タイプ別のデフォルト VLAN は削除できません。
- VLAN を削除すると、その VLAN に割り当てられ、アクセス ポートとして設定されている LAN ポートは、非アクティブになります。これらのポートは、新しい VLAN に割り当てられるまで、元の VLAN に（非アクティブのまま）対応付けられています。

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。

```
Router# configure terminal
Router(config)# vlan 3
Router(config-vlan)# end
Router# show vlan id 3

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
3    VLAN0003                         active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
3    enet  100003     1500  -      -      -        -    -        0      0

Primary Secondary Type              Interfaces
------- --------- ----------------- ------------------------------------------
```

VLAN へのレイヤ 2 LAN インターフェイスの割り当て

管理ドメイン内で作成された VLAN は、1 つまたは複数の LAN ポートを VLAN に割り当てない限り、未使用の状態です。

（注）　LAN ポートは必ず、適切なタイプの VLAN に割り当ててください。イーサネット ポートはイーサネットタイプの VLAN に割り当てます。

VLAN に 1 つまたは複数の LAN ポートを割り当てるには、「レイヤ 2 スイッチング用の LAN インターフェイスの設定方法」（P.20-6）に記載されている手順を行います。

内部 VLAN 割り当てポリシーの設定

VLAN 割り当ての詳細については、「VLAN の範囲」（P.25-3）を参照してください。

（注）　内部 VLAN 割り当てポリシーは、リロードのあとにだけ適用されます。

内部 VLAN 割り当てポリシーを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# vlan internal allocation policy {ascending | descending}`	内部 VLAN 割り当てポリシーを設定します。
ステップ 2	`Router(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	`Router# reload`	新しい内部 VLAN 割り当てポリシーを適用します。 **注意**　すぐに **reload** コマンドを入力する必要はありません。**reload** コマンドは、予定されているメンテナンス ウィンドウが表示されている間に入力します。

内部 VLAN 割り当てポリシーを設定する際、次の情報に注意してください。

- 1006 から昇順に内部 VLAN を割り当てるには、**ascending** キーワードを入力します。
- 4094 から降順に内部 VLAN を割り当てるには、**descending** キーワードを入力します。

次に、内部 VLAN 割り当てポリシーとして、降順を設定する例を示します。

```
Router# configure terminal
Router(config)# vlan internal allocation policy descending
```

VLAN 変換の設定

- 「VLAN 変換に関する注意事項および制約事項」（P.25-8）
- 「トランク ポート上の VLAN 変換の設定」（P.25-9）
- 「ポート グループ内の他のポートでの VLAN 変換のイネーブル化」（P.25-9）

（注）
- スパニングツリー ループが生じないように、VLAN 変換機能を正しく設定するよう注意してください。
- トランク ポート上では、ある VLAN 番号を他の VLAN 番号に変換することができます。これにより、ある VLAN で受信されたすべてのトラフィックが他の VLAN に転送されます。

VLAN 変換に関する注意事項および制約事項

VLAN の変換時には、次の注意事項および制約事項に従ってください。

- VLAN 変換設定は、レイヤ 2 トランクではないポートに適用される場合、非アクティブとなります。
- 802.1Q トランク上で、ネイティブ VLAN 入力トラフィックの変換を設定しないでください。802.1Q ネイティブ VLAN トラフィックはタグなしのため、変換の際に認識されません。他の VLAN から 802.1Q トランクのネイティブ VLAN に、トラフィックを変換することはできます。
- トランクの変換先の VLAN を削除しないでください。
- VLAN 変換の設定は、ポート グループ内のすべてのポートに適用されます。VLAN 変換は、ポート グループ内のすべてのポートで、デフォルトでディセーブルに設定されています。必要に応じて、ポートでの VLAN 変換をイネーブルにします。
- Cisco IOS Release 15.1SY では、IEEE 802.1Q トランキングのみサポートされます。

表 25-2　VLAN 変換をサポートするモジュール

製品番号	ポートの数	ポート グループの数	ポート範囲 ポート グループ単位	変換 ポート グループ単位
VS-S2T-10G-XL VS-S2T-10G	5	5	各グループで 1 つのポート	16
WS-X6908-10GE	8	8	各グループで 1 つのポート	16
WS-X6816-10T-2T、 WS-X6716-10T	16	16	各グループで 1 つのポート	16
WS-X6816-10G-2T、 WS-X6716-10GE	16	16	各グループで 1 つのポート	16
WS-X6704-10GE	4	4	各グループで 1 つのポート	128
WS-X6848-TX-2T、 WS-X6748-GE-TX	48	4	1 ～ 12 13 ～ 24 25 ～ 36 37 ～ 48	128
WS-X6848-SFP-2T、 WS-X6748-SFP	48	4	1 ～ 23（奇数） 2 ～ 24（偶数） 25 ～ 47（奇数） 26 ～ 48（偶数）	128
WS-X6824-SFP-2T、 WS-X6724-SFP	24	2	1 ～ 12 13 ～ 24	128

（注） ポートをトランクとして設定するには、「トランクとしてのレイヤ 2 スイッチング ポートの設定」（P.20-9）を参照してください。

トランク ポート上の VLAN 変換の設定

トランク ポート上で VLAN を変換するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface type slot/port`	設定するレイヤ 2 トランク ポートを選択します。
ステップ 2	`Router(config-if)# switchport vlan mapping enable`	VLAN 変換をイネーブルにします。
ステップ 3	`Router(config-if)# switchport vlan mapping original_vlan_ID translated_vlan_ID`	VLAN を他の VLAN に変換します。有効な範囲は、1 ～ 4094 です。 ポート上で元の VLAN から変換先 VLAN への VLAN マッピングを設定すると、元の VLAN に到着するトラフィックは、スイッチ ポートの入力時に変換先 VLAN にマッピングまたは変換されます。変換先 VLAN で内部的にタグ付けされたトラフィックは、スイッチ ポートを離れる前に元の VLAN にマッピングされます。この方式の VLAN マッピングが、双方向マッピングです。
ステップ 4	`Router(config-if)# end`	コンフィギュレーション モードを終了します。

次に、ギガビット イーサネット ポート 5/2 で VLAN 1649 を VLAN 755 にマッピングする例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 5/2
Router(config-if)# switchport vlan mapping 1649 755
Router(config-if)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show interface gigabitethernet 5/2 vlan mapping
State: enabled
Original VLAN Translated VLAN
------------- ---------------
  1649           755
```

ポート グループ内の他のポートでの VLAN 変換のイネーブル化

ポート グループ内の他のポートで VLAN 変換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	`Router(config)# interface type slot/port`	設定する LAN ポートを選択します。
ステップ 2	`Router(config-if)# switchport vlan mapping enable`	VLAN 変換をイネーブルにします。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。

次に、ポートで VLAN 変換をイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 5/2
Router(config-if)# switchport vlan mapping enable
Router(config-if)# end
```

VLAN 情報の保存

VLAN データベースは、vlan.dat ファイルに保存されます。running-config ファイルと startup-config ファイルのバックアップに加えて、vlan.dat ファイルのバックアップも作成しておく必要があります。既存のスーパーバイザ エンジンを交換する場合は、startup-config ファイルと vlan.dat ファイルをコピーしてシステムを復元します。vlan.dat ファイルはブートアップ時に読み取られるので、このファイルをアップロードしてから、スーパーバイザ エンジンをリロードする必要があります。ファイルの場所を表示するには、**dir vlan.dat** コマンドを使用します。ファイル（バイナリ）をコピーするには、**copy vlan.dat tftp** コマンドを使用します。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

プライベート VLAN

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

プライベート VLAN の前提条件

なし。

プライベート VLAN の制約事項

セカンダリ VLAN およびプライマリ VLAN

- プライベート VLAN を設定して、VTP をトランスペアレント モードに設定した後は、VTP モードをクライアントまたはサーバに変更できません。VTP については、第 24 章「VLAN トランキング プロトコル（VTP）」を参照してください。
- プライベート VLAN の設定後は、**copy running-config startup config** 特権 EXEC コマンドを使用して、VTP トランスペアレント モード設定およびプライベート VLAN 設定を startup-config ファイルに保存してください。スイッチがリセットした場合、プライベート VLAN をサポートするためにデフォルトで VTP トランスペアレント モードになる必要があります。
- VTP バージョン 1 および 2 では、VTP は、プライベート VLAN 設定を伝播しません。プライベート VLAN ポートを使用する装置ごとにプライベート VLAN を設定する必要があります。VTP バージョン 3 では、VTP はプライベート VLAN 設定を自動的に伝播します。
- VLAN 1 または VLAN 1002 ～ 1005 をプライマリ VLAN またはセカンダリ VLAN として設定できません。拡張 VLAN（VLAN ID 1006 ～ 4094）は、プライベート VLAN に属することができません。イーサネット VLAN だけをプライベート VLAN にすることができます。
- プライマリ VLAN には、1 つの独立 VLAN および複数のコミュニティ VLAN を関連付けることができます。独立 VLAN またはコミュニティ VLAN には、1 つのプライマリ VLAN だけを関連付けることができます。
- セカンダリ VLAN をプライマリ VLAN に関連付けられている場合、ブリッジ プライオリティなどのプライマリ VLAN の STP パラメータは、セカンダリ VLAN に伝播されます。ただし、STP パラメータが必ずしもその他のデバイスに伝播されるとはかぎりません。STP 設定を手動でチェックして、プライマリ VLAN、独立 VLAN、コミュニティ VLAN のスパニングツリー トポロジが一致することを確認してください。これらの VLAN が同じ転送データベースを適切に共有できるようにするためです。
- スイッチの MAC アドレス リダクション機能をイネーブルにする場合は、プライベート VLAN の STP トポロジが一致するように、ネットワーク内のすべてのデバイス上で MAC アドレス リダクション機能をイネーブルにする必要があります。
- プライベート VLAN が設定されているネットワーク内で、一部のデバイスの MAC アドレス リダクション機能をイネーブルにし、他のデバイスでディセーブルにした場合は（混在環境）、プライマリ VLAN や、関連付けられたすべての独立 VLAN およびコミュニティ VLAN に対してルート ブリッジが共通となるように、デフォルトのブリッジ プライオリティを使用します。MAC アドレス リダクション機能がシステム上でイネーブルであるかどうかに関係なく、この機能の対象範囲に矛盾がないようにしてください。MAC アドレス リダクションは個々のレベルにしか対応せず、範囲としてはすべての中間値を内部的に使用します。プライベート VLAN および MAC アドレス リダクション機能を持つルート ブリッジをディセーブルにし、ルート ブリッジに、ルート ブリッジ以外で使用される最も高いプライオリティの範囲よりもさらに高いプライオリティを設定する必要があります。
- セカンダリ VLAN に VLAN ACL（VACL）を適用できません（第 74 章「VLAN ACL（VACL）」を参照）。
- DHCP スヌーピングはプライベート VLAN 上でイネーブルにできます。プライマリ VLAN で DHCP スヌーピングをイネーブルにすると、DHCP スヌーピングはセカンダリ VLAN に伝播されます。セカンダリ VLAN で DHCP を設定しても、プライマリ VLAN をすでに設定している場合、DHCP 設定は有効になりません。
- プライベート VLAN でトラフィックを伝送しないデバイスのトランクから、プライベート VLAN をプルーニングすることを推奨します。
- プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN には、別々の Quality of Service（QoS）設定を適用できます （第 61 章「PFC QoS の概要」を参照）。

- プライベート VLAN を設定すると、スティッキ アドレス解決プロトコル（ARP）がデフォルトでイネーブルになり、レイヤ 3 プライベート VLAN インターフェイスで学習した ARP エントリはスティッキ ARP エントリになります。セキュリティ上の理由から、プライベート VLAN ポートのスティッキ ARP エントリには期限切れがありません。スティッキ ARP の設定については、「スティッキ ARP の設定」（P.76-10）を参照してください。
- プライベート VLAN インターフェイスの ARP エントリを表示して確認することを推奨します。
- スティッキ ARP は、ARP エントリ（IP アドレス、MAC アドレス、および送信元 VLAN）が期限切れしないようにすることにより、MAC アドレス スプーフィングを防ぎます。スティッキ ARP はインターフェイスごとに設定できます。スティッキ ARP の設定については、「スティッキ ARP の設定」（P.76-10）を参照してください。次の注意事項および制約事項が、プライベート VLAN のスティッキ ARP に適用されます。
  - レイヤ 3 プライベート VLAN インターフェイスで学習した ARP エントリは、スティッキ ARP エントリです。
  - IP アドレスが同じでも、MAC アドレスが異なるデバイスを接続すると、メッセージが表示され、ARP エントリは作成されません。
  - プライベート VLAN ポートのスティッキ ARP エントリには期限がないため、MAC アドレスが変更された場合は、プライベート VLAN ポートの ARP エントリを手動で削除する必要があります。プライベート VLAN の ARP エントリを手動で追加または削除する方法は、次のとおりです。

```
Router(config)# no arp 11.1.3.30
IP ARP:Deleting Sticky ARP entry 11.1.3.30

Router(config)# arp 11.1.3.30 0000.5403.2356 arpa
IP ARP:Overwriting Sticky ARP entry 11.1.3.30, hw:00d0.bb09.266e by
hw:0000.5403.2356
```

- プライマリ VLAN およびセカンダリ VLAN で VLAN マップを設定できます（「VLAN アクセス マップの適用」（P.74-5）を参照）。ただし、プライベート VLAN のプライマリ VLAN およびセカンダリ VLAN では、同一 VLAN マップを設定することを推奨します。
- フレームがプライベート VLAN 内においてレイヤ 2 で転送されると、入力側と出力側で同じ VLAN マップが適用されます。プライベート VLAN 内部から外部ポートにフレームがルーティングされると、プライベート VLAN マップが入力側で適用されます。
  - フレームがホスト ポートから無差別ポートにアップストリームで送信される場合は、セカンダリ VLAN で設定された VLAN マップが適用されます。
  - フレームが無差別ポートからホスト ポートにダウンストリームで送信される場合は、プライマリ VLAN で設定された VLAN マップが適用されます。

  プライベート VLAN の特定 IP トラフィックをフィルタリングするには、プライマリ VLAN およびセカンダリ VLAN の両方に VLAN マップを適用する必要があります。
- 発信されるすべてのプライベート VLAN トラフィックに Cisco IOS 出力 ACL を適用するには、プライマリ VLAN のレイヤ 3 VLAN インターフェイス上でこの ACL を設定します（第 72 章「MAC アドレスベースのトラフィック ブロッキング」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。
- Cisco IOS ACL を独立 VLAN またはコミュニティ VLAN には適用しないでください。独立 VLAN およびコミュニティ VLAN に適用される Cisco IOS ACL の設定は、VLAN がプライベート VLAN の設定に含まれている場合、非アクティブです。
- プライベート VLAN がレイヤ 2 でホストを分離していても、ホストはレイヤ 3 で互いに通信できます。

- プライベート VLAN では、次のスイッチド ポート アナライザ（SPAN）機能がサポートされます。
  - プライベート VLAN ポートを SPAN 送信元ポートとして設定できます。
  - プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN 上で VLAN-based SPAN（VSPAN; VLAN ベースの SPAN）を使用したり、単一の VLAN 上で SPAN を使用したりして、出力トラフィックまたは入力トラフィックを個別にモニタすることができます。
  - SPAN の詳細については、第 56 章「ローカル SPAN、RSPAN、および ERSPAN」を参照してください。

プライベート VLAN ポート

- プライマリ VLAN、独立 VLAN、またはコミュニティ VLAN にポートを割り当てるには、プライベート VLAN コンフィギュレーション コマンドだけを使用します。プライマリ VLAN、独立 VLAN、またはコミュニティ VLAN として設定する VLAN に割り当てられているレイヤ 2 アクセス ポートは、この VLAN がプライベート VLAN の設定に含まれている場合、非アクティブです。レイヤ 2 トランク インターフェイスは STP フォワーディング ステートのままです。
- PAgP または LACP EtherChannel に属するポートを、プライベート VLAN ポートとして設定しないでください。ポートがプライベート VLAN の設定に含まれている間は、そのポートの EtherChannel 設定はいずれも非アクティブです。
- 設定ミスによって STP ループが発生しないようにして、STP コンバージェンスを高速化するには、独立ホスト ポートおよびコミュニティ ホスト ポート上で PortFast および BPDU ガードをイネーブルにします（第 31 章「オプションの STP 機能」を参照）。イネーブルにすると、STP によってすべての PortFast 設定済みレイヤ 2 LAN ポートに BPDU ガード機能が適用されます。無差別ポートでは、PortFast および BPDU ガードをイネーブルにしないでください。
- プライベート VLAN の設定で使用される VLAN を削除すると、この VLAN に関連付けられたプライベート VLAN ポートが非アクティブになります。
- ネットワーク デバイスをトランク接続し、プライマリ VLAN およびセカンダリ VLAN がトランクから削除されていない場合、プライベート VLAN ポートはさまざまなネットワーク デバイス上で使用できます。
- プライベート VLAN に関連するすべてのプライマリ VLAN、独立 VLAN、コミュニティ VLAN では、トランク間で同一トポロジーを維持する必要があります。すべての関連 VLAN で同じ STP ブリッジ パラメータとトランク ポート パラメータを設定し、同一トポロジーを維持することを強く推奨します。

その他の機能の制限事項

- VTP バージョン 3 はプライベート VLAN（PVLAN）ポートではサポートされません。
- 一部の状況では、エラー メッセージが表示されずに設定が受け入れられますが、コマンドには効果がありません。
- プライベート VLAN が設定されたスイッチにフォールバック ブリッジングを設定しないでください。
- ポートが現在プライベート VLAN モードになっており、ポートがプライマリ ポート、独立ポート、コミュニティ ポートのうちのいずれかであることをプライベート VLAN 設定が示している場合、ポートはプライベート VLAN 機能だけに影響されます。ダイナミック トランキング プロトコル（DTP）などのその他のモードにポートがなっている場合、ポートはプライベート ポートとして機能しません。

- 次のようなその他の機能用に設定したインターフェイスでは、プライベート VLAN ポートを設定しないでください。
  - ポート集約プロトコル（PAgP）
  - リンク集約制御プロトコル（LACP）
  - 音声 VLAN
- IEEE 802.1x ポートベース認証をプライベート VLAN ポートで設定できますが、ポート セキュリティ、音声 VLAN、またはユーザごとの ACL と一緒に 802.1x をプライベート VLAN ポートに設定しないでください。
- プライベート VLAN のプライマリ VLAN またはセカンダリ VLAN として、Remote SPAN（RSPAN）VLAN を設定しないでください。SPAN の詳細については、第 56 章「ローカル SPAN、RSPAN、および ERSPAN」を参照してください。
- プライベート VLAN ホストまたは無差別ポートは、SPAN 宛先ポートにはできません。SPAN 宛先ポートをプライベート VLAN ポートとして設定すると、ポートは非アクティブになります。
- 宛先 SPAN ポートを独立ポートにしないでください。送信元 SPAN ポートを独立ポートにすることはできます。VSPAN を設定して、プライマリ VLAN およびセカンダリ VLAN の両方を拡張するか、入力トラフィックまたは出力トラフィックだけが重要な場合はそのどちらかを拡張できます。
- 各 VLAN 間でショートカットを使用する場合（このうちいずれかの VLAN がプライベート VLAN である場合）は、プライマリ VLAN、独立 VLAN、コミュニティ VLAN を考慮してください。プライマリ VLAN は、宛先および仮想送信元の両方として使用する必要があります。セカンダリ VLAN（真の送信元）が、レイヤ 2 FID テーブルでプライマリ VLAN に常に再マッピングされるからです。
- プライマリ VLAN の無差別ポートでスタティック MAC アドレスを設定する場合は、すべての関連セカンダリ VLAN に同じスタティック アドレスを追加する必要があります。セカンダリ VLAN のホスト ポートでスタティック MAC アドレスを設定する場合は、関連プライマリ VLAN に同じスタティック MAC アドレスを追加する必要があります。プライベート VLAN ポートからスタティック MAC アドレスを削除する場合は、設定した MAC アドレスのすべてのインスタンスをプライベート VLAN から削除する必要があります。

（注） プライベート VLAN の 1 つの VLAN で学習したダイナミック MAC アドレスは、関連 VLAN で複製されます。たとえば、セカンダリ VLAN で学習した MAC アドレスは、プライマリ VLAN で複製されます。元のダイナミック MAC アドレスが削除されるか期限切れになると、複製されたアドレスは MAC アドレス テーブルから削除されます。

- プライベート VLAN ポートを EtherChannel として設定しないでください。ポートはプライベート VLAN 設定の一部にすることができますが、ポートの EtherChannel 設定はいずれも非アクティブになります。

プライベート VLAN について

プライベート VLAN ドメイン

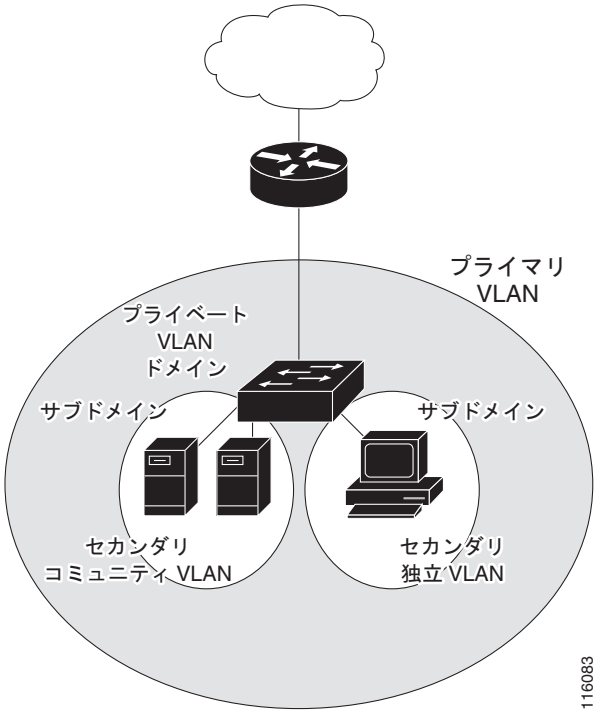
プライベート VLAN 機能では、サービス プロバイダーが VLAN の使用時に直面する、次の 2 つの問題に対処します。

- スイッチがサポートする VLAN は最大で 4096 です。サービス プロバイダーがカスタマーごとに 1 つの VLAN を割り当てる場合、サポートできるカスタマー数は制限されます。
- IP ルーティングをイネーブルにするには、各 VLAN にサブネット アドレス空間またはアドレス ブロックを割り当てます。これにより未使用の IP アドレスが無駄になり、IP アドレスの管理に問題が生じます。

プライベート VLAN を使用することにより、スケーラビリティの問題は解決され、サービス プロバイダーにとっては IP アドレスの管理が便利になり、カスタマーにはレイヤ 2 セキュリティが提供されます。

プライベート VLAN 機能により、VLAN のレイヤ 2 ブロードキャスト ドメインはサブドメインに分割されます。サブドメインは、プライマリ VLAN とセカンダリ VLAN で構成されるプライベート VLAN のペアで表されます。プライベート VLAN ドメインには複数のプライベート VLAN のペアを設定でき、それぞれのペアを各サブドメインに割り当てることができます。プライベート VLAN ドメイン内のすべての 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 は、サブドメインを識別します（図 26-1 を参照）。

図 26-1　　プライベート VLAN ドメイン



プライベート VLAN ドメインには、プライマリ VLAN が 1 つのみ含まれています。プライベート VLAN ドメインのポートはすべて、プライマリ VLAN のメンバです。言い換えれば、プライマリ VLAN はプライベート VLAN ドメイン全体です。

セカンダリ VLAN は、同じプライベート VLAN ドメイン内のポートをレイヤ 2 で分離します。セカンダリ VLAN には、次の 2 種類があります。

- 独立 VLAN：独立 VLAN 内のポートは、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 内のポートは相互に通信できますが、レイヤ 2 レベルでその他のコミュニティ内のポートと通信できません。

プライベート VLAN ポート

プライベート VLAN ポートには 3 種類があります。

- 無差別：無差別ポートはプライマリ VLAN に属し、プライマリ VLAN に関連付けられたセカンダリ VLAN に属するコミュニティ ホスト ポートおよび独立ホスト ポートも含めて、すべてのインターフェイスと通信できます。
- 独立：独立ポートは、独立セカンダリ VLAN に属するホスト ポートです。このポートは、無差別ポートを除く、同一プライベート VLAN ドメインのその他のポートからレイヤ 2 で完全に分離されています。プライベート VLAN は、無差別ポートからのトラフィックを除き、独立ポート宛のトラフィックをすべてブロックします。独立ポートから受信されたトラフィックは、無差別ポートだけに転送されます。
- コミュニティ：コミュニティ ポートは、コミュニティ セカンダリ VLAN に属するホスト ポートです。コミュニティ ポートは、同一コミュニティ VLAN のその他のポート、および無差別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他のすべてのインターフェイスおよびプライベート VLAN ドメイン内の独立ポートとレイヤ 2 で分離されます。

（注）　トランクは独立ポート、コミュニティ ポート、および無差別ポート間でトラフィックを伝達する VLAN をサポートできます。したがって、独立ポートおよびコミュニティ ポートのトラフィックはトランク インターフェイスを介してスイッチに送受信できます。

プライマリ VLAN、独立 VLAN、コミュニティ VLAN

プライマリ VLAN および 2 種類のセカンダリ VLAN（独立 VLAN およびコミュニティ VLAN）には、次の特性があります。

- プライマリ VLAN：無差別ポートからホスト ポート（独立とコミュニティ）およびその他の無差別ポートへの単一方向トラフィック ダウンストリームを搬送します。
- 独立 VLAN：プライベート VLAN ドメインの独立 VLAN は 1 つだけです。独立 VLAN はセカンダリ VLAN であり、ホストから無差別ポートおよびゲートウェイに向かう単一方向トラフィック アップストリームを搬送します。
- コミュニティ VLAN：コミュニティ VLAN はセカンダリ VLAN であり、コミュニティ ポートから同一コミュニティの無差別ポート ゲートウェイおよびその他のホスト ポートにアップストリーム トラフィックを搬送します。プライベート VLAN には、複数のコミュニティ VLAN を設定できます。

無差別ポートは、1 つのみのプライマリ VLAN、1 つの独立 VLAN、複数のコミュニティ VLAN を処理できます。レイヤ 3 ゲートウェイは一般的に、無差別ポートを介してスイッチに接続されます。無差別ポートでは、広範囲なデバイスをプライベート VLAN のアクセス ポイントとして接続できます。たとえば、すべてのプライベート VLAN サーバを管理ワークステーションからモニタしたりバックアップしたりするのに、無差別ポートを使用できます。

スイッチド環境では、個々の VLAN および対応する IP サブネットを、個々のステーションまたはステーションの共通のグループに割り当てることができます。エンド ステーションは、プライベート VLAN の外部にアクセスするために、デフォルト ゲートウェイだけと通信する必要があります。

プライベート VLAN ポートの分離

プライベート VLAN を使用すると、次のようにエンド ステーションへのアクセスを制御できます。

- エンド ステーションに接続されているインターフェイスを選択して独立ポートとして設定し、レイヤ 2 の通信をしないようにします。たとえば、エンド ステーションがサーバの場合、この設定によりサーバ間のレイヤ 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エンド ステーション（バックアップ サーバなど）に接続されているインターフェイスを無差別ポートとして設定し、すべてのエンド ステーションがデフォルト ゲートウェイにアクセスできるようにします。

複数のデバイスにわたるようにプライベート VLAN を拡張するには、プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN を、プライベート VLAN をサポートする他のデバイスにトランキングします。使用するプライベート VLAN 設定のセキュリティを確保して、プライベート VLAN 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、プライベート VLAN 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プライベート VLAN を設定します。

プライベート VLAN による IP アドレス指定方式

それぞれのカスタマーに別々の VLAN を割り当てると、次のように非効率的な IP アドレス指定方式が作成されます。

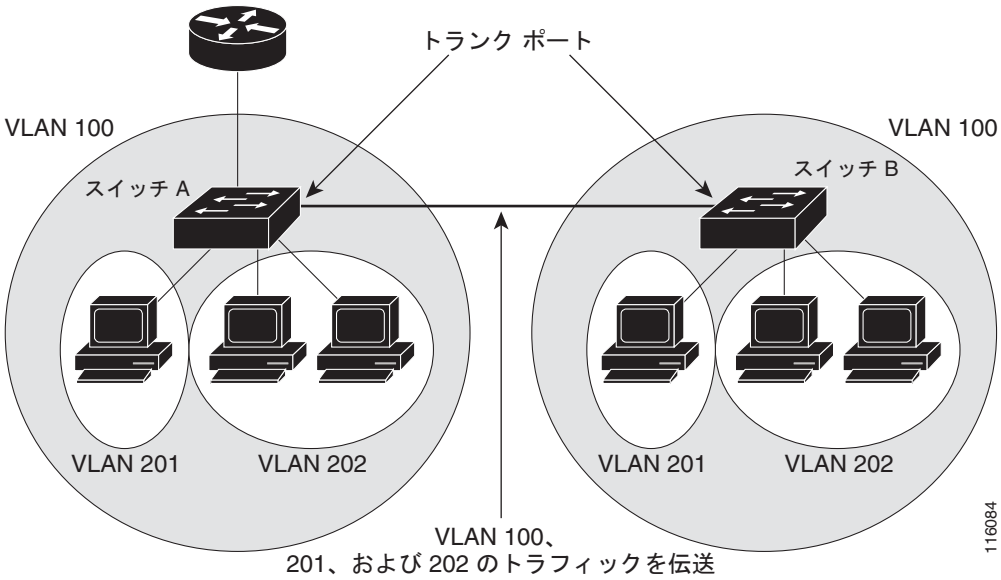
- カスタマー VLAN にアドレスのブロックを割り当てると、未使用 IP アドレスが発生することがあります。
- VLAN におけるデバイス数が増加する場合、割り当て済みアドレス数が増加に対応できるだけ十分に大きくないことがあります。

この問題は、プライベート VLAN を使用すると軽減します。プライベート VLAN では、プライベート VLAN のすべてのメンバが、プライマリ VLAN に割り当てられている共通アドレス空間を共有するためです。ホストはセカンダリ VLAN に接続され、プライマリ VLAN に割り当てられているアドレスのブロックから IP アドレスが DHCP サーバによってホストに割り当てられますが、同一プライマリ VLAN 内のセカンダリ VLAN には割り当てられません。さまざまなセカンダリ VLAN のカスタマー デバイスには後続 IP アドレスが割り当てられます。新しいデバイスを追加すると、サブネット アドレスの巨大プールから次に使用できるアドレスが、DHCP サーバによって割り当てられます。

複数のスイッチにまたがるプライベート VLAN

通常の VLAN と同様に、プライベート VLAN を複数のスイッチにまたがるように設定できます。トランク ポートはプライマリ VLAN およびセカンダリ VLAN を隣接スイッチに伝送します。トランク ポートは、プライベート VLAN をその他の VLAN のように処理します。複数のスイッチにまたがるプライベート VLAN の機能の場合、スイッチ A にある独立ポートからのトラフィックはスイッチ B に到達しません。（図 26-2 を参照）。

図 26-2　　複数のスイッチにまたがるプライベート 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 バージョン 1 および 2 はプライベート VLAN をサポートしないため、レイヤ 2 ネットワークのすべてのスイッチではプライベート VLAN を手動で設定する必要があります。ネットワーク内の一部のスイッチにプライマリおよびセカンダリ VLAN の関連を設定しない場合、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。この状況により、これらのスイッチ上のプライベート VLAN トラフィックが不要にフラッディングする可能性があります。

VTP バージョン 3 はプライベート VLAN をサポートしているため、レイヤ 2 ネットワークのすべてのスイッチではプライベート VLAN を手動で設定する必要はありません。

プライベート VLAN とその他の機能の相互作用

- 「プライベート VLAN 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.26-10）
- 「プライベート VLAN と SVI」（P.26-10）

プライベート VLAN 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

通常の VLAN の場合、同一 VLAN の各デバイスはレイヤ 2 レベルで相互に通信できますが、別々の VLAN のインターフェイスに接続しているデバイスはレイヤ 3 レベルで通信する必要があります。プライベート VLAN では、無差別ポートはプライマリ VLAN のメンバであり、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。プライベート VLAN ブロードキャスト転送は、次のようにブロードキャストを送信するポートに左右されます。

- 独立ポートは、無差別ポートまたはトランク ポートのみにブロードキャストを送信します。
- コミュニティ ポートは、すべての無差別ポート、トランク ポート、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。
- 無差別ポートは、プライベート VLAN のすべてのポート（他の無差別ポート、トランク ポート、独立ポート、コミュニティ ポート）にブロードキャストを送信します。

マルチキャスト トラフィックのルーティングとブリッジングは、プライベート VLAN 境界を横断して行われ、単一コミュニティ VLAN 内でも行われます。マルチキャスト トラフィックは、同じ独立 VLAN のポート間、または別々のセカンダリ VLAN のポート間では転送されません。

プライベート VLAN と SVI

スイッチ仮想インターフェイス（SVI）は、レイヤ 2 VLAN のレイヤ 3 インターフェイスです。レイヤ 3 デバイスは、セカンダリ VLAN ではなく、プライマリ VLAN だけを介してプライベート VLAN と通信します。プライマリ VLAN に対してだけ、レイヤ 3 VLAN SVI を設定します。セカンダリ VLAN にはレイヤ 3 VLAN インターフェイスを設定しないでください。VLAN がセカンダリ VLAN として設定されている間、セカンダリ VLAN の SVI は非アクティブになります。

- アクティブな SVI が設定された VLAN をセカンダリ VLAN として設定しようとすると、SVI をディセーブルにするまでは、設定が許可されません。
- セカンダリ VLAN として設定されている VLAN で SVI を作成し、セカンダリ VLAN がレイヤ 3 ですでにマッピングされている場合、SVI は作成されずにエラーが返されます。SVI がレイヤ 3 でマッピングされていない場合、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、マッピングされている場合、プライマリ VLAN 上のすべての設定がセカンダリ VLAN SVI に伝播されます。たとえば、プライマリ VLAN SVI に IP サブネットを割り当てると、このサブネットはプライベート VLAN 全体の IP サブネット アドレスになります。

プライベート VLAN のデフォルト設定

なし。

プライベート VLAN の設定方法

- 「プライベート VLAN としての VLAN の設定」（P.26-11）
- 「セカンダリ VLAN とプライマリ VLAN の関連付け」（P.26-12）

- 「プライマリ VLAN のレイヤ 3 VLAN インターフェイスへのセカンダリ VLAN のマッピング」（P.26-13）
- 「プライベート VLAN ホスト ポートとしてのレイヤ 2 インターフェイスの設定」（P.26-14）
- 「プライベート VLAN 無差別ポートとしてのレイヤ 2 インターフェイスの設定」（P.26-15）

（注）　VLAN がまだ定義されていない場合は、プライベート VLAN の設定プロセスを実行して、VLAN を定義します。

プライベート VLAN としての VLAN の設定

VLAN をプライベート VLAN 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	`Router(config)# vlan vlan_ID`	VLAN 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 2	`Router(config-vlan)# private-vlan {community | isolated | primary}`	VLAN をプライベート VLAN として設定します。 （注）　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実行されません。
ステップ 3	`Router(config-vlan)# end`	コンフィギュレーション モードを終了します。

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。

```
Router# configure terminal
Router(config)# vlan 202
Router(config-vlan)# private-vlan primary
Router(config-vlan)# end
Router# show vlan private-vlan

Primary Secondary Type              Interfaces
------- --------- ----------------- ------------------------------------------
202               primary
```

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。

```
Router# configure terminal
Router(config)# vlan 303
Router(config-vlan)# private-vlan community
Router(config-vlan)# end
Router# show vlan private-vlan

Primary Secondary Type              Interfaces
------- --------- ----------------- ------------------------------------------
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。

```
Router# configure terminal
Router(config)# vlan 440
Router(config-vlan)# private-vlan isolated
Router(config-vlan)# end
Router# show vlan private-vlan
```

```
Primary Secondary Type              Interfaces
------- --------- ----------------- ----------------------------------------
202               primary
        303       community
        440       isolated
```

セカンダリ VLAN とプライマリ VLAN 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、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# vlan primary_vlan_ID`	プライマリ VLAN の VLAN 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 2	`Router(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。
ステップ 3	`Router(config-vlan)# end`	VLAN コンフィギュレーション モードを終了します。

セカンダリ VLAN をプライマリ VLAN と関連付ける際は、次の情報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。複数のカンマ区切り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、単一のプライベート VLAN ID、またはハイフンで連結したプライベート VLAN 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 とプライマリ VLAN を関連付けるには、*secondary_vlan_list* を入力するか、*secondary_vlan_list* に **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 間の関連付けを消去するには、*secondary_vlan_list* に **remove** キーワードを使用します。
- このコマンドは、VLAN コンフィギュレーション サブモードを終了しない限り、有効になりません。

次の例は、コミュニティ VLAN 303 ～ 307、309、および独立 VLAN 440 をプライマリ VLAN 202 に関連付けて設定を確認する方法を示します。

```
Router# configure terminal
Router(config)# vlan 202
Router(config-vlan)# private-vlan association 303-307,309,440
Router(config-vlan)# end
Router# 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
```

プライマリ VLAN のレイヤ 3 VLAN インターフェイスへのセカンダリ VLAN のマッピング

（注）　独立 VLAN およびコミュニティ VLAN は、ともにセカンダリ VLAN と呼ばれます。

セカンダリ VLAN をプライマリ VLAN のレイヤ 3 VLAN インターフェイスにマッピングして、プライベート VLAN 入力トラフィックのレイヤ 3 スイッチングを可能にするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface vlan primary_vlan_ID`	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。
ステップ 2	`Router(config-if)# private-vlan mapping {secondary_vlan_list | add secondary_vlan_list | remove secondary_vlan_list}`	セカンダリ VLAN をプライマリ VLAN のレイヤ 3 VLAN インターフェイスにマッピングして、プライベート VLAN 入力トラフィックのレイヤ 3 スイッチングを可能にします。
	`Router(config-if)# [no] private-vlan mapping`	セカンダリ VLAN とプライマリ VLAN の間のマッピングを消去します。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。

セカンダリ VLAN をプライマリ VLAN のレイヤ 3 VLAN インターフェイスにマッピングする際は、次の情報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 スイッチングされるプライベート VLAN 入力トラフィックにだけ作用します。
- *secondary_vlan_list* パラメータには、スペースを含めないでください。複数のカンマ区切り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、単一のプライベート VLAN ID、またはハイフンで連結したプライベート VLAN 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* パラメータを入力するか、*secondary_vlan_list* パラメータに **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* パラメータに **remove** キーワードを使用します。

次の例は、プライベート VLAN 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て、設定を確認する例を示します。

```
Router# configure terminal
Router(config)# interface vlan 202
Router(config-if)# private-vlan mapping add 303-307,309,440
Router(config-if)# end
Router# 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

Router#
```

プライベート VLAN ホスト ポートとしてのレイヤ 2 インターフェイスの設定

レイヤ 2 インターフェイスをプライベート VLAN 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	`Router(config)# interface type slot/port`	設定する LAN ポートを選択します。
ステップ 2	`Router(config-if)# switchport`	LAN ポートをレイヤ 2 スイッチング用に設定します。 • LAN ポートをレイヤ 2 インターフェイス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 度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さらに **switchport** コマンドを入力してください。 • インターフェイスに対して **switchport** コマンドを一度も入力していない場合にかぎり、必須です。
ステップ 3	`Router(config-if)# switchport mode private-vlan {host | promiscuous}`	レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。
ステップ 4	`Router(config-if)# switchport private-vlan host-association primary_vlan_ID secondary_vlan_ID`	レイヤ 2 ポートをプライベート VLAN と関連付けます。 （注）　VLAN のロックがイネーブルになっている場合は、VLAN の番号の代わりに VLAN の名前を入力します。詳細については、「VLAN ロック」（P.25-5）を参照してください。
ステップ 5	`Router(config-if)# end`	コンフィギュレーション モードを終了します。

次に、インターフェイス GigabitEthernet 5/1 をプライベート VLAN 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。

```
Router# configure terminal
Router(config)# interface gigabitethernet 5/1
Router(config-if)# switchport mode private-vlan host
Router(config-if)# switchport private-vlan host-association 202 303
Router(config-if)# end
Router# show interfaces gigabitethernet 5/1 switchport | include private-vlan
Administrative Mode: private-vlan host
Administrative private-vlan host-association: 202 (VLAN0202) 303 (VLAN0303)
Administrative private-vlan mapping: none
Operational private-vlan: none
```

プライベート VLAN 無差別ポートとしてのレイヤ 2 インターフェイスの設定

レイヤ 2 インターフェイスをプライベート VLAN 無差別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	`Router(config)# interface type slot/port`	設定する LAN インターフェイスを選択します。
ステップ 2	`Router(config-if)# switchport`	LAN 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。 • LAN インターフェイスをレイヤ 2 インターフェイスとして設定するには、キーワードを指定せずに **switchport** コマンドを一度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さらに **switchport** コマンドを入力してください。 • インターフェイスに対して **switchport** コマンドを一度も入力していない場合にかぎり、必須です。
ステップ 3	`Router(config-if)# switchport mode private-vlan {host | promiscuous}`	レイヤ 2 ポートをプライベート VLAN 無差別ポートとして設定します。
ステップ 4	`Router(config-if)# switchport private-vlan mapping primary_vlan_ID {secondary_vlan_list | add secondary_vlan_list | remove secondary_vlan_list}`	プライベート VLAN 無差別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。 （注）　VLAN のロックがイネーブルになっている場合は、VLAN の番号の代わりに VLAN の名前を入力します。詳細については、「VLAN ロック」（P.25-5）を参照してください。
	`Router(config-if)# no switchport private-vlan mapping`	プライベート VLAN 無差別ポートと、プライマリ VLAN および任意のセカンダリ VLAN 間のすべてのマッピングを消去します。
ステップ 5	`Router(config-if)# end`	コンフィギュレーション モードを終了します。

レイヤ 2 インターフェイスをプライベート VLAN 無差別ポートとして設定する際は、次の情報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。複数のカンマ区切り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、単一のプライベート VLAN ID、またはハイフンで連結したプライベート VLAN ID の範囲です。
- VLAN ロックがイネーブルになっている場合は、VLAN の番号の代わりに VLAN の名前を *secondary_vlan_list* に入力します。VLAN の名前の範囲を入力する場合は、VLAN の名前とダッシュの間にスペースを入力してください。
- セカンダリ VLAN をプライベート VLAN 無差別ポートにマッピングするには、*secondary_vlan_list* の値を入力するか、または *secondary_vlan_list* の値を指定して **add** キーワードを使用します。
- セカンダリ VLAN とプライベート VLAN 無差別ポートの間のマッピングを消去するには、*secondary_vlan_list* の値を指定して **remove** キーワードを使用します。

次に、インターフェイス GigabitEthernet 5/2 をプライベート VLAN 無差別ポートとして設定し、そのインターフェイスをプライベート VLAN にマッピングする例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 5/2
Router(config-if)# switchport mode private-vlan promiscuous
Router(config-if)# switchport private-vlan mapping 202 303,440
Router(config-if)# end
```

次に、設定を確認する例を示します。

```
Router# show interfaces gigabitethernet 5/2 switchport | include private-vlan
Administrative Mode: private-vlan promiscuous
Administrative private-vlan host-association: none ((Inactive))
Administrative private-vlan mapping: 202 (VLAN0202) 303 (VLAN0303) 440 (VLAN0440)
Operational private-vlan: none
```

プライベート VLAN のモニタ

表 26-1 は、プライベート VLAN アクティビティをモニタするための特権 EXEC コマンドを示しています。

表 26-1　プライベート VLAN モニタリング コマンド

コマンド	目的
show interfaces status	インターフェイスが属している VLAN を含めて、インターフェイスのステータスを表示します。
show vlan private-vlan [type]	スイッチのプライベート VLAN 情報を表示します。
show interface switchport	インターフェイス上のプライベート VLAN 設定を表示します。
show interface private-vlan mapping	VLAN SVI のプライベート VLAN マッピングに関する情報を表示します。

次に、**show vlan private-vlan** コマンドの出力例を示します。

```
Switch(config)# show vlan private-vlan
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
10      501       isolated          Gi2/1, Gi3/1, Gi3/2
10      502       community         Gi2/11, Gi3/1, Gi3/4
10      503       non-operational
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

プライベート ホスト

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

プライベート ホストの前提条件

なし。

プライベート ホストの制約事項

- 「プライベート ホストのマルチキャスト動作」（P.27-4）

一般的なプライベート ホストの制約事項

- プライベート ホストおよびプライベート VLAN の両方は同じポート（インターフェイス）に設定できません。両方の機能はスイッチ上で共存できますが、それぞれの機能は異なるポートに設定する必要があります。
- プライベート ホストはエンドツーエンド機能です。この機能は DSLAM とアップストリーム デバイス（BRAS またはマルチキャスト サーバなど）の間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。
- 独立ポートとして設定できるのは信頼できるポートだけです。
- プライベート ホスト機能は、トランキング スイッチ ポートとして設定されているレイヤ 2 インターフェイス上でサポートされています。
- プライベート ホスト機能は、ポートチャネル インターフェイス上（EtherChannel、ファスト EtherChannel、ギガビット EtherChannel）でサポートされています。プライベート ホストは、ポートチャネル インターフェイス上でイネーブルにします。この機能をメンバ ポート上でイネーブルにできません。
- DAI および DHCP スヌーピングは、ポート上のすべての VLAN がスヌーピング対応に設定されている場合を除き、プライベート ホスト上でイネーブル化できません。

プライベート ホスト ACL の制約事項

- このリリースのプライベート ホスト機能は、プロトコル独立型 MAC ACL を使用します。

  プライベート ホスト用に設定されたポートには、IP ベース ACL を適用しないでください。適用すると、プライベート ホスト機能が無効になります（スイッチがポートにプライベート ホスト MAC ACL を適用できないため）。
- 次のインターフェイス タイプをプロトコル独立型 MAC ACL フィルタリングに設定できます。
  - IP アドレスのない VLAN インターフェイス
  - EoMPLS をサポートする物理 LAN ポート
  - EoMPLS をサポートする論理 LAN サブインターフェイス
- プロトコル独立型 MAC ACL フィルタリングでは、すべての入力トラフィック タイプ（MAC レイヤ トラフィック、IPv4 トラフィック、IPv6 トラフィック、MPLS トラフィックなど）に MAC ACL が適用されます。
- プロトコル独立型 MAC ACL によって許可または拒否された入力トラフィックは、出力インターフェイスによって MAC レイヤ トラフィックとして処理されます。プロトコル独立型 MAC ACL フィルタリング用に設定されたインターフェイスの MAC ACL によって許可または拒否されたトラフィックに、出力 IP ACL を適用できません。
- IP アドレスが設定されている VLAN インターフェイス上で、プロトコル独立型 MAC ACL フィルタリングを設定しないでください。
- 許可トラフィックが PFC または DFC によってハードウェアでブリッジングされる、またはレイヤ 3 スイッチングされた場合、microflow ポリシングにプロトコル独立型 MAC ACL フィルタリングを設定しないでください。
- 許可トラフィックがソフトウェアでルーティングされる場合、プロトコル独立型 MAC ACL フィルタリングはマイクロフロー ポリシングをサポートします。

- 既存の VLAN ACL（VACL）およびルーティング ACL（RACL）とトランク ポートの PACL との干渉を避けるには、トランク ポート インターフェイス上のアクセス グループ モードをポート モード優先に設定します。プライベート ホスト用に設定されているポートに VACL または RACL を設定しないでください。

トランク ポート上のプライベート ホスト VLAN の制約事項

- プライベート ホスト用に設定されたトランクポートを使用して VLAN 上で IGMP スヌーピングをイネーブル化できます。
- プライベート ホスト用に設定されたトランクポートを使用して VLAN 上で IP マルチキャストをイネーブル化できません。
- PACL はトランク ポート上で、上書きモードで動作するため、VLAN ベースの機能をスイッチ ポートに適用できません。
- マルチキャスト VLAN レジストレーション（MVR）機能は、マルチキャスト送信元が無差別ポートにある場合は、プライベート ホストと共存できます。

プライベート ホストとその他の機能の相互作用

- プライベート ホストはレイヤ 2 ベースのサービス（MAC 制限、ユニキャスト フラッディング プロテクション（UFP)、不明なユニキャストフラッディングのブロック（UUFB)）には影響しません。
- プライベート ホスト機能は、IGMP スヌーピングには影響しません。ただし、IGMP スヌーピングがグローバルにディセーブル化されている場合は、IGMP 制御パケットが ACL チェックの対象になります。IGMP 制御パケットを許可するには、プライベート ホスト ソフトウェアでマルチキャスト permit ステートメントを独立ホスト用の PACL に追加します。この操作は自動で行われ、ユーザの介入を必要としません。
- 独立ポートでポート セキュリティをイネーブルにして、これらのポートにセキュリティを追加できます。
- 無差別ポート、または混合ポートでイネーブル化された場合は、ポート セキュリティ機能がアップストリーム デバイス用（BRAS またはマルチキャスト サーバなど）の送信元ポート内の変更を制限する場合があります。
- アクセス ポートでイネーブル化された場合は、802.1X はプライベート ホスト機能の影響を受けません。

プライベート ホストのスプーフィングからの保護

プライベート ホスト機能は MAC アドレス スプーフィングを防ぎますが、カスタマー MAC または IP アドレスを有効化しません。MAC アドレス スプーフィングを防ぐため、プライベート ホスト機能は次の処理を行います。

- BRAS またはマルチキャスト サーバにスタティック MAC アドレスを使用します。
- レイヤ 2 転送テーブル上での学習をディセーブル化します。
- BRAS またはマルチキャスト サーバがソース ポートから別のポートに移動した場合に、スイッチ ソフトウェアに通知します。ソフトウェアは移動を確認し、レイヤ 2 転送テーブルを更新します。

プライベート ホストのマルチキャスト動作

アップストリーム デバイス（BRAS やマルチキャスト サーバなど）から発信されるマルチキャスト トラフィックは常に許可されます。また、プライベート ホスト PACL はマルチキャスト制御パケット（IGMP クエリーや Join 要求など）には適用されません。この動作により独立ホストは、マルチキャスト グループに参加したり、IGMP クエリーに応答したり、関連するすべてのグループからのトラフィックを受信できるようになります。

ホストから発信されたマルチキャスト トラフィックは、プライベート ホスト PACL によりドロップされます。ただし、他のホストが、あるホストから発信されたマルチキャスト トラックを受信する必要がある場合、プライベート ホスト機能は PACL に *multicast permit* エントリを追加します。

プライベート ホストについて

プライベート ホストの概要

一般的に、サービス プロバイダーはトリプルプレイ サービス（音声、ビデオ、データ）を提供する際、各ユーザ向けの 1 つの物理インターフェイス上で 3 つの VLAN を使用します。サービス プロバイダーが複数のエンド ユーザ向けに VLAN を 1 セット導入できれば、サービス インフラストラクチャは、よりシンプルになり拡張性も向上しますが、サービス プロバイダーはレイヤ 2 のユーザ（ホスト）間のトラフィックを分離できなければなりません。プライベート ホスト機能を使用すれば、この分離が可能になり複数のエンド ユーザ間で VLAN 共有ができます。

プライベート ホスト機能の主な利点は次のとおりです。

- 同じ VLAN ID を共有しているホスト（加入者）間のトラフィックを分離
- 異なる加入者間で VLAN ID を再利用することで、4096 の VLAN の使用率を高め、VLAN の拡張性を向上
- サービス拒絶（DoS）攻撃からの保護を目的としたメディア アクセス コントロール（MAC）アドレス スプーフィングの防止

プライベート ホスト機能はプロトコル独立型のポートベース アクセス コントロール リスト（PACL）を使用して、完全レイヤ 2 上における信頼できるポート上のホスト間のレイヤ 2 分離を可能にします。PACL では、スイッチ ポートにレイヤ 2 フォワーディング制約を課すことによって、ホストが分離されます。

VLAN でのホストの分離

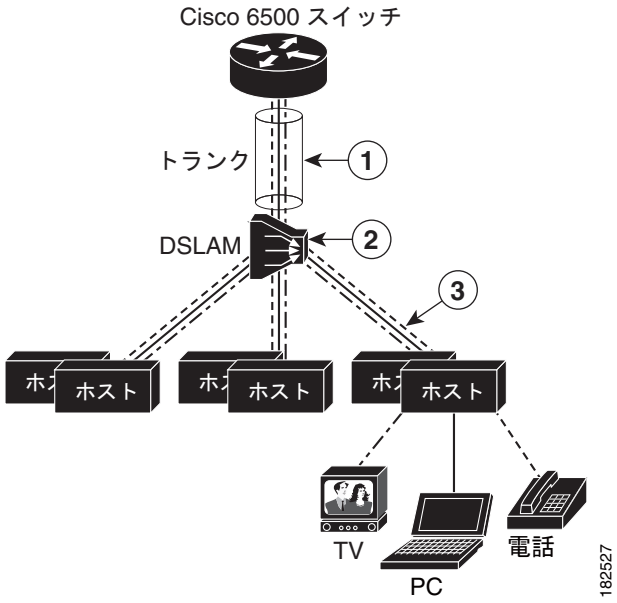
ホストを分離すると、サービス プロバイダーは同じセットのブロードバンド、またはメトロ イーサネット サービスを複数のエンド ユーザに配信する場合、1 セットの VLAN を使用できます。また、その VLAN 内でホスト同士が直接接続することもなくなります。たとえば、VLAN 10 を音声トラフィック、VLAN 20 をビデオ トラフィック、VLAN 30 をデータ トラフィックに使用できます。

スイッチが、デジタル加入者線アクセス マルチプレクサ（DSLAM）ギガビット イーサネット アグリゲータとして使われている場合、DSLAM は、複数の VLAN にデータを伝送できるトランク ポートを介してスイッチに接続されます。サービス プロバイダーは、1 つの物理ポートと 1 セットの VLAN を使って、サービスの同じセットを異なるエンド ユーザ（独立ホスト）に配信できます。それぞれの VLAN は個別のサービス（音声、ビデオ、データ）に使用できます。

図 27-1 に、スイッチから DSLAM に接続している複数のエンド ユーザにトリプルプレイ サービスを配信する例を示します。図における次の点に注意してください。

- スイッチと DSLAM 間の単一のトランク リンクによって、3 つの VLAN すべてのトラフィックが伝送されます。
- 仮想回線（VC）は、DSLAM から個別のエンド ユーザへ VLAN トラフィックを伝送します。

図 27-1　　VC から VLAN へのマッピング



1	トランク リンクは次の VLAN を伝送します。 • 音声 VLAN × 1 • ビデオ VLAN × 1 • データ VLAN × 1	2	DSLAM は、音声、ビデオ、およびデータ トラフィックを VLAN と VC の間にマッピングします。
		3	各 VC は、DSLAM と各ホスト間で音声、ビデオ、およびデータ トラフィックを伝送します。

トラフィック フローの制限（Private Hosts ポート モードおよび PACL の使用）

プライベート ホスト機能は PACL を使い、プライベート ホスト用に設定された各ポートを通過するトラフィックのタイプを制限できます。ポートのモード（ポートでプライベート ホストをイネーブルにするときに指定）によって、ポートに適用される PACL のタイプが決まります。各タイプの PACL は、それぞれ異なるタイプのトラフィックのトラフィック フローを制限します（たとえば、コンテンツ サーバから独立ホスト、独立ホストからサーバ、独立ホスト間のトラフィックなど）。

次のリストで、プライベート ホスト機能で使用されるポート モードを説明します（図 27-2 を参照）。

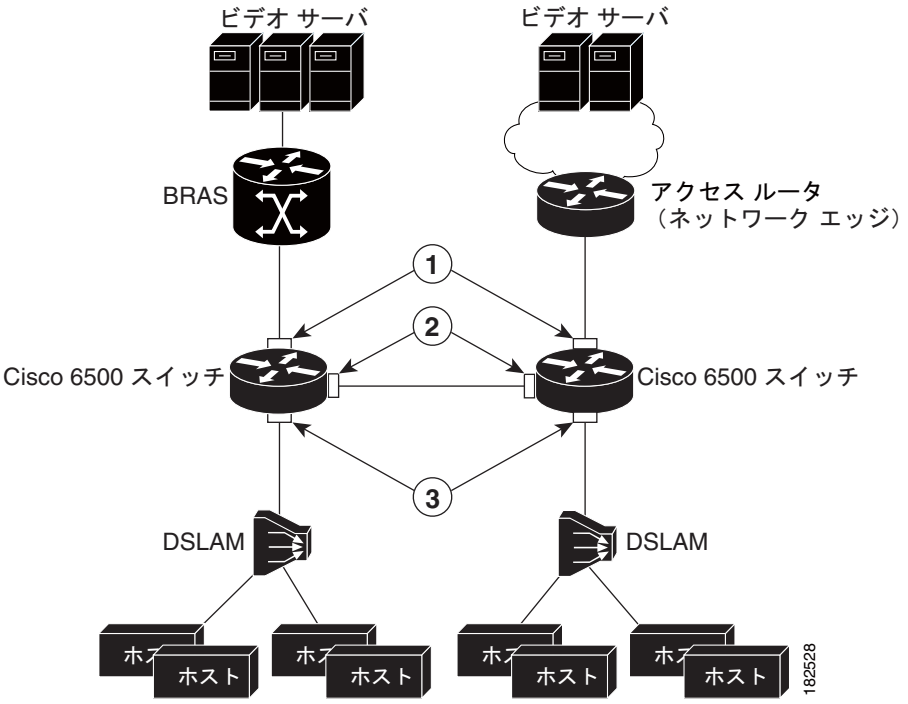
- 独立：エンド ユーザ（独立ホスト）が接続される DSLAM に接続されるポート。この場合ポートにおける VLAN 上のホストは、それぞれが独立している必要があります。このタイプのポートに接続されているホストは、アップストリーム デバイスだけにユニキャスト トラフィックを通過させることができます。
- 無差別：コア ネットワーク側か、Broadband Remote Access Server（BRAS; ブロードバンド リモート アクセス サーバ）デバイス側にあるポート、およびブロードバンド サービスを提供するマルチキャスト サーバ。
- 混合：スイッチを相互接続するポート。このタイプのポートは、スパニングツリー プロトコル（STP）の変更により、独立ポートとしても、無差別ポートとしても機能します。これらのポートは、アップストリーム デバイス（BRAS またはマルチキャスト サーバなど）へのユニキャスト トラフィックだけが可能です。

プライベート ホスト機能は、次の方法でトラフィックのフローを制限します。

- サービス プロバイダー ネットワークに入るブロードキャスト トラフィックは、BRAS およびマルチキャスト サーバ（ビデオ サーバなど）にリダイレクトされます。
- アクセス スイッチ（相互に接続されているスイッチ）間のユニキャスト トラフィックは、すべてブロックされます（BRAS またはマルチキャスト サーバに誘導されるものを除く）。
- Unknown Unicast Flood Blocking（UUFB; 不明なユニキャストフラッディングのブロック）機能は、DSLAM 側のポート上の不明なユニキャストのブロックに使用されます。

図 27-2 でプライベート ホストの設定で使用する各タイプのポート モード（独立、無差別、混合）を説明します。

図 27-2　プライベート ホストのポート タイプ（モード）



1	無差別ポート	BRAS からホストへのすべてのトラフィックを許可。
2	混合ポート	BRAS からのブロードキャスト トラフィックを許可。 ホストから無差別モード、および混合モードのポートへのブロードキャスト トラフィックをリダイレクト。 BRAS からホスト、およびホストから BRAS へのトラフィックを許可。 ホスト トラフィックへの他すべてのホストを拒否。
3	独立ポート	ホストから BRAS へのユニキャスト トラフィックだけを許可。ポート間のユニキャスト トラフィックをブロック。 ホストから BRAS へのすべてのブロードキャストをリダイレクト。 BRAS からのトラフィックを拒否（スプーフィング防止のため）。 マルチキャスト トラフィックを許可（IPv4 および IPv6）。

（注） このポート タイプの説明において、BRAS という用語は BRAS、マルチキャスト サーバ（ビデオ サーバなど）などのアップストリーム デバイス、またはこれらのデバイスへのアクセスを提供するコア ネットワーク デバイスを意味します。

ポート ACL

プライベート ホスト機能は、レイヤ 2 フォワーディングの制限をスイッチ ポートに課すために、ポート ACL（PACL）を数タイプ作成します。このソフトウェアは、ブロードバンド サービスと、これらのサービスを配信する独立ホストの VLAN ID を提供しているコンテンツ サーバの MAC アドレスに基づき、異なるタイプのプライベート ホスト ポート用に PACL を作成します。各プライベート ホスト ポートが動作するモードを指定すると、ポートのモード（独立、無差別、または混合）に基づいて、ソフトウェアによって適切な PACL がポートに適用されます。

次に、プライベート ホスト機能に使用される各タイプの PACL を示します。

独立ホスト PACL

独立ポート用 PACL の例：

```
deny host BRAS_MAC any
permit any host BRAS_MAC
redirect any host FFFF.FFFF.FFFF to LTLIndex 6
permit any 0100.5E00.0000/0000.007F.FFFF
permit any 3333.0000.0000/000.FFFF.FFFF
deny any any
```

無差別ポート PACL

無差別ポート用 PACL の例：

```
permit host BRAS_MAC any
deny any any
```

混合ポート PACL

混合ポート用 PACL の例：

```
permit host BRAS_MAC ffff.ffff.ffff
redirect any host FFFF.FFFF.FFFF to LTLIndex 6
permit host BRAS_MAC any
permit any host BRAS_MAC
deny any any
```

プライベート ホストのデフォルト設定

なし。

プライベート ホストの設定方法

設定の概要

1. Private Hosts 機能で使用するスイッチ ポート（インターフェイス）を決定します。トランキング スイッチ ポートまたはポートチャネル インターフェイスの機能を設定できます。プライベート ホストは、ポートチャネル インターフェイス上でイネーブルにする必要があります。この機能をメンバ ポート上でイネーブルにすることはできません。
2. 各ポート（インターフェイス）を標準、非プライベート ホスト サービス用に設定します。ポートのアクセス グループ モードをポート モード優先に設定します。この手順の VLAN 設定は、後で設定できます。
3. エンド ユーザにブロードバンド サービスを配信する VLAN または VLAN のセットを決定します。プライベート ホスト機能により、これらの VLAN におけるホスト間のレイヤ 2 分離が可能になります。
4. エンド ユーザ（独立ホスト）にブロードバンド サービスを提供するために使用するすべての BRAS とマルチキャスト サーバの MAC アドレスを識別します。

（注）　サーバがスイッチに直接接続されていない場合は、サーバへのアクセスを提供するコア ネットワーク デバイスの MAC アドレスを指定します。

5. （任意）異なるセットの独立ホストに、異なるタイプのブロードバンド サービスを提供する場合は、複数の MAC および VLAN リストを作成します。
   - 各 MAC アドレス リストでは、特定のタイプのサービスを提供するサーバまたはサーバ セットを指定します。
   - 各 VLAN リストが、そのサービスを配信する独立ホストを識別します。

6. 無差別ポートを設定し、特定のサービス タイプ用のサーバと受信ホストを識別する MAC リストと VLAN リストを指定します。

（注）　異なるセットのホストに、異なるタイプのサービスを配信できるようにするには、複数の MAC と VLAN の組み合わせを指定できます。たとえば、xxxx.xxxx.xxxx の BRAS を使用して VLAN 20、25、および 30 で基本的なサービス セットを提供し、yyyy.yyyy.yyyy の BRAS を使用して VLAN 5、10、および 15 で高品質のサービス セットを提供できます。

7. プライベート ホストをグローバルにイネーブル化します。
8. 個々のポート（インターフェイス）でプライベート ホストをイネーブル化し、ポートの動作モードを指定します。ポート モードを決定するには、ポートがアップストリーム側（コンテンツ サーバ方向、またはコアネットワーク方向）か、またはダウンストリーム側（DSLAM および独立ホスト方向）か、または他のスイッチに接続されているか（通常、リング トポロジの場合）を判断する必要があります。「トラフィック フローの制限（Private Hosts ポート モードおよび PACL の使用）」（P.27-5）を参照してください。

個別のポートで Private Hosts 機能をイネーブルにすると、スイッチでこの機能を実行する準備が整います。プライベート ホスト ソフトウェアは、ユーザが定義した MAC および VLAN リストを使用して、設定用の独立、無差別および混合モード PACL を作成します。次に、ソフトウェアが各プライベート ホストに適切な PACL を、ポート モードに基づいて適用します。

詳細設定手順

プライベート ホスト機能を設定するには、次の手順を実行します。次の手順は、プライベート ホストに使用するレイヤ 2 インターフェイスの設定がすでに済んでいることを前提としています。

（注）　トランキング スイッチ ポートまたは EtherChannel ポート上でだけ、プライベート ホストを設定できます。また、DSLAM とアップストリーム デバイスの間にあるすべてのスイッチで Private Hosts をイネーブルにする必要があります。

	コマンドまたはアクション	目的
ステップ 1	`Router# 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	`Router(config)# private-hosts mac-list mac_list_name mac_address [remark device-name | comment]`	ブロードバンド サービスの提供に使用する BRAS とマルチキャスト サーバを識別する MAC アドレス リストを作成します。 • *mac_list_name* は、このコンテンツ サーバのこのリストに割り当てる名前を指定します。 • *mac_address* は、特定のブロードバンド サービスまたはサービス セットを提供する BRAS またはマルチキャスト サーバ（サーバ セット）を指定します。 • **remark** を使用すると、この MAC リストに割り当てるデバイス名またはコメントをオプションで指定できます。 サービスを提供するために使用されるすべてのコンテンツ サーバの MAC アドレスを指定します。異なるタイプのサービスを異なるホストのセットに提供する場合は、特定のサービスを提供するサーバまたはサーバ セットごとに別々の MAC リストを作成します。 **（注）** サーバがスイッチに直接接続されていない場合は、サーバへのアクセスを提供するコア ネットワーク デバイスの MAC アドレスを指定します。
ステップ 3	`Router(config)# private-hosts vlan-list vlan-IDs`	分離する必要があるホストの VLAN（*vlan-IDs*）リストを作成し、そのホストがブロードバンド サービスを受信できるようにします。 特定のサービスを異なるホストのセットに提供する場合は、別々の VLAN リストを作成します。それ以外の場合は、すべてのブロードバンド サービスがすべての独立ホストに提供されます。
ステップ 4	`Router(config)# private-hosts promiscuous mac-list-name [vlan-list vlan-IDs]`	ブロードバンドで使用するコンテンツ サーバ、およびサービスを配信するエンド ユーザ（独立ホスト）を識別します。 • *mac-list-name* は、特定のタイプのブロードバンド サービスまたはサービス セットを提供する BRAS またはマルチキャスト サーバ（サーバ セット）を指定する MAC アドレス リストの名前を指定します。 • *vlan-IDs* は、ホストが上記のサーバからサービスを受信する VLAN または VLAN のセットを指定します。VLAN リストを指定しない場合、ソフトウェアによりグローバル VLAN リスト（ステップ 3 で設定）が使用されます。 **（注）** 複数の MAC と VLAN の組み合わせを設定し、それぞれを特定のタイプのサービス用のサーバ、および受信ホストとして定義するために、このコマンドを複数回入力できます。
ステップ 5	`Router(config)# private-hosts`	スイッチ上でプライベート ホストをグローバルにイネーブル化します。

	コマンドまたはアクション	目的
ステップ 6	`Router(config)# interface interface`	Private Hosts に対してイネーブルにするトランキング スイッチ ポートまたは EtherChannel を選択します。
ステップ 7	`Router(config-if)# access-group mode prefer port`	トランク ポート上に既存の VACL または RACL があれば、無視するように指定します。
ステップ 8	`Router(config-if)# private-hosts mode {promiscuous | isolated | mixed}`	ポート上でプライベート ホストをイネーブル化します。次のキーワードのいずれかを使用して、ポートが動作するモードを定義します。 • **promiscuous**：無差別。ブロードバンド サーバ（BRAS、マルチキャスト、またはビデオ）か、サーバにアクセスを提供するコア ネットワーク デバイスに接続しているアップストリーム側のポート。 • **isolated**：独立。DSLAM に接続されているポート。 • **mixed**：他のスイッチに接続するポート（通常は、リング トポロジを使用）。 **（注）** プライベート ホストに使用される各ポートに対してこの手順を実行する必要があります。
ステップ 9	`Router(config-if)# end`	インターフェイスおよびグローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。Private Hosts 設定が完了します。

設定例

次に、MAC アドレス リストおよび VLAN リストを作成し、VLAN 10、12、15、および 200 ～ 300 でホストを独立させる場合の例を示します。この例では、BRAS 側のポートは無差別に、ホストに接続している 2 つのポートは独立にしています。

```
Router# configure terminal
Router(config)# private-hosts mac-list BRAS_list 0000.1111.1111 remark BRAS_SanJose
Router(config)# private-hosts vlan-list 10,12,15,200-300
Router(config)# private-hosts promiscuous BRAS_list vlan-list 10,12,15,200-300
Router(config)# private-hosts
Router(config)# interface gig 4/2
Router(config-if)# private-hosts mode promiscuous
Router(config-if)# exit
Router(config)# interface gig 5/2
Router(config-if)# private-hosts mode isolated
Router(config-if)# exit
Router(config)# interface gig 5/3
Router(config-if)# private-hosts mode isolated
Router(config-if)# end
Router#
```

次に、プライベート ホストの独立ポートにおけるインターフェイスの設定例を示します。

```
Router# show run interface gig 5/2
Building configuration...

Current configuration : 200 bytes
!
interface GigabitEthernet5/2
 switchport
 switchport trunk encapsulation dot1q
```

```
 switchport mode trunk
 access-group mode prefer port
 private-hosts mode isolated
end
```

次に、プライベート ホストの無差別ポートにおけるインターフェイスの設定例を示します。

```
Router# show run interface gig 4/2
Building configuration...

Current configuration : 189 bytes
!
interface GigabitEthernet4/2
 switchport
 switchport access vlan 200
 switchport mode access
 private-hosts mode promiscuous
end

private-hosts
private-hosts vlan-list 200
private-hosts promiscuous bras-list
private-hosts mac-list bras-list 0000.1111.1111 remark BRAS-SERVER
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CHAPTER 28

IEEE 802.1Q トンネリング

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

802.1Q トンネリングの前提条件

なし。

802.1Q トンネリングの制約事項

- トラフィックをトンネルに送ったり、トンネルからトラフィックを削除したりする場合は、非対称リンクを使用します。
- 非対称リンクだけを形成するようにトンネル ポートを設定します。
- トンネルごとに専用の VLAN を 1 つずつ設定します。

- トンネリングに使用する VLAN にはトンネル ポートだけを割り当てます。
- トンネル VLAN を伝送するようにトランクを特別に設定する必要はありません。
- トンネル ポートはトランクではありません。ポートがトンネル ポートとして設定されている間は、トランキングを設定するコマンドはいずれも非アクティブです。
- トンネル ポートはカスタマー MAC アドレスを学習します。
- トンネル ポートが設定されていないデバイス間でトンネル トラフィックを伝送する場合は、ISL トランクを使用することを推奨します。802.1Q トランクには 802.1Q ネイティブ VLAN 機能が備わっているため、802.1Q トランクにトンネリングを設定する場合は注意してください。設定ミスによって、トンネル トラフィックが非トンネル ポートに送信されることがあります。
- デフォルトでは、dot1q トランクのネイティブ VLAN トラフィックはタグなしで送信されます。これは、サービス プロバイダー ネットワークで二重タグ付きにできません。こうした状況があるため、ネイティブ VLAN トラフィックは正しくトンネリングされない可能性があります。非対称リンク内ではネイティブ VLAN トラフィックが常にタグ付きで送信されるようにしてください。ネイティブ VLAN 出力トラフィックをタグ付けし、タグなし入力トラフィックをすべてドロップするには、グローバルな **vlan dot1q tag native** コマンドを入力します。
- トンネル ポートでジャンボ フレームのサポートを次のように設定してください。
  - 「ジャンボ フレーム サポートの設定」（P.10-6）を参照してください。
  - 「ジャンボ フレーム サポートの設定」で指定されている、ジャンボ フレームをサポートしないモジュールをメモします。
- ジャンボ フレーム長と 802.1Q タグの合計が最大フレーム サイズを超えない限り、ジャンボ フレームをトンネリングすることができます。
- トンネル トラフィックには Ethertype フィールドと Length フィールドがあり、スイッチ内に 802.1Q タグが保持されるため、次の制限が適用されます。
  - レイヤ 2 フレームに格納されたレイヤ 3 パケットは、トンネル トラフィックでは識別できません。
  - レイヤ 3 以上のパラメータは、トンネル トラフィックでは識別できません（レイヤ 3 宛先や送信元アドレスなど）。
  - パケット内ではレイヤ 3 アドレスを識別できないため、トンネル トラフィックはルーティングできません。
  - スイッチは、トンネル トラフィックに対して MAC レイヤ フィルタリングだけを提供できます（VLAN ID、および送信元や宛先の MAC アドレス）。
  - スイッチはトンネル トラフィックに対して MAC レイヤ アクセス コントロールおよび Quality of Service（QoS）だけを提供できます。
  - QoS は、802.1Q の 2 バイトの Tag Control Information フィールドに格納されて受信された CoS 値を検出できません。
- 非対称リンク上で、トンネル ポートの VLAN が 802.1Q トランクのネイティブ VLAN と一致しない場合、Cisco Discovery Protocol（CDP）はネイティブ VLAN の不一致をレポートします。802.1Q トンネル機能を使用する場合、VLAN が一致する必要はありません。VLAN が一致する必要のない設定の場合は、メッセージを無視してください。
- 非対称リンクでは 1 つのポートだけがトラッキングするため、Dynamic Trunking Protocol（DTP）をサポートしません。無条件でトランクになるように、非対称リンクの 802.1Q トランク ポートを設定します。
- 802.1Q トンネリング機能は、プライベート VLAN をサポートするように設定されたポートには設定できません。
- 802.1Q トンネリング機能は、EVC をサポートするように設定されたポートには設定できません。

- 次のレイヤ 2 プロトコルは、非対称リンクで接続されたデバイス間で機能します。
  - CDP
  - 単一方向リンク検出（UDLD）
  - ポート集約プロトコル（PAgP）
  - リンク集約制御プロトコル（LACP）
- PortFast BPDU フィルタリングは、トンネル ポートで自動的にイネーブルになります。
- CDP は、トンネル ポートで自動的にディセーブルになります。
- VLAN トランキング プロトコル（VTP）は、次のデバイス間で機能しません。
  - 非対称リンクで接続されたデバイス
  - トンネルを介して通信するデバイス

（注）　レイヤ 2 プロトコル トンネリングがイネーブルの場合、VTP はトンネリングされたデバイス間で機能します。設定の詳細については第 29 章「レイヤ 2 プロトコル トンネリング」を参照してください。

- EtherChannel を非対称リンクとして設定するには、EtherChannel 内のすべてのポートを同じトンネリング設定にする必要があります。レイヤ 2 フレーム内のレイヤ 3 パケットは識別できないため、MAC アドレスベースのフレーム配信を使用するように、EtherChannel を設定する必要があります。

レイヤ 2 プロトコル トンネリングを設定する場合は、次に示す設定時の注意事項に*必ず*従ってください。

- サービス プロバイダーのすべてのエッジ スイッチでは、次のように、802.1Q トンネル ポート上で PortFast BPDU フィルタリングをイネーブルにする必要があります。

```
Router(config-if)# spanning-tree bpdufilter enable
Router(config-if)# spanning-tree portfast
```

（注）　PortFast BPDU フィルタリングは、トンネル ポートで自動的にイネーブルになります。

- ネイティブ VLAN タギングに対して、1 つまたは複数の VLAN を使用可能にする必要があります（**vlan dot1q tag native** オプション）。使用可能なすべての VLAN を使用している場合に、**vlan dot1q tag native** オプションをイネーブルにしようとしても、イネーブルになりません。
- サービス プロバイダーのすべてのコア スイッチで、ネイティブ VLAN 出力トラフィックにタグを付け、タグなしのネイティブ VLAN 入力トラフィックをドロップするには、次のコマンドを入力します。

```
Router(config)# vlan dot1q tag native
```

- すべてのカスタマー スイッチで、**vlan dot1q tag native** オプションをグローバルにイネーブルまたはディセーブルの*いずれか一方に*設定します。

（注）　このオプションがイネーブルになっているスイッチとディセーブルになっている別のスイッチが混在している場合は、すべてのトラフィックがドロップされます。したがって、すべてのカスタマー スイッチでこのオプションをそれぞれ同じ設定にする必要があります。

レイヤ 2 プロトコル トンネリングを設定する場合は、*必要に応じて*、次に示す設定時の注意事項に従ってください。

- すべての BPDU がドロップされているため、次のように、レイヤ 2 プロトコル トンネル ポート上でスパニングツリー PortFast をイネーブルにすることができます。

```
Router(config-if)# spanning-tree portfast trunk
```

- カスタマーがサービス プロバイダー側のスイッチを認識できないようにする場合は、次のように 802.1Q トンネル ポート上で CDP をディセーブルにする必要があります。

```
Router(config-if)# no cdp enable
```

802.1Q トンネリングに関する情報

802.1Q トンネリングにより、サービス プロバイダーは、1 つの VLAN を使用して複数の VLAN を持つカスタマーをサポートすることができます。同時に、カスタマーの VLAN ID を保護したり、異なるカスタマー VLAN のトラフィックを分離しておくことができます。

802.1Q トンネリングをサポートするように設定されたポートを、トンネル ポートといいます。トンネリングを設定する場合は、トンネル ポートをトンネリング専用 VLAN に割り当てます。これがトンネル VLAN になります。カスタマーのトラフィックを分離するには、カスタマーごとに個別のトンネル VLAN が 1 つ必要ですが、1 つのトンネル VLAN でカスタマーの VLAN をすべてサポートできます。

802.1Q トンネリングは、ポイントツーポイント トンネル設定に制限されません。トンネル VLAN のすべてのトンネル ポートが、トンネルの入口ポイントおよび出口ポイントになります。802.1Q トンネルには、カスタマー スイッチへの接続に必要となる数のトンネル ポートをいくつでも含めることができます。

カスタマー スイッチはトランク接続されますが、802.1Q トンネリングを使用した場合は、サービス プロバイダー スイッチが、すべてのカスタマー VLAN を直接伝送する代わりに、1 つのサービス プロバイダー VLAN を使用してすべてのカスタマー VLAN を伝送します。

802.1Q トンネリングを使用すると、タグ付きカスタマー トラフィックはカスタマー デバイス上の 802.1Q トランク ポートから着信し、トンネル ポートを経由してサービス プロバイダー エッジ スイッチに着信します。カスタマー デバイス上の 802.1Q トランク ポートとトンネル ポート間のリンクは、非対称リンクといいます。これは、一端が 802.1Q トランク ポートとして設定され、もう一端がトンネル ポートとして設定されているからです。カスタマーごとに一意のアクセス VLAN ID に、トンネル ポートを割り当てます。図 28-1（P.28-5）および図 28-2（P.28-5）を参照してください。

図 28-1　サービス プロバイダー ネットワークにおける IEEE 802.1Q トンネル ポート

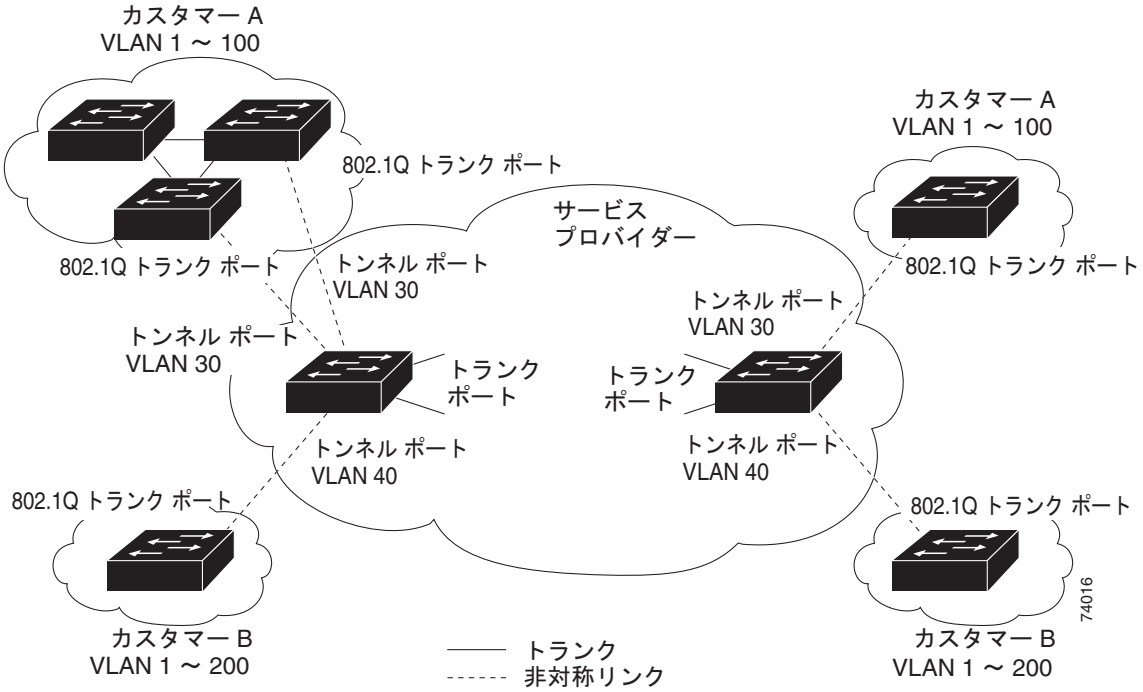
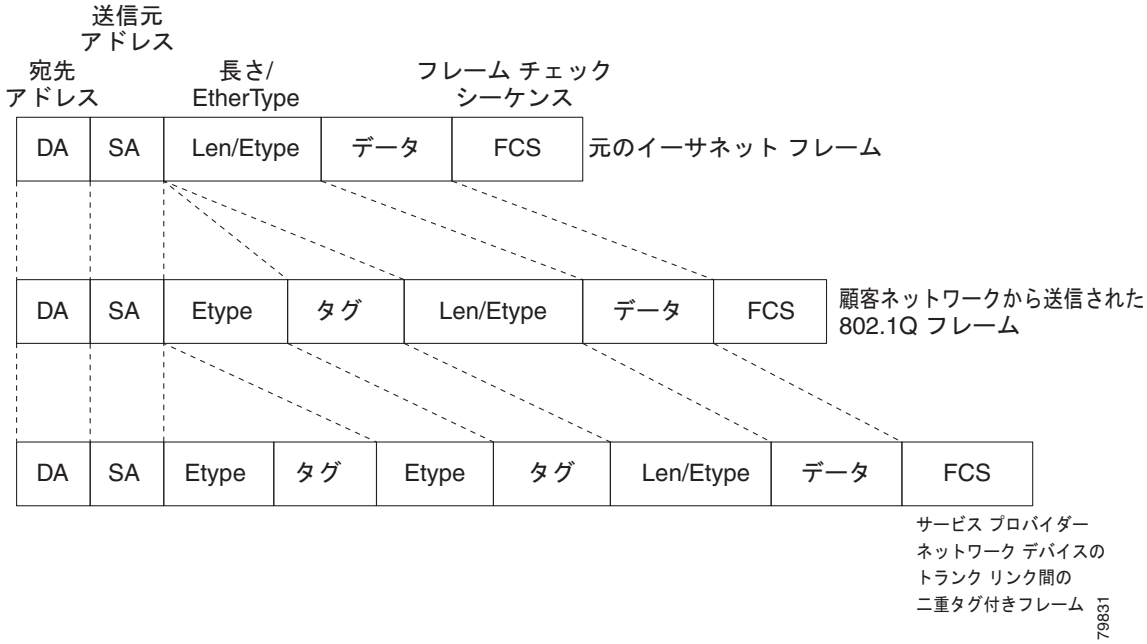


図 28-2　タグなし、802.1Q タグ付き、および二重タグ付きイーサネット フレーム



802.1Q トランク ポートから送信されたタグ付きカスタマー トラフィックを受信したトンネル ポートは、受信した 802.1Q タグをフレーム ヘッダーから削除しません。802.1Q タグを変更しないでそのまま残し、2 バイトの Ethertype フィールド（0x8100）を追加し、そのあとにプライオリティ（CoS）お

よび VLAN を格納する 2 バイトのフィールドを追加します。受信したカスタマー トラフィックは、トンネル ポートが割り当てられた VLAN に送信されます。この Ethertype 0x8100 トラフィック（受信した 802.1Q タグが変更されないトラフィック）は、トンネル トラフィックと呼ばれます。

トンネル トラフィックを伝送する VLAN は 802.1Q トンネルです。VLAN 内のトンネル ポートが、トンネルの入口および出口ポイントになります。

トンネル ポートは異なるネットワーク デバイス上に設定することもできます。トンネルは他のネットワーク リンクおよび他のネットワーク デバイスを通過して、出口トンネル ポートに到着します。トンネルを介しての通信が必要なカスタマー デバイスに対応するために、トンネルにはトンネル ポートを必要なだけ設定できます。

出口トンネル ポートは 2 バイトの Ethertype フィールド（0x8100）および 2 バイト長のフィールドを削除して、802.1Q タグを変更せずに、トラフィックをカスタマー デバイス上の 802.1Q トランク ポートに送信します。カスタマー デバイス上の 802.1Q トランク ポートは 802.1Q タグを削除して、トラフィックを適切なカスタマー VLAN に送ります。

（注） トンネル トラフィックは、2 番めの 802.1Q タグがサービス プロバイダー ネットワーク デバイス間のトランク リンク上にある場合だけ、そのタグを伝送します。この場合、外部タグはサービス プロバイダーが割り当てた VLAN ID を含み、内部タグはカスタマーが割り当てた VLAN ID を含みます。

802.1Q トンネリングのデフォルト設定

なし。

802.1Q トンネリングの設定方法

- 「802.1Q トンネル ポートの設定」（P.28-7）
- 「ネイティブ VLAN トラフィックにタグを付けるためのスイッチ設定」（P.28-7）

注意 トンネリングに使用するすべての VLAN 内に適切なトンネル ポートだけがあり、トンネルごとに VLAN が 1 つずつ使用されていることを確認します。VLAN へのトンネル ポートの割り当てが誤っていると、トラフィックが正しく転送されません。

802.1Q トンネル ポートの設定

特定のポート上で 802.1Q 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	`Router(config)# interface type slot/port`	設定する LAN ポートを選択します。
ステップ 2	`Router(config-if)# switchport`	LAN ポートをレイヤ 2 スイッチング用に設定します。 • LAN ポートをレイヤ 2 インターフェイス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 度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さらに **switchport** コマンドを入力してください。 • インターフェイスに対して **switchport** コマンドを一度も入力していない場合にかぎり、必須です。
ステップ 3	`Router(config-if)# switchport mode dot1q-tunnel`	レイヤ 2 ポートをトンネル ポートとして設定します。
ステップ 4	`Router(config-if)# no lldp transmit`	（PE ポートで必須）LLDP をディセーブルにします。 **（注）**　CDP は自動的にディセーブルになります。
ステップ 5	`Router(config-if)# end`	コンフィギュレーション モードを終了します。

次に、ポート 4/1 にトンネリングを設定して、その設定を確認する例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 4/1
Router(config-if)# switchport mode dot1q-tunnel
Router(config-if)# no lldp transmit
Router(config-if)# end
Router# show dot1q-tunnel interface
```

ネイティブ VLAN トラフィックにタグを付けるためのスイッチ設定

- 「ネイティブ VLAN トラフィックにグローバルにタグを付けるためのスイッチ設定」（P.28-8）
- 「ネイティブ VLAN トラフィックにタグを付けないようにするためのポート設定」（P.28-8）

ネイティブ VLAN トラフィックにグローバルにタグを付けるためのスイッチ設定

ネイティブ VLAN 内のトラフィックにグローバルにタグを付け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	`Router(config)# vlan dot1q tag native`	ネイティブ VLAN トラフィックにグローバルにタグを付けるようにスイッチを設定し、802.1Q トランク上で 802.1Q タグが付けられたフレームのみを許可し、ネイティブ VLAN のタグなしトラフィックを含むすべてのタグなしトラフィックをドロップします。 （注）　**no switchport trunk native vlan tag** インターフェイス コマンドを入力したポートでは、**vlan dot1q tag native** グローバル コマンドの機能はディセーブルになります。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

次に、ネイティブ VLAN トラフィックにタグを付けるようにスイッチを設定し、その設定を確認する例を示します。

```
Router# configure terminal
Router(config)# vlan dot1q tag native
Router(config)# end
Router# show vlan dot1q tag native | include globally
dot1q native vlan tagging is enabled globally
Router(config)#
```

ネイティブ VLAN トラフィックにタグを付けないようにするためのポート設定

ネイティブ VLAN 内のトラフィックにタグを付けない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
ステップ 1	`Router(config)# interface` *type slot/port*	設定する LAN ポートを選択します。
ステップ 2	`Router(config-if)# switchport`	LAN ポートをレイヤ 2 スイッチング用に設定します。 • LAN ポートをレイヤ 2 インターフェイス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 度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さらに **switchport** コマンドを入力してください。 • ポートに対して **switchport** コマンドを一度も入力していない場合にこの手順を行う必要があります。
ステップ 3	`Router(config-if)# no switchport trunk native vlan tag`	ネイティブ VLAN トラフィックにグローバルでタグを付けるようにスイッチが設定されている場合に、ネイティブ VLAN トラフィックにタグを付けないようにレイヤ 2 ポートを設定します。
ステップ 4	`Router(config-if)# end`	コンフィギュレーション モードを終了します。

（注）　ネイティブ VLAN トラフィックにグローバルにタグを付けるようにスイッチが設定されていないと、ネイティブ VLAN タギングは、**switchport trunk native vlan tag** インターフェイス コマンドを入力してもイネーブルになりません。

次に、ネイティブ VLAN 内のトラフィックにタグを付けるようにギガビット イーサネット ポート 1/4 を設定し、その設定を確認する例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 1/4
Router(config-if)# switchport trunk native vlan tag
Router(config-if)# end
Router# show interface gigabitethernet 1/4 switchport | include tagging
Administrative Native VLAN tagging: enabled
Operational Native VLAN tagging: disabled
Router#
```

ヒント　Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CHAPTER 29

レイヤ 2 プロトコル トンネリング

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

レイヤ 2 プロトコル トンネリングの前提条件

なし。

レイヤ 2 プロトコル トンネリングの制約事項

なし。

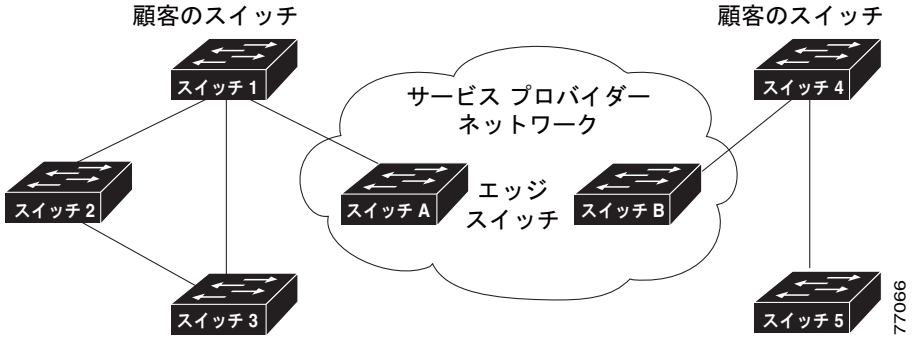
レイヤ 2 プロトコル トンネリングについて

レイヤ 2 プロトコル トンネリングを使用すると、レイヤ 2 プロトコル データ ユニット（PDU）（CDP、STP、および VLAN）をネットワーク経由でトンネリング（仮想 LAN）できます。ここで使用する用語は、次のとおりです。

- エッジ スイッチ：カスタマー スイッチに接続され、サービス プロバイダー ネットワークの境界に配置されたスイッチ（図 29-1 を参照）。
- レイヤ 2 プロトコル トンネル ポート：トンネリング対象の特定のプロトコルのカプセル化やカプセル化解除が可能なエッジ スイッチ上のポート。レイヤ 2 プロトコル トンネル ポートは CLI コマンドを使用して設定します。
- トンネル化 PDU：CDP、STP、または VTP PDU

レイヤ 2 プロトコル トンネリングがない場合、トンネル ポートは STP と VTP パケットをドロップし、CDP パケットを処理します。この PDU の処理方法に応じて、カスタマー スイッチに異なるスパニングツリー ドメイン（異なるスパニングツリー ルート）が作成されます。たとえば、スイッチ 1 の VLAN 用 STP（図 29-1 を参照）は、スイッチ 4 およびスイッチ 5 に基づくコンバージェンス パラメータを考慮しないで、スイッチ 1、スイッチ 2、およびスイッチ 3 のスパニングツリー トポロジを構築します。カスタマーに対応するスパニングツリー ドメインを 1 つだけにする目的で、制御プロトコル PDU（CDP、STP、および VTP）用に BPDU をトンネリングするための汎用方式が作成されました。このプロセスは、Generic Bridge PDU Tunneling（GBPT）といいます。

図 29-1　　レイヤ 2 プロトコル トンネリング ネットワークの設定



GBPT は、入力エッジ スイッチ内で PDU をソフトウェアでカプセル化してから、ハードウェアでマルチキャストすることにより PDU トンネリングを拡張する方式です。サービス プロバイダー ネットワーク内のすべてのスイッチは、カプセル化されたこれらのフレームをデータ パケットとして処理し、もう一方の端に転送します。出口のエッジ スイッチは、これらの特殊なカプセル化フレームを待ち受け、カプセル化を解除し、トンネルの外側へ転送します。

カプセル化では、PDU 内の宛先 Media Access Control（MAC; メディア アクセス コントロール）アドレスも書き換えられます。入力エッジ スイッチは、レイヤ 2 トンネル ポート上で受信された PDU の宛先 MAC アドレスを、シスコ独自のマルチキャスト アドレス（01-00-0c-cd-cd-d0）で書き換えます。次に、PDU はレイヤ 2 トンネル ポートのネイティブ VLAN にフラッディングされます。ポート上でレイヤ 2 プロトコル トンネリングをイネーブルにした場合、イネーブル化されたプロトコルの PDU は送信されません。ポート上でレイヤ 2 プロトコル トンネリングをディセーブルにすると、ディセーブルになったプロトコルは、そのポート上でレイヤ 2 プロトコル トンネリングがイネーブルになる前と同様に動作します。

レイヤ 2 プロトコル トンネリングのデフォルト設定

なし。

レイヤ 2 プロトコル トンネリングの設定方法

（注）

- 802.1Q トンネル ポートで受信されたカプセル化 PDU は、スイッチ上の同じ VLAN にある別のトンネル ポートから伝送されます。
- 次のように、レイヤ 2 プロトコル トンネリング ポートでジャンボ フレーム サポートを設定してください。
  - 「ジャンボ フレーム サポートの設定」（P.10-6）を参照してください。
  - 「ジャンボ フレーム サポートの設定」で指定されている、ジャンボ フレームをサポートしないモジュールをメモします。

特定のポート上でレイヤ 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	`Router(config)# interface type slot/port`	設定する LAN ポートを選択します。
ステップ 2	`Router(config-if)# switchport`	LAN ポートをレイヤ 2 スイッチング用に設定します。 • LAN ポートをレイヤ 2 インターフェイス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 度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さらに **switchport** コマンドを入力してください。 • インターフェイスに対して **switchport** コマンドを一度も入力していない場合にかぎり、必須です。
ステップ 3	`Router(config-if)# l2protocol-tunnel [cdp | lldp | stp | vtp]`	レイヤ 2 ポートを、すべてのプロトコルまたは指定されたプロトコルだけのレイヤ 2 プロトコル トンネル ポートとして設定します。
ステップ 4	`Router(config-if)# l2protocol-tunnel drop-threshold {[cdp | lldp | stp | vtp] packets}`	（任意）ポートをレイヤ 2 プロトコル トンネル ポートとして設定し、すべてのプロトコルまたは指定されたプロトコルだけのドロップしきい値を設定します。
ステップ 5	`Router(config-if)# l2protocol-tunnel shutdown-threshold {[cdp | lldp | stp | vtp] packets}`	（任意）ポートをレイヤ 2 プロトコル トンネル ポートとして設定し、すべてのプロトコルまたは指定されたプロトコルだけのシャットダウンしきい値を設定します。
ステップ 6	`Router(config-if)# no lldp transmit`	（PE ポートで必須）LLDP をディセーブルにします。 （注）　CDP は自動的にディセーブルになります。
ステップ 7	`Router(config)# end`	コンフィギュレーション モードを終了します。

レイヤ 2 ポートをレイヤ 2 プロトコル トンネル ポートとして設定する際、以下に注意してください。

- 任意で、そのポートのドロップしきい値を指定できます。1 ～ 4096 のドロップしきい値によって、そのインターフェイス上で 1 秒間にそのプロトコルに関して処理されるパケット数が決まります。処理パケット数がドロップしきい値を超えると、その特定のプロトコルの PDU は、1 秒間の残りの時間にドロップされます。ドロップしきい値を指定しない場合、値は 0 です（ドロップしきい値はディセーブルです）。
- 任意で、そのポートのシャットダウンしきい値を指定できます。1 ～ 4096 のシャットダウンしきい値によって、そのインターフェイス上で 1 秒間にそのプロトコルに関して処理されるパケット数が決まります。シャットダウンしきい値を超えると、ポートは errdisable ステートになります。shutdown-threshold 値を指定しない場合、値は 0 です（shutdown-threshold はディセーブルです）。
- ポートのドロップしきい値とシャットダウンしきい値の両方を指定すると、ドロップしきい値を超えたパケットは転送されませんが、シャットダウンしきい値に到達するまでカウントされます。

（注）　次のコマンドでは、**l2ptguard** キーワードがサポートされています。

- **errdisable detect cause**
- **errdisable recovery**

次に、CDP、STP、および VTP に対して、ポート 5/1 にレイヤ 2 プロトコル トンネリングおよびドロップしきい値とシャットダウンしきい値を設定し、その設定を確認する例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 5/1
Router(config-if)# switchport
Router(config-if)# l2protocol-tunnel shutdown-threshold cdp 400
Router(config-if)# l2protocol-tunnel shutdown-threshold stp 400
Router(config-if)# l2protocol-tunnel shutdown-threshold vtp 400
Router(config-if)# l2protocol-tunnel drop-threshold vtp 200
Router(config-if)# no lldp transmit
Router(config-if)# end
Router# show l2protocol-tunnel summary
COS for Encapsulated Packets: 5
Drop Threshold for Encapsulated Packets: 0

Port      Protocol    Shutdown            Drop                  Status
                      Threshold           Threshold
                      (cdp/lldp/stp/vtp)  (cdp/lldp/stp/vtp)
--------- ----------- ------------------- -------------------- ----------
Gi5/1     -- -- -- ---  400/----/ 400/ 400 ----/----/----/ 200   down(trunk)

Router#
```

次に、ポート 5/1 のカウンタ情報を表示する例を示します。

```
Router# show l2protocol-tunnel interface gigabitethernet 5/1
COS for Encapsulated Packets: 5

Port        Protocol Thresholds          Counters
                     Shutdown  Drop      Encap     Decap     Drop
----------- -------- --------- --------- --------- --------- ---------

Router#
```

次に、ポート 5/1 のレイヤ 2 プロトコル トンネリング設定をクリアする例を示します。

```
Router(config-if)# no l2protocol-tunnel shutdown-threshold cdp 400
Router(config-if)# no l2protocol-tunnel shutdown-threshold stp 400
```

```
Router(config-if)# no l2protocol-tunnel shutdown-threshold vtp 400
Router(config-if)# no l2protocol-tunnel drop-threshold vtp 200
Router(config-if)# no l2protocol-tunnel cdp
Router(config-if)# no l2protocol-tunnel stp
Router(config-if)# no l2protocol-tunnel vtp
Router(config-if)# lldp transmit
Router(config-if)# end
Router# show l2protocol-tunnel summary
COS for Encapsulated Packets: 5
Drop Threshold for Encapsulated Packets: 0

Port      Protocol    Shutdown            Drop                   Status
                      Threshold           Threshold
                      (cdp/lldp/stp/vtp)  (cdp/lldp/stp/vtp)
--------- ----------- ------------------- -------------------- ----------

Router#
```

次に、レイヤ 2 プロトコル トンネリング ポートのカウンタを消去する例を示します。

```
Router# clear l2protocol-tunnel counters
Router#
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CHAPTER 30

スパニングツリー プロトコル

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。
- この章では、スパニングツリー プロトコル（STP）および Multiple Spanning Tree（MST）プロトコルについて説明します。PortFast、UplinkFast、および BackboneFast STP 拡張機能の設定手順については、第 31 章「オプションの STP 機能」を参照してください。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

スパニングツリー プロトコルの前提条件

なし。

スパニングツリー プロトコルの制約事項

- 802.1s MST 規格では 65 までの MSTI が許可されます。無制限の数の VLAN を MSTI にマップできます。
- Rapid PVST+、MST はサポートされますが、同時にアクティブにできるバージョンは 1 つだけです。
- VTP は MST 設定を伝播しません。コマンドライン インターフェイス（CLI）または SNMP を使用し、MST リージョン内の各スイッチで MST 設定（リージョン名、リビジョン番号、VLAN とインスタンスのマッピング）を手動で設定する必要があります。
- ネットワークの冗長パスでロードバランスを実現するには、すべての VLAN とインスタンスのマッピング割り当てが一致する必要があります。一致しない場合、すべてのトラフィックは単一リンクを流れます。
- すべての MST 境界ポートは、PVST+ と MST クラウドの間、または Rapid PVST+ および MST クラウドの間におけるロードバランスのために転送する必要があります。このためには、MST クラウドの CIST リージョナル ルートが CST のルートである必要があります。MST クラウドが複数の MST 領域で構成されている場合、MST 領域の 1 つに CST ルートが含まれていなければならず、その他のすべての MST 領域では MST クラウド内に含まれるルートへのパスが、Rapid PVST+ クラウドよりも良好なものでなければなりません。
- 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。ただしこの状況を避けられない場合は、レイヤ 2 デバイスによって相互接続された、より小さい LAN にスイッチド LAN を分割することを推奨します。
- 既存の MST インスタンスに対して VLAN の追加または削除を行うと、その MST インスタンスでスパニングツリーが再計算され、そのすべての VLAN のトラフィックが中断されます

スパニングツリー プロトコルについて

STP について

STP の概要

STP（IEEE 802.1D ブリッジ プロトコル）は、ネットワークの不要なループを排除しながらパスの冗長性を提供する、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 ネットワークが正常に動作するには、任意の 2 つのステーション間で存在できるアクティブ パスは 1 つだけです。STP 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、単一の LAN セグメントに接続されているのか、それとも複数セグメントからなるスイッチド LAN に接続されているのかを、エンド ステーションが検知することはできません。

Per-VLAN Spanning Tree（PVST）として知られる拡張機能で、レイヤ 2 イーサネット ポートは、すべての VLAN で STP を使用できます。設定された各 VLAN においてデフォルトでイネーブルになっている（手動でディセーブルにしていなければ）Rapid PVST+ は、高速コンバージェンスを実現するために RSTP を使用します。独立 VLAN は、独自の RSTP インスタンスを実行します。

Rapid PVST+ では、ダイナミック エントリは、トポロジの変更を受信すると、ポート単位ですぐに消去されます。UplinkFast および BackboneFast 設定は Rapid PVST+ モードでは無視され、両機能は RSTP に含まれます。Rapid PVST+ モードは、「単一方向リンク障害の検出」（P.30-26）で説明されているように、単一方向リンク障害の検出をサポートします。

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 パスを構築する必要があります。STP 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。レイヤ 2 LAN ポートは定期的に STP フレームを送受信します。ネットワーク デバイスはこれらのフレームを転送しないで、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場合、エンド ステーションが重複したメッセージを受信したり、ネットワーク デバイスが複数のレイヤ 2 LAN ポート上でエンド ステーション MAC アドレスを学習したりする可能性があります。このような状況によって、ネットワークが不安定になります。

STP は、ルート ブリッジ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ネットワーク デバイスへのループフリー パスを備えたツリーを定義します。STP 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 1 つのネットワーク セグメントで障害が発生し、冗長パスが存在する場合、STP アルゴリズムはスパニングツリー トポロジーを再計算し、スタンバイ パスをアクティブにします。

ネットワーク デバイス上の 2 つのレイヤ 2 LAN ポートがループの一部になっている場合、どちらのポートがフォワーディング ステートになり、どちらのポートがブロッキング ステートになるかは、STP 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。STP ポート プライオリティ値は、ネットワーク トポロジーにおけるポートの位置を表すとともに、その位置によってポートがどれだけ効率的にトラフィックを通過させることができるかを表します。STP 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 について

ブリッジ プライオリティ値

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。拡張システム ID がイネーブルの場合、ブリッジ プライオリティは 4 ビット値です（表 30-1（P.30-4）および「VLAN のブリッジ プライオリティの設定」（P.30-36）を参照）。

拡張システム ID

12 ビットの拡張システム ID フィールドは、ブリッジ ID の一部です（表 30-1（P.30-4）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。1,024 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。

拡張システム ID は、次の条件ではデフォルトでイネーブルです。

- 64 個の MAC アドレスのみをサポートするシャーシ
- STP モードが MST の場合

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.30-30）を参照してください。

表 30-1　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				拡張システム ID（VLAN/MST インスタンス ID と同設定）											
ビット 16	ビット 15	ビット 14	ビット 13	ビット 12	ビット 11	ビット 10	ビット 9	ビット 8	ビット 7	ビット 6	ビット 5	ビット 4	ビット 3	ビット 2	ビット 1
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

STP MAC アドレスの割り当て

Catalyst 6500 シリーズ スイッチ シャーシには、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可能な 64 または 1024 の MAC アドレスがあります。シャーシの MAC アドレスの範囲を表示するには、**show catalyst6000 chassis-mac-address** コマンドを入力します。

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。

拡張システム ID がイネーブルでない場合、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。

拡張システム ID がイネーブルになっているネットワーク装置がネットワークにある場合、望ましくないルート ブリッジ選択やスパニングツリー トポロジ問題を回避するために、レイヤ 2 で接続されているその他すべてのネットワーク装置でも、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 がイネーブルの場合、ルート ブリッジのプライオリティは、4096 の倍数プラス VLAN ID になります。拡張システム ID がイネーブルだと、スイッチ ブリッジ ID（ルート ブリッジの ID を決定するためスパニングツリー アルゴリズムによって使用され、最小値のほうが優先される）には、4096 の倍数だけ指定できます。使用可能な値は、0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440 だけです。

同じスパニングツリー ドメイン内の別のブリッジで拡張システム ID がイネーブルでない場合、ブリッジ ID により細かい値を選択できるため、そのブリッジがルート ブリッジの所有権を取得する可能性があります。

ブリッジ プロトコル データ ユニットについて

ブリッジ プロトコル データ ユニット（BPDU）はルート ブリッジから一方向に送信されます。各ネットワーク デバイスはコンフィギュレーション BPDU を送信して、スパニングツリー トポロジを伝達および計算します。各コンフィギュレーション BPDU に含まれる最小限の情報は、次のとおりです。

- 送信側ネットワーク デバイスがルート ブリッジになると見なしているネットワーク デバイスの固有のブリッジ ID

- ルートまでの STP パス コスト
- 送信側ブリッジのブリッジ ID
- メッセージ エージ
- 送信側ポートの ID
- hello タイマー、転送遅延タイマー、および max-age プロトコル タイマーの値

ネットワーク デバイスが BPDU フレームを伝送すると、そのフレームが伝送される LAN に接続されたすべてのネットワーク デバイスが BPDU を受信します。ネットワーク デバイスが BPDU を受信すると、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、トポロジーが変更されると、BPDU の送信を開始します。

BPDU 交換によって次の処理が行われます。

- 1 つのネットワーク デバイスがルート ブリッジとして選定されます。
- パス コストに基づいて、各ネットワーク デバイスのルート 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ネットワーク デバイスであり、このネットワーク デバイス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、最高のプライオリティのブリッジ ID（数値的に最小の ID 値）を持つネットワーク装置がルート ブリッジとして選定されます。すべてのネットワーク デバイスがデフォルト プライオリティ（32768）に設定されている場合は、VLAN 内で最小の MAC アドレスを持つネットワーク デバイスがルート ブリッジになります。ブリッジ プライオリティ値はブリッジ ID の最上位ビットを占めます。

ブリッジのプライオリティの値を変更すると、スイッチがルート ブリッジとして選定される可能性を変更することになります。高いプライオリティ値を設定するとその確率が高くなり、低いプライオリティ値を設定すると低くなります。

STP ルート ブリッジは、レイヤ 2 ネットワークにおけるスパニングツリー トポロジーの論理上の中心です。レイヤ 2 ネットワーク内のどの場所からでも、ルート ブリッジに到達するために必要でないパスは、すべて STP ブロッキング モードになります。

BPDU には、送信側ブリッジおよび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。STP はこの情報を使用してレイヤ 2 ネットワークのルート ブリッジを選定し、ルート ブリッジへのルート ポートを選定し、各レイヤ 2 セグメントの指定ポートを判別します。

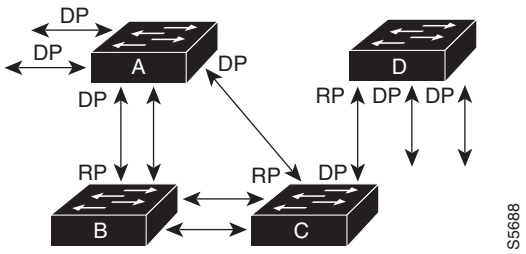
STP プロトコル タイマー

変数	説明
ハロー タイマー	ネットワーク デバイスが他のネットワーク デバイスへ hello メッセージをブロードキャストする間隔を決定します。
転送遅延タイマー	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。
最大エージング タイマー	ポートで受信したプロトコル情報がネットワーク デバイスによって保管される時間を決定します。

スパニングツリー トポロジーの作成

図 30-1 では、スイッチ A がルート ブリッジに選定されます。これは、すべてのネットワーク デバイスのブリッジ プライオリティがデフォルト（32768）に設定されており、スイッチ A の MAC アドレスが最小であるためです。ただし、トラフィック パターン、転送ポートの数、またはリンク 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。最適なネットワーク デバイスがルート ブリッジになるように、デバイスのプライオリティを上げる（数値を下げる）ことで、ルートとして最適なネットワーク デバイスを使用する、新しいスパニングツリー トポロジーを形成するように強制的に再計算させることができます。

図 30-1　　スパニングツリー トポロジー



RP = ルート ポート
DP = 指定ポート

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算出された場合、スイッチド ネットワークの送信元エンド ステーションから宛先エンド ステーションまでのパスが最適にならない場合があります。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 ポートが変更される場合があります。最高速のリンクをルート ポートにすることが重要です。

たとえば、スイッチ B の 1 つのポートが光ファイバ リンクであり、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 トラフィックを高速の光ファイバ リンクに流した方が効率的です。光ファイバ ポートの STP ポート プライオリティをルート ポートよりも高いプライオリティに変更すると（数値を下げる）、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

- 「STP ポート ステートの概要」（P.30-7）
- 「ブロッキング ステート」（P.30-9）

STP ポート ステートの概要

プロトコル情報がスイッチド LAN を通過するとき、伝播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ーの変化が発生します。レイヤ 2 LAN ポート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 ステートに直接遷移すると、一時的にデータ ループが発生する可能性があります。ポートは新しいトポロジー情報がスイッチド LAN 経由で伝播されるまで待機し、それからフレーム転送を開始する必要があります。さらに、古いトポロジーを使用して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。

STP を使用する各レイヤ 2 LAN ポートは、次の 5 種類のステートのいずれかになります。

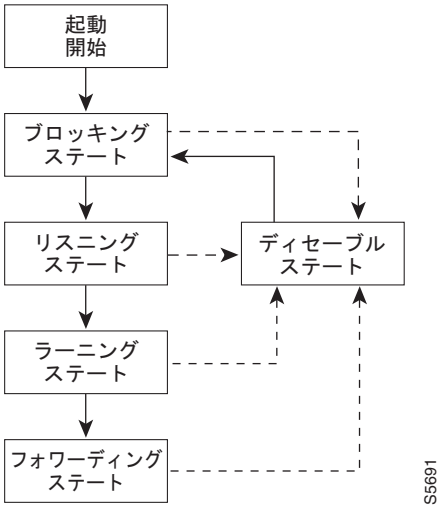
- ブロッキング：レイヤ 2 LAN ポートはフレーム転送に参加しません。
- リスニング：レイヤ 2 LAN ポートがフレーム転送に参加すべきであると STP が判断した場合に、ブロッキング ステートのあとで最初に開始する移行ステートです。
- ラーニング：レイヤ 2 LAN ポートがフレーム転送に参加する準備をしている状態です。
- フォワーディング：レイヤ 2 LAN ポートはフレームを転送します。
- ディセーブル：レイヤ 2 LAN ポートが STP に参加せず、フレームを転送しません。

レイヤ 2 LAN ポートは、次のように 5 種類のステートに移行します。

- 初期化からブロッキング
- ブロッキングからリスニングまたはディセーブル
- リスニングからラーニングまたはディセーブル
- ラーニングからフォワーディングまたはディセーブル
- フォワーディングからディセーブル

図 30-2 に、レイヤ 2 LAN ポートがどのように 5 種類のステートを移行するかを示します。

図 30-2　レイヤ 2 LAN インターフェイス ステート



STP をイネーブルにすると、すべてのポート、VLAN、およびネットワークは、電源投入時に必ずブロッキング ステートを経て、それからリスニングおよびラーニングという移行ステートに進みます。設定が適切であれば、各レイヤ 2 LAN ポートはフォワーディング ステートまたはブロッキング ステートで安定します。

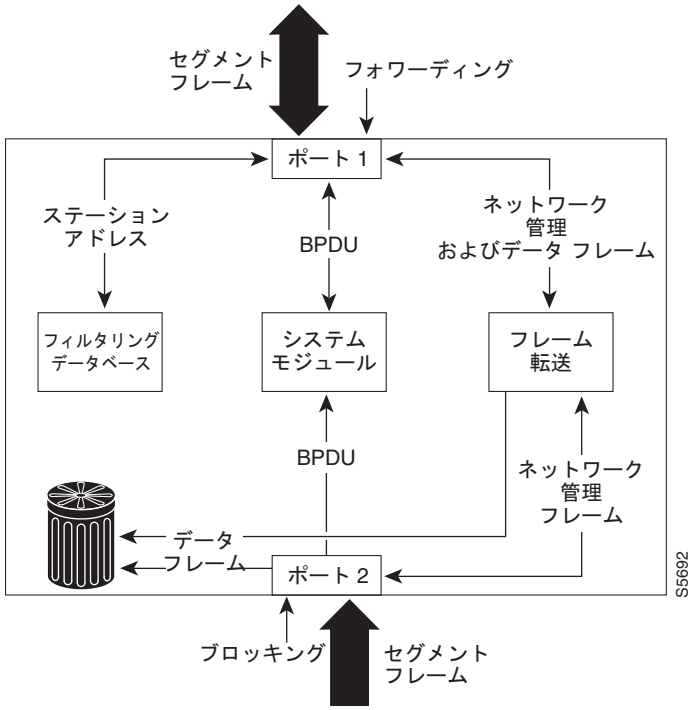
STP アルゴリズムによってレイヤ 2 LAN ポートがフォワーディング ステートになると、次の処理が行われます。

1. レイヤ 2 LAN ポートがリスニング ステートになり、ブロッキング ステートに移行するように指示するプロトコル情報を待ちます。
2. レイヤ 2 LAN ポートが転送遅延タイマーの満了を待ち、レイヤ 2 LAN ポートをラーニング ステートに移行し、転送遅延タイマーをリセットします。
3. ラーニング ステートで、レイヤ 2 LAN ポートはフレーム転送を引き続きブロックしながら、転送データベースのエンド ステーションが位置情報を学習します。
4. レイヤ 2 LAN ポートは、転送遅延タイマーがタイムアウトになるまで待機します。タイムアウトになったら、レイヤ 2 LAN ポートをフォワーディング ステートに移行します。フォワーディング ステートでは、ラーニングおよびフレーム転送が両方ともイネーブルになります。

ブロッキング ステート

ブロッキング ステートのレイヤ 2 LAN ポートは、フレーム転送に参加しません（図 30-3 を参照）。初期化後、各レイヤ 2 LAN ポートに BPDU が送信されます。ネットワーク デバイスは、他のネットワーク デバイスと BPDU を交換するまで、そのネットワーク デバイスをルートと見なします。この BPDU 交換により、ネットワーク上のどのネットワーク デバイスがルートまたはルート ブリッジであるかが確定します。ネットワークにネットワーク デバイスが 1 台しか存在しない場合は、BPDU 交換は行われず、転送遅延タイマーが失効し、ポートはリスニング ステートに移行します。初期化後、ポートは必ずブロッキング ステートになります。

図 30-3　　ブロッキング ステートのインターフェイス 2



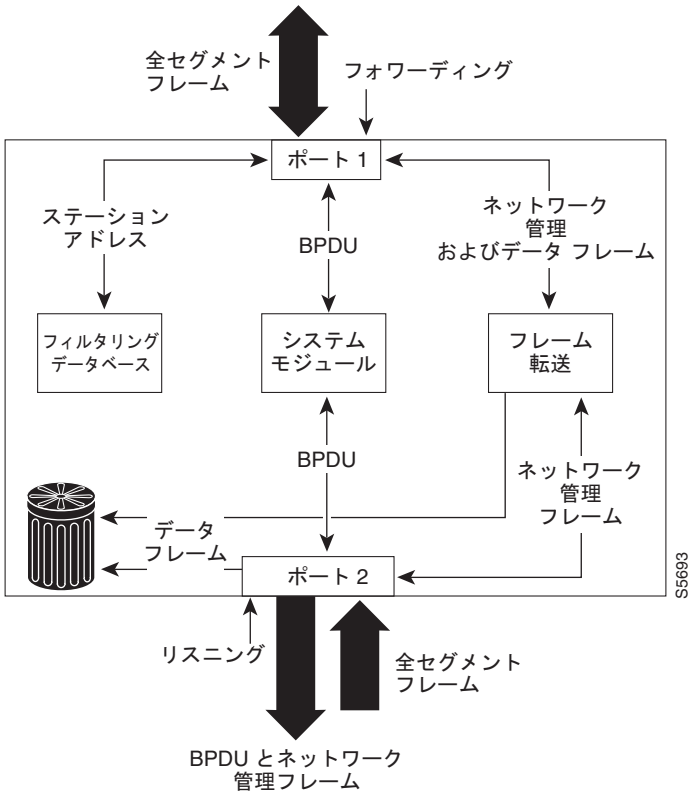
ブロッキング ステートのレイヤ 2 LAN ポートは、次の処理を実行します。

- 接続セグメントから受信したフレームを廃棄します。
- 転送用に他のポートからスイッチングされたフレームを廃棄します。
- アドレス データベースに、エンド ステーションの位置情報は組み込みません（ブロッキング状態のレイヤ 2 LAN ポートに関する学習は行われないため、アドレス データベースは更新されません）。
- BPDU を受信し、それをシステム モジュールに転送します。
- システム モジュールから受信した BPDU を送信しません。
- ネットワーク管理メッセージを受信して応答します。

リスニング ステート

リスニング ステートは、レイヤ 2 LAN ポートがブロッキング ステートを経て最初に開始する移行ステートです。レイヤ 2 LAN ポートがフレーム転送に参加すべきであると STP が判断した場合に、レイヤ 2 LAN ポートはこのステートを開始します。図 30-4 に、リスニング ステートのレイヤ 2 LAN ポートを示します。

図 30-4　　リスニング ステートのインターフェイス 2



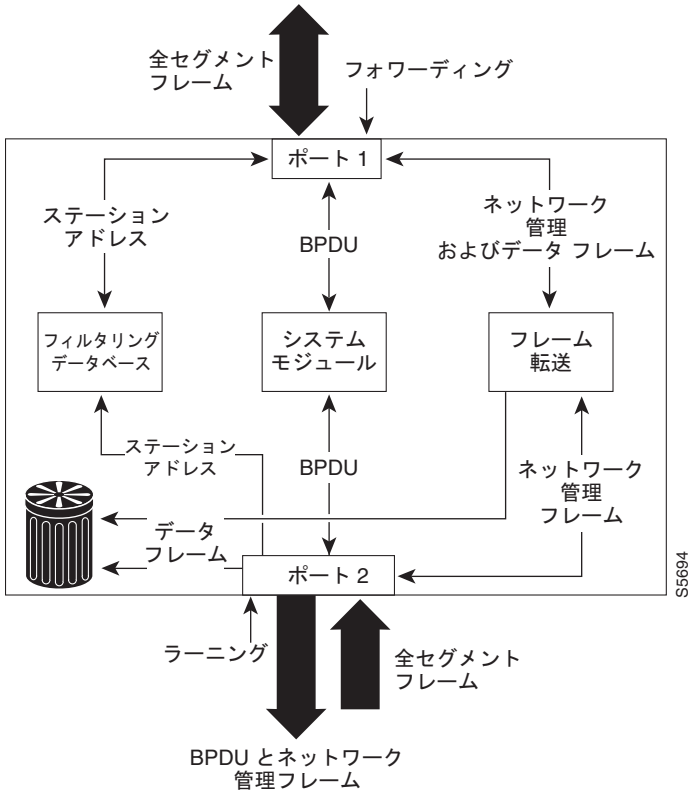
リスニング ステートのレイヤ 2 LAN ポートは、次の処理を実行します。

- 接続セグメントから受信したフレームを廃棄します。
- 転送用に他の LAN ポートからスイッチングされたフレームを廃棄します。
- アドレス データベースに、エンド ステーションの位置情報は組み込みません （この時点で学習は行われないため、アドレス データベースは更新されません）。
- BPDU を受信し、それをシステム モジュールに転送します。
- システム モジュールから送られた BPDU を受信し、処理して送信します。
- ネットワーク管理メッセージを受信して応答します。

ラーニング ステート

ラーニング ステートのレイヤ 2 LAN ポートは、フレーム転送に参加するための準備を行います。レイヤ 2 LAN ポートは、リスニング ステートからラーニング ステートを開始します。図 30-5 に、ラーニング ステートのレイヤ 2 LAN ポートを示します。

図 30-5　　ラーニング ステートのインターフェイス 2



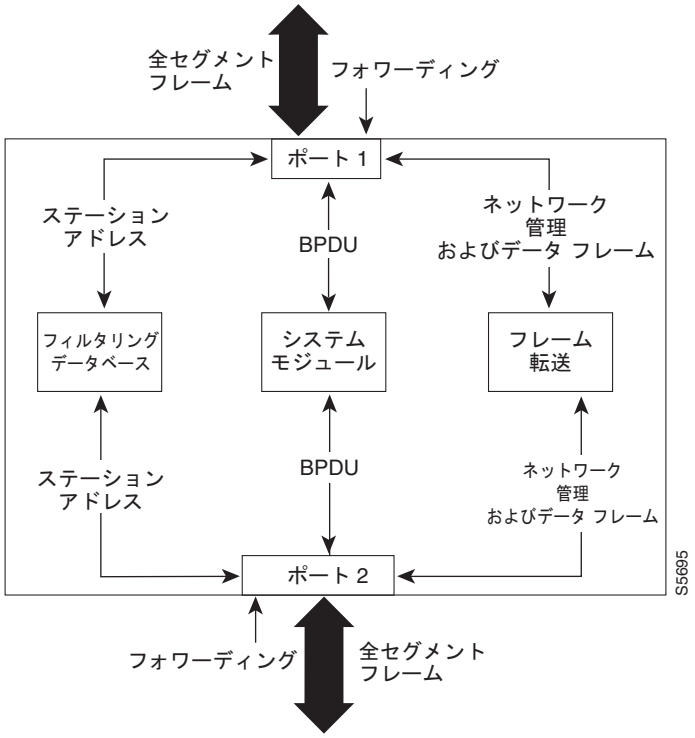
ラーニング ステートのレイヤ 2 LAN ポートは、次の処理を実行します。

- 接続セグメントから受信したフレームを廃棄します。
- 転送用に他のポートからスイッチングされたフレームを廃棄します。
- エンド ステーションの位置情報をアドレス データベースに組み込みます。
- BPDU を受信し、それをシステム モジュールに転送します。
- システム モジュールから送られた BPDU を受信し、処理して送信します。
- ネットワーク管理メッセージを受信して応答します。

フォワーディング ステート

フォワーディング ステートのレイヤ 2 LAN ポートは、フレームを転送します（図 30-6 を参照）。レイヤ 2 LAN ポートは、ラーニング ステートからフォワーディング ステートを開始します。

図 30-6　　フォワーディング ステートのインターフェイス 2



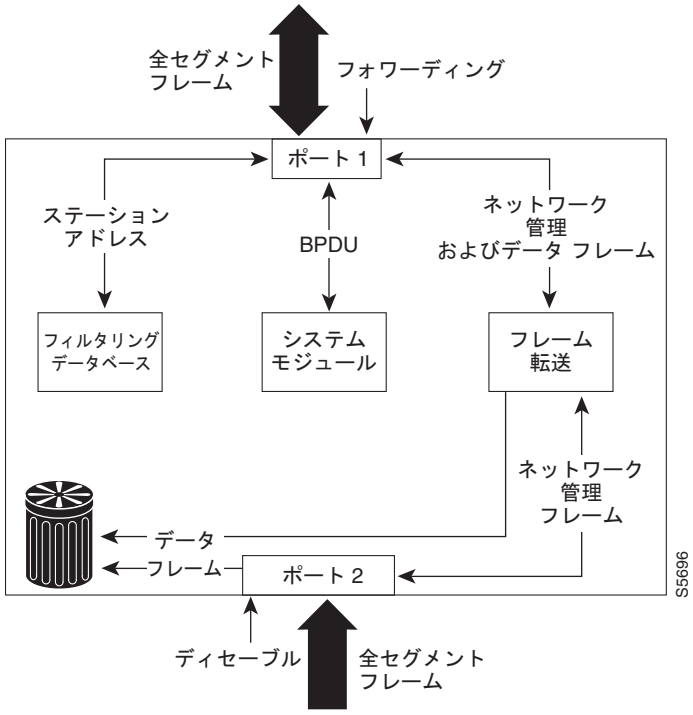
フォワーディング ステートのレイヤ 2 LAN ポートは、次の処理を実行します。

- 接続セグメントから受信したフレームを転送します。
- 転送用に他のポートからスイッチングされたフレームを転送します。
- エンド ステーションの位置情報をアドレス データベースに組み込みます。
- BPDU を受信し、それをシステム モジュールに転送します。
- システム モジュールから受信した BPDU を処理します。
- ネットワーク管理メッセージを受信して応答します。

ディセーブル ステート

ディセーブル ステートのレイヤ 2 LAN ポートは、フレーム転送または STP に参加しません（図 30-7 を参照）。ディセーブル ステートのレイヤ 2 LAN ポートは事実上、動作することはありません。

図 30-7　　ディセーブル ステートのインターフェイス 2



ディセーブルになったレイヤ 2 LAN ポートは、次の処理を実行します。

- 接続セグメントから受信したフレームを廃棄します。
- 転送用に他のポートからスイッチングされたフレームを廃棄します。
- アドレス データベースに、エンド ステーションの位置情報は組み込みません （ラーニングは行われないため、アドレス データベースは更新されません）。
- BPDU を受信しません。
- システム モジュールから送信用の BPDU を受信しません。

STP および IEEE 802.1Q トランク

802.1Q トランクによって、ネットワークの STP の構築方法に、いくつかの制約が課されます。802.1Q トランクを使用して接続しているシスコのネットワーク デバイスを使用したネットワークでは、ネットワーク デバイスがトランク上で許容される VLAN ごとに 1 つの STP インスタンスを維持します。しかし、他社製の 802.1Q ネットワーク デバイスでは、トランク上で許容されるすべての VLAN に対して 1 つの STP インスタンスしか維持されません。

802.1Q トランクを使用してシスコのネットワーク デバイスを他社製のネットワーク デバイスに接続する場合、シスコのネットワーク デバイスは、トランクの 802.1Q VLAN の STP インスタンスを、他社製の 802.1Q ネットワーク デバイスのインスタンスと統合します。ただし、VLAN 別の STP 情報はす

べて、他社製の 802.1Q ネットワーク デバイスのクラウドと切り離されて、シスコのネットワーク デバイスによって維持されます。シスコのネットワーク デバイスを隔てている他社製の 802.1Q 装置のクラウドは、ネットワーク デバイス間の単一トランク リンクとして処理されます。

802.1Q トランクの詳細については、第 20 章「レイヤ 2 スイッチング用 LAN ポート」を参照してください。

IEEE 802.1w RSTP について

RSTP 概要

デフォルトでイネーブルである RSTP は、ポイントツーポイントの配線を利用して、スパニングツリーの高速コンバージェンスを実現します。スパニングツリーの再設定は 1 秒以内に発生します（802.1D スパニングツリーのデフォルト設定では 50 秒）。

ポートの役割およびアクティブ トポロジー

RSTP では、ポートの役割の割り当て、およびアクティブ トポロジーの学習により、スパニングツリーの高速コンバージェンスが可能になります。RSTP は 802.1D STP 上に構築され、スイッチ プライオリティが最も高い（プライオリティの数値が最も小さい）スイッチが、「ルート ブリッジの選定」（P.30-5）で説明したようにルート ブリッジとして選択されます。RSTP は、次のうちいずれかのポートの役割をそれぞれのポートに割り当てます。

- ルート ポート：スイッチによりパケットがルート ブリッジに転送されるときに、最適のパス（最小コスト）を用意します。
- 指定ポート：指定スイッチに接続します。指定スイッチでは、LAN からルート ブリッジにパケットが転送されるときに、発生するパス コストが最小になります。指定スイッチが LAN に接続するポートのことを指定ポートと呼びます。
- 代替ポート：現在のルート ポートが提供するルート ブリッジへの代替パスを提供します。
- バックアップ ポート：指定ポートが提供した、スパニング ツリーのリーフに向かうパスのバックアップとして機能します。バックアップ ポートが存在できるのは、2 つのポートがポイントツーポイント リンクよってループバックで接続されている場合、または 1 つのスイッチに共有 LAN セグメントへの接続が 2 つ以上ある場合です。
- ディセーブル ポート：スパニング ツリーの動作において何もロールが与えられていません。

ルート ポートまたは DP の役割があるポートは、アクティブ トポロジーに組み込まれます。代替ポートまたはバックアップ ポートのロールがあるポートは、アクティブ トポロジから除外されます。

ネットワーク全体でポートの役割が一貫している安定したトポロジーの場合、RSTP は、すべてのルート ポートおよび DP をフォワーディング ステートにすぐに移行しますが、すべての代替ポートおよびバックアップ ポートは常に廃棄ステートになります（802.1D のブロッキングに相当）。ポートのステートにより、転送処理および学習処理の動作が制御されます。802.1D および RSTP のポート ステートの比較については、表 30-2 を参照してください。

表 30-2　　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（IEEE 802.1D）	RSTP ポート ステート	ポートがアクティブ トポロジに含まれているか
イネーブル	ブロック	廃棄	No
イネーブル	リスニング	廃棄	No
イネーブル	ラーニング	ラーニング	Yes
イネーブル	転送	転送	Yes
ディセーブル	ディセーブル	廃棄	No

Cisco STP の実装との一貫性を保つため、このマニュアルでは、ポート ステートを*廃棄*ではなく*ブロッキング*として定義します。DP はリスニング ステートから開始します。

高速コンバージェンス

RSTP を使用すると、スイッチ、スイッチ ポート、または LAN に障害が発生しても、ただちに接続を回復できます。エッジ ポート、新しいルート ポート、ポイントツーポイント リンクで接続したポートに、高速コンバージェンスが次のように提供されます。

- エッジ ポート：**spanning-tree portfast** 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、RSTP スイッチ上の 1 つのポートをエッジ ポートに設定すると、そのエッジ ポートはただちにフォワーディング ステートになります。エッジ ポートは Port Fast 対応ポートと同じであり、単一エンド ステーションに接続しているポートだけでイネーブルにする必要があります。
- ルート ポート：RSTP は、新しいルート ポートを選択した場合、古いルート ポートをブロックし、新しいルート ポートをフォワーディング ステートにすぐに移行します。
- ポイントツーポイント リンク：ポイントツーポイント リンクで別のポートにポートを接続し、ローカル ポートが DP になると、提案と合意のハンドシェークを使用して別のポートと高速移行がネゴシエーションされ、ループがないトポロジーが確保されます。

  図 30-8 で示したように、スイッチ A は、ポイントツーポイント リンクを介してスイッチ B に接続され、すべてのポートがブロッキング ステートになります。このとき、スイッチ A のプライオリティが、スイッチ B のプライオリティよりも小さい数値であるとします。スイッチ A は提案メッセージ（提案フラグ セットを設定したコンフィギュレーション BPDU）をスイッチ B に送信し、自分自身を指定スイッチとして提案します。

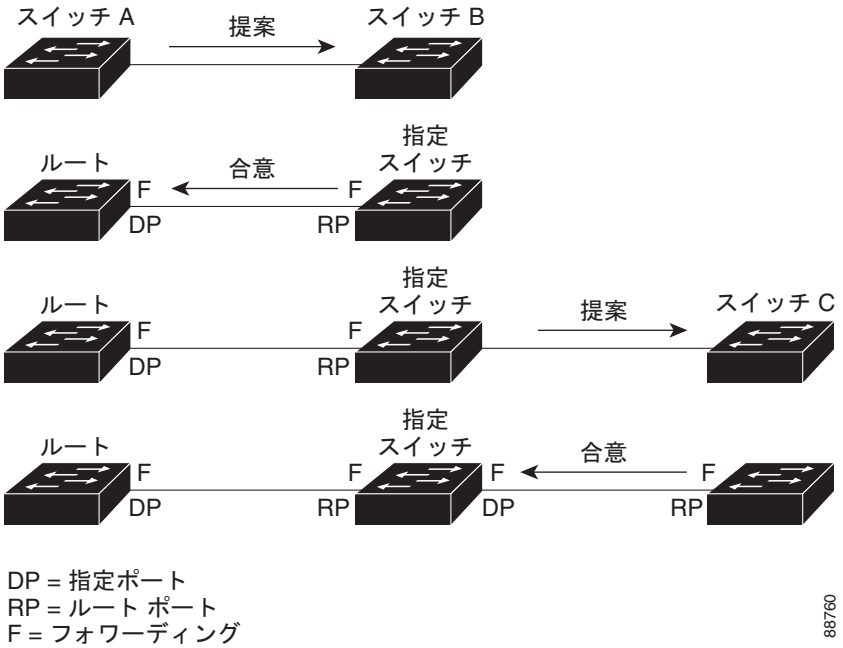
  スイッチ B が提案メッセージを受信すると、提案メッセージを受信したポートを新しいルート ポートとして選択し、すべての非エッジ ポートを強制的にブロッキング ステートにします。さらに、その新しいルート ポート経由で合意メッセージ（合意フラグが設定された BPDU）を送信します。

  スイッチ A は、スイッチ B の合意メッセージを受信すると、ただちに自身の指定ポートをフォワーディング ステートにします。スイッチ B はその非エッジ ポートをすべてブロックし、またスイッチ A とスイッチ B はポイントツーポイント リンクで接続されているので、ネットワークにループは形成されません。

スイッチ C がスイッチ B に接続された場合も、同様のハンドシェイク メッセージが交換されます。スイッチ C はスイッチ B に接続されたポートをルート ポートとして選択し、両端のポートはただちにフォワーディング ステートに移行します。アクティブ トポロジにスイッチが追加されるたびに、このハンドシェイク プロセスが実行されます。ネットワークの収束時には、この提案と合意のハンドシェーク処理がスパニングツリーのルートからリーフに進みます。

スイッチは、ポート デュプレックス モードからリンク タイプを認識します。全二重ポートはポイントツーポイント接続であると見なされ、半二重ポートは共有接続であると見なされます。**spanning-tree link-type** 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、デュプレックス設定によって制御されるデフォルト設定を無効にすることができます。

図 30-8　高速コンバージェンスの提案と合意のハンドシェーク



DP = 指定ポート
RP = ルート ポート
F = フォワーディング

ポートの役割の同期

スイッチのポートの 1 つで提案メッセージが受信され、そのポートが新しいルート ポートに選択されると、RSTP は他のすべてのポートを新しいルートの情報に同期させます。

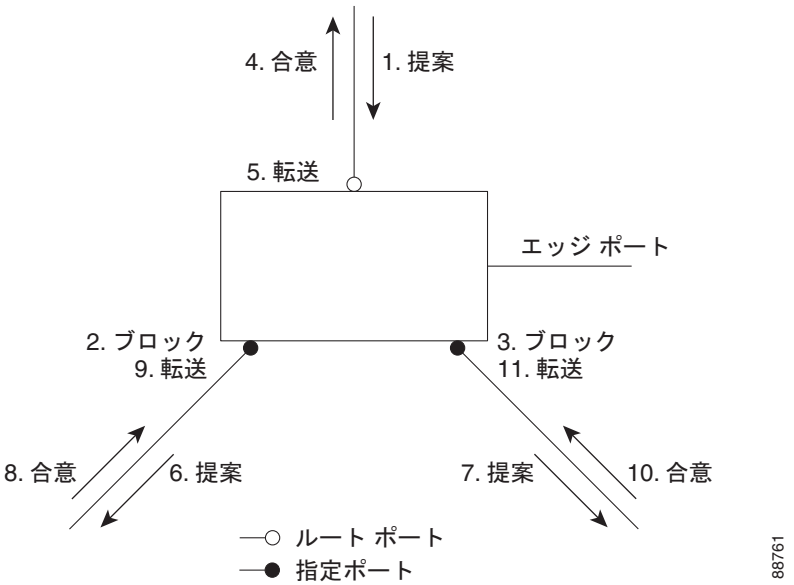
他のすべてのポートが同期化されると、スイッチはルート ポートで受信した優位のルート情報に同期化されます。次のような場合、スイッチ上の個別のポートが同期されます。

- ポートがブロッキング ステートである。
- エッジ ポートである（ネットワークのエッジに存在するように設定されたポート）。

DP は、フォワーディング ステートになっていてエッジ ポートとして設定されていない場合、RSTP によって DP が強制的に新しいルート情報で同期化すると、DP がブロッキング ステートに移行します。一般的に RSTP がルート情報でポートを強制的に同期化し、ポートが上の条件を満たしていない場合、そのポート ステートはブロッキングに設定されます。

スイッチは、すべてのポートが同期化されたことを確認すると、そのルート ポートに対応する指定スイッチに合意メッセージを送信します。ポイントツーポイント リンクで接続されたスイッチがポートの役割について互いに合意すると、RSTP はポート ステートをただちにフォワーディング ステートに移行させます。イベントのシーケンスについては、図 30-9 を参照してください。

図 30-9　高速コンバージェンス中のイベントのシーケンス



BPDU の形式および処理

BPDU の形式および処理の概要

RSTP BPDU の形式は 802.1D BPDU の形式と同じですが、プロトコル バージョンは 2 に設定されます。新しい 1 バイトの Version 1 Length フィールドはゼロに設定されます。つまり、バージョン 1 のプロトコル情報は存在しません。表 30-3 に、RSTP フラグ フィールドを示します。

表 30-3　RSTP BPDU フラグ

ビット	機能
0	トポロジーの変化（TC）
1	提案
2 ～ 3:	ポートの役割：
00	不明
01	代替ポートまたはバックアップ ポート
10	ルート ポート
11	指定ポート
4	ラーニング
5	転送
6	契約
7	トポロジー変更確認応答（TCA）

送信スイッチは、自身を LAN 上の指定スイッチにするために、RSTP BPDU に提案フラグを設定します。提案メッセージのポートの役割は、常に DP に設定されます。

送信スイッチは、提案を受け入れる場合、RSTP BPDU に合意フラグを設定します。合意メッセージのポートの役割は、常にルート ポートに設定されます。

RSTP には TCN BPDU がありません。TC フラグが使用されて、TC が示されます。ただし、802.1D スイッチとの相互運用性を保つために、RSTP スイッチは TCN BPDU の処理と生成を行います。

ラーニング フラグおよびフォワーディング フラグは、送信側ポートのステートに従って設定されます。

優位 BPDU 情報の処理

上位 BPDU は、ルート情報（低いスイッチ ID や低いパス コストなど）を持つ BPDU であり、ポート用に現在保存されているものより上位になります。

ポートが上位 BPDU を受信すると、RSTP は再設定を開始します。ポートが新しいルート ポートとして提案されて選択されると、RSTP は強制的にその他すべてのポートを同期化します。

受信した BPDU が提案フラグの設定された RSTP BPDU である場合、スイッチは他のすべてのポートを同期化した後、合意メッセージを送信します。BPDU が 802.1D BPDU である場合、スイッチは提案フラグを設定せずに、そのポートの転送遅延タイマーを開始します。新しいルート ポートでは、フォワーディング ステートに移行するために、2 倍の転送遅延時間が必要となります。

ポートで受信した上位情報によってポートがバックアップ ポートか代替ポートになった場合、RSTP はそのポートをブロッキング ステートに設定して合意メッセージを送信します。DP は、転送遅延タイマーが失効するまで、提案フラグを設定して BPDU を送信し続け、転送遅延タイマーの失効時に、ポートはフォワーディング ステートに移行します。

下位 BPDU 情報の処理

下位 BPDU は、ルート情報（高いスイッチ ID や高いパス コストなど）を持つ BPDU であり、ポート用に現在保存されているものより下位になります。

DP は、下位 BPDU を受信すると、独自の情報ですぐに応答します。

トポロジの変更

RSTP と 802.1D の間では、スパニングツリーの TC の処理が異なります。

- 検出：ブロッキング ステートとフォワーディング ステート間の*いずれか*の移行によって TC が発生する 802.1D とは異なり、ブロッキング ステートからフォワーディング ステートへの移行*だけ*が、RSTP で TC の原因となります（接続の増加だけが TC と見なされます）。エッジ ポートにおけるステート変更は、TC の原因になりません。RSTP スイッチは、トポロジの変更を検出すると、そのスイッチのすべての非エッジ ポート（TC 通知を受信したポートを除く）で学習した情報を削除します。
- 通知：802.1D とは異なり、RSTP は TCN BPDU を使用しません。ただし、802.1D との相互運用性を保つために、RSTP スイッチは TCN BPDU の処理と生成を行います。
- 確認：RSTP スイッチは、DP で 802.1D スイッチから TCN メッセージを受信した場合、TCA ビットが設定された 802.1D コンフィギュレーション BPDU で応答します。ただし、802.1D スイッチに接続されているルート ポートで TC While タイマー（802.1D の TC タイマーと同じ）がアクティブの場合、TCA がセットされたコンフィギュレーション BPDU を受信すると、TC While タイマーはリセットされます。

  この動作方式が必要なのは、802.1D スイッチを介してサポートする場合だけです。RSTP BPDU は TCA ビットが設定されていません。

- 伝播：RSTP スイッチは、指定ポートまたはルート ポートを介して別のスイッチから TC メッセージを受信すると、自身のすべての非エッジ ポート、指定ポート、およびルート ポート（この TC メッセージを受信したポートを除く）に変更を伝播します。スイッチは、これらのすべてのポートの TC 時間タイマーを起動し、これらのポート上で学習した情報を削除します。
- プロトコルの移行：802.1D スイッチとの下位互換性を保つため、RSTP は 802.1D コンフィギュレーション BPDU および TCN BPDU をポート単位で選択的に送信します。

  ポートが初期化されると、移行遅延タイマーが開始され（RSTP BPDU が送信される最低時間を指定）、RSTP BPDU が送信されます。このタイマーがアクティブな間、スイッチはそのポートで受信したすべての BPDU を処理し、プロトコル タイプを無視します。

  ポート移行遅延タイマーの期限切れ後にスイッチで 802.1D BPDU を受信した場合は、802.1D スイッチに接続していると見なして、802.1D BPDU のみを使用して開始します。ただし、RSTP スイッチが 1 つのポートで 802.1D BPDU を使用していて、タイマーが満了したあとに RSTP BPDU を受信した場合、タイマーが再起動し、そのポートで RSTP BPDU の使用が開始されます。

MST について

MST の概要

MST では複数の VLAN がスパニングツリー インスタンスにマッピングされ、それぞれのインスタンスには、その他のスパニングツリー インスタンスに依存しないスパニングツリー トポロジーが含まれます。このアーキテクチャによって複数の転送パスがデータ トラフィックに提供され、ロードバランスが可能になり、多数の VLAN のサポートに必要となるスパニングツリー インスタンスの数が減ります。MST では、1 つのインスタンス（転送パス）で障害が発生しても他のインスタンス（転送パス）に影響しないため、ネットワークのフォールトトレランスが向上します。

最も一般的には、レイヤ 2 スイッチド ネットワークのバックボーン レイヤおよび配布レイヤに最初に MST を配置します。この配置では、サービス プロバイダー環境で必要となる、一種の高可用性ネットワークが提供されます。

MST では明示的なハンドシェークによって高速スパニングツリー コンバージェンスが提供され、802.1D 転送遅延がなくなり、ルート ブリッジ ポートおよび DP がフォワーディング ステートに高速で移行します。

MST ではスパニング ツリーの動作が改善され、次の STP バージョンとの下位互換性を維持しています。

- 元の 802.1D スパニング ツリー
- 既存のシスコ固有の Multiple Instance STP（MISTP）
- 既存のシスコの PVST+
- Rapid Per-VLAN Spanning Tree Plus（Rapid PVST+）

（注）
- IEEE 802.1w では RSTP が定義されて、IEEE 802.1D に組み込まれました。
- IEEE 802.1s では MST が定義されて、IEEE 802.1Q に組み込まれました。

MST リージョン

MST インスタンスに加えるスイッチは、同じ MST 設定情報を使用して、設定を統一する必要があります。同じ MST コンフィギュレーションを持ち、相互接続されたスイッチの集合を MST リージョンといいます（図 30-10（P.30-22）を参照）。

各スイッチがどの MST リージョンに属しているかは、MST コンフィギュレーションによって制御されます。この設定には、領域の名前、バージョン番号、MST VLAN とインスタンスの割り当てマップが含まれます。

リージョンには、MST 設定が同一である、1 つ以上のメンバを含めることができます。各メンバでは、RSTP ブリッジ プロトコル データ ユニット（BPDU）を処理できる必要があります。ネットワークにおける MST リージョンの数に制限はありませんが、各リージョンでは 65 までのスパニングツリー インスタンスをサポートできます。インスタンスは、0 ～ 4094 の範囲の任意の番号で識別できます。スパニングツリー インスタンスに同時に割り当てられる VLAN は 1 つだけです。

IST、CIST、CST

IST、CIST、CST の概要

すべてのスパニングツリー インスタンスが独立しているその他のスパニングツリー プロトコルとは異なり、MST は、Internal Spanning Tree（IST）、Common and Internal Spanning Tree（CIST）、Common Spanning Tree（CST）インスタンス確立および維持します。

- IST は、MST リージョンで実行するスパニングツリーです。

  それぞれの MST リージョン内では、MST によって複数のスパニングツリー インスタンスが維持されます。インスタンス 0 は、IST という、領域の特殊インスタンスです。その他すべての MSTI には、1 ～ 4094 の番号が付きます。

  IST は、BPDU の送受信を行う唯一のスパニングツリー インスタンスです。その他すべてのスパニングツリー インスタンス情報は、MSTP レコード（M レコード）に含まれ、MST BPDU 内でカプセル化されます。MST BPDU はすべてのインスタンスの情報を搬送するので、複数のスパニングツリー インスタンスをサポートするために処理する必要がある BPDU の数は大きく削減されます。

  同一リージョン内のすべての MSTI は同一プロトコル タイマーを共有しますが、各 MSTI には、ルート ブリッジ ID やルート パス コストなど、独自のトポロジー パラメータがあります。デフォルトでは、すべての VLAN が IST に割り当てられます。

  MSTI はリージョンにローカルです。たとえばリージョン A およびリージョン B が相互接続されていても、リージョン A の MSTI 1 は、リージョン B の MSTI 1 に依存しません。

- CIST は、各 MST リージョンの IST の集合です。

- CST は、MST リージョンと単一スパニングツリーを相互接続します。

あるリージョンで算出されたスパニングツリーは、スイッチド ドメイン全体を含む CST のサブツリーとして認識されます。CIST は、802.1w、802.1s、802.1D の各規格をサポートするスイッチで実行されているスパニングツリー アルゴリズムによって形成されています。MST リージョン内の CIST は、リージョン外の CST と同じです。

詳細については、「MST 領域内でのスパニングツリーの動作」（P.30-21）および「MST 領域間のスパニングツリー動作」（P.30-21）を参照してください。

MST 領域内でのスパニングツリーの動作

IST は、リージョンにあるすべての MST スイッチを接続します。IST が収束するとき、IST のルートは、図 30-10（P.30-22）に示すように CIST リージョナル ルートになります（802.1s 規格の実装前の *IST マスター*）。ネットワークに領域が 1 つしかない場合、CIST リージョナル ルートは CIST ルートにもなります。CIST ルートがリージョンの外部にある場合、リージョンの境界に位置する MST スイッチの 1 つが CIST リージョナル ルートとして選択されます。

MST スイッチが初期化されると、スイッチ自体を識別する BPDU が、CIST のルートおよび CIST リージョナル ルートとして送信されます。このとき、CIST ルートと CIST リージョナル ルートへのパス コストは両方ゼロに設定されます。スイッチはさらに MST インスタンスをすべて初期化し、自身がこれらすべてのインスタンスのルートであると主張します。スイッチは、ポートに現在保存されているルート情報よりも優位の MST ルート情報（小さいスイッチ ID、パス コストなど）を受信すると、CIST リージョナル ルートとしての主張を撤回します。

リージョンには、初期化中に多くのサブ リージョンが含まれて、それぞれに独自の CIST リージョナル ルートが含まれることがあります。スイッチは、同一リージョンのネイバーから上位 IST 情報を受信すると、古いサブ リージョンを脱退し、真の CIST リージョナル ルートを含む新しいサブ リージョンに加入します。これにより、真の CIST リージョナル ルートを含むサブ リージョンを除くすべてのサブ リージョンは縮小します。

正常な動作のためには、MST リージョン内のすべてのスイッチが同じ CIST リージョナル ルートを承認する必要があります。共通の CIST リージョナル ルートに収束する場合、そのリージョン内にある 2 つのスイッチは、1 つの MST インスタンスに対するポートの役割のみを同期させます。

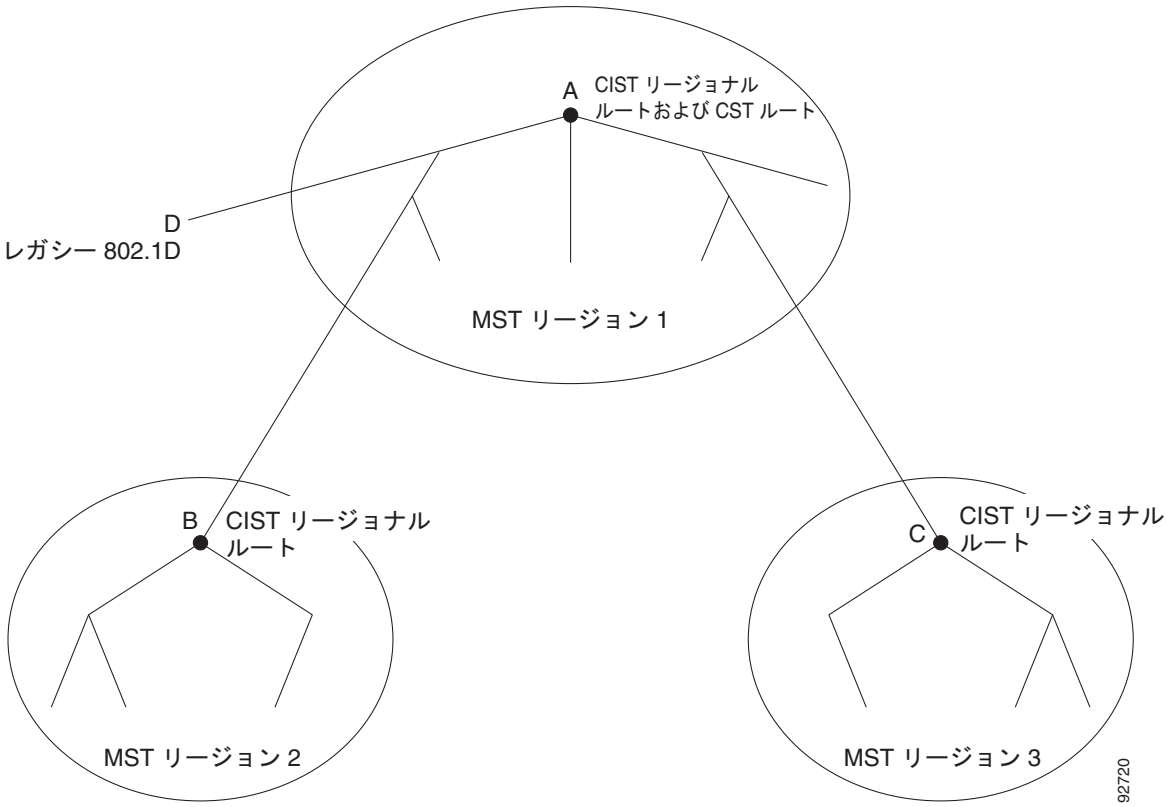
MST 領域間のスパニングツリー動作

ネットワーク内に複数のリージョンまたは 802.1D スイッチがある場合、MST は CST を確立して維持します。これには、ネットワーク内のすべての MST リージョンおよびすべての 802.1D STP スイッチが含まれます。MSTI は、リージョンの境界にある IST と組み合わさり、CST になります。

IST は、リージョン内のすべての MST スイッチを接続し、スイッチ ドメイン全体を含んだ CIST 内のサブツリーとして認識されます。サブツリーのルートは CIST リージョナル ルートです。MST リージョンは、隣接する STP スイッチや MST リージョンからは仮想スイッチとして認識されます。

図 30-10 に、3 つの MST 領域と 802.1D（D）があるネットワークを示します。リージョン 1 の CIST リージョナル ルート（A）は、CIST ルートでもあります。リージョン 2 の CIST リージョナル ルート（B）、およびリージョン 3 の CIST リージョナル ルート（C）は、CIST 内のそれぞれのサブツリーのルートです。

図 30-10　MST リージョン、CIST リージョナル ルート、CST ルート



BPDU を送受信するのは、CST インスタンスだけです。MST インスタンスは自身のスパニングツリー情報を BPDU に追加して、ネイバー スイッチと通信し、最終的なスパニングツリー トポロジを計算します。このため、BPDU 送信に関連するスパニングツリー パラメータ（hello タイム、転送時間、最大経過時間、最大ホップ数など）は CST インスタンス上でのみ設定されますが、すべての MSTI に影響します。スパニングツリー トポロジーに関連するパラメータ（スイッチ プライオリティ、ポート VLAN コスト、ポート VLAN プライオリティなど）は、CST インスタンスおよび MSTI の両方で設定できます。

MST スイッチは、802.1D 専用スイッチと通信する場合、バージョン 3 BPDU または 802.1D STP BPDU を使用します。MST スイッチは、MST スイッチと通信する場合、MST BPDU を使用します。

IEEE 802.1s の用語

準規格の実装で使用される、一部の MST 命名規則は変更され、一部の*内部*パラメータおよび*リージョナル*パラメータの識別が組み込まれました。これらのパラメータは MST 領域内だけで使用され、ネットワーク全体で使用される外部パラメータと比較されます。CIST だけがネットワーク全体に広がるスパニングツリー インスタンスなので、CIST パラメータだけに外部修飾子が必要になり、修飾子またはリージョン修飾子は不要です。

- CIST ルートは CIST のルート ブリッジで、ネットワーク全体にまたがる一意のインスタンスです。
- CIST 外部ルート パス コストは、CIST ルートまでのコストです。このコストは MST 領域内で変化しません。CIST では、MST リージョンが単一のスイッチのように見えるので注意してください。CIST 外部ルート パス コストは、これらの仮想スイッチとリージョンに属していないスイッチ間を計算して出したルート パス コストです。

- CIST リージョナル ルートは、準規格の実装で IST マスターと呼ばれていました。CIST ルートが領域内にある場合、CIST リージョナル ルートは CIST ルートです。または、CIST リージョナル ルートがそのリージョンで CIST ルートに最も近いスイッチになります。CIST リージョナル ルートは、IST のルート ブリッジとして動作します。
- CIST 内部ルート パス コストは、領域内の CIST リージョナル ルートまでのコストです。このコストは、IST つまりインスタンス 0 だけに関連します。

表 30-4 に、IEEE 規格とシスコ準規格の用語の比較を示します。

表 30-4　準規格と規格の用語

IEEE 規格の定義	シスコ準規格の実装	シスコ規格の実装
CIST リージョナル ルート	IST マスター	CIST リージョナル ルート
CIST 内部ルート パス コスト	IST マスター パス コスト	CIST 内部パス コスト
CIST 外部ルート パス コスト	ルート パス コスト	ルート パス コスト
MSTI リージョナル ルート	インスタンス ルート	インスタンス ルート
MSTI 内部ルート パス コスト	ルート パス コスト	ルート パス コスト

ホップ カウント

MST は、設定 BPDU のメッセージ エージ情報および最大エージ情報を使用せずにスパニングツリー トポロジーを算出します。その代わりに、IP Time To Live（TTL）メカニズムに似た、ルートまでのパス コストおよびホップ カウント メカニズムを使用します。

spanning-tree mst max-hops 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、領域内の最大ホップ数を設定し、IST およびその領域のすべての MSTI に適用できます。ホップ カウントは、メッセージ エージ情報と同じ結果になります（再設定を開始）。インスタンスのルート ブリッジは、コストが 0 でホップ カウントが最大値に設定された BPDU（M レコード）を常に送信します。この BPDU を受信したスイッチは、受信 BPDU の残存ホップ カウントから 1 だけ差し引いた値を残存ホップ カウントとする BPDU を生成し、これを伝播します。このホップ カウントが 0 になると、スイッチはその BPDU を廃棄し、ポート用に維持されていた情報を期限切れにします。

BPDU の RSTP 部分のメッセージ エージ情報および最大エージ情報は、リージョン全体で同じままです。同じ値が、境界にあるリージョンの DP によって伝播されます。

境界ポート

シスコ準規格の実装では、境界ポートが次のうちいずれかの STP リージョンに MST リージョンを接続します。

- RSTP が動作している単一スパニングツリー リージョン
- PVST+ または Rapid PVST+ が動作している単一スパニングツリー リージョン
- MST 設定が異なる別の MST リージョン

また、境界ポートは、指定スイッチが単一のスパニングツリー スイッチ、または異なる MST コンフィギュレーションを持つスイッチである LAN に接続されます。

802.1s 規格には、境界ポートの定義がありません。802.1Q-2002 規格では、内部（同一リージョンから着信）および外部という、ポートが受信できる 2 種類のメッセージが識別されています。メッセージが外部である場合、CIST だけが受信します。CIST の役割がルートや代替ルートの場合、または外部 BPDU のトポロジが変更された場合は、MST インスタンスに影響する可能性があります。メッセージ

が内部である場合、CIST は CIST 部分を受信し、各 MSTI はそれぞれの M レコードを受信します。シスコ準規格の実装では、外部メッセージを受信するポートが境界ポートとして扱われます。つまりポートは、内部メッセージと外部メッセージを一緒に受信できません。

MST リージョンには、スイッチと LAN の両方が含まれています。セグメントは、DP のリージョンに属します。このため、セグメントの DP と異なるリージョンのポートは境界ポートです。この定義では、リージョン内部の 2 つのポートが、別のリージョンに属するポートとセグメントを共有し、内部メッセージおよび外部メッセージの両方を 1 つのポートで受信できるようになります。

シスコ準規格の実装からの主な変更点は、DP が、STP 互換モードで動作していない場合、境界ポートとして定義されないことです。

（注）　802.1D STP スイッチがセグメントにある場合、メッセージは常に外部と見なされます。

準規格の実装からの変更点には、RSTP またはレガシー 802.1s スイッチに送信者スイッチ ID が含まれる場所に、CIST リージョナル ルート ブリッジ ID フィールドが挿入されることもあります。一貫した送信スイッチ ID をネイバー スイッチに送信することで、リージョン全体で 1 つの仮想スイッチのように動作します。この例では、スイッチ A または B がそのセグメントで指定されているかどうかにかかわらず、スイッチ C が、ルートの一貫した送信スイッチ ID を持つ BPDU を受信します。

規格準拠 MST 実装

- 「ポートの役割の命名規則の変更点」（P.30-24）
- 「レガシーおよび規格準拠スイッチの間のスパニングツリー相互運用」（P.30-24）

（注）　規格準拠 MST 実装には、規格を満たすために必要となる機能、および公開されている規格にまだ組み込まれていない、必要な準規格機能の一部が含まれます。

ポートの役割の命名規則の変更点

境界の役割は最終的な MST 規格から削除されましたが、この境界という概念は規格準拠実装で維持されます。ただしリージョンの境界にある MSTI ポートは、対応する CIST ポートの状態に従わないことがあります。現在、次の 2 つの状況があります。

- 境界ポートが CIST リージョナル ルートのルート ポートである：CIST インスタンス ポートは、提案されて同期化されると、合意を返送して、対応するすべての MSTI ポートが同期化された（フォワーディングになって）あとにだけフォワーディング ステートに移行します。MSTI ポートには、特別なマスターの役割があります。
- 境界ポートが CIST リージョナル ルートのルート ポートでない：MSTI ポートは、CIST ポートのステートおよび役割に従います。規格が提供する情報は少なく、MSTI ポートが BPDU（M レコード）を受信しないとき、交互にブロッキングできる理由を理解することは困難です。この状況の場合、境界の役割はすでに存在しませんが、**show** コマンドを入力すると、出力の *type* カラムでポートが境界として識別されます。

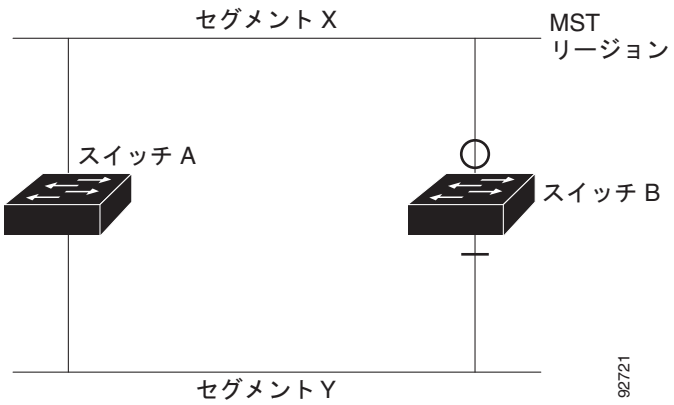
レガシーおよび規格準拠スイッチの間のスパニングツリー相互運用

先行標準のスイッチでは先行標準のポートを自動検出ができないため、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認識させます。標準と先行標準の間にあるリージョンは形成できませんが、CIST を使用する前に相互運用できます。この特定状況では、さまざまなインスタンスにおけるロードバランス機能だけが失われます。ポートが準規格 BPDU を受信したとき、CLI ではポート

設定によって異なるさまざまなフラグが表示されます。また、スイッチが、先行標準の BPDU 転送の設定がされてないポートで先行標準の BPDU を初めて受信すると、Syslog メッセージにも表示されます。

図 30-11 に、準規格スイッチに接続された規格準拠スイッチを示します。A は規格準拠スイッチ、B は準規格スイッチであり、両方とも同一リージョンに設定されているとします。A は CIST のルート ブリッジなので、B にはセグメント X にルート ポート（BX）およびセグメント Y に代替ポート（BY）があります。セグメント Y がフラップして、先行標準の BPDU を送信する前に BY のポートが代替ポートになった場合、AY は Y に接続している先行標準のスイッチを検出できないため、標準の BPDU を送信し続けます。ポート BY は境界に固定され、A と B の間でのロードバランスは不可能になります。セグメント X にも同じ問題がありますが、B は TC を送信することがあります。

図 30-11　規格準拠と準規格スイッチの相互運用



（注） 規格 MST 実装と準規格 MST 実装間の相互作用を最低限に抑えることを推奨します。

IEEE 802.1D-1998 STP とのインターオペラビリティ

MST を稼働しているスイッチは、802.1D スイッチとの相互運用を可能にする組み込みプロトコル移行機能をサポートします。このスイッチで、802.1D コンフィギュレーション BPDU（プロトコル バージョンが 0 に設定されている BPDU）を受信する場合、そのポート上の 802.1D BPDU のみが送信されます。MST スイッチは、802.1D BPDU、異なるリージョンに対応付けられた MST BPDU（バージョン 3）、または RSTP BPDU（バージョン 2）を受信すると、ポートがリージョンの境界にあることを検出できます。

ただし、スイッチは、802.1D BPDU を受信しなくなった場合でも、自動的には MSTP モードには戻りません。これは、802.1D スイッチが指定スイッチではない場合、802.1D スイッチがリンクから削除されたかどうかを検出できないためです。さらにスイッチは、接続先スイッチがリージョンに加入した場合であっても、引き続きポートに境界の役割を指定する可能性があります。プロトコル移行プロセスを再起動する（ネイバー スイッチとの再ネゴシエーションを強制する）には、**clear spanning-tree detected-protocols** 特権 EXEC コマンドを使用します。

リンクのすべての 802.1D スイッチが RSTP スイッチである場合、802.1D スイッチは、RSTP BPDU であるかのように MST BPDU を処理できます。このため MST スイッチは、バージョン 0 の設定および Topology Change Notification（TCN）BPDU、または境界ポートのバージョン 3 の MST BPDU を送信します。境界ポートは、指定スイッチがシングル スパニングツリー スイッチまたは異なる MST コンフィギュレーションを持つスイッチのいずれかである LAN に接続されます。

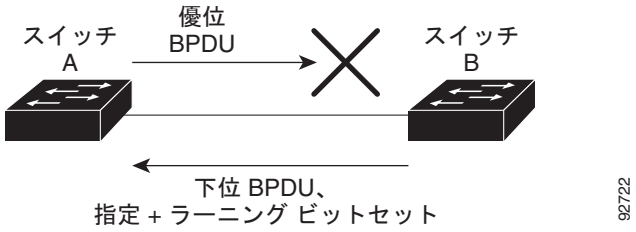
単一方向リンク障害の検出

IEEE 802.1D-2004 RSTP および IEEE 802.1Q-2005 MSTP 標準に含まれる解決メカニズムを使用して、スイッチは、受信した BPDU のポート ロールとステートの一貫性をチェックして、ブリッジング ループが発生する可能性のある単一方向リンク障害を検出します。

指定ポートが矛盾を検出するとロールは維持されますが、状態は廃棄（ブロッキング）ステートに戻ります。これは、接続に矛盾が生じた場合、ブリッジング ループを開始するよりも接続を中断する方が好ましいためです。

図 30-12 に、一般的にブリッジング ループになる単一方向リンク障害を示します。スイッチ A はルート ブリッジで、その BPDU は、スイッチ B へのリンク上では失われます。RSTP および MST BPDU には、送信側ポートの役割とステートが含まれます。この情報により、送信する上位 BPDU に対してスイッチ B が反応しないこと、スイッチ B はルート ブリッジではなく指定ポートであることが、スイッチ A によって検出できます。結果として、スイッチ A は自身のポートをブロックし（またはブロックを維持して）、ブリッジ処理のループを回避します。

図 30-12　単一方向リンク障害の検出



スパニングツリー プロトコルのデフォルト設定

STP のデフォルト設定

機能	デフォルト値
モード	Rapid PVST+
イネーブル ステート	すべての VLAN でイネーブル
ブリッジ プライオリティ	32768
SPT ポート プライオリティ（ポート単位で設定可能：レイヤ 2 アクセス ポートとして設定された LAN ポートで使用される）	128

機能	デフォルト値	
SPT ポート コスト（ポート単位で設定可能：レイヤ 2 アクセス ポートとして設定された LAN ポートで使用される）	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
	イーサネット：	100
STP VLAN ポート プライオリティ（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 LAN ポートで使用される）	128	
STP 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 LAN ポートで使用される）	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
	イーサネット：	100
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	

デフォルト MST 設定

機能	デフォルト設定	
スパニングツリー モード	Rapid PVST+ (MST はディセーブルに設定されている)	
スイッチ プライオリティ （MST ポートごとに設定可能）	32768	
スパニングツリー ポート プライオリティ （MST インスタンス ポートごとに設定可能）	128	
スパニングツリー ポート コスト （MST インスタンス ポートごとに設定可能）	10 ギガビット イーサネット：	2,000
	ギガビット イーサネット：	20,000
	ファスト イーサネット：	200,000
	イーサネット：	2,000,000
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	
最大ホップ カウント	20 ホップ	

スパニングツリー プロトコルの設定方法

STP の設定

（注）　この章で説明する STP コマンドは任意の LAN ポートに設定できますが、これらのコマンドが有効になるのは、**switchport** キーワードを使用して設定した LAN ポートに限られます。

注意　物理的なループの存在しないトポロジーであっても、スパニングツリーをディセーブルにすることは推奨しません。スパニングツリーは、設定の誤りおよび配線の誤りに対する保護手段として動作します。VLAN に物理ループが存在しないことを確認せずに、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。

STP のイネーブル化

（注）　STP は、VLAN 1 および新たに作成されたすべての VLAN で、デフォルトでイネーブルに設定されています。

STP は、VLAN 単位でイネーブルにできます。スイッチは VLAN ごとに個別の STP インスタンスを維持します（STP をディセーブルに設定した VLAN を除きます）。

VLAN 単位で STP 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	`Router(config)# spanning-tree vlan vlan_ID`	VLAN 単位で STP をイネーブルにします。*vlan_ID* の値は 1 ～ 4094 です（予約済み VLAN は除く。「STP のデフォルト設定」（P.30-26）を参照）。
	`Router(config)# default spanning-tree vlan vlan_ID`	指定された VLAN のすべての STP パラメータを、デフォルト値に戻します。
	`Router(config)# no spanning-tree vlan vlan_ID`	指定された VLAN で STP をディセーブルにします。このコマンドについては、次の「注意」を参照してください。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

注意　VLAN のすべてのスイッチおよびブリッジでスパニングツリーがディセーブルになっていない場合は、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。スパニングツリーは、VLAN の一部のスイッチおよびブリッジでディセーブルにしておきながら、VLAN のその他のスイッチおよびブリッジでイネーブルにしておくことはできません。スパニングツリーをイネーブルにしたスイッチとブリッジに、ネットワークの物理トポロジに関する不完全な情報が含まれることになるので、この処理によって予想外の結果となることがあります。

注意　物理的なループの存在しないトポロジーであっても、スパニングツリーをディセーブルにすることは推奨しません。スパニングツリーは、設定の誤りおよび配線の誤りに対する保護手段として動作します。VLAN に物理ループが存在しないことを確認せずに、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。

次に、VLAN 200 で STP をイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# spanning-tree vlan 200
Router(config)# end
Router#
```

（注）　STP 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設定の結果を表示しても、STP 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、設定を確認する例を示します。

```
Router# show spanning-tree vlan 200

VLAN0200
  Spanning tree enabled protocol ieee
  Root ID     Priority    32768
              Address     00d0.00b8.14c8
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32768
              Address     00d0.00b8.14c8
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300
```

```
Interface        Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
Gi1/4            Desg FWD 200000    128.196  P2p
Gi1/5            Back BLK 200000    128.197  P2p

Router#
```

（注） VLAN 200 スパニングツリーを作成するには、VLAN 200 にアクティブなインターフェイスが少なくとも 1 つ必要です。この例では、VLAN 200 内の 2 つのインターフェイスがアクティブです。

拡張システム ID のイネーブル化

（注）
- 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。
- 拡張範囲 VLAN（1006 ～ 4094）を設定するには、拡張システム ID をイネーブルにする必要があります。
- VTP ドメイン内の任意のスイッチでイネーブルになっている場合、拡張システム ID をイネーブルにする必要があります。

1024 MAC アドレスをサポートするシャーシの拡張システム ID をイネーブルにできます（「ブリッジ ID について」（P.30-3）を参照）。

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	`Router(config)# spanning-tree extend system-id`	拡張システム ID をイネーブルにします。 **（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（「VLAN の範囲」（P.25-3）を参照）。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

（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。

```
Router# configure terminal
Router(config)# spanning-tree extend system-id
Router(config)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show spanning-tree summary | include Extended
Extended system ID is enabled.
```

ルート ブリッジの設定

Cisco IOS Release 15.1SY でサポートされるスイッチは、アクティブな VLAN ごとに STP のインスタンスを個別に維持します。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の 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 を持つネットワーク デバイスが、その VLAN のルート ブリッジになります。

VLAN インスタンスがルート ブリッジになるように設定するには、**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（32768）から非常に小さな値へと変更します。

spanning-tree vlan *vlan_ID* **root** コマンドを入力すると、各 VLAN で現在ルートになっているブリッジのブリッジ プライオリティがスイッチによって確認されます。拡張システム ID をイネーブルにすると、24576 という値でスイッチが指定された VLAN のルートになる場合、スイッチはその VLAN のブリッジ プライオリティを 24576 に設定します。

拡張システム ID がイネーブルで、指定された VLAN のルート ブリッジのブリッジ プライオリティが 24576 より小さい場合、スイッチはその VLAN のブリッジ プライオリティを最小のブリッジ プライオリティより 4096 小さい値に設定します。(4096 は 4 ビット ブリッジ プライオリティの最下位ビットの値です。表 30-1（P.30-4）を参照)。

（注） ルート ブリッジになるために必要な値が 1 より小さい場合は、**spanning-tree vlan** *vlan_ID* **root** コマンドはエラーになります。

拡張システム ID がイネーブルで、たとえば VLAN 20 のすべてのネットワーク デバイスでデフォルト プライオリティが 32768 に設定されている場合に、スイッチ上で **spanning-tree vlan 20 root primary** コマンドを使用すると、ブリッジ プライオリティが 24576 に設定され、スイッチが VLAN 20 のルート ブリッジになります。

注意 STP 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 スイッチでなければなりません。アクセス スイッチは、STP 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（つまり、レイヤ 2 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。ネットワーク直径を指定すると、その直径のネットワークに最適な hello タイム、転送遅延時間、最大経過時間が自動的に選択されます。これにより、STP 収束の時間が大幅に削減されます。**hello** キーワードを使用して、自動的に計算される hello タイムを上書きすることができます。

（注） STP トポロジを安定した状態に保つには、スイッチをルート ブリッジとして設定したあと、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 ブリッジ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	`Router(config)# spanning-tree vlan vlan_ID root primary [diameter hops [hello-time seconds]]`	スイッチをルート ブリッジとして設定します。*vlan_ID* の値は 1 ～ 4094 です（予約済み VLAN は除く。「STP のデフォルト設定」（P.30-26）を参照）。
	`Router(config)# no spanning-tree vlan vlan_ID root`	ルート ブリッジ コンフィギュレーションを消去します。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

次の例は、ネットワーク直径を 4 にして、スイッチを VLAN 10 のルート ブリッジとして設定する方法を示しています。

```
Router# configure terminal
Router(config)# spanning-tree vlan 10 root primary diameter 4
Router(config)# end
Router#
```

セカンダリ ルート ブリッジの設定

スイッチをセカンダリ ルートとして設定すると、STP ブリッジ プライオリティはデフォルト値（32768）から変更されます。その結果、プライマリ ルート ブリッジに障害が発生した場合に（ネットワーク上の他のネットワーク装置がデフォルトのブリッジ プライオリティ 32768 を使用していると仮定して）、こ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。

拡張システム ID をイネーブルにしている場合、STP はブリッジ プライオリティを 28672 に設定します。

このコマンドは、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 ブリッジを設定できます。プライマリ ルート ブリッジ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。

スイッチをセカンダリ ルート ブリッジ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	`Router(config)# [no] spanning-tree vlan vlan_ID root secondary [diameter hops [hello-time seconds]]`	スイッチをセカンダリ ルート ブリッジとして設定します。*vlan_ID* の値は 1 ～ 4094 です（予約済み VLAN は除く。「STP のデフォルト設定」（P.30-26）を参照）。
	`Router(config)# no spanning-tree vlan vlan_ID root`	ルート ブリッジ設定を消去します。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

次の例は、ネットワーク直径を 4 にして、スイッチを VLAN 10 のセカンダリ ルート ブリッジとして設定する方法を示しています。

```
Router# configure terminal
Router(config)# spanning-tree vlan 10 root secondary diameter 4
Router(config)# end
Router#
```

STP ポート プライオリティの設定

ループが発生すると、STP はポート プライオリティを考慮して、フォワーディング ステートにする LAN ポートを選択します。STP に最初に選択させたい LAN ポートには高いプライオリティ値を、最後に選択させたい LAN ポートには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 LAN ポートの優先順位が同じである場合、STP は最小の LAN ポート番号を持つ LAN ポートをフォワーディング ステートに移行させ、その他の LAN ポートをブロックします。指定できるプライオリティの範囲は 0 ～ 240 であり（デフォルトは 128 です）、16 ずつ増加するよう設定できます。

Cisco IOS は LAN ポートがアクセス 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、LAN ポートがトランク 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。

レイヤ 2 LAN インターフェイスの STP 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	`Router(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	`Router(config-if)# spanning-tree port-priority port_priority`	LAN 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 1 ～ 252 で、4 ずつ増加します。
ステップ 3	`Router(config-if)# spanning-tree vlan vlan_ID port-priority port_priority`	LAN 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 *port_priority* 値の範囲は 1 ～ 252 で、4 ずつ増加します。*vlan_ID* の値は 1 ～ 4094 です（予約済み VLAN は除く。表 25-1（P.25-3）を参照）。
ステップ 4	`Router(config-if)# end`	コンフィギュレーション モードを終了します。

次に、ギガビット イーサネット ポート 1/4 の STP ポート プライオリティを設定する例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 1/4
Router(config-if)# spanning-tree port-priority 160
Router(config-if)# end
Router#
```

次に、ギガビット イーサネット ポート 1/4 の設定を確認する例を示します。

```
Router# show spanning-tree interface gigabitethernet 1/4
Vlan             Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
VLAN0001         Back BLK 200000    160.196  P2p
VLAN0006         Back BLK 200000    160.196  P2p
...
VLAN0198         Back BLK 200000    160.196  P2p
VLAN0199         Back BLK 200000    160.196  P2p
VLAN0200         Back BLK 200000    160.196  P2p
Router#
```

ギガビット イーサネット ポート 1/4 はトランクです。この例のように、複数の VLAN が設定され、アクティブになっています。ポート プライオリティ設定は、この VLAN インターフェイス上のすべての VLAN に適用されます。

（注）　**show spanning-tree interface** コマンドで情報が表示されるのは、ポートが接続され動作している場合に限られます。これらの条件が満たされていない場合は、**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、ギガビット イーサネット ポート 1/4 の VLAN ポート プライオリティを設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 1/4
Router(config-if)# spanning-tree vlan 200 port-priority 64
Router(config-if)# end
Router#
```

この例で入力した設定は VLAN 200 にだけ適用されます。200 以外のすべての VLAN のポート プライオリティは 160 のままです。

次に、設定を確認する例を示します。

```
Router# show spanning-tree interface gigabitethernet 1/4
Vlan             Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
VLAN0001         Back BLK 200000    160.196  P2p
VLAN0006         Back BLK 200000    160.196  P2p
...
VLAN0199         Back BLK 200000    160.196  P2p
VLAN0200         Desg FWD 200000     64.196  P2p

Router#
```

VLAN 200 のスパニングツリー情報を表示するには、次のコマンドも使用できます。

```
Router# show spanning-tree vlan 200 interface gigabitethernet 1/4
Interface        Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
Gi1/4            Desg LRN 200000     64.196  P2p
```

STP ポート コストの設定

STP ポート パス コストのデフォルト値は、LAN インターフェイスのメディア速度から決定されます。ループが発生すると、STP はポート コストを考慮して、フォワーディング ステートにする LAN インターフェイスを選択します。STP に最初に選択させたい LAN インターフェイスには低いコスト値を、最後に選択させたい LAN インターフェイスには高いコスト値を割り当てることができます。すべての LAN インターフェイスが同じコスト値を使用している場合には、STP は LAN インターフェイス番号が最も小さい LAN 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 LAN 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、0 ～ 200000000 です（デフォルトは、メディアによって異なります）。

STP は LAN 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、LAN 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。

レイヤ 2 LAN インターフェイスの STP 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	Router(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	Router(config-if)# **spanning-tree cost** *port_cost*	LAN 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 ～ 200000000 の範囲で指定します。
	Router(config-if)# **no spanning-tree cost**	デフォルトのポート コストに戻します。
ステップ 3	Router(config-if)# **spanning-tree vlan** *vlan_ID* **cost** *port_cost*	LAN 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 ～ 200000000 の範囲で指定します。*vlan_ID* の値は 1 ～ 4094 です（予約済み VLAN は除く。表 25-1（P.25-3）を参照）。
	Router(config-if)# **no spanning-tree vlan** *vlan_ID* **cost**	デフォルトの VLAN ポート コストに戻します。
ステップ 4	Router(config-if)# **end**	コンフィギュレーション モードを終了します。

次に、ギガビット イーサネット ポート 1/4 の STP ポート コストを変更する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 1/4
Router(config-if)# spanning-tree cost 1000
Router(config-if)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show spanning-tree interface gigabitethernet 1/4
Vlan             Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
VLAN0001         Back BLK 1000      160.196  P2p
VLAN0006         Back BLK 1000      160.196  P2p
VLAN0007         Back BLK 1000      160.196  P2p
VLAN0008         Back BLK 1000      160.196  P2p
VLAN0009         Back BLK 1000      160.196  P2p
VLAN0010         Back BLK 1000      160.196  P2p
Router#
```

次に、VLAN 200 の各ポート VLAN コストでポート プライオリティを設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 1/4
Router(config-if)# spanning-tree vlan 200 cost 2000
Router(config-if)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show spanning-tree vlan 200 interface gigabitethernet 1/4
Interface        Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
Gi1/4            Desg FWD 2000       64.196  P2p
```

（注） 次に示す出力では、他の VLAN（VLAN 1 など）はこの設定の影響を受けていません。

```
Router# show spanning-tree vlan 1 interface gigabitethernet 1/4
Interface        Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
Gi1/4            Back BLK 1000      160.196  P2p
Router#
```

（注）　**show spanning-tree** コマンドで情報が表示されるのは、ポートがリンクアップ動作可能ステートで、かつ DTP 用に正しく設定されている場合に限られます。これらの条件が満たされていない場合は、**show running-config** コマンドを入力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）　このコマンドを使用するときは注意してください。ブリッジ プライオリティを変更するには、ほとんどの状況で **spanning-tree vlan** *vlan_ID* **root primary** コマンドおよび **spanning-tree vlan** *vlan_ID* **root secondary** コマンドを使用することを推奨します。

VLAN の STP 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	`Router(config)# spanning-tree vlan` *vlan_ID* **priority** {**0** | **4096** | **8192** | **12288** | **16384** | **20480** | **24576** | **28672** | **32768** | **36864** | **40960** | **45056** | **49152** | **53248** | **57344** | **61440**}	拡張システム ID がイネーブルの場合に、VLAN のブリッジ プライオリティを設定します。*vlan_ID* の値は 1 ～ 4094 です（予約済み VLAN は除く。表 25-1 (P.25-3) を参照）。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

次に、拡張システム ID がディセーブルの場合に、VLAN 200 のブリッジ プライオリティを 33792 に設定する例を示します。

```
Router# configure terminal
Router(config)# spanning-tree vlan 200 priority 32768
Router(config)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show spanning-tree vlan 200 bridge
                                     Hello Max  Fwd
Vlan                 Bridge ID       Time  Age Delay  Protocol
---------------- -------------------- ---- ---- -----  --------
VLAN200          32768 0050.3e8d.64c8    2   20    15  ieee
Router#
```

hello タイムの設定

（注）　このコマンドを使用するときは注意してください。hello タイムを変更するには、ほとんどの状況で **spanning-tree vlan** *vlan_ID* **root primary** コマンドおよび **spanning-tree vlan** *vlan_ID* **root secondary** コマンドを使用することを推奨します。

VLAN の STP 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	`Router(config)# spanning-tree vlan vlan_ID hello-time hello_time`	VLAN の hello タイムを設定します。*hello_time* 値は、1 ～ 10 秒の範囲で指定します。*vlan_ID* の値は 1 ～ 4094 です（予約済み VLAN は除く。表 25-1（P.25-3）を参照）。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

次に、VLAN 200 の hello タイムを 7 秒に設定する例を示します。

```
Router# configure terminal
Router(config)# spanning-tree vlan 200 hello-time 7
Router(config)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show spanning-tree vlan 200 bridge
                                    Hello Max  Fwd
Vlan                 Bridge ID      Time  Age Delay  Protocol
---------------- -------------------- ---- ---- -----  --------
VLAN200          49152 0050.3e8d.64c8    7   20    15  ieee
Router#
```

VLAN の転送遅延時間の設定

VLAN の STP 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	`Router(config)# 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。*vlan_ID* の値は 1 ～ 4094 です（予約済み VLAN は除く。表 25-1（P.25-3）を参照）。
	`Router(config)# no spanning-tree vlan vlan_ID forward-time`	デフォルトの転送時間に戻します。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

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。

```
Router# configure terminal
Router(config)# spanning-tree vlan 200 forward-time 21
Router(config)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show spanning-tree vlan 200 bridge
                                    Hello Max  Fwd
Vlan                 Bridge ID      Time  Age Delay  Protocol
---------------- -------------------- ---- ---- -----  --------
VLAN200          49152 0050.3e8d.64c8    2   20    21  ieee
Router#
```

VLAN の最大エージング タイムの設定

VLAN の STP 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	`Router(config)# 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 ～ 40 秒の範囲で指定します。*vlan_ID* の値は 1 ～ 4094 です（予約済み VLAN は除く。表 25-1（P.25-3）を参照）。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

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。

```
Router# configure terminal
Router(config)# spanning-tree vlan 200 max-age 36
Router(config)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show spanning-tree vlan 200 bridge
                                     Hello Max  Fwd
Vlan                 Bridge ID       Time  Age Delay  Protocol
---------------- -------------------- ---- ---- -----  --------
VLAN200          49152 0050.3e8d.64c8    2   36    15  ieee
Router#
```

Rapid PVST+ のイネーブル化

- 「Rapid PVST+ 概要」（P.30-38）
- 「リンク タイプの設定」（P.30-38）
- 「プロトコル移行の再起動」（P.30-39）

（注）　Rapid PVST+ はデフォルトでイネーブルです。Rapid PVST+ を再度イネーブルにするには、次の手順を使用します。

Rapid PVST+ 概要

Rapid PVST+ 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+ 拡張機能も一部サポートします。

スイッチの Rapid PVST+ モードをイネーブルにするには、特権モードで **spanning-tree mode rapid-pvst** コマンドを入力します。Rapid PVST+ モードでスイッチを設定するには、「STP の設定」（P.30-28）を参照してください。

リンク タイプの設定

高速接続は、ポイントツーポイント リンク上だけに確立されます。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して見なします。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 リンクとして見なし、半二重リンクを共有リンクと見なすため、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** コマンドを入力します。

プロトコル移行の再起動

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。MSTP スイッチは、レガシー BPDU、異なる領域と関連する MST BPDU（バージョン 3）、または RST BPDU（バージョン 2）を受信するときに、ポートが領域の境界にあることも検出できます。

スイッチは、802.1D BPDU を受信しなくなっても、MSTP モードに自動的に戻りません。レガシー スイッチが指定スイッチでない場合、レガシー スイッチが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。さらにスイッチは、接続先スイッチがリージョンに加入した場合であっても、ポートに対して引き続き、境界の役割を割り当てる可能性もあります。

スイッチ全体で、プロトコル移行プロセスを再開するには（近接スイッチと強制的に再ネゴシエーションする）、**clear spanning-tree detected-protocols** イネーブル EXEC コマンドを使用できます。特定のインターフェイスでプロトコル移行プロセスを再開するには、**clear spanning-tree detected-protocols interface** *interface-id* 特権 EXEC コマンドを入力します。

MST の設定

- 「デフォルト MST 設定」（P.30-27）
- 「MST リージョン設定の指定および MST のイネーブル化」（P.30-39）（必須）
- 「ルート ブリッジの設定」（P.30-41）（任意）
- 「セカンダリ ルート ブリッジの設定」（P.30-32）（任意）
- 「STP ポート プライオリティの設定」（P.30-33）（任意）
- 「パス コストの設定」（P.30-44）（任意）
- 「スイッチのプライオリティの設定」（P.30-45）（任意）
- 「hello タイムの設定」（P.30-46）（任意）
- 「送信保留カウントの設定」（P.30-47）（任意）
- 「最大経過時間の設定」（P.30-47）（任意）
- 「最大ホップ カウントの設定」（P.30-48）（任意）
- 「高速移行を保証するリンク タイプの指定」（P.30-48）（任意）
- 「ネイバー タイプの指定」（P.30-48）（任意）
- 「プロトコル移行プロセスの再開」（P.30-49）（任意）
- 「MST の設定およびステータスの表示」（P.30-49）

MST リージョン設定の指定および MST のイネーブル化

2 台以上のスイッチを同一 MST リージョン内に存在させるには、同じ VLAN からインスタンスへのマッピング、同じ構成リビジョン番号、および同じ MST の名前が設定されている必要があります。

リージョンには、MST 設定が同一である、1 つ以上のメンバを含めることができます。各メンバでは、RSTP BPDU を処理できる必要があります。ネットワークにおける MST リージョンの数に制限はありませんが、各リージョンでは 65 までのスパニングツリー インスタンスしかサポートできません。スパニングツリー インスタンスに同時に割り当てられる VLAN は 1 つだけです。

MST リージョン設定を指定して MST 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	`Router# 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	`Router(config)# spanning-tree mst configuration`	MST 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	`Router(config-mst)# instance instance_id vlan vlan_range`	VLAN を MSTI にマップします。 • *instance_id* の範囲は 0 ～ 4094 です。 • **vlan** *vlan_range* の範囲は 1 ～ 4094 です。 VLAN を MSTI にマップする場合、マッピングは増加され、コマンドに指定した VLAN は、以前マッピングした VLAN に追加されるか、そこから削除されます。 VLAN の範囲を指定するには、ハイフンを使用します。たとえば **instance 1 vlan 1-63** では、VLAN 1 ～ 63 が MSTI 1 にマップされます。 一連の VLAN を指定するには、カンマを使用します。たとえば **instance 1 vlan 10, 20, 30** と指定すると、VLAN 10、20、30 が MSTI 1 にマップされます。
ステップ 4	`Router(config-mst)# name instance_name`	インスタンス名を指定します。*name* 文字列の最大の長さは 32 文字であり、大文字と小文字が区別されます。
ステップ 5	`Router(config-mst)# revision version`	設定リビジョン番号を指定します。指定できる範囲は 0 ～ 65535 です。
ステップ 6	`Router(config-mst)# show pending`	保留中の設定を表示し、設定を確認します。
ステップ 7	`Router(config)# exit`	すべての変更を適用し、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	`Router(config)# spanning-tree mode mst`	MST および RSTP をイネーブルにします。 **注意** スパニングツリー モードを変更すると、トラフィックが混乱することがあります。すべてのスパニングツリー インスタンスが以前のモードで停止し、新しいモードで再起動されるからです。 MST と Rapid PVST+ を同時に実行することはできません。
ステップ 9	`Router(config)# end`	特権 EXEC モードに戻ります。

デフォルトに戻すには、次のように操作します。

- デフォルトの MST リージョン設定に戻すには、**no spanning-tree mst configuration** 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 とインスタンスのデフォルト マップに戻すには、**no instance** *instance_id* [**vlan** *vlan_range*] MST コンフィギュレーション コマンド を使用します。
- デフォルト名に戻すには、**no name** MST コンフィギュレーション コマンド を使用します。

- デフォルトのリビジョン番号に戻すには、**no revision** MST コンフィギュレーション コマンドを使用します。

次の例は、MST コンフィギュレーション モードを開始し、VLAN 10 ～ 20 を MSTI 1 にマッピングし、リージョンに *region1* という名前を付けて、設定リビジョンを 1 に設定し、保留中の設定を表示し、変更を適用してグローバル コンフィギュレーション モードに戻る方法を示しています。

```
Router(config)# spanning-tree mst configuration
Router(config-mst)# instance 1 vlan 10-20
Router(config-mst)# name region1
Router(config-mst)# revision 1
Router(config-mst)# show pending
Pending MST configuration
Name      [region1]
Revision  1
Instances configured 2
Instance  Vlans Mapped
--------  ---------------------
0         1-9,21-4094
1         10-20
-------------------------------

Router(config-mst)# exit
Router(config)#
```

ルート ブリッジの設定

スイッチは、スパニングツリー インスタンスを VLAN グループとマッピングして維持します。各インスタンスには、スイッチ プライオリティとスイッチの MAC アドレスからなるスイッチ ID が対応付けられます。最小のスイッチ ID を持つスイッチがその VLAN グループのルート ブリッジになります。

スイッチがルート ブリッジになるように設定するには、**spanning-tree mst** *instance_id* **root** 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、デフォルト値（32768）から大幅に小さい値にスイッチ プライオリティを修正し、スイッチが、指定したスパニングツリー インスタンスのルート ブリッジになるようにします。このコマンドを入力すると、スイッチは、ルート ブリッジのスイッチ プライオリティを確認します。拡張システム ID のサポートのため、スイッチは指定されたインスタンスについて、自身のプライオリティを 24576 に設定します（この値によって、このスイッチが指定されたスパニングツリー インスタンスのルート ブリッジになる場合）。

指定されたインスタンスのルート ブリッジに、24576 に満たないスイッチ プライオリティが設定されている場合は、スイッチは自身のプライオリティを最小のスイッチ プライオリティより 4096 だけ小さい値に設定します。（4096 は 4 ビット スイッチ プライオリティの最下位ビットの値です。表 30-1（P.30-4）を参照）。

ネットワーク上に拡張システム ID をサポートするスイッチとサポートしないスイッチが混在する場合は、拡張システム ID をサポートするスイッチがルート ブリッジになることはほぼありません。拡張システム ID によって、旧ソフトウェアが稼働する接続スイッチのプライオリティより VLAN 番号が大きくなるたびに、スイッチ プライオリティ値が増大します。

各スパニングツリー インスタンスのルート ブリッジは、バックボーンまたはディストリビューション スイッチでなければなりません。アクセス スイッチは、スパニングツリーのプライマリ ルート ブリッジ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（レイヤ 2 ネットワークの任意の 2 つのエンド ステーション間にあるレイヤ 2 ホップの最大数）を指定するには、MSTI 0 だけに使用できる **diameter** キーワードを使用します。ネットワークの直径を指定すると、その直径のネットワークに最適な hello タイム、転送遅延時間、および最大エージング タイムをスイッチが自動的に設定するので、コンバージェンスの所要時間を大幅に短縮できます。**hello** キーワードを使用して、自動的に計算される hello タイムを上書きすることができます。

（注）　ルート ブリッジとして設定されているスイッチでは、hello タイム、転送遅延時間、最大エージング タイムは手動で設定（**spanning-tree mst hello-time**、**spanning-tree mst forward-time**、**spanning-tree mst max-age** の各グローバル コンフィギュレーション コマンドを使用）しないでください。

スイッチをルート ブリッジ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	`Router(config)# 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	`Router(config-config)# spanning-tree mst` *instance_id* **root primary** [**diameter** *net_diameter* [**hello-time** *seconds*]]	（任意）スイッチをルート ブリッジとして設定します。 • *instance_id* には、単一インスタンスを指定したり、インスタンスの範囲をハイフンで区切って指定したり、一連のインスタンスをカンマで区切って指定したりすることができます。指定できる範囲は 0 ～ 4094 です • （任意）**diameter** *net_diameter* には、任意の 2 つのエンド ステーション間におけるレイヤ 2 ホップの最大数を指定します。指定できる範囲は 2 ～ 7 です。このキーワードは、MSTI インスタンス 0 の場合にのみ使用できます。 • （任意）**hello-time** *seconds* には、ルート ブリッジが設定メッセージを生成する時間を秒単位で指定します。指定できる範囲は 1 ～ 10 秒です。デフォルトは 2 秒です。
ステップ 3	`Router(config-config)# end`	特権 EXEC モードに戻ります。

セカンダリ ルート ブリッジの設定

拡張システム ID をサポートするスイッチをセカンダリルートとして設定すると、スイッチ プライオリティはデフォルト値（32768）から 28672 に変更されます。プライマリ ルート ブリッジで障害が発生した場合は、このスイッチが指定インスタンスのルート ブリッジになる可能性があります。これは、他のネットワーク スイッチがデフォルトのスイッチ プライオリティ 32768 を使用し、ルート ブリッジになる可能性が低いことが前提です。

このコマンドは、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 ブリッジを設定できます。**spanning-tree mst** *instance_id* **root primary** グローバル コンフィギュレーション コマンドで、プライマリ ルート ブリッジの設定時に使用したものと同じネットワーク直径値と hello タイム値を使用してください。

スイッチをセカンダリ ルート ブリッジ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	`Router# 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	`Router(config)# spanning-tree mst` *instance_id* **root secondary** [**diameter** *net_diameter* [**hello-time** *seconds*]]	（任意）スイッチをセカンダリ ルート ブリッジとして設定します。 • *instance_id* には、単一インスタンスを指定したり、インスタンスの範囲をハイフンで区切って指定したり、一連のインスタンスをカンマで区切って指定したりすることができます。指定できる範囲は 0 ～ 4094 です • （任意）**diameter** *net_diameter* には、任意の 2 つのエンド ステーション間における最大数を指定します。指定できる範囲は 2 ～ 7 です。このキーワードは、MSTI インスタンス 0 の場合にのみ使用できます。 • （任意）**hello-time** *seconds* には、ルート ブリッジが設定メッセージを生成する時間を秒単位で指定します。指定できる範囲は 1 ～ 10 秒です。デフォルトは 2 秒です。 プライマリ ルート ブリッジ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。「ルート ブリッジの設定」（P.30-41）を参照してください。
ステップ 3	`Router(config)# end`	特権 EXEC モードに戻ります。

ポート プライオリティの設定

ループが発生する場合、MST は、フォワーディング ステートにするインターフェイスを選択するとき、ポート プライオリティを使用します。最初に選択されるインターフェイスには高いプライオリティ値（小さい数値）を割り当て、最後に選択されるインターフェイスには低いプライオリティ値（高い数値）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のプライオリティ値が同一である場合、MST はインターフェイス番号が最も低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、その他のインターフェイスをブロックします。

インターフェイスの MST 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	`Router# 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	`Router(config)# interface` {{**fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port* | {**port-channel** *number*}}	（任意）設定するインターフェイスを指定します。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	`Router(config-if)# spanning-tree mst instance_id port-priority priority`	ポート プライオリティを設定します。 • *instance_id* には、単一インスタンスを指定したり、インスタンスの範囲をハイフンで区切って指定したり、一連のインスタンスをカンマで区切って指定したりすることができます。指定できる範囲は 0 ～ 4094 です • *priority* 値の範囲は 0 ～ 240 で、16 ずつ増加します。デフォルトは 128 です。値が小さいほど、プライオリティが高くなります。 使用可能な値は、0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240 だけです。その他の値はすべて拒否されます。
ステップ 4	`Router(config-if)# end`	特権 EXEC モードに戻ります。

（注）　**show spanning-tree mst interface** *interface_id* 特権 EXEC コマンドでは、ポートがリンクアップ動作状態になっている場合に限って情報が表示されます。ポートがリンクアップ動作状態になっていない場合は、**show running-config interface** 特権 EXEC コマンドを使用して設定を確認できます。

パス コストの設定

MST パス コストのデフォルト値は、インターフェイスのメディア速度から取得されます。ループが発生する場合、MST は、フォワーディング ステートにするインターフェイスを選択するとき、コストを使用します。最初に選択されるインターフェイスには低いコスト値を割り当て、最後に選択されるインターフェイスには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のコスト値が同一である場合、MST はインターフェイス番号が最も低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、その他のインターフェイスをブロックします。

インターフェイスの MST 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	`Router# 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	`Router(config)# interface {{fastethernet | gigabitethernet | tengigabitethernet} slot/port | {port-channel number}}`	（任意）設定するインターフェイスを指定します。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	`Router(config-if)# spanning-tree mst instance_id cost cost`	コストを設定します。 ループが発生した場合、MST はパス コストを使用して、フォワーディング ステートにするインターフェイスを選択します。低いパス コストは高速送信を表します。 • *instance_id* には、単一インスタンスを指定したり、インスタンスの範囲をハイフンで区切って指定したり、一連のインスタンスをカンマで区切って指定したりすることができます。指定できる範囲は 0 ～ 4094 です • *cost* の範囲は 1 ～ 200000000 です。デフォルト値はインターフェイスのメディア速度から派生します。
ステップ 4	`Router(config-if)# end`	特権 EXEC モードに戻ります。

（注）　**show spanning-tree mst interface** *interface_id* 特権 EXEC コマンドでは、リンクアップ動作状態になっているポートだけの情報が表示されます。ポートがリンクアップ動作状態になっていない場合は、**show running-config** 特権 EXEC コマンドを使用して設定を確認できます。

スイッチのプライオリティの設定

スイッチ プライオリティを設定し、スイッチがルート ブリッジとして選択される可能性を高くすることができます。

（注）　このコマンドの使用には注意してください。スイッチ プライオリティを変更するには、ほとんどの状況で **spanning-tree mst** *instance_id* **root primary** および **spanning-tree mst** *instance_id* **root secondary** 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ことを推奨します。

スイッチ 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	`Router# 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	`Router(config)# spanning-tree mst` *instance_id* **priority** *priority*	（任意）スイッチ プライオリティを設定します。 • *instance_id* には、単一インスタンスを指定したり、インスタンスの範囲をハイフンで区切って指定したり、一連のインスタンスをカンマで区切って指定したりすることができます。指定できる範囲は 0 ～ 4094 です • *priority* の範囲は 0 ～ 61440 で、4096 ずつ増加します。デフォルトは 32768 です。数値が小さいほど、スイッチがルート ブリッジとして選択される可能性が高くなります。 使用可能な値は、0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440 です。その他の値はすべて拒否されます。
ステップ 3	`Router(config)# end`	特権 EXEC モードに戻ります。

hello タイムの設定

hello タイムを変更し、ルート ブリッジが設定メッセージを生成する時間を設定できます。

（注）　このコマンドの使用には注意してください。hello タイムを修正するには、ほとんどの状況で **spanning-tree mst** *instance_id* **root primary** および **spanning-tree mst** *instance_id* **root secondary** 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ことを推奨します。

すべての MSTI に 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	`Router# 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	`Router(config)# spanning-tree mst hello-time` *seconds*	（任意）すべての MSTI に hello タイムを設定します。hello タイムは、ルート ブリッジが設定メッセージを生成する時間です。これらのメッセージは、スイッチがアクティブであることを意味します。 *seconds* に指定できる範囲は 1 ～ 10 です。デフォルトは 2 です。
ステップ 3	`Router(config)# end`	特権 EXEC モードに戻ります。

転送遅延時間の設定

すべての MSTI に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	`Router# 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	`Router(config)# spanning-tree mst forward-time` *seconds*	（任意）すべての MSTI に転送時間を設定します。転送遅延は、ポートがスパニングツリー ラーニングおよびリスニング ステートからフォワーディング ステートに変更するまでに待機する秒数です。 *seconds* に指定できる範囲は 4 ～ 30 です。デフォルトは 15 です。
ステップ 3	`Router(config)# end`	特権 EXEC モードに戻ります。

送信保留カウントの設定

すべての MSTI に送信保留カウントを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# 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	`Router(config)# spanning-tree transmit hold-count` *hold_count_value*	すべての MSTI に送信保留カウントを設定します。 *hold_count_value* の範囲は 1 ～ 20 で、デフォルトは 6 です。
ステップ 3	`Router(config)# end`	特権 EXEC モードに戻ります。

最大経過時間の設定

すべての MSTI に最大エージング 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	`Router# 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	`Router(config)# spanning-tree mst max-age` *seconds*	（任意）すべての MSTI に最大エージング タイムを設定します。最大エージング タイムは、再構成を試行するまでにスイッチがスパニングツリー コンフィギュレーション メッセージを受信せずに待機する秒数です。 *seconds* に指定できる範囲は 6 ～ 40 です。デフォルトは 20 です。
ステップ 3	`Router(config)# end`	特権 EXEC モードに戻ります。

最大ホップ カウントの設定

すべての MSTI に最大ホップ カウントを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# 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	`Router(config)# spanning-tree mst max-hops` *hop_count*	（任意）BPDU が廃棄されて、ポート用に維持された情報が期限切れになるまでの、リージョン内のホップ数を指定します。 *hop_count* の範囲は 1 ～ 255、デフォルトは 20 です。
ステップ 3	`Router(config)# end`	特権 EXEC モードに戻ります。

高速移行を保証するリンク タイプの指定

ポイントツーポイント リンクでポート間を接続し、ローカル ポートが DP になると、RSTP は提案と合意のハンドシェークを使用して別のポートと高速移行をネゴシエーションし、「高速コンバージェンス」（P.30-15）で説明したようなループがないトポロジーを保証します。

デフォルトの場合、リンク タイプはインターフェイスのデュプレックス モードから制御されます。全二重ポートはポイントツーポイント接続、半二重ポートは共有接続と見なされます。MST が稼働しているリモート スイッチ上の 1 つのポートと物理的にポイントツーポイントで接続されている半二重リンクが存在する場合は、リンク タイプのデフォルト設定値を変更して、フォワーディング ステートへの高速移行をイネーブルにできます。

デフォルトのリンク タイプ設定を無効にするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# 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	`Router(config)# interface {{fastethernet | gigabitethernet | tengigabitethernet}` *slot/port* `| {port-channel` *number*`}}`	（任意）設定するインターフェイスを指定します。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	`Router(config)# spanning-tree link-type point-to-point`	ポートのリンク タイプがポイントツーポイントであることを指定します。
ステップ 4	`Router(config)# end`	特権 EXEC モードに戻ります。

ネイバー タイプの指定

トポロジーには、準規格準拠デバイスおよび 802.1s 規格準拠デバイスの両方を含めることができます。デフォルトの場合、ポートは準規格デバイスを自動的に検出できますが、規格 BPDU および準規格 BPDU の両方を受信できます。デバイスとそのネイバーの間に不一致がある場合は、CIST だけがインターフェイスで動作します。

準規格 BPDU だけを送信するようにポートを設定できます。ポートが STP 互換モードになっていても、すべての **show** コマンドで準規格フラグが表示されます。

デフォルトのリンク タイプ設定を無効にするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# 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	`Router(config)# interface {{fastethernet | gigabitethernet | tengigabitethernet} slot/port | {port-channel number}}`	（任意）設定するインターフェイスを指定します。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	`Router(config)# spanning-tree mst pre-standard`	ポートが準規格 BPDU だけを送信できることを指定します。
ステップ 4	`Router(config)# end`	特権 EXEC モードに戻ります。

プロトコル移行プロセスの再開

MST を稼働しているスイッチは、802.1D スイッチとの相互運用を可能にする組み込みプロトコル移行機能をサポートします。このスイッチで、802.1D コンフィギュレーション BPDU（プロトコル バージョンが 0 に設定されている BPDU）を受信する場合、そのポート上の 802.1D BPDU のみが送信されます。MST は、802.1D BPDU、異なるリージョンに対応付けられた MST BPDU（バージョン 3）、または RST BPDU（バージョン 2）を受信すると、ポートがリージョン境界にあることを検出できます。

ただし、スイッチは、802.1D BPDU を受信しなくなった場合でも、自動的には MSTP モードには戻りません。これは、802.1D スイッチが指定スイッチではない場合、802.1D スイッチがリンクから削除されたかどうかを検出できないためです。さらにスイッチは、接続先スイッチがリージョンに加入した場合であっても、ポートに対して引き続き、境界の役割を割り当てる可能性もあります。

スイッチでプロトコル移行プロセスを再起動する（ネイバー スイッチとの再ネゴシエーションを強制する）には、**clear spanning-tree detected-protocols** 特権 EXEC コマンドを使用します。

特定のインターフェイスでプロトコル移行プロセスを再開するには、**clear spanning-tree detected-protocols interface** *interface_id* 特権 EXEC コマンドを使用します。

MST の設定およびステータスの表示

スパニングツリーのステータスを表示するには、表 30-5 で説明する 1 つ以上の特権 EXEC コマンドを使用します。

表 30-5　MST ステータスを表示するコマンド

コマンド	目的
show spanning-tree mst configuration	MST リージョンの設定を表示します。
show spanning-tree mst configuration digest	現在の MSTCI に含まれる MD5 ダイジェストを表示します。
show spanning-tree mst *instance_id*	指定インスタンスの MST 情報を表示します。
show spanning-tree mst interface *interface_id*	指定インターフェイスの MST 情報を表示します。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CHAPTER 31

オプションの STP 機能

（注）

- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。
- スパニングツリー プロトコル（STP）の設定手順については、第 30 章「スパニングツリー プロトコル」を参照してください。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

PortFast

PortFast について

STP PortFast を使用すると、アクセス ポートとして設定されたレイヤ 2 LAN ポートが、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 ステートを開始します。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、STP のコンバージェンスを待たずに、デバイスがただちにネットワークに接続されます。1 台のワークステーションまたはサーバに接続されたインターフェイスがブリッジ プロトコル データ ユニット（BPDU）を受信しないようにする必要があります。PortFast 用に設定されているポートでも、STP は動作しています。PortFast 対応ポートは、必要に応じて、ブロッキング ステートにただちに移行できます（これは、上位 BPDU を受信したときに発生することがあります）。トランク ポート上で PortFast をイネーブルにできます。PortFast には、設定値と異なる動作値を設定できます。

エッジ ポート、ネットワーク ポート、または標準ポートのいずれかとして明確にポートを設定できます。レイヤ 2 ホストに接続されるエッジ ポートは、アクセス ポートまたはトランク ポートとして動作できます。ネットワーク ポートは、レイヤ 2 スイッチまたはブリッジだけに接続されます。

PortFast のイネーブル化

ヒント　STP PortFast とともに STP BPDU ガードを、BPDU を受信した場合に STP の PortFast 対応ポートをシャット ダウンするように設定します。

PortFast デフォルト ステートの設定

デフォルト PortFast のステ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	`Router(config)# spanning-tree portfast [edge | network | normal] default`	すべてのスイッチ アクセス ポートのデフォルト ステートを、エッジ、ネットワーク、または標準に設定します。Bridge Assurance は、デフォルトによりすべてのネットワーク アクセス ポート上でイネーブルになります。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

（注）
- デフォルトのスパニングツリー ポート タイプは、標準タイプです。これは単に、そのトポロジが指定されていないことを意味します。
- レイヤ 2 スイッチまたはブリッジに接続しているポートをエッジ ポートとして設定すると、ブリッジング ループが発生することがあります。
- レイヤ 2 にホスト接続されたポートを、間違ってスパニングツリー ネットワーク ポートとして設定すると、そのポートは自動的にブロッキング ステートになります。

次に、デフォルトのスイッチのアクセス ポート ステートをエッジに設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# spanning-tree portfast edge default
```

レイヤ 2 ポートでの PortFast のイネーブル化

レイヤ 2 アクセス ポートでの PortFast のイネーブル化

注意　VLAN を終端し、そこからポートが STP BPDU を受信することがない、次のようなエンド ホストのデバイスに接続されているポートでのみ、**spanning-tree portfast edge** [**trunk**] コマンドを入力します。
— ワーク ステーション。
— サーバ。
— ブリッジングをサポートするように設定されていないルータ上のポート。

レイヤ 2 アクセス ポート上で PortFast 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	`Router(config)# interface {type slot/port} | {port-channel port_channel_number}`	設定するポートを選択します。
ステップ 2	`Router(config-if)# spanning-tree portfast edge [trunk]`	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 ポート上でエッジの動作をイネーブルにします。リンクがトランクである場合、**trunk** キーワードを入力します。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。

次に、インターフェイス上で PortFast のイネーブル化および確認を行う方法を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 5/8
Router(config-if)# spanning-tree portfast edge
Router(config-if)# end
Router#
Router# show running-config interface gigabitethernet 5/8
Building configuration...

Current configuration:
```

```
!
interface GigabitEthernet5/8
 no ip address
 switchport
 switchport access vlan 200
 switchport mode access
 spanning-tree portfast edge
end
Router#
```

レイヤ 2 ネットワーク ポートでの PortFast のイネーブル化

レイヤ 2 ネットワーク ポート上で PortFast 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	`Router(config)# interface {type slot/port} | {port-channel port_channel_number}`	設定するポートを選択します。
ステップ 2	`Router(config-if)# spanning-tree portfast network`	ポートをネットワーク ポートとして設定します。Bridge Assurance は、グローバルでイネーブルになっている場合、ポート上でイネーブルになります。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。

次に、インターフェイス上で PortFast のイネーブル化および確認を行う方法を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 5/8
Router(config-if)# spanning-tree portfast edge
Router(config-if)# end
Router#
Router# show running-config interface gigabitethernet 5/8
Building configuration...

Current configuration:
!
interface GigabitEthernet5/8
 no ip address
 switchport
 switchport access vlan 200
 switchport mode access
 spanning-tree portfast edge
end
Router#
```

Bridge Assurance

Bridge Assurance について

Bridge Assurance を使用すると、ネットワーク内でブリッジング ループの原因となる問題の発生を防ぐことができます。具体的には、Bridge Assurance を使用して、単方向リンク障害または他のソフトウェア障害、およびスパニングツリー アルゴリズムの停止後もデータ トラフィックを転送し続けているデバイスから、ネットワークを保護します。

Bridge Assurance はデフォルトでイネーブルになっており、ディセーブル化はグローバルに限り可能です。さらに Bridge Assurance は、ポイントツーポイントのスパニングツリー ネットワーク ポートでだけイネーブルになります。Bridge Assurance は必ず、リンクの両端でイネーブルにする必要があります。リンクの一端のデバイスで Bridge Assurance がイネーブルであっても、他端のデバイスが Bridge Assurance をサポートしていない、または Bridge Assurance がイネーブルではない場合、接続ポートはブロックされます。

Bridge Assurance をイネーブルにすると、各 hello タイム期間中に、代替ポートやバックアップ ポートを含む動作中のすべてのネットワーク ポートで BPDU が送信されます。所定の期間に BPDU を受信しなかったポートは、一貫性のない（ブロッキング）ステートになります。このポートは、ルート ポートの計算には使用されません。BPDU を再度受信するようになると、そのポートで通常のスパニングツリー状態遷移が再開されます。

図 31-1 は、標準の STP トポロジを示しています。図 31-2 は、デバイスが故障しており、Bridge Assurance が実行されていない場合に想定されるネットワークの問題点を示しています。

図 31-1　標準的な STP トポロジのネットワーク

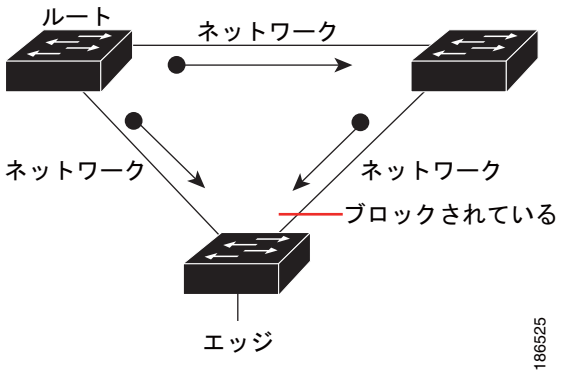


図 31-2　Bridge Assurance を実行していないネットワークの問題

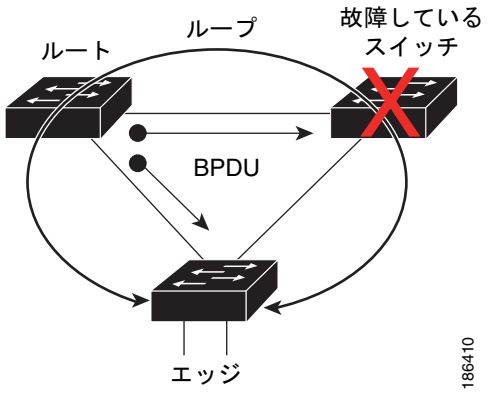


図 31-3 に、Bridge Assurance がイネーブルで、各 STP ネットワーク ポートから送出される双方向 BPDU によって STP トポロジが正常に進行するネットワークを示します。図 31-4 に、ネットワークで Bridge Assurance をイネーブルにすると、図 31-2 で示したネットワークの問題がどのように回避されるかを示します。

図 31-3　Bridge Assurance を実行しているネットワークの STP トポロジ

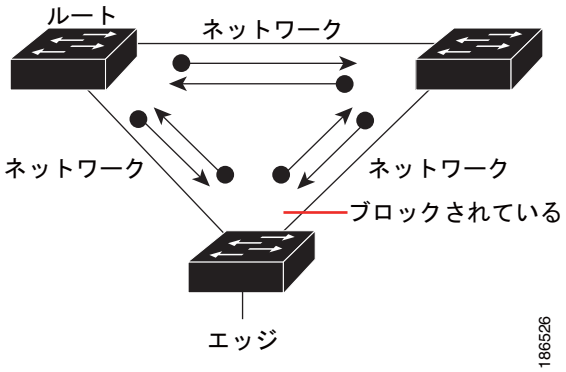
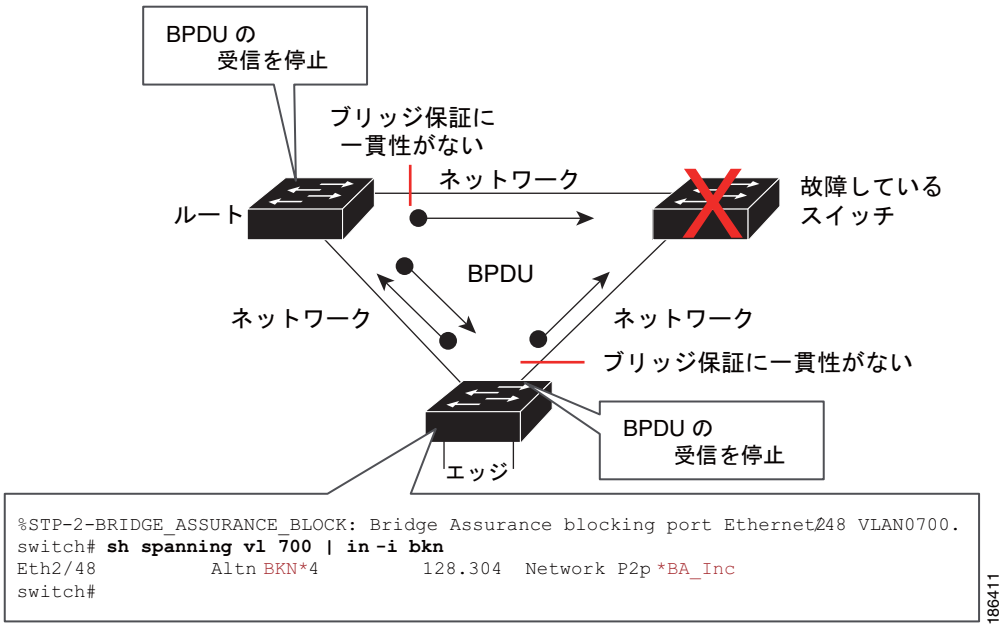


図 31-4　Bridge Assurance によるネットワーク上の問題の回避



Bridge Assurance を使用する場合は、次の注意事項に従ってください。

- Bridge Assurance は、ポイントツーポイントのスパニングツリー ネットワーク ポート上だけで実行されます。この機能は、リンクの両端で設定する必要があります。
- Bridge Assurance は、ネットワーク全体でイネーブルにすることを推奨します。

Bridge Assurance のイネーブル化

デフォルトでは、Bridge Assurance はスイッチのすべてのネットワーク ポートでイネーブルになっています。Bridge Assurance をディセーブルにすると、すべての設定済みネットワーク ポートが標準のスパニングツリー ポートとして動作します。Bridge Assurance をグローバルにイネーブル化またはディセーブル化するには、次の作業を行います。

コマンド	目的
`Router(config)# spanning-tree bridge assurance`	スイッチのすべてのネットワーク ポートで Bridge Assurance をイネーブルにします。

この例では、スイッチのすべてのネットワーク ポートで PortFast Bridge Assurance をイネーブルにし、ネットワーク ポートを設定する方法を示します。

```
Router(config)# spanning-tree bridge assurance
Router(config)# interface gigabitethernet 5/8
Router(config-if)# spanning-tree portfast network
Router(config-if)# exit
```

BPDU ガード

BPDU ガードについて

BPDU ガードがポート上でイネーブルになっている場合、BPDU ガードは BPDU を受信するポートをシャットダウンします。BPDU ガードがグローバルに設定されている場合、BPDU ガードは PortFast（エッジ）ステートのポート上だけで有効です。有効な設定では、PortFast レイヤ 2 LAN インターフェイス（エッジ ポート）は BPDU を受信しません。PortFast レイヤ 2 LAN 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。このように BPDU ガード機能では、管理者が手動でレイヤ 2 LAN インターフェイスを再び作動させなければならないので、無効な設定に対する安全な対処が可能になります。BPDU ガードはインターフェイス レベルで設定可能です。インターフェイス レベルで設定された BPDU ガードは、PortFast 設定に関係なく、ポートが BPDU を受信するとすぐにポートをシャットダウンします。

（注） グローバルにイネーブル化された BPDU ガードは、PortFast（エッジ）動作ステートのすべてのインターフェイスに適用されます。

BPDU ガードのイネーブル化

BPDU ガードのグローバルなイネーブル化

BPDU 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	`Router(config)# spanning-tree portfast edge bpduguard default`	スイッチのすべてのエッジ ポートで、BPDU ガードをデフォルトでグローバルにイネーブル化します。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

次に、BPDU ガードをイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# spanning-tree portfast edge bpduguard default
Router(config)# end
```

次に、設定を確認する例を示します。

```
Router# show spanning-tree summary totals
Root bridge for: Bridge VLAN0025
EtherChannel misconfiguration guard is enabled
Extended system ID                  is enabled
```

```
PortFast Edge BPDU Guard Default    is enabled
Portfast Edge BPDU Filter Default   is disabled
Portfast Default                    is edge
Bridge Assurance                    is enabled
Loopguard                           is disabled
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
```

ポートでの BPDU ガードのイネーブル化

ポート上で BPDU 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	Router(config)# **interface** {*type slot/port*} | {**port-channel** *port_channel_number*}	設定するポートを選択します。
ステップ 2	Router(config-if)# **spanning-tree bpduguard enable**	ポートで BPDU ガードをイネーブルにします。
ステップ 3	Router(config-if)# **end**	コンフィギュレーション モードを終了します。

次に、BPDU ガードをイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# spanning-tree portfast edge bpduguard default
Router(config)# end
```

PortFast エッジ BPDU フィルタリング

PortFast エッジ BPDU フィルタリングについて

PortFast エッジ BPDU フィルタリングを使うことで、管理者は特定ポート上での BPDU 送信や BPDU 受信をシステムで禁止することができます。

グローバルに設定された PortFast エッジ BPDU フィルタリングは、動作中のすべての PortFast（エッジ）ポートに適用されます。PortFast 動作ステートのポートは、ホストに接続されていると見なされ、通常は BPDU をドロップします。動作中の PortFast ポートが BPDU を受信すると、そのポートはただちに PortFast 動作ステータスが消失して標準ポートになります。この場合、PortFast エッジ BPDU フィルタリングはこのポート上でディセーブルになり、STP はポート上で BPDU の送信を再開します。

PortFast エッジ BPDU フィルタリングはポート単位で設定することもできます。PortFast エッジ BPDU フィルタリングがポート上で明示的に設定されている場合、BPDU は送信されず、受信したすべての BPDU はドロップされます。

注意　ホストに接続されていないポートで PortFast エッジ BPDU フィルタリングを明示的に設定すると、そのポートは受信したすべての BPDU を無視し、フォワーディング ステートに移行するため、ブリッジング ループが発生することがあります。

PortFast エッジ BPDU フィルタリングをグローバルにイネーブルにし、ポート設定を PortFast エッジ BPDU フィルタリングのデフォルトに設定すると（「PortFast エッジ BPDU フィルタリングのイネーブル化」（P.31-10）を参照）、PortFast は PortFast エッジ 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。

ポート設定がデフォルトに設定されていない場合、PortFast 設定は PortFast エッジ BPDU フィルタリングに影響しません。表 31-1 に、使用可能な PortFast エッジ BPDU フィルタリングの組み合わせを示します。PortFast エッジ BPDU フィルタリングを使用すると、エンド ホストの接続直後に、アクセス ポートがフォワーディング ステートに直接移行できます。

表 31-1　PortFast エッジ BPDU フィルタリング ポートの設定

ポート単位の設定	グローバル設定	PortFast のステート	PortFast BPDU フィルタリングのステート
デフォルト	イネーブル	イネーブル	イネーブル **（注）** ポートは 10 以上の BPDU を送信します。このポートがいずれかの BPDU を受信した場合、PortFast および PortFast エッジ BPDU フィルタリングはディセーブルになります。
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	N/A	ディセーブル
ディセーブル	N/A	N/A	ディセーブル
イネーブル	N/A	N/A	イネーブル

PortFast エッジ BPDU フィルタリングのイネーブル化

- 「PortFast エッジ BPDU フィルタリングのグローバルなイネーブル化」（P.31-10）
- 「非トランキング ポートでの PortFast エッジ BPDU フィルタリングのイネーブル化」（P.31-11）

PortFast エッジ BPDU フィルタリングのグローバルなイネーブル化

PortFast エッジ 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	`Router(config)# spanning-tree portfast edge bpdufilter default`	スイッチのすべてのエッジ ポートで、BPDU フィルタリングをデフォルトでグローバルにイネーブル化します。スイッチのすべてのエッジ ポートで、BPDU フィルタリングをデフォルトでグローバルにディセーブル化するには、**no** プレフィックスを使用します。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

各エッジ ポート上で、BPDU フィルタリングはデフォルトに設定されています。次に、ポート上で PortFast エッジ BPDU フィルタリングをイネーブルにして、PVST+ モードで設定を確認する例を示します。

```
Router(config)# spanning-tree portfast edge bpdufilter default
Router(config)# exit

Router# show spanning-tree summary totals
Root bridge for: Bridge VLAN0025
EtherChannel misconfiguration guard is enabled
Extended system ID                  is enabled
PortFast Edge BPDU Guard Default    is disabled
Portfast Edge BPDU Filter Default   is enabled
Portfast Default                    is edge
Bridge Assurance                    is enabled
Loopguard                           is disabled
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
Router#
```

非トランキング ポートでの PortFast エッジ BPDU フィルタリングのイネーブル化

非トランキング ポート上で PortFast エッジ BPDU フィルタリング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	`Router(config)# interface {type 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	`Router(config-if)# spanning-tree bpdufilter [enable | disable]`	ポート上で 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。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。

次に、非トランキング ポート上で PortFast エッジ BPDU フィルタリングをイネーブルにする例を示します。

```
Router(config)# interface gigabitethernet 4/4
Router(config-if)# spanning-tree bpdufilter enable
Router(config-if)# ^Z

Router# show spanning-tree interface gigabitethernet 4/4

Vlan             Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
VLAN0010         Desg FWD 1000      160.196  Edge P2p

Router# show spanning-tree interface gigabitethernet 4/4 detail
 Port 196 (GigabitEthernet4/4) 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
Router#
```

UplinkFast

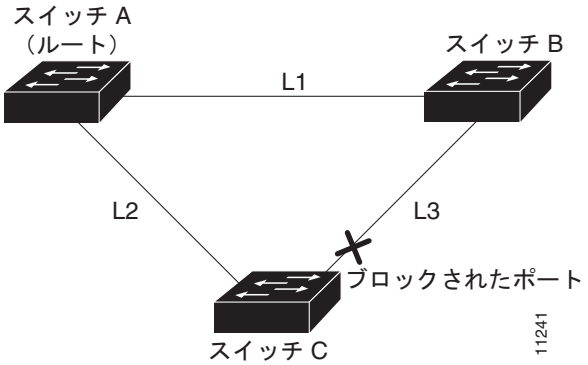
UplinkFast について

UplinkFast は、直接接続されたリンクの障害発生後高速コンバージェンスを行い、アップリンク グループを使用して、冗長レイヤ 2 リンク間でロードバランスを実行します。アップリンク グループは、（VLAN ごとの）レイヤ 2 LAN インターフェイスの集合であり、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）ルート ポートと、（セルフループを行うポートを除く）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。

（注）　UplinkFast は、配線クローゼット スイッチに使用すると最も効果的です。それ以外の用途には、この機能は有用でない場合もあります。

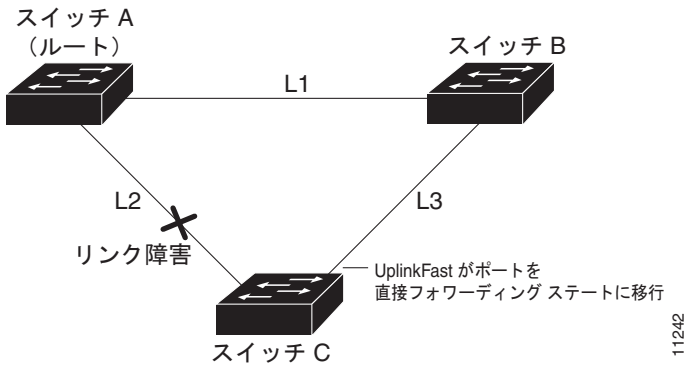
図 31-5 は、リンク障害が発生していないときのトポロジー例です。スイッチ A（ルート ブリッジ）は、リンク L1 を通じてスイッチ B に、リンク L2 を通じてスイッチ C に直接接続されています。スイッチ B に直接接続されているスイッチ C のレイヤ 2 LAN インターフェイスは、ブロッキング ステートです。

図 31-5　　直接リンク障害が発生する前の UplinkFast の例



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 31-6 を参照）。このスイッチ オーバーに要する時間は 1 ～ 5 秒です。

図 31-6　直接リンク障害が発生したあとの UplinkFast の例



UplinkFast のイネーブル化

UplinkFast を使用すると、ブリッジ プライオリティが 49152 に増えるとともに、スイッチ上のすべてのレイヤ 2 LAN ポートの STP ポート コストに 3000 が加算されます。その結果、スイッチがルート ブリッジになる確率が低くなります。ブリッジ プライオリティを設定している VLAN 上では、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** コマンドを入力して、VLAN のブリッジ プライオリティをデフォルトに戻します。

（注） UplinkFast をイネーブルにすると、スイッチのすべての VLAN に影響します。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	`Router(config)# spanning-tree uplinkfast` `Router(config)# spanning-tree uplinkfast [max-update-rate max_update_rate]`	UplinkFast をイネーブルにします。 UplinkFast をイネーブルにし、アップデート速度を秒単位で指定します。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

次の例では、UplinkFast をイネーブルにする方法を示します。

```
Router# configure terminal
Router(config)# spanning-tree uplinkfast
Router(config)# exit
```

次に、UplinkFast をイネーブルにして、アップデート速度を 400 パケット / 秒に設定する例を示します。

```
Router# configure terminal
Router(config)# spanning-tree uplinkfast
Router(config)# spanning-tree uplinkfast max-update-rate 400
Router(config)# exit
```

次に、UplinkFast がイネーブルになっていることを確認する例を示します。

```
Router# show spanning-tree uplinkfast
UplinkFast is enabled
```

BackboneFast

BackboneFast について

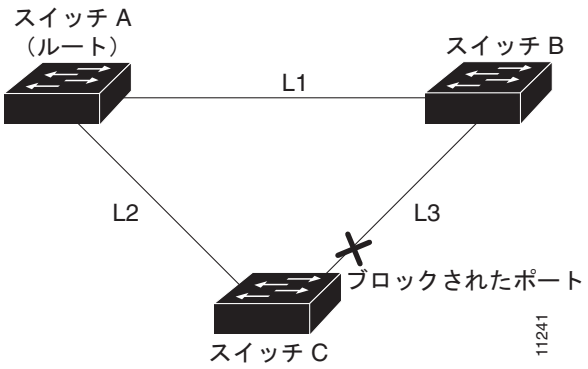
ネットワーク デバイス上のルート ポートまたはブロックされたポートが、そのポートの指定ブリッジから下位 BPDU を受信すると、BackboneFast が開始されます。下位 BPDU により、1 台のネットワーク デバイスをルート ブリッジおよび指定ブリッジの両方として識別します。ネットワーク デバイスが下位 BPDU を受信すると、ネットワーク デバイスはそのネットワーク デバイスが直接接続されていないリンク（*間接*リンク）で障害が発生した（つまり、指定ブリッジからルート ブリッジへの接続が切断された）ものと見なします。標準的な STP ルールに従う場合、ネットワーク デバイスは設定されている最大エージング タイム（STP の **max-age** コマンドで指定）の間下位 BPDU を無視します。

ネットワーク デバイスは、ルート ブリッジへの代替パスの有無を判別します。下位 BPDU がブロックされたポートに到達した場合には、ネットワーク デバイスのルート ポートおよび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（セルフループ ポートはルート ブリッジの代替パスとは見なされません）。下位 BPDU がルート ポートに到達した場合には、すべてのブロック ポートがルート ブリッジへの代替パスになります。下位 BPDU がルート ポートに到達し、かつブロックされたポートがない場合には、ネットワーク デバイスはルート ブリッジへの接続が切断されたものと見なし、ルートの最大エージング タイムを満了させ、通常の STP ルールに従ってルート ブリッジになります。

ネットワーク デバイスにルート ブリッジへの代替パスがある場合、ネットワーク デバイスはそれらの代替パスを使用して、ルート リンク クエリー プロトコル データ ユニット（PDU）と呼ばれる新しい種類の PDU を送信します。ネットワーク デバイスはルート ブリッジへのすべての代替パスに対して、ルート リンク クエリー PDU を送信します。ルートへの代替パスがまだ存在していることが判明すると、ネットワーク デバイスは、下位 BPDU を受信したポートの最大エージング タイムを満了させます。ルート ブリッジへのすべての代替パスが、ネットワーク デバイスとルート ブリッジ間の接続が切断されていることを示している場合には、ネットワーク デバイスは、下位 BPDU を受信したポートの最大エージング タイムを満了させます。1 つまたは複数の代替パスからルート ブリッジに引き続き接続できる場合には、ネットワーク デバイスは、下位 BPDU を受信したすべてのポートを指定ポートにして、（ブロッキング ステートになっていた場合）ブロッキング ステートから、リスニング ステートおよびラーニング ステートを経て、フォワーディング ステートに移行させます。

図 31-7 は、リンク障害が発生していないときのトポロジー例です。スイッチ A（ルート ブリッジ）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 LAN インターフェイスは、ブロッキング ステートです。

図 31-7　間接リンク障害が発生する前の BackboneFast の例



リンク L1 で障害が発生した場合、スイッチ C はリンク L1 に直接接続されていないので、この障害を検出できません。一方、スイッチ B は L1 を通じてルート ブリッジに直接接続されているので、この障害を検出し、自身をルートに選定し、スイッチ C に対して自身がルートであることを表す BPDU の送信を開始します。スイッチ C がスイッチ B から下位 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。この時点で、BackboneFast により、スイッチ C のブロック ポートは、そのポートに設定されている最大エージング タイムの満了を待たずに、ただちにリスニング ステートに移行します。BackboneFast はさらに、スイッチ C のレイヤ 2 LAN 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 までのパスを提供します。この切り替えに要する時間は約 30 秒で、転送遅延時間の 2 倍にあたります（転送遅延時間がデフォルトの 15 秒に設定されている場合）。図 31-8 に、BackboneFast がリンク L1 で発生した障害に応じてどのようにトポロジーを再設定するかを示します。

図 31-8　間接リンク障害が発生したあとの BackboneFast の例

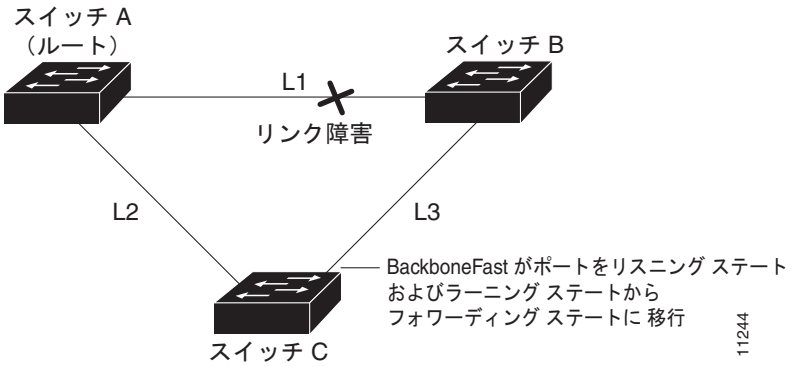
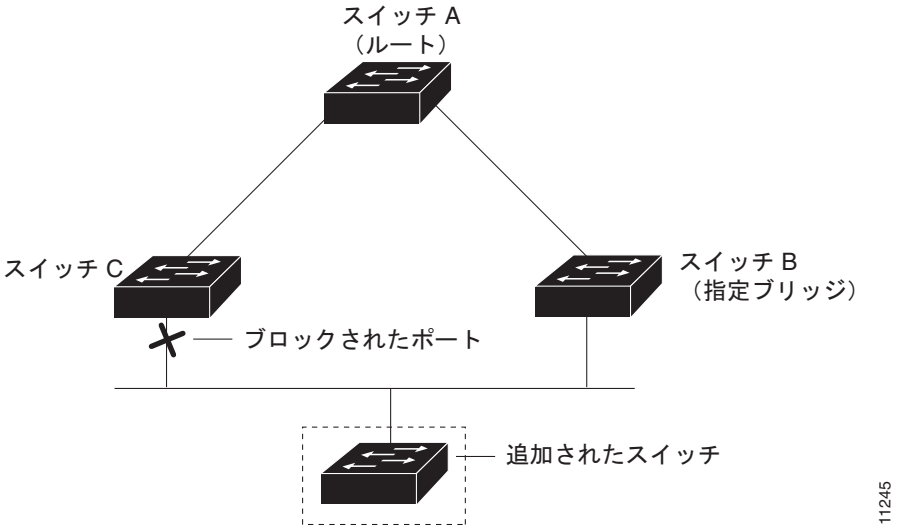


図 31-9 に示すメディア共有型トポロジーに新しいネットワーク デバイスが組み込まれた場合、BackboneFast は起動されません。これは、認識している指定ブリッジ（スイッチ B）から下位 BPDU が着信していないためです。新しいネットワーク デバイスは、自らがルート ブリッジであることを伝える下位 BPDU の送信を開始します。しかし、他のネットワーク デバイスはこれらの下位 BPDU を無視します。その結果、新しいネットワーク デバイスはスイッチ B がルート ブリッジであるスイッチ A への指定ブリッジであることを学習します。

図 31-9　メディア共有型トポロジーにおけるネットワーク デバイスの追加



BackboneFast のイネーブル化

（注）　BackboneFast が適切に動作するのは、ネットワーク内のすべてのネットワーク デバイス上でイネーブルになっている場合だけです。BackboneFast は、トークンリング VLAN ではサポートされません。この機能は、サードパーティ製のネットワーク デバイスと組み合わせて使用することができます。

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	`Router(config)# spanning-tree backbonefast`	BackboneFast をイネーブルにします。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

次に、BackboneFast をイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# spanning-tree backbonefast
Router(config)# end
```

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。

```
Router# show spanning-tree backbonefast
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
```

EtherChannel ガード

EtherChannel ガードについて

EtherChannel ガードは、正しく設定されていない EtherChannel を検出します（スイッチのインターフェイスが EtherChannel として設定されているが、他のデバイスのインターフェイスが EtherChannel として設定されていない場合、または他のデバイスのインターフェイスの一部が同じ EtherChannel に設定されていない場合など）。

他のデバイスの設定に誤りがあることが検出されると、EtherChannel ガードはスイッチのインターフェイスを errdisable ステートにします。

EtherChannel ガードのイネーブル化

EtherChannel 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	`Router(config)# spanning-tree etherchannel guard misconfig`	EtherChannel ガードをイネーブルにします。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

次に、EtherChannel ガードをイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# spanning-tree etherchannel guard misconfig
Router(config)# end
```

次に、設定を確認する例を示します。

```
Router# show spanning-tree summary | include EtherChannel
EtherChannel misconfiguration guard is enabled
```

errdisable ステートになっているインターフェイスを表示するには、**show interface status err-disable** コマンドを入力します。

誤っている設定が消去されると、errdisable ステートのインターフェイスは自動的に回復します。ポートを手動でサービス状態に戻すには、**shutdown** コマンドを入力してから、該当するインターフェイスに対して **no shutdown** コマンドを入力します。

ルート ガード

ルート ガードについて

STP ルート ガード機能を使用すると、ポートがルート ポートやブロックされたポートにならなくなります。ルート ガードに設定されたポートが上位 BPDU を受信すると、このポートはただちにルートとして一貫性のない（ブロックされた）ステートになります。

ルート ガードのイネーブル化

ルート 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	`Router(config)# interface {type slot/port} | {port-channel port_channel_number}`	設定するポートを選択します。
ステップ 2	`Router(config-if)# spanning-tree guard root`	ルート ガードをイネーブルにします。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。

ルートとして一貫性のないステートになっているポートを表示するには、**show spanning-tree inconsistentports** コマンドを入力します。

ループ ガード

ループ ガードについて

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されたループ 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されたポートを検出し、これらのポートがセグメント上の DP から BPDU を受信し続けるようにします。ループ ガードがイネーブルになっているルート ポートまたはブロックされたポートが DP からの BPDU の受信を停止した場合、このポートはポート上に物理リンク エラーがあると想定して、ループに一貫性のないブロッキング ステートに移行します。ポートが BPDU を受信すると、ただちにこのループに一貫性のない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することができます。ループ ガードをイネーブルにすると、すべてのアクティブ インスタンスまたはポートが属する 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した場合は、指定したポートに対して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、ループに一貫性のないすべての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、最初のリンクが単一方向になった場合、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 31-10 に、三角型のスイッチ設定におけるループ ガードを示します。

図 31-10　ループ ガードが設定された三角型のスイッチ設定

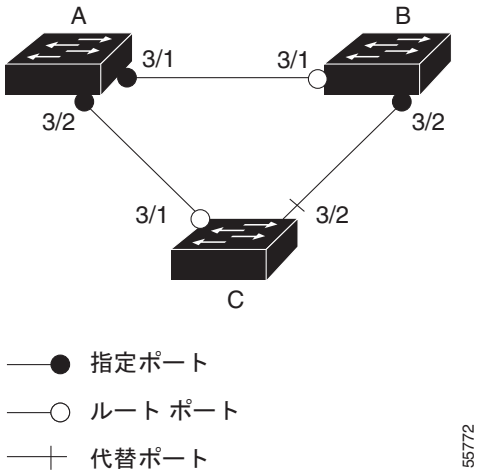


図 31-10 に、次の設定を示します。

- 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、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 ガードの使用時には、次の注意事項に従ってください。

- PortFast 対応ポートではループ ガードをイネーブルにできません。
- ルート ガードがイネーブルの場合は、ループ ガードをイネーブルにできません。

ループ ガードは、次のように他の機能と相互作用します。

- ループ ガードは UplinkFast または BackboneFast の機能には影響しません。
- 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、ポートを常にルート ポートとして指定された状態にします。ポートがルート ポートまたは代替ポートの場合だけ、ループ ガードは有効です。特定のポート上でループ ガードとルート ガードの両方を同時にイネーブルにすることはできません。
- ループ ガードはスパニングツリーで認識されているポートを使用します。ループ ガードは、ポート集約プロトコル（PAgP）が提供する論理ポートを利用できます。ただし、チャネルを形成するには、そのチャネルにグループ化するすべての物理ポートの設定に互換性がなければなりません。チャネルを形成するために、PAgP はすべての物理ポート上でルート ガードまたはループ ガードの設定を均一にします。

  ループ ガードに適用される注意事項は、次のとおりです。

  - スパニングツリーは、BPDU を送信するチャネル内で最初に動作するポートを常に選択します。このリンクが単一方向になった場合、チャネル内の他のリンクが適切に機能している場合でも、ループ ガードはチャネルをブロックします。
  - ループ ガードによってブロックされている一連のポートをグループ化して、チャネルを形成した場合、スパニングツリーはこれらのポートのステート情報をすべて失い、新しいチャネル ポートは指定された役割を使用してフォワーディング ステートに移行できます。

- チャネルがループ ガードによってブロックされている場合に、チャネルが切断されると、スパニングツリーはすべてのステート情報を失います。チャネルを形成する 1 つまたは複数のリンクが単一方向リンクである場合も、各物理ポートは指定されたロールを使用して、フォワーディング ステートに移行できます。

（注）　UniDirectional Link Detection（UDLD; 単一方向リンク検出）をイネーブルにして、リンク障害を特定することができます。UDLD が障害を検出するまでループが発生することがありますが、ループ ガードはこのループを検出できません。

- ディセーブル化されたスパニングツリー インスタンスまたは VLAN 上では、ループ ガードは無効です。

ループ ガードのイネーブル化

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	`Router(config)# spanning-tree loopguard default`	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	`Router(config)# end`	コンフィギュレーション モードを終了します。

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。

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# spanning-tree loopguard default
Router(config)# exit

Router# show spanning-tree interface gigabitethernet 4/4 detail
 Port 196 (GigabitEthernet4/4) 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
```

ポート上でループ 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	`Router(config)# interface {type slot/port} | {port-channel port_channel_number}`	設定するポートを選択します。
ステップ 2	`Router(config-if)# spanning-tree guard loop`	ループ ガードを設定します。
ステップ 3	`Router(config)# end`	コンフィギュレーション モードを終了します。

次に、ループ ガードをイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 4/4
Router(config-if)# spanning-tree guard loop
Router(config-if)# exit
```

次に、設定を確認する例を示します。

```
Router# show spanning-tree interface gigabitethernet 4/4 detail
 Port 196 (GigabitEthernet4/4) 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
```

PVST シミュレーション

PVST シミュレーションについて

MST は、Rapid PVST+ と相互運用し、ユーザ設定は不要です。PVST シミュレーション機能により、このシームレスな相互運用が可能になっています。

（注）　MST をイネーブルにすると、PVST シミュレーションがデフォルトでイネーブルになります。つまり、デフォルトでは、デバイス上のすべてのインターフェイスが MST および Rapid PVST+ 間で相互運用します。

MST と Rapid PVST+ 間の接続を制御して、Rapid PVST+ の実行がイネーブルに設定されたポートに MST 対応ポートを誤って接続するのを防止できます。Rapid PVST+ はデフォルトの STP モードなので、多数の Rapid PVST+ 接続が発生することがあります。

Rapid PVST+ シミュレーションのディセーブル化は、ポートごと、またはデバイス全体でグローバルに実行できます。Rapid PVST+ シミュレーションをディセーブルにした場合、MST 対応ポートは自身が Rapid PVST+ 対応ポートに接続されていることを検出すると、PVST ピアの一貫性がない（ブロッキング）ステートに移行します。このポートは、Shared Spanning Tree Protocol（SSTP）BPDU の受信を停止するまでは一貫性のないステートを維持し、受信停止後は通常の STP 移行プロセスを再開します。

すべての STP インスタンス用のすべてのルート ブリッジは、MST 領域または Rapid PVST+ 側のいずれかに配置されている必要があります。すべての STP インスタンスのルート ブリッジがどちらか一方の側に属していないと、ポートは PVST シミュレーション不整合ステートになります。

（注）　すべての STP インスタンス用ルート ブリッジは、MST 領域に配置することを推奨します。

PVST シミュレーションの設定

（注）　PVST シミュレーションはデフォルトでイネーブルになっているので、デバイス上のすべてのインターフェイスは MST および Rapid PVST+ 間で相互運用します。

MST をデフォルトの STP モードとして実行していないデバイスに誤って接続するのを避けるには、PVST シミュレーションをディセーブルにします。Rapid PVST+ シミュレーションをディセーブルにした場合、MST がイネーブルなポートが Rapid PVST+ がイネーブルなポートに接続されていることが検出されると、MST がイネーブルなポートは、ブロッキング ステートに移行します。このポートは、BPDU の受信が停止されるまで、一貫性のないステートのままになり、それから、ポートは、通常の STP 送信プロセスに戻ります。

PVST シミュレーションをグローバルにイネーブル化またはディセーブル化するには、次に示すように、**global** キーワードを使用してコマンドを入力します。

コマンド	目的
`Router(config)# spanning-tree mst simulate pvst global`	すべてのポートをイネーブルにして、Rapid PVST+ モードで動作している接続先デバイスと自動的に相互運用するようにします。デフォルトはイネーブルです。したがって、すべてのインターフェイスは、Rapid PVST+ および MST 間でシームレスに動作します。

ポートのグローバルな PVST シミュレーション設定を上書きするには、インターフェイス コマンド モードで次のようにコマンドを入力します。

	コマンド	目的
ステップ 1	`Router(config)# interface {type slot/port}`	設定するポートを選択します。
ステップ 2	`Router(config-if)# spanning-tree mst simulate pvst`	このインターフェイスをイネーブルにして、Rapid PVST+ モードで動作している接続先デバイスと自動的に相互運用するようにします。

次に、Rapid PVST+ を実行している接続先デバイスとの自動的な相互運用を回避する例を示します。

```
Router(config)# no spanning-tree mst simulate pvst global
```

次に、Rapid PVST+ を実行している接続先デバイスとポートが自動的に相互運用しないようにする例を示します。

```
Router(config)# interface gi3/13
Router(config-if)# spanning-tree mst simulate pvst disable
```

オプションの STP 機能の確認

- 「show spanning-tree コマンドの使用方法」（P.31-23）

show spanning-tree コマンドの使用方法

ここで説明する **show spanning-tree** コマンドを使用して、グローバル レベルとポート レベルの両方で、スパニングツリー ステータスと設定情報を表示できます。スパニングツリー ステータスと設定情報を表示するには、次のコマンドのいずれかを入力します。

コマンド	目的
`Router# show spanning-tree`	プロトコル タイプやポート タイプを含む、スパニングツリーに関する情報を表示します。
`Router# show spanning-tree summary`	スパニングツリー機能の設定および VLAN のスパニングツリー ステートの概要を表示します。
`Router# show spanning-tree summary totals`	スパニングツリー機能の設定の概要と VLAN ステート全体を表示します。
`Router# show spanning-tree interface {type slot/port} detail`	インターフェイスのスパニングツリー ステータスの詳細を表示します。
`Router# show spanning-tree interface {type slot/port} portfast edge`	すべてのインスタンスに対するスパニングツリー portfast エッジ インターフェイスの動作ステートを表示します。

show spanning-tree コマンドの例

次に、Bridge Assurance はイネーブルだが一貫性のないステートのスパニングツリー ステータスの例を示します。

```
Router# show spanning-tree
VLAN0010
  Spanning tree enabled protocol rstp
  Root ID     Priority    32778
              Address     0002.172c.f400
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32778  (priority 32768 sys-id-ext 10)
              Address     0002.172c.f400
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi3/14           Desg BKN*4         128.270  Network, P2p *BA_Inc
Router#
```

次の一貫性の欠如に関するメッセージを Type フィールドに追加できます。

- *BA_Inc：Bridge Assurance が一貫性のないステートであることを示します。
- *PVST_Peer_Inc：ポートがピア タイプに一貫性のないステートであることを示します。
- Dispute：競合する状態が検出されたことを示します。

次に、スパニングツリー設定の概要の例を示します。

```
Router# show spanning-tree summary

Switch is in rapid-pvst mode
Root bridge for: Bridge VLAN0025
EtherChannel misconfiguration guard is enabled
Extended system ID                  is enabled
PortFast Edge BPDU Guard Default    is disabled
Portfast Edge BPDU Filter Default   is disabled
Portfast Default                    is edge
Bridge Assurance                    is enabled
Loopguard                           is disabled
UplinkFast                          is disabled
BackboneFast                        is disabled
Pathcost method used is short
PVST Simulation Default             is enabled

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0025                  0        0         0        1          1
VLAN0030                  0        0         0        2          2
---------------------- -------- --------- -------- ---------- ----------
2 vlans                   0        0         0        3          3
```

Bridge Assurance フィールドで使用できるステートは次のとおりです。

- is enabled
- is disabled
- is enabled but not active in the PVST mode

次に、STP モードで PVST シミュレーションがディセーブルな場合のスパニングツリーの概要の例を示します。

```
Router# show spanning-tree summary

Switch is in mst mode (IEEE Standard)
Root bridge for: MST0
EtherChannel misconfig guard is enabled
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Pathcost method used         is long
PVST Simulation Default      is disabled

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
MST0                        2         0        0          0          2
---------------------- -------- --------- -------- ---------- ----------
1 mst                       2         0        0          0          2
```

PVST Simulation Default フィールドで使用できるステートは次のとおりです。

- is enabled
- is disabled
- is enabled but not active in rapid-PVST mode

次に、スパニングツリーの概要全体の例を示します。

```
Router# show spanning-tree summary totals
Root bridge for: Bridge VLAN0025
EtherChannel misconfiguration guard is enabled
Extended system ID                  is enabled
PortFast Edge BPDU Guard Default    is enabled
Portfast Edge BPDU Filter Default   is disabled
Portfast Default                    is edge
Bridge Assurance                    is enabled
Loopguard                           is disabled
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
Router#
```

次に、エッジ ポートのスパニングツリー設定詳細の例を示します。

```
Router# show spanning-tree interface gi3/13 detail
Port 269 (GigabitEthernet3/13) of VLAN0002 is forwarding
   Port path cost 4, Port priority 128, Port Identifier 128.269.
   Designated root has priority 32770, address 0002.172c.f400
   Designated bridge has priority 32770, address 0002.172c.f400
   Designated port id is 128.269, 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
   Loop guard is enabled by default on the port
   The port is in the portfast edge mode by default
   BPDU: sent 2183, received 0
```

次に、トランク ポートのスパニングツリー設定詳細の例を示します。

```
Router(config-if)# spanning-tree portfast edge trunk
%Warning:portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION

Router(config-if)# exit

Router# show spanning-tree interface gi3/13 detail
Port 269 (GigabitEthernet3/13) of VLAN0002 is forwarding
   Port path cost 4, Port priority 128, Port Identifier 128.269.
   Designated root has priority 32770, address 0002.172c.f400
   Designated bridge has priority 32770, address 0002.172c.f400
   Designated port id is 128.269, 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
   Loop guard is enabled by default on the port
   The port is in the portfast edge trunk mode
   BPDU: sent 2183, received 0
```

次に、競合する状態が検出された場合のエッジ ポートのスパニングツリー設定詳細の例を示します。

```
Router# show spanning-tree interface gi3/13 detail
Port 269 (GigabitEthernet3/13) of VLAN0002 is designated blocking (dispute)
   Port path cost 4, Port priority 128, Port Identifier 128.297.
   Designated root has priority 32769, address 0013.5f20.01c0
   Designated bridge has priority 32769, address 0013.5f20.01c0
```

```
   Designated port id is 128.297, 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 132, received 1
```

次に、すべてのインスタンスに対するスパニングツリー portfast エッジ インターフェイスの動作ステートの例を示します。

```
Router# show spanning-tree interface gi3/1 portfast edge
MST0              disabled
MST1              disabled
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

PART 7

IP スイッチング

IP ユニキャスト レイヤ 3 スイッチング

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。
- IP マルチキャスト レイヤ 3 スイッチングについては、第 43 章「IPv4 マルチキャスト レイヤ 3 機能」を参照してください。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

ハードウェア レイヤ 3 スイッチングの前提条件

なし。

ハードウェア レイヤ 3 スイッチングの制約事項

- IPX トラフィックは、ルート プロセッサ（RP）で高速スイッチングされます。
- ハードウェア レイヤ 3 スイッチングは、次の入力および出力カプセル化をサポートします。
  - イーサネット V2.0（ARPA）
  - 1 バイト制御を使用する 802.2 対応の 802.3（SAP1）
  - 802.2 対応の 802.3 および SNAP

レイヤ 3 スイッチングについて

ハードウェア レイヤ 3 スイッチング

ハードウェア レイヤ 3 スイッチングを使用すると、サブネット間における IP ユニキャスト トラフィックの転送を、RP ではなくポリシー フィーチャ カード（PFC）および Distributed Feature Card（DFC）で行うことができます。ハードウェア レイヤ 3 スイッチングは、RP 上のソフトウェアを使用せずに、PFC および DFC 上でワイヤ速度による転送機能を提供します。ハードウェア レイヤ 3 スイッチングの実行には、RP からの最低限のサポートが必要です。ハードウェア レイヤ 3 スイッチングが不可能なトラフィックは、RP がルーティングします。

ハードウェア レイヤ 3 スイッチングは、RP に設定されているルーティング プロトコルをサポートします。ハードウェア レイヤ 3 スイッチングは、RP に設定されているルーティング プロトコルに代わるものではありません。

各モジュールに IP ユニキャスト レイヤ 3 スイッチングをローカルで提供するために、ハードウェア レイヤ 3 スイッチングは、PFC および DFC 上で等しく稼働します。ハードウェア レイヤ 3 スイッチングでは、次の機能を提供します。

- Policy-based Routing（PBR; ポリシー ベース ルーティング）用のハードウェア アクセス コントロール リスト（ACL）スイッチング
- TCP 代行受信および再帰 ACL 転送の決定用のハードウェア フローベース スイッチング
- その他のすべての IP ユニキャスト トラフィック用のハードウェア Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）スイッチング

PFC 上のハードウェア レイヤ 3 スイッチングは、DFC を装備していないモジュールをサポートします。レイヤ 3 スイッチングが不可能なトラフィックは、RP が転送します。

トラフィックはアクセス リストおよび Quality of Service（QoS）によって処理されたあとで、ハードウェア レイヤ 3 スイッチングされます。

ハードウェア レイヤ 3 スイッチングは、入力ポート モジュール上でローカルに各パケットの転送先を決定し、出力ポートに各パケットの書き換え情報を送信します。パケットがスイッチから送信されるときに、出力ポート上で書き換えが行われます。

ハードウェア レイヤ 3 スイッチングにより、レイヤ 3 スイッチド トラフィックのフロー統計情報が生成されます。ハードウェア レイヤ 3 フロー統計情報は NetFlow に使用できます。（第 52 章「NetFlow ハードウェア サポート」を参照）。

レイヤ 3 スイッチド パケットの書き換え

特定のサブネット上の送信元から別のサブネット上の宛先へパケットをレイヤ 3 スイッチングするとき、スイッチは RP から学習した情報に基づいて、出力ポートでパケットの書き換えを行います。この書き換えにより、パケットは RP がルーティングしたように表示されます。

パケットの書き換えによって変更されるフィールドは、次の 5 つです。

- レイヤ 2（MAC）宛先アドレス
- レイヤ 2（MAC）送信元アドレス
- レイヤ 3 IP Time To Live（TTL）
- レイヤ 3 チェックサム
- レイヤ 2（MAC）チェックサム（別名フレーム チェックサムまたは FCS）

（注） パケットは、ネクスト ホップのサブネットに適したカプセル化を使用して書き換えられます。

送信元 A と宛先 B が異なるサブネットに属し、送信元 A が RP にパケットを送信して宛先 B へルーティングされる場合、スイッチはそのパケットが RP のレイヤ 2（MAC）アドレスに送信されたと認識します。

レイヤ 3 スイッチングを実行するため、スイッチはレイヤ 2 フレーム ヘッダーを書き換え、レイヤ 2 宛先アドレスを宛先 B のレイヤ 2 アドレスに変更し、レイヤ 2 送信元アドレスを RP のレイヤ 2 アドレスに変更します。レイヤ 3 アドレスは変更されません。

IP ユニキャストおよび IP マルチキャスト トラフィックの場合、スイッチはレイヤ 3 TTL 値を 1 だけ減らし、レイヤ 3 パケット チェックサムを再計算します。スイッチはレイヤ 2 フレーム チェックサムを再計算し、書き換えたパケットを宛先 B のサブネットに転送します（または、マルチキャスト パケットの場合、必要に応じて複製します）。

受信 IP ユニキャスト パケットは次のようにフォーマットされます（概念上）。

レイヤ 2 フレーム ヘッダー		**レイヤ 3 IP ヘッダー**				**データ**	**FCS**
宛先	送信元	宛先	送信元	TTL	チェックサム		
RP MAC	*Source A MAC*	*Destination B IP*	*Source A IP*	*n*	*calculation1*		

スイッチが IP ユニキャスト パケットの書き換えを行ったあとの形式は（概念的には）、次のとおりです。

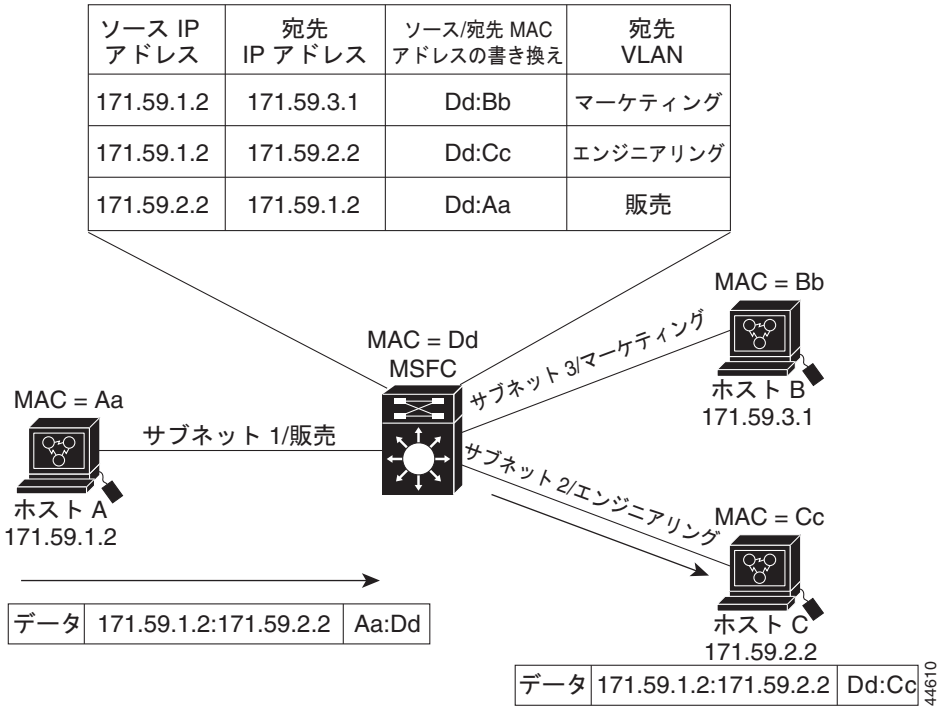
レイヤ 2 フレーム ヘッダー		**レイヤ 3 IP ヘッダー**				**データ**	**FCS**
宛先	送信元	宛先	送信元	TTL	チェックサム		
Destination B MAC	*RP MAC*	*Destination B IP*	*Source A IP*	*n-1*	*calculation2*		

ハードウェア レイヤ 3 スイッチングの例

図 32-1（P.32-4）に、単純なネットワーク トポロジーを示します。この例では、ホスト A は販売部門の VLAN（IP サブネット 171.59.1.0）、ホスト B はマーケティング部門の VLAN（IP サブネット 171.59.3.0）、ホスト C はエンジニアリング部門の VLAN（IP サブネット 171.59.2.0）にあります。

ホスト A がホスト C に対して HTTP ファイル転送を開始すると、ハードウェア レイヤ 3 スイッチングはローカル Forwarding Information Base（FIB; 転送情報ベース）および隣接テーブルの情報を使用して、ホスト A からホスト C にパケットを転送します。

図 32-1　　ハードウェア レイヤ 3 スイッチングのトポロジー例



ハードウェア レイヤ 3 スイッチングのデフォルト設定

機能	デフォルト値
ハードウェア レイヤ 3 スイッチングのイネーブル ステート	イネーブル（ディセーブルにはできません）
RP 上の Cisco IOS CEF イネーブル ステート	イネーブル（ディセーブルにはできません）
RP 上の Cisco IOS dCEF イネーブル ステート	イネーブル（ディセーブルにはできません）

ハードウェア レイヤ 3 スイッチングの設定方法

（注） RP 上のユニキャスト ルーティングの設定手順については、第 34 章「レイヤ 3 インターフェイス」を参照してください。

ハードウェア レイヤ 3 スイッチングは、永続的にイネーブルになります。設定は必要ありません。

レイヤ 3 スイッチド 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
Router# **show interface** {{*type slot/port*} | {**port-channel** *number*}} **| begin L3**	レイヤ 3 スイッチド トラフィックの要約を表示します。

次に、ギガビット イーサネット ポート 3/3 上のハードウェア レイヤ 3 スイッチド トラフィックに関する情報を表示する例を示します。

```
Router# show interface gigabitethernet 3/3 | 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 runs, 0 giants, 0 throttles
<...output truncated...>
Router#
```

（注） レイヤ 3 スイッチング パケット カウントは、約 5 秒間隔で更新されます。

Cisco IOS CEF および dCEF は、永続的にイネーブルになります。ハードウェア レイヤ 3 スイッチングをサポートするための設定作業は不要です。

PFC を（存在する場合は DFC も）利用して、ハードウェア レイヤ 3 スイッチングは、フローごとのロードバランスを IP の送信元および宛先のアドレスに基づいて使用します。フローごとのロードバランスは、パケットごとのロードバランスでは必要となるパケットの再配列を行いません。どのようなフローに対しても、PFC や DFC を装備したすべてのスイッチが、まったく同じロードバランスの判断を行うので、結果としてロードバランスがランダムにならない場合があります。

RP 上の Cisco IOS CEF **ip load-sharing per-packet**、**ip cef accounting per-prefix**、および **ip cef accounting non-recursive** コマンドは、RP 上のソフトウェアで CEF スイッチングされるトラフィックだけに適用されます。これらのコマンドは、PFC 上または DFC を搭載したスイッチング モジュール上でハードウェア レイヤ 3 スイッチングされるトラフィックには影響しません。

ハードウェア レイヤ 3 スイッチング統計情報の表示

ハードウェア レイヤ 3 スイッチング統計情報は、VLAN 単位で収集されます。

ハードウェア レイヤ 3 スイッチ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
Router# **show interfaces** {{*type slot/port*} | {**port-channel** *number*}}	ハードウェア レイヤ 3 スイッチング統計情報を表示します。

次に、ハードウェア レイヤ 3 スイッチング統計情報を表示する例を示します。

```
Router# show interfaces gigabitethernet 9/5 | include Switched
L2 Switched: ucast: 8199 pkt, 1362060 bytes - mcast: 6980 pkt, 371952 bytes
L3 in Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes mcast
L3 out Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes
```

隣接テーブルの情報を表示するには、次の作業を行います。

コマンド	目的
Router# **show adjacency** [{{*type slot/port*} | {**port-channel** *number*}} | **detail** | **internal** | **summary**]	隣接テーブルの情報を表示します。オプションの **detail** キーワードを指定すると、レイヤ 2 情報を含む詳細な隣接情報が表示されます。

次に、約 60 秒ごとに更新される隣接統計情報を表示する例を示します。

```
Router# show adjacency gigabitethernet 9/5 detail
Protocol Interface                 Address
IP       GigabitEthernet9/5        172.20.53.206(11)
                                   504 packets, 6110 bytes
                                   00605C865B82
                                   000164F83FA50800
                                   ARP        03:49:31
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

PART 8

IP ルーティング プロトコル

CHAPTER 33

Policy-Based Routing（PBR）

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

PBR の前提条件

なし。

PBR の制約事項

PFC および DFC では、次がハードウェアでサポートされます。

- 次の IPv4 PBR コマンド：
  - **match ip address**

  - **match length**
  - **set ip next-hop**（2,000 インスタンス）
  - **set ip default next-hop**
  - **set interface null0**
  - **set default interface null0**
  - **set ip vrf**
  - **set ip default vrf**
- RP のアドレスが PBR ACL の範囲内にある場合、RP にアドレス指定されたトラフィックは RP に転送されずに、ハードウェアでポリシー ルーティングされます。RP にアドレス指定されたトラフィックのポリシー ルーティングを防止するには、RP にアドレス指定されたトラフィックを拒否するように PBR ACL を設定します。
- ローカル PBR。
- ロード バランシングによる IPv4 PBR 再帰ネクスト ホップ。
- IPv6 PBR はソフトウェアでサポートされます。
- IPv6 PBR 再帰ネクスト ホップはサポートされません。

PBR について

PBR の概要

PBR は、ルーティング プロトコルの代替手段であり、ユニキャスト トラフィック フローのポリシーを設定できます。これによって、ルーティングに対して、ルーティング プロトコルよりも強化した制御を実施し、インターフェイス レベルのトラフィック分類設定の必要を避けられます。PBR は、ルーティング プロトコルが使用するのとは異なるパスにユニキャスト トラフィックをルーティングできます。PBR は次を提供します。

- 同等アクセス
- プロトコル別のルーティング
- 送信元別のルーティング
- 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

PBR ルート マップは、次のように設定できます。

- 特定のエンド システムのアイデンティティ、アプリケーション プロトコル、またはパケットのサイズ、あるいはこれらの値の組み合わせに基づいて、パスを許可または拒否する。
- 拡張アクセス リスト基準に基づいてトラフィックを分類する。
- IP precedence ビット設定する。
- 特定のパスにパケットをルーティングする。

PBR は、PBR 対応インターフェイスで受信されるすべての入力ユニキャスト トラフィックにルート マップを適用します。PBR は、出力トラフィックまたはマルチキャスト トラフィックに適用できません。

入力ユニキャスト トラフィックがルート マップ ステートメントと一致しない場合、ルート マップは、設定済みのすべての set 句を適用します。ルーティング プロトコルは、ルート マップの deny ステートメントと一致するトラフィックおよびルート マップの permit ステートメントと一致しないトラフィックを転送します。

IPv4 トラフィックの PBR 再帰ネクスト ホップ

PBR 再帰ネクスト ホップ機能は、PBR ルート マップの再帰ネクスト ホップ アドレスの設定をイネーブルにします。再帰ネクストホップ アドレスはルーティング テーブルにインストールされ、直接接続されていないサブネットにすることができます。再帰ネクストホップ アドレスを使用できない場合、トラフィックはデフォルト ルートを使ってルーティングされます。

PBR のデフォルト設定

なし。

PBR の設定方法

- PBR の設定
- ローカル PBR の設定
- PBR 再帰ネクスト ホップの設定

（注）　ポリシー ベース ルーティングを使用した複数の VRF 選択（PBR VRF）については、次のマニュアルを参照してください。

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_mltvrf_slct_pbr.html

PBR の設定

PBR をインターフェイスに設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	Router(config)# **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]	パケットの出力先を制御するためのルート 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	Router(config-route-map)# **match length** *min max* Router(config-route-map)# **match ip address** {*access-list-number* | *name*} [*...access-list-number* | *name*]	一致基準を指定します。 多くのルート マップ マッチング オプションがありますが、ここでは、長さおよび/または IP アドレスだけを指定できます。 • **length** はレベル 3 パケット長と一致します。 • **ip address** は、1 つまたは複数の標準または拡張アクセス リストで許可される送信元または送信先 IP アドレスを照合します。 **match** コマンドを指定しない場合、ルート マップはすべてのパケットに適用されます。
ステップ 3	Router(config-route-map)# **set ip precedence** [*number* | *name*] Router(config-route-map)# **set ip df** Router(config-route-map)# **set ip vrf** *vrf_name* Router(config-route-map)# **set ip next-hop** *ip-address* [*... ip-address*] Router(config-route-map)# **set ip next-hop recursive** *ip-address* [*... ip-address*] Router(config-route-map)# **set interface** *interface-type interface-number* [*... type number*] Router(config-route-map)# **set ip default next-hop** *ip-address* [*... ip-address*] Router(config-route-map)# **set default interface** *interface-type interface-number* [*... type ...number*]	基準に一致したパケットで実行されるアクション（1 つまたは複数）を指定します。次のうちの任意の項目またはすべてを指定できます。 • **precedence**：IP ヘッダーに precedence 値を設定します。precedence の番号または名前のいずれかを指定できます。 • **df**：IP ヘッダー内に、「Don't Fragment」（DF）ビットを設定します。 • **vrf**：VPN ルーティング/転送（VRF）インスタンスを設定します。 • **next-hop**：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。 • **next-hop recursive**：ホップが隣接していないルータへの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。 • **interface**：パケットの出力インターフェイスを設定します。 • **default next-hop**：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。 • **default interface**：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。

	コマンド	目的
ステップ 4	`Router(config-route-map)# interface interface-type interface-number`	インターフェイスを指定し、ルータでインターフェイス 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	`Router(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はただ 1 つのルート マップ タグしか指定できませんが、シーケンス番号を持つ複数のルート マップ項目を作成できます。項目は、最初の一致が現れるまで、シーケンス番号の順に評価されます。一致する項目がない場合、パケットは通常どおりに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 ルータは、ネクスト ホップと使用可能なインターフェイスを検出したら、パケットをルーティングします。

ローカル PBR の設定

スイッチで発信されるすべてのトラフィックに PBR を設定する手順は、次のとおりです。

コマンド	目的
`Router(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。

（注）
- ローカル PBR トラフィックは RP のソフトウェアで処理されます。
- ローカル PBR で使用するルート マップを表示するには、**show ip local policy** コマンドを使用します。

PBR 再帰ネクスト ホップの設定

再帰ネクストホップ IP アドレスの設定

（注）　PBR がサポートする再帰ネクストホップ IP アドレスは、ルートマップ エントリごとに 1 つのみです。

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** **例：** `Router# 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	**access-list permit** *source* **例：** `Router(config)# access-list 101 permit 10.60.0.0 0.0.255.255`	アクセス リストを設定します。設定例では、10.60.0.0.0.0.255.255 サブネット内に分類されるすべての発信元 IP アドレスが許可されます。
ステップ 4	**route-map** *map-tag* **例：** `Router(config)# route-map abccomp`	ポリシー ルーティングをイネーブルにし、ルートマップ コンフィギュレーション モードを開始します。
ステップ 5	**set ip next-hop** *ip-address* **例：** `Router(config-route-map)# set ip next-hop 10.10.1.1`	ネクストホップ ルータ IP アドレスを設定します。 **（注）** この IP アドレスは、ネクストホップ再帰ルータ設定とは別に設定します。
ステップ 6	**set ip next-hop** {*ip-address* [*...ip-address*] | **recursive** ip-address} **例：** `Router(config-route-map)# set ip next-hop recursive 10.20.3.3`	再帰ネクストホップ IP アドレスを設定します。 **（注）** 中継 IP アドレスが宛先への短いルートである場合、この設定によって、パケットが再帰 IP アドレスを使ってルーティングされるとは限りません。
ステップ 7	**match ip address** *access-list-number* **例：** `Router(config-route-map)# match ip address 101`	一致するアクセス リストを設定します。
ステップ 8	**end** **例：** `Router(config-route-map)# end`	現在のルート マップ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

再帰ネクストホップ設定の確認

再帰ネクストホップ設定を確認するには、次の手順を実行します。

ステップ 1　show running-config | begin abccomp

このコマンドを次の例のように使用し、ネクストホップの IP アドレスおよび再帰ネクストホップ IP アドレスを確認します。

```
Router# show running-config | begin abccomp

route-map abccomp permit 10
 match ip address 101 ! Defines the match criteria for an access list.
 set ip next-hop recursive 10.3.3.3 ! If the match criteria are met, the recursive IP
 address is set.
 set ip next-hop 10.1.1.1 10.2.2.2 10.4.4.4
```

ステップ 2　**show route-map** *map-name*

このコマンドを次の例のように使用し、ルート マップを表示します。

```
Router# show route-map abccomp

route-map abccomp, permit, sequence 10
 Match clauses:
  ip address (access-lists): 101
 Set clauses:
  ip next-hop recursive 10.3.3.3
  ip next-hop 10.1.1.1 10.2.2.2 10.4.4.4
 Policy routing matches: 0 packets, 0 bytes
```

PBR の設定例

（注）　次に、**access-list** コマンド（ACL）の使用が含まれる例を示します。ACL の割り込みレベルでロギングがサポートされていないため、log キーワードは、ポリシー ベース ルーティング（PBR）でこのコマンドと共に使用してはなりません。

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 209.165.200.225 から非同期インターフェイス 1 に着信したパケットは、209.165.200.228 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 209.165.200.226 から着信したパケットは、209.165.200.229 にあるルータへ送信されます。宛先についての明示的なルートがルータにない他のすべてのパケットは破棄されます。

```
access-list 1 permit 209.165.200.225
access-list 2 permit 209.165.200.226
!
interface async 1
 ip policy route-map equal-access
!
route-map equal-access permit 10
 match ip address 1
 set ip default next-hop 209.165.200.228
route-map equal-access permit 20
 match ip address 2
 set ip default next-hop 209.165.200.229
```

```
route-map equal-access permit 30
 set default interface null0
```

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）へルーティングし、IP ヘッダーに Precedence ビットを設定する例を示します。送信元 209.165.200.225 から着信したパケットはプライオリティに Precedence ビットを設定されて 209.165.200.227 にあるネクスト ホップに送信され、送信元 209.165.200.226 から着信したパケットはクリティカルに Precedence ビットを設定されて 209.165.200.228 にあるネクスト ホップへ送信されます。

```
access-list 1 permit 209.165.200.225
access-list 2 permit 209.165.200.226
!
interface ethernet 1
 ip policy route-map Texas
!
route-map Texas permit 10
 match ip address 1
 set ip precedence priority
 set ip next-hop 209.165.200.227
!
route-map Texas permit 20
 match ip address 2
 set ip precedence critical
 set ip next-hop 209.165.200.228
```

再帰ネクストホップ IP アドレス：例

次に、IP アドレス 10.3.3.3 を再帰ネクストホップ ルータとして設定する例を示します。

```
route-map abccomp
 set ip next-hop 10.1.1.1
 set ip next-hop 10.2.2.2
 set ip next-hop recursive 10.3.3.3
 set ip next-hop 10.4.4.4
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CHAPTER 34

レイヤ 3 インターフェイス

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

レイヤ 3 インターフェイスの制約事項

レイヤ 3 インターフェイスの設定時には、次の注意事項および制約事項に従ってください。

- 設定するレイヤ 3 VLAN インターフェイスは 2,000 個までにすることを推奨します。
- レイヤ 3 VLAN インターフェイスでは **ip unnumbered** コマンドがサポートされます。
- VLAN インターフェイスをサポートするには、VLAN を作成および設定し、レイヤ 2 LAN ポートに VLAN メンバーシップを割り当てます。詳細については、第 25 章「仮想ローカル エリア ネットワーク（VLAN）」および第 24 章「VLAN トランキング プロトコル（VTP）」を参照してください。
- ルーティングされないプロトコルのブリッジングを行うには、VLAN インターフェイス上でブリッジ グループを使用します。これはフォールバック ブリッジングと呼ばれることもあります。VLAN インターフェイスのブリッジ グループは、ルート プロセッサ（RP）のソフトウェアでサポートされます。

- Cisco IOS Release 15.1SY では、ブリッジ グループの IEEE ブリッジング プロトコルはサポートされません。VLAN ブリッジまたは Digital Equipment Corporation（DEC）スパニングツリー プロトコルを使用してブリッジ グループを設定します。
- PFC は LAN ポート レイヤ 3 サブインターフェイスで次の機能をサポートします。
  - MPLS VPN を含む、IPv4 ユニキャスト転送
  - MPLS VPN を含む、IPv4 マルチキャスト転送
  - 6PE
  - EoMPLS
  - IPv4 の番号付けなし
  - MIBS および **show vlans** コマンドによる、サブインターフェイスのカウンタ
  - iBGP および eBGP
  - OSPF
  - EIGRP
  - RIPv1/v2
  - RIPv2
  - ISIS
  - スタティック ルーティング
  - 単方向リンク ルーティング（UDLR）
  - IGMPv1、IGMPv2、IGMPv3
  - PIMv1、PIMv2
  - SSM IGMPv3lite および URD
  - IGMP Join
  - IGMP スタティック グループ
  - Multicast Routing Monitor（MRM）
  - Multicast Source Discovery Protocol（MSDP）
  - SSM
  - IPv4 ping
  - IPv6 ping
- VLAN ID が IEEE 802.1Q ネイティブ VLAN の ID の場合、**native** キーワードを必ず使用してください。**native** キーワードを使用せずに、IEEE 802.1Q トランクのネイティブ VLAN でカプセル化を設定しないでください。
- レイヤ 2 VLAN およびレイヤ 3 VLAN インターフェイスに使用される VLAN の ID は、レイヤ 3 サブ インターフェイスで設定されている VLAN ID とは異なります。レイヤ 2 VLAN またはレイヤ 3 VLAN インターフェイスとレイヤ 3 サブ インターフェイスで同じ VLAN ID を設定できます。
- VTP トランスペアレント モードでは、任意の標準範囲または拡張範囲の VLAN ID を使用して、サブインターフェイスを設定できます。VLAN ID 1 ～ 1005 は、VTP ドメインでグローバルであり、VTP ドメイン内の他のネットワーク デバイス上で定義することができるため、VTP クライア

ント / サーバ モードでは、拡張範囲 VLAN だけをサブインターフェイスとともに使用することができます。VTP クライアント / サーバ モードでは、標準範囲 VLAN がサブインターフェイスから除外されます。

（注）　サブインターフェイス上で標準範囲 VLAN を設定する場合、VTP モードをトランスペアレントから変更できません。

レイヤ 3 インターフェイスのサブ インターフェイスの設定方法

サブ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	`Router> enable`	特権 EXEC モードを開始します。
ステップ 2	`Router# 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	`Router(config)# interface {{type slot/port.subinterface} | {port-channel port_channel_number.subinterface}}`	インターフェイスを選択して、サブインターフェイス コンフィギュレーション モードを開始します。
ステップ 4	`Router(config-subif)# encapsulation dot1q vlan_ID [native]`	サブインターフェイスの 802.1Q カプセル化を設定します。
ステップ 5	`Router(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。

ヒント　Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CHAPTER 35

単一方向イーサネット（UDE）および単一方向リンク ルーティング（UDLR）

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。
- Cisco IOS Release 15.1SY は、WS-X6704-10GE 4 ポート 10 ギガビット イーサネット スイッチング モジュール上でのみ単一方向イーサネット（UDE）および単一方向リンク ルーティング（UDLR）をサポートします。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

UDE および UDLR の前提条件

なし。

UDE および UDLR の制約事項

UDE の制約事項

- STP では、単一方向リンクを含むトポロジーにおいてレイヤ 2 ループを防止できません。
- 送信専用ポートは、BPDU を受信しないので、STP フォワーディング ステートに常に移行します。
- 受信専用ポートは BPDU を送信できません。
- 単一方向ポートでは、次のようにリンクの反対側の終端にあるポートとのネゴシエーションが必要になる機能またはプロトコルがサポートされません。
  - 速度およびデュプレックス モードの自動ネゴシエーション
  - リンク ネゴシエーション
  - IEEE 802.3z フロー制御
  - ダイナミック トランキング プロトコル（DTP）

  レイヤ 2 プロトコルによって一般的に制御されるパラメータは、手動で設定する必要があります。
- VLAN トランキング プロトコル（VTP）サーバが VTP ドメインのすべてのスイッチに VTP フレームを送信できる場合、単一方向リンクを含むトポロジーでは、VTP だけがサポートされます。
- VTP プルーニングは情報の双方向の交換によって異なるので、送信専用ポートがあるスイッチでは VTP プルーニングをディセーブルにしてください。
- 単一方向 EtherChannel では PAgP または LACP をサポートできません。単一方向 EtherChannel を作成するには、EtherChannel「オン」モードを設定する必要があります。
- EtherChannel の物理ポートでソフトウェアベース UDE を設定できます。ポートチャネル インターフェイスなどの物理的でないインターフェイスでは、ソフトウェアベース UDE を設定できません。
- ハードウェアベース UDE をポートで実装するか、ソフトウェアベース UDE をポートで設定する場合、UDLD はそのポートで自動的にディセーブルになります。
- CDP は、送信専用ポートから CDP フレームを送信し、受信専用ポートから CDP フレームを受信します。つまり、単一方向リンクの送信専用側にあるスイッチは、CDP 情報を受信しません。
- SPAN は、単一方向ポートの設定を送信側や宛先に限定しません。
  - 送信専用ポートは、SPAN 宛先にすることができます。
  - 受信専用ポートは、SPAN 送信元にすることができます。
- 単一方向ポートでは、IEEE 802.1X ポートベース認証がサポートされません。
- IGMP スヌーピングでは、スイッチおよびマルチキャスト トラフィックを受信するホストの間に単一方向リンクがあるトポロジがサポートされません。
- スイッチの IGMP スヌーピングとマルチキャスト ルータの間で単一方向リンクによる通信をサポートするには、UDLR を UDE とともに設定します。
- 単一方向リンクでは ARP がサポートされません。

UDLR バックチャネル トンネルの制約事項

- PFC では、UDLR バックチャネル トンネルがハードウェアでサポートされません。UDLR バックチャネル トンネルはソフトウェアでサポートされます。
- 単一方向リンクごとに、UDLR バックチャネル トンネルを設定してください。
- UDE 送信専用インターフェイスでは、UDLR バックチャネル トンネル インターフェイスを受信に設定してください。
- UDE 受信専用インターフェイスでは、UDLR バックチャネル トンネル インターフェイスを送信に設定してください。
- UDLR バックチャネル トンネル インターフェイスでは、IPv4 アドレスを設定する必要があります。
- UDLR バックチャネル トンネル インターフェイスでは、送信元および宛先の IPv4 アドレスを設定する必要があります。
- UDLR バックチャネル トンネルのデフォルト モードは GRE です。
- UDLR バックチャネル トンネルでは、IPv6 または MPLS がサポートされません。

UDE および UDLR について

UDE および UDLR の概要

単一方向リンクが双方向リンクをエミュレートする場合に限り、ルーティング プロトコルは同一インターフェイスにおけるトラフィックを送受信するはずなので、ルーティング プロトコルでは単一方向リンクがサポートされます。

単一方向リンクには有利な点があります。ほとんど確認応答されていない単一方向の大量のトラフィック（ビデオ ブロードキャスト ストリームなど）を大容量全二重双方向リンクで送信する場合は、送信元からレシーバへのリンク、および同様に大容量な逆方向リンク（レシーバから送信元への少ない確認応答を搬送する「バック チャネル」と呼ばれる）の両方を使用するからです。

UDE および UDLR では、大量トラフィック用の大容量単一方向リンクの使用が、バック チャネル用の同様に大容量のリンクを消費せずにサポートされます。UDE では、大容量単一方向リンクが提供されます。UDLR では、通常の容量のリンクで設定されるトンネルでバック チャネルが提供されます。また、トランスペアレントにバック チャネルと大容量単一方向リンクと同じインターフェイス上にあるかのようにして双方向リンクをエミュレートします。

UDE について

UDE の概要

ハードウェアまたはソフトウェアで UDE を実装できます。ハードウェアベース UDE およびソフトウェアベース UDE の両方で、双方向トラフィックが必要とする 2 本のファイバではなく、1 本のファイバだけが使用されます。

サポートされる単一方向トランシーバ（WDM-XENPAK-REC）が受信専用 UDE を提供します。ソフトウェアベース UDE は、送信専用または受信専用のどちらかに設定できます。ハードウェアベース UDE を実装するポートで、ソフトウェアベース UDE を設定する必要はありません。

ハードウェアベース UDE

単一方向トランシーバを使用すると、単一方向リンクを構築できます。単一方向トランシーバは、双方向トランシーバより安価です。サポートされる単一方向トランシーバは WDM-XENPAK-REC です。

ソフトウェアベース UDE

トラフィックを単一方向で送信するか受信するように、双方向トランシーバに装備されているポートを設定し、単一方向リンクを作成できます。適切な単一方向トランシーバを使用できない場合は、ソフトウェアベース UDE を使用できます。たとえば、サポートされる送信専用トランシーバを使用しない場合は、ソフトウェアベース UDE で送信専用リンクを設定する必要があります。

UDLR について

UDLR では、単一方向大容量リンクのバック チャネルとしての単一方向トンネルが提供され、ユニキャスト トラフィックおよびマルチキャスト トラフィック用に 1 つの双方向リンクがトランスペアレントにエミュレートされます。

UDLR は、受信専用インターフェイスで送信する必要があるパケットを代行受信し、UDLR バックチャネル トンネルで送信します。ルータが UDLR バックチャネル トンネルでこのようなパケットを受信すると、パケットは、UDLR によって、送信専用インターフェイスで受信したかのような形になります。

UDLR バックチャネル トンネルでは、次の IPv4 機能がサポートされます。

- アドレス解決プロトコル（ARP）
- Next Hop Resolution Protocol（NHRP）
- すべての IPv4 トラフィックの双方向リンクのエミュレーション（ブロードキャストおよびマルチキャストの制御トラフィックだけではない）
- 受信専用トンネルにおける IPv4 GRE マルチポイント

（注）　UDLR バックチャネル トンネルでは、IPv6 または MPLS がサポートされません。

UDE および UDLR のデフォルト設定

なし。

UDE および UDLR の設定方法

（注）　次の説明は、UDLR をサポートするリリースで公開されています。ネイバー ISIS ルータは、UDLR トポロジで認識されません （CSCee56596）。

UDE の設定

ハードウェアベース UDE の設定

単一方向トランシーバを設置し、ハードウェアベース UDE を実装してください。ハードウェアベース UDE には、ソフトウェア設定手順は必要ありません。

ポートのハードウェアベース UDE を確認するには、次の作業を行います。

コマンド	目的
Router# **show interfaces** [{**gigabitethernet** | **tengigabitethernet**} *slot/interface*}] **status**	設定を確認します。

次に、ギガビット イーサネット ポート 1/1 の設定を確認する例を示します。

```
Router# show interfaces gigabitethernet 1/1 status

Port     Name               Status       Vlan       Duplex  Speed Type
Gi1/1                       notconnect   1            full   1000 WDM-RXONLY
```

ソフトウェアベース UDE の設定

ポートのソフトウェアベース UDE 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)# **interface** {{**gigabitethernet** | **tengigabitethernet**} *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	Router(config-if)# **unidirectional** {**send-only** | **receive-only**}	ソフトウェアベース UDE を設定します。
ステップ 3	Router(config-if)# **end**	コンフィギュレーション モードを終了します。

次に、10 ギガビット イーサネット ポート 1/1 を UDE 送信専用ポートとして設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface tengigabitethernet 1/1
Router(config-if)# unidirectional send-only
Router(config-if)# end
```

```
Warning!

Enable 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 l3 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、10 ギガビット イーサネット ポート 1/2 を UDE 受信専用ポートとして設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface tengigabitethernet 1/2
Router(config-if)# unidirectional receive-only
Router(config-if)# end

Warning!

Enable 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 l3 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。

```
Router> show interface tengigabitethernet 1/1 unidirectional
  Unidirectional configuration mode: send only
  CDP neighbour unidirectional configuration mode: receive only
```

次に、10 ギガビット イーサネット インターフェイス 1/1 で UDE をディセーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface tengigabitethernet 1/1
Router(config-if)# no unidirectional
Router(config-if)# end
```

次の例は、単一方向イーサネットをサポートしないポートで **show interface** コマンドを入力した結果を示しています。

```
Router# show interface gigabitethernet 6/1 unidirectional
Unidirectional Ethernet is not supported on GigabitEthernet6/1
```

UDLR の設定

- 「UDE 送信専用ポートの受信専用トンネル インターフェイスの設定」（P.35-7）
- 「UDE 受信専用ポートの送信専用トンネル インターフェイスの設定」（P.35-7）

UDE 送信専用ポートの受信専用トンネル インターフェイスの設定

UDE 送信専用ポートに受信専用トンネル 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	`Router(config)# interface tunnel number`	トンネル インターフェイスを選択します。
ステップ 2	`Router(config-if)# tunnel udlr receive-only ude_send_only_port`	トンネル受信専用インターフェイスを UDE 送信専用ポートと関連付けます。
ステップ 3	`Router(config-if)# ip address ipv4_address`	トンネル IPv4 アドレスを設定します。
ステップ 4	`Router(config-if)# tunnel source {ipv4_address | type number}`	トンネル送信元を設定します。
ステップ 5	`Router(config-if)# tunnel destination {hostname | ipv4_address}`	トンネル宛先を設定します。

UDE 受信専用ポートの送信専用トンネル インターフェイスの設定

UDE 受信専用ポートに送信専用トンネル 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	`Router(config)# interface tunnel number`	トンネル インターフェイスを選択します。
ステップ 2	`Router(config-if)# tunnel udlr send-only ude_receive_only_port`	トンネル送信専用インターフェイスを UDE 受信専用ポートと関連付けます。
ステップ 3	`Router(config-if)# ip address ipv4_address`	トンネル IPv4 アドレスを設定します。
ステップ 4	`Router(config-if)# tunnel source {ipv4_address | type number}`	トンネル送信元を設定します。
ステップ 5	`Router(config-if)# tunnel destination {hostname | ipv4_address}`	トンネル宛先を設定します。
ステップ 6	`Router(config-if)# tunnel udlr address-resolution`	ARP および NHRP をイネーブルにします。

次の UDE および UDLR の設定例は、次のようになっています。

- ルータ A の場合：
  - Open Shortest Path First（OSPF）および PIM が設定されています。
  - 10 ギガビット イーサネット ポート 1/1 が送信専用 UDE ポートになります。
  - UDLR バック チャネル トンネルが受信専用として設定され、10 ギガビット イーサネット ポート 1/1 に関連付けられます。
- ルータ B の場合：
  - OSPF および PIM が設定されています。
  - 10 ギガビット イーサネット ポート 1/2 が受信専用 UDE ポートになります。
  - UDLR バック チャネル トンネルが送信専用として設定され、10 ギガビット イーサネット ポート 1/2 に関連付けられます。
  - ARP および NHRP がイネーブルです。

ルータ A の設定

```
ip multicast-routing
```

```
!
! tengigabitethernet 1/1 is send-only
!
interface tengigabitethernet 1/1
 unidirectional send-only
 ip address 10.1.0.1 255.255.0.0
 ip pim sparse-dense-mode
!
! Configure tunnel as receive-only UDLR tunnel.
!
interface tunnel 0
 tunnel source 11.0.0.1
 tunnel destination 11.0.0.2
 tunnel udlr receive-only tengigabitethernet 1/1
!
! Configure OSPF.
!
router ospf <pid>
 network 10.0.0.0 0.255.255.255 area 0
```

ルータ B の設定

```
ip multicast-routing
!
! tengigabitethernet 1/2 is receive-only
!
interface tengigabitethernet 1/2
 unidirectional receive-only
 ip address 10.1.0.2 255.255.0.0
 ip pim sparse-dense-mode
!
! Configure tunnel as send-only UDLR tunnel.
!
interface tunnel 0
 tunnel source 11.0.0.2
 tunnel destination 11.0.0.1
 tunnel udlr send-only tengigabitethernet 1/2
 tunnel udlr address-resolution
!
! Configure OSPF.
!
router ospf <pid>
 network 10.0.0.0 0.255.255.255 area 0
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

PART 9

MPLS 機能

CHAPTER 36

マルチプロトコル ラベル スイッチング（MPLS）

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

MPLS の前提条件

なし。

MPLS の制約事項

- PFC および DFC は、最大 16 個の負荷分散パスをサポートします（他のプラットフォーム用の Cisco IOS リリースでは、8 個の負荷分散パスのみをサポート）。
- MTU サイズ チェックはハードウェアでサポートされます。
- IP として入り、MPLS として出るトラフィックなど、フラグメンテーションはソフトウェアでサポートされます。過剰な CPU 使用率を回避するために、**platform rate-limit all mtu-failure** コマンドを使用して、RP に送信されるトラフィックのフラグメンテーションのレートを制限できます。
- MPLS では以下のコマンドがサポートされます。
  - **mpls ip default route**
  - **mpls ip propagate-ttl**
  - **mpls ip ttl-expiration pop**
  - **mpls label protocol**
  - **mpls label range**
  - **mpls ip**
  - **mpls label protocol**
  - **mpls mtu**

  これらのコマンドの詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html

  Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

MPLS について

MPLS の概要

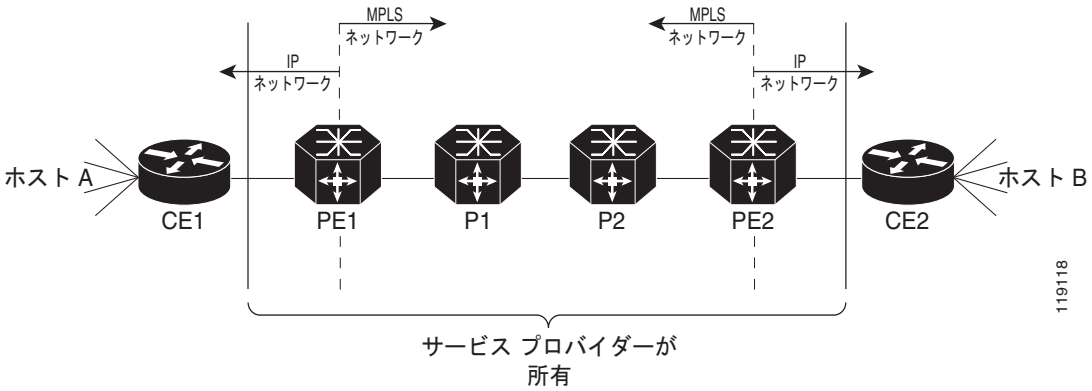
MPLS は、ラベル スイッチングを使用して、イーサネット経由でパケットを転送します。ラベルはグループ化または Forwarding Equivalence Class（FEC）に基づいて、パケットに割り当てられます。ラベルはレイヤ 2 ヘッダーとレイヤ 3 ヘッダーの間に追加されます。

MPLS ネットワークでは、ラベル エッジ ルータ（LER）が着信ラベルのラベル検索を実行し、着信ラベルを発信ラベルに切り替えて、パケットをラベル スイッチ ルータ（LSR）のネクスト ホップに送信します。ラベルがパケットに対してインポーズ（プッシュ）されるのは、MPLS ネットワークの入力エッジ上に限定されます。出力エッジでは、ラベルが削除（ポップ）されます。コア ネットワーク LSR（プロバイダー、または P ルータ）はラベルを読み取り、適切なサービスを適用し、ラベルに基づいてパケットを転送します。

着信ラベルには集約または非集約の 2 つのタイプがあります。集約ラベルの場合は、ネクスト ホップおよび発信インターフェイスを検出するときに、IP 検索を通して着信 MPLS パケットをスイッチングする必要があります。非集約ラベルの場合は、パケットに IP ネクスト ホップ情報が格納されます。

図 36-1 に、カスタマー ネットワークの 2 つのサイトを接続するサービス プロバイダーの MPLS ネットワークを示します。

図 36-1　　MPLS ネットワーク

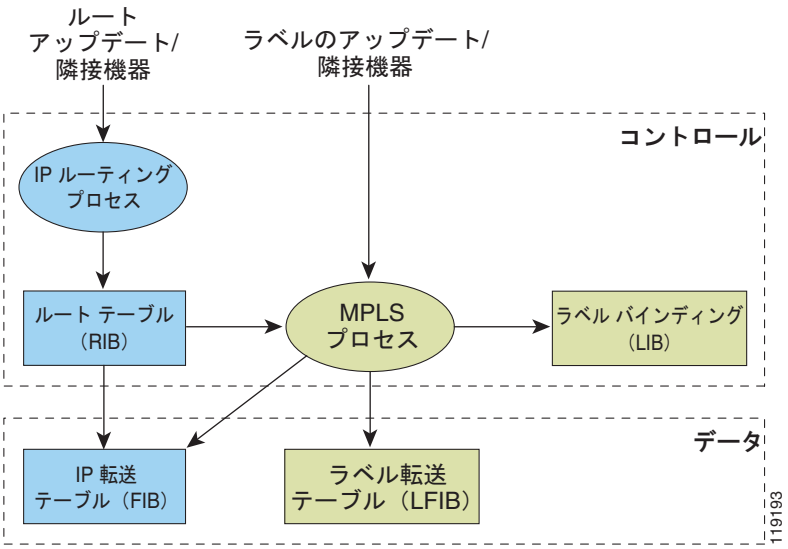


ルート プロセッサ（RP）は、アドレス解決やルーティング プロトコルなどのレイヤ 3 コントロール プレーン機能を実行します。RP はルーティング プロトコルおよびラベル配布プロトコル（LDP; Label Distribution Protocol）からの情報を処理し、IP 転送（Forwarding Information Base（FIB; 転送情報ベース））テーブルおよびラベル転送（Label Forwarding Information Base（LFIB））テーブルを構築します。RP は両方のテーブルの情報を PFC および DFC に配布します。

PFC および DFC は情報を取得し、FIB および LFIB テーブルのコピーを独自に作成します。同時に、これらのテーブルから FIB Ternary Content Addressable Memory（TCAM）を作成します。PFC および DFC は FIB TCAM テーブル内で、着信 IP パケットおよびラベル付きパケットを検索します。検索結果は、特定の隣接エントリへのポインタです。この隣接エントリには、ラベルのプッシュ（IP から MPLS へのパスの場合）、ラベルのスワップ（MPLS から MPLS へのパスの場合）、ラベルのポップ（MPLS から IP へのパスの場合）、およびカプセル化に関する適切な情報が格納されます。

図 36-2 に MPLS をサポートする各機能ブロックを示します。ルーティング プロトコルは、IP および MPLS データ パケットの転送に使用される Routing Information Base（RIB）を生成します。Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）の場合、必要なルーティング情報が RIB から抽出されて、Forwarding Information Base（FIB; 転送情報ベース）に構築されます。ラベル配布プロトコル（LDP）は RIB からルートを取得して、ラベル スイッチ パスを介してラベルを配布し、各 LSR および LER 内に Label Forwarding Information Base（LFIB）を構築します。

図 36-2　MPLS 転送、制御、およびデータ プレーン



IP to MPLS

PFC は MPLS ネットワークへの入口で IP パケットを調べて、FIB TCAM 内でルートを検索します。検索結果は、特定の隣接エントリへのポインタです。隣接エントリには、ラベルのプッシュ（IP から MPLS へのパスの場合）およびカプセル化に関する適切な情報が格納されています。PFC は、MPLS パケットのスイッチングに必要なインポジション ラベルを含む結果を生成します。

MPLS to MPLS

PFC は MPLS ネットワークのコアで最上位ラベルを使用して、FIB TCAM 内で検索を実行します。正常な検索結果によって隣接を示すと、パケット内の最上位ラベルを、ダウンストリーム Label Switch Router（LSR; ラベル スイッチング ルータ）によってアドバタイズされた新しいラベルで置き換えます。ルータが直前ホップ LSR ルータ（出力 LER の次のアップストリーム LSR）である場合、隣接は PFCBXL に最上位ラベルをポップするように指示します。これにより、VPN または Any Transport over MPLS（AToM）で使用するラベルが残っている MPLS パケット、またはネイティブ IP パケットが作成されます。

MPLS to IP

MPLS ネットワークの出口では、いくつかの処理が考えられます。

ネイティブ IP パケットの場合（直前ルータがラベルをポップした場合）、PFC は FIB TCAM 内でルートを検索します。

MPLS VPN パケットの場合は、内部ゲートウェイ プロトコル（IGP）ラベルが直前ルータでポップされたあとに、VPN ラベルが残ります。PFC が実行する処理は、VPN ラベル タイプによって異なります。集約ラベルを伝送するパケットでは、集約ラベルのポップ後に、IP ヘッダーに基づいてさらに検索する必要があります。非集約ラベルの場合、PFC は FIB TCAM 内でルートを検索し、IP ネクスト ホップ情報を取得します。

IGP ラベルおよび VPN ラベルが付加されたパケットの場合、Penultimate Hop Popping（PHP）が発生しなければ、パケットは VPN ラベルの上部で明示的 null ラベルを伝送します。PFC は FIB TCAM 内で最上位ラベルを検索し、パケットを再循環させます。その後、PFC は上記段落の説明に従って、集約ラベルであるか非集約ラベルであるかに応じて残りのラベルを処理します。

EoMPLS、MPLS、および MPLS VPN の場合、明示的 null ラベルが付加されたパケットについて、MPLS は同様に処理されます。

MPLS VPN 転送

直接接続ネットワークまたは集約ルート用の集約ラベル、および非集約ラベルという 2 種類の VPN ラベルがあります。集約ラベルを伝送するパケットでは、集約ラベルのポップ後に、IP ヘッダーに基づいてさらに検索する必要があります。VPN 情報（VPN-IPv4 アドレス、拡張コミュニティ、およびラベル）は Multiprotocol-Border Gateway Protocol（MP-BGP）によって配布されます。

再循環

場合により、PFC はパケットの再循環機能を提供します。再循環を使用すると、ACL または QoS TCAM、NetFlow テーブル、または FIB TCAM テーブル内で追加検索を実行できます。再循環は次の状況で必要となります。

- 4 つ以上のラベルをインポジションにプッシュする場合
- 3 つ以上のラベルをディスポジションにポップする場合
- 最上位の明示的 null ラベルをポップする場合
- VPN ルーティング/転送（VRF）番号が 511 よりも大きい場合
- 出力インターフェイスの IP ACL の場合（非集約（プレフィックス単位）ラベル専用）

パケット再循環が発生するのは、特定のパケット フローに対してだけです。その他のパケット フローには影響しません。パケットの書き替えはモジュールで行われます。書き替えられたパケットは PFC に転送されて、さらに処理されます。

ハードウェアでサポートされる機能

次の機能はハードウェアでサポートされます。

- ラベル処理：任意の個数のラベルをプッシュまたはポップできます。ただし、最適な結果を得るために、同じ処理内でプッシュするラベル数を最大で 3 つに、ポップするラベル数を最大で 2 つにしてください。
- IP から MPLS へのパス：IP パケットを受信して、MPLS パスに送信できます。
- MPLS から IP へのパス：ラベル付きパケットを受信して、IP パスに送信できます。
- MPLS から MPLS へのパス：ラベル付きパケットを受信して、そのラベル パスに送信できます。
- MPLS Traffic Engineering（MPLS TE）: MPLS バックボーンは、レイヤ 2 ATM およびフレーム リレー ネットワークのトラフィック エンジニアリング機能を反復および拡張できます。
- Time to Live（TTL）処理：MPLS ネットワークの入力エッジでは、MPLS フレーム ヘッダーの TTL 値を、IP パケット ヘッダーの TTL フィールドから受信したり、隣接エントリのユーザ設定値から受信したりできます。MPLS ネットワークの出口では、最終 TTL はラベル TTL と IP TTL のいずれか小さい方の値から 1 を引いた値になります。

（注）　均一モードでは、TTL は IP TTL から取得されます。パイプ モードでは、ハードウェア レジスタから取得した値 255 が発信ラベルに使用されます。

- QoS：IP パケットから取得された Differentiated Services（DiffServ）および ToS に関する情報を、MPLS EXP フィールドにマッピングできます。
- MPLS/VPN サポート：最大 1024 個の VRF をサポートできます（511 個を超える VRF を再循環する必要があります）。
- Ethernet over MPLS：MPLS ドメインの入口でイーサネット フレームをカプセル化し、出口でカプセル化解除できます。
- パケット再循環：PFC にはパケット再循環機能があります。「再循環」（P.36-5）を参照してください。
- MPLS スイッチング設定は、**mpls ip** コマンドを使用した VLAN インターフェイスでサポートされます。

サポートされている MPLS 機能

- MPLS 機能：
  - 基本的な MPLS
  - MPLS TE
  - MPLS TE DiffServ 認識（DS-TE）
  - MPLS TE 転送隣接
  - MPLS TE エリア間トンネル
  - MPLS バーチャル プライベート ネットワーク（VPN）
  - MPLS VPN Carrier Supporting Carrier（CSC）
  - MPLS VPN Carrier Supporting Carrier IPv4 BGP ラベル配信
  - MPLS VPN 相互自律システム（InterAS）のサポート
  - MPLS VPN Inter-AS IPv4 BGP ラベル配信

  詳細については、次のマニュアルを参照してください。

  http://www.cisco.com/en/US/docs/ios-xml/ios/mpls/config_library/15-sy/mp-15-sy-library.html

  http://www.cisco.com/en/US/tech/tk436/tk428/technologies_configuration_example09186a0080093fcb.shtml

  http://www.cisco.com/en/US/tech/tk436/tk428/technologies_configuration_example09186a0080093fd0.shtml
- MPLS VPN の HSRP サポート：次のマニュアルを参照。

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipapp_fhrp/configuration/15-sy/fhp-15-sy-book.html
- MPLS VPN の OSPF 模造リンク サポート：次のマニュアルを参照。

  http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/15-sy/iro-sham-link.html

- CE ルータ（VRF Lite）用のマルチ VPN ルーティングおよび転送（VRF）：VRF Lite は、次の機能でサポートされます。
  - VRF インターフェイス間の IPv4 転送
  - IPv4 ACL
  - IPv4 HSRP

  次の資料を参照してください。

  http://www.cisco.com/en/US/products/hw/routers/ps259/prod_bulletin09186a00800921d7.html

MPLS のデフォルト設定

なし。

MPLS 機能の設定方法

- 「MPLS の設定」（P.36-7）
- 「LAN カードでの MUX-UNI サポートの設定」（P.36-7）

MPLS の設定

MPLS を設定するには、次のマニュアルを使用してください。

http://www.cisco.com/en/US/docs/ios-xml/ios/mpls/config_library/15-sy/mp-15-sy-library.html

LAN カードでの MUX-UNI サポートの設定

ユーザ ネットワーク インターフェイス（UNI）は、CE 機器と入力 PE の接続ポイントで、接続 VLAN は UNI ポートの VLAN です。

LAN カードの MUX-UNI サポート機能では、接続 VLAN の物理ポートを分割して、単一の UNI で複数のレイヤ 2 およびレイヤ 3 サービスを提供できます。

LAN カードで MUX-UNI サポートを設定する場合、PE ルータで次の作業を行ってください。

	コマンド	目的
ステップ 1	`Router# 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	`Router(config)# interface type number`	設定するインターフェイスを選択し、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。イーサネット ポートだけで有効です。
ステップ 3	`Router(config-if)# switchport`	レイヤ 3 モードになっているインターフェイスを、レイヤ 2 設定用にレイヤ 2 モードにします。

ステップ 4	`Router(config-if)# switchport trunk encapsulation dot1q`	802.1Q カプセル化をサポートするようポートを設定します。 リンクの両端を同一カプセル化タイプで設定する必要があります。
ステップ 5	`Router(config-if)# switchport mode trunk`	ポートを VLAN トランクとして設定します。
ステップ 6	`Router(config-if)# switchport trunk allowed vlan` *vlan-list*	デフォルトの場合は、すべての VLAN が許可されます。VLAN を明示的に許可するには、このコマンドを使用します。*vlan-list* の有効な値は、1 ～ 4094 です。 （注）　メイン インターフェイスとサブインターフェイス間で VLAN 割り当てが重複しないようにしてください。メイン インターフェイスとサブインターフェイス間の VLAN 割り当ては、相互に排他的にする必要があります。
ステップ 7	`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。
ステップ 8	`Router(config)# interface` *type slot/port.subinterface-number*	設定するサブインターフェイスを選択し、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。イーサネット ポートだけで有効です。
ステップ 9	`Router(config-if)# encapsulation dot1q` *vlan_id*	サブインターフェイスでの 802.1Q VLAN パケットの受信をイネーブルにします。 Ethernet over MPLS が稼働している CE ルータと PE ルータ間のサブインターフェイスは、同じサブネット内になければなりません。その他のすべてのサブインターフェイスおよびバックボーン ルータは、同じサブネット内になくてもかまいません。
ステップ 10	`Router(config-if)# xconnect` *peer_router_id vcid* `encapsulation mpls`	接続回線を疑似接続 VC にバインドします。このコマンドの構文は、その他のレイヤ 2 トランスポートの場合と同じです。

次に、UNI として使用される物理トランク ポートの例を示します。

```
Router(config)# interface gigabitethernet 3/1
Router(config-if)# switchport
Router(config-if)# switchport encapsulation dot1q
Router(config-if)# switchport mode trunk
Router(config-if)# switchport trunk allowed vlan 200-250
Router(config-if)# exit

Router(config)# interface gigabitethernet 3/1.10
Router(config-if)# encap dot1q 3000
Router(config-if)# xconnect 10.0.0.1 3000 encapsulation mpls
Router(config-if)# exit
```

次に、UNI として使用されるレイヤ 2 ポート チャネルの例を示します。

```
Router(config)# interface port-channel 100
Router(config-if)# switchport
Router(config-if)# switchport trunk encapsulation dot1q
Router(config-if)# switchport trunk allowed vlan 100-200
Router(config-if)# switchport mode trunk
Router(config-if)# no ip address
Router(config-if)# exit
```

```
Router(config)# interface port-channel 100.1
Router(config-if)# encapsulation dot1Q 3100
Router(config-if)# xconnect 10.0.0.30 100 encapsulation mpls
Router(config-if)# exit
```

次に、多重化 UNI ポートのレイヤ 3 終端および VRF の例を示します。

```
Router(config)# vlan 200, 300, 400
Router(config)# interface gigabitethernet 3/1
Router(config-if)# switchport
Router(config-if)# switchport encapsulation dot1q
Router(config-if)# switchport mode trunk
Router(config-if)# switchport trunk allowed vlan 200-500
Router(config-if)# exit

Router(config)# interface gigabitethernet 3/1.10
Router(config-if)# encap dot1q 3000
Router(config-if)# xconnect 10.0.0.1 3000 encapsulation mpls
Router(config-if)# exit

Router(config)# interface vlan 200
Router(config-if)# ip address 1.1.1.3
Router(config-if)# exit

Router(config)# interface vlan 300
Router(config-if)# ip vpn VRF A
Router(config-if)# ip address 3.3.3.1
Router(config-if)# exit

Router(config)# interface vlan 400
Router(config-if)# ip address 4.4.4.1
Router(config-if)# ip ospf network broadcast
Router(config-if)# mpls label protocol ldp
Router(config-if)# mpls ip
Router(config-if)# exit
```

MPLS の設定例

次に、MPLS の基本設定の例を示します。

```
*****
Basic MPLS
*****


IP ingress interface:

Router# mpls label protocol ldp

interface GigabitEthernet6/2
 ip address 75.0.77.1 255.255.255.0
 media-type rj45
 speed 1000
end

Label egress interface:

interface GigabitEthernet7/15
 mtu 9216
 ip address 75.0.67.2 255.255.255.0
```

```
 logging event link-status
 mpls ip


Router# show ip route 188.0.0.0
Routing entry for 188.0.0.0/24, 1 known subnets

O IA    188.0.0.0 [110/1] via 75.0.77.2, 00:00:10, GigabitEthernet6/2


Router# show ip routing 88.0.0.0
Routing entry for 88.0.0.0/24, 1 known subnets

O E2    88.0.0.0 [110/0] via 75.0.67.1, 00:00:24, GigabitEthernet7/15
                 [110/0] via 75.0.21.2, 00:00:24, GigabitEthernet7/16
Router# show mpls forwarding-table 88.0.0.0
Local  Outgoing    Prefix              Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id        switched   interface
30     50          88.0.0.0/24       0          Gi7/15     75.0.67.1
       50          88.0.0.0/24       0          Gi7/16     75.0.21.2


Router# show platform cef 88.0.0.0 detail

Codes: M - mask entry, V - value entry, A - adjacency index, P - priority bit
       D - full don't switch, m - load balancing modnumber, B - BGP Bucket sel
       V0 - Vlan 0,C0 - don't comp bit 0,V1 - Vlan 1,C1 - don't comp bit 1
       RVTEN - RPF Vlan table enable, RVTSEL - RPF Vlan table select
Format: IPV4_DA - (8 | xtag vpn pi cr recirc tos prefix)
Format: IPV4_SA - (9 | xtag vpn pi cr recirc prefix)
M(3223   ): E | 1 FFF  0 0 0 0   255.255.255.0
V(3223   ): 8 | 1 0    0 0 0 0   88.0.0.0           (A:344105 ,P:1,D:0,m:1 ,B:0 )
M(3223   ): E | 1 FFF  0 0 0 255.255.255.0
V(3223   ): 9 | 1 0    0 0 0 88.0.0.0 (V0:0    ,C0:0 ,V1:0    ,C1:0 ,RVTEN:0 ,RVTSEL:0  )
Router# show platform cef adj ent 344105

Index: 344105  smac: 0005.9a39.a480, dmac: 000a.8ad8.2340
               mtu: 9234, vlan: 1031, dindex: 0x0, l3rw_vld: 1
               packets: 109478260, bytes: 7006608640

Router# show platform cef adj ent 344105 detail

Index: 344105  smac: 0005.9a39.a480, dmac: 000a.8ad8.2340
               mtu: 9234, vlan: 1031, dindex: 0x0, l3rw_vld: 1
               format: MPLS, flags: 0x1000008418
               label0: 0, exp: 0, ovr: 0
               label1: 0, exp: 0, ovr: 0
               label2: 50, exp: 0, ovr: 0
               op: PUSH_LABEL2
               packets: 112344419, bytes: 7190042816
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

MPLS VPN サポート

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

MPLS VPN の前提条件

なし。

MPLS VPN の制約事項

- MPLS VPN を設定する場合、VPN 数が 511 を超えると VPN が再循環されることに注意してください。
- MPLS VPN では以下のコマンドがサポートされます。
  - **address-family**
  - **exit-address-family**
  - **import map**
  - **ip route vrf**
  - **ip route forwarding**
  - **ip vrf**
  - **neighbor activate**
  - **rd**
  - **route-target**

  これらのコマンドの詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html

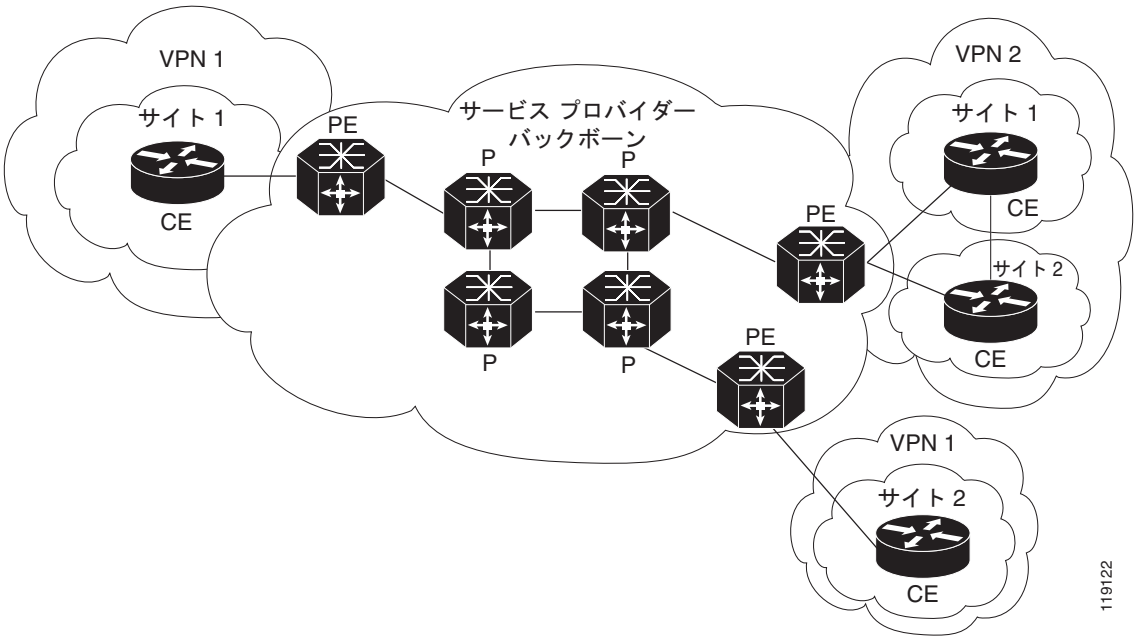
  Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

MPLS VPN サポートについて

Cisco IOS ネットワークに MPLS の IP VPN 機能を使用すると、スケーラブルな IP レイヤ 3 VPN バックボーン サービスを、共有インフラストラクチャに配置された複数のサイトに導入し、同時にプライベート ネットワークと同じアクセスまたはセキュリティを提供できます。MPLS テクノロジーに基づいた VPN には、ルーティングの隔離、セキュリティの向上、ルーティングの簡素化およびスケーラビリティの向上が実現するという利点があります。MPLS VPN の詳細については、次のマニュアルを参照してください。

http://www.cisco.com/en/US/docs/ios-xml/ios/mpls/config_library/15-sy/mp-15-sy-library.html

図 37-1　VPN および MPLS サービス プロバイダー バックボーン



PFC は入力 PE で、パケット ヘッダーに基づいて転送を判断します。PFC には、VLAN を VPN にマッピングするテーブルが格納されています。スイッチのアーキテクチャでは、システム内のすべての物理入力インターフェイスが特定の VPN に対応付けられます。PFC は CEF テーブル内で IP 宛先アドレスを検索しますが、対象となるのは特定の VPN 内のプレフィックスだけです（テーブル エントリは特定の隣接セットを指します。複数のパラレル パスが存在する場合は、ロードバランス判断によって特定の隣接が選択されます）。

テーブル エントリには、パケットに必要なレイヤ 2 ヘッダー情報、およびフレームにプッシュされる特定の MPLS ラベルが格納されます。パケット書き替え用のこの情報は、入力モジュールに送信されて書き替えが行われ、出力ライン インターフェイスに転送されます。

VPN トラフィックはプレフィックス単位のラベルまたは集約ラベルに基づいて、PE からの出口で処理されます。プレフィックス単位のラベルが使用される場合、各 VPN プレフィックスには一意のラベルが対応付けられます。これにより、PE は FIB 内のラベル検索に基づいて、パケットを最終宛先に転送できます。

（注）　PFC が割り当てるのは、VRF ごとに 1 つの集約ラベルだけです。

出力 PE でのディスポジションに集約ラベルが使用される場合、複数のインターフェイスの多数のプレフィックスをこのラベルに対応付けることができます。この場合、PFC は IP 検索を実行して最終宛先を判別する必要があります。IP 検索には再循環が必要となる場合があります。

MPLS VPN の設定方法

MPLS VPN の設定手順については、次のマニュアルを参照してください。

http://www.cisco.com/en/US/docs/ios-xml/ios/mpls/config_library/15-sy/mp-15-sy-library.html

（注）　別の MPLS デバイスとのレイヤ 2 ポート ピアリングで MPLS アップリンクとしてレイヤ 3 VLAN インターフェイスを使用する場合は、別のレイヤ 3 VLAN インターフェイスを VRF インターフェイスとして使用できます。

MPLS VPN の設定例

次に、LAN CE 方向のインターフェイスの設定例を示します。Cisco IOS Release 15.1SY の MPLS スイッチングのコンフィギュレーションは、他のリリースでのコンフィギュレーションと同じです。

```
!ip vrf blues
 rd 100:10
 route-target export 100:1
 route-target import 100:1
!
mpls label protocol ldp
mpls ldp logging neighbor-changes
!
interface Loopback0
 ip address 10.4.4.4 255.255.255.255
!
interface GigabitEthernet4/2
 description Catalyst link to P2
 no ip address
!
interface GigabitEthernet4/2.42
 encapsulation dot1Q 42
 ip address 10.0.3.2 255.255.255.0
 tag-switching ip
!
interface GigabitEthernet7/3
 description Catalyst link to CE2
 no ip address
!
interface GigabitEthernet7/3.73
 encapsulation dot1Q 73
 ip vrf forwarding blues
 ip address 10.19.7.1 255.255.255.0
!
router ospf 100
 log-adjacency-changes
 network 10.4.4.4 0.0.0.0 area 0
 network 10.0.0.0 0.0.255.255 area 0
!
router ospf 65000 vrf blues
 log-adjacency-changes
 redistribute bgp 100 subnets
 network 10.19.0.0 0.0.255.255 area 0
!
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.3.3.3 remote-as 100
 neighbor 10.3.3.3 description MP-BGP to PE1
 neighbor 10.3.3.3 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
 neighbor 10.3.3.3 activate
```

```
 neighbor 10.3.3.3 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf blues
 redistribute connected
 redistribute ospf 65000 match internal external 1 external 2
 no auto-summary
 no synchronization
 exit-address-family
!
```

Ethernet over MPLS（EoMPLS）

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

EoMPLS の前提条件

EoMPLS を設定する前に、ネットワークが次のように設定されていることを確認してください。

- PE ルータが IP を通して相互に到達できるように、コアに IP ルーティングを設定します。
- PE ルータ間に ラベル スイッチド パス（LSP）が存在するように、コアに MPLS を設定します。

EoMPLS の制約事項

- Cisco IOS Release 15.1SY の EoMPLS の場合、トンネル入口ではロードバランスは行われません。複数の IGP パスを使用できる場合でも、Interior Gateway Protocol（IGP）パスは 1 つだけ選択されますが、MPLS コアではロードバランスを使用できます。

- 受信された最大のレイヤ 2 パケットを伝達できるように、エンドポイント間のすべての中間リンクの最大伝送単位（MTU）を設定する必要があります。
- EoMPLS は、IEEE 802.1Q 標準に準拠する VLAN パケットをサポートします。802.1Q 仕様は、イーサネット フレームに VLAN メンバーシップ情報を挿入する標準方式を確立します。
- QoS がレイヤ 2 ポートでイネーブルの場合、802.1Q P ビットまたは IP precedence ビットのいずれかを、信頼できる設定を使用して保護できます。ただし、デフォルトでは、保護されていないビットは保護されたビットの値によって上書きされます。たとえば、P ビットが保護されている場合、IP precedence ビットは P ビットの値で上書きされます。IP precedence ビットを維持するには、**no platform qos rewrite ip dscp** コマンドを使用します。**no platform qos rewrite ip dscp** コマンドは、MPLS および MPLS VPN 機能と互換性がありません。
- プライベート VLAN では、EoMPLS がサポートされません。
- EoMPLS でトランクを使用する場合は、次の制約事項が適用されます。
  - EoMPLS クラウドでイーサネット スパニングツリー ブリッジ プロトコル データ ユニット（BPDU）をサポートするには、MPLS VLAN 上のイーサネットのスパニングツリーをディセーブルにする必要があります。このようにすると、EoMPLS VLAN のカスタマー スイッチへの伝送経路がトランクに限定されます。このようにしないと、BPDU は EoMPLS クラウドに転送されません。
  - トランクのネイティブ VLAN を EoMPLS VLAN として設定しないでください。
- Cisco IOS Release 15.1SY では、すべてのプロトコル（CDP、VTP、BPDU など）は無条件に MPLS クラウドでトンネリングされます。
- インターフェイス間には一意の VLAN が必要です。異なるインターフェイスで同じ VLAN ID は使用できません。
- PE から PE へのラベル スイッチド パス（LSP）を確保するには、ルーティング テーブルおよび CEF テーブル内の EoMPLS トンネル宛先ルートが /32 アドレス（マスクが 255.255.255.255 であるホスト アドレス）でなければなりません。
- 特定の EoMPLS 接続では、入力 PE の入力 EoMPLS インターフェイスおよび出力 PE の出力 EoMPLS インターフェイスを、dot1Q カプセル化が設定されたサブインターフェイスにする必要があります。このようにしないと、どちらもサブインターフェイスになりません。
- MPLS ネットワークに接続された発信インターフェイスがレイヤ 2 カードのポートである場合、802.1Q-in-802.1Q over EoMPLS がサポートされます。
- MPLS ネットワークに接続された出力インターフェイスがレイヤ 2 LAN ポート（PFC ベース EoMPLS と呼ばれるモード）である場合、EoMPLS トラフィックのシェーピングはサポートされません。
- PFC に基づいた EoMPLS では、宛先 MAC アドレスがローカルまたはリモート セグメント上にあるかどうかを判別するためのレイヤ 2 検索を実行しません。また、レイヤ 2 アドレス学習も実行しません（従来の LAN ブリッジングが実行します）。
- AToM 制御ワードはサポートされていません。
- ハードウェアレベルの巡回冗長検査（CRC）エラー、フレーミング エラー、およびラント パケットを含むイーサネット パケットは、入力時に廃棄されます。
- VLAN ベース EoMPLS はサブインターフェイスで設定する必要があります。
- ポートベース EoMPLS および VLAN ベース EoMPLS は相互に排他的です。メイン インターフェイスでポートツーポート トランスポートをイネーブルにした場合は、サブインターフェイスでのコマンド入力も不可能になります。
- レイヤ 3 VLAN インターフェイスでは EoMPLS がサポートされません。

- ポイントツーポイント EoMPLS は、物理インターフェイスおよびサブインターフェイスと連携します。

EoMPLS について

AToM の概要

Any Transport over MPLS（AToM）は MPLS バックボーン上でレイヤ 2 パケットを転送します。AToM はエッジ ルータ間で転送されたラベル配布プロトコル（LDP）セッションを使用して、接続の設定およびメンテナンスを行います。2 つのレベルのラベルを使用して、エッジ ルータ間でスイッチングを行うと、転送が生じます。外部ラベル（トンネル ラベル）は、MPLS バックボーンを介して入力 PE から出力 PE にパケットをルーティングします。VC ラベルは、トンネル エンドポイント（出力 PE の特定の出力インターフェイスおよびイーサネット フレームの VLAN ID）で接続を判別する逆多重化ラベルです。

EoMPLS の概要

EoMPLS は AToM トランスポート タイプの 1 つです。EoMPLS は MPLS パケットに Ethernet PDU をカプセル化し、MPLS ネットワーク上で転送することにより機能します。各 PDU は単一パケットとして転送されます。Cisco IOS Release 15.1SY は、次の 2 つの EoMPLS モードをサポートしています。

- VLAN モード：MPLS ネットワーク上の単一 VC を介して、送信元 802.1Q VLAN から宛先 802.1Q VLAN にイーサネット トラフィックを転送します。VLAN モードは、デフォルトとして VC タイプ 5（dot1q タグなし）を使用します。リモート PE がサブインターフェイス（VLAN）ベース EoMPLS に対して VC タイプ 5 をサポートしない場合は、VC タイプ 4（トランスポート dot1 タグ）を使用します。
- ポート モード：ポートのすべてのトラフィックが MPLS ネットワーク上の単一 VC を共有できるようにします。ポート モードは VC タイプ 5 を使用します。

（注）　VLAN モードおよびポート モードのどちらの場合も、ループバック インターフェイスを使用しない限り、Cisco IOS Release 15.1SY の EoMPLS は、インターフェイス間におけるパケットのローカル スイッチングを許可しません。

LAN ポートはレイヤ 2 トラフィックを受信し、ラベルをインポーズし、フレームを MPLS コアにスイッチングできます。

EoMPLS のデフォルト設定

なし。

EoMPLS の設定方法

VLAN ベース EoMPLS の設定

VLAN ベース EoMPLS を設定する場合、PE ルータで次の作業を行ってください。

	コマンド	目的
ステップ 1	`Router# 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	`Router(config)# interface gigabitethernet slot/interface.subinterface`	ギガビット イーサネット サブインターフェイスを指定します。隣接 CE ルータのサブインターフェイスがこの PE ルータと同じ VLAN 上にあることを確認します。
ステップ 3	`Router(config-if)# encapsulation dot1q vlan_id`	サブインターフェイスでの 802.1Q VLAN パケットの受信をイネーブルにします。 • Ethernet over MPLS が稼働している CE ルータと PE ルータ間のサブインターフェイスは、同じサブネット内になければなりません。 • その他のすべてのサブインターフェイスおよびバックボーン ルータは、同じサブネット内になくてもかまいません。
ステップ 4	`Router(config-if)# xconnect peer_router_id vcid encapsulation mpls`	接続回線を疑似接続 VC にバインドします。このコマンドの構文は、その他のレイヤ 2 トランスポートの場合と同じです。

次に、VLAN ベース EoMPLS の設定例を示します。

```
interface GigabitEthernet7/4.2
encapsulation dot1Q 3
xconnect 13.13.13.13 3 encapsulation mpls
no shut
```

（注）　IP アドレスは CE デバイスのサブインターフェイスに設定されます。

MPLS トンネルを介したレイヤ 2 VLAN トランスポートの設定を確認および表示するには、次の作業を行います。

- VLAN ごとに VLAN 名、ステータス、ポートを 1 行で表示するには、**show vlan brief** コマンドを使用します。

```
Router# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------
1    default                          active
2    VLAN0002                         active
3    VLAN0003                         active
```

```
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

- PE ルータ エンドポイントが相互に検出されたことを確認するには、**show mpls ldp discovery** コマンドを使用します。PE ルータが別の PE ルータから LDP の hello メッセージを受信した場合、そのルータおよび指定されたラベル スペースは「検出された」と見なされます。

```
Router# show mpls ldp discovery
 Local LDP Identifier:
    13.13.13.13:0
    Discovery Sources:
    Interfaces:
        GE-WAN3/3 (ldp): xmit/recv
            LDP Id: 12.12.12.12:0
    Targeted Hellos:
        13.13.13.13 -> 11.11.11.11 (ldp): active/passive, xmit/recv
            LDP Id: 11.11.11.11:0
```

- ラベル配布セッションが確立されたことを確認するには、**show mpls ldp neighbor** コマンドを使用します。出力の 3 行めは、LDP セッションのステートが動作可能であり、メッセージが送受信中であることを示します。

```
Router# show mpls ldp neighbor
    Peer LDP Ident: 12.12.12.12:0; Local LDP Ident 13.13.13.13:0
        TCP connection: 12.12.12.12.646 - 13.13.13.13.11010
        State: Oper; Msgs sent/rcvd: 1649/1640; Downstream
        Up time: 23:42:45
        LDP discovery sources:
          GE-WAN3/3, Src IP addr: 34.0.0.2
        Addresses bound to peer LDP Ident:
          23.2.1.14       37.0.0.2        12.12.12.12     34.0.0.2
          99.0.0.1
    Peer LDP Ident: 11.11.11.11:0; Local LDP Ident 13.13.13.13:0
        TCP connection: 11.11.11.11.646 - 13.13.13.13.11013
        State: Oper; Msgs sent/rcvd: 1650/1653; Downstream
        Up time: 23:42:29
        LDP discovery sources:
          Targeted Hello 13.13.13.13 -> 11.11.11.11, active, passive
        Addresses bound to peer LDP Ident:
          11.11.11.11     37.0.0.1        23.2.1.13
```

- ラベル転送テーブルが正しく構築されたことを確認するには、**show mpls forwarding-table** コマンドを入力して、リモート PE のラベルが学習されたこと、およびこのラベルが正しいインターフェイスから正しいネクスト ホップに送信されていることを確認します。

```
Router# show mpls forwarding-table
Local  Outgoing    Prefix              Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id        switched   interface
16     Untagged    223.255.254.254/32   \
                                   0          Gi2/1      23.2.0.1
20     Untagged    l2ckt(2)          133093     Vl2        point2point
21     Untagged    l2ckt(3)          185497     Vl3        point2point
24     Pop tag     37.0.0.0/8        0          GE3/3      34.0.0.2
25     17          11.11.11.11/32    0          GE3/3      34.0.0.2
26     Pop tag     12.12.12.12/32    0          GE3/3      34.0.0.2
```

出力では次のデータが表示されます。

- Local tag：現在のルータによって割り当てられたラベル
- Outgoing tag or VC：ネクスト ホップによって割り当てられたラベル
- Prefix or Tunnel Id：このラベルが付加されたパケットの送信先アドレスまたはトンネル

  - Bytes tag switched：この着信ラベルによってスイッチングされるバイト数
  - Outgoing interface：このラベルが付加されたパケットが送信されるときに経由するインターフェイス
  - Next Hop：発信ラベルに割り当てられたネイバーの IP アドレス
- 現在ルーティング中の VC のステートを表示するには、**show mpls l2transport vc** コマンドを入力します。

```
Router# show mpls l2transport vc

Local intf     Local circuit        Dest address    VC ID      Status
-------------  -------------------- --------------- ---------- ----------
Vl2            Eth VLAN 2           11.11.11.11     2          UP
Vl3            Eth VLAN 3           11.11.11.11     3          UP
```

各 VC の詳細情報を表示するには、**detail** キーワードを追加します。

```
Router# show mpls l2transport vc detail
Local interface: Vl2 up, line protocol up, Eth VLAN 2 up
  Destination address: 11.11.11.11, VC ID: 2, VC status: up
    Tunnel label: 17, next hop 34.0.0.2
    Output interface: GE3/3, imposed label stack {17 18}
  Create time: 01:24:44, last status change time: 00:10:55
  Signaling protocol: LDP, peer 11.11.11.11:0 up
    MPLS VC labels: local 20, remote 18
    Group ID: local 71, remote 89
    MTU: local 1500, remote 1500
    Remote interface description:
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 1009, send 1019
    byte totals:   receive 133093, send 138089
    packet drops:  receive 0, send 0

Local interface: Vl3 up, line protocol up, Eth VLAN 3 up
  Destination address: 11.11.11.11, VC ID: 3, VC status: up
    Tunnel label: 17, next hop 34.0.0.2
    Output interface: GE3/3, imposed label stack {17 19}
  Create time: 01:24:38, last status change time: 00:10:55
  Signaling protocol: LDP, peer 11.11.11.11:0 up
    MPLS VC labels: local 21, remote 19
    Group ID: local 72, remote 90
    MTU: local 1500, remote 1500
    Remote interface description:
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 1406, send 1414
    byte totals:   receive 185497, send 191917
    packet drops:  receive 0, send 0
```

ポートベース EoMPLS の設定

Cisco IOS Release 15.1SY の EoMPLS による 802.1Q-in-802.1Q トラフィックおよびイーサネット トラフィックをサポートするには、次の作業を行って、ポートベースの EoMPLS を設定します。

	コマンド	目的
ステップ1	Router# **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	Router(config)# **interface gigabitethernet** *slot/interface*	ギガビット イーサネット インターフェイスを指定します。隣接 CE ルータのインターフェイスがこの PE ルータと同じ VLAN 上にあることを確認します。
ステップ3	Router(config-if)# **xconnect** *peer_router_id vcid* **encapsulation mpls**	接続回線を疑似接続 VC にバインドします。このコマンドの構文は、その他のレイヤ 2 トランスポートの場合と同じです。

次に、ポートベース設定の例を示します。

```
Router# show mpls l2transport vc

Local intf     Local circuit        Dest address    VC ID      Status
-------------  -------------------- --------------- ---------- ----------
Gi8/48         Ethernet             75.0.78.1       1          UP
Gi7/11.2000    Eth VLAN 2000        75.0.78.1       2000       UP

Router# show run interface gigabitethernet 8/48
Building configuration...

Current configuration : 86 bytes
!
interface GigabitEthernet8/48
 no ip address
 xconnect 75.0.78.1 1 encapsulation mpls
end

Router# show run interface gigabitethernet 7/11
Building configuration...

Current configuration : 118 bytes
!
interface GigabitEthernet7/11
 description Traffic-Generator
 no ip address
 logging event link-status
 speed nonegotiate
end

Router# show run int gigabitethernet 7/11.2000
Building configuration...

Current configuration : 112 bytes
!
interface GigabitEthernet7/11.2000
 encapsulation dot1Q 2000
 xconnect 75.0.78.1 2000 encapsulation mpls
end

Router# show mpls l2transport vc 1 detail
Local interface: Gi7/47 up, line protocol up, Ethernet up
```

```
  Destination address: 75.0.80.1, VC ID: 1, VC status: up
    Tunnel label: 5704, next hop 75.0.83.1
    Output interface: Te8/3, imposed label stack {5704 10038}
  Create time: 00:30:33, last status change time: 00:00:43
  Signaling protocol: LDP, peer 75.0.80.1:0 up
    MPLS VC labels: local 10579, remote 10038
    Group ID: local 155, remote 116
    MTU: local 1500, remote 1500
    Remote interface description:
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 26, send 0
    byte totals:   receive 13546, send 0
    packet drops:  receive 0, send 0
```

VC タイプを表示するには、次を実行します。

```
Router# remote command switch show mpls l2transport vc 1 de

Local interface: GigabitEthernet7/47, Ethernet
  Destination address: 75.0.80.1, VC ID: 1
  VC status: receive UP, send DOWN
  VC type: receive 5, send 5
    Tunnel label: not ready, destination not in LFIB
    Output interface: unknown, imposed label stack {}
    MPLS VC label: local 10579, remote 10038
  Linecard VC statistics:
    packet totals:  receive: 0  send: 0
    byte totals:  receive: 0  send: 0
    packet drops:  receive: 0  send: 0
  Control flags:
    receive 1,  send: 31
!
```

MPLS トンネルを介したレイヤ 2 VLAN トランスポートの設定を確認および表示するには、次の作業を行います。

- VLAN ごとに VLAN 名、ステータス、ポートを 1 行で表示するには、**show vlan brief** コマンドを使用します。

```
Router# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
2    VLAN0002                         active    Gi1/4
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

- PE ルータ エンドポイントが相互に検出されたことを確認するには、**show mpls ldp discovery** コマンドを使用します。PE ルータが別の PE ルータから LDP の Hello メッセージを受信した場合、そのルータおよび指定されたラベル スペースは「検出された」と見なされます。

```
Router# show mpls ldp discovery
 Local LDP Identifier:
    13.13.13.13:0
    Discovery Sources:
    Interfaces:
        GE-WAN3/3 (ldp): xmit/recv
            LDP Id: 12.12.12.12:0
    Targeted Hellos:
        13.13.13.13 -> 11.11.11.11 (ldp): active/passive, xmit/recv
            LDP Id: 11.11.11.11:0
```

- ラベル配布セッションが確立されたことを確認するには、**show mpls ldp neighbor** コマンドを使用します。出力の 3 行めは、LDP セッションのステートが動作可能であり、メッセージが送受信中であることを示します。

```
Router# show mpls ldp neighbor
    Peer LDP Ident: 12.12.12.12:0; Local LDP Ident 13.13.13.13:0
        TCP connection: 12.12.12.12.646 - 13.13.13.13.11010
        State: Oper; Msgs sent/rcvd: 1715/1706; Downstream
        Up time: 1d00h
        LDP discovery sources:
          GE-WAN3/3, Src IP addr: 34.0.0.2
        Addresses bound to peer LDP Ident:
          23.2.1.14       37.0.0.2        12.12.12.12     34.0.0.2
          99.0.0.1
    Peer LDP Ident: 11.11.11.11:0; Local LDP Ident 13.13.13.13:0
        TCP connection: 11.11.11.11.646 - 13.13.13.13.11013
        State: Oper; Msgs sent/rcvd: 1724/1730; Downstream
        Up time: 1d00h
        LDP discovery sources:
          Targeted Hello 13.13.13.13 -> 11.11.11.11, active, passive
        Addresses bound to peer LDP Ident:
          11.11.11.11     37.0.0.1        23.2.1.13
```

- ラベル転送テーブルが正しく構築されたことを確認するには、**show mpls forwarding-table** コマンドを使用します。

```
Router# show mpls forwarding-table
Local  Outgoing    Prefix              Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id        switched   interface
16     Untagged    223.255.254.254/32   \
                                  0          Gi2/1      23.2.0.1
20     Untagged    l2ckt(2)           55146580   Vl2        point2point
24     Pop tag     37.0.0.0/8         0          GE3/3      34.0.0.2
25     17          11.11.11.11/32     0          GE3/3      34.0.0.2
26     Pop tag     12.12.12.12/32     0          GE3/3      34.0.0.2
```

- 出力には、次のデータが表示されます。
  - Local tag：現在のルータによって割り当てられたラベル
  - Outgoing tag or VC：ネクスト ホップによって割り当てられたラベル
  - Prefix or Tunnel Id：このラベルが付加されたパケットの送信先アドレスまたはトンネル
  - Bytes tag switched：この着信ラベルによってスイッチングされるバイト数
  - Outgoing interface：このラベルが付加されたパケットが送信されるときに経由するインターフェイス
  - Next Hop：発信ラベルに割り当てられたネイバーの IP アドレス
- 現在ルーティング中の VC のステートを表示するには、**show mpls l2transport vc** コマンドを入力します。

```
Router# show mpls l2transport vc

Local intf     Local circuit        Dest address    VC ID      Status
-------------  -------------------- --------------- ---------- ----------
Vl2            Eth VLAN 2           11.11.11.11     2          UP
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CHAPTER 39

仮想プライベート LAN サービス（VPLS）

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

VPLS の前提条件

VPLS を設定する前に、ネットワークが次のように設定されていることを確認してください。

- PE ルータが IP を介して相互に到達できるように、コアに IP ルーティングを設定します。
- PE ルータ間にラベル スイッチド パス（LSP）が存在するように、コアに MPLS を設定します。
- レイヤ 2 トラフィックの開始および終了のためのループバック インターフェイスを設定します。PE ルータが他のルータのループバック インターフェイスにアクセスできるようにします。ループバック インターフェイスは、すべてのケースで必要というわけではないことに注意してください。たとえば、VPLS が TE トンネルに直接マッピングされている場合、トンネル選択ではループバック インターフェイスは必要ありません。

VPLS 設定には、ピア PE ルータを識別する必要があり、各 PE ルータで VPLS にレイヤ 2 回線に対応付ける必要があります。

VPLS の制約事項

- Supervisor Engine 2T を使用する場合、レイヤ 2 プロトコル トンネリングは、VPLS（CSCue45974）ではサポートされません。
- ブロードキャスト パケットのループを回避し、レイヤ 2 トラフィックを分離するために、スプリット ホライズンが、デフォルト設定です。スプリット ホライズンは、エミュレート VC から受信したパケットが別のエミュレート VC に転送されることを防ぎます。この方法は、フルメッシュ ネットワークにループ フリー パスを作成するために重要です。
- サポートされる最大値：
  - VFI の総数：4,096（4K）
  - VFI ごとのエッジとコア ピア PE を組み合わせた最大数：
    - VPLS：250
    - H-VPLS 500
  - VC の総数：12,288（12 K）
- ソフトウェア ベースのデータ プレーンはサポートされません。
- 自動検出メカニズムはサポートされません。
- 冗長 CE-PE リンクでのロード シェアリングとフェールオーバーはサポートされません。
- ラベル配布プロトコル（LDP）を使用した MAC アドレスの追加または削除はサポートされません。
- 仮想転送インスタンス（VFI）は、**interface vlan** コマンドでのみサポートされています。

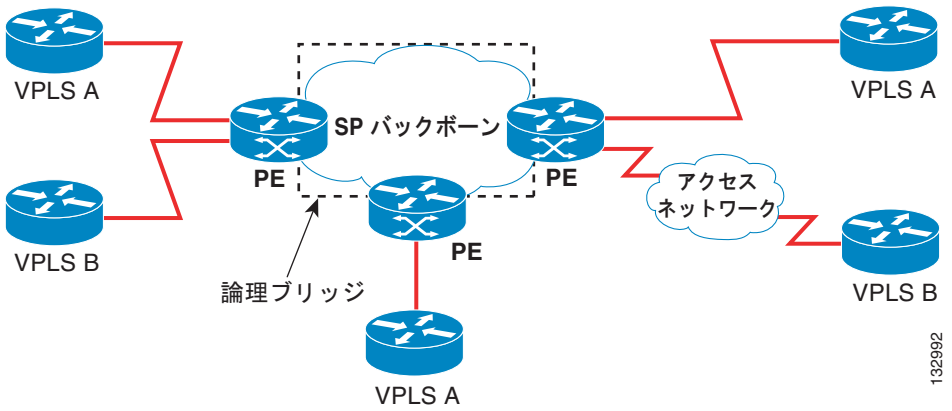
VPLS について

VPLS の概要

VPLS（仮想プライベート LAN サービス）により、企業では、サービス プロバイダーから提供されたインフラストラクチャを解して、複数のサイトからのイーサネット ベースの LAN をまとめてリンクすることが可能になります。企業の側からは、サービス プロバイダーのパブリック ネットワークは、1 つの大きなイーサネット LAN のように見えます。サービス プロバイダーからすると、VPLS は、大規模な設備投資なしで、既存のネットワーク上に収益を生み出す新たなサービスを導入するチャンスになります。オペレータは、ネットワークでの機器の運用年数を延長できます。

Virtual Private LAN Services（VPLS）は、プロバイダー コアを使用して複数のアタッチメント回路を 1 つにまとめることで、複数のアタッチメント回路を 1 つに接続する仮想ブリッジをシミュレートします。VPLS のトポロジは、カスタマーからは認識されません。すべての CE デバイスは、プロバイダー コアによってエミュレートされた論理ブリッジに接続されているように見えます（図 39-1 を参照）。

図 39-1　VPLS トポロジ



フルメッシュの設定

フルメッシュの設定では、VPLS に参加するすべての PE 間でトンネル ラベル スイッチド パス（LSP）のフルメッシュが必要です。フルメッシュでは、シグナリングのオーバーヘッドと、PE 上でプロビジョニング対象の各 VC に対するパケット複製の要件が多くなる場合があります。

VPLS のセットアップは、まず参加する各 PE ルータで Virtual Forwarding Instance（VFI）を作成して行います。VFI によって VPLS ドメインの VPN ID、そのドメインの他の PE ルータのアドレス、トンネルのシグナリングのタイプ、各ピア PE ルータのカプセル化のメカニズムが指定されます。

エミュレート VC の相互接続で形成される VFI のセットは、*VPLS インスタンス*と呼ばれます。これは、パケット スイッチド ネットワークを介して論理ブリッジを構成する VPLS インスタンスです。VPLS インスタンスには、一意の VPN ID が割り当てられます。

PE ルータは、VFI を使用して、エミュレートされた VC から VPLS インスタンスの他のすべての PE ルータまでのフルメッシュ LPS を確立します。PE ルータは、Cisco IOS CLI を使用して、スタティック設定を通じた VPLS インスタンスのメンバーシップを取得します。

フル メッシュ設定を行うと、PE ルータは、単一のブロードキャスト ドメインを維持できます。したがって、接続回線でブロードキャスト、マルチキャスト、または未知のユニキャスト パケットを受信すると、PE ルータは、他のすべての接続回線およびその VPLS インスタンスに属する他のすべての CE デバイスへのエミュレート回線にパケットを送信します。CE デバイスでは、VPLS インスタンスを、エミュレート LAN として認識します。

プロバイダー コアでのパケット ループの問題を回避するために、PE デバイスは、エミュレート VC に「スプリット ホライズン」の原則を適用します。つまり、エミュレート VC でパケットを受信した場合、パケットは、他のいずれのエミュレート VC にも転送されません。

VFI を定義したら、CE デバイスへの接続回線にバインドする必要があります。

パケット転送の判断は、特定の VPLS ドメインのレイヤ 2 仮想転送インスタンス（VFI）を検索することによって行われます。

特定の PE ルータの VPLS インスタンスは、特定の物理または論理ポートに着信するイーサネット フレームを受信し、イーサネット スイッチによる動作同様に、MAC テーブルに入力します。PE ルータでは、この MAC アドレスを使用して、リモート サイトにある別の PE ルータに配布するために、このようなフレームを適切な LSP に切り替えることができます。

MAC アドレスが MAC アドレス テーブルにない場合、PE ルータは、イーサネット フレームを複製し、直前に送信された入力ポートを除くその VPLS インスタンスに関連付けられたすべての論理ポートにフラッディングします。PE ルータは、個々のポートでパケットを受信したときに MAC テーブルを更新し、一定期間使用されていないアドレスを削除します。

H-VPLS

階層型 VPLS（H-VPLS）は、フルメッシュとハブ アンド スポーク構成の両方を使用することによって、シグナリングと複製の両方のオーバーヘッドを軽減します。ハブ アンド スポーク構成は、スプリット ホライズンと連動して疑似配線（PW）間でパケットをスイッチングさせるので、PE 間の PW 数が効果的に削減されます。

（注）　ブロードキャスト パケットのループを回避するために、スプリット ホライズンがデフォルト設定です。**no split-horizon** キーワードを使用した場合にループを回避しようとすると、ネットワーク構成で入念な配慮が必要になります。

サポートされる機能

マルチポイントツーマルチポイントのサポート

複数のデバイスがコア ネットワーク越しに関連付けられます。いずれのデバイスもルート ノードとして指定されていない一方で、すべてのデバイスがルート ノードとして扱われます。すべてのフレームをノード間で直接交換できます。

Non-Transparent 動作

Ethernet Virtual Connection（VEC）は、Ethernet PDU（つまり、BPDU）に関して透過的である場合も非透過的である場合もあります。VEC の非透過性の目的は、レイヤ 3 デバイス間のフレーム リレー型サービスをエンド ユーザが使用できるようにすることです。

回線多重化

回線多重化を使用すると、単一のイーサネット接続を介して、ノードが複数のサービスに加入できます。複数のサービスに参加することによって、イーサネット接続は、複数の論理ネットワークに対応付けられます。可能性のあるサービス製品の例としては、サイト間の VPN サービス、インターネット サービス、企業間コミュニケーションのためとサードパーティ接続などがあります。

MAC アドレス ラーニング、転送、およびエージング

PE は、リモート MAC アドレスおよびカスタマー側ポートに直接接続された MAC アドレスを学習する必要があります。MAC アドレス ラーニングでは、カスタマー サイトから送信されるパケットからトポロジおよび転送情報を抽出することによって、これを実現します。保存された MAC アドレスにタイマーが関連付けられます。タイマーが満了すると、エントリがテーブルから削除されます。

ジャンボ フレーム サポート

ジャンボ フレームのサポートでは、1548 ～ 9216 バイトのフレーム サイズをサポートします。上の範囲内で指定した任意の値に対してジャンボ フレーム サイズを設定するには、CLI を使用します。デフォルト値は、いずれのレイヤ 2/VLAN インターフェイスでも 1500 バイトです。ジャンボ フレーム サポートは、インターフェイスごとに設定できます。

Q-in-Q のサポートおよび EoMPLS への Q-in-Q のサポート

802.1Q トンネリング（Q-in-Q）では、CE は VLAN タグ付きパケットを発行し、VPLS は、このパケットを遠端 CE に転送します。Q-in-Q は、1 つ以上の 802.1Q タグが、ネットワーク内部の 1 つのパケットに配置されることがあるという意味です。パケットが CE デバイスから受信されると、別の CE デバイスとトラフィックを区別するために、追加の VLAN タグが着信イーサネット パケットに追加されます。CE から発信されるタグなしパケットでは、VLAN スイッチド ネットワーク内部の 1 重タグが使用される一方で、CE から発信される、事前にタグの付いたパケットは、複数のタグが使用されます。

VPLS サービス

透過型 LAN サービス

透過型 LAN サービス（TLS）は、ブリッジング プロトコルの透過性（ブリッジ プロトコル データ ユニット（BPDU）など）および VLAN 値を実施するために使用される、ポイントツーポイント ポート ベース EoMPLS の拡張です。ブリッジでは、このサービスをイーサネット セグメントとして認識します。TLS を使用する場合、PE ルータでは、カスタマー側インターフェイスからに受信したすべてのイーサネット パケット（タグ付けされたパケット、タグなしパケット、BPDU を含む）を次のように転送します。

- 宛先 MAC アドレスがレイヤ 2 転送テーブルにある場合は、ローカル イーサネット インターフェイスまたはエミュレート VC に転送。
- 宛先 MAC アドレスがマルチキャスト アドレスまたはブロードキャスト アドレスであるか、宛先 MAC アドレスがレイヤ 2 転送テーブルに存在しない場合は、同じ VPLS ドメインに属する他のすべてのローカル イーサネット インターフェイスおよびエミュレート VC に転送。

（注）　Supervisor Engine 2T を使用する場合、レイヤ 2 プロトコル トンネリングは、VPLS ではサポートされません。これにより、Cisco Discovery Protocol（CDP）、VLAN トランキング プロトコル（VTP）、および VPLS 上のスパニングツリー プロトコル（STP）の使用が回避されます（CSCue45974）。

Ethernet Virtual Connection Service

Ethernet Virtual Connection Service（EVCS）は、ルータが単一の物理ポートから複数のイントラネットおよびエクストラネット ロケーションに到達できる、ポイントツーポイント VLAN ベース EoMPLS の拡張です。ルータは、他のルータにアクセスするサブインターフェイスを認識します。EVCS を使用する場合、PE ルータでは、カスタマー側インターフェイスからに受信した特定の VLAN タグを持つイーサネット パケット（BPDU を除く）を次のように転送します。

- 宛先 MAC アドレスがレイヤ 2 転送テーブルにある場合は、ローカル イーサネット インターフェイスまたはエミュレート VC に転送。
- 宛先 MAC アドレスがマルチキャスト アドレスまたはブロードキャスト アドレスであるか、宛先 MAC アドレスがレイヤ 2 転送テーブルに存在しない場合は、同じ VPLS ドメインに属する他のすべてのローカル イーサネット インターフェイスおよびエミュレート VC に転送。

（注）　これはローカルでのみ意味を持つため、VPLS ドメインを識別する逆多重化 VLAN タグは、出力イーサネット インターフェイスまたはエミュレート VC にパケットを転送する前に削除されます。

VPLS のデフォルト設定

なし。

VPLS の設定方法

- 「CE への PE レイヤ 2 インターフェイスの設定」（P.39-7）
- 「PE でのレイヤ 2 VLAN インスタンスの設定」（P.39-10）
- 「PE における MPLS の設定」（P.39-11）
- 「PE における VFI の設定」（P.39-12）
- 「PE での接続回線と VSI の関連付け」（P.39-13）
- 「MPLS エッジでの H-VPLS」（P.39-14）
- 「VPLS Integrated Routing and Bridging」（P.39-17）
- 「マルチキャスト スヌーピング サポートの設定」（P.39-18）

（注）
- VPLS トラフィックの QoS を設定するには、QoS に関する章の手順を使用します。
- VPLS リンクをプロビジョニングするには、関連する接続回線および VFI を PE にプロビジョニングする必要があります。

CE への PE レイヤ 2 インターフェイスの設定

（注）
- トランク VLAN を定義することが重要です。最初の例に示すように **switchport trunk vlan** コマンドを使用します。
- ローカル ブリッジングのスイッチポートとしてレイヤ 2 インターフェイスを設定する必要があります。CE デバイスからのタグなしトラフィックまたはタグ付きトラフィックを選択するオプションがあります。

CE からタグ付きトラフィックを受け取る 802.1Q トランクの設定

（注）EVCS が設定されている場合、PE ルータでは、宛先 MAC アドレスがレイヤ 2 転送テーブルにあれば、特定の VLAN タグを持つすべてのイーサネット パケットを、ローカル イーサネット インターフェイスまたはエミュレート VC に転送します。

	コマンドまたはアクション	目的
ステップ 1	`Router(config)# interface type number`	設定するインターフェイスを選択します。
ステップ 2	`Router(config)# no ip address ip_address mask [secondary]`	IP 処理をディセーブルにして、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	`Router(config-if)# switchport`	レイヤ 2 スイッチド インターフェイスのスイッチング特性を変更します。
ステップ 4	`Router(config-if)# switchport trunk encapsulation dot1q`	スイッチ ポートのカプセル化形式を 802.1Q に設定します。
ステップ 5	`Router(config-if)# switchport trunk allow vlan vlan_ID`	許可 VLAN のリストを設定します。
ステップ 6	`Router(config-if)# switchport mode trunk`	トランキング VLAN レイヤ 2 インターフェイスへのインターフェイスを設定します。

次に、タグ付きトラフィックを設定する例を示します。

```
Router(config)# interface GigabitEthernet4/4
Router(config)# no ip address
Router(config-if)# switchport
Router(config-if)# switchport trunk encapsulation dot1q
Router(config-if)# switchport trunk allow vlan 501
Router(config-if)# switchport mode trunk
```

次に、show **run** interface コマンドを使用して設定を確認する例を示します。

```
Router# show run interface GigabitEthernet4/4
Building configuration...

Current configuration : 212 bytes
!
```

```
interface GigabitEthernet4/4
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 500-1999
 switchport mode trunk
end
```

CE からタグなしトラフィックを受け取る 802.1Q アクセス ポートの設定

	コマンドまたはアクション	目的
ステップ 1	Router(config)# **interface** *type number*	設定するインターフェイスを選択します。
ステップ 2	Router(config)# **no ip address** *ip_address mask* [**secondary**]	IP 処理をディセーブルにして、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	Router(config-if)# **speed** [**1000** | **nonegotiate**]	イーサネット インターフェイスのポート速度を設定します。ギガビット イーサネット ポートでリンク ネゴシエーション プロトコルをイネーブルまたはディセーブルにします。
ステップ 4	Router(config-if)# **switchport**	レイヤ 2 スイッチド インターフェイスのスイッチング特性を変更します。
ステップ 5	Router(config-if)# **switchport mode access**	インターフェイスを、非トランキング、タグなし、シングル VLAN レイヤ 2 インターフェイス タイプとして設定します。
ステップ 6	Router(config-if)# **switchport access vlan** *vlan_id*	インターフェイスがアクセス モードのときに VLAN を設定します。

次に、タグなしトラフィックを設定する例を示します。

```
Router(config)# interface GigabitEthernet4/4
Router(config)# no ip address
Router(config-if)# speed nonegotiate
Router(config-if)# switchport
Router(config-if)# switchport mode access
Router(config-if)# switchport access vlan 501
```

次に、show **run** interface コマンドを使用して設定を確認する例を示します。

```
Router# show run interface GigabitEthernet4/4
Building configuration...

Current configuration : 212 bytes
!
interface GigabitEthernet4/4
 speed nonegotiate
 switchport
 switchport mode access
 switchport access vlan 501
end
```

すべての VLAN を単一の VPLS インスタンスに配置する Q-in-Q の設定

（注）　TLS を設定すると、MAC アドレスがレイヤ 2 転送テーブルにない場合、PE ルータでは、CE デバイスから受信したすべてのイーサネット パケットを、すべてのローカル イーサネット インターフェイスおよび同じ VPLS ドメインに属するエミュレート VC に転送します。

	コマンドまたはアクション	目的
ステップ 1	`Router(config)# interface type number`	設定するインターフェイスを選択します。
ステップ 2	`Router(config)# no ip address ip_address mask [secondary]`	IP 処理をディセーブルにして、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	`Router(config-if)# speed [1000 | nonegotiate]`	イーサネット インターフェイスのポート速度を設定します。ギガビット イーサネット ポートでリンク ネゴシエーション プロトコルをイネーブルまたはディセーブルにします。
ステップ 4	`Router(config-if)# switchport`	レイヤ 2 スイッチド インターフェイスのスイッチング特性を変更します。
ステップ 5	`Router(config-if)# switchport access vlan vlan_id`	インターフェイスがアクセス モードのときに VLAN を設定します。
ステップ 6	`Router(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 7	`Router(config-if)# l2protocol-tunnel [cdp | stp | vtp]`	インターフェイスでプロトコル トンネリングをイネーブルにします。

次に、タグ付きトラフィックを設定する例を示します。

```
Router(config)# interface GigabitEthernet4/4
Router(config)# no ip address
Router(config-if)# speed nonegotiate
Router(config-if)# switchport
Router(config-if)# switchport access VLAN 501
Router(config-if)# switchport mode dot1q-tunnel
Router(config-if)# l2protocol-tunnel cdp
```

次に、show **run** interface コマンドを使用して設定を確認する例を示します。

```
Router# show run interface GigabitEthernet4/4
Building configuration...

Current configuration : 212 bytes
!
interface GigabitEthernet4/4
 no ip address
 speed nonegotiate
 switchport
 switchport access vlan 501
 switchport mode dot1q-tunnel
 l2protocol-tunnel cdp
end
```

ポートがブロックされた状態にないことを確認するには、**show spanning-tree vlan** コマンドを使用します。

```
Router# show spanning-tree vlan 501
```

```
VLAN0501
Spanning tree enabled protocol ieee
  Root ID    Priority    33269
             Address     0001.6446.2300
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    33269  (priority 32768 sys-id-ext 501)
             Address     0001.6446.2300
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 0

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- --------
--------------------------------
Gi4/4            Desg FWD 4         128.388  P2p
```

特定の VLAN のトラフィックを送受信するように、特定のポートが設定されていることを確認するには、**show vlan id** コマンドを使用します。

```
Router# show vlan id 501

VLAN Name                             Status    Ports
---- -------------------------------- ---------
501  VLAN0501                         active    Gi4/4

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1
Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------
501  enet  100501     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- -----------------
```

PE でのレイヤ 2 VLAN インスタンスの設定

PE にレイヤ 2 VLAN インターフェイスを設定すると、VLAN データベースへの PE ルータ上のレイヤ 2 VLAN インスタンスで、VPLS と VLAN 間のマッピングを設定できるようになります。

	コマンドまたはアクション	目的
ステップ 1	**vlan** *vlan-id* Router(config)# vlan 809	特定の仮想 LAN（VLAN）を設定します。
ステップ 2	**interface vlan** *vlan-id* Router(config)# interface vlan 501	この VLAN にインターフェイスを設定します。

次に、レイヤ 2 VLAN インスタンスを設定する例を示します。

```
Router# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# vlan 501
Router(config)# interface vlan 501
Router(config-if)#
```

VLAN がアップ状態であることを確認するには、**show interfaces vlan** コマンドを使用します（例示なし）。

PE における MPLS の設定

PE に MPLS を設定するには、必須 MPLS パラメータを指定する必要があります。

（注）　MPLS を設定する前に、PE 間に Interior Gateway Protocol（IGP）（Open Shortes Path First（OSPF）または Intermediate System to Intermediate System（IS-IS））を設定にすることにより、すべての PE 間に IP 接続を設定してあることを確認します。

	コマンドまたはアクション	目的
ステップ 1	**enable** Router> enable	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** Router# 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	**mpls label protocol {ldp | tdp}** Router(config)# mpls label protocol ldp	プラットフォームのデフォルト ラベル配布プロトコルを指定します。
ステップ 4	**mpls ldp logging neighbor-changes** Router(config)# mpls ldp logging neighbor-changes	（任意）ネイバーの変更の記録を指定します。
ステップ 5	tag-switching tdp discovery {hello | directed hello} {holdtime | interval} *seconds* Router(config)# tag-switching tdp discovery hello holdtime 5	Transmission of LDP（TDP）discovery hello メッセージの送信間隔、または LDP 転送接続のホールド タイムを設定します
ステップ 6	tag-switching tdp router-id Loopback0 force Router(config)# tag-switching tdp router-id Loopback0 force	MPLS を設定します。

この例では、グローバルな MPLS の設定を示します。

```
Router(config)# mpls label protocol ldp
Router(config)# tag-switching tdp discovery directed hello
Router(config)# tag-switching tdp router-id Loopback0 force
```

LDP ラベルが割り当てられていることを確認するには、**show ip cef** コマンドを使用します。

```
Router# show ip cef 192.168.17.7
192.168.17.7/32, version 272, epoch 0, cached adjacency to POS4/1
0 packets, 0 bytes
  tag information set
    local tag: 8149
    fast tag rewrite with PO4/1, point2point, tags imposed: {4017}
  via 11.3.1.4, POS4/1, 283 dependencies
    next hop 11.3.1.4, POS4/1
    valid cached adjacency
    tag rewrite with PO4/1, point2point, tags imposed: {4017}
```

PE における VFI の設定

仮想スイッチ インスタンス（VFI）は、VPLS ドメインの VPN ID、このドメインにある他の PE ルータのアドレス、および各ピアのトンネル シグナリングのタイプとカプセル化のメカニズムを指定します。（ここで、VSI および関連する VC を作成します）。VFI を次のように設定します。

（注）　MPLS カプセル化だけがサポートされます。

	コマンドまたはアクション	目的

ステップ 1	`l2 vfi name manual`
	
	`Router(config)# l2 vfi vfi17 manual`
		レイヤ 2 VFI 手動コンフィギュレーション モードをイネーブルにします。

ステップ 2	**vpn id** *vpn-id* `Router(config-vfi)# vpn id 17`	VPLS ドメインの VPN ID を設定します。このレイヤ 2 VRF にバインドされたエミュレート VC では、シグナリングにこの VPN ID を使用します。

ステップ 3	`neighbor remote router id {encapsulation mpls} [no-split-horizon]`
	
	`Router(config-vfi)# neighbor 1.5.1.1 encapsulation mpls`
		リモート ピアリング ルータ ID と、エミュレート VC をセット アップするために使用されるトンネル カプセル化タイプまたは疑似配線プロパティを指定します。
		（注）　ブロードキャスト パケットのループを回避し、レイヤ 2 トラフィックを分離するために、スプリット ホライズンが、デフォルト設定です。スプリット ホライズンをディセーブルにし、スポークごとに複数の VC を同じ VFI に設定するには、**no-split-horizon** キーワードを使用します。

ステップ 4	`shutdown`
	
	`Router(config-vfi)# shutdown`
		レイヤ 2 VFI の下にこれまで確立されていたすべてのエミュレート VC を切断して、新しい接続回線の確立を防止します。
		（注）　これは、CLI を使用してレイヤ 2 VFI が設定された新しい接続回線の確立を防止しません。

次に、VFI の設定例を示します。

```
Router(config)# l2 vfi VPLSA manual
Router(config-vfi)# vpn id 100
Router(config-vfi)# neighbor 11.11.11.11 encapsulation mpls
Router(config-vfi)# neighbor 33.33.33.33 encapsulation mpls
Router(config-vfi)# neighbor 44.44.44.44 encapsulation mpls
```

次に、ハブ アンド スポークの VFI の設定例を示します。

```
Router(config)# l2 vfi VPLSA manual
Router(config-vfi)# vpn id 100
Router(config-vfi)# neighbor 9.9.9.9 encapsulation mpls
Router(config-vfi)# neighbor 12.12.12.12 encapsulation mpls
Router(config-vfi)# neighbor 33.33.33.33 encapsulation mpls no-split-horizon
```

show mpls 12transport vc コマンドは、PE1 に関連するさまざまな情報を表示します。

（注）　**show mpls l2transport vc [detail]** コマンドは、次の例のように、PE ルータ上の VC に関する詳細を表示するためにも使用できます。

```
VPLS-PE2# show mpls l2transport vc 201

Local intf     Local circuit        Dest address    VC ID      Status
-------------  -------------------- --------------- ---------- ----------
VFI test1      VFI                  153.1.0.1       201        UP
VFI test1      VFI                  153.3.0.1       201        UP
VFI test1      VFI                  153.4.0.1       201        UP
```

（注）　出力の VC ID は VPN ID を表します。VC は、次の例で示すように、宛先アドレスと VC ID の組み合わせによって識別されます。

show vfi *vfi name* コマンドは、VFI の状態を表示します。

```
nPE-3# show vfi VPLS-2
VFI name: VPLS-2, state: up
  Local attachment circuits:
    Vlan2
  Neighbors connected via pseudowires:
  Peer Address     VC ID     Split-horizon
  1.1.1.1          2             Y
  1.1.1.2          2             Y
  2.2.2.3          2             N
```

PE での接続回線と VSI の関連付け

VFI を定義したら、1 つ以上の接続回線（インターフェイス、サブインターフェイス、または仮想回線）にバインドする必要があります。

	コマンドまたはアクション	目的
ステップ 1	**interface vlan** *vlan-id* Router(config-if)# interface vlan 100	動的なスイッチ仮想インターフェイス（SVI）を作成するか、使用します。
ステップ 2	no ip address Router(config-if)# no ip address	IP 処理をディセーブルにします。（IP アドレスを設定する場合は、VLAN のレイヤ 3 インターフェイスを設定します）。
ステップ 3	**xconnect vfi** *vfi name* Router(config-if)# xconnect vfi vfi16	VLAP ポートにバインドするレイヤ 2 VFI を指定します。

この例は、インターフェイス VLAN コンフィギュレーションを示します。

```
Router(config-if)# interface vlan 100
Router(config-if)# no ip address
Router(config-if)# xconnect vfi VPLS_501
```

VFI ステータスを確認するには、**show vfi** コマンドを使用します。

```
Router# show vfi VPLS_501
VFI name: VPLS_501, state: up
  Local attachment circuits:
    vlan 100
  Neighbors connected via pseudowires:
    192.168.11.1  192.168.12.2  192.168.13.3  192.168.16.6
    192.168.17.7
```

MPLS エッジでの H-VPLS

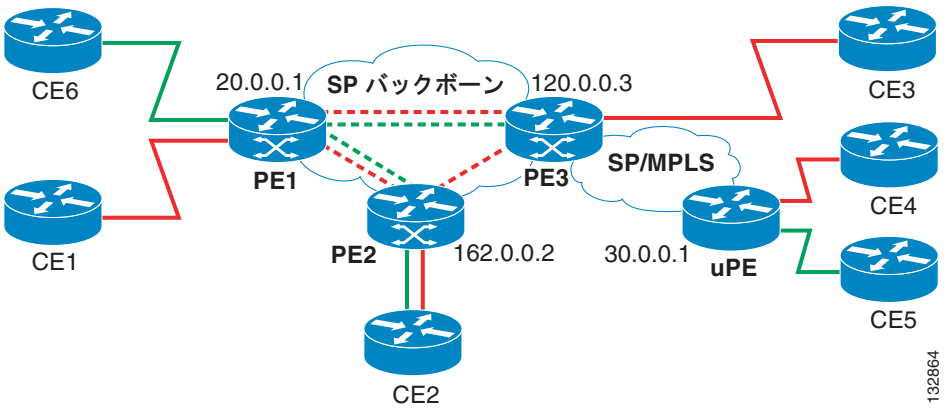
概要

階層型 VPLS のモデルは、ハブ アンド スポークとフルメッシュ ネットワークで構成されます。フルメッシュ コンフィギュレーションでは、各 PE ルータは、VFI を使用して VPLS ドメインの他のすべての PE ルータとのマルチポイントツーマルチポイント転送関係を作成します。

ハブ アンド スポーク構成では、PE ルータは、VLAN にレイヤ 2 ポートを追加する必要なしで VC 間接続を実現する、非スプリットホライズン モードで動作できます。

次の例では、CE1、CE2、CE3、CE4 の VLAN（赤色）は、フルメッシュ ネットワークを介して接続します。CE2、CE5 および ISP POP 上の VLAN は、ISP POP がハブで、CE2 と CE5 がスポークである、ハブ アンド スポーク ネットワークを介して接続します。図 39-2 に設定例を示します。

図 39-2　　H-VPLS 設定



PE1 の設定

VSI および VC の設定

次に、仮想スイッチ インスタンス（VSI）と関連する VC を作成する設定例を示します。緑色の VC では、**no split-horizon** キーワードが必要であることに注意してください。**no split-horizon** コマンドは、データ パスでのデフォルトのレイヤ 2 スプリット ホライズンをディセーブルにします。

```
l2 vfi Internet manual
 vpn id 100
 neighbor 120.0.0.3 encapsulation mpls no-split-horizon
 neighbor 162.0.0.2 encapsulation mpls no-split-horizon

l2 vfi PE1-VPLS-A manual
 vpn id 200
 neighbor 120.0.0.3 encapsulation mpls
 neighbor 162.0.0.2 encapsulation mpls

interface Loopback 0
 ip address 20.0.0.1 255.255.255.255
```

CE デバイス インターフェイスの設定

この設定例は、CE デバイス インターフェイスを示します（単一の VLAN に複数のレイヤ 2 インターフェイスがある場合があります）。

```
interface GigEthernet1/1
 switchport
 switchport mode trunk
 switchport trunk encap dot1q
 switchport trunk allow vlan 1001,1002-1005
```

接続回線と VFI の関連付け

次の設定例は、接続回線（VLAN）を VFI に関連付ける方法を示します。

```
interface Vlan 1001
 xconnect vfi Internet

interface FastEthernet2/1
 switchport
 switchport mode trunk
 switchport trunk encap dot1q
 switchport trunk allow vlan 211,1002-1005

interface Vlan 211
 xconnect vfi PE1-VPLS-A
```

PE2 の設定

VSI および VC の設定

次に、仮想スイッチ インスタンス（VSI）と関連する VC を作成する設定例を示します。

```
l2 vfi Internet manual
 vpn id 100
 neighbor 20.0.0.1 encapsulation mpls
```

```
l2 vfi PE2-VPLS-A manual
 vpn id 200:1
 neighbor 120.0.0.3 encapsulation mpls
 neighbor 20.0.0.1 encapsulation mpls

interface Loopback 0
 ip address 162.0.0.2 255.255.255.255
```

CE デバイス インターフェイスの設定

この設定例は、CE デバイス インターフェイスを示します（単一の VLAN に複数のレイヤ 2 インターフェイスがある場合があります）。

```
interface GigEthernet2/1
 switchport
 switchport mode trunk
 switchport trunk encap dot1q
 switchport trunk allow vlan 211,1001,1002-1005
```

接続回線と VFI の関連付け

次の設定例は、接続回線（VLAN）を VFI に関連付ける方法を示します。

```
interface Vlan 1001
 xconnect vfi Internet

interface Vlan 211
 xconnect vfi PE2-VPLS-A
```

PE3 の設定

VSI および VC の設定

次に、仮想スイッチ インスタンス（VSI）と関連する VC を作成する設定例を示します。

```
l2 vfi Internet manual
 vpn id 100
 neighbor 20.0.0.1 encapsulation mpls
 neighbor 162.0.0.2 encapsulation mpls
 neighbor 30.0.0.1 encapsulation mpls no-split horizon

l2 vfi PE3-VPLS-A manual
 vpn id 200
 neighbor 162.0.0.2 encapsulation mpls
 neighbor 20.0.0.1 encapsulation mpls

interface Loopback 0
 ip address 120.0.0.3 255.255.255.255
```

CE デバイス インターフェイスの設定

この設定例は、CE デバイス インターフェイスを示します（単一の VLAN に複数のレイヤ 2 インターフェイスがある場合があります）。

```
interface GigEthernet6/1
 switchport
 switchport mode trunk
 switchport trunk encap dot1q
 switchport trunk allow vlan 211
```

接続回線の設定

この設定例は、接続回線を示します。

```
interface Vlan 1001
 xconnect vfi Internet

interface Vlan 211
 xconnect vfi PE3-VPLS-A
```

uPE デバイスでのポート ベース EoMPLS の設定

この設定例では、uPE デバイスでのポート ベース EoMPLS を示します。

```
interface GigEthernet 1/1
 xconnect 120.0.0.3 100 encapsulation mpls
```

VPLS Integrated Routing and Bridging

VPLS Integrated Routing and Bridging は、レイヤ 3 トラフィックをルーティングできる他、仮想プライベート LAN サービス（VPLS）マルチポイント PE を使用して、プロバイダー エッジ（PE）デバイス間の疑似配線接続のためにレイヤ 2 フレームをスイッチングできます。フレームをこれらのインターフェイスとの間でルーティングできる機能は、同じスイッチ上のレイヤ 3 ネットワーク（VPN またはグローバル）への疑似配線の終了、またはレイヤ 2 トンネルを介したレイヤ 3 フレームのトンネリング（VPLS）をサポートします。

（注）
- VPLS Integrated Routing and Bridging は、ルーテッド疑似配線およびルーテッド VPLS とも呼ばれます。
- VPLS Integrated Routing and Bridging では、マルチキャスト ルーティングをサポートしていません。

疑似配線のルーティング サポートを設定するには、仮想 LAN（VLAN）インターフェイス設定のレイヤ 3 ドメイン（VPN またはグローバル）の IP アドレスおよびその他のレイヤ 3 機能を設定します。

- 次に、IP アドレス 10.10.10.1 を VLAN 100 インターフェイスに割り当てる例を示します。（レイヤ 2 フォワーディングは VFI VFI100 によって定義されます）。

```
interface vlan 100
  xconnect vfi VFI100
  ip address 10.10.10.1 255.255.255.0
```

- 次の例では、VPN ドメイン VFI200 の IP アドレス 20.20.20.1 を割り当てます。（レイヤ 2 フォワーディングは VFI VFI200 によって定義されます）。

```
interface vlan 200
```

```
xconnect vfi VFI200
ip vrf forwarding VFI200
ip address 20.20.20.1 255.255.255.0
```

マルチキャスト スヌーピング サポートの設定

リリース 15.1(1)SY1 以降のリリースでは、IGMP スヌーピングおよび PIM スヌーピングにより、H-VPLS または Integrated Routing and Bridging（IRB）の場合を除く、VPLS マルチキャスト トラフィックが抑制されます。この機能は、「VPLS PIM and IGMP Snooping (LAN Interfaces)」として Cisco Feature Navigator に表示されます。

VPLS トラフィックでマルチキャスト トラフィックを受信するためには、非 mrouter の PE を含むすべての PE に、レイヤ 2 マルチキャスト エントリを作成する必要があります。マルチキャスト スヌーピングでは、ローカルで受信したすべての IGMP レポートをすべてのピアにフラッディングできます。

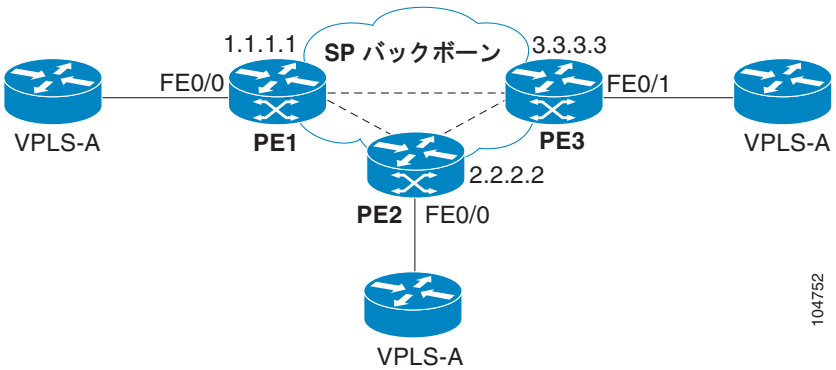
リモート ピアから受信した IGMP レポートや、IGMP スヌーピングによって生成されたレポートなど、ローカルで受信しなかった IGMP レポートを、すべてのピアに対してフラッディングすることはありません。IGMP 脱退、マルチキャスト トラフィックは、レイヤ 2 マルチキャスト エントリがタイムアウトするまで停止しないことがあります。

マルチキャスト スヌーピングのサポートは、platform multicast snooping flood-to-peer コマンドによってデフォルトでイネーブルになっています。

VPLS の設定例

フルメッシュ コンフィギュレーションでは、各 PE ルータは、VFI を使用して VPLS ドメインの他のすべての PE ルータとのマルチポイントツーマルチポイント転送関係を作成します。カスタマー ネットワークから受信したイーサネット パケットまたは VLAN パケットは、1 つ以上のローカル インターフェイスおよび（または）VPLS ドメインのエミュレート VC に転送できます。ネットワークでのブロードキャスト パケットのループを回避するために、エミュレート VC から受信したパケットは、PE ルータの VPLS ドメイン内のどのエミュレート VC にも転送できません。つまり、レイヤ 2 スプリット ホライズンは、フルメッシュ ネットワークでデフォルトとして常にイネーブルにする必要があります。

図 39-3　VPLS の設定例



PE 1 の設定

これは、仮想スイッチ インスタンス（VSI）と関連する VC の作成を示します。

```
l2 vfi PE1-VPLS-A manual
  vpn id 100
  neighbor 2.2.2.2 encapsulation mpls
  neighbor 3.3.3.3 encapsulation mpls
!
interface Loopback 0
  ip address 1.1.1.1 255.255.255.255
```

これは、CE デバイス インターフェイスを設定します（単一の VLAN に複数のレイヤ 2 インターフェイスがある場合があります）。

```
interface FastEthernet0/0
  switchport
  switchport mode dot1qtunnel
  switchport access vlan 100
```

ここで、接続回線（VLAN）は、VSI に関連付けられます。

```
interface vlan 100
  no ip address
 xconnect vfi PE1-VPLS-A
```

これは、レイヤ 2 VLAN インスタンスをイネーブルにします。

```
vlan 100
  state active
```

PE 2 の設定

これは、仮想スイッチ インスタンス（VSI）と関連する VC の作成を示します。

```
l2 vfi PE2-VPLS-A manual
  vpn id 100
  neighbor 1.1.1.1 encapsulation mpls
  neighbor 3.3.3.3 encapsulation mpls
!
interface Loopback 0
  ip address 2.2.2.2 255.255.255.255
```

これは、CE デバイス インターフェイスを設定します（単一の VLAN に複数のレイヤ 2 インターフェイスがある場合があります）。

```
interface FastEthernet0/0
  switchport
  switchport mode dot1qtunnel
  switchport access vlan 100
```

ここで、接続回線（VLAN）は、VSI に関連付けられます。

```
interface vlan 100
  no ip address
 xconnect vfi PE2-VPLS-A
```

これは、レイヤ 2 VLAN インスタンスをイネーブルにします。

```
vlan 100
  state active
```

PE 3 の設定

これは、仮想スイッチ インスタンス（VSI）と関連する VC の作成を示します。

```
l2 vfi PE3-VPLS-A manual
  vpn id 100
  neighbor 1.1.1.1 encapsulation mpls
  neighbor 2.2.2.2 encapsulation mpls
!
interface Loopback 0
  ip address 3.3.3.3 255.255.255.255
```

これは、CE デバイス インターフェイスを設定します（単一の VLAN に複数のレイヤ 2 インターフェイスがある場合があります）。

```
interface FastEthernet0/1
  switchport
  switchport mode dot1qtunnel
  switchport access vlan 100
!
```

ここで、接続回線（VLAN）は、VSI に関連付けられます。

```
interface vlan 100
  no ip address
 xconnect vfi PE3-VPLS-A .
!
```

これは、レイヤ 2 VLAN インスタンスをイネーブルにします。

```
vlan 100
  state active
```

show mpls l2 vc コマンドは、VC のステータス情報を表示します。

```
VPLS1# show mpls l2 vc

Local intf     Local circuit        Dest address    VC ID      Status
-------------  -------------------- --------------- ---------- ----------
Vi1            VFI                  22.22.22.22     100        DOWN
Vi1            VFI                  22.22.22.22     200        UP
Vi1            VFI                  33.33.33.33     100        UP
Vi1            VFI                  44.44.44.44     100        UP
Vi1            VFI                  44.44.44.44     200        UP
```

show vfi コマンドは VFI に関する情報を表示します。

```
PE-1# show vfi PE1-VPLS-A
VFI name: VPLSA, state: up
  Local attachment circuits:
    Vlan100
  Neighbors connected via pseudowires:
    2.2.2.2  3.3.3.3
```

show mpls 12transport vc コマンドは、仮想回線に関する情報を表示します。

```
Router# show mpls l2 vc det
Local interface: VFI vfi17 up
  Destination address: 1.3.1.1, VC ID: 17, VC status: up
    Tunnel label: imp-null, next hop point2point
    Output interface: PO3/4, imposed label stack {18}
  Create time: 3d15h, last status change time: 1d03h
  Signaling protocol: LDP, peer 1.3.1.1:0 up
    MPLS VC labels: local 18, remote 18
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    Remote interface description:
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 0, send 0
    byte totals:   receive 0, send 0
    packet drops:  receive 0, send 0
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

A-VPLS の設定

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

A-VPLS の前提条件

なし。

A-VPLS の制約事項

- 次に、サポートされる設定を示します。
  - 転送 vpls モードでの **neighbor** コマンドによる PE ルータの設定の MPLS コア。
  - 明示パスを使用した MPLS トラフィック エンジニアリング トンネル経由の PE ルータの設定を持つ MPLS コア。
  - MPLS over GRE トンネルを介した PE ルータの設定の IP コア。

  route-via コマンドの使用、BGP オートディスカバリ、PE 出力ポートへの VLAN の明示的な割り当てなど、他の設定方法はサポートされていません。
- A-VPLS のサポート対象は次のとおりです。
  - 最大 32 個の EtherChannel ポートチャネル インターフェイス。
  - **load-balance flow** コマンドで設定されているネイバーの数を引いた最大 60 の VPLS ネイバー。
- A-VPLS には、ノンストップ フォワーディングおよびステートフル スイッチオーバーが必要です。
- A-VPLS は次の機能と連動します。
  - 明示パスが設定されている MPLS トラフィック エンジニアリング トンネル。
  - トンネル宛先へのスタティック ルートが設定された総称ルーティング カプセル化（GRE トンネル）。

  MPLS トラフィック エンジニアリングおよび GRE トンネルの詳細については、次のマニュアルを参照してください。
  - *MPLS トラフィック エンジニアリングおよび拡張機能*
  - *トンネルの実装*
- Any Transport over MPLS Virtual Circuit Connection Verification（VCCV）機能をサポートする **ping** コマンドや **traceroute** コマンドは、FAT 疑似配線上ではサポートされません。
- VPLS オートディスカバリ機能は、A-VPLS でサポートされません。
- コア ルータでは、パケット転送にコアが IP を使用する場合、ロード バランシングはサポートされません。

A-VPLS について

A-VPLS では、VPLS に次の機能拡張を追加しています。

- 複数の等価コスト コア方向パス間のプロバイダー エッジ（PE）とコア インターフェイスでフローラベルを使用してトラフィックをロード バランシングする機能。
- 冗長 PE ルータのサポート。

A-VPLS では、Flow Aware Transport（FAT）疑似配線機能を使用して PE およびコア ルータ両方の PE 冗長性とロード バランシングを実現します。等価コスト マルチ パスが使用されている場合 FAT の疑似配線がコア トラフィックをロード バランシングするために使用されます。PE ルータは、各パケット（フロー ラベル）に追加の MPLS ラベルを追加します。各フローに一意のフロー ラベルがあります。FAT 疑似配線の詳細については、PWE3 インターネットドラフト『*Flow Aware Transport of MPLS Pseudowires*』（draft-bryant-filsfils-fat-pw）を参照してください。

A-VPLS の設定方法

ECMP および FAT 疑似配線によるロード バランシングのイネーブル化

次の手順は、プロバイダー エッジ（PE）ルータでロード バランシングを設定してコアの P ルータでイネーブルにする方法について説明します。コア P ルータで設定は不要です。

エッジ ルータでロード バランシングをイネーブルにするには、**load-balance flow** コマンドを発行します。ロード バランシング規則は **port-channel load-balance** コマンドのパラメータで設定されます（「Port-Channel Load-Balancing のイネーブル化」（P.40-4）を参照）。

コアのロード バランシングをイネーブルにするには、両方の PE ルータで **flow-label enable** コマンドを発行します。**load-balance flow** コマンドと **flow-label enable** コマンドを組み合わせて発行する必要があります。

	コマンド	目的
ステップ 1	`Router> 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	`Router# 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	`Router(config)# pseudowire-class` *name*	指定した名前の疑似回線クラスを確立して、疑似回線クラス コンフィギュレーション モードに入ります。
ステップ 4	`Router(config-pw)# encapsulation mpls`	MPLS トンネリングのカプセル化タイプを指定します。
ステップ 5	`Router(config-pw)# load-balance flow`	ECMP のロード バランシングをイネーブルにします。
ステップ 6	`Router(config-pw)# flow-label enable`	疑似配線のフロー ラベルのインポジションおよびディスポジションをイネーブルにします。
ステップ 7	`Router(config-pw)# end`	疑似回線クラス コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

Port-Channel Load-Balancing のイネーブル化

次の作業では、ポート チャネルのロードバランシングをイネーブルにする方法について説明します。ここでは、バンドル内のポート間での負荷分散方式を設定します。**port-channel load-balance** コマンドが設定されていない場合、ロードバランシングはデフォルトのパラメータを使用して行われます。

	コマンド	目的
ステップ 1	`Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	`Router# 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	`Router(config)# port-channel load-balance` *method*	バンドル内のポート間での負荷分散方式を指定します。
ステップ 4	`Router(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

仮想イーサネット インターフェイス設定の一部としての明示的な PE ルータ指定

トラフィックが通過する必要があるルートを指定するには、いくつかの方法があります。

- PE ルータの仮想イーサネット インターフェイスの設定の一部としての明示的な指定
- MPLS トラフィック エンジニアリング トンネルの設定
- GRE トンネルの設定

次の作業では、仮想イーサネット インターフェイス コンフィギュレーションの一部として PE ルータを明示的に指定する方法について説明します。

	コマンド	目的
ステップ 1	`Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	`Router# 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	`Router(config)# interface virtual-ethernet` *num*	仮想イーサネット インターフェイスを作成し、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 4	`Router(config-if)# transport vpls mesh`	疑似配線のフル メッシュを作成して、VPLS 転送モードを開始します。
ステップ 5	`Router(config-if-transport)# neighbor` *remote-router-id* [**pw-class** pw-class-name]	疑似配線で使用される PE ルータを指定します。
ステップ 6	`Router(config-if-transport)# exit`	VPLS 転送コンフィギュレーション モードを終了し、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 7	`Router(config-if)# switchport`	ポートをレイヤ 2 スイッチング用に設定します。
ステップ 8	`Router(config-if)# switchport mode trunk`	永続的なトランキング モードをイネーブルにし、リンクをトランク リンクに変換するようにネゴシエーションを行います。

	コマンド	目的
ステップ 9	`Router(config-if)# switchport trunk allowed vlan {add | except | none | remove} vlan [,vlan[,vlan[,...]]]`	トランク上で許可される VLAN のリストを設定します。
ステップ 10	`Router(config)# 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、特権 EXEC モードを開始します。

MPLS トラフィック エンジニアリング トンネルの設定

トラフィックが通過する必要があるルートを指定するには、いくつかの方法があります。

- PE ルータの仮想イーサネット インターフェイスの設定の一部としての明示的な指定
- MPLS トラフィック エンジニアリング トンネルの設定
- GRE トンネルの設定

次の作業では、MPLS トラフィック エンジニアリング トンネルを設定する方法について説明します。MPLS トラフィック エンジニアリング トンネルの詳細については、『*MPLS Traffic Engineering and Enhancements*』を参照してください。

	コマンド	目的
ステップ 1	`Router> 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	`Router# 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	`Router(config)# interface tunnel number`	インターフェイス タイプを設定し、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 4	`Router(config-if)# ip unnumbered type number`	トンネル インターフェイスに IP アドレスを割り当てます。MPLS トラフィック エンジニアリング トンネル インターフェイスは単一方向リンクを表すため、番号なしにする必要があります。
ステップ 5	`Router(config-if)# tunnel destination ip-address`	トンネルの宛先を指定します。*ip-address* キーワードは、ホスト宛先の IP アドレス（ドット付き 10 進表記）です。
ステップ 6	`Router(config-if)# tunnel mode mpls traffic-eng`	トンネル カプセル化モードを MPLS トラフィック エンジニアリングに設定します。
ステップ 7	`Router(config-if)# tunnel mpls traffic-eng autoroute announce`	拡張 SPF 計算でトンネルを使用するように IGP を設定します。
ステップ 8	`Router(config-if)# tunnel mpls traffic-eng path-option number {dynamic | explicit {name path-name} | identifier path-number} [lockdown]`	指定した IP 明示パス、またはトラフィック エンジニアリング トポロジ データベースからダイナミックに計算されたパスを使用するように、トンネルを設定します。明示パスが現在使用可能でない場合は、ダイナミック パスが使用されます。
ステップ 9	`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、特権 EXEC モードに戻ります。

GRE トンネルの設定

トラフィックが通過する必要があるルートを指定するには、いくつかの方法があります。

- PE ルータの仮想イーサネット インターフェイスの設定の一部としての明示的な指定
- MPLS トラフィック エンジニアリング トンネルの設定
- GRE トンネルの設定

次の作業では、GRE トンネルの設定方法について説明します。GRE トンネルの詳細については、『*Implementing Tunnels*』を参照してください。

	コマンド	目的
ステップ 1	`Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	`Router# 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	`Router(config)# interface type number`	インターフェイスのタイプと番号を指定し、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。トンネルを設定するには、type 引数に **tunnel** を使用します。
ステップ 4	`Router(config-if)# tunnel mode {gre ip | gre multipoint}`	トンネルで使用されるカプセル化プロトコルを指定します。
ステップ 5	`Router(config-if)# mpls ip`	トンネルの MPLS をイネーブルにします。
ステップ 6	`outer(config-if)# tunnel source {ip-address | interface-type interface-number}`	トンネル送信元を設定します。 • 送信元 IP アドレスを指定するには、*ip-address* 引数を使用します。 • 使用するインターフェイスを指定する場合は、*interface-type* 引数および *interface-number* 引数を使用します。 **（注）** トンネルの送信元および宛先 IP アドレスの両方の PE ルータで定義する必要があります。
ステップ 7	`Router(config-if)# tunnel destination {hostname | ip-address}`	トンネル宛先を設定します。 • ホストの宛先の名前を指定するには、hostname 引数を使用します。 • ホストの宛先の IP アドレスを指定する場合は、ip-address 引数を使用します。 **（注）** トンネルの送信元および宛先 IP アドレスの両方の PE ルータで定義する必要があります。
ステップ 8	`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、特権 EXEC モードに戻ります。
ステップ 9	`Router(config)# ip route ip-address tunnel num`	スタティック ルートを作成します。

次の例は、3 つのサポートされる A-VPLS 設定方法を示します。

明示的なピア PE ルータの指定

次に、VLAN 10 および 20 で 2 つの VPLS ドメインを作成する例を示します。各 VPLS ドメインには、ピア PE ルータ 10.2.2.2 および 10.3.3.3 への 2 つの疑似配線が含まれます。ロード バランシングは、**load-balance flow** コマンドと **flow-label enable** コマンドでイネーブルにします。

```
pseudowire-class cl1
   encap mpls
   load-balance flow
   flow-label enable
!
port-channel load-balance src-mac
!
interface virtual-ethernet 1
   transport vpls mesh
      neighbor 10.2.2.2 pw-class cl1
      neighbor 10.3.3.3 pw-class cl1
   switchport
   switchport mode trunk
   switchport trunk allowed vlan 10, 20
```

MPLS トラフィック エンジニアリング トンネルの使用方法

次の例では、2 つの VPLS ドメインの作成を示し、MPLS トラフィック エンジニアリング トンネルを使用して明示パスを指定します。

```
pseudowire-class cl1
   encap mpls
   load-balance flow
   flow-label enable
!
port-channel load-balance src-mac
!
interface Tunnel1
   ip unnumbered Loopback0
   tunnel mode mpls traffic-eng
   tunnel destination 192.168.1.1
   tunnel mpls traffic-eng autoroute announce
   tunnel mpls traffic-eng path-option 1 explicit name LSP1
!
ip explicit-path name LSP1 enable
   next-address 192.168.2.2
   next-address loose 192.168.1.1
!
interface Tunnel2
   ip unnumbered Loopback0
   tunnel mode mpls traffic-eng
   tunnel destination 172.16.1.1
   tunnel mpls traffic-eng autoroute announce
   tunnel mpls traffic-eng path-option 1 explicit name LSP2
!
ip explicit-path name LSP2 enable
   next-address 172.16.2.2
   next-address loose 172.16.1.1
!
interface virtual-ethernet 1
    transport vpls mesh
      neighbor 10.2.2.2 pw-class cl1
      neighbor 10.3.3.3 pw-class cl1
   switchport
   switchport mode trunk
   switchport trunk allowed vlan 10,20
```

MPLS over GRE トンネルの使用方法

次に、VLAN 10 および 20 で 2 つの VPLS ドメインを作成する例を示します。各 VPLS ドメインには、ピア PE 10.2.2.2 および 10.3.3.3 への 2 つの疑似配線が含まれます。疑似配線はコアが IP であるため MPLS over GRE トンネルです。

```
pseudowire-class cl1
   encap mpls
   load-balance flow
!
port-channel load-balance src-mac
!
interface tunnel 1
   tunnel mode gre ip
   mpls ip
   tunnel source 10.1.1.1
   tunnel destination 10.2.2.2
!
interface tunnel 2
   tunnel mode gre ip
   mpls ip
   tunnel source 10.1.1.1
   tunnel destination 10.3.3.3
!
interface virtual-ethernet 1
   transport vpls mesh
      neighbor 10.2.2.2 pw-class cl1
      neighbor 10.3.3.3 pw-class cl1
   switchport
   switchport mode trunk
   switchport trunk allowed vlan 10, 20

ip route 10.2.2.2 255.255.255.255 Tunnel1
ip route 10.3.3.3 255.255.255.255 Tunnel2
```

ルーテッド Pseudo-Wire（RPW）およびルーテッド VPLS

RPW およびルーテッド VPLS はレイヤ 3 トラフィックをルーティングし、プロバイダー エッジ（PE）デバイス間の疑似配線接続でレイヤ 2 フレームを切り替えることができます。Ethernet over MPLS（EoMPLS）の形式のポイントツーポイント PE 接続、および Virtual Private LAN Service（VPLS）マルチポイント PE 接続の両方がサポートされます。フレームをこれらのインターフェイスとの間でルーティングできる機能は、同じスイッチ上のレイヤ 3 ネットワーク（VPN またはグローバル）への疑似配線の終了、またはレイヤ 2 トンネルを介したレイヤ 3 フレームのトンネリング（EoMPLS または VPLS）をサポートします。この機能は、MPLS トラフィック エンジニアリング（MPLS-TE）および高速再ルーティング（FRR）機能を介して物理インターフェイスまたはデバイスの障害時のネットワーク収束をサポートします。特に、機能は、VPLS ドメイン上のレイヤ 3 マルチキャストの MPLS TE-FRR 保護をイネーブルにします。

（注） RPW が A-VPLS モードで設定されている場合、TE/FRR は A-VPLS が ECMP 上で実行され、ECMP 収束が TE/FRR と同等であるため、サポートされません。

疑似配線のルーティング サポートを設定するには、仮想 LAN（VLAN）インターフェイス設定のレイヤ 3 ドメイン（VPN またはグローバル）の IP アドレスおよびその他のレイヤ 3 機能を設定します。次に、VLAN 100 インターフェイスに IP アドレス 10.10.10.1 を割り当て、マルチキャスト PIM をイネーブルにする例を示します。（レイヤ 2 フォワーディングは VFI VFI100 によって定義されます）。

```
interface vlan 100
  xconnect vfi VFI100
  ip address 10.10.10.1 255.255.255.0
  ip pim sparse-mode
```

次の例では、VPN ドメイン VFI200 の IP アドレス 20.20.20.1 を割り当てます。（レイヤ 2 フォワーディングは VFI VFI200 によって定義されます）。

```
interface vlan 200
  xconnect vfi VFI200
  ip vrf forwarding VFI200
  ip address 20.20.20.1 255.255.255.0
```

Ethernet Virtual Connections（EVC; イーサネット バーチャル コネクション）

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

EVC の前提条件

なし。

EVC の制約事項

- LACP EtherChannel と 802.1ad プロバイダー ブリッジ モードは相互に排他的です。802.1ad プロバイダー ブリッジ モードがイネーブルの場合、LACP EtherChannel はトラフィックを送信できません。
- スイッチあたりの最大 EFP：10K。
- ブリッジ ドメインごとの最大 EFP：124。
- インターフェイスごとの最大 EFP：4K。
- スイッチあたりの最大ブリッジ ドメイン：4K。
- ブリッジ ドメインの設定は、EVC サービス インスタンスの設定の一部としてだけサポートされます。
- EVC をサポートするための前提条件は、次のとおりです。
  - スパニングツリー モードは MST である必要があります。
  - **dot1ad** グローバル コンフィギュレーション モード コマンドを設定する必要があります。
- サービス インスタンスは、**switchport nonegotiate** コマンドによって、無条件トランクとして設定されたポートでだけ設定できます。
- EVC ポートをサポートするために、PFC QoS を設定できます。
- サポートされる EVC 機能には、次のものがあります。
  - サービス インスタンス：イーサネット インターフェイスで EFP サービス インスタンスを作成、削除、変更します。
  - EVC のイーサネット サービスの保護。
    - イーサネット運用管理およびメンテナンス（EOAM）
    - 接続障害管理（CFM）
    - イーサネット ローカル管理インターフェイス（E-LMI）
  - IPv6 アクセス コントロール リスト（ACL）。
  - カプセル化：802.1Q VLAN（1 つの VLAN または VLAN のリストまたは範囲）に基づいて EFP にトラフィックをマッピングできます。
  - ブリッジ ドメインのメンバーとして EFP を設定できます。
  - ブリッジ ドメインでは、対称的なプッシュのみをサポートしています。サポートされている書き換え設定は、出力のプッシュ（タグの追加）を意味しています
  - ブリッジ ドメインは入力書き換えをサポートしています
  - EVC 転送
  - MAC アドレス ラーニングおよびエージング
  - EtherChannel の EVC
  - EVC MAC アドレス セキュリティ
  - スイッチポートと EFP のブリッジング
  - MSTP（EVC ブリッジ ドメインの MST）
  - EFP の統計情報（パケット数およびバイト数）
  - サービス インスタンス単位の QoS 対応 EVC/EFP

- 次のレイヤ 2 ポート ベースの機能は、ポートに設定された EVC で動作可能です。
  - PAGP
  - LACP
  - UDLD
  - LLDP
  - CDP
  - MSTP
- 次の機能は、EVC でサポートされていません。
  - レイヤ 2 マルチキャスト フレームのフラッディング
  - レイヤ 2 プロトコル トンネリング
  - QinQ タギング
  - VLAN 変換
  - Ethernet over MPLS（EoMPLS）
  - ブリッジ ドメイン ルーティング
  - スプリット ホライズン
  - サービス インスタンス グループ。別称は、イーサネット フロー ポイント（EFP）グループ
  - IPv6 アクセス コントロール リスト（ACL）

EVC について

EVC の概要

イーサネット仮想回線（EVC）は、イーサネット サービスをサポートするレイヤ 2 のブリッジング アーキテクチャを定義します。EVC は、サービス プロバイダー ネットワーク内のポイントツーポイントまたはマルチポイントツーマルチポイントのパスを識別する複数のユーザ ネットワーク インターフェイス間の関連付けとして Metro Ethernet Forum（MEF）によって定義されます。EVC は、サービス プロバイダー ネットワーク内の概念的なサービス パイプです。ブリッジ ドメインは、VLAN とは別に存在するローカル ブロードキャスト ドメインです。

イーサネット フロー ポイント

イーサネット フロー ポイント（EFP）サービス インスタンスは、物理ポートまたは EtherChannel にブリッジ ドメインを接続する論理インターフェイスです。レイヤ 2 ポートにサービス インスタンスを設定すると、EVC 機能を設定する疑似ポートまたは EFP が作成されます。各サービス インスタンスは、インターフェイスごとに一意の番号を持ちますが、異なるポート上のサービス インスタンス同士は関係を持たないため、異なるインターフェイスで同じ番号を使用できます。

EFP は、ユーザ定義の基準に基づいて、同じ物理ポートからのフレームを、そのポートに関連付けられた複数のサービス インスタンスの 1 つに分類します。各 EFP に、異なる転送アクションと動作を関連付けることができます。

EFP の 3 つの主な特性（またはパラメータ）は次のとおりです。

- カプセル化
- 書き換え情報
- 転送インスタンスまたは方式（ブリッジ ドメインまたは xconnect）

EVC ブロードキャスト ドメインは、ブリッジ ドメインおよびこれに接続されている EFP によって決まります。着信フレームは、インターフェイスの EFP 一致基準と照合され、一致する EFP で学習されて、ブリッジ ドメイン内の 1 つまたは複数の EFP に転送されます。一致する EFP がない場合、フレームはドロップされます。

EFP は、VLAN 変換を設定するために使用できます。たとえば、同じインターフェイスから出力に対する 2 つの EFP がある場合、異なる VLAN 書き換え処理を各 EFP に設定できます。これは、従来のスイッチ ポート VLAN 変換モデルよりも柔軟です。

EFP が作成されたとき、初期状態は UP です。次の状況では、状態が DOWN に変わります。

- ユーザが EFP を明示的にシャット ダウンする。
- EFP が関連付けられているメイン インターフェイスが停止しているか、削除されている。
- EFP がブリッジ ドメインに属する場合に、そのブリッジ ドメインが停止している。
- EFP が、特定の機能の問題防止手段として、強制停止されている。

サービス インスタンスおよび EFP

レイヤ 2 ポートまたは EtherChannel にサービス インスタンスを設定すると、EVC 機能を設定する疑似ポートまたはイーサネット フロー ポイント（EFP）が作成されます。各サービス インスタンスは、インターフェイスごとに一意の番号を持ちますが、異なるポート上のサービス インスタンス同士は関係を持たないため、異なるインターフェイスで同じ番号を使用できます。

ethernet evc *evc-id* 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 EVC を定義してあれば、EVC をサービス インスタンスと関連付けることができます（任意）。サービス インスタンスのデフォルトの動作はありません。サービス インスタンスは、許可 VLAN が設定されていないトランク ポートにのみ設定できます。その他の設定は許可されません。インターフェイスにサービス インスタンスを設定してある場合は、このインターフェイスでは switchport コマンドが許可されません。サービス インスタンスは、EtherChannel グループにも設定できます。

レイヤ 2 インターフェイスまたは EtherChannel に EFP を作成し、サービス インスタンス コンフィギュレーション モードを開始するには、**service instance** *number* **ethernet** [*name*] インターフェイス コンフィギュレーション コマンドを使用します。サービス インスタンス コンフィギュレーション モードは、インターフェイス単位でサービス インスタンスに適用される、管理プレーンとコントロール日付プレーンのすべての属性とパラメータを設定するために使用します。

- **service instance***number* は EFP ID で、1 ～ 4000 の整数です。
- オプションの **ethernet** *name* は事前に設定された EVC 名です。EVC *name* の入力は不要ですが、**ethernet** の入力は必要です。同じ EVC に対応するときは、異なる EFP に同じ名前を指定できます。EFP は、共通名を使用してグローバル EVC に関連付けられます。

サービス インスタンス コンフィギュレーション モードを開始すると、次のオプションを設定できます。

- **default**：コマンドをデフォルトに設定します
- **description**：サービス インスタンス固有の説明を追加します
- **encapsulation**：イーサネット フレームの一致基準を設定します
- **errdisable**：エラー ディセーブルを設定します
- **ethernet**：イーサネット LMI パラメータを設定します
- **exit**：サービス インスタンス コンフィギュレーション モードを終了します
- **l2protocol**：レイヤ 2 制御プロトコル処理を設定します
- **mac**：MAC アドレス ベースの機能のコマンド
- **no**：コマンドを無効にするか、デフォルト設定にします。
- **service-policy**：EFP にポリシーマップを対応付けます
- **shutdown**：サービス インスタンスをアウト オブ サービス状態にします

サービス インスタンスをシャット ダウンまたは起動するには、[**no**] **shutdown** サービス インスタンス コンフィギュレーション モードを開始します。

サービス インスタンスの設定されていないレイヤ 2 ポートでは、複数の **switchport** コマンドを使用できます（**access**、**backup**、**block**、**host**、**mode**、および **trunk**）。1 つまたは複数のサービス インスタンスがレイヤ 2 ポートに設定されている場合、このインターフェイスでは、いずれの **switchport** コマンドも受け入れません。

カプセル化（フレキシブル サービス マッピング）

カプセル化では、次の要素の任意の組み合わせをサービス インスタンスにマッピングする一致基準を定義します。

- VLAN
- VLAN の範囲
- サービス クラス（CoS）ビット
- Ethertype

VLAN タグと CoS には、単一の値、範囲、またはリストを指定できます。Ethertype には、単一のタイプまたはタイプのリストを指定できます。次のカプセル化タイプがあります。

- default
- dot1q
- priority-tagged

- untagged

プライオリティ タグ付きフレームは常に一重タグ付きです。すべてのイーサネット トラフィックがサポートされます。次のカプセル化分類オプションがあります。

- 内部タグ CoS
- 内部タグ VLAN

カプセル化方式を設定すると、フレキシブル サービス マッピングが可能になります。これにより、設定したカプセル化方式に基づき、EFP に着信パケットをマッピングできます。

外部 802.1q VLAN タグ値に基づくフレキシブル サービス マッピングのデフォルト動作は、nonexact です。これは、EFP カプセル化の設定で内部（第 2）VLAN タグ一致基準を指定していない場合、フレームが外部 VLAN タグ値の条件を満たす限り、ソフトウェアでは、一重タグ付きフレームと二重タグ付きフレームの両方を、この EFP にマッピングすることを意味します。コマンドライン インターフェイス（CLI）では、**exact** キーワードを使用した正確なマッピングを指定できます。このキーワードを指定した場合、EFP は一重タグ付きフレーム専用として指定され、二重タグ付きフレームは、この EFP に分類されません。

サービス インスタンス コンフィギュレーション モードで CLI **encapsulation** コマンドを使用すると、カプセル化の基準を設定できます。EFP（サービス インスタンス）ごとに encapsulation コマンドを 1 つ設定する必要があります。カプセル化方式を設定してあると、サービス インスタンス コンフィギュレーション モードで、次のコマンドを使用できます。

- **bridge-domain**：ブリッジ ドメインを設定します。
- **rewrite**：イーサネット書き換え基準を設定します。

表 41-1　サポートされているカプセル化タイプ

コマンド	説明
encapsulation dot1q {**any** | *vlan-id* [**,***vlan-id* [**-***vlan-id*]]}	インターフェイス上の入力 802.1q フレームを、適切な EFP にマッピングするために使用する照合基準を定義します。オプションは、単一 VLAN、VLAN の範囲、または VLAN か VLAN 範囲のリストです。VLAN ID は 1 ～ 4094 です。 • すべての VLANS（1 ～ 4094）と一致させるには、**any** キーワードを入力します。 • 最も外側のタグとの完全一致には単一の VLAN ID を入力します。 • 最も外側の範囲との一致には VLAN の範囲を入力します。
encapsulation dot1q *vlan-id* **cos** *cos-value*	CoS 値のカプセル化は、C タグの CoS を組み込んだあとの一致基準を定義します。CoS 値は、1 ～ 7 の間の 1 桁です。 CoS カプセル化は、**encapsulation untagged** コマンドによって設定できませんが、**encapsulation priority-tagged** コマンドを使用して設定できます。結果は、最も外側で完全一致する VLAN および CoS です。VLAN の範囲も使用できます。
encapsulation untagged	インターフェイスに入るタグなしイーサネット フレームを適切な EFP にマッピングするために使用する一致基準。 タグなしカプセル化は、ポートあたり 1 つの EFP のみに設定できます。ただし、タグなしトラフィックと一致する EFP を持つポートでは、タグ付きフレームと一致する他の EFP も持つことができます。 **（注）** **encapsulation priority-tagged** コマンドとともにはサポートされません。

表 41-1　サポートされているカプセル化タイプ （続き）

コマンド	説明
encapsulation priority-tagged	プライオリティ タグ付きフレームを指定します。プライオリティ タグ付きパケットは VLAN ID 0 および CoS 値 0 ～ 7 を持ちます。 （注）　**encapsulation untagged** コマンドとともにはサポートされません。
encapsulation default	他に一致する基準のないすべてのパケットと一致するデフォルト EFP をポートに設定します。ポートにデフォルト EFP のみが設定されている場合は、このポートのすべての入力フレームに一致します。 ポートにデフォルト EFP を設定した場合は、同じブリッジ ドメインを持つ他の EFP を同じポートに設定できません。

ポートに入るパケットがそのポートでカプセル化のいずれとも一致しない場合、パケットはドロップされるため、パケットをフィルタリングすることになります。フィルタリング基準を決めるためには、カプセル化は、ネットワーク上のパケットと一致する必要があります。ネットワーク上で、スイッチに入る書き換え前のパケットおよびスイッチから出る書き換え後のパケットを参照します。

EFP および MSTP

EFP ブリッジ ドメインは、マルチ スパニングツリー プロトコル（MSTP）によってでサポートされています。次の制限は、ブリッジ ドメインとともに STP を実行する場合に適用されます。

- 1 つのブリッジ ドメインにマッピングされたすべての着信 VLAN（最も外側または単一）は、同じ MST インスタンスに属する必要があり、そうでない場合、ループが発生するおそれがあります。
- 同じ MST インスタンスにマッピングされたすべての EFP について、ポートをブロックする STP が原因で接続が切断されないように、すべての冗長パスにバックアップ EFP を設定する必要があります。
- STP モードが PVST+ または PVRST の場合、EFP の情報はプロトコルに渡されません。EVC は MSTP だけをサポートします。
- マルチキャスト ポートの STP モードを MST から PVST+ または PVRST に変更することは許可されません。

ブリッジ ドメイン

ブリッジ ドメインの概要

ブリッジ ドメインは、プラットフォーム内部のブロードキャスト ドメインを定義し、VLAN からブロードキャスト ドメインを分離できます。この分離により、ポートごとの VLAN シグニフィカンスが可能になるため、単一のデバイスごとの VLAN ID 空間に関連する拡張性の制限がなくなります。ブリッジ ドメインに参加している EFP の 1 つから受信した、一致するフレームは、ブリッジングされます。

サービス インスタンスをブリッジ ドメインに対応付ける必要があります。ブリッジ ドメインのフラッディングおよび通信の動作は VLAN ドメインの動作と似ています。ブリッジ ドメイン メンバーシップは、ブリッジ ドメインに加入しているサービス インスタンスによって決まる一方で（カプセル化の基準に基づく）、VLAN ドメイン メンバーシップは、パケット内の VLAN タグによって決まります。

（注）　ブリッジ ドメインを設定する前に、カプセル化を設定する必要があります。

IGMP スヌーピングはスイッチとすべての VLAN で、デフォルトでイネーブルですが、4094 未満のブリッジ ドメインを設定すると VLAN で自動的にディセーブルになります。スイッチでは、ブリッジ ドメインを 124 個までサポートします。

イーサネット MAC アドレス ラーニング

MAC アドレス ラーニングは常にイネーブルになっており、ディセーブルにできません。

未知の MAC アドレスおよびブロードキャスト アドレスのレイヤ 2 フレームのフラッディング

不明なユニキャストまたはブロードキャストの宛先 MAC アドレスを持つレイヤ 2 フレームは、発信元 EFP を除く、ブリッジ ドメイン内のすべての EFP にフラッディングされます。

フレームのレプリケーションではフレームを複数回再循環させることが必要です。再循環は、転送のパフォーマンスに悪影響を与え、全機能のパケット転送率が下がります。

レイヤ 2 宛先 MAC アドレス ベースの転送

ブリッジングが設定されている場合、EFP から受信したユニキャスト フレームは宛先レイヤ 2 MAC アドレスに基づいて転送されます。宛先アドレスがわかっている場合、フレームは宛先アドレスに関連付けられた EFP/NNI だけに転送されます。

ブリッジと EFP 設定は相関しているため、ブリッジングは EFP でのみサポートされます。複数のブリッジ ドメインをサポートするために、MAC アドレス エントリが EFP のブリッジ ドメインと関連付けられます。動的に学習する必要があるのは、ユニキャスト MAC アドレスだけです。

EVC インフラストラクチャはフレームの内容を変更しません。

MAC アドレス エージング

MAC テーブルの動的に学習された MAC アドレス エントリは、定期的にエージング アウトされ、設定した期間を超えて非アクティブなエントリは、テーブルから削減されます。エージング タイム値のサポート範囲は、5 ～ 1000000 秒で、粒度は 1 秒単位です。デフォルトは 8 分です。**aging-time** パラメータはブリッジ ドメインごとに設定でき、相対値です。この値は、フレームがその MAC アドレスとともに受信された時刻に対する相対エージング タイムです。

MAC Address Table

MAC アドレス テーブルは、レイヤ 2 宛先 MAC アドレスに基づいてフレームを転送するために使用されます。テーブルには、ルート プロセッサ（RP）からダウンロードされたスタティック MAC アドレスと、データ パスによって動的に学習された MAC アドレスから構成されます。

MAC 学習機能をイネーブルにした状態で、データ パスで新しい一意の MAC アドレスを学習するとエントリが MAC テーブルに追加され、エージング アウトするとエントリがテーブルから削除されます。

書き換え処理

rewrite コマンドは 802.1ad クラウドでパケットを転送するために入力パケットに 802.1ad タグをプッシュします。

EFP に着信するフレームに追加の dot1ad タグのカプセル化を指定するには、**rewrite ingress tag push dot1ad** *vlan-id* **symmetric** サービス インスタンス コンフィギュレーション モード コマンドを入力します。

（注）　設定への書き換えを完了するには、**symmetric** キーワードが必要です。

symmetric キーワードを入力した場合、出力側の対応する処理では、逆のアクションを実行し、カプセル化 VLAN をプッシュ（追加）します。

レイヤ 3 およびレイヤ 4 ACL のサポート

EFP における ACL の設定は、他のタイプのインターフェイスに ACL を設定する場合と同じです。

（注）　ACL は、マルチプロトコル ラベル スイッチング（MPLS）ヘッダーとプレフィックスが付いたパケットではサポートされません。これには、MPLS パケットがサポートされるプロトコルのレイヤ 3 またはレイヤ 4 ヘッダーが含まれます。

高度なフレーム操作

高度なフレーム操作機能では、EFP の着信フレームと送信フレームの両方に 1 個の VLAN タグを追加する PUSH 処理をサポートしています。

VLAN タグが存在している場合に新しいタグが追加されると、新しいタグの CoS フィールドには、既存 VLAN タグの CoS フィールドと同じ値が設定されます。そうでない場合、CoS フィールドはデフォルトの 0 に設定されます。QoS マーキング コンフィギュレーション コマンドを使用して CoS マーキングを変更できます。

出力フレーム フィルタリング

出力フレーム フィルタリングは、EFP を出るフレームが EFP に関連付けられたカプセル化の特性に一致するレイヤ 2 ヘッダーを含むことを保障するために行われます。このフィルタリングは主に、意図しないフレームの漏洩を防ぐために行われ、EFP で常にイネーブルです。

EVC のデフォルト設定

なし。

EVC の設定方法

レイヤ 2 ポートにサービス インスタンスを設定すると、EVC 機能を設定できる EFP が作成されます。EFP を設定するには、次の作業を実行します。

	コマンドまたはアクション	目的
ステップ 1	`Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	`Router# 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	`Router(config)# dot1ad`	802.1ad プロバイダー ブリッジ モードをイネーブルにします。 （注）　LACP EtherChannel と 802.1ad プロバイダー ブリッジ モードは相互に排他的です。802.1ad プロバイダー ブリッジ モードがイネーブルの場合、LACP EtherChannel はトラフィックを送信できません。
ステップ 4	`Router(config)# interface` *type number*	インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	`Router(config-if)# switchport`	ポートをレイヤ 2 スイッチング用に設定します。 （注）　LAN ポートをレイヤ 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 度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さらに **switchport** コマンドを入力してください。
ステップ 6	`Router(config-if)# switchport mode trunk`	無条件にポートをトランクに設定します。
ステップ 7	`Router(config-if)# switchport nonegotiate`	DTP を使用しないようにトランクを設定します。
ステップ 8	`Router(config-if)# switchport trunk encapsulation dot1q`	トランク カプセル化を 802.1Q として設定します。
ステップ 9	`Router(config-if)# switchport trunk allowed vlan` *vlan* [,*vlan*[,*vlan*[,...]]	トランク上で許可される VLAN のリストを設定します。 （注）　VLAN のロックがイネーブルになっている場合は、VLAN の番号の代わりに VLAN の名前を入力します。詳細については、「VLAN ロック」（P.25-5）を参照してください。
ステップ 10	`Router(config-if)# dot1ad uni`	802.1ad プロバイダー ブリッジのユーザネットワーク インターフェイス（UNI）ポートとしてポートを設定します。 （注）　**dot1ad uni** インターフェイス モード コマンドにより、SPAN の制約事項が適用されます（「機能の非互換性」（P.56-2）を参照）。
ステップ 11	`Router(config-if)# no cdp enable`	ポート上で CPD をディセーブルにします。
ステップ 12	`Router(config-if)# no lldp transmit`	（PE ポートで必須）LLDP をディセーブルにします。

	コマンドまたはアクション	目的
ステップ 13	`Router(config-if)# spanning-tree bpdufilter enable`	ポートで BPDU フィルタリングをイネーブルにします。
ステップ 14	`Router(config-if)# service instance number ethernet [name]`	イーサネット サービス インスタンス（EFP）を設定し、サービス インスタンス コンフィギュレーション モードを開始します。 • *number* は EFP ID で、1 ～ 4000 の整数です。 • （任意）**ethernet** *name* は事前に設定された EVC 名です。サービス インスタンスでは、EVC 名を使用する必要はありません。
ステップ 15	`Router(config-if)# ip access-group access-list-number | access-list-name} {in | out}`	（任意）インターフェイスに IP アクセス リストまたはオブジェクトグループ アクセス コントロール リスト（OGACL）を適用します。
ステップ 16	`Router(config-if-srv)# encapsulation encapsulation-type vlan-id [cos cos_value]`	サービス インスタンスのカプセル化タイプを設定します。 • **default**：他に一致する基準のないすべてのパケットのマッチングを設定します。 • **dot1q**：802.1Q カプセル化を設定します。詳細については、「表 41-1」を参照してください。 • **priority-tagged**：プライオリティ タグ付きフレーム、VLAN-ID 0 および CoS 値 0 ～ 7 を指定します。 • **untagged**：タグなし VLAN にマップします。タグなしカプセル化は、ポートあたり 1 つの EFP のみに設定できます。 • CoS 値は、1 ～ 7 の整数で一致基準を定義します。
ステップ 17	`Router(config-if-srv)# rewrite ingress tag push dot1ad vlan-id [symmetric]`	（任意）サービス インスタンスに入るフレームで実行されるカプセル化調整を指定します。
ステップ 18	`Router(config-if-srv)# bridge-domain bridge-id`	ブリッジ ドメインを設定します。
ステップ 19	`Router(config-if-srv)# end`	特権 EXEC モードに戻ります。

複数サービス インスタンスの設定

```
Router(config)# interface gigabitethernet1/1
Router(config-if)# switchport mode trunk
Router(config-if)# switchport nonegotiate
Router(config-if)# service instance 1 ethernet evc1
Router(config-if-srv)# encapsulation dot1q 201 cos 1
Router(config-if-srv)# rewrite ingress tag push dot1ad 300 symmetric
Router(config-if-srv)# bridge-domain 300
Router(config-if-srv)# end
Router(config-if)# service instance 2 ethernet evc2
Router(config-if-srv)# encapsulation default
Router(config-if-srv)# rewrite ingress tag push dot1ad 301 symmetric
Router(config-if-srv)# bridge-domain 301
Router(config-if-srv)# end
Router(config-if)# service instance 3 ethernet evc3
Router(config-if-srv)# encapsulation priority-tagged cos 1
Router(config-if-srv)# rewrite ingress tag push dot1ad 302 symmetric
Router(config-if-srv)# bridge-domain 302
```

サービス インスタンスの設定

```
Router(config)# interface gigabitethernet1/1
Router(config-if)# switchport mode trunk
Router(config-if)# switchport nonegotiate
Router(config-if)# switchport trunk allowed vlan none
Router(config-if)# service instance 22 ethernet evc1
Router(config-if-srv)# encapsulation dot1q 100
Router(config-if-srv)# rewrite ingress tag push dot1ad 10 symmetric
Router(config-if-srv)# bridge-domain 10
```

VLAN 範囲を使用したカプセル化

```
Router(config)# interface gigabitethernet1/1
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q 22-44 cos 1
Router(config-if-srv)# rewrite ingress tag push dot1ad 10 symmetric
Router(config-if-srv)# bridge-domain 10
```

同じブリッジ ドメインに加わっている 2 つのサービス インスタンス

この例では、ギガビット イーサネット 1/1 および 1/2 のインターフェイスのサービス インスタンス 1 を相互にブリッジングできます。

```
Router(config)# interface gigabitethernet1/1
Router(config-if)# service instance 1 Ethernet
Router(config-if-srv)# encapsulation dot1q 10
Router(config-if-srv)# rewrite ingress tag push dot1ad 10 symmetric
Router(config-if-srv)# bridge-domain 10

Router(config)# interface gigabitethernet1/2
Router(config-if)# service instance 1 Ethernet
Router(config-if-srv)# encapsulation dot1q 10
Router(config-if-srv)# rewrite ingress tag push dot1ad 10 symmetric
Router(config-if-srv)# bridge-domain 10
```

ブリッジ ドメインおよび VLAN カプセル化

ブリッジ ドメイン番号としては、**encapsulation dot1q** コマンドで設定した VLAN ID ではなく、**rewrite ingress tag push dot1ad** コマンドで設定した VLAN ID を使用します。これらの値は、一致することも異なることもあります。

```
Router(config)# interface gigabitethernet1/1
Router(config-if)# service instance 1 ethernet evc1
Router(config-if-srv)# encapsulation dot1q 10
Router(config-if-srv)# rewrite ingress tag push dot1ad 4000 symmetric
Router(config-if-srv)# bridge-domain 4000

Router(config)# interface gigabitethernet1/2
Router(config-if)# service instance 1 ethernet evc1
Router(config-if-srv)# encapsulation dot1q 10
Router(config-if-srv)# rewrite ingress tag push dot1ad 4000 symmetric
Router(config-if-srv)# bridge-domain 4000
```

encapsulation dot1q コマンドで設定した VLAN ID がブリッジ ドメイン内で一致しない限り、トラフィックは転送できません。次の例では、カプセル化 VLAN ID が一致しないため（フィルタリング基準）、ギガビット イーサネット 1/1 および 1/2 のサービス インスタンスは、相互の間で転送できません。**rewrite** コマンドを使用すると、これら 2 つの間での通信を許可できます。

```
Router(config)# interface gigabitethernet1/1
Router(config-if)# service instance 1 ethernet evc1
Router(config-if-srv)# encapsulation dot1q 10
Router(config-if-srv)# rewrite ingress tag push dot1ad 4000 symmetric
Router(config-if-srv)# bridge-domain 4000

Router(config)# interface gigabitethernet1/2
Router(config-if)# service instance 1 ethernet evc1
Router(config-if-srv)# encapsulation dot1q 99
Router(config-if-srv)# rewrite ingress tag push dot1ad 4000 symmetric
Router(config-if-srv)# bridge-domain 4000
```

Rewrite

この例では、**rewrite ingress tag push dot1ad** コマンドで設定されている VLAN ID（この例では 4000）は、**encapsulation dot1q** コマンドで設定された VLAN ID（この例では 10）に一致するパケットにプッシュされます。symmetric キーワードを使用すると、逆方向のパケットで逆のアクションが可能です。このサービス インスタンスから出る VLAN ID 4000 のパケットはカプセル開放され、CoS 1 の VLAN ID 10 になります。

```
Router(config)# interface gigabitethernet1/1
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q 10 cos 1
Router(config-if-srv)# rewrite ingress tag push dot1ad 4000 symmetric
Router(config-if-srv)# bridge-domain 4000
```

EVC のモニタリング

表 41-2　サポートされている show コマンド

コマンド	説明
show ethernet service evc [**id** *evc-id* | **interface** *interface-id*] [**detail**]	すべての EVC、特定の EVC（EVC ID を入力）、または特定のインターフェイスにあるすべての EVC（インターフェイス ID を入力）に関する情報を表示します。**detail** オプションを指定すると、EVC の詳細情報が表示されます。
show ethernet service instance [**id** *instance-id* **interface** *interface-id* | **interface** *interface-id*] {[**detail**] | [**stats**]}	1 つまたは複数のサービス インスタンス（EFP）に関する情報が表示されます。EFP ID およびインターフェイスを指定すると、その具体的な EFP に関連するデータのみが表示されます。インターフェイス ID だけを指定した場合は、このインターフェイス上のすべての EFP に対するデータが表示されます。
show bridge-domain [*n*]	*n* を入力すると、指定された番号を持つブリッジ ドメインが存在する場合は、指定したブリッジ ドメインのすべてのメンバーがこのコマンドによって表示されます。 *n* を入力していない場合は、システムのすべてのブリッジ ドメインのすべてのメンバーこのコマンドによって表示されます。
show ethernet service instance detail	このコマンドは、レイヤ 2 プロトコル情報を含む詳細なサービス インスタンスの情報を表示します。出力例を次に示します。 **Router# show ethernet service instance detail** Service Instance ID: 2 Associated Interface: GigabitEthernet7/2 Associated EVC: evc2 L2protocol drop CE-Vlans: Encapsulation: dot1q 2 vlan protocol type 0x8100 Rewrite: ingress tag push dot1ad 2 vlan-type 0x88A8 symmetric Interface Dot1q Tunnel Ethertype: 0x8100 State: Up EFP Statistics: Pkts In Bytes In Pkts Out Bytes Out 0 0 0 0
show mac address-table	このコマンドは、動的に学習されたか静的に設定された MAC セキュリティ アドレスを表示します。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

マルチポイント GRE を介したレイヤ 2（L2omGRE）

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

L2omGRE の前提条件

なし。

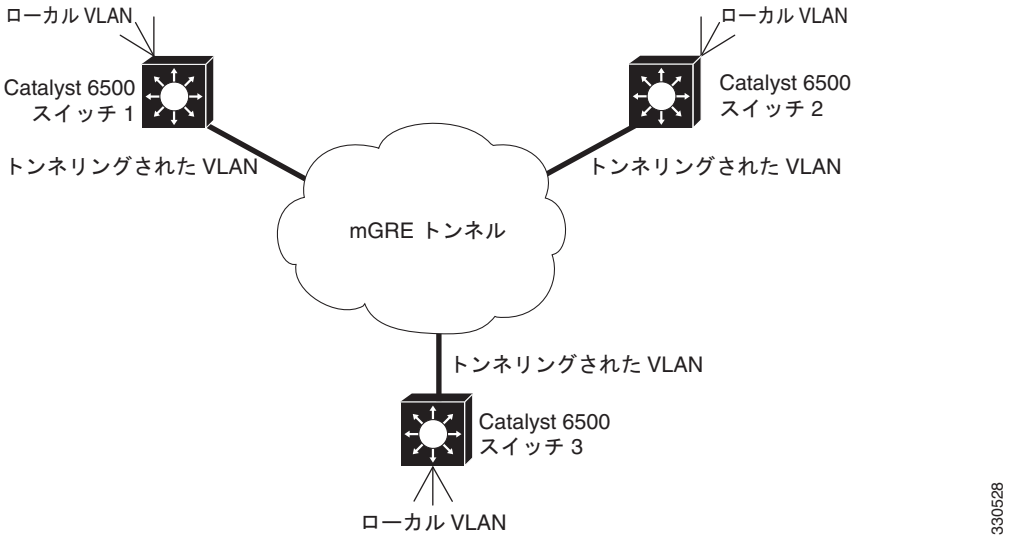
L2omGRE の制約事項

- L2omGRE 機能は、VSS モードでサポートされています。
- L2omGRE をサポートするために使用される VLAN インターフェイスは、任意のレイヤ 3 機能もサポートするようには設定できません。
- 現在再学習されていない MAC レイヤ宛先アドレスにアドレス指定されているため VLAN でフラッディングされるレイヤ 2 トラフィックをポリシング（レート制限）するように QoS を設定できます（「Traffic Classification」（P.63-2）の「**match l2 miss**」を参照）。

L2omGRE について

L2omGRE 機能では、mGRE トンネルを介してレイヤ 2 ブロードキャスト ドメインのトポロジを拡張することにより、複数の個別ネットワーク サイト間のレイヤ 2 接続を提供します（図 42-1 を参照）。

図 42-1　　L2omGRE トポロジ



L2omGRE 機能は、VLAN インターフェイスを mGRE トンネル インターフェイスに関連付けます。L2omGRE 機能をサポートするように設定された mGRE トンネル インターフェイスは、VLAN のあらゆるタイプのトラフィックに対するレイヤ 2 スイッチング（ブリッジング）を提供するように、レイヤ 2 LAN ポートのように機能します。これにより、トンネルでは、この mGRE トンネルを介してアクセス可能なデバイスにアドレス指定されたトラフィックだけを伝送します、（「レイヤ 2 イーサネット スイッチングについて」（P.20-3）を参照）。スイッチは mGRE トンネル経由でアクセスできる MAC アドレスを学習し、**show mac address-table** コマンドは学習されたアドレスを表示します。

PFC および DFC は、ハードウェアで、ブリッジングおよび mGRE トンネルのカプセル化とカプセル開放をサポートします。

各トンネルは L2omGRE 接続された VLAN を複数伝送できます。トンネル カプセル化には VLAN ID が含まれます。トンネリングされたトラフィックがカプセル開放されると、トラフィックに適した VLAN を選択するために、トンネリング トラフィックに含まれている VLAN ID が使用されます。

L2omGRE のデフォルト設定

なし。

L2omGRE の設定方法

ループバック インターフェイスの設定

L2omGRE をサポートするようにループバック インターフェイスを設定するには、次の作業を行います。

	コマンドまたはアクション	目的
ステップ 1	`Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	`Router# 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	`Router(config)# interface loopback number`	ループバック インターフェイスを作成し、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 4	`Router(config-if)# ip address address mask`	インターフェイスの IP アドレスを設定します。 （注）　他のスイッチのトンネル インターフェイスは、このスイッチのこの IP アドレスを参照します。
ステップ 5	`Router(config-if)# 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。

mGRE トンネル インターフェイスの設定

mGRE トンネル インターフェイスを設定するには、次の作業を行います。

	コマンドまたはアクション	目的
ステップ 1	`Router(config)# interface tunnel number`	トンネル インターフェイスを作成します。続いて、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。 （注）　このスイッチの VLAN インターフェイスは、このトンネル番号を参照します。
ステップ 2	`Router(config-if)# ip address address mask`	インターフェイスの IP アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 3	`Router(config-if)# ip nhrp map tunnel_address loopback_address`	L2omGRE トンネル インターフェイスを持つ他のスイッチに設定されているループバック インターフェイスの IP アドレスに対して、IP/NBMA（非ブロードキャスト マルチアクセス）アドレス マッピングを設定します。 • 他の L2omGRE スイッチに設定されている *tunnel_address loopback_address* 値を入力します。 • 他の L2omGRE スイッチごとにこのコマンドを繰り返します。
ステップ 4	`Router(config-if)# ip nhrp network-id ID`	mGRE トンネル用の Next Hop Resolution Protocol（NHRP）をイネーブルにします。すべての L2omGRE トンネル インターフェイスで同じ ID 値を使用します。
ステップ 5	`Router(config-if)# tunnel source loopback number`	このトンネル インターフェイスをループバック インターフェイスと関連付けます。
ステップ 6	`Router(config-if)# tunnel mode gre multipoint`	トンネル モードとしてマルチポイント GRE を設定します。
ステップ 7	`Router(config-if)# 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。

VLAN インターフェイスの設定

L2omGRE をサポートするように 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。

	コマンドまたはアクション	目的
ステップ 1	`Router(config)# interface vlan number`	VLAN インターフェイスを作成し、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 2	`Router(config-if)# no ip address`	インターフェイスに IP アドレスが設定されていないことを確認します。
ステップ 3	`Router(config-if)# platform xconnect l2gre tunnel number`	VLAN インターフェイスを L2omGRE トンネル インターフェイスと関連付けます。
ステップ 4	`Router(config-if)# 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。

L2omGRE の設定例

L2omGRE コンフィギュレーション コマンドは次のように調整する必要があります。

- 各スイッチの **ip nhrp map** コマンドは、他の各スイッチのトンネルおよびループバック IP アドレスを指します。
- 各スイッチで、**tunnel source loopback** コマンドは、そのスイッチに設定されているループバック インターフェイスを指します。
- 各スイッチで、**platform xconnect l2gre tunnel** コマンドは、そのスイッチの L2omGRE トンネル インターフェイスを指します。

スイッチの L2omGRE コンフィギュレーションに関する情報を表示するには、**show platform l2transport gre summary** コマンドを入力します。

スイッチ 1	スイッチ 2	スイッチ 3
interface loopback 1 ip address 10.1.1.1 255.255.255.255 interface tunnel 10 ip address 10.10.10.1 255.255.255.0 no ip redirects ip nhrp map 10.20.20.2 10.2.2.2 ip nhrp map 10.30.30.3 10.3.3.3 ip nhrp network-id 10 tunnel source loopback 1 tunnel mode gre multipoint interface vlan 10 no ip address platform xconnect l2gre tunnel 10	interface loopback 1 ip address 10.2.2.2 255.255.255.255 interface tunnel 10 ip address 10.20.20.2 255.255.255.0 no ip redirects ip nhrp map 10.10.10.1 10.1.1.1 ip nhrp map 10.30.30.3 10.3.3.3 ip nhrp network-id 10 tunnel source loopback 1 tunnel mode gre multipoint interface vlan 10 no ip address platform xconnect l2gre tunnel 10	interface loopback 1 ip address 10.3.3.3 255.255.255.255 interface tunnel 10 ip address 10.30.30.3 255.255.255.0 no ip redirects ip nhrp map 10.10.10.1 10.1.1.1 ip nhrp map 10.20.20.2 10.2.2.2 ip nhrp network-id 10 tunnel source loopback1 tunnel mode gre multipoint interface vlan 10 no ip address platform xconnect l2gre tunnel 10

L2omGRE の設定の確認

トラフィック統計情報を含む L2omGRE に関する情報を表示するには、**show platform l2transport gre** コマンドを入力します。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

PART 10

マルチキャスト

CHAPTER 43

IPv4 マルチキャスト レイヤ 3 機能

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

IPv4 マルチキャスト レイヤ 3 の前提条件

なし。

IPv4 マルチキャスト レイヤ 3 の制約事項

次のような場合に、IP マルチキャスト レイヤ 3 スイッチングは IP マルチキャスト フローに実行されません。

- 224.0.0.*（* は 0 ～ 255）の範囲の IP マルチキャスト グループ。これらのグループは、ルーティング プロトコルが使用します。レイヤ 3 スイッチングは、225.0.0.* ～ 239.0.0.*、および 224.128.0.* ～ 239.128.0.* のグループでサポートされます。

（注）　224.0.0.* の範囲のグループはルーティング コントロール パケット専用で、VLAN のすべての転送ポートにフラッディングする必要があります。これらのアドレスは、マルチキャスト MAC アドレス範囲 01-00-5E-00-00-*xx*（*xx* は 0 ～ 0xFF）に対応します。

- PIM 自動 RP マルチキャスト グループ（IP マルチキャスト グループ アドレス 224.0.1.39 および 224.0.1.40）
- IP オプションを指定されたパケット。ただし、フロー内で IP オプションを指定されていないパケットは、ハードウェア スイッチングされます。
- sparse モードの（S,G）エントリに、SPT ビット、RPT ビット、またはプルーニング フラグが設定されていない場合
- 1 つ以上の（S,G）エントリに（*,G）エントリの RPF とは異なる RPF があり、（S,G）がハードウェアでスイッチングされない場合、（*,G）エントリはハードウェアでスイッチングされません。
- （*,G）エントリが IPv4 双方向 PIM エントリでスイッチがグループの RP である場合を除き、（S,G）または（*,G）エントリの入力インターフェイスがヌルの場合。
- IP マルチキャスト レイヤ 3 スイッチングをイネーブルにした場合、レイヤ 3 インターフェイスに関する IP アカウンティングでは、正確な値が報告されません。**show ip accounting** コマンドはサポートされません。

IPv4 マルチキャスト レイヤ 3 機能について

IPv4 マルチキャスト レイヤ 3 機能の概要

Supervisor Engine 2T 上のマルチキャスト レイヤ 3 スイッチングでは、特定用途向け集積回路（ASIC）を使用して IP サブネット間の IP マルチキャスト データ パケット フローの転送をハードウェアでサポートします。これにより、プロセッサ集中的なマルチキャスト転送とレプリケーションがルート プロセッサからオフロードされます。

ポリシー フィーチャ カード（PFC）および分散型フォワーディング カード（DFC）では、転送情報ベース（FIB）および隣接関係テーブルを使用して、ハードウェア内で IP マルチキャスト フローを切り替えます。FIB テーブルはさまざまなエントリおよびマスク値をサポートしています。たとえば、（S/32, G/32）および（*/0, G/32）です。RPF RAM は、直接接続されたサブネットに到着するパケットを識別するために使用されます。

FIB ルックアップの結果は隣接情報です。これは、このエントリのレプリケーション リストになります。これまでのスーパーバイザ エンジンとは異なり、Supervisor Engine 2T では、レプリケーションのパケットの書き換えを実行します。これは、発信インターフェイスに対する強化された共有機能になります。

同じく、これまでのスーパーバイザ エンジンと異なり、Supervisor Engine 2T では、レイヤ 2 とレイヤ 3 の転送の決定を別々に実行します。ルーテッド インターフェイスでは、パケットの最終 LTL は、レイヤ 3 情報だけに基づいて決定されます。VLAN インターフェイスでは、パケットの LTL はレイヤ 2 ルックアップだけに基づいて決定されます。

分散 MRIB および MFIB インフラストラクチャ

Supervisor Engine 2T は、IPv4 マルチキャスト トラフィック用に MRIB および MFIB ベースのソフトウェア モデルを使用します。MRIB/MFIB インフラストラクチャは IPv4 と IPv6 の両方のフローに対して、レイヤ 3 マルチキャスト プロトコル（PIM sparse モード、SSM、双方向 PIM など）をサポートしており、IPv4 と IPv6 の両方にアドレスに一貫した CLI を用意しています。

マルチキャスト ルーティング情報ベース（MRIB）は、送信元、グループ、グループ マスクをキーとするマルチキャスト エントリの集合です。マルチキャスト コントロール プレーンは、このエントリをプログラミングします。エントリは、フォワーディング プレーンでのインターフェイスのロールを示す、さまざまなフラグを持つ、1 つ以上の関連インターフェイスを持つことができます。Supervisor Engine 2T で、PFC および各 DFC は、MRIB のクライアントとして登録する、マルチキャスト転送情報ベース（MFIB）の単一のインスタンスを持ちます。MFIB は、エントリと関連フラグに関して MRIB の対象を登録し、MRIB の更新に基づいて、送信元、グループ、グループ マスクをキーとするローカル データベースを保守します。

ハードウェア サポートがない場合は、MFIB がマルチキャスト トラフィックを転送します。Supervisor Engine 2T で、MFIB は、必要なすべてのソフトウェア転送に加え、レイヤ 3 スイッチング ハードウェア テーブルのマルチキャスト ルート アップデートを送信します。MRIB、MFIB、およびレイヤ 3 スイッチング ハードウェア テーブル間の通信は、次の要素に基づきます。

- マルチキャスト エントリ
- マルチキャスト エントリにセットされたフラグ
- マルチキャスト エントリに関連付けられたインターフェイス

（注） 他のスーパーバイザ エンジンを使用する場合、一部のフローは、ハードウェアで部分的にスイッチングされ、ソフトウェアで部分的にスイッチングされます。Supervisor Engine 2T では、マルチキャスト フローは、ソフトウェアとハードウェアのいずれかでスイッチングされます。

mroute、MRIB、および MFIB 情報の例。

```
Router# show ip mroute
(100.1.1.3, 239.2.1.1), 00:00:53/00:02:08, flags: sTI
  Incoming interface: TenGigabitEthernet3/0, RPF nbr 0.0.0.0
  Outgoing interface list:
    TenGigabitEthernet3/1, Forward/Sparse-Dense, 00:00:51/00:02:08
    TenGigabitEthernet3/2, Forward/Sparse-Dense, 00:00:51/00:02:08
    TenGigabitEthernet3/3, Forward/Sparse-Dense, 00:00:51/00:02:08
```

```
Router# show ip mrib route
(100.1.1.3,239.2.1.1)
  TenGigabitEthernet3/1 Flags: A
  TenGigabitEthernet3/2 Flags: F
  TenGigabitEthernet3/3 Flags: F
  TenGigabitEthernet3/4 Flags: F

Router# show ip mfib
(100.1.1.3,239.2.1.1) Flags:
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   TenGigabitEthernet3/1 Flags: A
     Pkts: 0/0
   TenGigabitEthernet3/2 Flags: F
     Pkts: 0/0
   TenGigabitEthernet3/3 Flags: F
     Pkts: 0/0
   TenGigabitEthernet3/4 Flags: F
     Pkts: 0/0
```

マルチキャスト レイヤ 3 ハードウェア機能のエントリ

ここでは、PFC および DFC により、レイヤ 3 スイッチング情報をハードウェア テーブルに維持する方法について説明します。

PFC および DFC は、適切なマスクを使用して（S,G）または（*,G）フローをハードウェア FIB テーブルに読み込みます。たとえば、（S/32, G/32）および（*/0, G/32）などです。RPF インターフェイスおよび隣接ポインタ情報も、各エントリに保存されます。隣接テーブルには、書き換え情報およびレプリケーション エントリへのポインタが含まれます。フローが FIB エントリと一致した場合、RPF チェックによって着信インターフェイス /VLAN がエントリと比較されます。一致しない場合は RPF 障害であり、レート制限機能がイネーブルになっている場合はレート制限の対象になります。転送情報データベース（FIB）に重大エラーが発生した場合は、デフォルトのエラー処理として、システムがリセットされ、FIB がリロードされます。

PFC およびすべての DFC は、MFIB クライアントを実行します。これは、MRIB のクライアントとして RP に登録されます。ハードウェア テーブルは、トラフィック フローのエントリをインストールまたは削除するか、既存のハードウェア エントリに発信インターフェイスを追加および削除するように、MFIB の更新に基づいてプログラムされています。

レイヤ 3 スイッチング エントリに影響するコマンドは、次のとおりです。

- **clear ip mroute** コマンドを使用してマルチキャスト ルーティング テーブルをクリアすると、すべてのマルチキャスト レイヤ 3 スイッチング キャッシュ エントリがクリアされます。
- **no ip multicast-routing** コマンドを使用して RP 上の IP マルチキャスト ルーティングをディセーブルにすると、PFC 上のマルチキャスト レイヤ 3 スイッチング キャッシュ エントリがすべて消去されます。
- **no platform multicast forwarding ip** インターフェイス モード コマンドによって、インターフェイスのハードウェア サポート マルチキャスト レイヤ 3 スイッチングをディセーブルにすると、このインターフェイスを RPF インターフェイスとして使用するフローは、ソフトウェア内の RP だけによってルーティングされます。
- **no ip mfib forwarding ip** コマンドを使用して MFIB 転送をインターフェイスごとにディセーブルにした場合、このインターフェイスを RPF インターフェイスとして使用するフローは、ハードウェアでも MFIB によっても転送されません。

レイヤ 3 スイッチド マルチキャスト統計情報

フローがハードウェアでスイッチングされている間も、エントリは、フローのパケット転送統計情報に基づいて、ソフトウェアで維持されます。PFC 上の MFIB エントリは、PFC およびすべての DFC から、エントリ統計情報を定期的に取得し、集約します。この統計情報により、エントリのハードウェア転送カウンタが増分されます。ソフトウェアまたはハードウェアの転送カウンタが増分されると、そのマルチキャスト ルートに対応する期限タイマーがリセットされます。

（注） PIM-RP または PIM-dense モードでは（*,G）ステートが作成されますが、フローの転送には使用されず、これらのフローについてはレイヤ 3 スイッチング エントリは作成されません。

レイヤ 3 スイッチド マルチキャスト パケットの書き換え

マルチキャスト送信元から宛先マルチキャスト グループへのマルチキャスト パケットにレイヤ 3 スイッチングが実行される場合、PFC および DFC は、RP から得た情報とその隣接テーブルに保存されている情報に基づき、パケットの書き換えを実行します。

たとえば、サーバ A が IP マルチキャスト グループ G1 を宛先とするマルチキャスト パケットを送信する場合を想定します。送信元 VLAN 以外の VLAN 上にグループ G1 のメンバーが存在する場合、PFC は送信元以外の VLAN にトラフィックを複製するとき、パケットの書き換えを実行しなければなりません（スイッチはさらに、送信元 VLAN 内でパケットをブリッジします）。

PFC がマルチキャスト パケットを受信した時点で、パケットは、次のようにフォーマットされます（概念上）。

レイヤ 2 フレーム ヘッダー		**レイヤ 3 IP ヘッダー**				**データ**	**FCS**
宛先	送信元	宛先	送信元	TTL	チェックサム		
Group G1 MAC **（注）** この例では、宛先 B はグループ G1 のメンバーです。	*Source A MAC*	*Group G1 IP*	*Source A IP*	*n*	*calculation1*		

PFC は、パケットを次のように書き換えます。

- レイヤ 2 フレーム ヘッダーの送信元 MAC アドレスを、ホストの MAC アドレスから RP の MAC アドレスに変更します（システムに組み込まれている MAC アドレスです。この MAC アドレスは、すべての出力インターフェイスの場合と同じで変更できません。この MAC アドレスを表示するには、**show platform multicast statistics** コマンドを使用します）。
- IP ヘッダーの Time To Live（TTL）を 1 だけ減らし、IP ヘッダー チェックサムを再計算します。

その結果、書き換えられた IP マルチキャスト パケットは、ルーティングされたような外見になります。PFC は書き換えたパケットを該当する宛先 VLAN に複製し、その VLAN 上でパケットが IP マルチキャスト グループ G1 のメンバーに転送されます。

PFC がパケットの書き換えを行ったあと、パケットは、次のようにフォーマットされます（概念上）。

フレーム ヘッダー		IP ヘッダー				データ	FCS
宛先	送信元	宛先	送信元	TTL	チェックサム		
Group G1 MAC	*RP MAC*	*Group G1 IP*	*Source A IP*	*n-1*	*calculation2*		

レプリケーション モード

Supervisor Engine 2T は、次のレプリケーション モードをサポートしています。

- 入力モード：入力モジュールは、すべてのモジュールで出力インターフェイスのレプリケーションを実行します。
- 出力モード（デフォルト）：入力マルチキャスト トラフィックは、ファブリックを介して出力モジュールに配信されます。出力モジュールは出力インターフェイスのレプリケーションを実行します。

Supervisor Engine 2T は入力専用のレガシー スイッチング モジュールに対して出力モードのレプリケーションを実行するため、入力専用のレガシー スイッチング モジュールが存在してもレプリケーション モードの変更は強制されません。

（注）　イントラネットおよびエクストラネット MVPN は、出力および入力レプリケーション モードでサポートされています。

ローカル出力レプリケーション モード

デュアル スイッチファブリック接続を含む DFC を装備したモジュールには、ファブリック接続ごとに 1 つずつ、合計 2 つのパケット レプリケーション エンジンがあります。それぞれのレプリケーション エンジンは、スイッチファブリック接続と関連したインターフェイスにパケットを転送したり、そのインターフェイスからパケットを転送したりします。スイッチファブリック接続と関連するインターフェイスは、パケット レプリケーション エンジン側から見て「ローカル」と見なされます。ローカル出力レプリケーション モードのない場合、両方のレプリケーション エンジンにすべてのモジュールの完全な発信インターフェイス リストが保持され、レプリケーション エンジンはローカルでないインターフェイスのトラフィックをいったん処理してからドロップします。Supervisor Engine 2T は、CFC を搭載したスイッチング モジュールのローカル出力レプリケーションを実現します。

ローカル出力レプリケーション モードによって、発信インターフェイス リストが各レプリケーション エンジンをサポートするローカル インターフェイスだけに制限され、不要なマルチキャスト トラフィックの処理を防止できます。

Cisco IOS Release 15.1SY では、ローカル出力レプリケーション モードがデフォルトでイネーブルです。

PIM-SM ハードウェア レジスタのサポート

PIM-SM プロトコルでは、送信元がパケットの送信を開始するときに、マルチキャスト送信元がランデブー ポイント（RP）に登録パケットを送信できるように、ファースト ホップ ルータが必要です。Supervisor Engine 2T では、PIM コントロール プレーンで MFIB インフラストラクチャを使用して、インターフェイスとして PIM レジスタ トンネルを表し、PIM Register パケットが送信されるときに発信インターフェイス リストにそれを追加します。新しい PIM RP が設定または学習されると、PIM レ

ジスタ トンネル インターフェイスが作成され、PIM Register パケット用に使用されます。register-stop パケットを受信すると、インターフェイスが削除されます。RP で、追加のインターフェイスが作成され、PIM Register パケットを受信したときに、パケットのカプセル開放に使用されます。

Supervisor Engine 2T はハードウェアで PIM Register パケットの送受信をサポートします。PIM Register パケットは PIM 登録プロセスのために RP に送信されます。CoPP では、PIM 登録プロセスのために RP に送信される PIM Register パケットをレート制限できます。

PIM-SM ハードウェア SPT switchover のサポート

PIM-SM ネットワークでの SPT switchover は、あるマルチキャスト グループについて、送信元への最短パスが、RP への最短パスから分岐する場合に発生します。最短パス ツリーから送信元ベースのツリーへの遷移中は、共有ツリーと送信元ツリーの両方からパケットが受信されるため、2 個のインターフェイスからのパケットを受け入れるようにマルチキャスト エントリをプログラムする必要があります。

ハードウェア サポートは、マルチキャスト FIB デュアル RPF モードで実装されます。マルチキャスト FIB エントリにデュアル RPF がプログラムされている場合、RP 方向の RPF で受信したパケットは転送され、送信元方向の RPF で受信したパケットは、PIM プロトコルで SPT switchover を完了するためにソフトウェアで処理するように送信されます。送信元ツリーへの切り替え後、マルチキャスト エントリは、再度単一 RPF インターフェイスに遷移します。スイッチオーバー プロセス中に CPU の過剰使用を避けるために、SPT switchover 中に RP に送信されるマルチキャスト パケットをレート制限するように CoPP を設定できます。

コントロール プレーン ポリシング（CoPP）

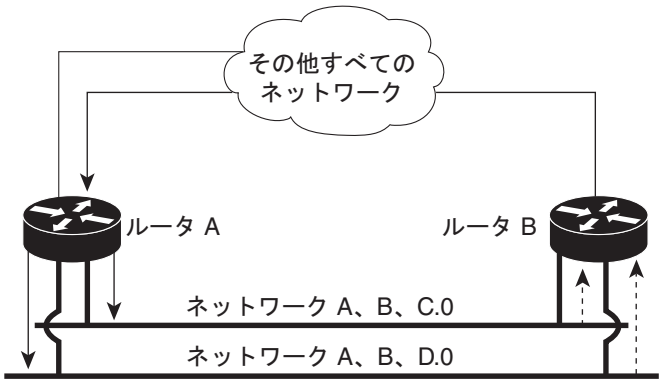
CoPP を設定して、不要なトラフィックや DoS トラフィックから CPU を保護できます。Cisco IOS Release 15.1SY では、CoPP が設定され、デフォルトでイネーブルです。CoPP は、ソフトウェア処理のために CPU に送信されるパケットに対するハードウェア レート制限になります。マルチキャスト レート リミッタはまだサポートされていますが、CoPP の方が効率的です。

（注） いずれのタイプの個別トラフィックに対しても、CoPP とレート リミッタのいずれかを設定し、両方は設定しないでください。

非 RPF トラフィックの処理

複数のルータが同一 LAN セグメントに接続する冗長構成では、1 台のルータだけが、出力インターフェイス上でマルチキャスト トラフィックを送信元からレシーバーまで転送します（図 43-1 を参照）。このようなトポロジーでは、PIM 指定ルータ（PIM DR）だけが共通の VLAN 内でデータを転送し、非 PIM DR 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。このトラフィックは、誤ったインターフェイスに着信して RPF チェックに失敗するため、冗長ルータ（非 PIM DR）はこのトラフィックを廃棄しなければなりません。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。

図 43-1　スタブ ネットワークにおける冗長マルチキャスト ルータの構成



— マルチキャスト トラフィック
--- 非 RPF トラフィック

デフォルトでイネーブルになっている非 RPF 保護は、適切なマルチキャスト ルーティング プロトコル処理をサポートするように、一部のパケットが引き続き CPU に到達できるようにしながら、非 RPF トラフィックによる過負荷から CPU を保護します。非 RPF 保護機能は、漏洩とドロップのメカニズムを使用します。非 RPF パケットは CPU に漏洩し、後続の非 RPF パケットはドロップされます。このシーケンスが定期的に繰り返されます。

設定した CoPP ポリシーに準拠している、RPF に失敗したマルチキャスト パケットは、CPU に到達します。準拠していないパケットはドロップされます。レート制限は CoPP ポリシーで設定されます。

マルチキャスト境界

マルチキャスト境界機能により、マルチキャスト グループ アドレスに管理境界を設定できます。マルチキャスト データ パケットのフローを制限することにより、1 つのマルチキャスト グループ アドレスを異なる管理ドメインで再利用できます。

インターフェイスにマルチキャスト境界を設定します。パケットのマルチキャスト グループ アドレスが、マルチキャスト境界機能に関連付けられたアクセス コントロール リスト（ACL）に一致する場合、このマルチキャスト データ パケットはインターフェイス上で送受信されないようにブロックされます。

マルチキャスト境界の ACL は、ハードウェアではポリシー フィーチャ カード（PFC）、分散型フォワーディング カード（DFC）で、ソフトウェアでは RP で処理できます。マルチキャスト境界の ACL は、パケットの宛先アドレスに一致するようにプログラムされます。これらの ACL は、両方向（入力および出力）のインターフェイス上のトラフィックに適用されます。

ハードウェアでマルチキャスト境界の ACL をサポートするため、スイッチは新しい ACL TCAM エントリを作成するか、または既存の ACL TCAM エントリを変更します（インターフェイス上で他の ACL ベースの機能がアクティブな場合）。TCAM リソースの利用率を確認するには、**show tcam counts ip** コマンドを入力します。

filter-autorp キーワードを設定すると、管理境界でも自動 RP ディスカバリおよび通知メッセージを検証して、境界 ACL により拒否された自動 RP グループ範囲の通知を自動 RP パケットから削除します。

IPv4 双方向 PIM

PFC および DFC は、IPv4 双方向 PIM グループのハードウェア転送をサポートしています。IPv4 双方向 PIM グループをサポートするために、PFC および DFC では、指定フォワーダ（DF）モードをサポートしています。DF は、IPv4 双方向 PIM グループのセグメントへ、またセグメントからパケットを転送するよう選定されたルータです。DF モードでは、スイッチは RPF および DF インターフェイスからパケットを受け入れます。

スイッチが IPv4 双方向 PIM グループを転送するとき、RPF インターフェイスは常に（*,G）エントリの発信インターフェイス リストに含まれ、DF インターフェイスが含まれるエントリは IGMP/PIM Join に応じて決まります。

RP へのルートが使用できない場合、グループは dense モードに変更されます。RP への RPF リンクが使用できなくなると、IPv4 双方向 PIM フローはハードウェア FIB から削除されます。

IPv4 双方向 PIM の設定手順については、「IPv4 双方向 PIM の設定」（P.43-27）を参照してください。

サポートされるマルチキャスト機能

ハードウェアでサポートされている IPv4 レイヤ 3 機能

- コントロール プレーン ポリシング（CoPP）
- 出力強制レプリケーション モード
- 出力レプリケーション ローカル
- 出力レプリケーション モード
- HW アシストされた SPT スイッチオーバー
- 入力 ACL ロギング
- 入出力 ACL フィルタリング
- マルチポイント IPv4 GRE トンネル上の IPv4 マルチキャスト
- P2P IPv4 GRE トンネル上の IPv4 マルチキャスト
- VRF での P2P IPv4 GRE トンネル上の IPv4 マルチキャストおよびトンネル エンドポイント
- P2P IPv4 VRF GRE トンネル上の IPv4 マルチキャスト
- ポートチャネルでのマルチキャスト パケットのロードバランシング
- マルチキャスト境界
- ルーテッド ポートでのマルチキャスト レイヤ 3 フォワーディング
- サブインターフェイスでのマルチキャスト レイヤ 3 フォワーディング
- SVI でのマルチキャスト レイヤ 3 フォワーディング
- パラレル リンク間のマルチキャスト ロード分割
- IPv4 エクストラネットをサポートするマルチキャスト VPN
- IPv4 イントラネットをサポートするマルチキャスト VPN
- マルチキャスト VRF-lite
- P2P IPv4 GRE トンネル上の MVPN
- NetFlow アカウンティング
- Non-RPF 保護
- IPv4 を介した PIM Register カプセル開放
- IPv4 を介した PIM Register カプセル化
- PIM-DM（S,G）転送
- PIM-SM（S,G）および（*,G）転送
- PIM-SSM
- 入力モードの QoS ポリシング
- レート リミッタ
- 統計情報
- UDLR：単方向リンク ルーティング
- URD：URL Rendezvous Directory
- ハードウェアで部分的にサポートされている IPv4 レイヤ 3 機能
- 出力レプリケーション モードおよび QoS マーキング
- 入力モードの QoS マーキング

- ソフトウェア サポートされている IPv4 レイヤ 3 機能
- IGMPv3/v2/v1
- MET 共有
- MRM/mrinfo/mmon
- MSDP/MBGP
- mtrace/Mping
- PGM ルータ アシスト
- VRF での PGM ルータ アシスト
- プラットフォーム依存の MIB サポート
- プラットフォームに依存しない MIB サポート
- SSM マッピング
- SSO/NSF

サポートされていない IPv4 レイヤ 3 機能

- IPv4 インフラストラクチャ上の 6PE IPv6（MDT トンネルを使用）
- 宛先 IP NAT マルチキャスト
- MTR マルチキャスト ToS ベースの参照
- マルチキャスト スタブ（12.2SX でサポート）
- 部分ショートカット（12.2SX でサポート）
- サービス リフレクション
- 送信元 IP NAT マルチキャスト
- 出力レプリケーション モードおよび QoS ポリシング
- 出力 ACL ロギング
- QoS 入力または出力シェーピング
- ルーティング中のマルチキャスト ブリッジされたフレームの QoS マーキング
- DVMRP 相互運用性（リリース 12.2SX でサポート）
- ISSU/MDR
- MFIB の整合性チェッカ
- MFIB HW 整合性チェッカ
- MTR マルチキャスト：グループ範囲用個別 RPF テーブル
- MTR マルチキャスト：個別 URIB RPF テーブル
- マルチキャスト ヘルパー マップ（リリース 12.2SX でサポート）
- RPF 変更のトラッキング
- **ip multicast rate-limit** コマンド（リリース 12.2SX でサポート）
- **ip multicast ttl-threshold** コマンド（リリース 12.2SX でサポート）

ハードウェアでサポートされている IPv6 レイヤ 3 マルチキャスト機能

- コントロール プレーン ポリシング（CoPP）
- 出力強制レプリケーション モード
- 出力レプリケーション ローカル
- 出力レプリケーション モード
- HW アシストされた SPT スイッチオーバー
- 入力 ACL ロギング
- 入出力 ACL フィルタリング
- P2P IPv4 GRE/IP-in-IP トンネル上の IPv6 マルチキャスト（6over4）
- ポートチャネルでのマルチキャスト パケットのロードバランシング
- ルーテッド ポートでのマルチキャスト レイヤ 3 フォワーディング
- サブインターフェイスでのマルチキャスト レイヤ 3 フォワーディング
- SVI でのマルチキャスト レイヤ 3 フォワーディング
- パラレル リンク間のマルチキャスト ロード分割
- NetFlow アカウンティング
- Non-RPF 保護
- IPv6 を介した PIM Register カプセル開放
- IPv6 を介した PIM Register カプセル化
- PIM-SM（S,G）および（*,G）転送
- PIM-SSM
- QoS 入力モード マーキング
- QoS 入力モード ポリシング
- レート リミッタ
- スコープ チェック
- 統計情報

ハードウェアで部分的にサポートされている IPv6 レイヤ 3 マルチキャスト機能

- 出力レプリケーション モードおよび QoS マーキング

ソフトウェアでサポートされている IPv6 レイヤ 3 マルチキャスト機能

- SSM マッピング
- MET 共有
- MLDv1/v2

サポートされていない IPv6 レイヤ 3 マルチキャスト機能

- P2P GRE トンネルを介した BIDIR PIM

- 宛先 IP NAT マルチキャスト
- P2P IPv6 GRE トンネル上の IPv4 マルチキャスト（4over6）
- マルチポイント IPv4 GRE トンネル上の IPv6 マルチキャスト（6over4 mGRE）
- マルチポイント IPv6 GRE トンネル上の IPv6 マルチキャスト
- P2P IPv6 GRE トンネル上の IPv6 マルチキャスト
- VRF での P2P IPv6 GRE トンネル上の IPv6 マルチキャストおよびトンネル エンドポイント
- P2P IPv6 VRF GRE トンネル上の IPv6 マルチキャスト
- MTR マルチキャスト：ToS ベースの参照
- IPv6 エクストラネットをサポートするマルチキャスト VPN
- IPv6 イントラネットをサポートするマルチキャスト VPN
- マルチキャスト VRF-lite
- P2P IPv6 GRE トンネル上の MVPN
- PIM-DM（S,G）転送
- 送信元 IP NAT マルチキャスト
- 出力レプリケーション モードおよび QoS ポリシング
- QoS 入力および出力：シェーピング サポート
- MIB のサポート
- マルチキャスト境界
- マルチキャスト ヘルパー マップ
- 出力 ACL ロギング
- PGM ルータ アシスト
- VRF での PGM ルータ アシスト
- PIM-BIDIR
- ルーティング中のマルチキャスト ブリッジされたフレームの QoS マーキング

ハードウェアでサポートされているレイヤ 2 共通マルチキャスト機能

- IGMP/PIM/MLD スヌーピングのための NSF/SSO サポート

サポートされていないレイヤ 2 共通マルチキャスト機能

- IGMP/PIM/MLD スヌーピングのための ISSU/MDR サポート
- MIB のサポート

ハードウェアでサポートされているレイヤ 2 エンタープライズ マルチキャスト機能

- IGMPv2/v1 スヌーピング：IP ベースの抑制
- IGMPv2/v1 スヌーピング：MAC ベースの抑制
- S, G 抑制を含む IGMPv3 スヌーピング
- MLD v1 スヌーピング：IP ベースの抑制

- MLD v1 スヌーピング：MAC ベースの抑制
- MLD v2 スヌーピング：IP ベースの抑制
- MLD v2 スヌーピング：MAC ベースの抑制
- BD を介した PVLAN のマルチキャスト サポート
- 不明な IP マルチキャスト フレームの最適なフラッディング
- PIM スヌーピング：IP ベースの抑制
- PIM スヌーピング：MAC ベースの抑制
- IGMP スヌーピング クエリア
- IGMPv3 スヌーピング：明示的なトラッキング
- MLD スヌーピング クエリア
- PIM スヌーピング：DR フラッディング

サポートされていないレイヤ 2 エンタープライズ マルチキャスト機能

- RGMP
- Source-Only 検出
- マルチキャスト フラッド保護
- IGMP スヌーピング用の CGMP 互換モード
- CGMP リダイレクトの抑制

ハードウェアでサポートされているレイヤ 2 Metro マルチキャスト機能

- マルチキャスト VLAN レジストレーション（MVR）

サポートされていないレイヤ 2 Metro マルチキャスト機能

- Q-in-Q タグ付きフレームを介した MLD v1/v2 スヌーピング
- LAN ポートでの VPLS マルチキャスト抑制の最適化
- Q-in-Q を介した PIM スヌーピング
- Q-in-Q タグ付きフレームを介した IGMPv3/v2/v1 スヌーピング
- MTP マルチキャストの最適化
- EOM を使用する BD のマルチキャスト ルーティング

サポートされていない MPLS マルチキャスト機能

- mLDP を使用した Inter-AS IPv4 マルチキャスト VPN
- mLDP を使用した Inter-AS IPv6 マルチキャスト VPN
- mLDP を使用したエッジでの IPv4 マルチキャスト トラフィック（グローバル ルーティング テーブル経由）
- P2MP RSVP TE LSP を介した、エッジでの IPv4 マルチキャスト トラフィック（グローバル ルーティング テーブル経由）

- P2MP RSVP TE LSP を介した VRF での IPv4 マルチキャスト トラフィック
- mLDP を使用した VRF での IPv4 マルチキャスト トラフィック
- mLDP を使用したエッジでの IPv6 マルチキャスト トラフィック（グローバル ルーティング テーブル経由）
- P2MP RSVP TE LSP を介した、エッジでの IPv6 マルチキャスト トラフィック（グローバル ルーティング テーブル経由）
- P2MP RSVP TE LSP を介した VRF での IPv6 マルチキャスト トラフィック
- mLDP を使用した VRF での IPv6 マルチキャスト トラフィック
- ISSU のサポート
- P2MP TE LSP に対するリンク保護（500 msec）
- P2MP TE LSP に対するノード保護（500 msec）
- SSO/NSF サポート
- mLDP を使用した IPv4 マルチキャスト VPN の Carrier Supporting Carrier（CSC）
- mLDP を使用した IPv6 マルチキャスト VPN の Carrier Supporting Carrier（CSC）
- Label Switched Multicast のための IPv4 マルチキャスト VPN に対するエクストラネット サポート
- Label Switched Multicast のための IPv6 マルチキャスト VPN に対するエクストラネット サポート
- mLDP ツリーに対するリンク保護（500 msec）
- mLDP ツリーに対するノード保護（500 msec）
- MIB のサポート

ハードウェアでサポートされているセキュリティ マルチキャスト機能

- マルチキャストとサービス ブレードの相互作用
- P2P GRE トンネルと VPNSM/IPSEC SPA モジュールの相互作用

ソフトウェアでサポートされているセキュリティ マルチキャスト機能

- IGMP スヌーピング フィルタリング

サポートされていないセキュリティ マルチキャスト機能

- マルチキャストのための CTS LinkSecurity
- RBACL および IPv4/IPv6 マルチキャスト データ パケット
- マルチキャストのための CTS 暗黙トンネル
- GDOI キー配布

IPv4 マルチキャスト レイヤ 3 機能のデフォルト設定

- マルチキャスト ルーティング：グローバルにディセーブルです。
- PIM ルーティング：すべてのインターフェイスでディセーブルです。

- IP マルチキャスト レイヤ 3 スイッチング：マルチキャスト ルーティングがイネーブルで、インターフェイスで PIM がイネーブルの場合、イネーブルです。
- IP MFIB 転送：インターフェイスで PIM がイネーブルにされている場合、イネーブルです。

Internet Group Management Protocol（IGMP）スヌーピングは、すべての VLAN インターフェイス上で、デフォルトでイネーブルに設定されています。インターフェイス上で IGMP スヌーピングをディセーブルにしても、マルチキャスト レイヤ 3 フローは引き続きハードウェアによりスイッチングされます。IGMP スヌーピングをディセーブルに設定したインターフェイス上でフローをブリッジングすると、VLAN のすべての転送インターフェイスにフラッディングが発生します。IGMP スヌーピングの設定については、第 44 章「IPv4 マルチキャスト トラフィックの IGMP スヌーピング」を参照してください。

IPv4 マルチキャスト レイヤ 3 機能の設定方法

IPv4 マルチキャスト ルーティングのグローバルなイネーブル化

レイヤ 3 インターフェイス上で IP マルチキャスト レイヤ 3 スイッチングをイネーブルにするには、事前に IP マルチキャスト ルーティングをグローバルにイネーブルにする必要があります。

IP マルチキャスト ルーティングをグローバルにイネーブルにするには、次の作業を行います。

コマンド	目的
`Router(config)# ip multicast-routing`	IP マルチキャスト ルーティングをグローバルにイネーブルにします。

次に、マルチキャスト ルーティングをグローバルにイネーブルにする例を示します。

```
Router(config)# ip multicast-routing
Router(config)#
```

レイヤ 3 インターフェイス上での IPv4 PIM のイネーブル化

レイヤ 3 インターフェイス上で IP マルチキャスト レイヤ 3 スイッチングを動作させるには、事前にレイヤ 3 インターフェイス上で PIM をイネーブルにする必要があります。

レイヤ 3 インターフェイス上で IP PIM をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {{vlan vlan_ID} | {type 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	`Router(config-if)# ip pim {dense-mode | sparse-mode | sparse-dense-mode}`	レイヤ 3 インターフェイス上で IP PIM をイネーブルにします。

次に、インターフェイス上でデフォルト モード（**sparse-dense-mode**）を使用して PIM をイネーブルにする例を示します。

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

次に、インターフェイス上で PIM sparse モードをイネーブルにする例を示します。

```
Router(config-if)# ip pim sparse-mode
```

（注）

- IP マルチキャスト レイヤ 3 スイッチングを動作させるには、事前に関与するすべてのレイヤ 3 インターフェイス上で PIM をイネーブルにする必要があります。レイヤ 3 インターフェイス上での PIM の設定手順については、「レイヤ 3 インターフェイス上での IPv4 PIM のイネーブル化」（P.43-17）を参照してください。
- PIM は、VLAN インターフェイスも含めて、任意のレイヤ 3 インターフェイス上でイネーブルに設定できます。

レイヤ 3 インターフェイス上での IP マルチキャスト レイヤ 3 スイッチングのイネーブル化

レイヤ 3 インターフェイス上で PIM をイネーブルにすると、インターフェイス上では IP マルチキャスト レイヤ 3 スイッチングがデフォルトでイネーブルになります。次の作業は、インターフェイス上で IP マルチキャスト レイヤ 3 スイッチングをディセーブルにしたあと、再びイネーブルにする場合に限り行います。

レイヤ 3 インターフェイス上で IP マルチキャスト レイヤ 3 スイッチ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	`Router(config)# interface {{vlan vlan_ID} | {type 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	`Router(config-if)# platform multicast forwarding ip`	レイヤ 3 インターフェイス上で IP マルチキャスト レイヤ 3 スイッチングをイネーブルにします。
ステップ 3	`Router(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 4	`Router # platform ip multicast syslog`	（任意）マルチキャストに関連した syslog メッセージのコンソールでの表示をイネーブルにします。

次に、レイヤ 3 インターフェイス上で IP マルチキャスト レイヤ 3 スイッチングをイネーブルにする例を示します。

```
Router(config-if)# platform multicast forwarding ip
Router(config-if)#
```

レイヤ 3 インターフェイスの IP MFIB 転送のイネーブル化

インターフェイスで MFIB 転送をディセーブルにすることは、インターフェイスの IP マルチキャスト レイヤ 3 スイッチングをディセーブルにするもう 1 つの方法です。インターフェイスで PIM がイネーブルにされている場合は、デフォルトで、着信および送信の MFIB 転送がイネーブルにされます。レイヤ 3 インターフェイス上で MFIB 転送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	`Router(config)# interface {{vlan vlan_ID} | {type 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	`Router(config-if)# ip mfib forwarding in`	レイヤ 3 インターフェイス上で MFIB 転送をイネーブルにします。
ステップ 3	`Router(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 4	`Router # [no] platform ip multicast syslog`	（任意）マルチキャストに関連した syslog メッセージのコンソールでの表示をイネーブルにします。

次に、レイヤ 3 インターフェイスで MFIB 転送をイネーブルにする例を示します。

```
Router(config-if)# ip mfib forwarding in
Router(config-if)#
```

レプリケーション モードの設定

デフォルトでは、Cisco IOS Release 15.1SY は、出力レプリケーション モードです。Supervisor Engine 2T は、入力だけのレガシー スイッチング モジュールに対する出力レプリケーションを用意しているため、出力レプリケーション モードは常にサポートされます。インストールまたは追加したモジュールによって、このレプリケーション モードは抑制されません。設定されているレプリケーション モードは変更できます。

レプリケーション 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
`Router(config)# [no] platform ip multicast routing replication egress`	レプリケーション モードを設定します。 • **platform multicast routing replication egress** コマンドは出力レプリケーション モードを設定します。 • **no platform multicast routing replication egress** コマンドは入力レプリケーション モードを設定します。 • レプリケーション モードを変更すると、トラフィックが中断する可能性があります。

次に、入力レプリケーション モードを設定する例を示します。

```
Router(config)# no platform multicast routing replication egress
```

次に、レプリケーション モードを表示する例を示します。

```
Router# show platform  multicast routing replication
Current mode of replication is Ingress
Configured mode of replication is Ingress

Slot                 Multicast replication capability
 2                              Egress
 5                              Egress
```

マルチキャスト境界の設定

マルチキャスト境界を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {{vlan vlan_ID} | {type slot/port} | {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	`Router(config-if)# ip multicast boundary access_list [filter-autorp]`	インターフェイス上で管理スコープ境界をイネーブルにします。 • *access_list* には、この境界でのトラフィックのフィルタリング用に設定されたアクセス リストを指定します。 • （任意）**filter-autorp** を指定して、この境界で自動 RP メッセージをフィルタリングします。

（注）　**filter-autorp** キーワードを設定すると、管理境界は自動 RP ディスカバリおよび通知メッセージを検証して、境界 ACL により拒否された自動 RP グループ範囲の通知を自動 RP パケットから削除します。自動 RP グループ範囲の通知が境界で許可され、通過できるのは、自動 RP グループ範囲のすべてのアドレスが境界 ACL により許可されている場合に限ります。いずれかのアドレスが許可されない場合、自動 RP メッセージが転送される前に、グループ範囲全体がフィルタリングされ、自動 RP メッセージから削除されます。

次に、すべての管理用スコープのアドレスにマルチキャスト境界を設定する例を示します。

```
Router (config)# access-list 1 deny 239.0.0.0 0.255.255.255
Router (config)# access-list 1 permit 224.0.0.0 15.255.255.255
Router (config)# interface gigabitethernet 5/2
Router (config-if)# ip multicast boundary 1
```

ローカル出力レプリケーションの確認

デュアル スイッチファブリック接続を含む DFC を装備したモジュールには、ファブリック接続ごとに 1 つずつ、合計 2 つのパケット レプリケーション エンジンがあります。それぞれのレプリケーション エンジンは、スイッチファブリック接続と関連したインターフェイスにパケットを転送したり、そのインターフェイスからパケットを転送したりします。スイッチファブリック接続と関連するインターフェイスは、パケット レプリケーション エンジン側から見て「ローカル」と見なされます。ローカル出力レプリケーション モードがイネーブルでない場合、両方のレプリケーション エンジンにすべてのモジュールの完全な発信インターフェイス リストが保持され、レプリケーション エンジンはローカルでないインターフェイスのトラフィックをいったん処理してからドロップします。

ローカル出力レプリケーション モードによって、発信インターフェイス リストが各レプリケーション エンジンをサポートするローカル インターフェイスだけに制限され、不要なマルチキャスト トラフィックの処理を防止できます。

ローカル出力レプリケーションは、次のソフトウェア設定およびハードウェアでサポートされます。

- 出力レプリケーション モード。
- デュアル ファブリック接続 DFC 搭載モジュール。
- CFC を搭載したモジュール（Supervisor Engine 2T で提供される機能）。
- レイヤ 3 EtherChannel のメンバーと VLAN インターフェイス。

次に、ローカル出力レプリケーション用に選択されたレプリケーション エンジンを確認する例を示します。

```
Router# show platform ip multicast capability
Current mode of replication is Ingress
Configured replication mode is Egress
Egress Local is Enabled
Slot Multicast replication capability Egress Local
2 Egress No
3 Egress Yes
4 Ingress No
5 Egress No
6 Egress No
```

IPv4 マルチキャスト PIM-SM レジスタ トンネル情報の表示

PIM RP に関連付けられているレジスタ トンネル インターフェイスを表示するには、**show ip pim tunnel** コマンドを入力します。

コマンド	目的
Router# **show ip pim rp mapping**	PIM RP 情報を表示します。
Router# **show ip pim tunnel**	すべてのルータの PIM Register カプセル化トンネル情報を表示します。 RP 上の追加の PIM Register カプセル開放トンネルを表示します。

次に、PIM レジスタ トンネル情報を表示する例を示します。

```
Router# show ip pim rp mapping
PIM Group-to-RP Mappings

Group(s): 224.0.0.0/4, Static
    RP: 11.1.1.1 (?)

Router# show ip pim tunnel
Tunnel0
  Type  : PIM Encap
  RP    : 11.1.1.1*
  Source: 11.1.1.1
Tunnel1*
  Type  : PIM Decap
  RP    : 11.1.1.1*
  Source: -
```

IPv4 マルチキャスト ルーティング テーブルの表示

mroute エントリを表示するには、**show ip mroute** コマンドを入力します。

コマンド	目的
Router# **show ip mroute** [*hostname* | *group_number*]	IP マルチキャスト ルーティング テーブルを表示します。

次に、IP マルチキャスト ルーティング テーブルを表示する例を示します。

```
Router# show ip mroute 225.1.1.1
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       G - Received BGP C-Mroute, g - Sent BGP C-Mroute,
       Q - Received BGP S-A Route, q - Sent BGP S-A Route,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
```

```
 Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 225.1.1.1), 00:25:35/00:02:52, RP 11.1.1.1, flags: SJC
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    GigabitEthernet1/4, Forward/Sparse-Dense, 00:21:43/00:02:52
    Vlan546, Forward/Sparse-Dense, 00:25:36/00:02:51

(22.2.2.1, 225.1.1.1), 00:25:36/00:01:49, flags: T
  Incoming interface: Vlan546, RPF nbr 0.0.0.0
  Outgoing interface list:
    GigabitEthernet1/4, Forward/Sparse-Dense, 00:21:46/00:03:24
```

IPv4 MRIB 情報の表示

show ip mrib コマンドを実行すると、IP MRIB に関する詳細情報が表示されます。詳細な MRIB 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
Router# **show ip mrib client**	MRIB に登録されているクライアントを表示します。
Router# **show ip mrib route** [*hostname* | *group_number* | **summary** | **reserved**]	MRIB ルート情報を表示します。

MRIB クライアントを表示するには、**show ip mrib client** コマンドを入力します。PFC および各 DFC で動作する MFIB は、MRIB のクライアントとして示す必要があります。次に、MRIB クライアントを表示する例を示します。

```
Router# show ip mrib client
IP MRIB client-connections
MRIB Trans for MVRF #0     table:434    (connection id 1)
IPv4_mfib(0x57D354C8):6.642     (connection id 2)
IPv4_mfib(0x555FC7D8):1.362     (connection id 3)
```

次に、MRIB テーブルを表示する例を示します。

```
Router# show ip mrib route 225.1.1.1
IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
    C - Directly-Connected Check, S - Signal, IA - Inherit Accept, D - Drop
    ET - Data Rate Exceeds Threshold,K - Keepalive,DDE - Data Driven Event
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
    LD - Local Disinterest, MD - mCAC Denied

(*,225.1.1.1) RPF nbr: 0.0.0.0 Flags: C
  Tunnel1 Flags: A
  GigabitEthernet1/4 Flags: F NS
  Vlan546 Flags: F NS

(22.2.2.1,225.1.1.1) RPF nbr: 0.0.0.0 Flags:
  Vlan546 Flags: A
  GigabitEthernet1/4 Flags: F NS
```

IPv4 MFIB 情報の表示

show ip mfib コマンドを実行すると、IP MFIB に関する詳細情報が表示されます。詳細な MFIB 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
Router# **show ip mfib interface** [*type name*]	MFIB インターフェイス情報を表示します
Router# **show ip mfib** [*hostname* | *group_number* | **global** | **verbose**]	MFIB ルート情報を表示します。
Router# **show ip mfib summary**	MFIB ステートの要約を表示します
Router# **show ip mfib status**	MFIB ステータスを表示します
Router# **show ip mfib count**	ルートおよびパケット カウント データを表示します

次に、MFIB インターフェイス情報を表示する例を示します。

```
Router# show ip mfib interface
IPv4 Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running
    Initialization State: Running
    Total signalling packets queued: 0
    Process Status: may enable - 3 - pid 642
    Tables 1/1/0 (active/mrib/io)

MFIB interface             status    CEF-based output
                                   [configured,available]
GigabitEthernet1/1         up      [yes       ,no       ]
GigabitEthernet1/2         up      [yes       ,no       ]
GigabitEthernet1/4         up      [yes       ,yes      ]
Loopback1                  up      [yes       ,yes      ]
Tunnel0                    up      [yes       ,yes      ]
Tunnel1                    up      [yes       ,no       ]
Vlan546                    up      [yes       ,yes      ]
```

次に、MFIB テーブルを表示する例を示します。

```
Router# show ip mfib 225.1.1.1
Entry Flags:    C - Directly Connected, S - Signal, IA - Inherit A flag,
                ET - Data Rate Exceeds Threshold, K - Keepalive
                DDE - Data Driven Event, HW - Hardware Installed
I/O Item Flags: IC - Internal Copy, NP - Not platform switched,
                NS - Negate Signalling, SP - Signal Present,
                A - Accept, F - Forward, RA - MRIB Accept, RF - MRIB Forward,
                MA - MFIB Accept
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:      Total/RPF failed/Other drops
I/O Item Counts:   FS Pkt Count/PS Pkt Count
Default
 (*,225.1.1.1) Flags: C HW
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   0/0/0/0, Other: 0/0/0
   Tunnel1 Flags: A
   GigabitEthernet1/4 Flags: F NS
     Pkts: 0/0
   Vlan546 Flags: F NS
     Pkts: 0/0
```

```
 (22.2.2.1,225.1.1.1) Flags: HW
   SW Forwarding: 0/0/0/0, Other: 37/0/37
   HW Forwarding:   536649628/234964/512/939858, Other: 0/0/0
   Vlan546 Flags: A
   GigabitEthernet1/4 Flags: F NS
     Pkts: 0/0
```

次に、MFIB サマリーを表示する例を示します。

```
Router# show ip mfib summary
Default
 211 prefixes (211/0/0 fwd/non-fwd/deleted)
 343 ioitems (343/0/0 fwd/non-fwd/deleted)
 Forwarding prefixes: [101 (S,G), 108 (*,G), 2 (*,G/m)]
 Table id 0x0, instance 0x57D354C8
 Database: epoch 2
```

次に、MFIB ステータスを表示する例を示します。

```
Router# show ip mfib status
IPv4 Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running
    Initialization State: Running
    Total signalling packets queued: 0
    Process Status: may enable - 3 - pid 642
    Tables 1/1/0 (active/mrib/io)
```

次に、MFIB カウントを表示する例を示します。

```
Router# show ip mfib count
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts:      Total/RPF failed/Other drops(OIF-null, rate-limit etc)
Default
 211 routes, 108 (*,G)s, 2 (*,G/m)s
Group: 224.0.0.0/4
  RP-tree,
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   0/0/0/0, Other: 0/0/0
Group: 224.0.1.40
  RP-tree,
   SW Forwarding: 0/0/0/0, Other: 0/0/0
Group: 225.1.1.1
  RP-tree,
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   0/0/0/0, Other: 0/0/0
  Source: 22.2.2.1,
   SW Forwarding: 0/0/0/0, Other: 37/0/37
   HW Forwarding:   38970288942/234961/512/939847, Other: 0/0/0
  Totals - Source count: 1, Packet count: 38970288942
```

直接接続されたエントリの表示

次に、直接接続されたサブネット エントリを表示する例を示します。

```
Router# show platform  hardware  cef | include receive
224    0.0.0.0/32            receive
225    255.255.255.255/32    receive
226    22.2.2.2/32           receive
227    22.2.2.0/32           receive
228    22.2.2.255/32         receive
229    10.10.10.10/32        receive
230    11.1.1.1/32           receive
```

```
231    11.1.1.0/32           receive
232    11.1.1.255/32         receive
3200   224.0.0.0/24          receive
198433 224.0.0.0/4           receive
```

IPv4 ハードウェア スイッチング情報の表示

show platform hardware multicast routing ip コマンドは、IP マルチキャスト レイヤ 3 スイッチングに関する詳細情報を表示します。IP マルチキャスト レイヤ 3 スイッチングに関する詳細情報を表示するには、次のうちいずれかの作業を行います。

コマンド	目的
Router# **show platform hardware multicast routing ip control**	レイヤ 3 IP マルチキャスト制御エントリを表示します。
Router# **show platform hardware multicast routing ip** [**source** *ip_address*] [**group** *ip_address* [**detail** | **verbose**]]	すべてのインターフェイスについて、IP マルチキャスト レイヤ 3 スイッチングの詳細情報を表示します。
Router# **show platform ip multicast summary**	IP マルチキャスト レイヤ 3 スイッチングの要約情報を表示します。

次に、レイヤ 3 IP マルチキャスト制御エントリを表示する例を示します。

```
Router# show platform  hardware multicast routing ip control
IPv4 Multicast CEF Entries for VPN#0
Flags: C - Control, B - Bidir, c - CoPP ELIF, Q - QoS ELIF, n - Non-primary Input
Source          Destination/mask          RPF/DF       Flags  #packets      #bytes
Output LIFs/Info
+--------------+--------------------+---------------+------+-----------+----------------
--+--------------------------+
*                  224.0.0.0/24        -              C      -           -
*                  224.0.1.39/32       -              C      -           -
*                  224.0.1.40/32       -              C      -           -
Found 3 entries.
```

次に、レイヤ 3 IP マルチキャスト スイッチング情報を表示する例を示します。

```
Router# show platform  hardware multicast routing ip source 22.2.2.1 group 225.1.1.1 de
IPv4 Multicast CEF Entries for VPN#0

(22.2.2.1, 225.1.1.1/32)
  FIBAddr: 0x20 IOSVPN: 0 RpfType:  SglRpfChk SrcRpf: Vl546
  CPx: 0 s_star_pri: 1 non-rpf drop: 0

  PIAdjPtr: 0x1C001 Format: IP rdt: off elif: 0xC5409
  fltr_en: off idx_sel/bndl_en: 0 dec_ttl: on mtu_idx: 2(1518)
  PV: 1 rwtype: MCAST_L3_REWRITE
  met3: 0x8000 met2: 0x0
  Packets: 0            Bytes: 0

  NPIAdjPtr: 0x1C002 Format: IP rdt: off elif: 0xC5409
  fltr_en: off idx_sel/bndl_en: 0 dec_ttl: off
  PV: 0 rwtype: NO_REWRITE
  smac_rwt: 0 ip_to_mac: 1
  Packets: 0            Bytes: 0
  MET offset: 0x8000
         OIF         AdjPtr      Elif        CR
    +-------------+----------+-----------+--------+
     EDT-2C001      0x2C001    0x8400A      6T1/T2
```

```
Found 1 entries.
```

次に、レイヤ 3 IP マルチキャスト スイッチング要約情報を表示する例を示します。

```
Router# show platform  hardware multicast routing ip summary
IPv4 Multicast CEF Entries Summary for VPN#0
 Slot     #shcut       #(S,G)       #(*,G)       #(*,G/m)       #Ctrl
+-----+-----------+------------+------------+------------+------------+
 6        203          101          101          1            3
```

IPv4 CoPP 情報の表示

マルチキャスト CoPP 情報を確認するために次のコマンドを使用できます。

コマンド	目的
Router# **show platform hardware multicast routing ip control**	レイヤ 3 IP マルチキャスト制御エントリを表示します。
Router# **show policy-map control-plane input class** *class_name*	コントロール プレーン ポリシーのクラス マップ情報を表示します。

次に、CoPP 情報を表示する例を示します。

```
Router# show platform  hardware  multicast  routing  ip control detail
IPv4 Multicast CEF Entries for VPN#0

(*, 224.0.0.0/24)
  FIBAddr: 0x2A0 IOSVPN: 0 RpfType: SkipRpf SrcRpf:
  CPx: 0 s_star_pri: 1 non-rpf drop: 0

  PIAdjPtr: 0x13110(IPv4 Control) Format: IP rdt: off elif: 0x9FC01
  fltr_en: off idx_sel/bndl_en: 0 dec_ttl: off mtu_idx: 0(9234)
  PV: 1 rwtype: NO_REWRITE
  smac_rwt: 0 ip_to_mac: 0

(*, 224.0.1.39/32)
  FIBAddr: 0x1E0 IOSVPN: 0 RpfType: SkipRpf SrcRpf:
  CPx: 0 s_star_pri: 1 non-rpf drop: 0

  PIAdjPtr: 0x13110(IPv4 Control) Format: IP rdt: off elif: 0x9FC01
  fltr_en: off idx_sel/bndl_en: 0 dec_ttl: off mtu_idx: 0(9234)
  PV: 1 rwtype: NO_REWRITE
  smac_rwt: 0 ip_to_mac: 0

(*, 224.0.1.40/32)
  FIBAddr: 0x1E2 IOSVPN: 0 RpfType: SkipRpf SrcRpf:
  CPx: 0 s_star_pri: 1 non-rpf drop: 0

  PIAdjPtr: 0x13110(IPv4 Control) Format: IP rdt: off elif: 0x9FC01
  fltr_en: off idx_sel/bndl_en: 0 dec_ttl: off mtu_idx: 0(9234)
  PV: 1 rwtype: NO_REWRITE
  smac_rwt: 0 ip_to_mac: 0
Found 3 entries.
```

```
Router# show policy-map control-plane input class class-copp-match-igmp

 Control Plane Interface

  Service-policy input: policy-default-autocopp

  Hardware Counters:

    class-map: class-copp-match-igmp (match-any)
      Match: access-group name acl-copp-match-igmp
      police :
        10000 pps 10000 limit 10000 extended limit
      Earl in slot 6 :
        0 packets
        5 minute offered rate 0 pps
        aggregate-forwarded 0 packets
                             action: set-discard-class-transmit
        exceeded 0 packets action: transmit
        aggregate-forward 0 pps exceed 0 pps

  Software Counters:

    Class-map: class-copp-match-igmp (match-any)
      7138 packets, 267084 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: access-group name acl-copp-match-igmp
        7138 packets, 267084 bytes
        5 minute rate 0 bps
      police:
          rate 10000 pps, burst 10000 packets
          conformed 7138 packets, 7138 bytes; action:
            set-discard-class-transmit 48
          exceeded 0 packets, 0 bytes; action:
            transmit
          conformed 0 pps, exceeded 0 pps
```

IGMPv3、IGMP v3lite、および URD を使用した送信元固有マルチキャスト

IGMPv3、IGMP v3lite、および URL Rendezvous Directory（URD）を使用した Source-Specific Multicast（SSM）の詳細および手順については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_igmp/configuration/15-sy/imc-igmp-15-sy-book.html

IPv4 双方向 PIM の設定

IPv4 双方向 PIM のグローバルなイネーブル化

IPv4 双方向 PIM 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
`Router(config)# ip pim bidir-enable`	スイッチ上で IPv4 双方向 PIM をグローバルにイネーブル化します。

次に、スイッチ上で IPv4 双方向 PIM をイネーブルにする例を示します。

```
Router(config)# ip pim bidir-enable
Router(config)#
```

IPv4 双方向 PIM グループのランデブー ポイントの設定

IPv4 双方向 PIM グループのランデブー ポイントをスタティックに設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# ip pim rp-adress ip_address access_list [override]`	グループのランデブー ポイントの IP アドレスをスタティックに設定します。**override** オプションを指定する場合、スタティック ランデブー ポイントを使用します。
ステップ 2	`Router(config)# access-list access-list [permit | deny] ip_address`	アクセス リストを設定します。
ステップ 3	`Router(config)# ip pim send-rp-announce type number scope ttl_value [group-list access-list] [interval seconds] [bidir]`	自動 RP を使用してルータがランデブー ポイント（RP）として動作するグループを設定するように、システムを設定します。
ステップ 4	`Router(config)# ip access-list standard access-list-name permit | deny ip_address`	標準 IP アクセス リストを設定します。
ステップ 5	`Router(config)# platform ip multicast`	ハードウェアでサポートされている IP マルチキャストをイネーブルにします。

次に、IPv4 双方向 PIM グループのスタティック RP を設定する例を示します。

```
Router(config)# ip pim rp-address 10.0.0.1 10 bidir override
Router(config)# access-list 10 permit 224.1.0.0 0.0.255.255
Router(config)# ip pim send-rp-announce Loopback0 scope 16 group-list c21-rp-list-0 bidir
Router(config)# ip access-list standard c21-rp-list-0 permit 230.31.31.1 0.0.255.255
```

IPv4 双方向 PIM 情報の表示

IPv4 双方向 PIM 情報を表示するには、次のうちいずれかの作業を行います。

コマンド	目的
Router# **show ip pim rp mapping** [**in-use**]	PIM グループとランデブー ポイントの間のマッピングを表示し、使用中の学習したランデブー ポイントを表示します。
Router# **show ip mfib**	双方向 PIM の MFIB 情報を表示します。
Router# **show platform hardware multicast routing ip**	IP マルチキャスト レイヤ 3 スイッチングの詳細を表示します。
Router# **show platform software multicast routing cmrp info**	割り当てられた DF インデックスと DF マスクに関する情報を表示します。
Router# **show platform ip multicast bidir**	IPv4 双方向 PIM 情報を表示します。

次に、PIM グループおよびランデブー ポイント マッピングの情報を表示する例を示します。

```
Router# show ip pim rp mapping
PIM Group-to-RP Mappings
This system is an RP (Auto-RP)
This system is an RP-mapping agent
Group(s) 230.31.0.0/16
  RP 60.0.0.60 (?), v2v1, bidir
    Info source:60.0.0.60 (?), elected via Auto-RP
         Uptime:00:03:47, expires:00:02:11
  RP 50.0.0.50 (?), v2v1, bidir
    Info source:50.0.0.50 (?), via Auto-RP
         Uptime:00:03:04, expires:00:02:55
  RP 40.0.0.40 (?), v2v1, bidir
    Info source:40.0.0.40 (?), via Auto-RP
         Uptime:00:04:19, expires:00:02:38
```

次に、IPv4 双方向 PIM に関連した IP マルチキャスト ルーティング テーブルの情報を表示する例を示します。

```
Router# show ip mroute bidirectional
(*,224.0.0.0/4), 00:17:18/-, RP 20.2.2.2, flags: B
  Bidir-Upstream: Loopback2, RPF nbr: 20.2.2.2
  Incoming interface list:
    TenGigabitEthernet3/8, Accepting/Sparse-Dense
    TenGigabitEthernet3/7, Accepting/Sparse-Dense
    GigabitEthernet1/12, Accepting/Dense
    GigabitEthernet1/1, Accepting/Sparse-Dense
    Port-channel2, Accepting/Sparse-Dense
    Loopback100, Accepting/Sparse-Dense
    Loopback10, Accepting/Sparse-Dense
    Loopback2, Accepting/Sparse-Dense

(*, 224.1.1.1), 00:17:18/00:02:26, RP 20.2.2.2, flags: BC
  Bidir-Upstream: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    TenGigabitEthernet3/8, Forward/Sparse-Dense, 00:17:17/00:02:26
```

次に、IPv4 双方向 PIM に関連した MFIB テーブルを表示する例を示します。

```
Router# show ip mfib
Entry Flags:    C - Directly Connected, S - Signal, IA - Inherit A flag,
```

```
                ET - Data Rate Exceeds Threshold, K - Keepalive
                DDE - Data Driven Event, HW - Hardware Installed
I/O Item Flags: IC - Internal Copy, NP - Not platform switched,
                NS - Negate Signalling, SP - Signal Present,
                A - Accept, F - Forward, RA - MRIB Accept, RF - MRIB Forward,
                MA - MFIB Accept
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:      Total/RPF failed/Other drops
I/O Item Counts:   FS Pkt Count/PS Pkt Count
Default
 (*,224.0.0.0/4) Flags: HW   ?- Indicates that Entry is installed in hardware
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   0/0/0/0, Other: 0/0/0
   GigabitEthernet1/1 Flags: A
   GigabitEthernet1/12 Flags: A
   TenGigabitEthernet3/7 Flags: A
   TenGigabitEthernet3/8 Flags: A
   Port-channel2 Flags: A
   Loopback100 Flags: A
   Loopback10 Flags: A
   Loopback2 Flags: A F
     Pkts: 0/0
   Null0 Flags: A
  (*,224.1.1.1) Flags: IA HW
   SW Forwarding: 0/0/0/0, Other: 3/3/0
   HW Forwarding:   3357168/3000/100/2343, Other: 0/0/0 ?--- Hw Forwarding Statistics
   TenGigabitEthernet3/7 Flags: F
     Pkts: 0/0
   TenGigabitEthernet3/8 Flags: F
     Pkts: 0/0
```

次に、IPv4 双方向 PIM に関連したハードウェア スイッチング テーブルを表示する例を示します。

```
Router# show platform hardware multicast routing ip group 224.0.0.0/4
IPv4 Multicast CEF Entries for VPN#0
Flags: C - Control, B - Bidir, c - CoPP ELIF, Q - QoS ELIF, n - Non-primary Input
Source          Destination/mask          RPF/DF       Flags  #packets      #bytes
Output LIFs/Info
+--------------+---------------------+----------------+------+-----------+----------------
--+--------------------------+
*                   224.0.0.0/4          0       B      0           0
*                   224.1.1.1/32         0       B      6539001     653900100
Te3/7, Te3/8 [2 oif(s)]
Found 2 entries.
```

次に、IPv4 双方向 PIM に関連した DF インデックスと DF マスク情報を表示する例を示します。

```
Router# show platform software multicast routing cmrp info

Replication Mode Information:
================================
  repl_mode: Ingress; pending_repl_mode: Ingress;
  notify_repl_mode: Ingress; repl_mode_chng_in_prog: 0;
  repl_mode_notif_pending: 0

Resource Information:
=======================
  fib_full_mask: 0x0; adj_full_mask: 0x0;
  met_full_mask: 0x0; met_unavail_mask: 0x0

Global HA Information:
=======================
  reconstruct_in_prog: 0; reconstruct_lc_mask: 0x0
```

```
Vrf Name: R; Vrf ID: 3; Df Idx Allocated: 8; mfib_sweep_mask: 0x0
================================================================================
  DF Idx Info for df_idx: 0
  ============================
  coll_obj: 0x530493CC; af:ipv4; df_state: USED
    DF Collection Obj Info
    ======================
    ref_count: 1; id_count: 4; app_data: 0x19D1D1A8; vrf_id: 3; df_idx: 0; cleanup: 0
    DF Set
    =======
    Tu100 (0x320004072), Tu108 (0x32000407A), Nu0 (0x32000407B), Tu3 (0x32000407F),
  DF Idx Info for df_idx: 1
  ============================
  coll_obj: 0x530493EC; af:ipv4; df_state: USED
    DF Collection Obj Info
    ======================
    ref_count: 1; id_count: 4; app_data: 0x19C3C740; vrf_id: 3; df_idx: 1; cleanup: 0
    DF Set
    =======
    Tu101 (0x320004073), Tu108 (0x32000407A), Nu0 (0x32000407B), Tu3 (0x32000407F),
  DF Idx Info for df_idx: 2
  ============================
  coll_obj: 0x5304936C; af:ipv4; df_state: USED
    DF Collection Obj Info
    ======================
    ref_count: 1; id_count: 4; app_data: 0x19D4D938; vrf_id: 3; df_idx: 2; cleanup: 0
    DF Set
    =======
    Tu102 (0x320004074), Tu108 (0x32000407A), Nu0 (0x32000407B), Tu3 (0x32000407F),
  DF Idx Info for df_idx: 3
  ============================
  coll_obj: 0x530492EC; af:ipv4; df_state: USED
    DF Collection Obj Info
    ======================
    ref_count: 1; id_count: 4; app_data: 0x19CE6338; vrf_id: 3; df_idx: 3; cleanup: 0
    DF Set
    =======
    Tu103 (0x320004075), Tu108 (0x32000407A), Nu0 (0x32000407B), Tu3 (0x32000407F),
  DF Idx Info for df_idx: 4
  ============================
  coll_obj: 0x5304930C; af:ipv4; df_state: USED
    DF Collection Obj Info
    ======================
    ref_count: 1; id_count: 4; app_data: 0x5C092894; vrf_id: 3; df_idx: 4; cleanup: 0
    DF Set
    =======
    Tu104 (0x320004076), Tu108 (0x32000407A), Nu0 (0x32000407B), Tu3 (0x32000407F),
  DF Idx Info for df_idx: 5
  ============================
  coll_obj: 0x530493AC; af:ipv4; df_state: USED
    DF Collection Obj Info
    ======================
    ref_count: 1; id_count: 4; app_data: 0x19D4D7FC; vrf_id: 3; df_idx: 5; cleanup: 0
    DF Set
    =======
    Tu105 (0x320004077), Tu108 (0x32000407A), Nu0 (0x32000407B), Tu3 (0x32000407F),
  DF Idx Info for df_idx: 6
  ============================
  coll_obj: 0x5304934C; af:ipv4; df_state: USED
    DF Collection Obj Info
    ======================
    ref_count: 1; id_count: 4; app_data: 0x19D4DC58; vrf_id: 3; df_idx: 6; cleanup: 0
    DF Set
    =======
```

```
  Tu106 (0x320004078), Tu108 (0x32000407A), Nu0 (0x32000407B), Tu3 (0x32000407F),
DF Idx Info for df_idx: 7
============================
coll_obj: 0x5304938C; af:ipv4; df_state: USED
  DF Collection Obj Info
  ======================
  ref_count: 1; id_count: 4; app_data: 0x5C09AD64; vrf_id: 3; df_idx: 7; cleanup: 0
  DF Set
  =======
  Tu107 (0x320004079), Tu108 (0x32000407A), Nu0 (0x32000407B), Tu3 (0x32000407F),
```

IPv4 デバッグ コマンドの使用

表 43-1 に、IPv4 マルチキャスト レイヤ 3 スイッチングのデバッグ コマンドを示します。これらのコマンドを使用して、IP マルチキャスト レイヤ 3 スイッチングの問題をトラブルシューティングできます。

表 43-1　IP マルチキャスト レイヤ 3 スイッチングのデバッグ コマンド

コマンド	説明
[no] debug platform software multicast routing cmrp {event | error} [verbose]	CMRP 関連イベントおよびエラーをデバッグします。
[no] debug platform software multicast routing edc server [event | error]	出力配布サーバ コンポーネントのエラーおよびイベントをデバッグします。
[no] debug platform software multicast routing edc client [event | error]	出力配布クライアント コンポーネントのエラーおよびイベントをデバッグします。
[no] debug platform software multicast routing hal [event | error]	マルチキャスト Hardware Abstraction Layer のエラーおよびイベントをデバッグします。
[no] debug platform software multicast routing cmfib [event | error]	コンステレーション MFIB コンポーネントのエラーおよびイベントをデバッグします。
[no] debug platform software met [event | error | detail | all]	MET マネージャのエラーおよびイベントをデバッグします。
[no] debug platform software filter *filter_id* {ip {destination | source} *ip_address* [*mask*] | string {exclude | include} *text_string*}	IPv4 の宛先アドレスまたは送信元アドレス、または入力文字列に基づいてメッセージをデバッグするためのフィルタリングをオンにします。

マルチキャスト トラフィックの冗長性

マルチキャスト トラフィックの冗長性には、次の条件が必要です。

- OSPF や EIGRP などのユニキャスト ルーティング プロトコル。

  PIM では、ユニキャスト ルーティング テーブルに対する RPF チェックを使用して、マルチキャスト データが通過する適切なパスを決定します。ユニキャスト ルーティング パスが変更されると、PIM は適切にコンバージするためにユニキャスト ルーティング プロトコル（OSPF）に依存するので、PIM で使用される RPF チェックは引き続き機能し、マルチキャスト ストリームを発信するサーバの発信元 IP アドレスとの間の有効なユニキャスト パスを表示します。

- 関連するすべてのレイヤ 3 インターフェイスに設定された PIM。

ユニキャスト ルーティング テーブルは、PIM のパスの選択に使用されます。PIM は RPF チェックを使用して、クライアント（受信者 VLAN）と発信元（マルチキャスト VLAN）の間の最終的な最短パス ツリー（SPT）を決定します。したがって、PIM の目的は、受信者サブネットと発信元サブネットの間の最短ユニキャスト パスを見つけることにあります。ユニキャスト ルーティング プロトコルが予期したとおりに動作しており、ユニキャスト ルーティング プロトコルに関連付けられたすべてのレイヤ 3 リンクに PIM が設定されている場合には、マルチキャストに他の設定を行う必要はありません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

IPv4 マルチキャスト トラフィックの IGMP スヌーピング

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。
- IPv6 マルチキャスト トラフィックを抑制する場合は、第 51 章「IPv6 MLD スヌーピング」を参照してください。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

IGMP スヌーピングの前提条件

なし。

IGMP スヌーピングの制約事項

一般的な IGMP スヌーピングの制約事項

- PIM スヌーピングが VLAN でイネーブルであり、IGMP スヌーピングが VLAN でディセーブルである場合、マルチキャスト パケットは、IGMP Join を送信するローカル レシーバへブリッジングされません。（CSCta03980）
- IP マルチキャストおよび IGMP の詳細については、RFC 1112 および RFC 2236 を参照してください。
- IGMP スヌーピングは、プライベート VLAN をサポートします。プライベート VLAN は、IGMP スヌーピングに制約を課しません。
- IGMP スヌーピングは MAC マルチキャスト グループ 0100.5e00.0001 ～ 0100.5eff.ffff のトラフィックを抑制します。
- 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 マルチキャストは抑制しません。

IGMP スヌーピング クエリアの制約事項

- IGMP スヌーピング クエリアはクエリア選択をサポートしません。VLAN 内の 1 つのスイッチだけで IGMP スヌーピング クエリアをイネーブルにします。（CSCsk48795）。
- グローバル コンフィギュレーション モードで VLAN を設定してください（第 25 章「仮想ローカル エリア ネットワーク（VLAN）」を参照）。
- VLAN インターフェイスの IP アドレスを設定してください（第 34 章「レイヤ 3 インターフェイス」を参照）。IGMP スヌーピング クエリアは、イネーブルの場合この IP アドレスをクエリーの送信元アドレスとして使用します。
- VLAN インターフェイスに IP アドレスが設定されていないと、IGMP スヌーピング クエリアは起動しません。IP アドレスが消去されると、IGMP スヌーピング クエリアは自身をディセーブルにします。IGMP スヌーピング クエリアをイネーブルにした場合、IP アドレスが設定されていれば、IGMP スヌーピング クエリアが再起動します。
- IGMP スヌーピング クエリアは、IGMPv3 クエリア メッセージを送信します。クエリア メッセージの IGMP バージョンは設定できませんが、クエリアは IGMPv2 ホストと互換性があります。
- IGMP スヌーピング クエリアは、イネーブルの場合、マルチキャスト ルータから IGMP トラフィックが検出されなければ、60 秒後に起動します。IGMP スヌーピング クエリアの起動後、マルチキャスト ルータまたは VLAN 内の他の IGMP スヌーピング クエリアからの IGMP トラフィックが検出されると、クエリアはディセーブルになります。
- IGMP スヌーピングがイネーブルの場合、QoS は IGMP パケットをサポートしません。
- リリース 15.1(1)SY1 以降のリリースでは、IGMP スヌーピングおよび PIM スヌーピングによって VPLS マルチキャスト トラフィックが抑制されます。

IGMP スヌーピングの情報

IGMP スヌーピングの概要

IGMP スヌーピングにより、スイッチで IGMP パケットを調べたり、パケットの内容に基づいて転送先を決定したりできます。IGMP または IGMP スヌーピング クエリアからの IGMP クエリーを受信するサブネットで、IGMP スヌーピングを使用するように、スイッチを設定できます。IGMP スヌーピングは、IPv4 マルチキャスト トラフィックを受信するポートだけにそのトラフィックをダイナミックに転送するように、レイヤ 2 LAN ポートを設定することにより、レイヤ 2 で IPv4 マルチキャスト トラフィックを抑制します。

一部のアプリケーションでは、単一のユニキャスト クラスタ IP アドレスおよびマルチキャスト クラスタ MAC アドレスを使用します。ユニキャスト クラスタ IP アドレスにアドレス指定されたマルチキャスト トラフィックは、共有マルチキャスト MAC アドレスで設定されているラスト ホップ ルータに転送されます。クラスタにアドレス指定されたマルチキャスト トラフィックをサポートするには、エンド ホストまたはクラスタの宛先 IP アドレスに対するスタティック マルチキャスト MAC アドレスを割り当てます。

IGMP スヌーピング検索方法は、VLAN ごとに設定できます。レイヤ 3 IGMP スヌーピング検索では、レイヤ 2 マルチキャスト テーブルの宛先 IP アドレスを使用します（これがデフォルト）。レイヤ 2 IGMP スヌーピング検索では、レイヤ 2 マルチキャスト テーブルの宛先 MAC アドレスを使用します。

（注）　検索モードを変更すると、中断が発生します。マルチキャスト転送は、すべてのマルチキャスト エントリが新しい検索モードでプログラムされるまで、最適ではありません。また、32 個の IP アドレスが 1 つの MAC アドレスにマッピングされていると、このデバイスでの転送は、準最適である場合があります。

IGMP は、マルチキャスト ルータのレイヤ 3 で稼働し、マルチキャスト トラフィックのルーティングが必要なサブネットでレイヤ 3 IGMP クエリーを生成します。

IGMP スヌーピング クエリアをスイッチに設定して、マルチキャスト ルータ インターフェイスがないサブネットにおいて IGMP スヌーピングをサポートできます。IGMP スヌーピング クエリアの詳細については、「IGMP スヌーピング クエリアのイネーブル化」（P.44-9）を参照してください。

IGMP（マルチキャスト ルータ上）またはローカルで、IGMP スヌーピング クエリアは、スイッチが VLAN のすべてのポートを通じて転送する、一般的な IGMP クエリーを定期的に送信し、ホストがそれに応答します。IGMP スヌーピングはレイヤ 3 IGMP トラフィックをモニタします。

（注）　マルチキャスト グループで、VLAN 中に送信元だけがありレシーバがない場合は、IGMP スヌーピングはマルチキャスト トラフィックをマルチキャスト ルータ ポート宛てだけに抑制します。

マルチキャスト グループへの加入

ホストは、マルチキャスト ルータからの一般的なクエリーに応じて、非送信請求 IGMP Join メッセージを送信するか、または IGMP Join メッセージを送信して、マルチキャスト グループに参加します（スイッチは、一般的なクエリーを、マルチキャスト ルータから VLAN 中のすべてのポートに転送します）。

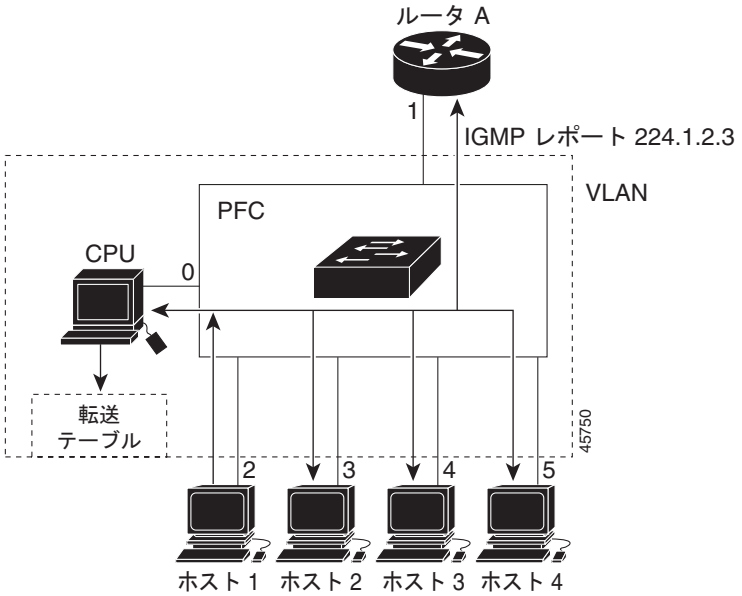
IGMP Join 要求の応答で、スイッチは、Join 要求を受信した VLAN のレイヤ 2 転送テーブルにエントリを 1 つ作成します。このマルチキャスト トラフィックに関係する別のホストが IGMP Join 要求を送信する場合、スイッチは、既存のレイヤ 2 転送テーブル エントリに要求を追加します。スイッチは、IGMP Join 要求を受信する各マルチキャスト グループ用レイヤ 2 転送テーブルで、VLAN あたり 1 つのエントリだけを生成します。

IGMP スヌーピングは、マルチキャスト グループごとに 1 つを残して他のすべてのホスト応答を抑制し、その 1 つの Join メッセージだけをマルチキャスト ルータに転送します。

スイッチは、Join メッセージで指定されたマルチキャスト グループ用のマルチキャスト トラフィックを、Join メッセージを受信したインターフェイスに転送します（図 44-1 を参照）。

IGMP スヌーピングを通じて学習されるレイヤ 2 マルチキャスト グループは、ダイナミックです。ただし、**mac address-table static** コマンドを使用して、レイヤ 2 マルチキャスト グループをスタティックに設定することもできます。マルチキャスト グループ アドレスのグループ メンバーシップをスタティックに指定した場合、そのスタティックな設定は、IGMP スヌーピングの学習よりも優先されます。マルチキャスト グループ メンバーシップのリストは、スタティックな設定値と、IGMP スヌーピングによって学習された設定値の両方で構成できます。

図 44-1　　最初の IGMP Join メッセージ



マルチキャスト ルータ A がスイッチに一般的なクエリーを送信し、ルータがそのクエリーをポート 2 ～ 5（同じ VLAN 内のすべてのメンバ）に転送します。ホスト 1 はマルチキャスト グループ 224.1.2.3 への加入を希望し、IGMP メンバーシップ レポート（IGMP Join メッセージ）を同等の MAC 宛先アドレス 0x0100.5E01.0203 を持つグループにマルチキャストします。CPU が、ホスト 1 による IGMP レポート マルチキャストを受信すると、この CPU は IGMP レポート内の情報を利用して、転送テーブル エントリを設定します。これには、ホスト 1 のポート番号、マルチキャスト ルータ、スイッチの内部 CPU が含まれます。

CPU は、検索の種類（IP または MAC、デフォルトでは、IP ベース）に基づいてスヌーピング転送エントリをインストールします。IP ベースの転送を使用すると、グループ アドレス エイリアス問題が回避され、グループごとまたはグループと送信元ごとに転送を最適化できます。

IP ベースが設定されている場合、IGMP スヌーピング転送テーブルには、次のエントリがあります。スイッチのエンジンは、マルチキャスト データ パケットの宛先 IP アドレスのマッチングを行います。これらが 224.1.2.3 の場合、グループおよびマルチキャスト ルータに参加しているホストに送信します。

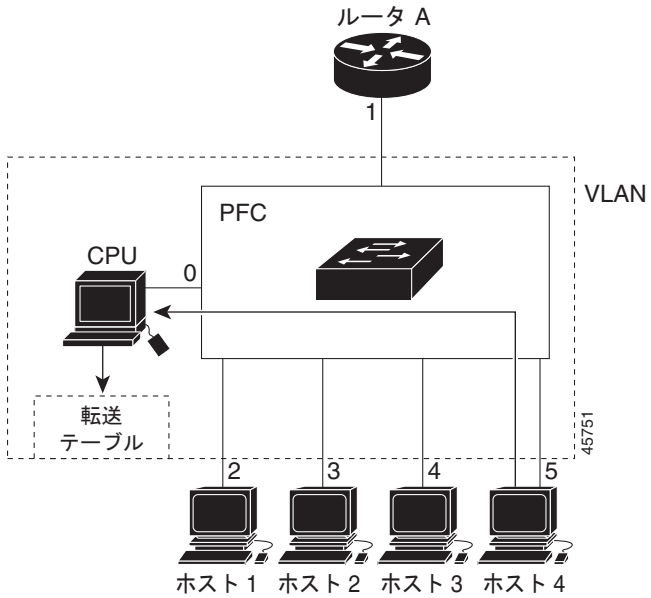
```
vlan        mac/ip address                          LTL         ports
+----+----------------------------------------+------+----------------------
200         ( *,224.1.2.3)                         0x924    Router, Gi3/11
```

MAC ベースが設定されている場合、エントリは次のように設定されます。この場合、スイッチ エンジンは、パケットの宛先 MAC アドレスのマッチングを行います。0100.5e01.0203 のパケットは、グループおよびマルチキャスト ルータに参加しているホストに送信されます。

```
vlan        mac/ip address                          LTL         ports
+----+----------------------------------------+------+----------------------
200         0100.5e01.0203                          0x92C    Router, Gi3/11
```

別のホスト（たとえば、ホスト 4）が、同じグループ用に非送信請求 IGMP Join メッセージを送信する場合（図 44-2 を参照）、CPU がそのメッセージを受け取り、ホスト 4 のポート番号を転送テーブルに追加します。転送テーブルは CPU 宛てだけに IGMP メッセージを送るので、メッセージは他のポートへフラッディングされません。認識されているマルチキャスト トラフィックは、CPU 宛てではなくグループ宛てに転送されます。

図 44-2　　2 番めのホストのマルチキャスト グループへの加入




```
vlan        mac/ip address                          LTL        ports
+----+----------------------------------------+------+----------------------
200         ( *,224.1.2.3)                         0x924    Router, Gi3/11, Gi1/10
```

マルチキャスト グループからの脱退

通常の脱退処理

関係するホストは、一般的 IGMP クエリーに定期的に応答を続ける必要があります。VLAN 中の少なくとも 1 つのホストが一般的 IGMP クエリーに定期的に応答している限り、マルチキャスト ルータはマルチキャスト トラフィックを VLAN に転送し続けます。ホストをマルチキャスト グループから脱退させたい場合は、そのホストで定期的な一般 IGMP クエリーを無視するか（「暗黙的脱退」と呼びます）、またはグループ固有の IGMPv2 Leave メッセージを送信します。

IGMP スヌーピングがグループ固有の IGMPv2 Leave メッセージをホストから受信すると、MAC ベースの一般的なクエリーを送信して、そのインターフェイスに接続されている他のデバイスがその特定のマルチキャスト グループに対するトラフィックに関係があるかどうかを判断します。IGMP スヌーピングが、この一般的クエリーに応答して IGMP Join メッセージを受信しなかった場合、インターフェイスに接続されている他のデバイスの中に、このマルチキャスト グループのトラフィックの受信に関与しているデバイスはないと見なし、マルチキャスト グループに対応するレイヤ 2 転送テーブル エントリからそのインターフェイスを削除します。残りのインターフェイスのうち、グループに関係するホストのインターフェイスだけから Leave メッセージが送信され、一般的なクエリーに応答する IGMP Join メッセージを IGMP スヌーピングが受信しない場合、IGMP スヌーピングはグループ エントリを削除して、IGMP 脱退をマルチキャスト ルータにリレーします。マルチキャスト ルータが VLAN からレポートを受信しない場合、マルチキャスト ルータは IGMP キャッシュからその VLAN 用のグループを削除します。

テーブル エントリを更新するまでスイッチが待機する時間は、「最終メンバ クエリー時間」といいます。時間を設定するには、**ip igmp snooping last-member-query-interval** *interval* コマンドを入力します。

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、IGMP スヌーピングは、最初にレイヤ 2 LAN インターフェイスに IGMP グループ対象のクエリーを送信せずに、転送テーブル エントリからそのインターフェイスを削除します。グループ特定の IGMPv2 Leave メッセージを受信すると、IGMP スヌーピングはすぐに、そのマルチキャスト グループ用のレイヤ 2 転送テーブル エントリからインターフェイスを削除します（ポート上でマルチキャスト ルータが学習された場合は除きます）。即時脱退処理により、スイッチド ネットワークにあるすべてのホストの帯域幅管理が強化されます。

（注）　即時脱退処理は、各レイヤ 2 LAN ポートに 1 つのホストのみが接続されている VLAN に限って使用してください。レイヤ 2 LAN ポートに複数のホストが接続されている VLAN 上で即時脱退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。即時脱退処理は、IGMP バージョン 2 およびバージョン 3 のホストについてだけサポートされます。

IGMP スヌーピング クエリアについて

マルチキャスト トラフィックをルーティングする必要がないため、PIM および IGMP を設定していない VLAN 内で IGMP スヌーピングをサポートするには、IGMP スヌーピング クエリアを使用します。

IP マルチキャスト ルーティングが設定されているネットワークでは、IP マルチキャスト ルータは IGMP クエリアとして機能します。VLAN の IP マルチキャスト トラフィックに、レイヤ 2 スイッチングだけを行う必要がある場合、IP マルチキャスト ルータは必要ではありません。ただし、VLAN 上に IP マルチキャスト ルータがない場合には、クエリーを送信できるよう他のスイッチを IGMP クエリアとして設定する必要があります。

IGMP スヌーピング クエリアは、イネーブルの場合、定期的に IGMPv3 クエリーを送信し、IP マルチキャスト トラフィックを受信するスイッチからの IGMP レポート メッセージをトリガーします。IGMP スヌーピングはこれらの IGMP レポートを待ち受けて、適切な転送を確立します。

IGMP を使用して IP マルチキャスト トラフィックへの関与をレポートするスイッチでサポートされている VLAN ごとに、1 つのスイッチを IGMP スヌーピング クエリアとして設定します。

IP マルチキャスト ルーティングがイネーブルであるかどうかにかかわらず、VLAN 上で IGMP クエリーを生成するようにスイッチを設定できます。

IGMP バージョン 3 サポートについて

IGMP バージョン 3 サポートの概要

IGMP スヌーピングは、IGMP バージョン 3（IGMPv3）をサポートします。IGMPv3 は送信元ベースのフィルタリングを使用します。これによりホストおよびルータは、特定のマルチキャスト グループで許可またはブロックされる送信元アドレスを指定できます。IGMPv3 スヌーピングをイネーブルにした場合、スイッチは特定の VLAN の特定のグループ用に受信したメッセージに基づいて IGMPv3 ステートを維持し、このメッセージ内の次の情報に基づいてトラフィックを許可またはブロックします。

- 送信元リスト
- 許可（include）またはブロック（exclude）フィルタリング オプション

ホストが限定された特定の送信元からのマルチキャスト トラフィックを受信する必要がある場合、ソース フィルタリングによって IGMPv3 join を送信できます。たとえば、ポート 3/11 の host1 が送信元 10.1.1.1 からグループ 224.1.2.3 へ join を送信し、ポート 3/12 の host2 が異なる送信元 20.1.1.1 から同じグループに join を送信するとき、IP ベースの検索が設定されている場合は、次のエントリが転送テーブルにインストールされます。

```
vlan         mac/ip address                          LTL      ports
+----+---------------------------------------+------+----------------------
200         ( *,224.1.2.3)                        0x920
200         (10.1.1.1,224.1.2.3)                  0x93E    Gi3/11
200         (20.1.1.1,224.1.2.3)                  0x940    Gi3/12
```

2 番めのエントリは、送信元 10.1.1.1 から host1 だけにグループ トラフィックを限定し、3 番めのエントリは、送信元 20.1.1.1 から Host2 へトラフィックを限定します。最初のエントリは、他の発信元を対象とする受信者が存在しないので、他の発信元からのグループ トラフィックをドロップします。

IGMPv3 即時脱退処理

明示的ホスト トラッキングがイネーブルの場合、IGMPv3 即時脱退処理はアクティブになります。IGMP バージョン 2 即時脱退処理をイネーブルにする **ip igmp snooping immediate-leave** コマンドは、IGMPv3 即時脱退処理には影響しません。

IGMPv3 での即時脱退処理は、ソフトウェアの送信元グループ ベースのメンバーシップ情報を維持し、LTL インデックスを MAC GDA 単位で割り当てることによって実装されます。

即時脱退処理がアクティブになると、ホストは送信元からこれ以上トラフィックを受信しない場合に特定のグループに対し BLOCK_OLD_SOURCES{src-list} メッセージを送信します。このようなメッセージをホストから受信すると、スイッチは所定のグループに対応するホストの送信元リストを解析します。この送信元リストが脱退メッセージで受信された送信元リストとまったく同じである場合、スイッチはこのホストを LTL インデックスから削除し、ホストへのマルチキャスト グループ トラフィックの転送を停止します。

送信元リストが一致しない場合、このホストがどの送信元からのトラフィック受信にも関与しなくなるまで、スイッチは LTL インデックスからホストを削除しません。

プロキシ レポート機能

IGMP では、IGMPv1 メッセージおよび IGMPv2 メッセージでプロキシ レポート機能がサポートされ、グループ固有のクエリーが処理されます。このクエリーはダウンストリームに送信されませんが、スイッチはクエリーに直接応答します。スイッチは、グループ固有のクエリーを受信すると、グループのレシーバがある場合、クエリーを終了して IGMP プロキシ レポートを送信します。IGMPv3 メッセージには、プロキシ レポート機能がありません。IGMPv3 の場合は、グループ固有のクエリーまたはグループ送信元固有のクエリーが、すべての VLAN メンバ ポートにフラッディングされます。IGMPv3 メンバーシップ レポートのデータベースは、受信レポートに基づいて構築されます。

特定クエリーに応答するホスト レポートは、レポート抑制機能によって抑制できます。レポート抑制は、IGMPv1、IGMPv2、および IGMPv3 メッセージに関してサポートされています。レポート抑制がイネーブルな状態では（デフォルト）、スイッチが、一般クエリーを受信したとき、すべてのホストから各グループまたはチャネル（S,G）へのレポート抑制サイクルを開始します。検出されたマルチキャスト ルータへの最初のレポートだけが転送されます。これ以外のレポートは、抑制されます。IGMPv1 および IGMPv2 の場合、抑制の時間は、一般クエリー メッセージに示されているレポート応答時間です。IGMPv3 の場合、抑制は一般クエリー時間全体で行われます。

（注）　このステートはソフトウェアでのみ維持され、明示的なホスト トラッキングおよび統計情報収集に使用されます。

明示的なホスト トラッキング

IGMPv3 では、ポート上のメンバーシップ情報の明示的なトラッキングをサポートします。明示的なトラッキング データベースは、IGMPv3 ホストの即時脱退処理、プロキシ レポート機能、統計情報収集に使用されます。VLAN で明示的なトラッキングがイネーブルの場合、IGMP スヌーピング ソフトウェアはホストから受信する IGMPv3 レポートを処理し、次の情報を含む明示的なトラッキング データベースを作成します。

- ホストに接続されたポート
- ホストによって報告されたチャネル
- ホストによって報告された各グループのフィルタ モード
- ホストによって報告された各グループの送信元リスト

- 各グループのルータ フィルタ モード
- 送信元を要求するグループごとのホスト リスト

（注）
- 明示的なトラッキングがイネーブル化されていて、スイッチがプロキシレポート モードで動作している場合、ルータは VLAN インターフェイスの背後にあるホストの一部を追跡できないことがあります。

IGMP スヌーピングのデフォルト設定

なし。

IGMP スヌーピングの設定方法

- 「IGMP スヌーピング クエリアのイネーブル化」（P.44-9）
- 「IGMP スヌーピングのイネーブル化」（P.44-10）
- 「IGMP スヌーピング検索方法の設定」（P.44-11）
- 「マルチキャスト レシーバへのスタティック接続の設定」（P.44-12）
- 「マルチキャスト ルータ ポートのスタティックな設定」（P.44-12）
- 「IGMP スヌーピング クエリー時間の設定」（P.44-12）
- 「IGMP スヌーピング即時脱退処理のイネーブル化」（P.44-13）
- 「IGMPv3 スヌーピングの明示的ホスト トラッキングの設定」（P.44-13）
- 「IGMP スヌーピング情報の表示」（P.44-14）

（注）IGMP スヌーピングを使用するには、マルチキャスト ルーティングできるようにサブネットでレイヤ 3 インターフェイスを設定するか（第 43 章「IPv4 マルチキャスト レイヤ 3 機能」を参照）、またはサブネットで IGMP スヌーピング クエリアをイネーブルにします（「IGMP スヌーピング クエリアのイネーブル化」（P.44-9）を参照）。

IGMP スヌーピング クエリアのイネーブル化

マルチキャスト トラフィックをルーティングする必要がないため、PIM および IGMP を設定していない VLAN 内で IGMP スヌーピングをサポートするには、IGMP スヌーピング クエリアを使用します。VLAN で IGMP スヌーピング クエリア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	`Router(config)# ip igmp snooping querier`	IGMP スヌーピング クエリアをグローバルにイネーブルにします。
ステップ 2	`Router(config)# vlan configuration vlan_ID`	VLAN を選択します。
ステップ 3	`Router(config-vlan-config)# ip igmp snooping querier address ip_address`	IP アドレスを割り当てます。

	コマンド	目的
ステップ 4	`Router(config-vlan-config)# ip igmp snooping querier`	VLAN で IGMP スヌーピング クエリアをイネーブルにします。
ステップ 5	`Router(config-vlan-config)# end`	コンフィギュレーション モードを終了します。

次に、VLAN 200 で IGMP スヌーピング クエリアをイネーブルにし、設定を確認する例を示します。

```
Router(config)# ip igmp snooping querier
Router(config)# vlan configuration 200
Router(config-vlan-config)# ip igmp snooping querier address 10.1.1.1
Router(config-vlan-config)# igmp snooping querier
Router(config-vlan-config)# end
```

IGMP スヌーピングのイネーブル化

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	`Router(config)# ip igmp snooping`	IGMP スヌーピングをイネーブルにします。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

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。

```
Router(config)# ip igmp snooping
Router(config)# end
Router# show ip igmp interface vlan 200 | include globally
  IGMP snooping is globally enabled
Router#
```

VLAN における IGMP スヌーピングのイネーブル化

特定の VLAN 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	`Router(config)# vlan configuration` *vlan_ID*	VLAN を選択します。
ステップ 2	`Router(config-vlan-config)# ip igmp snooping`	IGMP スヌーピングをイネーブルにします。
ステップ 3	`Router(config-vlan-config)# end`	コンフィギュレーション モードを終了します。

次に、VLAN 25 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。

```
Router# vlan configuration 25
Router(config-vlan-config)# ip igmp snooping
Router(config-vlan-config)# end
Router# show ip igmp snooping vlan 25
Global IGMP Snooping configuration:
```

```
-----------------------------------------
IGMP snooping Oper State    : Enabled
IGMPv3 snooping             : Enabled
Report suppression          : Disabled
EHT DB limit/count          : 100000/2
TCN solicit query           : Disabled
Robustness variable         : 2
Last member query count     : 3
Last member query interval  : 1000
Check TTL=1                 : No
Check Router-Alert-Option   : No

Vlan 25:
--------
IGMP snooping Admin State    : Enabled
IGMP snooping Oper State     : Enabled
IGMPv2 immediate leave       : Disabled
Explicit host tracking       : Enabled
Report suppression           : Enabled
Robustness variable          : 2
Last member query count      : 2
Last member query interval   : 1000
EHT DB limit/count           : 100000/2
Check TTL=1                  : Yes
Check Router-Alert-Option    : Yes
Query Interval               : 100
Max Response Time            : 10000
Router#
```

IGMP スヌーピング検索方法の設定

VLAN の IGMP スヌーピング検索方法を設定するには、次の作業を行います。

コマンド	目的
`Router(config-vlan-config)# multicast snooping lookup {ip | mac}`	VLAN の IGMP スヌーピング検索方法を設定します。 • IP アドレスを使用してマルチキャスト トラフィックを転送するには **ip** キーワードを入力します。 • 宛先 MAC アドレスを使用してマルチキャスト トラフィックを転送するには **mac** キーワードを入力します。

（注） 検索モードを変更すると、中断が発生します。マルチキャスト転送は、すべてのマルチキャスト エントリが新しい検索モードでプログラムされるまで、最適ではありません。また、32 個の IP アドレスが 1 つの MAC アドレスにマッピングされていると、このデバイスでの転送は、準最適である場合があります。

マルチキャスト レシーバへのスタティック接続の設定

マルチキャスト レシーバへのスタティック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
Router(config)# **mac address-table static** *mac_addr* **vlan** *vlan_id* **interface** *type slot/port* [**disable-snooping**]	マルチキャスト レシーバへのスタティックな接続を設定します。

スタティックな接続を設定する場合、**disable-snooping** キーワードを入力して、スタティックに設定されたマルチキャスト MAC アドレスにアドレス指定されたマルチキャスト トラフィックが、同じ VLAN 内の別のポートへ送信されるのを防止します。

次に、マルチキャスト レシーバへのスタティックな接続を設定する例を示します。

```
Router(config)# mac address-table static 0050.3e8d.6400 vlan 12 interface gigabitethernet 5/7
```

上記の static mac コマンドは、VLAN の検索の種類が MAC ベースの場合に使用できます。次のコマンドは、検索の種類に関係なく、グループのマルチキャスト レシーバへのスタティックな接続、または特定の送信元からのスタティックな接続を設定するために使用できます。

```
Router(config)# vlan configuration 200
Router(config-vlan-config)# ip igmp snooping static 224.1.2.3 interface g3/11
Router(config-vlan-config)# ip igmp snooping static 224.1.2.3 source 20.1.1.1 interface Gi3/12
```

マルチキャスト ルータ ポートのスタティックな設定

マルチキャスト ルータへのスタティック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	Router(config-vlan-config)# **ip igmp snooping mrouter interface** *type slot/port*	マルチキャスト ルータへのスタティック接続を設定します。
ステップ 2	Router(config-vlan-config)# **end**	コンフィギュレーション モードを終了します。

ルータへのインターフェイスは、コマンドを入力する VLAN 内である必要があります。インターフェイスは管理上アップ状態で、回線プロトコルはアップ状態である必要があります。

次に、マルチキャスト ルータへのスタティックな接続を設定する例を示します。

```
Router(config-if)# ip igmp snooping mrouter interface gigabitethernet 5/6
```

IGMP スヌーピング クエリー時間の設定

特定のマルチキャスト グループにホストがまだ関係しているかどうかを判別するグループ固有のクエリーを送信した後で、スイッチが待機する時間を設定できます。

（注）　IGMP 即時脱退処理と IGMP クエリー時間の両方を設定した場合は、即時脱退処理が優先されます。

スイッチによって送信される IGMP スヌーピング クエリー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	`Router(config)# vlan configuration vlan_ID`	VLAN を選択します。
ステップ 2	`Router(config-vlan-config)# ip igmp snooping last-member-query-interval interval`	スイッチによって送信される IGMP スヌーピング クエリー時間を設定します。デフォルトは 1 秒です。有効な範囲は 100 ～ 999 ミリ秒です。

次に、IGMP スヌーピング クエリー時間を設定する例を示します。

```
Router(config-vlan-config)# ip igmp snooping last-member-query-interval 200
Router(config-vlan-config)# exit
Router# show ip igmp interface vlan 200 | include last
  IGMP snooping last member query interval on this interface is 200 ms
```

IGMP スヌーピング即時脱退処理のイネーブル化

高速脱退設定は、IGMP バージョン 2 のホストだけに適用されます。特定の VLAN 上で IGMP スヌーピング高速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
ステップ 1	`Router(config)# vlan configuration vlan_ID`	VLAN を選択します。
ステップ 2	`Router(config-vlan-config)# ip igmp snooping`	IGMP スヌーピングをイネーブルにします。この手順は、IGMP スヌーピングがこの VLAN 上でイネーブルになっていない場合に限り必要です。
ステップ 3	`Router(config-vlan-config)# ip igmp snooping immediate-leave`	VLAN 上で IGMP 即時脱退処理をイネーブルにします。

次に、VLAN 200 インターフェイスで、IGMP スヌーピング バージョン 2 のホストに対して 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。

```
Router# interface vlan 200
Router(config-vlan-config)# ip igmp snooping
Router(config-vlan-config)# ip igmp snooping immediate-leave
Configuring immediate leave on vlan 200
Router(config-vlan-config)# end
Router# show ip igmp interface vlan 200 | include immediate-leave
IGMP snooping immediate-leave is enabled on this interface
```

IGMPv3 スヌーピングの明示的ホスト トラッキングの設定

特定の VLAN で IGMPv3 スヌーピングの明示的なホスト トラッキ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	`Router(config)# vlan configuration vlan_ID`	VLAN を選択します。
ステップ 2	`Router(config-vlan-config)# ip igmp snooping explicit-tracking limit limit`	特定の VLAN で IGMPv3 スヌーピングの明示的なホスト トラッキングをイネーブルにします。

次に、IGMPv3 スヌーピングの明示的なホスト トラッキングをイネーブルにする例を示します。

```
Router(config-vlan-config)# ip igmp snooping explicit-tracking limit 400
Router# show ip igmp snooping vlan 200
Global IGMP Snooping configuration:
-------------------------------------------
IGMP snooping Oper State    : Enabled
IGMPv3 snooping             : Enabled
Report suppression          : Disabled
EHT DB limit/count          : 100000/2
TCN solicit query           : Disabled
Robustness variable         : 2
Last member query count     : 3
Last member query interval  : 1000
Check TTL=1                 : No
Check Router-Alert-Option   : No

Vlan 200:
--------
IGMP snooping Admin State  : Enabled
IGMP snooping Oper State   : Enabled
IGMPv2 immediate leave     : Disabled
Explicit host tracking     : Enabled
Report suppression         : Enabled
Robustness variable        : 2
Last member query count    : 2
Last member query interval : 1000
EHT DB limit/count         : 100000/2
Check TTL=1                : Yes
Check Router-Alert-Option  : Yes
Query Interval             : 100
Max Response Time          : 10000
Router(config-vlan-config)# ip igmp snooping static 224.1.2.3 source 10.1.1.1 interface Gi3/11
Router# show ip igmp snooping groups vlan 200
Flags: I -- IGMP snooping, S -- Static, P -- PIM snooping, A -- ASM mode
Vlan       Group/source            Type      Version        Port List
------------------------------------------------------------------------
200        224.1.2.3                           v3
             /10.1.1.1               S                        Gi3/11
Router#
```

IGMP スヌーピング情報の表示

- 「マルチキャスト ルータ インターフェイスの表示」（P.44-14）
- 「MAC アドレス マルチキャスト エントリの表示」（P.44-15）
- 「VLAN インターフェイスの IGMP スヌーピング情報の表示」（P.44-16）

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
`Router# show ip igmp snooping 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。

```
Router# show ip igmp snooping vlan 200
Global IGMP Snooping configuration:
----------------------------------------
IGMP snooping Oper State    : Enabled
IGMPv3 snooping             : Enabled
Report suppression          : Disabled
EHT DB limit/count          : 100000/2
TCN solicit query           : Disabled
Robustness variable         : 2
Last member query count     : 3
Last member query interval  : 1000
Check TTL=1                 : No
Check Router-Alert-Option   : No

Vlan 200:
--------
IGMP snooping Admin State  : Enabled
IGMP snooping Oper State   : Enabled
IGMPv2 immediate leave     : Disabled
Explicit host tracking     : Enabled
Report suppression         : Enabled
Robustness variable        : 2
Last member query count    : 2
Last member query interval : 1000
EHT DB limit/count         : 100000/2
Check TTL=1                : Yes
Check Router-Alert-Option  : Yes
Query Interval             : 100
Max Response Time          : 10000
Router#
```

MAC アドレス マルチキャスト エントリの表示

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
Router# **show mac address-table multicast** *vlan_ID* [**count**]	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。

```
Router# show mac address-table multicast vlan 1
vlan   mac address     type    qos             ports
-----+---------------+--------+---+--------------------------------
  1  0100.5e02.0203  static   --  Gi1/1,Gi2/1,Gi3/48,Router
  1  0100.5e00.0127  static   --  Gi1/1,Gi2/1,Gi3/48,Router
  1  0100.5e00.0128  static   --  Gi1/1,Gi2/1,Gi3/48,Router
  1  0100.5e00.0001  static   --  Gi1/1,Gi2/1,Gi3/48,Router,Switch
Router#
```

次に、特定の VLAN について MAC アドレス エントリの総数を表示する例を示します。

```
Router# show mac address-table multicast 1 count

Multicast MAC Entries for vlan 1:    4
Router#
```

VLAN インターフェイスの IGMP スヌーピング情報の表示

特定の VLAN インターフェイスについて 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
Router# **show ip igmp interface** *vlan_ID*	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 200 インターフェイスの IGMP スヌーピング情報を表示する例を示します。

```
Router# show ip igmp interface vlan 43
Vlan43 is up, line protocol is up
  Internet address is 43.0.0.1/24
  IGMP is enabled on interface
  Current IGMP host version is 2
  Current IGMP router version is 2
  IGMP query interval is 60 seconds
  IGMP querier timeout is 120 seconds
  IGMP max query response time is 10 seconds
  Last member query count is 2
  Last member query response interval is 1000 ms
  Inbound IGMP access group is not set
  IGMP activity:1 joins, 0 leaves
  Multicast routing is enabled on interface
  Multicast TTL threshold is 0
  Multicast designated router (DR) is 43.0.0.1 (this system)
  IGMP querying router is 43.0.0.1 (this system)
  Multicast groups joined by this system (number of users):
      224.0.1.40(1)
  IGMP snooping is globally enabled
  IGMP snooping is enabled on this interface
  IGMP snooping immediate-leave is disabled and querier is disabled
  IGMP snooping explicit-tracking is enabled on this interface
  IGMP snooping last member query interval on this interface is 1000 ms
Router#
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

PIM スヌーピング

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

PIM スヌーピングの前提条件

なし。

PIM スヌーピングの制約事項

- PIM スヌーピングが VLAN でイネーブルであり、IGMP スヌーピングが VLAN でディセーブルである場合、マルチキャスト パケットは、IGMP Join を送信するローカル レシーバへブリッジングされません。（CSCta03980）
- PIM-Sparse Mode（PIM-SM）機能を使用すると、ダウンストリーム ルータは、PIM Join またはプルーニング メッセージを通じて事前に関係を示す場合、トラフィックだけを監視します。アップストリーム ルータは、PIM Join またはプルーニング プロセス中にアップストリーム ルータとして使用された場合、トラフィックだけを監視します。
- Join またはプルーニング メッセージは、ルータ ポートすべてにフラッディングされるわけではありませんが、Join またはプルーニング メッセージのペイロードに指定されたアップストリーム ルータに対応するポートにだけ、送信されます。
- 直接接続された送信元は、双方向 PIM グループでサポートされます。直接接続された送信元からのトラフィックは、VLAN の指定ルータおよび指定フォワーダに転送されます。Nondesignated Router（NDR）がダウンストリーム（S, G）Join を受信できる場合があります。送信元だけのネットワークでは、初回の不明なトラフィックは DR および指定フォワーダだけに転送されます。
- dense（密）グループ モード トラフィックは、不明なトラフィックとして見なされドロップされます。
- AUTO-RP グループ（224.0.1.39 および 224.0.1.40）は常にフラッディングされます。
- スイッチは指定フォワーダ選定時にスヌーピングし、VLAN の各 RP についてすべての指定フォワーダ ルータのリストを維持します。すべてのトラフィックは指定フォワーダすべてに送信されます。これにより双方向機能が正しく動作します。
- PIM スヌーピングおよび IGMP スヌーピングを、VLAN で同時にイネーブルできます。RGMP または PIM スヌーピングいずれかを VLAN でイネーブルにできますが、両方同時にはイネーブルにできません。
- 非 PIMv2 マルチキャスト ルータは、すべてのトラフィックを受信します。
- PIM スヌーピングは、VLAN 単位でイネーブルおよびディセーブルにすることができます。
- PIM Hello および Join/プルーニング制御パケットに示されたホールドタイムに基づき、mroute およびルータ情報はすべて時間切れとなります。mroute ステートおよびネイバー情報はすべて VLAN 単位で維持されます。
- リリース 15.1(1)SY1 以降のリリースでは、IGMP スヌーピングおよび PIM スヌーピングによって VPLS マルチキャスト トラフィックが抑制されます。

PIM スヌーピングについて

レイヤ 2 スイッチが Internet Exchange Point（IXP）など複数のルータと相互接続しているネットワークでは、マルチキャスト レシーバ ダウンストリームが存在しない場合でも、スイッチはデフォルトで、すべてのマルチキャスト ルータ ポートで IP マルチキャスト パケットをフラッディングします。PIM スヌーピングがイネーブルの場合、スイッチは各 IP マルチキャスト グループのマルチキャスト パケットを、そのグループに加入しているダウンストリーム レシーバが接続されたマルチキャスト ルータ ポートに限定します。PIM スヌーピングをイネーブルにすると、スイッチは PIM Hello メッセージ、PIM Join および Prune メッセージ、および双方向 PIM によって指定されたフォワーダ選定メッセージを待ち受けて、特定の VLAN 内でマルチキャスト トラフィックを受信する必要があるマルチキャスト ルータ ポートを学習します。

（注）　PIM スヌーピングを使用するには、スイッチ上で IGMP スヌーピングをイネーブルにする必要があります。IGMP スヌーピングは、ホストが接続されている LAN ポートからのマルチキャスト トラフィックの送信を制限します。IGMP スヌーピングは、1 つまたは複数のマルチキャスト ルータが接続されている LAN ポートからのトラフィックは制限しません。

次の図では、PIM スヌーピングがイネーブルでないネットワークによるトラフィックおよびフラッディング フローと、および PIM スヌーピングがイネーブルのときのトラフィック フローおよびトラフィック制限を示します。

図 45-1 では、PIM スヌーピングがイネーブルでない場合の PIM Join メッセージのフローを示します。この図では、スイッチはルータ B を対象とした PIM Join メッセージを接続されたすべてのルータにフラッディングします。

図 45-1　PIM スヌーピングがない場合の PIM Join メッセージ フロー

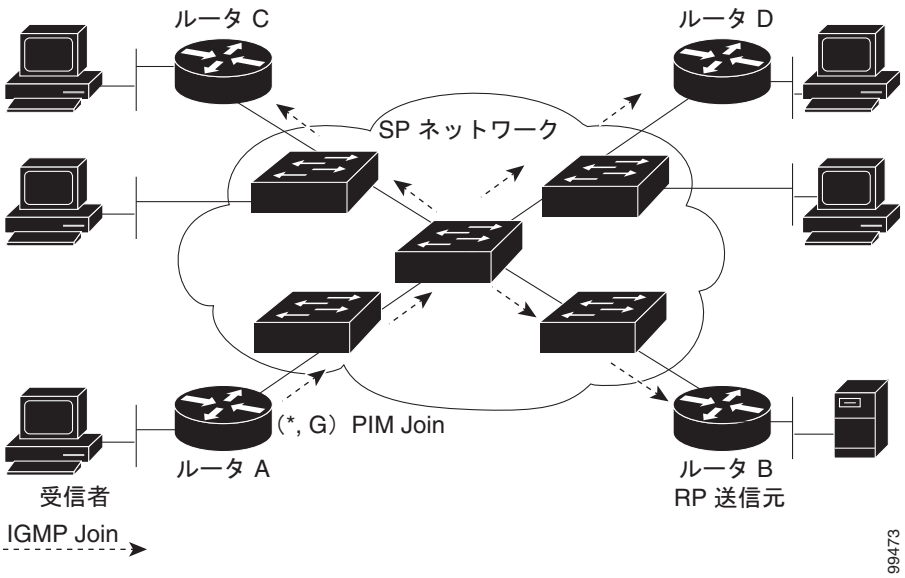


図 45-2 では、PIM スヌーピングがイネーブルの場合の PIM Join メッセージ フローを示します。この図では、スイッチは PIM Join メッセージを制限し、このメッセージを受信する必要があるルータ（ルータ B）だけに転送します。

図 45-2　PIM スヌーピングがある場合の PIM Join メッセージ フロー

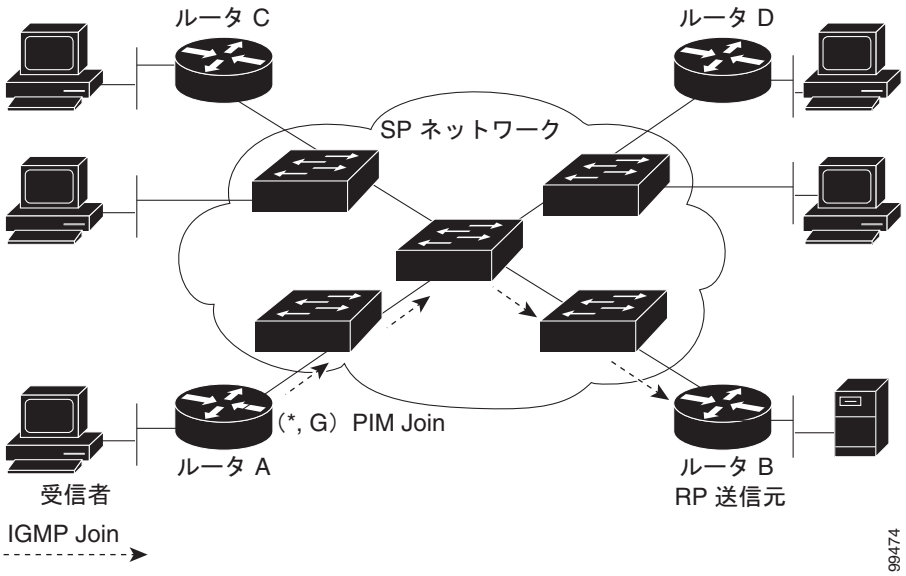


図 45-3 では、PIM スヌーピングがイネーブルでない場合のデータ トラフィック フローを示します。この図では、スイッチはルータ A を対象としたデータ トラフィックを接続されたすべてのルータにフラッディングします。

図 45-3　PIM スヌーピングがない場合のデータ トラフィック フロー

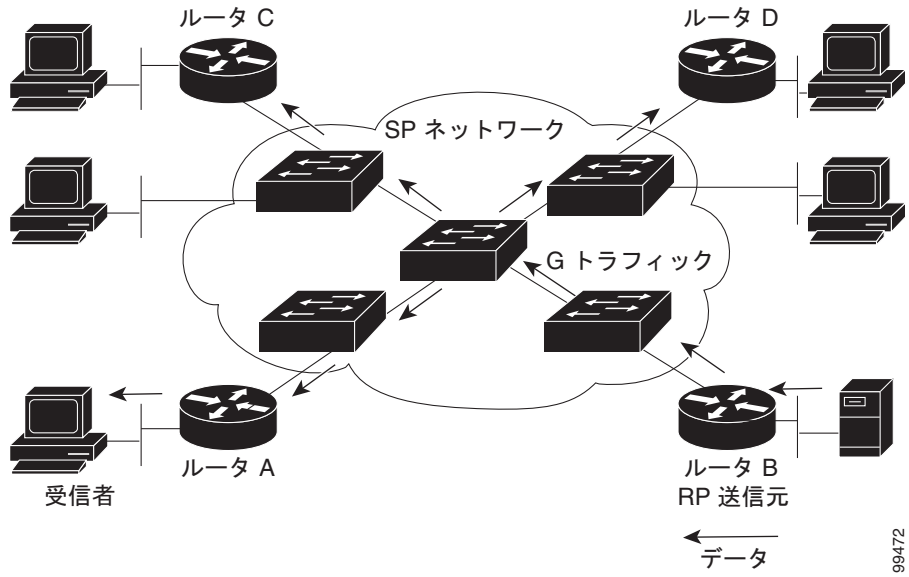
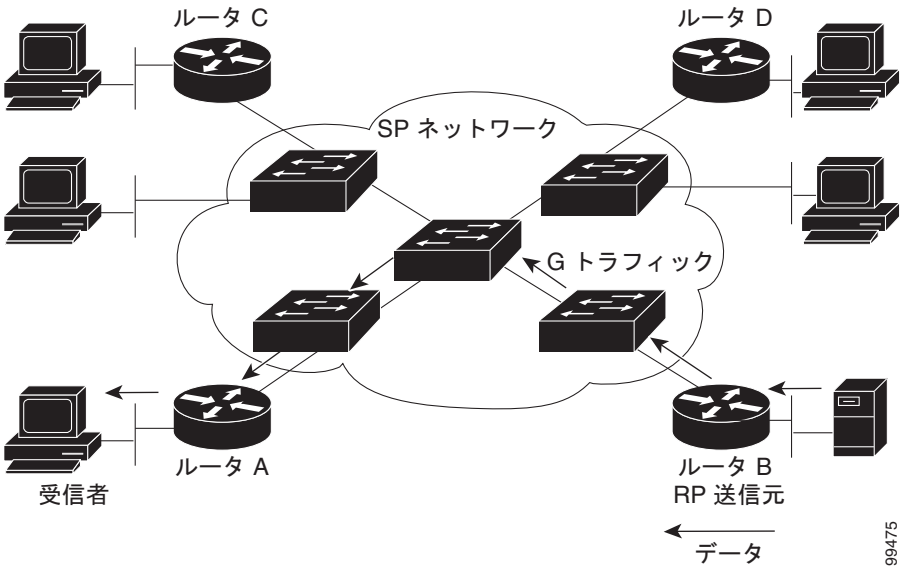


図 45-4 では、PIM スヌーピングがイネーブルの場合のデータ トラフィック フローを示します。この図では、スイッチはデータ トラフィックを受信する必要があるルータ（ルータ A）だけに転送します。

図 45-4　PIM スヌーピングがある場合のデータ トラフィック フロー



PIM スヌーピングのデフォルト設定

PIM スヌーピングは、デフォルトではディセーブルに設定されています。

PIM スヌーピングの設定方法

- 「PIM スヌーピングのグローバルなイネーブル化」（P.45-5）
- 「VLAN における PIM スヌーピングのイネーブル化」（P.45-6）
- 「PIM スヌーピング指定ルータ フラッディングのディセーブル化」（P.45-7）

PIM スヌーピングのグローバルなイネーブル化

PIM 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	`Router(config)# ip pim snooping`	PIM スヌーピングをイネーブルにします。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

次に、PIM 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。

```
Router(config)# ip pim snooping
Router(config)# end
Router# show ip pim snooping
Global runtime mode: Enabled
Global admin mode  : Enabled
```

```
Number of user enabled VLANs: 1
User enabled VLANs: 10
Router#
```

（注）　PIM スヌーピングを実行するには、IP アドレスまたは IP PIM を設定する必要はありません。

VLAN における PIM スヌーピングのイネーブル化

特定の VLAN で PIM 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	`Router(config)# vlan configuration vlan_ID`	VLAN を選択します。
ステップ 2	`Router(config-vlan-config)# ip pim snooping`	PIM スヌーピングをイネーブルにします。
ステップ 3	`Router(config-vlan-config)# end`	コンフィギュレーション モードを終了します。

次に、VLAN 10 で PIM 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。

```
Router# vlan configuration 10
Router(config-vlan-config)# ip pim snooping
Router(config-vlan-config)# end
Router# show ip pim snooping vlan 10
3 neighbors (0 DR priority incapable, 0 Bi-dir incapable)
6 mroutes, 3 mac entries
DR is 10.10.10.4
RP DF Set
Router#
```

PIM スヌーピング指定ルータ フラッディングのディセーブル化

（注）　マルチキャスト送信元をサポートするレイヤ 2 ブロードキャスト ドメインのスイッチにおいて、指定ルータ フラッディングをディセーブルにしないでください。

デフォルトの場合、PIM スヌーピングをイネーブルにしているスイッチは、指定ルータ（DR）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。この方法による動作では、不必要なマルチキャスト パケットが指定ルータに送信されることがあります。ネットワークは不必要なトラフィックを搬送する必要があり、DR は不必要なトラフィックを処理してドロップする必要があります。

ネットワークで指定ルータに送信されるトラフィックを減らすには、指定ルータ フラッディングをディセーブルにします。指定ルータ フラッディングをディセーブルにすると、PIM スヌーピングは、PIM スヌーピングが指定ルータへのリンクから明示的な Join を受信するマルチキャスト グループ内にあるトラフィックだけを指定ルータに渡します。

PIM スヌーピング指定ルータ 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	`Router(config)# no ip pim snooping dr-flood`	PIM スヌーピング指定ルータ フラッディングをディセーブルにします。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

次に、PIM スヌーピング指定ルータ フラッディングをディセーブルにする例を示します。

```
Router(config)# no ip pim snooping dr-flood
Router(config)# end
```

ヒント　Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CHAPTER 46

マルチキャスト VLAN レジストレーション（MVR）

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

MVR の制約事項

なし。

MVR の制約事項

- スイッチ上に存在できる MVR VLAN は 1 つだけで、同一ネットワーク内のすべてのスイッチで MVR VLAN と同じ VLAN を設定する必要があります。
- 送信元ポートは、MVR VLAN 内に存在できません。
- スイッチの受信ポートは別の VLAN 内に存在できますが、MVR VLAN 内には存在できません。
- 受信ポートはアクセス ポートでなければなりません。トランク ポートにはできません。
- プライベート VLAN を使用する場合、セカンダリ VLAN を MVR VLAN として設定できません。
- マルチキャスト ルータを受信ポートに接続しないでください。
- MVR VLAN を、マルチキャスト ルートの RPF インターフェイスにしないでください。
- MVR 受信ポートで受信した MVR データは、MVR 送信元ポートに転送されません。
- スイッチ上で設定できるマルチキャスト エントリ（MVR グループ アドレス）の最大数（受信できるテレビ チャネルの最大数）は 8000 です。
- MVR は、ネイティブ システムだけで使用できます。
- MVR VLAN の数が 1 ～ 1000 である場合は、VTP プルーニングをディセーブルにする必要があります。
- MVR はスイッチで IGMP スヌーピングと共存できます。
- MVR は、IGMPv3 メッセージをサポートします。

MVR について

MVR の概要

MVR は、イーサネット リングベースのサービス プロバイダー ネットワークでマルチキャスト トラフィックを広範囲に配信するアプリケーション（サービス プロバイダー ネットワークで複数の TV チャネルのブロードキャストなど）用に設計されています。MVR によってポート上の加入者は、ネットワークワイドなマルチキャスト VLAN 上のマルチキャスト ストリームに加入し、脱退できます。加入者は別個の VLAN 上にありながら、ネットワークで単一マルチキャスト VLAN を共有できます。MVR によって、マルチキャスト VLAN でマルチキャスト ストリームを連続送信する能力が得られますが、ストリームと加入者の VLAN は、帯域幅およびセキュリティ上の理由で分離されます。

MVR では、加入者ポートが IGMP Join および Leave メッセージを送信することによって、マルチキャスト ストリームへの加入および脱退（Join および Leave）を行うことが前提です。これらのメッセージは、イーサネットで接続され、IGMP バージョン 2 に準拠しているホストから発信できます。MVR は IGMP スヌーピングの基本メカニズムで動作しますが、この 2 つの機能はそれぞれ単独で動作します。それぞれ、もう一方の機能の動作に影響を与えずにイネーブルまたはディセーブルに設定できます。ただし、IGMP スヌーピングと MVR が両方ともイネーブルの場合、MVR は MVR 環境で設定されたマルチキャスト グループが送信した Join および Leave メッセージだけに反応します。他のマルチキャスト グループから送信された Join および Leave メッセージはすべて、IGMP スヌーピングが管理します。

MVR では、次の処理を行います。

- MVR IP マルチキャスト ストリーム、および関連するレイヤ 2 転送テーブルの IP マルチキャスト グループを識別します。
- IGMP メッセージを代行受信します。
- 受信者が送信元とは別の VLAN 内に存在する場合でも、レイヤ 2 転送テーブルで、マルチキャスト ストリームの受信者として加入者を含めるか、または削除するよう変更します。

この転送動作により、異なる VLAN の間でトラフィックを選択して伝送できます。

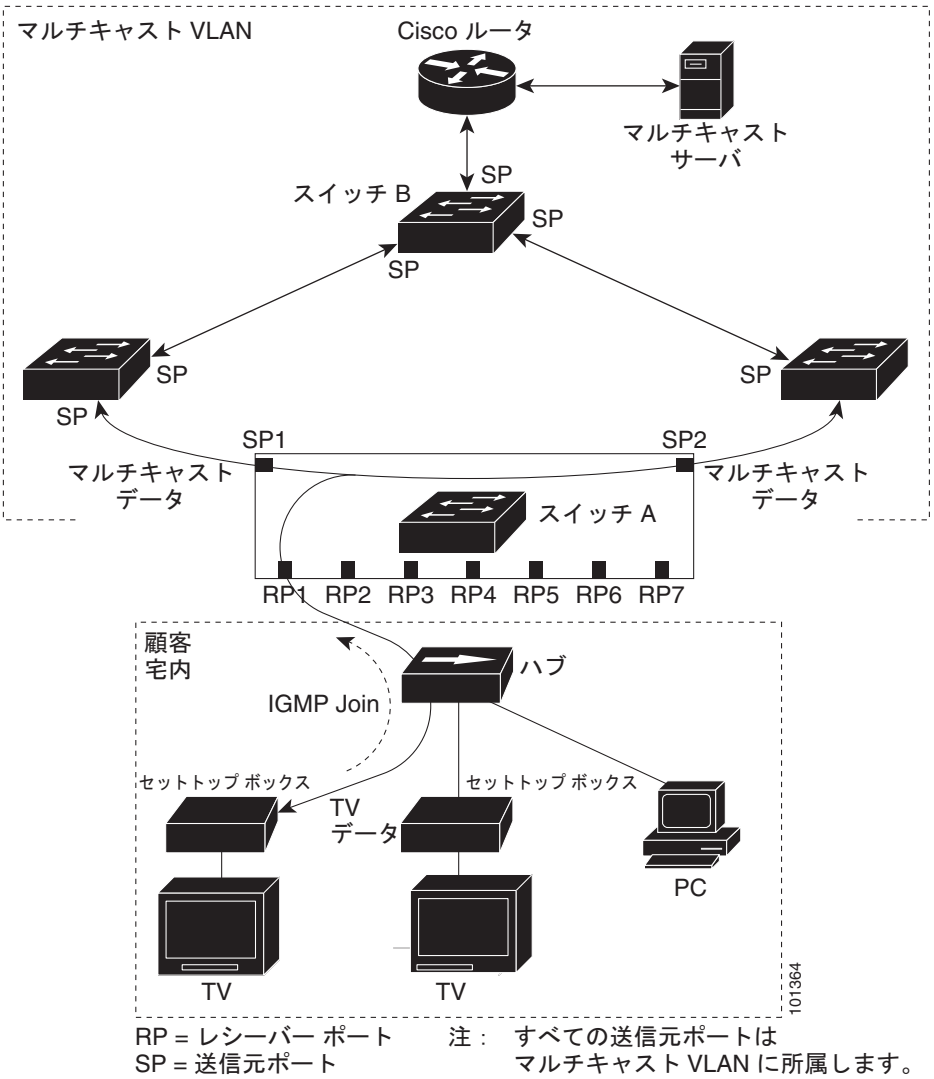
スイッチは、MVR IP マルチキャスト ストリームのマルチキャスト データを、IGMP レポートまたは MVR のスタティック コンフィギュレーションのいずれかを使用して、ホストが加入した MVR ポートに対してだけ転送します。スイッチは、MVR ホストから受信した IGMP レポートを送信元（uplink）ポートに対してだけ転送します。これにより、MVR データ ポート リンク上で不要な帯域幅が使用されなくなります。

MVR に参加するのは、レイヤ 2 ポートだけです。ポートを MVR 受信ポートとして設定する必要があります。スイッチごとに 1 つの MVR マルチキャスト VLAN だけがサポートされます。

マルチキャスト TV アプリケーションでの MVR の使用

マルチキャスト TV アプリケーションでは、PC またはセットトップ ボックスを装備したテレビでマルチキャスト ストリームを受信できます。1 つの加入者ポートに複数のセットトップ ボックスまたは PC を接続できます。加入者ポートは、MVR 受信ポートとして設定されたスイッチ ポートです。図 46-1 に構成例を示します。Dynamic Host Configuration Protocol（DHCP）によって、セットトップ ボックスまたは PC に IP アドレスが割り当てられます。加入者がチャネルを選択すると、適切なマルチキャストに加入するために、セットトップ ボックスまたは PC からスイッチ A に IGMP レポートが送信されます。IGMP レポートが、設定されている IP マルチキャスト グループ アドレスの 1 つと一致すると、スイッチがハードウェア アドレス テーブルを変更して、指定のマルチキャスト ストリームをマルチキャスト VLAN から受信したときの転送先として、レシーバ ポートと VLAN を追加します。マルチキャスト VLAN との間でマルチキャスト データを送受信するアップリンク ポートを、MVR 送信元ポートと呼びます。

図 46-1　MVR の例



加入者がチャネルを切り替えた場合、またはテレビのスイッチを切った場合には、セットトップ ボックスからマルチキャスト ストリームに対する IGMP Leave メッセージが送信されます。スイッチは、レシーバ ポートの VLAN 経由で MAC ベースの一般クエリーを送信します。VLAN に、このグループに加入している別のセットトップ ボックスがある場合、そのセットトップ ボックスはクエリーに指定された最大応答時間内に応答しなければなりません。応答を受信しなかった場合、CPU はこのグループの転送先としての受信ポートを除外します。

即時脱退機能がイネーブルでない場合、スイッチは受信ポートの加入者から IGMP Leave メッセージを受信すると、そのポートに IGMP クエリーを送信し、IGMP グループ メンバーシップ レポートを待ちます。設定された時間内にレポートを受信しなかった場合は、受信ポートがマルチキャスト グループ メンバーシップから削除されます。即時脱退機能がイネーブルの場合、IGMP Leave を受信した受信ポートから、IGMP クエリーは送信されません。Leave メッセージの受信後ただちに、受信ポートがマルチキャスト グループ メンバーシップから削除されるので、脱退遅延時間が短縮されます。即時脱退機能は、1 つの受信デバイスが接続された受信ポートでのみイネーブルにしてください。

MVR を使用すると、各 VLAN の加入者に対してテレビ チャネルのマルチキャスト トラフィックを重複して送信する必要がなくなります。すべてのチャネル用のマルチキャスト トラフィックは、マルチキャスト VLAN 上でのみ、VLAN トランクに 1 回だけ送信されます。IGMP Leave および Join メッセージは、加入者ポートが割り当てられている VLAN で送信されます。これらのメッセージにより、レイヤ 3 デバイス（スイッチ B）上のマルチキャスト VLAN 内のマルチキャスト トラフィック ストリームはダイナミックに登録されます。アクセス レイヤ スイッチ（スイッチ A）は、2 つの VLAN 間でのトラフィック伝送を選択的に許可し、マルチキャスト VLAN から別の VLAN 上の加入者ポートにトラフィックが転送されるように転送動作を変更します。

IGMP レポートは、マルチキャスト データと同じ IP マルチキャスト グループ アドレスに送信されます。スイッチ A の CPU は、受信ポートからのすべての IGMP Join および Leave メッセージを取り込んで、送信元（アップリンク）ポートのマルチキャスト VLAN に転送する必要があります。

MVR のデフォルト設定

- MVR：グローバルおよびインターフェイス単位でディセーブル
- マルチキャスト アドレス：未設定
- クエリー応答時間：1 秒
- マルチキャスト VLAN：VLAN 1
- インターフェイスのデフォルト（ポート単位）：受信側ポートでも送信元ポートでもない
- 即時脱退：すべてのポートでディセーブル

MVR の設定方法

- 「MVR グローバル パラメータの設定」（P.46-5）
- 「MVR インターフェイスの設定」（P.46-6）
- 「MVR 情報の表示」（P.46-8）
- 「MVR カウンタのクリア」（P.46-8）

MVR グローバル パラメータの設定

MVR グローバル 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	`Router# 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	`Router(config)# mvr`	スイッチ上で MVR をイネーブルにします。
ステップ 3	`Router(config)# mvr max-groups max-groups`	MVR グループの最大数を指定します。範囲は 1 ～ 8000 です。デフォルト値は 1000 です。

	コマンド	目的
ステップ 4	`Router(config)# mvr group ip-address [count]`	スイッチ上で IP マルチキャスト アドレスを設定するか、または *count* パラメータを使用して（*count* の範囲は 1 ～ 256 で、デフォルトは 1）連続する MVR グループ アドレスを設定します。このアドレスに送信されたマルチキャスト データは、スイッチ上のすべての送信元ポートおよびそのマルチキャスト アドレスのデータを受信するために選ばれた、すべてのレシーバ ポートに送信されます。マルチキャスト アドレスとテレビ チャネルは 1 対 1 の対応です。
ステップ 5	`Router(config)# mvr querytime value`	（任意）マルチキャスト グループ メンバーシップからポートを削除する前に、受信ポート上で IGMP レポート メンバーシップを待機する最大時間を定義します。この値は 10 分の 1 秒単位で設定します。指定できる範囲は 1 ～ 100 で、デフォルトは 10/10、つまり 1 秒です。
ステップ 6	`Router(config)# mvr vlan vlan-id`	（任意）マルチキャスト データを受信する VLAN を指定します。すべての送信元ポートはこの VLAN に属する必要があります。VLAN の範囲は 1 ～ 1001 および 1006 ～ 4094 です。デフォルトは VLAN 1 です。
ステップ 7	`Router(config)# end`	特権 EXEC モードに戻ります。

デフォルト値を使用する場合は、オプションの MVR パラメータを設定する必要はありません。デフォルトのパラメータ（MVR VLAN を除く）を変更する前に、まず MVR をイネーブルにする必要があります。

スイッチをデフォルト設定に戻すには、**no mvr** [**group** *ip-address* | **querytime** | **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、MVR をイネーブルにし、グループ アドレスを設定し、クエリー時間を 1 秒（10/10）に設定し、MVR マルチキャスト VLAN を VLAN 22 に指定する例を示します。

```
Router(config)# mvr
Router(config)# mvr group 228.1.23.4
Router(config)# mvr querytime 10
Router(config)# mvr vlan 22
Router(config)# end
```

show mvr groups 特権 EXEC コマンドを使用すると、スイッチ上の MVR マルチキャスト グループ アドレスを確認できます。

MVR インターフェイスの設定

レイヤ 2 MVR 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	`Router# 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	`Router(config)# mvr`	スイッチ上で MVR をイネーブルにします。
ステップ 3	`Router(config)# interface interface-id`	設定するレイヤ 2 ポートを指定して、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。

	コマンド	目的
ステップ 4	`Router(config-if)# mvr type {source | receiver}`	MVR ポートを、次のポート タイプのいずれかに設定します。 • **source**：マルチキャスト データを送受信するアップリンク ポートを送信元ポートとして設定します。加入者が送信元ポートに直接接続することはできません。スイッチ上のすべての送信元ポートは、単一マルチキャスト VLAN に所属します。 • **receiver**：ポートが加入者ポートで、マルチキャスト データの受信だけを行う場合には、ポートを受信ポートとして設定します。受信ポートは、スタティックな設定、または IGMP Leave および Join メッセージによってマルチキャスト グループのメンバになるまでは、データを受信しません。受信ポートをマルチキャスト VLAN に所属させることはできません。 非 MVR ポートに MVR 特性を設定しようとしても、エラーになります。デフォルトでは、非 MVR ポートとして設定されます。
ステップ 5	`Router(config-if)# mvr immediate`	（任意）ポート上で MVR の即時脱退機能をイネーブルにします。この機能は、デフォルトでディセーブルです。 **（注）** このコマンドが適用されるのは、受信ポートだけです。また、イネーブルにするのは、単一の受信デバイスが接続されている受信ポートに限定してください。
ステップ 6	`Router(config-if)# end`	特権 EXEC モードに戻ります。

インターフェイスをデフォルト設定に戻すには、**no mvr** [**type** | **immediate**] 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、送信元ポートおよび受信ポートを設定し、受信ポート上で即時脱退機能を設定する例を示します。

```
Router(config)# mvr
Router(config)# interface gigabitethernet 3/48
Router(config-if)# switchport
Router(config-if)# switchport access vlan 22
Router(config-if)# mvr type source
Router(config-if)# exit
Router(config)# interface gigabitethernet 3/47
Router(config-if)# switchport
Router(config-if)# switchport access vlan 30
Router(config-if)# mvr type receiver
Router(config-if)# mvr immediate
Router(config-if)# exit
```

MVR カウンタのクリア

スイッチ、送信元ポートまたは受信ポート、あるいは指定されたインターフェイスの MVR Join カウンタをクリアできます。MVR カウンタをクリアするには、次の作業を行います。

コマンド	目的
Router# **clear mvr counters** [[**receiver-ports** | **source-ports**] [*type module/port*]]	すべての MVR ポート、送信元ポートまたは受信ポート、あるいは指定された MVR インターフェイス ポートの Join カウンタをクリアします。

次に、ポート GigabitEthernet 1/7 上の受信ポートの Join カウンタをクリアする例を示します。

```
Router# clear mvr receiver-ports GigabitEthernet 1/7
Router# show mvr receiver-ports GigabitEthernet 1/7
Joins: v1,v2,v3 counter shows total IGMP joins
       v3 counter shows IGMP joins received with both MVR and non-MVR groups
Port   VLAN Status         Immediate          Joins
                           Leave        (v1,v2,v3)     (v3)
----   ---- -------------  -----------  ---------- -----------
Gi1/7   202 INACTIVE/UP    ENABLED              0           0
```

MVR 情報の表示

スイッチまたは指定されたインターフェイスの MVR 情報を表示できます。MVR 設定を表示するには、次の作業の 1 つ以上を実行します。

コマンド	目的
Router# **show mvr**	スイッチの MVR ステータスおよび値を表示します。MVR がイネーブルまたはディセーブルであるか、マルチキャスト VLAN、設定済みのマルチキャスト グループの最大数および現在の数、およびクエリー応答時間が表示されます。
Router# **show mvr groups**	MVR グループの設定を表示します。
Router# **show mvr interface** [*type module/port*]	すべての MVR インターフェイスおよびその MVR 設定を表示します。 特定のインターフェイスを指定すると、次の情報が表示されます。 • Type：Receiver または Source • Status：次のいずれか – Active：ポート上の MVR グループに対して、少なくとも 1 つの IGMP Join が受信されている。 – Inactive：ポートはいずれの MVR グループにも参加していない。 – UP/Down：ポートはフォワーディング（アップ）または非フォワーディング（ダウン）である。 • Immediate Leave：Enabled または Disabled
Router# **show mvr members** [[**vlan** *vlan-id*] | [*type module/port*]]	すべての MVR メンバまたは指定された VLAN またはポートの MVR メンバの詳細を表示します。

コマンド	目的
Router# **show mvr**	スイッチの MVR ステータスおよび値を表示します。MVR がイネーブルまたはディセーブルであるか、マルチキャスト VLAN、設定済みのマルチキャスト グループの最大数および現在の数、およびクエリー応答時間が表示されます。
Router# **show mvr groups**	MVR グループの設定を表示します。
Router# **show mvr members** [[**vlan** *vlan-id*] | [*type module/port*]] **count**	すべてのアクティブな MVR グループ、または指定された VLAN もしくはポートの MVR メンバの数を表示します。
Router# **show mvr** {**receiver-ports** | **source-ports**} [*type module/port*]	いずれかの IP マルチキャスト グループのメンバであるか、指定されたインターフェイス ポート上にある受信ポートまたは送信元ポートをすべて表示します。

次に、スイッチの MVR ステータスおよび値を表示する例を示します。

```
Router# show mvr
MVR Running: TRUE
MVR multicast vlan: 22
MVR Max Multicast Groups: 1000
MVR Current multicast groups: 256
MVR Global query response time: 10 (tenths of sec)
```

次に、MVR グループの設定を表示する例を示します。

```
Router# show mvr groups
MVR max Multicast Groups allowed: 8000
MVR current multicast groups: 8000
MVR groups:
        Group start     Group end       Type  Count/Mask
        --------------- --------------- ----- ---------------
        225.0.7.226     225.0.7.226     count 1
        225.0.7.227     225.0.7.227     count 1
        225.0.7.228     225.0.7.228     count 1
        225.0.7.229     225.0.7.229     count 1
        225.0.7.230     225.0.7.230     count 1
        225.0.7.231     225.0.7.231     count 1
        236.8.7.0       236.8.7.255     mask  255.255.255.0
        237.8.7.0       237.8.7.255     mask  255.255.255.0
        237.8.8.0       237.8.8.255     mask  255.255.255.0
```

次に、すべての MVR インターフェイスおよびその MVR 設定を表示します。

```
Router# show mvr interface
Port     VLAN  Type       Status           Immediate Leave
----     ----  ----       ------           ---------------
Gi1/20      2  RECEIVER   ACTIVE/UP        DISABLED
Gi1/21      2  SOURCE     ACTIVE/UP        DISABLED
```

次に、VLAN 2 上のすべての MVR メンバを表示する例を示します。

```
Router# show mvr members vlan 2
MVR Group IP     Status    Members
------------     ------    -------
224.000.001.001   ACTIVE    Gi1/20(u),Gi1/21(u)
224.000.001.002   ACTIVE    Gi3/2(d),Gi1/12(u)
```

次に、すべての MVR VLAN 上の MVR メンバ数を表示する例を示します。

```
Router# show mvr members count

Count of active MVR groups:
```

```
    Vlan 490: 400
    Vlan 600: 400
    Vlan 700: 0
    Vlan 950: 0
```

次に、いずれかの IP マルチキャスト グループのメンバである受信ポートすべてを表示する例を示します。

```
Router# show mvr receiver-ports
Joins: v1,v2,v3 counter shows total IGMP joins
       v3 counter shows IGMP joins received with both MVR and non-MVR groups
Port   VLAN Status         Immediate           Joins
                          Leave         (v1,v2,v3)      (v3)
----   ---- -------------  -----------   ----------- -----------
Gi1/7   202 INACTIVE/UP    ENABLED          305336            0
Gi1/8   202 ACTIVE/UP     DISABLED           4005            0
Gi1/9   203 INACTIVE/DOWN  DISABLED          53007            0
Gi1/10  203 ACTIVE/UP     DISABLED           6204            0
Gi1/11  204 ACTIVE/UP     DISABLED              0          940
Gi1/12  205 INACTIVE/UP    ENABLED            8623            0
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

IPv4 IGMP フィルタリング

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

IGMP フィルタリングの前提条件

なし。

IGMP フィルタリングの制約事項

なし。

IGMP フィルタリングについて

IGMP フィルタリングの概要

（注）　IGMP は、マルチキャスト ルータのレイヤ 3 で稼働し、マルチキャスト トラフィックのルーティングが必要なサブネットでレイヤ 3 IGMP クエリーを生成します。IGMP については、第 43 章「IPv4 マルチキャスト レイヤ 3 機能について」を参照してください。

IGMP スヌーピングは、レイヤ 2 レベルでマルチキャスト グループ メンバーシップを学習し、維持するプロトコルです。IGMP スヌーピングは、IGMP トラフィックを確認して、特定の送信元およびグループからのマルチキャスト トラフィックを受信できるポートを決定します。この情報は、マルチキャスト トラフィックを関係するポートにだけ転送するのに使用されます。IGMP スヌーピングの主な利点は、パケットのフラッディングを軽減することです。IGMP スヌーピングの詳細については、「IGMP フィルタリングについて」（P.47-2）を参照してください。

IGMP フィルタリングを使用することにより、ユーザはスイッチ仮想インターフェイス（SVI）上、ポート単位、またはポート単位/VLAN 単位でフィルタを設定し、ネットワークを経由する IGMP トラフィックの伝播を制御できるようになります。IGMP フィルタリングは、IGMP トラフィックを管理することにより、IGMP スヌーピングを管理する機能を提供し、その結果マルチキャスト トラフィックの転送を制御します。

IGMP パケットを受信すると、IGMP フィルタリングはユーザによって設定されたフィルタを使用して、IGMP パケットを廃棄するか、または既存の IGMP スヌーピング コードによる処理を許可するかを決定します。IGMP バージョン 1 または 2 のパケットの場合、パケット全体が廃棄されます。IGMPv3 パケットの場合、パケットはフィルタによって拒否されたメッセージ エレメントを削除するよう書き換えられます。

IGMP フィルタリング機能は、シングル サインオン（SSO）に準拠します。

IGMP トラフィック フィルタは、ポートのマルチキャスト トラフィックへのアクセスを制御します。アクセスは、次の事項に基づいて制限されます。

- ポート上に追加できるマルチキャスト グループまたはチャネル。チャネルには、グループおよびマルチキャスト トラフィックの送信元の両方を指定する IGMPv3 ホストが加入します。
- 特定のポートまたはインターフェイス上で許可されるグループまたはチャネルの最大数（サービスを要求するホスト数とは関係なく）。
- IGMP プロトコル バージョン（たとえば、すべての IGMPv1 メッセージを許可しない）。

IGMP フィルタリング コマンドを入力すると、ユーザ ポリシーがレイヤ 3 SVI インターフェイス、レイヤ 2 ポート、またはレイヤ 2 トランク ポート上の特定の VLAN に適用されます。レイヤ 2 ポートは、アクセス ポートまたはトランク ポートとなる可能性があります。IGMP フィルタリング機能は、IGMP スヌーピングがイネーブルの場合に限り動作します（インターフェイス上またはグローバルに）。

IGMP フィルタリングは通常、エンドユーザ デバイスに接続されたアクセス スイッチで使用されます。

IGMP フィルタには、以下の 3 つの異なるタイプがあります。IGMP グループとチャネル アクセス コントロール、複数の IGMP グループとチャネル制限、および IGMP の最小バージョンです。これらのフィルタは、異なるタイプのポート上で設定可能で、別々に動作します。

- SVI 単位
- ポート単位
- トランク ポート上での VLAN 単位

トランク ポートを経由する各 VLAN のためのフィルタを個別に設定できます。

IGMP フィルタの優先順位

アクセス モード

アクセス モードの場合、フィルタはポートおよび SVI の両方に設定できます。IGMP パケットがアクセス モードのポート上で受信された場合、最初にポート フィルタが確認されます。ポート フィルタが存在する場合は、これが適用され、SVI フィルタは無視されます。ポート単位のフィルタが存在しない場合、SVI フィルタが使用されます。

この階層はフィルタのタイプごとに別々に適用されます。たとえば、ポート上に設定された制限フィルタは、SVI 上のデフォルトの制限フィルタを無効にしますが、その他のフィルタには影響を与えません。

トランク モード

トランク モードのポートの場合、トランク ポート上の VLAN のいずれかに対応する SVI に設定できるフィルタ、トランク ポート自身に設定できるフィルタ、およびトランクをパススルーするレイヤ 2 VLAN のいずれかに設定できるフィルタがあります。IGMP パケットが受信されると、最初にトランクの VLAN 単位の固有フィルタが確認されます。このフィルタが存在する場合は、これが適用されます。メイン トランク ポート フィルタおよび SVI フィルタは無視されます。トランクの VLAN 単位のフィルタが存在しない場合は、メイン トランク ポート フィルタが使用されます。これらのフィルタがいずれも存在しない場合は、VLAN の SVI フィルタがトランク モードのポートの最後のデフォルトとして使用されます。

IGMP フィルタリングのデフォルト設定

なし。

IGMP フィルタの設定方法

IGMP グループおよびチャネル アクセス コントロールの設定

IGMP グループまたはチャネル上でフィルタリングすることにより、ユーザはポート上に、またはトランク ポート上の VLAN 単位で追加できる IGMP グループまたはチャネルを制御します。

IGMP グループまたはチャネルにフィルタリングを設定するには、次の CLI コマンドを使用します。

ip igmp snooping access-group *acl* [**vlan** *vlan_id*]

複数のグループまたはチャネルを許可または拒否するには、アクセス コントロール リストで複数のアクセス コントロール エントリ（ACE）を設定する必要があります。ACL が許可か拒否のいずれに設定されるかに応じて、対応するグループまたはチャネルが許可、あるいは拒否されます。指定される ACL は、単一の ACL または拡張 ACL のいずれかになります。

IGMP グループまたはチャネルによるフィルタリングは、レイヤ 3 SVI 上でデフォルト フィルタとして、この SVI の下のアクセス モードのすべてのポート、およびこれに対応する VLAN を伝送するすべてのトランク ポート上の VLAN に対して設定できます。また、フィルタはレイヤ 2 ポート上でも設定できます。ポートがアクセス モードの場合、このフィルタはすべてのデフォルトの SVI フィルタを無効にします。ポートがトランク モードの場合、このフィルタはそのトランク上のすべての VLAN に対してデフォルトとして動作し、対応する各 VLAN の SVI フィルタを無効にします。

ポートがトランク ポートの場合、**vlan** キーワードにより指定のレイヤ 2 VLAN に着信する IGMP パケットに対してだけフィルタを適用するようにできます。この VLAN 単位のフィルタ（**vlan** キーワードにより設定）は、同一 VLAN のすべてのインターフェイス レベルのフィルタおよびすべての SVI フィルタを無効にします。

IGMP グループおよびチャネル制限の設定

IGMP グループおよびチャネルの数を制限することにより、ポートまたはトランク ポートの VLAN 単位で追加できる IGMP グループおよびチャネルの数を制御できるようになります。

IGMP グループまたはチャネル数を制限するには、次のインターフェイス コマンドの CLI を使用します。

ip igmp snooping limit *n* [**except** *acl*] [**vlan** *vlan_id*]

最大 *n* 数のグループまたはチャネルが、ポートまたはインターフェイスに許可されます。**except** キーワードにより、設定された制限から除外するグループまたはチャネルを指定できます。**except** キーワードを使用した ACL の場合、単一 ACL または拡張 ACL のいずれかになります。

同一インターフェイス上の（*,G1）および（S1,G1）に対して Join が受信された場合、これらは 2 つの別個の Join としてカウントされます。インターフェイス上での制限が 2 と設定されていて、（*,G1）および（S1,G1）に対して Join が受信された場合、その他のすべての Join（これら 2 つ以外のグループまたはチャネルに対する）は廃棄されます。

このフィルタは、レイヤ 3 SVI 上でデフォルト フィルタとして、この SVI の下のアクセス モードのすべてのポート、およびこれに対応する VLAN を伝送するすべてのトランク ポート上の VLAN に対して設定できます。また、フィルタはレイヤ 2 ポート上でも設定できます。レイヤ 2 ポートがアクセス モードの場合、このフィルタはすべてのデフォルトの SVI フィルタを無効にします。レイヤ 2 スイッチ ポートがトランク モードの場合、このフィルタはそのトランク上のすべての VLAN に対してデフォルトとして動作し、対応する各 VLAN の SVI フィルタを無効にします。レイヤ 2 スイッチ ポートがトランク ポートの場合、**vlan** キーワードにより指定のレイヤ 2 VLAN に着信する IGMP パケットに対してだけフィルタを適用するようにできます。この VLAN 単位のフィルタ（**vlan** キーワードにより設定）は、同一 VLAN のすべてのインターフェイス レベルのフィルタおよびすべての SVI フィルタを無効にします。

IGMP バージョン フィルタリングの設定

IGMP プロトコルでのフィルタリングにより、SVI 上で許可される IGMP ホストの最小バージョンを設定できます。たとえば、すべての IGMPv1 ホストを禁止する（IGMP バージョン 2 以上を許可するなど）、またはすべての IGMPv1 および IGMPv2 ホストを禁止する（IGMP バージョン 3 以上を許可するなど）ことが可能です。このフィルタリングは、メンバーシップ レポートにだけ適用されます。

IGMP プロトコルにフィルタリングを設定するには、次の CLI コマンドを使用します。

```
ip igmp snooping minimum-version 2 | 3
```

このフィルタは、レイヤ 3 SVI 上でデフォルト フィルタとして、この SVI の下のアクセス モードのすべてのポート、およびすべてのトランク ポート上の対応する VLAN に対して設定できます。

IGMP フィルタリングの統計情報のクリア

IGMP フィルタリングの統計情報をクリアするには、次のいずれかの作業を行います。

コマンド	目的
`Router# clear ip igmp snooping filter statistics`	すべてのアクセス ポート、およびすべてのトランク ポート上のすべての VLAN に関する IGMP フィルタリングの統計情報をクリアします。
`Router# clear ip igmp snooping filter statistics interface interface_name`	特定のアクセス ポート、または特定のトランク ポート上のすべての VLAN の統計情報をクリアします。
`Router# clear ip igmp snooping filter statistics interface interface_name vlan vlan_ID`	トランク ポート上の特定の VLAN の統計情報をクリアします。

IGMP フィルタリングの設定の確認

IGMP フィルタリングの設定の表示

IGMP フィルタリングの規則を表示するには、次の作業を行います。

コマンド	目的
`Router(config-if)# show ip igmp snooping filter interface interface-name [details]`	指定のインターフェイスに設定されたフィルタを表示します。

次に、SVI 上に設定されたデフォルトのフィルタを表示する例を示します。

```
Router# show ip igmp snooping filter interface vlan 20
Access-Group: Channel1-Acl
Groups/Channels Limit:100 (Exception List: Channel6-Acl)
IGMP Minimum-Version:Not Configured
```

次に、SVI の下でアクセス モードのすべてのポート、および対応する VLAN を伝送するすべてのトランク ポートに設定されたフィルタを表示する例を示します。

```
Router# show ip igmp snooping filter interface g3/48
  Access-Group: Channel4-Acl
  Groups/Channels Limit:10 (Exception List: Channel3-Acl)
```

次に、この SVI の下でアクセス モードのすべてのポートに設定されたフィルタを表示する例を示します。

```
Router# show ip igmp snooping filter interface vlan 20 detail
```

```
GigabitEthernet3/47 :
  Access-Group: Not Configured
  Groups/Channels Limit: Not Configured
GigabitEthernet3/48      :
  Access-Group: Channel4-ACL
  Groups/Channels Limit: 10     (Exception-list: Channel3-Acl)
```

次に、デフォルトのトランク ポート フィルタを表示する例を示します。

```
Router# show ip igmp snooping filter interface g3/46
  Access-Group: Channel1-Acl
  Groups/Channels Limit: 10 (Exception List: Channel3-Acl)
```

次に、このトランク上のすべての VLAN の VLAN 単位フィルタを表示する例を示します。

```
Router# show ip igmp snooping filter interface g3/46 detail
Vlan 10  :
  Access-Group: Not Configured
  Groups/Channels Limit: Not Configured
Vlan 20  :
  Access-Group: Not Configured
        Groups/Channels Limit: 8 (Exception List: Channel4-Acl)
```

次に、このトランク上の特定の VLAN の VLAN 単位フィルタを表示する例を示します。

```
Router# show ip igmp snooping filter interface g3/46 vlan 20
  Access-Group: Not Configured
  Groups/Channels Limit: 8 (Exception List: Channel4-Acl)
```

（注） ポートがシャットダウン ステートの場合、ポートがトランク モードかアクセス モードかを判別できないため、フィルタ ステータスは表示されません。この場合、**show running-config interface** *xxxx* コマンドを使用して設定を確認します。

IGMP フィルタリングの統計情報の表示

統計情報は、アクセス モードのポートにはインターフェイス単位で、トランク モードのポートには VLAN 単位で維持されます。

IGMP フィルタリングの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(config-if)# **show ip igmp snooping filter interface** *interface-name* [**statistics**]	指定のインターフェイスから収集されるフィルタリングの統計情報を表示します。

次に、SVI の下のアクセス モードの各ポートの統計情報を表示する例を示します。

```
Router# show ip igmp snooping filter interface vlan 20 statistics
GigabitEthernet3/47       :
  IGMP Filters are not configured

GigabitEthernet3/48       :
  Access-group denied : 0
  Limit denied : 2
  Limit status : 0 active out of 2 max
  Minimum-version denied : 0
```

次に、アクセス モードの特定ポートに関する統計情報を表示する例を示します。

```
Router# show ip igmp snooping filter interface g3/48 statistics
```

```
  Access-group denied : 0
  Limit denied : 2
  Limit status : 0 active out of 2 max
  Minimum-version denied : 0
```

次に、デフォルトの SVI フィルタもポート フィルタも設定されていない、アクセス モードのポート Gigabit Ethernet 3/47 の統計情報を表示する例を示します。

```
Router# show ip igmp snooping filter interface g3/47 statistics
IGMP Filters are not configured
```

次に、トランクの下のすべての VLAN に関する統計情報を表示する例を示します。

```
Router# show ip igmp snooping filter interface g3/46 statistics
Vlan 10   :
IGMP Filters are not configured

Vlan 20   :
  Access-group denied : 0
  Limit denied : 0
  Minimum-version denied : 0
```

次に、トランクの下の特定の VLAN に関する統計情報を表示する例を示します。

```
Router# show ip igmp snooping filter interface g3/46 vlan 20 statistics
  Access-group denied : 0
  Limit denied : 0
  Minimum-version denied : 0
```

次に、トランクおよび VLAN フィルタが設定されていないトランク ポートの下の特定の VLAN の統計情報を表示する例を示します。

```
Router# show ip igmp snooping filter interface g3/46 vlan 10 statistics
IGMP Filters are not configured
```

（注） ポートがシャットダウン ステートの場合、ポートがトランク モードかアクセス モードかを判別できないため、フィルタの統計情報は表示されません。

IGMP フィルタリングの設定例

次に、フィルタ階層の例を示します。次の SVI VLAN 100 の設定には、3 つのアクセス ポート（g1/1、g1/2、および g1/3）が含まれます。

VLAN 100：

```
Router(config-if)# ip igmp snooping limit 20
```

ポート g1/1：

```
Router(config-if)# ip igmp snooping limit 35
```

ポート g1/2：

```
Router(config-if)# no limit filter
```

ポート g1/3：

```
Router(config-if)# no limit filter
```

この例では、g1/1 の制限値が 35 で、g1/2 の制限値が 20、また g1/3 の制限値も 20 となります。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CHAPTER 48

IPv4 ルータ ガード

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

ルータ ガードの前提条件

なし。

ルータ ガードの制約事項

なし。

ルータ ガードについて

ルータ ガード機能により、指定のポートをマルチキャスト ルータ ポートではなく、マルチキャスト ホスト ポートとしてだけ指定できます。このポートで受信されたマルチキャスト ルータ制御パケットは、ドロップされます。

スイッチが、マルチキャスト ルータ制御パケット（IGMP 一般クエリー、PIM hello、CGMP hello など）の 1 つを受信した場合、ポートはマルチキャスト ルータ ポートとなります。ポートがマルチキャスト ルータ ポートとなると、すべてのマルチキャスト トラフィック（既知および未知両方の送信元トラフィック）がすべてのマルチキャスト ルータ ポートに送信されます。これは、ルータ ガード機能がなければ防止できません。

ルータ ガード機能が設定されている場合、指定のポートをホスト ポートだけにすることができます。マルチキャスト ルータ制御パケットを受信した場合でも、ポートはルータ ポートになりません。

さらに、マルチキャスト ルータから通常どおり受信されたすべての制御パケット（IGMP クエリーおよび PIM Join など）も、このフィルタにより廃棄されます。

ルータ ガード コマンドを入力すると、ユーザ ポリシーがレイヤ 3 SVI インターフェイス、レイヤ 2 ポート、またはレイヤ 2 トランク ポート上の特定の VLAN に適用されます。レイヤ 2 ポートは、アクセス ポートまたはトランク ポートとなる可能性があります。

ルータ ガード機能では、IGMP スヌーピングをイネーブルにする必要はありません。

ルータ ガードは、IPv4 にだけ実装されます。

ルータ ガードは通常、イーサネットツーホームの配置シナリオでのエンドユーザ ボックスに接続されたアクセス スイッチで使用されます。

IPv4 マルチキャスト ルータ ガード機能は、SSO に準拠します。

ルータ ガードがイネーブルであるポート上で次のパケット タイプが受信された場合は、廃棄されます。

- IGMP クエリー メッセージ
- IPv4 PIMv2 メッセージ
- IGMP PIM メッセージ（PIMv1）
- IGMP Distance Vector Multicast Routing Protocol（DVMRP）メッセージ
- Router-Port Group Management Protocol（RGMP）メッセージ
- CGMP メッセージ

これらのパケットが廃棄されると、統計情報が更新され、パケットがルータ ガードによりドロップされていることが示されます。

ルータ ガードは、グローバルおよびインターフェイス単位で設定できます。グローバル設定は、すべてのレイヤ 2 ポートに対してルータ ガードを開始します。これは、たとえば、マルチキャスト ルータが接続されているポート上などで、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変更できます。

ルータ ガードのデフォルト設定

なし。

ルータ ガードの設定方法

ルータ ガードのグローバルなイネーブル化

ルータ 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
`Router# router-guard ip multicast switchports`	ルータ ガードをグローバルにイネーブルにします。

ポート上のルータ ガードのディセーブル化

マルチキャスト ルータが接続されているレイヤ 2 ポート上でルータ ガード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
`Router(config-if)# no router-guard ip multicast [vlan vlan_id]`	レイヤ 2 ポート上でルータ ガードをディセーブルにします。 （注）　**vlan** キーワードは、ポートがトランク モードの場合に限り有効です。このキーワードを使用すると、トランク ポート上の特定の VLAN に対するルータ ガードだけを無効にできます。

次に、トランク ポート Gigabit Ethernet 3/46、VLAN 20 上でマルチキャスト ルータ メッセージを許可する例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 3/46
Router(config-if)# no router-guard ip multicast vlan 20
```

ルータ ガードの統計情報のクリア

ルータ ガードの統計情報をクリアするには、次のいずれかの作業を行います。

コマンド	目的
`Router(config)# clear router-guard ip multicast statistics`	すべてのアクセス ポート、およびすべてのトランク ポート上のすべての VLAN に関する統計情報をクリアします。
`Router(config)# clear router-guard ip multicast statistics interface` *interface_name*	アクセス ポート、およびトランク ポート上のすべての VLAN に関する統計情報をクリアします。
`Router(config)# clear router-guard ip multicast statistics interface` *interface_name* `vlan` *v*	トランク ポート上の特定の VLAN の統計情報をクリアします。

次に、トランク ポート上の特定の VLAN の統計情報をクリアする例を示します。

```
Router# clear router-guard ip multicast statistics interface interface_name vlan v
```

ルータ ガードの設定の確認

ルータ ガードの設定の表示

グローバルなルータ ガード設定および特定のインターフェイスのルータ ガ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
`Router# show router-guard`	グローバルなルータ ガードの設定を表示します。
`Router# show router-guard interface` *interface_name*	特定のインターフェイスのルータ ガードの設定を表示します。

次に、ルータ ガードがアクティブではないアクセス モードのポートのインターフェイス コマンド出力を表示する例を示します。

```
Router# show router-guard interface g3/48
  Router Guard for IP Multicast:
Globally enabled for all switch ports
Enabled on this interface
Packets denied:
  IGMP Queries:
  PIMv2 Messages:
  PIMv1 Messages:
  DVMRP Messages:
  RGMP Messages:
  CGMP Messages:
```

次に、トランク モードのポートのインターフェイス コマンド出力を表示する例を示します。

```
Router# show router-guard interface g3/48
  Router Guard for IP Multicast:
Globally enabled for all switch ports
Disabled on this interface
```

次に、トランク ポートが VLAN 10 および 20 を伝送していることを確認する例を示します。

```
Router# show router-guard interface g3/46
  Router Guard for IP Multicast:
Globally enabled for all switch ports
Default: Enabled for all VLANs on this interface
VLAN 10:
Enabled on this VLAN
Packets denied:
  IGMP Queries:
  PIMv2 Messages:
  PIMv1 Messages:
  DVMRP Messages:
  RGMP Messages:
  CGMP Messages:
VLAN 20 :
Disabled on this VLAN
```

（注） ポートがシャットダウン ステートの場合、ポートがトランク モードかアクセス モードかを判別できないため、ステータスは表示されません。**show running-config interface** *xxxx* コマンドを使用すると、ルータ ガード設定を表示できます。

ルータ ガードのインターフェイスの表示

ルータ ガードがディセーブルなすべてのインターフェイスのリストを表示するには、次の作業を行います。

コマンド	目的
Router# **show router-guard interface** Router Guard for IP Multicast: Globally enabled for all switchports Interfaces: Gi3/46: Disabled on this port for VLANS: ALL	ルータ ガードがディセーブルなすべてのインターフェイスのリストを表示します。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

IPv4 マルチキャスト VPN サポート

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

mVPN の前提条件

なし。

mVPN に関する制約事項

一般的な制約事項

- マルチキャスト ドメインのすべての PE ルータでは、mVPN 機能をサポートする Cisco IOS ソフトウェア イメージを実行する必要があります。P ルータおよび CE ルータには、mVPN をサポートするための要件がありません。
- すべてのバックボーン ルータでは、IPv4 マルチキャスト トラフィックのサポートをイネーブルにする必要があります。
- マルチキャスト トラフィックをサポートするすべてのルータでは、ボーダー ゲートウェイ プロトコル（BGP）ルーティング プロトコルを設定して動作させる必要があります。BGP 拡張コミュニティをイネーブルにしないと（**neighbor send-community both** コマンドまたは **neighbor send-community extended** コマンドを使用）、ネットワークにおける MDT の使用がサポートされません。
- スイッチが PE として動作しており、Time-To-Live（TTL）値が 2 であるカスタマー ルータからマルチキャスト パケットを受信した場合、そのパケットは、カプセル化されて mVPN リンクを横断して転送される代わりにドロップされます。mVPN リンクの反対側の PE がこのようなパケットを正常にドロップするので、トラフィック フローは影響されません。
- コア マルチキャスト ルーティングが SSM を使用する場合は、データ Multicast Distribution Tree（MDT）グループおよびデフォルト マルチキャスト配信ツリー（MDT）グループを IPv4 アドレスの SSM 範囲内で設定する必要があります。
- BGP ピアリングの更新送信元インターフェイスは、ルータで設定されているすべての BGP ピアリングで同一でないと、デフォルト MDT は適切に設定されません。BGP ピアリングにループバック アドレスを使用する場合は、ループバック アドレスで PIM sparse モードをイネーブルにする必要があります。
- BGP ピアリング インターフェイスとして使用されるループバック インターフェイスで **ip mroute-cache** コマンドをイネーブルにしないと、分散マルチキャスト スイッチングは、それをサポートするプラットフォームで機能しません。このようなインターフェイスでは、**no ip mroute-cache** コマンドを*設定しないでください*。
- dense モード マルチキャスト フローにはフラッディングとプルーニングという性質があり、データ MDT の周期的な始動および分解という結果になるので、データ MDT は VRF PIM dense モード マルチキャスト ストリームで作成されません。
- 送信元情報が使用できないので、VRF PIM 双方向モードではデータ MDT が作成されません。
- mVPN では複数の BGP ピアリング更新送信元がサポートされず、これを設定すると、mVPN Reverse Path Forwarding（RPF）チェックが中断することがあります。mVPN トンネルの送信元 IPv4 アドレスは、BGP ピアリング更新送信元に使用される最高の IPv4 アドレスによって決まります。この IPv4 アドレスが、リモート PE ルータを含む BGP ピアリング アドレスとして使用される IPv4 アドレスでない場合、mVPN は適切に機能しません。
- MDT トンネルではユニキャスト トラフィックが搬送されません。
- mVPN が MPLS VPN ネットワークのインフラストラクチャを使用する場合、MPLS タグやラベルは、VPN 上のマルチキャスト トラフィックに適用できません。
- デフォルト MDT で設定されている各 mVRF は、ユーザに表示される外部 VLAN に加えて、3 つの非表示 VLAN（カプセル化、カプセル化解除、インターフェイスに 1 つずつ）を使用します。つまり各ルータでは、絶対最大値の 1,000 mVRF がサポートされます。（MDT が設定されていない mVRF では 1 つの内部 VLAN が使用されるので、未使用 mVRF を削除して VLAN 割り当てを維持する必要があります）。

- MPLS VPN ネットワークに VRF のネットワークがすでに含まれている場合は、そのネットワークを削除したり再作成したりしなくても、mVRF トラフィックをサポートできます。その代わりに次の手順に示すように **mdt default** コマンドおよび **mdt data** コマンドを設定し、VRF 上でマルチキャスト トラフィックをイネーブルにしてください。
- 特定 VPN 接続をサポートする各 PE ルータでは、同一 mVRF を設定する必要があります。
- 特定 mVRF をサポートする各 PE ルータは、同じ **mdt default** コマンドで設定する必要があります。

mVPN with L3VPN over mGRE の制約事項

- 15.1(1) SY よりも前のリリースでは、mVPN with L3VPN over mGRE が設定されている場合、スーパーバイザ エンジンのポート、または CFC のあるスイッチング モジュールのポートには、IPv4 ルーティングを設定しないでください。（CSCtr05033）
- RP へのユニキャスト パスがスーパーバイザ エンジンのポートを使用しないことを確認してください。さらに VSS モードで、RP へのユニキャスト パスが CFC のあるスイッチング モジュールのポートを使用しないことを確認してください。（CSCts43614）
- GRE トンネルの宛先アドレスおよび送信元アドレスが mGRE トンネルと同じである場合、GRE トンネルはルートキャッシュが切り替えられます。
- フラグメンテーションが必要なパケットは、ルートキャッシュが切り替えられます。
- L3VPN プロファイルをいったん削除して後で戻す場合、**clear ip bgp** *neighbor_ip_address* **soft** コマンドを使用して、ボーダー ゲートウェイ プロトコル（BGP）をクリアする必要があります。
- mGRE トンネルが作成されると、ダミー トンネルも作成されます。
- BGP コンフィギュレーションのアップデート元で使用されるループバックまたは IP アドレスは、L3VPN プロファイルの送信元と同じである必要があります。
- mGRE は、ステートフル スイッチオーバー（SSO）には対応していません。ただし、mGRE と SSO の両方が共存します。
- ハードウェア内で、すべての GRE オプションがサポートされているわけではありません（GRE 拡張ヘッダーや GRE キーなど）。
- トンネル上では、複数の同一 VLAN（インターネット制御メッセージ プロトコル（ICMP）リダイレクト）のチェックはサポートされていません。
- トンネル上では、ユニキャスト リバース パス転送（uRPF）や BGP ポリシー アカウントなどの機能はサポートされていません。

mVPN について

- 「mVPN with L3VPN over mGRE について」（P.49-9）

mVPN の概要

mVPN は仮想化されたプロバイダー ネットワーク（たとえば、MPLS または mGRE トンネルなど）全体で IPv4 マルチキャスト トラフィックを伝送する標準機能です。mVPN は、VPN を介してワイヤ速度でマルチキャスト トラフィックを転送するのに、IPv4 マルチキャスト トラフィックに対する PFC ハードウェア サポートを使用します。mVPN では、レイヤ 3 IPv4 VPN 上における IPv4 マルチキャスト トラフィックのサポートが、既存の IPv4 ユニキャスト サポートに追加されます。

mVPN では、VPN ルーティング/転送（VRF）インスタンスごとにマルチキャスト パケットのルーティングおよび転送が行われ、サービス プロバイダー バックボーンを横断して VPN トンネルでマルチキャスト パケットが送信されます。

mVPN は、フル メッシュのポイントツーポイント GRE トンネルの代替手段です。簡単に拡張できるソリューションではなく、カスタマーに提供される粒度に制限があります。

マルチキャスト ルーティング、転送、マルチキャスト ドメイン

mVPN では、VPN ルーティング/転送テーブルにマルチキャスト ルーティング情報が追加されます。プロバイダー エッジ（PE）ルータがマルチキャスト データまたは制御パケットをカスタマー エッジ（CE）ルータから受信すると、マルチキャスト VRF（mVRF）の情報に従って転送が実行されます。

それぞれの mVRF では、特定 VRF インスタンスに必要となるルーティング情報および転送情報が維持されます。mVRF の作成と設定は既存 VRF と同じ方法で行われますが、それぞれの mVRF ではマルチキャスト ルーティングもイネーブルになります。

マルチキャスト ドメインは、MPLS ネットワークで相互にマルチキャスト トラフィックを送信できるホストのセットで構成されます。たとえば、特定タイプのマルチキャスト トラフィックをすべてのグローバルな従業員に送信するカスタマーのマルチキャスト ドメインは、そのエンタープライズと関連するすべての CE ルータから構成されます。

Multicast Distribution Tree（MDT）

mVPN 機能では、少なくとも 1 つの Multicast Distribution Tree（MDT）がマルチキャスト ドメインごとに確立されます。MDT では、さまざまな PE ルータに存在する同一 mVRF の相互接続に必要となる情報が提供されます。

mVPN では、次の 2 つの MDT タイプがサポートされます。

- デフォルト MDT：特定マルチキャスト ドメインのすべての PE ルータ間における PIM 制御メッセージおよび低帯域幅ストリームの永続チャネルです。デフォルト MDT におけるすべてのマルチキャスト トラフィックは、ドメインのその他すべての PE ルータに複製されます。各 PE ルータは、ドメインのその他すべての PE ルータから、論理的に PIM ネイバー（1 ホップ先）と見なされます。
- データ MDT：これはオプションです。イネーブルにするとダイナミックに作成され、フルモーション ビデオなど、すべての PE ルータに送信する必要がない高帯域幅送信用に最適なパスが提供されます。これにより、PE ルータ間において高帯域幅トラフィックのオンデマンド転送が可能になるので、作成されるすべての高帯域幅ストリームですべての PE ルータがフラッディングされなくなります。

データ MDT を作成するため、バックボーンにマルチキャスト ストリームを定期的に転送する各 PE ルータは、各デフォルト MDT で送信されるトラフィックを次のように定期的に検査します。

1. 各 PE ルータはマルチキャスト トラフィックを定期的にサンプル抽出して（ソフトウェア スイッチングの場合は約 10 秒ごと、ハードウェア スイッチングの場合は 90 秒ごと）、マルチキャスト ストリームが設定しきい値を超えているかどうかを判断します （ストリームのサンプル抽出タイミングにより、最悪の場合は、高帯域幅ストリームが検出されるまでに最大 180 秒かかることがあります）。

   （注）　データ MDT は、VRF マルチキャスト ルーティング テーブル内で、（S,G）マルチキャスト ルート エントリ専用に作成されます。（*,G）エントリ用には作成されません。

2. 特定マルチキャスト ストリームが定義済みしきい値を超えた場合、送信側 PE ルータは、その特定マルチキャスト トラフィック用にデータ MDT をダイナミックに作成します。
3. 送信側 PE ルータは、その他の PE ルータに DATA-MDT JOIN 要求（ポート 3232 へのユーザ データグラム プロトコル（UDP）メッセージ）を送信し、新しいデータ MDT について通知します。
4. 受信側 PE ルータは VRF ルーティング テーブルを調べて、このデータ ストリームの受信に関係するカスタマーがいるかどうかを判断します。そのようなカスタマーがいる場合、受信側 PE ルータは PIM プロトコルを使用し、この特定データ MDT グループの PIM JOIN メッセージ（グローバル テーブル PIM インスタンス）を送信してストリームを受け入れます。このストリームのカスタマーがいないルータは、カスタマーがあとでそのストリームを要求したときのため、情報をキャッシュします。
5. 送信側 PE ルータは、DATA-MDT JOIN メッセージ送信の 3 秒後、高帯域幅マルチキャスト ストリームをデフォルト MDT から削除し、新しいデータ MDT で送信し始めます。
6. 送信側 PE ルータは、マルチキャスト ストリームが定義済みしきい値を超え続ける限り、60 秒ごとに DATA-MDT JOIN メッセージの送信を続けます。ストリームが 60 秒より長くしきい値を下回った場合、送信側 PE ルータは DATA-MDT JOIN メッセージの送信を停止し、ストリームをデフォルト MDT に戻します。
7. 受信側ルータは、3 分より長く DATA-MDT JOIN メッセージを受信しなかった場合、デフォルト MDT のキャッシュ情報と期限切れにします。

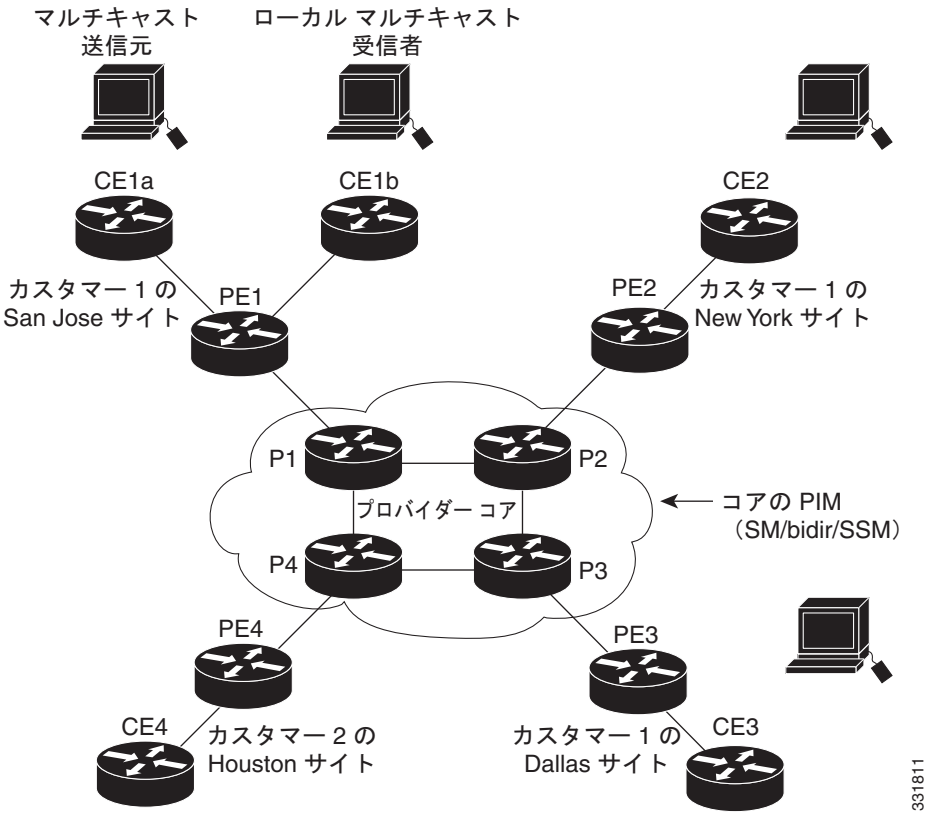
データ MDT では高帯域幅の送信元が VPN 内部で許可されますが、MPLS VPN コアでの最適トラフィック転送が確保されます。

次の例のサービス プロバイダーには、San Jose、New York、Dallas にオフィスがあるマルチキャスト カスタマーがいます。San Jose サイトは、単方向マルチキャスト プレゼンテーションを送信しています。サービス プロバイダー ネットワークでは、このカスタマーと関連する 3 つすべてのサイト、および別のエンタープライズ カスタマーの Houston サイトがサポートされます。

エンタープライズ カスタマーのデフォルト MDT は、プロバイダーのルータ P1、P2、P3、およびその関連 PE ルータから構成されています。PE4 は、MPLS コアのその他のルータに相互接続されていますが、別のカスタマーと関連しているので、デフォルト MDT の一部ではありません。

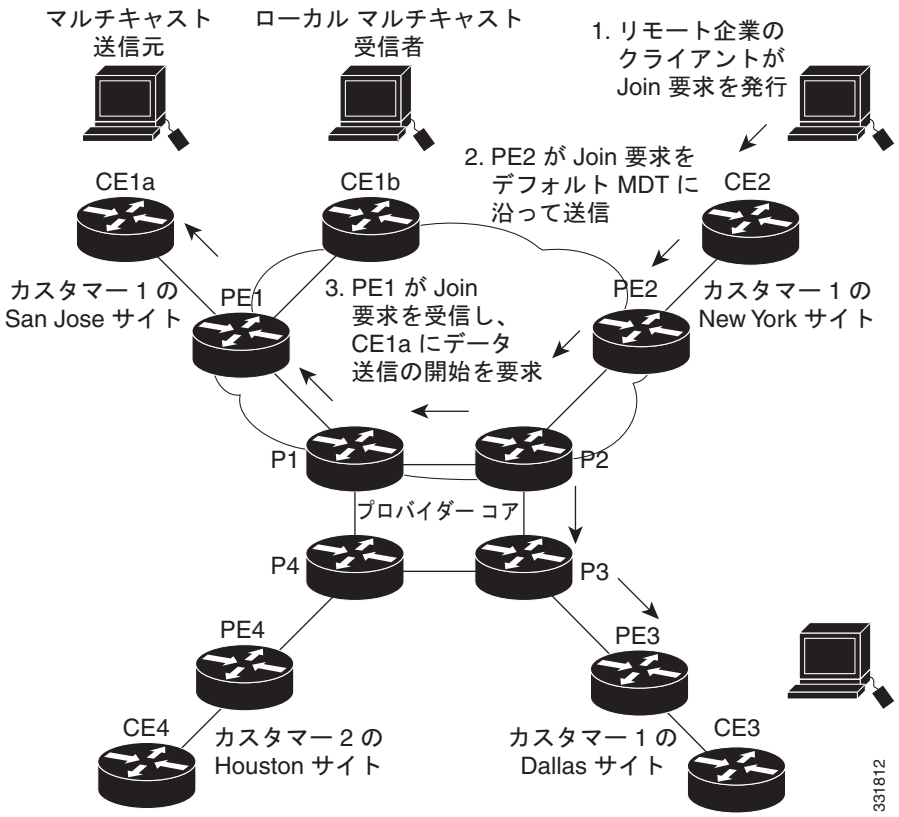
図 49-1 は、San Jose の外側でマルチキャスト ブロードキャストに加入するユーザがいない場合、つまりデフォルト MDT でデータが流れない場合のネットワークの状況を示しています。各 PE ルータはデフォルト MDT 上にあるその他の PE ルータとの PIM 関係を維持し、直接接続している PE ルータとの PIM 関係も維持します。

図 49-1　デフォルト マルチキャスト配信ツリーの概要



New York の従業員がマルチキャスト セッションに加入した場合、ニューヨーク サイトに関連する PE ルータは Join 要求を送信します。この Join 要求は、マルチキャスト ドメインのデフォルト MDT に流れます。マルチキャスト セッション送信元（PE1）と関連する PE ルータは、この要求を受信します。図 49-2 は、PE ルータが、マルチキャスト送信元（CE1a）と関連する CE ルータに要求を転送する方法を示しています。

図 49-2　データ MDT の初期化



CE ルータ（CE1a）は関連 PE ルータ（PE1）にマルチキャスト データを送信し始め、PE ルータは、マルチキャスト データが帯域幅しきい値を超えているためにデータ MDT を作成する必要があることを認識します。PE1 はデータ MDT を作成し、データ MDT に関する情報を含むデフォルト MDT を使用してすべてのルータにメッセージを送信します。

約 3 秒後、PE1 は、データ MDT を使用してその特定ストリームのマルチキャスト データを送信し始めます。この送信元に関係するレシーバは PE2 だけにいるので、PE2 だけがデータ MDT に加入してデータ MDT でトラフィックを受信します。

Multicast Tunnel Interface

PE ルータは、マルチキャスト ドメインのマルチキャスト VRF（mVRF）ごとに Multicast Tunnel Interface（MTI）を作成します。mVRF はトンネル インターフェイスを使用してマルチキャスト ドメインにアクセスし、mVRF とグローバル mVRF を接続するコンジットを提供します。

ルータの場合、MTI はクラス D マルチキャスト アドレスを含むトンネル インターフェイスです（**interface tunnel** コマンドで作成）。この mVRF 用にデフォルト MDT で設定したすべての PE ルータは論理ネットワークを作成し、この論理ネットワークでは、各 PE ルータが、マルチキャスト ドメインにあるその他すべての PE ルータの PIM ネイバー（1 ホップ先）として表示されます。この場合、各ルータ間の物理的な距離は関係ありません。

mVRF を設定すると、MTI は自動的に作成されます。BGP ピアリング アドレスは MTI インターフェイス送信元アドレスとして割り当てられ、PIM プロトコルは各 MTI で自動的にイネーブルになります。

ルータは、ネットワークのカスタマー側からマルチキャスト パケットを受信すると、着信インターフェイスの VRF を使用して、受信する mVRF を判断します。次にルータは、GRE カプセル化を使用してパケットをカプセル化します。ルータは、パケットをカプセル化するとき、送信元アドレスを BGP ピアリング インターフェイスの送信元アドレスに、デフォルト MDT のマルチキャスト アドレス、またはデータ MDT の送信元アドレス（設定されている場合）に宛先アドレスを設定します。次にルータは、適切な数の MTI インターフェイスで転送するために、必要に応じてパケットを複製します。

ルータは、MTI インターフェイスでパケットを受信すると、宛先アドレスを使用して適切なデフォルト MDT またはデータ MDT を識別し、適切な mVRF を識別します。次にパケットのカプセル化を解除し、必要なだけ複製して適切なインターフェイスに転送します。

（注）

- mVPN MTI は、Cisco ルータで一般的に使用されるその他のトンネル インターフェイスと異なり、ポイントツーポイント インターフェイスではなく、LAN インターフェイスとして分類されます。MTI インターフェイスは設定可能でありませんが、**show interface tunnel** コマンドを使用してそのステータスを表示できます。
- MTI インターフェイスは、VPN トンネル上のマルチキャスト トラフィックに排他的に使用されます。
- このトンネルは、ユニキャストでルーティングされたトラフィックを搬送しません。

mVPN の PE ルータ ルーティング テーブルのサポート

mVPN フィーチャをサポートする各 PE ルータは、次のルーティング テーブルを使用して、VPN トラフィックおよび mVPN トラフィックを正しくルーティングします。

- デフォルト ルーティング テーブル：すべての Cisco ルータで使用される標準ルーティング テーブル。このテーブルには、バックボーン トラフィック、および非 VPN 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（総称ルーティング カプセル化（GRE）マルチキャスト トラフィックを含む）に必要なルートが含まれています。
- VPN ルーティング/転送（VRF）テーブル：VRF インスタンスごとに作成されるルーティング テーブル。プロバイダー ネットワークの VPN 間でユニキャスト トラフィックをルーティングします。
- マルチキャスト VRF（mVRF）テーブル：VRF インスタンスごとに作成されるマルチキャスト ルーティング テーブルおよびマルチキャスト ルーティング プロトコル インスタンス。ネットワークのマルチキャスト ドメインでマルチキャスト トラフィックをルーティングします。このテーブルには、マルチキャスト ドメインへのアクセスに使用される Multicast Tunnel Interface も含まれます。

Multicast Distributed Switching サポート

mVPN では、インターフェイス単位および VRF 単位でマルチキャストをサポートするため、Multicast Distributed Switching（MDS）がサポートされます。MDS を設定するときには、ループバック インターフェイスも含めたすべてのインターフェイスに **no ip mroute-cache** コマンドが設定されていないことを確認する必要があります。

ハードウェア処理の IPv4 マルチキャスト

Cisco IOS Release 15.1SY では、VPN トラフィック上の IPv4 マルチキャスト用にハードウェア アクセラレーションがサポートされ、RP CPU の使用率を上げずにワイヤ速度で適切な VPN にマルチキャスト トラフィックが転送されます。

カスタマー VRF では、PFC のハードウェア アクセラレーションは、PIM dense（デンス）、PIM スパース、PIM 双方向、PIM Source-Specific Multicast（SSM）モードのマルチキャスト トラフィックをサポートします。

サービス プロバイダー コアでは、PFC のハードウェア アクセラレーションは、PIM スパース、PIM 双方向、PIM SSM モードのマルチキャスト トラフィックをサポートします。サービス プロバイダー コアの場合は、PFC ハードウェア アクセラレーションは PIM dense モードでマルチキャスト トラフィックをサポートしません。

mVPN with L3VPN over mGRE について

（注）　詳細については、「mVPN with L3VPN over mGRE の設定」（P.49-23）を参照してください。

概要

リリース 15.0(1) SY1 以降では、Multicast Virtual Private Network with Layer 3 Virtual Private Network over multipoint Generic Routing Encapsulation (mVPN with L3VPN over mGRE) をサポートします。mVPN with L3VPN over mGRE は標準 IP 専用ネットワークによって接続されている各ネットワーク間で VPN 接続を提供します。mGRE トンネルは、IP ネットワークをオーバーレイし、PE デバイスを接続して、IP コア経由の L3 PE ベースの VPN サービスの展開をサポートする VPN に転送します。

（注）
- mGRE は、ポイントツーマルチポイント モデルなので、各 PE デバイスを相互接続するうえでフル メッシュ構造の GRE トンネルは不要です。
- マルチキャストおよびユニキャスト トラフィックは、個別のトンネル、マルチキャスト用に MDT、およびユニキャスト用に mGRE を使用します。

ルート マップ

デフォルトでは、VPN ユニキャスト トラフィックの送信に LSP が使用されます。mVPN with L3VPN over mGRE 機能では、ユーザ定義のルート マップが使用されて、mGRE トンネルを介して到達可能な VPN プレフィックスと、LSP を使用して到達可能な VPN プレフィックスが決定されます。ルート マップは、VPNv4 および VPNv6 アドレス ファミリのアドバタイズメントに適用されます。ルート マップでは、VPN トラフィックのカプセル化方式の決定に Next Hop Tunnel Table が使用されます。

mGRE トンネルを経由してルーティングされるトラフィックは、代替アドレス空間を使用します。したがって、mGRE トンネルでのトラフィックのカプセル化によって、すべてのネクスト ホップに到達します。mGRE トンネルを使用するように特定のルートを設定するには、ルート マップにそのルートに対するエントリの設定が必要です。その新しいエントリによって、代替アドレス空間に対して、そのルートのネットワーク層到着可能性情報（NLRI）が再マッピングされます。あるルートのルート マップ内に再マッピング エントリが存在しない場合、そのルート上のトラフィックは LSP を介して転送されます。

mVPN with L3VPN over mGRE 機能は、代替アドレス空間を自動的にプロビジョニングします。この空間は通常、トンネルカプセル化された仮想ルーティングおよび転送（VRF）インスタンスに保持されます。アドレス空間を介して到達可能なトラフィックが確実にすべて mGRE トンネル内でカプセル化されるように、トンネル外への単一のデフォルト ルートが自動的にインストールされます。また、ルート マップ上にデフォルト トンネルも自動的に作成されます。デフォルト ルート マップは、適切な BGP アップデートに添付できます。

トンネル エンドポイントの検出およびフォワーディング

mVPN with L3VPN over mGRE 機能は、ネットワーク内のリモート PE を検出できなければならず、リモート PE のトンネル フォワーディング情報を構築できる必要があります。リモート PE が無効となったことが検出され、その PE のトンネル フォワーディング情報が削除されるようにする必要もあります。

入力 PE によって BGP を介して VPN アドバタイズメントが受信される場合、その入力 PE によってルート ターゲット属性（VRF に入力されます）および、アドバタイズメントからの MPLS VPN ラベルが使用され、その結果、プレフィックスと適切なお客様が関連付けられます。入力されたルートのネクスト ホップが、アドバタイズメントの NLRI に設定されます。

アドバタイズされたプレフィックスには、システム内のリモート PE に関する情報が（NLRI の形式で）格納され、PE では、この情報が使用されて、NLRI がアクティブまたは非アクティブになったときシステムに通知されます。システムでは、この通知が使用されて、PE フォワーディング情報がアップデートされます。

この機能によって、新しいリモート PE の通知が受信されると、Tunnel Endpoint Database にその情報が追加され、トンネル インターフェイスに関連付けられた隣接が作成されます。この隣接の説明として、カプセル化に関する情報、およびカプセル化されたパケットを新しいリモート PE に送信するために必要なその他の処理に関する情報が記述されています。

この機能によって、トンネル カプセル化 VRF に隣接情報が示されます。VPN NLRI が VRF 内のルートに（ルート マップを使用して）再マッピングされると、隣接に対して NLRI がリンクされ、これによりトンネルに VPN がリンクされます。

トンネルの非カプセル化

出力 PE が mVPN with L3VPN over mGRE 機能を使用するトンネル インターフェイスからパケットを受信すると、PE は VPN ラベルのタグ付きパケットを作成するために、パケットのカプセル化を解除し、パケットを転送します。

トンネルの送信元

mVPN with L3VPN over mGRE 機能では、大量のエンドポイント（リモート PE）を持つシステムの設定に、mGRE トンネルとして設定された単一のトンネルが使用されます。トンネルカプセル化パケットの送信元を特定するために、システムによってトンネル送信元情報が使用されます。

送信（入力）PE では、VPN パケットがトンネルに送信されるときのトンネル宛先は NLRI です。受信（出力）PE では、トンネル送信元は、mGRE トンネルでカプセル化されたパケットが受信されるアドレスです。そのため、出力 PE では、パケットの宛先がローカル PE からの NLRI と一致している必要があります。

mVPN のデフォルト設定

なし。

mVPN の設定方法

- 「Multicast VPN ルーティング / 転送インスタンスの設定」（P.49-11）
- 「マルチキャスト VRF ルーティングの設定」（P.49-17）
- 「mVPN をサポートするマルチキャスト ルーティング用インターフェイスの設定」（P.49-20）
- 「mVPN with L3VPN over mGRE の設定」（P.49-23）

（注）　この設定タスクでは、マルチキャスト トラフィックを送受信するすべてのルータで BGP がすでに設定されていて動作していることを想定しています。BGP 拡張コミュニティをイネーブルにしないと（**neighbor send-community both** コマンドまたは **neighbor send-community extended** コマンドを使用）、ネットワークにおける MDT の使用がサポートされません。

Multicast VPN ルーティング / 転送インスタンスの設定

- 「VRF エントリの設定」（P.49-12）
- 「ルート識別子の設定」（P.49-12）
- 「ルートターゲット拡張コミュニティの設定」（P.49-12）
- 「デフォルト MDT の設定」（P.49-13）
- 「データ MDT の設定（任意）」（P.49-14）
- 「データ MDT ロギングのイネーブル化」（P.49-14）
- 「設定例」（P.49-15）
- 「VRF 情報の表示」（P.49-15）

VRF エントリの設定

VRF エントリを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# 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	`Router(config)# ip vrf vrf_name`	VRF ルーティング テーブル エントリおよび 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 エントリを設定し、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 3	`Router(config-vrf)# do show ip vrf vrf_name`	設定を確認します。

次に、blue という名前の VRF を設定し、設定を確認する例を示します。

```
Router# configure terminal
Router(config)# ip vrf blue
Router(config-vrf)# do show ip vrf blue
Name                              Default RD          Interfaces
  blue                              <not set>
```

ルート識別子の設定

ルート識別子を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config-vrf)# rd route_distinguisher`	VPN IPv4 プレフィックスのルート識別子を指定します。
ステップ 2	`Router(config-vrf)# do show ip vrf vrf_name`	設定を確認します。

ルート識別子の設定時には、次のうちいずれかの形式でルート識別子を入力してください。

- 16 ビット AS 番号 : 32 ビット番号（101:3）
- 32 ビット IPv4 アドレス : 16 ビット番号（192.168.122.15:1）

次に、ルート識別子として 55:1111 を設定し、設定を確認する例を示します。

```
Router(config-vrf)# rd 55:1111
Router(config-vrf)# do show ip vrf blue
Name                              Default RD          Interfaces
blue                              55:1111
```

ルートターゲット拡張コミュニティの設定

ルートターゲット拡張コミュニ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	`Router(config-vrf)# route-target [import | export | both] route_target_ext_community`	ルートターゲット拡張コミュニティを VRF 用に設定します。
ステップ 2	`Router(config-vrf)# do show ip vrf detail`	設定を確認します。

ルートターゲット拡張コミュニティの設定時には、次に注意してください。

- **import**：ターゲット VPN 拡張コミュニティからルーティング情報をインポートします。
- **export**：ターゲット VPN 拡張コミュニティにルーティング情報をエクスポートします。
- **both**：インポートおよびエクスポートを行います。
- *route_target_ext_community*：48 ビット ルートターゲット拡張コミュニティを VRF に追加します。以下のいずれかの形式で番号を入力します。
  - 16 ビット AS 番号：32 ビット番号（101:3）
  - 32 ビット IPv4 アドレス：16 ビット番号（192.168.122.15:1）

次に、インポートおよびエクスポートのルートターゲット拡張コミュニティとして 55:1111 を設定し、設定を確認する例を示します。

```
Router(config-vrf)# route-target both 55:1111
Router(config-vrf)# do show ip vrf detail
VRF blue; default RD 55:1111; default VPNID <not set>
VRF Table ID = 1
  No interfaces
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:55:1111
  Import VPN route-target communities
    RT:55:1111
  No import route-map
  No export route-map
CSC is not configured.
```

デフォルト MDT の設定

デフォルト MDT を設定するには、次の作業を行います。

コマンド	目的
`Router(config-vrf)# mdt default group_address`	デフォルト MDT を設定します。

デフォルト MDT を設定する際、次の情報に注意してください。

- *group_address* は、デフォルト MDT グループのマルチキャスト IPv4 アドレスです。このアドレスは mVRF コミュニティの識別子として動作します。この同一グループ アドレスで設定したすべてのプロバイダー エッジ（PE）ルータはグループのメンバになり、メンバは、グループの他のメンバが送信した PIM 制御メッセージおよびマルチキャスト トラフィックを受信します。
- これと同じデフォルト MDT を各 PE ルータで設定しないと、PE ルータは、この特定 mVRF のマルチキャスト トラフィックを受信できません。

次に、デフォルト MDT として 239.1.1.1 を設定する例を示します。

```
Router(config-vrf)# mdt default 239.1.1.1
```

データ MDT の設定（任意）

任意のデータ MDT を設定するには、次の作業を行います。

コマンド	目的
Router(config-vrf)# **mdt data** *group_address wildcard_bits* [**threshold** *threshold_value*] [**list** *access_list*]	（任意）マルチキャスト アドレスの指定範囲にデータ MDT を設定します。

任意のデータ MDT の設定時には、次に注意してください。

- *group_address1*：マルチキャスト グループ アドレス。アドレスは 224.0.0.1 ～ 239.255.255.255 の範囲にすることができますが、デフォルト MDT に割り当てたアドレスと重複させることはできません。
- *wildcard_bits*：可能なアドレス範囲を作成するために、マルチキャスト グループ アドレスに適用されるワイルドカード ビット マスク。これにより、各 mVRF がサポートできるデータ MDT の最大数を制限できます。
- **threshold** *threshold_value*：（任意）しきい値をキロビット単位で定義します。このしきい値を超えると、マルチキャスト トラフィックはデフォルト MDT からデータ MDT に切り替わります。*threshold_value* パラメータの範囲は 1 ～ 4294967 キロビットです。
- **list** *access_list*：（任意）このトラフィックに適用するアクセス リスト名または番号を指定します。

次に、データ MDT を設定する例を示します。

```
Router(config-vrf)# mdt data 239.1.2.0 0.0.0.3 threshold 10
```

データ MDT ロギングのイネーブル化

データ MDT ロギ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
Router(config-vrf)# **mdt log-reuse**	（任意）データ MDT が再利用されるたびに Syslog メッセージを生成することで、データ MDT 再利用情報の記録をイネーブルにします。データ MDT が頻繁に再利用される場合は、**mdt data** コマンドで使用されるワイルドカード ビット マスクのサイズを増やして、データ MDT の許可数を増やす必要があります。

次に、データ MDT ロギングをイネーブルにする例を示します。

```
Router(config-vrf)# mdt log-reuse
```

設定例

次のコンフィギュレーション ファイルからの抜粋は、VRF の範囲の典型的な VRF 設定を示しています。表示を簡素にするため、先頭の VRF および末尾の VRF だけを示します。

```
!
ip vrf mvpn-cus1
 rd 200:1
 route-target export 200:1
 route-target import 200:1
 mdt default 239.1.1.1
!
ip vrf mvpn-cus2
 rd 200:2
 route-target export 200:2
 route-target import 200:2
 mdt default 239.1.1.2
!
ip vrf mvpn-cus3
 rd 200:3
 route-target export 200:3
 route-target import 200:3
 mdt default 239.1.1.3
!
...

ip vrf mvpn-cus249
 rd 200:249
 route-target export 200:249
 route-target import 200:249
 mdt default 239.1.1.249
 mdt data 239.1.1.128 0.0.0.7
```

VRF 情報の表示

スイッチで設定されているすべての VRF を表示するには、**show ip vrf** コマンドを使用します。

```
Router# show ip vrf

  Name                             Default RD          Interfaces
  green                            1:52                GigabitEthernet6/1
  red                              200:1               GigabitEthernet1/1
                                                       GigabitEthernet3/16
                                                       Loopback2

Router#
```

すべての mVRF 用に現在設定されている MDT に関する情報を表示するには、**show ip pim mdt** コマンドを使用します。次に、このコマンドの典型的な出力例を示します。

```
Router# show ip pim mdt

  MDT Group       Interface   Source                VRF
* 227.1.0.1       Tunnel1     Loopback0             BIDIR01
* 227.2.0.1       Tunnel2     Loopback0             BIDIR02
* 228.1.0.1       Tunnel3     Loopback0             SPARSE01
* 228.2.0.1       Tunnel4     Loopback0             SPARSE02
```

（注）　特定トンネル インターフェイスに関する情報を表示するには、**show interface tunnel** コマンドを使用します。トンネル インターフェイスの IPv4 アドレスは、mVRF のデフォルト MDT のマルチキャスト グループ アドレスです。

特定 VRF のルーティング情報を表示するには、**show ip route vrf** コマンドを使用します。

```
Router# show ip route vrf red

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     2.0.0.0/32 is subnetted, 1 subnets
C       2.2.2.2 is directly connected, Loopback2
     3.0.0.0/32 is subnetted, 1 subnets
B       3.3.3.3 [200/0] via 3.1.1.3, 00:20:09
C    21.0.0.0/8 is directly connected, GigabitEthernet3/16
B    22.0.0.0/8 [200/0] via 3.1.1.3, 00:20:09

Router#
```

特定 mVRF のマルチキャスト ルーティング テーブルおよびトンネル インターフェイスに関する情報を表示するには、**show ip mroute vrf** コマンドを使用します。次に、BIDIR01 という名前の mVRF の典型的な出力例を示します。

```
Router# show ip mroute vrf BIDIR01

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel
       Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags: H - Hardware switched
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
(*, 228.1.0.1), 00:16:25/stopped, RP 10.10.10.12, flags: SJCF
  Incoming interface: Tunnel1, RPF nbr 10.10.10.12, Partial-SC
  Outgoing interface list:
    GigabitEthernet3/1.3001, Forward/Sparse-Dense, 00:16:25/00:02:49, H
(6.9.0.100, 228.1.0.1), 00:14:13/00:03:29, flags: FT
  Incoming interface: GigabitEthernet3/1.3001, RPF nbr 0.0.0.0, RPF-MFD
  Outgoing interface list:
    Tunnel1, Forward/Sparse-Dense, 00:14:13/00:02:46, H

Router#
```

（注）　この例では、**show ip mroute vrf** コマンドによって、VRF が使用している MDT Tunnel Interface（MTI）が Tunnel1 であることが示されます。

マルチキャスト VRF ルーティングの設定

（注）　マルチキャスト トラフィックの送受信を行うすべてのルータでは、BGP を設定して動作させる必要があります。BGP 拡張コミュニティをイネーブルにしないと（**neighbor send-community both** コマンドまたは **neighbor send-community extended** コマンドを使用）、ネットワークにおける MDT の使用がサポートされません。

IPv4 マルチキャスト ルーティングのグローバルなイネーブル化

IPv4 マルチキャスト ルーティングをグローバルにイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# 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	`Router(config)# ip multicast-routing`	IPv4 マルチキャスト ルーティングをグローバルにイネーブルにします。

次に、IPv4 マルチキャスト ルーティングをグローバルにイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# ip multicast-routing
```

IPv4 マルチキャスト VRF ルーティングのイネーブル化

IPv4 マルチキャスト VRF ルーテ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
`Router(config)# ip multicast-routing vrf` *vrf_name* `[distributed]`	IPv4 マルチキャスト VRF ルーティングをイネーブルにします。

IPv4 マルチキャスト VRF ルーティングをイネーブルにするときは、次の情報に注意してください。

- *vrf_name*：マルチキャスト ルーティングの特定 VRF を指定します。*vrf_name* は、「Multicast VPN ルーティング/転送インスタンスの設定」（P.49-11）で示しているように、前に作成された VRF を参照するようにします。
- **distributed**：（任意）Multicast Distributed Switching（MDS）をイネーブルにします。

次に、IPv4 マルチキャスト VRF ルーティングをイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# ip multicast-routing vrf blue
```

PIM VRF RP アドレスの指定

PIM VRF ランデブー ポイント（RP）を指定するには、次の作業を行います。

コマンド	目的
`Router(config)# ip pim vrf vrf_name rp-address rp_address [access_list] [override] [bidir]`	PIM RP IPv4 アドレスを指定します（sparse PIM ネットワークの場合必須）。

PIM VRF RP アドレスの指定時には、次の情報に注意してください。

- **vrf** *vrf_name*：（任意）使用する特定 VRF インスタンスを指定します。
- *rp_address*：PIM RP ルータのユニキャスト IP アドレス。
- *access_list*：（任意）RP のマルチキャスト グループを定義するアクセス リストの番号または名前。
- **override**：（任意）RP アドレスが競合する場合は、この特定 RP により、Auto-RP で学習した RP を上書きします。
- **bidir**：（任意）*access_list* 引数で指定したマルチキャスト グループが双方向モードで動作することを指定します。このオプションを指定しない場合、グループは PIM sparse モードで動作します。
- できるだけ双方向モードを使用してください。スケーラビリティがより適切になります。

次に、PIM VRF RP アドレスを指定する例を示します。

```
Router(config)# ip pim vrf blue rp-address 198.196.100.33
```

PIM VRF 登録メッセージ送信元アドレスの設定（任意）

PIM VRF 登録メッセージ送信元アドレスを設定するには、次の作業を行います。

コマンド	目的
`Router(config)# ip pim vrf vrf_name register-source interface_type interface_number`	（任意）PIM VRF 登録メッセージ送信元アドレスを設定します。登録メッセージの送信元としてループバック インターフェイスを設定できます。

次に、PIM VRF 登録メッセージ送信元アドレスを設定する例を示します。

```
Router(config)# ip pim vrf blue register-source loopback 3
```

MSDP ピアの設定（任意）

Multicast Source Discovery Protocol（MSDP）ピアを設定するには、次の作業を行います。

コマンド	目的
`Router(config)# ip msdp vrf vrf_name peer {peer_name | peer_address} [connect-source interface_type interface_number] [remote-as ASN]`	（任意）MSDP ピアを設定します。

MSDP ピアの設定時には、次の情報に注意してください。

- **vrf** *vrf_name*：使用する特定 VRF インスタンスを指定します。
- {*peer_name* | *peer_address*}：MSDP ピア ルータのドメイン ネーム システム（DNS）名または IP アドレス。
- **connect-source** *interface_type interface_number*：プライマリ アドレスが TCP 接続の送信元 IP アドレスとして使用されるインターフェイスのインターフェイス名および番号。
- **remote-as** *ASN*：（任意）MSDP ピアの自律システム番号。これは表示専用です。

次に、MSDP ピアを設定する例を示します。

```
Router(config)# ip msdp peer router.cisco.com connect-source gigabitethernet 1/1 remote-as
109
```

マルチキャスト ルートの最大数の設定（任意）

マルチキャスト ルートの最大数を設定するには、次の作業を行います。

コマンド	目的
`Router(config)# ip multicast vrf vrf_name route-limit limit [threshold]`	（任意）マルチキャスト トラフィックに追加できるマルチキャスト ルートの最大数を設定します。

ルートの最大数の設定時には、次の情報に注意してください。

- **vrf** *vrf_name*：指定した VRF のルート制限をイネーブルにします。
- *limit*：追加できるマルチキャスト ルートの数。範囲は 1 ～ 2147483647 であり、デフォルトは 2147483647 です。
- *threshold*：（任意）警告メッセージが発生する前に追加できるマルチキャスト ルートの数。有効範囲は、1 から *limit* パラメータの値までです。

次に、マルチキャスト ルートの最大数を設定する例を示します。

```
Router(config)# ip multicast vrf blue route-limit 200000 20000
```

IPv4 マルチキャスト ルート フィルタリングの設定（任意）

IPv4 マルチキャスト ルート 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
`Router(config)# ip multicast mrinfo-filter access_list`	（任意）アクセス リストで IPv4 マルチキャスト ルート フィルタリングを設定します。*access_list* パラメータは、アクセス リストの名前または番号にすることができます。

次に、IPv4 マルチキャスト ルート フィルタリングを設定する例を示します。

```
Router(config)# ip multicast mrinfo-filter 101
```

設定例

次のコンフィギュレーション ファイルからの抜粋は、VRF の範囲でマルチキャスト ルーティングをサポートするために必要となる最低限の設定を示しています。表示を簡素にするため、先頭の VRF および末尾の VRF だけを示します。

```
!
ip multicast-routing
ip multicast-routing vrf lite
ip multicast-routing vrf vpn201
ip multicast-routing vrf vpn202

...

ip multicast-routing vrf vpn249
ip multicast-routing vrf vpn250


...

ip pim rp-address 192.0.1.1
ip pim vrf lite rp-address 104.1.1.2
ip pim vrf vpn201 rp-address 192.200.1.1
ip pim vrf vpn202 rp-address 192.200.2.1

...

ip pim vrf vpn249 rp-address 192.200.49.6
ip pim vrf vpn250 rp-address 192.200.50.6
...
```

IPv4 マルチキャスト VRF ルーティング情報の表示

特定 mVRF の既知の PIM ネイバーを表示するには、**show ip pim vrf neighbor** コマンドを使用します。

```
Router# show ip pim vrf 98 neighbor

PIM Neighbor Table
Neighbor          Interface                Uptime/Expires    Ver   DR
Address                                                            Prio/Mode
40.60.0.11        Tunnel96                 00:00:31/00:01:13 v2    1 / S
40.50.0.11        Tunnel96                 00:00:54/00:00:50 v2    1 / S

Router#
```

mVPN をサポートするマルチキャスト ルーティング用インターフェイスの設定

マルチキャスト ルーティング設定の概要

IPv4 マルチキャスト トラフィック用に使用されているすべてのインターフェイスでは、Protocol Independent Multicast（PIM）を設定する必要があります。VPN マルチキャスト環境では、最低でも次のインターフェイスのすべてで PIM をイネーブルにする必要があります。

- バックボーンに接続されているプロバイダー エッジ（PE）ルータの物理インターフェイス
- BGP ピアリングに使用されているループバック インターフェイス
- sparse PIM ランデブー ポイント（RP）ルータ アドレスの送信元として使用されているループバック インターフェイス

マルチキャスト トラフィックを転送する予定のインターフェイスと mVRF を関連付ける必要もあります。

マルチキャスト トラフィックの送受信を行うすべてのルータでは、BGP を設定して動作させる必要があります。BGP 拡張コミュニティをイネーブルにしないと（**neighbor send-community both** コマンドまたは **neighbor send-community extended** コマンドを使用）、ネットワークにおける MDT の使用がサポートされません。

インターフェイスでの PIM の設定

インターフェイスで PIM 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# 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	`Router(config)# interface` *type* {*slot/port* | *number*}	指定した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	`Router(config-if)# ip pim` {**dense-mode** | **sparse-mode** | **sparse-dense-mode**}	インターフェイスで PIM をイネーブルにします。

インターフェイスでの PIM の設定時には、次の情報に注意してください。

- 次のうちいずれかのインターフェイス タイプを使用できます。
  - バックボーンに接続されているプロバイダー エッジ（PE）ルータの物理インターフェイス
  - BGP ピアリングに使用されているループバック インターフェイス
  - スパース PIM ネットワーク RP アドレスの送信元として使用されるループバック インターフェイス
- PIM モードは次のとおりです。
  - **dense-mode**：動作の dense モードをイネーブルにします。
  - **sparse-mode**：動作の sparse モードをイネーブルにします。
  - **sparse-dense-mode**：マルチキャスト グループで RP ルータが定義されている場合は sparse モード、RP ルータが定義されていない場合は dense モードをイネーブルにします。
- バックボーンに接続されているすべての PE ルータの物理インターフェイス、および BGP ピアリングに使用されるか RP アドレス指定の送信元として使用されるすべてのループバック インターフェイスには、**sparse-mode** を使用してください。

次に、物理インターフェイス上で PIM sparse モードを設定する例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 10/1
Router(config-if)# ip pim sparse-mode
```

次に、ループバック インターフェイス上で PIM sparse モードを設定する例を示します。

```
Router# configure terminal
Router(config)# interface loopback 2
Router(config-if)# ip pim sparse-mode
```

IPv4 VRF 転送用インターフェイスの設定

IPv4 VRF 転送用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
`Router(config-if)# ip vrf forwarding vrf_name`	（任意）指定した VRF ルーティング テーブルおよび転送テーブルをインターフェイスと関連付けます。指定しない場合、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 テーブルの使用になります。 **（注）** インターフェイスでこのコマンドを入力すると、IP アドレスが削除されるので、IP アドレスを再設定してください。

次に、VRF blue 転送用インターフェイスを設定する例を示します。

```
Router(config-if)# ip vrf forwarding blue
```

設定例

次のコンフィギュレーション ファイルからの抜粋は、単一 mVRF 上でマルチキャスト トラフィックをイネーブルにするインターフェイス設定、および関連 mVRF 設定を示しています。

```
ip multicast-routing vrf blue
ip multicast-routing

ip vrf blue
 rd 100:27
 route-target export 100:27
 route-target import 100:27
 mdt default 239.192.10.2

interface GigabitEthernet1/1
 description blue connection
 ip vrf forwarding blue
 ip address 192.168.2.26 255.255.255.0
 ip pim sparse-mode

interface GigabitEthernet1/15
 description Backbone connection
 ip address 10.8.4.2 255.255.255.0
 ip pim sparse-mode

ip pim vrf blue rp-address 192.7.25.1
ip pim rp-address 10.1.1.1
```

mVPN with L3VPN over mGRE の設定

- 「L3VPN カプセル化プロファイルの設定」（P.49-23）（必須）
- 「BGP およびルート マップの設定」（P.49-24）（必須）

（注）　詳細については、「mVPN with L3VPN over mGRE について」（P.49-9）を参照してください。

L3VPN カプセル化プロファイルの設定

（注）　この設定では、IPv6、MPLS、IP、およびレイヤ 2 トンネル プロトコル バージョン 3（L2TPv3）のような転送プロトコルも使用できます。

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** **例：** `Router# 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	**l3vpn encapsulation ip** *profile-name* **例：** `Router(config)# l3vpn encapsulation ip tunnel encap`	L3 VPN カプセル化コンフィギュレーション モードを開始し、トンネルを作成します。
ステップ 4	**transport ipv4 [source** *interface-type interface-number***]** **例：** `Router(config-l3vpn-encap-ip)# transport ipv4 source loopback 0`	（任意）IPv4 送信元モードを指定して、送信元インターフェイスを定義します。 • **transport ipv4 source** *interface-type interface-number* コマンドを使用する場合、指定した送信元アドレスが、PE によってアドバタイズされた BGP アップデートにおけるネクスト ホップとして使用されていることを確認します。 • このコマンドを使用しない場合、**bgp update source** または **bgp next-hop** コマンドが、トンネル送信元として自動的に使用されます。
ステップ 5	**protocol gre [key** *gre-key***]** **例：** `Router(config-l3vpn-encap-ip)# protocol gre key 1234`	GRE をトンネル モードとして指定し、GRE キーを設定します。

	コマンドまたはアクション	目的
ステップ 6	**end** **例：** `Router(config-l3vpn-encap-ip)# end`	L3 VPN カプセル化コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 7	**show l3vpn encapsulation ip** *profile-name* **例：** `Router# show l3vpn encapsulation ip tunnel encap`	（任意）プロファイルの状態および基本となるトンネル インターフェイスを表示します。

BGP およびルート マップの設定

BGP およびルート マップを設定するには、次の作業を実行します。次の手順では、ルート マップをアプリケーション テンプレートにリンクし、アップデートがルート マップを介してフィルタ処理されるように BGP VPNv4 と VPNv6 の交換を設定することも可能です。

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** **例：** `Router# 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	**router bgp** *as-number* **例：** `Router(config)# router bgp 100`	他の BGP ルータに接続されたルータを特定する自律システムの番号を指定し、転送されるルーティング情報にタグ付けし、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 4	**bgp log-neighbor-changes** **例：** `Router(config-router)# bgp log-neighbor-changes`	BGP ネイバー リセットのロギングをイネーブルにします。
ステップ 5	**neighbor** *ip-address* **remote-as** *as-number* **例：** `Router(config-router)# neighbor 209.165.200.225 remote-as 100`	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。
ステップ 6	**neighbor** *ip-address* **update-source** *interface name* **例：** `Router(config-router)# neighbor 209.165.200.225 update-source loopback 0`	BGP セッションが、TCP 接続の動作インターフェイスを使用できるようにします。

	コマンドまたはアクション	目的
ステップ 7	**address-family ipv4** **例：** `Router(config-router)# address-family ipv4`	アドレス ファミリ コンフィギュレーション モードを開始し、IPv4 アドレス プレフィックスを使用するルーティング セッションを設定します。
ステップ 8	**no synchronization** **例：** `Router(config-router-af)# no synchronization`	IGP を待たずにネットワーク ルートをアドバタイズするよう、Cisco IOS ソフトウェアをイネーブルにします。
ステップ 9	**redistribute connected** **例：** `Router(config-router-af)# redistribute connected`	1 つのルーティング ドメインから別のルーティング ドメインにルートを再配布し、送信元プロトコルによって認識されたルート、および、送信元プロトコルが実行されているインターフェイスを介して接続されているプレフィックスを、ターゲット プロトコルで再配布できるようにします。
ステップ 10	**neighbor** *ip-address* **activate** **例：** `Router(config-router-af)# neighbor 209.165.200.225 activate`	BGP ネイバーとの情報交換をイネーブルにします。
ステップ 11	**no auto-summary** **例：** `Router(config-router-af)# no auto-summary`	自動サマライズをディセーブルにし、サブプレフィックス ルーティング情報をクラスフル ネットワーク境界間で送信します。
ステップ 12	**exit** **例：** `Router(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了します。
ステップ 13	**address-family vpnv4** **例：** `Router(config-router)# address-family vpnv4`	アドレス ファミリ コンフィギュレーション モードを開始して、標準 VPNv4 アドレス プレフィックスを使用する、BGP などのルーティング セッションを設定します。
ステップ 14	**neighbor** *ip-address* **activate** **例：** `Router(config-router-af)# neighbor 209.165.200.225 activate`	BGP ネイバーとの情報交換をイネーブルにします。
ステップ 15	**neighbor** *ip-address* **send-community both** **例：** `Router(config-router-af)# neighbor 209.165.200.225 send-community both`	標準コミュニティと拡張コミュニティの両方のコミュニティ属性が、BGP ネイバーに送信されるように指定します。
ステップ 16	**neighbor** *ip-address* **route-map** *map-name* **in** **例：** `Router(config-router-af)# neighbor 209.165.200.225 route-map SELECT_UPDATE_FOR_L3VPN in`	名前付きルート マップを受信ルートに適用します。

	コマンドまたはアクション	目的
ステップ 17	**exit** **例：** `Router(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了します。
ステップ 18	**address-family vpnv6** **例：** `Router(config-router)# address-family vpnv6`	アドレス ファミリ コンフィギュレーション モードを開始して、VPNv6 アドレス プレフィックスを使用する、BGP などのルーティング セッションを設定します。
ステップ 19	**neighbor** *ip-address* **activate** **例：** `Router(config-router-af)# neighbor 209.165.200.252 activate`	BGP ネイバーとの情報交換をイネーブルにします。
ステップ 20	**neighbor** *ip-address* **send-community both** **例：** `Router(config-router-af)# neighbor 209.165.200.252 send-community both`	標準コミュニティと拡張コミュニティの両方のコミュニティ属性が、BGP ネイバーに送信されるように指定します。
ステップ 21	**neighbor** *ip-address* **route-map** *map-name* **in** **例：** `Router(config-router-af)# neighbor 209.165.200.252 route-map SELECT_UPDATE_FOR_L3VPN in`	名前付きルート マップを受信ルートに適用します。
ステップ 22	**exit** **例：** `Router(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了します。
ステップ 23	**route-map** *map-tag* **permit** *position* **例：** `Router(config-router)# route-map SELECT_UPDATE_FOR_L3VPN permit 10`	ルート マップ コンフィギュレーション モードを開始し、1 つのルーティング プロトコルから別のルーティング プロトコルへルートを再配布する条件を定義します。 • **redistribute** ルータ コンフィギュレーション コマンドによって、指定されたマップ タグが使用され、このルート マップが参照されます。複数のルート マップで同じマップ タグ名を共有できます。 • このルート マップの一致基準が満たされている場合は、set アクションの制御に従ってルートが再配布されます。 • 一致基準が満たされないと、同じマップ タグを持つ次のルート マップが検査されます。あるルートが、同じ名前を共有するルート マップ セットの一致基準のいずれをも満たさない場合、そのセットによる再配布は行われません。 • *position* 引数は、同じ名前で設定済みのルート マップのリストに新しいルート マップが入る位置を示します。

	コマンドまたはアクション	目的
ステップ 24	**set ip next-hop encapsulate l3vpn** *profile-name* **例：** `Router(config-route-map)# set ip next-hop encapsulate l3vpn my profile`	ルート マップの match 句を渡す出力 IPv4 パケットは、トンネルのカプセル化のため、VRF に送信されます。
ステップ 25	**set ipv6 next-hop encapsulate l3vpn** *profile-name* **例：** `Router(config-route-map)# set ip next-hop encapsulate l3vpn tunnel encap`	ルート マップの match 句を渡す出力 IPv6 パケットは、トンネルのカプセル化のため、VRF に送信されます。
ステップ 26	**exit** **例：** `Router(config-route-map)# exit`	ルート マップ コンフィギュレーション モードを終了し、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 27	**exit** **例：** `Router(config)# 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。

mVPN の設定例

デフォルト MDT だけの mVPN 設定

次のコンフィギュレーション ファイルからの抜粋は、3 つの mVRF の mVPN 設定に関連する行を示しています。（必須 BGP 設定は表示されていません）。

```
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service compress-config
!
hostname MVPN Router
!
boot system flash slot0:
logging snmp-authfail
!
ip subnet-zero
!
no ip domain-lookup
ip host tftp 223.255.254.238
!
ip vrf mvpn-cus1
```

```
 rd 200:1
 route-target export 200:1
 route-target import 200:1
 mdt default 239.1.1.1
!
ip vrf mvpn-cus2
 rd 200:2
 route-target export 200:2
 route-target import 200:2
 mdt default 239.1.1.2
!
ip vrf mvpn-cus3
 rd 200:3
 route-target export 200:3
 route-target import 200:3
 mdt default 239.1.1.3
!
ip multicast-routing
ip multicast-routing vrf mvpn-cus1
ip multicast-routing vrf mvpn-cus2
ip multicast-routing vrf mvpn-cus3
ip multicast multipath
frame-relay switching
mpls label range 4112 262143
mpls label protocol ldp
mpls ldp logging neighbor-changes
mpls ldp explicit-null
mpls traffic-eng tunnels
mpls tdp discovery directed-hello accept from 1
mpls tdp router-id Loopback0 force
platform flow ip destination
no platform flow ipv6
platform rate-limit unicast cef glean 10 10
platform qos
platform cef error action freeze

...

vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
vlan 2001-2101,3501-3700,4001,4051-4080,4093
!
!
!
interface Loopback0
 ip address 201.252.1.14 255.255.255.255
 ip pim sparse-dense-mode
!
interface Loopback1
 ip address 209.255.255.14 255.255.255.255
!
interface Loopback10
 ip vrf forwarding mvpn-cus1
 ip address 210.101.255.14 255.255.255.255
!
interface Loopback11
 ip vrf forwarding mvpn-cus1
 ip address 210.111.255.14 255.255.255.255
 ip pim sparse-dense-mode
!
interface Loopback12
 ip vrf forwarding mvpn-cus1
 ip address 210.112.255.14 255.255.255.255
```

```
...

!
interface GigabitEthernet3/3
 mtu 9216
 ip vrf forwarding mvpn-cus3
 ip address 172.10.14.1 255.255.255.0
 ip pim sparse-dense-mode
!

...

!
interface GigabitEthernet3/19
 ip vrf forwarding mvpn-cus2
 ip address 192.16.4.1 255.255.255.0
 ip pim sparse-dense-mode
 ip igmp static-group 229.1.1.1
 ip igmp static-group 229.1.1.2
 ip igmp static-group 229.1.1.4
!
interface GigabitEthernet3/20
 ip vrf forwarding mvpn-cus1
 ip address 192.16.1.1 255.255.255.0
 ip pim sparse-dense-mode
!
...
```

デフォルト MDT およびデータ MDT を含む mVPN 設定

次の設定例には、デフォルト MDT とデータ MDT の両方で設定された 3 つの mVRF が含まれています。mVPN 設定に関連する設定だけを表示しています。

```
...
!
ip vrf v1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 mdt default 226.1.1.1
 mdt data 226.1.1.128 0.0.0.7 threshold 1
!
ip vrf v2
 rd 2:2
 route-target export 2:2
 route-target import 2:2
 mdt default 226.2.2.1
 mdt data 226.2.2.128 0.0.0.7
!
ip vrf v3
 rd 3:3
 route-target export 3:3
 route-target import 3:3
 mdt default 226.3.3.1
 mdt data 226.3.3.128 0.0.0.7
!
ip vrf v4
 rd 155.255.255.1:4
 route-target export 155.255.255.1:4
 route-target import 155.255.255.1:4
 mdt default 226.4.4.1
```

```
 mdt data 226.4.4.128 0.0.0.7
!
ip multicast-routing
ip multicast-routing vrf v1
ip multicast-routing vrf v2
ip multicast-routing vrf v3
ip multicast-routing vrf v4
mpls label protocol ldp
mpls ldp logging neighbor-changes
mpls tdp router-id Loopback1
platform ip multicast replication-mode ingress
platform ip multicast bidir gm-scan-interval 10
no platform flow ip
no platform flow ipv6
platform cef error action freeze
!

...

vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
!
interface Loopback1
 ip address 155.255.255.1 255.255.255.255
 ip pim sparse-mode
!
interface Loopback11
 ip vrf forwarding v1
 ip address 155.255.255.11 255.255.255.255
 ip pim sparse-dense-mode
!
interface Loopback22
 ip vrf forwarding v2
 ip address 155.255.255.22 255.255.255.255
 ip pim sparse-mode
!
interface Loopback33
 ip vrf forwarding v3
 ip address 155.255.255.33 255.255.255.255
 ip pim sparse-mode
!
interface Loopback44
 ip vrf forwarding v4
 ip address 155.255.4.4 255.255.255.255
 ip pim sparse-mode
!
interface Loopback111
 ip vrf forwarding v1
 ip address 1.1.1.1 255.255.255.252
 ip pim sparse-dense-mode
 ip ospf network point-to-point
!
interface GigabitEthernet1/1
 description Gi1/1 - 155.50.1.155 255.255.255.0 - peer dut50 - mpls
 mtu 9216
 ip address 155.50.1.155 255.255.255.0
 ip pim sparse-mode
 mpls ip
!
interface GigabitEthernet1/2
 ip vrf forwarding v1
 ip address 155.1.2.254 255.255.255.0
 ip pim sparse-mode
```

```
!
interface GigabitEthernet1/3
 description Gi1/3 - 185.155.1.155/24 - vrf v1 stub peer 185.Gi1/3
 ip vrf forwarding v1
 ip address 185.155.1.155 255.255.255.0
 ip pim sparse-mode
!

...

!
interface GigabitEthernet1/48
 ip vrf forwarding v1
 ip address 157.155.1.155 255.255.255.0
 ip pim bsr-border
 ip pim sparse-dense-mode
!
interface GigabitEthernet6/1
 no ip address
 shutdown
!
interface GigabitEthernet6/2
 ip address 9.1.10.155 255.255.255.0
 media-type rj45
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 11 vrf v1
 router-id 155.255.255.11
 log-adjacency-changes
 redistribute connected subnets tag 155
 redistribute bgp 1 subnets tag 155
 network 1.1.1.0 0.0.0.3 area 155
 network 155.255.255.11 0.0.0.0 area 155
 network 155.0.0.0 0.255.255.255 area 155
 network 157.155.1.0 0.0.0.255 area 0
!
router ospf 22 vrf v2
 router-id 155.255.255.22
 log-adjacency-changes
 network 155.255.255.22 0.0.0.0 area 155
 network 155.0.0.0 0.255.255.255 area 155
 network 157.155.1.0 0.0.0.255 area 0
!
router ospf 33 vrf v3
 router-id 155.255.255.33
 log-adjacency-changes
 network 155.255.255.33 0.0.0.0 area 155
!
router ospf 1
 log-adjacency-changes
 network 155.50.1.0 0.0.0.255 area 0
 network 155.255.255.1 0.0.0.0 area 155
!
router bgp 1
 bgp router-id 155.255.255.1
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 175.255.255.1 remote-as 1
 neighbor 175.255.255.1 update-source Loopback1
 neighbor 185.255.255.1 remote-as 1
 neighbor 185.255.255.1 update-source Loopback1
```

```
 !
 address-family vpnv4
 neighbor 175.255.255.1 activate
 neighbor 175.255.255.1 send-community extended
 neighbor 185.255.255.1 activate
 neighbor 185.255.255.1 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf v4
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf v3
 redistribute ospf 33
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf v2
 redistribute ospf 22
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf v1
 redistribute ospf 11
 no auto-summary
 no synchronization
 exit-address-family
!
ip classless
ip route 9.255.254.1 255.255.255.255 9.1.10.254
no ip http server
ip pim bidir-enable
ip pim rp-address 50.255.2.2 MCAST.MVPN.MDT.v2 override bidir
ip pim rp-address 50.255.3.3 MCAST.MVPN.MDT.v3 override bidir
ip pim rp-address 50.255.1.1 MCAST.MVPN.MDT.v1 override bidir
ip pim vrf v1 spt-threshold infinity
ip pim vrf v1 send-rp-announce Loopback11 scope 16 group-list MCAST.GROUP.BIDIR bidir
ip pim vrf v1 send-rp-discovery Loopback11 scope 16
ip pim vrf v1 bsr-candidate Loopback111 0
ip msdp vrf v1 peer 185.255.255.11 connect-source Loopback11
ip msdp vrf v1 cache-sa-state
!
!
ip access-list standard MCAST.ANYCAST.CE
 permit 2.2.2.2
ip access-list standard MCAST.ANYCAST.PE
 permit 1.1.1.1
ip access-list standard MCAST.BOUNDARY.VRF.v1
 deny   226.192.1.1
 permit any
ip access-list standard MCAST.GROUP.BIDIR
 permit 226.192.0.0 0.0.255.255
ip access-list standard MCAST.GROUP.SPARSE
 permit 226.193.0.0 0.0.255.255
ip access-list standard MCAST.MVPN.BOUNDARY.DATA.MDT
 deny   226.1.1.128
 permit any
ip access-list standard MCAST.MVPN.MDT.v1
 permit 226.1.0.0 0.0.255.255
ip access-list standard MCAST.MVPN.MDT.v2
 permit 226.2.0.0 0.0.255.255
```

```
ip access-list standard MCAST.MVPN.MDT.v3
 permit 226.3.0.0 0.0.255.255
ip access-list standard MCAST.MVPN.RP.v4
 permit 227.0.0.0 0.255.255.255
!
access-list 1 permit 226.1.1.1
access-list 2 deny   226.1.1.1
access-list 2 permit any
...
```

mVPN with L3VPN over mGRE 設定の確認

設定が正しく動作していることを確認する例を次に示します。

エンドポイントの作成

トンネルのエンドポイントが作成されているかどうかを確認します。

```
Router# show tunnel endpoints tunnel 0

 Tunnel0 running in multi-GRE/IP mode

 Endpoint transport 209.165.200.251 Refcount 3 Base 0x2AE93F0 Create Time 00:00:42
   overlay 209.165.200.254 Refcount 2 Parent 0x2AE93F0 Create Time 00:00:42
```

隣接

対応する隣接が作成されているかどうかを確認します。

```
Router# show adjacency tunnel 0

   Protocol Interface                 Address
  IP       Tunnel0                   209.165.200.251(4)
  TAG      Tunnel0                   209.165.200.251(3)
```

プロファイルの状態

show l3vpn encapsulation *profile-name* コマンドを使用して、アプリケーションの基本的な状態に関する情報を取得できます。このコマンドの出力には、基本となるトンネルの詳細が表示されます。

```
Router# show l3vpn encapsulation ip tunnel encap

    Profile: tunnel encap
    transport ipv4 source Auto: Loopback0
    protocol gre
    Tunnel Tunnel0 Created [OK]
    Tunnel Linestate [OK]
    Tunnel Transport Source (Auto) Loopback0 [OK]
```

mVPN with L3VPN over mGRE の設定シーケンス

次に、mVPN with L3VPN over mGRE の設定シーケンスの例を示します。

```
vrf definition Customer A
 rd 100:110
 route-target export 100:1000
 route-target import 100:1000
 !
address-family ipv4
 exit-address-family
```

```
 !
address-family ipv6
 exit-address-family
!
!
ipv6 unicast-routing
!
l3vpn encapsulation ip sample_profile_name
 transport ipv4 source loopback 0
!
!
interface Loopback0
  ip address 209.165.200.252 255.255.255.224
  ip router isis
!
interface gigabitethernet 1/1
 vrf forwarding Customer A
 ip address 209.165.200.253 255.255.255.224
 ipv6 address 3FFE:1001::/64 eui-64
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 209.165.200.254 remote-as 100
 neighbor 209.165.200.254 update-source Loopback0
 !
address-family ipv4
  no synchronization
  redistribute connected
  neighbor 209.165.200.254 activate
  no auto-summary
 exit-address-family
 !
address-family vpnv4
  neighbor 209.165.200.254 activate
  neighbor 209.165.200.254 send-community both
  neighbor 209.165.200.254 route-map SELECT_UPDATE_FOR_L3VPN in
 exit-address-family
 !
address-family vpnv6
  neighbor 209.165.200.254 activate
  neighbor 209.165.200.254 send-community both
  neighbor 209.165.200.254 route-map SELECT_UPDATE_FOR_L3VPN in
 exit-address-family
 !
address-family ipv4 vrf Customer A
  no synchronization
  redistribute connected
 exit-address-family
 !
address-family ipv6 vrf Customer A
  redistribute connected
  no synchronization
 exit-address-family
!
!
route-map SELECT_UPDATE_FOR_L3VPN permit 10
set ip next-hop encapsulate sample_profile_name
set ipv6 next-hop encapsulate sample_profile_name
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

IPv6 マルチキャストのサポート

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

IPv6 マルチキャストの前提条件

なし。

IPv6 マルチキャストの制約事項

- PFC および DFC では、以下がハードウェアでサポートされます。
  - 完全にスイッチングされた IPv6 マルチキャスト フロー
  - IPv6 PIM スパース モード（PIM-SM）（S,G）および（*,G）転送
  - NetFlow テーブルを使用した IPv6 PIM-SM（S,G）トラフィックのマルチキャスト RPF 確認
  - マルチキャスト RPF チェックでエラーになった IPv6 PIM-SM（S,G）トラフィックのレート制限
  - スタティック IPv6 マルチキャスト ルート
  - IPv6 の SSM Mapping（PIM-SSM）
  - NetFlow テーブルを使用した IPv6 マルチキャスト転送情報ベース（MFIB）
  - NetFlow テーブルを使用した IPv6 Distributed MFIB（dMFIB）
  - リンクローカルおよびリンクグローバル IPv6 マルチキャスト スコープ

  - ipv6 mfib hardware-switching コマンドを使用した出力マルチキャスト複製
  - マルチキャスト ルートの入力インターフェイス統計（出力インターフェイス統計は使用不可）
  - RPR および RPR+ 冗長モード（第 9 章「Route Processor Redundancy（RPR）」を参照）
  - 入力および出力 PFC QoS（第 61 章「PFC QoS の概要」を参照）
  - 入力および出力の Cisco アクセス コントロール リスト（ACL）
- PFC および DFC では、以下がハードウェアでサポートされません。
  - 部分的にスイッチングされた IPv6 マルチキャスト フロー
  - PIM-SM（*,G）トラフィックのマルチキャスト RPF チェック
  - マルチキャスト ヘルパー マップ
  - サイトローカル マルチキャスト スコープ
  - IPv4 トンネル上で手動設定した IPv6
  - IPv6 マルチキャスト 6to4 トンネル
  - IPv6 マルチキャスト自動トンネル
  - GRE トンネル上の IPv6
  - IPv6-in-IPv6 PIM レジスタ トンネル
  - IPv6 マルチキャスト基本 ISATAP トンネル
  - 6to4 トンネルを組み込んだ ISATAP トンネル

IPv6 マルチキャスト サポートについて

ハードウェアでサポートされている IPv6 レイヤ 3 マルチキャスト機能

- コントロール プレーン ポリシング（CoPP）
- 出力強制レプリケーション モード
- 出力レプリケーション ローカル
- 出力レプリケーション モード
- HW アシストされた SPT スイッチオーバー
- 入力 ACL ロギング
- 入出力 ACL フィルタリング
- P2P IPv4 GRE/IP-in-IP トンネル上の IPv6 マルチキャスト（6over4）
- ポートチャネルでのマルチキャスト パケットのロードバランシング
- ルーテッド ポートでのマルチキャスト レイヤ 3 フォワーディング
- サブインターフェイスでのマルチキャスト レイヤ 3 フォワーディング

- SVI でのマルチキャスト レイヤ 3 フォワーディング
- パラレル リンク間のマルチキャスト ロード分割
- NetFlow アカウンティング
- Non-RPF 保護
- IPv6 を介した PIM Register カプセル開放
- IPv6 を介した PIM Register カプセル化
- PIM-SM（S,G）および（*,G）転送
- PIM-SSM
- QoS 入力モード マーキング
- QoS 入力モード ポリシング
- レート リミッタ
- スコープ チェック
- 統計情報

ハードウェアで部分的にサポートされている IPv6 レイヤ 3 マルチキャスト機能

- 出力レプリケーション モードおよび QoS マーキング

ソフトウェアでサポートされている IPv6 レイヤ 3 マルチキャスト機能

- SSM マッピング
- MET 共有
- MLDv1/v2

サポートされていない IPv6 レイヤ 3 マルチキャスト機能

- P2P GRE トンネルを介した BIDIR PIM
- 宛先 IP NAT マルチキャスト
- P2P IPv6 GRE トンネル上の IPv4 マルチキャスト（4over6）
- マルチポイント IPv4 GRE トンネル上の IPv6 マルチキャスト（6over4 mGRE）
- マルチポイント IPv6 GRE トンネル上の IPv6 マルチキャスト
- P2P IPv6 GRE トンネル上の IPv6 マルチキャスト
- VRF での P2P IPv6 GRE トンネル上の IPv6 マルチキャストおよびトンネル エンドポイント
- P2P IPv6 VRF GRE トンネル上の IPv6 マルチキャスト
- MTR マルチキャスト：ToS ベースの参照
- IPv6 エクストラネットをサポートするマルチキャスト VPN
- IPv6 イントラネットをサポートするマルチキャスト VPN

- マルチキャスト VRF-lite
- P2P IPv6 GRE トンネル上の MVPN
- PIM-BIDIR
- PIM-DM（S,G）転送
- 送信元 IP NAT マルチキャスト
- 出力レプリケーション モードおよび QoS ポリシング
- QoS 入力および出力：シェーピング サポート
- MIB のサポート
- マルチキャスト境界
- マルチキャスト ヘルパー マップ
- 出力 ACL ロギング
- PGM ルータ アシスト
- VRF での PGM ルータ アシスト
- ルーティング中のマルチキャスト ブリッジされたフレームの QoS マーキング

IPv6 マルチキャスト サポートの設定方法

PFC および DFC では、IPv6 マルチキャスト トラフィックがハードウェアでサポートされます。Cisco IOS Release 15.1SY で IPv6 マルチキャストを設定する場合、次のマニュアルを使用してください。

- 『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Multicast」
  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-0sy/ipv6-15-0sy-book.html
- 『*Cisco IOS IPv6 Command Reference*』
  http://www.cisco.com/en/US/docs/ios/ipv6/command/reference/ipv6_book.html

IPv6 マルチキャスト レイヤ 3 設定の確認

- 「FIB ハードウェア ブリッジングおよび廃棄カウントの表示」（P.50-7）
- 「共有および well-known ハードウェア隣接カウンタの表示」（P.50-8）

MFIB クライアントの確認

次に、**show ipv6 mrib client** コマンドの完全な出力例を示します。

```
Router# show ipv6 mrib client
```

スイッチング機能の表示

次に、**show platform software ipv6-multicast capability** コマンドの完全な出力例を示します。

```
Router# show platform software ipv6-multicast capability
```

（S,G）転送機能の確認

次に、（S,G）転送を確認する例を示します。

```
Router# show platform software ipv6-multicast capability | include (S,G)
 (S,G) forwarding for IPv6 supported using Netflow
```

（*,G）転送機能の確認

次に、（*,G）転送を確認する例を示します。

```
Router# show platform software ipv6-multicast capability | include (\*,G)
 (*,G) bridging for IPv6 is supported using FIB
```

サブネット エントリ サポート ステータスの確認

次に、サブネット エントリ サポート ステータスを確認する例を示します。

```
Router# show platform software ipv6-multicast capability | include entries
 Directly-connected entries for IPv6 is supported using ACL-TCAM.
```

現行レプリケーション モードの確認

次に、現行レプリケーション モードを確認する例を示します。

```
Router# show platform software ipv6-multicast capability | include Current
Current System HW Replication Mode : Ingress
```

（注）　レプリケーション モード自動検出をイネーブルにするには、**no ipv6 mfib hardware-switching replication-mode ingress** を入力します。

レプリケーション モード自動検出ステータスの表示

次に、レプリケーション モード自動検出ステータスを表示する例を示します。

```
Router# show platform software ipv6-multicast capability | include detection
Auto-detection of Replication Mode : ON
```

レプリケーション モード機能の表示

次に、インストールされているモジュールのレプリケーション モード機能を表示する例を示します。

```
Router# show platform software ipv6-multicast capability | begin ^Slot
Slot Replication-Capability Replication-Mode
   1 Ingress                Ingress
   2 Egress                 Ingress
   6 Egress                 Ingress
   8 Ingress                Ingress
```

サブネット エントリの表示

次に、サブネット エントリを表示する例を示します。

```
Router# show platform software ipv6-multicast connected
IPv6 Multicast Subnet entries
Flags : H - Installed in ACL-TCAM
        X - Not installed in ACL-TCAM due to
            label-full exception
Interface: Vlan20 [ H ]
         S:20::1 G:FF00::
Interface: Vlan10 [ H ]
         S:10::1 G:FF00::
```

（注） この例では、VLAN 10 および VLAN 20 にサブネット エントリがあります。

IPv6 マルチキャスト概要の表示

次に、IPv6 マルチキャスト概要を表示する例を示します。

```
Router# show platform software ipv6-multicast summary
IPv6 Multicast Netflow SC summary on Slot[1]:
Shortcut Type               Shortcut count
----------------------------+--------------
(S, G)                      100
(*, G)                      0
IPv6 Multicast FIB SC summary on Slot[1]:
Shortcut Type               Shortcut count
----------------------------+--------------
(*, G/128)                  10
(*, G/m)                    47

IPv6 Multicast Netflow SC summary on Slot[6]:
Shortcut Type               Shortcut count
----------------------------+--------------
(S, G)                      100
(*, G)                      0
IPv6 Multicast FIB SC summary on Slot[6]:
```

```
Shortcut Type               Shortcut count
--------------------------+--------------
(*, G/128)                  10
(*, G/m)                    47
```

NetFlow ハードウェア転送カウントの表示

次に、NetFlow ハードウェア転送カウントを表示する例を示します。

```
Router# show platform software ipv6-multicast summary
IPv6 Multicast Netflow SC summary on Slot[1]:
Shortcut Type               Shortcut count
--------------------------+--------------
(S, G)                      100
(*, G)                      0

<...Output deleted...>

IPv6 Multicast Netflow SC summary on Slot[6]:
Shortcut Type               Shortcut count
--------------------------+--------------
(S, G)                      100
(*, G)                      0
<...Output truncated...>
```

（注） PIM-SM（*,G）の転送が RP のソフトウェアでサポートされているため、NetFlow（*, G）のカウントは常にゼロです。

FIB ハードウェア ブリッジングおよび廃棄カウントの表示

次に、FIB ハードウェア ブリッジング カウントおよび廃棄ハードウェア カウントを表示する例を示します。

```
Router# show platform software ipv6-multicast summary | begin FIB
IPv6 Multicast FIB SC summary on Slot[1]:
Shortcut Type               Shortcut count
--------------------------+--------------
(*, G/128)                  10
(*, G/m)                    47

<...Output deleted...>

IPv6 Multicast FIB SC summary on Slot[6]:
Shortcut Type               Shortcut count
--------------------------+--------------
(*, G/128)                  10
(*, G/m)                    47
```

（注）

- （*,G/128）の値は、ハードウェア ブリッジ エントリ カウントです。
- （*,G/m）の値は、ハードウェア ブリッジ/廃棄エントリ カウントです。

共有および well-known ハードウェア隣接カウンタの表示

show platform software ipv6-multicast shared-adjacencies コマンドでは、FIB および ACL-TCAM のエントリによって IPv6 マルチキャストに使用される、共有および well-known のハードウェア隣接カウンタが表示されます。

```
Router# show platform software ipv6-multicast shared-adjacencies

---- SLOT [1] ----

Shared IPv6 Mcast Adjacencies Index  Packets       Bytes
----------------------------- ------ ------------ ------------------
Subnet bridge adjacency       0x7F802  0            0
Control bridge adjacency      0x7      0            0
StarG_M bridge adjacency      0x8      0            0
S_G bridge adjacency          0x9      0            0
Default drop adjacency        0xA      0            0
StarG (spt == INF) adjacency  0xB      0            0
StarG (spt != INF) adjacency  0xC      0            0

---- SLOT [6] ----

Shared IPv6 Mcast Adjacencies Index  Packets       Bytes
----------------------------- ------ ------------ ------------------
Subnet bridge adjacency       0x7F802  0            0
Control bridge adjacency      0x7      0            0
StarG_M bridge adjacency      0x8      0            0
S_G bridge adjacency          0x9      0            0
Default drop adjacency        0xA      28237        3146058
StarG (spt == INF) adjacency  0xB      0            0
StarG (spt != INF) adjacency  0xC      0            0
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

IPv6 MLD スヌーピング

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。
- IPv4 マルチキャスト トラフィックを抑制するには、第 44 章「IPv4 マルチキャスト トラフィックの IGMP スヌーピング」を参照してください。
- すべての PFC モードで、マルチキャスト リスナー検出（MLD）バージョン 1（MLDv1）および MLD バージョン 2（MLDv2）がサポートされています。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

MLD スヌーピングの前提条件

なし。

MLD スヌーピングの制約事項

一般的な MLD スヌーピングの制約事項

- すべての PFC モードで、MLD バージョン 1（MLDv1）および MLD バージョン 2（MLDv2）がサポートされています。
- MLD は、Internet Group Management Protocol version 3（IGMPv3）から派生したものです。MLD プロトコル動作とステート移行、ホストとルータの動作、クエリーとレポート メッセージの処理、メッセージ転送ルール、タイマー動作は、IGMPv3 とまったく同じです。MLD プロトコルの詳細については、draft-vida-mld-.02.txt を参照してください。
- MLD プロトコル メッセージは、Internet Control Message Protocol version 6（ICMPv6）メッセージです。
- MLD メッセージ形式は、IGMPv3 メッセージとほぼ同一です。
- Cisco IOS ソフトウェアの IPv6 マルチキャストでは MLD バージョン 2 が使用されます。このバージョンの MLD には、MLD バージョン 1 との完全な下位互換性があります（RFC 2710 で規定）。MLD バージョン 1 だけをサポートするホストは、MLD バージョン 2 を実行しているルータと相互運用します。MLD バージョン 1 ホストおよび MLD バージョン 2 ホストの両方を含む混在 LAN はサポートされます。
- MLD スヌーピングは、プライベート VLAN をサポートします。プライベート VLAN は、MLD スヌーピングに制約を課しません。
- MLD スヌーピングは MAC マルチキャスト グループ 0100.5e00.0001 ～ 0100.5eff.ffff のトラフィックを抑制します。
- MLD 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 マルチキャストは抑制しません。

MLD スヌーピング クエリアの制約事項

- VLAN インターフェイスに IPv6 アドレスを設定してください（第 34 章「レイヤ 3 インターフェイス」を参照）。MLD スヌーピング クエリアがイネーブルの場合、IPv6 アドレスをクエリー送信元アドレスとして使用します。
- VLAN インターフェイスに IPv6 アドレスが設定されていないと、MLD スヌーピング クエリアは起動しません。MLD スヌーピング クエリアは、IPv6 アドレスが消去されるとディセーブルになります。MLD スヌーピング クエリアは、イネーブルの場合、IPv6 アドレスを設定すると再起動します。
- MLD スヌーピング クエリアをイネーブルにすると、IPv6 マルチキャスト ルータからの MLD トラフィックを検出しても起動しません。
- MLD スヌーピング クエリアをイネーブルにすると、IPv6 マルチキャスト ルータから MLD トラフィックが検出されない場合、60 秒後に起動します。
- MLD スヌーピング クエリアをイネーブルにしても、IPv6 マルチキャスト ルータからの MLD トラフィックを検出するとディセーブルになります。
- MLD スヌーピングがイネーブルの場合、QoS（Quality of Service）は MLD パケットをサポートしません。

- VLAN 内のスイッチは、MLD スヌーピング クエリアをサポートする場合はすべてで、MLD スヌーピング クエリアをイネーブルにできます。1 台のスイッチがクエリアとして選定されます。
- 冗長 MLD スヌーピング クエリアを設定するには、VLAN 上の複数のスイッチで、「MLD スヌーピング クエリアのイネーブル化」（P.51-10）のタスクを実行します。

  複数の MLD スヌーピング クエリアが VLAN でイネーブルになっている場合は、VLAN 内で最小の IP アドレスのクエリアがアクティブな MLD スヌーピング クエリアとして選択されます。

  アクティブな MLD スヌーピング クエリアがダウンするか、またはいずれかのクエリアで IP アドレスが変更された場合に、MLD スヌーピング クエリアの選択が発生します。

（注）　不要でアクティブなクエリアのタイムアウトを回避するには、VLAN のすべてのクエリアで同じ値を使用して **ipv6 mld snooping last-member-query-interval** コマンドを設定します。

MLD スヌーピングについて

MLD スヌーピングの概要

MLD スヌーピングにより、スイッチで MLD 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。

MLD または MLD スヌーピング クエリアからの MLD クエリーを受信するサブネットで、MLD スヌーピングを使用するように、スイッチを設定できます。MLD スヌーピングは、IPv6 マルチキャスト トラフィックが受信対象のポートだけに転送されるようにレイヤ 2 LAN ポートをダイナミックに設定し、それによって、レイヤ 2 で IPv6 マルチキャスト トラフィックを抑制します。

MLD は、マルチキャスト ルータのレイヤ 3 で稼働し、マルチキャスト トラフィックのルーティングが必要なサブネットでレイヤ 3 MLD クエリーを生成します。MLD の詳細については、次のマニュアルを参照してください。

http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2mt/ip6-multicast.html

MLD スヌーピング クエリアをスイッチに設定して、マルチキャスト ルータ インターフェイスがないサブネットにおいて MLD スヌーピングをサポートできます。MLD スヌーピング クエリアの詳細については、「MLD スヌーピング クエリアのイネーブル化」（P.51-10）を参照してください。

MLD（マルチキャスト ルータ上）またはローカルで、MLD スヌーピング クエリアは、スイッチが VLAN のすべてのポートを通じて転送する、一般的な MLD クエリーを定期的に送信し、ホストがそれに応答します。MLD スヌーピングはレイヤ 3 MLD トラフィックをモニタします。

（注）　マルチキャスト グループで、VLAN 中に送信元だけがありレシーバがない場合は、MLD スヌーピングはマルチキャスト トラフィックをマルチキャスト ルータ ポート宛てだけに抑制します。

MLD メッセージ

- マルチキャスト リスナー クエリー：
  - 一般クエリー：どのマルチキャスト アドレスにリスナーがあるかを学習するために、マルチキャスト ルータが送信します。
  - マルチキャスト アドレス固有クエリー：特定マルチキャスト アドレスにリスナーがあるかどうかを学習するために、マルチキャスト ルータが送信します。
  - マルチキャスト アドレスおよび送信元固有クエリー：特定マルチキャスト アドレスの指定リストからの送信元にリスナーがあるかどうかを学習するために、マルチキャスト ルータが送信します。
- マルチキャスト リスナー レポート
  - 現行状態レコード（送信請求）：クエリーに応答してホストが送信し、ホストが関係するマルチキャスト グループごとに INCLUDE モードまたは EXCLUDE モードを指定します。
  - フィルタ モード変更レコード（非送信請求）：1 つ以上のマルチキャスト グループの INCLUDE モードまたは EXCLUDE モードを変更するため、ホストが送信します。
  - 送信元リスト変更レコード（非送信請求）：マルチキャスト送信元に関する情報を変更するため、ホストが送信します。

送信元ベース フィルタリング

MLD は送信元ベースのフィルタリングを使用します。これによりホストおよびルータは、特定のマルチキャスト グループで許可またはブロックされる送信元アドレスを特定できます。送信元ベースのフィルタリングでは、MLD メッセージ内にある以下の情報に基づいてトラフィックの許可またはブロックを行います。

- 送信元リスト
- INCLUDE モードまたは EXCLUDE モード

レイヤ 2 テーブルが（MAC グループ、VLAN）ベースのため、MLD のホストを使用する場合、マルチキャストの送信元は、各 MAC グループごとに 1 つだけ設定することを推奨します。

（注）　送信元ベース フィルタリングはハードウェアでサポートされません。このステートはソフトウェアでのみ維持され、明示的なホスト トラッキングおよび統計情報収集に使用されます。

明示的なホスト トラッキング

MLD では、ポート上のメンバーシップ情報の明示的なトラッキングをサポートします。明示的なトラッキング データベースは、高速脱退処理、プロキシ レポート機能、統計情報収集に使用されます。VLAN で明示的なトラッキングがイネーブルの場合、MLD スヌーピング ソフトウェアはホストから受信する MLD 通知を処理し、次の情報を含む明示的なトラッキング データベースを作成します。

- ホストに接続されたポート

- ホストによって報告されたチャネル
- ホストによって報告された各グループのフィルタ モード
- ホストによって報告された各グループの送信元リスト
- 各グループのルータ フィルタ モード
- 送信元を要求するグループごとのホスト リスト

（注）
- 明示的なホスト トラッキングをディセーブルにすると、高速脱退処理およびプロキシ レポート機能はディセーブルになります。
- 明示的なホスト追跡がイネーブル化されていて、スイッチがレポート抑制モードになっている場合、マルチキャスト ルータは VLAN インターフェイス経由でアクセスするすべてのホストを追跡できないことがあります。

MLD スヌーピング プロキシ レポート機能

MLD にはレポート抑制がないので、すべてのホストがクエリーに応じて詳細なマルチキャスト メンバーシップ情報をルータに送信します。スイッチはこれらの応答を調べて、データベースを更新し、レポートをマルチキャスト ルータに転送します。マルチキャスト ルータがレポートで過負荷になるのを防止するために、MLD スヌーピングはプロキシ レポート機能を実行します。

プロキシ レポート機能では、マルチキャスト グループの最初のレポートだけがルータに転送され、同一マルチキャスト グループのその他すべてのレポートが抑制されます。

プロキシ レポート機能では、送信請求レポートおよび非送信請求レポートが処理されます。プロキシ レポート機能はイネーブルになっており、ディセーブルにすることはできません。

（注）明示的なホスト トラッキングをディセーブルにすると、高速脱退処理およびプロキシ レポート機能はディセーブルになります。

IPv6 マルチキャスト グループへの加入

ホストは、IPv6 マルチキャスト ルータからの一般的なクエリーに応じて、非送信請求 MLD レポートを送信するか、または MLD レポートを送信して、IPv6 マルチキャスト グループに参加します（スイッチは、一般的なクエリーを、IPv6 マルチキャスト ルータから VLAN 中のすべてのポートに転送します）。スイッチはこれらのレポートをスヌーピングします。

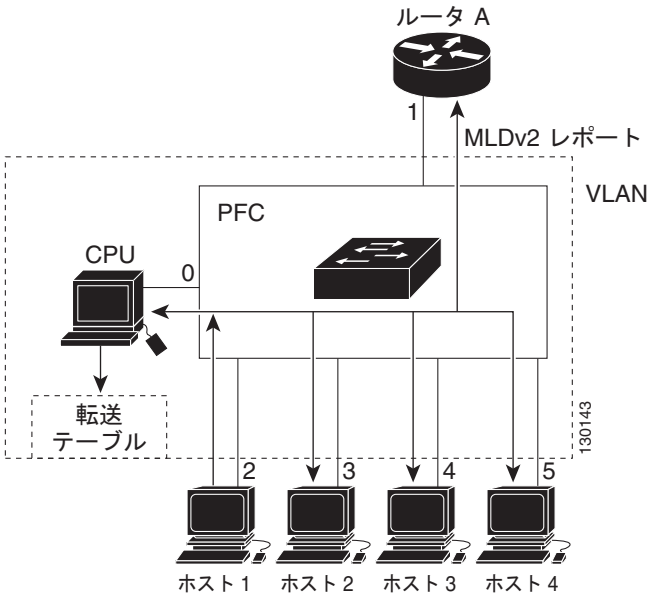
スヌーピングされた MLD レポートに応じて、スイッチは、レポートを受信した VLAN のレイヤ 2 転送テーブルにエントリを 1 つ作成します。このマルチキャスト トラフィックに関係する別のホストが MLD レポートを送る場合、スイッチは、レポートをスヌーピングして既存のレイヤ 2 転送テーブル エントリにそれを追加します。スイッチは、MLD レポートをスヌーピングする各マルチキャスト グループ用レイヤ 2 転送テーブルで、VLAN あたり 1 つのエントリだけを生成します。

MLD スヌーピングは、マルチキャスト グループごとに 1 つを除いたすべてのホスト レポートを抑制し、その 1 つのレポートを IPv6 マルチキャスト ルータに転送します。

スイッチは、レポートで指定されたマルチキャスト グループ用のマルチキャスト トラフィックを、レポートを受信したインターフェイスに転送します（図 51-1 を参照）。

MLD スヌーピングを通じて学習されるレイヤ 2 マルチキャスト グループは、ダイナミックです。ただし、**mac address-table static** コマンドを使用して、レイヤ 2 マルチキャスト グループをスタティックに設定することもできます。マルチキャスト グループ アドレスのグループ メンバーシップをスタティックに指定した場合、そのスタティックな設定は、MLD スヌーピングの学習よりも優先されます。マルチキャスト グループ メンバーシップのリストは、スタティックな設定値と、MLD スヌーピングによって学習された設定値の両方で構成できます。

図 51-1　　初期 MLD リスナー レポート



マルチキャスト ルータ A が MLD 一般クエリーをスイッチに送信し、スイッチがそのクエリーを、同じ VLAN のすべてのメンバのポート 2 ～ 5 に転送します。ホスト 1 は、IPv6 マルチキャスト グループに加入する意思があり、MLD レポートを 0x0100.5E01.0203 と同じ MAC 宛先アドレスを持つグループにマルチキャストします。スイッチは、ホスト 1 による MLD レポート マルチキャストをスヌーピングすると、スイッチは、MLD レポート内の情報を利用して、転送テーブル エントリを作成します。

表 51-1　　MLD スヌーピング転送テーブル

宛先 MAC アドレス	パケットのタイプ	ポート
0100.5exx.xxxx	MLD	0
0100.5e01.0203	!MLD	1、2

スイッチのハードウェアは、マルチキャスト グループの他のパケットと MLD 情報パケットを区別できます。テーブル中の最初のエントリは、MLD パケットだけを CPU に送信するように指示します。これによって、スイッチがマルチキャスト フレームで過負荷になるのを防止できます。2 番めのエントリは、MLD パケット（!MLD）ではない 0x0100.5E01.0203 マルチキャスト MAC アドレス宛てのフレームをマルチキャスト ルータとグループに加入したホストに送信するように指示します。

別のホスト（たとえば、ホスト 4）が、同じグループ用に非送信請求 MLD レポートを送る場合（図 51-2 を参照）、スイッチがそのメッセージをスヌーピングし、ホスト 4 のポート番号を転送テーブルに追加します（表 51-2 を参照）。転送テーブルはスイッチ宛てだけに MLD メッセージを送るので、メッセージは他のポートへフラッディングされません。認識されているマルチキャスト トラフィックは、スイッチ宛てではなくグループ宛てに転送されます。

図 51-2　2 番めのホストのマルチキャスト グループへの加入

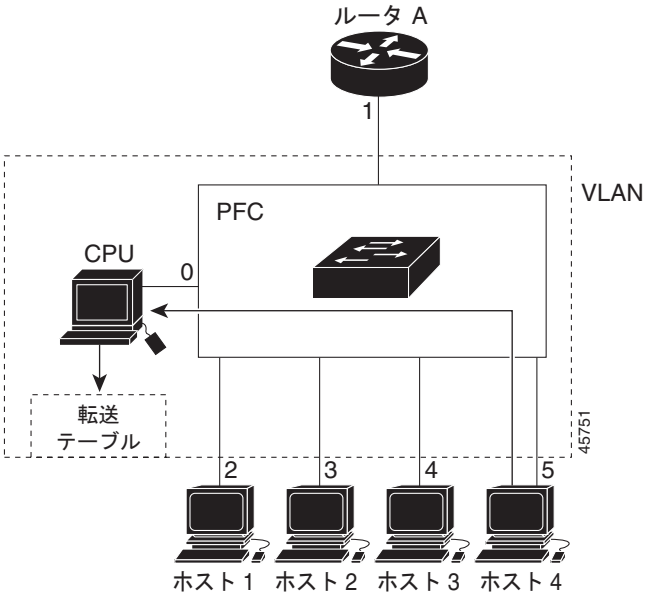


表 51-2　更新された MLD スヌーピング転送テーブル

宛先 MAC アドレス	パケットのタイプ	ポート
0100.5exx.xxxx	MLD	0
0100.5e01.0203	!MLD	1, 2, 5

マルチキャスト グループからの脱退

通常の脱退処理

関連するホストは、一般的な MLD クエリーに定期的に応答を続ける必要があります。VLAN 中の 1 つ以上のホストが一般的な MLD クエリーに定期的に応答しているかぎり、マルチキャスト ルータは引き続きマルチキャスト トラフィックを VLAN に転送します。ホストをマルチキャスト グループから脱退させたい場合は、そのホストで定期的な MLD 一般クエリーを無視するか（「暗黙的脱退」といいます）、または MLD フィルタ モード変更レコードを送信します。

MLD スヌーピングが、グループの EXCLUDE モードを設定するホストからフィルタ モード変更レコードを受信すると、MAC アドレスの一般的なクエリーを送信して、そのインターフェイスに接続されている他のホストがその特定のマルチキャスト グループに対するトラフィックに関係があるかどうかを判断します。

MLD スヌーピングが、この一般的なクエリーに対して MLD レポートを受信しなかった場合、インターフェイスに接続されている他のホストの中に、このマルチキャスト グループのトラフィックの受信に関与しているホストはないと見なし、指定されたマルチキャスト グループに対応するレイヤ 2 転送テーブル エントリからそのインターフェイスを削除します。

残りのインターフェイスのうち、グループに関係するホストが接続されたインターフェイスだけからフィルタ モード変更レコードが送信され、一般的なクエリーに応答する MLD レポートを MLD スヌーピングが受信しない場合、MLD スヌーピングはグループ エントリを削除して、MLD フィルタ モード変更レコードをマルチキャスト ルータにリレーします。マルチキャスト ルータが VLAN からレポートを受信しない場合、マルチキャスト ルータは MLD キャッシュからその VLAN 用のグループを削除します。

テーブル エントリを更新するまでスイッチが待機する時間は、「最終メンバ クエリー時間」といいます。時間を設定するには、**ipv6 mld snooping last-member-query-interval** *interval* コマンドを入力します。

高速脱退処理

高速脱退処理は、デフォルトでイネーブルになっています。高速脱退処理をディセーブルにするには、明示的なホスト トラッキングをオフにします。

高速脱退処理は、ソフトウェアで送信元グループ ベースのメンバーシップ情報を維持し、LTL インデックスを MAC GDA 単位で割り当てることによって実装されます。

高速脱退処理をイネーブルにすると、ホストは送信元からこれ以上トラフィックを受信したくない場合に特定のグループに対し BLOCK_OLD_SOURCES{src-list} メッセージを送信します。このようなメッセージをホストから受信すると、スイッチは所定のグループに対応するホストの送信元リストを解析します。この送信元リストが脱退メッセージで受信された送信元リストとまったく同じである場合、スイッチはこのホストを LTL インデックスから削除し、ホストへのマルチキャスト グループ トラフィックの転送を停止します。

送信元リストが一致しない場合、このホストがどの送信元からのトラフィック受信にも関与しなくなるまで、スイッチは LTL インデックスからホストを削除しません。

（注） 明示的なホスト トラッキングをディセーブルにすると、高速脱退処理およびプロキシ レポート機能はディセーブルになります。

MLD スヌーピング クエリアについて

マルチキャスト トラフィックをルーティングする必要がないため、PIM および MLD を設定していない VLAN 内で MLD スヌーピングをサポートするには、MLD スヌーピング クエリアを使用します。

IP マルチキャスト ルーティングが設定されたネットワークでは、IP マルチキャスト ルータが MLD クエリアとして機能します。VLAN の IP マルチキャスト トラフィックに、レイヤ 2 スイッチングだけを行う必要がある場合、IP マルチキャスト ルータは必要ではありません。ただし、VLAN 上に IP マルチキャスト ルータがない場合には、クエリーを送信できるよう他のスイッチを MLD クエリアとして設定する必要があります。

MLD スヌーピング クエリアがイネーブルの場合、MLD スヌーピング クエリアは、IP マルチキャスト トラフィックの受信を希望するスイッチから、MLD レポート メッセージを開始する MLD クエリーを定期的に送信します。MLD スヌーピングはこれらの MLD レポートを待ち受けて、適切な転送を確立します。

MLD スヌーピング クエリアは、VLAN 内のすべてのスイッチでイネーブルにできますが、MLD を使用して IP マルチキャスト トラフィックの情報をレポートするスイッチに接続されている VLAN ごとに、少なくとも 1 つのスイッチを MLD スヌーピング クエリアとして設定する必要があります。

IP マルチキャスト ルーティングがイネーブルであるかどうかにかかわらず、VLAN 上で MLD クエリーを生成するようにスイッチを設定できます。

MLD スヌーピングのデフォルト設定

- MLD スヌーピング クエリア：ディセーブル
- MLD スルーピング：イネーブル
- マルチキャスト ルータ：未設定
- MLD レポート抑制：イネーブル
- MLD スヌーピング ルータの学習方式：PIM または MLD パケットによって自動的に学習
- 高速脱退処理：イネーブル
- MLD 明示的ホスト トラッキング：イネーブル

MLD スヌーピングの設定方法

- 「MLD スヌーピング クエリアのイネーブル化」（P.51-10）
- 「MLD スヌーピング クエリー時間の設定」（P.51-10）
- 「MLD スヌーピングのイネーブル化」（P.51-11）
- 「マルチキャスト レシーバへのスタティック接続の設定」（P.51-12）
- 「マルチキャスト ルータ ポートのスタティックな設定」（P.51-12）
- 「高速脱退処理のイネーブル化」（P.51-12）
- 「SSM セーフ レポート機能のイネーブル化」（P.51-13）
- 「明示的なホスト トラッキングの設定」（P.51-13）
- 「レポート抑制の設定」（P.51-14）

（注）
- MLD スヌーピングを使用するには、IPv6 マルチキャスト ルーティング用にサブネットでレイヤ 3 インターフェイスを設定するか、またはサブネットで MLD スヌーピング クエリアをイネーブルにします（「MLD スヌーピング クエリアのイネーブル化」（P.51-10）を参照）。
- グローバルにイネーブルにするコマンドを除き、すべての MLD スヌーピング コマンドは VLAN インターフェイス上だけでサポートされます。

MLD スヌーピング クエリアのイネーブル化

マルチキャスト トラフィックをルーティングする必要がないため、PIM および MLD を設定していない VLAN 内で MLD スヌーピングをサポートするには、MLD スヌーピング クエリアを使用します。VLAN で MLD スヌーピング クエリア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	`Router(config)# vlan configuration vlan_ID`	VLAN を選択します。
ステップ 2	`Router(config-vlan-config)# ipv6 address prefix/prefix_length`	IPv6 アドレスおよびサブネットを設定します。
ステップ 3	`Router(config-vlan-config)# ipv6 mld snooping querier`	MLD スヌーピング クエリアをイネーブルにします。
ステップ 4	`Router(config-vlan-config)# end`	コンフィギュレーション モードを終了します。

次に、VLAN 200 で MLD スヌーピング クエリアをイネーブルにし、設定を確認する例を示します。

```
Router# vlan configuration 200
Router(config-vlan-config)# ipv6 address 2001:0DB8:0:1::/64 eui-64
Router(config-vlan-config)# ipv6 mld snooping querier
Router(config-vlan-config)# end
Router# show ipv6 mld interface vlan 200 | include querier
  MLD snooping fast-leave is enabled and querier is enabled
```

MLD スヌーピング クエリー時間の設定

特定のマルチキャスト グループにホストがまだ関係しているかどうかを判別するグループ固有のクエリーを送信した後で、スイッチが待機する時間を設定できます。

（注）　MLD スヌーピング高速脱退処理と MLD スヌーピング クエリー時間の両方を設定した場合は、高速脱退処理が優先されます。

スイッチによって送信される MLD スヌーピング クエリー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	`Router(config)# vlan configuration vlan_ID`	VLAN を選択します。
ステップ 2	`Router(config-vlan-config)# ipv6 mld snooping last-member-query-interval interval`	スイッチによって送信される IGMP クエリーの待機時間を設定します。デフォルトは 1 秒です。有効な範囲は 1000 ～ 9990 ミリ秒です。

次に、MLD スヌーピング クエリー時間を設定する例を示します。

```
Router(config-vlan-config)# ipv6 mld snooping last-member-query-interval 1000
Router(config-vlan-config)# exit
Router# show ipv6 mld interface vlan 200 | include last
  MLD snooping last member query response interval is 1000 ms
```

MLD スヌーピングのイネーブル化

MLD スヌーピングのグローバルなイネーブル化

MLD スヌーピングをグローバルにイネーブル化するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# ipv6 mld snooping`	MLD スヌーピングをイネーブルにします。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

次に、MLD 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。

```
Router(config)# ipv6 mld snooping
Router(config)# end
Router# show ipv6 mld interface vlan 200 | include globally
  MLD snooping is globally enabled
Router#
```

VLAN における MLD スヌーピングのイネーブル化

特定の VLAN で MLD 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	`Router(config)# vlan configuration vlan_ID`	VLAN を選択します。
ステップ 2	`Router(config-vlan-config)# ipv6 mld snooping`	MLD スヌーピングをイネーブルにします。
ステップ 3	`Router(config-vlan-config)# end`	コンフィギュレーション モードを終了します。

次に、VLAN 25 で MLD 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。

```
Router# vlan configuration 25
Router(config-vlan-config)# ipv6 mld snooping
Router(config-vlan-config)# end
Router# show ipv6 mld interface vlan 25 | include snooping
  MLD snooping is globally enabled
  MLD snooping is enabled on this interface
  MLD snooping fast-leave is enabled and querier is enabled
  MLD snooping explicit-tracking is enabled
  MLD snooping last member query response interval is 1000 ms
  MLD snooping report-suppression is disabled
Router#
```

マルチキャスト レシーバへのスタティック接続の設定

マルチキャスト レシーバへのスタティック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	Router(config)# **mac address-table static** *mac_addr* **vlan** *vlan_id* **interface** *type slot/port* [**disable-snooping**]	マルチキャスト レシーバへのスタティックな接続を設定します。
ステップ 2	Router(config)# **end**	コンフィギュレーション モードを終了します。

スタティックな接続を設定する場合、**disable-snooping** キーワードを入力して、スタティックに設定されたマルチキャスト MAC アドレスにアドレス指定されたマルチキャスト トラフィックが、同じ VLAN 内の別のポートへ送信されるのを防止します。

次に、マルチキャスト レシーバへのスタティックな接続を設定する例を示します。

```
Router(config)# mac address-table static 0050.3e8d.6400 vlan 12 interface gigabitethernet
5/7
```

マルチキャスト ルータ ポートのスタティックな設定

マルチキャスト ルータへのスタティック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	Router(config)# **vlan configuration** *vlan_ID*	VLAN を選択します。
ステップ 2	Router(config-vlan-config)# **ipv6 mld snooping mrouter interface** *type slot/port*	マルチキャスト ルータへのスタティック接続を設定します。
ステップ 3	Router(config-vlan-config)# **end**	コンフィギュレーション モードを終了します。

ルータへのインターフェイスは、コマンドを入力する VLAN 内である必要があります。インターフェイスは管理上アップ状態で、回線プロトコルはアップ状態である必要があります。

次に、マルチキャスト ルータへのスタティックな接続を設定する例を示します。

```
Router(config-vlan-config)# ipv6 mld snooping mrouter interface gigabitethernet 5/6
Router(config-vlan-config)#
```

高速脱退処理のイネーブル化

特定の VLAN 上で高速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
ステップ 1	Router(config)# **vlan configuration** *vlan_ID*	VLAN を選択します。
ステップ 2	Router(config-vlan-config)# **ipv6 mld snooping fast-leave**	VLAN 上で高速脱退処理をイネーブルにします。

次に、VLAN 200 インターフェイスで高速脱退処理をイネーブルにし、設定を確認する例を示します。

```
Router# vlan configuration 200
Router(config-vlan-config)# ipv6 mld snooping fast-leave
Configuring fast leave on vlan 200
Router(config-vlan-config)# end
Router# show ipv6 mld interface vlan 200 | include fast-leave
  MLD snooping fast-leave is enabled and querier is enabled
Router#
```

SSM セーフ レポート機能のイネーブル化

Source-Specific Multicast（SSM）セーフ レポート機能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	`Router(config)# vlan configuration vlan_ID`	VLAN を選択します。
ステップ 2	`Router(config-vlan-config)# ipv6 mld snooping ssm-safe-reporting`	SSM セーフ レポート機能をイネーブルにします。

次に、SSM セーフ レポート機能をイネーブルにする例を示します。

```
Router(config)# vlan configuration 10
Router(config-vlan-config)# ipv6 mld snooping ssm-safe-reporting
```

明示的なホスト トラッキングの設定

（注）　明示的なホスト トラッキングをディセーブルにすると、高速脱退処理およびプロキシ レポート機能はディセーブルになります。

特定の VLAN で明示的なホスト トラッキ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	`Router(config)# vlan configuration vlan_ID`	VLAN を選択します。
ステップ 2	`Router(config-vlan-config)# ipv6 mld snooping explicit-tracking`	明示的なホスト トラッキングをイネーブルにします。

次に、明示的なホスト トラッキングをイネーブルにする例を示します。

```
Router(config)# vlan configuration 25
Router(config-vlan-config)# ipv6 mld snooping explicit-tracking
Router(config-vlan-config)# end
Router# show ipv6 mld snooping explicit-tracking vlan 25
Source/Group                    Interface    Reporter        Filter_mode
-------------------------------------------------------------------------
10.1.1.1/226.2.2.2              Vl25:1/2     16.27.2.3       INCLUDE
10.2.2.2/226.2.2.2              Vl25:1/2     16.27.2.3       INCLUDE
```

レポート抑制の設定

VLAN でレポート抑制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	`Router(config)# vlan configuration vlan_ID`	VLAN を選択します。
ステップ 2	`Router(config-vlan-config)# ipv6 mld snooping report-suppression`	レポート抑制をイネーブルにします。

次に、明示的なホスト トラッキングをイネーブルにする例を示します。

```
Router(config)# vlan configuration 25
Router(config-vlan-config)# ipv6 mld snooping report-suppression
Router(config-vlan-config)# end
Router# Router# show ipv6 mld interface vlan 25 | include report-suppression
  MLD snooping report-suppression is enabled
```

MLD スヌーピング設定の確認

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
`Router# show ipv6 mld snooping mrouter 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。

```
Router# show ipv6 mld snooping mrouter vlan 1
vlan            ports
-----+---------------------------------------
  1          Gi1/1,Gi2/1,Gi3/48,Router
Router#
```

MAC アドレス マルチキャスト エントリの表示

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
Router# **show mac address-table multicast** *vlan_ID* [**count**]	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。

```
Router# show mac address-table multicast vlan 1
vlan   mac address     type    qos             ports
-----+---------------+--------+---+--------------------------------
  1  0100.5e02.0203  static   --  Gi1/1,Gi2/1,Gi3/48,Router
  1  0100.5e00.0127  static   --  Gi1/1,Gi2/1,Gi3/48,Router
  1  0100.5e00.0128  static   --  Gi1/1,Gi2/1,Gi3/48,Router
  1  0100.5e00.0001  static   --  Gi1/1,Gi2/1,Gi3/48,Router,Switch
Router#
```

次に、特定の VLAN について MAC アドレス エントリの総数を表示する例を示します。

```
Router# show mac address-table multicast 1 count

Multicast MAC Entries for vlan 1:    4
Router#
```

VLAN インターフェイスの MLD スヌーピング情報の表示

VLAN インターフェイスについて MLD 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
Router# **show ipv6 mld snooping** {{**explicit-tracking** *vlan_ID*}| {**mrouter** [**vlan** *vlan_ID*]} | {**report-suppression vlan** *vlan_ID*} | {**statistics vlan** *vlan_ID*}	特定の VLAN インターフェイス上の MLD スヌーピング情報を表示します。

次に、VLAN 25 の明示的トラッキング情報を表示する例を示します。

```
Router# show ipv6 mld snooping explicit-tracking vlan 25
Source/Group                    Interface    Reporter        Filter_mode
--------------------------------------------------------------------------
10.1.1.1/226.2.2.2              Vl25:1/2     16.27.2.3       INCLUDE
10.2.2.2/226.2.2.2              Vl25:1/2     16.27.2.3       INCLUDE
```

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。

```
Router# show ipv6 mld snooping mrouter vlan 1
vlan            ports
-----+---------------------------------------
  1          Gi1/1,Gi2/1,Gi3/48,Router
```

次に、VLAN 25 の IGMP スヌーピング統計情報の例を示します。

```
Router# show ipv6 mld snooping statistics interface vlan 25

Snooping staticstics for Vlan25
#channels:2
#hosts   :1

Source/Group            Interface       Reporter      Uptime        Last-Join    Last-Leave
10.1.1.1/226.2.2.2      Gi1/2:Vl25      16.27.2.3     00:01:47      00:00:50       -
10.2.2.2/226.2.2.2      Gi1/2:Vl25      16.27.2.3     00:01:47      00:00:50       -
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

PART 11

ネットワーク管理

CHAPTER 52

NetFlow ハードウェア サポート

（注） Cisco IOS Release 15.1SY では、Flexible NetFlow 機能により、統計情報収集およびデータ エクスポートを実行できます。次の資料を参照してください。

http://www.cisco.com/en/US/docs/ios-xml/ios/fnetflow/command/fnf-cr-book.html

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

NetFlow ハードウェア サポートの前提条件

なし。

NetFlow ハードウェア サポートの制約事項

- Cisco IOS Release 15.1SY 以降のリリースでは、NetFlow バージョン 7 および NetFlow バージョン 8 はサポートされません。Flexible NetFlow では、NetFlow バージョン 5 を制限付きでサポートしています。
- 統計情報は、NetFlow テーブルが満杯になると転送されているフローには使用できません。
- NetFlow テーブルの使用率が、次の表に示す推奨レベルの使用率を超過すると、統計情報を保存するための十分な領域が不足する確率が高くなります。表 52-1 に、推奨の最大使用率を示します。

表 52-1　NetFlow テーブルの使用率

PFC モード	有効な NetFlow テーブルの使用率		NetFlow テーブルの合計容量	
PFC4XL	506,184 個の入力エントリ	506,184 個の出力エントリ	524,288（512k）個の入力エントリ	524,288（512k）個の出力エントリ
PFC4	515,032 個の入力 + 出力エントリ		524,288（512k）個の入力 + 出力エントリ	

- フローが PBR 範囲のアドレスを宛先とする場合、または PBR 範囲のアドレスから発信されている場合、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）または null です。

NetFlow ハードウェア サポートに関する情報

PFC および任意の DFC の NetFlow テーブルは、ハードウェアで転送されるフローのデータをキャプチャします。次に、NetFlow テーブルを使用する機能の一部を示します。

- Flexible NetFlow
- ネットワーク アドレス変換（NAT）
- QoS マイクロフロー ポリシング
- 再帰 ACL
- WCCP

テーブルから削除できる古いフローを識別するエージング タイマーを設定すると、NetFlow CPU の使用を制限できます。NetFlow は、失効エントリを削除し、新しいエントリのためにテーブルのスペースをクリアします。

NetFlow ハードウェア サポートのデフォルト設定

- 非アクティブ フロー エージング：イネーブル（300 秒）
- ファースト エージング：ディセーブル
- アクティブ フロー エージング：イネーブル（1920 秒）

NetFlow ハードウェア サポートの設定方法

- 「非アクティブ フロー エージングの設定」（P.52-3）
- 「ファースト エージングの設定」（P.52-3）
- 「アクティブ フロー エージングの設定」（P.52-4）

（注）

- NetFlow テーブル エージングにより、NetFlow テーブルのサイズを推奨使用率未満に保ちます。NetFlow テーブルのエントリの数が推奨使用率（「NetFlow ハードウェア サポートの制約事項」（P.52-1）を参照）を超えると、一部のフローで隣接統計情報しか使用できなくなる場合があります。
- ネットワーク イベント（ルーティングの変更、リンク ステートの変化など）によっても、NetFlow テーブルのエントリが削除されることがあります。

非アクティブ フロー エージングの設定

非アクティブ フロー エージングを設定するには、次の作業を行います。

コマンド	目的
`Router(config)# flow platform cache timeout inactive` *seconds*	設定した時間の値よりも長い間非アクティブ状態である NetFlow テーブル エントリに対するエージング タイムを設定します。 • デフォルト：イネーブル。値：300 秒。 • *seconds* の値の範囲：32 ～ 512。

次に、設定した時間の値よりも長い間非アクティブ状態である NetFlow テーブル エントリに対するエージング タイムを設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# flow platform cache timeout inactive 300
```

ファースト エージングの設定

ファースト エージングを設定するには、次の作業を行います。

コマンド	目的
`Router(config)# flow platform cache timeout fast [[time` *seconds*`] [threshold` *packets*`]]`	設定した時間の値よりも長い間非アクティブ状態であり、設定したしきい値よりも転送したパケットの数が少ない、NetFlow テーブル エントリに対するエージング タイムを設定します。 • デフォルトではディセーブルになっています。 • **time** *seconds* を入力しない場合のデフォルト：32 秒。*seconds* の値の範囲：60 ～ 4092。 • **threshold** *packets* を入力しない場合のデフォルト：100 パケット *packets* の値の範囲：1 ～ 4000。

（注）　ファースト エージングをイネーブルにする場合、最初はこの値を 128 秒に設定します。NetFlow テーブル サイズが増え続け、推奨利用率を超えた場合は、テーブル サイズが推奨利用率未満になるまで設定値を下げます。テーブルが推奨使用率を超えて拡大し続ける場合は、非アクティブ NetFlow テーブルのエージング タイムを短くしてください。

次に、NetFlow テーブルのエージング タイムを設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# flow platform cache timeout fast time 32 threshold 100
```

アクティブ フロー エージングの設定

アクティブ フロー エージングを設定するには、次の作業を行います。

コマンド	目的
`Router(config)# flow platform cache timeout active` *seconds*	パケット アクティビティを問わない NetFlow テーブル エントリのエージング タイムを設定します。これにより、カウンタ ラップアラウンドおよび統計が不正確になることを防止できます。 • デフォルト：イネーブル。値：1920 秒。 • *seconds* の値の範囲：60 ～ 4092。

次の例は、アクティブ フロー エージングを設定する方法を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# flow platform cache timeout active 1920
```

NetFlow テーブルのエージング設定の確認

NetFlow テーブルのエージング設定を表示するには、次の作業を行います。

コマンド	目的
`Router# show platform flow aging`	NetFlow テーブルのエージング設定を表示します。

次に、NetFlow テーブルのエージング タイムの設定を表示する例を示します。

```
Router# show platform flow aging
Aging scheme   Enabled   Timeout   Packet threshold
-------------+---------+---------+-----------------
       Fast        No         32           100
   Inactive       Yes        300           N/A
     Active       Yes       1920           N/A
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

Call Home

（注）

- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。
- Cisco IOS Release 15.1SY は、次の Call Home 拡張機能をサポートします。
  - Call Home シングル コマンド設定
  - Anonymous Reporting
  - Crash アラート グループ
  - データ プライバシー
  - 診断シグニチャ
  - HTTP プロキシ サーバのサポート
  - Call Home メッセージの IOS コマンドに対する AAA 認証
  - Snapshot アラート グループ
  - syslog スロットリング
  - Call Home メッセージの圧縮：大きいメッセージの切り捨てを防ぐには、圧縮し、base64 バイナリ エンコーディングを、Smart Call Home サーバに送信される、10KB より大きな XML 形式の CLI 出力に適用します。
  - HTTPS 接続用の CA 証明書の自動更新

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

Call Home の前提条件

- 受信者が受信メッセージの発信元を判別できるように設定される Call Home 連絡先に関する次の情報を取得します。
  - 顧客連絡先の電子メール（Smart Call Home へのフル登録の場合は必須、Call Home が匿名モードでイネーブルの場合は任意）
  - 顧客の電話番号（任意）
  - 顧客の住所（任意）
- 電子メール メッセージ配信を使用している場合は、プライマリ シンプル メール転送プロトコル（SMTP）サーバとバックアップ サーバの名前または、IPv4 または IPv6 アドレスを特定します。
- （Release 15.1SY 以降のリリースでは不要）セキュア HTTP（HTTPS）メッセージ配信を使用する場合、トラストポイント認証局（CA）を設定します。Call Home の CiscoTAC-1 プロファイルで Cisco Smart Call Home サービス用に HTTPS サーバを使用している場合、この手順は必須です。
- ルータから電子メール サーバ（1 つまたは複数）または宛先 HTTP サーバへの IP 接続を確認します。
- サーバを名前で指定する場合は、スイッチがドメイン ネーム サーバに IP 接続できる必要があります。
- Cisco Smart Call Home を使用する場合は、設定するデバイスが有効なサービス契約の対象となっていることを確認します。

ヒント Smart Call Home Web アプリケーションから、基本的な設定スクリプトをダウンロードして、Smart Call Home およびシスコ TAC とともに使用するよう Call Home 機能を設定するために利用できます。現状のままで提供される、このスクリプトは、次の URL からダウンロードできます。
https://supportforums.cisco.com/community/netpro/solutions/smart_services/smartcallhome

Call Home の制約事項

- Cisco TAC プロファイルの場合、電子メール メッセージまたは HTTP メッセージを送信するように Call Home を設定できます。ただし、両方を送信するように設定することはできません。
- Call Home アラートは、その Call Home アラートが含まれているアラート グループに登録されている宛先プロファイルにしか送信されません。さらに、アラート グループをイネーブルにする必要があります。
- Call Home データ プライバシーをイネーブルにすると、大量のデータのスクラビング処理を行ったときに CPU 使用率に影響を及ぼすことがあります。

- Call Home データ プライバシーでは、**show running-config all** および **show startup-config** データ内の設定メッセージに対して **show** コマンド出力のスクラビング処理が行われます。
- VSS モードでは、設定メッセージのホスト名のスクラビング処理を行うと、Cisco TAC バックエンド サーバで Smart Call Home の処理に失敗することがあります。
- Call Home 診断シグニチャ機能の使用は、今後サポートされる予定です。Call Home 診断シグニチャ コマンドは、すでに CLI にあります。

```
Router(cfg-call-home)# diagnostic-signature
Router(cfg-call-home-diag-sign)# active
Router(cfg-call-home-diag-sign)# profile profile_name
Router# show call-home diagnostic-signature
Router# call-home diagnostic-signature download
Router# call-home diagnostic-signature install
Router# clear call-home diagnostic-signature statistics
Router# debug call-home diagnostic-signature
```

Call Home について

Call Home の概要

Call Home には、クリティカルなシステム イベントに対して次の通知オプションがあります。

- 電子メール（たとえば Network Operations Center へ）または Web ベース。
- 自動解析用のサポート Web サイトへの XML の配信。
- Cisco Smart Call Home は、シスコ Technical Assistance Center（TAC）の直接ケース生成をサポートします。

Call Home アラート メッセージには、設定、診断、環境条件、インベントリ、syslog、スナップショット、クラッシュ イベントの情報が含まれます。

Call Home 機能では、*Call Home 宛先プロファイル*に従って複数の受信者にアラートを送信できます。宛先プロファイルには、メッセージ形式とコンテンツのカテゴリを設定できます。定義済みの宛先プロファイル（CiscoTAC-1）が提供されており、独自の宛先プロファイルを定義することもできます。CiscoTAC-1 プロファイルを使用して、Cisco TAC へのサービス要求の作成に使用できる Smart Call Home サービスのバック エンド サーバに（デバイスに提供される Smart Call Home サービス サポートおよびアラートの重大度に応じて）アラートを送信します。

柔軟なメッセージ送信オプションと形式オプションにより、特定のサポート要件に簡単に統合できます。複数の宛先プロファイルが設定されている場合、システムは、設定した各プロファイルから Call Home メッセージを送信しようとします。

Call Home 機能では、次の機能が提供されます。

- 複数のメッセージ形式オプション
  - ショート テキスト：ポケットベルまたは印刷形式のレポートに最適。
  - ロング テキスト：人間が読むのに適した形式に完全整形されたメッセージ情報。
  - XML：Extensible Markup Language（XML）および Adaptive Markup Language（AML）Document Type Definitions（DTD; 文書タイプ定義）を使用するマシンが判読可能な形式です。XML 形式により、Cisco Smart Call Home サーバとの通信が可能。
- 複数のメッセージ宛先への同時配信が可能。
- 設定、クラッシュ、診断、環境条件、インベントリ、スナップショットおよび syslog イベントを含む複数のメッセージ カテゴリ。
- 重大度とパターン マッチングによるメッセージのフィルタリング。
- 定期的なメッセージ送信のスケジューリング。
- 連続的なデバイスのヘルス モニタリングとリアルタイム診断アラート。
- デバイスから送られた Call Home メッセージの分析。サポートされている場合は、自動サービス要求が作成され、詳細な診断情報を含め、適切な TAC チームにルーティングされて、問題解決の高速化が実現されます。
- お使いのデバイスから直接、またはダウンロード可能な転送ゲートウェイ（TG）集約ポイントを介して転送されたメッセージのセキュリティ保護。複数のデバイスをサポートする必要のある場合や、セキュリティ要件によってデバイスがインターネットに直接接続されないことが必要とされる場合は、TG 集約ポイントを使用できます。
- すべての Call Home デバイスの Call Home メッセージと推奨事項、コンポーネント情報、および設定情報への Web アクセス。これにより、関連するフィールド通知、セキュリティ勧告、およびサポート終了日情報にアクセスできます。

Anonymous Reporting

Smart Call Home は、多くのシスコ サービス契約に含まれるサービス機能で、顧客が問題をより迅速に解決できるように支援することを目的としています。また、クラッシュ メッセージから取得した情報は、シスコが現場の機器や発生している問題を理解しやすくします。Smart Call Home を使用しない場合でも、Anonymous Reporting をイネーブルにすると、シスコはデバイスから最小限のエラーおよびヘルス情報をセキュアに受信できます。Anonymous Reporting をイネーブルにした場合、顧客が誰であるかは匿名のままで、識別情報は送信されません。

（注）　Anonymous Reporting をイネーブルにすると、シスコまたはシスコに代わって業務を行うベンダーに指定データを転送することに同意することになります（米国以外の国を含む）。シスコでは、すべてのお客様のプライバシーを保護しています。シスコの個人情報の取り扱いについては、http://www.cisco.com/web/siteassets/legal/privacy.html でシスコのプライバシー ステートメントを参照してください。

Call Home が匿名で設定されていると、クラッシュ、インベントリ、およびテスト メッセージだけがシスコに送信されます。顧客の識別情報は送信されません。

これらのメッセージの送信内容の詳細については、「アラート グループの起動イベントとコマンド」（P.53-5）を参照してください。

Smart Call Home

シスコと直接サービス契約を結んでいる場合は、Cisco Smart Call Home サービス用の Call Home デバイスを登録できます。

Smart Call Home には次の機能があります。

- 継続的なデバイス ヘルス モニタリングとリアルタイムの診断アラート
- Smart Call Home メッセージの分析。必要に応じて、自動サービス要求（詳細な診断情報が含まれる）が作成され、該当する TAC チームにルーティングされるため、問題解決を高速化できます。
- セキュアなメッセージ転送が、ご使用のデバイスから直接、または HTTP プロキシ サーバやダウンロード可能な転送ゲートウェイ（TG）を経由して行われます。TG 集約ポイントは、複数のデバイスをサポートする場合またはセキュリティ要件によって、デバイスをインターネットに直接接続できない場合に使用できます。
- すべての Smart Call Home デバイスの Smart Call Home メッセージと推奨事項、インベントリ情報、および設定情報に Web アクセスすることにより、関連するフィールド通知、セキュリティ勧告、およびサポート終了日情報にアクセスできます。

既知と特定できる問題、特に GOLD 診断エラーについては、デバイスに提供される Smart Call Home サービス サポートおよびアラートの重大度に応じて、シスコ TAC によって自動サービス要求が生成されます。

次の項目を登録する必要があります。

- ご使用のスイッチの SMARTnet 契約番号。
- 電子メール アドレス
- Cisco.com ID

Smart Call Home の詳細については、次の URL の Smart Call Home ページを参照してください。

https://supportforums.cisco.com/community/netpro/solutions/smart_services/smartcallhome

アラート グループの起動イベントとコマンド

Call Home 起動イベントはアラート グループにグループ化され、各アラート グループにはイベントの発生時に実行するよう CLI コマンドが割り当てられます。CLI コマンド出力は転送されるメッセージに含まれます。次の表に、各アラート グループに含まれる起動イベントを示します。これには、各イベントの重大度と実行されるアラート グループの CLI コマンドも含まれます。

- 「Call Home の Syslog アラート グループのイベントとアクション」、表 53-1（P.53-6）
- 「Call Home の Crash アラート グループのイベントとアクション」、表 53-2（P.53-6）
- 「Call Home の Configuration アラート グループのイベントとアクション」、表 53-3（P.53-7）
- 「Call Home の Snapshot アラート グループのイベントとアクション」、表 53-4（P.53-7）
- 「Call Home の Environmental アラート グループのイベントとアクション」、表 53-5（P.53-8）
- 「Call Home の Inventory アラート グループのイベントとアクション」、表 53-6（P.53-11）
- 「Call Home の Diagnostic Failure アラート グループのイベントとアクション」、表 53-7（P.53-13）
- 「Call Home の Test アラート グループのイベントとアクション」、表 53-8（P.53-14）

表 53-1　Call Home の Syslog アラート グループのイベントとアクション

アラート グループの説明：	syslog にログ記録されるイベント		
TAC への送信：	No		
実行されるコマンド：	**show logging**、**show inventory**、**show switch virtual**（VSS モードのみ）		
Call Home 起動イベント	**Syslog イベント**	**重大度**	**説明**
SYSLOG	LOG_EMERG	0	システムは使用不能
	LOG_ALERT	1	即時対処が必要
	LOG_CRIT	2	クリティカルな状態
	LOG_ERR	3	エラー
	LOG_WARNING	4	警告
	LOG_NOTICE	5	正常だが重大な状態
	LOG_INFO	6	情報
	LOG_DEBUG	7	デバッグレベル メッセージ

表 53-2　Call Home の Crash アラート グループのイベントとアクション

TAC への送信：	Yes		
Call Home 起動イベント	**Syslog イベント**	**重大度**	**説明と実行されるコマンド：**
SYSTEM_CRASH	—	—	システム クラッシュに関連するイベント。 **show version** **show logging** **show region** **show inventory** **show stack** **show switch virtual**（VSS モードのみ） **more crashinfo**（このコマンドは、crashinfo ファイルの内容を表示します）
MODULE_CRASH	—	—	システム クラッシュに関連するイベント。 **show version** **show logging** **show region** **show stack** **show switch virtual**（VSS モードのみ） **more crashinfo**（このコマンドは、crashinfo ファイルの内容を表示します）
TRACEBACK	—	—	ソフトウェアのトレース バック イベントを検出します。 **show version** **show logging** **show region** **show stack** **show switch virtual**（VSS モードのみ）

表 53-3　Call Home の Configuration アラート グループのイベントとアクション

アラート グループの説明：	設定または設定変更イベントのユーザ生成の要求		
TAC への送信：	Yes		
実行されるコマンド：	**show module**、**show version**、**show running-config all**、**show startup-config**、**show inventory**、**show switch virtual**（VSS モードのみ）		
Call Home 起動イベント	**Syslog イベント**	**重大度**	**説明**
—	—	—	—

表 53-4　Call Home の Snapshot アラート グループのイベントとアクション

アラート グループの説明：	ユーザ設定のコマンド リストからの出力。		
TAC への送信：	Yes		
実行されるコマンド：	Snapshot アラート グループ コンフィギュレーション モードで設定された IOS コマンド。		
Call Home 起動イベント	**Syslog イベント**	**重大度**	**説明**
—	—	—	—

表 53-5　Call Home の Environmental アラート グループのイベントとアクション

アラート グループの説明：	電源、ファン、温度アラームのような環境感知要素に関連するイベント		
TAC への送信：	Yes		
実行されるコマンド：	**show module**、**show environment**、**show logging**、**show inventory**、**show power**		
Call Home 起動イベント	**Syslog イベント**	**重大度**	**説明**
FAN_FAILURE	FANPSINCOMPAT	4	ファン トレイと電源モジュール %d に互換性がない
	ALARMCLR	4	指定されたアラーム条件がクリアされ、シャットダウンがキャンセルされた。
	FANHIOUTPUT	4	バージョン %d 高出力ファン トレイが有効である
	FANLOOUTPUT	4	バージョン %d 低出力ファン トレイが有効である
	FANVERCHK	4	挿入されている電源モジュール %d はバージョン %d ファン トレイとだけ互換性がある。
	FANTRAYFAILED	4	ファン トレイに障害が発生した
	FANTRAYOK	4	ファン トレイは正常である
	FANCOUNTFAILED	4	必要な数のファン トレイがない
	FANCOUNTOK	4	必要な数のファン トレイがある
	PSFANFAIL	4	電源モジュールのファンに障害が発生した
	PSFANOK	4	電源モジュールのファンは正常である
TEMPERATURE_ALARM	MAJORTEMPALARM	2	可能な動作温度範囲を超えている。
	MAJORTEMPALARMRECOVER	4	可能な動作温度範囲に戻った。
	MINORTEMPALARM	4	正常な動作温度範囲を超えている。
	MINORTEMPALARMRECOVER	4	正常な動作温度範囲に戻った。
VTT_FAILED	VTTFAILED	4	VTT %d に障害が発生した。
	VTTOK	4	VTT %d は動作可能である。
	VTTMAJFAILED	0	システムの動作を続行するには VTT の障害が多すぎる。
	VTTMAJRECOVERED	2	システムの動作を続行するために十分な VTT が動作している。

表 53-5　Call Home の Environmental アラート グループのイベントとアクション （続き）

アラート グループの説明：	電源、ファン、温度アラームのような環境感知要素に関連するイベント		
TAC への送信：	Yes		
実行されるコマンド：	**show module**、**show environment**、**show logging**、**show inventory**、**show power**		
Call Home 起動イベント	**Syslog イベント**	**重大度**	**説明**
CLOCK_FAILED	CLOCKFAILED	4	クロックに障害が発生した
	CLOCKOK	4	クロックは動作可能である
	CLOCKMAJFAILED	0	システムの動作を続行するにはクロックの障害が多すぎる
	CLOCKMAJRECOVERED	2	システムの動作を続行するために十分なクロックが動作している
	SHUTDOWN-SCHEDULED	2	%d 秒以内に %s のシャットダウンがスケジュールされている
	SHUTDOWN_NOT_SCHEDULED	2	%s の重大なセンサー アラームは無視され、%s はシャット ダウンされない
	SHUTDOWN-CANCELLED	2	シャットダウンがキャンセルされた
	SHUTDOWN	2	%s により %s をただちにシャットダウンする
	SHUTDOWN-DISABLED	1	%s をただちにシャット ダウンする必要があるが、シャットダウン処理がディセーブルになっている。
	RESET_SCHEDULED	2	数秒内にシステムのリセットがスケジュールされている
	CLOCK_SWITCHOVER	2	システム スイッチング クロックの変更
	CLOCK_A_MISSING	4	システム内でクロック A が検出できない
	CLOCK_B_MISSING	4	システム内でクロック B が検出できない
	USE_RED_CLOCK	4	システムは冗長クロック（クロック B）を使用している。
	ENABLED	4	スロット %d のモジュールへの電源がオンに設定されている
	DISABLED	4	スロット %d のモジュールへの電源が %s に設定されている
	PSOK	4	電源モジュール %d がオンになった。

表 53-5　Call Home の Environmental アラート グループのイベントとアクション （続き）

アラート グループの説明：	電源、ファン、温度アラームのような環境感知要素に関連するイベント		
TAC への送信：	Yes		
実行されるコマンド：	**show module**、**show environment**、**show logging**、**show inventory**、**show power**		
Call Home 起動イベント	**Syslog イベント**	**重大度**	**説明**
POWER_SUPPLY_FAILURE	PSFAIL	4	電源モジュール %d の出力に障害が発生した。
	PSREDUNDANTMODE	4	電源モジュールは冗長モードに設定されている。
	PSCOMBINEDMODE	4	電源モジュールは連結モードに設定されている。
	PSREDUNDANTMISMATCH	4	電源モジュールのレート出力が一致しない。
	PSMISMATCH	4	電源モジュールのレート出力が一致しない。
	PSNOREDUNDANCY	4	電源モジュールの冗長性が完全ではない。電源の使用量が供給容量の下限を超えた
	PSOCPSHUTDOWN	2	電源の使用量が電源モジュール %d の許容量を超えた。
	PSREDUNDANTONESUPPLY	4	電源冗長モードで、システムは 1 つの電源モジュールで動作している
	PSREDUNDANTBOTHSUPPLY	4	電源冗長モードで、システムは両方の電源モジュールで動作している
	UNDERPOWERED	4	システム内のすべての FRU を動作させるには電力が不十分である。
	COULDNOTREPOWER	4	FRU（スロット %d）に電力を再供給したかったが、できなかった。
	POWERDENIED	4	電力が不十分。スロット %d のモジュールに電力が供給できない。
	UNSUPPORTED	4	スロット %d のモジュールはサポートされておらず、電力が供給できない：%s。
	INSUFFICIENTPOWER	2	重要なすべてのカードを動作させるのに十分な電力がないため、ラインカードすべての電源を切断する
	INPUTCHANGE	4	電源モジュール %d の入力が変更された。電力容量が %sW に調整された
	PSINPUTDROP	4	電源モジュール %d の入力がドロップされた

表 53-6　Call Home の Inventory アラート グループのイベントとアクション

アラート グループの説明：	Inventory ステータスは、ユニットがコールド ブートされた場合や、FRU が挿入または取り外された場合に指定される。これは、重大ではないイベントと見なされ、情報はステータスと権限付与に使用される。		
TAC への送信：	Yes		
実行されるコマンド：	匿名モードで送信されるすべてのインベントリ メッセージとフル登録モードで送信されるデルタ インベントリ メッセージに対して実行されるコマンド： **show module**、**show version**、**show inventory oid**、**show idprom all**、**show power**、**show ip traffic**、**show switch virtual**（VSS モードのみ） フル登録モードで送信されるフル インベントリ メッセージに対して実行されるコマンド： **show module**、**show version**、**show inventory oid**、**show idprom all**、**show power**、**show interfaces**、**show file systems**、**show data-corruption**、**show memory statistics**、**show process memory**、**show process cpu**、**show process cpu history**、**show crypto engine configuration**、**show buffers**、**show ip nat statistics**、**show ip traffic**、**show switch virtual**（VSS モードのみ）		
Call Home 起動イベント	**Syslog イベント**	**重大度**	**説明**
HARDWARE_INSERTION	INSPS	6	電源モジュールがスロット %d に挿入された
HARDWARE_REMOVAL	REMPS	6	電源モジュールがスロット %d から取り外された
	REMCARD	6	カードがスロット %d から取り外され、インターフェイスがディセーブルになった
	STDBY_REMCARD	6	スタンバイ スーパーバイザの OIR 機能が、アクティブによって、スロット [n] からプロセッサが取り外されたと通知された
HARDWARE_INSERTION	INSCAR	6	カードがスロット %d に挿入され、インターフェイスがオンラインになった
	STDBY_INSCARD	6	スタンバイが通知された。スロット %d のカードがオンラインになっている
	SEQ_MISMATCH	6	スロット %d のカードの SCP シーケンスが一致しない：%s

表 53-6　Call Home の Inventory アラート グループのイベントとアクション （続き）

アラート グループの説明：	Inventory ステータスは、ユニットがコールド ブートされた場合や、FRU が挿入または取り外された場合に指定される。これは、重大ではないイベントと見なされ、情報はステータスと権限付与に使用される。		
TAC への送信：	Yes		
実行されるコマンド：	匿名モードで送信されるすべてのインベントリ メッセージとフル登録モードで送信されるデルタ インベントリ メッセージに対して実行されるコマンド： **show module**、**show version**、**show inventory oid**、**show idprom all**、**show power**、**show ip traffic**、**show switch virtual**（VSS モードのみ） フル登録モードで送信されるフル インベントリ メッセージに対して実行されるコマンド： **show module**、**show version**、**show inventory oid**、**show idprom all**、**show power**、**show interfaces**、**show file systems**、**show data-corruption**、**show memory statistics**、**show process memory**、**show process cpu**、**show process cpu history**、**show crypto engine configuration**、**show buffers**、**show ip nat statistics**、**show ip traffic**、**show switch virtual**（VSS モードのみ）		
Call Home 起動イベント	**Syslog イベント**	**重大度**	**説明**
HARDWARE_REMOVAL	UNKNOWN	3	スロット %d のカードが不明。カードはディセーブルになる
	STDBY_UNKNOWN	3	スタンバイが通知された。スロット %d のカードが不明
	UNSUPPORTED	3	スロット %d のカードはサポートされていない。%s
	PWRCYCLE	3	モジュール %d のカードは電源サイクル中 %s
	STDBY_PWRCYCLE	3	スタンバイが通知された。モジュール %d のカードは電源サイクル中 %s
	CONSOLE	6	%s プロセッサへのコンソール所有権の変更
	RUNNING_CONFIG	6	スイッチオーバー中に OIR 機能は running-config プロセッサをクリーン アップできない。
	DISALLOW	6	EHSA モードでセカンダリとしてアップさせようとしたスーパーバイザは許可されない
	REMFAN	6	ファン %d が取り外された
HARDWARE_INSERTION	INSFAN	6	ファン %d が挿入された
	PSINSERTED	4	電源モジュールがスロット %d に挿入された。

表 53-7　Call Home の Diagnostic Failure アラート グループのイベントとアクション

アラート グループの説明：	標準またはインテリジェント ラインカードに関連するイベント	
TAC への送信：	Yes	
実行されるコマンド：	**show module**、**show diagnostic result Module <#> detail**、**show version**、**show inventory**、**show buffers**、**show logging**、**show diagnostic result module all**、**show logging system last 100**	
Call Home 起動イベント：	DIAGNOSTICS_FAILURE	
Syslog イベント	**重大度**	**説明**
C2PLUSWITHNODB	2	スロット %d のコンステレーション 2 プラス モジュールにはフォワーディング ドーター ボードがない。電力が供給できない。
DFCMISMATCH	2	モジュール %d DFC はスーパーバイザ DFC と互換性がない。電力が供給できない。
BADFLOWCTRL	2	モジュール %d は DFC をサポートするのに適切なハードウェア リビジョン レベルではない。電力が供給できない。
BADFLOWCTRL_WARN	2	警告：モジュール %d は DFC3 をサポートするのに適切なハードウェア リビジョン レベルではない
BADPINN1	2	モジュール %d は、システムと共存するのに適切なハードウェア リビジョン レベルではない。電力が供給できない。
FANUPGREQ	2	ファンをアップグレードしなければ、モジュール %d はサポートされない
INSUFFCOO	4	モジュール %d は適切に冷却できない
PROVISION	6	モジュール %d はプロビジョニング要件を満たしていない。電力が供給できない
PWRFAILURE	6	電源コンバータの障害により、モジュール %d はディセーブルになる
LC_FAILURE	3	モジュール %d には重大なオンライン診断障害、%s がある
HARD_RESET	3	スイッチオーバー エラー回復の一環としてモジュール %d はハード リセットされる
SOFT_RESET	3	スイッチオーバー エラー回復の一環としてモジュール %d はソフト リセットされる
DOWNGRADE	6	ファブリック対応モジュール %d は適切なハードウェア リビジョン レベルではなく、フロースルー モードでしか実行できない
DIAG_OK		
DIAG_BYPASS		
DIAG_ERROR		
DIAG_MINOR_ERROR		
DIAG_MAJOR_ERROR		
DIAG_LINE_CARD_NOT_PRESENT		
DIAG_LINE_CARD_REMOVED		
DIAG_INVALID_TEST_ID_RANGE		
DIAG_INVALID_PORT_RANGE		
DIAG_IS_BUSY		

表 53-7　Call Home の Diagnostic Failure アラート グループのイベントとアクション （続き）

アラート グループの説明：	標準またはインテリジェント ラインカードに関連するイベント	
TAC への送信：	Yes	
実行されるコマンド：	**show module**、**show diagnostic result Module <#> detail**、**show version**、**show inventory**、**show buffers**、**show logging**、**show diagnostic result module all**、**show logging system last 100**	
Call Home 起動イベント：	DIAGNOSTICS_FAILURE	
Syslog イベント	**重大度**	**説明**
DIAG_IS_IDLE		
DIAG_NO_SCHEDULE		
DIAG_SCHEDULE_EXIST		
DIAG_NO_TEST		
DIAG_UNKNOWN		
DIAG_NOT_AVAILABLE		
DIAG_EXIT_ON_ERROR		
DIAG_EXIT_ON_FAIL_LIMIT_REACHED		
DIAG_INVALID_SCHEDULE		
DIAG_PF_DIAG_NOT_SUPORTED		
DIAG_IS_STOPPED		
DIAG_INVALID_DEVICE_RANGE		

表 53-8　Call Home の Test アラート グループのイベントとアクション

アラート グループの説明：	—	
TAC への送信：	Yes	
実行されるコマンド：	**show version**、**show module**、**show inventory**	
Call Home 起動イベント：	—	
Syslog イベント	**重大度**	**説明**
TEST	2	ユーザが作成したテスト メッセージ

メッセージの内容

次の表に、アラート グループ メッセージの内容の形式を示します。

- 表 53-9 では、ショート テキスト メッセージの内容フィールドについて説明しています。
- 表 53-10 では、ロング テキスト メッセージと XML メッセージすべてに共通の内容フィールドについて説明しています。特定のアラート グループ メッセージに固有のフィールドは、共通フィールドの後に挿入されています。
- 表 53-11 に、リアクティブ メッセージ（TAC ケースが必要なシステム障害）およびプロアクティブ メッセージ（システム パフォーマンスの低下を招くことがある問題）の内容フィールドを示します。
- 表 53-12 に、インベントリ メッセージの内容フィールドを示します。

表 53-9　ショート テキスト メッセージの形式

データ項目	説明
Device identification	設定されたデバイス名
Date/time stamp	起動イベントのタイム スタンプ
Error isolation message	起動イベントの簡単な説明（英語）
Alarm urgency level	システム メッセージに適用されるようなエラー レベル

表 53-10　ロング テキスト メッセージと XML メッセージすべてに共通のフィールド

データ項目（プレーン テキストと XML）	説明（プレーン テキストと XML）	XML タグ（XML のみ）
Time stamp	ISO 時刻通知でのイベントの日付/タイム スタンプ *YYYY-MM-DDTHH:MM:SS*	CallHome/EventTime
Message name	メッセージの名前。特定のイベント名は 「アラート グループの起動イベントとコマンド」（P.53-5）に記載。	（ショート テキスト メッセージのみ）
Message type	具体的に Call Home。	CallHome/Event/Type
Message subtype	特定のタイプのメッセージ、full、delta、または test。	CallHome/Event/SubType
Message group	具体的に reactive または proactive。	（ロング テキスト メッセージのみ）
Severity level	メッセージの重大度（表 53-13（P.53-36）を参照）。	Body/Block/Severity
Source ID	ルーティングのための製品タイプ。具体的に Catalyst 6500。	（ロング テキスト メッセージのみ）

表 53-10　ロング テキスト メッセージと XML メッセージすべてに共通のフィールド （続き）

データ項目（プレーン テキストと XML）	説明（プレーン テキストと XML）	XML タグ（XML のみ）
Device ID	メッセージを生成するエンド デバイスの Unique Device Identifier（UDI）。メッセージがファブリック スイッチに固有でない場合、このフィールドは空白。形式は、*type*@*Sid*@*serial*。 • *type* は、バックプレーン IDPROM からの製品の型番。 • @ は区切り文字。 • *Sid* は、シャーシのシリアル番号としてシリアル ID を特定する C。 • *serial* は、[Sid] フィールドによって特定される数字。 例：WS-C6509@C@12345678	CallHome/CustomerData/ContractData/DeviceId
Customer ID	サポート サービスによって契約情報やその他の ID に使用されるオプションのユーザ設定可能なフィールド。	CallHome/CustomerData/ContractData/CustomerId
Contract ID	サポート サービスによって契約情報やその他の ID に使用されるオプションのユーザ設定可能なフィールド。	CallHome/CustomerData/ContractData/ContractId
Site ID	シスコが提供したサイト ID または別のサポート サービスにとって意味のあるその他のデータに使用されるオプションのユーザ設定可能なフィールド。	CallHome/CustomerData/ContractData/SiteId
Server ID	メッセージがファブリック スイッチから生成されている場合、これはスイッチの固有のデバイス ID（UDI）。 形式は、*type*@*Sid*@*serial*。 • *type* は、バックプレーン IDPROM からの製品の型番。 • @ は区切り文字。 • *Sid* は、シャーシのシリアル番号としてシリアル ID を特定する C。 • *serial* は、[Sid] フィールドによって特定される数字。 例：WS-C6509@C@12345678	(ロング テキスト メッセージのみ)
Message description	エラーを説明する短い文章。	CallHome/MessageDescription
Device name	イベントが発生するノード。これは、デバイスのホスト名。	CallHome/CustomerData/SystemInfo/Name
Contact name	イベントの発生するノードに関連する問題を連絡する人物の名前。	CallHome/CustomerData/SystemInfo/Contact

表 53-10　ロング テキスト メッセージと XML メッセージすべてに共通のフィールド （続き）

データ項目（プレーン テキストと XML）	説明（プレーン テキストと XML）	XML タグ（XML のみ）
Contact email	このユニットの連絡先として識別される担当者の電子メールアドレス。	CallHome/CustomerData/SystemInfo/ContactEmail
Contact phone number	このユニットの連絡先である人物の電話番号。	CallHome/CustomerData/SystemInfo/ContactPhoneNumber
Street address	このユニットに関連付けられた RMA 部品出荷の住所を含むオプションのフィールド。	CallHome/CustomerData/SystemInfo/StreetAddress
Model name	スイッチのモデル名。これは、製品ファミリ名の一部として固有のモデル。	CallHome/Device/Cisco_Chassis/Model
Serial number	ユニットのシャーシのシリアル番号。	CallHome/Device/Cisco_Chassis/SerialNumber
Chassis part number	シャーシの最上アセンブリ番号。	CallHome/Device/Cisco_Chassis/AdditionalInformation/AD@name="PartNumber"/
System Object ID	システムを一意に識別するシステム オブジェクト ID。	CallHome/Device/Cisco_Chassis/AdditionalInformation/AD@name="sysObjectID"
SysDesc	管理対象デバイスのシステム説明。	CallHome/Device/Cisco_Chassis/AdditionalInformation/AD@name="sysDescr"
このアラート グループに対して複数の CLI コマンドが実行されると、次のフィールドが繰り返される場合があります。		
Command output name	発行される CLI コマンドの正確な名前。	/aml/Attachments/Attachment/Name
Attachment type	タイプ（通常はインライン）。	/aml/Attachments/Attachment@type
MIME type	通常はテキスト/プレーンまたは符号化タイプ。	/aml/attachments/attachment/Data@encoding
Command output text	自動的に実行されたコマンドの出力（「アラート グループの起動イベントとコマンド」（P.53-5）を参照）	/aml/attachments/attachment/atdata

表 53-11　リアクティブまたはプロアクティブ イベント メッセージのフィールド

データ項目（プレーン テキストと XML）	説明（プレーン テキストと XML）	XML タグ（XML のみ）
Chassis hardware version	シャーシのハードウェア バージョン。	CallHome/Device/Cisco_Chassis/HardwareVersion
Supervisor module software version	最上レベルのソフトウェア バージョン。	CallHome/Device/Cisco_Chassis/AdditionalInformation/AD@name="SoftwareVersion"
Affected FRU name	イベント メッセージを生成する、影響のある FRU の名前。	CallHome/Device/Cisco_Chassis/Cisco_Card/Model
Affected FRU serial number	問題を起こした FRU のシリアル番号。	CallHome/Device/Cisco_Chassis/Cisco_Card/SerialNumber

表 53-11　リアクティブまたはプロアクティブ イベント メッセージのフィールド （続き）

データ項目（プレーン テキストと XML）	説明（プレーン テキストと XML）	XML タグ（XML のみ）
Affected FRU part number	問題を起こした FRU の部品番号。	CallHome/Device/Cisco_Chassis/Cisco_Card/PartNumber
FRU slot	イベント メッセージを生成している FRU のスロット番号。	CallHome/Device/Cisco_Chassis/Cisco_Card/LocationWithinContainer
FRU hardware version	問題を起こした FRU のハードウェア バージョン。	CallHome/Device/Cisco_Chassis/Cisco_Card/HardwareVersion
FRU software version	問題を起こした FRU で動作するソフトウェア バージョン。	CallHome/Device/Cisco_Chassis/Cisco_Card/SoftwareIdentity/VersionString
Process name	プロセスの名前。	/aml/body/process/name
Process ID	固有のプロセス ID。	/aml/body/process/id
Process state	プロセスの状態（実行中、中止など）。	/aml/body/process/processState
Process exception	原因コードの例外。	/aml/body/process/exception

表 53-12　Inventory イベント メッセージのフィールド

データ項目（プレーン テキストと XML）	説明（プレーン テキストと XML）	XML タグ（XML のみ）
Chassis hardware version	シャーシのハードウェア バージョン。	CallHome/Device/Cisco_Chassis/HardwareVersion
Supervisor module software version	最上レベルのソフトウェア バージョン。	CallHome/Device/Cisco_Chassis/AdditionalInformation/AD@name="Software Version"
FRU name	イベント メッセージを生成する、影響のある FRU の名前。	CallHome/Device/Cisco_Chassis/Cisco_Card/Model
FRU s/n	FRU のシリアル番号。	CallHome/Device/Cisco_Chassis/Cisco_Card/SerialNumber
FRU part number	FRU の部品番号。	CallHome/Device/Cisco_Chassis/Cisco_Card/PartNumber
FRU slot	FRU のスロット番号。	CallHome/Device/Cisco_Chassis/Cisco_Card/LocationWithinContainer
FRU hardware version	FRU のハードウェア バージョン。	CallHome/Device/Cisco_Chassis/Cisco_Card/HardwareVersion
FRU software version	FRU で動作するソフトウェア バージョン。	CallHome/Device/Cisco_Chassis/Cisco_Card/SoftwareIdentity/VersionString

ロング テキスト形式の Syslog アラート通知の例

```
source:MDS9000
Switch Priority:7
Device Id:WS-C6509@C@FG@07120011
Customer Id:Example.com
Contract Id:123
Site Id:San Jose
Server Id:WS-C6509@C@FG@07120011
Time of Event:2004-10-08T11:10:44
Message Name:SYSLOG_ALERT
Message Type:Syslog
Severity Level:2
System Name:10.76.100.177
Contact Name:User Name
Contact Email:admin@yourcompany.com
Contact Phone:+1 408 555-1212
Street Address:#1234 Picaboo Street, Any city, Any state, 12345
Event Description:2006 Oct  8 11:10:44 10.76.100.177 %PORT-5-IF_TRUNK_UP: %$VSAN 1%$
Interface fc2/5, vsan 1 is up

syslog_facility:PORT
start chassis information:
Affected Chassis:WS-C6509
Affected Chassis Serial Number:FG@07120011
Affected Chassis Hardware Version:0.104
Affected Chassis Software Version:3.1(1)
Affected Chassis Part No:73-8607-01
end chassis information:
```

XML 形式の Syslog アラート通知の例

```
From: example
Sent: Wednesday, April 25, 2007 7:20 AM
To: User (user)
Subject: System Notification From Router - syslog - 2007-04-25 14:19:55
GMT+00:00

<?xml version="1.0" encoding="UTF-8"?>
<soap-env:Envelope xmlns:soap-env="http://www.w3.org/2003/05/soap-envelope">
<soap-env:Header>
<aml-session:Session xmlns:aml-session="http://www.example.com/2004/01/aml-session"
soap-env:mustUnderstand="true"
soap-env:role="http://www.w3.org/2003/05/soap-envelope/role/next">
<aml-session:To>http://tools.example.com/services/DDCEService</aml-session:To>
<aml-session:Path>
<aml-session:Via>http://www.example.com/appliance/uri</aml-session:Via>
</aml-session:Path>
<aml-session:From>http://www.example.com/appliance/uri</aml-session:From>
<aml-session:MessageId>M2:69000101:C9D9E20B</aml-session:MessageId>
</aml-session:Session>
</soap-env:Header>
<soap-env:Body>
<aml-block:Block xmlns:aml-block="http://www.example.com/2004/01/aml-block">
<aml-block:Header>
<aml-block:Type>http://www.example.com/2005/05/callhome/syslog</aml-block:Type>
<aml-block:CreationDate>2007-04-25 14:19:55 GMT+00:00</aml-block:CreationDate>
<aml-block:Builder>
<aml-block:Name>Cat6500</aml-block:Name>
<aml-block:Version>2.0</aml-block:Version>
</aml-block:Builder>
```

```
<aml-block:BlockGroup>
<aml-block:GroupId>G3:69000101:C9F9E20C</aml-block:GroupId>
<aml-block:Number>0</aml-block:Number>
<aml-block:IsLast>true</aml-block:IsLast>
<aml-block:IsPrimary>true</aml-block:IsPrimary>
<aml-block:WaitForPrimary>false</aml-block:WaitForPrimary>
</aml-block:BlockGroup>
<aml-block:Severity>2</aml-block:Severity>
</aml-block:Header>
<aml-block:Content>
<ch:CallHome xmlns:ch="http://www.example.com/2005/05/callhome" version="1.0">
<ch:EventTime>2007-04-25 14:19:55 GMT+00:00</ch:EventTime>
<ch:MessageDescription>03:29:29: %CLEAR-5-COUNTERS: Clear counter on all interfaces by
console</ch:MessageDescription>
<ch:Event>
<ch:Type>syslog</ch:Type>
<ch:SubType></ch:SubType>
<ch:Brand>Cisco Systems</ch:Brand>
<ch:Series>Catalyst 6500 Series Switches</ch:Series>
</ch:Event>
<ch:CustomerData>
<ch:UserData>
<ch:Email>user@example.com</ch:Email>
</ch:UserData>
<ch:ContractData>
<ch:CustomerId>12345</ch:CustomerId>
<ch:SiteId>building 1</ch:SiteId>
<ch:ContractId>abcdefg12345</ch:ContractId>
<ch:DeviceId>WS-C6509@C@69000101</ch:DeviceId>
</ch:ContractData>
<ch:SystemInfo>
<ch:Name>Router</ch:Name>
<ch:Contact></ch:Contact>
<ch:ContactEmail>user@example.com</ch:ContactEmail>
<ch:ContactPhoneNumber>+1 408 555-1212</ch:ContactPhoneNumber>
<ch:StreetAddress>270 E. Tasman Drive, San Jose, CA</ch:StreetAddress>
</ch:SystemInfo>
</ch:CustomerData>
<ch:Device>
<rme:Chassis xmlns:rme="http://www.example.com/rme/4.0">
<rme:Model>WS-C6509</rme:Model>
<rme:HardwareVersion>1.0</rme:HardwareVersion>
<rme:SerialNumber>69000101</rme:SerialNumber>
<rme:AdditionalInformation>
<rme:AD name="PartNumber" value="73-3438-03 01" />
<rme:AD name="SoftwareVersion" value="12.2(20070421:012711)" />
</rme:AdditionalInformation>
</rme:Chassis>
</ch:Device>
</ch:CallHome>
</aml-block:Content>
<aml-block:Attachments>
<aml-block:Attachment type="inline">
<aml-block:Name>show logging</aml-block:Name>
<aml-block:Data encoding="plain">
<![CDATA[
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited, 0 flushes, 0
overruns, xml disabled, filtering disabled)
    Console logging: level debugging, 53 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging: level debugging, 53 messages logged, xml disabled,
                    filtering disabled
```

```
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    Trap logging: level informational, 72 message lines logged

Log Buffer (8192 bytes):

00:00:54: curr is 0x20000

00:00:54: RP: Currently running ROMMON from F2 region
00:01:05: %SYS-5-CONFIG_I: Configured from memory by console
00:01:09: %SYS-5-RESTART: System restarted --
Cisco IOS Software, s72033_rp Software (s72033_rp-ADVENTERPRISEK9_DBG-VM), Experimental
Version 12.2(20070421:012711)
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 26-Apr-07 15:54 by xxx

Firmware compiled 11-Apr-07 03:34 by integ Build [100]


00:01:01: %PFREDUN-6-ACTIVE: Initializing as ACTIVE processor for this switch

00:01:01: %SYS-3-LOGGER_FLUSHED: System was paused for 00:00:00 to ensure console
debugging output.

00:03:00: SP: SP: Currently running ROMMON from F1 region
00:03:07: %C6K_PLATFORM-SP-4-CONFREG_BREAK_ENABLED: The default factory setting for config
register is 0x2102.It is advisable to retain 1 in 0x2102 as it prevents returning to
ROMMON when break is issued.

00:03:18: %SYS-SP-5-RESTART: System restarted --
Cisco IOS Software, s72033_sp Software (s72033_sp-ADVENTERPRISEK9_DBG-VM), Experimental
Version 12.2(20070421:012711)
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 26-Apr-07 18:00 by xxx
00:03:18: %SYS-SP-6-BOOTTIME: Time taken to reboot after reload =  339 seconds
00:03:18: %OIR-SP-6-INSPS: Power supply inserted in slot 1
00:03:18: %C6KPWR-SP-4-PSOK: power supply 1 turned on.
00:03:18: %OIR-SP-6-INSPS: Power supply inserted in slot 2
00:01:09: %SSH-5-ENABLED: SSH 1.99 has been enabled
00:03:18: %C6KPWR-SP-4-PSOK: power supply 2 turned on.
00:03:18: %C6KPWR-SP-4-PSREDUNDANTMISMATCH: power supplies rated outputs do not match.
00:03:18: %C6KPWR-SP-4-PSREDUNDANTBOTHSUPPLY: in power-redundancy mode, system is
operating on both power supplies.
00:01:10: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
00:01:10: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
00:03:20: %C6KENV-SP-4-FANHIOUTPUT: Version 2 high-output fan-tray is in effect
00:03:22: %C6KPWR-SP-4-PSNOREDUNDANCY: Power supplies are not in full redundancy, power
usage exceeds lower capacity supply
00:03:26: %FABRIC-SP-5-FABRIC_MODULE_ACTIVE: The Switch Fabric Module in slot 6 became
active.
00:03:28: %DIAG-SP-6-RUN_MINIMUM: Module 6: Running Minimal Diagnostics...
00:03:50: %DIAG-SP-6-DIAG_OK: Module 6: Passed Online Diagnostics
00:03:50: %OIR-SP-6-INSCARD: Card inserted in slot 6, interfaces are now online
00:03:51: %DIAG-SP-6-RUN_MINIMUM: Module 3: Running Minimal Diagnostics...
00:03:51: %DIAG-SP-6-RUN_MINIMUM: Module 7: Running Minimal Diagnostics...
00:03:51: %DIAG-SP-6-RUN_MINIMUM: Module 9: Running Minimal Diagnostics...
00:01:51: %MFIB_CONST_RP-6-REPLICATION_MODE_CHANGE: Replication Mode Change Detected.
Current system replication mode is Ingress
00:04:01: %DIAG-SP-6-DIAG_OK: Module 3: Passed Online Diagnostics
00:04:01: %OIR-SP-6-DOWNGRADE: Fabric capable module 3 not at an appropriate hardware
revision level, and can only run in flowthrough mode
00:04:02: %OIR-SP-6-INSCARD: Card inserted in slot 3, interfaces are now online
00:04:11: %DIAG-SP-6-DIAG_OK: Module 7: Passed Online Diagnostics
00:04:14: %OIR-SP-6-INSCARD: Card inserted in slot 7, interfaces are now online
```

```
00:04:35: %DIAG-SP-6-DIAG_OK: Module 9: Passed Online Diagnostics
00:04:37: %OIR-SP-6-INSCARD: Card inserted in slot 9, interfaces are now online
00:00:09: DaughterBoard (Distributed Forwarding Card 3)

Firmware compiled 11-Apr-07 03:34 by integ Build [100]


00:00:22: %SYS-DFC4-5-RESTART: System restarted --
Cisco IOS Software, c6lc2 Software (c6lc2-SPDBG-VM), Experimental Version
12.2(20070421:012711)
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 26-Apr-07 17:20 by xxx
00:00:23: DFC4: Currently running ROMMON from F2 region
00:00:25: %SYS-DFC2-5-RESTART: System restarted --
Cisco IOS Software, c6slc Software (c6slc-SPDBG-VM), Experimental Version
12.2(20070421:012711)
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 26-Apr-07 16:40 by username1
00:00:26: DFC2: Currently running ROMMON from F2 region
00:04:56: %DIAG-SP-6-RUN_MINIMUM: Module 4: Running Minimal Diagnostics...
00:00:09: DaughterBoard (Distributed Forwarding Card 3)

Firmware compiled 11-Apr-07 03:34 by integ Build [100]

slot_id is 8

00:00:31: %FLASHFS_HES-DFC8-3-BADCARD: /bootflash:: The flash card seems to be corrupted
00:00:31: %SYS-DFC8-5-RESTART: System restarted --
Cisco IOS Software, c6lc2 Software (c6lc2-SPDBG-VM), Experimental Version
12.2(20070421:012711)
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 26-Apr-07 17:20 by username1
00:00:31: DFC8: Currently running ROMMON from S (Gold) region
00:04:59: %DIAG-SP-6-RUN_MINIMUM: Module 2: Running Minimal Diagnostics...
00:05:12: %DIAG-SP-6-RUN_MINIMUM: Module 8: Running Minimal Diagnostics...
00:05:13: %DIAG-SP-6-RUN_MINIMUM: Module 1: Running Minimal Diagnostics...
00:00:24: %SYS-DFC1-5-RESTART: System restarted --
Cisco IOS Software, c6slc Software (c6slc-SPDBG-VM), Experimental Version
12.2(20070421:012711)
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 26-Apr-07 16:40 by username1
00:00:25: DFC1: Currently running ROMMON from F2 region
00:05:30: %DIAG-SP-6-DIAG_OK: Module 4: Passed Online Diagnostics
00:05:31: %SPAN-SP-6-SPAN_EGRESS_REPLICATION_MODE_CHANGE: Span Egress HW Replication Mode
Change Detected. Current replication mode for unused asic session 0 is Centralized
00:05:31: %SPAN-SP-6-SPAN_EGRESS_REPLICATION_MODE_CHANGE: Span Egress HW Replication Mode
Change Detected. Current replication mode for unused asic session 1 is Centralized
00:05:31: %OIR-SP-6-INSCARD: Card inserted in slot 4, interfaces are now online
00:06:02: %DIAG-SP-6-DIAG_OK: Module 1: Passed Online Diagnostics
00:06:03: %OIR-SP-6-INSCARD: Card inserted in slot 1, interfaces are now online
00:06:31: %DIAG-SP-6-DIAG_OK: Module 2: Passed Online Diagnostics
00:06:33: %OIR-SP-6-INSCARD: Card inserted in slot 2, interfaces are now online
00:04:30: %XDR-6-XDRIPCNOTIFY: Message not sent to slot 4/0 (4) because of IPC error
timeout. Disabling linecard. (Expected during linecard OIR)
00:06:59: %DIAG-SP-6-DIAG_OK: Module 8: Passed Online Diagnostics
00:06:59: %OIR-SP-6-DOWNGRADE_EARL: Module 8 DFC installed is not identical to system PFC
and will perform at current system operating mode.
00:07:06: %OIR-SP-6-INSCARD: Card inserted in slot 8, interfaces are now online

Router#]]></aml-block:Data>
</aml-block:Attachment>
</aml-block:Attachments>
</aml-block:Block>
</soap-env:Body>
```

```
</soap-env:Envelope>
```

Call Home のデフォルト設定

- Call Home 機能のステータス：ディセーブル
- ユーザ定義プロファイルのステータス：アクティブ
- 定義済みのシスコ TAC プロファイルのステータス：非アクティブ
- 転送方式：電子メール
- メッセージのフォーマット タイプ：XML
- ロング テキスト、ショート テキスト、または XML 形式で送信されるメッセージの宛先メッセージ サイズ：3,145,728
- アラート グループのステータス：イネーブル
- Call Home メッセージの重大度しきい値：0（デバッグ）
- 1 分間に送信するメッセージのレート制限：20
- AAA 認証：ディセーブル
- Call Home の syslog メッセージ スロットリング：イネーブル
- データ プライバシー レベル：標準

Call Home の設定方法

- 「Call Home の顧客連絡先情報の設定」（P.53-23）
- 「宛先プロファイルの設定」（P.53-24）
- 「アラート グループへの登録」（P.53-33）
- 「Call Home データ プライバシーの設定」（P.53-39）
- 「Call Home のイネーブル化」（P.53-40）
- 「Call Home トラフィック レート制限の設定」（P.53-40）
- 「syslog スロットリングの設定」（P.53-40）
- 「Call Home の通信のテスト」（P.53-41）
- 「Smart Call Home サービスの設定」（P.53-44）

Call Home の顧客連絡先情報の設定

顧客の連絡先情報を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# 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	`Router(config)# call-home`	Call Home 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	`Router(cfg-call-home)# contact-email-addr email-address`	（匿名モードのオプション）顧客の電子メール アドレスを割り当てます。スペースを入れず電子メール アドレス形式で 200 文字まで入力します。
ステップ 4	`Router(cfg-call-home)# phone-number +phone-number`	（任意）顧客の電話番号を割り当てます。 **（注）** 番号はプラス（+）記号で始まり、ダッシュ（-）と数字だけが含まれるようにしてください。最大 16 文字まで入力できます。スペースを入力する場合は、エントリを引用符（""）で囲みます。
ステップ 5	`Router(cfg-call-home)# street-address street-address`	（任意）RMA 機器の配送先である顧客の住所を割り当てます。最大 200 文字まで入力できます。スペースを入力する場合は、エントリを引用符（""）で囲みます。
ステップ 6	`Router(cfg-call-home)# customer-id text`	（任意）カスタマー ID を指定します。最大 64 文字まで入力できます。スペースを入力する場合は、エントリを引用符（""）で囲みます。
ステップ 7	`Router(cfg-call-home)# site-id text`	（任意）カスタマーのサイト ID を指定します。最大 200 文字まで入力できます。スペースを入力する場合は、エントリを引用符（""）で囲みます。
ステップ 8	`Router(cfg-call-home)# contract-id text`	（任意）顧客のスイッチの契約 ID を指定します。最大 64 文字まで入力できます。スペースを入力する場合は、エントリを引用符（""）で囲みます。

次に、連絡先情報の設定例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# call-home
Router(cfg-call-home)# contact-email-addr username@example.com
Router(cfg-call-home)# phone-number +1-800-555-4567
Router(cfg-call-home)# street-address "1234 Picaboo Street, Any city, Any state, 12345"
Router(cfg-call-home)# customer-id Customer1234
Router(cfg-call-home)# site-id Site1ManhattanNY
Router(cfg-call-home)# contract-id Company1234
Router(cfg-call-home)# exit
Router(config)#
```

宛先プロファイルの設定

宛先プロファイルの概要

宛先プロファイルには、アラート通知に必要な送信情報が含まれています。少なくとも 1 つの宛先プロファイルが必要です。1 つまたは複数のタイプの複数の宛先プロファイルを設定できます。

定義済みの宛先プロファイルを使用することも、プロファイルを定義することもできます。新しい宛先プロファイルを定義する場合は、プロファイル名を割り当てる必要があります。

宛先プロファイルには、次の属性を設定できます。

- プロファイル名：ユーザ定義宛先プロファイルを一意に識別する文字列。プロファイル名は 31 文字までで大文字と小文字は区別されません。プロファイル名として **all** は使用できません。
- 転送方法：アラートを送信するための転送メカニズム（電子メールまたは HTTP（HTTPS を含む））。
  - ユーザ定義の宛先プロファイルの場合、電子メールがデフォルトで、どちらかまたは両方の転送メカニズムをイネーブルにできます。両方の方法をディセーブルにすると、電子メールがイネーブルになります。
  - あらかじめ定義された Cisco TAC プロファイルの場合、いずれかの転送メカニズムをイネーブルにできますが、同時にはイネーブルにできません。
- 宛先アドレス：アラートを送信する転送方法に関連した実際のアドレス。
- メッセージ形式：アラートの送信に使用するメッセージ形式。
  - ユーザ定義の宛先プロファイルの場合、形式オプションは、ロング テキスト、ショート テキスト、または XML です。デフォルトは XML です。
  - 定義済みのシスコ TAC プロファイルは XML を使用します。
- メッセージ サイズ：宛先メッセージの最大サイズ。有効な範囲は、50 ～ 3,145,728 バイトで、デフォルトは 3,145,728 バイトです。

（注）
- Call Home 機能は、デフォルトで非アクティブな CiscoTAC-1 という名前の事前に定義されたプロファイルを提供します。CiscoTAC-1 プロファイルは、Smart Call Home サービスで使用することを目的としており、このサービスを Call Home 機能でイネーブルにするための特定の追加設定手順が必要です。このプロファイルの詳細については、「定義済みの CiscoTAC-1 宛先プロファイルの使用」（P.53-32）を参照してください。
- Cisco Smart Call Home サービスを使用する場合、宛先プロファイルは XML メッセージ形式を使用する必要があります。

VRF を使用するように Call Home を設定

Call Home 電子メールまたは HTTP メッセージに VRF インターフェイスを使用するように Call Home を設定するには、次の作業を行います。

	コマンドまたはアクション	目的
ステップ 1	`Router# 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 1	`Router(config)# interface type`	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# ip address ip_address mask`	IP アドレスとサブネット マスクをインターフェイスに割り当てます。

	コマンドまたはアクション	目的
ステップ 3	`Router(config-if)# vrf forwarding call_home_vrf_name`	インターフェイスに *call_home_vrf_name* VRF インスタンスを関連付けます。
ステップ 4	`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。

次に、VRF インターフェイスを使用するように Call Home を設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 1/1
Router(config-if)# ip address 10.10.10.10 0.0.0.0
Router(config-if)# vrf forwarding call_home_vrf
Router(config-if)# exit
Router(config)#
```

電子メール メッセージを送信するように宛先プロファイルを設定

- 「電子メール メッセージに VRF を使用するように Call Home を設定」（P.53-26）（任意）
- 「メール サーバの設定」（P.53-27）（必須）
- 「電子メールの宛先プロファイルの設定」（P.53-27）（必須）

（注）　VRF インターフェイスを介して Call Home 電子メール メッセージを送信するには、VRF を使用するように Call Home を設定します（「VRF を使用するように Call Home を設定」（P.53-25）を参照）。

電子メール メッセージに VRF を使用するように Call Home を設定

Call Home 電子メール メッセージに VRF インスタンスを使用するように Call Home を設定するには、次の作業を行います。

	コマンドまたはアクション	目的
ステップ 1	`Router# 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	`Router(config)# call-home`	Call Home 設定サブモードを開始します。
ステップ 3	`Router(cfg-call-home)# vrf call_home_vrf_name`	Call Home 電子メール メッセージに使用する VRF インスタンスを指定します。

次に、VRF インターフェイスを使用するように Call Home を設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# call-home
Router(cfg-call-home)# vrf call_home_vrf
Router(cfg-call-home)# exit
Router(config)#
```

メール サーバの設定

電子メール メッセージの転送を使用するには、次の作業を行います。

	コマンドまたはアクション	目的
ステップ 1	`Router# 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	`Router(config)# call-home`	Call Home 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	`Router(cfg-call-home)# mail-server {ipv4-address | ipv6-address | name} priority number`	電子メール サーバ、および設定された電子メール サーバ間の相対プライオリティを指定します。それぞれの説明は次のとおりです。 • *ipv4-address*：メール サーバの IPv4 アドレスを指定します。 • *ipv6-address*：メール サーバの IPv6 アドレスを指定します。 • *name*：電子メール サーバの完全修飾ドメイン名（FQDN）を 64 文字以下で指定します。 • *number*：1（最高のプライオリティ）から 100（最低のプライオリティ）の番号を割り当てます。より高いプライオリティ（より小さい数値）が最初に試行されます。 • バックアップ電子メール サーバを定義するために繰り返します。最大で 4 つのバックアップ電子メール サーバ、つまり合計で 5 つの電子メール サーバを設定できます。

次に、プライマリ メール サーバ（「smtp.example.com」という名前）と、IP アドレスが 192.168.0.1 のセカンダリ メール サーバの設定の例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# call-home
Router(cfg-call-home)# mail-server smtp.example.com priority 1
Router(cfg-call-home)# mail-server 192.168.0.1 priority 2
Router(cfg-call-home)# exit
Router(config)#
```

電子メールの宛先プロファイルの設定

電子メール転送の宛先プロファイルを設定するには、次の作業を実行します。

	コマンドまたはアクション	目的
ステップ 1	`Router# 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	`Router(config)# call-home`	Call Home 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	`Router(cfg-call-home)# sender from email-address`	（任意）Call Home 電子メール メッセージの [from] フィールドに表示される電子メール アドレスを割り当てます。アドレスを指定しなかった場合は、連絡先の電子メール アドレスが使用されます。

	コマンドまたはアクション	目的
ステップ 4	`Router(cfg-call-home)# sender reply-to email-address`	（任意）Call Home 電子メール メッセージの [reply-to] フィールドに表示される電子メール アドレスを割り当てます。
ステップ 5	`Router(cfg-call-home)# source-ip-address ip_address`	（任意）Call Home 電子メール メッセージに使用する送信元 IPv4 または IPv6 アドレスを割り当てます。
ステップ 6	`Router(cfg-call-home)# source-interface interface-name`	（任意）Call Home E メール メッセージの宛先となる送信元インターフェイス名を指定します。送信元インターフェイス名または送信元 IP アドレスが指定されていない場合、ルーティング テーブルのインターフェイスが使用されます。
ステップ 7	`Router(config-call-home)# profile name`	指定された宛先プロファイル名の Call Home 宛先プロファイル コンフィギュレーション モードを開始します。指定された宛先プロファイルが存在しない場合、作成されます。
ステップ 8	`Router(cfg-call-home-profile)# destination transport-method email`	電子メールのメッセージ転送方法を設定します。（これはデフォルトです）。
ステップ 9	`Router(cfg-call-home-profile)# destination address email email_address`	Call Home メッセージが送信される宛先電子メール アドレスを設定します。
ステップ 10	`Router(cfg-call-home-profile)# destination preferred-msg-format {long-text | short-text | xml}`	（任意）使用するメッセージ形式を設定します。デフォルトは XML です。
ステップ 11	`Router(cfg-call-home-profile)# destination message-size bytes`	（任意）宛先プロファイルの最大宛先メッセージ サイズ（50 ～ 3145728 バイト）を設定します。デフォルトは 3145728 バイトです。
ステップ 12	`Router(cfg-call-home-profile)# active`	（任意）宛先プロファイルをイネーブルにします。デフォルトでは、ユーザ定義プロファイルは作成時にイネーブルになります。
ステップ 13	`Router(cfg-call-home-profile)# exit`	Call Home 宛先プロファイル コンフィギュレーション モードを終了して、Call Home コンフィギュレーション モードに戻ります。
ステップ 14	`Router(cfg-call-home)# end`	特権 EXEC モードに戻ります。

匿名モード プロファイルの設定

匿名モードのプロファイルを設定するには、次の作業を行います。

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例：** `Router# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	**call-home** **例：** `Router(config)# call-home`	Call Home 設定サブモードに入ります。

	コマンドまたはアクション	目的
ステップ 3	**profile** *name* **例：** `Router(cfg-call-home) profile CiscoTAC-1`	TAC プロファイルを選択し、プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**anonymous-reporting-only** **例：** `Router(cfg-call-home-profile)# anonymous-reporting-only`	TAC プロファイルに対して匿名モードをイネーブルにします。 **（注）** デフォルトでは、CiscoTAC-1 プロファイルはプロファイルに登録されているすべてのイベント タイプが記載された完全なレポートを送信します。**anonymous-reporting-only** が設定されていると、クラッシュ、インベントリ、およびテスト メッセージだけが送信されます。

HTTP プロキシ サーバの設定

Call Home HTTP（S）メッセージの HTTP プロキシ サーバを指定するには、次の作業を行います。

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例：** `Router# 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	**call-home** **例：** `Router(config)# call-home`	Call Home 設定サブモードを開始します。
ステップ 3	**http-proxy** {*ipv4-address* | *ipv6-address* | *name*} **port** *port-number* **例：** `Router(cfg-call-home)# http-proxy 1.1.1.1 port 1`	HTTP 要求のプロキシ サーバを指定します。

HTTP メッセージを送信するように宛先プロファイルを設定

- 「HTTP ソース インターフェイスの設定」（P.53-30）
- 「HTTP の宛先プロファイルの設定」（P.53-30）

HTTP ソース インターフェイスの設定

HTTP クライアント ソース インターフェイスを設定するには、次の作業を行います。

	コマンドまたはアクション	目的
ステップ 1	`Router# 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	`Router(config)# ip http client source-interface` *type number*	HTTP クライアントのソース インターフェイスを設定します。インターフェイスが VRF インスタンスに関連付けられている場合、HTTP メッセージは VRF インスタンスを使用します。

HTTP の宛先プロファイルの設定

HTTP 転送の宛先プロファイルを設定するには、次の作業を行います。

	コマンドまたはアクション	目的
ステップ 1	`Router# 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	`Router(config)# call-home`	Call Home 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	`Router(config-call-home)# profile` *name*	指定された宛先プロファイルの Call Home 宛先プロファイル コンフィギュレーション モードを開始します。指定された宛先プロファイルが存在しない場合、作成されます。
ステップ 4	`Router(cfg-call-home-profile)# destination transport-method http`	HTTP メッセージの転送方法をイネーブルにします。
ステップ 5	`Router(cfg-call-home-profile)# destination address http` *url*	Call Home メッセージが送信される宛先 URL を設定します。 **（注）** 宛先 URL を入力する場合は、サーバがセキュア サーバであるかどうかに応じて **http://** または **https://** を指定します。宛先がセキュア サーバである場合、トラストポイント CA も設定する必要があります。
ステップ 6	`Router(cfg-call-home-profile)# destination preferred-msg-format {long-text | short-text | xml}`	（任意）使用するメッセージ形式を設定します。デフォルトは XML です。
ステップ 7	`Router(cfg-call-home-profile)# destination message-size` *bytes*	（任意）宛先プロファイルの宛先メッセージの最大サイズを設定します。
ステップ 8	`Router(cfg-call-home-profile)# active`	宛先プロファイルをイネーブルにします。デフォルトでは、プロファイルは作成時にイネーブルになります。
ステップ 9	`Router(cfg-call-home-profile)# exit`	Call Home 宛先プロファイル コンフィギュレーション モードを終了して、Call Home コンフィギュレーション モードに戻ります。
ステップ 10	`Router(cfg-call-home)# end`	特権 EXEC モードに戻ります。

次に、HTTP 転送の宛先プロファイルを設定する例を示します。

```
Router# configure terminal
Router(config)# call-home
Router(config-call-home)# profile test
Router(cfg-call-home-profile)# destination transport-method http
Router(cfg-call-home-profile)# destination address http https://example.url.com
```

```
Router(cfg-call-home-profile)# destination preferred-msg-format xml
Router(cfg-call-home-profile)# destination message-size 3,145,728
Router(cfg-call-home-profile)# active
Router(cfg-call-home-profile)# exit
Router(cfg-call-home)# end
```

宛先プロファイル管理

宛先プロファイルのアクティブ化および非アクティブ化

定義済み CiscoTAC-1 プロファイルを除き、すべての Call Home 宛先プロファイルが作成時に自動的にアクティブになります。プロファイルをすぐに使用しない場合は、そのプロファイルを非アクティブ化できます。CiscoTAC-1 プロファイルは、デフォルトで非アクティブとなっており、使用するにはアクティブにする必要があります。

宛先プロファイルをアクティブ化または非アクティブ化するには、次の作業を行います。

	コマンドまたはアクション	目的
ステップ 1	`Router# 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	`Router(config)# call-home`	Call Home 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	`Router(config-call-home)# profile` *name*	指定された宛先プロファイルの Call Home 宛先プロファイル コンフィギュレーション モードを開始します。指定された宛先プロファイルが存在しない場合、作成されます。
ステップ 4	`Router(cfg-call-home-profile)# active`	宛先プロファイルをイネーブルにします。デフォルトでは、新しいプロファイルは作成時にイネーブルになります。
ステップ 5	`Router(cfg-call-home-profile)# no active`	宛先プロファイルをディセーブルにします。
ステップ 6	`Router(cfg-call-home)# end`	Call Home 宛先プロファイル コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

次に、宛先プロファイルをアクティブにする例を示します。

```
Router# configure terminal
Router(config)# call-home
Router(config-call-home)# profile test
Router(cfg-call-home-profile)# active
Router(cfg-call-home)# end
```

次に、宛先プロファイルを非アクティブにする例を示します。

```
Router# configure terminal
Router(config)# call-home
Router(config-call-home)# profile test
Router(cfg-call-home-profile)# no active
Router(cfg-call-home)# end
```

宛先プロファイルのコピー

既存のプロファイルをコピーして新しい宛先プロファイルを作成するには、次の作業を行います。

	コマンドまたはアクション	目的
ステップ 1	`Router# 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	`Router(config)# call-home`	Call Home 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	`Router(cfg-call-home)# copy profile source_profile target_profile`	既存の宛先プロファイルと同じ設定で新しい宛先プロファイルを作成します。それぞれの説明は次のとおりです。 • *source_profile*：既存プロファイル名を指定します。 • *target_profile*：プロファイルの新しいコピーの名前を指定します。

次に、宛先プロファイルをアクティブにする例を示します。

```
Router# configure terminal
Router(config)# call-home
Router(config-call-home)# profile test
Router(cfg-call-home-profile)# copy profile profile1 profile2
```

宛先プロファイルの名前変更

既存のプロファイルの名前を変更するには、次の作業を行います。

	コマンドまたはアクション	目的
ステップ 1	`Router# 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	`Router(config)# call-home`	Call Home 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	`Router(cfg-call-home)# rename profile source_profile target_profile`	既存のソース ファイルの名前を変更します。それぞれの説明は次のとおりです。 • *source_profile*：既存プロファイル名を指定します。 • *target_profile*：既存プロファイルの新しい名前を指定します。

次に、宛先プロファイルをアクティブにする例を示します。

```
Router# configure terminal
Router(config)# call-home
Router(config-call-home)# profile test
Router(cfg-call-home-profile)# rename profile profile1 profile2
```

定義済みの CiscoTAC-1 宛先プロファイルの使用

CiscoTAC-1 プロファイルは、Cisco Smart Call Home サービスで使用するために、Call Home 機能で自動的に設定されています。このプロファイルには、宛先電子メールアドレスや HTTPS URL などの特定の情報、および Smart Call Home サービスと通信するためのデフォルトのアラート グループが含まれています。宛先電子メールアドレス、HTTPS URL、メッセージ形式など、一部の属性は変更できません。

電子メールまたは HTTP 転送を使用して、Smart Call Home サービスのバックエンド サーバと通信できます。デフォルトでは、CiscoTAC-1 プロファイルは非アクティブであり、デフォルトの転送方法として電子メールが使用されます。電子メール転送を使用するには、このプロファイルをイネーブルにす

るだけです。ただし、(HTTPS を介して) Cisco Smart Call Home サービス セキュア サーバでこのプロファイルを使用する場合は、プロファイルをイネーブルにするだけでなく、次の例に示すように、転送方法を HTTP に変更することも必要です。

```
Router# configure terminal
Router(config)# call-home
Router(config-call-home)# profile CiscoTAC-1
Router(cfg-call-home-profile)# destination transport-method http
Router(cfg-call-home-profile)# active
```

Smart Call Home サービスを設定するための追加要件の詳細については、「Smart Call Home の概要」（P.53-44）を参照してください。

Call Home プロファイル設定の確認

Call Home のプロファイル設定を確認するには、**show call-home profile** コマンドを使用します。詳細および例については、「Call Home 設定の確認」（P.53-47）を参照してください。

アラート グループへの登録

アラート グループの登録の概要

アラート グループは、すべてのスイッチでサポートされる Call Home アラートの定義済みのサブセットです。Call Home アラートはタイプごとに別のアラート グループにグループ化されます。次のアラート グループが使用できます。

- Crash
- Configuration
- Diagnostic
- Environment
- Inventory
- Snapshot
- Syslog

各アラート グループの起動イベントは 「アラート グループの起動イベントとコマンド」（P.53-5）に示しています。アラート グループ メッセージの内容は「メッセージの内容」（P.53-15）に示しています。

宛先プロファイルごとに受信するアラート グループを 1 つまたは複数選択できます。

（注）　Call Home アラートは、その Call Home アラートが含まれているアラート グループに登録されている宛先プロファイルにしか送信されません。さらに、アラート グループをイネーブルにする必要があります。

アラート グループの登録の設定

宛先プロファイルをアラート グループに登録するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# 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	`Router(config)# call-home`	Call Home 設定サブモードを開始します。
ステップ 3	`Router(cfg-call-home)# alert-group {all | configuration | crash | diagnostic | environment | inventory | snapshot | syslog}`	指定されたアラート グループをイネーブルにします。すべてのアラート グループをイネーブルにするには、**all** キーワードを使用します。デフォルトでは、すべてのアラート グループがイネーブルになります。
ステップ 4	`Router(cfg-call-home)# profile name`	指定された宛先プロファイルに対する Call Home 宛先プロファイル設定サブモードを開始します。
ステップ 5	`Router(cfg-call-home-profile)# subscribe-to-alert-group all`	最も低い重大度を使用しているすべての使用可能なアラート グループにこの宛先プロファイルを登録します。 **（注）** • このコマンドは、syslog のデバッグのデフォルトの重大度に登録されます。これにより、大量の syslog メッセージが生成されます。可能な場合は、適切な重大度およびパターンを使用してアラート グループに個別に登録してください。 • 代わりに、次の手順に従って、特定のタイプごとにアラート グループに個別に登録できます。
ステップ 6	`Router(cfg-call-home-profile)# subscribe-to-alert-group configuration [periodic {daily hh:mm | monthly date hh:mm | weekly day hh:mm}]`	この宛先プロファイルを Configuration アラート グループに登録します。Configuration アラート グループは、「定期通知」（P.53-35）で説明しているように、定期的な通知用に設定できます。

ステップ 7	`subscribe-to-alert-group crash`
	
	例：
	`Router(cfg-call-home-profile)# subscribe-to-alert-group crash`
		ユーザ プロファイルの Crash アラート グループに登録します。デフォルトで TAC プロファイルは Crash アラート グループに登録され、登録を解除できません。

ステップ 8	`Router(cfg-call-home-profile)# subscribe-to-alert-group diagnostic [severity {catastrophic | critical | debugging | disaster | fatal | major | minor | normal | notification | warning}]`	この宛先プロファイルを Diagnostic アラート グループに登録します。Diagnostic アラート グループは、「メッセージの重大度しきい値」（P.53-35）で説明しているように、重大度に応じてメッセージをフィルタするよう設定できます。
ステップ 9	`Router(cfg-call-home-profile)# subscribe-to-alert-group environment [severity {catastrophic | critical | debugging | disaster | fatal | major | minor | normal | notification | warning}]`	この宛先プロファイルを Environment アラート グループに登録します。Environment アラート グループは、「メッセージの重大度しきい値」（P.53-35）で説明しているように、重大度に応じてメッセージをフィルタするよう設定できます。

	コマンド	目的
ステップ 10	`Router(cfg-call-home-profile)#` **`subscribe-to-alert-group inventory`** [**`periodic`** {**`daily`** *`hh:mm`* | **`monthly`** *`date hh:mm`* | **`weekly`** *`day hh:mm`*}]	この宛先プロファイルを Inventory アラート グループに登録します。Inventory アラート グループは、「定期通知」（P.53-35）で説明しているように、定期的な通知用に設定できます。

ステップ 11	**`subscribe-to-alert-group snapshot`** [**`periodic`** {**`daily`** *`hh:mm`* | **`hourly`** *`mm`* | **`interval`** *`mm`* | **`monthly`** *`date hh:mm`* | **`weekly`** *`day hh:mm`*}]
	
	例：
	`Router(cfg-call-home-profile)#`
	`subscribe-to-alert-group snapshot periodic daily 12:00`
		この宛先プロファイルを Snapshot アラート グループに登録します。Snapshot アラート グループは、「定期通知」（P.53-35）で説明しているように、定期的な通知用に設定できます。
		
		デフォルトでは、Snapshot アラート グループに実行するコマンドはありません。コマンド出力をスナップショット メッセージに表示するには、「スナップショット コマンド リストの設定」（P.53-37）で説明しているように、アラート グループにコマンドを追加します。

ステップ 12	`Router(cfg-call-home-profile)#` **`subscribe-to-alert-group syslog`** [**`severity`** {**`catastrophic`** | **`disaster`** | **`fatal`** | **`critical`** | **`major`** | **`minor`** | **`warning`** | **`notification`** | **`normal`** | **`debugging`**} [**`pattern`** *`string`*]]	この宛先プロファイルを Syslog アラート グループに登録します。Syslog アラート グループは、「メッセージの重大度しきい値」（P.53-35）で説明しているように、重大度に応じてメッセージをフィルタするよう設定できます。「Syslog パターン マッチングの設定」（P.53-38）で説明しているように、syslog メッセージで一致するパターンを指定できます。パターンにスペースが含まれている場合は、引用符（""）で囲みます。
ステップ 13	`Router(cfg-call-home-profile)#` **`exit`**	Call Home 宛先プロファイル設定サブモードを終了します。

定期通知

Configuration、Snapshot、または Inventory アラート グループに宛先プロファイルを登録すると（「アラート グループの登録の設定」（P.53-34）を参照）、指定した時間で非同期にまたは定期的にアラート グループ メッセージを受信するよう選択できます。送信期間は、次のいずれかにできます。

- 毎日：24 時間の時間：分形式 *hh:mm*（例：14:30）で送信する時刻を指定します。
- 毎週：*day hh:mm* という形式で曜日と時刻を指定します。ここで、day は曜日をスペルアウトします（例：monday）。
- 毎月：*date hh:mm* という形式で 1 ～ 31 の日と時刻を指定します。

Snapshot アラート グループは、次のオプションをサポートします。

- 間隔：定期的なメッセージが送信される間隔を 1 ～ 60 分で指定します。
- 毎時：定期的なメッセージが送信される時刻（分）を 0 ～ 59 分で指定します。

メッセージの重大度しきい値

宛先プロファイルを Diagnostic、Environment、または Syslog アラート グループに登録すると（「アラート グループの登録の設定」（P.53-34）を参照）、メッセージの重大度に基づいてアラート グループ メッセージを送信するしきい値を設定できます。宛先プロファイルに指定したしきい値より低い値のメッセージは、宛先に送信されません。

重大度しきい値は、表 53-13 のキーワードと、catastrophic（レベル 9、最高レベルの緊急性）から debugging（レベル 0、最低レベルの緊急性）までの範囲を使用して設定します。重大度しきい値が設定されていない場合、デフォルトは debugging（レベル 0）です。

（注）　Call Home の重大度は、システム メッセージ ロギングの重大度とは異なります。

表 53-13　　重大度と Syslog レベルのマッピング

レベル	キーワード	Syslog レベル	説明
9	**catastrophic**	N/A	ネットワーク全体に壊滅的な障害が発生しています。
8	**disaster**	N/A	ネットワークへの重大な影響。
7	**fatal**	緊急（0）	システムを使用できません。
6	**critical**	アラート（1）	クリティカルな状態、ただちに注意が必要。
5	**major**	重要（2）	重大な状態。
4	**minor**	エラー（3）	軽微な状態。
3	**warning**	警告（4）	警告状態です。
2	**notification**	通知（5）	基本的な通知と情報メッセージ。他と関係しない、重要性の低い障害。
1	**normal**	情報（6）	標準状態に戻ることを示す標準イベント。
0	**debugging**	デバッグ（7）	デバッグ メッセージです。

スナップショット コマンド リストの設定

スナップショット コマンド リストを設定するには、次の作業を行います。

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例：** `Router# 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	**call-home** **例：** `Router(config)# call-home`	Call Home 設定サブモードを開始します。
ステップ 3	**alert-group-config snapshot** **例：** `Router(cfg-call-home)# alert-group-config snapshot`	スナップショット コンフィギュレーション モードを開始します。 **no** または **default** コマンドは、すべてのスナップショット コマンドを削除します。
ステップ 4	**add-command** *command string* **例：** `Router(cfg-call-home-snapshot)# add-command "show version"`	Snapshot アラート グループにコマンドを追加します。**no** または **default** コマンドは、対応するコマンドを削除します。 • *command string*：IOS コマンド。最大長は 128 文字です。
ステップ 5	**exit** **例：** `Router(cfg-call-home-snapshot)# exit`	終了し、設定を保存します。

Call Home メッセージの IOS コマンドを実行するための AAA 認証のイネーブル化

AAA 認証をイネーブルにして Call Home メッセージの出力の収集をイネーブルにする IOS コマンドを実行するには、次の作業を行います。

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例：** `Router# 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	**call-home** **例：** `Router(config)# call-home`	Call Home 設定サブモードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**aaa-authorization** **例：** `Router(cfg-call-home)# aaa-authorization`	AAA 認証をイネーブルにします。 **（注）** デフォルトでは、AAA 認証は Call Home でディセーブルです。
ステップ 4	**aaa-authorization** [**username** *username*] **例：** `Router(cfg-call-home)# aaa-authorization username user`	許可のためのユーザ名を指定します。 • **username** *username*：デフォルトのユーザ名は callhome です。最大長は 64 文字です。

Syslog パターン マッチングの設定

宛先プロファイルを Syslog アラート グループに登録すると（「アラート グループの登録の設定」（P.53-34）を参照）、各 syslog メッセージ内で一致するテキスト パターンを任意で指定できます。パターンを設定すると、指定されたパターンが含まれ、重大度しきい値に一致する場合にだけ Syslog アラート グループ メッセージが送信されます。パターンにスペースが入っている場合、設定時にそのパターンを引用符（""）で囲みます。宛先プロファイルごとにパターンを 5 つまで指定できます。

Call Home データ プライバシーの設定

Call Home データ プライバシー機能では、顧客のプライバシーを保護するために実行コンフィギュレーション ファイルの潜在的な機密データ（IP アドレスなど）のスクラビング処理が行われます。

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例：** `Router# 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	**call-home** **例：** `Router(config)# call-home`	Call Home 設定サブモードを開始します。
ステップ 3	**data-privacy** {**level** {**normal** | **high**} | **hostname**} **例：** `Router(cfg-call-home)# data-privacy level high`	顧客のプライバシーを保護するために、実行コンフィギュレーション ファイルのデータのスクラビング処理を行います。 **（注）** data-privacy コマンドをイネーブルにすると、大量のデータのスクラビング処理を行ったときに CPU 使用率に影響を及ぼすことがあります。 • **normal**（デフォルト）：すべての標準レベル コマンドのスクラビング処理を行います。 • **high**：標準レベル コマンドに加えて、IP ドメイン名と IP アドレスのコマンドのスクラビング処理を行います。 • **hostname**：高レベル コマンドに加えて hostname コマンドのスクラビング処理を行います。 **（注）** VSS モードでは、設定メッセージのホスト名のスクラビング処理を行うと、Cisco TAC バックエンド サーバで Smart Call Home の処理に失敗することがあります。

次に、SR 番号が指定され、XML メッセージ形式で Cisco TAC バックエンド サーバへ送信されたコマンド出力の例を示します。

```
Router# call-home send "show version; show run" http tac-service-request 123456
```

次に、Cisco TAC バックエンド サーバに HTTP プロトコルを使用して送信され、ユーザが指定した電子メール アドレスに転送されたコマンド出力の例を示します。

```
Router# call-home send "show version; show run" http destination-email-address
user@company.com
```

Call Home のイネーブル化

Call Home 機能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	`Router# 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	`Router(config)# service call-home`	Call Home 機能をイネーブルにします。

Call Home トラフィック レート制限の設定

Call Home トラフィック レート制限を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# 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	`Router(config)# call-home`	Call Home 設定サブモードを開始します。
ステップ 3	`Router(cfg-call-home)# rate-limit number`	（任意）1 分間に送信するメッセージ数の上限を指定します（1 ～ 60）。デフォルトは 20 です。

次に、Call Home トラフィック レート制限を設定する例を示します。

```
Router# configure terminal
Router(config)# call-home
Router(config-call-home)# profile test
Router(cfg-call-home-profile)# rate-limit 20
```

syslog スロットリングの設定

Call Home syslog メッセージを繰り返し送信しないように Call Home syslog メッセージのスロットリングをイネーブルにするには、次の作業を行います。

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例：** `Router# 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	**call-home** **例：** `Router(config)# call-home`	Call Home 設定サブモードを開始します。
ステップ 3	**syslog-throttling** **例：** `Router(cfg-call-home)# syslog-throttling`	Call Home syslog メッセージのスロットリングをイネーブルにします。これにより、Call Home syslog メッセージは繰り返し送信されません。デフォルトでは、syslog メッセージ スロットリングはイネーブルです。

Call Home の通信のテスト

Call Home テスト メッセージの手動送信

Call Home テスト メッセージを手動で送信するには、次の作業を行います。

コマンド	目的
`Router# call-home test ["test-message"] profile name`	指定された宛先プロファイルにテスト メッセージを送信します。ユーザ定義のテスト メッセージ テキストは任意ですが、スペースが含まれる場合は、引用符（""）で囲みます。ユーザ定義のメッセージが設定されていない場合、デフォルト メッセージが送信されます。

Call Home アラート グループ メッセージの手動送信

Call Home アラート グループ メッセージを手動で起動するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# call-home send alert-group configuration [profile name]`	宛先プロファイルの 1 つ（指定されている場合）または登録されているすべての宛先プロファイルに Configuration アラート グループ メッセージを送信します。
ステップ 2	`Router# call-home send alert-group {crash | diagnostic | snapshot} {module number | slot/subslot | slot/bay_number | switch x module number} [profile name]`	設定された宛先プロファイル（指定されている場合）または登録されているすべての宛先プロファイルに Diagnostic アラート グループ メッセージを送信します。診断情報が送信されるモジュールまたはポートを指定する必要があります。Virtual Switching System（VSS）を使用する場合は、スイッチとモジュールを指定する必要があります。
ステップ 3	`Router# call-home send alert-group inventory [profile name]`	宛先プロファイルの 1 つ（指定されている場合）または登録されているすべての宛先プロファイルに Inventory アラート グループ メッセージを送信します。

- 手動で送信できるのは、Configuration、Diagnostic、または Inventory アラート グループだけです。
- Configuration、Diagnostic、または Inventory アラート グループ メッセージを手動で起動し、宛先プロファイル名を指定すると、プロファイルのアクティブ ステータス、登録ステータス、または重大度設定に関係なくメッセージが宛先プロファイルに送信されます。

- Configuration または Inventory アラート グループ メッセージを手動で起動し、宛先プロファイル名を指定しないと、normal または指定されたアラート グループへの定期的な登録に指定されたアクティブなプロファイルすべてにメッセージが送信されます。
- Diagnostic アラート グループ メッセージを手動で起動し、宛先プロファイル名を指定しないと、コマンドによって次の動作が行われます。
  - 重大度が minor より下の診断イベントに登録されたアクティブなプロファイルの場合、モジュールまたはインターフェイスが診断イベントを遵守しているかどうかに関係なくメッセージが送信されます。
  - 重大度が minor 以上の診断イベントに登録されたアクティブなプロファイルの場合、指定されたモジュールまたはインターフェイスが、少なくとも登録された重大度の診断イベントを遵守している場合にだけメッセージが送信されます。遵守していない場合、診断メッセージは宛先プロファイルに送信されません。

分析およびレポート要求の送信

レポートおよび分析情報の要求を Cisco アウトプットインタープリタ ツールから送信するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# call-home request output-analysis "show-command" [profile name] [ccoid user-id]`	分析用として指定した show コマンドの出力を送信します。show コマンドは二重引用符（" "）で囲みます。
ステップ 2	`Router# call-home request {config-sanity | bugs-list | command-reference | product-advisory} [profile name] [ccoid user-id]`	**show running-config all**、**show version**、**show module**（スタンドアロン）または **show module switch all**（VS システム）コマンドなどのあらかじめ定められているコマンド群の出力を分析用に送信します。要求するレポートのタイプを指定します。

- **profile** *name* を指定すると、要求はプロファイルに送信されます。プロファイルを指定しなければ、要求は Cisco TAC プロファイルに送信されます。Call Home 要求の受信者プロファイルをイネーブルにする必要はありません。要求メッセージを Cisco TAC に転送し、Smart Call Home サービスから返信を受信できるように、転送ゲートウェイが設定された電子メール アドレスをプロファイルに指定します。
- **ccoid** *user-id* は、Smart Call Home ユーザの登録 ID です。*user-id* を指定すると、応答は登録ユーザの電子メール アドレスに送信されます。*user-id* を指定しなければ、応答はデバイスの連絡先電子メール アドレスに送信されます。
- 要求されるレポートのタイプを示すキーワードに応じて、次の情報が返されます。
  - **config-sanity**：現在の実行コンフィギュレーションに関連するベスト プラクティスの情報。
  - **bugs-list**：実行中のバージョンおよび現在適用されている機能の既知のバグ。
  - **command-reference**：実行コンフィギュレーションに含まれるすべてのコマンドへの参照リンク。
  - **product-advisory**：ネットワークのデバイスに影響する可能性のある Product Security Incident Response Team（PSIRT）通知、End of Life（EOL）または End of Sales（EOS）通知、あるいは Field Notice（FN）。

次に、ユーザが指定した show コマンドの分析を要求する例を示します。

```
Router# call-home request output-analysis "show diagnostic result module all" profile TG
```

コマンド出力の送信

1 つまたは複数の CLI コマンドを実行し、HTTP または電子メールでコマンド出力を送信するには、次の作業を行います。

コマンド	目的
Router# **call-home send** {*cli command* | *cli list*} [**email** *email* **msg-format** {**long-text** | **xml**} | **http** {**destination-email-address** *email*}] [**tac-service-request** *SR#*]	CLI または CLI リストを実行し、電子メールまたは HTTP 経由で出力を送信します。 • {*cli command* | *cli command list*} : IOS コマンドまたは IOS コマンドのリスト（「;」で区切ります）を指定します。すべてのモジュールに対するコマンドを含む、あらゆる run コマンドを指定できます。このコマンドは引用符（""）で囲む必要があります。 • **email** または **http** キーワードを指定しないと、出力は指定されたサービス要求番号でロング テキスト形式で Cisco TAC（attach@cisco.com）に送信されます。 • **email** *email* **msg-format** {**long-text** | **xml**} : **email** キーワードおよび電子メール アドレスを指定すると、コマンド出力がそのアドレスに送信されます。 • **http** {**destination-email-address** *email*} : **http** キーワードを指定すると、Smart Call Home バックエンド サーバ（TAC プロファイルで指定された URL）にコメント出力が XML 形式で送信されます。バックエンド サーバから電子メール アドレスにメッセージを転送するには、**destination-email-address** *email* を指定します。電子メール アドレス、サービス要求番号、またはその両方を指定する必要があります。 • **tac-service-request** *SR#* : サービス要求番号を指定します。電子メール アドレスを指定しない場合、または Cisco TAC 電子メール アドレスを指定した場合、サービス要求番号が必要です。

次に、コマンドの出力をユーザ指定の電子メール アドレスに送信する例を示します。

```
Router# call-home send "show diag" email support@example.com
```

次に、SR 番号が指定され、ロング テキスト形式で attach@cisco.com に送信されるコマンド出力の例を示します。

```
Router# call-home send "show version; show run" tac-service-request 123456
```

次に、XML メッセージ形式で callhome@cisco.com に送信されるコマンド出力の例を示します。

```
Router# call-home send "show version; show run" email callhome@cisco.com msg-format xml
```

次に、SR 番号が指定され、XML メッセージ形式で Cisco TAC バックエンド サーバへ送信されたコマンド出力の例を示します。

```
Router# call-home send "show version; show run" http tac-service-request 123456
```

次に、Cisco TAC バックエンド サーバに HTTP プロトコルを使用して送信され、ユーザが指定した電子メール アドレスに転送されたコマンド出力の例を示します。

```
Router# call-home send "show version; show run" http destination-email-address
user@company.com
```

Smart Call Home サービスの設定

（注）　単一コマンドによる Smart Call Home の設定は、Smart Call Home サービスのイネーブル化および Smart Call Home の登録の開始の代替手段です。

Smart Call Home の概要

Cisco Smart Call Home サービスの適用と設定情報については、次の URL にある『*Smart Call Home User Guide*』の「Quick Start for Smart Call Home」を参照してください。

http://www.cisco.com/en/US/docs/switches/lan/smart_call_home/SCH31_Ch1.html#Quick_Start_for_Smart_Call_Home

ユーザ ガイドには、デバイスから直接、または転送ゲートウェイ（TG）集約ポイントを介して Smart Call Home メッセージを送信するための設定例が記載されています。複数のデバイスをサポートする必要のある場合や、セキュリティ要件によってデバイスがインターネットに直接接続されないことが必要とされる場合は、TG 集約ポイントを使用できます。

Smart Call Home サービスは転送方法として HTTPS を使用するため、『*Smart Call Home User Guide*』で説明されているように CA をトラストポイントとして設定する必要もあります。

ヒント　Smart Call Home の Web サイトから基本的な設定スクリプトをダウンロードして、Smart Call Home サービスおよびシスコ TAC とともに使用するよう Call Home 機能を設定するために利用できます。このスクリプトは、Smart Call Home サービスとセキュアな通信を行うために、トラストポイント CA を設定する際にも有用です。現状のまま提供されるスクリプトは、次の URL にある「Smart Call Home Resources」という見出しの下にあるリンクからダウンロードできます。
https://supportforums.cisco.com/community/netpro/solutions/smart_services/smartcallhome

Smart Call Home サービスの前提条件

- 設定するデバイスが有効なサービス契約の対象となっていることを確認します。
- Cisco HTTPS サーバと IP 接続できることを確認します。
- 最新のシスコ サーバ セキュリティ証明書を取得します。

単一コマンドによる Smart Call Home の設定

（注）　この手順は、Smart Call Home サービスのイネーブル化および Smart Call Home の登録の開始の代替手段です。

1 つのコマンドを使用してすべての Call Home の基本設定をイネーブルにするには、次の作業を行います。

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例：** `Router# 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	**call-home reporting** {**anonymous** | **contact-email-addr** *email-address*} [**http-proxy** {*ipv4-address* | *ipv6-address* | *name*} **port** *port-number*] **例：** `Router(config)# call-home reporting contact-email-addr email@company.com`	1 つのコマンドを使用してすべての Call Home の基本設定をイネーブルにします。 • **anonymous**：Call Home TAC プロファイルがクラッシュ、インベントリ、およびテスト メッセージだけを送信し、匿名でメッセージを送信できるようにします。 • **contact-email-addr**：Smart Call Home サービスのフル レポート機能をイネーブルにし、フル インベントリ メッセージを Call Home TAC プロファイルから Smart Call Home サーバに送信してフル登録プロセスを開始します。 • **http-proxy** {*ipv4-address* | *ipv6-address* | *name*}：IPv4 または IPv6 アドレスまたはサーバ名。最大長は 64 文字です。 • **port** *port-number*：ポート番号。有効値の範囲は 1 ～ 65535 です。 （注）　HTTP プロキシ オプションでは、バッファリングするための独自のプロキシ サーバおよびデバイスからのセキュア接続を利用できます。 （注）　**call-home reporting** コマンドを使用して匿名またはフル登録モードで Call Home を正常にイネーブルにした後、インベントリ メッセージが送信されます。Call Home がフル登録モードでイネーブルになっている場合、フル登録モードのフル インベントリ メッセージが送信されます。Call Home が匿名モードでイネーブルになっている場合、匿名のインベントリ メッセージが送信されます。これらのメッセージの送信内容の詳細については、「アラート グループの起動イベントとコマンド」（P.53-5）を参照してください。

Smart Call Home サービスのイネーブル化

（注）　この手順および Smart Call Home の登録の開始は、単一コマンドによる Smart Call Home の設定の代替手段です。

CiscoTAC-1 プロファイルは、電子メールを使用して Smart Call Home サービスのバック エンド サーバと通信するように Call Home 機能で事前定義されています。Cisco HTTPS バック エンド サーバへの URL も定義されています。このプロファイルは、デフォルトで非アクティブです。

両方の転送方法をサポートするように Call Home で設定できる他のプロファイルとは異なり、CiscoTAC-1 プロファイルは一度に 1 つの転送方法のみを使用できます。Cisco Smart Call Home HTTPS サーバでこのプロファイルを使用するには、転送方法を電子メールから HTTP に変更し、このプロファイルをイネーブルにする必要があります。また、連絡先の電子メールアドレスを最小限指定し、Call Home 機能をイネーブルにする必要があります。

Smart Call Home サービスをイネーブルにするには、次の作業を行います。

	コマンドまたはアクション	目的
ステップ 1	`Router# 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	`Router(config)# call-home`	Call Home 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	`Router(config-call-home)# profile CiscoTAC-1`	CiscoTAC-1 宛先プロファイルの Call Home 宛先プロファイル コンフィギュレーション モードを開始します。
ステップ 4	`Router(cfg-call-home-profile)# destination transport-method http`	（HTTPS の場合は必須）http のメッセージ転送方法を設定します。
ステップ 5	`Router(cfg-call-home-profile)# active`	宛先プロファイルをイネーブルにします。
ステップ 6	`Router(cfg-call-home-profile)# exit`	Call Home 宛先プロファイル コンフィギュレーション モードを終了して、Call Home コンフィギュレーション モードに戻ります。
ステップ 7	`Router(cfg-call-home)# contact-email-addr customer_email_address`	顧客の電子メール アドレスを割り当てます。スペースを入れず電子メール アドレス形式で 200 文字まで入力します。
ステップ 8	`Router(cfg-call-home)# exit`	Call Home コンフィギュレーション モードを終了し、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	`Router(config)# service call-home`	Call Home 機能をイネーブルにします。
ステップ 10	`Router(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 11	`Router# copy running-config startup-config`	設定を保存します。

次に、Smart Call Home サービスをイネーブルにする例を示します。

```
Router(cfg-call-home-profile)# destination transport-method http
Router(cfg-call-home-profile)# active
Router(cfg-call-home-profile)# exit
Router(cfg-call-home)# contact-email-addr username@example.com
Router(cfg-call-home)# exit
Router(config)# service call-home
Router(config)# exit
Router# copy running-config startup-config
```

Smart Call Home の登録の開始

（注）　この手順および Smart Call Home サービスのイネーブル化は、単一コマンドによる Smart Call Home の設定の代替手段です。

Smart Call Home の登録プロセスを開始するには、次の作業を行います。

コマンドまたはアクション	目的
`Router# call-home send alert-group inventory profile CiscoTAC-1`	Inventory アラート グループ メッセージを CiscoTAC-1 宛先プロファイルに手動で送信します。

Smart Call Home サービスが登録されると、シスコから電子メールを受信します。電子メールの指示に従います。この指示には次の手順が含まれています。

- デバイス登録を完了するには、次の URL にある Smart Call Home Web アプリケーションを起動します。

  https://tools.cisco.com/sch/

- 法的な契約書を受け入れます。
- 登録が保留中であった Call Home デバイスのデバイス登録を確認します。

Smart Call Home Web アプリケーションの使用の詳細については、『*Smart Call Home User Guide*』を参照してください。このユーザ ガイドには、デバイスから直接、または転送ゲートウェイ（TG）集約ポイントを介して Smart Call Home メッセージを送信するための設定例も含まれています。複数のデバイスをサポートする必要のある場合や、セキュリティ要件によってデバイスがインターネットに直接接続されないことが必須である場合は、TG 集約ポイントを使用できます。

Call Home 設定の確認

設定された Call Home 情報を表示するには、次の作業を行います。

コマンド	目的
`Router# show call-home`	Call Home 設定の概要を表示します。
`Router# show call-home detail`	Call Home 設定の詳細を表示します。
`Router# show call-home alert-group`	使用可能なアラート グループとそれらのステータスを表示します。
`Router# show call-home mail-server status`	設定済みの電子メール サーバのアベイラビリティをチェックして表示します。
`Router# show call-home profile {all | name}`	指定された宛先プロファイルの設定を表示します。**all** キーワードを使用してすべての宛先プロファイルの設定を表示します。
`Router# show call-home statistics [detail | profile profile_name]`	Call Home イベントの統計情報を表示します。

例 53-1 ～ 53-9 は、**show call-home** コマンドの各種オプションを使用した Release 15.1(1)SY の結果の例を示しています。

例 53-1　設定済みの Call Home 情報

```
Router# show call-home
Current call home settings:
    call home feature : enable
    call home message's from address: switch@example.com
    call home message's reply-to address: support@example.com

    vrf for call-home messages: Not yet set up

    contact person's email address: technical@example.com

    contact person's phone number: +1-408-555-1234
    street address: 1234 Any Street, Any city, Any state, 12345
    customer ID: ExampleCorp
    contract ID: X123456789
    site ID: SantaClara

    source ip address: Not yet set up
    source interface: GigabitEthernet7/2
    Mail-server[1]: Address: smtp.example.com Priority: 1
    Mail-server[2]: Address: 192.168.0.1 Priority: 2
    http proxy: 192.168.1.2:80

    aaa-authorization: disable
    aaa-authorization username: callhome (default)
    data-privacy: normal
    syslog throttling: enable

    Rate-limit: 20 message(s) per minute

    Snapshot command[0]: show version
    Snapshot command[1]: show module

Available alert groups:
    Keyword                  State   Description
    ------------------------ ------- --------------------------------
    configuration            Enable  configuration info
    crash                    Enable  crash and traceback info
    diagnostic               Enable  diagnostic info
    environment              Enable  environmental info
    inventory                Enable  inventory info
    snapshot                 Enable  snapshot info
    syslog                   Enable  syslog info

Profiles:
    Profile Name: campus-noc
    Profile Name: CiscoTAC-1

Router#
```

例 53-2　設定済みの Call Home 情報の詳細

```
Router# show call-home detail
Current call home settings:
    call home feature : enable
    call home message's from address: switch@example.com
    call home message's reply-to address: support@example.com

    vrf for call-home messages: Not yet set up

    contact person's email address: technical@example.com

    contact person's phone number: +1-408-555-1234
    street address: 1234 Any Street, Any city, Any state, 12345
    customer ID: ExampleCorp
    contract ID: X123456789
    site ID: SantaClara

    source ip address: Not yet set up
    source interface: GigabitEthernet7/2
    Mail-server[1]: Address: smtp.example.com Priority: 1
    Mail-server[2]: Address: 192.168.0.1 Priority: 2
    http proxy: 192.168.1.2:80

    aaa-authorization: disable
    aaa-authorization username: callhome (default)
    data-privacy: normal
    syslog throttling: enable

    Rate-limit: 20 message(s) per minute

    Snapshot command[0]: show version
    Snapshot command[1]: show module

Available alert groups:
    Keyword                 State   Description
    ----------------------- ------- --------------------------------
    configuration           Enable  configuration info
    crash                   Enable  crash and traceback info
    diagnostic              Enable  diagnostic info
    environment             Enable  environmental info
    inventory               Enable  inventory info
    snapshot                Enable  snapshot info
    syslog                  Enable  syslog info

Profiles:

Profile Name: campus-noc
    Profile status: ACTIVE
    Profile mode: Full Reporting
    Preferred Message Format: long-text
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): noc@example.com
    HTTP  address(es): Not yet set up

    Alert-group             Severity
    ----------------------  ------------
    inventory               normal

    Syslog-Pattern          Severity
    ----------------------  ------------
    N/A                     N/A

Profile Name: CiscoTAC-1
    Profile status: ACTIVE
    Profile mode: Full Reporting
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
```

```
    Transport Method: email
    Email address(es): callhome@cisco.com
    HTTP  address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService

    Periodic configuration info message is scheduled every 12 day of the month at 17:06

    Periodic inventory info message is scheduled every 12 day of the month at 16:51

    Alert-group               Severity
    ------------------------  ------------
    crash                     normal
    diagnostic                minor
    environment               minor
    inventory                 normal

    Syslog-Pattern            Severity
    ------------------------  ------------
    .*                        major

Router#
```

例 53-3　使用可能な Call Home アラート グループ

```
Router# show call-home alert-group
Available alert groups:
    Keyword                   State   Description
    ------------------------ ------- --------------------------------
    configuration             Enable  configuration info
    crash                     Enable  crash and traceback info
    diagnostic                Enable  diagnostic info
    environment               Enable  environmental info
    inventory                 Enable  inventory info
    snapshot                  Enable  snapshot info
    syslog                    Enable  syslog info

Router#
```

例 53-4　電子メール サーバのステータス情報

```
Router# show call-home mail-server status
Please wait. Checking for mail server status ...

Translating "smtp.example.com"
    Mail-server[1]: Address: smtp.example.com Priority: 1 [Not Available]
    Mail-server[2]: Address: 192.168.0.1 Priority: 2 [Not Available]

Router#
```

例 53-5　すべての宛先プロファイルの情報（定義済みおよびユーザ定義）

```
Router# show call-home profile all

Profile Name: campus-noc
    Profile status: ACTIVE
    Profile mode: Full Reporting
    Preferred Message Format: long-text
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): noc@example.com
    HTTP  address(es): Not yet set up

    Alert-group               Severity
    ------------------------  ------------
    inventory                 normal
```

```
    Syslog-Pattern            Severity
    ------------------------  ------------
    N/A                       N/A

Profile Name: CiscoTAC-1
    Profile status: ACTIVE
    Profile mode: Full Reporting
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): callhome@cisco.com
    HTTP  address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService

    Periodic configuration info message is scheduled every 12 day of the month at 17:06

    Periodic inventory info message is scheduled every 12 day of the month at 16:51

    Alert-group               Severity
    ------------------------  ------------
    crash                     normal
    diagnostic                minor
    environment               minor
    inventory                 normal

    Syslog-Pattern            Severity
    ------------------------  ------------
    .*                        major

Router#
```

例 53-6　　ユーザ定義宛先プロファイルの情報

```
Router# show call-home profile campus-noc

Profile Name: campus-noc
    Profile status: ACTIVE
    Profile mode: Full Reporting
    Preferred Message Format: long-text
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): noc@example.com
    HTTP  address(es): Not yet set up

    Alert-group               Severity
    ------------------------  ------------
    inventory                 normal

    Syslog-Pattern            Severity
    ------------------------  ------------
    N/A                       N/A

Router#
```

例 53-7　　Call Home の統計情報

```
Router# show call-home statistics
Message Types    Total                Email                HTTP
-------------   -------------------- -------------------- ------------------
Total Success   1                    1                    0
    Config      0                    0                    0
    Crash       0                    0                    0
    Diagnostic  0                    0                    0
    Environment 0                    0                    0
    Inventory   0                    0                    0
    Snapshot    0                    0                    0
```

```
    SysLog      0                   0                   0
    Test        0                   0                   0
    Request     0                   0                   0
    Send-CLI    1                   1                   0

Total In-Queue  0                   0                   0
    Config      0                   0                   0
    Crash       0                   0                   0
    Diagnostic  0                   0                   0
    Environment 0                   0                   0
    Inventory   0                   0                   0
    Snapshot    0                   0                   0
    SysLog      0                   0                   0
    Test        0                   0                   0
    Request     0                   0                   0
    Send-CLI    0                   0                   0

Total Failed    0                   0                   0
    Config      0                   0                   0
    Crash       0                   0                   0
    Diagnostic  0                   0                   0
    Environment 0                   0                   0
    Inventory   0                   0                   0
    Snapshot    0                   0                   0
    SysLog      0                   0                   0
    Test        0                   0                   0
    Request     0                   0                   0
    Send-CLI    0                   0                   0

Total Ratelimit
      -dropped  0                   0                   0
    Config      0                   0                   0
    Crash       0                   0                   0
    Diagnostic  0                   0                   0
    Environment 0                   0                   0
    Inventory   0                   0                   0
    Snapshot    0                   0                   0
    SysLog      0                   0                   0
    Test        0                   0                   0
    Request     0                   0                   0
    Send-CLI    0                   0                   0

Last call-home message sent time: 2012-10-22 21:35:48 GMT+08:00
```

例 53-8　Call Home の統計情報の詳細

```
Router# show call-home statistics detail
Type/Subtype           Total               Email               HTTP
-------------------   -------------------- -------------------- ------------------
Total Success         1                   1                   0
 Config/delta         0                   0                   0
 Config/full          0                   0                   0
 Crash/module crash   0                   0                   0
 Crash/system crash   0                   0                   0
 Crash/traceback      0                   0                   0
 Diagnostic           0                   0                   0
 Environment          0                   0                   0
 Inventory/delta      0                   0                   0
 Inventory/full       0                   0                   0
 Snapshot             0                   0                   0
 SysLog               0                   0                   0
 Test                 0                   0                   0
 Request              0                   0                   0
```

```
 Send-CLI             1                    1                    0

Total In-Queue        0                    0                    0
 Config/delta         0                    0                    0
 Config/full          0                    0                    0
 Crash/module crash   0                    0                    0
 Crash/system crash   0                    0                    0
 Crash/traceback      0                    0                    0
 Diagnostic           0                    0                    0
 Environment          0                    0                    0
 Inventory/delta      0                    0                    0
 Inventory/full       0                    0                    0
 Snapshot             0                    0                    0
 SysLog               0                    0                    0
 Test                 0                    0                    0
 Request              0                    0                    0
 Send-CLI             0                    0                    0

Total Failed          0                    0                    0
 Config/delta         0                    0                    0
 Config/full          0                    0                    0
 Crash/module crash   0                    0                    0
 Crash/system crash   0                    0                    0
 Crash/traceback      0                    0                    0
 Diagnostic           0                    0                    0
 Environment          0                    0                    0
 Inventory/delta      0                    0                    0
 Inventory/full       0                    0                    0
 Snapshot             0                    0                    0
 SysLog               0                    0                    0
 Test                 0                    0                    0
 Request              0                    0                    0
 Send-CLI             0                    0                    0

Total Ratelimit
      -dropped        0                    0                    0
 Config/delta         0                    0                    0
 Config/full          0                    0                    0
 Crash/module crash   0                    0                    0
 Crash/system crash   0                    0                    0
 Crash/traceback      0                    0                    0
 Diagnostic           0                    0                    0
 Environment          0                    0                    0
 Inventory/delta      0                    0                    0
 Inventory/full       0                    0                    0
 Snapshot             0                    0                    0
 SysLog               0                    0                    0
 Test                 0                    0                    0
 Request              0                    0                    0
 Send-CLI             0                    0                    0

Last call-home message sent time: 2012-10-22 21:35:48 GMT+08:00

Router#
```

例 53-9　Call Home 統計情報プロファイル campus-noc

```
Router#show call-home statistics profile campus-noc
                                                          Rate-limit   Last msg sent
Type/Subtype       Subscribe Success Inqueue Failed  Drop          (GMT+08:00)
------------------ ------------------------------------------------------------
Config/delta       normal    0       0       0       0               n/a
Config/full        bootup    0       0       0       0               n/a
```

```
Config/full         ondemand  0       0       0       0               n/a
Config/full         periodic  0       0       0       0               n/a
Crash/module crash  normal    0       0       0       0               n/a
Crash/system crash  normal    0       0       0       0               n/a
Crash/system crash  ondemand  0       0       0       0               n/a
Crash/traceback     normal    0       0       0       0               n/a
Diagnostic          normal    0       0       0       0               n/a
Diagnostic          ondemand  0       0       0       0               n/a
Environment         normal    0       0       0       0               n/a
Inventory/delta     normal    0       0       0       0               n/a
Inventory/full      bootup    0       0       0       0               n/a
Inventory/full      ondemand  0       0       0       0               n/a
Inventory/full      periodic  0       0       0       0               n/a
Snapshot            normal    0       0       0       0               n/a
Snapshot            ondemand  0       0       0       0               n/a
SysLog              normal    0       0       0       0               n/a
Test                normal    0       0       0       0               n/a
Request             normal    0       0       0       0               n/a

Router#
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CHAPTER 54

システム イベント アーカイブ（SEA）

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

システム イベント アーカイブの概要

システム障害の原因を見つける際に、システム メッセージを確認することは有効な方法です。システム メッセージに障害の原因を判別するために必要な情報が見つからないときは、デバッグ トレースをイネーブルにして、障害を再現してみます。ただし、このような方法でも最適な解決策が見つからない場合もあります。

- 障害の原因を判別するとき、大量のシステム メッセージを確認していくのは、効率的な方法とはいえません。
- デフォルトでは通常、デバッグ トレースは設定されていません。
- デバッグ トレースを使用している間は、障害を再現することができません。
- 障害が発生したスイッチがクリティカル ネットワークの一部である場合、デバッグ トレースは使用できません。

SEA では、スイッチの各 CPU がアウトオブバンド インターフェイスを使用して管理プロセッサにイベントを報告するようにできます。各イベントは、タイムスタンプとともに非揮発メモリに記録されます。デバイス上のブートフラッシュにアクセスしてイベント ログを検索したり、取り外し可能なストレージ デバイスなど別の場所にログをコピーしたりできます。

SEA は、最大 32 MB を使用して 2 つのファイルをブートディスクに保存します。これらのファイルには、ログに記録された最新のメッセージが記述されます。

- sea_log.dat：最新のシステム イベントがこのファイルに保存されます。
- sea_console.dat：最新のコンソール メッセージがこのファイルに保存されます。

これらのファイルはシステムで使用されるものなので、削除をしないでください。

SEA ログ システムを表示する方法

SEA のログ システムを表示するには、次の作業を行います。

コマンド	目的
Router# **show logging system** [**disk** | **size**]	SEA の内容を表示します。 （任意）キーワード **disk** を使用して、SEA が保存されている場所を表示します。SEA の現在のサイズを表示するには、キーワード **size** を使用します。
Router# **clear logging system**	SEA に保存されているイベント レコードを削除します。

次に、SEA を表示する例を示します。

```
Router# show logging system
SEQ: MM/DD/YY HH:MM:SS MOD/SUB: SEV, COMP,    MESSAGE
=====================================================

1: 01/24/07 15:38:40   6/-1 : MAJ, GOLD, syndiagSyncPinnacle failed in slot 6

2: 01/24/07 15:38:40   6/-1 : MAJ, GOLD, queryHyperionSynched[6]: Hyperion out of sync in sw_mode 1

3: 01/24/07 15:38:40   6/-1 : MAJ, GOLD, queryHyperionSynched[6]: Hyperion out of sync in sw_mode 1

4: 01/24/07 15:38:40   6/-1 : MAJ, GOLD, queryHyperionSynched[6]: Hyperion out of sync in sw_mode 1

5: 01/24/07 15:38:40   6/-1 : MAJ, GOLD, queryHyperionSynched[6]: Hyperion out of sync in sw_mode 1

6: 01/24/07 15:38:40   6/-1 : MAJ, GOLD, queryHyperionSynched[6]: Hyperion out of sync in sw_mode 1

7: 01/24/07 15:38:39   6/-1 : MAJ, GOLD, queryHyperionSynched[6]: Hyperion out of sync in sw_mode 1
```

次に、SEA ログ システム ディスクを表示する例を示します。

```
Router# show logging system disk
SEA log disk: bootdisk:
```

次に、SEA の現在のサイズを表示する例を示します。

```
Router# show logging system size
SEA log size: 33554432 bytes
```

次に、SEA をクリアする例を示します。

```
Router# clear logging system
Clear logging system operation will take a while.
Do you want to continue? [no]: yes
Router#
```

別のデバイスに SEA をコピーする方法

SEA を取り外し可能メモリ デバイスなどの別のデバイスにコピーするには、次の作業を行います。

コマンド	目的
Router# **copy logging system** *file_system*	SEA の内容を指定した宛先ファイル システムまたはプロセスにコピーします。

file_system の有効な値は次のとおりです。

- **bootflash:**
- **disk0:**
- **disk1:**
- **ftp:**
- **http:**
- **https:**
- **rcp:**
- **slavebootflash:**
- **slavedisk0:**
- **slavedisk1:**
- **slavebootdisk:**
- **slavebootflash:**
- **bootdisk:**
- **bootflash:**
- **tftp:**

次に、SEA を disk0 ファイル システムにコピーする例を示します。

```
Router# copy logging system disk0:
Destination filename [sea_log.dat]?
Copy in
progress...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
33554432 bytes copied in 112.540 secs (298156 bytes/sec)
```

次に、リモート ファイル コピー機能（rcp）を使用して SEA をコピーする例を示します。

```
Router# copy logging system rcp:
Address or name of remote host []? 192.0.2.1
```

```
Destination username [Router]? username1
Destination filename [sea_log.dat]? /auto/tftpboot-users/username1/sea_log.dat
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
33554432 bytes copied in 48.172 secs (696555 bytes/sec)
```

ヒント　Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CHAPTER 55

Backplane Traffic Monitoring

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

Backplane Traffic Monitoring の前提条件

なし。

Backplane Traffic Monitoring の制約事項

Syslog メッセージ バッファのサイズには制限があります。誤認アラームおよび Syslog メッセージの数を減らすため、次の注意事項に従ってください。

- トラフィックは、バーストで発生する場合があります。モニタリング間隔で発生するバーストが少ない場合、システムに対する容量の過負荷による問題を示すものではありません。このような影響はハードウェア バッファによって吸収され、パケット ドロップの原因とはなりません。たとえば、

モニタリング間隔を 10 秒、しきい値を 80% に設定している場合、トラフィック利用率の測定値は合計で 10 あります。この測定値の内 2 つだけが 90% に到達し、他の 8 つが 20% であると仮定します。ピークのしきい値である 90% を使用してしきい値を比較した場合、不要な警告 Syslog メッセージが生成されます。この場合のしきい値の比較には、10 個の測定値の平均値である 34% を使用して、警告メッセージが生成されないようにすることを推奨します。ピーク値の比較が実際に必要な場合は、間隔を 1 秒に設定できます。間隔を 1 秒に設定すると、測定値が直接しきい値と比較されます。

- Syslog メッセージを生成する Syslog メッセージの数は、しきい値を下回る値からしきい値を超える値までの範囲に相当します。

トラフィック モニタリングに関する情報

Backplane Traffic Monitoring では、バックプレーンおよびファブリックチャネル トラフィックの利用率を設定された間隔およびしきい値でモニタできます。

トラフィック モニタリングにより、スイッチはバックプレーンおよびファブリックチャネルのトラフィック利用率を設定された間隔としきい値でモニタできます。トラフィック利用率が設定されたしきい値を超えた場合または下回った場合は、Syslog メッセージが生成されます。Syslog メッセージのいくつかのタイプの例を次に示します。

- 00:08:03: %TRAFFIC_UTIL-SP-4-MONITOR_BACKPLANE_REACH_THR：バックプレーン トラフィック利用率が 26% であり、10 秒間隔以内にしきい値（20%）に到達しました。
- 00:08:13: %TRAFFIC_UTIL-SP-4-MONITOR_BACKPLANE_BELOW_THR：バックプレーン トラフィック利用率が 18% であり、10 秒間隔以内にしきい値（20%）を下回りました。
- 00:08:44: %TRAFFIC_UTIL-SP-4-MONITOR_FABRIC_IG_REACH_THR：モジュール 1、チャネル 0 入力トラフィック利用率が 5% であり、30 秒間隔以内にしきい値（3%）に到達しました。
- 00:08:44: %TRAFFIC_UTIL-SP-4-MONITOR_FABRIC_EG_REACH_THR：モジュール 1、チャネル 0 出力トラフィック利用率が 5% であり、30 秒間隔以内にしきい値（3%）に到達しました。
- 00:09:14: %TRAFFIC_UTIL-SP-4-MONITOR_FABRIC_IG_BELOW_THR：モジュール 1、チャネル 0 入力トラフィック利用率が 1% であり、30 秒間隔以内にしきい値（3%）を下回りました。
- 00:09:14: %TRAFFIC_UTIL-SP-4-MONITOR_FABRIC_EG_BELOW_THR：モジュール 1、チャネル 0 出力トラフィック利用率が 1% であり、30 秒間隔以内にしきい値（3%）を下回りました。

Backplane Traffic Monitoring のデフォルト設定

- デフォルトのしきい値は、80% です。
- デフォルトでは、トラフィックのモニタはオフです。

Backplane Traffic Monitoring の設定方法

Backplane Traffic Monitoring 機能を設定するには、次の作業の 1 つまたは複数を実行します。

コマンド	目的
Router(config)# **monitor traffic-util backplane interval** *interval* **threshold** *percentage*	バックプレーン利用率トラフィック モニタリングを設定します。
Router(config)# **monitor traffic-util fabric module** {*mod-num* | **all**} {**channel** {**0**|**1**|**both**}} {**direction** {**egress** | **ingress** | **both**}} [**interval** *interval* **threshold** *percentage*]	ファブリック チャネル利用率トラフィック モニタリングを設定します。
Router(config)# **monitor traffic-util fabric logging interval** *second*	トラフィック利用率を上回った場合の、ファブリック チャネル利用率トラフィック モニタの SYSLOG 間隔を設定します。
Router(config)# **monitor traffic-util backplane logging interval** *second*	トラフィック利用率を上回った場合の、トラフィック モニタのバックプレーンの SYSLOG 間隔を設定します。
Router# **show catalyst6000 traffic-meter**	バックプレーン（共有バス）の利用率のパーセンテージとトラフィック モニタ情報を表示します。

インターフェイスの範囲を設定する際に、範囲を示すリストとして *mod-num* を使用できます。各エントリはカンマで区切り、範囲はハイフン（-）で表します。たとえば、1,3,5-9,12 と入力します。

次に、バックプレーン トラフィック利用率のモニタリングをイネーブルにする例を示します。

```
Router(config)# monitor traffic-util backplane logging interval 50 threshold 100
```

次に、バックプレーン トラフィック利用率のモニタリングをディセーブルにする例を示します。

```
Router(config)# no monitor traffic-util backplane
```

次に、特定のモジュールのファブリック チャネルに対してファブリック チャネル トラフィック利用率のモニタ間隔としきい値を指定する例を示します。

```
Router(config)# monitor traffic-util fabric module 8 channel both direction both interval
50 threshold 60
```

次に、特定のファブリック チャネルおよび出力トラフィックだけに対してファブリック チャネル トラフィック利用率のモニタのしきい値を指定する例を示します。

```
Router(config)# monitor traffic-util fabric module 6 channel 0 direction egress interval
100 threshold 90
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

ローカル SPAN、RSPAN、および ERSPAN

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

ローカル SPAN、RSPAN、および ERSPAN の前提条件

なし。

ローカル SPAN、RSPAN、および ERSPAN の制約事項

機能の非互換性

- 出力 SPAN は出力マルチキャスト モードではサポートされていません。（CSCsa95965）。
- 不明なユニキャストフラッディングのブロック（UUFB）ポートは、RSPAN またはローカル SPAN 出力専用宛先として使用できません (CSCsj27695)。
- ポートチャネル インターフェイス（EtherChannel）は SPAN 送信元として使用できますが、EtherChannel のアクティブなメンバ ポートを SPAN 送信元ポートとして設定することはできません。EtherChannel の非アクティブ メンバ ポートは SPAN 送信元として設定できますが、これらのポートは中断ステートになり、トラフィックを伝送しません。
- 次の機能は、SPAN 宛先との互換性がありません。
  - プライベート VLAN
  - IEEE 802.1x ポートベースの認証
  - ポート セキュリティ
  - スパニングツリー プロトコル（STP）および関連機能（PortFast、PortFast BPDU フィルタリング、BPDU ガード、UplinkFast、BackboneFast、EtherChannel ガード、ルート ガード、ループ ガード）
  - VLAN トランキング プロトコル（VTP）
  - ダイナミック トランキング プロトコル（DTP）
  - IEEE 802.1Q トンネリング
- dot1ad uni コマンド（第 41 章「Ethernet Virtual Connections（EVC; イーサネット バーチャル コネクション）」を参照）は、次の SPAN の制約事項を適用します。
  - **dot1ad uni** コマンドでは出力 SPAN の設定を制限しません。
  - **dot1ad uni** コマンドは、RSPAN の入力 SPAN 送信元ポートの設定を制限しませんが、送信元 VLAN フィルタリング、**dot1ad uni** コマンドを使用して設定された RSPAN の入力 SPAN 送信元ポートからのトラフィックには適用されません。
  - **dot1ad uni** コマンドを使用して設定されたポートは、ローカル SPAN または ERSPAN の入力 SPAN 送信元ポートとして使用できません。

（注）
- SPAN 宛先は、IEEE 802.3Z フロー制御に関与できます。
- 出力パケット レプリケーションを使用している IP マルチキャスト スイッチングは、SPAN との互換性がありません。一部の場合、出力レプリケーションでは、SPAN 宛先ポートにマルチキャスト パケットが送信されない結果となることがあります。SPAN を使用していて、スイッチング モジュールが出力レプリケーションに対応している場合、出力レプリケーションを強制するには、**platform ip multicast replication-mode ingress** コマンドを入力します。

ローカル SPAN、RSPAN、および ERSPAN セッションの制限

	ローカル セッションと送信元セッション		宛先セッション	
総セッション数	ローカル SPAN、 RSPAN 送信元、 ERSPAN 送信元 入力と出力のどちらか、または両方	ローカル SPAN の出力のみ	RSPAN	ERSPAN
80	2	14	64	23

ローカル SPAN、RSPAN、および ERSPAN インターフェイスの制限

	ローカル SPAN セッションごと	RSPAN 送信元セッションごと	ERSPAN 送信元セッションごと	RSPAN 宛先セッションごと	ERSPAN 宛先セッションごと
出力または「両方」の送信元	128	128	128	—	—
入力送信元	128	128	128	—	—
RSPAN および ERSPAN 宛先セッションの送信元	—	—	—	1 RSPAN VLAN	1 IP アドレス
セッションごとの宛先	64	1 RSPAN VLAN	1 IP アドレス	64	64

ローカル SPAN、RSPAN、および ERSPAN の一般的な制約事項

- 1 つの出力 SPAN 送信元ポートからトラフィックをコピーした SPAN の宛先は、出力トラフィックだけをネットワーク アナライザに送信します。複数の出力 SPAN 送信元ポートを設定している場合、ネットワーク アナライザに送信されるトラフィックに、出力 SPAN 送信元ポートから受信した特定タイプの入力トラフィックも含まれます。この入力トラフィックのタイプは次のとおりです。
  - VLAN 上でフラッディングしたすべてのユニキャスト トラフィック
  - ブロードキャストおよびマルチキャスト トラフィック

  この状況が発生するのは、出力 SPAN 送信元ポートがこれらのトラフィック タイプを VLAN から受信したあと、自身がトラフィックの送信元であることを認識し、受信したトラフィックの送信元にこのトラフィックを返送せず、ドロップしてしまうためです。SPAN はドロップする前にこのトラフィックをコピーし、SPAN の宛先に送信します。(CSCds22021)
- 再び **monitor session** コマンドを入力しても、前に設定した SPAN パラメータを消去しません。設定済みの SPAN パラメータを消去するには、**no monitor session** コマンドを使用する必要があります。
- ネットワーク アナライザを SPAN 宛先に接続します。

- SPAN セッション内では、すべての SPAN の宛先は、すべてのトラフィックをすべての SPAN 送信元から受信します。ただし、送信元 VLAN フィルタリングが SPAN の送信元に設定されている場合を除きます。
- SPAN の宛先から送信されるトラフィックを選択するよう、宛先トランク VLAN フィルタリングを設定できます。
- レイヤ 2 LAN ポート（**switchport** コマンドで設定された LAN ポート）とレイヤ 3 LAN ポート（**switchport** コマンドを使用せずに設定された LAN ポート）の両方を送信元または宛先として設定できます。
- 1 つのセッションに、個別の送信元ポートおよび送信元 VLAN を混在させることはできません。
- 複数の入力送信元ポートを指定する場合、各ポートはそれぞれ異なる VLAN に属するものであってもかまいません。
- セッション内では、VLAN を SPAN 送信元として設定することと、送信元 VLAN フィルタリングを行うことの、両方を設定することはできません。VLAN を SPAN 送信元として設定するか、または、送信元ポートおよび EtherChannel からのトラフィックの送信元 VLAN フィルタリングを行うことはできますが、同じセッションで両方を行うことはできません。
- 内部 VLAN に対し、送信元 VLAN フィルタリングは設定できません。
- イネーブルなローカル SPAN、RSPAN、および ERSPAN は、すでに入力された設定があれば、その設定を使用します。
- 送信元を指定し、トラフィックの方向（入力、出力、または両方）を指定しない場合、「両方」がデフォルトで使用されます。
- SPAN は、レイヤ 2 イーサネット フレームをコピーしますが、SPAN は送信元トランク ポート 802.1Q タグをコピーしません。宛先をトランクとして設定し、タグ付きトラフィックをトラフィック アナライザにローカルに送信できます。

（注） トランクとして設定した宛先は、レイヤ 3 LAN 送信元からのトラフィックを、レイヤ 3 LAN 送信元によって使用される内部 VLAN としてタグを付けます。

- ローカル SPAN セッション、RSPAN 送信元セッション、および ERSPAN 送信元セッションは、RSPAN VLAN を伝送する送信元トランク ポートから送信元 RSPAN VLAN トラフィックをローカルにコピーしません。
- ローカル SPAN セッション、RSPAN 送信元セッション、および ERSPAN 送信元セッションは、送信元ポートからローカルに送信された ERSPAN GRE カプセル化トラフィックをコピーしません。
- ポートまたは EtherChannel は、1 つの SPAN セッションでのみ SPAN の宛先にできます。SPAN セッションは、共有の宛先にはできません。
- SPAN の宛先は、SPAN の送信元にはできません。
- 宛先は、スパニングツリー インスタンスには関与しません。ローカル SPAN はモニタ対象トラフィックに BPDU を含めます。したがってモニタリングの宛先で確認される BPDU は、送信元から送られたものです。RSPAN は BPDU モニタリングをサポートしません。
- 出力 SPAN 送信元として設定されているポートからの伝送用にスイッチを経由して転送されるすべてのパケットは、SPAN 宛先にコピーされます。このパケットには、STP が出力ポートをブロッキング ステートにするため出力ポート経由でスイッチから送出されないパケットや、STP が VLAN をトランク ポートでブロッキング ステートに移行するので、出力トランク ポートにあるパケットが含まれます。

VSPAN の制約事項

（注）　ローカル SPAN、RSPAN、および ERSPAN は、すべて VSPAN をサポートします。

- VSPAN セッションは、送信元 VLAN フィルタリングをサポートしません。
- 入力および出力の両方が設定されている VSPAN セッションについては、2 つのパケットが同じ VLAN でスイッチングされている場合、それらは宛先から（1 つは入力ポートからの入力トラフィックとして、もう 1 つは出力ポートからの出力トラフィックとして）アナライザへ転送されます。
- VSPAN は、VLAN 内のレイヤ 2 ポートを出入りするトラフィックだけをモニタします。
  - VLAN を入力送信元として設定し、トラフィックがモニタ対象 VLAN にルーティングされる場合、ルーティングされたトラフィックは、VLAN 内のレイヤ 2 ポートで受信する入力トラフィックとして見なされないため、モニタされません。
  - VLAN を出力送信元として設定し、トラフィックがモニタ対象 VLAN からルーティングされる場合、ルーティングされたトラフィックは、VLAN 内のレイヤ 2 ポートから送信される出力トラフィックとして見なされないため、モニタされません。

RSPAN の制約事項

- 参加しているすべてのスイッチは、レイヤ 2 トランクによって接続されている必要があります。
- RSPAN VLAN をサポートするネットワーク デバイスは、RSPAN 中間デバイスとすることができます。
- ネットワークが伝送する RSPAN VLAN の数に制限はありません。
- 中間ネットワーク デバイスでは、サポートできる RSPAN VLAN の数が制限される場合があります。
- すべての送信元、中間、宛先ネットワーク デバイスにおいて、RSPAN VLAN を設定しなければなりません。VLAN トランキング プロトコル（VTP）がイネーブルの場合、1 ～ 1024 の番号が付いた VLAN の設定を RSPAN VLAN として伝播できます。1024 より大きい番号の VLAN は、すべての送信元、中間、および宛先ネットワーク デバイスで、RSPAN VLAN として手動で設定する必要があります。
- VTP および VTP プルーニングをイネーブルにすると、RSPAN トラフィックはトランクでプルーニングされて、RSPAN トラフィックがネットワーク全体に不必要にフラッディングするのを防ぎます。
- RSPAN VLAN は、RSPAN トラフィックに対してだけ使用できます。
- 管理トラフィックを伝送するのに使用する VLAN を、RSPAN VLAN として設定しないでください。
- アクセス ポートを RSPAN VLAN に割り当てないでください。RSPAN は、RSPAN VLAN 中のアクセス ポートを中断ステートにします。
- RSPAN VLAN 内の RSPAN トラフィックの伝送用に選択されたトランク ポート以外のポートは設定しないでください。
- MAC アドレス ラーニングは、RSPAN VLAN 上でディセーブルです。
- RSPAN 送信元スイッチの RSPAN VLAN 上にある出力アクセス コントロール リスト（ACL）を使用して、RSPAN 宛先へ送信されるトラフィックをフィルタリングできます。

- RSPAN は BPDU モニタリングをサポートしません。
- RSPAN VLAN を VSPAN セッション中の送信元として設定しないでください。
- すべての関与しているネットワーク デバイスが RSPAN VLAN の設定をサポートし、すべての関与しているネットワーク デバイスで各 RSPAN セッションに対して同じ RSPAN VLAN を使用する限り、VLAN を RSPAN VLAN として設定できます。

ERSPAN の制約事項

- ERSPAN パケットでは、GRE ヘッダー内の「protocol type」フィールドの値は 0x88BE です。
- レイヤ 3 ERSPAN パケットのペイロードは、コピーされたレイヤ 2 イーサネット フレームからすべての 802.1Q タグを取り除いたものです。
- ERSPAN は、コピーされた個々のレイヤ 2 イーサネット フレームに 50 バイトのヘッダーを追加し、4 バイトの巡回冗長検査（CRC）トレーラーと置き換えます。
- ERSPAN は、最大 9,202 バイトのレイヤ 3 パケットを保持するジャンボ フレームをサポートします。コピーされたレイヤ 2 イーサネット フレームの長さが 9,170（9,152 バイトのレイヤ 3 パケット）を超える場合は、ERSPAN はコピーされたレイヤ 2 イーサネット フレームを切り捨て、9,202 バイトの ERSPAN レイヤ 3 パケットを作成します。

（注）　切り捨てられたパケットのレイヤ 3 IP ヘッダーは切り捨てられていないレイヤ 3 パケットのサイズを保持します。6500 である ERSPAN 宛先のレイヤ 2 フレームとレイヤ 3 パケット間の長さの整合性検査は、ERSPAN 宛先 6500 スイッチで **no platform verify ip length consistent** グローバル コンフィギュレーション コマンドを設定しない限り、切り捨てられた ERSPAN パケットをドロップします。

- 設定された MTU サイズとは関係なく、ERSPAN は最長 9,202 バイトのレイヤ 3 パケットを作成します。ERSPAN トラフィックは、MTU サイズを 9,202 バイト未満に規定しているネットワーク内のインターフェイスによってドロップされる可能性があります。
- デフォルトの MTU サイズ（1,500 バイト）の場合、コピーされたレイヤ 2 イーサネット フレームの長さが 1,468 バイト（1,450 バイトのレイヤ 3 パケット）を超えると、MTU サイズを 1,500 バイトに規定しているネットワーク内のインターフェイスによって ERSPAN トラフィックがドロップされます。

（注）　**mtu** インターフェイス コマンド、および **system jumbomtu** コマンド（「ジャンボ フレーム サポートの設定」（P.10-6）を参照）は、レイヤ 3 パケットの最大サイズを設定します（デフォルト値は 1,500 バイト、最大値は 9,216 バイト）。

- 参加しているすべてのスイッチはレイヤ 3 に接続されている必要があり、ネットワーク パスが ERSPAN トラフィックのサイズをサポートしている必要があります。
- ERSPAN はパケット分割をサポートしません。ERSPAN パケットの IP ヘッダー内には、「do not fragment」ビットが設定されます。ERSPAN 宛先セッションでは、分割された ERSPAN パケットを再構成できません。
- ERSPAN トラフィックは、ネットワークのトラフィック負荷条件の影響を受けます。ERSPAN パケットの IP precedence または DSCP 値を設定することで、QoS において ERSPAN トラフィックを優先できます。
- ERSPAN トラフィックでサポートされる唯一の宛先は、ERSPAN 宛先セッションです。

- スイッチ上のすべての ERSPAN 送信元セッションには、同一の起点 IP アドレスを使用する必要があります。これは、**origin ip address** コマンドで設定します（「ERSPAN 送信元セッションの設定」（P.56-27）を参照）。
- スイッチ上のすべての ERSPAN 宛先セッションは、同じ宛先インターフェイス上の同一の IP アドレスを使用する必要があります。宛先インターフェイスの IP アドレスは、**ip address** コマンドを使用して入力します（「ERSPAN 宛先セッションの設定」（P.56-29）を参照）。
- ERSPAN 送信元セッションの宛先 IP アドレス（宛先スイッチのインターフェイス上で設定する必要がある）は、ERSPAN 宛先セッションが宛先ポートまで送信するトラフィックの送信元です。**ip address** コマンドを使用して、送信元セッションおよび宛先セッションの両方に同一のアドレスを設定します。
- ERSPAN ID は、さまざまな ERSPAN 送信元セッションから送られ、同一の宛先 IP アドレスに到着した ERSPAN トラフィックを区別します。

分散型出力 SPAN モードの制約事項

一部のスイッチング モジュールには、ERSPAN 送信元に対する分散型出力 SPAN モードをサポートしない ASIC があります。

ERSPAN 送信元に対して分散型出力 SPAN モードをサポートしないスイッチング モジュールのスロット番号を表示するには、**show monitor session egress replication-mode | include Distributed.*Distributed.*Centralized** コマンドを入力します。

ERSPAN 送信元に対して分散型出力 SPAN モードがサポートされないスロットにあるスイッチング モジュールの ASIC のバージョンを表示するには、**show asic-version slot** *slot_number* コマンドを入力します。

Hyperion ASIC バージョン レベル 5.0 以上および Metropolis ASIC のすべてのバージョンは、ERSPAN 送信元に対する分散型出力 SPAN モードをサポートします。Hyperion ASIC バージョン レベル 5.0 未満のスイッチング モジュールは、ERSPAN 送信元に対する分散型出力 SPAN モードをサポートしません。

ローカル SPAN、RSPAN、および ERSPAN について

ローカル SPAN、RSPAN、および ERSPAN の概要

SPAN の操作

SPAN は、1 つ以上のポート、1 つ以上の EtherChannel、または 1 つ以上の VLAN からトラフィックをコピーし、SwitchProbe デバイスまたは他の Remoter Monitoring（RMON）プローブなどのネットワーク アナライザが分析できるように、1 つ以上の宛先にコピーしたトラフィックを送信します。トラフィックは、第 60 章「ミニ プロトコル アナライザ」で説明されているように、ミニ プロトコル アナライザでパケットをキャプチャするために送信することもできます。

SPAN は、送信元上のトラフィックのスイッチングには影響しません。その宛先は、SPAN 専用に設定する必要があります。SPAN が生成したトラフィックのコピーは、送信元スイッチのユーザ トラフィックと競合します。

ローカル SPAN の概要

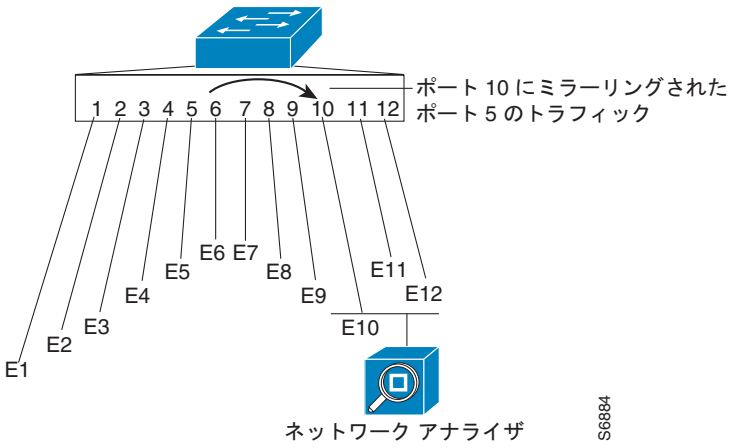
ローカル SPAN セッションは、送信元ポートおよび送信元 VLAN を、1 つまたは複数の宛先に対応付けたものです。ローカル SPAN セッションは、単一スイッチの上に設定します。ローカル SPAN には、個別の送信元および宛先のセッションはありません。

ローカル SPAN セッションは、RSPAN VLAN を伝送する送信元トランク ポートから送信元 RSPAN VLAN トラフィックをローカルにコピーしません。ローカル SPAN セッションは、送信元ポートからローカルに送信された RSPAN VLAN GRE（総称ルーティング カプセル化）カプセル化トラフィックをコピーしません。

ローカル SPAN セッションごとに、送信元としてポートまたは VLAN を使用することはできますが、両方は使用できません。

ローカル SPAN は、任意の VLAN 上の 1 つまたは複数の送信元ポートからのトラフィック、あるいは 1 つまたは複数の VLAN からのトラフィックを分析するために宛先へコピーします（図 56-1 を参照）。たとえば図 56-1 の場合、イーサネット ポート 5（送信元ポート）上の全トラフィックが、イーサネット ポート 10 にコピーされます。イーサネット ポート 10 のネットワーク アナライザは、イーサネット ポート 5 に物理的に接続していなくても、このポートからのあらゆるトラフィックを受信できます。

図 56-1　　SPAN の設定例



RSPAN の概要

RSPAN は、さまざまなスイッチ上の送信元ポート、送信元 VLAN、および宛先をサポートし、ネットワーク全体に存在する複数のスイッチをリモート モニタします（図 56-2 を参照）。RSPAN は、レイヤ 2 VLAN を使用して、スイッチ間の SPAN トラフィックを伝送します。

RSPAN は、RSPAN 送信元セッション、RSPAN VLAN、および RSPAN 宛先セッションで構成されています。異なるスイッチで RSPAN 送信元セッションおよび宛先セッションを個別に設定します。1 つのスイッチ上で RSPAN 送信元セッションを設定するには、一連の送信元ポートまたは VLAN を 1 つの RSPAN VLAN に対応付けます。別のスイッチ上で RSPAN 宛先セッションを設定するには、宛先を RSPAN VLAN に対応付けます。

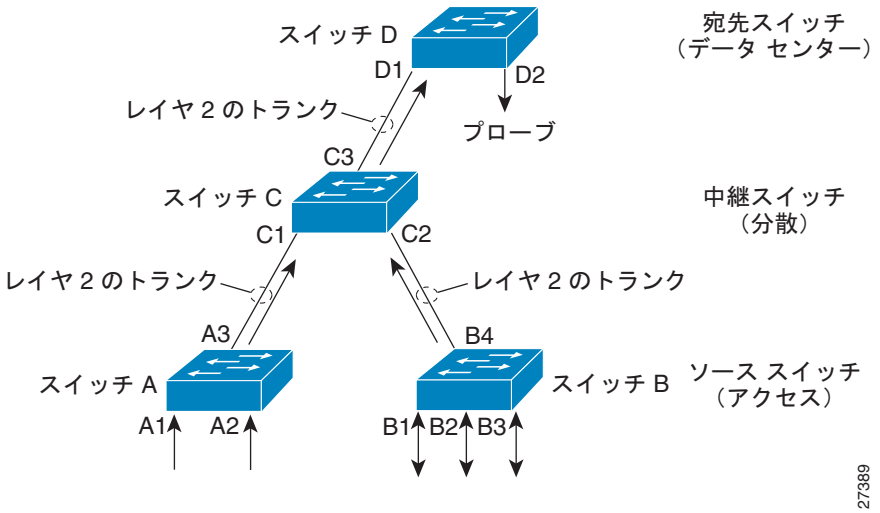
各 RSPAN セッションのトラフィックは、レイヤ 2 非ルーティング トラフィックとして、ユーザが指定した RSPAN VLAN 上で伝送されます。この RSPAN VLAN は、参加しているすべてのスイッチの RSPAN セッション専用です。参加しているすべてのスイッチは、レイヤ 2 によってトランク接続されている必要があります。

RSPAN 送信元セッションは、RSPAN VLAN を伝送する送信元トランク ポートから送信元 RSPAN VLAN トラフィックをローカルにコピーしません。RSPAN 送信元セッションは、送信元 RSPAN GRE でカプセル化されたトラフィックを送信元ポートからローカルにコピーしません。

RSPAN 送信元セッションごとに、送信元としてポートまたは VLAN を使用することはできますが、両方は使用できません。

RSPAN 送信元セッションは、送信元ポートまたは送信元 VLAN からトラフィックをコピーし、RSPAN VLAN 上のトラフィックを RSPAN 宛先セッションへスイッチングします。RSPAN 宛先セッションでは、トラフィックを宛先にスイッチングします。

図 56-2　　RSPAN の設定



ERSPAN の概要

ERSPAN は、さまざまなスイッチ上の送信元ポート、送信元 VLAN、および宛先ポートをサポートし、ネットワーク全体に存在する複数のスイッチをリモート モニタします（図 56-3 を参照）。ERSPAN は、GRE トンネルを使用して、スイッチ間のトラフィックを伝送します。

ERSPAN は、ERSPAN 送信元セッション、ルーティング可能な ERSPAN GRE カプセル化トラフィック、および ERSPAN 宛先セッションで構成されています。異なるスイッチで ERSPAN 送信元セッションおよび宛先セッションを個別に設定します。

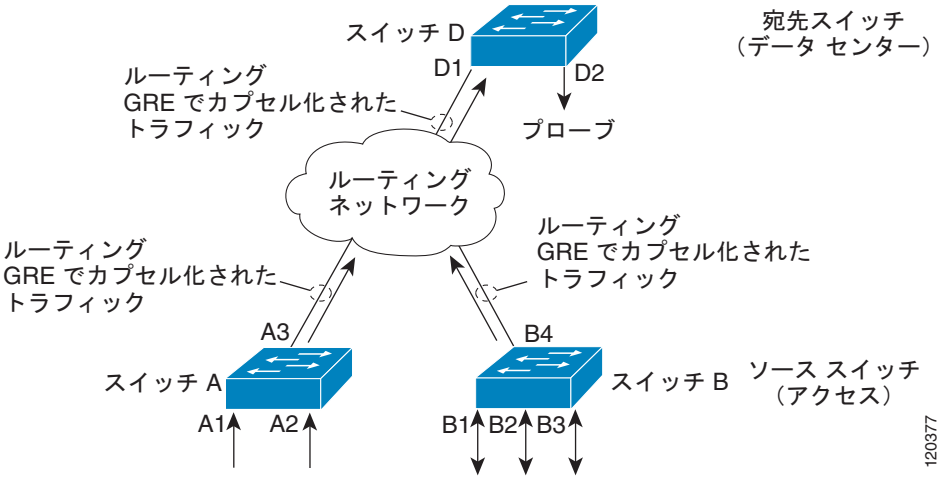
ERSPAN 送信元セッションを 1 つのスイッチ上で設定するには、送信元ポートまたは VLAN のセットを宛先 IP アドレス、ERSPAN ID 番号、およびオプションとして VRF（VPN ルーティング/転送）名に対応付けます。ERSPAN 宛先セッションを別のスイッチ上で設定するには、宛先を送信元 IP アドレス、ERSPAN ID 番号、およびオプションとして VRF 名に対応付けます。

ERSPAN 送信元セッションは、RSPAN VLAN を伝送する送信元トランク ポートから送信元 RSPAN VLAN トラフィックをローカルにコピーしません。ERSPAN 送信元セッションは、送信元 ERSPAN GRE でカプセル化されたトラフィックを送信元ポートからローカルにコピーしません。

ERSPAN 送信元セッションごとに、送信元としてポートまたは VLAN を使用することはできますが、両方は使用できません。

ERSPAN 送信元セッションは、送信元ポートまたは送信元 VLAN からのトラフィックをコピーし、このトラフィックを、ルーティング可能な GRE カプセル化パケットを使用して ERSPAN 宛先セッションに転送します。ERSPAN 宛先セッションはトラフィックを宛先へスイッチングします。

図 56-3　　ERSPAN の設定



SPAN 送信元でのトラフィックのモニタリング

- 「モニタ対象トラフィックの方向」（P.56-11）
- 「モニタ対象トラフィックのタイプ」（P.56-11）
- 「重複トラフィック」（P.56-11）

モニタ対象トラフィックの方向

ローカル SPAN セッション、RSPAN 送信元セッション、および ERSPAN 送信元セッションを設定して、次のトラフィックをモニタできます。

- 入力トラフィック
  - 呼び出された入力 SPAN。
  - 送信元が受信するトラフィックをコピーします（入力トラフィック）。
  - 入力トラフィックは、コピーされるスーパーバイザ エンジン SPAN ASIC に送信されます。
- 出力トラフィック
  - 呼び出された出力 SPAN。
  - 送信元から送信するトラフィックをコピーします（出力トラフィック）。
  - 分散型出力 SPAN モード：一部のファブリック対応スイッチング モジュールでは、出力トラフィックがスイッチング モジュール SPAN ASIC によってローカルにコピーされ、SPAN 宛先に送信されます。分散型出力 SPAN モードをサポートするスイッチング モジュールについては、「分散型出力 SPAN モードの制約事項」（P.56-7）を参照してください。
  - 集中型出力 SPAN モード：他のすべてのスイッチング モジュールでは、出力トラフィックがコピーされるスーパーバイザ エンジン SPAN ASIC に送信され、さらに SPAN 宛先に送信されます。
- 両方
  - 受信トラフィックと送信トラフィックの両方をコピーします（入力および出力トラフィック）。
  - 入力トラフィックと出力トラフィックのいずれも、コピーされるスーパーバイザ エンジン SPAN ASIC に送信されます。

モニタ対象トラフィックのタイプ

デフォルトでは、ローカル SPAN および ERSPAN がマルチキャスト フレームおよびブリッジ プロトコル データ ユニット（BPDU）フレームを含む、すべてのトラフィックをモニタリングします。RSPAN は BPDU モニタリングをサポートしません。

重複トラフィック

設定によっては、SPAN が、同じ送信元のトラフィックの複数のコピーを、宛先に送信します。たとえば、双方向 SPAN（入力および出力の両方）セッションが、s1 および s2 の 2 つを SPAN 送信元、d1 を SPAN の宛先として設定している場合、パケットが s1 からスイッチに入って、出力パケットとしてスイッチから s2 に送信されると、s1 の入力 SPAN および s2 の出力 SPAN 両方が、パケットのコピーを SPAN の宛先 d1 に送信します。パケットが s1 から s2 へスイッチングされたレイヤ 2 だった場合、両方の SPAN パケットは同一になります。パケットが s1 から s2 にスイッチングされたレイヤ 3 だった場合は、レイヤ 3 書き換えによって送信元および宛先レイヤ 2 アドレスが変更され、SPAN パケットは異なるものとなります。

ローカル SPAN、RSPAN、および ERSPAN の送信元

- 「送信元ポートと EtherChannel」（P.56-12）
- 「送信元 VLAN」（P.56-12）

送信元ポートと EtherChannel

送信元ポートまたは EtherChannel は、トラフィック分析のためにモニタされるポートまたは EtherChannel です。レイヤ 2 およびレイヤ 3 のポートと EtherChannel はいずれも、SPAN 送信元として設定できます。SPAN は、1 つまたは複数の送信元ポートまたは EtherChannel を、単一の SPAN セッションでモニタできます。任意の VLAN に、SPAN 送信元としてポートまたは EtherChannel を設定できます。トランク ポートまたは EtherChannel を、送信元として設定したり、非トランク送信元と混在させることができます。

（注）　SPAN は、トランク送信元からのカプセル化をコピーしません。SPAN 宛先をトランクとして設定し、分析用に送信される前に、モニタ対象トラフィックにタグを付けることができます。

送信元 VLAN

送信元 VLAN は、トラフィック分析のためにモニタ対象になる VLAN です。VLAN-based SPAN（VSPAN）は、VLAN を SPAN 送信元として使用します。送信元 VLAN にあるすべてのポートおよび EtherChannel が、SPAN トラフィックの送信元になります。

（注）　送信元 VLAN 上のレイヤ 3 VLAN インターフェイスは、SPAN トラフィックの送信元ではありません。レイヤ 3 VLAN インターフェイスを介して VLAN に入ってくるトラフィックは、送信元 VLAN にある出力ポートまたは EtherChannel を介してスイッチから送信されるときにモニタされます。

ローカル SPAN、RSPAN、および ERSPAN の宛先

SPAN 宛先ポートは、ローカル SPAN、RSPAN、または ERSPAN が分析用のトラフィックを送信するレイヤ 2 ポート、レイヤ 3 ポートまたは EtherChannel です。ポートまたは EtherChannel を SPAN の宛先として設定すると、そのポートは SPAN 機能専用になります。

宛先 EtherChannel は、Port Aggregation Control Protocol（PAgP）または Link Aggregation Control Protocol（LACP）EtherChannel プロトコルをサポートしません。すべての EtherChannel プロトコルのサポートがディセーブルになっているときだけ、オン モードがサポートされます。

宛先 EtherChannel のメンバ リンクが、EtherChannel がサポートされるデバイスに接続される際の、要件はありません。たとえば、メンバ リンクに接続し、ネットワーク アナライザと分離できます。EtherChannel についての詳細は、第 22 章「EtherChannel」を参照してください。

デフォルトでは、宛先で、任意のトラフィックを受信することはできません。任意の接続デバイスからトラフィックを受信するようにレイヤ 2 宛先を設定できます。

デフォルトでは、宛先で、SPAN 以外のトラフィックは送信されません。トラフィックを受信するために設定したレイヤ 2 の宛先は、宛先に接続された任意のデバイスのレイヤ 2 アドレスを認識し、そのデバイスあてに送信されるトラフィックを送信するよう、設定できます。

トランクは宛先として設定でき、これによってトランク宛先がカプセル化トラフィックを送信できるようになります。許可される VLAN のリストを使用して、宛先トランク VLAN フィルタリングを設定できます。

ローカル SPAN、RSPAN、および ERSPAN のデフォルト設定

- ローカル SPAN：ディセーブル
- RSPAN：ディセーブル
- ERSPAN：ディセーブル
- 出力 SPAN セッションのデフォルト操作モード：集中型

ローカル SPAN、RSPAN、および ERSPAN の設定方法

無条件トランクとしての宛先ポートの設定（任意）

モニタ対象トラフィックが宛先を通過するときにタグ付けされるように宛先を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	`Router# 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	`Router(config)# interface {type slot/port | 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 3	`Router(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（この操作はインターフェイスがレイヤ 2 スイッチング用に設定されていない場合にだけ必要です）。
ステップ 4	`Router(config-if)# switchport trunk encapsulation dot1q`	カプセル化を設定して、インターフェイスを 802.1Q トランクとして設定します。
ステップ 5	`Router(config-if)# switchport mode trunk`	無条件にインターフェイスをトランクに設定します。

次に、無条件 IEEE 802.1Q トランクとしてポートを設定する例を示します。

```
Router(config)# interface gigabitethernet 5/12
Router(config-if)# switchport
Router(config-if)# switchport trunk encapsulation dot1q
Router(config-if)# switchport mode trunk
```

宛先トランクの VLAN フィルタリングの設定（任意）

（注）
- トランク上での VLAN のフィルタリングに加え、許可される VLAN リストも適用してポートにアクセスできます。
- 宛先トランクの VLAN フィルタリングは、宛先に適用されます。宛先トランク VLAN フィルタリングを使用する場合、SPAN の送信元から SPAN の宛先に送信されるトラフィックの量は削減されません。

宛先がトランクの場合、トランクで許可される VLAN のリストを使用して宛先から送信されるトラフィックをフィルタリングできます （CSCeb01318）。

宛先トランク VLAN フィルタリングを使用すると、SPAN セッション内で、すべての宛先がすべての送信元からのトラフィックを全部受信するという制限が解除されます。宛先トランク VLAN フィルタリングを使用すると、各宛先トランクからネットワーク アナライザに送信されるトラフィックを VLAN 単位で選択できます。

宛先トランク VLAN フィルタリングを宛先トランク上に設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# 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	`Router(config)# interface type slot/port`	設定する宛先トランク ポートを選択します。
ステップ 3	`Router(config-if)# switchport trunk allowed vlan {add | except | none | remove} vlan [,vlan[,vlan[,...]]]`	トランク上で許可される VLAN のリストを設定します。

- *vlan* パラメータは、1 ～ 4094 の間の 1 つの VLAN 番号、または 2 つの VLAN 番号で指定する（小さい方の数を先にして、間をダッシュで区切る）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。
- デフォルトでは、すべての VLAN が許可されます。
- 許可リストからすべての VLAN を削除するには、**switchport trunk allowed vlan none** コマンドを入力します。
- 許可リストに VLAN を追加するには、**switchport trunk allowed vlan add** コマンドを入力します。
- SPAN 設定を削除しないで、許可 VLAN リストを変更できます。

次に、複数の VLAN が送信元で複数のトランク ポートが宛先であるローカル SPAN セッションを設定する例を示します。宛先トランク VLAN フィルタリングは SPAN トラフィックをフィルタリングし、各宛先トランク ポートが、1 つの VLAN からトラフィックを伝送します。

```
interface GigabitEthernet1/1
description SPAN destination interface for VLAN 10
no ip address
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10
switchport mode trunk
switchport nonegotiate
!
interface GigabitEthernet1/2
```

```
description SPAN destination interface for VLAN 11
no ip address
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 11
switchport mode trunk
switchport nonegotiate
!
interface GigabitEthernet1/3
description SPAN destination interface for VLAN 12
no ip address
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 12
switchport mode trunk
switchport nonegotiate
!
interface GigabitEthernet1/4
description SPAN destination interface for VLAN 13
no ip address
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 13
switchport mode trunk
switchport nonegotiate
!
monitor session 1 source vlan 10 - 13
monitor session 1 destination interface Gi1/1 - 4
```

宛先ポートの許可リストの設定（任意）

ポートを誤って宛先として設定してしまうことがないように、宛先として有効なポートのリストを示す許可リストを作成できます。宛先ポートの許可リストを設定すると、許可リスト内のポートだけが宛先として設定できるようになります。

宛先ポートの許可リ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	Router# **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	Router(config)# **monitor permit-list**	宛先ポートの許可リストの使用をイネーブルにします。
ステップ 3	Router(config)# **monitor permit-list destination interface** *type slot/port*[**-***port*] [**,** *type slot/port* **-** *port*]	宛先ポートの許可リストを設定するか、または既存の宛先ポートの許可リストに追加します。

次に、ギガビット イーサネット ポート 5/1 ～ 5/4、および 6/1 を含む宛先ポートの許可リストを設定する例を示します。

```
Router# configure terminal
Router(config)# monitor permit-list
Router(config)# monitor permit-list destination interface gigabitethernet 5/1-4,
gigabitethernet 6/1
```

次に、設定を確認する例を示します。

```
Router(config)# do show monitor permit-list
 SPAN Permit-list      :Admin Enabled
 Permit-list ports     :Gi5/1-4,Gi6/1
```

出力 SPAN モードの設定（任意）

集中型出力 SPAN モードがデフォルトとなります。分散型出力 SPAN モードをサポートするスイッチング モジュールについては、「分散型出力 SPAN モードの制約事項」（P.56-7）を参照してください。

出力 SPAN 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	`Router# 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	`Router(config)# monitor session egress replication-mode distributed`	分散型出力 SPAN モードをイネーブルにします。 （注）　集中型出力 SPAN モードをイネーブルにするには、**no monitor session egress replication-mode distributed** コマンドを入力します。
ステップ 3	`Router(config)# end`	コンフィギュレーション モードを終了します。

次に、分散型出力 SPAN モードをイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# monitor session egress replication-mode distributed
Router(config)# end
```

次に、分散型出力 SPAN モードをディセーブルにする例を示します。

```
Router# configure terminal
Router(config)# monitor session egress replication-mode centralized
Router(config)# end
```

次に、設定された出力 SPAN モードを表示する例を示します。

```
Router# show monitor session egress replication-mode | include Configured
Configured mode  : Centralized
```

ローカル SPAN の設定

- 「ローカル SPAN の設定（SPAN コンフィギュレーション モード）」（P.56-17）
- 「ローカル SPAN の設定（グローバル コンフィギュレーション モード）」（P.56-19）

ローカル SPAN の設定（SPAN コンフィギュレーション モード）

（注）　宛先を脱退するときにモニタ対象トラフィックにタグを付けるには、無条件で宛先をトランクに設定してから、宛先として設定する必要があります（「無条件トランクとしての宛先ポートの設定（任意）」（P.56-13）を参照）。

SPAN コンフィギュレーション モードでローカル SPAN セッションを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# 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	`Router(config)# monitor session` *local_SPAN_session_number* `type [local | local-tx]`	ローカル SPAN セッション番号を設定し、ローカル SPAN セッション コンフィギュレーション モードを開始します。 **（注）** • 入力もしくは出力、またはその両方の SPAN セッションを設定するには、**local** キーワードを入力します。 • 出力だけの SPAN セッションを設定するには、**local-tx** キーワードを入力します。
ステップ 3	`Router(config-mon-local)# description` *session_description*	（任意）ローカル SPAN セッションの説明を入力します。
ステップ 4	`Router(config-mon-local)# source {`*single_interface* | *interface_list* | *interface_range* | *mixed_interface_list* | *single_vlan* | *vlan_list* | *vlan_range* | *mixed_vlan_list*`} [rx | tx | both]`	ローカル SPAN セッション番号を送信元ポートまたは VLAN に関連付け、モニタするトラフィック方向を選択します。 **（注）** • **local-tx** キーワードを入力するとき、**rx** および **both** キーワードは使用できなくなり、**tx** キーワードが必要になります。 • 使用可能な SPAN セッションを最大限に活用するには、**tx** 付きで **local** セッションを使用する代わりに、常に **local-tx** セッションを使用することを推奨します。
ステップ 5	`Router(config-mon-local)# filter` *single_vlan* | *vlan_list* | *vlan_range* | *mixed_vlan_list*	（任意）ローカル SPAN 送信元がトランク ポートである場合、送信元 VLAN フィルタリングを設定します。
ステップ 6	`Router(config-mon-local)# destination {`*single_interface* | *interface_list* | *interface_range* | *mixed_interface_list*`} [ingress [learning]]`	ローカル SPAN セッション番号を宛先と関連付けます。
ステップ 7	`Router(config-mon-local)# no shutdown`	ローカル SPAN セッションを開始します。 **（注）**　**no shutdown** コマンドおよび **shutdown** コマンドは、local-tx 出力専用 SPAN セッションではサポートされていません。
ステップ 8	`Router(config-mon-local)# end`	コンフィギュレーション モードを終了します。

- *session_description* には最大 240 文字を使用できますが、特殊文字は使用できません。説明にスペースを含めることができます。

（注）　**description** コマンドのあとに、240 文字を入力できます。

- *local_span_session_number* の範囲は、1 ～ 80 です。
- *single_interface* は次のとおりです。
  - **interface** *type slot/port* の形式で、*type* は、**fastethernet**、**gigabitethernet**、または **tengigabitethernet** になります。
  - **interface port-channel** *number*

（注）　宛先ポート チャネル インターフェイスは、**channel-group** *group_num* **mode on** コマンドおよび **no channel-protocol** コマンドで設定する必要があります。「EtherChannel の設定方法」（P.22-8）を参照してください。

- *interface_list* は *single_interface* , *single_interface* , *single_interface* ... です。

（注）　各リストでは、カンマの前後にスペースを入れる必要があります。各範囲では、ダッシュの前後にスペースを入れる必要があります。

- *interface_range* は、**interface** *type slot/first_port - last_port* です。
- *mixed_interface_list* は、順不同で *single_interface* , *interface_range* , ... です。
- *single_vlan* は、単一の VLAN の ID 番号です。
- *vlan_list* は *single_vlan* , *single_vlan* , *single_vlan* ... です。
- *vlan_range* は、*first_vlan_ID - last_vlan_ID* です。
- *mixed_vlan_list* は、順不同で *single_vlan* , *vlan_range* , ... です。
- **ingress** キーワードを入力し、接続デバイスからトラフィックを受信する宛先を設定します。
- **learning** キーワードを入力して、宛先から MAC アドレス ラーニングをイネーブルにします。これにより、スイッチによって、宛先に接続されているデバイスに対してトラフィックを送信できます。

  ingress キーワードと **learning** キーワードで宛先を設定する際は、次の点に注意してください。
  - レイヤ 2 スイッチング用の宛先を設定します。「レイヤ 2 スイッチング用の LAN インターフェイスの設定方法」（P.20-6）を参照してください。
  - 宛先がトランクで、接続デバイスがタグなしトラフィックをスイッチに返信する場合、設定されているネイティブ VLAN で 802.1Q トランキングを使用して、接続デバイスからのトラフィックを受信します。
  - レイヤ 3 アドレスに宛先を設定しないでください。VLAN インターフェイスを使用して、宛先に接続されているデバイスとの間でトラフィックを送受信します。
  - 宛先はダウン ステートのままです。接続デバイスとの間でトラフィックを送受信するには、追加のアクティブなレイヤ 2 ポートを VLAN に設定し、VLAN インターフェイスがアップされたままになるようにします。

次に、セッション 1 がギガビット イーサネット ポート 1/1 からの入力トラフィックをモニタするように設定し、さらにギガビット イーサネット ポート 1/2 を宛先として設定する例を示します。

```
Router(config)# monitor session 1 type local
Router(config-mon-local)# source interface gigabitethernet 1/1 rx
Router(config-mon-local)# destination interface gigabitethernet 1/2
```

詳細については、「SPAN のコンフィギュレーション例」（P.56-32）を参照してください。

ローカル SPAN の設定（グローバル コンフィギュレーション モード）

（注）

- 宛先を脱退するときにモニタ対象トラフィックにタグを付けるには、無条件で宛先をトランクに設定してから、宛先として設定する必要があります（「無条件トランクとしての宛先ポートの設定（任意）」（P.56-13）を参照）。
- グローバル コンフィギュレーション モードでは、最大 2 つまでのローカル SPAN セッションを設定できます。
- すべての SPAN 設定作業に対して、SPAN コンフィギュレーション モードを使用できます。
- サポートされる最大数の SPAN を設定するには、SPAN コンフィギュレーション モードを使用する必要があります。

ローカル SPAN は、個別の送信元および宛先セッションを使用しません。ローカル SPAN セッションを設定するには、ローカル SPAN 送信元および宛先に同じセッション番号を設定します。ローカル SPAN セッションを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# 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	`Router(config)# monitor session` *local_span_session_number* **source** {*single_interface* | *interface_list* | *interface_range* | *mixed_interface_list* | *single_vlan* | *vlan_list* | *vlan_range* | *mixed_vlan_list*} [**rx** | **tx** | **both**]	ローカル SPAN 送信元セッション番号を送信元ポートまたは VLAN に関連付け、モニタするトラフィック方向を選択します。
ステップ 3	`Router(config)# monitor session` *local_span_session_number* **destination** {*single_interface* | *interface_list* | *interface_range* | *mixed_interface_list*} [**ingress** [**learning**]]	ローカル SPAN セッション番号と宛先を関連付けます。

- *local_span_session_number* の範囲は、1 ～ 80 です。
- *single_interface* は次のとおりです。
  - **interface** *type slot/port* の形式で、*type* は、**fastethernet**、**gigabitethernet**、または **tengigabitethernet** になります。
  - **interface port-channel** *number*

（注）　宛先ポート チャネル インターフェイスは、**channel-group** *group_num* **mode on** コマンドおよび **no channel-protocol** コマンドで設定する必要があります。「EtherChannel の設定方法」（P.22-8）を参照してください。

- *interface_list* は *single_interface* , *single_interface* , *single_interface* ... です。

（注）　各リストでは、カンマの前後にスペースを入れる必要があります。各範囲では、ダッシュの前後にスペースを入れる必要があります。

- *interface_range* は、**interface** *type slot/first_port* - *last_port* です。
- *mixed_interface_list* は、順不同で *single_interface* , *interface_range* , ... です。
- *single_vlan* は、単一の VLAN の ID 番号です。
- *vlan_list* は *single_vlan* , *single_vlan* , *single_vlan* ... です。
- *vlan_range* は、*first_vlan_ID* - *last_vlan_ID* です。
- *mixed_vlan_list* は、順不同で *single_vlan* , *vlan_range* , ... です。
- **ingress** キーワードを入力し、接続デバイスからトラフィックを受信する宛先を設定します。
- **learning** キーワードを入力して、宛先から MAC アドレス ラーニングをイネーブルにします。これにより、スイッチによって、宛先に接続されているデバイスに対してトラフィックを送信できます。

  ingress キーワードと **learning** キーワードで宛先を設定する際は、次の点に注意してください。

  - レイヤ 2 スイッチング用の宛先を設定します。「レイヤ 2 スイッチング用の LAN インターフェイスの設定方法」（P.20-6）を参照してください。
  - 宛先がトランクで、接続デバイスがタグなしトラフィックをスイッチに返信する場合、設定されているネイティブ VLAN で 802.1Q トランキングを使用して、接続デバイスからのトラフィックを受信します。
  - レイヤ 3 アドレスに宛先を設定しないでください。VLAN インターフェイスを使用して、宛先に接続されているデバイスとの間でトラフィックを送受信します。
  - 宛先はダウン ステートのままです。接続デバイスとの間でトラフィックを送受信するには、追加のアクティブなレイヤ 2 ポートを VLAN に設定し、VLAN インターフェイスがアップされたままになるようにします。

次に、セッション 1 の双方向送信元として、ギガビット イーサネット ポート 5/1 を設定する例を示します。

```
Router(config)# monitor session 1 source interface gigabitethernet 5/1
```

次に、SPAN セッション 1 の宛先として、ギガビット イーサネット ポート 5/48 を設定する例を示します。

```
Router(config)# monitor session 1 destination interface gigabitethernet 5/48
```

詳細については、「SPAN のコンフィギュレーション例」（P.56-32）を参照してください。

RSPAN の設定

- 「RSPAN VLAN の設定」（P.56-21）
- 「RSPAN セッションの設定（SPAN コンフィギュレーション モード）」（P.56-21）
- 「RSPAN セッションの設定（グローバル コンフィギュレーション モード）」（P.56-24）

RSPAN VLAN の設定

VLAN を RSPAN VLAN 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	`Router# 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	`Router(config)# vlan vlan_ID[{-|,}vlan_ID]`	単独のイーサネット VLAN、イーサネット VLAN の範囲、またはカンマで区切ったリストで複数のイーサネット VLAN を作成または変更します（スペースは挿入しないでください）。
ステップ 3	`Router(config-vlan)# remote-span`	VLAN を RSPAN VLAN として設定します。
ステップ 4	`Router(config-vlan)# end`	VLAN データベースを更新して、特権 EXEC モードに戻ります。

RSPAN セッションの設定（SPAN コンフィギュレーション モード）

- 「SPAN コンフィギュレーション モードでの RSPAN 送信元セッションの設定」（P.56-21）
- 「SPAN コンフィギュレーション モードでの RSPAN 宛先セッションの設定」（P.56-22）

SPAN コンフィギュレーション モードでの RSPAN 送信元セッションの設定

SPAN コンフィギュレーション モードで SPAN 送信元セッションを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# 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	`Router(config)# monitor session RSPAN_source_session_number type rspan-source`	RSPAN 送信元セッション番号を設定し、このセッションに対する RSPAN 送信元セッション 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	`Router(config-mon-rspan-src)# description session_description`	（任意）RSPAN 送信元セッションの説明を入力します。
ステップ 4	`Router(config-mon-rspan-src)# source {single_interface | interface_list | interface_range | mixed_interface_list | single_vlan | vlan_list | vlan_range | mixed_vlan_list} [rx | tx | both]`	RSPAN 送信元セッションの番号と送信元ポートまたは VLAN を対応付けて、モニタするトラフィックの方向を選択します。
ステップ 5	`Router(config-mon-rspan-src)# filter single_vlan | vlan_list | vlan_range | mixed_vlan_list`	（任意）RSPAN 送信元がトランク ポートである場合、送信元 VLAN フィルタリングを設定します。
ステップ 6	`Router(config-mon-rspan-src)# destination remote vlan rspan_vlan_ID`	RSPAN 送信元セッション番号を RSPAN VLAN に関連付けます。
ステップ 7	`Router(config-mon-rspan-src)# no shutdown`	RSPAN 送信元セッションをアクティブにします。
ステップ 8	`Router(config-mon-rspan-src)# end`	コンフィギュレーション モードを終了します。

- *session_description* には最大 240 文字を使用できますが、特殊文字は使用できません。説明にスペースを含めることができます。

（注）　**description** コマンドのあとに、240 文字を入力できます。

- *RSPAN_source_span_session_number* の範囲は、1 ～ 80 です。
- *single_interface* は次のとおりです。
  - **interface** *type slot/port* の形式で、*type* は、**fastethernet**、**gigabitethernet**、または **tengigabitethernet** になります。
  - **interface port-channel** *number*
- *interface_list* は *single_interface* , *single_interface* , *single_interface* ... です。

（注）　各リストでは、カンマの前後にスペースを入れる必要があります。各範囲では、ダッシュの前後にスペースを入れる必要があります。

- *interface_range* は、**interface** *type slot/first_port - last_port* です。
- *mixed_interface_list* は、順不同で *single_interface* , *interface_range* , ... です。
- *single_vlan* は、単一の VLAN の ID 番号です。
- *vlan_list* は *single_vlan* , *single_vlan* , *single_vlan* ... です。
- *vlan_range* は、*first_vlan_ID - last_vlan_ID* です。
- *mixed_vlan_list* は、順不同で *single_vlan* , *vlan_range* , ... です。
- RSPAN VLAN ID については、「RSPAN VLAN の設定」（P.56-21）を参照してください。

次の例は、ポート GigabitEthernet 1/1 からの双方向トラフィックをモニタするようにセッション 1 を設定する方法を示します。

```
Router(config)# monitor session 1 type rspan-source
Router(config-mon-rspan-src)# source interface gigabitethernet 1/1
Router(config-mon-rspan-src)# destination remote vlan 2
```

詳細については、「SPAN のコンフィギュレーション例」（P.56-32）を参照してください。

SPAN コンフィギュレーション モードでの RSPAN 宛先セッションの設定

（注）

- モニタ対象トラフィックにタグ付けをするには、ポートを無条件にトランクに設定してから、そのポートを宛先として設定する必要があります（「無条件トランクとしての宛先ポートの設定（任意）」（P.56-13）を参照）。
- RSPAN 送信元セッション スイッチに RSPAN 宛先セッションを設定し、RSPAN トラフィックをローカルにモニタするようにできます。

RSPAN 宛先セッションを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# 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	`Router(config)# monitor session` *RSPAN_destination_session_number* `type rspan-destination`	RSPAN 宛先セッション番号を設定し、このセッションに対する RSPAN 宛先セッション 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	`Router(config-mon-rspan-dst)# description` *session_description*	（任意）RSPAN 宛先セッションの説明を入力します。
ステップ 4	`Router(config-mon-rspan-dst)# source remote vlan` *rspan_vlan_ID*	RSPAN 宛先セッション番号を RSPAN VLAN に関連付けます。
ステップ 5	`Router(config-mon-rspan-dst)# destination` {*single_interface* | *interface_list* | *interface_range* | *mixed_interface_list*} [**ingress** [**learning**]]	RSPAN 宛先セッション番号を宛先に関連付けます。
ステップ 6	`Router(config-mon-rspan-dst)# end`	コンフィギュレーション モードを終了します。

- *RSPAN_destination_span_session_number* は 1 ～ 80 の範囲で指定できます。
- *single_interface* は次のとおりです。
  - **interface** *type slot*/*port* の形式で、*type* は、**fastethernet**、**gigabitethernet**、または **tengigabitethernet** になります。
  - **interface port-channel** *number*

  （注）　宛先ポート チャネル インターフェイスは、**channel-group** *group_num* **mode on** コマンドおよび **no channel-protocol** コマンドで設定する必要があります。「EtherChannel の設定方法」（P.22-8）を参照してください。

- *interface_list* は *single_interface* , *single_interface* , *single_interface* ... です。

  （注）　各リストでは、カンマの前後にスペースを入れる必要があります。各範囲では、ダッシュの前後にスペースを入れる必要があります。

- *interface_range* は、**interface** *type slot*/*first_port* - *last_port* です。
- *mixed_interface_list* は、順不同で *single_interface* , *interface_range* , ... です。
- **ingress** キーワードを入力し、接続デバイスからトラフィックを受信する宛先を設定します。
- **learning** キーワードを入力して、宛先から MAC アドレス ラーニングをイネーブルにします。これにより、スイッチによって、宛先に接続されているデバイスに対してトラフィックを送信できます。

  ingress キーワードと **learning** キーワードで宛先を設定する際は、次の点に注意してください。
  - レイヤ 2 スイッチング用の宛先を設定します。「レイヤ 2 スイッチング用の LAN インターフェイスの設定方法」（P.20-6）を参照してください。
  - 宛先がトランクで、接続デバイスがタグなしトラフィックをスイッチに返信する場合、設定されているネイティブ VLAN で 802.1Q トランキングを使用して、接続デバイスからのトラフィックを受信します。

  - レイヤ 3 アドレスに宛先を設定しないでください。VLAN インターフェイスを使用して、宛先に接続されているデバイスとの間でトラフィックを送受信します。
  - 宛先はダウン ステートのままです。接続デバイスとの間でトラフィックを送受信するには、追加のアクティブなレイヤ 2 ポートを VLAN に設定し、VLAN インターフェイスがアップされたままになるようにします。
- **no shutdown** コマンドおよび **shutdown** コマンドは、RSPAN 宛先セッションではサポートされていません。

次に、セッション 1 の送信元として、および、ギガビット イーサネット ポート 1/2 の宛先として、RSPAN VLAN 2 を設定する例を示します。

```
Router(config)# monitor session 1 type rspan-destination
Router(config-rspan-dst)# source remote vlan 2
Router(config-rspan-dst)# destination interface gigabitethernet 1/2
```

詳細については、「SPAN のコンフィギュレーション例」（P.56-32）を参照してください。

RSPAN セッションの設定（グローバル コンフィギュレーション モード）

グローバル コンフィギュレーション モードでの RSPAN 送信元セッションの設定

グローバル コンフィギュレーション モードで RSPAN 送信元セッションを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# 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	`Router(config)# monitor session` *RSPAN_source_session_number* **source** {*single_interface* | *interface_list* | *interface_range* | *mixed_interface_list* | *single_vlan* | *vlan_list* | *vlan_range* | *mixed_vlan_list*} [**rx** | **tx** | **both**]	RSPAN 送信元セッションの番号と送信元ポートまたは VLAN を対応付けて、モニタするトラフィックの方向を選択します。
ステップ 3	`Router(config)# monitor session` *RSPAN_source_session_number* **destination remote vlan** *rspan_vlan_ID*	RSPAN 送信元セッション番号を RSPAN VLAN に関連付けます。

- RSPAN VLAN を設定するには、「RSPAN VLAN の設定」（P.56-21）を参照してください。
- *RSPAN_source_span_session_number* の範囲は、1 ～ 80 です。

- *single_interface* は次のとおりです。
  - **interface** *type slot/port* の形式で、*type* は、**fastethernet**、**gigabitethernet**、または **tengigabitethernet** になります。
  - **interface port-channel** *number*
- *interface_list* は *single_interface* , *single_interface* , *single_interface* ... です。

（注）　各リストでは、カンマの前後にスペースを入れる必要があります。各範囲では、ダッシュの前後にスペースを入れる必要があります。

- *interface_range* は、**interface** *type slot/first_port - last_port* です。
- *mixed_interface_list* は、順不同で *single_interface* , *interface_range* , ... です。
- *single_vlan* は、単一の VLAN の ID 番号です。
- *vlan_list* は *single_vlan* , *single_vlan* , *single_vlan* ... です。
- *vlan_range* は、*first_vlan_ID - last_vlan_ID* です。
- *mixed_vlan_list* は、順不同で *single_vlan* , *vlan_range* , ... です。
- RSPAN VLAN ID については、「RSPAN VLAN の設定」（P.56-21）を参照してください。

次に、セッション 2 の送信元として、ポート ギガビット イーサネット ポート 5/2 を設定する例を示します。

```
Router(config)# monitor session 2 source interface gigabitethernet 5/2
```

次に、セッション 2 の宛先として、RSPAN VLAN 200 を設定する例を示します。

```
Router(config)# monitor session 2 destination remote vlan 200
```

詳細については、「SPAN のコンフィギュレーション例」（P.56-32）を参照してください。

グローバル コンフィギュレーション モードでの RSPAN 宛先セッションの設定

（注）

- モニタ対象トラフィックにタグ付けをするには、ポートを無条件にトランクに設定してから、そのポートを宛先として設定する必要があります（「無条件トランクとしての宛先ポートの設定（任意）」（P.56-13）を参照）。
- RSPAN 送信元セッション スイッチに RSPAN 宛先セッションを設定し、RSPAN トラフィックをローカルにモニタするようにできます。

グローバル コンフィギュレーション モードで RSPAN 宛先セッションを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# 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	`Router(config)# monitor session` *RSPAN_destination_session_number* `source remote vlan` *rspan_vlan_ID*	RSPAN 宛先セッション番号を RSPAN VLAN に関連付けます。
ステップ 3	`Router(config)# monitor session` *RSPAN_destination_session_number* `destination` {*single_interface* | *interface_list* | *interface_range* | *mixed_interface_list*} [`ingress` [`learning`]]	RSPAN 宛先セッション番号を宛先に関連付けます。

- *RSPAN_destination_span_session_number* は 1 ～ 80 の範囲で指定できます。
- RSPAN VLAN ID については、「RSPAN VLAN の設定」（P.56-21）を参照してください。
- *single_interface* は次のとおりです。
  - **interface** *type slot/port* の形式で、*type* は、**fastethernet**、**gigabitethernet**、または **tengigabitethernet** になります。
  - **interface port-channel** *number*

（注）　宛先ポート チャネル インターフェイスは、**channel-group** *group_num* **mode on** コマンドおよび **no channel-protocol** コマンドで設定する必要があります。「EtherChannel の設定方法」（P.22-8）を参照してください。

- *interface_list* は *single_interface* , *single_interface* , *single_interface* ... です。

（注）　各リストでは、カンマの前後にスペースを入れる必要があります。各範囲では、ダッシュの前後にスペースを入れる必要があります。

- *interface_range* は、**interface** *type slot/first_port* - *last_port* です。
- *mixed_interface_list* は、順不同で *single_interface* , *interface_range* , ... です。
- **ingress** キーワードを入力し、接続デバイスからトラフィックを受信する宛先を設定します。
- **learning** キーワードを入力して、宛先から MAC アドレス ラーニングをイネーブルにします。これにより、スイッチによって、宛先に接続されているデバイスに対してトラフィックを送信できます。

  ingress キーワードと **learning** キーワードで宛先を設定する際は、次の点に注意してください。
  - レイヤ 2 スイッチング用の宛先を設定します。「レイヤ 2 スイッチング用の LAN インターフェイスの設定方法」（P.20-6）を参照してください。
  - 宛先がトランクで、接続デバイスがタグなしトラフィックをスイッチに返信する場合、設定されているネイティブ VLAN で 802.1Q トランキングを使用して、接続デバイスからのトラフィックを受信します。
  - レイヤ 3 アドレスに宛先を設定しないでください。VLAN インターフェイスを使用して、宛先に接続されているデバイスとの間でトラフィックを送受信します。

– 宛先はダウン ステートのままです。接続デバイスとの間でトラフィックを送受信するには、追加のアクティブなレイヤ 2 ポートを VLAN に設定し、VLAN インターフェイスがアップされたままになるようにします。

次に、セッション 3 の送信元として、RSPAN VLAN 200 を設定する例を示します。

```
Router(config)# monitor session 3 source remote vlan 200
```

次に、セッション 3 の宛先として、ギガビット イーサネット ポート 5/47 を設定する例を示します。

```
Router(config)# monitor session 3 destination interface gigabitethernet 5/47
```

詳細については、「SPAN のコンフィギュレーション例」（P.56-32）を参照してください。

ERSPAN の設定

ERSPAN 送信元セッションの設定

ERSPAN 送信元セッションを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# 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	`Router(config)# monitor session` *ERSPAN_source_session_number* `type erspan-source`	ERSPAN 送信元セッション番号を設定し、このセッションに対する ERSPAN 送信元セッション 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	`Router(config-mon-erspan-src)# description` *session_description*	（任意）ERSPAN 送信元セッションの説明を入力します。
ステップ 4	`Router(config-mon-erspan-src)# source` {*single_interface* | *interface_list* | *interface_range* | *mixed_interface_list* | *single_vlan* | *vlan_list* | *vlan_range* | *mixed_vlan_list*} [**rx** | **tx** | **both**]}	ERSPAN 送信元セッションの番号と送信元ポートまたは VLAN を関連付けて、モニタするトラフィックの方向を選択します。
ステップ 5	`Router(config-mon-erspan-src)# filter` *single_vlan* | *vlan_list* | *vlan_range* | *mixed_vlan_list*	（任意）ERSPAN 送信元がトランク ポートである場合、送信元 VLAN フィルタリングを設定します。
ステップ 6	`Router(config-mon-erspan-src)# destination`	ERSPAN 送信元セッションの宛先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	`Router(config-mon-erspan-src-dst)# ip address` *ip_address*	ERSPAN フローの宛先 IP アドレスを設定します。これは、宛先スイッチのインターフェイス上でも設定する必要があるほか、ERSPAN 宛先セッションの設定でも入力する必要があります（「ERSPAN 宛先セッションの設定」（P.56-29）、ステップ 6 を参照）。
ステップ 8	`Router(config-mon-erspan-src-dst)# erspan-id` *ERSPAN_flow_id*	ERSPAN トラフィックを識別するため、送信元および宛先セッションで使用される ID 番号を設定します。これは、ERSPAN 宛先セッションの設定でも入力する必要があります（「ERSPAN 宛先セッションの設定」（P.56-29）、ステップ 7 を参照）。

	コマンド	目的
ステップ 9	`Router(config-mon-erspan-src-dst)# origin ip address ip_address [force]`	ERSPAN トラフィックの送信元として使用される IP アドレスを設定します。
ステップ 10	`Router(config-mon-erspan-src-dst)# ip ttl ttl_value`	（任意）ERSPAN トラフィック内のパケットの IP Time to Live（TTL）値を設定します。
ステップ 11	`Router(config-mon-erspan-src-dst)# ip prec ipp_value`	（任意）ERSPAN トラフィック内のパケットの IP precedence 値を設定します。
ステップ 12	`Router(config-mon-erspan-src-dst)# ip dscp dscp_value`	（任意）ERSPAN トラフィック内のパケットの IP DSCP 値を設定します。
ステップ 13	`Router(config-mon-erspan-src-dst)# vrf vrf_name`	（任意）グローバル ルーティング テーブルの代わりに使用する VRF 名を設定します。
ステップ 14	`Router(config-mon-erspan-src)# no shutdown`	ERSPAN 送信元セッションをアクティブにします。
ステップ 15	`Router(config-mon-erspan-src-dst)# end`	コンフィギュレーション モードを終了します。

- *session_description* には最大 240 文字を使用できますが、特殊文字は使用できません。説明にスペースを含めることができます。

（注）　**description** コマンドのあとに、240 文字を入力できます。

- *ERSPAN_source_span_session_number* は 1 ～ 80 の範囲で指定できます。
- *single_interface* は次のとおりです。
  - **interface** *type slot/port* の形式で、*type* は、**fastethernet**、**gigabitethernet**、または **tengigabitethernet** になります。
  - **interface port-channel** *number*

（注）　ポート チャネル インターフェイスは、**channel-group** *group_num* **mode on** コマンドおよび **no channel-protocol** コマンドで設定する必要があります。「EtherChannel の設定方法」（P.22-8）を参照してください。

- *interface_list* は *single_interface* , *single_interface* , *single_interface* ... です。

（注）　各リストでは、カンマの前後にスペースを入れる必要があります。各範囲では、ダッシュの前後にスペースを入れる必要があります。

- *interface_range* は、**interface** *type slot/first_port* - *last_port* です。
- *mixed_interface_list* は、順不同で *single_interface* , *interface_range* , ... です。
- *single_vlan* は、単一の VLAN の ID 番号です。
- *vlan_list* は *single_vlan* , *single_vlan* , *single_vlan* ... です。
- *vlan_range* は、*first_vlan_ID* - *last_vlan_ID* です。
- *mixed_vlan_list* は、順不同で *single_vlan* , *vlan_range* , ... です。
- *ERSPAN_flow_id* の範囲は、1 ～ 1023 です。

- 1 つのスイッチのすべての ERSPAN 送信元セッションは、同一の送信元 IP アドレスを使用する必要があります。スイッチ上ですべての ERSPAN 送信元セッションに設定された起点 IP アドレスを変更するには、**origin ip address** *ip_address* **force** コマンドを入力します。
- *ttl_value* は 1 ～ 255 の範囲で指定できます。
- *ipp_value* は 0 ～ 7 の範囲で指定できます。
- *dscp_value* は 0 ～ 63 の範囲で指定できます。

次に、ギガビット イーサネット ポート 4/1 からの双方向トラフィックをモニタするようにセッション 3 を設定する例を示します。

```
Router(config)# monitor session 3 type erspan-source
Router(config-mon-erspan-src)# source interface gigabitethernet 4/1
Router(config-mon-erspan-src)# destination
Router(config-mon-erspan-src-dst)# ip address 10.1.1.1
Router(config-mon-erspan-src-dst)# origin ip address 20.1.1.1
Router(config-mon-erspan-src-dst)# erspan-id 101
```

詳細については、「SPAN のコンフィギュレーション例」（P.56-32）を参照してください。

ERSPAN 宛先セッションの設定

（注）　ERSPAN トラフィックをローカルにモニタすることはできません。

ERSPAN 宛先セッションを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# 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	`Router(config)# monitor session` *ERSPAN_destination_session_number* `type erspan-destination`	ERSPAN 宛先セッション番号を設定し、このセッションに対する ERSPAN 宛先セッション 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	`Router(config-mon-erspan-dst)# description` *session_description*	（任意）ERSPAN 宛先セッションの説明を入力します。
ステップ 4	`Router(config-mon-erspan-dst)# destination` {*single_interface* | *interface_list* | *interface_range* | *mixed_interface_list*} [**ingress** [**learning**]]	ERSPAN 宛先セッション番号と宛先を対応付けます。
ステップ 5	`Router(config-mon-erspan-dst)# source`	ERSPAN 宛先セッションの送信元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	`Router(config-mon-erspan-dst-src)# ip address` *ip_address* [**force**]	ERSPAN フローの宛先 IP アドレスを設定します。これは、ローカル インターフェイス上のアドレスであり、「ERSPAN 送信元セッションの設定」（P.56-27）のステップ 7 で入力したアドレスと一致する必要があります。
ステップ 7	`Router(config-mon-erspan-dst-src)# erspan-id` *ERSPAN_flow_id*	ERSPAN トラフィックを識別するため、宛先および宛先セッションで使用される ID 番号を設定します。これは、「ERSPAN 送信元セッションの設定」（P.56-27）のステップ 8 で入力した ID と一致する必要があります。

	コマンド	目的
ステップ 8	`Router(config-mon-erspan-dst-src)# vrf vrf_name`	（任意）グローバル ルーティング テーブルの代わりに使用する VRF 名を設定します。
ステップ 9	`Router(config-mon-erspan-dst)# no shutdown`	ERSPAN 宛先セッションをアクティブにします。
ステップ 10	`Router(config-mon-erspan-dst-src)# end`	コンフィギュレーション モードを終了します。

- *ERSPAN_destination_span_session_number* は 1 ～ 80 の範囲で指定できます。
- *single_interface* は次のとおりです。
  - **interface** *type slot/port* の形式で、*type* は、**fastethernet**、**gigabitethernet**、または **tengigabitethernet** になります。
  - **interface port-channel** *number*

  （注）　宛先ポート チャネル インターフェイスは、**channel-group** *group_num* **mode on** コマンドおよび **no channel-protocol** コマンドで設定する必要があります。「EtherChannel の設定方法」（P.22-8）を参照してください。

- *interface_list* は *single_interface* , *single_interface* , *single_interface* ... です。

  （注）　各リストでは、カンマの前後にスペースを入れる必要があります。各範囲では、ダッシュの前後にスペースを入れる必要があります。

- *interface_range* は、**interface** *type slot/first_port* - *last_port* です。
- *mixed_interface_list* は、順不同で *single_interface* , *interface_range* , ... です。
- スイッチ上のすべての ERSPAN 宛先セッションは、同じ宛先インターフェイス上の同一の IP アドレスを使用する必要があります。スイッチ上ですべての ERSPAN 宛先セッションに設定された IP アドレスを変更するには、**ip address** *ip_address* **force** コマンドを入力します。

  （注）　また、すべての ERSPAN 送信元セッションの宛先 IP アドレスを変更することも必要です（「ERSPAN 送信元セッションの設定」（P.56-27）、ステップ 7 を参照）。

- *ERSPAN_flow_id* の範囲は、1 ～ 1023 です。
- **ingress** キーワードを入力し、接続デバイスからトラフィックを受信する宛先を設定します。
- **learning** キーワードを入力して、宛先から MAC アドレス ラーニングをイネーブルにします。これにより、スイッチによって、宛先に接続されているデバイスに対してトラフィックを送信できます。

  ingress キーワードと **learning** キーワードで宛先を設定する際は、次の点に注意してください。
  - レイヤ 2 スイッチング用の宛先を設定します。「レイヤ 2 スイッチング用の LAN インターフェイスの設定方法」（P.20-6）を参照してください。
  - 宛先がトランクで、接続デバイスがタグなしトラフィックをスイッチに返信する場合、設定されているネイティブ VLAN で 802.1Q トランキングを使用して、接続デバイスからのトラフィックを受信します。
  - レイヤ 3 アドレスに宛先を設定しないでください。VLAN インターフェイスを使用して、宛先に接続されているデバイスとの間でトラフィックを送受信します。

- 宛先はダウン ステートのままです。接続デバイスとの間でトラフィックを送受信するには、追加のアクティブなレイヤ 2 ポートを VLAN に設定し、VLAN インターフェイスがアップされたままになるようにします。

次に、IP アドレス 10.1.1.1 に着信した ERSPAN ID 101 トラフィックを、ギガビット イーサネット ポート 2/1 に送信するように ERSPAN 宛先セッションを設定する例を示します。

```
Router(config)# monitor session 3 type erspan-destination
Router(config-erspan-dst)# destination interface gigabitethernet 2/1
Router(config-erspan-dst)# source
Router(config-erspan-dst-src)# ip address 10.1.1.1
Router(config-erspan-dst-src)# erspan-id 101
```

詳細については、「SPAN のコンフィギュレーション例」（P.56-32）を参照してください。

グローバル コンフィギュレーション モードでの送信元 VLAN フィルタリングの設定

（注）

- SPAN コンフィギュレーション モードで送信元 VLAN フィルタリングを設定するには、次を参照してください。
  - 「ローカル SPAN の設定（SPAN コンフィギュレーション モード）」（P.56-17）
  - 「SPAN コンフィギュレーション モードでの RSPAN 送信元セッションの設定」（P.56-21）
  - 「ERSPAN の設定」（P.56-27）
- 送信元 VLAN フィルタリングにより、SPAN 送信元から SPAN 宛先に送信されるトラフィックの量が減ります。

送信元がトランク ポートである場合に、送信元 VLAN フィルタリングは特定の VLAN をモニタします。

ローカル SPAN または RSPAN 送信元がトランク ポートである場合、送信元 VLAN 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
ステップ 1	`Router# 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	`Router(config)# monitor session` *session_number* **filter** *single_vlan* | *vlan_list* | *vlan_range* | *mixed_vlan_list*	ローカル SPAN または RSPAN 送信元がトランク ポートである場合、送信元 VLAN フィルタリングを設定します。

- *single_vlan* は、単一の VLAN の ID 番号です。
- *vlan_list* は *single_vlan* , *single_vlan* , *single_vlan* ... です。
- *vlan_range* は、*first_vlan_ID* - *last_vlan_ID* です。
- *mixed_vlan_list* は、順不同で *single_vlan* , *vlan_range* , ... です。

次に、送信元がトランク ポートである場合に、VLAN 1 ～ 5 および VLAN 9 をモニタする例を示します。

```
Router(config)# monitor session 2 filter vlan 1 - 5 , 9
```

SPAN の設定確認

設定を確認するには、**show monitor session** コマンドを入力します。

次に、セッション 2 の設定を確認する例を示します。

```
Router# show monitor session 2
Session 2
------------
Type : Remote Source Session

Source Ports:
    RX Only:       Gi3/1
Dest RSPAN VLAN:   901
Router#
```

次に、セッション 2 の詳細を完全に表示する例を示します。

```
Router# show monitor session 2 detail
Session 2
------------
Type : Remote Source Session

Source Ports:
    RX Only:       Gi1/1-3
    TX Only:       None
    Both:          None
Source VLANs:
    RX Only:       None
    TX Only:       None
    Both:          None
Source RSPAN VLAN: None
Destination Ports: None
Filter VLANs:      None
Dest RSPAN VLAN:   901
```

SPAN のコンフィギュレーション例

次に、RSPAN 送信元セッション 2 の設定例を示します。

```
Router(config)# monitor session 2 source interface gigabitethernet1/1 - 3 rx
Router(config)# monitor session 2 destination remote vlan 901
```

次に、セッション 1 とセッション 2 の設定を消去する例を示します。

```
Router(config)# no monitor session range 1-2
```

次に、複数の送信元のある RSPAN 送信元セッションの設定例を示します。

```
Router(config)# monitor session 2 source interface gigabitethernet 5/15 , 7/3 rx
Router(config)# monitor session 2 source interface gigabitethernet 1/2 tx
Router(config)# monitor session 2 source interface port-channel 102
Router(config)# monitor session 2 source filter vlan 2 - 3
Router(config)# monitor session 2 destination remote vlan 901
```

次に、セッションの送信元を削除する例を示します。

```
Router(config)# no monitor session 2 source interface gigabitethernet 5/15 , 7/3
```

次に、セッションの送信元に対するオプションを削除する例を示します。

```
Router(config)# no monitor session 2 source interface gigabitethernet 1/2
```

```
Router(config)# no monitor session 2 source interface port-channel 102 tx
```

次に、セッションの送信元 VLAN フィルタリングを削除する例を示します。

```
Router(config)# no monitor session 2 filter vlan 3
```

次に、RSPAN 宛先セッション 8 の設定例を示します。

```
Router(config)# monitor session 8 source remote vlan 901
Router(config)# monitor session 8 destination interface gigabitethernet 1/2 , 2/3
```

次に、ERSPAN 送信元セッション 12 の設定例を示します。

```
monitor session 12 type erspan-source
 description SOURCE_SESSION_FOR_VRF_GRAY
 source interface Gi8/48 rx
 destination
  erspan-id 120
  ip address 10.8.1.2
  origin ip address 32.1.1.1
  vrf gray
```

次に、ERSPAN 宛先セッション 12 の設定例を示します。

```
monitor session 12 type erspan-destination
 description DEST_SESSION_FOR_VRF_GRAY
 destination interface Gi4/48
 source
  erspan-id 120
  ip address 10.8.1.2
  vrf gray
```

次に、ERSPAN 送信元セッション 13 の設定例を示します。

```
monitor session 13 type erspan-source
 source interface Gi6/1 tx
 destination
  erspan-id 130
  ip address 10.11.1.1
  origin ip address 32.1.1.1
```

次に、ERSPAN 宛先セッション 13 の設定例を示します。

```
monitor session 13 type erspan-destination
 destination interface Gi6/1
 source
  erspan-id 130
  ip address 10.11.1.1
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CHAPTER 57

SNMP ifIndex パーシステンス

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

SNMP ifIndex パーシステンスの前提条件

なし。

SNMP ifIndex パーシステンスの制約事項

なし。

SNMP ifIndex パーシステンスについて

SNMP ifIndex パーシステンス機能は、スイッチが再起動するときに保持され使用されているインターフェイス インデックス（ifIndex）値を提供します。ifIndex 値は、物理または、論理インターフェイスに関連する一意の識別番号です。

関連する RFC では、特定の ifIndex 値とインターフェイス間のやりとりが、スイッチの再起動時に維持されているための要件はありませんが、多くのアプリケーション（たとえば、デバイス インベントリ、課金情報、障害検出）はこのやりとりの維持を必要とします。

インターフェイスを ifIndex に関連付けるのに、一定のインターバルでスイッチをポーリングすることができますが、定期的にポーリングすることは実用的ではありません。SNMP ifIndex パーシステンス機能は、持続的な ifIndex 値を提供し、それによってインターフェイスをポーリングする必要がなくなります。

次の定義は、RFC 2233『The Interfaces Group MIB using SMIv2』に基づいています。次の用語は、Interfaces MIB（IF-MIB）に含まれる値です。

- **ifIndex**：一意の番号（ゼロより大きい）で、各インターフェイスをそのインターフェイスの SNMP 識別に関して識別します。
- **ifName**：テキストベースのインターフェイス名（例：ethernet 3/1）。
- **ifDescr**：インターフェイスの記述。この説明用の推奨情報としては、メーカー名、製品名、インターフェイスのハードウェアとソフトウェアのバージョンがあります。

SNMP ifIndex パーシステンスのデフォルト設定

SNMP ifIndex パーシステンスは、デフォルトでディセーブルになります。

SNMP ifIndex パーシステンスの設定方法

SNMP ifIndex パーシステンスのグローバルなイネーブル化

SNMP ifIndex パーシステンス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
`Router(config)# snmp-server ifindex persist`	SNMP ifIndex パーシステンスをグローバルにイネーブルにします。

次の例では、SNMP ifIndex パーシステンスがすべてのインターフェイスでイネーブルにされます。

```
router(config)# snmp-server ifindex persist
```

SNMP ifIndex パーシステンスのグローバルなディセーブル化

SNMP ifIndex パーシステンスをイネーブルにしたあと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
`Router(config)# no snmp-server ifindex persist`	SNMP ifIndex パーシステンスをグローバルにディセーブルにします。

次の例では、SNMP ifIndex パーシステンスがすべてのインターフェイスでディセーブルにされます。

```
router(config)# no snmp-server ifindex persist
```

特定のインターフェイス上における SNMP ifIndex パーシステンスのイネーブル化およびディセーブル化

特定のインターフェイス上でだけ、SNMP ifIndex パーシステンス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	`Router(config)# interface {vlan vlan_ID} | {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	`Router(config-if)# snmp ifindex persist`	特定のインターフェイスで SNMP ifIndex パーシステンス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。

（注）　[**no**] **snmp ifindex persistence** インターフェイス コマンドは、サブインターフェイスでは使用できません。インターフェイスに適用されるコマンドは、そのインターフェイスに関連するすべてのサブインターフェイスに自動的に適用されます。

次の例では、SNMP ifIndex パーシステンスが、インターフェイス Ethernet 3/1 でだけイネーブルになります。

```
router(config)# interface ethernet 3/1
router(config-if)# snmp ifindex persist
router(config-if)# exit
```

次の例では、SNMP ifIndex パーシステンスが、インターフェイス Ethernet 3/1 でだけディセーブルになります。

```
router(config)# interface ethernet 3/1
router(config-if)# no snmp ifindex persist
router(config-if)# exit
```

特定のインターフェイスにおける SNMP ifIndex パーシステンス設定の消去

インターフェイス固有の SNMP ifIndex パーシステンス設定を消去し、インターフェイスがグローバル コンフィギュレーション設定を使用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
ステップ 1	`Router(config)# interface type slot/port`	指定した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。インターフェイス コマンドの構文は使用しているプラットフォームにより異なることに注意してください。
ステップ 2	`Router(config-if)# snmp ifindex clear`	インターフェイス固有の SNMP ifIndex パーシステンス設定を消去し、グローバル コンフィギュレーション設定に戻します。
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。

次の例では、インターフェイス Ethernet 3/1 における SNMP ifIndex パーシステンスに対する以前の設定を、コンフィギュレーションから削除します。SNMP ifIndex パーシステンスがグローバルにイネーブルに設定されている場合、SNMP ifIndex パーシステンスはインターフェイス Ethernet 3/1 でイネーブルになります。SNMP ifIndex パーシステンスがグローバルにディセーブルに設定されている場合、SNMP ifIndex パーシステンスは、インターフェイス Ethernet 3/1 でディセーブルになります。

```
router(config)# interface ethernet 3/1
router(config-if)# snmp ifindex clear
router(config-if)# exit
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

Top-N レポート

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

Top-N レポートの前提条件

なし。

Top-N レポートの制約事項

なし。

Top-N レポートに関する情報

レポート

Top-N レポートの概要

Top-N レポートを使用して、スイッチ上の各物理ポートのデータを収集し、解析することができます。起動後、Top-N レポートは適切なハードウェア カウンタから統計情報を取得してから、ユーザが指定したインターバルの間、スリープ モードに入ります。インターバルが経過すると、レポートは同じハードウェア カウンタから現在の統計情報を取得して、前回収集した統計情報と比較し、その差分を保存します。各ポートの統計情報は、表 58-1 に示すいずれかの統計タイプによってソートされます。

表 58-1　有効な Top-N 統計タイプ

統計タイプ	定義
broadcast	入力および出力ブロードキャスト パケット数
bytes	入力および出力バイト数
errors	入力エラー数
multicast	入力および出力マルチキャスト パケット数
overflow	バッファ オーバーフローの数
packets	入力および出力パケット数
utilization	使用率

（注）　Top-N レポートはポート利用率を計算する際、Tx および Rx 回線を同一カウンタにまとめます。また、利用率の割合（%）の計算では、全二重帯域幅が対象となります。たとえば、ギガビット イーサネット ポートの場合は 2000 Mbps 全二重となります。

Top-N レポートの操作

collect top コマンドを入力すると、処理が開始され、システム プロンプトがただちに再び表示されます。処理が完了すると、レポートはその場で画面上に表示されるのではなく、あとで参照できるように保存されます。Top-N レポートはレポートの生成が完了すると、画面に Syslog メッセージを送信して通知します。

生成が完了したレポートを表示するには、**show top counters interface report** コマンドを入力します。完了したレポートだけが表示されます。まだ完了していないレポートに対しては、処理についての簡単な概要情報を表示します。

Top-N レポートの処理を終了するには、**clear top counters interface report** コマンドを入力します。Ctrl+C キーを押しても、Top-N レポートの処理は中止されません。完了したレポートは、明示的に削除するまで表示可能です。削除するには、**clear top counters interface report** {**all** | *report_num*} コマンドを入力します。

Top-N レポートのデフォルト設定

なし。

Top-N レポートの使用方法

Top-N レポート作成のイネーブル化

Top-N レポート作成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
`Router# collect top [number_of_ports] counters interface {type | all | layer-2 | layer-3} [sort-by statistic_type] [interval seconds]`	Top-N レポート作成をイネーブルにします。

Top-N レポートの作成をイネーブルにする場合は、次の点に注意してください。

- レポート作成の対象として、最もビジーなポート数を指定できます（デフォルトは 20）。
- ポートが最もビジーと見なされる統計タイプを指定できます（デフォルトは utilization）。*statistic_type* のサポートされる値は、**broadcast**、**bytes**、**errors**、**multicast**、**overflow**、**packets** および **utilization** です。
- 統計情報を収集するためのインターバルを指定できます（有効範囲は 0 ～ 999、デフォルトは 30 秒）。
- utilization レポートを除き（**sort-by utilization** キーワードを使用して設定）、レポート作成のインターバルを 0 に指定できます。この場合は、インターバル開始時のカウンタ値とインターバル終了時のカウンタ値の差分ではなく、現在のカウンタ値がレポートに表示されます。

次の例は、利用率が最も高い 4 つのポートに対し、Top-N レポートの作成をイネーブルにします。インターバルは 76 秒に設定します。

```
Router# collect top 4 counters interface all sort-by utilization interval 76
TopN collection started.
```

Top-N レポートの表示

Top-N レポートを表示する手順は、次のとおりです。

コマンド	目的
Router# **show top counters interface report** [*report_num*]	Top-N レポートを表示します。 **（注）** すべてのレポート情報を表示する場合は、*report_num* 値を入力しないでください。

Top-N レポートの統計情報は、次の状況では表示されません。

- 最初のポーリング実行時にポートが存在しない場合
- 2 回めのポーリング実行時にポートが存在しない場合
- ポーリング インターバルの間にポートの速度またはデュプレックスが変更された場合。
- ポーリング インターバルの間にポート タイプがレイヤ 2 からレイヤ 3 に変更された場合。
- ポーリング インターバルの間にポート タイプがレイヤ 3 からレイヤ 2 に変更された場合。

次に、すべての Top-N レポート情報を表示する例を示します。

```
Router# show top counters interface report
Id Start Time                    Int N   Sort-By   Status  Owner
-- ----------------------------- --- --- --------- ------- ----------------------
1  08:18:25 UTC Tue Nov 23 2004 76  20  util      done    console
2  08:19:54 UTC Tue Nov 23 2004 76  20  util      done    console
3  08:21:34 UTC Tue Nov 23 2004 76  20  util      done    console
4  08:26:50 UTC Tue Nov 23 2004 90  20  util      done    console
```

（注） 統計情報の収集が完了していないレポートの場合は、ステータスが pending として表示されます。

次に、特定の Top-N レポートを表示する例を示します。

```
Router# show top counters interface report 1
Started By        : console
Start Time        : 08:18:25 UTC Tue Nov 23 2004
End Time          : 08:19:42 UTC Tue Nov 23 2004
Port Type         : All
Sort By           : util
Interval          : 76 seconds
Port    Band  Util Bytes       Packets     Broadcast  Multicast  In-  Buf-
        width      (Tx + Rx)   (Tx + Rx)   (Tx + Rx)  (Tx + Rx)  err  ovflw
------- ----- ---- ----------- ----------- ---------- ---------- ---- -----

Gi2/5   100   50   726047564   11344488    11344487   1          0    0
Gi2/48  100   35   508018905   7937789     0          43         0    0
Gi2/46  100   25   362860697   5669693     0          43         0    0
Gi2/47  100   22   323852889   4762539     4762495    43         0    0
```

Top-N レポートの消去

Top-N レポートを消去するには、次のいずれかの作業を行います。

コマンド	目的
`Router# clear top counters interface report`	ステータスが done のすべての Top-N レポートを消去します。
`Router# clear top counters interface report [report_num]`	ステータスに関係なく、番号が *report_num* の Top-N レポートを消去します。

次に、ステータスが done のすべてのレポートを消去する例を示します。

```
Router# clear top counters interface report
04:00:06: %TOPN_COUNTERS-5-DELETED: TopN report 1 deleted by the console
04:00:06: %TOPN_COUNTERS-5-DELETED: TopN report 2 deleted by the console
04:00:06: %TOPN_COUNTERS-5-DELETED: TopN report 3 deleted by the console
04:00:06: %TOPN_COUNTERS-5-DELETED: TopN report 4 deleted by the console
```

次に、番号 4 のレポートを消去する例を示します。

```
Router# clear top counters interface report 4
04:52:12: %TOPN_COUNTERS-5-KILLED: TopN report 4 killed by the console
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

レイヤ 2 traceroute ユーティリティ

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

レイヤ 2 Traceroute ユーティリティの前提条件

なし。

レイヤ 2 Traceroute ユーティリティの制約事項

- Cisco Discovery Protocol（CDP）がネットワーク上のすべてのデバイスでイネーブルでなければなりません。CDP をディセーブルにすると、レイヤ 2 Traceroute ユーティリティが正しく動作しません。レイヤ 2 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と、レイヤ 2 Traceroute ユーティリティはパス上でこのデバイスを識別できません。

- スイッチは、**ping** 特権 EXEC コマンドを使用して接続をテストする場合に他のスイッチから到達可能であるとして定義されています。レイヤ 2 パス内のすべてのデバイスは、互いに到達可能である必要があります。ping 接続を確認するには、CDP がレイヤ 2 インターフェイスでアドバタイズする IP アドレスを使用する必要があります。
- 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までのレイヤ 2 パス上にないスイッチでは、**traceroute mac** または **traceroute mac ip** 特権 EXEC コマンドを入力できます。パス内のすべてのデバイスは、このスイッチから到達可能でなければなりません。
- **traceroute mac** コマンドの出力結果としてレイヤ 2 パスが表示されるのは、指定の送信元および宛先 MAC アドレスが、同一の VLAN に属している場合だけです。指定した送信元および宛先 MAC アドレスが、それぞれ異なる VLAN に属している場合は、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 アドレスを指定すると、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 に属する場合は、送信元および宛先 MAC アドレスの両方が属している VLAN を指定する必要があります。VLAN を指定しないと、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 MAC アドレスが同一サブネットに属する場合、**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と、レイヤ 2 Traceroute ユーティリティはアドレス解決プロトコル（ARP）を使用して、IP アドレスと、これに対応する MAC アドレスおよび VLAN ID を関連付けます。
  - 指定の IP アドレスに対する ARP エントリが存在する場合は、レイヤ 2 Traceroute ユーティリティはこれに関連付けられた MAC アドレスを使用して、レイヤ 2 パスを識別します。
  - ARP エントリが存在しない場合は、レイヤ 2 Traceroute ユーティリティは ARP クエリーを送信し、この IP アドレスの解決を試みます。IP アドレスが解決されない場合は、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介して 1 つのポートに接続されている場合は（1 つのポート上で複数の CDP ネイバーが検出された場合など）、レイヤ 2 Traceroute ユーティリティはこのホップで終了し、エラー メッセージが表示されます。
- レイヤ 2 Traceroute ユーティリティは、トークン リング VLAN ではサポートされません。

レイヤ 2 Traceroute ユーティリティについて

レイヤ 2 Traceroute ユーティリティは、送信元デバイスから宛先デバイスまでのパケットの経路を表すレイヤ 2 パスを識別します。レイヤ 2 Traceroute は、ユニキャストの送信元および宛先 MAC アドレスだけをサポートします。このユーティリティは、パス上の各スイッチが持つ MAC アドレス テーブルを使用して、パスを特定します。レイヤ 2 Traceroute ユーティリティは、レイヤ 2 Traceroute をサポートしないデバイスをパス上で検出すると、レイヤ 2 トレース クエリーを送信し続け、これらのクエリーをタイムアウトにします。

レイヤ 2 Traceroute ユーティリティが識別できるのは、送信元デバイスから宛先デバイスまでのパスだけです。パケットが送信元ホストから送信元デバイスに到達するパスや、宛先デバイスから宛先ホストへのパスは識別できません。

レイヤ 2 Traceroute ユーティリティの使用方法

パケットが通過した送信元デバイスから宛先デバイスまでのレイヤ 2 パスを表示するには、特権 EXEC モードで、次のいずれかの作業を行います。

コマンド	目的
Router# **traceroute mac** [**interface** *type interface_number*] *source_mac_address* [**interface** *type interface_number*] *destination_mac_address* [**vlan** *vlan_id*] [**detail**]	MAC アドレスを使用して、パケットがネットワーク上で通過したパスを追跡します。
Router# **traceroute mac ip** {*source_ip_address* | *source_hostname*} {*destination_ip_address* | *destination_hostname*} [**detail**]	IP アドレスを使用して、パケットがネットワーク上で通過したパスを追跡します。

次の例は、**traceroute mac** および **traceroute mac ip** コマンドを使用して、パケットが宛先に到達するまでに通過したネットワーク上の物理パスを表示します。

```
Router# 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
con5                 (2.2.5.5        )  :    Fa0/3 => Gi0/1
con1                 (2.2.1.1        )  :    Gi0/1 => Gi0/2
con2                 (2.2.2.2        )  :    Gi0/2 => Fa0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
Router#
Router# traceroute mac 0001.0000.0204 0001.0000.0304 detail
Source 0001.0000.0204 found on VAYU[WS-C6509] (2.1.1.10)
1 VAYU / WS-C6509 / 2.1.1.10 :
               Gi6/1 [full, 1000M] => Po100 [auto, auto]
2 PANI / WS-C6509 / 2.1.1.12 :
               Po100 [auto, auto] => Po110 [auto, auto]
3 BUMI / WS-C6509 / 2.1.1.13 :
               Po110 [auto, auto] => Po120 [auto, auto]
4 AGNI / WS-C6509 / 2.1.1.11 :
               Po120 [auto, auto] => Gi8/12 [full, 1000M] Destination 0001.0000.0304
found on AGNI[WS-C6509] (2.1.1.11) Layer 2 trace completed.
Router#
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

ミニ プロトコル アナライザ

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

ミニ プロトコル アナライザの前提条件

なし。

ミニ プロトコル アナライザの制約事項

PFC およびすべての DFC では、IPv4 トラフィックの分析がハードウェアでサポートされます。少量 IPv6 トラフィックの分析は、ソフトウェアでサポートされています。

ミニ プロトコル アナライザについて

Mini Protocol Analyzer は SPAN セッションからネットワーク トラフィックをキャプチャし、キャプチャしたパケットをローカル メモリ バッファに保存します。提供されているフィルタリング オプションを使用することで、キャプチャするパケットを次のとおり制限できます。

- 選択した VLAN、ACL、または MAC アドレスからのパケット
- 特定の EtherType のパケット
- 特定のパケット サイズのパケット

即時コマンドを入力してキャプチャを開始、終了したり、キャプチャをスケジューリングして特定の日時にキャプチャを開始できます。

キャプチャしたデータは、コンソールに表示したり、ローカル ファイル システムに保存したり、または標準的なファイル転送プロトコルを使用して外部サーバへエクスポートできます。キャプチャしたファイルの形式は libpcap です。この形式は、多くのパケット分析プログラムおよび sniffer プログラムによってサポートされています。このファイル形式の詳細については、次の URL を参照してください。

http://www.tcpdump.org/

デフォルトでは、各パケットの最初の 68 バイトだけがキャプチャされます。

ミニ プロトコル アナライザの設定方法

キャプチャ セッションの設定

Mini Protocol Analyzer を使用してキャプチャ セッションを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# 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	`Router(config)# [no] monitor session number type capture`	キャプチャ用としてプロセッサに割り当てられているパケットを使用して SPAN セッション番号を設定します。キャプチャ セッションのコンフィギュレーション モードを開始します。セッション番号の範囲は 1 ～ 80 です。 接頭辞に **no** を使用するとセッションが削除されます。
ステップ 3	`Router(config-mon-capture)# buffer-size buf_size`	（任意）キャプチャ バッファのサイズを KB 単位で設定します。指定できる範囲は 32 ～ 65535 KB です。デフォルトは 2048 KB です。

	コマンド	目的
ステップ 4	`Router(config-mon-capture)# description session_description`	（任意）キャプチャ セッションの説明を入力します。説明には最大 240 文字まで入力できますが、特殊文字は入力できません 説明にスペースを含める場合、引用符（""）で囲む必要があります。
ステップ 5	`Router(config-mon-capture)# rate-limit pps`	（任意）1 秒当たりにキャプチャできるパケット数（*pps*）を制限します。指定できる範囲は 10 ～ 100000 パケットで、デフォルトは 1 秒あたり 10000 パケットです。
ステップ 6	`Router(config-mon-capture)# source {{interface {single_interface | interface_list | interface_range | mixed_interface_list} | port-channel channel_id}} | {vlan {vlan_ID | vlan_list | vlan_range | mixed_vlan_list}}[rx | tx | both]`	キャプチャ セッションと送信元ポートまたは VLAN を対応付けて、モニタするトラフィックの方向を選択します。デフォルトは双方向です。
ステップ 7	`Router(config-mon-capture)# exit`	キャプチャ セッションのコンフィギュレーション モードを終了します。

- 一度に設定できるキャプチャ セッションは 1 つだけです。同時キャプチャ セッションを複数設定することはできません。
- **source interface** コマンド引数は、単一のインターフェイス、2 つのインターフェイス番号（小さい番号が先、ダッシュで区切る）で指定するインターフェイスの範囲、またはインターフェイスと範囲をカンマで区切ったリストのいずれかです。

（注） 送信元インターフェイスのリストを設定する場合、カンマの前後にスペースを入れる必要があります。送信元インターフェイスの範囲を設定する場合、ダッシュの前後にスペースを入れる必要があります。

- **source vlan** コマンド引数は、1 ～ 4094 の範囲の単一の VLAN 番号（予約済み VLAN を除く）、2 つの VLAN 番号（小さい番号が先、ダッシュで区切る）で指定する VLAN 範囲、または VLAN と範囲のリストのいずれかです。

（注） 送信元の VLAN のリストを設定する場合、カンマの前後にスペースを入れないでください。送信元の VLAN の範囲を設定する場合、ダッシュの前後にスペースを入れないでください。この要件は、送信元インターフェイスのリストと範囲を指定する場合の要件とは異なることに注意してください。

- キャプチャ セッションの設定時は、データのキャプチャは開始されません。「キャプチャの開始および停止」（P.60-5）に示すとおり、キャプチャは **monitor capture start** または **monitor capture schedule** コマンドによって開始されます。
- キャプチャ バッファは、デフォルトでは linear（直線）ですが、**monitor capture start** または **monitor capture schedule** コマンドのランタイム オプションとして circular（循環）に設定できます。
- 使用可能なハードウェア レート制限レジスタがない場合、キャプチャ セッションはディセーブルになります。
- VLAN フィルタが設定されている場合、送信元 VLAN は変更できません。VLAN フィルタを削除してから、送信元 VLAN を変更してください。

キャプチャ対象となるパケットのフィルタリング

Mini Protocol Analyzer のキャプチャ対象となるパケットをフィルタリングするには、この作業をキャプチャ セッションのコンフィギュレーション モードで行います。

	コマンド	目的
ステップ 1	`Router(config-mon-capture)# filter access-group {acl_number | acl_name}`	（任意）指定した ACL からのパケットだけをキャプチャします。
ステップ 2	`Router(config-mon-capture)# filter vlan {vlan_ID | vlan_list | vlan_range | mixed_vlan_list}`	（任意）指定した送信元 VLAN（1 つまたは複数）からのパケットをキャプチャします。
ステップ 3	`Router(config-mon-capture)# filter ethertype type`	（任意）指定した EtherType のパケットだけをキャプチャします。*type* は、10 進数、16 進数、または 8 進数で指定できます。 **（注）** IPv6 トラフィックをフィルタリングするために、*type* に **0x86dd** を設定します。少量 IPv6 トラフィックの分析は、ソフトウェアでサポートされています。
ステップ 4	`Router(config-mon-capture)# filter length min_len [max_len]`	（任意）サイズが *min_len* ～ *max_len*（両方の値を含む）の範囲のパケットだけをキャプチャします。*max_len* が指定されていない場合は、サイズが *min_len* のパケットだけがキャプチャされます。*min_len* の範囲は 0 ～ 9216 バイト、*max_len* の範囲は 1 ～ 9216 バイトです。
ステップ 5	`Router(config-mon-capture)# filter mac-address mac_addr`	（任意）指定された MAC アドレスからのパケットだけをキャプチャします。
ステップ 6	`Router(config-mon-capture)# end`	コンフィギュレーション モードを終了します。

- キャプチャ対象となるパケットのフィルタリング用にいくつかのオプションが提供されています。レート制限が適用される前に、ハードウェアでは ACL および VLAN によるフィルタリングが実行され、ソフトウェアではその他すべてのフィルタが実行されます。ソフトウェアのフィルタリングを実行すると、キャプチャ レートが下がる可能性があります。
- **filter vlan** 引数は、1 ～ 4094 の範囲の単一の VLAN 番号（予約済み VLAN を除く）、2 つの VLAN 番号（小さい番号が先、ダッシュで区切る）で指定する VLAN 範囲、または VLAN と範囲のリストのいずれかです。

（注） フィルタリング用 VLAN リストを設定する場合、カンマの前後にスペースを入れる必要があります。フィルタリング用 VLAN 範囲を設定する場合、ダッシュの前後にスペースを入れる必要があります。この要件は、前述した送信元の VLAN リストと範囲を指定する場合の要件とは異なることに注意してください。

- EtherType を 10 進数値として入力するには、先頭にゼロの付かない値（1 ～ 65535）を入力します。16 進数値を入力するには、4 文字の 16 進数の前にプレフィックスの 0x を入力します。8 進数値を入力するには、先頭にゼロを付けた数値（0 ～ 7）を入力します。たとえば、802.1Q EtherType を入力する場合、10 進数値では 33024、16 進数値では 0x8100、8 進数値では 0100400 となります。

- MAC アドレスは、ドット付き 16 進表記の 3 つの 2 バイト値で入力します。例：0123.4567.89ab
- **no** キーワードを使用するとフィルタが削除されます。

（注）　**no** キーワードを使用して VLAN フィルタを削除した後は、コンフィギュレーション モードを終了して、キャプチャ コンフィギュレーション モードを再度有効にし、**source vlan** コマンドを実行してからその他のキャプチャ設定を変更する必要があります。

- VLAN フィルタの設定時は、キャプチャの送信元または宛先は VLAN であることが必要です。ポート フィルタの設定時は、キャプチャの送信元または宛先はポートであることが必要です。

キャプチャの開始および停止

キャプチャを開始および停止するコマンドは、コンフィギュレーション設定として保存されていません。これらのコマンドは、コンソールから EXEC モードで実行されます。キャプチャをすぐに開始することも、キャプチャを開始する将来の日時を設定することもできます。次のいずれかの状況が発生すると、キャプチャが終了します。

- コンソールから、停止またはクリア コマンドが入力された。
- キャプチャ バッファがいっぱいになった（循環バッファとして設定されていない場合）。
- オプションで指定した秒数が経過した。
- オプションで指定したパケット数がキャプチャされた。

キャプチャが停止すると、SPAN セッションが終了し、キャプチャ セッションのパケットはプロセッサに転送されなくなります。

パケットのキャプチャを開始するときに、一部のコンフィギュレーション設定を上書きするかどうかを選択できます。

キャプチャを開始、停止、またはキャンセルするには、次の作業を行います。

	コマンド	目的
ステップ 1	Router# **monitor capture** [**buffer size** *buf_size*][**length** *cap_len*][**linear** | **circular**][**filter** *acl_number* | *acl_name*] {**start** [**for** *count* (**packets** | **seconds**)] | **schedule at** *time date*}	オプションのランタイム設定を変更してキャプチャを開始します。キャプチャはただちに開始することも、指定した日時に開始することもできます。 • **buffer size** オプションでは、設定済みまたはデフォルトのキャプチャ バッファ サイズを上書きします。 • **length** オプションでは、各パケットからキャプチャするバイト数を決定します。*cap_len* の範囲は 0 ～ 9216 バイトで、デフォルトは 68 バイトです。値に 0 を指定すると、パケット全体がキャプチャされます。 • **circular** オプションは、キャプチャ バッファがいっぱいになった時点で、先に入力された項目から上書きするよう指定します。**linear** オプションは、キャプチャ バッファがいっぱいになった時点でキャプチャを停止するよう指定します。デフォルトは **linear** です。 • **filter** オプションにより、指定された ACL が適用されます。 • **for** オプションでは、指定した時間（単位：秒）が経過するか、または指定した数のパケットがキャプチャされた後、キャプチャを停止するよう指定します。
ステップ 2	Router# **monitor capture stop**	キャプチャを停止します。
ステップ 3	Router# **monitor capture clear** [**filter**]	ランタイム コンフィギュレーション設定、保留中のスケジュール設定されたキャプチャ、およびキャプチャ バッファをクリアします。**filter** オプションを指定すると、ランタイム フィルタ設定だけがクリアされます。

上記のコマンドを使用する際は、次の点に注意してください。

- *time* および *date* の形式は、hh:mm:ss dd mmm yyyy です。時間は 24 時間表記で指定し、月は 3 文字の略語で指定します。たとえば、キャプチャの開始時刻を 2006 年 10 月 31 日の午後 7 時 30 分に設定するには、19:30:00 31 oct 2006 と表記します。時間帯は、GMT で指定します。
- 開始コマンドでキャプチャ フィルタの ACL を使用する場合、設定済みの ACL が新しい ACL によって上書きされることはありません。新しい ACL はソフトウェアで実行されます。

キャプチャ バッファの表示およびエクスポート

キャプチャされたパケットまたはキャプチャ セッションに関する情報を表示したり、キャプチャされたパケットを分析用にエクスポートするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# show monitor capture`	キャプチャ セッションの設定を表示します。
ステップ 2	`Router# show monitor capture status`	キャプチャ セッションのステート、モード、パケットの統計情報を表示します。
ステップ 3	`Router# show monitor capture buffer [start [end]] [detail][dump [nowrap [dump_length]] [acl acl_number | acl_name]]`	キャプチャ バッファの内容を表示します。 • *start* および *end* パラメータでは、キャプチャ バッファ内のパケット番号インデックスを指定します。*start* インデックスが指定され、*end* インデックスが指定されていない場合、*start* インデックスの 1 つのパケットだけが表示されます。*start* および *end* インデックスが共に指定されている場合、この 2 つのインデックス間にあるすべてのパケットが表示されます。指定できる範囲は 1 ～ 4294967295 です。 • **detail** オプションでは、各パケットについて、拡張およびフォーマットされたプロトコルとエンベロープ情報（パケットの到着時刻など）が追加されます。 • **dump** オプションは、パケットの内容を 16 進数で表示します。*nowrap* が *dump_length* と共に指定されている場合、パケットの内容を示す *dump_length* 文字の 16 進数が各パケットについて 1 行で表示されます。*dump_length* が指定されていない場合、72 文字の行が 1 行表示されます。*dump_length* の範囲は 14 ～ 256 です。 • **acl** オプションにより、指定された ACL に一致するパケットだけが表示されます。
ステップ 4	`Router# show monitor capture buffer [start [end]] brief [acl acl_number | acl_name]`	パケットのヘッダー情報だけを表示します。
ステップ 5	`Router# monitor capture export buffer url`	キャプチャ バッファの内容を指定されたファイル システムまたはファイル転送メカニズムにコピーします。

ミニ プロトコル アナライザの設定例

一般的な設定例

次に、Mini Protocol Analyzer の最小限の設定を行う例を示します。

```
Router#
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# monitor session 1 type capture
Router(config-mon-capture)# end

Router# show mon cap
Capture instance [1] :
======================
Capture Session ID : 1
Session status     : up
rate-limit value   : 10000
redirect index     : 0x807
buffer-size        : 2097152
capture state      : OFF
capture mode       : Linear
capture length     : 68

Router#
```

次に、バッファ サイズ、セッションの説明、レート制限を設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# monitor session 1 type capture
Router(config-mon-capture)# buffer-size 4096
Router(config-mon-capture)# description "Capture from ports, no filtering."
Router(config-mon-capture)# rate-limit 20000
Router(config-mon-capture)# end
Router#
Router# show monitor capture
Capture instance [1] :
======================
Capture Session ID : 1
Session status     : up
rate-limit value   : 20000
redirect index     : 0x807
buffer-size        : 4194304
capture state      : OFF
capture mode       : Linear
capture length     : 68

Router#
```

次に、送信元をポートの混合リストとして設定する例を示します。

```
Router(config-mon-capture)# source interface gig 3/1 - 3 , gig 3/5
```

次に、送信元を VLAN の混合リストとして設定する例を示します。

```
Router(config-mon-capture)# source vlan 123,234-245
```

フィルタリング設定例

次に、次の属性を持つパケットをキャプチャするよう設定する例を示します。

- パケットは 123 または 234 ～ 245 の VLAN に所属
- パケットは 802.1Q EtherType（16 進数値 0x8100、10 進数値 33024）
- パケット サイズは 8192 バイト
- 送信元 MAC アドレスは 01:23:45:67:89:ab
- パケットは ACL 番号 99 に準拠

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# monitor session 1 type capture
Router(config-mon-capture)# source vlan 123,234-245
Router(config-mon-capture)# filter ethertype 0x8100
Router(config-mon-capture)# filter length 8192
Router(config-mon-capture)# filter mac-address 0123.4567.89ab
Router(config-mon-capture)# filter access-group 99
Router(config-mon-capture)# end

Router# show monitor capture
Capture instance [1] :
======================
Capture Session ID : 1
Session status     : up
rate-limit value   : 20000
redirect index     : 0x7E07
Capture vlan       : 1019
buffer-size        : 4194304
capture state      : OFF
capture mode       : Linear
capture length     : 68
Sw Filters          :
     ethertype   : 33024
     src mac     : 0123.4567.89ab
  Hw  acl          : 99

Router# show monitor session 1
Session 1
---------
Type                   : Capture Session
Description            : capture from ports
Source VLANs           :
    Both               : 123,234-245
Capture buffer size    : 4096 KB
Capture rate-limit
             value     : 20000
Capture filters        :
     ethertype         : 33024
     src mac           : 0123.4567.89ab
     acl               : 99

Egress SPAN Replication State:
Operational mode       : Centralized
Configured mode        : Distributed (default)

Router#
```

次に、サイズが 128 バイト未満のパケットをキャプチャする例を示します。

```
Router(config-mon-capture)# filter length 0 128
```

次に、サイズが 256 バイトを超えるパケットをキャプチャする例を示します。

```
Router(config-mon-capture)# filter length 256 9216
```

操作例

次に、キャプチャを開始および停止する例を示します。

```
Router# monitor capture start
Router# monitor capture stop
Router#
```

次に、キャプチャを開始して 60 秒後に停止する例を示します。

```
Router# monitor capture start for 60 seconds
Router#
```

次に、キャプチャを今後のある日時に開始する例を示します。

```
Router# monitor capture schedule at 11:22:33 30 jun 2008
capture will start at : <11:22:33 UTC Mon Jun 30 2008>  after 32465825 secs
Router#
```

次に、バッファ サイズを上書きして循環バッファに変更するオプションを指定して、キャプチャを開始する例を示します。

```
Router# monitor capture buffer size 65535 circular start
Router#
```

次に、キャプチャ バッファを外部サーバとローカル ディスクにエクスポートする例を示します。

```
Router# monitor capture export buffer tftp://server/user/capture_file.cap
Router# monitor capture export buffer disk1:capture_file.cap
```

表示例

設定の表示

キャプチャ セッションの設定を表示するには、**show monitor capture** コマンドを入力します。

```
Router# show monitor capture
Capture instance [1] :
======================
Capture Session ID : 1
Session status     : up
rate-limit value   : 10000
redirect index     : 0x807
buffer-size        : 2097152
capture state      : OFF
capture mode       : Linear
```

```
capture length     : 68
```

次に、**show monitor session** *n* コマンドを使用して詳細を表示する例を示します。

```
Router# show monitor session 1
Session 1
---------
Type                  : Capture Session
Source Ports          :
    Both              : Gi3/1-3,Gi3/5
Capture buffer size   : 32 KB
Capture filters       : None

Egress SPAN Replication State:
Operational mode      : Centralized
Configured mode       : Distributed (default)
```

次に、**show monitor session** *n* **detail** コマンドを使用して、全詳細を表示する例を示します。

```
Router# show monitor session 1 detail
Session 1
---------
Type                  : Capture Session
Description           : -
Source Ports          :
    RX Only           : None
    TX Only           : None
    Both              : Gi3/1-3,Gi3/5
Source VLANs          :
    RX Only           : None
    TX Only           : None
    Both              : None
Source RSPAN VLAN     : None
Destination Ports     : None
Filter VLANs          : None
Dest RSPAN VLAN       : None
Source IP Address     : None
Source IP VRF         : None
Source ERSPAN ID      : None
Destination IP Address : None
Destination IP VRF    : None
Destination ERSPAN ID  : None
Origin IP Address     : None
IP QOS PREC           : 0
IP TTL                : 255
Capture dst_cpu_id    : 1
Capture vlan          : 0
Capture buffer size   : 32 KB
Capture rate-limit
             value    : 10000
Capture filters       : None

Egress SPAN Replication State:
Operational mode      : Centralized
Configured mode       : Distributed (default)
```

キャプチャ セッション ステータスの表示

キャプチャ セッション ステータスを表示するには、**show monitor capture status** コマンドを入力します。

```
Router# show monitor capture status
capture state      : ON
capture mode       : Linear
Number  of packets
          received : 253
           dropped : 0
          captured : 90
```

キャプチャ バッファの内容の表示

キャプチャ セッションの内容を表示するには、**show monitor capture status** コマンドを入力します。次に、このコマンドのいくつかのオプションを使用した場合の表示例を示します。

```
Router# show monitor capture buffer
 1     IP: s=10.12.0.5 , d=224.0.0.10, len 60
 2     346   0180.c200.000e  0012.44d8.5000  88CC 020707526F7
 3     60    0180.c200.0000  0004.c099.06c5  0026 42420300000
 4     60    ffff.ffff.ffff  0012.44d8.5000  0806 00010800060
 5     IP: s=7.0.84.23 , d=224.0.0.5, len 116
 6     IP: s=10.12.0.1 , d=224.0.0.10, len 60


Router# show monitor capture buffer detail
 1      Arrival time : 09:44:30 UTC Fri Nov 17 2006
        Packet Length : 74 , Capture Length : 68
        Ethernet II :  0100.5e00.000a  0008.a4c8.c038  0800
        IP: s=10.12.0.5 , d=224.0.0.10, len 60, proto=88
 2      Arrival time : 09:44:31 UTC Fri Nov 17 2006
        Packet Length : 346 , Capture Length : 68
346   0180.c200.000e  0012.44d8.5000  88CC 020707526F757463031


Router# show monitor capture buffer dump
 1     IP: s=10.12.0.5 , d=224.0.0.10, len 60
08063810:                       0100 5E00000A            ..^...
08063820: 0008A4C8 C0380800 45C0003C 00000000  ..$H@8..E@.<....
08063830: 0258CD8F 0A0C0005 E000000A 0205EE6A  .XM.....`.....nj
08063840: 00000000 00000000 00000000 00000064  ...............d
08063850: 0001000C 01000100 0000000F 0004      ..............
 2     346   0180.c200.000e  0012.44d8.5000  88CC 020707526F757465720415
 3     60    0180.c200.0000  0004.c099.06c5  0026 4242030000000000800000
 4     60    ffff.ffff.ffff  0012.44d8.5000  0806 0001080006040001001244
 5     IP: s=7.0.84.23 , d=224.0.0.5, len 116
0806FCB0:                       0100 5E000005            ..^...
0806FCC0: 0015C7D7 AC000800 45C00074 00000000  ..GW,...E@.t....
0806FCD0: 01597D55 07005417 E0000005 0201002C  .Y}U..T.`......,
0806FCE0: 04040404 00000000 00000002 00000010  ................
0806FCF0: 455D8A10 FFFF0000 000A1201 0000      E]............


Router# show monitor capture buffer dump nowrap
 1     74    0100.5e00.000a  0008.a4c8.c038  0800 45C0003C000000
 2     346   0180.c200.000e  0012.44d8.5000  88CC 020707526F7574
 3     60    0180.c200.0000  0004.c099.06c5  0026 42420300000000
 4     60    ffff.ffff.ffff  0012.44d8.5000  0806 00010800060400
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

PART 12

Quality of Service

CHAPTER 61

PFC QoS の概要

この章では、Cisco IOS Release 15.1SY でポリシー フィーチャ カード（PFC）と分散型フォワーディング カード（DFC）に実装された Quality of Service（QoS）機能の概要を説明します。「PFC QoS」という用語は、ハードウェアでアクセラレートされた QoS を示します。PFC QoS は、PFC および DFC に加えて、各種のスイッチ コンポーネントに実装されています。

（注）

- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。
- AutoQoS については、第 66 章「自動 QoS」を参照してください。
- QoS と MPLS の詳細については、第 67 章「MPLS QoS」を参照してください。
- Cisco IOS Release 15.1SY の QoS（PFC QoS）では、一部の Cisco IOS のモジュラ QoS CLI（MQC）を使用します。PFC QoS はハードウェアに実装されるので、MQC 構文のサブセットだけがサポートされます。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

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。QoS なしの場合、ネットワークは、*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、適度な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。輻輳が発生すると、すべてのトラフィックが等しくドロップされます。QoS は、プライオリティ トラフィックがドロップされる確率を最小化します。

PFC QoS には、次の機能があります。

- 分類
- マーキング
- ポリシング

- 輻輳回避
- 変換

2 種類のポリシーを設定できます。

- 出力 DSCP 変換、出力 EXP 変換、分類、マーキング、ポリシングの任意の組み合わせを定義するポリシー。
- キューイングを定義するポリシー。

キューイングの設定と分類、マーキング、およびポリシング設定は、いずれも任意です。

キューイング設定および分類、マーキング、およびポリシング設定には、共通のパラメータもコマンドもありません。

QoS ポリシーは、次のコマンドを使用して設定します。

- **class-map**：パケット一致基準に基づいてトラフィック クラスを定義します。クラス マップはポリシー マップ内で参照されます。
- **table-map**：1 組の traffic フィールド値から、別の 1 組の traffic フィールド値へのマッピングを定義します。テーブル マップはポリシー マップ内で参照されます。キューイング ポリシーでは使用されません。
- **policy-map**：次の要素の任意の組み合わせを定義または使用します。
  - 分類のクラス マップ
  - マーキングおよび変換のテーブル マップ
  - ポリシー信頼モード
  - ポリシング
  - キューイング（分類、マーキング、信頼モード、またはポリシングとの組み合わせは不可）
- **service-policy**：ポリシーをインターフェイスに適用します。

次の章では、QoS について説明します。

- 「PFC QoS に関する制約事項」（P.62-1）
- 「分類、マーキング、およびポリシング」（P.63-1）
- 「ポリシーベース キューイング」（P.64-1）
- 「QoS のグローバル オプションおよびインターフェイス オプション」（P.65-1）

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

PFC QoS に関する制約事項

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

全般的な注意事項

- リリース 15.0(1) SY1 以降のリリースでは、サポートされる QoS TCAM エントリの数を増やすことができます。

	TCAM バンク	QoS TCAM エントリ	
		PFC4 モード	PFC4XL モード
リリース 15.0(1)SY • リリース 15.0(1) SY では設定できません。 • 15.0(1) SY1 以降のリリースのデフォルトです。 • リリース 15.0(1)SY1 以降のリリースでの次のコマンド： `platform hardware acl reserve qos-banks 1`	1	16K	64K
リリース 15.0(1)SY1 以降のリリース コマンド： `platform hardware acl reserve qos-banks 2`	2	32K	128K

サポートされる QoS TCAM エントリ数の変更は、リロード後に有効になります。QoS TCAM エントリ設定を表示するには、**show platform hardware acl global-config** コマンドを入力します。

```
Router# show platform hardware acl global-config | include [Bb]anks
Reserved QoS Banks:
Current 1 banks
 Latest set 1 banks
 After next reload 1 banks
Router#
```

PFC モードを表示するには、**show platform hardware pfc mode** コマンドを入力します。

- PFC QoS は、IGMP、MLD、PIM トラフィックをサポートしています。
- **match ip precedence** および **match ip dscp** コマンドは、IPv4 トラフィックだけをフィルタリングします。
- **match precedence** および **match dscp** コマンドは、IPv4 および IPv6 トラフィックをフィルタリングします。
- **set ip dscp** および **set ip precedence** コマンドは、**set dscp** および **set precedence** コマンドとしてコンフィギュレーション ファイルに保存されます。
- PFC QoS では、IPv4 および IPv6 トラフィック用の **setdscp** および **set precedence** ポリシー マップ クラス コマンドがサポートされます。
- QoS、NetFlow、および NetFlow データ エクスポート（NDE）のフローマスク要件は、特にマイクロフロー ポリシングを設定する場合に競合する可能性があります。
- 再マーキングされた DSCP に対する出力 ACL サポート、および VACL キャプチャの両方を 1 つのインターフェイス上に設定すると、VACL キャプチャによって各パケットが 2 コピーずつキャプチャされることがあります。この場合、2 つめのコピーは壊れている可能性があります。
- 再マーキングされた DSCP に対する出力 ACL サポートは、トンネル インターフェイスには設定できません。
- 再マーキングされた DSCP に対する出力 ACL のサポートは、IP ユニキャスト トラフィックをサポートします。

- 再マーキングされた DSCP に対する出力 ACL のサポートは、マルチキャスト トラフィックとは無関係です。PFC QoS は出力 QoS を適用する前に、入力 QoS の変更をマルチキャスト トラフィックに適用します。
- NetFlow および NetFlow データ エクスポート（NDE）は、再マーキングされた DSCP に対する出力 ACL のサポートが設定されたインターフェイスはサポートしません。
- 再マーキングされた DSCP に対する出力 ACL のサポートをいずれかのインターフェイスに設定している場合に、これを設定していないインターフェイスで NetFlow および NDE のサポートをイネーブルにするには、インターフェイス固有のフローマスクを設定する必要があります。**platform flow ip interface-destination-source**、または **platform flow ip interface-full** のいずれかのグローバル コンフィギュレーション モード コマンドを入力してください。
- 再マーキングされた DSCP に対する出力 ACL のサポートを設定しているインターフェイスでは、インターフェイス カウンタの値が不正確となります。
- 再マーキングされた DSCP に対する出力 ACL のサポートによって許可されたトラフィックには、マイクロフロー ポリシングを適用できません。
- 再マーキングされた DSCP に対する出力 ACL のサポートによって許可されたトラフィックには、MPLS トラフィックとしてタグを付けることはできません （このトラフィックは、他のネットワーク装置上では MPLS トラフィックとしてタグ付けできます）。
- 入力および出力ポリシング両方を同じトラフィックに適用した場合、入力および出力ポリシーの両方がトラフィックのマークダウンまたはトラフィックのドロップのいずれかを実行する必要があります。PFC QoS では、出力ドロップを使用した入力マークダウン、または出力マークダウンを使用した入力ドロップをサポートしません。（CSCea23571）。
- トラフィックに集約ポリシングとマイクロフロー ポリシングを実行する場合、集約ポリサーおよびマイクロフロー ポリサーを同じポリシー マップ クラスに組み込み、各ポリサーで同じ **conform-action** および **exceed-action** キーワード オプションを使用する必要があります（**drop**、**set-dscp-transmit**、**set-prec-transmit**、または **transmit**）。
- トンネル インターフェイス上では、PFC QoS 機能を設定できません。
- PFC QoS は、トンネル トラフィックのペイロード ToS バイトを書き換えません。
- PFC QoS フィルタリングの基準になるのは、ACL、DSCP 値、または IP precedence 値だけです。
- 次のコマンドに対し、PFC QoS は同一 ASIC によって制御されるすべての LAN ポートに、同じ設定を適用します。
  - **rcv-queue cos-map**
  - **wrr-queue cos-map**
- WS-X6904-40G-2T、WS-X6908-10GE、WS-X6816-10T-2T、WS-X6716-10T、WS-X6816-10G-2T、WS-X6716-10GE、WS-X6704-10GE、WS-X6848-SFP-2T、WS-X6748-SFP、WS-X6824-SFP-2T、WS-X6724-SFP、WS-X6848-TX-2T、WS-X6748-GE-TX のモジュールを除き、次のコマンドに関して、PFC QoS では、同一の特定用途向け集積回路（ASIC）によって制御されているすべての LAN ポートに同じ設定を適用します。
  - **rcv-queue random-detect**
  - **rcv-queue queue-limit**
  - **wrr-queue queue-limit**
  - **wrr-queue bandwidth**
  - **priority-queue cos-map**
  - **wrr-queue threshold**
  - **rcv-queue threshold**

  - **wrr-queue random-detect**
  - **wrr-queue random-detect min-threshold**
  - **wrr-queue random-detect max-threshold**
- これらのコマンドは、物理ポートだけで設定してください。論理インターフェイスでは設定できません。
  - **priority-queue cos-map**
  - **wrr-queue cos-map**
  - **wrr-queue random-detect**
  - **wrr-queue random-detect max-threshold**
  - **wrr-queue random-detect min-threshold**
  - **wrr-queue threshold**
  - **wrr-queue queue-limit**
  - **wrr-queue bandwidth**
  - **rcv-queue cos-map**
  - **rcv-queue bandwidth**
  - **rcv-queue random-detect**
  - **rcv-queue random-detect max-threshold**
  - **rcv-queue random-detect min-threshold**
  - **rcv-queue queue-limit**
  - **rcv-queue cos-map**
  - **rcv-queue threshold**

（注） 出力パケット レプリケーションを使用する IP マルチキャスト スイッチングは、QoS と互換性がありません。この場合に、出力レプリケーションを実行するとパケットで不正な CoS または DSCP マーキングが行われる可能性があります。QoS を使用していて、スイッチング モジュールが出力レプリケーションに対応している場合、出力レプリケーションを強制するには、**platform ip multicast replication-mode ingress** コマンドを入力します。

PFC および DFC のガイドライン

- PFC および DFC では、IPv6 ユニキャストおよびマルチキャスト トラフィックの QoS をサポートしています。
- IPv6 PFC QoS についての情報を表示するには、**show platform qos ipv6** コマンドを入力します。
- ポート ASIC（キュー アーキテクチャおよびデキューイング アルゴリズム）に実装された QoS 機能は、IPv4 および IPv6 トラフィックをサポートします。
- PFC および DFC では IPv6 の名前付き拡張 ACL と名前付き標準 ACL をサポートしています。
- PFC および DFC では、**match protocol ipv6** コマンドをサポートしています。
- 再マーキングされた DSCP に対する出力 ACL サポートを設定すると、PFC および DFC は、次の機能に対するハードウェア支援を行わなくなります。
  - Cisco IOS 再帰 ACL

  - ネットワーク アドレス変換（NAT）
- ARP トラフィックには、マイクロフロー ポリシングを適用できません。
- PFC および DFC は、RP へブリッジされるトラフィックに出力ポリシングを適用しません。
- PFC および DFC は、RP からのマルチキャスト トラフィックに、出力ポリシングも出力 DSCP 変換も適用しません。
- PFC QoS は、ブリッジド マルチキャスト トラフィックの ToS バイトを書き換えません。
- PFC および DFC は、最大 1022 個の集約ポリサーをサポートしますが、**police** コマンド以外の一部の PFC QoS コマンドはこのカウントに含まれます。デフォルトでは、**set** コマンドまたは **trust** コマンドを使用するポリシーは集約ポリサー カウントに含まれます。**no platform qos marking statistics** コマンドを入力することにより、集約ポリサー カウントへの **set** コマンドまたは **trust** コマンドの追加をディセーブルにすることができますが、これらのコマンドに関連付けられたクラス マップの統計情報が収集できなくなります。**show platform hardware capacity qos** コマンドの出力の QoS Policer Resources セクションで、集約ポリサー カウントを確認することができます。

クラス マップ コマンドの制約事項

- PFC QoS は、**class-map match-all** クラス マップで単一の **match** コマンドをサポートします。ただし、**match protocol** コマンドは、**match dscp** または **match precedence** コマンドを含むクラス マップで設定できます。
- PFC QoS は、**class-map match-any** クラス マップで複数の **match** コマンドをサポートします。
- PFC QoS では、次のクラス マップ コマンドはサポートされません。
  - **match classmap**
  - **match destination-address**
  - **match input-interface**
  - **match source-address**

ポリシー マップ クラス コマンドの制約事項

PFC QoS では、次のポリシー マップ クラス コマンドはサポートされません。

- **set qos-group**
- **service-policy**

CIR および PIR レート値に対してサポートされる粒度

CIR および PIR レート値の範囲	粒度
32768 ～ 2097152（2 Mbs）	32768（32 Kb）
2097153 ～ 4194304（4 Mbps）	65536（64 Kb）
4194305 ～ 8388608（8 Mbps）	131072（128 Kb）
8388609 ～ 16777216（16 Mbps）	262144（256 Kb）
16777217 ～ 33554432（32 Mbps）	524288（512 Kb）

CIR および PIR レート値の範囲	粒度
33554433 ～ 67108864（64 Mbps）	1048576（1 Mb）
67108865 ～ 134217728（128 Mbps）	2097152（2 Mb）
134217729 ～ 268435456（256 Mbps）	4194304（4 Mb）
268435457 ～ 536870912（512 Mbps）	8388608（8 Mb）
536870913 ～ 1073741824（1 Gbs）	16777216（16 Mb）
1073741825 ～ 2147483648（2 Gbs）	33554432（32 Mb）
2147483649 ～ 4294967296（4 Gbs）	67108864（64 Mb）
4294967296 ～ 8589934592（8 Gbs）	134217728（128 Mb）
8589934593 ～ 17179869184（16 Gbs）	268435456（256 Mb）
17179869185 ～ 34359738368（32 Gbs）	536870912（512 Mb）
34359738369 ～ 68719476736（64 Gbs）	1073741824（1024 Mb）

各範囲で、PFC QoS は粒度の倍数に相当するレート値を使用して、PFC をプログラミングします。

CIR および PIR トークン バケット サイズに対してサポートされる粒度

CIR および PIR トークン バケット サイズの範囲	粒度
1 ～32768（32 KB）	1024（1 KB）
32769 ～65536（64 KB）	2048（2 KB）
65537 ～131072（128 KB）	4096（4 KB）
131073 ～262144（256 KB）	8196（8 KB）
262145 ～524288（512 KB）	16392（16 KB）
524289 ～1048576（1 MB）	32768（32 KB）
1048577 ～2097152（2 MB）	65536（64 KB）
2097153 ～4194304（4 MB）	131072（128 KB）
4194305 ～8388608（8 MB）	262144（256 KB）
8388609 ～16777216（16 MB）	524288（512 KB）
16777217 ～33554432（32 MB）	1048576（1 MB）

各範囲で、PFC QoS は粒度の倍数に相当するトークン バケット サイズを使用して、PFC をプログラミングします。

IP precedence 値と DSCP 値

3 ビット IP Precedence	ToS の最上位 6 ビット						6 ビット DSCP
	8	7	6	5	4	3	
0	0	0	0	0	0	0	0
	0	0	0	0	0	1	1
	0	0	0	0	1	0	2
	0	0	0	0	1	1	3
	0	0	0	1	0	0	4
	0	0	0	1	0	1	5
	0	0	0	1	1	0	6
	0	0	0	1	1	1	7
1	0	0	1	0	0	0	8
	0	0	1	0	0	1	9
	0	0	1	0	1	0	10
	0	0	1	0	1	1	11
	0	0	1	1	0	0	12
	0	0	1	1	0	1	13
	0	0	1	1	1	0	14
	0	0	1	1	1	1	15
2	0	1	0	0	0	0	16
	0	1	0	0	0	1	17
	0	1	0	0	1	0	18
	0	1	0	0	1	1	19
	0	1	0	1	0	0	20
	0	1	0	1	0	1	21
	0	1	0	1	1	0	22
	0	1	0	1	1	1	23
3	0	1	1	0	0	0	24
	0	1	1	0	0	1	25
	0	1	1	0	1	0	26
	0	1	1	0	1	1	27
	0	1	1	1	0	0	28
	0	1	1	1	0	1	29
	0	1	1	1	1	0	30
	0	1	1	1	1	1	31

3 ビット IP Precedence	ToS の最上位 6 ビット						6 ビット DSCP
	8	7	6	5	4	3	
4	1	0	0	0	0	0	32
	1	0	0	0	0	1	33
	1	0	0	0	1	0	34
	1	0	0	0	1	1	35
	1	0	0	1	0	0	36
	1	0	0	1	0	1	37
	1	0	0	1	1	0	38
	1	0	0	1	1	1	39
5	1	0	1	0	0	0	40
	1	0	1	0	0	1	41
	1	0	1	0	1	0	42
	1	0	1	0	1	1	43
	1	0	1	1	0	0	44
	1	0	1	1	0	1	45
	1	0	1	1	1	0	46
	1	0	1	1	1	1	47
6	1	1	0	0	0	0	48
	1	1	0	0	0	1	49
	1	1	0	0	1	0	50
	1	1	0	0	1	1	51
	1	1	0	1	0	0	52
	1	1	0	1	0	1	53
	1	1	0	1	1	0	54
	1	1	0	1	1	1	55
7	1	1	1	0	0	0	56
	1	1	1	0	0	1	57
	1	1	1	0	1	0	58
	1	1	1	0	1	1	59
	1	1	1	1	0	0	60
	1	1	1	1	0	1	61
	1	1	1	1	1	0	62
	1	1	1	1	1	1	63

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CHAPTER 63

分類、マーキング、およびポリシング

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

分類、マーキング、およびポリシング ポリシーに関する情報

分類、マーキング、およびポリシング ポリシーの概要

分類、マーキング、およびポリシング設定は、インターフェイスに対応付けられポリシーによって定義されます。分類、マーキング、およびポリシングは、入力インターフェイスに設定されている QoS コマンドや、キューイング ポリシーの影響を受けません。

Traffic Classification

トラフィック分類により、設定したクラスに分類されるときに、ネットワークでそのトラフィックを認識できるようになります。特定の QoS を適用するためには、ネットワーク トラフィックを分類する必要があります。

分類は、包括的にすることもできれば（レイヤ 2 VLAN のすべてのトラフィック、あるインターフェイスを通るすべてのトラフィックなど）、極端に具体的にすることもできます（たとえば、トラフィックの特定の側面を認識する **match** コマンドによるクラス マップを使用可能）。

QoS を分類および適用してから（マーキングなど）、別のインターフェイスまたはネットワーク デバイスで、マークした値に基づいて分類し、別の QoS を適用することができます。

PFC および任意の DFC は、**class-map match-all** クラス マップで単一の **match** コマンドをサポートします。ただし、**match protocol** コマンドは、**match dscp** または **match precedence** コマンドによってクラス マップに設定できます。

PFC および任意の DFC は、**class-map match-any** クラス マップで複数の **match** コマンドをサポートします。

クラス マップでは、表 63-1 に記載されている **match** コマンドを使用して、一致基準に基づくトラフィック クラスを設定できます。

表 63-1　トラフィック分類のクラス マップの match コマンドと一致基準

match コマンド	方向	一致基準
match access-group {*access_list_number* | **name** *access_list_name*}	両方	アクセス コントロール リスト（ACL）。 **（注）** ACL は、次の要素の照合に使用します。 - CoS 値 - VLAN ID - パケット長
match any	両方	任意の一致基準
match cos	入力	CoS 値
match discard-class	両方	廃棄クラスの値。
match dscp **（注）** **match protocol** コマンドは、**match dscp** コマンドでクラス マップに設定できます。	両方	DSCP 値。
match l2 miss	入力	現在学習されていない MAC レイヤの宛先アドレスにアドレス指定されているため、VLAN でフラッディングしたレイヤ 2 トラフィック。
match mpls experimental topmost	両方	最上位ラベルの MPLS EXP 値。
match precedence **（注）** **match protocol** コマンドは、**match precedence** コマンドでクラス マップに設定できます。	両方	IP precedence 値。
match protocol {**arp** | **ip** | **ipv6**} **（注）** **match protocol** コマンドは、**match dscp** コマンドまたは **match precedence** コマンドでクラス マップに設定できます。	両方	プロトコル。
match qos-group	両方	QoS グループ ID。

PFC および任意の DFC は、**match access group** コマンドで使用するために、次の ACL タイプをサポートしています。

プロトコル	番号付き ACL の有無	拡張 ACL の有無	名前付き ACL の有無
IPv4	Yes： 1 ～ 99 1300 ～ 1999	Yes： 100 ～ 199 2000 ～ 2699	Yes
IPv6	N/A	Yes（名前付き）	Yes
MAC レイヤ	N/A	N/A	Yes
ARP	N/A	N/A	Yes

トラフィック マーキング

（注）　ポリシングでもトラフィックをマーキングできます。

ネットワーク トラフィックをマーキングすると、特定のトラフィック クラスの属性を設定または変更できます。これにより、クラス ベースの QoS 機能で、マーキングに基づいてトラフィック クラスを認識できるようになります。

次の 2 種類のトラフィック マーキング方法があります。

- ポリシーマップ **set** コマンドで設定値を適用できます。表 63-2 に、使用可能なポリシーマップ **set** コマンドと対応する属性を示します。

表 63-2　Configured-Value Policy-Map コマンド

set コマンド	トラフィック属性	入力	出力
set cos *cos_value*	レイヤ 2 CoS 値	Y	Y
set dscp *dscp_value*	レイヤ 3 DSCP 値	Y	Y
set precedence *precedence_value*	レイヤ 3 IP precedence 値	Y	Y
set dscp tunnel *dscp_value*	総称ルーティング カプセル化（GRE）トンネリングされたパケットのトンネル ヘッダーにあるレイヤ 3 DSCP 値	Y	Y
set discard-class *discard_value*	discard-class 値	Y	Y
set qos-group *group_id*	QoS グループ ID	Y	Y
set mpls experimental imposition *exp_value*	すべての割り当て済みラベル エントリの MPLS 実験（EXP）フィールド	Y	Y
set mpls experimental topmost *exp_value*	すべての最上位ラベル エントリの MPLS 実験（EXP）フィールド	Y	Y

- ポリシーマップ **set** コマンドで、受信した値にマップを適用できます。表 63-3 に、使用可能なポリシーマップ **set** コマンドと対応する属性を示します。

表 63-3　Mapped-Value Policy-Map コマンド

set コマンド	マップ名	トラフィック属性	入力	出力
set dscp cos	**dscp-cos-map**	レイヤ 3 DSCP 値	Y	N
set dscp precedence	**dscp-precedence-map**	レイヤ 3 DSCP 値	Y	N

ポリシングについて

ポリシングの概要

次の処理を行うポリサーを設定できます。

- トラフィックのマーキング
- 帯域利用率の制限およびトラフィックのマーキング

ポリサーは、入力および出力インターフェイスに適用できます。入力ポリシングが最初に適用され、続いて出力ポリシングが適用されます。

ポリシングを使用すると、QoS 設定で定義されたトラフィック転送ルールに適合するように、着信および発信トラフィックをレート制限できます。システムにおいてトラフィックが転送される方法を定義した設定済みルールは、契約と呼ばれます。この契約に適合しないトラフィックは、低い DSCP 値にマーク ダウンされるか、またはドロップされます。

ポリシングでは、アウトオブプロファイル パケットがバッファに保存されません。したがって、ポリシングが伝搬遅延に影響することはありません。逆に、トラフィック シェーピングではアウトオブプロファイル トラフィックをバッファに保存することで、トラフィック バーストを緩和します （PFC QoS はシェーピングをサポートしません）。

PFC および DFC は、入力および出力 PFC QoS をサポートしています。これには、入力および出力ポリシングが含まれます。ポリサーは、ポート単位または VLAN 単位で入力トラフィックに適用されます。出力トラフィックに対するポリシングは、VLAN 単位だけで行われます。

ポリシングでは、レイヤ 2 フレーム サイズを使用します。帯域利用率限度は、認定情報レート（CIR）で指定します。より高い最大情報レート（Peak Information Rate）も指定できます。レートを超過するパケットは、「アウト オブ プロファイル」または「不適合」です。

ポリサーごとに、アウトオブプロファイル パケットをドロップするか、新しい DSCP 値を適用するかを指定します（新しい DSCP 値を適用することを「マークダウン」といいます）。アウトオブプロファイル パケットは、元のプライオリティを維持しないため、インプロファイル パケットが消費した帯域幅の一部としてカウントされません。

PIR を設定する場合は、PIR アウトオブプロファイル アクションを CIR アウトオブプロファイル アクションよりも厳密なものする必要があります。たとえば、CIR アウトオブプロファイル アクションがトラフィックをマークダウンするアクションの場合、PIR アウトオブプロファイル アクションはトラフィックを送信するアクションにできません。

PFC QoS はあらゆるポリサーで、設定変更可能なグローバル テーブルを使用して、内部 DSCP 値をマークダウンされた DSCP 値にマッピングします。マークダウンが発生すると、PFC QoS はこのテーブルからマークダウンされた DSCP 値を取得します。ユーザが個々のポリサーでマークダウン後の DSCP 値を指定できません。

（注）

- デフォルトでは、マークダウン テーブルは、マークダウンが起こらないように設定されています。つまり、マークダウンされた DSCP 値は、元の DSCP 値と同じです。マークダウンをイネーブルにするには、ネットワークに合わせてテーブルを適切に設定します。
- 入力および出力ポリシング両方を同じトラフィックに適用した場合、入力および出力ポリシーの両方がトラフィックのマークダウンまたはトラフィックのドロップのいずれかを実行する必要があります。PFC QoS では、出力ドロップを使用した入力マークダウン、または出力マークダウンを使用した入力ドロップをサポートしません。

Per-Interface ポリサー

PFC QoS は、インターフェイス別のポリサーで指定された帯域幅制限を、一致したトラフィックに適用します。たとえば、一致するすべての TFTP トラフィックに 1 Mbps を許可するようインターフェイス別のポリサーを設定すると、TFTP トラフィックが 1 Mbps に制限されます。

ポリシー マップ クラスのインターフェイス別ポリサーは、**police** コマンドを使用して定義します。インターフェイス別ポリサーを複数の入力ポートに対応付けると、各ポリサーによって、各入力ポート上の一致するトラフィックが個別にポリシングされます。

集約ポリサー

集約ポリサーの概要

PFC QoS は、1 つの集約ポリサーで指定される帯域幅限度を、一致するトラフィックのすべてのフローに対して累積方式で適用します。たとえば、VLAN 1 および VLAN 3 上のすべての TFTP トラフィック フローの帯域幅として、1 Mbps を許可するように集約ポリサーを設定すると、VLAN 1 および VLAN 3 上のすべての TFTP トラフィック フローは、合計 1 Mbps となるように制限されます。

名前付き集約ポリサーは、**platform qos aggregate-policer** コマンドを使用して作成します。名前付き集約ポリサーを複数の入力ポートに対応付けると、そのポリサーが付加された全入力ポートからの一致するトラフィックがポリシングされます。

最大 1,023 個の集約ポリサーを設定できます。設定されている集約ポリサーをインターフェイスに適用して、最大 16,384 個のポリサー インスタンスを設定できます。

分散型の集約ポリサー

分散型の集約ポリシングがイネーブルの場合、集約ポリサーは、DFC を搭載したさまざまなスイッチング モジュールまたは PFC によってサポートされているインターフェイスで、ポリシングを同期します。分散型の集約ポリシングは、次のタイプに分類される最初の 4,096 個の集約ポリサー インスタンスに適用されます。

- VLAN、トンネル、ポート チャネル インターフェイスに適用された集約ポリサー。

- 共有集約ポリサー。
- 出力ポリシー内の集約ポリサー。

分散型の集約ポリシングがイネーブルの場合、ハードウェアでサポートされている機能を超える部分の集約ポリサーは、非分散型の集約ポリサーとして機能します。

非分散型の集約ポリサー

非分散型の集約ポリシングは、DFC を装備した各スイッチング モジュール上、および PFC（DFC を装備していないスイッチング モジュールをサポート）上で独立して動作します。集約ポリシングでは、DFC を装備した異なるスイッチング モジュールからのフロー統計情報は合算されません。集約ポリシングの統計情報は、DFC を装備した各スイッチング モジュール、PFC、および PFC がサポートする DFC を装備していないスイッチング モジュールについて、表示できます。

個々の PFC または DFC ポリシングは独立して実行されます。これにより、PFC およびすべての DFC 間で分散されているトラフィックに適用される QoS 機能が影響を受けることがあります。このような QoS 機能には、次のようなものがあります。

- ポート チャネル インターフェイスに適用されたポリサー。
- スイッチ仮想インターフェイスに適用されたポリサー。
- レイヤ 3 インターフェイスまたは SVI のいずれかに適用された出力ポリサー。

この制限の影響を受けるポリサーは、集約レートを提供します。これは、独立したすべてのポリシングレートの合計です。

マイクロフロー ポリサー

PFC QoS は、マイクロフロー ポリサーで指定される帯域幅限度を、一致するトラフィックの各フローに対して個別に適用します。たとえば、VLAN 1 および VLAN 3 で TFTP トラフィックを 1 Mbps に制限するようにマイクロフロー ポリサーを設定すると、VLAN 1 の各フローに 1 Mbps が、VLAN 3 の各フローに 1 Mbps がそれぞれ許可されます。つまり、VLAN 1 上に 3 つのフロー、VLAN 3 上に 4 つのフローが存在する場合、microflow ポリサーは、これらの各フローに対して 1 Mbps を許可します。

マイクロフロー ポリサーの帯域幅限度を適用するように、PFC QoS を次のように設定できます。

- マイクロフロー ポリサーは、最大 127 通りのレートとバースト パラメータの組み合わせを使用して作成できます。
- ポリシー マップ クラスのマイクロフロー ポリサーは、**police flow** コマンドを使用して作成します。
- 送信元アドレスだけを使用するようにマイクロフロー ポリサーを設定できます。これにより宛先アドレスに関係なく、特定の送信元アドレスからのすべてのトラフィックにマイクロフロー ポリサーを適用します。
- 宛先アドレスだけを使用するようにマイクロフロー ポリサーを設定できます。これにより、送信元アドレスに関係なく、特定の宛先アドレスへのすべてのトラフィックにマイクロフロー ポリサーが適用されます。

- MAC レイヤ microflow ポリシングの場合、PFC QoS はプロトコルおよび送信元と宛先の MAC レイヤ アドレスが同じである MAC レイヤ トラフィックについては、EtherType が異なるトラフィックでも、同じフローの一部であると見なします。IPX トラフィックをフィルタリングするように MAC ACL を設定できます。
- ARP トラフィックには、マイクロフロー ポリシングを適用できません。
- リリース 15.1(1) SY1 以降のリリースでは、出力マイクロフロー宛先専用ポリシングをサポートしています。出力ポリシングは VLAN ごとで、レイヤ 3 インターフェイスまたは SVI に適用されます。リリース 15.1(1) SY1 よりも前のリリースでは、**output** キーワードで対応付けられたポリシーはマイクロフロー ポリシングをサポートしません。

各ポリシー マップ クラスに集約ポリサーおよびマイクロフロー ポリサーの両方を含めると、単独の帯域利用率と、他のフローと合算された帯域利用率に基づいて、フローのポリシングを行うことができます。

（注）　トラフィックに集約ポリシングとマイクロフロー ポリシングを実行する場合、集約ポリサーおよびマイクロフロー ポリサーを同じポリシー マップ クラスに組み込み、各ポリサーで同じ **conform-action** および **exceed-action** キーワード オプションを使用する必要があります（**drop**、**set-dscp-transmit**、**set-prec-transmit**、または **transmit**）。

たとえば、グループの個々のメンバーに適した帯域幅限度を設定してマイクロフロー ポリサーを作成し、さらに、グループ全体として適切な帯域幅限度を設定して名前付き集約ポリサーを作成できます。グループのトラフィックと一致するポリシー マップ クラスに、この両方のポリサーを含めます。この組み合わせは、個々のフローには別々に作用し、グループには集約的に作用します。

ポリシー マップ クラスに集約ポリサーおよびマイクロフロー ポリサーの両方が含まれている場合、PFC QoS はいずれかのポリサーに基づいてアウトオブプロファイル ステータスに対応し、そのポリサーの指定に従って、新しい DSCP 値を適用するか、またはパケットをドロップします。両方のポリサーからアウトオブプロファイル ステータスが戻された場合には、いずれかのポリサーでパケットのドロップが指定されていれば、パケットはドロップされます。指定されていない場合は、マークダウンされた DSCP 値が適用されます。

分類、マーキング、およびポリシング ポリシーの設定方法

分散型の集約ポリシングのイネーブル化

分散型の集約ポリシング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
`Router(config)# platform qos police distributed {strict | loose}`	分散型の集約ポリシングをイネーブルにします。 • **strict** キーワードを使用すると、使用可能なハードウェア リソースを超えるインターフェイスに対して集約ポリサーが適用されません。 • **loose** キーワードを使用すると、使用可能なハードウェア リソースを超えるインターフェイスに、非分散型として集約ポリサーを適用できます。

次に、厳密な分散型集約ポリシングをグローバルにイネーブルにする例を示します。

```
Router(config)# platform qos police distributed strict
Router(config)#
```

次に、分散型集約ポリシングをグローバルにディセーブルにする例を示します。

```
Router(config)# no platform qos police distributed
Router(config)#
```

クラス マップの設定

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
`Router(config)# class-map [match-all | match-any] class_name`	クラス マップを作成します。 （注）　**match** キーワードを入力しない場合、デフォルトは **match-all** です。

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、表 63-1、「トラフィック分類のクラス マップの match コマンドと一致基準」を参照して、match コマンドを入力します。

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	目的
ステップ 1	`Router (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	`Router# 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。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# class-map ipp5
Router(config-cmap)# match ip precedence 5
Router(config-cmap)# end
```

次に、設定を確認する例を示します。

```
Router# show class-map ipp5
 Class Map match-all ipp5 (id 1)
   Match ip precedence 5
```

ポリシー マップ コンフィギュレーション

ポリシー マップの概要

ポリシー マップには、ポリシー マップ コマンドがそれぞれ異なる 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 タイプ用の全コマンドを、同一のポリシー マップ クラスに入れます。PFC QoS は、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。

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
`Router(config)# policy-map policy_name`	ポリシー マップを作成します。

ポリシー マップ クラスの設定に関する注意事項および制約事項

- PFC QoS は、**class** *class_name* **destination-address**、**class** *class_name* **input-interface**、**class** *class_name* **qos-group**、および **class** *class_name* **source-address** ポリシー マップ コマンドをサポートしていません。
- PFC QoS は、**class default** ポリシー マップ コマンドをサポートします。
- PFC QoS は、インターフェイスにポリシー マップが付加されないかぎり、サポート対象外のコマンドが使用されているかどうかを検出しません。
- PFC QoS は、クラスごとに複数の ACL の一致をサポートしません。

ポリシー マップ クラスの作成およびフィルタリングの設定

ポリシー マップ クラスを作成し、クラス マップを使用してフィルタリング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
`Router(config-pmap)# class class_name`	ポリシー マップ クラスを作成し、クラス マップを使用してフィルタリングするように設定します。 **（注）** PFC QoS は、**match** コマンドが 1 つだけ指定されているクラス マップをサポートします。

ポリシー マップ クラス アクションの設定

- 「ポリシー マップ クラス アクションの制約事項」（P.63-10）
- 「ポリシー マップ クラス マーキングの設定」（P.63-11）
- 「ポリシー マップ クラスの信頼状態の設定」（P.63-12）
- 「ポリシー マップ クラスのポリシングの設定」（P.63-12）

ポリシー マップ クラス アクションの制約事項

- ポリシー マップには、1 つ以上のポリシー マップ クラスを含めることができます。
- 各トラフィック タイプ用の全コマンドを、同一のポリシー マップ クラスに入れます。
- PFC QoS は、1 つのポリシー マップ クラスのコマンドだけをトラフィックに適用します。QoS で、1 つのポリシー マップ クラスのフィルタリングに一致したトラフィックには、他のポリシー マップ クラスで設定したフィルタリングは適用されません。

- ハードウェアでスイッチングされるトラフィックの場合、PFC QoS は **bandwidth**、**priority**、**queue-limit**、または **random-detect** ポリシー マップ クラス コマンドをサポートしません。これらのコマンドはソフトウェアでスイッチングされるトラフィックに使用できるので、設定が可能です。
- PFC QoS では、**set qos-group** ポリシー マップ クラス コマンドはサポートされません。
- PFC QoS は、IPv4 トラフィックに対して **set ip dscp** および **set ip precedence** ポリシー マップ クラス コマンドをサポートします。
  - 非 IP トラフィック上で **set ip dscp** および **set ip precedence** コマンドを使用して、出力レイヤ 2 CoS 値の基準である内部 DSCP 値をマーキングできます。
  - **set ip dscp** および **set ip precedence** コマンドは、**set dscp** および **set precedence** コマンドとしてコンフィギュレーション ファイルに保存されます。
- PFC QoS では、IPv4 および IPv6 トラフィック用の **setdscp** および **set precedence** ポリシー マップ クラス コマンドがサポートされます。
- ポリシー マップ クラスで、次の 3 つすべてを実行することができません。
  - **set** コマンドによるトラフィックのマーキング
  - 信頼状態の設定
  - ポリシングの設定

  ポリシー マップ クラスでは、トラフィックを **set** コマンドによってマーキングするか、次のいずれか、あるいは両方を実行できます。
  - 信頼状態の設定
  - ポリシングの設定

（注） ポリシングを設定する場合は、ポリシング キーワードでトラフィックをマーキングできます。

ポリシー マップ クラス マーキングの設定

PFC QoS は、すべてのトラフィックに対し、**set** ポリシー マップ クラス コマンドを使用したポリシー マップ クラス マーキングをサポートします。ポリシー マップ クラス マーキングを設定するには、次の作業を行います。

コマンド	目的
`Router(config-pmap-c)# set {dscp dscp_value | precedence ip_precedence_value}`	ポリシー マップ クラスを設定して、設定されている DSCP 値または IP precedence 値と一致するトラフィックをマーキングするようにします。

ポリシー マップ クラスの信頼状態の設定

（注）　**service-policy output** コマンドを使用して、信頼状態を設定するポリシー マップを対応付けることができません。

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
`Router(config-pmap-c)# trust {cos | dscp | ip-precedence}`	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、PFC QoS が初期内部 DSCP 値の作成元として使用する値が選択されます。

ポリシー マップ クラスの信頼状態を設定する場合、次の点に注意してください。

- 入力ポート上に設定されている信頼状態を使用するには、**no trust** コマンド（これがデフォルトです）を使用します。
- **cos** キーワードを使用すると、PFC QoS は受信した CoS または入力ポートの 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、PFC QoS は受信した DSCP を使用します。
- **ip-precedence** キーワードを使用すると、PFC QoS は受信した IP precedence に基づいて DSCP を設定します。

ポリシー マップ クラスのポリシングの設定

- 「ポリシー マップ クラスのポリシングの制約事項」（P.63-12）
- 「名前付き集約ポリサーの使用」（P.63-12）
- 「インターフェイス別ポリサーの設定」（P.63-13）
- 「インターフェイス別マイクロフロー ポリサーの設定」（P.63-15）

ポリシー マップ クラスのポリシングの制約事項

- PFC QoS は **set-qos-transmit** ポリサー キーワードをサポートしません。
- PFC QoS は、**exceed-action** キーワードの引数として **set-dscp-transmit** キーワードまたは **set-prec-transmit** キーワードをサポートしません。
- PFC QoS は、インターフェイスにポリシー マップが対応付けられない限り、サポート対象外のキーワードが使用されているかどうかを検出しません。
- **conform-action transmit** キーワードによるポリシングでは、一致するトラフィックのポート信頼状態が、trust dscp またはポリシー マップ クラスの **trust** コマンドで設定される信頼状態に設定されます。

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、次の作業を行います。

コマンド	目的
`Router(config-pmap-c)# police aggregate aggregate_name`	定義済みの名前付き集約ポリサーを使用するように、ポリシー マップ クラスを設定します。

- 分散型の集約ポリシングがイネーブルの場合は、次の情報に注意してください。
  - 分散型の集約ポリサーは、DFC を搭載したさまざまなスイッチング モジュールまたは PFC によってサポートされているインターフェイスで、ポリシングを同期します。分散型の集約ポリシングは、次のタイプに分類される最初の 4,096 個の集約ポリサーに適用されます。
    - VLAN、トンネル、ポート チャネル インターフェイスに適用された集約ポリサー。
    - 共有集約ポリサー。
    - 出力ポリシー内の集約ポリサー。
  - ハードウェアでサポートされている機能を超える部分の分散型の集約ポリサーは、非分散型の集約ポリサーとして機能します。
- 分散型の集約ポリシングがイネーブルでない場合は、次の情報に注意してください。
  - 集約ポリシングは、DFC を装備した各スイッチング モジュール上、および PFC（DFC を装備していないスイッチング モジュールをサポート）上で独立して動作します。集約ポリシングでは、DFC を装備した異なるスイッチング モジュールからのフロー統計情報は合算されません。集約ポリシングの統計情報は、DFC を装備した各スイッチング モジュール、PFC、および PFC がサポートする DFC を装備していないスイッチング モジュールについて、表示できます。
  - 個々の PFC または DFC ポリシングは独立して実行されます。これにより、PFC およびすべての DFC 間で分散されているトラフィックに適用される QoS 機能が影響を受けることがあります。このような QoS 機能には、次のようなものがあります。
    - ポート チャネル インターフェイスに適用されたポリサー。
    - スイッチ仮想インターフェイスに適用されたポリサー。
    - レイヤ 3 インターフェイスまたは SVI のいずれかに適用された出力ポリサー。
  - この制限の影響を受けるポリサーは、集約レートを提供します。これは、独立したすべてのポリシング レートの合計です。

インターフェイス別ポリサーの設定

インターフェイス別のポリサーを設定するには、次の作業を行います。

コマンド	目的
`Router(config-pmap-c)# police` *bits_per_second normal_burst_bytes* [*maximum_burst_bytes*] [**pir** *peak_rate_bps*] [[[**conform-action** {**drop** | **set-dscp-transmit** *dscp_value* | **set-prec-transmit** *ip_precedence_value* | **transmit**}] **exceed-action** {**drop** | **policed-dscp** | **transmit**}] **violate-action** {**drop** | **policed-dscp** | **transmit**}]	インターフェイス別のポリサーを作成して、それを使用するようにポリシー マップ クラスを設定します。

- 入力および出力ポリシング両方を同じトラフィックに適用した場合、入力および出力ポリシーの両方がトラフィックのマークダウンまたはトラフィックのドロップのいずれかを実行する必要があります。PFC QoS では、出力ドロップを使用した入力マークダウン、または出力マークダウンを使用した入力ドロップをサポートしません。
- ポリシングでは、レイヤ 2 フレーム サイズを使用します。
- レートおよびバースト サイズの粒度については、「PFC QoS に関する制約事項」（P.62-1）を参照してください。
- 有効な CIR *bits_per_second* パラメータ値の範囲は、次のとおりです。
  - 最小値：32 Kbps（32000 と入力）
  - 最大：256 Gbps（256000000000 と入力）

- *normal_burst_bytes* パラメータでは、CIR トークン バケット サイズを設定します。
- *maximum_burst_bytes* パラメータでは、PIR トークン バケット サイズを設定します。
- トークン バケット サイズを設定する場合、次の点に注意してください。
  - トークン バケットは 1 つ以上のフレームを格納できる容量が必要なので、トークン バケット サイズには、ポリシングするトラフィックの最大サイズより大きい値を設定してください。
  - TCP トラフィックの場合は、トークン バケット サイズを TCP ウィンドウ サイズの倍数になるように設定します。最小値はポリシングするトラフィックの最大サイズの 2 倍以上にする必要があります。
  - *maximum_burst_bytes* パラメータは、*normal_burst_bytes* パラメータより大きい値に設定する必要があります。
  - 特定のレートを維持するには、トークン バケット サイズがレート値を 2000 で割った値よりも大きくなるように設定します。
  - 最小トークン バケット サイズは 1 バイトで、1 と入力します。
  - 最大トークン バケット サイズは 512 MB で、512000000 と入力されます。
- 有効な **pir** *bits_per_second* パラメータ値の範囲は、次のとおりです。
  - 最小：32 kbps（32000 と入力。CIR *bits_per_second* パラメータより小さい値は使用できません）
  - 最大：256 Gbps（256000000000 と入力）
- （任意）一致するインプロファイル トラフィックに対応する conform アクションを、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。このアクションでは、ポリシー マップ クラスに **trust** コマンドが含まれている場合を除いて、ポリシー マップ クラスの信頼状態が *trust dscp* に設定されます。
  - 信頼できないトラフィックで PFC QoS ラベルを設定するには、**set-dscp-transmit** キーワードを入力し、一致する信頼できないトラフィックに新しい DSCP 値をマーキングするか、または **set-prec-transmit** キーワードを入力し、一致する信頼できないトラフィックに新しい IP precedence 値をマーキングします。**set-dscp-transmit** キーワードおよび **set-prec-transmit** キーワードは IP トラフィックに対してだけサポートされます。PFC QoS は、設定された値に基づいて出力 ToS および CoS を設定します。
  - 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。
  - 同じトラフィックに適用する集約ポリサーおよびマイクロフロー ポリサーで、それぞれ同じ conform アクションの動作が指定されていることを確認してください。
- （任意）CIR を超過するトラフィックに対しては、exceed アクションを次のように指定できます。
  - ポリシングなしでマーキングするには、**transmit** キーワードを入力して、一致したすべてのアウトオブプロファイル トラフィックを送信します。
  - デフォルトの exceed アクションは、*maximum_burst_bytes* パラメータを使用しない場合は **drop** です（*maximum_burst_bytes* パラメータでは、**drop** はサポートされません）。

    （注） exceed アクションが **drop** の場合、PFC QoS は設定された violate アクションを無視します。

  - 一致したすべての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。

（注）　**pir** キーワードを使用せずにポリサーを作成し、かつ *maximum_burst_bytes* パラメータが *normal_burst_bytes* パラメータに等しい場合（*maximum_burst_bytes* パラメータを入力しない場合）、**exceed-action policed-dscp-transmit** キーワードを使用すると、PFC QoS は **policed-dscp max-burst** マークダウン マップの定義に従ってトラフィックをマークダウンします。

- （任意）PIR を超過するトラフィックについて、violate アクションを次のように指定できます。
  - ポリシングなしでマーキングするには、**transmit** キーワードを入力して、一致したすべてのアウトオブプロファイル トラフィックを送信します。
  - デフォルトの violate アクションは、exceed アクションと同じものです。
  - 一致したすべての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。

次に、**max-pol-ipp5** という名前のポリシー マップを作成する例を示します。このポリシー マップは、クラス マップ **ipp5** を使用し、受信した IP precedence 値に基づいて信頼状態を設定し、最大容量に関する集約ポリサーおよびマイクロフロー ポリサーを設定します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# policy-map max-pol-ipp5
Router(config-pmap)# class ipp5
Router(config-pmap-c)# trust ip-precedence
Router(config-pmap-c)# police 2000000000 2000000 conform-action set-prec-transmit 6
exceed-action policed-dscp-transmit
Router(config-pmap-c)# police flow 10000000 10000 conform-action set-prec-transmit 6
exceed-action policed-dscp-transmit
Router(config-pmap-c)# end
```

インターフェイス別マイクロフロー ポリサーの設定

インターフェイス別のマイクロフロー ポリサーを設定するには、次の作業を行います。

コマンド	目的
Router(config-pmap-c)# **police flow** [**mask** {**src-only** | **dest-only** | **full-flow**}] *bits_per_second normal_burst_bytes* [[[**conform-action** {**drop** | **set-dscp-transmit** *dscp_value* | **set-prec-transmit** *ip_precedence_value* | **transmit**}] **exceed-action** {**drop** | **policed-dscp** | **transmit**}] **violate-action** {**drop** | **policed-dscp** | **transmit**}]	インターフェイス別のマイクロフロー ポリサーを作成して、それを使用するようにポリシーマップ クラスを設定します。

- 入力および出力ポリシング両方を同じトラフィックに適用した場合、入力および出力ポリシーの両方がトラフィックのマークダウンまたはトラフィックのドロップのいずれかを実行する必要があります。PFC QoS では、出力ドロップを使用した入力マークダウン、または出力マークダウンを使用した入力ドロップをサポートしません。
- ポリシングでは、レイヤ 2 フレーム サイズを使用します。
- レートおよびバースト サイズの粒度については、「PFC QoS に関する制約事項」（P.62-1）を参照してください。
- 送信元アドレスだけに基づいてフローの識別を行うには、**mask src-only** キーワードを入力します。これにより、マイクロフロー ポリサーが、各送信元アドレスからのすべてのトラフィックに適用されます。PFC QoS では、IP トラフィックおよび MAC トラフィック両方に対して **mask src-only** キーワードをサポートします。

- 宛先アドレスだけに基づいてフローの識別を行うには、**mask dest-only** キーワードを入力します。これにより、マイクロフロー ポリサーが、各送信元アドレスへのすべてのトラフィックに適用されます。PFC QoS では、IP トラフィックおよび MAC トラフィック両方に対して **mask dest-only** キーワードをサポートします。リリース 15.1(1) SY1 以降のリリースでは、出力マイクロフロー宛先専用ポリシングをサポートしています。出力ポリシングは VLAN ごとで、レイヤ 3 インターフェイスまたは SVI に適用されます。
- デフォルトおよび **mask full-flow** キーワードを使用する場合は、PFC QoS は送信元 IP アドレス、宛先 IP アドレス、レイヤ 3 プロトコル、レイヤ 4 ポート番号に基づいて IP フローの識別を行います。
- PFC QoS は、プロトコルおよび送信元と宛先 MAC レイヤ アドレスが同じである MAC レイヤ トラフィックについては、EtherType が違っていても、同じフローの一部であると見なします。
- マイクロフロー ポリサーでは、*maximum_burst_bytes* パラメータ、**pir** *bits_per_second* キーワードおよびパラメータ、または **violate-action** キーワードはサポートされません。

（注） マイクロフロー ポリシング、NetFlow、および NetFlow データ エクスポート（NDE）のフローマスク要件は、競合する可能性があります。

- 有効な CIR *bits_per_second* パラメータ値の範囲は、次のとおりです。
  - 最小値：32 Kbps（32000 と入力）
  - 最大：256 Gbps（256000000000 と入力）
- *normal_burst_bytes* パラメータでは、CIR トークン バケット サイズを設定します。
- トークン バケット サイズを設定する場合、次の点に注意してください。
  - トークン バケットは 1 つ以上のフレームを格納できる容量が必要なので、トークン バケット サイズには、ポリシングするトラフィックの最大サイズより大きい値を設定してください。
  - TCP トラフィックの場合は、トークン バケット サイズを TCP ウィンドウ サイズの倍数になるように設定します。最小値はポリシングするトラフィックの最大サイズの 2 倍以上にする必要があります。
  - *maximum_burst_bytes* パラメータは、*normal_burst_bytes* パラメータより大きい値に設定する必要があります。
  - 特定のレートを維持するには、トークン バケット サイズがレート値を 2000 で割った値よりも大きくなるように設定します。
  - 最小トークン バケット サイズは 1 バイトで、1 と入力します。
  - 最大トークン バケット サイズは 512 MB で、512000000 と入力されます。
- （任意）一致するインプロファイル トラフィックに対応する conform アクションを、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。このアクションでは、ポリシー マップ クラスに **trust** コマンドが含まれている場合を除いて、ポリシー マップ クラスの信頼状態が *trust dscp* に設定されます。
  - 信頼できないトラフィックで PFC QoS ラベルを設定するには、**set-dscp-transmit** キーワードを入力し、一致する信頼できないトラフィックに新しい DSCP 値をマーキングするか、または **set-prec-transmit** キーワードを入力し、一致する信頼できないトラフィックに新しい IP precedence 値をマーキングします。**set-dscp-transmit** キーワードおよび **set-prec-transmit** キーワードは IP トラフィックに対してだけサポートされます。PFC QoS は、設定された値に基づいて出力 ToS および CoS を設定します。
  - 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。

- 同じトラフィックに適用する集約ポリサーおよびマイクロフロー ポリサーで、それぞれ同じ conform アクションの動作が指定されていることを確認してください。

- （任意）CIR を超過するトラフィックに対しては、exceed アクションを次のように指定できます。
  - ポリシングなしでマーキングするには、**transmit** キーワードを入力して、一致したすべてのアウトオブプロファイル トラフィックを送信します。
  - デフォルトの exceed アクションは、*maximum_burst_bytes* パラメータを使用しない場合は **drop** です（*maximum_burst_bytes* パラメータでは、**drop** はサポートされません）。

    （注）　exceed アクションが **drop** の場合、PFC QoS は設定された violate アクションを無視します。

  - 一致したすべての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。

    （注）　**pir** キーワードを使用せずにポリサーを作成し、かつ *maximum_burst_bytes* パラメータが *normal_burst_bytes* パラメータに等しい場合（*maximum_burst_bytes* パラメータを入力しない場合）、**exceed-action policed-dscp-transmit** キーワードを使用すると、PFC QoS は **policed-dscp max-burst** マークダウン マップの定義に従ってトラフィックをマークダウンします。

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
ステップ 1	`Router(config-pmap-c)# end`	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。 （注）　ポリシー マップで追加クラスを作成するには、追加の **class** コマンドを入力します。
ステップ 2	`Router# 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。

```
Router# show policy-map max-pol-ipp5
 Policy Map max-pol-ipp5
  class  ipp5

  class ipp5
    police flow 10000000 10000 conform-action set-prec-transmit 6 exceed-action
policed-dscp-transmit
    trust precedence
    police 2000000000 2000000 2000000 conform-action set-prec-transmit 6 exceed-action
policed-dscp-transmit

Router#
```

インターフェイスへのポリシー マップの対応付け

ポリシー マップをインターフェイスに対応付けるには、次の作業を行います。

	コマンド	目的
ステップ1	`Router(config)# interface {{vlan vlan_ID}	{type slot/port[.subinterface]}	{port-channel number[.subinterface]}}`	設定するインターフェイスを選択します。
ステップ2	`Router(config-if)# service-policy [input	output] policy_map_name`	ポリシー マップをインターフェイスに対応付けます。
ステップ3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。

- EtherChannel のメンバーであるポートに、サービス ポリシーを付加しないでください。
- PFC QoS は、レイヤ 3 インターフェイス（レイヤ 3 インターフェイスとして設定された LAN ポートまたは VLAN インターフェイスのいずれか）上だけで **output** キーワードをサポートします。レイヤ 3 インターフェイスには、入力および出力ポリシー マップの両方を付加できます。
- レイヤ 2 ポート上の VLAN ベースまたはポートベースの PFC QoS は、**output** キーワードを使用してレイヤ 3 インターフェイスに対応付けられたポリシーとは関係ありません。
- リリース 15.1(1) SY1 以降のリリースでは、出力マイクロフロー宛先専用ポリシングをサポートしています。出力ポリシングは VLAN ごとで、レイヤ 3 インターフェイスまたは SVI に適用されます。リリース 15.1(1) SY1 よりも前のリリースでは、**output** キーワードで対応付けられたポリシーはマイクロフロー ポリシングをサポートしません。
- **service-policy output** コマンドを使用して、信頼状態を設定するポリシー マップを対応付けることができません。
- **output** キーワードを使用して対応付けられたポリシーの IP precedence または DSCP に基づいたフィルタリングでは、受信した IP precedence 値または DSCP 値が使用されます。**output** キーワードを使用して対応付けられたポリシーの IP precedence または DSCP に基づいたフィルタリングは、入力 QoS による IP precedence または DSCP の変更には基づいていません。
- 共有集約ポリサーは、入力と出力の両方の方向には適用できません。
- 分散型の集約ポリシングがイネーブルの場合、集約ポリサーは、DFC を搭載したさまざまなスイッチング モジュールまたは PFC によってサポートされているインターフェイスで、ポリシングを同期します。分散型の集約ポリシングは、次のタイプに分類される最初の 4,096 個の集約ポリサー インスタンスに適用されます。
  - VLAN、トンネル、ポート チャネル インターフェイスに適用された集約ポリサー。
  - 共有集約ポリサー。
  - 出力ポリシー内の集約ポリサー。

  分散型の集約ポリシングがイネーブルの場合、ハードウェアでサポートされている機能を超える部分の集約ポリサーは、非分散型の集約ポリサーとして機能します。

- 非分散型の集約ポリシングは、DFC を装備した各スイッチング モジュール上、および PFC（DFC を装備していないスイッチング モジュールをサポート）上で独立して動作します。集約ポリシングでは、DFC を装備した異なるスイッチング モジュールからのフロー統計情報は合算されません。集約ポリシングの統計情報は、DFC を装備した各スイッチング モジュール、PFC、および PFC がサポートする DFC を装備していないスイッチング モジュールについて、表示できます。

  個々の PFC または DFC ポリシングは独立して実行されます。これにより、PFC およびすべての DFC 間で分散されているトラフィックに適用される QoS 機能が影響を受けることがあります。このような QoS 機能には、次のようなものがあります。

  - ポート チャネル インターフェイスに適用されたポリサー。
  - スイッチ仮想インターフェイスに適用されたポリサー。
  - レイヤ 3 インターフェイスまたは SVI のいずれかに適用された出力ポリサー。

  この制限の影響を受けるポリサーは、集約レートを提供します。これは、独立したすべてのポリシング レートの合計です。

- 非集約ポリサーの場合は、個々の PFC または DFC ポリシングは独立して実行されます。これにより、PFC およびすべての DFC 間で分散されているトラフィックに適用される QoS 機能が影響を受けることがあります。このような QoS 機能には、次のようなものがあります。

  - ポート チャネル インターフェイスに適用されたポリサー。
  - スイッチ仮想インターフェイスに適用されたポリサー。
  - レイヤ 3 インターフェイスまたは SVI のいずれかに適用された出力ポリサー。

  この制限の影響を受けるポリサーは、集約レートを提供します。これは、独立したすべてのポリシング レートの合計です。

- 入力および出力ポリシング両方を同じトラフィックに適用した場合、入力および出力ポリシーの両方がトラフィックのマークダウンまたはトラフィックのドロップのいずれかを実行する必要があります。PFC QoS では、出力ドロップを使用した入力マークダウン、または出力マークダウンを使用した入力ドロップをサポートしません。

次に、ポリシー マップ **pmap1** をギガビット イーサネット ポート 5/36 に対応付ける例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 5/36
Router(config-if)# service-policy input pmap1
Router(config-if)# end
```

次に、設定を確認する例を示します。

```
Router# show policy-map interface gigabitethernet 5/36
 gigabitethernet5/36
  service-policy input: pmap1
    class-map: cmap1 (match-all)
      0 packets, 0 bytes
      5 minute rate 0 bps
      match: ip precedence 5
  class cmap1
    police 8000 8000 conform-action transmit exceed-action drop
    class-map: cmap2 (match-any)
      0 packets, 0 bytes
      5 minute rate 0 bps
      match: ip precedence 2
        0 packets, 0 bytes
        5 minute rate 0 bps
  class cmap2
    police 8000 10000 conform-action transmit exceed-action drop
Router#
```

ポリシー マップの動的セッション単位接続の設定

ポリシー マップの動的セッション単位接続の前提条件

- ユーザが認証されるときに割り当てられる、入力および出力 QoS ポリシー マップを定義します。
- アイデンティティ ポリシーを設定して、割り当てられるポリシー マップを指定します。
- RADIUS サーバのユーザ プロファイルで、Cisco ベンダー固有属性（VSA）を設定して、各ユーザに割り当てられる入力および出力 QoS ポリシー マップを指定します。

ポリシー マップの定義と関連付け

ポリシー マップを定義して、アイデンティティ ポリシーに関連付けるには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# policy-map` *in_policy_name*	入力 QoS ポリシー マップを設定します。
ステップ 2	`Router(config-pmap)# class` *class_map_name* `...`	ポリシー マップ クラスを設定します。
ステップ 3	`Router(config-pmap-c)# exit`	ポリシー マップ クラス 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 4	`Router(config)# policy-map` *out_policy_name*	出力 QoS ポリシー マップを設定します。
ステップ 5	`Router(config-pmap)# class` *class_map_name* `...`	ポリシー マップ クラスを設定します。
ステップ 6	`Router(config-pmap-c)# exit`	ポリシー マップ クラス 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 7	`Router(config)# identity policy` *policy1*	アイデンティティ ポリシーを作成し、アイデンティティ ポリシー 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 8	`Router(config-identity-policy)# service-policy type qos input` *in_policy_name*	入力 QoS ポリシー マップとこのアイデンティティを関連付けます。
ステップ 9	`Router(config-identity-policy)# service-policy type qos output` *out_policy_name*	出力 QoS ポリシー マップとこのアイデンティティを関連付けます。
ステップ 10	`Router(config-identity-policy)# end`	アイデンティティ ポリシー コンフィギュレーション サブモードを停止して、特権 EXEC モードに戻ります。

アイデンティティ ポリシーを削除するには、**no identity-policy** *policy_name* コマンドを使用します。

ポリシー マップを定義したら、次に示すように、ポリシー マップ名を使用して、RADIUS サーバの各ユーザ プロファイルで Cisco AV ペア属性を設定します。

- cisco-avpair = "ip:sub-policy-In=*in_policy_name*"
- cisco-avpair = "ip:sub-policy-Out=*out_policy_name*"

RADIUS サーバで Cisco AV ペア属性を設定するには、次の作業を行います。

コマンドまたはアクション	目的
sub-policy-In=*in_policy_name* **sub-policy-Out=***out_policy_name*	ユーザ ファイルで RADIUS サーバのサービス ポリシーの 2 つの Cisco AV ペアを入力します。スイッチがポリシー名を要求すると、ユーザ ファイルのこの情報が提供されます。 RADIUS ユーザ ファイルには、RADIUS サーバが認証する各ユーザのエントリが含まれます。各エントリは、*ユーザ プロファイル* とも呼ばれ、ユーザがアクセスできる属性を確立します。 この例で設定されるサービス ポリシーでは、QoS ポリシー マップがインターフェイスに接続され、方向が指定されます（方向は、データ パケットがインターフェイスに送信される場合はインバウンド、データ パケットがインターフェイスから送信される場合はアウトバウンドです）。 インバウンド方向で適用されるポリシー マップは、example_in_qos で、アウトバウンド ポリシー マップは example_out_qos です。

次に、RADIUS サーバのユーザ ファイルのコンフィギュレーションの例を示します。

```
userid    Password ="cisco"
   Service-Type = Framed,
   Framed-Protocol = PPP,
   cisco-avpair = "sub-policy-In=example_in_qos",
   cisco-avpair = "sub-policy-Out=example_out_qos"
```

次に、セッションがアクティブの場合、**show epm session summary** コマンドの出力例を示します。

```
Router# show epm session summary

EPM Session Information
-----------------------
Total sessions seen so far : 5
Total active sessions      : 1
Session IP Address         : 192.0.2.1
-------------------
```

次に、IP アドレスが 192.0.2.1 のインターフェイスでセッションがアクティブの場合の **show epm session ip** *ip_addr* コマンドの出力例を示します。

```
Router# show epm session ip 192.0.2.1

Admission feature       : AUTHPROXY
AAA Policies            :
Input Service Policy    : in_policy_name
Output Service Policy   : out_policy_name
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CHAPTER 64

ポリシーベース キューイング

（注）
- キューイングはオプションです。輻輳したリンクを処理するポートにキューイングを設定するには、ここで説明するコマンドを使用します。
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

ポリシー ベースのキューイングの前提条件

なし。

ポリシー ベースのキューに関する制約事項

- WS-X6904-40G-2T スイッチング モジュールのポートには、2 個のプライオリティ キュー（2p6q4t）を設定できます。プライオリティ キュー 1 は、プライオリティ キュー 2 よりもプライオリティが高くなります。
- WS-X6904-40G-2T 出力キューでは、QoS シェーピングをサポートしています。
  - シェーピングでは、総出力ポート帯域幅を超えるトラフィックをバッファ処理します。シェーピングは、出力キューおよびポートの出力トラフィックに設定できます。
  - シェーピングは、総出力ポート帯域幅のパーセンテージとして設定します。
  - シェーピングは、WS-X6904-40G-2T ポートの出力キューだけに設定できます。ポートチャネル インターフェイスには、シェーピングを設定できません。
  - シェーピングが設定されたポートは EtherChannel のメンバーになれますが、シェーピングによって出力トラフィック レートが大幅に変わることがあり、メンバ ポート間で大きな違いが生じる可能性があります。
  - シェーピングは、**shape average percent** コマンドで設定します。**show running-configuration** コマンドでは **shape average percent** コマンドが表示される一方、**show policy-map type lan-queuing** コマンドでは、「Average Rate Traffic Shaping」という見出しの下に、**cir** *percentage* コマンドを使用したシェーピング設定が表示されます。

  「WS-X6904-40G-2T ポートでのポリシー ベース キューイングの設定」（P.64-13）を参照してください。
- DSCP ベースのキューイングは、8q4t、1p7q2t、2p6q4t、および 1p7q4t ポートでサポートされています。Supervisor Engine 2T-10GE ポートは **platform qos 10g-only** 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 8q4t/1p7q4t ポートです。このコマンドにより、スーパーバイザ エンジンのギガビット イーサネット ポートはディセーブルになります。
- ポートに対応付けられているキューイング ポリシーで使用されるクラス マップに、**match dscp** コマンドまたは **match precedence** コマンドがあると、キューイング ポリシーが対応付けられている方向での DSCP ベースのキューイングがポートで可能になります。
- CoS ベースのキューイングは、非 IP トラフィック、IP マルチキャスト トラフィック、および IP の未知のユニキャスト フラッディング トラフィックに、常に使用されます。
- キューイング ポリシーで使用されるクラス マップでは、**match dscp**、**match precedence**、または **match cos** コマンドを、任意の数、任意に組み合わせて使用できます。
- マーキングまたはポリシングを設定するポリシーに加えて、入力と出力のキューイング ポリシー 1 つずつをインターフェイスに対応付けられます。WS-X6904-40G-2T 出力非プライオリティ キューで、キューごとのシェーピングをサポートするために、WS-X6904-40G-2T ポート出力キューの出力キューイング ポリシーでは、子ポリシーをサポートしています。
- Cisco IOS Release 12.2SX 設定からの移行をサポートするために、Cisco IOS Release 15.1SY では、グローバル コンフィギュレーション モードとインターフェイス コンフィギュレーション モードのキューイング コマンドをサポートしています。
  - ポートに入力または出力のキューイング ポリシーを対応付けると、このポートのすべてのインターフェイス コンフィギュレーション モード キューイング コマンドが削除されます。
  - 対応付けられた入力または出力のキューイング ポリシーにより、設定されているすべてのグローバル コンフィギュレーション モード キューイング コマンドの作用が上書きされます。

  - 1 方向のみにキューイング ポリシーを対応付けた場合、もう 1 方向に対するキューイング設定は、デフォルトになるか、設定されている任意のグローバル コンフィギュレーション モード キューイング コマンドで定義されます。
  - キューイング ポリシーが対応付けられているポートには、いずれのインターフェイス コンフィギュレーション モード キューイング コマンドも設定できません。
- ポリシー ベースのキューイングは、Cisco IOS Release 15.1SY で Supervisor Engine 2T-10GE と合わせてサポートしている、すべてのモジュールでサポートされています。
- キューイング ポリシーでは、対応付けられるポートでサポートされていないコマンドを含むことができないため、キューイング ポリシーは、特定のポート タイプに固有です（「ポリシー ベース キューイングの設定例」（P.64-19）を参照）。ポートでサポートされないコマンドは無視されません。サポート対象外のコマンドを含むポリシーは、ポートに正常に適用できません。
- わかりやすくするために、キューイング ポリシーの名前には、**1q2t_1q8t_ingress** など、サポートするポート タイプに対応する名前を設定してください。
- キューイング ポリシーは、複数のクラス マップを含むことができます。各クラス マップで、キューを設定します。
- クラス マップを使用する **class** コマンドで定義されており、ポリシーマップ クラス **priority** コマンドを含んでいるポリシー マップ クラスは、プライオリティ キューを設定します。（プライオリティ キューは、最大の番号を持つキューです）。クラス マップは、設定されている QoS 値（CoS または DSCP）をプライオリティ キューに対してフィルタリングします。
- ポートの SRR をイネーブルにするとプライオリティ キューがディセーブルになります。
- クラス マップを使用する **class** コマンドで定義されており、ポリシーマップ クラス **priority** コマンドを含んでいないポリシー マップ クラスは、最大番号の非プライオリティ キューを設定します。（ポートにプライオリティ キューがある場合、最大番号の非プライオリティ キューには、プライオリティ キューから 1 を引いた番号が付けられます。ポートにプライオリティ キューがない場合、最大番号のキューは非プライオリティ キューです。）後続のこのようなコマンドでは、逆の番号順で、残りの非プライオリティ キューの設定が定義されます。キューはスキップできませんが、すべてのキューを設定する必要はありません。クラス マップは、設定されている QoS 値を、設定中の非プライオリティ キューにフィルタリングします。
- **class-default** キーワードを使用する **class** コマンドは、キュー 1 を設定します。**class-default** キーワードは、残りのすべての QoS 値をキュー 1 にフィルタリングします。
- 各非プライオリティ キューに対し、ポリシーマップ クラス **queue-buffers** または **random-detect** コマンドは、QoS 値（CoS または DSCP）をキュー内のしきい値に割り当てます。しきい値は、番号順に設定されます。しきい値はスキップできませんが、すべてのしきい値を設定する必要はありません。しきい値に適用されている QoS 値は、クラス マップがキューにフィルタリングする値のグループに含まれている必要があります。
  - 最初の **queue-buffers** コマンドまたは **random-detect** コマンドは、最初のしきい値に QoS 値を割り当て、これに適用されるパーセント値を設定します。
  - 同じパーセント値で設定されている後続の **queue-buffers** コマンドまたは **random-detect** コマンドは、追加の QoS 値を最初のしきい値に割り当てます。
  - 異なるパーセント値で設定されている次の **queue-buffers** コマンドまたは **random-detect** コマンドは、数値的に次のしきい値に QoS 値を割り当て、これに適用されるパーセント値を設定します。
  - 同じパーセント値で設定されている後続の **queue-buffers** コマンドまたは **random-detect** コマンドは、数値的に次のしきい値に追加の QoS 値を割り当てます。
  - 異なるパーセンテージの各 **queue-buffers** コマンドまたは **random-detect** コマンドは、次の未構成のしきい値を定義し、単一のパーセント値を繰り返す後続のすべてのコマンドは、設定されているしきい値に追加の QoS 値を割り当てます。

- すべての未設定のしきい値は 100% になります。
- 未割り当てのすべての QoS ラベルは、最大番号のしきい値に割り当てられます。

ポリシー ベース キューイングに関する情報

ポート ベースのキュー タイプ

入力および出力のバッファとキュー

（注）　WS-X6904-40G-2T 出力キューでは、QoS シェーピングをサポートしています。

イーサネット ポートの ASIC は、固定数のキューに分割されるバッファを備えています。輻輳回避をイネーブルにすると、PFC QoS では、トラフィックのレイヤ 2 CoS 値を使用するか、特定のポート タイプの場合にレイヤ 3 DSCP 値を使用して、キューにトラフィックを割り当てます。バッファとキューは、スイッチを中継する際、一時的にフレームを保存します。PFC QoS はポートの ASIC メモリを、各ポートの各キューに対するバッファとして割り当てます。

イーサネット ポートは、次のキュー タイプをサポートします。

- 非プライオリティ キュー
- プライオリティ キュー

イーサネット ポートは、キュー間で次のスケジューリング アルゴリズムをサポートします。

- シェイプド ラウンド ロビン（SRR）：SRR を使用すると、1 つのキューは、割り当てられた帯域幅だけの使用が許可されます。
- Deficit Weighted Round Robin（DWRR）：より高いプライオリティのキュー内のトラフィックによってプライオリティを低く設定されている、転送中のすべてのキューを追跡し、次回のラウンドでこの差分を補います。
- 重み付きラウンドロビン（WRR）：WRR は、キューに対する帯域幅を明示的に確保しておきません。各キューに割り当てられる帯域幅の量は、ユーザが設定できます。キューに割り当てられる割合（重み）は、このキューに割り当てられる帯域幅の量を定義します。
- プライオリティ キューイング：完全優先キューイングは、他のキューのパケットがデキューイングされる前に、音声などの遅延に影響されやすいデータのデキューイングおよび送信を許可し、遅延に影響されやすいデータを他のトラフィックより優先させます。スイッチは、完全優先送信キュー内のトラフィックを処理してから、非プライオリティ キューを処理します。非プライオリティ キューのパケットが送信されたあと、スイッチが完全優先キュー内のトラフィックを確認し

ます。スイッチは完全優先キュー内でトラフィックを検出すると、非プライオリティ キューの処理を中断し、先に完全優先キュー内のすべてのトラフィックを処理してから、非プライオリティ キューに戻ります。

イーサネット ポートの LAN モジュールは、輻輳回避を実行する際、キュー内で次のタイプのしきい値を使用します。

- 重み付きランダム早期検出（WRED）：WRED ドロップしきい値を設定したポートでは、バッファの輻輳を回避する目的のランダムな確率に基づき、特定の QoS ラベルを持つフレームがキューへの入力を許可されます。特定の QoS ラベルを持つフレームがキューへの入力を許可、または廃棄される確率は、この QoS ラベルに割り当てられた重みとしきい値に依存します。

  たとえば、しきい値が 2 のキュー 1 に CoS 2 が割り当てられ、しきい値 2 のレベルが 40%（ロー）および 80%（ハイ）であるとします。この場合、CoS 2 を持つフレームは、キュー 1 が 40% 以上占有されるまではドロップされません。キュー項目数が 80% に近づくにつれ、CoS 2 を持つフレームは、キューへの入力が許可される確率よりも、廃棄される確率のほうが高くなります。キューの占有率が 80% を超えると、キューの占有率が 80% 未満となるまで、CoS 2 フレームはすべてドロップされます。キュー レベルが低しきい値と高しきい値の間にあるときにスイッチが廃棄するフレームは、フロー単位または FIFO 方式ではなく、ランダムに抽出されます。この方法は、バックオフや転送ウィンドウ サイズの調整によって、定期的なパケット ドロップに適応することが可能な、TCP などのプロトコルに適します。

- テールドロップしきい値：テールドロップしきい値を設定したポートでは、特定の QoS ラベルを持つフレームは、この QoS ラベルに関連付けられたドロップしきい値を超過するまで、キューへの入力を許可されます。同じ QoS ラベルを持つ以降のフレームは、しきい値の超過状態が解消するまで廃棄されます。たとえば、しきい値が 2 のキュー 1 に CoS 1 が割り当てられ、しきい値 2 の水準が 60% であるとします。この場合、CoS 1 を持つフレームは、キュー 1 が 60% 占有されるまではドロップされません。以降のすべての CoS 1 フレームは、キューの占有率が 60 % 未満になるまでドロップされます。一部のポート タイプでは、テールドロップしきい値および WRED ドロップしきい値の両方を使用するように非プライオリティ受信キューを設定するには、CoS 値をキューにマッピングするか、またはキューおよびしきい値にマッピングします。スイッチでは、キューにだけマッピングされている CoS 値を伝送するトラフィックには、テール ドロップしきい値が使用されます。キューとしきい値にマッピングされた CoS 値を伝送するトラフィックには、WRED ドロップしきい値が使用されます。同じタイプの LAN ポートは、すべて同じドロップしきい値の設定を使用します。

（注）

- キューイング ポリシーまたはレガシー インターフェイス コマンド（「DSCP ベースのキュー マッピングのレガシー コンフィギュレーション手順」（P.65-14）を参照）を使用して、8q4t、1p7q2t、および 1p7q4t ポート（「モジュールとキュー タイプのマッピング」（P.64-7）を参照）で、DSCP ベースのキューおよびしきい値をイネーブルにできます。
- DSCP ベースのキューイングは、8q4t、1p7q2t、および 1p7q4t ポートでサポートされています。Supervisor Engine 2T-10GE のポートは、**platform qos 10g-only** 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 8q4t/1p7q4t です。Supervisor Engine 2T ポートに DSCP ベースのキュー マッピングを設定するには、**shutdown** インターフェイス コンフィギュレーション モード コマンドを Supervisor Engine 2T ギガビット イーサネット ポートに対して入力する必要があります。次に、**platform qos 10g-only** グローバル コンフィギュレーション コマンドを入力し、Supervisor Engine 2T 上のギガビット イーサネット ポートをディセーブルにします。

スイッチは、複数のキューと各キューに関連付けられたスケジューリング アルゴリズムの組み合わせによって輻輳回避を実現します。

入力キュー タイプ

LAN ポートのキュー構造を表示するには、**show queueing interface** *type slot/port* | **include type** コマンドを入力します。このコマンドを実行すると、次のいずれかのアーキテクチャが表示されます。

- **1q2t** は、1 つの設定変更可能なテールドロップしきい値および 1 つの設定変更できないテールドロップしきい値がある、1 つの非プライオリティ キューを示します。
- **2q4t** は、それぞれ 4 つの設定変更可能なテールドロップしきい値がある 2 つの非プライオリティ キューを示します。
- **2q8t** は、それぞれ 8 つの設定変更可能なテールドロップしきい値がある 2 つの非プライオリティ キューを示します。
- **8q4t** は、8 つの非プライオリティ キューがあり、それぞれ 4 つのしきい値を持ち、それぞれ WRED ドロップまたはテールドロップとして設定可能で、DSCP ベースのキューイングをサポートすることを示します。
- **8q8t** は、それぞれ WRED ドロップまたはテールドロップとして設定変更可能な 8 つのしきい値がある 8 つの非プライオリティ キューを意味します。
- **1p1q4t** は次を意味します。
  - 1 つの完全優先キュー
  - 4 つの設定変更可能なテールドロップしきい値がある 1 つの非プライオリティ キュー
- **1p7q2t** は次を意味します。
  - 1 つの完全優先キュー
  - WRED ドロップまたはテールドロップのいずれかとして設定変更可能なしきい値がそれぞれ 2 つある、7 つの非プライオリティ キュー
  - DSCP ベースのキューイングをサポート
- **2p6q4t** は次を意味します。
  - 2 つの完全優先キュー
  - WRED ドロップまたはテールドロップのいずれかとして設定変更可能なしきい値がそれぞれ 4 つある、6 つの非プライオリティ キュー
  - DSCP ベースのキューイングをサポート
- **1p7q4t** は次を意味します。
  - 1 つの完全優先キュー
  - WRED ドロップまたはテールドロップのいずれかとして設定変更可能なしきい値がそれぞれ 4 つある、7 つの非プライオリティ キュー
  - DSCP ベースのキューイングをサポート

出力キューのタイプ

出力 LAN ポートのキュー構造を表示するには、**show queueing interface** *type slot/port* | **include type** コマンドを入力します。このコマンドを実行すると、次のいずれかのアーキテクチャが表示されます。

- **1p3q8t** は次を意味します。
  - 1 つの完全優先キュー
  - WRED ドロップまたはテールドロップのどちらかとして設定変更可能なしきい値が 8 つずつある 3 つの非プライオリティ キュー

- **2p6q4t** は次を意味します。
  - 2 つの完全優先キュー
  - WRED ドロップまたはテールドロップのいずれかとして設定変更可能なしきい値がそれぞれ 4 つある、6 つの非プライオリティ キュー
  - DSCP ベースのキューイングをサポート
  - キューごとのシェーピングおよびポートごとのシェーピングをサポート
- **1p7q4t** は次を意味します。
  - 1 つの完全優先キュー
  - WRED ドロップまたはテールドロップのいずれかとして設定変更可能なしきい値がそれぞれ 4 つある、7 つの非プライオリティ キュー
  - DSCP ベースのキューイングをサポート
  - WS-X6904-40G-2T で、キューごとのシェーピングおよびポートごとのシェーピングをサポート
- **1p7q8t** は次を意味します。
  - 1 つの完全優先キュー
  - WRED ドロップまたはテールドロップのいずれかとして設定変更可能なしきい値が 8 つずつある 7 つの非プライオリティ キュー

モジュールとキュー タイプのマッピング

- 表 64-1—「スーパーバイザ エンジン モジュールの QoS キュー構造」
- 表 64-2—「40 ギガビット イーサネット モジュール」
- 表 64-3—「10 ギガビット イーサネット モジュール」
- 表 64-4—「ギガビットおよび 10/100/1000 イーサネット モジュール」

表 64-1　スーパーバイザ エンジン モジュールの QoS キュー構造

スーパーバイザ エンジン	入力キューおよびドロップしきい値	入力キュースケジューラ	出力キューおよびドロップしきい値	出力キュースケジューラ	合計バッファサイズ	入力バッファサイズ	出力バッファサイズ
VS-S2T-10G-XL、VS-S2T-10G							
ギガビット イーサネット ポートがイネーブルな場合	2q4t	WRR	1p3q4t	DWRR または SRR		128 MB	112 MB
	DSCP ベースのキューイングはサポートされません。						
ギガビット イーサネット ポートがディセーブルな場合	8q4t	WRR	1p7q4t	DWRR または SRR			
	• DSCP ベースのキューイングをサポートします。						

表 64-2　40 ギガビット イーサネット モジュール

モジュール	入力キューおよびドロップしきい値	入力キュースケジューラ	出力キューおよびドロップしきい値	出力キュースケジューラ	合計バッファサイズ	入力バッファサイズ	出力バッファサイズ
WS-X6904-40G-2TXL、WS-X6904-40G-2T（DSCP ベースのキューイングをサポート。出力キュー シェーピングをサポート）	1p7q4t または 2p6q4t	DWRR	1p7q4t または 2p6q4t	DWRR	Catalyst 6900 シリーズのデータ シートを参照してください。		
	（注）　WS-X6904-40G-2T ポートで、**bandwidth** コマンドは、ポートの他のキューイング コマンドにデフォルト以外の値を設定する場合、設定する必要があります。（CSCtz05347）						

表 64-3　10 ギガビット イーサネット モジュール

モジュール	入力キューおよびドロップしきい値	入力キュースケジューラ	出力キューおよびドロップしきい値	出力キュースケジューラ	合計バッファサイズ	入力バッファ サイズ	出力バッファサイズ
WS-X6908-10GE（DSCP ベースのキューイングをサポート）	8q4t	DWRR	1p7q4t	DWRR SRR	200 MB	108 MB	90 MB
WS-X6816-10T-2T、WS-X6716-10T、WS-X6816-10G-2T、WS-X6716-10GE（DSCP ベースのキューイングをサポート）							
パフォーマンス モード	8q4t	DWRR	1p7q4t	DWRR SRR	198 MB	108 MB/ポート	90 MB/ポート
オーバーサブスクリプション モード	1p7q2t	DWRR	1p7q4t	DWRR SRR	91 MB	90 MB/ポート	1 MB/ポート グループ
WS-X6704-10GE	8q8t	WRR	1p7q8t	DWRR	16 MB	2 MB	14 MB

表 64-4　ギガビットおよび 10/100/1000 イーサネット モジュール

モジュール	入力キューおよびドロップしきい値	入力キュースケジューラ	出力キューおよびドロップしきい値	出力キュースケジューラ	Total Buffer Size	入力バッファ サイズ	出力バッファ サイズ
WS-X6848-TX-2T、WS-X6748-GE-TX、WS-X6848-SFP-2T、WS-X6748-SFP、WS-X6824-SFP-2T、WS-X6724-SFP							
	2q8t	WRR	1p3q8t	DWRR	1.3 MB	166 KB	1.2 MB

キューイング ポリシー

キューイング ポリシーでは、**match** コマンドによるクラス マップ（表 64-5 を参照）と、スケジューリング コマンドと輻輳管理コマンドによるポリシー マップ（表 64-6 を参照）を使用します。

表 64-5　キューイング ポリシーのクラス マップの match コマンドと一致基準

match コマンド	一致基準
match cos *cos_list*	CoS 値。
match dscp *dscp_list*	DSCP 値。
match precedence *precedence_list*	優先順位値。

（注）

- ポートに対応付けられているキューイング ポリシーで使用されるクラス マップに **match dscp** コマンドまたは **match precedence** コマンドでは、そのポートのポリシーの方向（入力または出力）に DSCP ベースのキューイングを設定します。
- CoS ベースのキューイングは、非 IP トラフィック、IP マルチキャスト トラフィック、および IP の未知のユニキャスト フラッディング トラフィックに、常に使用されます。
- キューイング ポリシーで使用されるクラス マップでは、**match dscp** コマンドと **match cos** コマンドの両方を含むことができます。

表 64-6　キューイング ポリシーマップ クラス コマンド

キューイング コマンド	説明
`bandwidth [remaining] percent percentage`	非プライオリティ キュー間の帯域幅を割り当てます。**remaining** キーワードは、プライオリティ キューを持つポートで必要です。
`shape average percent percentage`	WS-X6904-40G-2T ポートでは、出力プライオリティ キューにシェーピングを設定します。 他のポートの SRR をイネーブルにします。これは、非プライオリティ出力キュー間に制限付き帯域幅を割り当てます（「モジュールとキュー タイプのマッピング」（P.64-7）の「SRR」を参照）。
`priority`	プライオリティ キューにポリシーマップ クラスを適用します。
`priority level {1|2} [percent percentage]`	（複数のプライオリティ キューまたはシェーピングを設定する場合に必要です）。WS-X6904-40G-2T ポートで、プライオリティ キューの 1 つにポリシーマップ クラスを適用します。プライオリティ キュー 1 は、プライオリティ キュー 2 よりもプライオリティが高くなります。 オプションの **percent** *percentage* キーワードおよび引数は、出力プライオリティ キューにシェーピングを設定します。
`queue-buffers ratio weight`	キュー サイズを設定します。
`queue-limit multiple-type-based`	テールドロップしきい値に CoS、優先順位、および DSCP 値を適用できるようにします。
`queue-limit cos cos_value percent percent_of_qsize`	単一の CoS 値をテール ドロップしきい値に適用し、しきい値パーセンテージを設定します。
`queue-limit dscp dscp_value percent percent_of_qsize`	単一の DSCP 値をテール ドロップしきい値に適用し、しきい値パーセンテージを設定します。
`queue-limit precedence precedence_value percent percent_of_qsize`	単一の優先順位値をテール ドロップしきい値に適用し、しきい値パーセンテージを設定します。
`queue-limit cos values cos_list percent percent_of_qsize`	複数の CoS 値をテール ドロップしきい値に適用し、しきい値パーセンテージを設定します。
`queue-limit dscp values dscp_list percent percent_of_qsize`	複数の DSCP 値をテール ドロップしきい値に適用し、しきい値パーセンテージを設定します。
`queue-limit precedence values precedence_list percent percent_of_qsize`	複数の優先順位値をテール ドロップしきい値に適用し、しきい値パーセンテージを設定します。

表 64-6　キューイング ポリシーマップ クラス コマンド （続き）

キューイング コマンド	説明
`random-detect cos-based [aggregate]`	WRED ドロップしきい値に CoS 値を適用できるようにします。**aggregate** キーワードを指定すると **values** キーワードを使用できるようになります。
`random-detect dscp-based [aggregate]`	WRED ドロップしきい値に DSCP 値を適用できるようにします。**aggregate** キーワードを指定すると **values** キーワードを使用できるようになります。
`random-detect precedence-based [aggregate]`	WRED ドロップしきい値に優先順位値を適用できるようにします。**aggregate** キーワードを指定すると **values** キーワードを使用できるようになります。
`random-detect multiple-type-based [aggregate]`	WRED ドロップしきい値に CoS、優先順位、および DSCP 値を適用できるようにします。**aggregate** キーワードを指定すると **values** キーワードを使用できるようになります。
`random-detect cos` *cos_value* `percent` *min_percent max_percent*	単一の CoS 値を WRED ドロップしきい値に適用し、しきい値パーセンテージを設定します。
`random-detect dscp` *dscp_value* `percent` *min_percent max_percent*	単一の DSCP 値を WRED ドロップしきい値に適用し、しきい値パーセンテージを設定します。
`random-detect precedence` *precedence_value* `percent` *min_percent max_percent*	単一の DSCP 値を WRED ドロップしきい値に適用し、しきい値パーセンテージを設定します。
`random-detect cos values` *cos_list* `percent` *min_percent max_percent*	複数の CoS 値を WRED ドロップしきい値に適用し、しきい値パーセンテージを設定します。**aggregate** キーワードが必要です。
`random-detect dscp values` *dscp_list* `percent` *min_percent max_percent*	複数の DSCP 値を WRED ドロップしきい値に適用し、しきい値パーセンテージを設定します。**aggregate** キーワードが必要です。
`random-detect precedence values` *precedence_list* `percent` *min_percent max_percent*	複数の優先順位値を WRED ドロップしきい値に適用し、しきい値パーセンテージを設定します。

ポリシー ベース キューイングの設定方法

- 「キューイング ポリシーのクラス マップの設定」（P.64-12）
- 「キューイング ポリシーのクラス マップの確認」（P.64-12）
- 「キューイング ポリシー マップの設定」（P.64-12）
- 「キューイング ポリシー マップの確認」（P.64-18）
- 「インターフェイスへのキューイング ポリシー マップの付加」（P.64-18）

（注）　各キュー タイプでサポートされていキューイング コマンドの詳細については、「ポリシー ベース キューイングの設定例」（P.64-19）を参照してください。

キューイング ポリシーのクラス マップの設定

キューイング ポリシーのクラス 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	`Router(config)# class-map type lan-queuing match-any class_name`	クラス マップを作成します。設定している各キュー タイプのしきい値に対するクラス マップを作成します。クラス マップには、これを設定するキュー タイプおよびしきい値と簡単に関連付けることのできる名前を付けます。
ステップ 2	`Router (config-cmap)# match cos cos_value1 [cos_value2 ... [cos_valueN]]`	（任意）CoS 値に基づいてフィルタリングするために、キューイング ポリシーのクラス マップを設定します。複数のコマンドを入力できます。
ステップ 3	`Router (config-cmap)# match dscp dscp_value1 [dscp_value2 ... [dscp_valueN]]`	（任意）DSCP 値に基づいてフィルタリングするためにキューイング ポリシー クラス マップを設定し、このキューイング ポリシーを対応付ける方向での DSCP ベースのキューイングをポートで可能にします。複数のコマンドを入力できます。
ステップ 4	`Router (config-cmap)# match precedence precedence_value1 [precedence_value2 ... [precedence_valueN]]`	（任意）優先順位値に基づいてフィルタリングするためにキューイング ポリシー クラス マップを設定し、このキューイング ポリシーを対応付ける方向での DSCP ベースのキューイングをポートで可能にします。複数のコマンドを入力できます。
ステップ 5	`Router (config-cmap)# end`	コンフィギュレーション モードを終了します。

次に、**cos5** という名前のクラス マップを作成し、CoS 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。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# class-map cos5
Router(config-cmap)# match cos 5
Router(config-cmap)# end
```

キューイング ポリシーのクラス マップの確認

キューイング ポリシーのクラス マップを確認するには、次の作業を行います。

コマンド	目的
`Router# show class-map class_name`	設定を確認します。

キューイング ポリシー マップの設定

- 「WS-X6904-40G-2T ポートでのポリシー ベース キューイングの設定」（P.64-13）
- 「キューイング ポリシーの作成」（P.64-14）
- 「プライオリティ キューの設定」（P.64-15）

- 「非プライオリティ キューの設定」（P.64-15）
- 「しきい値の設定」（P.64-16）

（注）
- 1 つのインターフェイスには、入力キューイング ポリシー マップと出力キューイング ポリシー マップを 1 つずつ対応付けられます。
- キューイング ポリシー マップは、キューごとに 1 個のポリシーマップ クラスを含みます。
- 各ポリシーマップ クラスは、単一のキューを設定します。

WS-X6904-40G-2T ポートでのポリシー ベース キューイングの設定

- 「WS-X6904-40G-2T 非プライオリティ出力キュー シェーピングの設定（class-default を除く）」（P.64-13）
- 「WS-X6904-40G-2T の複数プライオリティ キューまたは出力プライオリティ キューのシェーピングの設定」（P.64-14）
- 「WS-X6904-40G-2T Class-Default の出力シェーピングの設定」（P.64-14）

（注）シェーピングを行わない、WS-X6904-40G-2T に非プライオリティの入力キューおよび単一プライオリティのキュー（入力または出力）を設定するには、次のセクションの手順を使用してください。

- 「キューイング ポリシーの作成」（P.64-14）
- 「プライオリティ キューの設定」（P.64-15）
- 「非プライオリティ キューの設定」（P.64-15）

しきい値を設定します。「しきい値の設定」（P.64-16）を参照してください。

WS-X6904-40G-2T 非プライオリティ出力キュー シェーピングの設定（class-default を除く）

入力した最初の **class** *class_map_name* コマンドは、最大番号の非プライオリティ キューを設定します。後続の **class** *class_map_name* コマンドは、逆の番号（キュー #2 に次ぐ最大番号）順に残りの非プライオリティ キューを設定します。非プライオリティ出力キューのシェーピ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	`Router(config)# policy-map type lan-queuing child_policy_name`	非プライオリティ キューの子ポリシー マップを作成します。
ステップ 2	`Router(config-pmap)# class class_map_name`	1 より大きい番号を持つ非プライオリティ出力キューのポリシー マップ クラスを作成します。
ステップ 3	`Router(config-pmap-c)# bandwidth remaining percent percentage`	DWRR の帯域幅を割り当てます。
ステップ 4	`Router(config-pmap-c)# shape average percent percentage`	シェーピングを設定します。
ステップ 5	`Router(config-pmap-c)# queue-buffers ratio weight`	（任意）キューのバッファ サイズを設定します。
ステップ 6	`Router(config-pmap-c)# end`	（任意）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。

WS-X6904-40G-2T の複数プライオリティ キューまたは出力プライオリティ キューのシェーピングの設定

WS-X6904-40G-2T 2p6q4t ポート アーキテクチャ（2 プライオリティ キュー）をイネーブルにするか、出力プライオリティ キューのシェーピ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	`Router(config-pmap)# class class_map_name`	ポリシー マップ クラスを作成します。
ステップ 2	`Router(config-pmap-c)# priority level {1|2} [percent percentage]`	プライオリティ キューの 1 つにクラス マップを適用します。プライオリティ キュー 1 は、プライオリティ キュー 2 よりもプライオリティが高くなります。 オプションで、出力キューにシェーピングを設定します。
ステップ 3	`Router(config-pmap-c)# queue-buffers ratio weight`	（任意）キューのバッファ サイズを設定します。
ステップ 4	`Router(config-pmap-c)# end`	（任意）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。

WS-X6904-40G-2T Class-Default の出力シェーピングの設定

class class-default コマンドはキュー #1 を設定します。class-default 出力シェーピ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	`Router(config)# policy-map type lan-queuing parent_policy_name`	ポートの親ポリシー マップを作成します。
ステップ 2	`Router(config-pmap)# class class-default`	class-default ポリシー マップ クラスを設定します。
ステップ 3	`Router(config-pmap-c)# bandwidth remaining percent percentage`	DWRR の帯域幅を割り当てます。
ステップ 4	`Router(config-pmap-c)# shape average percent percentage`	シェーピングを設定します。
ステップ 5	`Router(config-pmap-c)# queue-buffers ratio weight`	（任意）キューのバッファ サイズを設定します。
ステップ 6	`Router(config-pmap-c)# service-policy child_service_policy`	1 よりも大きい番号の WS-X6904-40G-2T の非プライオリティ出力キューのシェーピングをサポートするために必要です。（class-default ではサポートされません）
ステップ 7	`Router(config-pmap-c)# end`	（任意）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。

キューイング ポリシーの作成

キューイング ポリシーを作成するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# policy-map type lan-queuing policy_name`	ポリシー マップを作成します。
ステップ 2	`Router(config-pmap)# end`	（任意）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。

プライオリティ キューの設定

1p1q4t、1p1q8t、1p7q2t、1p3q8t、1p7q8t、および 1p7q4t ポートにプライオリティ キューがあります。プライオリティ キューを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config-pmap)# class` *class_map_name*	ポリシー マップ クラスを作成します。
ステップ 2	`Router(config-pmap-c)# priority`	プライオリティ キューにクラス マップを適用します。 **（注）**　プライオリティ キューは SRR がイネーブルのときはサポートされません。
ステップ 3	`Router(config-pmap-c)# queue-buffers ratio` *weight*	（任意）キューのバッファ サイズを設定します。
ステップ 4	`Router(config-pmap-c)# end`	（任意）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。

非プライオリティ キューの設定

続けて **priority** キーワードを指定していない、最初に入力した **class** *class_map_name* コマンドは、最大番号の非プライオリティ キューを設定します。後続の **class** *class_map_name* コマンドは、逆の番号（キュー #2 に次ぐ最大番号）順に残りの非プライオリティ キューを設定します。**class class-default** コマンドはキュー #1 を設定します。非プライオリティ キューを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config-pmap)# class {`*class_map_name* `| class-default}`	ポリシー マップ クラスを作成します。 **（注）** • 1 よりも大きい番号を持つ非プライオリティ キューを設定するためにクラス マップ名を入力します。 • キュー #1 を設定するために、`class-default` キーワードを入力します。
ステップ 2	`Router(config-pmap-c)# bandwidth [remaining] percent` *percentage*	WRR または DWRR の帯域幅を割り当てます。 **（注）** • WS-X6904-40G-2T ポートで、**bandwidth** コマンドは、ポートの他のキューイング コマンドにデフォルト以外の値を設定する場合、設定する必要があります。（CSCtz05347） • 1 個のキューを持つポートでは必要ありません。 • **remaining** キーワードは、プライオリティ キューを持つポートで必要です。
ステップ 3	`Router(config-pmap-c)# shape average percent` *percentage*	（出力キューのみ）SRR をイネーブルにします（WS-X6904-40G-2T のポートではサポート対象外）。これは、非プライオリティ出力キュー間に制限付き帯域幅を割り当てます（の「SRR」を参照）。 • 「モジュールとキュー タイプのマッピング」（P.64-7）の「SRR」を参照）。 • SRR を設定すると、プライオリティ キューがディセーブルになります。

	コマンド	目的
ステップ 4	`Router(config-pmap-c)# queue-buffers ratio weight`	（任意）キューのバッファ サイズを設定します。 （注）　1 個のキューを持つポートでは必要ありません。
ステップ 5	`Router(config-pmap-c)# end`	（任意）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。

しきい値の設定

しきい値設定時の注意事項および制約事項

- テール ドロップしきい値を設定するには、**queue-limit** コマンドを入力します。
- テール ドロップまたは WRED ドロップとしての設定をサポートするポートの場合。
  - テール ドロップとしてしきい値を設定するには **queue-limit** コマンドを入力します。
  - WRED ドロップとしてしきい値を設定するには **random-detect** コマンドを入力します。
- 入力した最初の **queue-limit cos**、**queue-limit dscp**、**random-detect cos**、または **random-detect dscp** コマンドは、しきい値 #1 を設定します。
- 異なるしきい値パーセント値を持つ後続コマンドは、残りのしきい値を番号順（しきい値 #2 から最大番号のしきい値の順）に設定します。
- すでに設定したしきい値パーセント値を持つ後続のコマンドは、このパーセント値で示されたしきい値に、追加の QoS 値を適用します。
- DSCP ベースのキューイングが設定されたポートでは、非 IP トラフィック、IP マルチキャスト トラフィック、および IP の未知のユニキャスト フラッディング トラフィックに CoS ベースのキューイングを使用します。DSCP ベースのキューイングを設定するキューイング ポリシーで、非 IP トラフィック、IP マルチキャスト トラフィック、および IP の未知のユニキャスト フラッディング トラフィックに固有の QoS を提供するために CoS ベースのキューイングを設定します。

CoS ベースのキューイングを使用するテール ドロップとしてしきい値を設定

CoS ベースのキューイングを使用するテール ドロップとして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	`Router(config-pmap-c)# queue-limit cos {one_value | values value_list} percent percentage`	CoS をテール ドロップしきい値に適用し、しきい値パーセンテージを設定します。
ステップ 2	`Router(config-pmap-c)# end`	（任意）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。

CoS ベースのキューイングを使用する WRED ドロップとしてしきい値を設定

CoS ベースのキューイングを使用する WRED ドロップとして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	`Router(config-pmap-c)# random-detect cos-based [aggregate]`	WRED ドロップしきい値に CoS 値を適用できるようにします。**values** キーワードを使用して複数の CoS 値をしきい値に設定するには、**aggregate** キーワードを入力します。
ステップ 2	`Router(config-pmap-c)# random-detect cos {one_value | values value_list} percent min_% max_%`	CoS を WRED ドロップしきい値に適用し、しきい値パーセンテージを設定します。
ステップ 3	`Router(config-pmap-c)# end`	（任意）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。

DSCP ベースのキューイングを使用するテール ドロップとしてしきい値を設定

DSCP ベースのキューイングを使用するテール ドロップとして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	`Router(config-pmap-c)# queue-limit multiple-type-based`	（任意）テールドロップしきい値に CoS、DSCP、または優先順位値を適用できるようにします。
ステップ 2	`Router(config-pmap-c)# queue-limit {cos | dscp | precedence} {one_value | values value_list} percent percentage`	複数の QoS 値を単一のテール ドロップしきい値に適用し、しきい値パーセンテージを設定します。
ステップ 3	`Router(config-pmap-c)# end`	（任意）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。

DSCP ベースのキューイングを使用する WRED ドロップとしてしきい値を設定

DSCP ベースのキューイングを使用する WRED ドロップとして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	`Router(config-pmap-c)# random-detect {dscp-based | precedence-based | multiple-type-based} [aggregate]`	WRED ドロップしきい値に QoS 値を適用できるようにします。 （注） • WRED ドロップしきい値に DSCP 値を適用できるようにするには **dscp-based** キーワードを入力します。 • WRED ドロップしきい値に優先順位値を適用できるようにするには **precedence-based** キーワードを入力します。 • WRED ドロップしきい値に CoS、DSCP の両方または優先順位値を適用できるようにするには **multiple-type-based** キーワードを入力します。 • **values** キーワードを使用して複数の QoS 値をしきい値に設定するには、**aggregate** キーワードを入力します。
ステップ 2	`Router(config-pmap-c)# random-detect {cos | dscp | precedence} {one_value | values value_list} percent min_% max_%`	複数の QoS 値を単一の WRED ドロップしきい値に適用し、しきい値パーセンテージを設定します。
ステップ 3	`Router(config-pmap-c)# end`	（任意）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。

キューイング ポリシー マップの確認

設定を確認するには、**show policy-map** *policy_name* を使用します。

インターフェイスへのキューイング ポリシー マップの付加

キューイング ポリシーをインターフェイスに対応付けるには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface type 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	`Router(config-if)# service-policy type lan-queuing [input | output] policy_map_name`	キューイング ポリシーをインターフェイスに対応付けます。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。

設定を確認するには、**show policy-map interface** コマンドを使用します。

ポリシー ベース キューイングの設定例

キューイング ポリシーの設定例

コメントなし：

```
policy-map type lan-queuing p1
  class cos5
    priority
  class cos123
    bandwidth remaining percent 25
    queue-limit cos 2 percent 20
    queue-limit cos 3 percent 30
  class class-default
    queue-limit cos 6 percent 60
```

コメントあり：

```
policy-map type lan-queuing p1 ! For 1p3q8t
  class cos5 ! Configured to filter CoS 5
!The filtering configured in the class map selects the values that go to the queue
!
    priority ! Applies the class map to the priority queue (#4)
!
!
!First non-priority class applies to highest-numbered non-priority queue (#3)
  class cos123 ! Configured to filter CoS 1, 2, and 3
!The filtering configured in the class map selects the values that go to the queue
!
!
!'remaining' keyword required on ports that have a priority queue
    bandwidth remaining percent 25
!
!
!First queue-limit command assigns CoS 2 to threshold #1 and configures it at 20%
    queue-limit cos 2 percent 20
!Any other queue-limit command with the same percentage
!applies additional configuration to this threshold
!
!Next queue-limit command with different percentage value configures the next threshold
!Assigns CoS 3 to threshold #2 and configures it at 30%
    queue-limit cos 3 percent 30
!Any other queue-limit command with the same percentage
!applies additional configuration to this threshold
!
!Thresholds 3-8 are unconfigured
!All unconfigured thresholds are at 100%
!No explicit configuration provided for CoS 1: defaults to last threshold
!
!End of queue 3 configuration
!
!Queue 2 is unconfigured
!
  class class-default ! applies to queue #1
!'class-default' gets all remaining CoS values:
```

```
!0, 4, 6, and 7
!
!
!Threshold 1 is explicitly configured:
    queue-limit cos 6 percent 50
!
!Remaining thresholds (2-8) are not configured by the queueing policy
!and cannot be configured by anything else
!No explicit configuration provided for CoS 0, 4, and 7:
!CoS values not explicitly configured default to the last threshold
```

各キュー タイプでサポートされているキューイング ポリシー コマンド

1q2t、1q8t 入力キューでサポートされるコマンド

（注）
- テールドロップしきい値と CoS ベース キューイングの組み合わせをサポートしています。
- サポート対象外のコマンドは、コメントとしてこのセクションに含まれています。

```
policy-map type lan-queuing policy_map_name ! For 1q2t, 1q8t
```

- 非プライオリティ キュー 1 ポリシー コマンド：

```
class class-default ! Receives all CoS values.
    ! bandwidth percent percentage ! WRR or DWRR bandwidth allocation.
    !queue-buffers ratio weight !Queue buffer size.
```

- 非プライオリティ キューのしきい値の設定（連続するしきい値を設定する場合は繰り返す）：

```
    ! queue-limit multiple-type-based
    ! Enables application of CoS, precedence, and DSCP values
    ! to a tail-drop threshold.

    queue-limit cos {one_value | values value_list} percent percentage

    ! queue-limit dscp {one_value | values value_list} percent percentage
    ! Applies one DSCP value to a tail-drop threshold
    ! and configures the threshold percentage

    ! random-detect cos-based [aggregate]
    ! Enables application of CoS values to a WRED-drop threshold.
    ! The 'aggregate' keyword allows use of the 'values' keyword

    ! random-detect dscp-based [aggregate]
    ! Enables application of DSCP values to a WRED-drop threshold.
    ! The 'aggregate' keyword allows use of the 'values' keyword

    ! random-detect precedence-based [aggregate]
    ! Enables application of precedence values to a WRED-drop threshold.
    ! The 'aggregate' keyword allows use of the 'values' keyword

    ! random-detect multiple-type-based [aggregate]
    ! Enables application of CoS, precedence, and DSCP values
    ! to a WRED-drop threshold.
    ! The 'aggregate' keyword allows use of the 'values' keyword

    ! random-detect cos {one_value | values value_list} percent min_% max_%
    ! Applies CoS to a WRED-drop threshold and configures the threshold percentages.

    ! random-detect dscp {one_value | values value_list} percent min_% max_%
    ! Applies DSCP to a WRED-drop threshold and configures the threshold percentages.

    ! random-detect {precedence one_value | values precedence value_list} percent min_% max_%
    ! Applies DSCP to a WRED-drop threshold and configures the threshold percentages.
```

2q8t 入力キューでサポートされるコマンド

（注）
- テールドロップしきい値と CoS ベース キューイングの組み合わせをサポートしています。
- サポート対象外のコマンドは、コメントとしてこのセクションに含まれています。

```
policy-map type lan-queuing policy_map_name ! For 2q8t, 8q8t
```

- 1 よりも大きい番号が付いた非プライオリティ キューに対するクラス コマンド：逆の番号順でキューを設定します。次のキューを設定するには繰り返します。

  ```
  class class_map_name ! Receives CoS values filtered by class_map_name.
  ```

- キュー #1 のクラス コマンド：

  ```
  class class-default ! Receives all remaining CoS values.
  ```

- 非プライオリティ キュー コンフィギュレーション コマンド：

  ```
  bandwidth percent percentage ! WRR or DWRR bandwidth allocation.

  queue-buffers ratio weight !Queue buffer size.
  ```

- 非プライオリティ キューのしきい値の設定：各キューで、連続するしきい値を設定するには繰り返します。

  ```
  ! queue-limit multiple-type-based
  ! Enables application of CoS, precedence, and DSCP values to a tail-drop threshold.

  queue-limit cos {one_value | values value_list} percent percentage
  ! Applies CoS to a tail-drop threshold and configures the threshold percentage

  ! queue-limit dscp {one_value | values value_list} percent percentage
  ! Applies one DSCP value to a tail-drop threshold
  ! and configures the threshold percentage

  ! random-detect cos-based [aggregate]
  ! Enables application of CoS values to a WRED-drop threshold.
  ! The 'aggregate' keyword allows use of the 'values' keyword

  ! random-detect dscp-based [aggregate]
  ! Enables application of DSCP values to a WRED-drop threshold.
  ! The 'aggregate' keyword allows use of the 'values' keyword

  ! random-detect precedence-based [aggregate]
  ! Enables application of precedence values to a WRED-drop threshold.

  ! random-detect multiple-type-based [aggregate]
  ! Enables application of CoS, precedence, and DSCP values
  ! to a WRED-drop threshold.
  ! The 'aggregate' keyword allows use of the 'values' keyword

  ! random-detect cos {one_value | values value_list} percent min_% max_%
  ! Applies CoS to a WRED-drop threshold and configures the threshold percentages.

  ! random-detect dscp {one_value | values value_list} percent min_% max_%
  ! Applies DSCP to a WRED-drop threshold and configures the threshold percentages.

  ! random-detect {precedence one_value | values precedence value_list} percent min_% max_%
  ! Applies DSCP to a WRED-drop threshold and configures the threshold percentages.
  ```

8q4t 入力キューでサポートされるコマンド

（注）
- CoS ベース、DSCP ベース、および優先順位ベースのキューイングと、テール ドロップと WRED ドロップのしきい値の組み合わせをサポートしています。
- サポート対象外のコマンドは、コメントとしてこのセクションに含まれています。

```
policy-map type lan-queuing policy_map_name ! For 8q4t
```

- 1 よりも大きい番号が付いた非プライオリティ キューに対するクラス コマンド：逆の番号順でキューを設定します。次のキューを設定するには繰り返します。

```
class class_map_name
! Receives QoS values (CoS, DSCP, precedence) values filtered by class_map_name.
```

- キュー #1 のクラス コマンド：

```
class class-default ! Receives all remaining QoS values (CoS, DSCP, precedence).
```

- 非プライオリティ キュー コンフィギュレーション コマンド：

```
bandwidth percent percentage ! WRR or DWRR bandwidth allocation.

queue-buffers ratio weight !Queue buffer size.
```

- 非プライオリティ キューのしきい値の設定：各キューで、連続するしきい値を設定するには繰り返します。

```
queue-limit multiple-type-based
! Enables application of CoS, precedence, and DSCP values to a tail-drop threshold.

queue-limit cos {one_value | values value_list} percent percentage
! Applies CoS to a tail-drop threshold and configures the threshold percentage

queue-limit dscp {one_value | values value_list} percent percentage
! Applies one DSCP value to a tail-drop threshold
! and configures the threshold percentage

random-detect cos-based [aggregate]
! Enables application of CoS values to a WRED-drop threshold.
! The 'aggregate' keyword allows use of the 'values' keyword

random-detect dscp-based [aggregate]
! Enables application of DSCP values to a WRED-drop threshold.
! The 'aggregate' keyword allows use of the 'values' keyword

random-detect precedence-based [aggregate]
! Enables application of precedence values to a WRED-drop threshold.
! The 'aggregate' keyword allows use of the 'values' keyword

random-detect multiple-type-based [aggregate]
! Enables application of CoS, precedence, and DSCP values to a WRED-drop threshold.
! The 'aggregate' keyword allows use of the 'values' keyword

random-detect cos {one_value | values value_list} percent min_% max_%
! Applies CoS to a WRED-drop threshold and configures the threshold percentages.

random-detect dscp {one_value | values value_list} percent min_% max_%
! Applies DSCP to a WRED-drop threshold and configures the threshold percentages.

random-detect {precedence one_value | values precedence value_list} percent min_% max_%
! Applies DSCP to a WRED-drop threshold and configures the threshold percentages.
```

8q8t 入力キューでサポートされるコマンド

（注）
- CoS ベース キューイングとテールドロップまたは WRED ドロップのしきい値の組み合わせをサポートしています。
- サポート対象外のコマンドは、コメントとしてこのセクションに含まれています。

```
policy-map type lan-queuing policy_map_name ! For 1p1q8t
```

- プライオリティ キュー：

```
class class_map_name ! Receives CoS values filtered by class_map_name.
    priority ! Applies the class map to the priority queue
```

- 非プライオリティ キュー ポリシー コマンド：

```
class class-default ! Receives all remaining CoS values.
    ! bandwidth remaining percent percentage ! WRR or DWRR bandwidth allocation.
    !queue-buffers ratio weight !Queue buffer size.
```

- 非プライオリティ キューのしきい値の設定：連続するしきい値を設定するには繰り返します。

```
    ! queue-limit multiple-type-based
    ! Enables application of CoS, precedence, and DSCP values to a tail-drop threshold.
    !
    queue-limit cos {one_value | values value_list} percent percentage
    ! Applies CoS to a tail-drop threshold and configures the threshold percentage
    !
    ! queue-limit dscp {one_value | values value_list} percent percentage
    ! Applies one DSCP value to a tail-drop threshold
    ! and configures the threshold percentage
    !
    random-detect cos-based [aggregate]
    ! Enables application of CoS values to a WRED-drop threshold.
    ! The 'aggregate' keyword allows use of the 'values' keyword
    !
    ! random-detect dscp-based [aggregate]
    ! Enables application of DSCP values to a WRED-drop threshold.
    ! The 'aggregate' keyword allows use of the 'values' keyword
    !
    ! random-detect precedence-based [aggregate]
    ! Enables application of precedence values to a WRED-drop threshold.
    ! The 'aggregate' keyword allows use of the 'values' keyword
    !
    ! random-detect multiple-type-based [aggregate]
    ! Enables application of CoS, precedence, and DSCP values
    ! to a WRED-drop threshold.
    ! The 'aggregate' keyword allows use of the 'values' keyword
    !
    random-detect cos {one_value | values value_list} percent min_% max_%
    ! Applies CoS to a WRED-drop threshold and configures the threshold percentages.
    !
    ! random-detect dscp {one_value | values value_list} percent min_% max_%
    ! Applies DSCP to a WRED-drop threshold and configures the threshold percentages.
    !
    ! random-detect {precedence one_value | values precedence value_list} percent min_% max_%
    ! Applies DSCP to a WRED-drop threshold and configures the threshold percentages.
```

1p1q4t 入力キューでサポートされるコマンド

（注）
- テールドロップしきい値と CoS ベース キューイングの組み合わせをサポートしています。
- サポート対象外のコマンドは、コメントとしてこのセクションに含まれています。

```
policy-map type lan-queuing policy_map_name ! For 1p1q4t
```

- プライオリティ キュー：

```
class class_map_name ! Receives CoS values filtered by class_map_name.
   priority ! Applies the class map to the priority queue
```

- 非プライオリティ キュー ポリシー コマンド：

```
class class-default ! Receives all remaining CoS values.
    ! bandwidth remaining percent percentage ! WRR or DWRR bandwidth allocation.
    !queue-buffers ratio weight !Queue buffer size.
```

- 非プライオリティ キューのしきい値の設定：連続するしきい値を設定するには繰り返します。

```
    ! queue-limit multiple-type-based
    ! Enables application of CoS, precedence, and DSCP values
    ! to a tail-drop threshold.
    !
    queue-limit cos {one_value | values value_list} percent percentage
    ! Applies CoS to a tail-drop threshold and configures the threshold percentage
    !
    ! queue-limit dscp {one_value | values value_list} percent percentage
    ! Applies one DSCP value to a tail-drop threshold
    ! and configures the threshold percentage
    !
    ! random-detect cos-based [aggregate]
    ! Enables application of CoS values to a WRED-drop threshold.
    ! The 'aggregate' keyword allows use of the 'values' keyword
    !
    ! random-detect dscp-based [aggregate]
    ! Enables application of DSCP values to a WRED-drop threshold.
    ! The 'aggregate' keyword allows use of the 'values' keyword
    !
    ! random-detect precedence-based [aggregate]
    ! Enables application of precedence values to a WRED-drop threshold.
    ! The 'aggregate' keyword allows use of the 'values' keyword
    !
    ! random-detect multiple-type-based [aggregate]
    ! Enables application of CoS, precedence, and DSCP values
    ! to a WRED-drop threshold.
    ! The 'aggregate' keyword allows use of the 'values' keyword
    !
    ! random-detect cos {one_value | values value_list} percent min_% max_%
    ! Applies CoS to a WRED-drop threshold and configures the threshold percentages.
    !
    ! random-detect dscp {one_value | values value_list} percent min_% max_%
    ! Applies DSCP to a WRED-drop threshold and configures the threshold percentages.
    !
    ! random-detect {precedence one_value | values precedence value_list} percent min_% max_%
    ! Applies DSCP to a WRED-drop threshold and configures the threshold percentages.
```

1p1q8t 入力キューでサポートされるコマンド

（注）
- CoS ベース キューイングとテールドロップまたは WRED ドロップのしきい値の組み合わせをサポートしています。
- サポート対象外のコマンドは、コメントとしてこのセクションに含まれています。

```
policy-map type lan-queuing policy_map_name ! For 1p1q8t
```

- プライオリティ キュー：

```
class class_map_name ! Receives CoS values filtered by class_map_name.
    priority ! Applies the class map to the priority queue
```

- 非プライオリティ キュー ポリシー コマンド：

```
class class-default ! Receives all remaining CoS values.
    ! bandwidth remaining percent percentage ! WRR or DWRR bandwidth allocation.
    !queue-buffers ratio weight !Queue buffer size.
```

- 非プライオリティ キューのしきい値の設定：連続するしきい値を設定するには繰り返します。

```
    ! queue-limit multiple-type-based
    ! Enables application of CoS, precedence, and DSCP values to a tail-drop threshold.
    !
    queue-limit cos {one_value | values value_list} percent percentage
    ! Applies CoS to a tail-drop threshold and configures the threshold percentage
    !
    ! queue-limit dscp {one_value | values value_list} percent percentage
    ! Applies one DSCP value to a tail-drop threshold
    ! and configures the threshold percentage
    !
    random-detect cos-based [aggregate]
    ! Enables application of CoS values to a WRED-drop threshold.
    ! The 'aggregate' keyword allows use of the 'values' keyword
    !
    ! random-detect dscp-based [aggregate]
    ! Enables application of DSCP values to a WRED-drop threshold.
    ! The 'aggregate' keyword allows use of the 'values' keyword
    !
    ! random-detect precedence-based [aggregate]
    ! Enables application of precedence values to a WRED-drop threshold.
    ! The 'aggregate' keyword allows use of the 'values' keyword
    !
    ! random-detect multiple-type-based [aggregate]
    ! Enables application of CoS, precedence, and DSCP values
    ! to a WRED-drop threshold.
    !
    random-detect cos {one_value | values value_list} percent min_% max_%
    ! Applies CoS to a WRED-drop threshold and configures the threshold percentages.
    !
    ! random-detect dscp {one_value | values value_list} percent min_% max_%
    ! Applies DSCP to a WRED-drop threshold and configures the threshold percentages.
    !
    ! random-detect {precedence one_value | values precedence value_list} percent min_% max_%
    ! Applies DSCP to a WRED-drop threshold and configures the threshold percentages.
```

1p7q2t 入力キューでサポートされるコマンド

（注）
- CoS ベース、DSCP ベース、および優先順位ベースのキューイングと、テール ドロップと WRED ドロップのしきい値の組み合わせをサポートしています。
- サポート対象外のコマンドは、コメントとしてこのセクションに含まれています。

```
policy-map type lan-queuing policy_map_name ! For 1p7q2t
```

- プライオリティ キュー：

```
class class_map_name
! Receives QoS values (CoS, DSCP, precedence) values filtered by class_map_name.
   priority ! Applies the class map to the priority queue
```

- 1 よりも大きい番号が付いた非プライオリティ キューに対するクラス コマンド：逆の番号順でキューを設定します。次のキューを設定するには繰り返します。

```
class class_map_name
! Receives QoS values (CoS, DSCP, precedence) values filtered by class_map_name.
```

- キュー #1 のクラス コマンド：

```
class class-default ! Receives all remaining QoS values (CoS, DSCP, precedence).
```

- 非プライオリティ キュー コンフィギュレーション コマンド：

```
bandwidth percent percentage ! WRR or DWRR bandwidth allocation.
!
queue-buffers ratio weight !Queue buffer size.
```

- 非プライオリティ キューのしきい値の設定：各キューで、連続するしきい値を設定するには繰り返します。

```
queue-limit multiple-type-based
! Enables application of CoS, precedence, and DSCP values to a tail-drop threshold.
!
queue-limit cos {one_value | values value_list} percent percentage
! Applies CoS to a tail-drop threshold and configures the threshold percentage
!
queue-limit dscp {one_value | values value_list} percent percentage
! Applies one DSCP value to a tail-drop threshold
! and configures the threshold percentage
!
random-detect cos-based [aggregate]
! Enables application of CoS values to a WRED-drop threshold.
! The 'aggregate' keyword allows use of the 'values' keyword
!
random-detect dscp-based [aggregate]
! Enables application of DSCP values to a WRED-drop threshold.
! The 'aggregate' keyword allows use of the 'values' keyword
!
random-detect precedence-based [aggregate]
! Enables application of precedence values to a WRED-drop threshold.
! The 'aggregate' keyword allows use of the 'values' keyword
!
random-detect multiple-type-based [aggregate]
! Enables application of CoS, precedence, and DSCP values to a WRED-drop threshold.
! The 'aggregate' keyword allows use of the 'values' keyword
!
random-detect cos {one_value | values value_list} percent min_% max_%
```

```
! Applies CoS to a WRED-drop threshold and configures the threshold percentages.
!
random-detect dscp {one_value | values value_list} percent min_% max_%
! Applies DSCP to a WRED-drop threshold and configures the threshold percentages.
!
random-detect {precedence one_value | values precedence value_list} percent min_%
max_%
! Applies DSCP to a WRED-drop threshold and configures the threshold percentages.
```

1p3q8t 出力キューでサポートされるコマンド

（注）
- CoS ベース キューイングとテールドロップおよび WRED ドロップのしきい値の組み合わせをサポートしています。
- サポート対象外のコマンドは、コメントとしてこのセクションに含まれています。

```
policy-map type lan-queuing policy_map_name ! For 1p3q8t
```

- プライオリティ キュー：

```
class class_map_name ! Receives CoS values filtered by class_map_name.
    priority ! Applies the class map to the priority queue
```

- 1 よりも大きい番号が付いた非プライオリティ キューに対するクラス コマンド：逆の番号順でキューを設定します。次のキューを設定するには繰り返します。

```
class class_map_name ! Receives CoS values filtered by class_map_name.
```

- キュー #1 のクラス コマンド：

```
class class-default ! Receives all remaining CoS values.
```

- 非プライオリティ キュー コンフィギュレーション コマンド：

```
bandwidth percent percentage ! WRR or DWRR bandwidth allocation.
!
! shape average percent percentage ! SRR bandwidth allocation.
!
queue-buffers ratio weight !Queue buffer size.
```

- 非プライオリティ キューのしきい値の設定：連続するしきい値を設定するには繰り返します。

```
! queue-limit multiple-type-based
! Enables application of CoS, precedence, and DSCP values to a tail-drop threshold.
!
queue-limit cos {one_value | values value_list} percent percentage
! Applies CoS to a tail-drop threshold and configures the threshold percentage
!
! queue-limit dscp {one_value | values value_list} percent percentage
! Applies one DSCP value to a tail-drop threshold
! and configures the threshold percentage
!
random-detect cos-based [aggregate]
! Enables application of CoS values to a WRED-drop threshold.
! The 'aggregate' keyword allows use of the 'values' keyword
!
! random-detect dscp-based [aggregate]
! Enables application of DSCP values to a WRED-drop threshold.
! The 'aggregate' keyword allows use of the 'values' keyword
!
! random-detect precedence-based [aggregate]
```

```
! Enables application of precedence values to a WRED-drop threshold.
! The 'aggregate' keyword allows use of the 'values' keyword
!
! random-detect multiple-type-based [aggregate]
! Enables application of CoS, precedence, and DSCP values
! to a WRED-drop threshold.
! The 'aggregate' keyword allows use of the 'values' keyword
!
random-detect cos {one_value | values value_list} percent min_% max_%
! Applies CoS to a WRED-drop threshold and configures the threshold percentages.
!
! random-detect dscp {one_value | values value_list} percent min_% max_%
! Applies DSCP to a WRED-drop threshold and configures the threshold percentages.
!
! random-detect {precedence one_value | values precedence value_list}
percent min_% max_%
! Applies DSCP to a WRED-drop threshold and configures the threshold percentages.
```

1p7q8t 出力キューでサポートされるコマンド

（注）
- CoS ベース キューイングとテールドロップおよび WRED ドロップのしきい値の組み合わせをサポートしています。
- サポート対象外のコマンドは、コメントとしてこのセクションに含まれています。

```
policy-map type lan-queuing policy_map_name ! For 1p7q8t
```

- プライオリティ キュー：

```
class class_map_name ! Receives CoS values filtered by class_map_name.
    priority ! Applies the class map to the priority queue
```

- 1 よりも大きい番号が付いた非プライオリティ キューに対するクラス コマンド：逆の番号順でキューを設定します。次のキューを設定するには繰り返します。

```
class class_map_name ! Receives CoS values filtered by class_map_name.
```

- キュー #1 のクラス コマンド：

```
class class-default ! Receives all remaining CoS values.
```

- 非プライオリティ キュー コンフィギュレーション コマンド：

```
bandwidth percent percentage ! WRR or DWRR bandwidth allocation.
!
! shape average percent percentage ! SRR bandwidth allocation.
!
queue-buffers ratio weight !Queue buffer size.
```

- 非プライオリティ キューのしきい値の設定：連続するしきい値を設定するには繰り返します。

```
! queue-limit multiple-type-based
! Enables application of CoS, precedence, and DSCP values to a tail-drop threshold.
!
queue-limit cos {one_value | values value_list} percent percentage
! Applies CoS to a tail-drop threshold and configures the threshold percentage
!
! queue-limit dscp {one_value | values value_list} percent percentage
! Applies one DSCP value to a tail-drop threshold
! and configures the threshold percentage
!
random-detect cos-based [aggregate]
```

```
! Enables application of CoS values to a WRED-drop threshold.
! The 'aggregate' keyword allows use of the 'values' keyword
!
! random-detect dscp-based [aggregate]
! Enables application of DSCP values to a WRED-drop threshold.
! The 'aggregate' keyword allows use of the 'values' keyword
!
! random-detect precedence-based [aggregate]
! Enables application of precedence values to a WRED-drop threshold.
! The 'aggregate' keyword allows use of the 'values' keyword
!
! random-detect multiple-type-based [aggregate]
! Enables application of CoS, precedence, and DSCP values
! to a WRED-drop threshold.
! The 'aggregate' keyword allows use of the 'values' keyword
!
random-detect cos {one_value | values value_list} percent min_% max_%
! Applies CoS to a WRED-drop threshold and configures the threshold percentages.
!
! random-detect dscp {one_value | values value_list} percent min_% max_%
! Applies DSCP to a WRED-drop threshold and configures the threshold percentages.
!
! random-detect {precedence one_value | values precedence value_list}
percent min_% max_%
! Applies DSCP to a WRED-drop threshold and configures the threshold percentages.
```

1p7q4t、2p6q4t 入力または出力キューでサポートされるコマンド

（注）

- CoS ベース、DSCP ベース、および優先順位ベースのキューイングと、テール ドロップと WRED ドロップのしきい値の組み合わせをサポートしています。SRR（WS-X6904-40G-2T を除く）または DWRR デキューイングをサポートしています。
- WS-X6904-40G-2T はシェーピングをサポートしています。「WS-X6904-40G-2T 1p7q4t、2p6q4t 出力キューでサポートされるコマンド」（P.64-32）を参照してください。
- サポート対象外のコマンドは、コメントとしてこのセクションに含まれています。

- 複数プライオリティ キューの WS-X6904-40G-2T を除くプライオリティ キュー：

```
class class_map_name
! Receives QoS values (CoS, DSCP, precedence) values filtered by class_map_name.
    priority ! Applies the class map to the priority queue
    ! Not supported if SRR mode is enabled.
    !
    queue-buffers ratio weight !Queue buffer size.
    !
```

- WS-X6904-40G-2T プライオリティ キュー：

```
class class_map_name
! Receives QoS values (CoS, DSCP, precedence) values filtered by class_map_name.
    priority [level { 1 | 2}]
    ! Applies the class map to one of the priority queues
    !
    queue-buffers ratio weight !Queue buffer size.
    !
```

- 1 よりも大きい番号が付いた非プライオリティ キューに対するクラス コマンド：逆の番号順でキューを設定します。次のキューを設定するには繰り返します。

```
class class_map_name
```

```
! Receives QoS values (CoS, DSCP, precedence) values filtered by class_map_name.
```

- キュー #1 のクラス コマンド：

```
class class-default ! Receives all remaining QoS values (CoS, DSCP, precedence).
```

- 非プライオリティ キュー コンフィギュレーション コマンド：

```
shape average percent percentage
! Enables SRR on nonpriority egress queues.

bandwidth remaining percent percentage
! DWRR bandwidth allocation.
```

（注）　WS-X6904-40G-2T ポートで、**bandwidth** コマンドは、ポートの他のキューイング コマンドにデフォルト以外の値を設定する場合、設定する必要があります。（CSCtz05347）

```
!
queue-buffers ratio weight !Queue buffer size.
!
```

- 非プライオリティ キューのしきい値の設定：各キューで、連続するしきい値を設定するには繰り返します。

```
queue-limit multiple-type-based
! Enables application of CoS, precedence, and DSCP values to a tail-drop threshold.
!
queue-limit cos {one_value | values value_list} percent percentage
! Applies CoS to a tail-drop threshold and configures the threshold percentage
!
queue-limit dscp {one_value | values value_list} percent percentage
! Applies one DSCP value to a tail-drop threshold
! and configures the threshold percentage
!
random-detect cos-based [aggregate]
! Enables application of CoS values to a WRED-drop threshold.
! The 'aggregate' keyword allows use of the 'values' keyword
!
random-detect dscp-based [aggregate]
! Enables application of DSCP values to a WRED-drop threshold.
! The 'aggregate' keyword allows use of the 'values' keyword
!
random-detect precedence-based [aggregate]
! Enables application of precedence values to a WRED-drop threshold.
! The 'aggregate' keyword allows use of the 'values' keyword
! The 'aggregate' keyword allows use of the 'values' keyword
!
random-detect multiple-type-based [aggregate]
! Enables application of CoS, precedence, and DSCP values to a WRED-drop threshold.
! The 'aggregate' keyword allows use of the 'values' keyword
!
random-detect cos {one_value | values value_list} percent min_% max_%
! Applies CoS to a WRED-drop threshold and configures the threshold percentages.
!
random-detect dscp {one_value | values value_list} percent min_% max_%
! Applies DSCP to a WRED-drop threshold and configures the threshold percentages.
!
random-detect {precedence one_value | values precedence value_list} percent min_% max_%
! Applies DSCP to a WRED-drop threshold and configures the threshold percentages.
```

WS-X6904-40G-2T 1p7q4t、2p6q4t 出力キューでサポートされるコマンド

（注）
- CoS ベース、DSCP ベース、および優先順位ベースのキューイングと、テール ドロップと WRED ドロップのしきい値の組み合わせをサポートしています。DWRR デキューイングをサポートしています。
- サポート対象外のコマンドは、コメントとしてこのセクションに含まれています。
- class-default 親ポリシー マップに適用する、非プライオリティ キューの子ポリシー マップとともにシェーピングを設定します。
- シェーピングなしの場合は、1 つのポリシー マップにすべてのポリシーマップ クラス コマンドを設定します。

- （シェーピングの場合）非プライオリティ キューの子ポリシー マップ コマンドには、1 よりも大きい番号が付いています。

```
policy-map type lan-queuing child_policy_name
```

- 1 よりも大きい番号が付いた非プライオリティ キューに対するポリシー マップ クラス コマンド：逆の番号順で非プライオリティ キューを設定します。次のキューを設定するには繰り返します。

```
class class_map_name
! Receives QoS values (CoS, DSCP, precedence) values filtered by class_map_name.
```

- 1 よりも大きい番号の非プライオリティ キューに対するコンフィギュレーション コマンド：

```
shape average percent percentage
! Configures shaping on egress nonpriority queues.

bandwidth remaining percent percentage
! DWRR bandwidth allocation.
```

（注）　WS-X6904-40G-2T ポートで、**bandwidth** コマンドは、ポートの他のキューイング コマンドにデフォルト以外の値を設定する場合、設定する必要があります。（CSCtz05347）

```
!
queue-buffers ratio weight !Queue buffer size.
!
```

- 非プライオリティ キューのしきい値の設定：各キューで、連続するしきい値を設定するには繰り返します。

```
queue-limit multiple-type-based
! Enables application of CoS, precedence, and DSCP values to a tail-drop
threshold.
!
queue-limit cos {one_value | values value_list} percent percentage
! Applies CoS to a tail-drop threshold and configures the threshold percentage
!
queue-limit dscp {one_value | values value_list} percent percentage
! Applies one DSCP value to a tail-drop threshold
! and configures the threshold percentage
!
random-detect cos-based [aggregate]
! Enables application of CoS values to a WRED-drop threshold.
! The 'aggregate' keyword allows use of the 'values' keyword
!
random-detect dscp-based [aggregate]
```

```
    ! Enables application of DSCP values to a WRED-drop threshold.
    ! The 'aggregate' keyword allows use of the 'values' keyword
    !
    random-detect precedence-based [aggregate]
    ! Enables application of precedence values to a WRED-drop threshold.
    ! The 'aggregate' keyword allows use of the 'values' keyword
    ! The 'aggregate' keyword allows use of the 'values' keyword
    !
    random-detect multiple-type-based [aggregate]
    ! Enables application of CoS, precedence, and DSCP values to a WRED-drop
    threshold.
    ! The 'aggregate' keyword allows use of the 'values' keyword
    !
    random-detect cos {one_value | values value_list} percent min_% max_%
    ! Applies CoS to a WRED-drop threshold and configures the threshold percentages.
    !
    random-detect dscp {one_value | values value_list} percent min_% max_%
    ! Applies DSCP to a WRED-drop threshold and configures the threshold percentages.
    !
    random-detect {precedence one_value | values precedence value_list} percent min_%
    max_%
    ! Applies DSCP to a WRED-drop threshold and configures the threshold percentages.
```

- シェーピングを行わない単一のプライオリティ キュー：

```
class class_map_name
! Receives QoS values (CoS, DSCP, precedence) values filtered by class_map_name.
    priority ! Applies the class map to the priority queue
    !
    queue-buffers ratio weight ! Queue buffer size.
    !
```

- シェーピングを行わない複数のプライオリティ キュー：

```
class class_map_name
! Receives QoS values (CoS, DSCP, precedence) values filtered by class_map_name.
    priority level { 1 | 2}
    ! Applies the class map to one of the priority queues
    !
    queue-buffers ratio weight ! Queue buffer size.
    !
```

- シェーピングを行う、出力プライオリティ キュー（単一または複数）：

```
class class_map_name
! Receives QoS values (CoS, DSCP, precedence) values filtered by class_map_name.
    priority level { 1 | 2} percent percentage
    ! Applies the class map to one of the priority queues
    ! Configures shaping on the queue
    !
    queue-buffers ratio weight ! Queue buffer size.
    !
```

- （シェーピングの場合）キュー #1（class-default）の親ポリシー マップ コマンド：

```
policy-map type lan-queuing parent_policy_name
```

- キュー #1（class-default）のクラス コマンド：

```
class class-default ! Receives all remaining QoS values (CoS, DSCP, precedence).

    shape average percent percentage
    ! Configures shaping on egress nonpriority queues.

    bandwidth remaining percent percentage
    ! DWRR bandwidth allocation.
```

（注）　WS-X6904-40G-2T ポートで、**bandwidth** コマンドは、ポートの他のキューイング コマンドにデフォルト以外の値を設定する場合、設定する必要があります。（CSCtz05347）

```
!
queue-buffers ratio weight ! Queue buffer size.
!
service-policy child_service_policy
! If shaping is configured on the other nonpriority queues
```

class-default しきい値を設定するには、「非プライオリティ キューのしきい値の設定」を参照してください。

各キュー タイプのキューイング ポリシー コマンドの設定例

（注）　次の設定例は、**auto qos default** および **platform qos queueing-only** グローバル コンフィギュレーション コマンドによって実現されるデフォルトのキューイングとほぼ同等です。

1q2t 入力キューの設定例

（注）　テールドロップしきい値と CoS ベース キューイングの組み合わせをサポートしています。

```
policy-map type lan-queuing p_map_1q2t
    class class-default ! Receives all CoS values.
        !
        ! Configures threshold #1:
        queue-limit cos values 0 1 3 4 percent 80
        ! Applies CoS values to threshold 1 and configures the threshold percentage
        !
        ! Other thresholds unconfigured; default to 100%
        ! Remaining CoS values are not explicitly configured:
        ! default to threshold 8 at 100%
```

1q8t 入力キューの設定例

（注）　テールドロップしきい値と CoS ベース キューイングの組み合わせをサポートしています。

```
policy-map type lan-queuing p_map_1q8t
    class class-default ! Receives all CoS values.
        !
        ! Configures threshold #1:
        queue-limit cos 0 percent 50
        ! Applies CoS 0 to threshold 1 and configures the threshold percentage
        !
        ! Configures threshold #2:
        queue-limit cos values 1 2 3 4 percent 60
        ! Applies CoS 1, 2, 3, 4 to threshold 2 and configures the threshold percentage
        !
        ! Configures threshold #3:
        queue-limit cos values 6 7 percent 80
        ! Applies CoS 6 and 7 to threshold 3 and configures the threshold percentage
        !
        ! Other thresholds unconfigured; default to 100%
        ! CoS 5 is not explicitly configured: defaults to threshold 8 at 100%
```

2q8t 入力キューの設定例

（注）　テールドロップしきい値と CoS ベース キューイングの組み合わせをサポートしています。

```
class-map type lan-queuing match-any c_map_cos_5
    match cos 5
!
policy-map type lan-queuing p_map_2q8t ! For 2q8t
!
    ! Configures queue #2:
    class c_map_cos_5
    ! Receives QoS values (CoS, DSCP, precedence) values filtered by c_map_cos_5.
    !
        bandwidth percent 10 ! WRR bandwidth allocation.
        queue-buffers ratio 20 !Queue buffer size.
        !
        queue-limit cos 5 percent 100
        ! Applies CoS 5 to threshold 1 and configures the threshold percentage
    !
    ! Configures queue #1:
    class class-default ! Receives all remaining CoS values.
    !
        bandwidth percent 90 ! WRR bandwidth allocation.
        !
        queue-buffers ratio 20 !Queue buffer size.
        !
        ! Configures threshold #1:
        queue-limit cos values 0 1 percent 70
        ! Applies CoS 0 1 to threshold 1 and configures the threshold percentage
        !
        ! Configures threshold #2:
        queue-limit cos values 2 3 percent 80
        ! Applies CoS 2 3 to threshold 2 and configures the threshold percentage
        !
        ! Configures threshold #3:
```

```
        queue-limit cos 4 percent 90
        ! Applies CoS 4 to threshold 3 and configures the threshold percentage
        !
        ! CoS 6 and 7 default to threshold 4 at 100%
```

8q4t 8q8t 入力キューの設定例（CoS ベースのキューイング）

（注）

- CoS ベース、DSCP ベース、および優先順位ベースのキューイングと、テール ドロップと WRED ドロップのしきい値の組み合わせをサポートしています。次の例では、CoS ベースのキューイングを設定します。

```
class-map type lan-queuing match-any c_map_cos_5
    match cos 5
!
policy-map type lan-queuing p_map_8q4t_cos_8q8t ! For 8q4t CoS-based queueing and 8q8t

    ! Configures queue #8:
    class c_map_cos_5 ! Receives CoS values values filtered by c_map_cos_5.
    !
        bandwidth percent 90 ! WRR bandwidth allocation.
        queue-buffers ratio 20 !Queue buffer size.
        !
        ! CoS 5 defaults to threshold 4 at 100%
    !
    ! Configures queue #1:
    class class-default
    ! Receives all remaining CoS values.
    !
        bandwidth percent 10 ! WRR bandwidth allocation.
        queue-buffers ratio 80 !Queue buffer size.
        !
        ! Configures threshold #1:
        random-detect cos-based aggregate
        ! The 'aggregate' keyword allows use of the 'values' keyword
        !
        random-detect cos values 0 1 percent 40 70
        !
        ! Configures threshold #2:
        random-detect cos-based aggregate
        ! The 'aggregate' keyword allows use of the 'values' keyword
        !
        random-detect cos values 2 3 percent 40 80
        !
        ! Configures threshold #3:
        random-detect cos-based
        !
        random-detect cos value 4 percent 50 90
        !
        ! Configures threshold #4:
        random-detect cos-based aggregate
        ! The 'aggregate' keyword allows use of the 'values' keyword
        !
        random-detect cos values 6 7 percent 50 100
```

8q4t 入力キューの設定例（DSCP ベースのキューイング）

（注）
- CoS ベース、DSCP ベース、および優先順位ベースのキューイングと、テール ドロップと WRED ドロップのしきい値の組み合わせをサポートしています。この例では、DSCP ベースのキューイングを設定します。

```
class-map type lan-queuing match-any c_map_cos_5_dscp_40_46
    match cos 5
    !
    match dscp 40 46
    ! NOTE: Enables DSCP-based queueing on the port in the direction of the queueing policy.
!
class-map type lan-queuing match-any c_map_dscp_48-63
    match dscp 48 49 50 51 52 53 54 55
    match dscp 56 57 58 59 60 61 62 63

    ! NOTE: Enables DSCP-based queueing on the port in the direction of the queueing policy.
!
class-map type lan-queuing match-any c_map_dscp_32_34-38
    match dscp 32 34 35 36 37 38
    ! NOTE: Enables DSCP-based queueing on the port in the direction of the queueing policy.
!
class-map type lan-queuing match-any c_map_dscp_24_26_28_30
    match dscp 24 26 28 30
    ! NOTE: Enables DSCP-based queueing on the port in the direction of the queueing policy.
!
class-map type lan-queuing match-any c_map_dscp_18_20_22
    match dscp 18 20 22
    ! NOTE: Enables DSCP-based queueing on the port in the direction of the queueing policy.
!
class-map type lan-queuing match-any c_map_dscp_10_12_14
    match dscp 10 12 14
    ! NOTE: Enables DSCP-based queueing on the port in the direction of the queueing policy.
    !
policy-map type lan-queuing p_map_8q4t_dscp ! For 8q4t DSCP-based queueing

    ! Configures queue #8:
    class c_map_cos_5_dscp_40_46
    ! Receives QoS values (CoS, DSCP, precedence) values filtered by c_map_cos_5.
    !
        bandwidth percent 90 ! WRR bandwidth allocation.
        queue-buffers ratio 20 !Queue buffer size.
        !
        ! CoS 5 and DSCP 40, 46 default to threshold 4 at 100%
    !
    ! Configures queue #7:
    class c_map_dscp_48-63
    ! Receives QoS values (CoS, DSCP, precedence) values filtered by c_map_dscp_48-63.
        !
        bandwidth remaining percent 10 ! WRR bandwidth allocation.
        queue-buffers ratio 10 !Queue buffer size.
        !
        ! DSCP 48-63 default to threshold 4 at 100%
        !
    ! Configures queue #6:
    class c_map_dscp_32_34-38
    ! Receives QoS values (CoS, DSCP, precedence) values filtered by c_map_dscp_32_34-38.
        !
```

```
    bandwidth remaining percent 10 ! WRR bandwidth allocation.
    queue-buffers ratio 10 !Queue buffer size.
    !
    ! DSCP 32, 34-38 default to threshold 4 at 100%
    !
! Configures queue #5:
class c_map_dscp_24_26_28_30
! Receives QoS values (CoS, DSCP, precedence) values filtered by c_map_dscp_24_26_28_30.
    !
    bandwidth remaining percent 10 ! WRR bandwidth allocation.
    queue-buffers ratio 10 !Queue buffer size.
    !
    ! DSCP 24, 26, 28, 30 default to threshold 4 at 100%
    !
! Configures queue #4:
class c_map_dscp_18_20_22
! Receives QoS values (CoS, DSCP, precedence) values filtered by c_map_dscp_18_20_22.
    !
    bandwidth remaining percent 10 ! WRR bandwidth allocation.
    queue-buffers ratio 10 !Queue buffer size.
    !
    ! Configures threshold #1:
    random-detect dscp-based
    random-detect dscp 20 percent 70 100
    random-detect dscp 22 percent 70 100
    random-detect dscp 18 percent 70 100
    !
! Configures queue #3:
class c_map_dscp_10_12_14
! Receives QoS values (CoS, DSCP, precedence) values filtered by c_map_dscp_10_12_14.
    !
    bandwidth remaining percent 10 ! WRR bandwidth allocation.
    queue-buffers ratio 10 !Queue buffer size.
    !
    ! Configures threshold #1:
    random-detect dscp-based
    random-detect dscp 14 percent 70 100
    random-detect dscp 12 percent 70 100
    random-detect dscp 10 percent 70 100
    !
! Configures queue #1:
class class-default
! Receives all remaining QoS values (CoS, DSCP, precedence).
!
    bandwidth percent 10 ! WRR bandwidth allocation.
    queue-buffers ratio 80 !Queue buffer size.
    !
    ! Configures threshold #1:
    random-detect cos-based aggregate
    random-detect cos values 0 1 percent 40 70
    !
    ! Configures threshold #2:
    random-detect cos-based aggregate
    random-detect cos values 2 3 percent 40 80
    !
    ! Configures threshold #3:
    random-detect cos-based
    random-detect cos value 4 percent 50 90
    !
    ! Configures threshold #4:
    random-detect cos-based aggregate
    random-detect cos values 6 7 percent 50 100
    ! DSCP values default to this threshold
    ! 0-9, 11, 13, 15-17, 19, 21, 23, 25, 27, 29, 31, 33, 39, 41-45, 47
```

1p1q4t 入力キューの設定例

（注）　テールドロップしきい値と CoS ベース キューイングの組み合わせをサポートしています。

```
class-map type lan-queuing match-any c_map_cos_5
    match cos 5
!
policy-map type lan-queuing p_map_1p1q4t ! For 1p1q4t
!
    ! Configures the priority queue:
    class c_map_cos_5 ! Receives CoS values filtered by c_map_cos_5.
        priority ! Applies the class map to the priority queue
    !
    ! Configures queue #1:
    class class-default ! Receives all remaining CoS values.
    !
        ! Configures threshold #1
        queue-limit cos values 0 1 percent 70
        ! Applies CoS 0 1 to threshold 1 and configures the threshold percentage
        !
        ! Configures threshold #2
        queue-limit cos values 2 3 percent 80
        ! Applies CoS 2 3 to threshold 2 and configures the threshold percentage
        !
        ! Configures threshold #3
        queue-limit cos 4 percent 90
        ! Applies CoS 4 to threshold 3 and configures the threshold percentage
        !
        ! CoS 6 and 7 default to threshold 4 at 100%
```

1p1q8t 入力キューの設定例

（注）　CoS ベース キューイングとテールドロップまたは WRED ドロップのしきい値の組み合わせをサポートしています。

```
class-map type lan-queuing match-any c_map_cos_5
    match cos 5
!
policy-map type lan-queuing p_map_1p1q8t ! For 1p1q8t
!
    ! Configures the priority queue:
    class c_map_cos_5 ! Receives CoS values filtered by c_map_cos_5.
        priority ! Applies the class map to the priority queue
    !
    class class-default ! Receives all remaining CoS values.
        !
        random-detect cos-based
        ! Enables application of CoS values to a WRED-drop threshold.
        !
        ! Configures threshold #1
        random-detect cos 0 percent 40 70
        ! Applies CoS to WRED-drop threshold 1 and configures the threshold percentages.
        !
        ! Configures threshold #2
        random-detect cos 1 percent 40 70
        ! Applies CoS to WRED-drop threshold 2 and configures the threshold percentages.
```

```
    !
    ! Configures threshold #3
    random-detect cos 2 percent 50 80
    ! Applies CoS to WRED-drop threshold 3 and configures the threshold percentages.
    !
    ! Configures threshold #4
    random-detect cos 3 percent 50 80
    ! Applies CoS to WRED-drop threshold 4 and configures the threshold percentages.
    !
    ! Configures threshold #5
    random-detect cos 4 percent 60 90
    ! Applies CoS to WRED-drop threshold 5 and configures the threshold percentages.
    !
    ! Configures threshold #6
    random-detect cos 6 percent 60 90
    ! Applies CoS to WRED-drop threshold 6 and configures the threshold percentages.
    !
    ! Configures threshold #7
    random-detect cos 7 percent 70 100
    ! Applies CoS to WRED-drop threshold 7 and configures the threshold percentages.
```

1p3q8t 出力キューの設定例

（注）　CoS ベース キューイングとテールドロップおよび WRED ドロップのしきい値の組み合わせをサポートしています。

```
class-map type lan-queuing match-any c_map_cos_2_3_4
    match cos 2 3 4
!
class-map type lan-queuing match-any c_map_cos_5
    match cos 5
!
class-map type lan-queuing match-any c_map_cos_6_7
    match cos 6 7
!
policy-map type lan-queuing p_map_1p3q8t
!
    ! Configures the priority queue:
    class c_map_cos_5 ! Receives CoS values filtered by c_map_cos_5.
        priority ! Applies the class map to the priority queue
    !
    ! Configures queue #3 for 1p3q8t:
    class c_map_cos_6_7
    ! Receives CoS values values filtered by c_map_cos_6_7.
    !
        bandwidth remaining percent 40 ! WRR bandwidth allocation.
        queue-buffers ratio 15 !Queue buffer size.
        !
        ! Configures threshold #1:
        random-detect cos-based aggregate
        ! The 'aggregate' keyword allows use of the 'values' keyword
        !
        random-detect cos values 6 7 percent 70 100
    !
    ! Configures queue #2 for 1p3q8t:
    class c_map_cos_2_3_4
    ! Receives CoS values values filtered by c_map_cos_2_3_4.
    !
        bandwidth remaining percent 30 ! WRR bandwidth allocation.
        queue-buffers ratio 20 !Queue buffer size.
```

```
        !
        ! Configures threshold #1:
        random-detect cos-based
        !
        random-detect cos 2 percent 40 70
        ! Applies CoS to WRED-drop threshold 1 and configures the threshold percentages.
        !
        ! Configures threshold #2:
        random-detect cos-based aggregate
        ! The 'aggregate' keyword allows use of the 'values' keyword
        !
        random-detect cos values 3 4 percent 70 100
        ! Applies CoS to WRED-drop threshold 2 and configures the threshold percentages.
    !
    ! Configures queue #1:
    class class-default
    ! Receives all remaining CoS values.
    !
        bandwidth remaining percent 25 ! WRR bandwidth allocation.
        queue-buffers ratio 20 !Queue buffer size.
        !
        ! Configures threshold #1:
        random-detect cos-based
        !
        random-detect cos 0 percent 40 70
        ! Applies CoS to WRED-drop threshold 1 and configures the threshold percentages.
        !
        ! Configures threshold #2:
        random-detect cos-based
        !
        random-detect cos 1 percent 70 100
        ! Applies CoS to WRED-drop threshold 2 and configures the threshold percentages.
```

1p7q8t 出力キューの設定例

（注）　CoS ベース キューイングとテールドロップおよび WRED ドロップのしきい値の組み合わせをサポートしています。

```
class-map type lan-queuing match-any c_map_cos_2_3_4
    match cos 2 3 4
!
class-map type lan-queuing match-any c_map_cos_5
    match cos 5
!
class-map type lan-queuing match-any c_map_cos_6_7
    match cos 6 7
!
policy-map type lan-queuing p_map_1p7q8t
!
    ! Configures the priority queue:
    class c_map_cos_5 ! Receives CoS values filtered by c_map_cos_5.
        priority ! Applies the class map to the priority queue
    !
    ! Configures queue #7:
    class c_map_cos_6_7
    ! Receives CoS values values filtered by c_map_cos_6_7.
    !
        bandwidth remaining percent 40 ! WRR bandwidth allocation.
        queue-buffers ratio 15 !Queue buffer size.
        !
```

```
    ! Configures threshold #1:
    random-detect cos-based aggregate
    ! The 'aggregate' keyword allows use of the 'values' keyword
    !
    random-detect cos values 6 7 percent 70 100
!
! Configures queue #6 for 1p7q8t:
class c_map_cos_2_3_4
! Receives CoS values values filtered by c_map_cos_2_3_4.
!
    bandwidth remaining percent 30 ! WRR bandwidth allocation.
    queue-buffers ratio 20 !Queue buffer size.
    !
    ! Configures threshold #1:
    random-detect cos-based
    !
    random-detect cos 2 percent 40 70
    ! Applies CoS to WRED-drop threshold 1 and configures the threshold percentages.
    !
    ! Configures threshold #2:
    random-detect cos-based aggregate
    ! The 'aggregate' keyword allows use of the 'values' keyword
    !
    random-detect cos values 3 4 percent 70 100
    ! Applies CoS to WRED-drop threshold 2 and configures the threshold percentages.
!
! Configures queue #1:
class class-default
! Receives all remaining CoS values.
!
    bandwidth remaining percent 25 ! WRR bandwidth allocation.
    queue-buffers ratio 50 !Queue buffer size.
    !
    ! Configures threshold #1:
    random-detect cos-based
    !
    random-detect cos 0 percent 40 70
    ! Applies CoS to WRED-drop threshold 1 and configures the threshold percentages.
    !
    ! Configures threshold #2:
    random-detect cos-based
    !
    random-detect cos 1 percent 70 100
    ! Applies CoS to WRED-drop threshold 2 and configures the threshold percentages.
```

1p7q4t 入力または出力キューの設定例（CoS ベースのキューイング）

（注） CoS ベース、DSCP ベース、および優先順位ベースのキューイングと、テール ドロップと WRED ドロップのしきい値の組み合わせをサポートしています。SRR（WS-X6904-40G-2T を除く）または DWRR デキューイングをサポートしています。次の例では、CoS ベースのキューイングを設定します。

```
class-map type lan-queuing match-any c_map_cos_5
    match cos 5
!
policy-map type lan-queuing p_map_1p7q4t_cos

    ! Configures the priority queue:
    class c_map_cos_5 ! Receives CoS values filtered by c_map_cos_5.
```

```
    priority ! Applies the class map to the priority queue
!
! Configures queue #1:
class class-default
! Receives all remaining CoS values.
!
    bandwidth remaining percent 85 ! WRR bandwidth allocation.
```

（注）　WS-X6904-40G-2T ポートで、**bandwidth** コマンドは、ポートの他のキューイング コマンドにデフォルト以外の値を設定する場合、設定する必要があります。（CSCtz05347）

```
    queue-buffers ratio 10 !Queue buffer size.
    !
    ! Configures threshold #1:
    random-detect cos-based aggregate
    ! The 'aggregate' keyword allows use of the 'values' keyword
    !
    random-detect cos values 0 1 percent 40 70
    !
    ! Configures threshold #2:
    random-detect cos-based aggregate
    ! The 'aggregate' keyword allows use of the 'values' keyword
    !
    random-detect cos values 2 3 percent 40 80
    !
    ! Configures threshold #3:
    random-detect cos-based
    !
    random-detect cos value 4 percent 50 90
    !
    ! Configures threshold #4:
    random-detect cos-based aggregate
    ! The 'aggregate' keyword allows use of the 'values' keyword
    !
    random-detect cos values 6 7 percent 50 100
```

1p7q4t 入力または出力キューの設定例（DSCP ベースのキューイング）

（注）　CoS ベース、DSCP ベース、および優先順位ベースのキューイングと、テール ドロップと WRED ドロップのしきい値の組み合わせをサポートしています。SRR（WS-X6904-40G-2T を除く）または DWRR デキューイングをサポートしています。この例では、DSCP ベースのキューイングを設定します。

```
class-map type lan-queuing match-any c_map_cos_5_dscp_40_46
    match cos 5
    !
    match dscp 40 46
    ! NOTE: Enables DSCP-based queueing on the port in the direction of the queueing policy.
!
class-map type lan-queuing match-any c_map_dscp_48-63
    match dscp 48 49 50 51 52 53 54 55
    match dscp 56 57 58 59 60 61 62 63
    ! NOTE: Enables DSCP-based queueing on the port in the direction of the queueing policy.
!
class-map type lan-queuing match-any c_map_dscp_32_34-38
    match dscp 32 34 35 36 37 38
    ! NOTE: Enables DSCP-based queueing on the port in the direction of the queueing policy.
```

```
!
class-map type lan-queuing match-any c_map_dscp_24_26_28_30
    match dscp 24 26 28 30
    ! NOTE: Enables DSCP-based queueing on the port in the direction of the queueing policy.
!
class-map type lan-queuing match-any c_map_dscp_18_20_22
    match dscp 18 20 22
    ! NOTE: Enables DSCP-based queueing on the port in the direction of the queueing policy.
!
class-map type lan-queuing match-any c_map_dscp_10_12_14
    match dscp 10 12 14
    ! NOTE: Enables DSCP-based queueing on the port in the direction of the queueing policy.
    !
policy-map type lan-queuing p_map_1p7q4t_dscp

    ! Configures the priority queue:
    class c_map_cos_5_dscp_40_46 ! Receives CoS values filtered by c_map_cos_5_dscp_40_46.
        priority ! Applies the class map to the priority queue
        !
    ! Configures queue #7:
    class c_map_dscp_48-63
    ! Receives QoS values (CoS, DSCP, precedence) values filtered by c_map_dscp_48-63.
        !
        bandwidth remaining percent 10 ! WRR bandwidth allocation.
```

（注） WS-X6904-40G-2T ポートで、**bandwidth** コマンドは、ポートの他のキューイング コマンドにデフォルト以外の値を設定する場合、設定する必要があります。(CSCtz05347)

```
        queue-buffers ratio 10 !Queue buffer size.
        !
        ! DSCP 48-63 default to threshold 4 at 100%
        !
    ! Configures queue #6:
    class c_map_dscp_32_34-38
    ! Receives QoS values (CoS, DSCP, precedence) values filtered by c_map_dscp_32_34-38.
        !
        bandwidth remaining percent 10 ! WRR bandwidth allocation.
        queue-buffers ratio 10 !Queue buffer size.
        !
        ! DSCP 32, 34-38 default to threshold 4 at 100%
        !
    ! Configures queue #5:
    class c_map_dscp_24_26_28_30
    ! Receives QoS values (CoS, DSCP, precedence) values
    ! filtered by c_map_dscp_24_26_28_30.
        !
        bandwidth remaining percent 10 ! WRR bandwidth allocation.
        queue-buffers ratio 10 !Queue buffer size.
        !
        ! Configures threshold #1
        queue-limit dscp values 24 30 percent 100
        !
        ! Configures threshold #2
        queue-limit dscp 28 percent 100
        !
        ! Configures threshold #3
        queue-limit dscp 26 percent 100
        !
    ! Configures queue #4:
    class c_map_dscp_18_20_22
    ! Receives QoS values (CoS, DSCP, precedence) values filtered by c_map_dscp_18_20_22.
```

```
    !
    bandwidth remaining percent 10 ! WRR bandwidth allocation.
    queue-buffers ratio 10 !Queue buffer size.
    !
    ! Configures threshold #1:
    random-detect dscp-based
    random-detect dscp 20 percent 70 100
    !
    ! Configures threshold #2:
    random-detect dscp-based
    random-detect dscp 22 percent 70 100
    !
    ! Configures threshold #3:
    random-detect dscp-based
    random-detect dscp 18 percent 70 100
    !
! Configures queue #3:
class c_map_dscp_10_12_14
! Receives QoS values (CoS, DSCP, precedence) values filtered by ! c_map_dscp_10_12_14.
    !
    bandwidth remaining percent 10 ! WRR bandwidth allocation.
    queue-buffers ratio 10 !Queue buffer size.
    !
    ! Configures threshold #1:
    random-detect dscp-based
    random-detect dscp 14 percent 70 100
    random-detect dscp 12 percent 70 100
    random-detect dscp 10 percent 70 100
    !
! Configures queue #1:
class class-default
! Receives all remaining QoS values (CoS, DSCP, precedence).
!
    bandwidth remaining percent 25 ! WRR bandwidth allocation.
    queue-buffers ratio 10 !Queue buffer size.
    !
    ! Configures threshold #1:
    random-detect cos-based aggregate
    random-detect cos values 0 1 percent 40 70
    !
    ! Configures threshold #2:
    random-detect cos-based aggregate
    random-detect cos values 2 3 percent 40 80
    !
    ! Configures threshold #3:
    random-detect cos-based
    random-detect cos value 4 percent 50 90
    !
    ! Configures threshold #4:
    ! Remaining DSCP values default to this threshold
    ! 0-9, 11, 13, 15-17, 19, 21, 23, 25, 27, 29, 31, 33, 39, 41-45, 47
    !
    random-detect cos-based aggregate
    random-detect cos values 6 7 percent 50 100
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CHAPTER 65

QoS のグローバル オプションおよびインターフェイス オプション

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

入力 LAN ポートの CoS 値を設定する方法

（注）　ポートに適用されたサービス ポリシーによって、このポートに設定されているすべてのコマンドがオーバーライドされます。

PFC QoS が **platform qos cos** コマンドによって適用された CoS 値を使用するかどうかは、ポートの信頼状態とそのポート経由で受信したトラフィックの信頼状態によって決まります。**platform qos cos** コマンドを入力しても、ポートの信頼状態またはポート経由で受信したトラフィックの信頼状態は設定されません。

platform qos cos コマンドを使用して適用された CoS 値を内部 DSCP の基準として使用するには、次の設定を行います。

- タグなし入力トラフィックだけを受信するポートでは、入力ポートを信頼できるポートとして設定するか、または入力トラフィックと一致する trust CoS ポリシー マップを設定します。
- タグ付き入力トラフィックを受信するポートでは、入力トラフィックと一致する trust CoS ポリシー マップを設定します。
- 元の入力 CoS 値は、引き続き認識されます。
  - IPv4 と IPv6 のトラフィックの場合、デフォルトでは、入力 CoS 値が DSCP 値で上書きされます。
  - タグ付けされていない他のトラフィックの場合、デフォルトでは、設定されているポート CoS 値ではなく、入力 CoS 値が使用されます。
  - 元の入力 CoS 値の代わりに、**platform qos cos** インターフェイス コマンドで設定された値を使用するには、**platform qos cos override** インターフェイス コマンドを使用します。

trusted として設定されている入力 LAN ポートからのタグなしフレーム、および untrusted として設定されている入力 LAN ポートからの全フレームに PFC QoS が割り当てる CoS 値を設定できます。

入力 LAN ポートの 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	`Router(config)# interface {{type slot/port} | {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	`Router(config-if)# platform qos cos port_cos`	入力 LAN ポートの CoS 値を設定します。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。

次に、ファスト イーサネット ポート 5/24 の CoS 値 5 を設定し、設定を確認する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 5/24
Router(config-if)# platform qos cos 5
Router(config-if)# end
Router# show queueing interface fastethernet 5/24 | include Default COS
  Default COS is 5
Router#
```

出力 DSCP 変換を設定する方法

名前付き DSCP 変換マップの設定

名前付き DSCP 変換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	`Router(config)# platform qos map dscp-mutation map_name dscp1 [dscp2 [dscp3 [dscp4 [dscp5 [dscp6 [dscp7 [dscp8]]]]]]] to mutated_dscp`	名前付き DSCP 変換マップを設定します。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

- 変換された DSCP 値にマッピングする、最大 8 つの DSCP 値を入力できます。
- 複数のコマンドを入力して、追加の DSCP 値を変換された DSCP 値にマッピングできます。
- 変換された DSCP 値ごとに個別のコマンドを入力できます。

次に、DSCP 30 を変換された DSCP 値 8 にマッピングする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# platform qos map dscp-mutation mutmap1 30 to 8
Router(config)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show platform qos maps dscp-mutation
DSCP mutation map mutmap1:                    (dscp= d1d2)
     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 :    08 31 32 33 34 35 36 37 38 39
      4 :    40 41 42 43 44 45 46 47 48 49
      5 :    50 51 52 53 54 55 56 57 58 59
      6 :    60 61 62 63
<...Output Truncated...>
Router#
```

（注）　DSCP 変換マップ表示では、マークダウンされた DSCP 値がマトリクスの本体に表示されます。元の DSCP 値の 1 桁目が d1 列に表示され、2 桁目が一番上の行に表示されます。上記の例では、DSCP 30 は DSCP 08 にマッピングされています。

インターフェイスへの出力 DSCP 変換マップの対応付け

出力 DSCP 変換マップをインターフェイスに対応付けるには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {{vlan vlan_ID} | {type slot/port[.subinterface]} | {port-channel number[.subinterface]}}`	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# platform qos dscp-mutation mutation_map_name`	出力 DSCP 変換マップをインターフェイスに対応付けます。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。

次に、出力 DSCP 変換マップ mutmap1 をファスト イーサネット ポート 5/36 に対応付ける例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 5/36
Router(config-if)# platform qos dscp-mutation mutmap1
Router(config-if)# end
```

IEEE 802.1Q トンネル ポートの入力 CoS 変換の設定方法

（注）

- 受信した CoS を信頼するように設定された IEEE 802.1Q トンネル ポートは、入力 CoS 変換をサポートします（サポート対象モジュールのリストについては、「IEEE 802.1Q トンネル ポートへの入力 CoS 変換マップの適用」（P.65-6）を参照してください）。

受信した CoS を信頼するように設定された IEEE 802.1Q トンネル ポート上で入力 CoS 変換を設定する場合、PFC QoS は、入力ドロップしきい値内および任意の trust-CoS マーキングおよびポリシング用の受信した CoS 値ではなく、変換された CoS 値を使用します。

入力 CoS 変換の設定に関する注意事項および制約事項

- IEEE 802.1Q トンネル ポートとして設定されていないポートは、入力 CoS 変換をサポートしません。
- 受信した CoS を信頼するよう設定されていないポートは、入力 CoS 変換をサポートしません。
- 入力 CoS 変換では、カスタマー フレームにより伝送された CoS 値を変更しません。カスタマー トラフィックが 802.1Q トンネルから送出される場合、元の CoS がそのまま残ります。
- 次のスイッチング モジュールでは、入力 CoS 変換をサポートしています。
  - WS-X6704-10GE
  - WS-X6848-SFP-2T、WS-X6748-SFP

  - WS-X6824-SFP-2T、WS-X6724-SFP
  - WS-X6848-TX-2T、WS-X6748-GE-TX
- 入力 CoS 変換の設定は、ポート グループ内のすべてのポートに適用されます。ポート グループは次のとおりです。
  - WS-X6704-10GE：
    4 ポート、4 ポート グループ、各グループに 1 ポート
  - WS-X6848-SFP-2T、WS-X6748-SFP：
    48 ポート、4 ポート グループ：ポート 1 ～ 12、13 ～ 24、25 ～ 36、および 37 ～ 48
  - WS-X6824-SFP-2T、WS-X6724-SFP：
    24 ポート、2 ポート グループ：ポート 1 ～ 12 および 13 ～ 24
  - WS-X6848-TX-2T、WS-X6748-GE-TX：
    48 ポート、4 ポート グループ：ポート 1 ～ 12、13 ～ 24、25 ～ 36、および 37 ～ 48
- 入力 CoS 変換の設定エラーを回避するために、メンバー ポートのすべてが入力 CoS 変換をサポートしている、またはメンバー ポートのすべてが入力 CoS 変換をサポートしていない EtherChannel だけを作成してください。入力 CoS 変換に対するサポートが混在する EtherChannel を作成しないでください。
- EtherChannel のメンバーであるポート上で入力 CoS 変換を設定する場合、入力 CoS 変換はポートチャネル インターフェイスに適用されます。
- ポートチャネル インターフェイス上で、入力 CoS 変換を設定できます。
- ポートチャネル インターフェイス上で入力 CoS 変換が設定されている場合、次の動作が発生します。
  - 入力 CoS 変換の設定は、EtherChannel のすべてのメンバー ポートのポート グループに適用されます。任意のメンバー ポートが、入力 CoS 変換をサポートできない場合、設定はエラーになります。
  - ポート グループ内のあるポートが、2 番めの EtherChannel のメンバーである場合、入力 CoS 変換の設定は、2 番めのポートチャネル インターフェイスおよび 2 番めの EtherChannel のすべてのメンバー ポートのポート グループに適用されます。2 番めの EtherChannel の任意のメンバー ポートが入力 CoS 変換をサポートできない場合、1 番めの EtherChannel 上の設定がエラーになります。1 番めの EtherChannel のメンバー ポートがあるポート グループ内の非メンバー ポートで、設定が行われた場合、この設定は非メンバー ポート上でエラーになります。
  - ポートが CoS を信用するように設定されているかどうか、または IEEE 802.1Q トンネル ポートとして設定されているかどうかにかかわらず、入力 CoS 変換の設定はポート グループ、メンバー ポート、ポートチャネル インターフェイスを通して、制限なく伝播します。
- 入力 CoS 変換を設定する予定の EtherChannel では、入力 CoS 変換をサポートしていないメンバー ポートがある他の EtherChannel のメンバー ポートを含むポート グループ内のポートをメンバーとすることができません（この制約は、ポートグループにリンクされるすべてのメンバー ポートおよびポートチャネルインターフェイスにリンクされるすべてのポートに、制限なく適用されます）。
- 入力 CoS 変換を設定する予定のポートは、入力 CoS 変換をサポートしていないメンバーがある EtherChannel のメンバー ポートを含むポート グループ内に組み込むことはできません（この制約は、ポートグループにリンクされるすべてのメンバー ポートおよびポートチャネルインターフェイスにリンクされるすべてのポートに、制限なく適用されます）。
- ポートグループにリンクされるメンバー ポートおよびポートチャネルインターフェイスにリンクされるポートすべてに適用される入力 CoS 変換の設定は、1 つだけです。

入力 CoS 変換マップの設定

入力 CoS 変換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	Router(config)# **platform qos map cos-mutation** *mutation_map_name mutated_cos1 mutated_cos2 mutated_cos3 mutated_cos4 mutated_cos5 mutated_cos6 mutated_cos7 mutated_cos8*	入力 CoS 変換マップを設定します。PFC QoS が入力 CoS 値 0 ～ 7 をマッピングする、8 つの変換 CoS 値を入力する必要があります。
ステップ 2	Router(config)# **end**	コンフィギュレーション モードを終了します。

次に、testmap という名前の CoS 変換マップを設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# platform qos map cos-mutation testmap 4 5 6 7 0 1 2 3
Router(config)# end
Router#
```

次に、マップの設定を確認する例を示します。

```
Router(config)# show platform qos maps cos-mutation
COS mutation map testmap
cos-in  :   0  1  2  3  4  5  6  7
-------------------------------------
cos-out :   4  5  6  7  0  1  2  3
Router#
```

IEEE 802.1Q トンネル ポートへの入力 CoS 変換マップの適用

IEEE 802.1Q トンネル ポートに入力 CoS 変換マップを対応付けるには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** {{*type slot/port*} | {**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	Router(config-if)# **platform qos cos-mutation** *mutation_map_name*	入力 CoS 変換マップをインターフェイスに対応付けます。
ステップ 3	Router(config-if)# **end**	コンフィギュレーション モードを終了します。

次に、testmap という名前の入力 CoS 変換マップを、ポート GigabitEthernet 1/1 に対応付ける例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 1/1
Router(config-if)# platform qos cos-mutation testmap
Router(config-if)# end
Router# show platform qos maps cos-mutation
COS mutation map testmap
cos-in  :   0  1  2  3  4  5  6  7
-------------------------------------
cos-out :   4  5  6  7  0  1  2  3

testmap is attached on the following interfaces
Gi1/1
Router#
```

DSCP 値マッピングの設定方法

受信 CoS 値から内部 DSCP 値へのマッピング

受信した CoS 値から、PFC QoS が PFC 上で内部的に使用する DSCP 値へのマッピ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	`Router(config)# table-map cos-discard-class-map` *dscp1 dscp2 dscp3 dscp4 dscp5 dscp6 dscp7 dscp8*	受信した CoS 値から内部 DSCP 値へのマッピングを設定します。PFC QoS が CoS 値 0 ～ 7 をマッピングする、8 つの DSCP 値を入力する必要があります。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

次に、受信した CoS 値から内部 DSCP 値へのマッピングを設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# table-map cos-discard-class-map 0 1 2 3 4 5 6 7
Router(config)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show platform qos maps cos-discard-class
Router#
```

受信 IP precedence 値から内部 DSCP 値へのマッピング

受信した IP precedence 値から、PFC QoS が PFC 上で内部的に使用する DSCP 値へのマッピ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	`Router(config)# table-map precedence-discard-class-map` *dscp1 dscp2 dscp3 dscp4 dscp5 dscp6 dscp7 dscp8*	受信した IP precedence 値から内部 DSCP 値へのマッピングを設定します。PFC QoS が受信した IP precedence 値 0 ～ 7 をマッピングする、8 つの内部 DSCP 値を入力する必要があります。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

次に、受信した IP precedence 値から内部 DSCP 値へのマッピングを設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# table-map precedence-discard-class-map 0 1 2 3 4 5 6 7
Router(config)# end
```

次に、設定を確認する例を示します。

```
Router# show platform qos maps precedence-discard-class
Router#
```

DSCP マークダウン値の設定

ポリサーが使用する DSCP マークダウン値のマッピ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	`Router(config)# table-map policed-discard-class {normal-burst | max-burst} dscp1 [dscp2 [dscp3 [dscp4 [dscp5 [dscp6 [dscp7 [dscp8]]]]]]] to markdown_dscp`	DSCP マークダウン値のマッピングを設定します。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

DSCP マークダウン値のマッピングを設定する場合、次の点に注意してください。

- **exceed-action policed-dscp-transmit** キーワードによって使用されるマークダウン値のマッピングを設定するには、**normal-burst** キーワードを使用します。
- **violate-action policed-dscp-transmit** キーワードによって使用されるマークダウン値のマッピングを設定するには、**max-burst** キーワードを使用します。

（注）　**pir** キーワードを使用せずにポリサーを作成し、かつ *maximum_burst_bytes* パラメータが *normal_burst_bytes* パラメータに等しい場合（*maximum_burst_bytes* パラメータを入力しない場合に発生）、**exceed-action policed-dscp-transmit** キーワードを使用すると、PFC QoS は **policed-dscp max-burst** マークダウン マップの定義に従ってトラフィックをマークダウンします。

- パケットの順序誤りを防ぐため、適合するトラフィックおよび適合しないトラフィックが同じキューを使用するように、マークダウン値のマッピングを設定してください。
- マークダウンされた DSCP 値にマッピングする、最大 8 つの DSCP 値を入力することができます。
- 複数のコマンドを入力して、追加の DSCP 値をマークダウンされた DSCP 値にマッピングできます。
- マークダウンされた DSCP 値ごとに 1 つずつのコマンドを入力できます。

（注）　マークダウンされた DSCP 値は、マークダウン ペナルティと矛盾しない CoS 値にマッピングするように設定してください。

次に、DSCP 1 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。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# table-map policed-discard-class normal-burst 1 to 0
Router(config)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show table-map policed-discard-class-normal-burst-map
```

```
   Normal Burst Policed-dscp map:                                    (dscp= d1d2)
     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 :    50 51 52 53 54 55 56 57 58 59
      6 :    60 61 62 63
Router#
```

（注）　Policed-dscp 表示では、マークダウンされた DSCP 値がマトリクスの本体に表示されます。元の DSCP 値の 1 桁目が d1 カラムに表示され、2 桁目が一番上の行に表示されます。上記の例では、DSCP 41 は DSCP 41 にマッピングされています。

内部 DSCP 値から出力 CoS 値へのマッピング

PFC QoS が PFC 上で内部的に使用する DSCP 値から、出力 LAN ポートのスケジューリングおよび輻輳回避に使用される CoS 値へのマッピ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	`Router(config)# table-map discard-class-cos-map` *dscp1* [*dscp2* [*dscp3* [*dscp4* [*dscp5* [*dscp6* [*dscp7* [*dscp8*]]]]]]] **to** *cos_value*	内部 DSCP 値から出力 CoS 値へのマッピングを設定します。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

- PFC QoS が CoS 値にマッピングする DSCP 値は、8 つまで入力できます。
- 複数のコマンドを入力して、追加の DSCP 値を CoS 値にマッピングできます。
- CoS 値ごとに個別のコマンドを入力できます。

次に、内部 DSCP 値 0、8、16、24、32、40、48、および 54 を、出力 CoS 値 0 にマッピングする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# table-map discard-class-cos-map 0 8 16 24 32 40 48 54 to 0
Router(config)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show table-map discard-class-cos-map
   Dscp-cos map:                                      (dscp= d1d2)
     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 :    06 06 06 06 00 06 07 07 07 07
      6 :    07 07 07 07
Router#
```

（注）　Dscp-cos map の出力で、マトリクスの本体に表示されるのが CoS 値です。DSCP 値の最初の桁の数字は d1 のカラムに、2 番めの桁の数字は一番上の行に表示されます。上記の例では、DSCP 値 41 ～ 47 は、いずれも CoS 05 にマッピングしています。

シスコ デバイス検証による信頼境界を設定する方法

シスコ デバイス検証による信頼境界機能は、CDP を使用して、Cisco IP Phone がポートに接続されているかどうかを検出するように、イーサネット LAN ポートを設定します。

- CDP が Cisco IP Phone を検出すると、QoS は、設定されている **mls qos trust dscp**、**mls qos trust ip-precedence** または **mls qos trust cos** インターフェイス コマンドを適用します。
- CDP が Cisco IP Phone を検出しない場合、QoS は、設定されているデフォルト以外の信頼状態をすべて無視します。

シスコ デバイス検証による信頼境界を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** {{*type slot/port*} | {**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	Router(config-if)# **platform qos trust device cisco-phone**	シスコ デバイス検証による信頼境界を設定します。
ステップ 3	Router(config-if)# **end**	コンフィギュレーション モードを終了します。

シスコ デバイス検証による信頼境界を設定するときは、シスコ デバイス検証による信頼境界を使用するように、ポートで CDP をイネーブルにする必要があります。

次に、ギガビット イーサネット ポート 1/1 にシスコ デバイス検証による信頼境界を設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 1/1
Router(config-if)# mls qos trust device cisco-phone
Router(config-if)# end
Router#
```

次に、CoS を信頼するようにポートが設定されているが、Cisco IP Phone が接続されていないコンフィギュレーションを確認する例を示します。

```
Router# show queueing interface gigabitethernet 1/1 | include [Tt]rust
Trust boundary enabled
  Port is untrusted
  Extend trust state: not trusted [COS = 0]
Router#
```

queueing-only モードのレガシー コンフィギュレーション手順

（注）　queueing-only 機能は、サービス ポリシーとともにのみ設定できます。

スイッチで queueing-only モ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	`Router(config)# platform qos queueing-only`	スイッチで queueing-only モードをイネーブルにします。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

queueing-only モードをイネーブルにすると、次のアクションが実行されます。

- サービス ポリシーが設定されたポートを除き、ポリシングおよびマーキングをディセーブルにします（すべての入力 QoS ラベルを保持）。
- 入力キューイング ポリシーが対応付けられていないポートで入力キューイングを設定します。出力キューイング ポリシーが対応付けられていないポートで出力キューイングを設定します。
- すべてのポートがレイヤ 2 CoS を信頼するように設定します。

（注）　スイッチでは、タグなし入力トラフィックと、trust CoS に設定できないポートを介して受信されるトラフィックにポート CoS 値が適用されます。

次に、queueing-only モードをイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# platform qos queueing-only
Router(config)# end
Router#
```

レイヤ 2 LAN ポートでの VLAN ベースの PFC QoS のレガシー コンフィギュレーション手順

（注）
- 出力トラフィックに対する PFC QoS アプリケーション用に、レイヤ 3 インターフェイスにポリシー マップを対応付けることができます。レイヤ 2 ポート上の VLAN ベースまたはポート ベースの PFC QoS は、レイヤ 3 インターフェイス上の出力トラフィックに対する PFC QoS アプリケーションとは関係ありません。
- デフォルトでは、PFC QoS は LAN ポートに付加されたポリシー マップを使用します。**switchport** キーワードを使用してレイヤ 2 LAN ポートとして設定されているポートでは、PFC QoS が VLAN に対応付けられたポリシー マップを使用するように設定できます。**switchport** キーワードを使用せずに設定されたポートは、VLAN に対応付けられません。

レイヤ 2 LAN ポートで VLAN ベース PFC QoS 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	`Router(config)# interface {{type slot/port} | {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	`Router(config-if)# platform qos vlan-based`	レイヤ 2 LAN ポートまたはレイヤ 2 EtherChannel で VLAN ベース PFC QoS をイネーブルにします。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。

- **platform qos vlan-based** インターフェイス コマンドが設定されている場合、設定されたポートの信頼状態は、マーキングに影響しません。
- レイヤ 3 VLAN インターフェイスに対応付けられたサービス ポリシーは、**platform qos vlan-based** インターフェイス コマンドが設定されているポートの QoS を定義します。
- **platform qos vlan-based** インターフェイス コマンドで設定されたポートに対応付けられたサービス ポリシーは無視されます。
- レイヤ 2 LAN ポートを VLAN ベースの PFC QoS に設定しても、ポリシー マップに関するポート設定はそのままの状態です。**no platform qos vlan-based** ポート コマンドを使用すると、すでに設定されていたポート コマンドが再びイネーブルになります。

次に、ポート FastEthernet 5/42 で VLAN ベースの PFC QoS をイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 5/42
Router(config-if)# platform qos vlan-based
Router(config-if)# end
```

次に、設定を確認する例を示します。

```
Router# show platform qos | begin QoS is vlan-based
  QoS is vlan-based on the following interfaces:
    Fa5/42
<...Output Truncated...>
```

ポートの信頼状態のレガシー コンフィギュレーション手順

サービス ポリシーが対応付けられていないポートを信頼できない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	Router(config)# **interface** {{*type slot/port*} | {**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	Router(config-if)# **platform qos trust none remark**	ポートを信頼できないポートとして設定し、すべての非 MPLS トラフィックをマーキングします。
ステップ 3	Router(config-if)# **end**	コンフィギュレーション モードを終了します。

CoS または IP precedence を信頼するように、サービス ポリシーが対応付けられていない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	Router(config)# **interface** {{*type slot/port*} | {**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	Router(config-if)# **platform qos trust** [**precedence** | **cos**]	ポートの信頼状態を設定します。 **（注）**　DSCP は、デフォルトで信頼されます。
ステップ 3	Router(config-if)# **end**	コンフィギュレーション モードを終了します。

（注） ポートの信頼状態は、入力キューイングをイネーブルにすることとは無関係です。CoS 値が矛盾しているためにトラフィックがドロップされないようにするには、ネットワーク ポリシーと整合しているとわかっている CoS 値を伝送している受信トラフィックの場合にだけ、CoS を信頼するようにポートを設定します。

次に、**trust cos** キーワードを使用してポート GigabitEthernet 1/1 を設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 1/1
Router(config-if)# platform qos trust cos
Router(config-if)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show queueing interface gigabitethernet 1/1 | include trust
  Trust state: trust COS
Router#
```

DSCP ベースのキュー マッピングのレガシー コンフィギュレーション手順

（注）
- ポリシー ベースのキューイングを設定してある場合は、この項の手順を使用しないでください。
- DSCP ベースのキューおよびしきい値は、8q4t、1p7q2t、および 1p7q4t ポートでイネーブルにできます（「モジュールとキュー タイプのマッピング」（P.64-7）を参照）
- DSCP ベースのキューイングは、8q4t、1p7q2t、および 1p7q4t ポートでサポートされています。Supervisor Engine 2T-10GE のポートは、**platform qos 10g-only** 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 8q4t/1p7q4t です。Supervisor Engine 2T ポートに DSCP ベースのキュー マッピングを設定するには、**shutdown** インターフェイス コンフィギュレーション モード コマンドを Supervisor Engine 2T ギガビット イーサネット ポートに対して入力する必要があります。次に、**platform qos 10g-only** グローバル コンフィギュレーション コマンドを入力し、Supervisor Engine 2T 上のギガビット イーサネット ポートをディセーブルにします。
- CSCts82932 が解決されていないリリースでは、サポート帯域幅およびキュー制限を設定する場合を除き、8q4t 入力キューのデフォルトの DSCP ベースのキュー マッピングを使用しないでください。

DSCP ベースのキュー マッピングのイネーブル化

DSCP ベースのキュー マッ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	`Router(config)# interface 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	`Router(config-if)# platform qos queue-mode mode-dscp`	DSCP ベースのキュー マッピングをイネーブルにします。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。

次に、DSCP ベースのキュー マッピングを 10 ギガビット イーサネット ポート 6/1 でイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface tengigabitethernet 6/1
Router(config-if)# platform qos queue-mode mode-dscp
Router(config-if)# end
```

次に、設定を確認する例を示します。

```
Router# show queueing interface tengigabitethernet 6/1 | include Queueing Mode
    Queueing Mode In Tx direction: mode-dscp
    Queueing Mode In Rx direction: mode-dscp
```

入力 DSCP ベースのキュー マッピングの設定

（注）　入力 DSCP とキューとのマッピングは、DSCP を信頼するように設定されたポートだけでサポートされます。

標準受信キューしきい値への DSCP 値のマッピング

DSCP 値を標準受信キューしきい値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	`Router(config)# interface 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	`Router(config-if)# rcv-queue dscp-map queue_# threshold_# dscp1 [dscp2 [dscp3 [dscp4 [dscp5 [dscp6 [dscp7 [dscp8]]]]]]]`	標準受信キューしきい値に DSCP 値をマッピングします。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。

DSCP 値をマッピングする場合、次の点に注意してください。

- キューおよびしきい値にマッピングする、最大 8 つの DSCP 値を入力できます。
- 複数のコマンドを入力して、追加の DSCP 値をキューおよびしきい値にマッピングできます。
- キューおよびしきい値ごとに個別のコマンドを入力する必要があります。

次に、10 ギガビット イーサネット ポート 6/1 に対して、標準受信キューのしきい値 1 に DSCP 値 0 および 1 をマッピングする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface tengigabitethernet 6/1
Router(config-if)# rcv-queue dscp-map 1 1 0 1
Router(config-if)# end
Router#
```

（注）　受信キュー マッピングは、**show queueing interface** コマンドによって表示される、2 回めの「queue thresh dscp-map」に表示されます。

次に、設定を確認する例を示します。

```
Router# show queueing interface tengigabitethernet 1/1 | begin queue thresh dscp-map
<...Output Truncated...>
queue thresh dscp-map
----------------------------------------
1     1       0 1 2 3 4 5 6 7 8 9 11 13 15 16 17 19 21 23 25 27 29 31 33 39 41 42 43 44 45
47
1     2
1     3
1     4
2     1       14
2     2       12
2     3       10
2     4
3     1       22
3     2       20
3     3       18
3     4
4     1       24 30
4     2       28
4     3       26
4     4
5     1       32 34 35 36 37 38
5     2
5     3
5     4
6     1       48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63
6     2
6     3
6     4
7     1
7     2
7     3
7     4
8     1       40 46
8     2
8     3
8     4
<...Output Truncated...>
Router#
```

標準送信キューしきい値への DSCP 値のマッピング

標準送信キューしきい値に DSCP 値を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	Router(config)# **interface 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	Router(config-if)# **wrr-queue dscp-map** *transmit_queue_# threshold_# dscp1* [*dscp2* [*dscp3* [*dscp4* [*dscp5* [*dscp6* [*dscp7* [*dscp8*]]]]]]]	標準送信キューのしきい値に DSCP 値をマッピングします。
ステップ 3	Router(config-if)# **end**	コンフィギュレーション モードを終了します。

- キューおよびしきい値にマッピングする、最大 8 つの DSCP 値を入力できます。
- 複数のコマンドを入力して、追加の DSCP 値をキューおよびしきい値にマッピングできます。
- キューおよびしきい値ごとに個別のコマンドを入力する必要があります。

次に、10 ギガビット イーサネット ポート 6/1 に対して、標準送信キュー 1/ しきい値 1 に DSCP 値 0 および 1 をマッピングする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface tengigabitethernet 6/1
Router(config-if)# wrr-queue dscp-map 1 1 0 1
Router(config-if)# end
Router#
```

（注）　**show queueing interface** コマンドの出力では、8 番めのキューは完全プライオリティ キューです。

次に、設定を確認する例を示します。

```
Router# show queueing interface tengigabitethernet 6/1 | begin queue thresh dscp-map
queue thresh dscp-map
----------------------------------------
1     1      0 1 2 3 4 5 6 7 8 9 11 13 15 16 17 19 21 23 25 27 29 31 33 39 41 42 43 44 45
47
1     2
1     3
1     4
2     1      14
2     2      12
2     3      10
2     4
3     1      22
3     2      20
3     3      18
3     4
4     1      24 30
4     2      28
4     3      26
4     4
5     1      32 34 35 36 37 38
5     2
5     3
5     4
6     1      48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63
6     2
6     3
6     4
7     1
7     2
7     3
7     4
8     1      40 46
<...Output Truncated...>
Router#
```

送信完全優先キューへの DSCP 値のマッピング

DSCP 値を送信完全優先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	`Router(config)# interface 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	`Router(config-if)# priority-queue dscp-map queue_# dscp1 [dscp2 [dscp3 [dscp4 [dscp5 [dscp6 [dscp7 [dscp8]]]]]]]`	DSCP 値を送信完全優先キューにマッピングします。複数の **priority-queue dscp-map** コマンドを入力することで、9 つ以上の DSCP 値を完全優先キューにマッピングできます。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。

- キュー番号は、常に 1 です。
- キューにマッピングする、最大 8 つの DSCP 値を入力できます。
- 複数のコマンドを入力して、追加の DSCP 値をキューにマッピングできます。

次に、10 ギガビット イーサネット ポート 6/1 の完全優先キューに、DSCP 値 7 をマッピングする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface tengigabitethernet 6/1
Router(config-if)# priority-queue dscp-map 1 7
Router(config-if)# end
Router#
```

（注）　**show queueing interface** コマンドの出力では、完全プライオリティ キューは 8 番めのキューです。

次に、設定を確認する例を示します。

```
 Router# show queueing interface tengigabitethernet 6/1 | begin queue thresh dscp-map
    queue thresh dscp-map
    ----------------------------------------
<...Output Truncated...>
    8     1       7 40 46
<...Output Truncated...>
Router#
```

ヒント　Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

自動 QoS

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

AutoQoS の前提条件

なし。

AutoQoS の制約事項

- 自動 QoS はポートに対するコマンドを生成し、それらを実行コンフィギュレーションに追加します。
- 生成された QoS コマンドは、CLI から入力した場合と同様に適用されます。既存の設定がある場合、生成されたコマンドを適用できなかったり、生成されたコマンドにより既存の設定が上書きされる可能性があります。これらのアクションは、警告を表示せずに実行されます。生成されたコマンドが正常に適用された場合、上書きされなかった設定はすべて実行コンフィギュレーションに残されます。上書きされたコマンドはすべて、startup-config ファイルに残されます。
- 生成されたコマンドの一部は、ポート ASIC が制御するすべてのポートに適用される PFC QoS コマンドのタイプとなります。これらのコマンドのいずれかが適用されると、PFC QoS は、ポート ASIC により制御されるすべてのポートにコマンドが適用されたことによって生成されるメッセージを表示します。これらのコマンドは、モジュールに応じて 48 ものポートに適用されます。『*Release Notes for Cisco IOS Release 15.1SY*』の各モジュールの説明を参照し、ポート グループの数およびポート グループごとのポート範囲を確認してください。
- 同じポート ASIC が制御するポート上では、ポートの信頼状態の要件が競合するため、Cisco IP Phone およびその他の自動 QoS のオプションのサポートを設定できない場合があります。
- 生成されたコマンドを適用できない場合は、以前の実行コンフィギュレーションが元に戻されます。
- 自動 QoS をイネーブルにしてから、他の QoS コマンドを設定してください。自動 QoS 設定の完了後、必要に応じて、QoS 設定を変更できます。
- 自動 QoS では、すでにポリシー マップが付加されているインターフェイスにポリシー マップを付加できません。
- 名前に AUTOQOS が含まれるポリシー マップまたはクラス マップを変更しないでください。
- 次のインターフェイス上では、自動 QoS を設定できません。
  - ポートチャネル インターフェイス
  - VLAN インターフェイス（スイッチ仮想インターフェイス（SVI）とも言う）
  - トンネル インターフェイス
  - ループバック インターフェイス
  - すべてのタイプのインターフェイス上のサブインターフェイス

AutoQoS について

（注）　自動 QoS は、推奨する Architecture for Voice, Video, and Integrated Data（AVVID）QoS 設定をポートに適用するマクロです。

Cisco IP Phone の自動 QoS のサポート

Cisco IP Phone は通常、ポートに直接接続されます。必要に応じて PC を電話機に接続し、スイッチのホップとして使用できます。

電話機から発信されるトラフィックは、802.1Q または 802.1p タグでマーク付けできます。タグには、VLAN ID および CoS 値が含まれます。電話機から発信される CoS 値を信頼するようにポートを設定すると、スイッチはその CoS 値を使用して、電話機のトラフィックの優先順位付けを行います。

Cisco IP Phone には、3 ポートのスイッチが組み込まれていて、PC、電話機、およびスイッチ ポートから発信されるトラフィックを転送します。Cisco IP Phone には、設定が必要な信頼機能および分類機能があります（「Cisco IP Phone サポートの設定方法」（P.18-5）を参照）。

自動 QoS は、**auto qos voip cisco-phone** インターフェイス コンフィギュレーション コマンドにより Cisco IP Phone をサポートします。IP Phone をサポートするよう設定されていて、IP Phone が接続されているポートで、**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、自動 QoS 機能は次の処理を実行します。

- QoS がイネーブルになっていない場合は、QoS をグローバルにイネーブルにします。
- ポートに VLAN ベースの QoS が設定されている場合は、デフォルトのポートベースの QoS に戻します（**1p1q0t/1p3q1t** ポートがあるスイッチング モジュール上のすべてのポートで実行される）。
- ポートの信頼状態を trust CoS に設定します。
- trust CoS の QoS ポリシーを作成し、ポートの信頼をサポートしない **1q4t/2q2t** 非ギガビット イーサネット ポートがあるスイッチング モジュール上のポートに適用します。

Cisco IP Communicator の自動 QoS のサポート

Cisco IP Communicator プログラムは、PC 上で実行して、Cisco IP Phone をエミュレートします。Cisco IP Communicator は、CoS 値ではなく DSCP 値を使用してその音声トラフィックをマーク付けします。Cisco IP Communicator から発信された DSCP 値を信頼するようポートを設定すると、スイッチは DSCP 値を使用して、Cisco IP Communicator トラフィックの優先付けを行います。

自動 QoS は、**auto qos voip cisco-softphone** インターフェイス コンフィギュレーション コマンドにより Cisco IP Communicator プログラムをサポートします。Cisco IP Communicator プログラムを実行している装置に接続されたポートで **auto qos voip cisco-softphone** 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、自動 QoS 機能は次の処理を行います。

- QoS がイネーブルになっていない場合は、QoS をグローバルにイネーブルにします。
- ポートに VLAN ベースの QoS が設定されている場合は、デフォルトのポートベースの QoS に戻します（**1p1q0t/1p3q1t** ポートがあるスイッチング モジュール上のすべてのポートで実行される）。
- ポートに信頼状態が設定されている場合は、デフォルトの信頼状態（untrusted）に戻します。
- 入力ポリサーを作成し、trust DSCP 46 に適用し、DSCP 26 パケットを DSCP 24 に再マーク付けします。その他の DSCP 値を持つパケットまたはプロファイル外パケットは DSCP 0 で再マーク付けされます。

マーク付けされたトラフィックの自動 QoS のサポート

ネットワーク内部に接続されたポートは、そのネットワークの QoS ポリシーと矛盾しない QoS ラベルによりマーク済みのトラフィックを受信する場合があります。この場合は、QoS ラベルを変更する必要がありません。QoS の信頼機能を使用すると、受信した QoS 値を使用して、マーク済みのトラフィックを処理できます。

自動 QoS は、**auto qos voip trust** インターフェイス コンフィギュレーション コマンドによりマーク済みトラフィックをサポートします。**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、自動 QoS 機能は次の処理を行います。

- QoS がイネーブルになっていない場合は、QoS をグローバルにイネーブルにします。
- ポートに VLAN ベースの QoS が設定されている場合は、デフォルトのポートベースの QoS に戻します（**1p1q0t**/**1p3q1t** ポートがあるスイッチング モジュール上のすべてのポートで実行される）。
- **switchport** コマンドによりポートが設定されている場合は、ポートの信頼状態を trust CoS に設定します。
- **switchport** コマンドによりポートが設定されていない場合は、ポートの信頼状態を trust DSCP に設定します。
- trust CoS または trust DSCP の QoS ポリシーを作成し、ポートの信頼をサポートしない **1q4t**/**2q2t** 非ギガビット イーサネット ポートがあるスイッチング モジュール上のポートに適用します。

AutoQoS のデフォルト設定

なし。

AutoQoS の設定方法

- 「Cisco IP Phone の自動 QoS のサポートの設定」（P.66-5）
- 「Cisco IP Communicator の自動 QoS のサポートの設定」（P.66-6）
- 「マーク付けされたトラフィックの自動 QoS のサポートの設定」（P.66-7）

（注）　自動 QoS は、**auto qos voip** コマンドが入力されたポートの QoS ポート アーキテクチャに適したコマンドを生成します。自動 QoS は、異なる **auto qos voip** コマンドごとに、これらの各 QoS ポート アーキテクチャに応じて異なる QoS コマンドを生成します。

- 1p1q0t/1p3q1t
- 1p1q4t/1p2q2t
- 1p1q4t/1p3q8t
- 1p1q8t/1p2q1t
- 1q2t/1p2q2t
- 1q2t/1p3q8t
- 1q4t/2q2t
- 1q8t/1p3q8t
- 1q8t/1p7q8t
- 2q8t/1p3q8t
- 8q4t/1p7q4t
- 8q8t/1p7q8t

次に示す手順には、生成されたコマンドを表示するのに必要なコマンドは含まれますが、自動 QoS が生成する個々のコマンドはこのマニュアルに記載されていません。

Cisco IP Phone の自動 QoS のサポートの設定

（注）　Cisco IP Phone に自動 QoS を設定する前に、「Cisco IP Phone サポートの設定方法」（P.18-5）の設定手順を実行します。

Cisco IP Phone に自動 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	`Router# 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	`Router(config)# interface type slot/port`	設定するインターフェイスを選択します。
ステップ 3	`Router(config-if)# auto qos voip cisco-phone`	Cisco IP Phone に自動 QoS を設定します。
ステップ 4	`Router(config-if)# end`	特権 EXEC モードに戻ります。

Cisco IP Phone に自動 QoS を設定する場合は、次の情報に注意してください。

- インターフェイス上で自動 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。

（注）　**no auto qos voip** インターフェイス コンフィギュレーション コマンドは、自動 QoS により作成された受信 CoS 値から内部 DSCP へのマッピングを削除しません。

- 他のポートに trust CoS を設定するよう指示するメッセージが表示される場合があります。自動 QoS が生成したコマンドをイネーブルにするには、この指示に従う必要があります。

次に、ギガビット イーサネット インターフェイス 1/1 上で自動 QoS をイネーブルにする例を示します。

```
Router(config)# interface gigabitethernet 1/1
Router(config-if)# auto qos voip cisco-phone
```

生成した受信 CoS 値から内部 DSCP 値へのマッピングを表示します。

```
Router# show running-config | include qos map cos-dscp
```

Cisco IP Communicator の自動 QoS のサポートの設定

Cisco IP Communicator に自動 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	`Router# 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	`Router(config)# interface type slot/port`	設定するインターフェイスを選択します。
ステップ 3	`Router(config-if)# auto qos voip cisco-softphone`	Cisco IP Communicator に自動 QoS を設定します。
ステップ 4	`Router(config-if)# end`	特権 EXEC モードに戻ります。

- インターフェイス上で自動 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。

（注）　**no auto qos voip** インターフェイス コンフィギュレーション コマンドは、自動 QoS によって作成されたポリシー、クラス、および DSCP マークダウン マップを削除しません。

- **switchport** キーワードにより設定されたポート上では、Cisco IP Communicator のサポートを設定できません。
- PFC QoS は、1023 の集約ポリサーをサポートし、ポート上で **auto qos voip cisco-softphone** コマンドを使用するたびに、2 つの集約ポリサーを使用します。

次に、ギガビット イーサネット インターフェイス 1/1 上で自動 QoS をイネーブルにする例を示します。

```
Router(config)# interface gigabitethernet 1/1
Router(config-if)# auto qos voip cisco-softphone
```

設定した自動 QoS コマンドを表示します。

```
Router# show auto qos interface type slot/port
```

自動 QoS により作成されたポリシー マップおよびポリサーを表示します。

```
Router# show policy-map AUTOQOS-CISCO-SOFT-PHONE
```

自動 QoS により作成されたクラス マップを表示します。

```
Router# show class-map AUTOQOS-CISCO-SOFTPHONE-SIGNAL
Router# show class-map AUTOQOS-CISCO-SOFTPHONE-DATA
```

自動 QoS により作成された DSCP マークダウン マップを表示します。

```
Router# show running-config | include qos map policed-dscp
```

マーク付けされたトラフィックの自動 QoS のサポートの設定

マーク付けされたトラフィックに対する自動 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	`Router# 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	`Router(config)# interface type slot/port`	設定するインターフェイスを選択します。
ステップ 3	`Router(config-if)# auto qos voip trust`	マーク付けされたトラフィックに対する自動 QoS を設定します。
ステップ 4	`Router(config-if)# end`	特権 EXEC モードに戻ります。

マーク付けされたトラフィックを信頼するように自動 QoS を設定する場合は、次の情報に注意してください。

- インターフェイス上で自動 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。

（注）　**no auto qos voip** インターフェイス コンフィギュレーション コマンドは、自動 QoS により作成された受信 CoS 値から内部 DSCP へのマッピングを削除しません。

- **switchport** コマンドにより設定されたポートの場合、他のポートを trust CoS に設定するよう指示するメッセージが表示される場合があります。自動 QoS が生成したコマンドをイネーブルにするには、この指示に従う必要があります。

次に、ギガビット イーサネット インターフェイス 1/1 上で自動 QoS をイネーブルにする例を示します。

```
Router(config)# interface gigabitethernet 1/1
Router(config-if)# auto qos voip trust
```

設定した自動 QoS コマンドを表示します。

```
Router# show auto qos interface type slot/port
```

switchport コマンドにより設定されたポートに対して、生成された受信 CoS 値から内部 DSCP へのマッピングを表示します。

```
Router# show running-config | include qos map cos-dscp
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

MPLS QoS

（注）

- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。
- MPLS QoS は、第 61 章「PFC QoS の概要」で説明する PFC QoS 機能を MPLS トラフィックに拡張します。
- ここでは、MPLS QoS の各機能についての補足情報を説明します。この章を読むには、PFC QoS 機能を理解していることが前提となります。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

用語

- *サービス クラス*（CoS）：スイッチド ネットワークを通過するときにイーサネット フレームのプライオリティを示す 802.1Q ヘッダーの 3 ビットのことです。802.1Q ヘッダーの CoS ビットは通常 802.1p ビットと呼ばれます。パケットがレイヤ 2 およびレイヤ 3 ドメインの両方を横断するときに QoS を維持するため、タイプ オブ サービス（ToS）値と CoS 値は互いにマッピングすることができます。
- *分類*：QoS をマーキングするトラフィックを選択する処理です。
- *DiffServ コード ポイント*（DSCP）：IP ヘッダーの ToS バイトの上位 6 ビットです。DSCP は、IP パケットだけに存在します。
- *E-LSP*：ラベル スイッチド パス（LSP）の 1 つであり、ノードはここで MPLS ヘッダーの Experimental（EXP）ビットから排他的に MPLS パケットの QoS 処理を判断します。QoS 処理が EXP（クラスおよびドロップ優先順位の両方）から判断されるため、いくつかのクラスのトラフィックを 1 つの LSP に多重化することができます（同じラベルを使用）。EXP フィールドは 3 ビット フィールドであるため 1 つの LSP は最大 8 つのトラフィックのクラスをサポートすることができます。コントロール プレーン トラフィック用にいくつかの値が予約されている場合、またはクラスのいくつかがそれらに対応するドロップ優先順位を持っている場合、クラスの最大数はさらに少なくなります。
- *EXP ビット*：ノードがパケットに与える QoS 処理（Per-Hop Behavior）を定義します。これは、IP ネットワークの DiffServ コード ポイント（DSCP）に相当します。DSCP は、クラスとドロップ優先順位を定義します。EXP ビットは、一般に IP DSCP でエンコードされた情報をすべて伝送するのに使用されます。ただし、ドロップ優先順位をエンコードするために EXP ビットが排他的に使用される場合もあります。
- *フレーム*は、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。
- *IP precedence*：IP ヘッダーの ToS バイトの最上位 3 ビットです。
- *QoS タグ*：レイヤ 3 パケットおよびレイヤ 2 フレームで伝達されるプライオリティ値です。レイヤ 2 CoS ラベルは、0（ロー プライオリティ）～ 7（ハイ プライオリティ）の範囲です。レイヤ 3 IP precedence ラベルは、0（ロー プライオリティ）～ 7（ハイ プライオリティ）の範囲です。IP precedence 値は、1 バイトの ToS バイトの最上位 3 ビットで定義されます。レイヤ 3 DSCP ラベルは、0 ～ 63 の値を持つことができます。DSCP 値は 1 バイトの IP ToS フィールドのうち最上位 6 ビットで定義されます。
- *LER*（ラベル エッジ ルータ）：パケット上のラベルのインポーズおよびディスポーズを行うデバイスであり、プロバイダー エッジ（PE）ルータとも呼ばれます。
- *LSR*（ラベル スイッチング ルータ）：パケット上のラベルに基づいてトラフィックを転送するデバイスであり、プロバイダー（P）ルータとも呼ばれます。
- *マーキング*：パケットのレイヤ 3 DSCP 値を設定するプロセスです。マーキングはまた、MPLS EXP フィールドで異なった値を選択してパケットにマーキングし、輻輳時にパケットが必要なプライオリティを持つようにするプロセスでもあります。
- *パケット*：レイヤ 3 でトラフィックを伝送します。
- *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。

MPLS QoS の機能

MPLS 実験フィールド

MPLS EXP（実験）フィールド値を設定すると、サービス プロバイダーが自己のネットワークで伝送された IP パケット内で変更された IP precedence フィールドの値を望まない場合に、サービス プロバイダーの要件を満たすことができます。

MPLS EXP フィールドで異なった値を選択することにより、輻輳時にパケットが必要なプライオリティを持つようパケットをマーキングすることができます。

デフォルトでは、インポジション中に、IP precedence 値が MPLS EXP フィールドにコピーされます。MPLS EXP ビットは、MPLS QoS ポリシーによってマーキングできます。

信頼

受信レイヤ 3 MPLS パケットに対し、PFC は、通常、受信最上位ラベルの EXP 値を信頼します。MPLS パケットは、次のいずれの影響も受けません。

- インターフェイスの信頼状態
- ポートの CoS 値
- policy-map **trust** コマンド

受信レイヤ 2 MPLS パケットの場合、PFC は、CoS および出力キュー処理の目的で、受信最上位ラベルの EXP 値を信頼するか、ポートまたはポリシーの信頼を MPLS パケットに適用できます。

分類

分類とはマーキングするトラフィックを選択するプロセスです。分類は、トラフィックを複数の優先順位レベル、つまり、サービス クラスに分割することによりこのプロセスを実施します。トラフィック分類は、クラス ベースの QoS プロビジョニングのプライマリ コンポーネントです。PFC は、（ポリシーのインストール後）受信 MPLS パケットの受信最上位ラベルの EXP ビットに基づいて分類を決定します。詳細については、「MPLS パケットを分類するためのクラス マップの設定」（P.67-18）を参照してください。

ポリシングおよびマーキング

ポリシングを行うと、設定レートを超えたトラフィックは廃棄されるか、またはより高いドロップ優先順位にマークダウンされます。マーキングは、パケット フローを識別して、これらを区別する手法です。パケット マーキングを利用すれば、ネットワークを複数の優先プライオリティ レベルまたはサービス クラスに分割することができます。

実装可能な MPLS QoS ポリシングおよびマーキング機能は、受信したトラフィック タイプ、およびトラフィックに適用される転送処理によって決まります。詳細については、「ポリシー マップの設定」（P.67-20）を参照してください。

IP ToS の保持

PFC は、インポジション、スワッピング、ディスポジションを含むすべての MPLS 動作中、自動的に IP ToS を保持します。IP ToS を保存するコマンドを入力する必要はありません。

EXP 変換

最大 8 個の出力 EXP 変換マップを設定して、内部 EXP 値が出力 EXP 値として書き込まれる前に内部 EXP 値を変換することができます。出力 EXP 変換マップは、次のインターフェイス タイプに付加できます。

- LAN ポート サブインターフェイス
- レイヤ 3 VLAN インターフェイス
- レイヤ 3 LAN ポート

レイヤ 2 LAN ポート（**switchport** コマンドにより設定されるポート）に、EXP 変換マップを付加できます。

設定の詳細については、「MPLS QoS の出力 EXP 変換の設定」（P.67-25）を参照してください。

MPLS DiffServ トンネリング モード

PFC は、MPLS DiffServ トンネリング モードを使用します。トンネリングは、ネットワークの 1 つのエッジから、そのネットワークの別のエッジまでの QoS 透過性を提供します。詳細については、「MPLS DiffServ トンネリング モード」（P.67-27）を参照してください。

MPLS QoS の概要

ネットワーク管理者は MPLS QoS を使用することで、差別化したサービス タイプを MPLS ネットワーク上で提供できます。差別化サービスは、QoS によって各送信パケットに指定されたサービスを提供することにより、幅広い要件を満たします。サービスは、IP パケット内の IP precedence ビット設定を使用するなどさまざまな方法で指定することができます。

IP precedence フィールドでの QoS の指定

IP パケットを 1 つのサイトから別のサイトへ送信する場合、IP precedence フィールド（IP パケットのヘッダーの DSCP フィールドの上位 3 ビット）が QoS を指定します。IP precedence マーキングに基づき、パケットにはその QoS に対して設定された処理が適用されます。サービス プロバイダー ネットワークが MPLS ネットワークである場合、ネットワークのエッジで IP precedence ビットが MPLS EXP フィールドにコピーされます。ただし、サービス プロバイダーは、ある MPLS パケットの QoS に、提供するサービスによって決定される異なった値を設定することが必要な場合もあります。

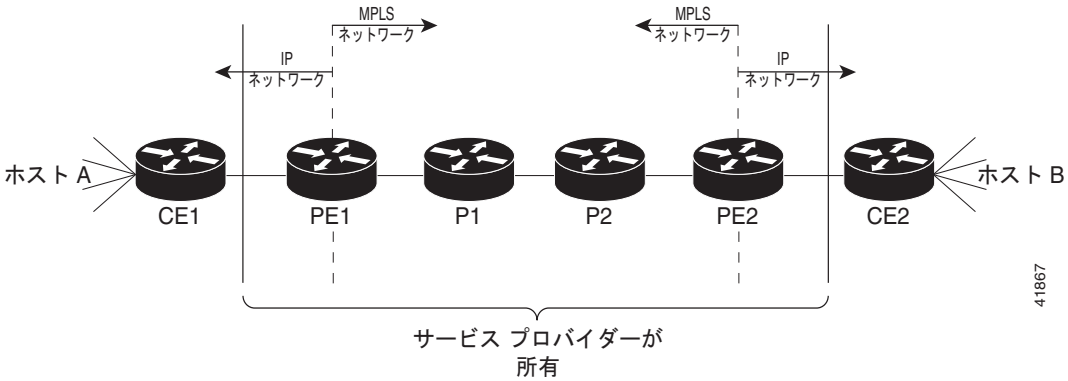
この場合、サービス プロバイダーは MPLS EXP フィールドを設定できます。IP ヘッダーはカスタマーが利用できるよう引き続き利用可能であり、IP パケットの QoS はパケットが MPLS ネットワークを移動する間は変更されません。

詳細については、「MPLS DiffServ トンネリング モード」（P.67-27）を参照してください。

MPLS QoS

MPLS トポロジの概要

図 67-1　カスタマーの IP ネットワークの 2 つのサイトを接続する MPLS ネットワーク



- このネットワークは両方向ですが、ここではパケットは左から右へ移動します。
- CE1：カスタマー装置 1
- PE1：サービス プロバイダー入力ラベル エッジ ルータ（LER）
- P1：サービス プロバイダーのネットワークのコア内のラベル スイッチ ルータ（LSR）

- P2：サービス プロバイダーのネットワークのコア内の LSR
- PE2：サービス プロバイダー出力 LER
- CE2：カスタマー装置 2
- PE1 および PE2 は、MPLS ネットワークと IP ネットワークの境界にあります。

MPLS QoS は、IP QoS をサポートしています。MPLS パケットについては、PFC が非 MPLS の QoS マーキングおよびポリシングを適用できるように、EXP 値が内部 DSCP にマッピングされます。

入力および出力ポリシーでは、MPLS QoS マーキングおよびポリシングの決定が、入力 PFC でインターフェイス単位で行われます。入力インターフェイスは物理ポート、サブインターフェイス、または VLAN です。

QoS ポリシー ACL は、入力および出力検索用に別途 QoS Ternary Content Addressable Memory（TCAM）でプログラミングされます。TCAM 出力検索は、IP 転送テーブル（Forwarding Information Base（FIB; 転送情報ベース））および NetFlow の検索が完了したあとで行われます。

各 QoS TCAM の検索結果により、ポリサー設定とポリシング カウンタを含む RAM へのインデックスが生成されます。追加 RAM には、microflow ポリサー設定が含まれ、microflow ポリシング カウンタは QoS ACL と一致する各 NetFlow エントリ内に維持されます。

入力および出力集約および microflow ポリシングの結果は統合されて最終ポリシング決定となります。不適合パケットは、ドロップするか、DSCP 内でマークダウンすることがきます。

MPLS ネットワークの入力エッジでの LER

（注）　着信ラベルには集約または非集約の 2 つのタイプがあります。集約ラベルの場合は、ネクスト ホップおよび発信インターフェイスを検出するときに、IP 検索を通して着信 MPLS または MPLS VPN パケットをスイッチングする必要があります。非集約ラベルの場合は、パケットに IP ネクスト ホップ情報が格納されます。

ここでは、MPLS ネットワークの入力側または出力側で、エッジ LER がどのように動作するかを説明します。

MPLS ネットワークの入力側では、LER がパケットを次のように処理します。

1. レイヤ 2 またはレイヤ 3 トラフィックはエッジ LER（PE1）で MPLS ネットワークのエッジに入ります。
2. PFC は、入力インターフェイスからトラフィックを受信し、802.1p ビットまたは IP ToS ビットを使用して EXP ビットを判別し、分類、マーキング、ポリシングを実行します。着信 IP パケットの分類については、入力サービス ポリシーもアクセス コントロール リスト（ACL）を使用することができます。
3. PFC は着信 IP パケットごとに IP アドレスの検索を行い、ネクストホップ ルータを決定します。
4. 適切なラベルがパケットにプッシュ（インポジション）され、QoS 決定の結果としての EXP 値はラベル ヘッダーの MPLS EXP フィールドにコピーされます。
5. PFC は、ラベル付きパケットを適切な処理用出力インターフェイスに転送します。
6. PFC はまた、802.1p ビットまたは IP ToS ビットを出力インターフェイスに転送します。
7. 出力インターフェイスでは、ラベル付きパケットはクラスごとに区別され、マーキングまたはポリシングが行われます。LAN インターフェイスについては、出力分類はまだ MPLS ではなく IP に基づいて行われています。

8. （EXP によってマーキングされた）ラベル付きパケットは、コア MPLS ネットワークに送信されます。

MPLS ネットワークのコアにある LSR

ここでは、MPLS ネットワーク コアで使用される LSR がパケットを処理する方法について説明します。

1. エッジ LER（または他のコア デバイス）からの着信 MPLS ラベル付きパケット（および 802.1p ビットまたは IP ToS ビット）がコア LSR に着信します。
2. PFC は、入力インターフェイスからトラフィックを受信し、EXP ビットを使用して、分類、マーキング、ポリシングを実行します。
3. PFC または DFC は、テーブルを検索してネクストホップ LSR を決定します。
4. 適切なラベルがパケットに配置（スワップ）され、MPLS EXP ビットがラベル ヘッダーにコピーされます。
5. PFC は、ラベル付きパケットを適切な処理用出力インターフェイスに転送します。
6. PFC はまた、802.1p ビットまたは IP ToS ビットを出力インターフェイスに転送します。
7. 送信パケットは、MPLS EXP フィールドによって区別され、マーキングまたはポリシングが行われます。
8. （EXP によってマーキングされた）ラベル付きパケットは、コア MPLS ネットワークの別の LSR または出力エッジの LER に送信されます。

（注）　パケットは MPLS パケットであるため、サービス プロバイダー ネットワーク内には、使用するキューイング アルゴリズム用の IP precedence フィールドはありません。パケットは、プロバイダー エッジ ルータである PE2 に着信するまで MPLS パケットのままです。

MPLS ネットワークの出力エッジでの LER

MPLS ネットワークの出力側では、LER がパケットを次のように処理します。

1. コア LSR からの MPLS ラベル付きパケット（および 802.1p ビットまたは IP ToS ビット）が MPLS ネットワーク バックボーンから接続される出力 LER（PE2）に着信します。
2. PFC は、パケットから MPLS ラベルをポップします（ディスポジション）。集約ラベルは、元の 802.1p ビットまたは IP ToS ビットを使用して分類されます。非集約ラベルは、デフォルトでは EXP 値で分類されます。
3. 集約ラベルの場合、PFC は IP アドレスの検索を行い、パケットの宛先を決定します。次に、PFC はパケット処理のため、パケットを適切な出力インターフェイスに転送します。非集約ラベルの場合、転送はラベルに基づいて行われます。デフォルトでは、非集約ラベルは出力 PE ルータではなく最後から 2 番めのホップ ルータでポップされます。
4. PFC はまた、802.1p ビットまたは IP ToS ビットを出力インターフェイスに転送します。
5. パケットは、802.1p ビットまたは IP ToS ビットに従って区別され、それに従って処理されます。

（注）　MPLS EXP ビットを使用すると、MPLS パケットの QoS を指定することができます。IP precedence および DSCP ビットを使用すると、IP パケットの QoS を指定することができます。

EoMPLS エッジの LER

ここでは、LER で機能する Ethernet over MPLS（EoMPLS）QoS の概要を説明します。EoMPLS QoS サポートは、IP-to-MPLS QoS に似ています。

- EoMPLS では、ポートが untrusted の場合、CoS の信頼状態は自動的に VC タイプ 5（ポート モード）ではなく、VC タイプ 4（VLAN モード）に設定されます。これは、トンネル上での 802.1q CoS 保存機能に似ています。
- トンネル入力で受信されたパケットは、EoMPLS インターフェイスでは untrusted として扱われます。ただし、trust CoS が入力ポートで自動的に設定され、ポリシー マーキングが適用されない VC タイプ 4 は例外です。
- 入力ポートが trusted として設定された場合、EoMPLS インターフェイスで受信されたパケットは元の IP パケット ヘッダーの QoS ポリシーによってマーキングされません（IP ポリシーによるマーキングは信頼できないポートで機能します）。
- 802.1p CoS が 802.1q ヘッダーを介して利用可能な場合、802.1p CoS は入口から出口まで保持されます。
- トンネル出口から先では、1p タグが EoMPLS ヘッダー（VC タイプ 4）でトンネリングされている場合には、キューイングは保持された 802.1p CoS に基づいて行われます。それ以外の場合には、キューイングは QoS 決定から導出された CoS に基づいて行われます。

IP エッジ（MPLS、MPLS VPN）での LER

ここでは、MPLS および MPLS VPN ネットワークの入力（CE-to-PE）および出力（PE-to-CE）エッジでの LER の QoS 機能について説明します。MPLS と MPLS VPN のどちらも一般 MPLS QoS 機能をサポートします。追加的な MPLS VPN 特定 QoS については「MPLS VPN」（P.67-11）を参照してください。

IP to MPLS

IP to MPLS の概要

PFC は IP-to-MPLS エッジで次の MPLS QoS 機能を提供します。

- **platform qos trust** コマンドまたは **policy-map** コマンドに基づく EXP 値の割り当て
- ポリシーを利用した EXP 値のマーキング
- ポリシーを利用したトラフィックのポリシング

ここでは、IP-to-MPLS エッジで PFC がサポートする MPLS QoS 分類に関する情報を提供します。さらに、入力および出力インターフェイス モジュールによって提供される機能についても説明します。Ethernet to MPLS では、入力インターフェイス、MPLS QoS、出力インターフェイスの各機能は、IP to MPLS における該当機能と類似しています。

IP-to-MPLS 分類

PFC の IP トラフィック用入力および出力ポリシーでは、IP precedence、IP DSCP、IP ACL の **match** コマンドを使用して元の受信 IP でトラフィックが分類されます。出力ポリシーでは、トラフィックはインポーズされた EXP 値や入力ポリシーによって行われたマーキングに基づいて分類されません。

PFC はポートの信頼および QoS ポリシーを適用したあと、内部 DSCP を割り当てます。次に PFC は、インポーズしたラベルに内部 DSCP-to-EXP グローバル マップに基づいて EXP 値を割り当てます。複数のラベルがインポーズされている場合、EXP 値は各ラベルとも同じです。MPLS ラベルがインポーズされている場合、PFC は元の IP ToS を保持します。

PFC は、内部 DSCP-to-CoS グローバル マップに基づいて出力 CoS を割り当てます。デフォルトの内部 DSCP-to-EXP マップおよび内部 DSCP-to-CoS マップが整合している場合、出力 CoS はインポーズされた EXP と同じ値を持ちます。

入力ポートが IP-to-IP および IP-to-MPLS トラフィックの両方を受信した場合、分類を使用してこの 2 つのタイプのトラフィックを分離する必要があります。たとえば、IP-to-IP および IP-to-MPLS トラフィックの宛先アドレス範囲が異なっている場合、宛先アドレスに基づいてトラフィックを分類し、次に IP ToS ポリシーを IP-to-IP トラフィックに適用し、（インポーズされた MPLS ヘッダーに EXP 値をマーキングまたは設定する）ポリシーを IP-to-MPLS トラフィックに適用することができます。次の 2 つの例を参照してください。

- IP ToS をマーキングする PFC ポリシーによって内部 DSCP を設定：このポリシーがトラフィックすべてに適用された場合は、IP-to-IP トラフィックでは出力ポートによって、出力パケット内の CoS（内部 DSCP から作成）が IP ToS バイトに書き換えられます。IP-to-MPLS トラフィックでは、PFC は、内部 DSCP をインポーズされた EXP 値にマッピングします。
- MPLS EXP をマーキングする PFC ポリシーによって内部 DSCP を設定：このポリシーがトラフィックすべてに適用された場合は、IP-to-IP トラフィックでは出力ポートによって、入力 IP ポリシー（または trust）に従って IP ToS が書き換えられます。CoS は ToS からマッピングされます。IP-to-MPLS トラフィックでは、PFC は、内部 DSCP をインポーズされた EXP 値にマッピングします。

IP-to-MPLS モード MPLS QoS の分類

MPLS QoS は、PE1 への入力時に以下をサポートします。

- IP precedence 値または DSCP 値に基づくマッチング、またはアクセス グループによるフィルタリング
- **set mpls experimental imposition** および **police** コマンド

MPLS QoS は、PE1 からの出力時に **mpls experimental topmost** コマンドをサポートします。

IP-to-MPLS 入力ポートでの分類

IP-to-MPLS の分類は、IP-to-IP と同じです。LAN ポートでの分類は、受信レイヤ 2 802.1Q CoS 値に基づいて行われます。

IP-to-MPLS 出力ポートでの分類

LAN ポートでの分類は、受信した EXP 値に基づいて行われます。出力 CoS 値は、その値からマッピングされます。

出力ポートがトランクの場合は、LAN ポートは出力 CoS を出力 802.1Q フィールドにコピーします。

MPLS to IP

MPLS to IP への概要

MPLS QoS は、MPLS-to-IP エッジで次の機能をサポートします。

- 出力インターフェイスに従い MPLS ドメインからの送信時に EXP 値を IP DSCP に伝播するオプション
- MPLS-to-IP 出力インターフェイスで IP サービス ポリシーを使用するオプション

ここでは、MPLS-to-IP MPLS QoS 分類について説明します。さらに、入力および出力モジュールによって提供される機能についても説明します。

MPLS to Ethernet の場合、入力インターフェイス、MPLS QoS、出力インターフェイスの各機能は、MPLS to IP における該当機能と類似しています。ただし、EoMPLS カプセル開放では、出力 IP ポリシーを適用できません（パケットは MPLS としてだけ分類できます）。

MPLS-to-IP 分類

PFC は QoS の結果に基づき、内部 DSCP（PFC が各フレームに割り当てる内部プライオリティ）を割り当てます。QoS 結果は次の影響を受けます。

- デフォルトの信頼 EXP 値
- ラベル タイプ（プレフィックス単位または集約）
- VPN の数
- 明示的 NULL の使用
- QoS ポリシー

次のような 3 つの異なった分類モードがあります。

- 正規 MPLS 分類 : 非集約ラベルについては、MPLS の再循環がないため、PFC は MPLS EXP 入力または出力ポリシーに基づいてパケットを分類します。PFC は EXP/DSCP/CoS マッピングから作成した CoS に基づき、パケットをキューイングします。この基になる IP DSCP は、出力カプセル開放後保持されるか、（EXP-to-DSCP マップを介して）EXP から上書きされます。
- VPN CAM 内の集約ラベルの一致による IP 分類 : PFC は、次のいずれかを行います。
  - 基礎となる IP ToS を保存
  - EXP-to-DSCP グローバル マップから導出された値によって IP ToS を書き換え
  - IP ToS を、出力 IP ポリシーから導出された値 に変更

  どの場合も、出力キューイングは DSCP-to-CoS マップから導出された最終 IP ToS に基づいています。

- VPN CAM にない集約ラベルでの IP 分類：再循環のあと、PFC は MPLS カプセル開放隣接で指定された入力予約 VLAN に基づき MPLS-to-IP パケットを正規 IP-to-IP パケットと区別します。予約された VLAN は VPN および非 VPN の両方について VRF に従い割り当てられます。再循環後の入力 ToS は元の IP ToS 値でも、元の EXP 値から導出したものでもかまいません。出力 IP ポリシーはこの入力 ToS を任意の値に上書きすることができます。

（注）　再循環の詳細については、「再循環」（P.36-5）を参照してください。

PE-to-CE 入力上の着信 MPLS パケットの場合、PFC では MPLS 分類だけがサポートされます。入力 IP ポリシーはサポートされません。MPLS コアからの PE-to-CE トラフィックは出力時に IP として分類またはポリシングされます。

MPLS-to-IP MPLS QoS の分類

MPLS QoS は、PE2 への入力時に、EXP 値の照合および **police** コマンドをサポートします。

MPLS QoS は、PE2 からの出力時に、IP precedence または DSCP 値の照合、またはアクセス グループと **police** コマンドによるフィルタリングをサポートします。

MPLS-to-IP 入力ポートでの分類

LAN ポートでの分類は、EXP 値に基づきます。**match mpls experimental** コマンドは受信最上位ラベルの EXP 値のマッチングを行います。

MPLS-to-IP 出力ポートでの分類

MPLS-to-IP の分類は、IP-to-IP と同じです。

LAN インターフェイス分類は出力 CoS に基づきます。

出力ポートがトランクの場合は、LAN ポートは出力 CoS を出力 802.1Q フィールドにコピーします。

（注）　MPLS to IP については、出力インターフェイスの MPLS IP（またはタグ IP）がイネーブルの場合は出力 IP ACL または QoS は出力インターフェイスでは有効ではありません。例外は VPN CAM ヒットです。この場合パケットは出力では IP として分類されます。

MPLS VPN

MPLS VPN では次の PE MPLS QoS 機能がサポートされます。

- VPN サブインターフェイスを介した CE-to-PE IP トラフィックの分類、ポリシング、マーキング
- VPN 単位の QoS（ポート単位、VLAN 単位、またはサブインターフェイス単位）

カスタマー エッジ（CE）-to-PE トラフィック、または CE-to-PE-to-CE トラフィックでは、サブインターフェイス サポートにより IP QoS 入力または出力ポリシーをサブインターフェイスおよび物理インターフェイスに適用することができます。CE 側のある VPN に対応する特定のインターフェイスまたはサブインターフェイスでは VPN 単位のポリシングも提供されます。

複数のインターフェイスが同じ VPN に属する状況では、同じ PFC に関連付けられた類似インターフェイスすべてに対し、入力または出力サービス ポリシー内で同一の共有ポリサーを使用することで、VPN 単位のポリシング集約を実行できます。

集約 VPN ラベルについては、再循環の場合の EXP 伝播はサポートされない可能性があります。これは、最終パケットがどの出力インターフェイスを使用するのかということを、MPLS 隣接が認識していないためです。

（注）　再循環については、「再循環」（P.36-5）を参照してください。

VPN 内のすべてのインターフェイスが EXP 伝播をイネーブルにしている場合、PFC は EXP 値を伝播します。

次の PE MPLS QoS 機能がサポートされています。

- IP パケット用の一般的な MPLS QoS 機能
- VPN サブインターフェイスを介した CE-to-PE IP トラフィックの分類、ポリシング、マーキング
- VPN 単位の QoS（ポート単位、VLAN 単位、またはサブインターフェイス単位）

MPLS コアでの LSR

ここでは、MPLS および MPLS VPN ネットワークのコア（MPLS-to-MPLS）での LSR の MPLS QoS 機能について説明します。Carrier Supporting Carrier（CsC）QoS 機能の入力機能、出力インターフェイス、および PFC の機能は、次の項で説明する MPLS to MPLS のものと同じです。CsC と MPLS to MPLS の相違は、CsC ラベルが MPLS ドメイン内部にインポーズできることです。

MPLS to MPLS

MPLS to MPLS の概要

MPLS コアでの MPLS QoS は、次の機能をサポートします。

- サービス ポリシーに基づく EXP 単位のポリシング
- 入力最上位 EXP 値を新たにインポーズされた EXP 値へのコピーすること
- MPLS ドメイン間の出力境界での EXP 変換オプション（隣り合った 2 つの MPLS ドメイン間でインターフェイス エッジ上の EXP 値を変更）
- 特定の EXP 値について個々のラベル フローに基づくマルチフロー ポリシング
- 最上位ラベルをマルチラベル スタックからポップする場合に最上位 EXP 値を基礎となる EXP 値へ伝播するオプション

ここでは、MPLS-to-MPLS QoS 分類に関する情報を提供します。さらに、入力および出力モジュールによって提供される機能についても説明します。

MPLS-to-MPLS 分類

PFC は、受信 MPLS パケットについてポート信頼状態、入力 CoS、およびあらゆる policy-map **trust** コマンドを無視します。その代わり、PFC は最上位ラベルの EXP 値を信頼します。

（注）　**match mpls experimental** コマンドを入力すると、MPLS トラフィックに対する MPLS QoS 入力ポリシーおよび出力ポリシーは、受信した最上位ラベルの EXP 値に基づきトラフィックを分類します。

MPLS QoS は、EXP-to-DSCP グローバル マップを使用して、EXP 値を内部 DSCP にマッピングします。 PFC の次の手順は、ラベルをスワッピングしているのか、新しいラベルをインポーズしているのか、それともラベルをポップしているのかによって異なります。

- ラベルのスワップ：ラベルをスワップする場合、PFC は受信した最上位ラベルの EXP 値を保持し、発信する最上位ラベルの EXP 値にこの値をコピーします。PFC は、内部 DSCP-to-CoS グローバル マップを使用して出力 CoS を割り当てます。DSCP グローバル マップが整合している場合は、出力 CoS は送信最上位ラベルの EXP に基づきます。

  PFC は、**police** コマンドの **exceed** および **violate** アクションを使用して、アウトオブプロファイル トラフィックをマークダウンできます。適合するトラフィックはマーキングしないため、**conform** アクションは transmitted である必要があり、**set** コマンドを使用することはできません。PFC がマークダウンを実行している場合、内部 DSCP は内部 DSCP マークダウン マップへのインデックスとして使用されます。PFC は、内部 DSCP-to-EXP グローバル マップを使用して内部 DSCP マークダウンの結果を EXP 値にマッピングします。PFC は新しい EXP 値を最上位送信ラベルに書き換え、新しい EXP 値をスタックの他のラベルにはコピーしません。PFC は、内部 DSCP-to-CoS グローバル マップを使用して出力 CoS を割り当てます。DSCP マップが整合している場合は、出力 CoS は送信最上位ラベルの EXP 値に基づきます。

- 追加ラベルのインポーズ：新しいラベルを既存のラベル スタックにインポーズする場合、PFC は内部 DSCP-to-EXP マップを使用して内部 DSCP をインポーズされたラベルの EXP 値にマッピングします。そして次にインポーズされたラベルの EXP 値を基礎となるスワップされたラベルにコピーします。PFC は、内部 DSCP-to-CoS グローバル マップを使用して出力 CoS を割り当てます。DSCP マップが整合している場合は、出力 CoS はインポーズされたラベルの EXP 値に基づきます。

  PFC は適合するトラフィックをマーキングし、アウトオブプロファイル トラフィックをマークダウンすることができます。PFC は、内部 DSCP をマーキングしたあと、内部 DSCP-to-EXP グローバル マップを使用して内部 DSCP を新しくインポーズされたラベルの EXP 値にマッピングします。そして PFC は、インポーズされたラベルの EXP 値を基礎となるスワップされたラベルにコピーします。PFC は、内部 DSCP-to-CoS グローバル マップを使用して出力 CoS を割り当てます。したがって、出力 CoS はインポーズされたラベルの EXP 値に基づきます。

- ラベルのポップ：ラベルをマルチラベル スタックからポップする場合、PFC はエクスポーズされたラベルの EXP 値を保持します。PFC は、内部 DSCP-to-CoS グローバル マップを使用して出力 CoS を割り当てます。DSCP マップが整合している場合は、出力 CoS はポップされたラベルの EXP 値に基づきます。

- EXP 伝播が出力インターフェイスで設定されている場合、PFC は DSCP-to-EXP グローバル マップを使用して、エクスポーズされたラベルの EXP 値に内部 DSCP をマッピングします。PFC は、内部 DSCP-to-CoS グローバル マップを使用して出力 CoS を割り当てます。DSCP マップが整合している場合は、出力 CoS はエクスポーズされたラベルの EXP 値に基づきます。

MPLS-to-MPLS QoS の分類

P1 または P2 への入力時に、MPLS QoS は次の機能をサポートします。

- **mpls experimental topmost** コマンドによるマッチング
- **set mpls experimental imposition**、**police**、**set imposition** を併用する **police** コマンド

MPLS QoS は、P1 または P2 からの出力時に **mpls experimental topmost** コマンドによる照合をサポートします。

MPLS-to-MPLS 入力ポートでの分類

LAN ポートでの分類は、PFC からの出力 CoS に基づきます。**match mpls experimental** コマンドは受信最上位ラベルの EXP 値のマッチングを行います。

MPLS-to-MPLS 出力ポートでの分類

LAN ポートでの分類は、PFC からの出力 CoS 値に基づきます。**match mpls experimental** コマンドは出力 CoS のマッチングを行いますが、最上位ラベルの EXP 値のマッチングは行いません。出力ポートがトランクの場合は、LAN ポートは出力 CoS を出力 802.1Q フィールドにコピーします。

MPLS QoS のデフォルト設定

機能	デフォルト値
PFC QoS のグローバル イネーブル ステート	デフォルト値の他のすべての PFC QoS パラメータによって、デフォルト EXP は IP precedence からマッピングされます。 PFC QoS がイネーブルで、他のすべての PFC QoS パラメータがデフォルト値の場合、PFC QoS は LAN ポート（デフォルトは untrusted）から送信されたすべてのトラフィックでレイヤ 3 DSCP を 0（**untrusted** ポートに限る）に、レイヤ 2 CoS を 0、インポーズされた EXP を 0 に設定します。trust CoS では、デフォルトの EXP 値が COS からマッピングされます。trust DSCP では、デフォルトの EXP 値が IP precedence からマッピングされます。
PFC QoS ポート イネーブル ステート	PFC QoS がグローバルにイネーブルの場合、イネーブル
ポートの CoS 値	0
マイクロフロー ポリシング	イネーブル
VLAN 内マイクロフロー ポリシング	ディセーブル
ポートベースまたは VLAN ベースの PFC QoS	ポートベース
EXP から DSCP へのマップ（EXP 値から設定された DSCP）	EXP 0 = DSCP 0 EXP 1 = DSCP 8 EXP 2 = DSCP 16 EXP 3 = DSCP 24 EXP 4 = DSCP 32 EXP 5 = DSCP 40 EXP 6 = DSCP 48 EXP 7 = DSCP 56
IP precedence から DSCP へのマップ（IP precedence 値から設定された DSCP）	IP precedence 0 = DSCP 0 IP precedence 1 = DSCP 8 IP precedence 2 = DSCP 16 IP precedence 3 = DSCP 24 IP precedence 4 = DSCP 32 IP precedence 5 = DSCP 40 IP precedence 6 = DSCP 48 IP precedence 7 = DSCP 56

機能	デフォルト値
DSCP から EXP へのマップ（DSCP 値から設定された EXP）	DSCP　0–7　= EXP 0 DSCP　8–15 = EXP 1 DSCP 16–23 = EXP 2 DSCP 24–31 = EXP 3 DSCP 32–39 = EXP 4 DSCP 40–47 = EXP 5 DSCP 48–55 = EXP 6 DSCP 56–63 = EXP 7
DSCP マップからマークダウンされた DSCP	マークダウンされた DSCP 値は元の DSCP 値と等しい（マークダウンなし）
EXP 変換マップ	デフォルトでは変換マップなし
ポリサー	なし
ポリシー マップ	なし
NetFlow テーブルの MPLS フロー マスク	ラベル ＋ EXP 値
MPLS コア QoS	MPLS コア QoS では 4 つの可能性があります。 • スワッピング：着信 EXP フィールドが送信 EXP フィールドにコピーされます。 • スワッピング ＋ インポーズ：着信 EXP フィールドはスワッピングされた EXP フィールドとインポーズされた EXP フィールドの両方にコピーされます。 （注）　EXP フィールドのセット付きサービス ポリシーがある場合、その EXP フィールドはインポーズされたラベルとスワッピングされたラベルに置かれます。 • 最上位ラベルのディスポジション：エクスポーズされた EXP フィールドは保持されます。 • ラベルだけのディスポジション：エクスポーズされた IP DSCP は保持されます。
MPLS to IP エッジの QoS	エクスポーズされた IP DSCP を保持します。

MPLS QoS コマンド

MPLS QoS は、次の MPLS QoS コマンドをサポートします。

- **match mpls experimental topmost**
- **set mpls experimental imposition**
- **police**
- **platform qos map exp-dscp**
- **platform qos map dscp-exp**
- **platform qos map exp-mutation**
- **platform qos exp-mutation**

- **show platform qos mpls**
- **no platform qos mpls trust exp**

（注）　サポートされる非 MPLS QoS コマンドについては、第 61 章「PFC QoS の概要」を参照してください。

次のコマンドはサポートされません。

- **set qos-group**
- **set discard-class**

MPLS QoS の制約事項

MPLS QoS を設定する際に、以下の注意事項と制約事項に従ってください。

- 受信パケットが IP パケットの場合の IP-to-MPLS または EoMPLS のインポジション
  - QoS がディセーブルの場合、EXP 値は受信 IP ToS に基づきます。
  - QoS がキューイングだけの場合、EXP 値は受信 IP ToS に基づきます。
- 受信パケットが非 IP パケットの場合の EoMPLS インポジション
  - QoS がディセーブルの場合、EXP 値は入力 CoS に基づきます。
  - QoS がキューイングだけの場合、EXP 値は受信 IP ToS に基づきます。
- MPLS-to-MPLS 動作
  - QoS がディセーブルのときにスワッピングする場合、EXP 値は元の EXP 値に基づきます（EXP 変換がない場合）。
  - QoS がキューイングだけのときにスワッピングする場合、EXP 値は元の EXP 値に基づきます（EXP 変換がない場合）。
  - QoS がディセーブルのときに追加ラベルをインポーズする場合、EXP 値は元の EXP 値に基づきます（EXP 変換がない場合）。
  - QoS がキューイングだけのときに追加ラベルをインポーズする場合、EXP 値は元の EXP 値に基づきます（EXP 変換がない場合）。
  - QoS がディセーブルのときに 1 つのラベルをポップする場合、EXP 値は基礎となる EXP 値に基づきます。
  - QoS がキューイングだけのときに 1 つのラベルをポップする場合、EXP 値は基礎となる EXP 値に基づきます。
- EXP 値は MPLS-to-IP ディスポジションとは関係がありません。
- **no platform qos rewrite ip dscp** コマンドは、MPLS とは非互換です。デフォルトの **platform qos rewrite ip dscp** コマンドは、PFC がインポーズしたラベルで正しい EXP 値を割り当てられるようイネーブルの状態にしておく必要があります。
- **no platform qos mpls trust exp** コマンドを使用すると、CoS および出力キューイングの目的で、MPLS パケットをレイヤ 2 パケットと同様に扱うことができます。この場合、デフォルトの EXP 値ではなく、ポートの信頼状態またはポリシーの信頼状態が適用されます。

MPLS QoS の設定方法

queueing-only モードのイネーブル化

queueing-only モ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	`Router(config)# platform qos queueing-only`	queueing-only モードをイネーブルにします。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

queueing-only モードをイネーブルにする場合、ルータは次の処理を行います。

- マーキングおよびポリシングをグローバルにディセーブルにします。
- すべてのポートがレイヤ 2 CoS を信頼するように設定します。

（注）　スイッチでは、タグなし入力トラフィックと、trust CoS に設定できないポートを介して受信されるトラフィックにポート CoS 値が適用されます。

次に、queueing-only モードをイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# platform qos queueing-only
Router(config)# end
Router#
```

制約事項および使用上の注意事項

PFC で QoS がディセーブル（**no platform qos**）の場合、EXP 値は次のように決定されます。

- 受信パケットが IP パケットのときの IP-to-MPLS または EoMPLS インポジションの場合、QoS がキューイングのみであれば（**platform qos queueing-only**）、EXP 値は受信した IP ToS に基づきます。
- 受信パケットが IP パケットでない EoMPLS インポジションの場合、QoS がキューイングのみであれば、EXP 値は受信した IP ToS に基づきます。
- MPLS-to-MPLS 動作
  - QoS がキューイングだけのときにスワッピングする場合、EXP 値は元の EXP 値に基づきます（EXP 変換がない場合）。
  - QoS がキューイングだけのときに追加ラベルをインポーズする場合、EXP 値は元の EXP 値に基づきます（EXP 変換がない場合）。

  - QoS がキューイングだけのときに 1 つのラベルをポップする場合、EXP 値は基礎となる EXP 値に基づきます。
- EXP 値は MPLS-to-IP ディスポジションとは関係がありません。

MPLS パケットを分類するためのクラス マップの設定

match mpls experimental topmost コマンドを使用して、パケット EXP 値による MPLS ドメイン内のトラフィック クラスを定義することができます。これにより、**police** コマンドを使用してインターフェイス ベースで EXP トラフィックをポリシングするためのサービス ポリシーを定義することができます。

クラス マップを設定するには、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
ステップ 1	`Router(config)# class-map` *class_name*	パケットがマッチングされるクラス マップを指定します。
ステップ 2	`Router(config-cmap)# match mpls experimental topmost` *value*	そのクラスにマッチングされるパケット特性を指定します。
ステップ 3	`Router(config-cmap)# 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。

次に、MPLS EXP 値 3 を含むすべてのパケットが exp3 という名前のトラフィック クラスによってマッチングされる例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# class-map exp3
Router(config-cmap)# match mpls experimental topmost 3
Router(config-cmap)# exit
Router(config)# policy-map exp3
Router(config-pmap)# class exp3
Router(config-pmap-c)# police 1000000 8000000 conform-action transmit exceed-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# end
Router# show class exp3
 Class Map match-all exp3 (id 61)
   Match mpls experimental topmost 3
Router# show policy-map exp3
  Policy Map exp3
    Class exp3
     police cir 1000000 bc 8000000 be 8000000 conform-action transmit exceed-action drop
Router# show running-config interface gigabitethernet 3/27
Building configuration...

Current configuration : 173 bytes
!
interface GigabitEthernet3/27
  ip address 47.0.0.1 255.0.0.0
  tag-switching ip
 end

Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 3/27
Router(config-if)# service-policy input exp3
Router(config-if)#
```

```
Router#
Enter configuration commands, one per line.  End with CNTL/Z.
Router# show running-config interface gigabitethernet 3/27
Building configuration...

Current configuration : 173 bytes
!
interface GigabitEthernet3/27
  ip address 47.0.0.1 255.0.0.0
  tag-switching ip
  service-policy input exp3
 end

Router#
1w4d: %SYS-5-CONFIG_I: Configured from console by console
Router# show platform qos mpls
 QoS Summary [MPLS]:      (* - shared aggregates, Mod - switch module)

      Int Mod Dir  Class-map DSCP  Agg  Trust Fl   AgForward-By   AgPoliced-By
                                   Id         Id
-------------------------------------------------------------------------------
    Gi3/27  5  In       exp3    0    2   dscp  0              0              0

       All  5   -    Default    0    0*    No  0     3466140423              0
Router# show policy-map interface gigabitethernet 3/27
 GigabitEthernet3/27

  Service-policy input: exp3

    class-map: exp3 (match-all)
      Match: mpls experimental topmost 3
      police :
        1000000 bps 8000000 limit 8000000 extended limit
      Earl in slot 5 :
        0 bytes
        5 minute offered rate 0 bps
        aggregate-forwarded 0 bytes action: transmit
        exceeded 0 bytes action: drop
        aggregate-forward 0 bps exceed 0 bps

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any

Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 3/27
Router(config-if)# service-policy output ip2tag
Router(config-if)# end
Router# show platform qos ip
 QoS Summary [IPv4]:      (* - shared aggregates, Mod - switch module)

      Int Mod Dir  Class-map DSCP  Agg  Trust Fl   AgForward-By   AgPoliced-By
                                   Id         Id
-------------------------------------------------------------------------------
     Vl300  5  In          x   44    1     No  0              0              0
    Gi3/27  5 Out      iptcp   24    2     --  0              0              0

       All  5   -    Default    0    0*    No  0     3466610741              0
```

制約事項および使用上の注意事項

- **match mpls experimental** コマンドは、パケットがクラス マップによって指定されるクラスに属しているかどうかを判別するためにパケットをチェックする一致基準として使用すべき EXP フィールド値の名前を指定します。
- **match mpls experimental** コマンドを使用するには、まず **class-map** コマンドを入力して設定する一致基準のクラスの名前を指定する必要があります。クラスを識別したあとで、**match mpls experimental** コマンドを使用してその一致基準を設定できます。
- クラス マップで複数のコマンドを指定する場合、最後に入力されたコマンドだけが適用されます。最後のコマンドは、それ以前に入力されたコマンドを無効にします。

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、ポリシー マップ コマンドがそれぞれ異なる 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 タイプ用の全コマンドを、同一のポリシー マップ クラスに入れます。MPLS QoS は、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。

EXP 値をすべてのインポーズされたラベルに設定するためのポリシー マップの設定

MPLS EXP フィールドの値をすべてのインポーズされたラベル エントリに設定するには、QoS 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 **set mpls experimental imposition** コマンドを使用します。設定をディセーブルにするには、コマンドの **no** 形式を入力します。

（注）　**set mpls experimental imposition** コマンドは、**set mpls experimental** コマンドと置き換わったものです。

	コマンド	目的
ステップ 1	`Router(config)# policy-map policy_name`	ポリシー マップを作成します。
ステップ 2	`Router(config-pmap)# class-map name [match-all | match-any]`	QoS クラス マップ コンフィギュレーション モードにアクセスして QoS クラス マップを設定します。
ステップ 3	`Router(config-pmap-c)# set mpls experimental imposition {mpls-exp-value | from-field [table table-map-name]}`	MPLS 実験（EXP）フィールドの値をすべてのインポーズされたラベル エントリに設定します。
ステップ 4	`Router(config-pmap-c)# 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。

次に、MPLS EXP 値 3 で定義された DSCP 値に従って、MPLS EXP インポジション値を設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# access-l 101 p tcp any any
Router(config)# class-map iptcp
```

```
Router(config-cmap)# match acc 101
Router(config-cmap)# exit
Router(config)#
Router(config-cmap)# policy-map ip2tag
Router(config-pmap)# class iptcp
Router(config-pmap-c)# set mpls exp imposition 3
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)#
Router#
1w4d: %SYS-5-CONFIG_I: Configured from console by console
Router#
Router# show policy-map ip2tag
  Policy Map ip2tag
    Class iptcp
      set mpls experimental imposition 3
Router# show class iptcp
 Class Map match-all iptcp (id 62)
   Match access-group101

Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 3/27
Router(config-if)# ser in ip2tag
Router(config-if)#
Routers
1w4d: %SYS-5-CONFIG_I: Configured from console by console
Router# show pol ip2tag
  Policy Map ip2tag
    Class iptcp
      set mpls experimental imposition 3
Router# show class-map iptcp
 Class Map match-all iptcp (id 62)
   Match access-group  101

Router# show access-l 101
Extended IP access list 101
    10 permit tcp any any
Router# show policy-map interface gigabitethernet 3/27
 GigabitEthernet3/27

  Service-policy input: ip2tag

    class-map: iptcp (match-all)
      Match: access-group 101
      set mpls experimental 3:
      Earl in slot 5 :
        0 bytes
        5 minute offered rate 0 bps
        aggregate-forwarded 0 bytes

    class-map: class-default (match-any)
      Match: any

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

次に、設定を確認する例を示します。

```
Router# show policy map ip2tag
  Policy Map ip2tag
    Class iptcp
      set mpls experimental imposition 3
```

EXP 値のインポジションに関する注意事項および制約事項

インポーズしたすべてのラベルに EXP 値を設定する場合、次の注意事項および制約事項に従ってください。

- ラベル インポジション中には **set mpls experimental imposition** コマンドを使用してください。このコマンドは MPLS EXP フィールドをすべてのインポーズされたラベル エントリに設定します。
- **set mpls experimental imposition** コマンドは、入力インターフェイス（インポジション）上でのみサポートされます。
- **set mpls experimental imposition** コマンドは、EXP 値を直接マーキングしません。その代わり、このコマンドは内部 DSCP-to-EXP グローバル マップを介して EXP にマッピングされる内部 DSCP をマーキングします。
- （元の受信 IP ヘッダーに基づく）分類および（内部 DSCP に行われる）マーキングでは IP-to-IP トラフィックと IP-to-MPLS トラフィックが区別されないことに十分注意してください。IP ToS および EXP のマーキングに使用されるコマンドを使用した場合、内部 DSCP のマーキングと同じ結果となります。
- ラベル インポジション中に、プッシュされたラベル エントリ値をデフォルト値とは異なった値に設定するには、**set mpls experimental imposition** コマンドを使用します。
- また任意で IP precedence、DSCP フィールド、または QoS IP ACL とともに **set mpls experimental imposition** コマンドを利用して、すべてのインポーズされたラベル エントリに MPLS EXP フィールドの値を設定できます。
- ラベルを PFC で受信 IP トラフィックにインポーズする場合は、**set mpls experimental imposition** コマンドで EXP フィールドをマーキングすることができます。

police コマンドを使用したポリシー マップの設定

ポリシングは特定のトラフィック クラスを特定のレートに速度制限する機能を提供する PFC のハードウェアの機能です。PFC は集約ポリシングおよびマイクロフロー ポリシングをサポートします。

集約ポリシングは、送信元、宛先、プロトコル、送信元ポート、宛先ポートが異なっていても関係なくポートに着信するすべてのトラフィックを測定します。マイクロフロー ポリシングは、フロー ベース（送信元、宛先、プロトコル、送信元ポート、宛先ポート ベース）でポートに着信するすべてのトラフィックを測定します。集約ポリシングとマイクロフロー ポリシングの詳細については、第 63 章「分類、マーキング、およびポリシング」を参照してください。

	コマンド	目的
ステップ 1	`Router(config)# policy-map policy_name`	ポリシー マップを作成します。
ステップ 2	`Router(config-pmap)# class-map name [match-all | match-any]`	QoS クラス マップ コンフィギュレーション モードにアクセスして QoS クラス マップを設定します。
ステップ 3	`Router(config-pmap-c)# police {aggregate name}`	クラスを共有集約ポリサーに追加します。
ステップ 4	`Router(config-pmap-c)# police bps burst_normal burst_max conform-action action exceed-action action violate-action action`	per-class-per-interface ポリサーを作成します。

	コマンド	目的
ステップ 5	Router(config-pmap-c)# **police flow** {*bps* [*burst_normal*] | [**conform-action** *action*] [**exceed-action** *action*]	入力フロー ポリサーを作成します （出力ポリシーではサポートされません）。
ステップ 6	Router(config-pmap-c)# **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。

次に、ポリサーでポリシー マップを作成する例を示します。

```
Router(config)# policy-map ip2tag
Router(config-pmap)# class iptcp
Router(config-pmap-c)# no set mpls exp topmost 3
Router(config-pmap-c)# police 1000000 1000000 c set-mpls-exp?
set-mpls-exp-imposition-transmit

Router(config-pmap-c)# police 1000000 1000000 c set-mpls-exp-imposit 3 e d
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface gigabitethernet 3/27
Router(config-if)# ser in ip2tag
Router(config-if)#
```

次に、設定を確認する例を示します。

```
Router# show pol ip2tag
  Policy Map ip2tag
    Class iptcp
     police cir 1000000 bc 1000000 be 1000000 conform-action
set-mpls-exp-imposition-transmit 3 exceed-action drop
Router# show running-config interface gigabitethernet 3/27
Building configuration...

Current configuration : 202 bytes
!
interface GigabitEthernet3/27
  logging event link-status
  service-policy input ip2tag
end

Router# show policy interface gigabitethernet 3/27
 GigabitEthernet3/27

  Service-policy input: ip2tag

    class-map: iptcp (match-all)
      Match: access-group 101
      police :
        1000000 bps 1000000 limit 1000000 extended limit
      Earl in slot 5 :
        0 bytes
        5 minute offered rate 0 bps
        aggregate-forwarded 0 bytes action: set-mpls-exp-imposition-transmit
        exceeded 0 bytes action: drop
        aggregate-forward 0 bps exceed 0 bps

    class-map: class-default (match-any)
      Match: any

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

制約事項および使用上の注意事項

police コマンドを使用してポリシー マップを設定するときには、次の制約事項および注意事項が適用されます。

- MPLS では、**exceed-action** *action* コマンドおよび **violate-action** *action* コマンドが IP 使用と同様に動作します。パケットはドロップされる場合もあり、EXP 値がマークダウンされる場合もあります。
- MPLS では、**set-dscp transmit** *action* コマンドおよび **set-prec-transmit** *action* コマンドがキューイングに影響を与える CoS ビットにマッピングされる内部 DSCP を設定します。ただし、インポジションを除き EXP 値の変更は行いません。
- 受信 MPLS トラフィックのラベルを PFC でスワッピングするときは、**police** コマンドの **exceed-action policed-dscp-transmit** および **violate-action policed-dscp-transmit** キーワードを使用して、アウトオブプロファイル トラフィックをマークダウンすることができます。PFC では適合するトラフィックはマーキングされません。アウトオブプロファイル トラフィックをマークダウンする場合は、PFC は送信最上位ラベルをマーキングします。PFC はマーク ダウンをラベル スタックに伝播しません。
- MPLS では、フロー キーはラベルおよび EXP 値に基づきます。フローマスク オプションはありません。それ以外では、フロー キー動作は IP-to-IP と同様です。
- **police** コマンドを使用すれば、ラベル インポジション中に、プッシュされたラベル エントリ値をデフォルト値とは異なった値に設定できます。
- ラベルを PFC で受信 IP トラフィックにインポーズする場合は、**conform-action set-mpls-exp-imposition-transmit** キーワードを使用して、EXP フィールドをマーキングすることができます。
- IP-to-MPLS インポジション中、IP ToS マーキングはサポートされません。ポリシーを設定して IP ToS をマーキングする場合は、PFC が EXP 値をマーキングします。

ポリシー マップの表示

MPLS QoS クラスのインターフェイス サマリーまたは指定されたインターフェイス上のすべてのサービス ポリシーで設定されたすべてのクラスのコンフィギュレーションでポリシー マップを表示することができます。

すべてのクラスのコンフィギュレーションの表示

指定されたインターフェイス上のすべてのサービス ポリシーに設定されたすべてのクラス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
`Router# show policy interface` *interface_type interface_number*	指定されたインターフェイス上のすべてのポリシー マップに設定されたすべてのクラスのコンフィギュレーションを表示します。

次に、ギガビット イーサネット インターフェイス 3/27 の全クラスのコンフィギュレーションを表示する例を示します。

```
Router# show policy interface gigabitethernet 3/27
 GigabitEthernet3/27
```

```
Service-policy input: ip2tag

  class-map: iptcp (match-all)
    Match: access-group 101
    police :
      1000000 bps 1000000 limit 1000000 extended limit
    Earl in slot 5 :
      0 bytes
      5 minute offered rate 0 bps
      aggregate-forwarded 0 bytes action: set-mpls-exp-imposition-transmit
      exceeded 0 bytes action: drop
      aggregate-forward 0 bps exceed 0 bps

  class-map: class-default (match-any)
    Match: any

  Class-map: class-default (match-any)
    0 packets, 0 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: any
```

MPLS QoS の出力 EXP 変換の設定

名前付き EXP 変換マップの設定

名前付き EXP 変換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	`Router(config)# platform qos map exp-mutation name mutated_exp1 mutated_exp2 mutated_exp3 mutated_exp4 mutated_exp5 mutated_exp6 mutated_exp7 mutated_exp8`	名前付き EXP 変換マップを設定します。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

名前付き EXP 変換マップを設定する場合、次の点に注意してください。

- 変換された EXP 値にマッピングする、最大 8 つの EXP 値を入力することができます。
- 複数のコマンドを入力して、追加の EXP 値を変換された EXP 値にマッピングできます。
- 変換された EXP 値ごとに個別のコマンドを入力できます。
- 内部 EXP 値が入力 EXP 値として書き込まれる前に内部 EXP 値を変換するため、15 個の入力 EXP 変換マップを設定できます。入力 EXP 変換マップを、PFC QoS がサポートする任意のインターフェイスに付加できます。
- PFC QoS は、内部 DSCP 値から出力 EXP 値を導出します。入力 EXP 変換を設定する場合、PFC QoS は変換された EXP 値から入力 EXP 値を導出しません。

インターフェイスへの出力 EXP 変換マップの付加

出力 EXP 変換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	目的
ステップ 1	`Router(config)# interface {{vlan vlan_ID} | {type slot/port[.subinterface]} | {port-channel number[.subinterface]}}`	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# platform qos exp-mutation exp-mutation-table-name`	出力 EXP 変換マップをインターフェイスに付加します。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。

次に、mutemap2 という名前の出力 EXP 変換マップを付加する例を示します。

```
Router(config)# interface gigabitethernet 3/26
Router(config-if)# platform qos exp-mutation mutemap2
Router(config-if)# end
```

EXP 値マッピングの設定

- 「入力 EXP から内部 DSCP へのマッピングの設定」（P.67-26）
- 「名前付き出力 DSCP から出力 EXP へのマッピングの設定」（P.67-27）

入力 EXP から内部 DSCP へのマッピングの設定

入力 EXP から内部 DSCP へのマッピ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	`Router(config)# platform qos map exp-dscp values`	入力 EXP 値から内部 DSCP 値へのマッピングを設定します。EXP 値に対応する 8 つの DSCP 値を入力する必要があります。有効値は 0 ～ 63 です。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

次に、入力 EXP から内部 DSCP へのマッピングを設定する例を示します。

```
Router(config)# platform qos map exp-dscp 43 43 43 43 43 43 43 43
Router(config)#
```

次に、設定を確認する例を示します。

```
Router(config)# show platform qos map exp-dscp
   Exp-dscp map:
        exp:   0  1  2  3  4  5  6  7
     ------------------------------------
        dscp:  43 43 43 43 43 43 43 43
```

名前付き出力 DSCP から出力 EXP へのマッピングの設定

名前付き出力 DSCP から出力 EXP へのマッピ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	`Router(config)# platform qos map dscp-exp dscp_values to exp_values`	名前付き出力 DSCP から出力 EXP へのマッピングを設定します。1 つの EXP 値には 1 回に最大 8 つの DSCP 値を入力することができます。有効値は 0 ～ 7 です。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

次に、名前付き出力 DSCP から出力 EXP へのマッピングを設定する例を示します。

```
Router(config)# platform qos map dscp-exp 20 25 to 3
Router(config)#
```

MPLS DiffServ トンネリング モード

トンネリングは、QoS にネットワークの 1 つのエッジから、そのネットワークの別のエッジまでをトランスペアレントにする機能を提供します。トンネルは、ラベル インポジションのある場所から開始します。トンネルは、ラベル ディスポジションのある場所、つまり、ラベルがスタックから除去された場所で終了します。そしてパケットは下部に異なった Per-Hop Behavior（PHB）レイヤを持つ MPLS パケットとして、または IP PHB レイヤ付き IP パケットとして送信されます。

PFC では、ネットワーク経由でパケットを転送する方法が 2 つあります。

- ショート パイプ モード：ショート パイプ モードでは、出力 PE ルータは中間プロバイダー（P）ルータによって使用されるマーキングの代わりに元のパケット マーキングを使用します。EXP マーキングはパケット ToS バイトには伝播しません。

  モードの説明については、「ショート パイプ モード」（P.67-28）を参照してください。

  コンフィギュレーションについては、「ショート パイプ モードの設定例」（P.67-31）を参照してください。

- 均一モード：均一モードでは、IP パケットのマーキングはサービス プロバイダーの QoS マーキングをコアに反映するよう操作することができます。このモードでは、CE およびコア ルータを含むネットワーク全体で矛盾のない QoS 分類およびマーキングが提供されます。EXP マーキングは基礎となる ToS バイトへ伝播されます。

  説明については、「均一モード」（P.67-29）を参照してください。

  設定手順については、「均一モードの設定方法」（P.67-35）を参照してください。

どちらのトンネリング モードもラベルがパケットに付与されたりパケットから削除されたりするエッジおよび最後から 2 番めのラベル スイッチング ルータ（LSR）の動作に影響を与えます。これらのモードは、中間ルータのラベル スワッピングには影響を与えません。サービス プロバイダーは、カスタマーごとに異なったタイプのトンネリング モードを選択することができます。

追加情報については、次の URL にある「MPLS DiffServ Tunneling Modes」を参照してください：
http://www.cisco.com/en/US/docs/ios-xml/ios/mp_te_diffserv/configuration/15-mt/mp-diffserv-tun-mode.html。

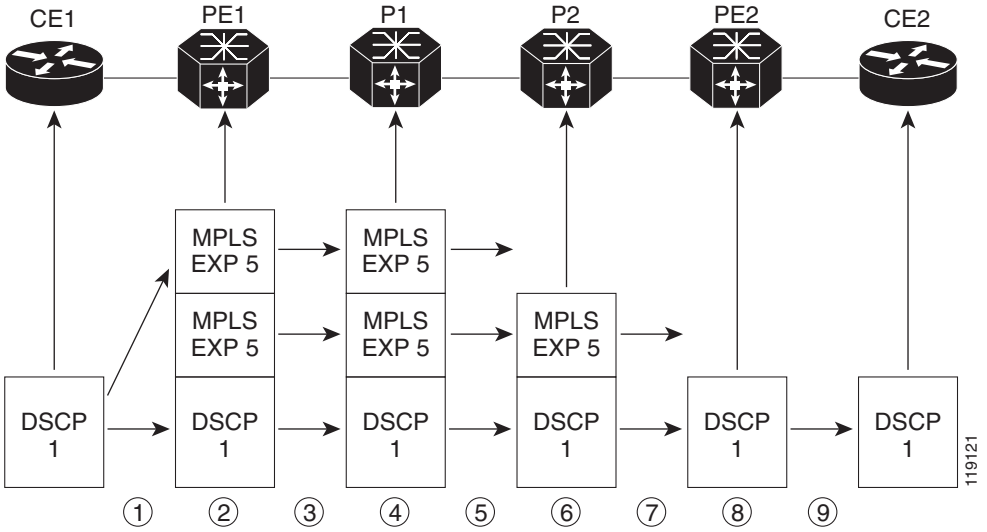
ショート パイプ モード

ショート パイプ モードはカスタマーおよびサービス プロバイダーが異なった DiffServ ドメインにある場合に使用されます。このモードを利用することにより、サービス プロバイダーはカスタマーの DiffServ 情報を保持しながら自身の DiffServ ポリシーを実施することができるため、サービス プロバイダー ネットワークを通して DiffServ の透過性が提供されます。

コアで実施される QoS ポリシーはパケット ToS バイトには伝播しません。MPLS EXP 値に基づく分類は、カスタマー側に向かう出力 PE インターフェイスで終了します。カスタマー側に向かう出力 PE インターフェイスは、元の IP パケット ヘッダーに基づいており、MPLS ヘッダーに基づいてはいません。

（注） （カスタマーの PHB マーキングに基づいており、プロバイダーの PHB マーキングには基づいていない）出力 IP ポリシーが存在する場合は自動的にショート パイプ モードとなります。

図 67-2　VPN でのショート パイプ モード動作



ショート パイプ モードは次のように機能します。

1. CE1 は IP パケットを IP DSCP 値 1 で PE1 に送信します。
2. PE1 はインポーズされたラベル エントリで MPLS EXP フィールドを 5 に設定します。
3. PE1 はパケットを P1 に送信します。
4. P1 はスワッピングされたラベル エントリで MPLS EXP フィールド値を 5 に設定します。
5. P1 はパケットを P2 に送信します。
6. P2 は IGP ラベル エントリをポップします。
7. P2 はパケットを PE2 に送信します。
8. PE2 は BGP ラベルをポップします。
9. PE2 はパケットを CE2 に送信しますが、QoS は IP DSCP 値に基づきます。

詳細については、次の URL にある『MPLS DiffServ Tunneling Modes』を参照してください。

http://www.cisco.com/en/US/docs/ios-xml/ios/mp_te_diffserv/configuration/15-mt/mp-diffserv-tun-mode.html

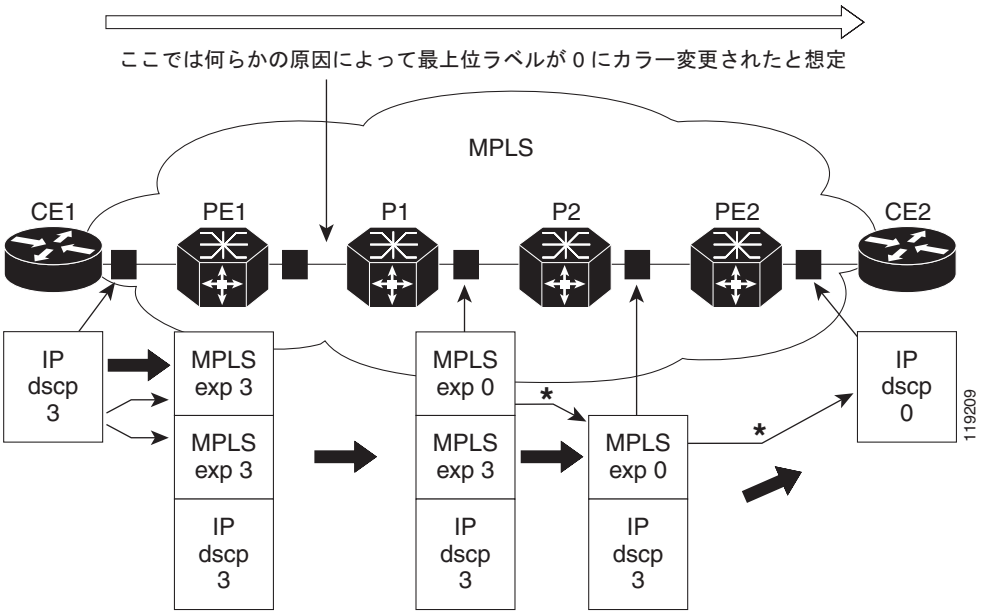
ショート パイプ モードの制約事項

MPLS-to-IP 出力インターフェイスが EoMPLS（隣接には End of Marker（EoM）ビット セットがある）である場合、ショート パイプ モードはサポートされません。

均一モード

均一モードでは、パケットは IP および MPLS ネットワークで一律に扱われます。つまり、IP precedence 値および MPLS EXP ビットは常に同じ PHB に対応しています。ルータがパケットの PHB の変更またはカラー変更をする場合はいつでも、その変更はすべてのカプセル化マーキングに伝播されなくてはなりません。パケット パス上のルータでのラベル インポジションまたはディスポジションにより PHB が追加またはエクスポーズされる場合、伝播はルータだけによって実行されます。カラーはすべてのレベルのすべての場所で反映される必要があります。たとえば、パケットの QoS マーキングが MPLS ネットワークで変更された場合、IP QoS マーキングはその変更を反映します。

図 67-3　　均一モード動作



*MPLS-to-MPLS、MPLS-to-IP のいずれの場合もラベルが残っていない場合は、
最上位の PHB ポップ ラベルが新規最上位ラベルまたは IP DSCP にコピーされます。

この手順は、IP precedence ビット マーキングまたは DSCP マーキングが存在するかどうかによって異なります。

IP precedence ビット マーキングが存在する場合は次のアクションが発生します。

1. IP パケットがサービス プロバイダー エッジ ルータである PE1 で MPLS ネットワークに着信します。

2. ラベルはパケットにコピーされます。
3. MPLS EXP フィールド値のカラー変更が行われた場合（たとえば、あまりに多くのパケットが送信中であるためパケットがレート外となった場合）、この値は IGP ラベルにコピーされます。BGP ラベルの値は変更されません。
4. 最後から 2 番めのホップでは、IGP は削除されます。この値は次の低レベルのラベルにコピーされます。
5. すべての MPLS ラベルが IP パケットとして送出されたパケットから削除されたとき、IP precedence または DSCP 値はコアで最後に変更された EXP 値として設定されます。

次に、IP precedence ビット マーキングが存在する例を示します。

1. CE1（カスタマー装置 1）で、IP パケットは IP precedence 値 3 を持っています。
2. パケットが PE1（サービス プロバイダーのエッジ ルータ）で MPLS ネットワークに着信すると、IP precedence 値 3 はパケットのインポーズされたラベル エントリにコピーされます。
3. IGP ラベル ヘッダーの MPLS EXP フィールドはマークダウンにより MPLS コア（たとえば P1）内で変更される可能性があります。

（注） IP precedence ビットは 3 であるため、BGP ラベルおよび IGP ラベルも 3 を含みます。均一モードではラベルは常に同一であるためです。パケットは IP ネットワークと MPLS ネットワークで一律に扱われます。

均一モードの制約事項

出力 IP ACL またはサービス ポリシーが MPLS-to-IP 出口点で設定された場合には、再循環のため均一モードが常に実施されます。

MPLS DiffServ トンネリングの制約事項および使用上のガイドライン

ここでは、MPLS DiffServ トンネリングの制約事項および使用上のガイドラインについて説明します。

- MPLS EXP フィールドは 3 ビット フィールドであるため 1 つのラベルスイッチド パス（LSP）は最大 8 クラスのトラフィック（つまり、8 つの PHB）をサポートすることができます。
- MPLS DiffServ トンネリング モードは E-LSP をサポートします。E-LSP は LSP の 1 つであり、ノードはここで MPLS ヘッダーの EXP ビットから排他的に MPLS パケットの QoS 処理を判別します。

次の機能は、MPLS DiffServ トンネリング モードでサポートされます。

- MPLS Per-Hop Behavior（PHB）レイヤ管理。（レイヤ管理は、PHB マーキングの追加レイヤをパケットに提供する機能です）。
- 管理されたカスタマー エッジ（CE）ルータでの制御による MPLS レイヤ管理の拡張性向上。
- MPLS はパケットの QoS をトンネリングすることができます（つまり、QoS はエッジ間でトランスペアレント）。QoS 透過性により、IP パケットの IP マーキングは MPLS ネットワーク全体で保持されます。
- MPLS EXP フィールドには、IP precedence または DSCP フィールドでマーキングされた PHB とは異なった値を別途マーキングすることができます。

ショート パイプ モードの設定例

（注）
- このステップは 1 つの方法を示すものですが、ショート パイプ モードを設定する唯一の方法というわけではありません。
- IP クラスを含む出力サービス ポリシーをインターフェイスに付加した場合、出力 PE（または PHP）でのショート パイプ モードは自動的に設定されます。

入力 PE ルータ：カスタマー側に向かうインターフェイス

この手順は、ポリシー マップを設定して、インポーズされたラベル エントリに MPLS EXP フィールドを設定するものです。

EXP 値を設定するには、入力 LAN ポートが信頼できない（untrusted）状態である必要があります。

MPLS と VPN については、入力 PE はすべての入力 PFC IP ポリシーをサポートします。

インポーズされたラベル エントリで MPLS EXP フィールドを設定するポリシー 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	`Router(config)# access-list ipv4_acl_number_or_name permit any`	IPv4 アクセス リストを作成します。
ステップ 2	`Router(config)# class-map class_name`	クラス マップを作成します。
ステップ 3	`Router(config-cmap)# match access-group ipv4_acl_number_or_name`	ステップ 1 で作成した ACL に基づくフィルタリングを行うように、クラス マップを設定します。
ステップ 4	`Router(config)# policy-map policy_map_name`	名前付き QoS ポリシーを作成します。
ステップ 5	`Router(config-pmap)# class class_name`	ステップ 2 で作成したクラス マップを使用するように、ポリシーを設定します。
ステップ 6	`Router(config-pmap-c)# police bits_per_second [normal_burst_bytes] conform-action set-mpls-exp-transmit exp_value exceed-action drop`	ポリシングを設定します。ここでは、次の内容を設定します。 • サービス レベル契約（SLA）で指定されたレート制限に適合するパケットをとるアクション • SLA で指定されたレート制限を超えるパケットをとるアクション。 *exp_value* は、MPLS EXP フィールドを設定します。
ステップ 7	`Router(config)# interface type slot/port`	設定するインターフェイスを選択します。
ステップ 8	`Router(config-if)# no platform qos trust`	インターフェイスを untrusted として設定します。
ステップ 9	`Router(config-if)# service-policy input policy_map_name`	ステップ 4 で作成したポリシー マップを、入力サービス ポリシーとしてインターフェイスに付加します。

設定例

次に、インポーズされたラベル エントリで MPLS EXP フィールドを設定するポリシー マップを設定する例を示します。

```
Router(config)# access-list 1 permit any
Router(config)# class-map CUSTOMER-A
Router(config-cmap)# match access-group 1
Router(config)# policy-map set-MPLS-PHB
Router(config-pmap)# class CUSTOMER-A
Router(config-pmap-c)# police 50000000 conform-action set-mpls-exp-transmit 4
exceed-action drop
Router(config)# interface gigabitethernet 3/1
Router(config-if)# no platform qos trust
Router(config)# interface gigabitethernet 3/1.31
Router(config-if)# service-policy input set-MPLS-PHB
```

入力 PE ルータの設定：P 側に向かうインターフェイス

この手順は MPLS EXP フィールドに基づいてパケットを分類し、適切な廃棄およびスケジューリング処理を提供するものです。

MPLS EXP フィールドに基づいてパケットを分類し、適切な廃棄およびスケジューリング処理を提供するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# class-map class_name`	どのパケットがマッピング（マッチング）されるのかを示すクラス マップを指定します。トラフィック クラスを作成します。
ステップ 2	`Router(config-c-map)# match mpls experimental exp_list`	パケットがそのクラスに属しているかどうかを判別するためにパケットをチェックする一致基準として使用する MPLS EXP フィールド値を指定します。
ステップ 3	`Router(config)# policy-map name`	1 つまたは複数のクラスに一致するパケットの QoS ポリシーを設定します。
ステップ 4	`Router(config-p-map)# class class_name`	トラフィック クラスをサービス ポリシーに関連付けます。
ステップ 5	`Router(config-p-map-c)# bandwidth {bandwidth_kbps | percent percent}`	トラフィック クラスに最小帯域幅保証を指定します。kbps（キロビット/秒）または全体的な帯域幅のパーセント値で最小帯域幅保証を指定することができます。
ステップ 6	`Router(config-p-map)# class class-default`	ポリシーを設定または変更できるようデフォルト クラスを指定します。
ステップ 7	`Router(config-p-map-c)# random-detect`	帯域幅保証を持つトラフィック クラスの WRED ドロップ ポリシーをイネーブルにします。
ステップ 8	`Router(config)# interface type slot/port`	設定するインターフェイスを選択します。
ステップ 9	`Router(config-if)# service-policy output name`	QoS ポリシーをインターフェイスに付加し、そのインターフェイスを脱退するパケット上で適用すべきポリシーを指定します。

（注）　**bandwidth** コマンドおよび **random-detect** コマンドは、LAN ポートではサポートされません。

設定例

次に、MPLS EXP フィールドに基づいてパケットを分類し、適切な廃棄およびスケジューリング処理を提供する例を示します。

```
Router(config)# class-map MPLS-EXP-4
Router(config-c-map)# match mpls experimental 4
Router(config)# policy-map output-qos
Router(config-p-map)# class MPLS-EXP-4
Router(config-p-map-c)# bandwidth percent 40
Router(config-p-map)# class class-default
Router(config-p-map-c)# random-detect
Router(config)# interface pos 4/1
Router(config-if)# service-policy output output-qos
```

P ルータの設定：出力インターフェイス

MPLS EXP フィールドに基づいてパケットを分類し、適切な廃棄およびスケジューリング処理を提供するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# class-map class_name`	どのパケットがマッピング（マッチング）されるのかを示すクラス マップを指定します。トラフィック クラスを作成します。
ステップ 2	`Router(config-c-map)# match mpls experimental exp_list`	パケットがそのクラスに属しているかどうかを判別するためにパケットをチェックする一致基準として使用する MPLS EXP フィールド値を指定します。
ステップ 3	`Router(config)# policy-map name`	1 つまたは複数のクラスに一致するパケットの QoS ポリシーを設定します。
ステップ 4	`Router(config-p-map)# class class_name`	トラフィック クラスをサービス ポリシーに関連付けます。
ステップ 5	`Router(config-p-map-c)# bandwidth {bandwidth_kbps | percent percent}`	トラフィック クラスに最小帯域幅保証を指定します。kbps（キロビット/秒）または全体的な帯域幅のパーセント値で最小帯域幅保証を指定することができます。
ステップ 6	`Router(config-p-map)# class class-default`	ポリシーを設定または変更できるようデフォルト クラスを指定します。
ステップ 7	`Router(config-p-map-c)# random-detect`	WRED を IP precedence または MPLS EXP フィールド値に基づくポリシーに適用します。
ステップ 8	`Router(config)# interface type slot/port`	設定するインターフェイスを選択します。
ステップ 9	`Router(config-if)# service-policy output name`	QoS ポリシーをインターフェイスに付加し、そのインターフェイスを脱退するパケット上で適用すべきポリシーを指定します。

（注）　**bandwidth** コマンドおよび **random-detect** コマンドは、LAN ポートではサポートされません。

設定例

次に、MPLS EXP フィールドに基づいてパケットを分類し、適切な廃棄およびスケジューリング処理を提供する例を示します。

```
Router(config)# class-map MPLS-EXP-4
Router(config-c-map)# match mpls experimental 4
Router(config)# policy-map output-qos
Router(config-p-map)# class MPLS-EXP-4
Router(config-p-map-c)# bandwidth percent 40
Router(config-p-map)# class class-default
Router(config-p-map-c)# random-detect
Router(config)# interface pos 2/1
Router(config-if)# service-policy output output-qos
```

出力 PE ルータの設定：カスタマー側に向かうインターフェイス

IP DSCP 値に基づいてパケットを分類し、適切な廃棄およびスケジューリング処理を提供するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# class-map class_name`	どのパケットがマッピング（マッチング）されるのかを示すクラス マップを指定します。トラフィック クラスを作成します。
ステップ 2	`Router(config-c-map)# match ip dscp dscp_values`	DSCP 値を一致基準として使用します。
ステップ 3	`Router(config)# policy-map name`	1 つまたは複数のクラスに一致するパケットの QoS ポリシーを設定します。
ステップ 4	`Router(config-p-map)# class class_name`	トラフィック クラスをサービス ポリシーに関連付けます。
ステップ 5	`Router(config-p-map-c)# bandwidth {bandwidth_kbps | percent percent}`	トラフィック クラスに最小帯域幅保証を指定します。kbps（キロビット/秒）または全体的な帯域幅のパーセント値で最小帯域幅保証を指定することができます。
ステップ 6	`Router(config-p-map)# class class-default`	ポリシーを設定または変更できるようデフォルト クラスを指定します。
ステップ 7	`Router(config-p-map-c)# random-detect dscp-based`	帯域幅保証を持つトラフィック クラスの WRED ドロップ ポリシーをイネーブルにします。
ステップ 8	`Router(config)# interface type slot/port`	設定するインターフェイスを選択します。
ステップ 9	`Router(config-if)# service-policy output name`	QoS ポリシーをインターフェイスに付加し、そのインターフェイスを脱退するパケット上で適用すべきポリシーを指定します。

設定例

次に、IP DSCP 値に基づいてパケットを分類し、適切な廃棄およびスケジューリング処理を提供する例を示します。

```
Router(config)# class-map IP-PREC-4
Router(config-c-map)# match ip precedence 4
Router(config)# policy-map output-qos
Router(config-p-map)# class IP-PREC-4
Router(config-p-map-c)# bandwidth percent 40
Router(config-p-map)# class class-default
```

```
Router(config-p-map-c)# random-detect
Router(config)# interface gigabitethernet 3/2.32
Router(config-if)# service-policy output output-qos
```

均一モードの設定方法

- 「入力 PE ルータの設定：カスタマー側に向かうインターフェイス」（P.67-35）
- 「入力 PE ルータの設定：P 側に向かうインターフェイス」（P.67-36）
- 「出力 PE ルータの設定：カスタマー側に向かうインターフェイス」（P.67-37）

（注）　このステップは 1 つの方法を示すものですが、均一モードを設定する唯一の方法というわけではありません。

入力 PE ルータの設定：カスタマー側に向かうインターフェイス

Uniform モードで、IP precedence または IP DSCP に信頼状態を設定すると、PFC は IP PHB を MPLS PHB にコピーできます。

（注）　この説明は、LAN ポートの PFC に適用されます。

インポーズされたラベル エントリで MPLS EXP フィールドを設定するポリシー 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	`Router(config)# access-list ipv4_acl_number_or_name permit any`	IPv4 アクセス リストを作成します。
ステップ 2	`Router(config)# class-map class_name`	クラス マップを作成します。
ステップ 3	`Router(config-cmap)# match access-group ipv4_acl_number_or_name`	ステップ 1 で作成した ACL に基づくフィルタリングを行うように、クラス マップを設定します。
ステップ 4	`Router(config)# policy-map policy_map_name`	名前付き QoS ポリシーを作成します。
ステップ 5	`Router(config-pmap)# class class_name`	ステップ 2 で作成したクラス マップを使用するように、ポリシーを設定します。
ステップ 6	`Router(config-pmap-c)# police bits_per_second [normal_burst_bytes] conform-action transmit exceed-action drop`	ポリシングを設定します。ここでは、次の内容を設定します。 • SLA で指定されたレート制限に適合するパケットをとるアクション。 • SLA で指定されたレート制限を超えるパケットをとるアクション。
ステップ 7	`Router(config)# interface type slot/port`	設定するインターフェイスを選択します。
ステップ 8	`Router(config-if)# platform qos trust dscp`	受信した DSCP を、全ポートの入力トラフィックに対する内部 DSCP 基準値として設定します。
ステップ 9	`Router(config-if)# service-policy input policy_map_name`	ステップ 4 で作成したポリシー マップを、入力サービス ポリシーとしてインターフェイスに付加します。

設定例

次に、インポーズされたラベル エントリで MPLS EXP フィールドを設定するポリシー マップを設定する例を示します。

```
Router(config)# access-list 1 permit any
Router(config)# class-map CUSTOMER-A
Router(config-cmap)# match access-group 1
Router(config)# policy-map SLA-A
Router(config-pmap)# class CUSTOMER-A
Router(config-pmap-c)# police 50000000 conform-action transmit exceed-action drop
Router(config)# interface gigabitethernet 3/1
Router(config-if)# platform qos trust dscp
Router(config)# interface gigabitethernet 3/1.31
Router(config-if)# service-policy input SLA-A
```

入力 PE ルータの設定：P 側に向かうインターフェイス

MPLS EXP フィールドに基づいてパケットを分類し、適切な廃棄およびスケジューリング処理を提供するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# class-map class_name`	どのパケットがマッピング（マッチング）されるのかを示すクラス マップを指定します。トラフィック クラスを作成します。
ステップ 2	`Router(config-c-map)# match mpls experimental exp_list`	パケットがそのクラスに属しているかどうかを判別するためにパケットをチェックする一致基準として使用する MPLS EXP フィールド値を指定します。
ステップ 3	`Router(config)# policy-map name`	1 つまたは複数のクラスに一致するパケットの QoS ポリシーを設定します。
ステップ 4	`Router(config-p-map)# class class_name`	トラフィック クラスをサービス ポリシーに関連付けます。
ステップ 5	`Router(config-p-map-c)# bandwidth {bandwidth_kbps | percent percent}`	トラフィック クラスに最小帯域幅保証を指定します。kbps（キロビット/秒）または全体的な帯域幅のパーセント値で最小帯域幅保証を指定することができます。
ステップ 6	`Router(config-p-map)# class class-default`	ポリシーを設定または変更できるようデフォルト クラスを指定します。
ステップ 7	`Router(config-p-map-c)# random-detect`	帯域幅保証を持つトラフィック クラスの WRED ドロップ ポリシーをイネーブルにします。
ステップ 8	`Router(config)# interface type slot/port`	設定するインターフェイスを選択します。
ステップ 9	`Router(config-if)# service-policy output name`	QoS ポリシーをインターフェイスに付加し、そのインターフェイスを脱退するパケット上で適用すべきポリシーを指定します。

（注）　**bandwidth** コマンドおよび **random-detect** コマンドは、LAN ポートではサポートされません。

設定例

次に、MPLS EXP フィールドに基づいてパケットを分類し、適切な廃棄およびスケジューリング処理を提供する例を示します。

```
Router(config)# class-map MPLS-EXP-3
Router(config-c-map)# match mpls experimental 3
Router(config)# policy-map output-qos
Router(config-p-map)# class MPLS-EXP-3
Router(config-p-map-c)# bandwidth percent 40
Router(config-p-map)# class class-default
Router(config-p-map-c)# random-detect
Router(config)# interface pos 4/1
Router(config-if)# service-policy output output-qos
```

出力 PE ルータの設定：カスタマー側に向かうインターフェイス

カスタマー側に向かうインターフェイスで出力 PE ル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	`Router(config)# class-map class_name`	どのパケットがマッピング（マッチング）されるのかを示すクラス マップを指定します。トラフィック クラスを作成します。
ステップ 2	`Router(config-c-map)# match ip precedence precedence-value`	IP precedence 値を一致基準として識別します。
ステップ 3	`Router(config)# policy-map name`	1 つまたは複数のクラスに一致するパケットの QoS ポリシーを設定します。
ステップ 4	`Router(config-p-map)# class class_name`	トラフィック クラスをサービス ポリシーに関連付けます。
ステップ 5	`Router(config-p-map-c)# bandwidth {bandwidth_kbps | percent percent}`	トラフィック クラスに最小帯域幅保証を指定します。kbps（キロビット/秒）または全体的な帯域幅のパーセント値で最小帯域幅保証を指定することができます。
ステップ 6	`Router(config-p-map)# class class-default`	ポリシーを設定または変更できるようデフォルト クラスを指定します。
ステップ 7	`Router(config-p-map-c)# random-detect`	WRED を IP precedence または MPLS EXP フィールド値に基づくポリシーに適用します。
ステップ 8	`Router(config)# interface type slot/port`	設定するインターフェイスを選択します。
ステップ 9	`Router(config-if) mpls propagate-cos`	EXP 値が MPLS ドメイン出口 LER 出力ポートで基礎となる IP DSCP へ伝播するのをイネーブルにします。
ステップ 10	`Router(config-if)# service-policy output name`	QoS ポリシーをインターフェイスに付加し、そのインターフェイスに着信するパケット上で適用すべきポリシーを指定します。

（注）　**bandwidth** コマンドおよび **random-detect** コマンドは、LAN ポートではサポートされません。

設定例

次に、カスタマー側に向かうインターフェイスで出力 PE ルータを設定する例を示します。

```
Router(config)# class-map IP-PREC-4
```

```
Router(config-c-map)# match ip precedence 4
Router(config)# policy-map output-qos
Router(config-p-map)# class IP-PREC-4
Router(config-p-map-c)# bandwidth percent 40
Router(config-p-map)# class class-default
Router(config-p-map-c)# random-detect
Router(config)# interface gigabitethernet 3/2.32
Router(config-if) mpls propagate-cos
Router(config-if)# service-policy output output-qos
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

PFC QoS 統計データ エクスポート

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

PFC QoS 統計データ エクスポートの前提条件

なし。

PFC QoS 統計データ エクスポートの制約事項

なし。

PFC QoS 統計データ エクスポートについて

PFC QoS 統計データ エクスポート機能により、LAN ポート別および集約ポリサー別に使用率に関する情報を作成し、UDP パケットに格納して、トラフィックのモニタ、計画、アカウンティング用アプリケーションに転送できます。PFC QoS 統計データ エクスポートは、LAN ポート別および集約ポリサー別にイネーブルにできます。ポート別に生成された統計データは、入力パケット数と出力パケット数、およびバイト数で構成されます。集約ポリサー別に生成された統計データは、許可されたパケット数、およびポリシーで設定された速度を超えるパケット数で構成されます。

PFC QoS 統計データは一定の間隔で定期的に収集されますが、データがエクスポートされる間隔を設定できます。すべてのポートおよび設定されている集約ポリサーに対するデフォルト設定では、PFC QoS 統計の収集はイネーブルに、データ エクスポート機能はディセーブルになっています。

（注）　PFC QoS 統計データ エクスポート機能は、NetFlow Data Export（NDE; NetFlow データ エクスポート）から完全に独立していて、相互作用はありません。

PFC QoS 統計データ エクスポートのデフォルト設定

機能	デフォルト値
グローバルな PFC QoS データ エクスポート	ディセーブル
ポート別の PFC QoS データ エクスポート	ディセーブル
名前付き集約ポリサー別の PFC QoS データ エクスポート	ディセーブル
クラス マップ ポリサー別の PFC QoS データ エクスポート	ディセーブル
PFC QoS データ エクスポート間隔	300 秒
エクスポート先	未設定
PFC QoS データ エクスポート フィールド デリミタ	パイプ文字（|）

PFC QoS 統計データ エクスポートの設定方法

- 「PFC QoS 統計データ エクスポートのグローバルなイネーブル化」（P.68-3）
- 「ポートの PFC QoS 統計データ エクスポートのイネーブル化」（P.68-3）
- 「名前付き集約ポリサーの PFC QoS 統計データ エクスポートのイネーブル化」（P.68-4）
- 「クラス マップの PFC QoS 統計データ エクスポートのイネーブル化」（P.68-5）
- 「PFC QoS 統計データ エクスポート間隔の設定」（P.68-6）
- 「PFC QoS 統計データ エクスポートの宛先ホストおよび UDP ポートの設定」（P.68-7）
- 「PFC QoS 統計データ エクスポートのフィールド デリミタの設定」（P.68-9）

PFC QoS 統計データ エクスポートのグローバルなイネーブル化

PFC QoS 統計データ エクスポートをグローバルにイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# platform qos statistics-export`	PFC QoS 統計データ エクスポートをグローバルにイネーブルにします。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

次に、PFC QoS 統計データ エクスポートをグローバルにイネーブルにし、設定を確認する例を示します。

```
Router# configure terminal
Router(config)# platform qos statistics-export
Router(config)# end
% Warning: Export destination not set.
% Use 'platform qos statistics-export destination' command to configure the export
destination
Router# show platform qos statistics-export info
QoS Statistics Data Export Status and Configuration information
---------------------------------------------------------------
Export Status : enabled
Export Interval : 300 seconds
Export Delimiter : |
Export Destination : Not configured
Router#
```

（注）　その他の PFC QoS 統計データ エクスポートの設定を有効にするには、PFC QoS 統計データ エクスポートをグローバルにイネーブルにする必要があります。

ポートの PFC QoS 統計データ エクスポートのイネーブル化

特定のポートの PFC QoS 統計データのエクスポー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	`Router(config)# interface` *type 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	`Router(config-if)# platform qos statistics-export`	指定したポートの PFC QoS 統計データ エクスポートをイネーブルにします。
ステップ 3	`Router(config)# end`	コンフィギュレーション モードを終了します。

次に、ポート GigabitEthernet 5/24 で PFC QoS 統計データのエクスポートをイネーブルにし、設定を確認する例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 5/24
Router(config-if)# platform qos statistics-export
Router(config-if)# end
Router# show platform qos statistics-export info
QoS Statistics Data Export Status and Configuration information
---------------------------------------------------------------
Export Status : enabled
Export Interval : 300 seconds
Export Delimiter : |
```

```
Export Destination : Not configured

QoS Statistics Data Export is enabled on following ports:
-----------------------------------------------------------
GigabitEthernet5/24
Router#
```

ポートの PFC QoS 統計データ エクスポートをイネーブルにすると、エクスポートされたデータには次に示すフィールドがデリミタ文字で区切られて格納されます。

- エクスポート タイプ（ポートの場合は「1」）
- スロット/ポート
- 入力パケット数
- 入力バイト数
- 出力パケット数
- 出力バイト数
- タイム スタンプ

名前付き集約ポリサーの PFC QoS 統計データ エクスポートのイネーブル化

名前付き集約ポリサーの PFC QoS 統計データ エクスポー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	`Router(config)# platform qos statistics-export aggregate-policer` *aggregate_policer_name*	名前付き集約ポリサーの PFC QoS 統計データ エクスポートをイネーブルにします。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

次に、aggr1M という名前の集約ポリサーの PFC QoS 統計データ エクスポートをイネーブルにして、設定を確認する例を示します。

```
Router# configure terminal
Router(config)# platform qos statistics-export aggregate-policer aggr1M
Router(config)# end
Router# show platform qos statistics-export info
QoS Statistics Data Export Status and Configuration information
---------------------------------------------------------------
Export Status : enabled
Export Interval : 300 seconds
Export Delimiter : |
Export Destination : Not configured

QoS Statistics Data Export is enabled on following ports:
-----------------------------------------------------------
GigabitEthernet5/24

QoS Statistics Data export is enabled on following shared aggregate policers:
-------------------------------------------------------------------------------
aggr1M
Router#
```

名前付き集約ポリサーの PFC QoS 統計データ エクスポートをイネーブルにすると、エクスポートされたデータには次に示すフィールドがデリミタ文字で区切られて格納されます。

- エクスポート タイプ（集約ポリサーの場合は「3」）

- 集約ポリサー名
- 方向（「in」）
- PFC または DFC スロット番号
- 適合するバイト数
- CIR を超えるバイト数
- PIR を超えるバイト数
- タイム スタンプ

クラス マップの PFC QoS 統計データ エクスポートのイネーブル化

クラス マップの PFC QoS 統計データ エクスポー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	`Router(config)# platform qos statistics-export class-map` *classmap_name*	クラス マップの PFC QoS 統計データ エクスポートをイネーブルにします。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

次に、class3 という名前のクラス マップの PFC QoS 統計データ エクスポートをイネーブルにして、設定を確認する例を示します。

```
Router# configure terminal
Router(config)# platform qos statistics-export class-map class3
Router(config)# end
Router# show platform qos statistics-export info
QoS Statistics Data Export Status and Configuration information
---------------------------------------------------------------
Export Status : enabled
Export Interval : 300 seconds
Export Delimiter : |
Export Destination : Not configured

QoS Statistics Data Export is enabled on following ports:
---------------------------------------------------------
GigabitEthernet5/24

QoS Statistics Data export is enabled on following shared aggregate policers:
-----------------------------------------------------------------------------
aggr1M

QoS Statistics Data Export is enabled on following class-maps:
---------------------------------------------------------------
class3
Router#
```

クラス マップの PFC QoS 統計データ エクスポートをイネーブルにすると、エクスポート データには次に示すフィールドがデリミタで区切られて格納されます。

- 物理ポートからのデータ：
  - エクスポート タイプ（クラス マップおよびポートの場合は「4」）
  - クラス マップ名
  - 方向（「in」）
  - スロット/ポート

  - 適合するバイト数
  - CIR を超えるバイト数
  - PIR を超えるバイト数
  - タイム スタンプ
- VLAN インターフェイスからのデータ：
  - エクスポート タイプ（クラス マップおよび VLAN の場合は「5」）
  - クラス マップ名
  - 方向（「in」）
  - PFC または DFC スロット番号
  - VLAN ID
  - 適合するバイト数
  - CIR を超えるバイト数
  - PIR を超えるバイト数
  - タイム スタンプ
- ポート チャネル インターフェイスからのデータ：
  - エクスポート タイプ（クラス マップおよびポート チャネルの場合は「6」）
  - クラス マップ名
  - 方向（「in」）
  - PFC または DFC スロット番号
  - ポート チャネル ID
  - 適合するバイト数
  - CIR を超えるバイト数
  - PIR を超えるバイト数
  - タイム スタンプ

PFC QoS 統計データ エクスポート間隔の設定

PFC QoS 統計データ エクスポートの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	`Router(config)# platform qos statistics-export interval` *interval_in_seconds*	PFC QoS 統計データ エクスポートの間隔を設定します。 （注）　間隔は、使用している設定内のアクティビティにカウンタ ラップアラウンドが発生しない程度に短くする必要があります。ただし、PFC QoS 統計データ エクスポートを実行するとスイッチにかなりの負荷が発生するため、間隔を小さくするときは注意してください。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

次に、PFC QoS 統計データ エクスポートの間隔を設定し、設定を確認する例を示します。

```
Router# configure terminal
Router(config)# platform qos statistics-export interval 250
Router(config)# end
Router# show platform qos statistics-export info
QoS Statistics Data Export Status and Configuration information
---------------------------------------------------------------
Export Status : enabled
Export Interval : 250 seconds
Export Delimiter : |
Export Destination : Not configured

QoS Statistics Data Export is enabled on following ports:
---------------------------------------------------------
GigabitEthernet5/24

QoS Statistics Data export is enabled on following shared aggregate policers:
-----------------------------------------------------------------------------
aggr1M

QoS Statistics Data Export is enabled on following class-maps:
--------------------------------------------------------------
class3
Router#
```

PFC QoS 統計データ エクスポートの宛先ホストおよび UDP ポートの設定

PFC QoS 統計データ エクスポートの宛先ホストおよび UDP ポート番号を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# platform qos statistics-export destination {host_name | host_ip_address} {port port_number | syslog [facility facility_name] [severity severity_value]}`	PFC QoS 統計データ エクスポートの宛先ホストおよび UDP ポート番号を設定します。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

（注）　PFC QoS データ エクスポートの宛先を Syslog サーバにした場合、エクスポート データの先頭に Syslog ヘッダーが付きます。

表 68-1　サポートされている PFC QoS データ エクスポート機能パラメータ値

名前	定義	名前	定義
kern	カーネル メッセージ	cron	cron/at サブシステム
user	ランダムなユーザレベル メッセージ	local0	ローカルで使用するために確保
mail	メール システム	local1	ローカルで使用するために確保
daemon	システム デーモン	local2	ローカルで使用するために確保
auth	セキュリティ / 認証メッセージ	local3	ローカルで使用するために確保
syslog	内部 Syslog メッセージ	local4	ローカルで使用するために確保
lpr	ライン プリンタ サブシステム	local5	ローカルで使用するために確保

表 68-1　サポートされている PFC QoS データ エクスポート機能パラメータ値 （続き）

名前	定義	名前	定義
news	ネットニュース サブシステム	local6	ローカルで使用するために確保
uucp	uucp サブシステム	local7	ローカルで使用するために確保

表 68-2　サポートされている PFC QoS データ エクスポートの重大度パラメータ値

重大度パラメータ		
名前	**番号**	**定義**
emerg	0	システムは使用不能
alert	1	即時対処が必要
crit	2	クリティカルな状態
err	3	エラー
warning	4	警告
notice	5	正常だが重大な状態
info	6	情報
debug	7	デバッグレベル メッセージ

次に、172.20.52.3 を宛先ホストとして、Syslog を UDP ポート番号として設定し、その設定を確認する例を示します。

```
Router# configure terminal
Router(config)# platform qos statistics-export destination 172.20.52.3 syslog
Router(config)# end
Router# show platform qos statistics-export info
QoS Statistics Data Export Status and Configuration information
---------------------------------------------------------------
Export Status : enabled
Export Interval : 250 seconds
Export Delimiter : |
Export Destination : 172.20.52.3, UDP port 514 Facility local6, Severity debug

QoS Statistics Data Export is enabled on following ports:
---------------------------------------------------------
GigabitEthernet5/24

QoS Statistics Data export is enabled on following shared aggregate policers:
-----------------------------------------------------------------------------
aggr1M

QoS Statistics Data Export is enabled on following class-maps:
--------------------------------------------------------------
class3
```

PFC QoS 統計データ エクスポートのフィールド デリミタの設定

PFC QoS 統計データ エクスポートのフィールド デリミタを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# platform qos statistics-export delimiter` *delimiter_character*	PFC QoS 統計データ エクスポートのフィールド デリミタを設定します。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

次に、PFC QoS 統計データ エクスポートのフィールド デリミタを設定し、設定を確認する例を示します。

```
Router# configure terminal
Router(config)# platform qos statistics-export delimiter ,
Router(config)# end
Router# show platform qos statistics-export info
QoS Statistics Data Export Status and Configuration information
---------------------------------------------------------------
Export Status : enabled
Export Interval : 250 seconds
Export Delimiter : ,
Export Destination : 172.20.52.3, UDP port 514 Facility local6, Severity debug

QoS Statistics Data Export is enabled on following ports:
---------------------------------------------------------
GigabitEthernet5/24

QoS Statistics Data export is enabled on following shared aggregate policers:
-----------------------------------------------------------------------------
aggr1M

QoS Statistics Data Export is enabled on following class-maps:
--------------------------------------------------------------
class3
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

PART 13

セキュリティ

Cisco IOS ACL のサポート

（注）
- Cisco IOS ACL の詳細な設定手順については、次のマニュアルを参照してください。
  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_data_acl/configuration/15-sy/sec-data-acl-15-sy-book.html
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。
  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。
http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

Cisco IOS ACL の制約事項

- Cisco IOS ACL をレイヤ 3 ポートおよび VLAN インターフェイスに直接、適用できます。

- VLAN ACL とポート ACL をレイヤ 2 インターフェイスと VLAN に適用できます（第 73 章「ポート ACL（PACL）」および第 74 章「VLAN ACL（VACL）」を参照）。
- 各タイプの ACL（IP、IPX、および MAC）は対応するトラフィック タイプだけをフィルタリングします。**mac packet-classify** コンフィギュレーション コマンドがイネーブルでない限り、Cisco IOS MAC ACL は、IP または IPX トラフィックと一致しません。デフォルトでは、**mac packet-classify** 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。
- **mac packet-classify** コンフィギュレーション コマンドを入力すると、MAC ACL がすべてのプロトコル トラフィックに適用されます。
- PFC では、ハードウェアで Cisco IOS IPX ACL をサポートしません。Cisco IOS IPX ACL は、ルート プロセッサ（RP）のソフトウェアでサポートされます。
- デフォルトでは、パケットがアクセス グループによって拒否された場合、インターネット制御メッセージ プロトコル（ICMP）到達不能メッセージが RP によって送信されます。

  ip unreachables コマンドがイネーブルの場合（デフォルト）、スイッチは拒否されたパケットの大部分をハードウェアでドロップし、一部のパケットだけが RP に送信されてソフトウェアでドロップされます（これにより ICMP 到達不能メッセージが生成されます）。

  ip unreachables コマンドは、ACL ドロップ パケットのハードウェアの動作に影響を与えず、ACL 拒否パケットのリークはデフォルトでイネーブルです。インターフェイス上のイーサネット ICMP 到達不能メッセージをディセーブルにするには、**no ip unreachables** インターフェイス コンフィギュレーション コマンドを入力します。
- パケットが VACL または PACL によって拒否された場合、ICMP 到達不能メッセージは送信されません。
- 名前付き ACL を使用すると、ACL 設定の作成または変更時およびシステム再起動中の CPU 使用率を低く抑えられるため、番号付き ACL ではなく名前付き ACL を使用してください。ACL エントリを作成する（または既存の ACL エントリを変更する）場合、ソフトウェアでは ACL 設定を PFC ハードウェアにロードするために ACL マージと呼ばれる CPU 中心の動作が行われます。ACL マージはまた、システム再起動中にスタートアップ コンフィギュレーションを適用する際にも発生します。

  名前付き ACL を使用すると、ユーザが **named-acl** コンフィギュレーション モードを終了するときにだけ ACL マージが開始されます。ただし、名前付き ACL では、ACL 定義すべてについて ACL マージが開始されるため、中規模のマージが ACL 設定中に何度も行われることになります。
- グローバル デフォルト結果は、ヒットレス アップデートが成功しない場合、または機能が特定のインターフェイスに設定されていない場合に使用されます。

ACL のレイヤ 4 演算の制約事項

レイヤ 4 演算の使用

次のタイプの演算子を指定できます。

- gt（greater than：より大きい）
- lt（less than：より小さい）
- neq（not equal：等しくない）

- eq（equal：等しい）
- range（inclusive range：包含範囲）

1 つの ACL に、*9* つより多くの*異なる*演算を指定しないよう推奨します。この数を超えると、新しい演算によって影響される ACE が、複数の ACE に分割されることがあります。

レイヤ 4 演算を使用するときは、次の 2 つ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、違う演算であると見なされます。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 演算です）。

```
... gt 10 permit
... lt 9 deny
... gt 11 deny
```

（注） 「eq」演算子の使用に制限はありません。「eq」演算子は論理演算ユニット（LOU）またはレイヤ 4 演算ビットを使用しないためです。LOU については、「論理演算ユニット（LOU）の使用」（P.69-3）を参照してください。

- レイヤ 4 演算は、同じ演算子 / 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。たとえば次の ACL では、1 つの ACE には送信元ポート、もう 1 つの ACE には宛先ポートが指定されているので、2 つの異なるレイヤ 4 演算が定義されていることになります。

```
... Src gt 10 ...
... Dst gt 10
```

論理演算ユニット（LOU）の使用

Logical Operation Unit（LOU; 論理演算ユニット）は、演算子 / オペランドの組み合わせを保存するレジスタです。ACL はすべて、LOU を使用します。最大 104 の LOU があります。各 LOU には、2 つの異なる演算子 / オペランドの組み合わせを保存でき、LOU レジストの総数は、208 になります。レイヤ 4 演算は、次のように LOU を使用します。

- gt は、1/2 LOU を使用します。
- lt は、1/2 LOU を使用します。
- neq は、1/2 LOU を使用します。
- range は、1 LOU を使用します。
- eq は、LOU を使用しません。

たとえば、次の ACL では、1 つの LOU に 2 つの異なる演算子 / オペランドの組み合わせが保存されます。

```
... Src gt 10 ...
... Dst gt 10
```

以下は、より詳細な例です。

```
ACL1
... (dst port) gt 10 permit
... (dst port) lt 9 deny
... (dst port) gt 11 deny
... (dst port) neq 6 permit
... (src port) neq 6 deny
... (dst port) gt 10 deny
```

```
ACL2
... (dst port) gt 20 deny
... (src port) lt 9 deny
... (src port) range 11 13 deny
... (dst port) neq 6 permit
```

レイヤ 4 演算数と LOU 数は、次のとおりです。

- ACL1 のレイヤ 4 演算：5
- ACL2 のレイヤ 4 演算：4
- LOU：4

LOU は、次のように使用されています。

- LOU1 に、「gt 10」および「lt 9」が保存されます。
- LOU2 に、「gt 11」および「neq 6」が保存されます。
- LOU 3 に、「gt 20」が保存されます（半分は空き）。
- LOU 4 に、「range 11 13」が保存されます（range は 1 LOU を使用）。

ACL サポートについて

ACL は、ハードウェアの場合にはポリシー フィーチャ カード（PFC）、分散型フォワーディング カード（DFC）で、ソフトウェアの場合にはルート プロセッサ（RP）で処理できます。

- 標準 ACL および拡張 ACL（入力および出力）の「deny」ステートメントに一致する ACL フローは、「ip unreachables」がディセーブルに設定されている場合、ハードウェアによってドロップされます。
- 標準 ACL および拡張 ACL（入力および出力）の「permit」ステートメントに一致する ACL フローは、ハードウェアで処理されます。
- VLAN ACL（VACL）フローおよびポート ACL（PACL）フローはハードウェアで処理されます。VACL または PACL で指定されたフィールドのハードウェア処理がサポートされていない場合、このフィールドは無視されるか（ACL の **log** キーワードなど）、または設定全体が拒否されます（IPX ACL パラメータを含む VACL など）。
- IPv6 ACL は 32 ビット符号化を使用します。
- VACL ログ機能はソフトウェアで処理されます。
- VACL は IPX アクセス リストではサポートされません。
- VACL は、拒否パケットのロギングだけをサポートします。
- ダイナミック ACL フローはハードウェアで処理されます。
- アイドル タイムアウトはソフトウェアで処理されます。

（注） アイドル タイムアウトは設定できません。Cisco IOS Release 15.1SY では、**access-enable host timeout** コマンドがサポートされていません。

- MPLS インターフェイス以外では、セッション内の最初のパケットが RP 上のソフトウェアで処理された後、リフレクシブ ACL フローがハードウェアで処理されます。

- リフレクシブ ACL フローは、IP からの各種のタグへのトラフィックの場合、および各種のタグから IP へのトラフィックの場合は、ハードウェアによって加速されません。リフレクシブ ACL フローは、すべてのトンネル インターフェイスへの着信および発信トラフィックの場合、ハードウェアによって加速化されません。
- 特定のポート上の ACL アクセス違反の IP アカウンティングは、拒否されリークされた ACL パケットの場合にのみ、そのポート上で拒否された全パケットを RP に転送し、ソフトウェアで処理させることによってサポートされます。この動作は他のフローには影響しません。
- MAC ACL は、スイッチ ポート（MAC PACL）または VLAN 上で、ハードウェアで VACL の一部としてサポートされます。
- PFC では、ハードウェアで Cisco IOS IPX ACL をサポートしません。Cisco IOS IPX ACL は、RP のソフトウェアでサポートされます。
- 名前ベースの拡張 MAC アドレス ACL は、ハードウェアでサポートされています。
- 次の ACL タイプは、ソフトウェアによって処理されます。
  - Internetwork Packet Exchange（IPX）アクセス リスト
  - 標準 XNS アクセス リスト
  - 拡張 XNS アクセス リスト
  - DECnet アクセス リスト
  - プロトコル タイプコード アクセス リスト

（注） ヘッダー長が 5 バイト未満の IP パケットは、アクセス コントロールされません。

- Optimized ACL Logging（OAL; 最適化 ACL ロギング）を設定しない限り、ロギングを必要とするフローはソフトウェアで処理され、ハードウェアでの非ロギング フローの処理には影響しません（「最適化された ACL ロギング」（P.69-13）を参照）。
- ソフトウェアで処理されるフローの転送レートは、ハードウェアで処理されるフローに比べると、大幅に小さくなります。
- ハードウェア統計情報機能がイネーブルである場合に、**show ip access-list** コマンドの出力に表示される一致カウントには、ハードウェアで処理されたパケットが含まれます。
- PFC インターフェイスで **ip unreachables config** コマンドを入力すると、ハードウェアの動作は、変更されないままです。
- IPv4 および IPv6 のヒットレス TCAM アップデートは、TCAM の新機能のアップデート一方で、着信トラフィックに既存の機能を適用する機能があります。特定のインターフェイスの IPv6 ACL の変更によって、すべてのインターフェイス上のすべての IPv6 機能の再プログラミングをトリガーする IPv6 トラフィックには、ヒットレス機能アップデートが必須です。
- ヒットレス アップデートは、デフォルトでイネーブルです。ヒットレス アップデートをディセーブルにするには、**no platform hardware acl update-mode hitless** コマンドを入力します。

（注） 一部のリリース固有の制限事項については、「eFSU の制約事項」（P.5-2）を参照してください。

- ヒットレス アップデートがイネーブルである場合、FM（機能マネージャ）またはスイッチが最近変更された ACL に対してアップデートを実行すると、各 TCAM エントリのコピーがハードウェアにプログラムされます。ACL が変更されていない場合、ヒットレス アップデート用に予約された TCAM スペースは、最も大きい ACL で使用される TCAM エントリの数と等しくなります。

ポリシーベース ACL（PBACL）

PBACL の制約事項

- PBACL はレイヤ 3 インターフェイスでサポートされています（ルーテッド インターフェイスおよび VLAN インターフェイスなど）。
- PBACL 機能によりサポートされるのは IPv4 ACE だけです。
- PBACL 機能では、Cisco IOS ACL だけがサポートされます。それ以外の機能との組み合わせはサポートされません。キーワード **reflexive** および **evaluate** はサポートされていません。
- PBACL 機能では、名前付き Cisco IOS ACL だけがサポートされます。番号付き ACL はサポートされません。
- ポリシーベース ACL の相互作用機能は Cisco IOS ACL と同じです。

PBACL について

PBACL により、オブジェクト グループ全体にアクセス コントロール ポリシーを適用することができます。オブジェクト グループとはユーザまたはサーバの集合です。

オブジェクト グループを IP アドレスの集合として、またはプロトコル ポートの集合として定義します。それからポリシー（許可や拒否など）をオブジェクト グループに適用するアクセス コントロール エントリ（ACE）を作成します。たとえば、ユーザ グループがあるサーバ グループにアクセスすることを許可するポリシーベース ACE を作成することができます。

グループ名を使用して定義された ACE は、ACE が複数あるのと同じです（オブジェクト グループの各エントリに 1 つ適用されます）。PBACL ACE はシステムにより複数の Cisco IOS ACE に拡張され（グループ内の各エントリに対して 1 つの ACE）、ACE は TCAM に読み込まれます。したがって、PBACL 機能により設定が必要なエントリ数が削減されますが、TCAM 使用率は削減されません。

グループ メンバーシップまたはアクセス グループを使用する ACE の内容に変更を行う場合、TCAM 内の ACE がシステムにより更新されます。次に、更新を開始する変更のタイプを示します。

- グループへのメンバの追加
- グループからのメンバの削除
- アクセス グループを使用する ACE のポリシー文の変更

Cisco IOS ACL 拡張コンフィギュレーション コマンドを使用して PBACL を設定します。通常の ACE と同様に、同じアクセス ポリシーを 1 つまたは複数のインターフェイスと関連付けることができます。

ACE の設定時にオブジェクト グループを使用して送信元、宛先、またはその両方を定義できます。

PBACL の設定方法

- 「PBACL オブジェクト グループを使用する ACL の作成」（P.69-8）
- 「インターフェイスでの PBACL の設定」（P.69-8）

PBACL の IP アドレスのオブジェクト グループの設定

PBACL の IP アドレスのオブジェクト グループを作成または変更するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# object-group ip address object_group_name`	オブジェクト グループ名を定義します。IP アドレス オブジェクト グループ コンフィギュレーション モードを開始します。
ステップ 2	`Router(config-ipaddr-ogroup)# {ip_address mask} | {host {name | ip_address} }`	グループのメンバを設定します。メンバは、ネットワーク アドレスにマスクを付加したものか（ホスト名または IP アドレスにより識別される）ホストかのどちらかです。
ステップ 3	`Router(config-ipaddr-ogroup)# {end} | {exit}`	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。 IP アドレス オブジェクト グループ コンフィギュレーション モードを終了するには、**exit** コマンドを入力します。

次に、3 つのホストと 1 つのネットワーク アドレスを含むオブジェクト グループを作成する例を示します。

```
Router(config)# object-group ip address myAG
Router(config-ipaddr-pgroup)# host 10.20.20.1
Router(config-ipaddr-pgroup)# host 10.20.20.5
Router(config-ipaddr-pgroup)# 10.30.0.0 255.255.0.0
```

PBACL のプロトコル ポートのオブジェクト グループの設定

PBACL のプロトコル ポートのオブジェクト グループを作成または変更するには、次の作業を行います。

コマンド	目的
`Router(config)# object-group ip port object_group_name`	オブジェクト グループ名を定義します。ポート オブジェクト グループ コンフィギュレーション モードを開始します。
`Router(config-port-ogroup)# {eq number} | {gt number} | {lt number} | {neq number} | {range number number}`	グループのメンバを設定します。メンバは、ポート番号と等しいまたは等しくない、ポート番号より大きいまたは小さい、またはポート番号の範囲のいずれかです。
`Router(config-port-ogroup)# end | exit`	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。 ポート オブジェクト グループ コンフィギュレーション モードを終了するには、**exit** コマンドを入力します。

次に、プロトコル ポート 100 と、300 以外の 200 より大きいポートと一致するポートのオブジェクト グループを作成する例を示します。

```
Router(config)# object-group ip port myPG
Router(config-port-pgroup)# eq 100
Router(config-port-pgroup)# gt 200
Router(config-port-pgroup)# neq 300
```

PBACL オブジェクト グループを使用する ACL の作成

PBACL オブジェクト グループを使用するように ACL 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 access-list extended acl_name`	名前を指定して拡張 ACL を定義します。拡張 ACL 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	`Router(config-ext-nacl)# permit tcp addrgroup object_group_name addrgroup object_group_name`	IP アドレスのオブジェクト グループを送信元ポリシーとして、オブジェクト グループを宛先ポリシーとして使用する、TCP トラフィックの ACE を設定します。
ステップ 3	`Router(config-ext-nacl)# exit`	拡張 ACL コンフィギュレーション モードを終了します。

次に、プロトコル ポートが myPG に指定されたポートと一致する場合に、myAG 内のユーザからのパケットを許可するアクセス リストを作成する例を示します。

```
Router(config)# ip access-list extended my-pbacl-policy
Router(config-ext-nacl)# permit tcp addrgroup myAG portgroup myPG any
Router(config-ext-nacl)# deny tcp any any
Router(config-ext-nacl)# exit
Router(config)# exit
Router# show ip access-list my-pbacl-policy
Extended IP access list my-pbacl-policy
10  permit tcp addrgroup AG portgroup PG any
20  permit tcp any any
Router# show ip access-list my-pbacl-policy expand
Extended IP access list my-pbacl-policy expanded
20 permit tcp host 10.20.20.1 eq 100 any
20 permit tcp host 10.20.20.1 gt 200 any
20 permit tcp host 10.20.20.1 neq 300 any
20 permit tcp host 10.20.20.5 eq 100 any
20 permit tcp host 10.20.20.5 gt 200 any
20 permit tcp host 10.20.20.5 neq 300 any
20 permit tcp 10.30.0.0 255.255.0.0 eq 100 any
20 permit tcp 10.30.0.0 255.255.0.0 gt 200 any
20 permit tcp 10.30.0.0 255.255.0.0 neq 300 any
```

インターフェイスでの PBACL の設定

インターフェイスでの PBACL を設定するには、**ip access-group** コマンドを使用します。このコマンド構文および使用方法は Cisco IOS ACL と同じです。詳細は、「Cisco IOS ACL の制約事項」（P.69-1）を参照してください。

次に、アクセス リスト my-pbacl-policy と VLAN 100 を関連付ける例を示します。

```
Router(config)# int vlan 100
Router(config-if)# ip access-group mp-pbacl-policy in
```

MAC ACL

（注）　VLAN ACL（VACL）で MAC ACL を使用できます。詳細については、第 74 章「VLAN ACL（VACL）」を参照してください。

Protocol-Independent MAC ACL フィルタリングの設定方法

プロトコル独立型 MAC ACL フィルタリングでは、すべての入力トラフィック タイプ（MAC レイヤ トラフィック、IPv4 トラフィック、IPv6 トラフィック、MPLS トラフィックなど）に MAC ACL が適用されます。

次のインターフェイス タイプをプロトコル独立型 MAC ACL フィルタリングに設定できます。

- VLAN インターフェイス
- ルーテッド インターフェイス
- 物理 LAN ポート
- 論理 LAN サブインターフェイス

プロトコル独立型 MAC ACL フィルタリング用に設定されたインターフェイスの MAC ACL によって許可または拒否された入力トラフィックは、出力インターフェイスによって MAC レイヤ トラフィックとして処理されます。プロトコル独立型 MAC ACL フィルタリング用に設定されたインターフェイスの MAC ACL によって許可または拒否されたトラフィックには、出力 IP ACL を適用できません。

プロトコル独立型 MAC ACL 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
ステップ 1	`Router(config)# interface {{vlan vlan_ID}	{type slot/port[.subinterface]}	{port-channel number[.subinterface]}}`	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# [no] mac packet-classify {input	output	use {ce_cos {input	output}	dscp {input	output}}}`	インターフェイス上でプロトコル独立型 MAC ACL フィルタリングをイネーブルにします。デフォルトでは、**mac packet-classify** 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。

- IP アドレスが設定されている VLAN インターフェイス上で、プロトコル独立型 MAC ACL フィルタリングを設定しないでください。
- MAC ACL フィルタリングがイネーブルの場合、RACL、マイクロフロー ポリシングなどの他のプロトコル機能は、すべてハードウェアでは無視されます。

次に、VLAN インターフェイス 4018 をプロトコル独立型 MAC ACL フィルタリングに設定し、設定を確認する例を示します。

```
Router(config)# interface vlan 4018
Router(config-if)# mac packet-classify
Router(config-if)# end
```

```
Router# show running-config interface vlan 4018 | begin 4018
interface Vlan4018
mtu 9216
ipv6 enable
mac packet-classify
end
```

次に、インターフェイス GigabitEthernet 6/1 をプロトコル独立型 MAC ACL フィルタリングに設定し、設定を確認する例を示します。

```
Router(config)# interface gigabitethernet 6/1
Router(config-if)# mac packet-classify
Router(config-if)# end
Router# show running-config interface gigabitethernet 6/1 | begin 6/1
interface GigabitEthernet6/1
mtu 9216
no ip address
mac packet-classify
mpls l2transport route 4.4.4.4 4094
end
```

次に、インターフェイス GigabitEthernet 3/24 およびサブインターフェイス 4000 をプロトコル独立型 MAC ACL フィルタリングに設定し、設定を確認する例を示します。

```
Router(config)# interface gigabitethernet 3/24.4000
Router(config-if)# mac packet-classify
Router(config-if)# end
Router# show running-config interface gigabitethernet 3/24.4000 | begin 3/24.4000
interface GigabitEthernet3/24.4000
encapsulation dot1Q 4000
mac packet-classify
mpls l2transport route 4.4.4.4 4000
end
```

VLAN ベースの MAC QoS フィルタリングをイネーブルにする方法

MAC ACL の VLAN ベースの QoS フィルタリングをグローバルにイネーブルまたはディセーブルにできます。MAC ACL の VLAN ベースの QoS フィルタリングは、デフォルトではディセーブルに設定されています。

MAC ACL の VLAN ベースの QoS 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
`Router(config)# mac packet-classify use outer-vlan`	MAC ACL の VLAN ベースの QoS フィルタリングをイネーブルにします。MAC ACL の VLAN フィールドは外側 VLAN タグに一致します。 オプションは、**in**（入力 MAC ACL に適用する）および **out**（出力 MAC ACL に適用する）です。

MAC ACL の VLAN ベースの QoS フィルタリ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
`Router(config)# no mac packet-classify use outer-vlan`	MAC ACL の VLAN ベースの QoS フィルタリングをディセーブルにします。

MAC ACL の設定

MAC アドレスに基づいて IP、IPX、DECnet、AppleTalk、VINES、または XNS トラフィックをフィルタリングする名前付き ACL を設定できます。

VLAN ベースのフィルタリング、CoS ベースのフィルタリング、またはその両方を行う MAC ACL を設定できます。

MAC ACL の VLAN ベースの QoS フィルタリングを、グローバルにイネーブルまたはディセーブルにできます（デフォルトではディセーブル）。

MAC ACL 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)# mac host name mac_addr`	（任意）名前 MAC アドレスに割り当てます。
ステップ 2	`Router(config)# mac access-list extended list_name`	MAC ACL を設定します。
ステップ 3	`Router(config-ext-macl)# {permit | deny} {src_mac_mask | {host name src_mac_name} | any} {dest_mac_mask | {host name dst_mac_name} | any} [{protocol_keyword | {ethertype_number ethertype_mask}} [vlan vlan_ID] [cos cos_value]]`	MAC ACL にアクセス コントロール エントリ（ACE）を設定します。送信元および宛先 MAC アドレスは、MAC アドレス マーク、または **mac host** コマンドで作成された名前で指定できます。

- Cisco IOS Release 15.1SY は **vlan** および **cos** キーワードをサポートします。
- MAC ACL の VLAN ベースの QoS フィルタリング用の **vlan** キーワードを、グローバルにイネーブルまたはディセーブルにすることができます（デフォルトではディセーブル）。
- MAC アドレスは、ドット付き 16 進表記の 3 つの 2 バイト値で入力できます。たとえば、0030.9629.9f84 を入力できます。
- MAC アドレス マスクは、ドット付き 16 進表記の 3 つの 2 バイト値で入力できます。1 のビットをワイルドカードとして使用します。たとえば、アドレスを完全に一致させるには、0000.0000.0000 を使用します（0.0.0 として入力できます）。
- EtherType および EtherType マスクを 16 進値で入力できます。
- protocol パラメータなしのエントリはどのプロトコルとも一致します。
- ACL エントリは、入力順にスキャンされます。最初に一致したエントリが使用されます。パフォーマンスを向上させるには、最もよく使用されるエントリを ACL の先頭に置きます。
- ACL の末尾に **permit any any** エントリを明示的に指定する場合を除いて、ACL の末尾には暗黙的な **deny any any** エントリが存在します。
- 新しいエントリはすべて既存のリストの最後に置かれます。リストの中間にエントリを追加することができません。
- 次に、EtherType の値と対応するプロトコル キーワードを示します。
  - 0x0600 - xns-idp - Xerox XNS IDP
  - 0x0BAD - vines-ip - Banyan VINES IP
  - 0x0baf - vines-echo - Banyan VINES Echo
  - 0x6000 - etype-6000 - DEC 未割り当て、実験的
  - 0x6001 - mop-dump - DEC Maintenance Operation Protocol（MOP; メンテナンス オペレーション プロトコル）ダンプ/ロード補助
  - 0x6002 - mop-console - DEC MOP リモート コンソール

- 0x6003 - decnet-iv - DEC DECnet Phase IV Route
- 0x6004 - lat - DEC Local Area Transport（LAT; ローカルエリア トランスポート）
- 0x6005 - diagnostic - DEC DECnet Diagnostics
- 0x6007 - lavc-sca - DEC Local-Area VAX Cluster（LAVC）、SCA
- 0x6008 - amber - DEC AMBER
- 0x6009 - mumps - DEC MUMPS
- 0x0800 - ip - 不正な形式、無効、または意図的に壊された IP フレーム
- 0x8038 - dec-spanning - DEC LANBridge Management
- 0x8039 - dsm - DEC DSM/DDP
- 0x8040 - netbios - DEC PATHWORKS DECnet NETBIOS Emulation
- 0x8041 - msdos - DEC Local Area System Transport
- 0x8042 - etype-8042 - DEC 未割り当て
- 0x809B - appletalk - Kinetics EtherTalk（AppleTalk over Ethernet）
- 0x80F3 - aarp - Kinetics AppleTalk Address Resolution Protocol（AARP）

次に、mac_layer という名前の MAC レイヤ ACL を作成する例を示します。この ACL は、送信元アドレスが 0000.4700.0001、宛先アドレスが 0000.4700.0009 である dec-phase-iv トラフィックを拒否しますが、それ以外のトラフィックをすべて許可します。

```
Router(config)# mac access-list extended mac_layer
Router(config-ext-macl)# deny 0000.4700.0001 0.0.0 0000.4700.0009 0.0.0 dec-phase-iv
Router(config-ext-macl)# permit any any
```

ARP ACL

ここでは、ARP ACL の設定方法について説明します。ARP トラフィック（EtherType 0x0806）をフィルタリングする名前付き ACL を設定できます。ARP ACL 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)# arp access-list list_name`	ARP ACL を設定します。
ステップ 2	`Router(config-arp-nacl)# {permit | deny} {ip {any | host sender_ip | sender_ip sender_ip_wildcardmask} mac any`	ARP ACL にアクセス コントロール エントリ（ACE）を設定します。

- ここでは、PFC によってハードウェアでサポートされる ARP ACL 構文について説明します。疑問符（?）を入力した場合に CLI ヘルプで表示されるその他の ARP ACL 構文はサポートされず、QoS の ARP トラフィックのフィルタリング処理にも使用できません。
- ACL エントリは、入力した順序に従ってスキャンされます。最初に一致したエントリが使用されます。パフォーマンスを向上させるには、最もよく使用されるエントリを ACL の先頭に置きます。
- リストの末尾に **permit ip any mac any** エントリを明示的に指定する場合を除いて、ACL の末尾には暗黙的な **deny ip any mac any** エントリが存在します。
- 新しいエントリはすべて既存のリストの最後に置かれます。リストの中間にエントリを追加することができません。
- PFC は IP ACL を ARP トラフィックに適用しません。

- ARP トラフィックには、マイクロフロー ポリシングを適用できません。

次に、arp_filtering という名前の ARP ACL を作成する例を示します。この ACL は、IP アドレスが 1.1.1.1 から始まるトラフィックだけを許可します。

```
Router(config)# arp access-list arp_filtering
Router(config-arp-nacl)# permit ip host 1.1.1.1 mac any
```

最適化された ACL ロギング

OAL の制約事項

- OAL キャプチャと VACL キャプチャには互換性がありません。スイッチに両方の機能を設定しないでください。OAL が設定された状態で、SPAN を使用してトラフィックをキャプチャします。
- OAL は、VACL キャプチャ、合法的傍受（LI）、および IPv6 学習などのキャプチャを使用して他の機能との競合をチェックします。
- OAL は IPv4 ユニキャスト パケットだけをサポートしています。
- OAL はポート ACL（PACL）ではサポートされません。
- OAL は、次のものに対してはハードウェアでのサポートをしていません。
  - 再帰 ACL
  - 他の機能（QoS など）のトラフィックのフィルタ処理に使用される ACL
  - Unicast Reverse Path Forwarding（uRPF; ユニキャスト RPF）チェック例外のための ACL
  - 例外パケット（Time To Live（TTL）障害や MTU 障害など）
  - IP オプションが指定されたパケット
  - レイヤ 3 でルータへのアドレスが指定されたパケット
  - ICMP 到達不能メッセージを生成するために RP へ送信されるパケット
  - ハードウェアでは加速されず、機能によって処理されるパケット

OAL について

OAL は、ACL ロギングをハードウェアでサポートしています。OAL を設定しないかぎり、ロギングを必要とするパケットは、RP のソフトウェアで完全に処理されます。OAL では、PFC または DFC のハードウェアでパケットの許可またはドロップを行います。情報は最適化ルーチンを使用して RP に送信され、ロギング メッセージが生成されます。

OAL の設定方法

- 「OAL 情報の表示」（P.69-15）
- 「キャッシュされた OAL エントリのクリア」（P.69-15）

OAL グローバル パラメータの設定

OAL グローバル 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
`Router(config)# logging ip access-list cache {{entries number_of_entries} | {interval seconds} | {rate-limit number_of_packets} | {threshold number_of_packets}}`	OAL グローバル パラメータを設定します。

- **entries** *number_of_entries*
  - キャッシュされるエントリの最大数を設定します。
  - 範囲：0 ～ 1,048,576（カンマを含めないで入力）
  - デフォルト：8192
- **interval***seconds*
  - ログのためにエントリが送信されるまでの最大時間を設定します。この時間中エントリが非アクティブの場合、キャッシュから削除されます。
  - 範囲：5 ～ 86,400（1440 分つまり 24 時間、カンマを含めないで入力）
  - デフォルト：300 秒（5 分）
- **rate-limit** *number_of_packets*
  - ソフトウェアで 1 秒間にログに記録されるパケット数を設定します。
  - 範囲：10 ～ 1,000,000（カンマを含めないで入力）
  - デフォルト：0（レート制限がオフになり、すべてのパケットがログに記録されます）
- **threshold** *number_of_packets*
  - エントリがログに記録されるまでに一致するパケット数を設定します。
  - 範囲：1 ～ 1,000,000（カンマを含めないで入力）
  - デフォルト：0（一致パケット数に達してもログの記録は開始されません）

インターフェイスでの OAL の設定

インターフェイスで OAL 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)# interface {{type 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	`Router(config-if)# logging ip access-list cache in`	インターフェイスの入力トラフィックに対して OAL をイネーブルにします。
ステップ 3	`Router(config-if)# logging ip access-list cache out`	インターフェイスの出力トラフィックに対して OAL をイネーブルにします。

OAL 情報の表示

OAL 情報を表示するには、次の作業を行います。

コマンド	目的
`Router# show logging ip access-list cache`	OAL 情報を表示します。

キャッシュされた OAL エントリのクリア

キャッシュされた OAL エントリをクリアするには、次の作業を行います。

コマンド	目的
`Router# clear logging ip access-list cache`	キャッシュされた OAL エントリをクリアします。

ACL のドライ ランのサポート

ドライ ランのサポートの制約事項

- ドライ ランは IPv4 RACL に対してだけサポートされており、インターフェイスにだけ適用できます。
- ドライ ランは名前付き ACL（標準または拡張）でのみサポートされ、番号付き ACL ではサポートされません。
- 1 つのドライ ラン セッションだけが、ドライ ラン セッション上の 1 つまたは複数の ACL と同時に割り当てられます。
- ACL がコンフィギュレーション モードで変更されると、1 つまたは複数のドライ ラン セッション ACL は削除されます。
- ドライ ラン セッションを終了しても、既存の設定はクリアされません。新しい設定を開始する前に、既存のセッションをクリアします。
- 検証プロセス中に設定またはハードウェアの変更がある場合、検証プロセスは中断される可能性があります。
- ドライ ラン モードは、実行コンフィギュレーションに対する変更のコミットをサポートしません。
- ドライ ランは QoS ポリシーで使用される ACL ではサポートされません。
- ドライ ランは、ハードウェア統計情報をイネーブルにした ACL ではサポートされません。
- ドライ ランセッションの進行中に、別の Telnet セッションを使用してスイッチにアクセスできます。

ドライ ランのサポートについて

他のリリースでは、他の機能とともに設定されたインターフェイスに既存の機能の新しい機能を適用する場合、および新しい機能が TCAM に適合しない場合、既存の機能も影響を受け、TCAM から削除されます。機能を段階的にアップデートし、インストールすることなしに機能が TCAM に適合するかどうかを判断するため、スイッチはドライ ランをサポートします。これによって、アプリケーションは通常の要求を送信して、要求を正常にプログラムすることができるかどうかをテストできます。スイッチは、ドライ ラン要求を受信し、その要求に必要な総 TCAM リソースを計算し、使用可能な空きリソースに対してこれらのリソースを比較します。要求が正常に適合した場合は、スイッチが成功を返し、そうでない場合は、失敗を返します。ドライ ラン サポートは、アプリケーションがインテリジェントな判断を行うために役立ちます。

ACL のドライ ラン サポートの設定方法

ドライ ラン 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	`Router(config)# configure session session_name`	コンフィギュレーション セッションを作成し、ドライ ラン モードを開始します
ステップ 2	`Router(dry-run-config)# {default | exit | ip | no | validate}`	ドライ ラン セッションを設定するオプションを選択します。
ステップ 3	`Router(dry-run-config)# ip access-list {extended | standard} acl_name`	ACL タイプを選択します。

次に、既存の ACL RACL10K でセッションにドライ ラン サポートを設定する例を示します。

```
Router(config)# configure session test
Router(dry-run-config)# ip access-list extended RACL10K
Router(dr-config-ext-nacl)# permit tcp host 10.20.0.1 host 11.20.0.1
Router(dr-config-ext-nacl)# permit tcp host 10.20.0.2 host 11.20.0.2
Router(dr-config-ext-nacl)# permit tcp host 10.20.0.3 host 11.20.0.3
Router(dr-config-ext-nacl)# permit tcp host 10.20.0.4 host 11.20.0.4
Router(dr-config-ext-nacl)# permit tcp host 10.20.0.5 host 11.20.0.5

Router(dr-config-ext-nacl)# exit

Router(dry-run-config)# validate

Router(dry-run-config)# exit
Router#
.Feb 23 2010 13:46:52.528: Validation is in progress !!
.Feb 23 2010 13:46:52.528: Please try again later.
.Feb 23 2010 13:46:53.136: %FM-6-SESSION_VALIDATION_RESULT_INFO: Session Validation Result
:  "Validation Completed Sucessfully."
. Please use 'show config session test status' to get more details of the config
validation status

Router# show configuration session test status
=====================================
Status of last config validation:
Timestamp: 2010-02-23@13:46:51
=====================================
SLOT = [1]    Result = Configuration will fit in TCAM
SLOT = [2]    Result = Configuration will fit in TCAM
SLOT = [5]    Result = Configuration will fit in TCAM
```

```
Router# clear configuration session test

Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# ip access-list extended RACL10K
Router(config-ext-nacl)# permit tcp host 10.20.0.1 host 11.20.0.1
Router(config-ext-nacl)# permit tcp host 10.20.0.2 host 11.20.0.2
Router(config-ext-nacl)# permit tcp host 10.20.0.3 host 11.20.0.3
Router(config-ext-nacl)# permit tcp host 10.20.0.4 host 11.20.0.4
Router(config-ext-nacl)# permit tcp host 10.20.0.5 host 11.20.0.5
Router(config-ext-nacl)# end

Router#
```

ハードウェア ACL 統計情報

ハードウェア ACL 統計情報の制約事項

- ハードウェア ACL 統計情報は、入力と出力の両方向の IPv4 および IPv6 RACL でサポートされます。
- IPv4 では、ハードウェア ACL 統計情報は、番号付きと名前付きの両方の ACL でサポートされます。
- ハードウェア統計情報は、60 秒ごとにハードウェアをポーリングすることによって取得されます。
- ハードウェア統計情報はステートフル スイッチオーバー（SSO）後に失われます。
- ハードウェア統計情報は ACL ごとに保持されます。複数のインターフェイスが同じ ACL を使用している場合、統計情報は集約されます。
- ODM（Order-Dependent Merge）の最適化をイネーブルにすると、ハードウェア統計情報はディセーブルになります。

ハードウェア ACL 統計情報について

ハードウェア ACL 統計情報を使用して、特定の ACL のハードウェア カウンタは収集され、集約され、IOS のアクセス リストの出力に表示されます。

ACE ヒット カウントはハードウェアから取得され、次のコマンドを使用して表示できます。

show ip access-list および **show ipv6 access-list**

ハードウェア統計は、デフォルトではディセーブルです。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、ハードウェア統計情報のコマンドを入力します。

ハードウェア ACL 統計情報の設定方法

次に、ACL racl1 のハードウェア統計情報をイネーブルにする例を示します。

```
Router(config)# ip access-list extended racl1
Router(config-ext-nacl)# [no] hardware statistics
Router(config-ext-nacl)# permit ip host 1.1.1.1 host 2.2.2.2
Router(config-ext-nacl)# permit ip host 3.3.3.3 host 4.4.4.4
Router(config-ext-nacl)# deny ip any any
Router(config-ext-nacl)# end
```

次に、ACL racl1 のハードウェア統計情報を表示する例を示します。

```
Router# show ip access-lists racl1
Extended IP access list racl1
    hardware statistics
    10 permit ip host 1.1.1.1 host 2.2.2.2
acl hw hit count 5
    20 permit ip host 3.3.3.3 host 4.4.4.4
acl hw hit count 20
    30 deny ip any any
```

各 ACE のハードウェア統計情報は、**acl hw hit count** の文字列の後に表示され、ハードウェアでスイッチングされたパケットの数を示します。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

Cisco TrustSec（CTS）

Cisco TrustSec は、ネットワーク内のユーザ、ホスト、およびネットワーク デバイスを強力に識別する機能に基づいた、シスコ ネットワーク デバイスのセキュリティの改善に関する包括的な用語です。TrustSec は、特定のロールについてデータ トラフィックを一意に分類することで、トポロジに依存しない、スケーラブルなアクセス コントロールを実現します。TrustSec は、認証されたピアおよびこれらのピアとの暗号化リンク間で信頼を確立することで、データの機密保持および整合性を保証します。

Cisco TrustSec の主要コンポーネントは、Cisco Identity Services Engine です。これは、Cisco ISE で TrustSec アイデンティティおよびセキュリティ グループ ACL（SGACL）を使用してスイッチをプロビジョニングする場合に一般的です。ただし、これらは Catalyst 6500 で手動で設定する場合があります。

Cisco Catalyst 6500 シリーズ スイッチで Cisco Trustsec を設定するには、次の URL の『*Cisco TrustSec Switch Configuration Guide*』を参照してください。

http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/trustsec.html

Cisco TrustSec General Availability リリースのリリース ノートについては、次の URL を参照してください。

http://www.cisco.com/en/US/docs/switches/lan/trustsec/release/notes/rn_cts_crossplat.html

Cisco TrustSec Solution の詳細（概要、データシート、およびケース スタディなど）については、次の URL を参照してください。

http://www.cisco.com/en/US/netsol/ns1051/index.html

表 1 に、TrustSec がイネーブルになった Cisco スイッチで実装される TrustSec 機能を示します。継続的な TrustSec の General Availability リリースによって、サポートされるスイッチの数および各スイッチでサポートされる TrustSec 機能の数は増加しています。

Catalyst 6500 ラインカードでサポートされる TrustSec 機能の詳細については、「サポートされるハードウェア」を参照してください。

表 1　Cisco TrustSec の主要機能：TrustSec 1.0 General Availability 2010 Release

Cisco TrustSec の機能	説明
802.1AE タギング（MACSec）	IEEE 802.1AE に基づくワイヤレート ホップ単位レイヤ 2 暗号化のプロトコル。 MACSec 対応デバイス間において、パケットは送信デバイスからの出力で暗号化され、受信デバイスへの入力で復号化されます。デバイス内では平文です。 この機能は、TrustSec ハードウェア対応デバイス間だけで利用できます。
エンドポイント アドミッション コントロール（EAC）	EAC は、TrustSec ドメインに接続しているエンドポイント ユーザまたはデバイスの認証プロセスです。通常、EAC はアクセス レベル スイッチで実行されます。EAC プロセスの認証および許可に成功すると、ユーザまたはデバイスに対してセキュリティ グループ タグが割り当てられます。現在、EAC は 802.1X、MAC 認証バイパス（MAB）、および Web 認証プロキシ（WebAuth）とすることができます。
ネットワーク デバイス アドミッション コントロール（NDAC）	NDAC は、TrustSec ドメイン内の各ネットワーク デバイスがピア デバイスのクレデンシャルおよび信頼性を確認できる認証プロセスです。NDAC は、IEEE 802.1X ポート ベースの認証に基づく認証フレームワークを利用し、EAP 方式として EAP-FAST を使用します。NDAC プロセスの認証および許可に成功すると、IEEE 802.1AE 暗号化のセキュリティ アソシエーション プロトコル ネゴシエーションとなります。
セキュリティ グループ アクセス コントロール リスト（SGACL）	セキュリティ グループ アクセス コントロール リスト（SGACL）は、セキュリティ グループ タグをポリシーと関連付けます。ポリシーは、TrustSec ドメインから出力される SGT タグ付きトラフィックに対して適用されます。
セキュリティ アソシエーション プロトコル（SAP）	NDAC 認証のあと、セキュリティ アソシエーション プロトコル（SAP）は、その後の TrustSec ピア間の MACSec リンク暗号化のキーおよび暗号スイートについて、自動的にネゴシエーションを行います。SAP は IEEE 802.11i で定義されます。
セキュリティ グループ タグ（SGT）	SGT は、TrustSec ドメイン内の送信元のセキュリティ分類を示す 16 ビットの単一ラベルです。イーサネット フレームまたは IP パケットに追加されます。
SGT 交換プロトコル（SXP）	Security Group Tag Exchange Protocol（SXP）。TrustSec ハードウェア対応ではないデバイスは、SXP により、Cisco ACS から認証されたユーザまたはデバイスの SGT 属性を受信し、sourceIP-to-SGT バインディングを TrustSec ハードウェア対応デバイスに転送し、タギングおよび SGACL を適用できます。

サポートされるハードウェア

表 70-2 に、Catalyst 6500 ラインカードでサポートされている Cisco TrustSec レベルの一覧を示します。この表の内容は、次の URL にあるホワイト ペーパー『*Cisco Catalyst 6500 Series with Supervisor Engine 2T: Enabling Cisco TrustSec with Investment Protection*』から入手されたものです。

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/white_paper_c11-658388.html

表 70-2　Cisco TrustSec の Cisco Catalyst 6500 ラインカードのサポート レベル

Cisco TrustSec のサポート レベル	説明	ラインカード
Cisco TrustSec 対応	セキュリティ グループ タグ インポジションおよび IEEE 802.1AE MACsec のハードウェア アクセラレーションを使用する完全な Cisco TrustSec 機能をサポートします。	Supervisor Engine 2T、およびすべての 6900 シリーズ ラインカード
Cisco TrustSec 認識	セキュリティ グループ タグ インポジションまたは IEEE 802.1AE MACsec をサポートしていません。これらのラインカードは、セキュリティ グループ タグ情報を含む転送の決定を理解できます。これにより、出力の Cisco TrustSec 対応ラインカードにトラフィックを転送できます。	• WS-X6816-10T-2T、WS-X6716-10T • WS-X6816-10G-2T、WS-X6716-10GE
Cisco TrustSec の使用に非対応	セキュリティ グループ タグ インポジションまたは IEEE 802.1AE MACsec をサポートせず、セキュリティ グループ タグ情報を含む転送の決定を解釈できません。	• WS-X6824-SFP-2T WS-X6724-SFP • WS-X6848-SFP-2T WS-X6748-SFP • WS-X6848-TX-2T WS-X6748-GE-TX • WS-X6704-10G • WS-X6148 シリーズ（すべて）

すべての Cisco TrustSec ハードウェア プラットフォームおよび機能のサポートの詳細については、次の URL にある TrustSec Product Bulletin を参照してください。

http://www.cisco.com/en/US/netsol/ns1051/index.html

CHAPTER 71

AutoSecure

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

AutoSecure の前提条件

これらの質問に答える準備ができている必要があります。

- 装置はインターネットに接続する予定かどうか。
- いくつのインターフェイスをインターネットに接続するか。
- インターネットに接続するインターフェイスの名前は何か。
- どのようなローカル ユーザ名およびパスワードを使用するか。
- スイッチのホスト名およびドメイン名は何か。

AutoSecure の制約事項

- AutoSecure によって行われた設定変更を元に戻すコマンドがないため、AutoSecure の設定を行う前に実行コンフィギュレーションを必ず保存してください。
- AutoSecure の設定は、実行時またはセットアップ時に行います。AutoSecure をイネーブルにした後に、関連する設定を変更した場合は、AutoSecure の設定が完全に有効にならないことがあります。
- AutoSecure がイネーブルになると、装置のモニタおよび設定のために SNMP を使用するツールは、SNMP を使用する装置との通信を行うことができなくなります。
- 使用している装置を NM アプリケーションによって管理している場合は、マネジメント プレーンのセキュリティ保護によって HTTP サーバなどのいくつかのサービスがディセーブルになり、NM アプリケーションのサポートが中断されます。
- SDM を使用している場合は、**ip http server** コマンドを使用して、HTTP サーバを手動でイネーブルにする必要があります。
- CDP を使用してネットワーク トポロジを検出する NM アプリケーションは、検出を実行できなくなります。

AutoSecure について

注意　AutoSecure はスイッチのセキュリティ保護に役立ちますが、スイッチの完全なセキュリティを保証するものではありません。

AutoSecure の概要

AutoSecure の利点

AutoSecure 機能を使用すると、すべてのセキュリティ機能を理解することなく、スイッチが保護されます。AutoSecure は簡単なセキュリティ設定プロセスです。不必要なシステム サービスをディセーブルにし、基本的な推奨セキュリティ ポリシーをイネーブルにすることで、セキュアなネットワーキング サービスを保証します。

簡素化されたスイッチのセキュリティ設定

AutoSecure は、スイッチのセキュリティ機能の設定を完全に自動化します。AutoSecure はセキュリティ ホールとして悪用されるおそれがある、デフォルトでイネーブルになっているある種の機能をディセーブルにします。AutoSecure は、個々のニーズに応じて次の 2 つのモードで実行できます。

- インタラクティブ モード：サービスおよびその他のセキュリティ機能を指示に従ってイネーブルまたはディセーブルにするオプションです。各オプションのデフォルト設定が示されます。
- 非インタラクティブ モード：シスコの推奨するデフォルト設定を自動的に実行します。

AutoSecure によってイネーブルになる拡張パスワードのセキュリティ

- 最低限必要なパスワード長を指定できます。これにより、ネットワーク上で広く使用されている「lab」や「cisco」などの脆弱なパスワードの使用を制限できます。

  パスワードの最小長を設定するコマンドは **security passwords min-length** です。
- ログイン試行の失敗回数が設定したしきい値を超えると、Syslog メッセージが生成されるようにすることができます。

  ログイン試行の失敗許容回数（しきい値率）を設定するには、**security authentication failure rate** コマンドを使用します。

システム ロギング メッセージのサポート

システム ロギング メッセージは、実行コンフィギュレーションに適用されている AutoSecure 設定に対してあとから変更が行われた場合にその変更をキャプチャします。その結果、AutoSecure を実行するときにさらに詳細な監査証跡が可能になります。

AutoSecure にってイネーブルになるマネジメント プレーンのセキュリティ

注意　使用している装置をネットワーク管理（NM）アプリケーションによって管理している場合は、マネジメント プレーンのセキュリティ保護によって HTTP サーバなどのいくつかのサービスがディセーブルになり、NM アプリケーションのサポートが中断されます。

マネジメント プレーンのセキュリティの概要

AutoSecure により、スイッチ管理インターフェイス（マネジメント プレーン）およびデータ ルーティングとスイッチングの機能（フォワーディング プレーン。「AutoSecure にってイネーブルになるフォワーディング プレーンのセキュリティ」（P.71-6）を参照）を保護できます。マネジメント プレーンの

セキュリティ保護は、セキュリティ攻撃で悪用される可能性のある特定のグローバル サービスおよびインターフェイス サービスをディセーブルにし、攻撃の脅威を最小限に抑える役に立つグローバル サービスをイネーブルにすることで実施されます。また、セキュア アクセスおよびセキュア ロギングをスイッチに設定します。

AutoSecure によってディセーブルになるグローバル サービス

- Finger：攻撃の前のシステムの情報を収集（探査）します。
- PAD：すべてのパケット アセンブラ/ディスアセンブラ（PAD）コマンドと、PAD デバイスとアクセス サーバとの接続をイネーブルにします。
- スモール サーバ：TCP およびユーザ データグラム プロトコル（UDP）診断ポート攻撃を引き起こします。送信者は、スイッチの UDP 診断サービスに偽の要求を大量に送信して、すべての CPU リソースを消費させます。
- BOOTP サーバ：BOOTP はセキュアではないプロトコルです。攻撃で悪用されます。
- HTTP サーバ：Secure HTTP サーバを使用するか、関連する ACL を持つ HTTP サーバに組み込まれた認証を使用しなければ、HTTP サーバはセキュアではなく、攻撃で悪用されます（HTTP サーバをイネーブルにする必要がある場合は、適切な認証またはアクセス リストの指定を求めるメッセージが表示されます）。

（注）　SDM を使用している場合は、**ip http server** コマンドを使用して、HTTP サーバを手動でイネーブルにする必要があります。

- 識別サービス：セキュアではないプロトコル（RFC 1413 で定義）です。外部ホストから TCP ポートに識別情報を照会できます。攻撃者は、ID サーバでユーザに関する個人的な情報にアクセスできます。
- CDP：大量の Cisco Discovery Protocol（CDP）パケットがスイッチに送信されると、スイッチの利用可能なメモリが消費され、スイッチがクラッシュします。

（注）　CDP を使用してネットワーク トポロジを検出する NM アプリケーションは、検出を実行できなくなります。

- NTP：認証またはアクセス コントロールを行っていない場合は、ネットワーク タイム プロトコル（NTP）はセキュアではありません。攻撃者は、このプロトコルを使用して NTP パケットを送信してスイッチをクラッシュまたは過負荷状態にさせます。

  NTP が必要な場合は、MD5 および **ntp access-group** コマンドを使用して、NTP 認証を設定する必要があります。NTP がグローバルでイネーブルになっている場合は、NTP を必要としないインターフェイスすべてでディセーブルにします。
- 送信元ルーティング：送信元ルーティングはデバッグ目的でだけ提供されており、それ以外の場合はディセーブルにする必要があります。そうしないと、パケットがスイッチのアクセス コントロール メカニズムのいくつかを回避する可能性があります。

AutoSecure によってディセーブルになるインターフェイス単位のサービス

- ICMP リダイレクト：すべてのインターフェイスでディセーブルになります。機能が正しく設定されているネットワークにとっては特に有用というわけではなく、攻撃者はセキュリティ ホールを悪用するためにこの機能を使用することがあります。

- ICMP 到達不能：すべてのインターフェイスでディセーブルになります。Internet Control Management Protocol（ICMP）到達不能は、ICMP ベースの DoS 攻撃（サービス拒絶攻撃）を可能にする方法の 1 つとして知られています。
- ICMP マスク応答メッセージ：すべてのインターフェイスでディセーブルになります。ICMP マスク応答メッセージにより、攻撃者はインターネットワークの特定のサブネットワークのサブネットマスクを入手できます。
- プロキシ ARP：すべてのインターフェイス上でディセーブルにします。プロキシ ARP 要求は、DoS 攻撃を可能にする方法の 1 つとして知られています。これは、攻撃者が繰り返し送信した要求に応答しようとすることで、スイッチの利用可能な帯域幅およびリソースを消費するためです。
- ダイレクト ブロードキャスト：すべてのインターフェイス上でディセーブルにします。DoS を生じさせるための SMURF 攻撃の原因となる可能性があります。
- メンテナンス オペレーション プロトコル（MOP）サービス：すべてのインターフェイスでディセーブルになります。

AutoSecure によってイネーブルになるグローバル サービス

- **service password-encryption** コマンド：パスワードが設定で表示されなくなります。
- **service tcp-keepalives-in** コマンドと **service tcp-keepalives-out** コマンド：異常終了した TCP セッションが確実に削除されます。

AutoSecure によってセキュリティが確保されるスイッチ アクセス

注意　デバイスが NM アプリケーションによって管理されている場合に、スイッチへのアクセスをセキュリティ保護すると、重要なサービスが無効化されたり、NM アプリケーションのサポートが妨げられたりすることがあります。

- テキスト バナーがない場合は、バナーを追加するよう要求されます。AutoSecure 機能には次のサンプル バナーが用意されています。

```
Authorized access only
    This system is the property of ABC Enterprise
    Disconnect IMMEDIATELY if you are not an authorized user!
    Contact abc@example.com +1 408 5551212 for help.
```

- ログインおよびパスワード（サポートされている場合はシークレット パスワードを推奨）は、コンソール、AUX、TTY の各回線で設定されます。**transport input** コマンドおよび **transport output** コマンドも、これらのすべての回線で設定されます （Telnet およびセキュア シェル（SSH）だけが有効な転送方法です）。**exec-timeout** コマンドは、コンソールと AUX の各回線で 10 に設定されます。
- 装置上のイメージが暗号化イメージである場合、AutoSecure はスイッチにアクセスし、ファイル転送を行うために SSH およびセキュア コピー プロトコル（SCP）をイネーブルにします。**ip ssh** コマンドの **timeout** *seconds* および **authentication-retries** *integer* の各オプションは最小数に設定されます （Telnet および FTP は、この操作の影響を受けず、引き続き動作します）。
- スイッチで簡易ネットワーク管理プロトコル（SNMP）を使用しないとユーザが指定する場合は、次の機能のいずれかが発生します。
  - インタラクティブ モードでは、ユーザはコミュニティ ストリングの値にかかわらず SNMP をディセーブルにするかどうか尋ねられます。コミュニティ ストリングはパスワードと同様に機能し、スイッチ上のエージェントへのアクセスを規制します。

  - 非インタラクティブ モードでは、コミュニティ ストリングが public または private である場合に、SNMP はディセーブルになります。

（注）　AutoSecure がイネーブルになると、装置のモニタおよび設定のために SNMP を使用するツールは、SNMP を使用する装置との通信を行うことができなくなります。

- 認証、許可、アカウンティング（AAA）が設定されていない場合は、AutoSecure はローカル AAA を設定します。AutoSecure はユーザにスイッチ上でローカル ユーザ名およびパスワードを設定するよう要求します。

AutoSecure によってイネーブルになるロギング オプション

- すべてのデバッグ メッセージおよびログ メッセージのシーケンス番号とタイム スタンプ。このオプションは、ロギング メッセージを監査するときに役立ちます。
- ログイン関連イベントに対するロギング メッセージ。たとえば、ログイン攻撃が検出され、スイッチが待機モードに入ると、メッセージ「Blocking Period when Login Attack Detected」が表示されます。（待機モードでは、スイッチは Telnet、HTTP、または SSH を使用したログイン試行を許可しません）。
- **logging console critical** コマンド。これにより、システム ロギング（syslog）メッセージがすべての使用可能な TTY 回線に送信され、重大度に応じてメッセージが制限されます。
- **logging buffered** コマンド。これにより、ロギング メッセージが内部バッファにコピーされ、バッファに記録されるメッセージが重大度に応じて制限されます。
- **logging trap debugging** コマンド。これにより、デバッグよりも重大度の高いコマンドをすべてロギング サーバに送信できます。

AutoSecure にってイネーブルになるフォワーディング プレーンのセキュリティ

- ストリクト ユニキャスト リバース パス転送（uRPF）を設定して、偽装された（スプーフィングされた）送信元 IP アドレスが入ってくることで引き起こされる問題を軽減できます。uRPF では、検証可能な送信元 IP アドレスがない IP パケットが破棄されます。
- ハードウェアのレート制限：AutoSecure では、ユーザにプロンプトを表示することなく、次のトラフィック タイプのハードウェアのレート制限をイネーブルにします。
  - IP エラー
  - RPF 失敗
  - ICMP のルートなしメッセージ
  - ICMP の ACL ドロップ メッセージ
  - IPv4 マルチキャスト FIB 欠落メッセージ
  - 部分的にスイッチングされている IPv4 マルチキャスト フローのメッセージ

  AutoSecure では、次のトラフィック タイプについて、ハードウェアのレート制限のオプションが利用できます。
  - ICMP リダイレクト
  - TTL 失敗

- MTU 失敗
- IP ユニキャスト オプション
- IP マルチキャスト オプション
- 入力と出力の ACL ブリッジド パケット

（注）　入力および出力 ACL ブリッジド パケットのレート制限は、ACL ロギングの障害となることがあり、TCP 代行受信、NAT、レイヤ 3 WCCP などのハードウェア加速機能のセッション セットアップ レートを増大させることがあります。

AutoSecure の設定方法

AutoSecure パラメータの設定

auto secure コマンドを使用すると、マネジメント プレーンおよびフォワーディング プレーンのセキュリティを保護するための半インタラクティブなセッション（別名 AutoSecure セッション）を実行できます。このコマンドは、マネジメント プレーンまたはフォワーディング プレーンのセキュリティを保護するだけです。コマンド ラインでどちらのオプションも選択されていない場合は、セッション中にどちらかのプレーンまたは両方のプレーンを選択して設定できます。

またこのコマンドでは、セッションの非インタラクティブな部分の設定をすべて行ってから、インタラクティブな部分の設定を行います。セッションの非インタラクティブな部分は、任意で **no-interact** キーワードを選択することでイネーブルにできます。

プロンプトが表示されているときに疑問符（**?**）を入力するとヘルプが表示され、Ctrl+C を押すとセッションが中断されます。

インタラクティブ モードでは、セッション終了時に、生成された設定をスイッチの実行コンフィギュレーションにコミットするかどうか尋ねられます。非インタラクティブ モードでは、変更は実行コンフィギュレーションに自動的に適用されます。

（注）　AutoSecure により行われた設定変更を元に戻すコマンドはありません。**auto secure** コマンドを実行する前に実行コンフィギュレーションを必ず保存する必要があります。

AutoSecure 設定プロセスを実行するには、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
`Router# auto secure [management | forwarding] [no-interact | full]`	スイッチのどちらかのプレーンか両方のプレーンを設定するために AutoSecure セッションを実行します。 • **management**：マネジメント プレーンのみがセキュリティ保護されます。 • **forwarding**：フォワーディング プレーンのみがセキュリティ保護されます。 • **no-interact**：インタラクティブな設定を行うためのメッセージがまったく表示されません。 • **full**：インタラクティブな質問メッセージがすべて表示されます。これはデフォルトです。

AutoSecure セッションの例については、「AutoSecure の設定例」（P.71-9）を参照してください。

その他のセキュリティ設定

AutoSecure 設定が終わってから、次の作業を行うことでスイッチへの管理アクセスのセキュリティをさらに強化できます。

	コマンドまたはアクション	目的
ステップ 1	`Router# 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	`Router(config)# security passwords min-length length`	設定される各パスワードが、指定した長さ以上になるようにします。 • *length*：設定されるパスワードの最小長です。範囲は 0 ～ 16 文字です。
ステップ 3	`Router(config)# enable password {password | [encryption-type] password}`	さまざまな権限レベルへのアクセスを制御するローカル パスワードを設定します。 • *encryption-type*：値が 0 である場合は、暗号化されないパスワードを指定することを示します。値が 7 である場合は、隠しパスワードを指定することを示します。 （注）　シスコのルータまたはスイッチにより暗号化されているパスワードを入力する場合を除いて、暗号化タイプを入力することは通常ありません。
ステップ 4	`Router(config)# security authentication failure rate threshold-rate log`	許容されるログイン失敗回数を設定します。 • *threshold-rate*：許容されるログイン失敗回数。有効範囲は 1 ～ 1024 です。 • **log**：1 分間に失敗回数がしきい値を超える場合の Syslog 認証失敗

次に、スイッチで最短パスワード長を 10 文字に、パスワードの失敗の許容しきい値を 1 分間に 3 回に設定する例を示します。また、非表示ローカル パスワードを設定する例も示します。

```
Router# configure terminal
Router(config)# security passwords min-length 10
Router(config)# security authentication failure rate 3
Router(config)# enable password 7 elephant123
```

AutoSecure の確認

AutoSecure 機能の実行に成功していることを確認するには、次の作業を行います。

コマンド	目的
`Router# show auto secure config`	AutoSecure 設定の一部として追加されているすべてのコンフィギュレーション コマンドを表示します。出力はコンフィギュレーションにより生成される出力と同じです。

AutoSecure の設定例

次に、AutoSecure セッションの例を示します。**auto secure** コマンドを実行すると、AutoSecure は **no-interact** キーワードをイネーブルにしている場合を除いて、これと同様の応答が自動的に表示されます （ディセーブルにする機能とイネーブルにする機能の詳細については、「AutoSecure にってイネーブルになるマネジメント プレーンのセキュリティ」（P.71-3）および「AutoSecure にってイネーブルになるフォワーディング プレーンのセキュリティ」（P.71-6）を参照してください）。

```
Router# auto secure
                --- AutoSecure Configuration ---

*** AutoSecure configuration enhances the security of
the router, but it will not make it absolutely resistant
to all security attacks ***

 AutoSecure will modify the configuration of your device.

All the configuration changes will be shown. For a detailed
explanation of how the configuration changes enhance security
and any possible side effects, please refer to Cisco.com for
AutoSecure documentation.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.

If this device is being managed by a network management station,
AutoSecure configuration may block network management traffic.
Continue with AutoSecure? [no]: y

Gathering information about the router for AutoSecure

Is this router connected to internet? [no]: y
Enter the number of interfaces facing the internet [1]: 1
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  unassigned      YES NVRAM  administratively down down
Vlan77                 77.1.1.4        YES NVRAM  down                  down
GigabitEthernet6/1     unassigned      YES NVRAM  administratively down down
GigabitEthernet6/2     21.30.30.1      YES NVRAM  up                    up
Loopback0              3.3.3.3         YES NVRAM  up                    up
Tunnel1                unassigned      YES NVRAM  up                    up
```

```
Enter the interface name that is facing the internet: Vlan77

Securing Management plane services...

Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol

Disabling the bootp server
Disabling the http server
Disabling the finger service
Disabling source routing
Disabling gratuitous arp

Here is a sample Security Banner to be shown
at every access to device. Modify it to suit your
enterprise requirements.

Authorized Access only
  This system is the property of <Name of Enterprise>.
  UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.
  You must have explicit permission to access this
  device. All activities performed on this device
  are logged. Any violations of access policy will result
  in disciplinary action.

Enter the security banner {Put the banner between
k and k, where k is any character}:
k
banner
k
Enter the new enable secret:
Confirm the enable secret :
Enable password is not configured or its length
is less than minimum no. of charactersconfigured
Enter the new enable password:
Confirm the enable password:

Configuration of local user database
Enter the username: cisco
Enter the password:
Confirm the password:
Configuring AAA local authentication
Configuring Console, Aux and VTY lines for
local authentication, exec-timeout, and transport
Securing device against Login Attacks
Configure the following parameters

Blocking Period when Login Attack detected (in seconds): 5

Maximum Login failures with the device: 3

Maximum time period for crossing the failed login attempts (in seconds): ?
% A decimal number between 1 and 32767.

Maximum time period for crossing the failed login attempts (in seconds): 5

Configure SSH server? [yes]: no

Configuring interface specific AutoSecure services
```

```
Disabling mop on Ethernet interfaces

Securing Forwarding plane services...

Enabling unicast rpf on all interfaces connected
to internet

The following rate-limiters are enabled by default:
  ...

Would you like to enable the following rate-limiters also?
...

Enable the above rate-limiters also? [yes/no]: yes

Would you like to enable the rate-limiters for Ingress/EgressACL bridged packets also?
NOTE: Enabling the ACL in/out rate-limiters can affect ACL logging
      and session setup rate for hardware accelerated features such
      as NAT, Layer 3 WCCP and TCP Intercept
...

Enable the ACL in/out rate-limiters also? [yes/no]: no

This is the configuration generated:

no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
service password-encryption
service tcp-keepalives-in
service tcp-keepalives-out
no cdp run
no ip bootp server
no ip http server
no ip finger
no ip source-route
no ip gratuitous-arps
no ip identd
banner k
banner
k
security passwords min-length 6
security authentication failure rate 10 log
enable secret 5 $1$30kP$f.KDndYPz/Hv/.yTlJStN/
enable password 7 08204E4D0D48574446
username cisco password 7 08204E4D0D48574446
aaa new-model
aaa authentication login local_auth local
line console 0
 login authentication local_auth
 exec-timeout 5 0
 transport output telnet
line vty 0 15
 login authentication local_auth
 transport input telnet
login block-for 5 attempts 3 within 5
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
logging facility local2
logging trap debugging
service sequence-numbers
logging console critical
logging buffered
```

```
int Vlan1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
int Vlan77
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
int GigabitEthernet6/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
int GigabitEthernet6/2
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
interface Vlan77
 ip verify unicast source reachable-via rx
...
!
end


Apply this configuration to running-config? [yes]: yes

Applying the config generated to running-config

Router#
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CHAPTER 72

MAC アドレスベースのトラフィック ブロッキング

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

特定の VLAN 内の MAC アドレスを経由するすべてのトラフィックをブロックするには、次の作業を行います。

コマンド	目的
`Router(config)# mac address-table static mac_address vlan vlan_ID drop`	特定の VLAN で設定されている MAC アドレスを経由するすべてのトラフィックをブロックします。

次に、VLAN 12 内で MAC アドレス 0050.3e8d.6400 を経由するすべてのトラフィックをブロックする例を示します。

```
Router# configure terminal
Router(config)# mac address-table static 0050.3e8d.6400 vlan 12 drop
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CHAPTER 73

ポート ACL（PACL）

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。
- ポート ACL は access-list キーワードである **log** または **reflexive** をサポートしません。アクセス リスト内のこれらのキーワードは無視されます。OAL は PACL をサポートしません。
- PACL はプライベート VLAN 上ではサポートされません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

PACL の前提条件

なし。

PACL の制約事項

- 同じレイヤ 2 インターフェイスに方向別に適用できるのは、多くても IP アクセス リストを 1 つと MAC アクセス リストを 1 つです。
- PACL は MPLS、または ARP メッセージに適用されません。

- IP アクセス リストは、IPv4 および IPv6 パケットだけをフィルタリングします。IP アクセス リストでは、標準アクセスリスト、拡張アクセスリスト、または名前付きアクセスリストを定義できます。
- MAC アクセス リストは、イーサネット データグラムのフィールドに基づいて、サポートされないタイプの入力パケット（IP、ARP、MPLS 以外のパケット）をフィルタリングします。MAC アクセス リストは、IP、MPLS、または ARP メッセージには適用されません。定義できるのは名前付き MAC アクセス リストだけです。
- 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ているさまざまな ACL 機能（VACL など）により共有されます。PACL をハードウェアに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は、PACL が適用されません。
- PACL は access-list **log** および **reflect/evaluate** キーワードをサポートしません。これらのキーワードを PACL のアクセス リストに追加しても、無視されます。
- OAL は PACL をサポートしません。
- 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 プラットフォーム全体の動作を一貫させるには、デフォルトのアクセス グループ モード（マージ モード）を使用します。
- PACL は、CDP、VTP、DTP、PAgP、UDLD、および STP などの物理リンク プロトコルおよび論理リンク プロトコルをフィルタリングできません。これらのプロトコルは ACL が有効になる前に RP にリダイレクトされるためです。物理リンク プロトコルおよび論理リンク プロトコル トラフィックに CoPP または QoS を適用できます。

PACL について

PACL の概要

PACL は、レイヤ 3 情報、レイヤ 4 ヘッダー情報、または非 IP レイヤ 2 情報を使用して、レイヤ 2 インターフェイスに着信するトラフィックをフィルタリングします。

PACL 機能は、ポートに適用する標準 IP ACL または拡張 IP ACL、または名前付き MAC 拡張 ACL を使用します。

ポート ACL によるアクセス コントロールは、指定されたレイヤ 2 ポートに着信するすべてのトラフィックに対して行われます。

PACL および VACL は、レイヤ 3 アドレス（IP プロトコル向け）またはレイヤ 2 MAC アドレス（IP 以外のプロトコル向け）に基づいてアクセス コントロールを行います。

ポート ACL 機能により、特定のレイヤ 2 ポートに対してアクセス コントロールを行うことができます。レイヤ 2 ポートは、VLAN に属する物理的な LAN ポートまたはトランク ポートです。ポート ACL は、入力トラフィックだけに適用されます。ポート ACL 機能は、ハードウェアだけでサポートされます（ポート ACL は、ソフトウェアでルーティングされたパケットには適用されません）。

ポート ACL を作成すると、ACL TCAM にエントリが作成されます。利用可能な TCAM スペースを確認するには、**show tcam counts** コマンドを使用します。

PACL 機能は、ポートで受信するレイヤ 2 制御パケットには影響を与えません。

PACL とその他の ACL との相互作用の方法を変更するには、**access-group mode** コマンドを使用します。

PACL は次のモードを使用します。

- 優先ポート モード : PACL がレイヤ 2 インターフェイスで設定されている場合は、PACL が有効になり、その他の ACL（Cisco IOS ACL および VACL）を無効になります。PACL 機能がレイヤ 2 インターフェイスで設定されていない場合は、そのインターフェイスに適用可能なその他の機能が結合されて適用されます。
- マージ モード : このモードでは、図 73-2 に示す論理シリアル モデルに従って、PACL、VACL、および Cisco IOS ACL が入力方向に結合されます。これがデフォルトのアクセス グループ モードです。

各インターフェイスで **access-group mode** コマンドを設定します。デフォルトはマージ モードです。

（注） PACL は、優先ポート モードが選択された場合だけ、トランク ポート上で設定できます。トランク ポートはマージ モードをサポートしません。

アクセス グループ モードについて説明するために、VLAN100 に属する物理ポートに次の ACL が設定されているとします。

- Cisco IOS ACL R1 がルーテッド インターフェイス VLAN100 に適用されます。
- VACL（VLAN フィルタ）V1 が VLAN100 に適用されます。
- PACL P1 が物理ポートに適用されます。

この状況では、次のような ACL の相互作用が行われます。

- 優先ポート モードでは、Cisco IOS ACL R1 および VACL V1 は無視されます。
- マージ モードでは、Cisco IOS ACL R1、VACL V1、および PACL P1 は結合され、ポートに適用されます。

（注） PACL を作成するための CLI 構文は、Cisco IOS ACL を作成する構文と同じです。レイヤ 2 ポートにマッピングされている ACL のインスタンスが PACL です。レイヤ 3 インターフェイスにマッピングされている ACL のインスタンスは Cisco IOA ACL です。同じ ACL をレイヤ 2 ポートとレイヤ 3 インターフェイスの両方にマッピングできます。

PACL 機能は MAC ACL、IPv4 および IPv6 ACL をサポートします。PACL 機能は ARP、またはマルチプロトコル ラベル スイッチング（MPLS）トラフィック用の ACL をサポートしません。

EtherChannel と PACL の相互作用

ここでは、EtherChannel と PACL の相互作用における注意事項について説明します。

- PACL はメイン レイヤ 2 チャネル インターフェイス上でサポートされますが、ポート メンバ上ではサポートされません。PACL が設定されているポートは、EtherChannel メンバ ポートとして設定されていない場合があります。EtherChannel コンフィギュレーション コマンドは、PACL が設定されたポートでは使用できません。

- 論理ポートの設定変更は、チャネル内のすべてのポートに影響します。チャネルに属する論理ポートに ACL をマッピングすると、そのチャネル内のすべてのポートにもマッピングされます。

ダイナミック ACL（マージ モードだけに適用）

ダイナミック ACL は VLAN ベースで、CBAC および GWIP の 2 つの機能によって使用されます。マージ モードは、ダイナミック ACL と PACL の結合をサポート*しません*。マージ モードでは、次のような設定はできません。

- 対応する VLAN にダイナミック ACL がマッピングされているポートに PACL を設定しようとすること。この場合、PACL はポート上のトラフィックに適用されません。
- 構成ポートの 1 つに PACL がインストールされている VLAN にダイナミック ACL を適用しようとすること。この場合、動的 ACL は適用されません。

トランク ポート

トランク ポートで PACL を設定するには、ポート優先モードを先に設定する必要があります。**access-group mode prefer port** インターフェイス コマンドを入力してポート優先モードを設定するまで、トランク ポートまたはダイナミック ポートに PACL を適用するコンフィギュレーション コマンドは使用できません。トランク ポートはマージ モードをサポートしません。

レイヤ 2 ポートからレイヤ 3 ポートへの変換

ポートをレイヤ 2 からレイヤ 3 に再設定する場合、ポート上に設定されているすべての PACL は非アクティブになりますが、設定からは削除されません。その後ポートをレイヤ 2 として設定すると、ポート上に設定されているすべての PACL は再度アクティブになります。

ポート/VLAN アソシエーション変更

ポート/VLAN アソシエーションを変更するポート コンフィギュレーション コマンドを入力すると、ACL 再結合を開始できます。

PACL、VACL、または Cisco IOS ACL をマッピング解除したあとに再度マッピングすると、再結合が自動的に開始されます。

マージ モードでは、モジュール上のポートに PACL が設定されている場合は、スイッチング モジュールの活性挿抜によっても再結合が開始されます。

PACL と VACL の相互作用

- 「PACL の VACL および Cisco IOS ACL との相互作用」（P.73-5）
- 「ブリッジド パケット」（P.73-5）
- 「ルーティング対象パケット」（P.73-5）
- 「マルチキャスト パケット」（P.73-6）

PACL の VACL および Cisco IOS ACL との相互作用

ここでは、PACL の VACL および Cisco IOS ACL との相互作用における注意事項について説明します。

PACL はまず、物理ポートの着信パケットに適用されます。パケットが PACL により許可されると、次に入力 VLAN の VACL が適用されます。パケットがレイヤ 3 で転送され、VACL により許可される場合は、同じ VLAN 上の Cisco IOS ACL によりフィルタリングされます。出力方向では同じプロセスが逆に発生します。ただし、出力 PACL はハードウェアで現在サポートされていません。

ポートが優先ポート モードに設定されている場合、PACL により VACL と Cisco IOS ACL の両方が無効になります。このルールの 1 つの例外は、パケットがルート プロセッサ（RP）によってソフトウェアで転送される場合です。RP は PACL モードに関係なく入力 Cisco IOS ACL を適用します。パケットがソフトウェアで転送される 2 つの例は、次のとおりです。

- 出力ブリッジド パケット（ロギングや NAT などの機能のため）
- IP オプションが指定されたパケット

ブリッジド パケット

図 73-1 に、ブリッジド パケットに適用される PACL および VACL を示します。マージ モードでは、ACL は次の順序で適用されます。

1. 入力ポートの PACL
2. 入力 VLAN の VACL
3. 出力 VLAN の VACL

図 73-1　　ブリッジド パケットへの ACL の適用

優先ポート モードでは、入力パケットに適用されるのは PACL だけです（入力 VACL は適用されません）。

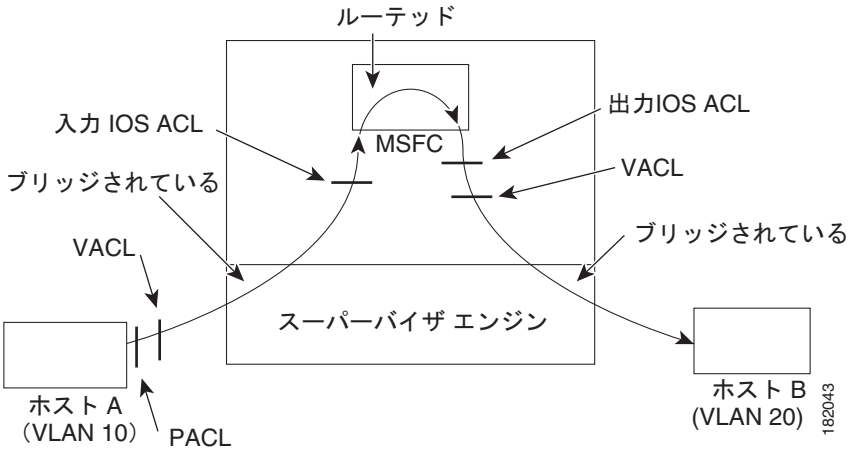
ルーティング対象パケット

図 73-2 に、ルーティング対象パケットおよびレイヤ 3 スイッチング対象パケットに ACL を適用する方法を示します。マージ モードでは、ACL は次の順序で適用されます。

1. 入力ポートの PACL
2. 入力 VLAN の VACL
3. 入力 Cisco IOS ACL
4. 出力 Cisco IOS ACL
5. 出力 VLAN の VACL

優先ポート モードでは、入力パケットに適用されるのは PACL だけです（入力 VACL および Cisco IOS ACL は適用されません）。

図 73-2　　ルーテッド パケットへの ACL の適用



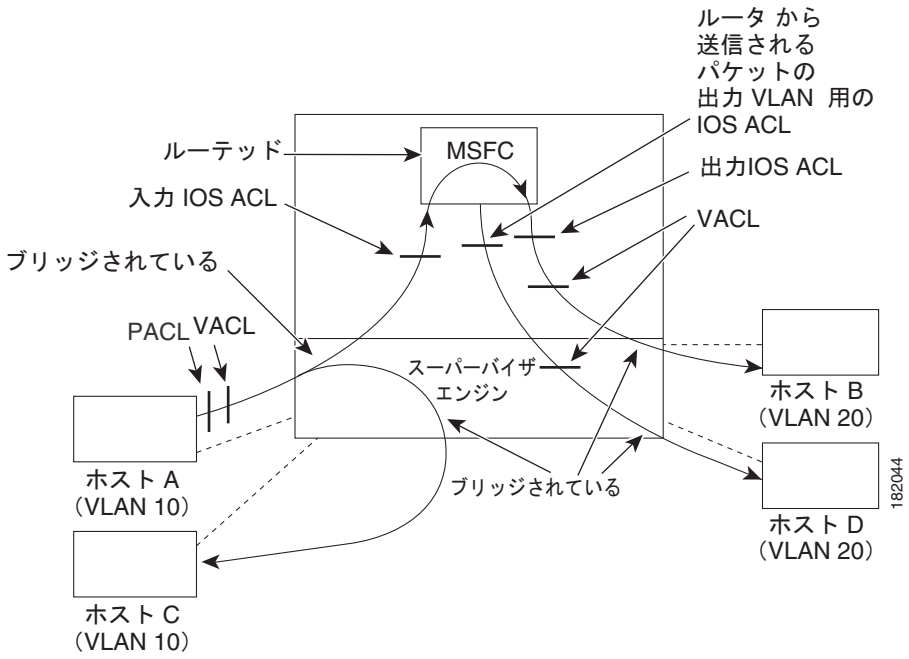
マルチキャスト パケット

図 73-3 に、マルチキャスト拡張が必要なパケットに ACL を適用する方法を示します。マルチキャスト拡張が必要なパケットに対して、ACL は次の順番で適用されます。

1. マルチキャスト拡張が必要なパケット：
   a. 入力ポートの PACL
   b. 入力 VLAN の VACL
   c. 入力 Cisco IOS ACL
2. マルチキャスト拡張後のパケット：
   a. 出力 Cisco IOS ACL
   b. 出力 VLAN の VACL
3. ルータから送られるパケット
   a. 出力 Cisco IOS ACL
   b. 出力 VLAN の VACL

優先ポート モードでは、入力パケットに適用されるのは PACL だけです（入力 VACL および Cisco IOS ACL は適用されません）。

図 73-3　マルチキャスト パケットへの ACL の適用



PACL の設定方法

レイヤ 2 インターフェイスの IP ACL および MAC ACL の設定

IP ACL および MAC ACL はレイヤ 2 物理インターフェイスに適用できます。（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 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`	レイヤ 2 ポート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)# {ip | mac} access-group {name | number | in | out}`	番号付き ACL または名前付き ACL をレイヤ 2 インターフェイスに適用します。
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、他のすべての IP トラフィックを暗黙的に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 を任意の宛先ホストで許可する、名前付き拡張 MAC ACL 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
```

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

アクセス モードをレイヤ 2 インターフェイス上で設定するには、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`	レイヤ 2 ポート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。
ステップ 3	`Switch(config-if)# [no] access-group mode {prefer port | merge}`	このレイヤ 2 インターフェイスのモードを設定します。**no** プレフィックスは、モードをデフォルト（マージ）に設定します。
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。

次の例では、優先ポート モードを使用するようインターフェイスを設定します。

```
Switch# configure terminal
Switch(config)# interface gigabitEthernet 6/1
Switch(config-if)# access-group mode prefer port
```

次の例では、マージ モードを使用するようインターフェイスを設定します。

```
Switch# configure terminal
Switch(config)# interface gigabitEthernet 6/1
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**	IP ACL をレイヤ 2 インターフェイスに適用します。
Switch(config-if)# **mac access-group** *mac-acl* **in**	レイヤ 2 インターフェイスに MAC ACL を適用します。

次に、名前付き拡張 IP ACL simple-ip-acl をインターフェイス GigabitEthernet 6/1 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 gigabitEthernet 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 GigabitEthernet 6/1 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 gigabitEthernet 6/1
Switch(config-if)# mac access-group simple-mac-acl in
```

ポート チャネルへの ACL の適用

ポート チャネルの論理インターフェイスに IP ACL および MAC ACL を適用にするには、次の作業を行います。

コマンド	目的
Switch(config-if)# **interface port-channel** *number*	ポート チャネルのコンフィギュレーション モードを開始します。
Switch(config-if)# **ip access-group** *ip-acl* {**in** | **out**}	IP ACL をポート チャネル インターフェイスに適用します。
Switch(config-if)# **mac access-group** *mac-acl* {**in** | **out**}	MAC ACL をポート チャネル インターフェイスに適用します。

次に、名前付き拡張 IP ACL simple-ip-acl をポート チャネル 3 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 port-channel 3
Switch(config-if)# ip access-group simple-ip-acl in
```

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 access-lists** [**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。

コマンド	目的
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 gigabitethernet 6/1
GigabitEthernet6/1 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 Gigabit Ethernet 6/1 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 gigabitethernet 6/1
Interface GigabitEthernet6/1:
   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 Gigabit Ethernet 6/1 に設定されている例を示します。

```
Switch# show access-group mode interface gigabitethernet 6/1
Interface GigabitEthernet6/1:
   Access group mode is: merge
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CHAPTER 74

VLAN ACL（VACL）

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。
- 最適化された ACL ロギング（OAL）と VACL キャプチャには互換性がありません。スイッチに両方の機能を設定しないでください。OAL が設定されている場合は（「最適化された ACL ロギング」（P.69-13）を参照）、SPAN を使用してトラフィックをキャプチャします。
- 「PACL の VACL および Cisco IOS ACL との相互作用」（P.73-5）も参照してください。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

VACL の前提条件

なし。

VACL の制約事項

- VACL は、標準および拡張 Cisco IOS IP、MAC レイヤ名前付き ACL（「MAC ACL」（P.69-9）を参照）、および VLAN アクセス マップを使用します。
- IGMP パケットは VACL と照合されません。
- VLAN アクセス マップは、VACL キャプチャの VLAN に適用できます。
- 各 VLAN アクセス マップは、1 つまたは複数のマップ シーケンスで構成できます。各シーケンスには match 句と action 句が含まれます。match 句はトラフィック フィルタリング用の IP または MAC ACL を指定します。action 句は一致した場合に実行するアクションを指定します。フローが許可（permit）ACL エントリと一致した場合、関連付けられたアクションが実行され、それ以降の残りのシーケンスに対してフローはチェックされません。フローが拒否（deny）ACL エントリと一致した場合、同じシーケンス内の次の ACL、または次のシーケンスに対してフローがチェックされます。フローがどの ACL エントリとも一致せず、1 つまたは複数の ACL がそのパケット タイプ用に設定されている場合、パケットは拒否されます。
- ブリッジド トラフィックとルーテッド トラフィックの両方にアクセス コントロールを適用するには、VACL を単独で使用するか、または VACL と ACL を組み合わせて使用します。VLAN インターフェイス上で ACL を定義して、入力と出力両方のルーテッド トラフィックに対してアクセス コントロールを適用できます。VACL を定義して、ブリッジド トラフィックに対してアクセス コントロールを適用します。
- VACL とともに ACL を使用する場合は、次の点に注意してください。
  - 発信 ACL での記録の必要があるパケットは、VACL で拒否された場合、記録されません。
  - VACL は NAT（ネットワーク アドレス変換）変換前のパケットに適用されます。アクセス コントロールされなかった変換フローは、VACL 設定により、変換後にアクセス コントロールされる場合があります。
- VACL は、OAL、合法的傍受（LI）、および IPv6 学習などのキャプチャを使用して、他の機能との競合をチェックします。
- 同じインターフェイス上で Policy Based Routing（PBR; ポリシー ベース ルーティング）を使用して VACL キャプチャが設定されている場合は、BDD を ACL 結合アルゴリズムとして選択しないでください。
- VACL キャプチャが、ソフトウェアによるトラフィック処理を必要とする別の入力機能とともに入力インターフェイスに設定されている場合、重複するトラフィックのパケットは 2 回キャプチャされる可能性があります。
- VACL の action コマンドには、転送（forward）、ドロップ（drop）、キャプチャ（capture）、またはリダイレクト（redirect）を指定できます。トラフィックをログに記録することもできます。

（注）
- VACL のマップの最後には、暗黙的な拒否エントリがあります。パケットがどの ACL エントリとも一致せず、1 つまたは複数の ACL がそのパケット タイプ用に設定されている場合、パケットは拒否されます。
- VACL 内で空または未定義の ACL が指定されている場合、いずれかのパケットがこの ACL に一致し、関連付けられたアクションが実行されます。

VACL について

VLAN ACL（VACL）は、VLAN 内でブリッジされるか、VACL キャプチャのために VLAN の内側または外側へルーティングされるすべてのパケットのアクセス コントロールを行います。ルーティングされるパケットだけに適用される Cisco IOS ACL と異なり、VACL はすべてのパケットに適用され、どの VLAN にも適用できます。VACL は ACL TCAM ハードウェアで処理されます。VACL は、ハードウェアでサポートされていないすべての Cisco IOS ACL フィールドを無視します。

IP および MAC 層トラフィックの場合は、VACL を設定できます。

VACL が特定のパケット タイプ用に設定されていて、あるパケットの該当タイプが VACL と一致しない場合、デフォルト動作では、パケットが拒否されます。

パケットはルーティングされたあと、レイヤ 2 ポートまたはレイヤ 3 ポートから VLAN に着信します。VACL を使用して、同じ VLAN 上のデバイス間のトラフィックをフィルタリングすることもできます。

VACL の設定方法

VLAN アクセス マップの定義

VLAN アクセス マップを定義するには、次の作業を行います。

コマンド	目的
`Router(config)# vlan access-map map_name [0-65535]`	VLAN アクセス マップを定義します。任意で、VLAN アクセス マップのシーケンス番号を指定できます。

- エントリを追加または変更する場合は、マップのシーケンス番号を指定します。
- マップのシーケンス番号を指定しないと、番号が自動的に割り当てられます。
- 各マップ シーケンスには、match コマンドおよび action コマンドをそれぞれ 1 つだけ指定できます。
- マップ シーケンスを削除する場合は、シーケンス番号を指定して **no** キーワードを使用します。
- マップを削除する場合は、シーケンス番号を指定しないで、**no** キーワードを使用します。

「VLAN アクセス マップの設定および確認の例」（P.74-5）を参照してください。

VLAN アクセス マップ シーケンスでの match コマンドの設定

VLAN アクセス マップ シーケンスに match コマンドを設定するには、次の作業を行います。

コマンド	目的
`Router(config-access-map)# match {[ip | ipv6] address {1-199 | 1300-2699 | acl_name} | {mac address acl_name}}`	VLAN アクセス マップ シーケンスに match コマンドを設定します。

- Release 15.0(1)SY1 以降のリリースで、IPv6 ACL がサポートされます。
- 1 つまたは複数の ACL を選択できます。
- match コマンドを削除したり、match コマンド内の特定の ACL を削除したりする場合は、**no** キーワードを使用します。
- 名前付き MAC レイヤ ACL の詳細については、「MAC ACL」（P.69-9）を参照してください。
- Cisco IOS ACL の詳細については、第 69 章「Cisco IOS ACL のサポート」および「VLAN アクセス マップの設定および確認の例」（P.74-5）を参照してください。

VLAN アクセス マップ シーケンスでの action コマンドの設定

VLAN アクセス マップ シーケンスに action コマンドを設定するには、次の作業を行います。

コマンド	目的
`Router(config-access-map)# action {drop [log]} | {forward [capture | vlan vlan_ID]} | {redirect {{fastethernet | gigabitethernet | tengigabitethernet} slot/port} | {port-channel channel_id}}`	VLAN アクセス マップ シーケンスに action コマンドを設定します。

- パケットをドロップ、転送、転送してキャプチャ、またはリダイレクトするアクションを設定できます。
- 転送されたパケットも、設定済み Cisco IOS セキュリティ ACL による制約を受けます。
- **capture** アクションを指定すると、転送されたパケットのキャプチャ ビットが設定されて、キャプチャ機能がイネーブルであるポートがパケットを受信できるようになります。キャプチャできるのは、転送されたパケットだけです。**capture** アクションの詳細については、「キャプチャ ポートの設定」（P.74-6）を参照してください。
- **forward vlan** アクションは、ポリシーベース転送（PBF）を実行し、VLAN 間をブリッジします。
- **log** アクションが指定されている場合、ドロップされたパケットがソフトウェアで記録されます。記録できるのは、ドロップされた IP パケットだけです。
- **redirect** アクションを指定すると、物理インターフェイスまたは EtherChannel のいずれかのインターフェイスを 5 つまで指定できます。EtherChannel メンバまたは VLAN にパケットをリダイレクトするように指定することはできません。
- リダイレクト インターフェイスは、VACL アクセス マップが設定されている VLAN 内に存在する必要があります。
- VACL が出力 SPAN 送信元ポートにトラフィックをリダイレクトする場合、SPAN は VACL リダイレクト トラフィックをコピーしません。
- SPAN および RSPAN 宛先ポートは、VACL リダイレクトされたトラフィックを送信します。

- action コマンドを削除するか、または指定されたリダイレクト インターフェイスを削除する場合は、**no** キーワードを使用します。

「VLAN アクセス マップの設定および確認の例」（P.74-5）を参照してください。

VLAN アクセス マップの適用

VLAN アクセス マップを適用するには、次の作業を行います。

コマンド	目的
`Router(config)# vlan filter map_name vlan-list`	VLAN アクセス マップを指定された VLAN に適用します。

- VLAN アクセス マップは、1 つまたは複数の VLAN に適用できます。
- *vlan_list* パラメータには、単一の VLAN ID、カンマで区切った VLAN ID リスト、または VLAN ID 範囲（*vlan_ID-vlan_ID*）を指定できます。
- 各 VLAN に適用できるのは、1 つの VLAN アクセス マップだけです。
- VLAN に適用した VACL がアクティブになるのは、レイヤ 3 VLAN インターフェイスが設定されている VLAN に対してだけです。レイヤ 3 VLAN インターフェイスを持たない VLAN に VLAN アクセス マップを適用すると、VLAN アクセス マップをサポートするために、レイヤ 3 VLAN インターフェイスが、管理上のダウン状態で作成されます。
- レイヤ 2 VLAN が存在しないか動作していない場合、VLAN に適用される VACL は非アクティブです。
- セカンダリ プライベート VLAN に VACL を適用することはできません。プライマリ プライベート VLAN に適用された VACL は、セカンダリ プライベート VLAN にも適用されます。
- VLAN から VLAN アクセス マップを消去するには、**no** キーワードを使用します。

「VLAN アクセス マップの設定および確認の例」（P.74-5）を参照してください。

VLAN アクセス マップの設定の確認

VLAN アクセス 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	目的
`Router# show vlan access-map [map_name]`	VLAN アクセス マップの内容を表示して、VLAN アクセス マップの設定を確認します。
`Router# show vlan filter [access-map map_name | vlan vlan_id]`	VACL と VLAN 間のマッピングの内容を表示して、VLAN アクセス マップの設定を確認します。

VLAN アクセス マップの設定および確認の例

net_10 および **any_host** という名前の IP ACL が、次のように定義されていると想定します。

```
Router# show ip access-lists net_10
Extended IP access list net_10
    permit ip 10.0.0.0 0.255.255.255 any

Router# show ip access-lists any_host
Standard IP access list any_host
```

```
    permit any
```

次に、IP パケットを転送するよう、VLAN アクセス マップを定義および適用する例を示します。この例では、net_10 に一致する IP トラフィックは転送され、それ以外のすべての IP パケットはデフォルトのドロップ アクションによってドロップされます。このマップは VLAN 12 ～ 16 に適用されます。

```
Router(config)# vlan access-map thor 10
Router(config-access-map)# match ip address net_10
Router(config-access-map)# action forward
Router(config-access-map)# exit
Router(config)# vlan filter thor vlan-list 12-16
```

次に、IP パケットをドロップおよび記録するよう、VLAN アクセス マップを定義および適用する例を示します。この例では、net_10 に一致する IP トラフィックはドロップおよび記録され、それ以外のすべての IP パケットは転送されます。

```
Router(config)# vlan access-map ganymede 10
Router(config-access-map)# match ip address net_10
Router(config-access-map)# action drop log
Router(config-access-map)# exit
Router(config)# vlan access-map ganymede 20
Router(config-access-map)# match ip address any_host
Router(config-access-map)# action forward
Router(config-access-map)# exit
Router(config)# vlan filter ganymede vlan-list 7-9
```

次に、IP パケットを転送およびキャプチャするよう、VLAN アクセス マップを定義および適用する例を示します。この例では、net_10 に一致する IP トラフィックは転送およびキャプチャされ、それ以外のすべての IP パケットはドロップされます。

```
Router(config)# vlan access-map mordred 10
Router(config-access-map)# match ip address net_10
Router(config-access-map)# action forward capture
Router(config-access-map)# exit
Router(config)# vlan filter mordred vlan-list 2, 4-6
```

キャプチャ ポートの設定

（注）

- VACL フィルタリングされたトラフィックをキャプチャするよう設定されたポートを、「キャプチャ ポート」といいます。
- キャプチャされたトラフィックに IEEE 802.1Q タグを適用するには、キャプチャ ポートで無条件にトランクするように設定します（「802.1Q トランクとしてのレイヤ 2 スイッチング ポートの設定」（P.20-9）および「DTP を使用しないようにするためのレイヤ 2 トランクの設定」（P.20-10）を参照）。

キャプチャ 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	`Router(config)# interface {{type slot/port}`	設定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 2	`Router(config-if)# switchport capture allowed vlan {add | all | except | remove} vlan_list`	（任意）宛先 VLAN 単位で、キャプチャされたトラフィックをフィルタリングします。デフォルトは、**all** です。
ステップ 3	`Router(config-if)# switchport capture`	VACL フィルタリングされたトラフィックをキャプチャするよう、ポートを設定します。

- 任意のポートをキャプチャ ポートとして設定できます。
- *vlan_list* パラメータには、単一の VLAN ID、カンマで区切った VLAN ID リスト、または VLAN ID 範囲（*vlan_ID-vlan_ID*）を指定できます。
- キャプチャされたトラフィックをカプセル化するには、**switchport trunk encapsulation** コマンドでキャプチャ ポートを設定してから（「トランクとしてのレイヤ 2 スイッチング ポートの設定」（P.20-9）を参照）、**switchport capture** コマンドを入力します。
- キャプチャされたトラフィックをカプセル化しない場合は、**switchport mode access** コマンドでキャプチャ ポートを設定してから（「レイヤ 2 アクセス ポートとしての LAN インターフェイスの設定」（P.20-15）を参照）、**switchport capture** コマンドを入力します。
- キャプチャ ポートは、出力トラフィックだけをサポートします。トラフィックは、キャプチャ ポートからスイッチに入ることができません。

次に、ギガビット イーサネット インターフェイス 5/1 をキャプチャ ポートとして設定する例を示します。

```
Router(config)# interface gigabitEthernet 5/1
Router(config-if)# switchport capture
Router(config-if)# end
```

次に、VLAN アクセス マップの情報を表示する例を示します。

```
Router# show vlan access-map mymap
Vlan access-map "mymap"  10
        match: ip address net_10
        action: forward capture
Router#
```

次に、VACL と VLAN 間のマッピングを表示する例を示します。各 VACL マップでは、マップが設定されている VLAN、およびマップがアクティブである VLAN についての情報があります。VLAN 内にインターフェイスがない場合、VACL は、アクティブになりません。

```
Router# show vlan filter
VLAN Map mordred:
        Configured on VLANs:  2,4-6
            Active on VLANs:  2,4-6
Router#
```

VACL ログ機能の設定

VACL ログ機能が設定されているときに、次の状況で IP パケットが拒否されると、ログ メッセージが生成されます。

- 一致する最初のパケットを受信した場合
- 直前の 5 分間に、一致するパケットを受信した場合
- 5 分経過する前にしきい値に達している場合

ログ メッセージはフロー単位で生成されます。フローは、同じ IP アドレスおよびレイヤ 4（UDP または TCP）ポート番号を持つパケットとして定義されます。ログ メッセージが生成されると、タイマーおよびパケット カウントがリセットされます。

VACL ログ機能には、次の制限事項が適用されます。

- リダイレクトされたパケットにはレート制限機能が適用されるので、VACL ログ カウンタが不正確になることがあります。
- 拒否された IP パケットだけが記録されます。

VACL ロギングを設定するには、VLAN アクセス マップ サブモードの **action drop log** コマンド アクションを使用します（「VLAN アクセス マップ シーケンスでの action コマンドの設定」（P.74-4）を参照してください）。この作業をグローバル コンフィギュレーション モードで実行して、グローバル VACL ロギング パラメータを指定します。

	コマンド	目的
ステップ 1	`Router(config)# vlan access-log maxflow` *max_number*	ログ テーブルのサイズを設定します。maxflow の値を 0 に設定すると、ログ テーブルの内容を削除できます。デフォルトは 500、有効範囲は 0 ～ 2048 です。ログ テーブルが満杯になると、新しいフローのパケットが記録されても、ソフトウェアによってドロップされます。
ステップ 2	`Router(config)# vlan access-log ratelimit` *pps*	VACL ログ パケットの最大リダイレクト速度を設定します。デフォルトのパケット転送速度は 2000 パケット/秒、有効範囲は 0 ～ 5000 です。制限を超えたパケットは、ハードウェアによってドロップされます。
ステップ 3	`Router(config)# vlan access-log threshold` *pkt_count*	ログしきい値を設定します。5 分経過する前にフローのしきい値に達すると、ロギング メッセージが生成されます。デフォルトでは、しきい値は設定されません。
ステップ 4	`Router(config)# exit`	VLAN アクセス マップ コンフィギュレーション モードを終了します。

次に、グローバル VACL ログ機能をハードウェア内で設定する例を示します。

```
Router(config)# vlan access-log maxflow 800
Router(config)# vlan access-log ratelimit 2200
Router(config)# vlan access-log threshold 4000
```

設定された VACL ロギング プロパティを表示します。

```
Router# show vlan access-log config
```

VACL ログ テーブルの内容を表示します。

```
Router# show vlan access-log flow protocol {{src_addr src_mask} | any | {host {hostname |
host_ip}}} {{dst_addr dst_mask} | any | {host {hostname | host_ip}}}
[vlan vlan_id]
```

パケット数、メッセージ数などの統計情報を表示します。

```
Router# show vlan access-log statistics
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CHAPTER 75

Policy-Based Forwarding（PBF）

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。
- 最適化された ACL ロギング（OAL）と VACL キャプチャには互換性がありません。スイッチに両方の機能を設定しないでください。OAL が設定されている場合は（「最適化された ACL ロギング」（P.69-13）を参照）、SPAN を使用してトラフィックをキャプチャします。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

PBF の前提条件

なし。

PBF の制約事項

- PBF は、CPU の使用率を制御するためにオプションのレート リミッタによってソフトウェアで実行されます。
- PBF は入力トラフィックだけに適用されます。
- 2 つの VLAN 間で両方向のトラフィックを許可するには、両方の VLAN で PBF を設定する必要があります。
- PBF は、異なるスイッチのホスト間に設定することができます。
- デフォルトでは、同じ VLAN 内にある PBF ホスト同士で通信できません。ローカル通信を許可するには、**local** キーワードを使用します。
- **vlan filter** コマンドを設定する場合は、**vlan-list** キーワードのあとに VLAN を 1 つだけ指定します。複数の VLAN を指定すると、PBF はリストの最後にある VLAN 以外はすべて無視します。
- レイヤ 2 ポート ACL（PACL）は、PBF よりも優先されます。
- 送信側 VLAN がシャットダウンされても、PBF は機能します。VLAN をシャットダウンすると、レイヤ 3 の機能がディセーブルになります。PBF はレイヤ 2 の機能です。

PBF について

PBF は、VLAN 間のパケットをブリッジする MAC アドレス VACL です。PBF は、送信元と宛先の MAC アドレスだけに基づいてパケットを転送し、レイヤ 2 より上位の情報は無視します。

PBF のデフォルト設定

なし。

PBF の設定方法

PBF を設定するには、各送信元 VLAN で次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# mac host my_host mac_addr`	（任意）送信元ホストの MAC アドレスに名前を割り当てます。
ステップ 2	`Router(config)# mac access-list extended macl_name`	MAC ACL を設定します。
ステップ 3	`Router(config-ext-macl)# permit host my_host any`	名前を割り当てたホストから他の任意のアドレスへのトラフィックを許可するように、アクセス コントロール エントリ（ACE）を設定します。ホストは名前または MAC アドレスで指定できます。
ステップ 4	`Router(config-ext-macl)# permit host my_host host other_host`	名前を割り当てたホストからさらに別のアドレスへのトラフィックを許可するように、ACE を設定します。
ステップ 5	`Router(config-ext-macl)# exit`	ACL の設定を終了します。
ステップ 6	`Router(config)# vlan access-map map_name`	VLAN アクセス マップを定義します。

	コマンド	目的
ステップ 7	`Router(config-access-map)# match mac address macl_name`	MAC ACL をこの VLAN アクセス マップに適用します。
ステップ 8	`Router(config-access-map)# action forward vlan other_vlan_ID [local]`	一致するトラフィックを他の VLAN に転送します。 （注）　デフォルトでは、同じ VLAN 上にある PBF 指定のデバイス同士で通信できません。ホストによるローカル通信を許可するには、**local** キーワードを使用します。
ステップ 9	`Router(config-access-map)# exit`	アクセス マップの設定を終了します。
ステップ 10	`Router(config)# vlan filter map_name vlan-list my_vlan_ID`	VLAN アクセス マップを指定された VLAN に適用します。
ステップ 11	`Router(config)# interface vlan my_vlan_ID`	VLAN のインターフェイス コンフィギュレーション モードを入力します。
ステップ 12	`Router(config-if)# mac packet-classify`	この VLAN 上の着信または送信レイヤ 3 パケットをレイヤ 2 パケットとして分類します。
ステップ 13	`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。
ステップ 14	`Router(config)# 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。

PBF のモニタリング

- **show vlan mac-pbf config** コマンドの出力には、設定された PBF パスに対して次のフィールドが表示されます。
  - Rcv Vlan：PBF によるパケット転送の受信側 VLAN 数。
  - Snd Vlan：PBF によるパケット転送の送信側 VLAN 数。
  - DMAC：受信側 VLAN 上の宛先ホストの MAC アドレス。
  - SMAC：送信側 VLAN 上の送信元ホストの MAC アドレス。
  - (Local)：送信側 VALN で **action forward vlan** コマンドに **local** キーワードが設定された場合は 1 を表示し、**local** キーワードが設定されていない場合は 0 を表示します。
  - (Packet counter)：送信側 VLAN から受信側 VLAN に転送されたパケット数。このカウンタをクリアするには、**clear vlan mac-pbf counters** コマンドを入力します。
  - Pkts dropped：送信側 VLAN によってドロップされたパケット数。このカウンタをクリアするには、**clear vlan mac-pbf counters** コマンドを入力します。

PBF の設定例

次に、別々の VLAN（「red」VLAN 100 と「blue」VLAN 200）にある 2 つのホストが同じスイッチ上でパケットを交換できるように、PBF を設定および表示する例を示します。

```
Router(config)# mac host host_red3 0001.0002.0003
Router(config)# mac access-list extended macl_red
Router(config-ext-macl)# permit host host_red host host_blue
Router(config-ext-macl)# exit
Router(config)# vlan access-map red_to_blue
```

```
Router(config-access-map)# match mac address macl_red
Router(config-access-map)# action forward vlan 200 local
Router(config-access-map)# exit
Router(config)# vlan filter red_to_blue vlan-list 100
Router(config)# interface vlan 100
Router(config-if)# mac packet-classify
Router(config-if)# exit
Router(config)#
Router(config)# mac host host_blue5 0001.0002.0005
Router(config)# mac access-list extended macl_blue
Router(config-ext-macl)# permit host host_blue host host_red
Router(config-ext-macl)# exit
Router(config)# vlan access-map blue_to_red
Router(config-access-map)# match mac address macl_blue
Router(config-access-map)# action forward vlan 100
Router(config-access-map)# exit
Router(config)# vlan filter blue_to_red vlan-list 200
Router(config)# interface vlan 200
Router(config-if)# mac packet-classify
Router(config-if)# exit
Router#
Router# show vlan mac-pbf config
 Rcv Vlan 100, Snd Vlan 200, DMAC 0001.0002.0003, SMAC 0001.0002.0005 1 15
 Rcv Vlan 200, Snd Vlan 100, DMAC 0001.0002.0005, SMAC 0001.0002.0003 0 23
 Pkts Dropped 0
Router#
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CHAPTER 76

サービス拒否（DoS）からの保護

（注）

- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。
- 次のセクションも参照してください。
  - 第 72 章「MAC アドレスベースのトラフィック ブロッキング」
  - 第 81 章「トラフィック ストーム制御」
  - 第 77 章「コントロール プレーン ポリシング（CoPP）」
  - http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/15-sy/secdata-15-sy-library.html

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

セキュリティ ACL および VACL

ネットワークが DoS 攻撃を受けている場合、DoS パケットがターゲットに達する前に DoS パケットをドロップする有効な方法は ACL です。特定ホストからの攻撃が検出された場合は、セキュリティ ACL を使用します。

次の例では、ホスト 10.1.1.10 およびそのホストからのすべてのトラフィックが拒否されます。

```
Router(config)# access-list 101 deny ip host 10.1.1.10 any
Router(config)# access-list 101 permit ip any any
```

セキュリティ ACL は、アドレスのスプーフィングからも保護します。たとえば送信元アドレス A がネットワーク内にあり、スイッチ インターフェイスがインターネットに向いているとします。スイッチ インターネット インターフェイスで着信 ACL を適用すれば、送信元が A（内部アドレス）になっているすべてのアドレスを拒否できます。この処理では、攻撃者が内部送信元アドレスになりすます攻撃が防止されます。パケットは、スイッチ インターフェイスに到着したとき、その ACL と一致してドロップされるので、被害は発生しません。

スイッチを Cisco Intrusion Detection Module（CIDM）で使用している場合は、感知エンジンによる攻撃の検出に対応して、セキュリティ ACL をダイナミックにインストールできます。

VACL は、レイヤ 2、レイヤ 3、レイヤ 4 の情報に基づくセキュリティ処理ツールです。パケットに対する VACL ルックアップの結果は、許可、拒否、許可および取り込み、リダイレクトのうちいずれかになります。VACL を特定 VLAN に関連付けると、すべてのトラフィックは、VACL によって許可されないと VLAN に入ることができません。VACL はハードウェア内で適用されます。したがって VLAN に VACL を適用しても、パフォーマンス ペナルティは発生しません。

第 69 章「Cisco IOS ACL のサポート」および第 74 章「VLAN ACL（VACL）」を参照してください。

QoS レート制限

QoS ACL は、RP によって処理される、特定の種類のトラフィックの量を制限します。RP に対して DoS 攻撃が開始されると、QoS ACL は DoS トラフィックが RP データ パスに到達し、輻輳を防ぎます。PFC および DFC は QoS をハードウェア内で実行します。この仕組みは、DoS トラフィックを制限して（DoS トラフィックの検知後）、スイッチが RP に影響を与えることを防ぐうえで効果的です。

たとえば、ネットワークが ping-of-death や SMURF アタックなどを受けた場合、管理者はこの DoS 攻撃に対処するため ICMP トラフィックをレート制限する必要がありますが、同時に正規のトラフィックのプロセッサ処理、または RP やホストへの転送を許可する必要があります。このレート制限設定は、レート制限が必要なフローごとに実行する必要があり、レート制限ポリシー アクションはインターフェイスに適用する必要があります。

次の例では、アクセス リスト 101 が、任意の送信元から任意の宛先への ping（エコー）ICMP メッセージを許可してトラフィックとして識別します。ポリシー マップ内では、ポリシング ルールが特定 Committed Information Rate（CIR; 認定情報速度）とバースト値（96000 bps および 16000 bps）を定義し、シャーシを経由する ping（ICMP）トラフィックをレート制限します。ポリシー マップはインターフェイスまたは VLAN に適用されます。ポリシー マップが適用されている VLAN またはインターフェイスにおいて ping トラフィックが指定したレートを超えた場合、ping トラフィックはマークダウン マップに指定されたようにドロップされます（通常バースト設定のマークダウン マップは、この例に示していません）。

```
Router(config)# access-list 101 permit icmp any any echo
Router(config)# class-map match-any icmp_class
Router(config-cmap)# match access-group 101
Router(config-cmap)# exit
Router(config)# policy-map icmp_policer
Router(config-pmap)# class icmp_class
```

```
Router(config-pmap-c)# police 96000 16000 conform-action transmit exceed-action
policed-dscp-transmit drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
```

第 63 章「分類、マーキング、およびポリシング」を参照してください。

グローバル プロトコル パケット ポリシング

グローバル プロトコル パケット ポリシングの前提条件

なし。

グローバル プロトコル パケット ポリシングの制約事項

- **platform qos protocol arp police** コマンドでサポートされている最小値は、実稼働ネットワークでは小さすぎます。
- ARP パケットの長さは約 40 バイトで、ARP 応答パケットの長さは約 60 バイトです。ポリサー レート値の単位はビット/秒です。バースト値の単位はバイト/秒です。まとめると、ARP 要求および応答は、約 800 ビットです。
- 設定したレート制限は、PFC および各 DFC に別々に適用されます。RP CPU は、設定値にフォワーディング エンジンの数を乗算した数を受け取ります。
- ポリシー ベースのプロトコル パケット ポリシングは、フォワーディング エンジン（PFC およびすべての DFC）ごとに適用されます。
- Supervisor Engine 2T を使用する場合、ポリシー ベースのプロトコル パケット ポリシングは、分散集約ポリシングをサポートします（「分散型の集約ポリシングのイネーブル化」（P.63-8）を参照）。
- プロトコル パケット ポリシング メカニズムは、ラインレート ARP 攻撃などの攻撃から RP CPU を事実上保護しますが、スイッチ へのルーティング プロトコルと ARP パケットの両方をポリシングし、CoPP を下回る粒度で、スイッチを介するトラフィックをポリシングします。
- ポリシング メカニズムとポリシング回避メカニズムは、ルート設定を共有します。ポリシング回避メカニズムでは、ルーティング プロトコルと ARP パケットが、QoS ポリサーに達したとき、ネットワークを流れます。このメカニズムは、**platform qos protocol** *protocol_name* **pass-through** コマンドを使用して設定できます。
- ポリシー ベースのプロトコル パケット ポリシングは、マイクロフロー ポリサーをサポートしていません。
- 入力ポリシー ベースのプロトコル パケット ポリシングだけがサポートされています。

- ポリシー ベースのプロトコル パケット ポリシングは、レイヤ 4 ACL 演算子（「ACL のレイヤ 4 演算の制約事項」（P.69-2）を参照）をサポートしていません。この結果、さらに、次の制限が課されます。
  - IPv4 トラフィックまたは IPv6 トラフィックで、UDP または TCP のポート範囲マッチングがサポートしません
  - IPv6 トラフィックで、優先順位または DSCP のマッチングがサポートされません
- プロトコル パケット ポリシング ポリシーでは、QoS ポリシーと、1 つの集約ポリサーを共有できます。
- 集約ポリサーは、入力トラフィックと出力トラフィックの両方には適用できません。
- Supervisor Engine 2T を使用する場合、ポリシー ベースのプロトコル パケット ポリシングでは、最大 1,000 個のグローバル TCAM エントリをサポートします。
- ポリシー ベースのプロトコル パケット ポリシングでは、**class default** and **permit** *protocol_name* **any any** コマンドをサポートしていますが、プロトコル パケット ポリシング ポリシーでは、一致するすべてのトラフィックを処理するため、トラフィック フローに大きく影響することがあります。
- Supervisor Engine 2T を使用する場合、ポリシー ベースのプロトコル パケット ポリシングは、設定されている任意のポートの信頼状態で動作します。
- 単一コマンドのプロトコル パケット ポリシングとポリシー ベースのプロトコル パケット ポリシングの両方を設定できます。単一コマンドのプロトコル パケット ポリシングが最初に適用され、次に、ポリシー ベースのプロトコル パケット ポリシングが適用されます。

（注）　ソフトウェアでは、単一コマンドのプロトコル パケット ポリシングとポリシー ベースのプロトコル パケット ポリシングの間にある設定の不整合を検出せず、解決も試みません。

- ポリシー ベースのプロトコル パケット ポリシングとコントロール プレーン ポリシングの両方を設定できます（第 77 章「コントロール プレーン ポリシング（CoPP）」を参照）。ポリシー ベースのプロトコル パケット ポリシングが最初に適用され、次に、CoPP が適用されます。
- 単一コマンドのプロトコル パケット ポリシングは、入力トラフィック用に設定されたプロトコル固有のアクションをプログラムし、入力結果の出力トラフィックを維持するために、対応する出力トラフィックパススルー アクションを自動的にプログラムします。
- ポリシー ベースのプロトコル パケット ポリシングでは、出力トラフィックで入力ポリシングの結果を自動的に保持しません。
  - ポリシー ベースのプロトコル パケット ポリシングを使用して、出力トラフィックで入力ポリシングの結果を保持するには、適切な出力ポリシーを設定します。出力トラフィックを未変更で渡すには、出力ポリシー内の各入力クラスを複製し、クラス マップのアクションとして **trust dscp** を設定します。
  - 出力ポリシーマップがない場合、出力トラフィックは、設定された任意のインターフェイス ベース ポリシーマップによって処理され、入力のグローバル ポリシーの結果は上書きされます。
- PFC および任意の DFC は、**class-map match-all** クラス マップで単一の **match** コマンドをサポートします。ただし、**match protocol** コマンドは、**match dscp** または **match precedence** コマンドによってクラス マップに設定できます。
- PFC および任意の DFC は、**class-map match-any** クラス マップで複数の **match** コマンドをサポートします。
- クラス マップでは、表 76-1 に記載されている **match** コマンドを使用して、一致基準に基づくトラフィック クラスを設定できます。

表 76-1　トラフィック分類のクラス マップの match コマンドと一致基準

match コマンド	方向	一致基準
match access-group {*access_list_number* | **name** *access_list_name*}	入力	アクセス コントロール リスト（ACL）。 （注）　ACL は、次の要素の照合に使用します。 - CoS 値 - VLAN ID - パケット長
match any	入力	任意の一致基準
match cos	入力	CoS 値
match discard-class	入力	廃棄クラスの値。
match dscp （注）　**match protocol** コマンドは、**match dscp** コマンドでクラス マップに設定できます。	入力	DSCP 値。
match l2 miss	入力	現在学習されていない MAC レイヤの宛先アドレスにアドレス指定されているため、VLAN でフラッディングしたレイヤ 2 トラフィック。
match mpls experimental topmost	入力	最上位ラベルの MPLS EXP 値。
match precedence （注）　**match protocol** コマンドは、**match precedence** コマンドでクラス マップに設定できます。	入力	IP precedence 値。
match protocol {**arp** | **ip** | **ipv6**} （注）　**match protocol** コマンドは、**match dscp** コマンドまたは **match precedence** コマンドでクラス マップに設定できます。	入力	プロトコル。
match qos-group	入力	QoS グループ ID。

PFC および任意の DFC は、**match access group** コマンドで使用するために、次の ACL タイプをサポートしています。

プロトコル	番号付き ACL の有無	拡張 ACL の有無	名前付き ACL の有無
IPv4	Yes： 1 ～ 99 1300 ～ 1999	Yes： 100 ～ 199 2000 ～ 2699	Yes
IPv6	N/A	Yes（名前付き）	Yes
MAC レイヤ	N/A	N/A	Yes
ARP	N/A	N/A	Yes

グローバル プロトコル パケット ポリシングに関する情報

攻撃者はルーティング プロトコル制御パケット（ARP パケットなど）によって、RP CPU を過負荷にしようと試みることがあります。プロトコル パケット ポリシングでは、ハードウェアでこのトラフィックをレート制限します。リリース 15.1(1) SY1 以降のリリースでは、Cisco Feature Navigator にグローバル QoS ポリシー機能として表示される、ポリシー ベースのグローバル プロトコル パケット ポリシングをサポートしています。

単一コマンドのグローバル プロトコル パケット ポリシングの設定方法

platform qos protocol ? と入力して、サポートされているルーティング プロトコルを表示します。

プラットフォーム タイプ qos protocol arp police コマンドは、ARP パケットをレート制限します。次に、1 秒あたり、ARP 要求と応答を合計 200 個許可する例を示します。

```
Router(config)# platform qos protocol arp police 200000 6000
```

次に、プロトコル パケット ポリシングで使用できるプロトコルを表示する例を示します。

```
Router(config)# platform qos protocol ?
  isis
  eigrp
  ldp
  ospf
  rip
  bgp
  ospfv3
  bgpv2
  ripng
  neigh-discover
  wlccp
  arp
```

次に、**platform qos protocol** コマンドで使用できるキーワードを表示する例を示します。

```
Router(config)# platform qos protocol protocol_name ?
  pass-through  pass-through keyword
  police        police keyword
  precedence    change ip-precedence(used to map the dscp to cos value)
```

ポリシー ベースのグローバル プロトコル パケット ポリシングの設定方法

次の QoS セクションおよびグローバル プロトコル パケット ポリシング ポリシー マップ コンフィギュレーション セクションを参照してください。

- 「クラス マップの設定」（P.63-8）
- 「ポリシー マップ コンフィギュレーション」（P.63-9）
- 「グローバル プロトコル パケット ポリシング ポリシー マップの設定」（P.76-7）

グローバル プロトコル パケット ポリシング ポリシー マップの設定

グローバル プロトコル パケット ポリシング 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
`Router(config)# platform qos service-policy input policy_map_name`	グローバル プロトコル パケット ポリシング ポリシー マップを設定します。 **（注）**　入力ポリシーを 1 つ設定できます。

ユニキャスト リバース パス転送（uRPF）チェック

uRPF チェックの前提条件

なし。

uRPF チェックの制約事項

- ユニキャスト RPF は、スプーフィングに対する完全な保護を提供しません。送信元 IP アドレスに戻る適切なルートが存在する場合は、スプーフィングされたパケットが、ユニキャスト RPF に対応したインターフェイスを介してネットワークに侵入する可能性があります。
- 各インターフェイスにユニキャスト RPF モードを 1 つ設定できます。
- ユニキャスト RPF モードの「allow default」オプションでは、スプーフィングを十分に防止できません。
  - Allow Default を使用したストリクト ユニキャスト RPF チェック：ルーティング テーブルに存在するプレフィックスが送信元である受信 IP トラフィックは、そのプレフィックスが入力インターフェイス経由で到達可能な場合、ユニキャスト RPF チェックに合格します。デフォルト ルートが設定されている場合、ルーティング テーブル内に存在しない送信元プレフィックスを持つ IP パケットは、入力インターフェイスがデフォルト ルートのリバース パスである場合は、ユニキャスト RPF チェックに合格します。
  - Allow Default を使用したルーズ ユニキャスト RPF チェック：デフォルト ルートが設定されている場合、すべての IP パケットがユニキャスト RPF チェックに合格します。
- ユニキャスト RPF ストリクト モード：ユニキャスト RPF ストリクト モードでは、スプーフィングされたトラフィックに対して最高のセキュリティを提供します。ユニキャスト RPF チェック対応のすべてのインターフェイスで、トラフィックのリバース パスであるインターフェイス経由で有効な IP トラフィックをスイッチが受信すると、ストリクト モードがオプションとなります。

- ユニキャスト RPF のルーズ モード：ユニキャスト RPF のルーズ モードは、ストリクト モードほど保護できない一方で、トラフィックのリバース パスでないインターフェイスで有効な IP トラフィックを受信するスイッチのオプションとなります。ユニキャスト RPF ルーズ モードでは、受信したトラフィックの送信元が、トラフィックが到着したインターフェイスに関係なく、ルーティング テーブル内に存在するプレフィックスであることを確認します。

uRPF チェックについて

ユニキャスト RPF チェックでは、受信した IP パケットの送信元アドレスが到達可能であることを確認します。ユニキャスト RPF チェックでは、検証可能な IP 送信元プレフィックス（ルート）がない IP パケットは廃棄されます。これにより、変形または偽造（スプーフィング）された IP 送信元アドレスを持つトラフィックによる問題が軽減されます。

PFC4 および DFC4 は最大 16 個のパスで、ACL フィルタリングの有無を問わず、IPv4 と IPv6 の両方のトラフィックのユニキャスト RPF チェックに対するハードウェア サポートを提供します。

17 以上のリバース パス インターフェイスが各プレフィックスのルーティング テーブルに存在しなことを確認するには、OSPF、EIGRP、または BGP の設定時に config-router モードで **maximum-paths 16** コマンドを入力します。

ユニキャスト RPF チェックの設定手順

- 「ユニキャスト RPF チェック モードの設定」（P.76-9）
- 「self-ping のイネーブル化」（P.76-10）

（注）　次のコマンドは CLI にありますが、機能しません。

- **platform ip cef rpf interface-group**
- **platform ip cef rpf multipath interface-group**
- **platform ip cef rpf multipath pass**
- **platform ip cef rpf multipath punt**

ユニキャスト RPF チェック モードの設定

ユニキャスト RPF チェック 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	Router(config)# **interface** {{**vlan** *vlan_ID*} | {*type slot/port*} | {**port-channel** *number*}}	設定するインターフェイスを選択します。 **（注）** ユニキャスト RPF チェックは次の宛先にパケットを転送する前に、入力ポートに基づいて、最適なリターン パスを確認します。
ステップ 2	Router(config-if)# **ip verify unicast source reachable-via** {**rx** | **any**} [**allow-default**] [*list*]	IPv4 ユニキャスト RPF チェック モードを設定します。
ステップ 3	Router(config-if)# **ipv6 verify unicast source reachable-via** {**rx** | **any**} [**allow-default**] [*list*]	IPv6 ユニキャスト RPF チェック モードを設定します。
ステップ 4	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。
ステップ 5	Router# **show platform hardware cef ip rpf**	IPv4 の設定を確認します。
ステップ 6	Router# **show platform hardware cef ipv6 rpf**	IPv6 の設定を確認します。

- strict チェック モードをイネーブルにするには、**rx** キーワードを使用します。
- exist-only チェック モードをイネーブルにするには、**any** キーワードを使用します。
- RPF の確認にデフォルト ルートを使用できるようにするには、**allow-default** キーワードを使用します。
- アクセス リストを識別するには、*list* オプションを使用します。
  - アクセス リストによってネットワークへのアクセスが拒否された場合は、拒否されたパケットがポートでドロップされます。
  - アクセス リストによってネットワークへのアクセスが許可された場合は、パケットが宛先アドレスに転送されます。転送されたパケットは、インターフェイスの統計情報にカウントされます。
  - アクセス リストにログ アクションが含まれている場合、パケットに関する情報がログ サーバに送信されます。

次に、ギガビット イーサネット ポート 4/1 でユニキャスト RPF の exist-only チェック モードをイネーブルにする例を示します。

```
Router(config)# interface gigabitethernet 4/1
Router(config-if)# ipv6 verify unicast source reachable-via any
Router(config-if)# ip verify unicast source reachable-via any
Router(config-if)# end
Router#
```

次に、ギガビット イーサネット ポート 4/2 でユニキャスト RPF の strict チェック モードをイネーブルにする例を示します。

```
Router(config)# interface gigabitethernet 4/2
Router(config-if)# ipv6 verify unicast source reachable-via rx
Router(config-if)# ip verify unicast source reachable-via rx
Router(config-if)# end
Router#
```

self-ping のイネーブル化

ユニキャスト RPF チェックがイネーブルの場合、スイッチはデフォルトで自身を ping できません。self-ping 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	`Router(config)# interface {{vlan vlan_ID} | {type slot/port} | {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	`Router(config-if)# ip verify unicast source reachable-via any allow-self-ping`	self-ping またはセカンダリ アドレスへの ping を実行できるように、スイッチ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。

次に、self-ping をイネーブルにする例を示します。

```
Router(config)# interface gigabitethernet 4/1
Router(config-if)# ip verify unicast source reachable-via any allow-self-ping
Router(config-if)# end
```

スティッキ ARP の設定

スティッキ ARP では、ARP エントリ（IP アドレス、MAC アドレス、送信元 VLAN）が上書きされないようにして、MAC アドレスのスプーフィングを防止します。スイッチは ARP エントリを、エンドデバイスまたはその他のスイッチにトラフィックを転送するために維持します。ARP エントリは、一般的に定期的に更新されるか、ARP ブロードキャストを受信したときに修正されます。攻撃中に ARP ブロードキャストは、スプーフィングされた MAC アドレス（正当な IP アドレスを含む）を使用して送信されるので、スイッチは、スプーフィングされた MAC アドレスを含む正当な IP アドレスを学習し、その MAC アドレスにトラフィックを転送し始めます。スティッキ ARP をイネーブルにすると、スイッチは ARP エントリを学習し、ARP ブロードキャストで受信した修正を受け入れません。スティッキ ARP 設定を上書きしようとすると、エラー メッセージが表示されます。

sticky ARP をレイヤ 3 インターフェイス上で設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface type[1] slot/port`	スティッキ ARP を適用するインターフェイスを選択します。
ステップ 2	`Router(config-if)# ip sticky-arp`	スティッキ ARP をイネーブルにします。
ステップ 3	`Router(config-if)# ip sticky-arp ignore`	スティッキ ARP をディセーブルにします。

1. *type* = **fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、インターフェイス 5/1 でスティッキ ARP をイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 5/1
Router(config-if)# ip sticky-arp
Router(config-if)# end
Router#
```

パケット ドロップ統計のモニタ

パケット ドロップ統計の前提条件

なし。

パケット ドロップ統計の制約事項

- 着信取り込みトラフィックはフィルタ処理されません。
- 着信取り込みトラフィックは、取り込み宛先にレート制限されません。

パケット ドロップ統計について

パケット ドロップ統計を表示するには、show コマンドを使用できます。トラフィックをインターフェイス上でキャプチャし、このトラフィックのコピーをポートに接続されたトラフィック アナライザに送信します。トラフィック アナライザは、パケット ドロップ統計を集約します。

ドロップされたパケットのモニタ方法

show コマンドの使用

PFC および DFC では、ハードウェア内の ACL ヒット カウンタがサポートされます。ACL TCAM におけるそれぞれのエントリを表示するには、**show platform hardware acl entry interface** コマンドを使用できます。TTL および IP のオプション カウンタを使用し、レイヤ 3 フォワーディング エンジンのパフォーマンスをモニタすることもできます。

次に、**show platform hardware acl entry interface** コマンドを使用して、レイヤ 3 フォワーディング エンジンに関連するパケット統計およびエラーを表示する例を示します。

```
Router# show platform hardware statistics

 --- Hardware Statistics for Module 6 ---


L2 Forwarding Engine
    Switched in L2 : 59624 @ 7 pps

L3 Forwarding Engine
```

```
    Processed in L3 : 59624 @ 7 pps
    Switched in L3  : 13 @ 0 pps

    Bridged         : 4602
    FIB Switched
        IPv4 Ucast : 7
        IPv6 Ucast : 1
        EoMPLS     : 1
        MPLS       : 1
        (S , *)    : 0
        IGMP MLD   : 0
        IPv4 Mcast : 2
        IPv6 Mcast : 0
        Mcast Leak : 0
    ACL Routed
        Input      : 1
        Output     : 518
    Netflow Switched
        Input      : 2
        Output     : 0
    Exception Redirected
        Input      : 0
        Output     : 1
    Mcast Bridge Disable & No Redirect
                   : 0
    Total packets with TOS Changed              : 3
    Total packets with TC  Changed              : 0
    Total packets with COS Changed              : 64
    Total packets with EXP Changed              : 0
    Total packets with QOS Tunnel Encap Changed : 1
    Total packets with QOS Tunnel Decap Changed : 1
    Total packets dropped by ACL                : 1
    Total packets dropped by Policing           : 0
Errors
    MAC/IP length inconsistencies               : 0
    Short IP packets received                   : 0
    IP header checksum errors                   : 0
    TTL failures                                : 0
    MTU failures                                : 0

Total packets L3 Processed by all Modules: 59624 @ 7 pps
```

SPAN の使用方法

次に、**monitor session** コマンドを使用して、トラフィックを取り込んで外部インターフェイスに転送する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# monitor session 1 source vlan 44 both
Router(config)# monitor session 1 destination interface g9/1
Router(config)# end
Router#
```

次に、**show monitor session** コマンドを使用して、宛先ポートを表示する例を示します。

```
Router# show monitor session 1
Session 1
---------
Source Ports:
    RX Only:       None
    TX Only:       None
    Both:          None
```

```
Source VLANs:
    RX Only:        None
    TX Only:        None
    Both:           44
Destination Ports: Gi9/1
Filter VLANs:       None
```

詳細については、第 56 章「ローカル SPAN、RSPAN、および ERSPAN」を参照してください。

VACL キャプチャの使用

VACL 取り込み機能では、取り込みトラフィックを転送するように設定されたポートにトラフィックを転送できます。capture アクションを指定すると、転送されたパケットのキャプチャ ビットが設定されて、キャプチャ機能がイネーブルであるポートがパケットを受信できるようになります。キャプチャできるのは、転送されたパケットだけです。

各 VLAN から別のインターフェイスにトラフィックを割り当てるには、VACL 取り込みを使用できます。

VACL 取り込みでは、HTTP などの、あるタイプのトラフィックを 1 つのインターフェイスに、DNS などの別のタイプのトラフィックを別のインターフェイスに送信できません。VACL 取り込み粒度は、ローカルにスイッチングされるトラフィックだけに適用可能です。トラフィックをリモート スイッチに転送する場合は、粒度を維持できません。

詳細については、第 74 章「VLAN ACL（VACL）」を参照してください。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

コントロール プレーン ポリシング（CoPP）

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- CoPP の詳細については、次のドキュメントを参照してください。

  http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/white_paper_c11-663623.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CoPP の前提条件

なし。

CoPP の制約事項

- PFC および DFC では、マルチキャスト トラフィックと一致するクラスがハードウェアでサポートされます。
- ブロードキャスト パケットについては、ハードウェアでは CoPP がサポートされません。ブロードキャスト DoS 攻撃からの保護を実現するには、ACL、トラフィック ストーム制御、および CoPP ソフトウェア保護を組み合わせて使用します。
- CoPP では、デフォルトの非 IP クラスを除いて、非 IP クラスがサポートされません。非 IP クラスの代わりに ACL を使用して非 IP トラフィックをドロップでき、デフォルトの非 IP CoPP クラスを使用して、RP CPU に到達する非 IP トラフィックに制限できます。
- CoPP ポリシー ACL では **log** キーワードを使用しないでください。
- QoS 設定が大きい場合は、TCAM スペースが不足することがあります。この場合は、CoPP がソフトウェアで実行される場合があります。
- その他のインターフェイスで QoS 設定が大きい場合は、TCAM スペースが不足することがあります。この状況が発生した場合は、CoPP が全体的にソフトウェアで実行され、パフォーマンスの低下および CPU サイクルの消費という結果になることがあります。
- CoPP ポリシーによって、ルーティング プロトコルまたはスイッチへの対話型アクセスなどの重要なトラフィックがフィルタリングされないことを確認してください。このトラフィックをフィルタリングすると、スイッチへのリモート アクセスが妨害され、コンソール接続が必要になることがあります。
- PFC および DFC は、組み込みの special-case レート リミッタをサポートします。これは、ACL を使用できない状況（TTL、MTU、IP オプションなど）で便利です。特殊ケース レート リミッタをイネーブルにする場合は、この特殊ケース レート リミッタにより、レート リミッタの基準に一致するパケットの CoPP ポリシーが上書きされることに注意してください。
- 出力 CoPP もサイレント モードもサポートされません。CoPP は入力だけでサポートされます（サービス ポリシー出力 CoPP は、制御プレーン インターフェイスに適用できません）。
- ハードウェアの ACE ヒット カウンタは ACL ロジック専用です。ソフトウェア ACE ヒット カウンタ、および **show access-list** コマンド、**show policy-map control-plane** コマンド、**show platform ip qos** コマンドを使用して、CPU トラフィックのトラブルシューティングと評価ができます。
- CoPP はフォワーディング エンジンごとに実行され、ソフトウェア CoPP は一括で実行されます。
- CoPP では、**log** キーワードを使用した ACE がサポートされません。
- CoPP では、ハードウェア QoS TCAM リソースが使用されます。**show tcam utilization** コマンドを入力し、TCAM の使用状況を確認してください。
- 後続クラスで設定されるフィルタリングとポリシングに一致しないようにするには、クラスごとにポリシングを設定します。CoPP は、police コマンドを含まないクラスでフィルタリングを適用しません。police コマンドを含まないクラスはどのトラフィックとも一致しません。
- 分類に使用される ACL は QoS ACL です。サポートされる QoS ACL は、IP 標準 ACL、拡張 ACL、および名前付き ACL です。
- サポートされる一致タイプは以下だけです。
  - **ip precedence**
  - **ip dscp**
  - **access-group**
- ハードウェアでは IP ACL だけがサポートされます。

- MAC ベースの照合はソフトウェアだけで実行されます。
- 単一クラス マップで入力できる **match** コマンドは 1 つだけです。
- サービス ポリシーを定義する場合、サポートされているアクションは **police** ポリシー マップ アクションだけです。
- 制御プレーンにサービス ポリシーを適用する場合は、**input** 方向だけがサポートされます。

CoPP の概要

RP によって管理されるトラフィックは、次の 3 つの機能コンポーネント（*プレーン*）に分類されます。

- データ プレーン
- 管理プレーン
- 制御プレーン

コントロール プレーン ポリシング（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 RP 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スイッチのセキュリティを向上させます。PFC および DFC では、CoPP がハードウェアでサポートされます。CoPP はハードウェア レート リミッタと連携して動作します。

PFC および DFC では、組み込みの「特殊ケース」レート リミッタがサポートされます。IP オプション ケース、TTL および MTU のエラー ケース、エラーを含むパケット、マルチキャスト パケットなどの特定シナリオを ACL が分類できない場合は、これを使用できます。特殊ケース レート リミッタをイネーブルにすると、この特殊ケース レート リミッタにより、レート リミッタの基準に一致するパケットの CoPP ポリシーが上書きされます。

RP の管理するトラフィックのほとんどは、コントロール プレーンおよびマネジメント プレーンによって処理されます。CoPP を使用すると、制御プレーンおよび管理プレーンを保護でき、ルーティングの安定性、到達可能性、パケット配信を確保できます。CoPP では、Modular QoS CLI（MQC）で専用制御プレーン設定が使用され、フィルタ機能およびレート制限機能が制御プレーン パケットに提供されます。

最初にクラス マップを定義し、分類するトラフィックを識別する必要があります。クラス マップでは、特定トラフィック クラスのパケットが定義されます。トラフィックを分類したら、識別されたトラフィックにポリシー アクションを実行するための、ポリシー マップを作成できます。

CoPP のデフォルト設定

CoPP はデフォルトで有効になっています。デフォルトの CoPP 設定をディセーブルにするには、**no service-policy input policy-default-autocopp** コントロール プレーン コンフィギュレーション モード コマンドを入力します。

これらは、デフォルトの CoPP クラス マップです。

```
class-map match-any class-copp-icmp-redirect-unreachable
class-map match-all class-copp-glean
class-map match-all class-copp-receive
class-map match-all class-copp-options
class-map match-all class-copp-broadcast
class-map match-all class-copp-mcast-acl-bridged
class-map match-all class-copp-slb
class-map match-all class-copp-mtu-fail
class-map match-all class-copp-ttl-fail
class-map match-all class-copp-arp-snooping
```

```
class-map match-any class-copp-mcast-copy
class-map match-any class-copp-ip-connected
class-map match-any class-copp-match-igmp
  match access-group name acl-copp-match-igmp
class-map match-all class-copp-unknown-protocol
class-map match-any class-copp-vacl-log
class-map match-all class-copp-mcast-ipv6-control
class-map match-any class-copp-match-pimv6-data
  match access-group name acl-copp-match-pimv6-data
class-map match-any class-copp-mcast-punt
class-map match-all class-copp-unsupp-rewrite
class-map match-all class-copp-ucast-egress-acl-bridged
class-map match-all class-copp-ip-admission
class-map match-all class-copp-service-insertion
class-map match-all class-copp-mac-pbf
class-map match-any class-copp-match-mld
  match access-group name acl-copp-match-mld
class-map match-all class-copp-ucast-ingress-acl-bridged
class-map match-all class-copp-dhcp-snooping
class-map match-all class-copp-wccp
class-map match-all class-copp-nd
class-map match-any class-copp-ipv6-connected
class-map match-all class-copp-mcast-rpf-fail
class-map match-any class-copp-ucast-rpf-fail
class-map match-all class-copp-mcast-ip-control
class-map match-any class-copp-match-pim-data
  match access-group name acl-copp-match-pim-data
class-map match-any class-copp-match-ndv6
  match access-group name acl-copp-match-ndv6
class-map match-any class-copp-mcast-v4-data-on-routedPort
class-map match-any class-copp-mcast-v6-data-on-routedPort
```

これは、デフォルトの CoPP ポリシー マップです。

```
policy-map policy-default-autocopp
  class class-copp-mcast-v4-data-on-routedPort
   police rate 10 pps burst 1 packets
     conform-action drop
     exceed-action drop
  class class-copp-mcast-v6-data-on-routedPort
   police rate 10 pps burst 1 packets
     conform-action drop
     exceed-action drop
  class class-copp-icmp-redirect-unreachable
   police rate 100 pps burst 10 packets
     conform-action transmit
     exceed-action drop
  class class-copp-ucast-rpf-fail
   police rate 100 pps burst 10 packets
     conform-action transmit
     exceed-action drop
  class class-copp-vacl-log
   police rate 2000 pps burst 1 packets
     conform-action transmit
     exceed-action drop
  class class-copp-mcast-punt
   police rate 1000 pps burst 256 packets
     conform-action transmit
     exceed-action drop
  class class-copp-mcast-copy
   police rate 1000 pps burst 256 packets
     conform-action transmit
     exceed-action drop
  class class-copp-ip-connected
```

```
 police rate 1000 pps burst 256 packets
   conform-action transmit
   exceed-action drop
class class-copp-ipv6-connected
 police rate 1000 pps burst 256 packets
   conform-action transmit
   exceed-action drop
class class-copp-match-pim-data
 police rate 1000 pps burst 1000 packets
   conform-action transmit
   exceed-action drop
class class-copp-match-pimv6-data
 police rate 1000 pps burst 1000 packets
   conform-action transmit
   exceed-action drop
class class-copp-match-mld
 police rate 10000 pps burst 10000 packets
   conform-action set-discard-class-transmit 48
   exceed-action transmit
class class-copp-match-igmp
 police rate 10000 pps burst 10000 packets
   conform-action set-discard-class-transmit 48
   exceed-action transmit
class class-copp-match-ndv6
 police rate 1000 pps burst 1000 packets
   conform-action set-discard-class-transmit 48
   exceed-action drop
```

CoPP の設定方法

CoPP の設定

CoPP 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 access-list extended access_list_name`	拡張 ACL を作成します。 **（注）** ほとんどの場合は、重要なトラフィックまたは重要でないトラフィックを識別する ACL を設定する必要があります。
ステップ 2	`Router(config-ext-nacl)# {permit | deny} protocol source source_wildcard destination destination_wildcard [precedence precedence] [tos tos] [established] [log | log-input] [time-range time_range_name] [fragments]`	ACL のフィルタリングを設定します。 • **permit** では、パケットが名前付き IP アクセス リストで合格する条件を設定します。 • **deny** では、パケットが名前付き IP アクセス リストで不合格になる条件を設定します。
ステップ 3	`Router(config)# class-map traffic_class_name`	クラス マップを作成します。
ステップ 4	`Router(config-cmap)# match {ip precedence | ip dscp | access_group}`	クラス マップでの一致を設定します。
ステップ 5	`Router(config)# policy-map service-policy-name`	サービス ポリシー マップを定義します。

	コマンド	目的
ステップ 6	`Router(config-pmap)# class traffic_class_name`	ポリシー マップ クラスを作成します。

ステップ 7	`Router(config-pmap-c)# police bits_per_second [normal_burst_bytes [maximum_burst_bytes]] [pir peak_rate_bps] [[[conform-action selected_action] exceed-action selected_action] violate-action selected_action]`
	
	`Router(config-pmap-c)# police rate units bps [burst burst_bytes bytes] [peak-rate peak_rate_bps bps] [peak-burst peak_burst_bytes bytes] [conform-action selected_action] [exceed-action selected_action] [violate-action selected_action]`
	
	`Router(config-pmap-c)# police rate units pps [burst burst_packets packets] [peak-rate peak_rate_pps pps] [peak-burst peak_burst_packets packets] [conform-action selected_action] [exceed-action selected_action] [violate-action selected_action]`
	
	`Router(config-pmap-c)# police flow [mask {src-only | dest-only | full-flow}] bits_per_second normal_burst_bytes [[[conform-action {drop | set-dscp-transmit dscp_value | set-prec-transmit ip_precedence_value | transmit}] exceed-action {drop | policed-dscp | transmit}] violate-action {drop | policed-dscp | transmit}]`
		サービス ポリシー マップでのポリシングを設定します。次のいずれかを設定できます。
		• バイト ベースのポリシング。
		• パケット ベースのポリシング。
		• フロー ベースのポリシング。
		「ポリシー マップ クラスのポリシングの設定」（P.63-12）を参照してください。

ステップ 8	`Router(config)# control-plane`	制御プレーン 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	`Router(config-cp)# service-policy input service-policy-name`	QoS サービス ポリシーを制御プレーンに適用します。

CoPP トラフィック分類の定義

トラフィック分類の概要

任意の数のクラスを定義できますが、一般的にトラフィックは、相対的な重要性に基づいたクラスにグループ化されます。グループ化の例を以下に示します。

- ボーダー ゲートウェイ プロトコル（BGP）：BGP キープアライブおよびルーティング アップデートなどの BGP ルーティング プロトコルのネイバー関係の維持で重要となるトラフィック。BGP ルーティング プロトコルを維持することは、ネットワーク内の接続を維持するために、またはサービス プロバイダーにとって重要です。BGP を実行しないサイトでこのクラスを使用する必要はありません。

- Interior Gateway Protocol（IGP; 内部ゲートウェイ プロトコル）：Open Shortest Path First（OSPF）、Enhanced Interior Gateway Routing Protocol（EIGRP）、Routing Information Protocol（RIP）などの IGP ルーティング プロトコルの維持で重要になるトラフィック。IGP ルーティング プロトコルを維持することは、ネットワーク内の接続を維持するために重要となります。
- 管理：日常業務で必要な、頻繁に使用される必須トラフィック。たとえば、リモート ネットワーク アクセスに使用するトラフィックや、Cisco IOS イメージの更新および管理トラフィックです。これには、Telnet、Secure Shell（SSH; セキュア シェル）、ネットワーク タイム プロトコル（NTP）、簡易ネットワーク管理プロトコル（SNMP）、Terminal Access Controller Access Control System（TACACS）、ハイパーテキスト転送プロトコル（HTTP）、Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）、ファイル転送プロトコル（FTP）などがあります。
- レポート：レポートする目的でネットワーク パフォーマンス統計を生成するために使用されるトラフィック。たとえば、さまざまな QoS データ クラス内の応答時間でレポートするために、Cisco IOS IP サービス レベル契約（SLA）を使用して、さまざまな DSCP 設定で ICMP を生成することなど。
- モニタ：スイッチのモニタに使用されるトラフィック。このトラフィックは許可する必要がありますが、スイッチを危険にさらすことがあってはなりません。CoPP を使用すると、このトラフィックは許可されますが、低いレートに制限できます。たとえば、ICMP エコー要求（ping）および traceroute など。
- クリティカル アプリケーション：特定カスタマーの環境に固有で重要なクリティカル アプリケーション トラフィック。このクラスに分類するトラフィックは、ユーザに必要なアプリケーションの要件に合わせて、特別に調整する必要があります。マルチキャストを使用するお客様もいれば、IP セキュリティまたは総称ルーティング カプセル化（GRE）を使用するお客様もいます。たとえば、GRE、ホットスタンバイ ルータ プロトコル（HSRP）、仮想ルータ冗長プロトコル（VRRP）、Session Initiation Protocol（SIP）、データ リンク スイッチング（DLSw）、ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）、Multicast Source Discovery Protocol（MSDP）、インターネット グループ管理プロトコル（IGMP）、Protocol Independent Multicast（PIM）、マルチキャスト トラフィック、IPSec など。
- レイヤ 2 プロトコル：アドレス解決プロトコル（ARP）に使用されるトラフィック。ARP パケットが過剰に発生すると、RP リソースが独占され、他の重要なプロセスがリソース不足になってしまう可能性があります。CoPP を使用して ARP パケットをレート制限すると、このような状況を回避できます。一致プロトコル分類基準を使用して明確に分類できるレイヤ 2 プロトコルは、ARP だけです。
- 不要：RP へのアクセスを無条件でドロップおよび拒否する必要のある、不正な、または悪意あるトラフィックを明示的に指定します。この分類は、スイッチ宛ての既知のトラフィックを常に拒否する必要があり、デフォルト カテゴリに含まれないようにする場合に特に便利です。トラフィックを明示的に拒否する場合は、**show** コマンドを入力して拒否トラフィックに関する概算統計を収集してレートを見積もることができます。
- デフォルト：他に分類されない、RP 宛ての残りのトラフィックすべてを収容。MQC はデフォルト クラスを提供するので、ユーザは、その他のユーザ定義クラスで明示的に識別されないトラフィックに適用する処置を指定できます。このトラフィックの RP へのアクセス レートは、大幅に制限されます。デフォルト分類を適切に使用すると、統計をモニタし、これを使用しない場合は識別されないコントロール プレーンを宛先とするトラフィックのレートを判断できます。このトラフィックが識別されたあとは、さらに分析を実行して分類し、必要な場合は、その他の CoPP ポリシー エントリを更新してこのトラフィックに対応できます。

トラフィックの分類が完了したら、ポリシーの定義に使用される、トラフィックのクラスを ACL が構築します。CoPP 分類の基本的な ACL の例については、「CoPP トラフィック分類の基本 ACL 例」（P.77-8）を参照してください。

トラフィック分類の制約事項

- 実際の CoPP ポリシーを開発する前に、必要なトラフィックを識別してさまざまなクラスに分類する必要があります。トラフィックは、相対的な重要性に基づく 9 個のクラスにグループ化されます。実際に必要となるクラスの数は異なることがあり、ローカルの要件とセキュリティ ポリシーに基づいて選択する必要があります。
- 双方向に一致するポリシーを定義する必要はありません。ポリシーは入力だけに適用されるため、トラフィックは一方向（ネットワークから RP へ）だけで識別します。

CoPP トラフィック分類の基本 ACL 例

ここでは、CoPP 分類の基本的な ACL 例を示します。この例では、一般的に必要なトラフィックが、次の ACL で識別されます。

- ACL 120：クリティカル トラフィック
- ACL 121：重要トラフィック
- ACL 122：通常トラフィック
- ACL 123：不要なトラフィックを明示的に拒否
- ACL 124：その他すべてのトラフィック

次に、クリティカル トラフィック用に ACL 120 を定義する例を示します。

```
Router(config)# access-list 120 remark CoPP ACL for critical traffic
```

次に、既知のピアからこのスイッチの BGP TCP ポートへの BGP を許可する例を示します。

```
Router(config)# access-list 120 permit tcp host 47.1.1.1 host 10.9.9.9 eq bgp
```

次に、ピアの BGP ポートからこのスイッチへの BGP を許可する例を示します。

```
Router(config)# access-list 120 permit tcp host 47.1.1.1 eq bgp host 10.9.9.9
Router(config)# access-list 120 permit tcp host 10.86.183.120 host 10.9.9.9 eq bgp
Router(config)# access-list 120 permit tcp host 10.86.183.120 eq bgp host 10.9.9.9
```

次に、重要クラス用に ACL 121 を定義する例を示します。

```
Router(config)# access-list 121 remark CoPP Important traffic
```

次に、TACACS ホストからのリターン トラフィックを許可する例を示します。

```
Router(config)# access-list 121 permit tcp host 1.1.1.1 host 10.9.9.9 established
```

次に、サブネットからスイッチへの SSH アクセスを許可する例を示します。

```
Router(config)# access-list 121 permit tcp 10.0.0.0 0.0.0.255 host 10.9.9.9 eq 22
```

次に、特定サブネットのホストからスイッチへの Telnet の完全アクセスを許可し、残りのサブネットをポリシングする例を示します。

```
Router(config)# access-list 121 deny tcp host 10.86.183.3 any eq telnet
Router(config)# access-list 121 permit tcp 10.86.183.0 0.0.0.255 any eq telnet
```

次に、NMS ホストからスイッチへの SNMP アクセスを許可する例を示します。

```
Router(config)# access-list 121 permit udp host 1.1.1.2 host 10.9.9.9 eq snmp
```

次に、スイッチが既知のクロック ソースから NTP パケットを受信できるようにする例を示します。

```
Router(config)# access-list 121 permit udp host 1.1.1.3 host 10.9.9.9 eq ntp
```

次に、通常トラフィック クラス用に ACL 122 を定義する例を示します。

```
Router(config)# access-list 122 remark CoPP normal traffic
```

次に、スイッチからの traceroute トラフィックを許可する例を示します。

```
Router(config)# access-list 122 permit icmp any any ttl-exceeded
Router(config)# access-list 122 permit icmp any any port-unreachable
```

次に、ping を発信したスイッチに応答の受信を許可する例を示します。

```
Router(config)# access-list 122 permit icmp any any echo-reply
```

次に、スイッチへの ping を許可する例を示します。

```
Router(config)# access-list 122 permit icmp any any echo
```

次に、不要クラス用に ACL 123 を定義する例を示します。

```
Router(config)# access-list 123 remark explicitly defined "undesirable" traffic
```

（注） 次の例において、ACL 123 は分類とモニタを目的とした許可エントリであり、トラフィックは CoPP ポリシーの結果としてドロップされます。

次に、UDP 1434 を宛先とするすべてのトラフィックをポリシング用に許可する例を示します。

```
Router(config)# access-list 123 permit udp any any eq 1434
```

次に、その他すべてのトラフィック用に ACL 124 を定義する例を示します。

```
Router(config)# access-list 124 remark rest of the IP traffic for CoPP
Router(config)# access-list 124 permit ip any any
```

CoPP のモニタ

サイト固有ポリシーを開発して制御プレーン ポリシーの統計をモニタし、CoPP をトラブルシューティングするには、**show policy-map control-plane** コマンドを入力できます。このコマンドでは、レート情報、およびハードウェアとソフトウェアの両方で設定されたポリシーに適合するバイト数（およびパケット数）と適合しないバイト数（およびパケット数）など、実際に適用されたポリシーに関するダイナミックな情報が表示されます。

show policy-map control-plane コマンドの出力は次のようになります。

```
Router# show policy-map control-plane
Control Plane Interface
  Service policy CoPP-normal
Hardware Counters:
class-map: CoPP-normal (match-all)
      Match: access-group 130
      police :
        96000 bps 3000 limit 3000 extended limit
      Earl in slot 3 :
        0 bytes
        5 minute offered rate 0 bps
        aggregate-forwarded 0 bytes action: transmit
        exceeded 0 bytes action: drop
        aggregate-forward 0 bps exceed 0 bps
      Earl in slot 5 :
        0 bytes
        5 minute offered rate 0 bps
```

```
        aggregate-forwarded 0 bytes action: transmit
        exceeded 0 bytes action: drop
        aggregate-forward 0 bps exceed 0 bps

Software Counters:
    Class-map: CoPP-normal (match-all) 0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group 130
      police:
        96000 bps, 3125 limit, 3125 extended limit
        conformed 0 packets, 0 bytes; action: transmit
        exceeded 0 packets, 0 bytes; action: drop
        conformed 0 bps, exceed 0 bps, violate 0 bps
Router#
```

ポリシーによってドロップされたり転送されたりしたバイトのハードウェア カウンタを表示するには、**show platform qos ip** コマンドを入力します。

```
Router# show platform qos ip
 QoS Summary [IP]:      (* - shared aggregates, Mod - switch module)

Int Mod Dir  Class-map DSCP  Agg  Trust Fl   AgForward-By   AgPoliced-By
                             Id         Id
-------------------------------------------------------------------------------
CPP  5  In CoPP-normal    0    1   dscp  0         505408       83822272
CPP  9  In CoPP-normal    0    4   dscp  0              0              0
Router#
```

CoPP アクセス リストの情報を表示するには、**show access-lists coppacl-bgp** コマンドを入力します。

```
Router# show access-lists coppacl-bgp
Extended IP access list coppacl-bgp
10 permit tcp host 47.1.1.1 host 10.9.9.9 eq bgp (4 matches)
20 permit tcp host 47.1.1.1 eq bgp host 10.9.9.9
30 permit tcp host 10.86.183.120 host 10.9.9.9 eq bgp (1 match)
40 permit tcp host 10.86.183.120 eq bgp host 10.9.9.9
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CHAPTER 78

Dynamic Host Configuration Protocol（DHCP）スヌーピング

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

DHCP スヌーピングの前提条件

なし。

DHCP スヌーピングの制約事項

DHCP スヌーピング設定時の制約事項

- DHCP スヌーピング データベースには少なくとも 12,000 バインディングが格納されます。
- DHCP スヌーピングをイネーブルにすると、スイッチでは次の Cisco IOS DHCP コマンドを使用できなくなります。
  - **ip dhcp relay information check** グローバル コンフィギュレーション コマンド
  - **ip dhcp relay information policy** グローバル コンフィギュレーション コマンド
  - **ip dhcp relay information trust-all** グローバル コンフィギュレーション コマンド
  - **ip dhcp relay information option** グローバル コンフィギュレーション コマンド
  - **ip dhcp relay information trusted** インターフェイス コンフィギュレーション コマンド

  次のコマンドを入力しても、スイッチからはエラー メッセージが返され、設定は適用されません。

DHCP スヌーピング設定時の注意事項

- 少なくとも 1 つの VLAN で DHCP スヌーピングをイネーブルにして、DHCP をスイッチでグローバルにイネーブルにするまで、DHCP スヌーピングはアクティブにはなりません。
- スイッチ上で DHCP スヌーピングをグローバルにイネーブルにする前に、DHCP サーバや DHCP リレー エージェントとして機能するデバイスが設定され、イネーブルになっていることを確認してください。
- DHCP サーバの設定については、次の資料を参照してください。

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_dhcp/configuration/15-sy/dhcp-15-sy-book.html
- レイヤ 2 LAN ポートが DHCP サーバに接続されている場合は、**ip dhcp snooping trust** インターフェイス コンフィギュレーション コマンドを入力して、このポートを信頼できるポートとして設定します。
- レイヤ 2 LAN ポートが DHCP クライアントに接続されている場合は **no ip dhcp snooping trust** インターフェイス コンフィギュレーション コマンドを入力して、このポートを信頼できないポートとして設定します。
- DHCP スヌーピングはプライベート VLAN 上でイネーブルにできます。
  - DHCP スヌーピングをイネーブルにすると、プライマリ VLAN の設定はすべて、関連付けられたセカンダリ VLAN に伝播します。
  - プライマリ VLAN で DHCP スヌーピングを設定してから、関連付けられたセカンダリ VLAN で DHCP スヌーピングを別の値で設定すると、セカンダリ VLAN の設定は無効になります。
  - プライマリ VLAN で DHCP スヌーピングが設定されていない場合に、セカンダリ VLAN で DHCP スヌーピングを設定すると、設定はセカンダリ VLAN だけで有効になります。
  - セカンダリ VLAN 上で DHCP スヌーピングを手動設定すると、次のメッセージが表示されます。

    ```
    DHCP Snooping configuration may not take effect on secondary vlan XXX
    ```

  - **show ip dhcp snooping** コマンドを実行すると、DHCP スヌーピングがイネーブルにされたすべての VLAN（プライマリおよびセカンダリの両方）が表示されます。

DHCP スヌーピングの最小限の設定

1. DHCP サーバを定義し、設定します。次の資料を参照してください。

   http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_dhcp/configuration/15-sy/dhcp-15-sy-book.html

2. 少なくとも 1 つの VLAN で、DHCP スヌーピングをイネーブルにします。

   デフォルトでは、すべての VLAN で DHCP スヌーピングは非アクティブです。「VLAN 上での DHCP スヌーピングのイネーブル化」（P.78-12）を参照してください。

3. DHCP サーバが、信頼できるインターフェイスを介して接続されていることを確認します。

   デフォルトでは、すべてのインターフェイスのデフォルトの信頼状態は、信頼できない状態になります。「レイヤ 2 LAN インターフェイスでの DHCP 信頼状態の設定」（P.78-13）を参照してください。

4. DHCP スヌーピング データベース エージェントの設定を設定します。

   この手順では、再起動またはスイッチオーバー後に、データベース エントリがリストアされます。「DHCP スヌーピング データベース エージェント」（P.78-14）を参照してください。

5. DHCP スヌーピングをグローバルにイネーブルにします。

   この機能は、この手順を完了するまでアクティブになりません。「DHCP スヌーピングのグローバルなイネーブル化」（P.78-9）を参照してください。

DHCP リレーのスイッチを設定する場合、次の追加手順が必要です。

1. DHCP リレー エージェント IP アドレスを定義し、設定します。

   DHCP サーバが、DHCP クライアントと異なるサブネットにある場合、クライアント側の VLAN のヘルパー アドレス フィールドで、IP アドレスを設定します。

2. 信頼できないポートで DHCP Option 82 を設定します。

   「信頼できないポートの DHCP Option 82 機能のイネーブル化」（P.78-10）を参照してください。

DHCP スヌーピングの概要

DHCP スヌーピングの概要

DHCP スヌーピングは、信頼できないホストと信頼済み DHCP サーバとの間でファイアウォールのような役割を果たすセキュリティ機能です。DHCP スヌーピング機能では、次のアクティビティが実行されます。

- 信頼できない送信元からの DHCP メッセージを検証し、無効なメッセージをフィルタ処理して除外します。
- 信頼できるソースおよび信頼できないソースからの DHCP トラフィックのレートを制限する。
- DHCP スヌーピング バインディング データベースを構築し、管理します。このデータベースには、リース IP アドレスがある信頼できないホストに関する情報が保存されています。
- DHCP スヌーピング バインディング データベースを使用して、信頼できないホストからの以降の要求を検証します。

ダイナミック ARP インスペクション（DAI）などの他のセキュリティ機能でも、DHCP スヌーピング バインディング データベースに保存されている情報が使用されます。

DHCP スヌーピングは、VLAN ベースごとにイネーブルに設定されます。デフォルトでは、すべての VLAN でこの機能は非アクティブです。この機能は、1 つの VLAN または特定の VLAN 範囲でイネーブルにできます。

DHCP スヌーピング機能はルート プロセッサ（RP）上でソフトウェアに実装されています。したがって、対応 VLAN の全 DHCP メッセージが PFC で代行受信され、処理用に RP へ転送されます。

信頼できるソースおよび信頼できないソース

DHCP スヌーピング機能では、トラフィック ソースが信頼できるかできないかについて特定されます。信頼できない送信元の場合、トラフィック攻撃やその他の敵対的アクションが開始される可能性があります。このような攻撃を防ぐために、DHCP スヌーピング機能では、メッセージをフィルタ処理し、信頼できないソースからのトラフィックのレートを制限します。

企業ネットワークでは、管理担当者の管理下にあるデバイスは、信頼できるソースです。これらの装置には、ネットワーク内のスイッチ、ルータ、およびサーバが含まれます。ファイアウォールで保護されていないデバイスまたはネットワークの外側にあるデバイスは、信頼できないソースです。ホスト ポートおよび不明な DHCP サーバは、通常信頼できない送信元として取り扱われます。

信頼できないポートの不明なネットワーク上の DHCP サーバは、*スプリアス DHCP サーバ*といいます。スプリアス DHCP サーバは、DHCP サーバをイネーブルにしてロードされた任意の機器です。例として、DHCP サーバをイネーブルにしてロードされたデスクトップ システムとラップトップ システムや、ネットワークに接続された側で DHCP 要求を受け入れるワイヤレス アクセス ポイントがあります。スプリアス DHCP サーバが検出されない場合、ネットワーク障害のトラブルシューティングが困難になります。スプリアス DHCP サーバを検出するには、応答がスイッチに返信されるように、ダミーの DHCPDISCOVER パケットをすべての DHCP サーバに送信します。

サービス プロバイダーの環境では、サービス プロバイダー ネットワークにないデバイスは、信頼できない送信元です（カスタマー スイッチなど）。ホスト ポートは、信頼できない送信元です。

スイッチでは、接続インターフェイスの信頼状態を設定することにより送信元が信頼されることを示します。

すべてのインターフェイスのデフォルトの信頼状態は、信頼できない状態になります。DHCP サーバ インターフェイスは、信頼できるインターフェイスとして設定する必要があります。ユーザのネットワーク内でデバイス（スイッチまたはルータ）に接続されている場合、他のインターフェイスも信頼できるインターフェイスとして設定できます。ホスト ポート インターフェイスは、通常、信頼できるインターフェイスとしては設定しません。

（注）　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だけ転送されるようにする必要があります。

DHCP スヌーピング バインディング データベース

DHCP スヌーピング バインディング データベースは、DHCP スヌーピング バインディング テーブルとも呼ばれます。

DHCP スヌーピング機能では、止められた DHCP メッセージから抽出された情報を使用して、データベースがダイナミックに構築され、維持されます。DHCP スヌーピングがイネーブルにされた VLAN に、ホストが関連付けられている場合、データベースには、リース IP アドレスがある信頼できない各ホストのエントリが保存されています。データベースには、信頼できるインターフェイスを介して接続するホストに関するエントリは保存されません。

DHCP スヌーピング機能では、スイッチで特定の DHCP メッセージを受信すると、データベースが更新されます。たとえば、サーバからの DHCPACK メッセージをスイッチで受信すると、この機能により、データベースにエントリが追加されます。IP アドレスのリース期限が切れると、またはホストからの DHCPRELEASE メッセージをスイッチで受信すると、この機能により、データベースのエントリが削除されます。

DHCP スヌーピング バインディング データベースの各エントリには、ホストの MAC アドレス、リース IP アドレス、リース期間、バインディング タイプ、VLAN 番号、およびホストに関連するインターフェイス情報が保存されます。

パケットの検証

スイッチでは、DHCP スヌーピングがイネーブルな VLAN の信頼できないインターフェイス上で受信した DHCP パケットが検証されます。次の条件が発生（この場合パケットは破棄される）しない限り、スイッチでは、DHCP パケットが転送されます。

- スイッチで、ネットワークまたはファイアウォール外部の DHCP サーバから、（DHCPOFFER、DHCPACK、DHCPNAK、DHCPLEASEQUERY などの）パケットを受信した場合。
- スイッチが信頼できないインターフェイスでパケットを受信し、この送信元 MAC アドレスと DHCP クライアント ハードウェア アドレスが一致しない場合。このチェックは、DHCP スヌーピングの MAC アドレス検証オプションがオンの場合だけ、実行されます。
- スイッチが DHCP スヌーピング バインディング テーブル内にエントリを持つ信頼できないホストから DHCPRELEASE または DHCPDECLINE メッセージを受信したが、バインディング テーブル内のインターフェイス情報が、このメッセージを受信したインターフェイスと一致しない場合。
- スイッチがリレー エージェントの IP アドレス（0.0.0.0 以外）を含む DHCP パケットを受信した場合。

信頼できない集約スイッチのポートに接続された信頼できるエッジ スイッチをサポートするため、信頼できないポートの機能で DHCP Option 82 をイネーブルにして、信頼できない集約スイッチのポートが Option 82 情報を含む DHCP パケットを受信するようにできます。信頼ポートとして集約スイッチに接続されているエッジ スイッチで、ポートを設定します。

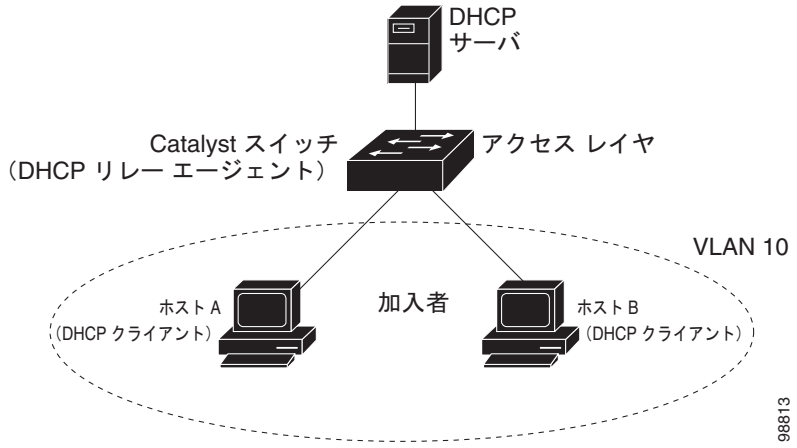
（注）　信頼できないポート機能で DHCP Option 82 がイネーブルである場合は、集約スイッチでダイナミック ARP インスペクションを使用して、信頼できない入力インターフェイスを保護します。

DHCP スヌーピングの Option 82 データ挿入

住宅地域にあるメトロポリタン イーサネット アクセス環境では、DHCP は多数の加入者に対し、IP アドレスの割り当てを一元的に管理できます。スイッチで DHCP スヌーピングの Option 82 機能をイネーブルにすると、加入者装置は MAC アドレスだけでなく、その装置をネットワークに接続するスイッチ ポートによっても識別されます。サブスクライバ LAN 上の複数のホストをアクセス スイッチの同じポートに接続できます。これらのホストは一意に識別されます。

図 78-1 に、一元的な DHCP サーバがアクセス レイヤのスイッチに接続された加入者に IP アドレスを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。各 DHCP クライアントと、これらに関連付けられた DHCP サーバは、同一の IP ネットワークまたはサブネット内に存在しません。したがって、DHCP リレー エージェントをヘルパー アドレスによって設定することで、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 メッセージを転送します。

図 78-1　メトロポリタン イーサネット ネットワークにおける DHCP リレー エージェント



スイッチで DHCP スヌーピング情報オプション Option 82 をイネーブルにすると、次のイベントがこの順序で発生します。

- ホスト（DHCP クライアント）は DHCP 要求を生成し、これをネットワーク上にブロードキャストします。
- スイッチは、この DHCP 要求を受信すると、パケットに Option 82 情報を追加します。Option 82 情報には、スイッチの MAC アドレス（リモート ID サブオプション）、およびパケットを受信したポートの識別子である vlan-mod-port（回線 ID サブオプション）が含まれます。
- IEEE 802.1X ポートベース認証がイネーブルの場合、スイッチはホストの 802.1X 認証済みユーザ ID 情報（RADIUS 属性サブオプション）もパケットに追加します。「DHCP スヌーピングを使用した 802.1X 認証」（P.83-16）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は、スイッチは DHCP パケット内にこの IP アドレスを追加します。
- 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 サーバはこのパケットを受信します。Option 82 に対応しているサーバであれば、このリモート ID または回線 ID、またはその両方を使用して、IP アドレスの割り当てやポリシーの実装を行うことができます。たとえば、単一のリモート ID または回線 ID に割り当てることのできる IP アドレスの数を制限するポリシーなどです。次に DHCP サーバは、DHCP 応答内に Option 82 フィールドをエコーします。

- スイッチによって要求が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。クライアントとサーバが同じサブネット上にある場合は、サーバはこの応答をブロードキャストします。スイッチは、リモート ID フィールドと、場合によっては回線 ID フィールドを調べ、Option 82 データが挿入済みであることを確認します。スイッチは Option 82 フィールドを削除してから、DHCP 要求を送信した DHCP クライアントに接続するスイッチ ポートにパケットを転送します。

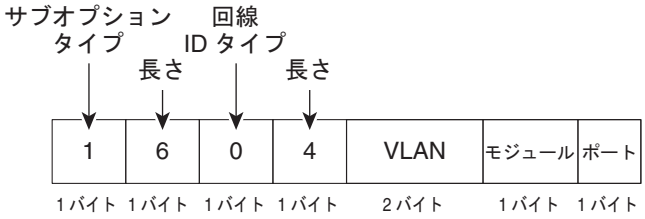
上記の一連のイベントが発生する間、図 78-2 に示す次のフィールドの値は変更されません。

- 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
  - 回線 ID タイプの長さ

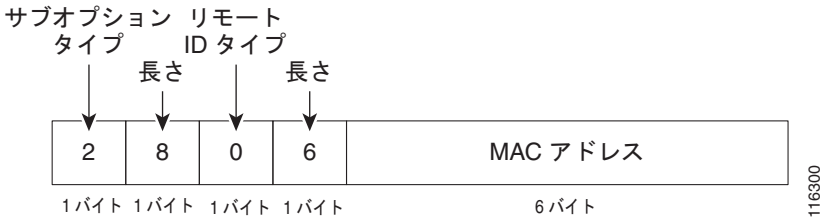
図 78-2 は、リモート ID サブオプションおよび回線 ID サブオプションのパケット形式を示します。スイッチは、DHCP スヌーピングがグローバルにイネーブルで **ip dhcp snooping information option** グローバル コンフィギュレーション コマンドが入力される場合にこれらのパケット形式を使用します。回線 ID サブオプションの場合、モジュール フィールドはモジュールのスロット番号となります。

図 78-2　　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 フォーマット



リモート ID サブオプション フレーム フォーマット



DHCP スヌーピング データベース エージェントの概要

リロード後もバインディングを維持するには、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。このエージェントを使用しないと、DHCP スヌーピングによって確立されたバインディングはリロード後に失われてしまい、同様に接続も失われます。

データベース エージェントは、設定された場所のファイルにバインディングを保存します。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。

バインディングを保持するファイルの形式は、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
```

ファイル内の各エントリには、チェックサムを示すタグが付けられます。これは、ファイルが読み取られるたびに、エントリの検証に使用されます。1 行めの <initial-checksum> エントリは、最新の書き込みに関連する各エントリを、以前の書き込みに関連する各エントリから区別します。

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
END
```

各エントリは、IP アドレス、VLAN、MAC アドレス、リース期間（16 進数単位）、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を示します。各エントリの最後に示されるチェックサムは、ファイルの冒頭から、エントリに関連付けられたすべてのバイトの合計に基づいて計算されます。各エントリは、72 バイトのデータ、スペース、およびチェックサムの順で設定されます。

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。計算されたチェックサムが保存されたチェックサムと異なる場合は、ファイルから読み取られたこのエントリは無視され、このエントリ以降の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 （リース時間が期限切れの時刻を示している場合があるため、これは可能です）。エントリ内で参照されるインターフェイスが、システム上にすでに存在しない場合、ルータ ポートである場合、または DHCP スヌーピングにおける信頼できるインターフェイスである場合も、ファイル内のエントリは無視されます。

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。より多くの変更を蓄積してから、実際の書き込みを一括して行えるように、この書き込みの実行には遅延時間を設定できます。個々の転送には、未完了の転送が中断されるまでの時間を示すタイムアウトが関連付けられます。このようなタイマーを、書き込み遅延および中断タイムアウトと呼びます。

DHCP スヌーピングのデフォルト設定

オプション	デフォルト値 / 状態
DHCP スヌーピング	ディセーブル
DHCP スヌーピング情報オプション	イネーブル
信頼できないポートの DHCP Option 82 機能	ディセーブル
DHCP スヌーピング レート制限	なし
DHCP スヌーピング信頼状態	信頼できない
DHCP スヌーピング VLAN	ディセーブル
DHCP スヌーピング スプリアス サーバ検出	ディセーブル
DHCP スヌーピング検出スプリアス間隔	30 分

DHCP スヌーピングを設定する方法

DHCP スヌーピングのグローバルなイネーブル化

（注）　このコマンドは、最後の設定手順として設定してください（または、予定されているメンテナンス期間中に DHCP 機能をイネーブルにしてください）。これは、DHCP スヌーピングをグローバルにイネーブル化すると、ポートを設定しない限り、スイッチが DHCP 要求をドロップするためです。

DHCP 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	`Router(config)# ip dhcp snooping`	DHCP スヌーピングをグローバルにイネーブル化します。
ステップ 2	`Router(config)# do show ip dhcp snooping | include Switch`	設定を確認します。

次に、DHCP スヌーピングをグローバルにイネーブル化する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip dhcp snooping
Router(config)# do show ip dhcp snooping | include Switch
Switch DHCP snooping is enabled
Router(config)#
```

（注）　DHCP スヌーピングがディセーブルで、DAI がイネーブルの場合、スイッチはすべてのホストをシャットダウンします。これは、ARP テーブルのすべての ARP エントリが、存在しない DHCP データベースと照合されるためです。DHCP スヌーピングをディセーブルにしている場合、または DHCP 以外の環境では、ARP ACL を使用して ARP パケットの許可および拒否を行います。

DHCP Option 82 データ挿入のイネーブル化

DHCP Option 82 データ挿入をイネーブル化するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# ip dhcp snooping information option`	DHCP Option 82 データ挿入をイネーブルにします。
ステップ 2	`Router(config)# do show ip dhcp snooping | include 82`	設定を確認します。

次に、DHCP Option 82 データ挿入をディセーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# no ip dhcp snooping information option
Router(config)# do show ip dhcp snooping | include 82
Insertion of option 82 is disabled
Router(config)#
```

次に、DHCP Option 82 データ挿入をイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip dhcp snooping information option
Router(config)# do show ip dhcp snooping | include 82
Insertion of option 82 is enabled
Router(config)#
```

信頼できないポートの DHCP Option 82 機能のイネーブル化

（注）　信頼できないポートの DHCP Option 82 機能をイネーブルにした場合、スイッチは信頼できないポートで受信された Option 82 情報を含む DHCP パケットをドロップしません。信頼できないデバイスが接続されている集約スイッチでは、**ip dhcp snooping information option allowed-untrusted** コマンドは入力しないでください。

信頼できないポートで Option 82 情報を含む DHCP パケットを受信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
ステップ 1	`Router(config)# ip dhcp snooping information option allow-untrusted`	（任意）Option 82 情報が含まれている DHCP の着信パケットを受け付けるよう、信頼できないポートをイネーブル化します。 デフォルト設定では無効になっています。
ステップ 2	`Router(config)# do show ip dhcp snooping`	設定を確認します。

次に、信頼できないポートの DHCP Option 82 機能をイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip dhcp snooping information option allow-untrusted
Router(config)#
```

DHCP スヌーピングの MAC アドレス検証のイネーブル化

DHCP スヌーピングの MAC アドレス検証をイネーブルにすると、信頼できないポートで受信した DHCP パケット内のクライアント ハードウェア アドレスが、送信元 MAC アドレスと一致するかどうかが検証されます。送信元 MAC アドレスは、パケットに関連付けられているレイヤ 2 フィールドで、クライアント ハードウェア アドレスは、DHCP パケットのレイヤ 3 フィールドです。

DHCP スヌーピングの MAC アドレス検証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	`Router(config)# ip dhcp snooping verify mac-address`	DHCP スヌーピングの MAC アドレス検証をイネーブルにします。
ステップ 2	`Router(config)# do show ip dhcp snooping | include hwaddr`	設定を確認します。

次に、DHCP スヌーピングの MAC アドレス検証をディセーブルにする例を示します。

```
Router(config)# no ip dhcp snooping verify mac-address
Router(config)# do show ip dhcp snooping | include hwaddr
Verification of hwaddr field is disabled
Router(config)#
```

次に、DHCP スヌーピングの MAC アドレス検証をイネーブルにする例を示します。

```
Router(config)# ip dhcp snooping verify mac-address
Router(config)# do show ip dhcp snooping | include hwaddr
Verification of hwaddr field is enabled
Router(config)#
```

VLAN 上での DHCP スヌーピングのイネーブル化

デフォルトでは、すべての VLAN で DHCP スヌーピング機能は非アクティブです。この機能は、1 つの VLAN または特定の VLAN 範囲でイネーブルにできます。

VLAN でイネーブル化されている場合、DHCP スヌーピング機能では、MFC3 の VACL テーブルで 4 つのエントリが作成されます。これらのエントリにより、PFC または DFC はこの VLAN 上のすべての DHCP メッセージを代行受信し、RP に送信します。DHCP スヌーピング機能は RP 上でソフトウェアに実装されています。

VLAN 上で DHCP スヌーピングをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# ip dhcp snooping vlan {{vlan_ID [vlan_ID]} | {vlan_range}`	VLAN または VLAN 範囲に対して DHCP スヌーピングをイネーブルにします。
ステップ 2	`Router(config)# do show ip dhcp snooping`	設定を確認します。

DHCP スヌーピングは 1 つの VLAN、または特定の VLAN 範囲に対して設定できます。

- 1 つの VLAN で設定するには、1 つの VLAN 番号を入力します。
- 特定の VLAN 範囲を設定するには、開始 VLAN 番号と終了 VLAN 番号を入力するか、または一組の VLAN 番号をダッシュ（-）でつなげて入力します。
- 複数の VLAN 番号をカンマで区切って入力することも、一組の VLAN 番号をダッシュでつなげて入力することもできます。

次に、VLAN 10 ～ 12 で DHCP スヌーピングをイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# ip dhcp snooping vlan 10 12
Router(config)#
```

次に、VLAN 10 ～ 12 で DHCP スヌーピングをイネーブルにするもう 1 つの方法を示します。

```
Router# configure terminal
Router(config)# ip dhcp snooping vlan 10-12
```

次に、VLAN 10 ～ 12 で DHCP スヌーピングをイネーブルにするもう 1 つの方法を示します。

```
Router# configure terminal
Router(config)# ip dhcp snooping vlan 10,11,12
```

次に、VLAN 10 ～ 12 および VLAN 15 で DHCP スヌーピングをイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# ip dhcp snooping vlan 10-12,15
```

次に、設定を確認する例を示します。

```
Router(config)# do show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10-12,15
DHCP snooping is operational on following VLANs:
none
DHCP snooping is configured on the following Interfaces:

Insertion of option 82 is enabled
Verification of hwaddr field is enabled
Interface                    Trusted    Rate limit (pps)
```

```
------------------------     -------     ----------------
Router#
```

レイヤ 2 LAN インターフェイスでの DHCP 信頼状態の設定

レイヤ 2 LAN インターフェイス上で DHCP 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	`Router(config)# interface {type slot/port | port-channel number}`	設定するインターフェイスを選択します。 （注）　**switchport** コマンドで設定した LAN ポート、またはレイヤ 2 ポートチャネル インターフェイスだけを選択してください。
ステップ 2	`Router(config-if)# ip dhcp snooping trust`	インターフェイスを trusted として設定します。
ステップ 3	`Router(config-if)# do show ip dhcp snooping | begin pps`	設定を確認します。

次に、ギガビット イーサネット ポート 5/12 を信頼できるポートとして設定する例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 5/12
Router(config-if)# ip dhcp snooping trust
Router(config-if)# do show ip dhcp snooping | begin pps
Interface                    Trusted     Rate limit (pps)
------------------------     -------     ----------------
GigabitEthernet5/12             yes          unlimited
Router#
```

次に、ギガビット イーサネット ポート 5/12 を信頼できないポートとして設定する例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 5/12
Router(config-if)# no ip dhcp snooping trust
Router(config-if)# do show ip dhcp snooping | begin pps
Interface                    Trusted     Rate limit (pps)
------------------------     -------     ----------------
GigabitEthernet5/12             no           unlimited
Router#
```

スプリアス DHCP サーバ検出の設定

スプリアス DHCP サーバを検出するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# ip dhcp snooping detect spurious vlan range`	指定した VLAN 範囲でスプリアス DHCP サーバの検出をイネーブルにします。
ステップ 2	`Router(config)# ip dhcp snooping detect spurious interval time`	間隔を設定します。デフォルトは 30 分です。
ステップ 3	`Router# show ip dhcp snooping detect spurious`	スプリアス DHCP サーバ検出を確認します。

次の例では、VLAN 20 ～ 25 で DHCP スプリアス サーバ検出を設定し、間隔を 50 分に設定する方法を示します。

```
Router# configure terminal
Router(config)# ip dhcp snooping detect spurious vlan 20-25
Router(config)# ip dhcp snooping detect spurious interval 50
Router# do show ip dhcp snooping detect spurious
Spurious DHCP server detection is enabled.

Detection VLAN list : 20-25
Detection interval : 50 minutes
Router#
```

レイヤ 2 LAN インターフェイスでの DHCP スヌーピング レート制限の設定

レイヤ 2 LAN インターフェイス上で DHCP スヌーピングのレート制限を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {type slot/port | port-channel number}`	設定するインターフェイスを選択します。 （注）　**switchport** コマンドで設定した LAN ポート、またはレイヤ 2 ポートチャネル インターフェイスだけを選択してください。
ステップ 2	`Router(config-if)# ip dhcp snooping limit rate rate`	DHCP パケットのレート制限を設定します。
ステップ 3	`Router(config-if)# do show ip dhcp snooping | begin pps`	設定を確認します。

レイヤ 2 LAN インターフェイス上で DHCP スヌーピングのレート制限を設定する場合、次の点に注意してください。

- 信頼できないインターフェイスでのレートは、100 pps（パケット / 秒）以下に制限することを推奨します。
- 信頼できるインターフェイスにレート制限を設定する場合は、DHCP スヌーピングをイネーブルにしている VLAN を複数収容するトランク ポートでは、レート制限を高い値に設定しなければならない場合があります。
- DHCP スヌーピングでは、レート制限を超過したポートは errdisable ステートとなります。

次に、ギガビット イーサネット ポート 5/12 を、DHCP パケットのレート制限によって 100 pps に設定する例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 5/12
Router(config-if)# ip dhcp snooping limit rate 100
Router(config-if)# do show ip dhcp snooping | begin pps
Interface                      Trusted     Rate limit (pps)
------------------------       -------     ----------------
GigabitEthernet5/12               no           100
Router#
```

DHCP スヌーピング データベース エージェント

- 「DHCP スヌーピング データベース エージェントの前提条件」（P.78-15）
- 「DHCP スヌーピング データベース エージェントの制約事項」（P.78-15）

DHCP スヌーピング データベース エージェントの前提条件

なし。

DHCP スヌーピング データベース エージェントの制約事項

- DHCP スヌーピング データベースには少なくとも 8,000 バインディングが格納されます。
- スイッチのストレージ デバイスの記憶域が消費されることを避けるため、ファイルは TFTP サーバ上に保存します。
- スイッチオーバーが発生した場合、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保存されていれば、新たにアクティブになったスーパーバイザ エンジンはこのバインディング リストを使用できます。
- ネットワークベースの URL（TFTP および FTP 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。

DHCP スヌーピング データベース エージェントのデフォルト設定

なし。

DHCP スヌーピング データベース エージェントの設定方法

DHCP スヌーピング データベース エージェントを設定するには、次の 1 つまたは複数の作業を行います。

コマンド	目的
`Router(config)# ip dhcp snooping database { _url | write-delay seconds | timeout seconds }`	データベース エージェント（またはファイル）の URL、および関連するタイムアウト値を設定します。
`Router# show ip dhcp snooping database [detail]`	データベース エージェントの現在の動作状態、および転送に関連する統計情報を表示します。
`Router# clear ip dhcp snooping database statistics`	データベース エージェントに関連する統計情報を消去します。
`Router# renew ip dhcp snooping database [validation none] [url]`	指定の URL にあるファイルからのエントリの読み取りを要求します。
`Router# ip dhcp snooping binding mac_address vlan vlan_ID ip_address interface ifname expiry lease_in_seconds`	バインディングをスヌーピング データベースに追加します。

データベース エージェントの設定例

例 1：データベース エージェントのイネーブル化

次に、指定の場所にバインディングを保存するように DHCP スヌーピング データベース エージェントを設定し、この設定内容と動作状態を表示する例を示します。

```
Router# configure terminal
Router(config)# ip dhcp snooping database tftp://10.1.1.1/directory/file
Router(config)# end
Router# 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 Succeeded Time : None
Last Failed Time : 17:14:25 UTC Sat Jul 7 2001
Last Failed Reason : Unable to access URL.

Total Attempts       :       21   Startup Failures :        0
Successful Transfers :        0   Failed Transfers :       21
Successful Reads     :        0   Failed Reads     :        0
Successful Writes    :        0   Failed Writes    :       21
Media Failures       :        0

First successful access: Read

Last ignored bindings counters :
Binding Collisions    :        0   Expired leases    :        0
Invalid interfaces    :        0   Unsupported vlans :        0
Parse failures        :        0
Last Ignored Time : None

Total ignored bindings counters:
Binding Collisions    :        0   Expired leases    :        0
Invalid interfaces    :        0   Unsupported vlans :        0
Parse failures        :        0

Router#
```

出力結果の最初の 3 行は、設定した URL、および関連するタイマー設定値を表します。次の 3 行は、動作状態のほか、書き込み遅延時間および中断タイマーが経過するまでに残された時間を表します。

出力結果にはこのほか、スタートアップ時の失敗として、スタートアップ時の読み取りまたはファイル作成の試みに失敗した回数が表示されます。

（注） TFTP サーバ上に一時ファイルを作成するには、**touch** コマンドを使用して、TFTP サーバのデーモン ディレクトリ内に作成します。一部の UNIX 実装では、ファイルには完全な読み取りおよび書き込みアクセス許可（777）を設定する必要があります。

DHCP スヌーピング バインディングは、MAC アドレスと VLAN の組み合わせに重点を置いています。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。このような状態を、*バインディング コリジョン*と呼びます。

ファイル内のエントリに示されたリース期間が、ファイルの読み取り時にすでに経過している場合は、このエントリは無効になります。期限切れリース カウンタは、このような状況によって無視されたバインディングの数を示します。無効なインターフェイス カウンタは、読み取りが行われた時点で、エ

エントリが参照するインターフェイスがシステム内にすでに存在しない場合、ルータである場合、または DHCP スヌーピングにおいて信頼できるインターフェイス（存在する場合）である場合に無視されたバインディングの数を示します。サポートされない VLAN は、エントリの示す VLAN がシステム上でサポートされない場合に無視されたエントリの数を示します。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、上記の条件が 1 つ以上該当するために無視された 1 つ以上のバインディングを持つ、個々の読み取りに対するカウンタです。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、スイッチが起動されて以降のすべての読み取りで無視されたバインディングの総数を表します。これらの 2 種類のカウンタは、**clear** コマンドによって消去されます。合計カウンタのセットは、最後に消去した時点からの無視されたバインディングの累積数と見なすことができます。

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

TFTP ファイルからエントリを手動で読み取るには、次の作業を行います。

	コマンド	目的
ステップ 1	Router# **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	Router# **renew ip dhcp snoop data** *url*	この 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	Router# **show ip dhcp snoop data**	読み取りのステータスを表示します。
ステップ 4	Router# **show ip dhcp snoop bind**	バインディングの読み取りが適切に行われたかどうかを確認します。

次に、tftp://10.1.1.1/directory/file からエントリを手動で読み取る例を示します。

```
Router# show 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 Succeeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.

Total Attempts       :        0   Startup Failures :        0
Successful Transfers :        0   Failed Transfers :        0
Successful Reads     :        0   Failed Reads     :        0
Successful Writes    :        0   Failed Writes    :        0
Media Failures       :        0
Router# 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.

Router#
00:01:29: %DHCP_SNOOPING-6-AGENT_OPERATION_SUCCEEDED: DHCP snooping database Read
succeeded.
Router# 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 Succeeded Time : 15:24:34 UTC Sun Jul 8 2001
Last Failed Time : None
Last Failed Reason : No failure recorded.

Total Attempts       :        1   Startup Failures :        0
Successful Transfers :        1   Failed Transfers :        0
Successful Reads     :        1   Failed Reads     :        0
Successful Writes    :        0   Failed Writes    :        0
Media Failures       :        0
Router#
Router# 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
00:01:00:01:00:02   1.1.1.1          49810       dhcp-snooping  512   GigabitEthernet1/1
00:01:00:01:00:04   1.1.1.1          49810       dhcp-snooping  1536  GigabitEthernet1/1
00:01:00:01:00:03   1.1.1.1          49810       dhcp-snooping  1024  GigabitEthernet1/1
00:01:00:01:00:01   1.1.1.1          49810       dhcp-snooping  1     GigabitEthernet1/1
Router# clear ip dhcp snoop bind
Router# show ip dhcp snoop bind
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
Router#
```

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	`Router# 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	`Router# 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	`Router# show ip dhcp snooping binding`	DHCP スヌーピング データベースをチェックします。

次に、DHCP スヌーピング データベースにバインディングを手動で追加する例を示します。

```
Router# show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
Router#
Router# ip dhcp snooping binding 1.1.1 vlan 1 1.1.1.1 interface gi1/1 expiry 1000

Router# show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:01:00:01:00:01   1.1.1.1          992         dhcp-snooping  1     GigabitEthernet1/1
Router#
```

DHCP スヌーピング 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ディング エントリが格納されています。このテーブルには、信頼できるポートと相互接続するホストについての情報は含まれません。相互接続する各スイッチは、それぞれ独自の 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。

```
Router# show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:02:B3:3F:3B:99   55.5.5.2         6943        dhcp-snooping  10    GigabitEthernet6/10
```

表 78-1 では、**show ip dhcp snooping binding** コマンドの出力結果における各フィールドについて説明します。

表 78-1　show ip dhcp snooping binding コマンドの出力結果

フィールド	説明
MAC Address	クライアント ハードウェアの 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 (seconds)	IP アドレスのリース期間
Type	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 バインディングか、またはスタティックに設定されたバインディングです。
VLAN	クライアント インターフェイスの VLAN 番号
Interface	DHCP クライアント ホストに接続されるインターフェイス

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

IP ソース ガード

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

IP ソース ガードの前提条件

なし。

IP ソース ガードの制約事項

IP ソース ガード機能はハードウェアでだけサポートされているため、十分なハードウェア リソースが利用できない場合 IP ソース ガードは適用されません。これらのハードウェア リソースはシステムに設定されている他のさまざまな ACL 機能と共有されています。次の制約事項が IP ソース ガードに適用されます。

- 入力レイヤ 2 ポートでだけサポートされます。
- ハードウェアでだけサポートされます。ソフトウェアで処理されるトラフィックには適用されません。
- MAC アドレスに基づくトラフィックのフィルタリングはサポートしていません。
- プライベート VLAN ではサポートされません。

IP ソース ガードの概要

IP ソース ガードの概要

IP ソース ガードは、レイヤ 2 ポートで送信元 IP アドレス フィルタリングを提供して、悪意のあるホストが正規のホストの IP アドレスを装うことで正規のホストを偽装することを防ぎます。この機能では、ダイナミックな Dynamic Host Configuration Protocol（DHCP）スヌーピングおよびスタティックな IP ソース バインディングを使用して、IP アドレスと信頼できないレイヤ 2 アクセス ポート上のホストを照合します。

まず、DHCP パケットを除く、保護済みポート上の全 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 IP アドレスを受信したあと、またスタティック IP ソース バインディングが管理者によって設定されたあと、その IP 送信元アドレスのある全トラフィックがそのクライアントから許可されます。他のホストからのトラフィックは拒否されます。このフィルタリングは、ネイバー ホストの IP アドレスを要求することで、ネットワークを攻撃するホストの能力を制限します。IP ソース ガードは、暗黙的なポート アクセス コントロール リスト（PACL）を自動的に作成するポートベースの機能です。

IP ソース ガードと VLAN ベース機能との相互作用

access-group mode コマンドを使用して、IP ソース ガードと VLAN ベース機能（VACL、Cisco IOS ACL、RACL など）との相互作用方法を指定します。

優先ポート モードでは、IP ソース ガードがインターフェイスに設定されている場合、IP ソース ガードが他の VLAN ベース機能を無効にします。IP ソース ガードがインターフェイスに設定されていない場合、他の VLAN ベース機能が入力方向に結合されてインターフェイスに適用されます。

結合モードでは、IP ソース ガードと VLAN ベース機能が入力方向に結合されて、インターフェイスに適用されます。これがデフォルトのアクセスグループ モードです。

チャネル ポート

IP ソース ガードは、レイヤ 2 ポートチャネル インターフェイスでサポートされていますが、ポート メンバではサポートされていません。IP ソース ガードがレイヤ 2 ポートチャネル インターフェイスに適用されている場合、EtherChannel 内のすべてのメンバ ポートに適用されます。

レイヤ 2 およびレイヤ 3 ポート変換

IP ソース ガード ポリシーがレイヤ 2 ポートで設定されている場合、ポートがレイヤ 3 ポートとして再設定されると、その IP ソース ガード ポリシーは機能しなくなりますが、設定にはまだ存在しています。ポートがレイヤ 2 ポートとして再設定された場合は、IP ソース ガード ポリシーが再び有効になります。

IP ソース ガードと音声 VLAN

IP ソース ガードは、音声 VLAN に属するレイヤ 2 ポートをサポートしています。音声 VLAN でアクティブになっている IP ソース ガードの場合、DHCP スヌーピングが音声 VLAN でイネーブルになっている必要があります。結合モードで、IP ソース ガード機能はアクセス VLAN 上に設定されている VLAN ACL（VACL）と Cisco IOS ACL に結合されます。

IP ソース ガードと Web ベース認証

同じインターフェイスで IP ソース ガードと Web ベース認証を設定できます（第 84 章「Web ベース認証」を参照）。IP ソース ガードと Web ベース認証が組み合わされているときは、その他の VLAN ベース機能はサポートされません。

IP ソース ガードのデフォルト設定

なし。

IP ソース ガードの設定方法

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	`Router(config)# ip dhcp snooping`	DHCP スヌーピングをグローバルにイネーブル化します。
ステップ 2	`Router(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	`Router(config)# interface interface-name`	設定するインターフェイスを選択します。

	コマンド	目的
ステップ 4	`Router(config-if)# no ip dhcp snooping trust`	インターフェイスを信頼できないと設定する場合は、**no** キーワードを使用します。
ステップ 5	`Router(config-if)# ip verify source vlan dhcp-snooping [port-security]`	IP ソース ガード、送信元 IP アドレス フィルタリングをポートでイネーブルにします。コマンド パラメータは次のとおりです。 • **vlan** の場合、インターフェイス上の特定の VLAN にだけ機能が適用されます。**dhcp-snooping** オプションの場合、DHCP スヌーピングがイネーブルであるインターフェイス上にあるすべての VLAN に機能が適用されます。 • **port-security** により MAC アドレス フィルタリングがイネーブルになります。この機能は現在サポートされていません。
ステップ 6	`Router(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 7	`Router(config)# ip source binding mac_address vlan vlan-id ip-address interface interface_name`	（任意）スタティック IP バインディングをポートに設定します。
ステップ 8	`Router(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 9	`Router# show ip verify source [interface interface_name]`	設定を確認します。

（注） スタティック IP ソース バインディングは、レイヤ 2 ポートにだけ設定可能です。**ip source binding vlan interface** コマンドをレイヤ 3 ポートに設定した場合、次のようなエラー メッセージを受信します。

```
Static IP source binding can only be configured on switch port.
```

no キーワードは、対応する IP ソース バインディング エントリを削除します。削除が正常に実行されるために、このコマンドではすべての必須パラメータが正確に一致しなければなりません。

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。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip dhcp snooping
Router(config)# ip dhcp snooping vlan 10 20
Router(config)# interface gigabitethernet 6/1
Router(config-if)# switchport mode access
Router(config-if)# switchport access vlan 10
Router(config-if)# no ip dhcp snooping trust
Router(config-if)# ip verify source vlan dhcp-snooping
Router(config-if)# end
Router# show ip verify source interface gigabitethernet 6/1
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----------
Gi6/1      ip           active       10.0.0.1                            10
Gi6/1      ip           active       deny-all                            11-20
Router#
```

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。

次の例では、優先ポート モードを使用するようインターフェイスを設定します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 6/1
Router(config-if)# access-group mode prefer port
```

次の例では、マージ モードを使用するようインターフェイスを設定します。

```
Router# configure terminal
Router(config)# interface gigabitEthernet 6/1
Router(config-if)# access-group mode merge
```

IP ソース ガード PACL 情報の表示

スイッチ上にあるすべてのインターフェイスの IP ソース ガード PACL 情報を表示するには、次の作業を行います。

コマンド	目的
Router# **show ip verify source** [**interface** *interface-name*]	スイッチ上にあるすべてのインターフェイスまたは指定のインターフェイス上にある IP ソース ガード PACL 情報を表示します。

次に、DHCP スヌーピングが VLAN 10 ～ 20 でイネーブルであり、インターフェイス fa6/1 が IP フィルタリング用に設定されていて、既存の IP アドレス バインディング 10.0.01 が VLAN 10 上にある例を示します。

```
Router# show ip verify source interface fa6/1
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
```

（注） 2 番めのエントリは、デフォルト PACL（全 IP トラフィックを拒否）が有効な IP ソース バインディングのないスヌーピング対応 VLAN のポートにインストールされていることを示しています。

次に、信頼できるポートの PACL 情報が表示されている例を示します。

```
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
fa6/2      ip           inactive-trust-port
```

次に、DHCP スヌーピングが設定されていない VLAN 内にあるポートの PACL 情報が表示されている例を示します。

```
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
fa6/3      ip           inactive-no-snooping-vlan
```

次に、IP/MAC フィルタリング用に設定された複数のバインディングのあるポートの PACL 情報が表示されている例を示します。

```
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
fa6/4      ip           active       10.0.0.2         aaaa.bbbb.cccc  10
fa6/4      ip           active       11.0.0.1         aaaa.bbbb.cccd  11
fa6/4      ip           active       deny-all         deny-all        12-20
```

次に、IP/MAC フィルタリングが設定されているもののポート セキュリティが設定されていないポートの PACL 情報が表示されている例を示します。

```
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
fa6/5      ip           active       10.0.0.3         permit-all      10
fa6/5      ip           active       deny-all         permit-all      11-20
```

（注）　ポート セキュリティがイネーブルでないため MAC アドレス フィルタは全許可を示しているので、MAC フィルタはポート /VLAN に適用されておらず、事実上ディセーブルです。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で **show ip verify source** コマンドを入力したときのエラー メッセージの例を示します。

```
Router# show ip verify source interface fa6/6
IP Source Guard is not configured on the interface fa6/6.
```

次に、IP ソース ガードがイネーブルであるスイッチの全インターフェイスを表示する例を示します。

```
Router# show ip verify source
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-trust-port
fa6/3      ip           inactive-no-snooping-vlan
fa6/4      ip           active       10.0.0.2         aaaa.bbbb.cccc  10
fa6/4      ip           active       11.0.0.1         aaaa.bbbb.cccd  11
fa6/4      ip           active       deny-all         deny-all        12-20
fa6/5      ip           active       10.0.0.3         permit-all      10
fa6/5      ip           active       deny-all         permit-all      11-20
```

IP 送信元バインディング情報の表示

スイッチ上にあるすべてのインターフェイスに設定されたすべての IP ソース バインディングを表示するには、次の作業を行います。

コマンド	目的
Router# **show ip source binding** [*ip_address*] [*mac_address*] [**dhcp-snooping** | **static**] [**vlan** *vlan_id*] [**interface** *interface_name*]	オプションの指定表示フィルタを使用した IP ソース バインディングを表示します。 **dhcp-snooping** フィルタは、DHCP スヌーピングがイネーブルであるインターフェイス上にあるすべての VLAN を表示します。

次に、スイッチ上にあるすべてのインターフェイスに設定されたすべての IP ソース バインディングを表示する例を示します。

```
Router# show ip source binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:02:B3:3F:3B:99   55.5.5.2         6522        dhcp-snooping  10    GigabitEthernet6/10
00:00:00:0A:00:0B   11.0.0.1         infinite    static         10    GigabitEthernet6/10
Router#
```

表 79-1 では、**show ip source binding** コマンドの出力結果における各フィールドについて説明します。

表 79-1　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 ハードウェアの 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 (seconds)	IP アドレスのリース期間
Type	バインディング タイプ。CLI から DHCP スヌーピングで学習されたダイナミック バインディングに設定されたスタティック 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
Interface	DHCP クライアント ホストに接続されるインターフェイス

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CHAPTER 80

ダイナミック ARP インスペクション（DAI）

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。
- PFC および DFC では、ハードウェアで DAI がサポートされます。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

DAI の前提条件

なし。

DAI の制約事項

- ハードウェア アクセラレーション DAI はデフォルトでイネーブルです。
- DAI のハードウェア アクセラレーションを実行する場合は、CoPP を設定して、RP によって処理される ARP トラフィック（たとえば、RP のブロードキャスト宛先 MAC アドレスまたは MAC アドレスを含むパケット。第 77 章「コントロール プレーン ポリシング（CoPP）」を参照してください）のレート制限を行えます。
- DAI ロギング（ACL ロギングおよび DHCP ロギングの両方を含む）には、DAI ハードウェア アクセラレーションとの互換性がありません。DAI のハードウェア アクセラレーションを実行すると、DAI ロギングはディセーブルになります。

（注）　DAI のハードウェア アクセラレーションのイネーブル状態に関係なく、acl-match matchlog キーワードにより ARP ACL を使用するように設定された DAI はソフトウェアで処理され、ロギングをサポートします。

- DAI は入力セキュリティ機能であるため、出力検査は行いません。
- DAI は、DAI をサポートしないスイッチ、またはこの機能がイネーブルにされていないスイッチに接続されているホストに対しては、効果がありません。man-in-the-middle 攻撃は 1 つのレイヤ 2 ブロードキャスト ドメインに限定されるため、DAI 検査が有効なドメインを、DAI 検査の行われないドメインから切り離します。これにより、DAI をイネーブルにしたドメイン内のホストの ARP キャッシュをセキュリティ保護できます。
- DAI では、着信 ARP 要求および ARP 応答内の IP アドレスと MAC アドレスとのバインディングを、DHCP スヌーピング バインディング データベース内のエントリに基づいて検証します。IP アドレスがダイナミックに割り当てられた ARP パケットを許可する際は、DHCP スヌーピングをイネーブルにしてください。コンフィギュレーションについては、第 78 章「Dynamic Host Configuration Protocol（DHCP）スヌーピング」を参照してください。
- DHCP スヌーピングをディセーブルにしている場合、または DHCP 以外の環境では、ARP ACL を使用してパケットの許可または拒否を行います。
- DAI は、アクセス ポート、トランク ポート、EtherChannel ポート、およびプライベート VLAN ポートでサポートされます。
- 物理ポートを EtherChannel ポート チャネルに結合するには、この物理ポートとチャネル ポートの信頼状態が一致する必要があります。ポート チャネルの信頼状態を変更すると、スイッチはそのチャネルを構成するすべての物理ポートに対し、新しい信頼状態を設定します。
- ポート チャネルの動作レートは、チャネル内のすべての物理ポートによる累積値です。たとえば、ポート チャネルの ARP レート制限を 400 pps に設定した場合、このチャネルに結合されたすべてのインターフェイスは、合計で 400 pps を受信します。EtherChannel ポートで受信される ARP パケットのレートは、すべてのチャネル メンバからの受信パケット レートの合計となります。EtherChannel ポートのレート制限は、各チャネル ポート メンバが受信する ARP パケットのレートを確認してから設定してください。

  物理ポートで受信されるパケットのレートは、物理ポートの設定ではなく、ポート チャネルの設定に照合して検査されます。ポート チャネルのレート制限設定は、物理ポートの設定には依存しません。

  EtherChannel が、設定したレートより多くの ARP パケットを受信すると、このチャネル（すべての物理ポートを含む）は errdisable ステートとなります。
- 着信トランク ポートでは、ARP パケットを必ずレート制限してください。トランク ポートは、各ポートのアグリゲーションを考慮し、DAI をイネーブルにした複数の VLAN でパケットを処理できるように、高い値に設定します。また、**ip arp inspection limit none** 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、レートを無制限として設定できます。1 つの VLAN に高いレート制限値を設定すると、ソフトウェアによってこのポートが errdisable ステートにされた場合に、他の VLAN への DoS 攻撃を招く可能性があります。

DAI の概要

ARP について

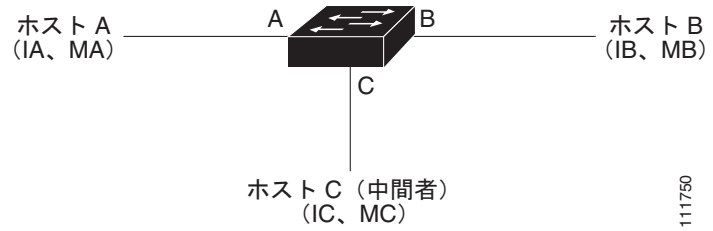
ARP では、IP アドレスを MAC アドレスにマッピングすることで、レイヤ 2 ブロードキャスト ドメイン内の IP 通信を実現します。たとえば、ホスト B がホスト A に情報を送信しようとする場合、ホスト B の ARP キャッシュにホスト A の MAC アドレスが存在しないとします。ホスト B はホスト A の IP アドレスに関連付けられた MAC アドレスを取得するため、このブロードキャスト ドメイン内の全ホストに対してブロードキャスト メッセージを送信します。ブロードキャスト ドメイン内の全ホストはこの ARP 要求を受信し、これに対してホスト A は自身の MAC アドレスで応答します。

ARP スプーフィング攻撃

ARP スプーフィング攻撃と ARP キャッシュ ポイズニングは、ARP 要求を受信していないホストでも応答できる ARP の機能性を利用して行う攻撃です。攻撃が開始されると、攻撃を受けたデバイスからのすべてのトラフィックは、攻撃者のコンピュータを経由してルータ、スイッチ、またはホストに送信されるようになります。

ARP スプーフィング攻撃は、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（汚染）し、このサブネット上の他のホスト宛てのトラフィックを代行受信することで、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することができます。図 80-1 は、ARP キャッシュ ポイズニングの例を示します。

図 80-1　ARP キャッシュ ポイズニング



ホスト A、B、および C は、インターフェイス A、B、および C 上にあるスイッチに接続されています。これらはすべて同一のサブネット上にあります。カッコ内は、各ホストの IP および MAC アドレスを示します。たとえば、ホスト A は IP アドレス IA および MAC アドレス MA を使用します。ホスト A が IP レイヤ上でホスト B と通信する場合は、ホスト A は IP アドレス IB に関連付けられた MAC アドレスを尋ねる ARP 要求をブロードキャストします。スイッチとホスト B は、この ARP 要求を受信すると、IP アドレスが IA で、MAC アドレスが MA のホストに対する ARP バインディングを ARP キャッシュに読み込みます。たとえば、IP アドレス IA は、MAC アドレス MA にバインドされています。ホスト B が応答すると、スイッチ、およびホスト A は、IP アドレスが IB で、MAC アドレスが MB のホストに対するバインディングを ARP に読み込みます。

ホスト C は、IP アドレス IA（または IB）および MAC アドレス MC を持つホストのバインディングによって偽装した ARP 応答をブロードキャストすることで、ホスト A、およびホスト B のスイッチの ARP キャッシュをポイズニングできます。ARP キャッシュがポイズニングされたホストは、IA または IB 宛てのトラフィックに、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、ホスト C がこのトラフィックを代行受信することになります。ホスト C は IA および IB に関連付けられた本物の 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とで、代行受信したトラフィックをこれらのホストに転送できます。ホスト C は、ホスト A からホスト B へのトラフィック ストリーム内に自身を割り込ませています。これは、*man-in-the-middle* 攻撃の典型的なトポロジーです。

DAI および ARP スプーフィング攻撃

PFC およびすべての DFC では、DAI がハードウェアでサポートされます。DAI は、ネットワーク内の ARP パケットを検証するセキュリティ機能です。DAI は、IP アドレスと MAC アドレスとの無効なバインディングを持つ ARP パケットを代行受信、記録、および廃棄します。この機能により、一部の man-in-the-middle 攻撃からネットワークを保護できます。

DAI を使用することで、有効な ARP 要求および応答だけがリレーされるようになります。スイッチが実行する機能は次のとおりです。

- 信頼できないポートを経由したすべての ARP 要求および ARP 応答を代行受信します。
- 代行受信した各パケットが、IP アドレスと MAC アドレスの有効なバインディングを持つことを確認してから、ローカル ARP キャッシュを更新するか、または適切な宛先にパケットを転送します。
- 無効な ARP パケットはドロップします。

DAI は信頼できるデータベースに保存された IP アドレスと MAC アドレスとの有効なバインディングに基づき、ARP パケットの有効性を判断します。このデータベースを、Dynamic Host Configuration Protocol（DHCP）スヌーピング バインディング データベースと呼びます。このデータベースは、VLAN およびスイッチ上で DHCP スヌーピングがイネーブルになっている場合に、DHCP スヌーピングにより構築されます。信頼できるインターフェイスで ARP パケットが受信されると、スイッチは何もチェックせずに、このパケットを転送します。信頼できないインターフェイスでは、スイッチはこのパケットが有効である場合だけ、このパケットを転送します。

DAI では、スタティックに設定した IP アドレスを持つホストに対し、ユーザ設定の ARP アクセス コントロール リスト（ACL）に照合することで ARP パケットを検証できます（「DAI フィルタリングのための ARP ACL の適用」（P.80-10）を参照）。スイッチは、ドロップされたパケットを記録します（「ドロップ パケットのロギング」（P.80-6）を参照）。

DAI では、パケット内の IP アドレスが無効な場合に ARP パケットをドロップするのか、ARP パケット本体の 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のかを設定できます（「追加検証のイネーブル化」（P.80-12）を参照）。

インターフェイスの信頼状態とネットワーク セキュリティ

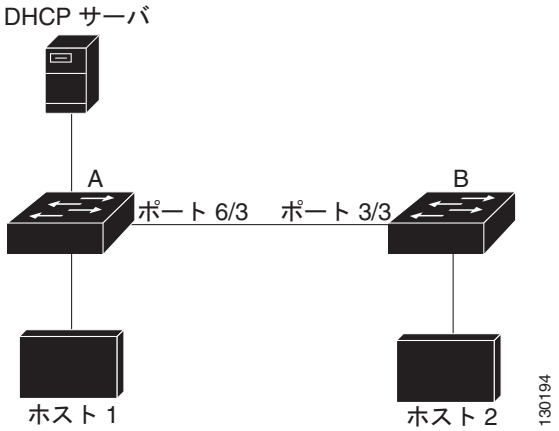
DAI は、スイッチの各インターフェイスに信頼状態を関連付けます。信頼できるインターフェイス上で受信されたパケットは、DAI のすべての有効性検査をバイパスしますが、信頼できないインターフェイス上で受信されたパケットには、DAI の有効性検査が行われます。

一般的なネットワーク構成では、ホスト ポートに接続されているスイッチ ポートすべてを信頼できないものに設定し、スイッチに接続されているスイッチ ポートすべてを信頼できるものに設定します。この構成では、指定されたスイッチからネットワークに入ってくる ARP パケットはすべて、セキュリティ チェックをバイパスします。VLAN 内、またはネットワーク内のその他の場所では、他の検査を実行する必要はありません。信頼状態を設定するには、**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。

注意　信頼状態の設定は、慎重に行ってください。信頼すべきインターフェイスを信頼できないインターフェイスとして設定すると、接続が失われる場合があります。

図 80-2 では、スイッチ A とスイッチ B の両方が VLAN に対して DAI を実行しているとします。この VLAN には、ホスト 1 とホスト 2 が含まれています。ホスト 1 とホスト 2 が、スイッチ A に接続している DHCP サーバから IP アドレスを取得している場合、スイッチ A だけが、ホスト 1 の IP/MAC アドレスをバインディングします。したがって、スイッチ A とスイッチ B の間のインターフェイスが信頼できない場合、ホスト 1 からの ARP パケットは、スイッチ B によりドロップされます。こうして、ホスト 1 とホスト 2 の間の接続が失われます。

図 80-2　DAI をイネーブルにした VLAN での ARP パケット検証



実際には信頼できないインターフェイスを信頼できるインターフェイスとして設定すると、ネットワーク内にセキュリティ ホールが生じます。スイッチ A で DAI が実行されていない場合、ホスト 1 はスイッチ B の ARP キャッシュを簡単にポイズニングできます（および、これらのスイッチの間のリンクが信頼できるものとして設定されている場合はホスト 2）。この状況は、スイッチ B が DAI を実行している場合でも起こりえます。

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場所にあるホストが、DAI を実行するスイッチに接続されたホストのキャッシュをポイズニングする可能性は防止できません。

VLAN のスイッチの一部が DAI を実行し、残りのスイッチは実行していない場合、このようなスイッチに接続しているインターフェイスは信頼できないものとして設定します。ただし、DAI が設定されていないスイッチからのパケットのバインディングを検証するには、DAI を実行するスイッチ上で ARP ACL を設定します。こうしたバインディングを判断できない場合は、レイヤ 3 において、DAI を実行するスイッチを DAI を実行しないスイッチから切り離します。設定については、「1 台のスイッチが DAI をサポートする場合」（P.80-22）を参照してください。

（注）　DHCP サーバとネットワークの設定によっては、VLAN 上のすべてのスイッチで指定された ARP パケットを検証できない可能性があります。

ARP パケットのレート制限

スイッチは、DAI 有効性検査を実行することで着信 ARP パケットをレート制限して、サービス拒否攻撃を防止します。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 パケット / 秒（pps）です。信頼できるインターフェイスは、レート制限されません。この設定を変更するには、**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。

着信 ARP パケットのレートが設定された制限を超えると、スイッチはポートを errdisable ステートにします。ユーザが介入するまで、ポートはこの状態を維持します。**errdisable recovery** 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、errdisable ステートの回復をイネーブルにできます。これによって、ポートは指定のタイムアウト時間が経過すると、この状態から自動的に回復するようになります。

設定については、「ARP パケットのレート制限の設定」（P.80-11）を参照してください。

ARP ACL および DHCP スヌーピング エントリの相対的なプライオリティ

DAI では DHCP スヌーピング バインディング データベースを使用して、IP アドレスと MAC アドレスとの有効なバインディングのリストを維持します。

DHCP スヌーピング バインディング データベース内のエントリより、ARP ACL の方が優先されます。スイッチが ACL を使用するのは、ACL が **ip arp inspection filter** グローバル コンフィギュレーション コマンドを使用して作成されている場合だけです。スイッチは、まず、ARP パケットをユーザ設定の ARP ACL と比較します。DHCP スヌーピングによりデータが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していても、ARP ACL が ARP パケットを拒否する場合、スイッチもこのパケットを拒否します。

ドロップ 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記録され、その割合に応じて、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、スイッチにより、ログ バッファからこのエントリが消去されます。各ログ エントリには、受信側の VLAN、ポート番号、送信元 IP アドレスおよび宛先 IP アドレス、送信元 MAC アドレスおよび宛先 MAC アドレスといったフロー情報が記録されます。

ip arp inspection log-buffer グローバル コンフィギュレーション コマンドを使用して、バッファ内のエントリ数や、システム メッセージ生成までの指定のインターバルに必要とされるエントリ数を設定します。記録されるパケットの種類を指定するには、**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。設定については、「DAI ログ機能の設定」（P.80-14）を参照してください。

DAI のデフォルト設定

機能	デフォルト設定
DAI	すべての VLAN でディセーブル。
インターフェイスの信頼状態	すべてのインターフェイスは untrusted。
着信 ARP パケットのレート制限	信頼できないインターフェイスでは、レートを 15 pps に制限。ネットワークがレイヤ 2 スイッチド ネットワークであり、ホストが 1 秒間に 15 の新規ホストに接続することが前提です。 信頼できるすべてのインターフェイスでは、レート制限は行われません。 バースト インターバルは 1 秒です。
非 DHCP 環境に対する ARP ACL	ARP ACL は定義されません。
有効性検査	検査は実行されません。
ログ バッファ	DAI をイネーブルにした場合は、拒否またはドロップされたすべての ARP パケットが記録されます。 ログ内のエントリ数は 32 です。 システム メッセージ数は、毎秒 5 つに制限されます。 ロギング レート インターバルは、1 秒です。
VLAN 単位のロギング	拒否またはドロップされたすべての ARP パケットが記録されます。

DAI の設定方法

VLAN での DAI のイネーブル化

VLAN で DAI 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	Router# **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	Router(config)# **ip arp inspection vlan** {*vlan_ID* | *vlan_range*}	VLAN で DAI をイネーブルにします。
ステップ 3	Router(config-if)# **do show ip arp inspection vlan** {*vlan_ID* | *vlan_range*} **| begin Vlan**	設定を確認します。

DAI は 1 つの VLAN、または特定の VLAN 範囲でイネーブルにできます。

- 1 つの VLAN でイネーブルにするには、1 つの VLAN 番号を入力します。
- 特定の VLAN 範囲でイネーブルにするには、一組の VLAN 番号をダッシュ（-）でつなげて入力します。
- 複数の VLAN 番号をカンマで区切って入力することも、一組の VLAN 番号をダッシュでつなげて入力することもできます。

次に、VLAN 10 ～ 12 で DAI をイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# ip arp inspection vlan 10-12
```

次に、VLAN 10 ～ 12 で DAI をイネーブルにするもう 1 つの方法を示します。

```
Router# configure terminal
Router(config)# ip arp inspection vlan 10,11,12
```

次に、VLAN 10 ～ 12、および VLAN 15 で DAI をイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# ip arp inspection vlan 10-12,15
```

次に、設定を確認する例を示します。

```
Router(config)# do show ip arp inspection vlan 10-12,15 | begin Vlan
Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
   10     Enabled          Inactive
   11     Enabled          Inactive
   12     Enabled          Inactive
   15     Enabled          Inactive

 Vlan     ACL Logging      DHCP Logging
 ----     -----------      ------------
   10     Deny             Deny
   11     Deny             Deny
   12     Deny             Deny
   15     Deny             Deny
```

DAI のハードウェア アクセラレーションの設定

DAI がイネーブルの場合、デフォルトで DAI アクセラレーションもイネーブルになります。DAI のハードウェア アクセラレーションのステ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	`Router# 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	`Router(config)# ip arp inspection accelerate`	DAI のハードウェア アクセラレーションをイネーブルにします。
	`Router(config)# no ip arp inspection accelerate`	DAI のハードウェア アクセラレーションをディセーブルにします。
ステップ 3	`Router(config)# do show ip arp inspection | include Acceleration`	設定を確認します。

次に、DAI のハードウェア アクセラレーションを再度イネーブルにする例を示します。

```
Router# configure terminal
Router(config)# ip arp inspection accelerate
Router(config)# do show ip arp inspection | include Acceleration
Hardware Acceleration Mode : Enabled
Router(config)#
```

DAI インターフェイスの信頼状態の設定

スイッチは、信頼できるインターフェイス上で受信した ARP パケットを転送しますが、検査は行いません。

信頼できないインターフェイスでは、スイッチはすべての ARP 要求と応答を代行受信します。ルータは、代行受信した各パケットが、IP アドレスと MAC アドレスとの有効なバインディングを持つことを確認してから、ローカル キャッシュを更新するか、適切な宛先にパケットを転送します。スイッチは、無効なパケットをドロップし、**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ログ バッファに記録します。詳細については、「DAI ログ機能の設定」（P.80-14）を参照してください。

DAI 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	`Router# 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	`Router(config)# interface {`*type slot/port* `| port-channel` *number*`}`	別のスイッチに接続されてい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	`Router(config-if)# ip arp inspection trust`	スイッチ間の接続を trusted に設定します。
ステップ 4	`Router(config-if)# do show ip arp inspection interfaces`	DAI の設定を確認します。

次に、ギガビット イーサネット ポート 5/12 を信頼できるポートとして設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
Router(config)# interface gigabitethernet 5/12
Router(config-if)# ip arp inspection trust
Router(config-if)# do show ip arp inspection interfaces | include Int|--|5/12
Interface        Trust State     Rate (pps)    Burst Interval
 ---------------  -----------     ----------    --------------
 Gi5/12           Trusted              None               N/A
```

DAI フィルタリングのための ARP ACL の適用

ARP 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	`Router# 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	`Router# ip arp inspection filter` *arp_acl_name* **vlan** {*vlan_ID* | *vlan_range*} [**static**]	ARP ACL を VLAN に適用します。
ステップ 3	`Router(config)# do show ip arp inspection vlan` {*vlan_ID* | *vlan_range*}	入力を確認します。

- **arp access-list** コマンドの詳細については、コマンド リファレンスを参照してください。
- *vlan_range* には、1 つの VLAN、または特定の VLAN 範囲を指定できます。
  - 1 つの VLAN を指定するには、1 つの VLAN 番号を入力します。
  - 特定の VLAN 範囲で指定にするには、一組の VLAN 番号をダッシュ（-）でつなげて入力します。
  - 複数の VLAN 番号をカンマで区切って入力することも、一組の VLAN 番号をダッシュでつなげて入力することもできます。
- （任意）**static** を指定すると、ARP ACL 内の暗黙的な拒否が明示的な拒否と見なされ、それ以前に指定された ACL 句に一致しないパケットはドロップされます。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 内にはパケットを拒否する明示的な拒否が存在しないことになります。この場合は、ACL 句に一致しないパケットを許可するか拒否するかは、DHCP バインディングによって決定されます。
- IP アドレスと MAC アドレスとのバインディングしか持たない ARP パケットは、ACL に照合されます。パケットは、アクセス リストで許可された場合だけに許可されます。

次に、example_arp_acl という名前の ARP ACL を、VLAN 10 ～ 12、および VLAN 15 に適用する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip arp inspection filter example_arp_acl vlan 10-12,15
Router(config)# do show ip arp inspection vlan 10-12,15 | begin Vlan
 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
   10     Enabled          Inactive    example_arp_acl    No
   11     Enabled          Inactive    example_arp_acl    No
   12     Enabled          Inactive    example_arp_acl    No
   15     Enabled          Inactive    example_arp_acl    No
Vlan     ACL Logging      DHCP Logging
 ----     -----------      ------------
   10     Deny             Deny
   11     Deny             Deny
   12     Deny             Deny
```

```
15      Deny              Deny
```

ARP パケットのレート制限の設定

（注）　DAI のハードウェア アクセラレーションを実行する場合は、CoPP を設定して、RP によって処理される ARP トラフィック（たとえば、RP のブロードキャスト宛先 MAC アドレスまたは MAC アドレスを含むパケット。第 77 章「コントロール プレーン ポリシング（CoPP）」を参照してください）のレート制限を行えます。

アクセラレーションを実行しない DAI をイネーブルにすると、スイッチは ARP パケットの有効性検査を実行します。これにより、スイッチは ARP パケットのサービス拒否攻撃を受けやすくなります。ARP パケットをレート制限することで、ARP パケットの DoS 攻撃を防止できます。

ARP パケットのレート制限をポートに設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# 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	`Router(config)# interface {type slot/port | 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 3	`Router(config-if)# ip arp inspection limit {rate pps [burst interval seconds] | none}`	（任意）ARP パケットのレート制限を設定します。
ステップ 4	`Router(config-if)# do show ip arp inspection interfaces`	設定を確認します。

- デフォルト 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。
- **rate** *pps* には、1 秒あたりに処理される着信パケット数の上限を指定します。有効な範囲は 0 ～ 2048 pps です。
- **rate none** キーワードは、処理できる着信 ARP パケットのレートに上限がないことを指定します。
- （任意）**burst interval** *seconds*（デフォルトは 1）には、インターフェイスをモニタして高レートの ARP パケットの有無を確認するための、連続するインターバルを秒単位で指定します。有効な範囲は 1 ～ 15 です。
- 着信 ARP パケットのレートが設定された制限を超えると、スイッチはポートを errdisable ステートにします。ポートは、errdisable ステートの回復がイネーブルにされるまで、errdisable ステートを維持します。errdisable ステートの回復をイネーブルにすると、指定のタイムアウト時間が経過した時点で、ポートは errdisable ステートから回復します。
- インターフェイスのレート制限値を設定しない限り、インターフェイスの信頼状態を変更すると、このレート制限値も、設定した信頼状態に対応するデフォルト値に変更されます。レート制限値を設定すると、信頼状態を変更した場合でも、インターフェイスはこのレート制限値を維持します。**no ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを入力すると、インターフェイスはデフォルトのレート制限値に戻ります。
- トランク ポートおよび EtherChannel ポートで受信される ARP パケットのレート制限を設定するうえでの注意事項については、「DAI の制約事項」（P.80-2）を参照してください。

次に、ギガビット イーサネット ポート 5/14 に ARP パケットのレート制限を設定する例を示します。

```
Router# configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 5/14
Router(config-if)# ip arp inspection limit rate 20 burst interval 2
Router(config-if)# do show ip arp inspection interfaces | include Int|--|5/14
 Interface        Trust State     Rate (pps)     Burst Interval
 ---------------  -----------     ----------     --------------
 Gi5/14           Untrusted               20                  2
```

DAI errdisable ステート回復のイネーブル化

DAI の errdisable ステート回復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	`Router# 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	`Router(config)# errdisable recovery cause arp-inspection`	（任意）DAI の errdisable ステート回復をイネーブルにします。
ステップ 3	`Router(config)# do show errdisable recovery | include Reason|---|arp-`	設定を確認します。

次に、DAI の errdisable ステート回復をイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# errdisable recovery cause arp-inspection
Router(config)# do show errdisable recovery | include Reason|---|arp-
ErrDisable Reason    Timer Status
-----------------    --------------
arp-inspection       Enabled
```

追加検証のイネーブル化

DAI は、IP アドレスと MAC アドレスとの無効なバインディングを持つ ARP パケットを代行受信、記録、および廃棄します。宛先 MAC アドレス、送信元および宛先 IP アドレス、送信元 MAC アドレスに対し、追加検証をイネーブルにすることができます。

追加検証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	`Router# 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	`Router(config)# ip arp inspection validate {[dst-mac] [ip] [src-mac]}`	（任意）追加検証をイネーブルにします。
ステップ 3	`Router(config)# do show ip arp inspection | include abled$`	設定を確認します。

追加検証では、以下を実行します。

- **dst-mac** : イーサネット ヘッダー内の宛先 MAC アドレスを、ARP 本体のターゲット MAC アドレスと比較して検査します。この検査は、ARP 応答に対して実行されます。イネーブルにすると、異なる MAC アドレスを持つパケットは無効パケットとして分類され、ドロップされます。
- **ip** : ARP 本体を検査し、無効かつ予期されない IP アドレスの有無を確認します。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。送信元 IP アドレスはすべての ARP 要求および ARP 応答内で検査され、宛先 IP アドレスは ARP 応答内だけで検査されます。
- **src-mac** : イーサネット ヘッダー内の送信元 MAC アドレスを、ARP 本体の送信元 MAC アドレスと比較して検査します。この検査は、ARP 要求および ARP 応答の両方に対して実行されます。イネーブルにすると、異なる MAC アドレスを持つパケットは無効パケットとして分類され、ドロップされます。

追加検証をイネーブルにする場合、次の点に注意してください。

- 少なくとも 1 つのキーワードを指定する必要があります。
- 各 **ip arp inspection validate** コマンドは、それまでに指定したコマンドの設定を上書きします。**ip arp inspection validate** コマンドによって **src -mac** および **dst-mac** 検証をイネーブルにし、2 つめの **ip arp inspection validate** コマンドで IP 検証だけをイネーブルにした場合は、2 つめのコマンドの結果によって **src-mac** および **dst-mac** 検証がディセーブルになります。

次に、**src-mac** 追加検証をイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip arp inspection validate src-mac
Router(config)# do show ip arp inspection | include abled$
Source Mac Validation      : Enabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
```

次に、**dst-mac** 追加検証をイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip arp inspection validate dst-mac
Router(config)# do show ip arp inspection | include abled$
Source Mac Validation      : Disabled
Destination Mac Validation : Enabled
IP Address Validation      : Disabled
```

次に、**ip** 追加検証をイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip arp inspection validate ip
Router(config)# do show ip arp inspection | include abled$
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Enabled
```

次に、**src-mac** および **dst-mac** 追加検証をイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip arp inspection validate src-mac dst-mac
Router(config)# do show ip arp inspection | include abled$
Source Mac Validation      : Enabled
Destination Mac Validation : Enabled
IP Address Validation      : Disabled
```

次に、**src-mac**、**dst-mac**、および **ip** 追加検証をイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip arp inspection validate src-mac dst-mac ip
Router(config)# do show ip arp inspection | include abled$
Source Mac Validation      : Enabled
Destination Mac Validation : Enabled
IP Address Validation      : Enabled
```

DAI ログ機能の設定

DAI ログ機能の概要

DAI はパケットをドロップすると、ログ バッファ内にエントリを作成して、レート制限に基づくシステム メッセージを生成します。メッセージが生成されたあとは、DAI はこのエントリをログ バッファから消去します。各ログ エントリには、受信側の VLAN、ポート番号、送信元 IP アドレスおよび宛先 IP アドレス、送信元 MAC アドレスおよび宛先 MAC アドレスといったフロー情報が記録されます。

1 つのログ バッファ エントリで複数のパケットを表すことができます。たとえば、同じ ARP パラメータを持つ同一 VLAN 上で、1 つのインターフェイスが多数のパケットを受信した場合は、DAI のログ バッファではこれらのパケットが 1 つのエントリとして結合され、このエントリに対して 1 つのシステム メッセージが生成されます。

ログ バッファでオーバーフローが生じた場合は、1 つのログ イベントがログ バッファ内に収まらなかったことを意味し、**show ip arp inspection log** 特権 EXEC コマンドによる出力が影響を受けます。この場合は、パケット数と時間だけが表示され、あとはデータの代わりに 2 つのダッシュ（--）が表示されます。このエントリに対しては、その他の統計情報は表示されません。このようなエントリが表示された場合は、ログ バッファ内のエントリ数を増やすか、またはログ レートを高くしてください。

DAI ロギングの制約事項

DAI ロギング（ACL ロギングおよび DHCP ロギングの両方を含む）には、DAI ハードウェア アクセラレーションとの互換性がありません。DAI のハードウェア アクセラレーションを実行すると、DAI ロギングはディセーブルになります。DAI のハードウェア アクセラレーションのイネーブル状態に関係なく、acl-match matchlog キーワードにより ARP ACL を使用するように設定された DAI はソフトウェアで処理され、ロギングをサポートします。

DAI のログ バッファ サイズの設定

DAI のログ バッファ 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	Router# **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	Router(config)# **ip arp inspection log-buffer entries** *number*	DAI のログ バッファ サイズを設定します（有効範囲は 0 ～ 1024）。
ステップ 3	Router(config)# **do show ip arp inspection log | include Size**	設定を確認します。

次に、DAI ログ バッファを 64 メッセージに設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip arp inspection log-buffer entries 64
Router(config)# do show ip arp inspection log | include Size
Total Log Buffer Size : 64
```

DAI のログ システム メッセージの設定

DAI のログ システム メッセージを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router# **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	Router(config)# **ip arp inspection log-buffer logs** *number_of_messages* **interval** *length_in_seconds*	DAI のログ バッファを設定します。
ステップ 3	Router(config)# **do show ip arp inspection log**	設定を確認します。

- **logs** *number_of_messages* の有効範囲は 0 ～ 1024 です（デフォルトは 5）。0 は、エントリはログ バッファ内に入力されますが、システム メッセージが生成されないことを意味します。
- **interval** *length_in_seconds* の有効範囲は 0 ～ 86400 秒（1 日）です（デフォルトは 1）。0 は、システム メッセージがただちに生成されることを意味します。この場合、ログ バッファは常に空となります。インターバル値を 0 に設定すると、ログ値 0 は上書きされます。
- システム メッセージは、*length_in_seconds* あたり *number_of_messages* のレートで送信されます。

次に、2 秒おきに 12 メッセージが送信されるように DAI のログ機能を設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip arp inspection log-buffer logs 12 interval 2
Router(config)# do show ip arp inspection log | include Syslog
Syslog rate : 12 entries per 2 seconds.
```

次に、60 秒おきに 20 メッセージが送信されるように DAI のログ機能を設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip arp inspection log-buffer logs 20 interval 60
Router(config)# do show ip arp inspection log | include Syslog
Syslog rate : 20 entries per 60 seconds.
```

DAI のログ フィルタリングの設定

DAI のログ 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
ステップ 1	`Router# 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	`Router(config)# ip arp inspection vlan` *vlan_range* `logging {acl-match {matchlog | none} | dhcp-bindings {all | none | permit}}`	各 VLAN に対するログ フィルタリングを設定します。
ステップ 3	`Router(config)# do show running-config | include ip arp inspection vlan` *vlan_range*	設定を確認します。

- デフォルトでは、拒否されたすべてのパケットが記録されます。
- *vlan_range* には、1 つの VLAN、または特定の VLAN 範囲を指定できます。
  - 1 つの VLAN を指定するには、1 つの VLAN 番号を入力します。
  - 特定の VLAN 範囲で指定にするには、一組の VLAN 番号をダッシュ（-）でつなげて入力します。
  - 複数の VLAN 番号をカンマで区切って入力することも、一組の VLAN 番号をダッシュでつなげて入力することもできます。
- **acl-match matchlog** : DAI ACL の設定に基づきパケットを記録します。このコマンドに **matchlog** キーワードを指定して、さらに **permit** または **deny** ARP アクセス リスト コンフィギュレーション コマンドに **log** キーワードを指定すると、ACL によって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** : ACL と一致したパケットを記録しません。
- **dhcp-bindings all** : DHCP バインディングと一致したすべてのパケットが記録されます。
- **dhcp-bindings none** : DHCP バインディングと一致したパケットは記録されません。
- **dhcp-bindings permit** : DHCP バインディングによって許可されたパケットが記録されます。

次に、VLAN 100 の DAI ログ フィルタリングを、ACL と一致したパケットを記録しないように設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip arp inspection vlan 100 logging acl-match none
Router(config)# do show running-config | include ip arp inspection vlan 100
ip arp inspection vlan 100 logging acl-match none
```

DAI 情報の表示

コマンド	説明
show arp access-list [*acl_name*]	ARP ACL についての詳細情報を表示します。
show ip arp inspection interfaces [*interface_id*]	指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対して、ARP パケットの信頼状態およびレート制限を表示します。

コマンド	説明
show ip arp inspection vlan *vlan_range*	指定の VLAN に対し、DAI の設定内容および動作状態を表示します。VLAN を指定しない場合、または VLAN を範囲で指定した場合は、DAI がイネーブル（アクティブ）にされている VLAN だけの情報が表示されます。
show ip arp inspection statistics [**vlan** *vlan_range*]	指定の VLAN において、転送されたパケット、ドロップされたパケット、MAC 検証に失敗したパケット、IP 検証に失敗したパケット、ACL によって許可および拒否されたパケット、DHCP によって許可および拒否されたパケットの統計情報を表示します。VLAN を指定しない場合、または VLAN を範囲で指定した場合は、DAI がイネーブル（アクティブ）にされている VLAN だけの情報が表示されます。 スイッチは信頼された DAI ポート上の各 ARP 要求および応答パケットの転送済みパケット数を増加させます。スイッチは、送信元 MAC、宛先 MAC、または IP 検証チェックによって拒否された各パケットの ACL 許可済みまたは DHCP 許可済みパケット数を増加させ、適切な失敗数を増加させます。
show ip arp inspection log	DAI ログ バッファの設定および内容を表示します。

DAI の設定例

2 台のスイッチが DAI をサポートする場合

概要

2 つのスイッチがこの機能をサポートする場合の DAI の設定手順を示します。図 80-2（P.80-5）に示すとおり、ホスト 1 はスイッチ A に、ホスト 2 はスイッチ B に接続されています。両方のスイッチは、これらのホストが置かれている VLAN 1 上で DAI を実行しています。DHCP サーバはスイッチ A に接続されています。両方のホストは、同一の DHCP サーバから IP アドレスを取得します。スイッチ A はホスト 1 およびホスト 2 に対するバインディングを、スイッチ B はホスト 2 に対するバインディングを持ちます。スイッチ A のギガビット イーサネット ポート 6/3 は、スイッチ B のギガビット イーサネット ポート 3/3 に接続されます。

（注）
- DAI では、着信 ARP 要求および ARP 応答内の IP アドレスと MAC アドレスとのバインディングを、DHCP スヌーピング バインディング データベース内のエントリに基づいて検証します。IP アドレスがダイナミックに割り当てられた ARP パケットを許可する際は、DHCP スヌーピングをイネーブルにしてください。コンフィギュレーションについては、第 78 章「Dynamic Host Configuration Protocol（DHCP）スヌーピング」を参照してください。

- この構成は、DHCP サーバがスイッチ A から別の場所に移動されると機能しません。
- この構成によってセキュリティが損なわれないようにするには、スイッチ A のギガビット イーサネット ポート 6/3、およびスイッチ B のギガビット イーサネット ポート 3/3 を、信頼できるポートとして設定します。

スイッチ A の設定

スイッチ A において DAI をイネーブルにし、ギガビット イーサネット ポート 6/3 を信頼できるポートとして設定するには、次の作業を行います。

ステップ 1　スイッチ A およびスイッチ B 間の接続を確認します。

```
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          Fas 6/3            177         R S I     WS-C6506  Fas 3/3
SwitchA#
```

ステップ 2　VLAN 1 で DAI をイネーブルにし、設定を確認します。

```
SwitchA# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)# ip arp inspection vlan 1
SwitchA(config)# end
SwitchA# show ip arp inspection vlan 1

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
    1     Enabled          Active

 Vlan     ACL Logging      DHCP Logging
 ----     -----------      ------------
    1     Deny             Deny
SwitchA#
```

ステップ 3　ギガビット イーサネット ポート 6/3 を、信頼できるポートとして設定します。

```
SwitchA# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)# interface gigabitethernet 6/3
SwitchA(config-if)# ip arp inspection trust
SwitchA(config-if)# end
SwitchA# show ip arp inspection interfaces gigabitethernet 6/3

Interface        Trust State     Rate (pps)
 ---------------  -----------     ----------
 Gi6/3            Trusted              None
SwitchA#
```

ステップ 4　バインディングを確認します。

```
SwitchA# show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
```

```
00:02:00:02:00:02   1.1.1.2          4993        dhcp-snooping  1     GigabitEthernet6/4
SwitchA#
```

ステップ 5　DAI がパケットを処理する前後の統計情報を調べます。

```
SwitchA# show ip arp inspection statistics vlan 1

Vlan      Forwarded        Dropped     DHCP Drops     ACL Drops
 ----      ---------        -------     ----------     ----------
    1              0              0              0              0

 Vlan   DHCP Permits    ACL Permits   Source MAC Failures
 ----   ------------    -----------   -------------------
    1              0              0                    0

 Vlan   Dest MAC Failures   IP Validation Failures
 ----   -----------------   ----------------------
    1                  0                       0
SwitchA#
```

このあと、ホスト 1 が IP アドレス 1.1.1.2 および MAC アドレス 0002.0002.0002 を持つ 2 つの ARP 要求を送信すると、両方の要求が許可されます。これは、次の統計情報で確認できます。

```
SwitchA# show ip arp inspection statistics vlan 1

 Vlan      Forwarded        Dropped     DHCP Drops     ACL Drops
 ----      ---------        -------     ----------     ----------
    1              2              0              0              0

 Vlan   DHCP Permits    ACL Permits   Source MAC Failures
 ----   ------------    -----------   -------------------
    1              2              0                    0

 Vlan   Dest MAC Failures   IP Validation Failures
 ----   -----------------   ----------------------
    1                  0                       0
SwitchA#
```

ホスト 1 がこのあと、IP アドレス 1.1.1.3 を持つ ARP 要求を送信しようとすると、このパケットはドロップされ、エラー メッセージが記録されます。

```
00:12:08: %SW_DAI-4-DHCP_SNOOPING_DENY: 2 Invalid ARPs (Req) on Gi6/4, vlan
1.([0002.0002.0002/1.1.1.3/0000.0000.0000/0.0.0.0/02:42:35 UTC Tue Jul 10 2001])
SwitchA# show ip arp inspection statistics vlan 1
SwitchA#
```

この場合に表示される統計情報は次のようになります。

```
Vlan      Forwarded        Dropped     DHCP Drops     ACL Drops
 ----      ---------        -------     ----------     ----------
    1              2              2              2              0

 Vlan   DHCP Permits    ACL Permits   Source MAC Failures
 ----   ------------    -----------   -------------------
    1              2              0                    0

 Vlan   Dest MAC Failures   IP Validation Failures
 ----   -----------------   ----------------------
    1                  0                       0
SwitchA#
```

スイッチ B の設定

スイッチ B において DAI をイネーブルにし、ギガビット イーサネット ポート 3/3 を信頼できるポートとして設定するには、次の作業を行います。

ステップ 1　接続を確認します。

```
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          Fas 3/3            120         R S I     WS-C6506  Fas 6/3
SwitchB#
```

ステップ 2　VLAN 1 で DAI をイネーブルにし、設定を確認します。

```
SwitchB# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchB(config)# ip arp inspection vlan 1
SwitchB(config)# end
SwitchB# show ip arp inspection vlan 1

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
    1     Enabled          Active

 Vlan     ACL Logging      DHCP Logging
 ----     -----------      ------------
    1     Deny             Deny
SwitchB#
```

ステップ 3　ギガビット イーサネット ポート 3/3 を、信頼できるポートとして設定します。

```
SwitchB# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchB(config)# interface gigabitethernet 3/3
SwitchB(config-if)# ip arp inspection trust
SwitchB(config-if)# end
SwitchB# show ip arp inspection interfaces


Interface        Trust State     Rate (pps)
 ---------------  -----------     ----------
 Gi1/1            Untrusted              15
 Gi1/2            Untrusted              15
 Gi3/1            Untrusted              15
 Gi3/2            Untrusted              15
 Gi3/3            Trusted              None
 Gi3/4            Untrusted              15
 Gi3/5            Untrusted              15
 Gi3/6            Untrusted              15
 Gi3/7            Untrusted              15

<output truncated>
SwitchB#
```

ステップ 4　DHCP スヌーピング バインディングのリストを確認します。

```
SwitchB# show ip dhcp snooping binding
```

```
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:01:00:01:00:01   1.1.1.1          4995        dhcp-snooping  1     GigabitEthernet3/4
SwitchB#
```

ステップ 5　DAI がパケットを処理する前後の統計情報を調べます。

```
SwitchB# show ip arp inspection statistics vlan 1

Vlan      Forwarded        Dropped     DHCP Drops     ACL Drops
 ----      ---------        -------     ----------     ----------
    1              0              0              0              0

 Vlan   DHCP Permits    ACL Permits   Source MAC Failures
 ----   ------------    -----------   -------------------
    1              0              0                    0

 Vlan   Dest MAC Failures   IP Validation Failures
 ----   -----------------   ----------------------
    1                  0                       0
SwitchB#
```

ホスト 2 がこのあと、IP アドレス 1.1.1.1 および MAC アドレス 0001.0001.0001 を持つ ARP 要求を送信すると、このパケットは転送され、統計情報も適切に更新されます。

```
SwitchB# show ip arp inspection statistics vlan 1

Vlan      Forwarded        Dropped     DHCP Drops     ACL Drops
 ----      ---------        -------     ----------     ----------
    1              1              0              0              0

 Vlan   DHCP Permits    ACL Permits   Source MAC Failures
 ----   ------------    -----------   -------------------
    1              1              0                    0

 Vlan   Dest MAC Failures   IP Validation Failures
 ----   -----------------   ----------------------
    1                  0                       0
SwitchB#
```

ホスト 2 が IP アドレス 1.1.1.2 を持つ ARP 要求を送信しようとすると、この要求はドロップされ、システム メッセージが記録されます。

```
00:18:08: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Gi3/4, vlan
1.([0001.0001.0001/1.1.1.2/0000.0000.0000/0.0.0.0/01:53:21 UTC Fri May 23 2003])
SwitchB#
```

この場合に表示される統計情報は次のようになります。

```
SwitchB# show ip arp inspection statistics vlan 1

Vlan      Forwarded        Dropped     DHCP Drops     ACL Drops
 ----      ---------        -------     ----------     ----------
    1              1              1              1              0

 Vlan   DHCP Permits    ACL Permits   Source MAC Failures
 ----   ------------    -----------   -------------------
    1              1              0                    0

 Vlan   Dest MAC Failures   IP Validation Failures
 ----   -----------------   ----------------------
    1                  0                       0
SwitchB#
```

1 台のスイッチが DAI をサポートする場合

ここでは、図 80-2（P.80-5）のように、スイッチ B が、DAI も DHCP スヌーピングもサポートしていない場合の DAI の設定方法を示します。

スイッチ B が DAI または DHCP スヌーピングをサポートしていない場合は、スイッチ A のファストイーサネット ポート 6/3 を信頼できるポートとして設定すると、セキュリティ ホールが生じます。これは、スイッチ A およびホスト 1 が、スイッチ B またはホスト 2 によって攻撃される可能性があるためです。

この可能性を排除するには、スイッチ A のギガビット イーサネット ポート 6/3 を信頼できないポートとして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 をセットアップして、これを VLAN 1 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。

スイッチ A に対して ARP ACL をセットアップするには、次の作業を行います。

ステップ 1　IP アドレス 1.1.1.1 および MAC アドレス 0001.0001.0001 を許可するアクセス リストを設定して、設定内容を確認します。

```
SwitchA# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)# arp access-list H2
SwitchA(config-arp-nacl)# permit ip host 1.1.1.1 mac host 1.1.1
SwitchA(config-arp-nacl)# end
SwitchA# show arp access-list
ARP access list H2
    permit ip host 1.1.1.1 mac host 0001.0001.0001
```

ステップ 2　VLAN 1 に ACL を適用して、設定を確認します。

```
SwitchA# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)# ip arp inspection filter H2 vlan 1
SwitchA(config)# end
SwitchA#

SwitchA# show ip arp inspection vlan 1

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
    1     Enabled          Active      H2                 No

 Vlan     ACL Logging      DHCP Logging
 ----     -----------      ------------
    1     Deny             Deny
SwitchA#
```

ステップ 3　ギガビット イーサネット ポート 6/3 を信頼できないポートとして設定し、設定内容を確認します。

```
SwitchA# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
SwitchA(config)# interface gigabitethernet 6/3
SwitchA(config-if)# no ip arp inspection trust
SwitchA(config-if)# end
Switch# show ip arp inspection interfaces gigabitethernet 6/3

 Interface        Trust State     Rate (pps)
 ---------------  -----------     ----------
 Gi6/3            Untrusted               15

Switch#
```

ホスト 2 がスイッチ A のギガビット イーサネット ポート 6/3 から 5 つの ARP 要求を送信し、1 つの「get」要求がスイッチ A によって許可された場合は、統計情報は次のように適切に更新されます。

```
Switch# show ip arp inspection statistics vlan 1
Vlan      Forwarded        Dropped     DHCP Drops     ACL Drops
 ----      ---------        -------     ----------     ----------
    1              5              0              0              0
Vlan   DHCP Permits    ACL Permits   Source MAC Failures
 ----   ------------    -----------   -------------------
    1              0              5                    0
Vlan   Dest MAC Failures   IP Validation Failures
 ----   -----------------   ----------------------
    1                  0                       0
Switch#
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CHAPTER 81

トラフィック ストーム制御

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

トラフィック ストーム制御の前提条件

なし。

トラフィック ストーム制御の制約事項

- 次の LAN スイッチング モジュールは、トラフィック ストーム制御をサポートしていません。
  - WS-X6148A-GE-45AF
  - WS-X6148A-GE-TX

- スイッチは、WS-X6148A-RJ-45、ギガビット イーサネット、および 10 ギガビット イーサネット LAN ポートでマルチキャストおよびユニキャスト トラフィック ストーム制御をサポートします。
- スイッチは、上記のモジュールを除く、すべての LAN ポートでブロードキャスト トラフィック ストーム制御をサポートします。
- BPDU 以外、トラフィック ストーム制御は、制御トラフィックとデータトラフィックを区別しません。
- マルチキャスト抑制をイネーブルにすると、次のモジュールでマルチキャスト抑制しきい値が超過した場合に、トラフィック ストーム制御によって BPDU が抑制されます。
  - WS-X6848-SFP-2T、WS-X6748-SFP
  - WS-X6824-SFP-2T、WS-X6724-SFP
  - WS-X6848-TX-2T、WS-X6748-GE-TX
  - WS-X6704-10GE

  上記のモジュールでマルチキャスト抑制をイネーブルにする場合は、BPDU を受信する必要がある STP 保護されたポートには、トラフィック ストーム制御を設定しないでください。

  上記のモジュール以外では、BPDU はトラフィック ストーム制御によって抑制されません。

トラフィック ストーム制御の概要

トラフィック ストームは、パケットが LAN でフラッディングする場合に発生するもので、過剰なトラフィックを生成し、ネットワークのパフォーマンスを低下させます。トラフィック ストーム制御機能は、LAN ポートが、物理インターフェイスのブロードキャスト、マルチキャスト、またはユニキャスト トラフィック ストームによって中断されるのを防ぎます。

トラフィック ストーム制御（トラフィック抑制）は着信トラフィック レベルを、1 秒ごとのトラフィック ストーム制御でモニタします。そのインターバルの中で、トラフィック レベルを、設定したトラフィック ストーム制御レベルと比較します。トラフィック ストーム制御レベルは、ポートの利用可能な帯域幅全体に対する割合です。各ポートには、すべてのタイプのトラフィック（ブロードキャスト、マルチキャスト、およびユニキャスト）用に使用されている単一のトラフィック ストーム制御レベルがあります。

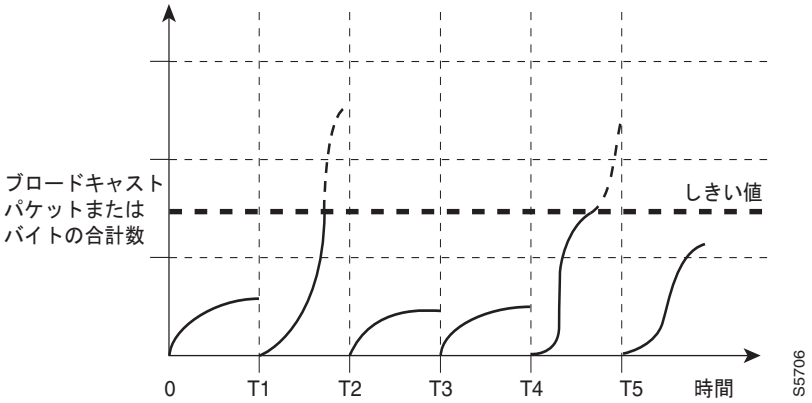
トラフィック ストーム制御は、1 秒ごとのトラフィック ストーム制御で、トラフィック ストーム制御をイネーブルにする各トラフィック タイプのレベルをモニタします。1 つのインターバルの中で、トラフィック ストーム制御がイネーブルにされている入力トラフィックが、ポートで設定されているトラフィック ストーム制御レベルに達する場合、トラフィック ストーム制御は、そのトラフィック ストーム制御インターバルが終了するまでトラフィックをドロップします。

デフォルトでは、1 つのインターバルの中で、トラフィック ストーム制御がイネーブルにされている入力トラフィックが、ポートで設定されているトラフィック ストーム制御レベルに達する場合、トラフィック ストーム制御は、そのトラフィック ストーム制御インターバルが終了するまでトラフィックをドロップします。設定可能なトラフィック ストーム制御の任意のアクションは、次のとおりです。

- シャットダウン：トラフィック ストームが発生すると、トラフィック ストーム制御はポートを errdisable ステートにします。ポートを再度イネーブルにするには、errdisable 検出と回復機能を使用するか、または **shutdown** コマンドと **no shutdown** コマンドを使用します。
- トラップ：トラフィック ストームが発生すると、トラフィック ストーム制御は SNMP トラップを生成します。

図 81-1 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、トラフィック ストーム制御が T1 と T2 時間の間、および T4 と T5 時間の間で発生します。これらの間隔中に、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。

図 81-1　　ブロードキャスト抑制



トラフィック ストーム制御しきい値の値とタイム インターバルの組み合わせによって、トラフィック制御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、通過できるパケット数が多くなります。

トラフィック ストーム制御は、ハードウェアに実装されています。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トラフィック ストーム制御回路でモニタされます。パケットの宛先アドレスの個別/グループ ビットを使用すると、トラフィック ストーム制御回路はパケットがユニキャストまたはブロードキャストの場合、1 秒のインターバル内の現在のパケット数を追跡します。この値がしきい値に達すると、以降のパケットは排除されます。

ハードウェアによるトラフィック ストーム制御では、トラフィックの測定に帯域ベースの方式が使用されるので、制御された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、制御されたトラフィック 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、トラフィック ストーム制御の動作が影響を受ける場合があります。

次に、トラフィック ストーム制御動作の例を示します。

- ブロードキャスト トラフィック ストーム制御をイネーブルにし、ブロードキャスト トラフィックが 1 秒間のトラフィック ストーム制御の間に制御レベルを超える場合、トラフィック ストーム制御はそのトラフィック ストーム制御インターバルが終了するまで、すべてのブロードキャスト トラフィックをドロップします。
- ブロードキャストおよびマルチキャスト トラフィック ストーム制御をイネーブルにし、そのブロードキャストとマルチキャスト トラフィックの合計が 1 秒間のトラフィック ストーム制御の間に制御レベルを超える場合、トラフィック ストーム制御はそのトラフィック ストーム制御インターバルが終了するまで、すべてのブロードキャストおよびマルチキャスト トラフィックをドロップします。
- ブロードキャストおよびマルチキャスト トラフィック ストーム制御をイネーブルにし、ブロードキャスト トラフィックが 1 秒間のトラフィック ストーム制御の間に制御レベルを超える場合、トラフィック ストーム制御はそのトラフィック ストーム制御インターバルが終了するまで、すべてのブロードキャストおよびマルチキャスト トラフィックをドロップします。

- ブロードキャストおよびマルチキャスト トラフィック ストーム制御をイネーブルにし、マルチキャスト トラフィックが 1 秒間のトラフィック ストーム制御の間に制御レベルを超える場合、トラフィック ストーム制御はそのトラフィック ストーム制御インターバルが終了するまで、すべてのブロードキャストおよびマルチキャスト トラフィックをドロップします。

トラフィック ストーム制御のデフォルト設定

なし。

トラフィック ストーム制御をイネーブルにする方法

トラフィック 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	`Router(config)# interface {{type slot/port} | {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	`Router(config-if)# storm-control broadcast level level[.level]`	インターフェイス上のブロードキャスト トラフィック ストーム制御をイネーブルにし、トラフィック ストーム制御レベルを設定し、そのトラフィック ストーム制御レベルを、インターフェイス上でイネーブルにされているすべてのトラフィック ストーム制御モードに適用します。
ステップ 3	`Router(config-if)# storm-control multicast level level[.level]` （注） **storm-control multicast** コマンドは、ギガビット イーサネット インターフェイスでのみサポートされています。	インターフェイス上のマルチキャスト トラフィック ストーム制御をイネーブルにし、トラフィック ストーム制御レベルを設定し、そのトラフィック ストーム制御レベルを、インターフェイス上でイネーブルにされているすべてのトラフィック ストーム制御モードに適用します。
ステップ 4	`Router(config-if)# storm-control unicast level level[.level]` （注） **storm-control unicast** コマンドは、ギガビット イーサネット インターフェイスでのみサポートされています。	インターフェイス上のユニキャスト トラフィック ストーム制御をイネーブルにし、トラフィック ストーム制御レベルを設定し、そのトラフィック ストーム制御レベルを、インターフェイス上でイネーブルにされているすべてのトラフィック ストーム制御モードに適用します。
ステップ 5	`Router(config-if)# end`	コンフィギュレーション モードを終了します。

- ポート チャネル インターフェイス上にトラフィック ストーム制御を設定できます。
- トラフィック ストーム制御を、EtherChannel のメンバであるポートに設定しないでください。トラフィック ストーム制御を EtherChannel のメンバとして設定されているポートに設定すると、そのポートは中断状態になります。
- レベルをインターフェイスの帯域幅全体に対する割合として指定します。
  - レベルの指定範囲は 0 ～ 100 です。
  - 任意で、レベルの小数部を 0 ～ 99 の範囲で指定できます。
  - 100% は、トラフィック ストーム制御がないことを意味します。
  - 0.0% は、すべてのトラフィックを抑制します。

- 次のモジュールで、すべてのトラフィックが抑制されるレベルを示します。
  - WS-X6704-10GE：0.33 % 以下
  - WS-X6824-SFP-2T、WS-X6724-SFP 10 Mbps ポート：0.33 % 以下
  - WS-X6848-SFP-2T、WS-X6748-SFP 100 Mbps ポート：0.03 % 以下
  - WS-X6848-TX-2T、WS-X6748-GE-TX 100 Mbps ポート：0.03 % 以下
  - WS-X6816-10G-2T、WS-X6716-10G
    オーバーサブスクリプション モード：0.29 % 以下

ハードウェアの制限およびサイズの異なるパケットがカウントされる方式のため、レベルの割合は概数になります。着信トラフィックを構成するフレームのサイズにより、実際に実行されるレベルは、設定レベルと数パーセント程度異なる場合があります。

次に、ギガビット イーサネット インターフェイス 3/16 でマルチキャスト トラフィック ストーム制御をイネーブルにして、トラフィック ストーム制御レベルを 70.5% に設定する例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 3/16
Router(config-if)# storm-control multicast level 70.5
Router(config-if)# end
```

この例は、あるモードに対して設定されたトラフィック ストーム制御レベルが、ギガビット イーサネット インターフェイス 4/10 ですでに設定されている他のすべてのモードにどのように影響するかを示しています。

```
Router# show run inter gig4/10
Building configuration...

Current configuration : 176 bytes
!
Router# interface GigabitEthernet4/10
Router# switchport
Router# switchport mode access
Router# storm-control broadcast level 70.00
Router# storm-control multicast level 70.00
Router# spanning-tree portfast edge
Router# end

Router# configure terminal
Router(config)# interface gigabitethernet 4/10
Router(config-if)# storm-control unicast level 20
Router(config-if)# end

Router# show interfaces gigabitethernet 4/10 counters storm-control

Port      UcastSupp %     McastSupp %     BcastSupp %  TotalSuppDiscards
Gi4/10      20.00           20.00           20.00              0

Router#
```

トラフィック ストーム制御設定の表示

コマンド	目的
`Router# show interfaces [{type slot/port} | {port-channel number}] switchport`	すべてのレイヤ 2 LAN ポートまたは特定のレイヤ 2 LAN ポートの管理および動作ステータスを表示します。
`Router# show interfaces [{type slot/port} | {port-channel number}] counters storm-control`	すべてのインターフェイス上、または指定のインターフェイス上で、3 つのトラフィック ストーム制御モードすべてによって廃棄される合計パケット数を表示します。
`Router# show interfaces counters storm-control [module slot_number]`	

（注）　**show interfaces** [{*interface_type slot/port*} | {**port-channel** *number*}] **counters** コマンドは、廃棄数を表示しません。廃棄数を表示するには、**storm-control** キーワードを入力する必要があります。

ヒント　Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CHAPTER 82

不明なユニキャストおよびマルチキャストのフラッディング コントロール

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

不明なトラフィック フラッディング コントロールの前提条件

なし。

不明なトラフィック フラッディング コントロールの制約事項

- VLAN の非受信（ルータ）ポート上で **switchport block multicast** コマンドを入力すると、ルーティング プロトコルが中断されることがあります。また、このコマンドは、224.0.0.0/24 の範囲のローカル サブネットワーク マルチキャスト コントロール グループを利用する ARP 機能や他のプロトコル（ネットワーク タイム プロトコル（NTP）など）も中断する可能性があります。
- 不明なユニキャスト フラッディング レート制限（UUFRL）がイネーブルの場合、VLAN 単位のラーニングをすべてのレイヤ 3 ルーテッド ポート上でイネーブルにしなければなりません。そうしなければ、ルーテッド ポートに着信するすべてのユニキャスト フラッディング パケットが UUFRL によってレート制限されることになります。

不明なトラフィック フラッディング コントロールに関する情報

デフォルトでは、不明なユニキャストおよびマルチキャストのトラフィックは、VLAN 内のすべてのレイヤ 2 ポートに対してフラッディングされます。不明なユニキャスト フラッディングのブロック（UUFB）機能、不明なマルチキャスト フラッディングのブロック（UMFB）機能、および不明なユニキャスト フラッディングのレート制限（UUFRL）機能を使用して、このトラフィックを防止または制限できます。

UUFB 機能と UMFB 機能では、特定のポートで、不明なユニキャストおよびマルチキャストのトラフィックのフラッディングがブロックされます。それにより、そのポート上で存在が既知の MAC アドレスを持つ出力トラフィックだけが許可されます。UUFB 機能と UMFB 機能は、Private VLAN（PVLAN; プライベート VLAN）ポートも含め、**switchport** コマンドで設定したすべてのポートでサポートされます。

UUFRL 機能は、すべての VLAN 上での不明なユニキャスト トラフィックに対するグローバルなレート制限を行います。

不明なトラフィック フラッディング コントロールのデフォルト設定

なし。

不明なトラフィック フラッディング コントロールの設定方法

- 「UUFB または UMFB の設定方法」（P.82-3）
- 「UUFRL の設定方法」（P.82-3）

UUFB または UMFB の設定方法

UUFB または UMFB 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# 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	`Router(config)# interface {{type slot/port} | {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 3	`Router(config-if)# switchport`	ポートをレイヤ 2 スイッチング用に設定します。
ステップ 4	`Router(config-if)# switchport block {unicast | multicast}`	不明なユニキャストまたはマルチキャストのフラッディングのブロックをポート上でイネーブルにします。

UUFRL の設定方法

UUFRL を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`Router# 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	`Router(config)# platform rate-limit layer2 unknown rate-in-pps [burst-size]`	UUFRL をイネーブルにして、最大パケット レートを設定します。 （任意）バースト サイズ制限を指定します。
ステップ 3	`Router(config)# exit`	コンフィギュレーション モードを終了します。

UUFRL を設定する場合、次の点に注意してください。

- *rate-in-pps* 値
  - 有効値の範囲は 10 ～ 1,000,000（1000000 と入力）です。
  - デフォルト値はありません。
  - 1,000（1000 と入力）未満の値は、十分な保護を提供できます。
- *burst-size* 値
  - 有効値の範囲は 1 ～ 255 です。
  - デフォルトは 10 です。
  - デフォルト値で、十分な保護を提供できます。

不明なトラフィック フラッディング コントロールの設定例

次に、ギガビット イーサネット ポート 5/12 に対して UUFB 設定し、この内容を確認する例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 5/12
```

```
Router(config-if)# switchport
Router(config-if)# switchport block unicast
Router(config-if)# do show interface gigabitethernet 5/12 switchport | include Unknown
Unknown unicast blocked: enabled
```

次に、レート制限が 1000 pps でバーストが 20 パケットになるように UUFRL を設定する例を示します。

```
Router# configure terminal
Router(config)# platform rate-limit layer2 unknown 1000 20
Router(config)# exit
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CHAPTER 83

IEEE 802.1X ポートベースの認証

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

802.1X 認証の前提条件

なし。

802.1X 認証の制約事項

802.1X 認証

- 802.1X 認証をイネーブルにすると、ポートが認証されてから、他のレイヤ 2 機能またはレイヤ 3 機能がイネーブルになります。
- 802.1X 対応ポートのモードを（たとえばアクセスからトランクに）変更しようとしても、エラー メッセージが表示されてポート モードは変更されません。
- 推奨しませんが、ポート セキュリティと 802.1X ポートベース認証は同じポート上に設定できます。

（注）　802.1X 認証は、sticky MAC アドレスまたはスタティック セキュア MAC アドレスによるポート セキュリティと互換性がありません。リリース 15.1(1) SY1 以降では、sticky MAC アドレスまたはスタティック セキュア MAC アドレスによるポート セキュリティと合わせて 802.1X 認証を設定できません。

- 802.1X 対応ポートが割り当てられている VLAN が変更された場合、この変更は透過的でスイッチには影響しません。たとえば、RADIUS サーバが割り当てた VLAN に割り当てられているポートが、再認証後に別の VLAN に割り当てられた場合に、この変更が発生します。

  802.1X ポートが割り当てられている VLAN がシャットダウン、ディセーブル化、または削除された場合、ポートは無許可になります。たとえば、ポートが割り当てられたアクセス VLAN がシャットダウンまたは削除された後、ポートは無許可になります。
- 802.1X プロトコルは、レイヤ 2 のスタティック アクセス ポート、音声 VLAN ポート、レイヤ 3 ルーテッド ポートではサポートされますが、次のポート タイプではサポートされません。
  - トランク ポート：トランク ポートで 802.1X 認証をイネーブルにしようとすると、エラー メッセージが表示され、802.1X 認証はイネーブルになりません。802.1X 対応ポートのモードをトランクに変更しようとしても、エラー メッセージが表示されてポート モードは変更されません。
  - ダイナミック ポート：ダイナミック モードのポートは、ネイバーとトランク ポートへの変更をネゴシエートする場合があります。ダイナミック ポートで 802.1X 認証をイネーブルにしようとすると、エラー メッセージが表示され、802.1X 認証はイネーブルになりません。802.1X 対応ポートのモードをダイナミックに変更しようとしても、エラー メッセージが表示されてポート モードは変更されません。
  - ダイナミック アクセス ポート：ダイナミック アクセス（VLAN Query Protocol（VQP））ポートで 802.1X 認証をイネーブルにしようとすると、エラー メッセージが表示され、802.1X 認証はイネーブルになりません。802.1X 対応ポートをダイナミック VLAN 割り当てに変更しようとしても、エラー メッセージが表示され、VLAN 設定は変更されません。

  - EtherChannel ポート：EtherChannel のアクティブ メンバであるポートまたはまだアクティブになっていないポートを 802.1X ポートとして設定しないでください。EtherChannel ポートで 802.1X 認証をイネーブルにしようとすると、エラー メッセージが表示され、802.1X 認証はイネーブルになりません。
  - スイッチド ポート アナライザ（SPAN）およびリモート SPAN（RSPAN）宛先ポート：SPAN または RSPAN 宛先ポートであるポートで 802.1X 認証をイネーブルにすることができます。ただし、SPAN または RSPAN 宛先ポートとしてポートが削除されるまで 802.1X 認証はディセーブルです。SPAN または RSPAN 送信元ポートでは 802.1X 認証をイネーブルにできます。
- スイッチ上で、**dot1x system-auth-control** 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 802.1X 認証をグローバルにイネーブルにする前に、802.1X 認証と EtherChannel が設定されているインターフェイスから、EtherChannel の設定を削除してください。
- 認証されていないホストからのトラフィックはすべてスイッチ プロセッサに転送されるので、このトラフィックにレート制限を適用することを推奨します。

802.1X ホスト モード

- ポート上でホスト モードが変更されると、ほとんどの場合、そのポート上の既存の 802.1X 認証は削除されます。ただし、シングルホスト モードから他のモードへの変更時とマルチドメイン モードからマルチ認証モードへの変更時は例外です。これら 2 つの場合は、既存の 802.1X 認証が維持されます。
- **authentication open** 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、認証が成功する前でも、ポートで検出された新しい MAC アドレスは、ネットワークに対して無制限のレイヤ 2 アクセスが許可されます。このコマンドを使用する場合は、デフォルトのスタティック ACL を使用してレイヤ 3 トラフィックを制限する必要があります。詳細については、「認証前オープン アクセス」（P.83-15）を参照してください。
- マルチホスト モードを設定すると、マルチホスト ポートが無許可になった場合（再認証が失敗した場合、または EAPOL ログオフ メッセージを受信した場合）、接続されたすべてのクライアントがネットワーク アクセスを拒否されます。
- MDA ホスト モードを設定すると、サードパーティ製 IP Phone の MAC アドレスは最初はデータ VLAN に割り当てられます。タグ付き音声パケットが確認されると、装置はデータ VLAN から削除され、音声 VLAN に配置されます。
- マルチ認証ホスト モードを設定する場合は、次の注意事項に留意してください。
  - マルチ認証ポートの 1 つのクライアントが無許可ステートになった場合（再認証が失敗した場合、またはそのクライアントから EAPOL ログオフ メッセージを受信した場合）、接続された他のクライアントの許可ステータスは変更されません。
  - RADIUS が割り当てた VLAN は、マルチ認証ポートではサポートされません。1 つのデータ VLAN しか持つことができないためです。認証サーバが VLAN 関連の属性を送信した場合、認証は成功しますが、VLAN 割り当ては無視されます。
  - データ VLAN では複数のホストが許可されますが、音声 VLAN で許可されるホストは 1 つだけです。1 つの IP Phone が認証されている場合、同じポートの他の IP Phone は認証を拒否されます。
  - マルチ認証ポートでは、ゲスト VLAN、認証失敗 VLAN、またはクリティカル VLAN はサポートされません。

VLAN 割り当て、ゲスト VLAN、制限付き VLAN、アクセス不能認証バイパス

- 802.1X 認証がポートでイネーブルになっている場合、音声 VLAN と同じポート VLAN を設定できません。
- VLAN 割り当て機能を使った 802.1X 認証は、トランク ポート上、ダイナミック ポート上、および VMPS を介したダイナミックアクセス ポート割り当てではサポートされません。
- RSPAN VLAN、プライベート プライマリ PVLAN、または音声 VLAN を除き、任意の VLAN を 802.1X ゲスト VLAN として設定できます。ゲスト VLAN の機能は、内部 VLAN（ルーテッド ポート）またはトランク ポート上ではサポートされません。サポートされるのはアクセス ポートだけです。
- DHCP クライアントが接続されている 802.1X ポートのゲスト VLAN を設定したあとで、ホスト IP アドレスを DHCP サーバから取得する必要がある場合もあります。クライアント上の DHCP プロセスが時間切れとなり DHCP サーバからホスト IP アドレスを取得しようとする前に、スイッチ上の 802.1X 認証プロセスを再起動する設定を変更できます。802.1X 認証プロセス（**dot1x timeout quiet-period** および **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）の設定を減らします。設定を減らす量は、接続されている 802.1X クライアントのタイプによって異なります。
- 802.1X VLAN ユーザ分散機能を設定する場合は、次の注意事項に従ってください。
  - 最大 100 の VLAN グループを設定でき、1 つの VLAN グループに最大 4094 の VLAN をマッピングできます。
  - 1 つの VLAN を複数の VLAN グループにマッピングできます。
  - VLAN グループにはゲスト VLAN、クリティカル VLAN、または制限 VLAN をマッピングできます。
  - VLAN グループ名を guest VLAN、critical VLAN、または restricted VLAN として指定できません。
  - VLAN グループは VLAN を追加または削除することで変更できますが、少なくとも 1 つの VLAN が VLAN グループにマッピングされている必要があります。VLAN グループから最後の VLAN を削除すると、その VLAN グループは削除されます。
  - VLAN グループ名から既存の VLAN を削除した場合、その VLAN にあるポートの認証ステータスは取り消されませんが、マッピングは既存の VLAN グループから削除されます。
  - 既存の VLAN グループ名を削除した場合、そのグループ内の VLAN にあるポートの認証ステータスは取り消されませんが、その VLAN グループへの VLAN マッピングは削除されます。
- アクセス不能認証バイパス機能を設定する際には、次の注意事項に従ってください。
  - アクセス不能認証バイパス機能は、シングルホスト モード、マルチホスト モード、および MDA モードの 802.1X ポートでサポートされます。
  - Windows XP を稼働しているクライアントに接続されたポートがクリティカル認証ステートの場合、Windows XP はインターフェイスが認証されないと報告する場合があります。
  - Widows XP クライアントが DHCP 用に設定されていて、DHCP サーバからの IP アドレスがある場合、クリティカル ポートで EAP-Success メッセージを受信しても DHCP 設定プロセスが再開されない場合があります。

  - アクセス不能認証バイパス機能とクリティカル VLAN を 802.1X ポートに設定することができます。スイッチがクリティカル VLAN 内のクリティカル ポートを再認証しようとして、すべての RADIUS サーバが利用不能な場合、スイッチはポート ステートをクリティカル認証ステートに変更し、ポートはクリティカル VLAN に残ります。
  - アクセス不能認証バイパス機能とポートセキュリティを同じポートに設定できます。
- RSPAN VLAN または音声 VLAN を除き、任意の VLAN を 802.1X 制限 VLAN として設定できます。制限付き VLAN 機能は、内部 VLAN（ルーテッド ポート）またはトランク ポートではサポートされていません。アクセス ポート上でだけサポートされます。

MAC 認証バイパス

- 特記されている場合を除き、MAC 認証バイパスの注意事項は、802.1X 認証の注意事項と同じです。詳細については、「802.1X 認証」（P.83-2）を参照してください。
- ポートが MAC アドレスにより許可されたあと、ポートの MAC 認証バイパスをディセーブルにする場合、ポート ステートに影響はありません。
- EAP を使った MAC 認証バイパスがインターフェイス上でイネーブルになっている場合は、その後にインターフェイス上で実行される **default interface** コマンドによってディセーブルになることはありません。
- ポートが未許可ステートであり、クライアント MAC アドレスが認証サーバ データベースにない場合、ポートは未許可ステートのままです。ただし、クライアント MAC アドレスがデータベースに追加された場合、スイッチは MAC 認証バイパスを使用してポートを再許可します。
- ポートが許可ステートの場合、再許可が発生するまでポートはこのステートのままになります。
- MAC 認証バイパスをルーテッド ポートで使用するために、MAC アドレス ラーニングがポートでイネーブルになっていることを確認してください。
- MAC 認証バイパスにより接続されているが、非アクティブなホストのタイムアウト時間を任意で設定できます。指定できる範囲は 1 ～ 65535 秒ですが、再認証タイムアウトよりも小さい値に設定する必要があります。タイムアウト値を設定する前に、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。詳細については、「ポート セキュリティの設定方法」（P.85-5）を参照してください。

Web ベース認証

- Web ベース認証に対するフォールバックは、スイッチ ポート上のアクセス モードで設定されます。トランク モードのポートはサポートされません。
- Web ベース認証に対するフォールバックは、EtherChannels または EtherChannel メンバではサポートされません。
- Web ベース認証に対するフォールバックは、インターフェイス固有の設定ですが、Web ベース認証の動作は、グローバル フォールバック プロファイルで定義されます。フォールバックのグローバル設定が変更された場合、新しいプロファイルは次の認証フォールバック インスタンスまで使用されません。

Web ベース認証の設定方法の詳細については、第 84 章「Web ベース認証」を参照してください。

ネットワーク エッジ アクセス トポロジ（NEAT）と Client Information Signalling Protocol（CISP）

- NEAT ポートは、他の認証ポートと同じコンフィギュレーションで設定できます。サプリカント スイッチが認証すると、ポート モードはベンダー固有属性（VSA）に基づいて*アクセスからトランク*に変更されます （device-traffic-class=switch）。
- VSA はオーセンティケータ スイッチ ポート モードをアクセスからトランクに変更し、802.1x トランク カプセル化およびアクセス VLAN をイネーブルにします（任意の VLAN がネイティブ トランク VLAN に変換される場合）。VSA はサプリカントのポート コンフィギュレーションは変更しません。

802.1X ポートベース認証について

802.1X の概要

ここでは、認証、許可、アカウンティング（AAA）の一部として IEEE 802.1X ポートベース認証のロールについて説明します。802.1X 規格は、クライアントおよびサーバ ベースのアクセス コントロールと認証プロトコルについて定義しており、不正なクライアントが公的にアクセス可能なポートを介し

て LAN に接続することを制限しています。認証サーバは、スイッチ ポートに接続する各クライアントを認証し、ポートを VLAN に割り当てたうえで、スイッチや LAN によって提供されるサービスを利用できるようにします。

802.1X アクセス コントロールでは、クライアントが認証されるまで、そのクライアントが接続しているポート経由では Extensible Authentication Protocol over LAN（EAPOL）トラフィックだけが許可されます。認証に成功すると、通常のトラフィックはポートを通過できるようになります。

802.1x デバイスの役割

802.1X ポートベース認証では、図 83-1 に示すように、ネットワーク上の装置にはそれぞれ特定のロールがあります。

図 83-1　802.1x デバイスの役割

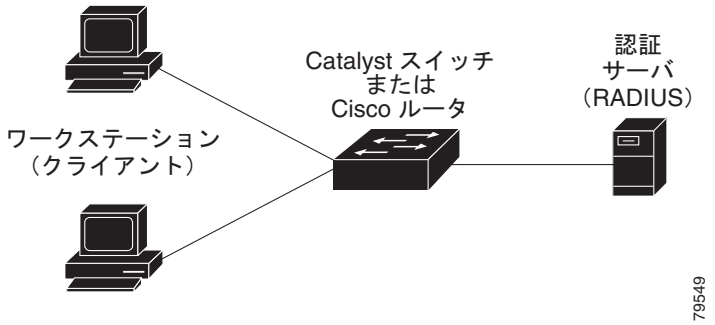


図 83-1 に示す特定の役割は、次のとおりです。

- *クライアント*：LAN およびスイッチ サービスへのアクセスを要求して、スイッチからの要求に応答するデバイス（ワークステーション）。ワークステーションでは、Microsoft Windows XP オペレーティング システムで提供されるクライアントなど、802.1X 準拠のクライアント ソフトウェアが稼働している必要があります。（クライアントは、IEEE 802.1X 規格では*サプリカント*といいます）。

（注）　Windows XP のネットワーク接続および 802.1X ポートベース認証の問題に関しては、次の URL にある Microsoft Knowledge Base を参照してください。
http://support.microsoft.com/kb/q303597/

- *認証サーバ*：実際にクライアントの認証を行います。認証サーバはクライアントの識別情報を確認し、そのクライアントに LAN およびスイッチ サービスへのアクセスを許可すべきかどうかをスイッチに通知します。スイッチはプロキシとして動作するので、認証サービスはクライアントに対して透過的に行われます。認証サーバとして、Extensible Authentication Protocol（EAP）拡張機能を備えた Remote Authentication Dial-In User Service（RADIUS）セキュリティ システムだけがサポートされています。この認証サーバは、Cisco Secure Access Control Server（ACS）Version 3.0 で使用可能です。RADIUS はクライアント サーバ モデルで動作し、RADIUS サーバと 1 つまたは複数の RADIUS クライアントとの間でセキュア認証情報を交換します。
- *スイッチ（オーセンティケータおよびバックエンドのオーセンティケータともいう）*：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的アクセスを制御します。スイッチはクライアントと認証サーバとの仲介デバイス（プロキシ）として動作し、クライアントに識別情報を要

求し、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。スイッチには、EAP フレームのカプセル化とカプセル化解除、および認証サーバとの対話を処理する RADIUS クライアントが含まれています

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。カプセル化では EAP フレームの変更または検証は行われず、認証サーバはネイティブ フレーム フォーマットの EAP をサポートしなければなりません。スイッチが認証サーバからフレームを受信すると、サーバのフレーム ヘッダーが削除され、残りの EAP フレームがイーサネット用にカプセル化され、クライアントに送信されます。

ポートベース認証プロセス

802.1X ポートベース認証をイネーブルにすると、次のようなイベントが発生します。

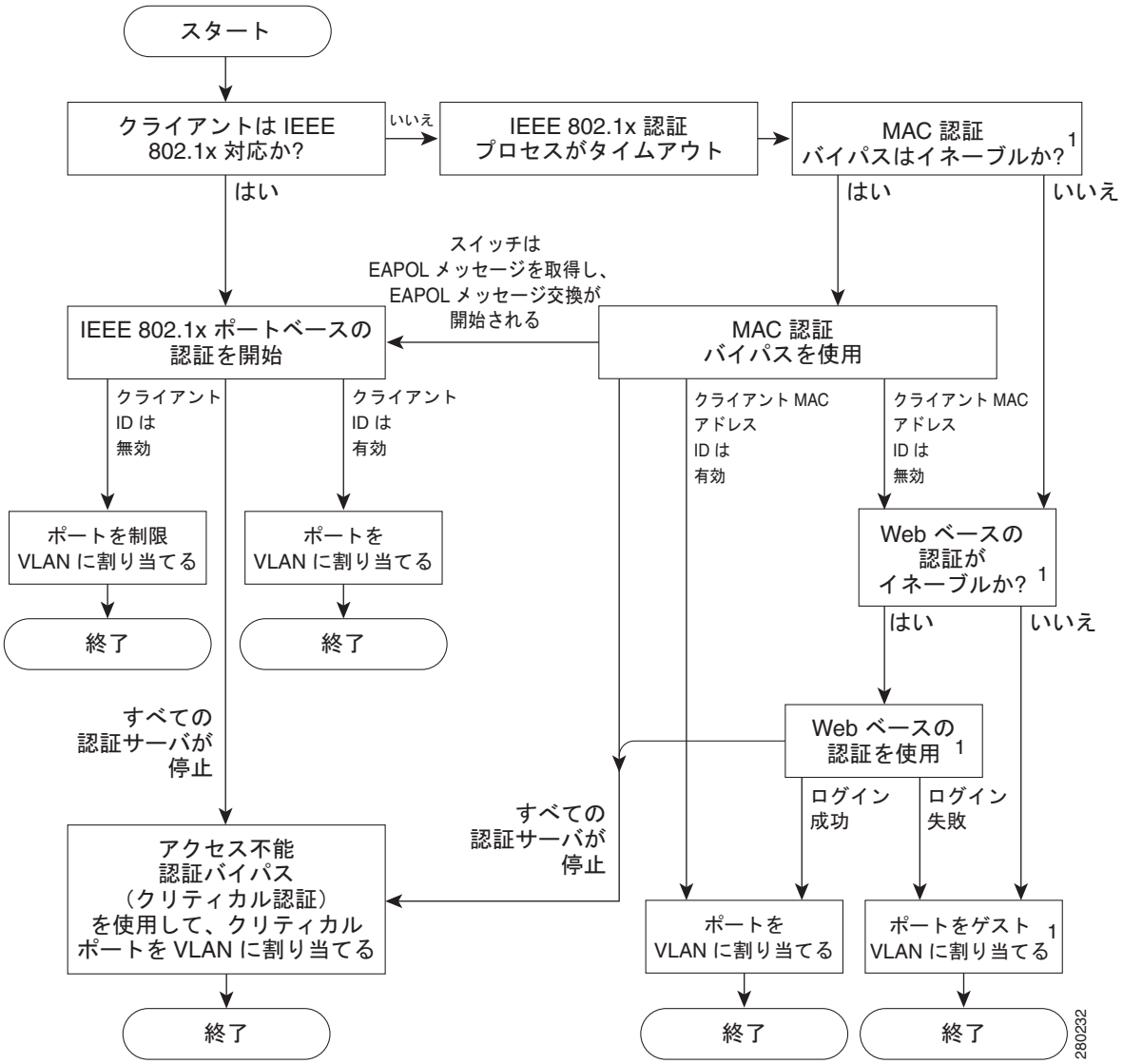
- クライアントが 802.1X 準拠クライアント ソフトウェアをサポートしており、クライアントの ID が有効である場合、802.1X 認証は成功し、スイッチがクライアントに対してネットワークへのアクセスを許可します。
- EAPOL メッセージ交換の待機中に 802.1X 認証がタイムアウトした場合、スイッチは MAC 認証バイパス（MAB）や Web ベース認証（webauth）などのフォールバック認証方式を使用できます（いずれかまたは両方がイネーブルになっている場合）。
  - MAC 認証バイパスがイネーブルの場合、スイッチは許可のためにクライアントの MAC アドレスを AAA サーバにリレーします。クライアントの MAC アドレスが有効であれば、正常に許可され、スイッチがクライアントに対してネットワークへのアクセスを許可します。
  - Web ベース認証がイネーブルの場合、スイッチは HTTP ログイン ページをクライアントに送信します。スイッチは許可のためにクライアントのユーザ名とパスワードを AAA サーバにリレーします。ログインが成功すると、スイッチがネットワークに対するクライアント アクセスを許可します。

（注）　認証方式のデフォルトの順序は、802.1X、次に MAB、次に Web ベース認証です。順序は変更でき、これらの方式のいずれかをディセーブルにすることもできます。

- フォールバック認証方式がイネーブルになっていない、または成功しない場合、ゲスト VLAN が設定されていれば、スイッチは限定的なサービスを提供するゲスト VLAN にクライアントを割り当てます。
- スイッチが 802.1X 対応クライアントから無効な ID を受信し、制限付き VLAN が指定されている場合、スイッチはクライアントに限定的なサービスを提供する制限付き VLAN を割り当てることができます。
- RADIUS 認証サーバが（ダウンして）利用できず、アクセス不能認証バイパスがイネーブルの場合、ユーザ指定のクリティカル VLAN 内でポートをクリティカル認証ステートにすることで、スイッチがクライアントに対してネットワークへのアクセスを許可します。

（注）　アクセス不能認証バイパスは、クリティカル認証または AAA 失敗ポリシーとも呼ばれます。

図 83-2　認証フローチャート



1 = これはスイッチがクライアントから EAPOL パケットを検出できない場合に発生する

スイッチは、次のいずれかの状況が発生するとクライアントを再認証します。

- 定期再認証がイネーブルで、再認証タイマーが満了した場合。

  スイッチ固有の値を使用するか、RADIUS サーバの値に基づいて、再認証タイマーを設定できます。

  RADIUS サーバを使用した 802.1X 認証が設定されていると、スイッチは Session-Timeout RADIUS 属性（属性 [27]）、および Termination-Action RADIUS 属性（属性 [29]）に基づいてタイマーを使用します。

  Session-Timeout RADIUS 属性（属性 [27]）は、再認証が発生するまでの時間を指定します。

Termination-Action RADIUS 属性（属性 [29]）は、再認証中に実行するアクションを指定します。アクションは Initialize および ReAuthenticate に設定できます。初期化アクションが設定されている場合（属性値は DEFAULT）、802.1X セッションが終了して、再認証中に接続は失われます。再認証アクションが設定されている場合（属性値は RADIUS-Request）、再認証中にセッションは影響を受けません。

- **dot1x re-authenticate interface** *type slot/port* 特権 EXEC コマンドを入力して、クライアントを手動で再認証した場合。

認証の開始およびメッセージ交換

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 pae authenticator** および **authentication 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した場合、スイッチはポートのリンク ステートがダウンからアップに移行したと判断した時点で、認証を開始しなければなりません。次に、スイッチは EAP 要求/アイデンティティ 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、スイッチは最初のアイデンティティ/要求フレームを送信して、そのあとで 1 つまたは複数の認証情報の要求を送信します）。クライアントはフレームを受信すると、EAP 応答/アイデンティティ フレームで応答します。

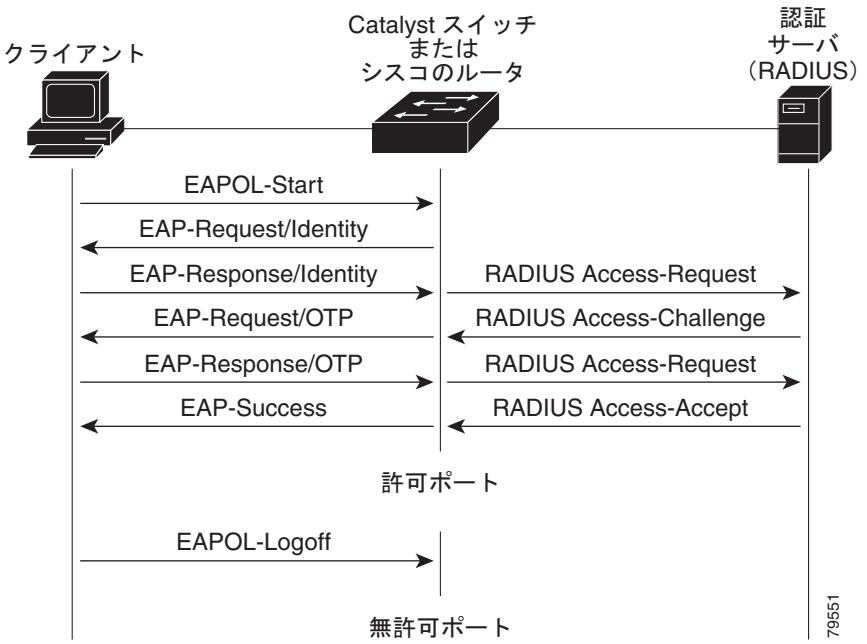
ただし、クライアントが起動時にスイッチから EAP 要求/アイデンティティ フレームを受信しなかった場合、クライアントは EAPOL 開始フレームを送信して認証を開始することができます。このフレームはスイッチに対し、クライアントの識別情報を要求するように指示します。

（注）　ネットワーク アクセス装置で 802.1X がイネーブルに設定されていない、またはサポートされていない場合には、クライアントからの EAPOL フレームはすべてドロップされます。クライアントが認証の開始を 3 回試みても EAP 要求/アイデンティティ フレームを受信しなかった場合、クライアントはポートが許可ステートであるものとしてフレームを送信します。ポートが許可ステートであるということは、クライアントの認証が成功したことを実質的に意味します。詳細については、「許可ステートおよび無許可ステートのポート」（P.83-12）を参照してください。

クライアントが自らの識別情報を提示すると、スイッチは仲介デバイス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の間で EAP フレームを送受信します。認証が成功すると、ポートは許可ステートになります。認証に失敗した場合、認証が再試行されるか、ポートが限定的なサービスを提供する VLAN に割り当てられるか、あるいはネットワーク アクセスが許可されないかのいずれかになります。詳細については、「許可ステートおよび無許可ステートのポート」（P.83-12）を参照してください。

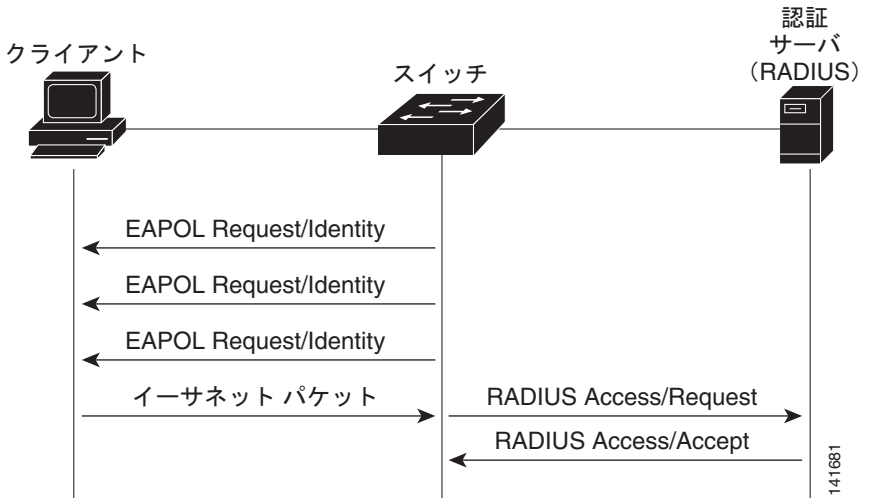
実際に行われる EAP フレーム交換は、使用する認証方式によって異なります。図 83-3 に、クライアントが RADIUS サーバとの間でワンタイム パスワード（OTP）認証方式を使用する場合に行われるメッセージ交換を示します。

図 83-3　メッセージ交換



EAPOL メッセージ交換の待機中に 802.1X 認証がタイムアウトし、MAC 認証バイパスがイネーブルの場合、スイッチはクライアントからイーサネット パケットを検出するとそのクライアントを認証できます。スイッチは、クライアントの MAC アドレスを ID として使用し、RADIUS サーバに送信される RADIUS Access/Request フレームにこの情報を保存します。サーバがスイッチに RADIUS Access/Accept フレームを送信（認証が成功）すると、ポートが許可されます。MAB 認証に失敗してゲスト VLAN が指定されている場合、スイッチはポートをゲスト VLAN に割り当てます。イーサネット パケットの待機中にスイッチが EAPOL パケットを検出すると、スイッチは MAC 認証バイパス プロセスを停止して、802.1X 認証を開始します。

図 83-4　MAC 認証バイパス中のメッセージ交換



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。ポートは最初、*無許可*ステートです。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。クライアントの認証が成功すると、ポートは*許可*ステートに移行し、クライアントのトラフィック送受信を通常どおりに許可します。

802.1X 認証をサポートしていないクライアントが、無許可ステートの 802.1X ポートに接続すると、スイッチはそのクライアントの ID を要求します。この状況では、クライアントは要求に応答せず、ポートは引き続き無許可ステートとなり、クライアントはネットワーク アクセスを許可されません。

反対に、802.1x 対応のクライアントが、802.1x プロトコルの稼働していないポートに接続すると、クライアントは EAPOL 開始フレームを送信して認証プロセスを開始します。応答がなければ、クライアントは同じ要求を所定の回数だけ送信します。応答がないので、クライアントはポートが許可ステートであるものとしてフレーム送信を開始します。

authentication port-control インターフェイス コンフィギュレーション コマンドおよび次のキーワードを使用して、ポートの許可ステートを制御できます。

- **force-authorized**：802.1x ポートベースの認証をディセーブルにして、必要な認証交換を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との 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。これがデフォルト設定です。
- **force-unauthorized**：ポートを無許可ステートのままにして、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経由でクライアントに認証サービスを提供できません。
- **auto**：802.1x ポートベースの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、または 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との間で認証メッセージのリレーを開始します。ネットワークへのアクセスを試行する各クライアントは、クライアントの MAC アドレスを使用してスイッチにより一意に識別されます。

クライアントが認証に成功すると（認証サーバから Accept フレームを受信すると）、ポートが許可ステートに変わり、認証されたクライアントからの全フレームがポート経由での送受信を許可されます。認証が失敗すると、ポートは無許可ステートのままですが、認証を再試行することはできます。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。所定の回数だけ試行してもサーバから応答が得られない場合には、認証が失敗し、ネットワーク アクセスは許可されません。

クライアントはログオフすると EAPOL ログオフ メッセージを送信します。これにより、スイッチ ポートは無許可ステートに移行します。

ポートのリンク ステートがアップからダウンに移行した場合、または EAPOL ログオフ 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。

802.1X ホスト モード

ホスト モードの概要

802.1X ポートのホスト モードによって、ポート上で複数のクライアントの認証が可能かどうかと、認証の実行方法が決まります。次の各項で説明する 4 つのホスト モードのいずれかを使用して、802.1X ポートを設定できます。さらに、各モードは、認証前オープン アクセスを許可するように変更される場合もあります。

シングルホスト モード

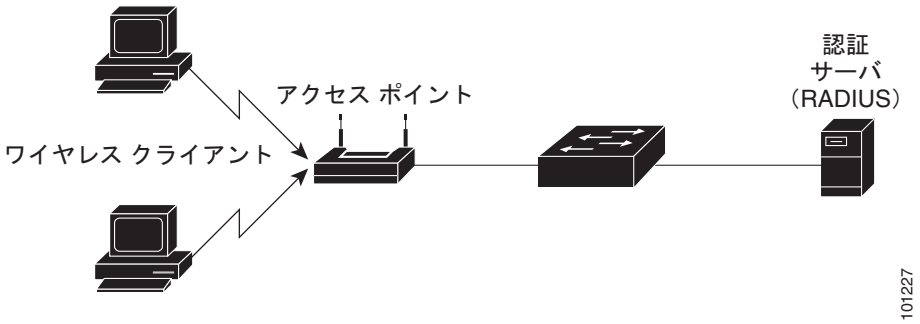
シングルホスト モード（図 83-1（P.83-7）を参照）では、802.1X 対応ポートには、クライアントが 1 つしか接続できません。スイッチは、ポートのリンク ステートがアップに変化したときに、EAPOL フレームを送信することでクライアントを検出します。クライアントがログオフしたとき、または別のクライアントに代わったときには、スイッチはポートのリンク ステートをダウンに変更し、ポートは無許可ステートに戻ります。

複数ホスト モード

複数ホスト モードでは、複数のホストを 1 つの 802.1X 対応ポートに接続できます。図 83-5 に、ワイヤレス LAN における 802.1x ポート ベースの認証を示します。このモードでは、接続されたクライアントのうち 1 つが許可されれば、クライアントすべてのネットワーク アクセスが許可されます。ポートが無許可ステートになると（再認証が失敗した場合、または EAPOL ログオフ メッセージを受信した場合）、スイッチは接続されたすべてのクライアントのネットワーク アクセスを拒否します。このトポロジでは、ワイヤレス アクセス ポイントが接続しているクライアントの認証を処理し、スイッチに対してクライアントとしての役割を果たします。

マルチホスト モードがイネーブルの場合、802.1X 認証を使用してポートを認証できます。また、ポート セキュリティを使用してすべての MAC アドレス（クライアントの MAC アドレスを含む）のネットワーク アクセスを管理できます。

図 83-5　　マルチ ホスト モードの例

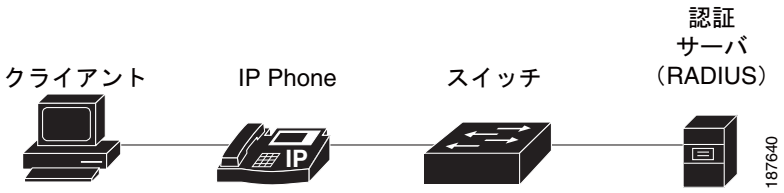


マルチドメイン認証モード

マルチドメイン認証（MDA）モードを使用すると、802.1X、MAC 認証バイパス（MAB）、または Web ベース認証（ホスト用のみ）を使用して、IP Phone（シスコ製またはサードパーティ製）と IP Phone の背後の単一のホストでそれぞれ独立して認証を実行できるようになります。この用途では、マルチドメインは 2 つのドメイン（データと音声）を意味し、ポートあたり 2 つの MAC アドレスだけが許可されます。スイッチではホストをデータ VLAN に、IP Phone を音声 VLAN に配置することができますが、これらは同じスイッチ ポート上にあるように見えます。データ VLAN 割り当ては、認証中に認証、許可、アカウンティング（AAA）サーバから受信されたベンダー固有属性（VSA）から取得することができます。

図 83-6 に、802.1X がイネーブルのポートに接続されている IP Phone に接続された単一ホストがある、典型的な MDA アプリケーションを示します。クライアントはスイッチに直接接続されないため、クライアントの接続が切断されても、スイッチでは、ポート リンクの切断を検出できません。切断されたクライアントの確立済みの認証を別のデバイスが使用する可能性を防ぐために、より最近の Cisco IP Phone は、接続されたクライアントのポートのリンク ステートに変更があったことをスイッチに通知するために、Cisco Discovery Protocol（CDP）のホストの存在を示す Type Length Value（TLV）を送信します。

図 83-6　　マルチドメイン認証モードの例



マルチ認証の VLAN 割り当て

マルチ認証の VLAN 割り当てでは、次の状況が発生すると、既存のコマンドを使用してマルチ認証モードの RADIUS サーバから提供された VLAN の割り当てをサポートします。

- ホストがポートで最初に許可されたホストであり、RADIUS サーバが VLAN 情報を提供している。
- 後続のホストが、動作 VLAN に一致する VLAN を使用して許可される。
- ホストは VLAN が割り当てられていないポートで許可され、後続のホストでは VLAN 割り当てが設定されていないか、VLAN 情報が動作 VLAN と一致している。
- ポートで最初に許可されたホストにはグループ VLAN が割り当てられ、後続のホストでは VLAN 割り当てが設定されていないか、グループ VLAN がポート上のグループ VLAN と一致している。後続のホストが、最初のホストと同じ VLAN グループの VLAN を使用する必要がある。VLAN リストが使用されている場合、すべてのホストは VLAN リストで指定された条件に従う。
- VLAN がポート上のホストに割り当てられると、後続のホストは一致する VLAN 情報を持つ必要があり、この情報がなければポートへのアクセスを拒否される。
- クリティカル認証 VLAN の動作が、マルチ認証モード用に変更されない。ホストが認証を試みたときにサーバに到達できない場合、許可されたすべてのホストは、設定された VLAN で再初期化される。

（注）
- 1 つの音声 VLAN だけマルチ認証ポートでサポートされます。
- ゲスト VLAN または認証失敗 VLAN をマルチ認証モードで設定できません。

マルチ認証モード

マルチ認証モードでは、音声 VLAN 上に 1 つの 802.1X/MAB クライアントと、データ VLAN 上に複数の認証済み 802.1X/MAB/Web 認証クライアントが許可されます。図 83-5 のように、ハブまたはアクセス ポイントが 802.1X ポートに接続される場合、マルチ認証モードでは、接続クライアントごとに認証を要求することで、マルチホスト モードよりもセキュリティが強化されます。802.1X 以外の装置では、個々のホストを認証するフォールバック方式として MAB または Web ベース認証を使用できるので、単一ポート上で異なるホストを異なる方式で認証することが可能になります。

また、マルチ認証では、認証サーバから受信した VSA に従って認証済み装置をデータ VLAN または音声 VLAN に割り当てることで、音声 VLAN での MDA 機能がサポートされます。

認証前オープン アクセス

認証前にデバイスからネットワークにアクセスできるよう、4 つのホスト モードのうち任意のモードを追加設定することができます。この認証前オープン アクセスは、Pre-boot eXecution Environment（PXE）などのアプリケーションで役に立ちます。PXE では、デバイスがネットワークにアクセスし、認証クライアントを含むブート可能イメージをダウンロードする必要があります。

認証前オープン アクセスは、ホスト モードの設定後に **authentication open** コマンドを入力することでイネーブルになり、設定済みのホスト モードの拡張として機能します。たとえば、シングルホスト モードで認証前オープン アクセスをイネーブルにした場合、ポートでは 1 つの MAC アドレスだけが許可されます。認証前オープン アクセスがイネーブルの場合、ポート上に設定されている 802.1X とは別の他のアクセス制限によってのみ、ポート上の初期トラフィックは、制限されます。ポートに 802.1X 以外のアクセス制限が設定されていない場合、クライアント装置は設定されている VLAN 上でフル アクセスが可能です。

DHCP スヌーピングを使用した 802.1X 認証

データ挿入機能を備えた Dynamic Host Configuration Protocol（DHCP）スヌーピングの Option 82 をイネーブルにすると、スイッチがクライアントの 802.1X 認証されたユーザ ID 情報を DHCP ディスカバリ プロセスに挿入でき、DHCP サーバによって別の IP アドレス プールの IP アドレスが別のエンド ユーザのクラスに割り当てられます。この機能により、アカウンティング目的でエンド ユーザに付与する IP アドレスのセキュリティを確保することができ、レイヤ 3 基準に基づいてサービスを許可することができます。

サプリカントと RADIUS サーバとの間で 802.1X 認証が成功すると、スイッチはポートをフォワーディング ステートに設定し、RADIUS サーバから受信した属性を格納します。DHCP スヌーピングを実行している場合、スイッチは DHCP リレー エージェントとして機能し、DHCP メッセージを受信し、別のインターフェイスで送信するためにこれらのメッセージを再度生成します。クライアントが 802.1X 認証後に DHCP ディスカバリ メッセージを送信すると、スイッチはパケットを受信します。スイッチは、保存されたクライアントの RADIUS 属性を含む RADIUS 属性サブオプション セクションをパケットに追加します。スイッチは、その後、ディスカバリ ブロードキャストを再度送信します。DHCP サーバは変更された DHCP ディスカバリ パケットを受信して、IP アドレス リースの作成時に認証済みユーザ ID 情報を使用することができます（設定されている場合）。ユーザと IP アドレスは、1 対 1、1 対多、多対多でマッピングできます。1 対多のマッピングを使用すれば、同一ユーザを複数ポートの 802.1X ホストで認証できます。

スイッチは、802.1X 認証機能とデータ挿入による DHCP スヌーピング Option 82 機能がイネーブルになると、自動的に認証済みユーザ ID 情報を挿入します。データ挿入による DHCP スヌーピング Option 82 を設定するには、「DHCP スヌーピングの Option 82 データ挿入」（P.78-6）を参照してください。

RADIUS 属性サブオプションに挿入されるデータの詳細については、RFC 4014「Remote Authentication Dial-In User Service (RADIUS) Attributes Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Information Option」を参照してください。

802.1X アカウンティング

IEEE 802.1X 標準には、ネットワーク アクセスに対するユーザの許可と認証方法は定義されていますが、ネットワークの使用状況を追跡するものではありません。IEEE 802.1X アカウンティングは、デフォルトでディセーブルに設定されています。802.1X アカウンティングをイネーブルにすると、802.1X 対応ポートで次のアクティビティをモニタできます。

- 正常にユーザを認証します。
- ユーザがログ オフします。
- リンクダウンが発生します。
- 再認証の正常な発生
- 再認証の失敗

スイッチは IEEE 802.1X アカウンティング情報を記録しません。その代わり、スイッチはこの情報を 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。

RADIUS サーバに送信された情報は、Attribute Value（AV; 属性値）ペアの形式で表示されます。これらの AV ペアのデータは、各種アプリケーションによって使用されます （たとえば課金アプリケーションの場合、RADIUS パケットの Acct-Input-Octets または Acct-Output-Octets 属性の情報が必要です）。

AV ペアは、802.1X アカウンティングが設定されているスイッチによって自動的に送信されます。次の種類の RADIUS アカウンティング パケットがスイッチによって送信されます。

- START：新規ユーザ セッションの開始時に送信されます。
- INTERIM：既存のセッション中にアップデートのために送信されます。
- STOP：セッション終了時に送信されます。

表 83-1 は AV ペアの一覧で、スイッチによって送信されるタイミングを示しています。

表 83-1　アカウンティング AV ペア

属性番号	AV ペア名	START	INTERIM	STOP
属性 [1]	User-Name	常時送信	常時送信	常時送信
属性 [4]	NAS-IP-Address	常時送信	常時送信	常時送信
属性 [5]	NAS-Port	常時送信	常時送信	常時送信
属性 [8]	Framed-IP-Address	非送信	条件に応じて送信	条件に応じて送信
			（注） Framed-IP-Address AV ペアは、DHCP スヌーピング バインディング テーブル内のホストに対して有効な DHCP バインディングが存在する場合にだけ送信されます。	
属性 [25]	Class	常時送信	常時送信	常時送信
属性 [26]	Vendor-Specific	—	—	—
	（注） ベンダー固有属性（VSA）は、他の 802.1X 機能によって使用されます。			
属性 [30]	Called-Station-ID	常時送信	常時送信	常時送信
属性 [31]	Calling-Station-ID	常時送信	常時送信	常時送信
属性 [40]	Acct-Status-Type	常時送信	常時送信	常時送信
属性 [41]	Acct-Delay-Time	常時送信	常時送信	常時送信
属性 [42]	Acct-Input-Octets	非送信	非送信	常時送信
属性 [43]	Acct-Output-Octets	非送信	非送信	常時送信
属性 [44]	Acct-Session-ID	常時送信	常時送信	常時送信
属性 [45]	Acct-Authentic	常時送信	常時送信	常時送信
属性 [46]	Acct-Session-Time	非送信	非送信	常時送信
属性 [49]	Acct-Terminate-Cause	非送信	非送信	常時送信
属性 [61]	NAS-Port-Type	常時送信	常時送信	常時送信

スイッチによって送信された AV ペアは、**debug radius accounting** 特権 EXEC コマンドを入力することで表示できます。AV ペアの詳細については、RFC 3580「IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines」を参照してください。

VLAN 割り当てを使用した 802.1X 認証

ポートの 802.1X 認証が成功すると、RADIUS サーバは VLAN 割り当てを送信してポートを設定します。RADIUS サーバはデータベースにユーザ名と VLAN マッピングを維持し、ポートに接続されたクライアントのユーザ名に基づいて VLAN を割り当てます。この機能を使用して、特定のユーザのネットワーク アクセスを制限できます。

スイッチと RADIUS サーバ上で設定された場合、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。

- 802.1X 認証がポートでイネーブルになっており、RADIUS サーバからのすべての情報が有効である場合、ポートは認証後に RADIUS サーバが割り当てた VLAN に配置されます。
- マルチホスト モードが 802.1X ポートでイネーブルになっている場合、ポート上のすべてのホストが、最初に認証されたホストと同じ RADIUS サーバが割り当てた VLAN に配置されます。
- マルチ認証モードが 802.1X ポートでイネーブルになっている場合、VLAN 割り当ては無視されます。
- RADIUS サーバから VLAN 番号が提供されなかった場合、認証の成功後にポートはアクセス VLAN 内に設定されます。アクセス VLAN は、アクセス ポートに割り当てられた VLAN です。このポート上で送受信されるパケットはすべて、この VLAN に所属します。
- 802.1X 認証がイネーブルになっていても、RADIUS サーバからの VLAN 情報が有効でない場合は、ポートは無許可ステートに戻り、設定されたアクセス VLAN に残ります。これにより、設定エラーによって不適切な VLAN に予期せぬポートが現れることを防ぎます。

  設定エラーには、ルーテッド ポートへの VLAN の指定、誤った VLAN ID、存在しないまたは内部（ルーテッド ポートの）の VLAN ID、あるいは音声 VLAN ID への割り当て試行、などがあります。
- 802.1X 認証がポートでディセーブルになっている場合、ポートは設定済みアクセス VLAN に戻されます。

ポートが強制許可、強制無許可、無許可、またはシャットダウン ステートの場合、ポートは設定済みアクセス VLAN に配置されます。

802.1X ポートが認証され、RADIUS サーバが割り当てた VLAN に配置された場合、ポートのアクセス VLAN 設定に対する変更はすべて有効になりません。

VLAN 割り当て機能を使った 802.1X 認証は、トランク ポート上、ダイナミック ポート上、および VLAN メンバーシップ ポリシー サーバ（VMPS）を介したダイナミックアクセス ポート割り当てではサポートされません。

VLAN 割り当てを設定するには、次の作業を行います。

ステップ 1　**network** キーワードを使用して AAA 認証をイネーブルにし、RADIUS サーバからのインターフェイス設定を可能にします。

ステップ 2　802.1X 認証をイネーブルにします。

ステップ 3　アクセス ポートでの 802.1X 認証を設定すると、VLAN 割り当て機能は自動的にイネーブルになります。

ステップ 4　RADIUS サーバにベンダー固有のトンネル属性を割り当てます。RADIUS サーバは次の属性をスイッチに返す必要があります。

- [64] Tunnel-Type = VLAN
- [65] Tunnel-Medium-Type = 802
- [81] Tunnel-Private-Group-ID = VLAN 名または VLAN ID

属性 [64] は、値 *VLAN*（タイプ 13）でなければなりません。属性 [65] は、値 *802*（タイプ 6）でなければなりません。属性 [81] は 802.1X 認証済みユーザに割り当てられた *VLAN 名*または *VLAN ID* を指定します。

VLAN 割り当てでの複数 VLAN および VLAN ユーザ分散

RADIUS が提供する VLAN 割り当てでは、複数の VLAN 間で 802.1X 認証済みユーザを分散してロード バランシングを実行できます。

以前のリリースでは、RADIUS サーバが認証中のユーザの割り当て用に提供できるのは、1 つの VLAN 名または ID でした。RADIUS サーバは、複数の VLAN 名と ID または複数の VLAN を含む VLAN グループの名前を提供できます。次の 2 つの方法のいずれかを使用して、異なる VLAN 間のユーザのロード バランシングを行います。

- 認証中のユーザに対する応答の一部として複数の VLAN ID または VLAN 名を送信するように、RADIUS サーバを設定します。802.1X VLAN ユーザ グループ機能は、特定の VLAN のユーザを追跡し、新たに認証されたユーザを、RADIUS が提供する VLAN ID の追加数が最も少ない VLAN に配置することで、ロード バランシングを実現します。

  「VLAN 割り当てを使用した 802.1X 認証」（P.83-17）に記載された手順を実行します（次の例外を除く）。

  属性 [81] Tunnel-Private-Group-ID は、複数の VLAN 名または VLAN ID を指定します。

- 複数の VLAN を含む VLAN グループを定義します。認証中のユーザに対する応答の一部として、VLAN ID の代わりに VLAN グループ名を提供するように、RADIUS サーバを設定します。提供された VLAN グループ名が定義済みの VLAN グループ名の中に見つかった場合、新たに認証されたユーザは、VLAN グループ内でユーザ追加数が最も少ない VLAN に配置されます。

  「VLAN 割り当てを使用した 802.1X 認証」（P.83-17）に記載された手順を実行します（次の例外を除く）。

  属性 [81] Tunnel-Private-Group-ID は、定義済みの VLAN グループ名を指定します。

詳細については、「VLAN ユーザ分散の設定」（P.83-45）を参照してください。

ゲスト VLAN を使用した 802.1X 認証

スイッチの各 802.1X ポートにゲスト VLAN を設定し、802.1X クライアント ソフトウェアをダウンロードするなど、802.1X に準拠していないクライアントに対して限定的なサービスを提供できます。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、スイッチが EAP 要求/アイデンティティ フレームに対する応答を受信しない場合や、EAPOL パケットがクライアントから送信されず、フォールバック認証方式がイネーブルになっていない場合に、スイッチはクライアントをゲスト VLAN に割り当てます。

さらに、スイッチは EAPOL パケット履歴を維持します。EAPOL パケットがリンクの存続時間内にインターフェイスで検出された場合、スイッチはそのインターフェイスに接続されているデバイスが 802.1X 対応サプリカントであると判断します。インターフェイスはゲスト VLAN ステートにはなりません。インターフェイスのリンク ステータスがダウンになると EAPOL パケット履歴はクリアされます。

dot1x guest-vlan supplicant グローバル コンフィギュレーション コマンドを使用して、EAPOL パケット履歴に関係なくインターフェイスをゲスト VLAN ステートに変更できるようにします。つまり、そのインターフェイスの前のホストが 802.1X 対応であっても、802.1X 非対応のホストがゲスト VLAN に割り当てられます。

（注）　インターフェイスがゲスト VLAN に変更されたあとで EAPOL パケットが検出された場合、インターフェイスは無許可ステートに戻り、802.1X 認証が再開されます。

ポートがゲスト VLAN に移動されると、802.1X 非対応クライアントは数に制限なくアクセスを許可されます。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。

802.1X ゲスト VLAN として動作する際、ポートに設定されたホスト モードに関係なく、ポートはマルチホスト モードで機能します。

RSPAN VLAN、プライベート プライマリ PVLAN、または音声 VLAN を除き、任意のアクティブ VLAN を 802.1X ゲスト VLAN として設定できます。ゲスト VLAN の機能は、内部 VLAN（ルーテッド ポート）またはトランク ポート上ではサポートされません。サポートされるのはアクセス ポートだけです。

スイッチは MAC 認証バイパスをサポートします。MAC 認証バイパスが 802.1X ポートでイネーブルの場合、スイッチは、EAPOL メッセージ交換を待機している間に 802.1X 認証がタイムアウトすると、クライアント MAC アドレスに基づいてクライアントを許可できます。スイッチは、802.1X ポート上のクライアントを検出したあとで、クライアントからのイーサネット パケットを待機します。スイッチは、MAC アドレスに基づいたユーザ名およびパスワードを持つ RADIUS-access/request フレームを認証サーバに送信します。認証に成功すると、スイッチはクライアントにネットワークへのアクセスを許可します。認証に失敗すると、スイッチはポートにゲスト VLAN を割り当てます（指定されていない場合）。

詳細については、「MAC 認証バイパスを使用した 802.1X 認証」（P.83-26）および「ゲスト VLAN の設定」（P.83-45）を参照してください。

制限付き VLAN を使用した 802.1X 認証

認証に失敗し、ゲスト VLAN にもアクセスできないクライアント向けに限定的なサービスを提供するために、スイッチ上の各 802.1X ポートに制限 VLAN（*認証失敗 VLAN* とも呼ばれます）を設定できます。これらのクライアントは 802.1X 準拠で、認証プロセスに失敗しているため別の VLAN にアクセスすることができません。制限付き VLAN を使用すると、認証サーバの有効なクレデンシャルを持っていないユーザ（通常、企業にアクセスするユーザ）に、サービスを制限したアクセスを提供できます。管理者は制限付き VLAN のサービスを制御できます。

（注）　両方のタイプのユーザに同じサービスを提供する場合、ゲスト VLAN と制限付き VLAN の両方を同じに設定できます。

この機能がないと、クライアントは認証の試行と失敗をいつまでも繰り返すことになり、ポートがスパニングツリーのブロッキング ステートのままになります。この機能を使用すると、指定された回数の認証試行のあと、ポートが制限 VLAN となるように設定することができます。

認証サーバはクライアントの認証試行回数をカウントします。RADIUS サーバが Access-Reject EAP 失敗または EAP パケットのない空の応答で応答すると、試行失敗カウントが増加します。このカウントが設定された最大認証試行数を超過すると、ポートは制限 VLAN に移動し、失敗試行カウンタはリセットされ、失敗したクライアントからの後続の EAPOL 開始メッセージは無視されます。

認証に失敗したユーザは、次にスイッチが再認証を試行するまで制限 VLAN に残ります。制限 VLAN のポートは、設定された間隔（デフォルトで 60 秒）で再認証を試行します。再認証に失敗した場合、ポートは制限 VLAN に残ります。再認証に成功した場合、ポートは設定された VLAN または RADIUS サーバによって送信される VLAN に移動します。再認証はディセーブルにすることができます。ディセーブルにすると、link down または EAP logoff イベントを受信しない限り、ポートの認証プロセスを再起動できません。クライアントがハブを介して接続される可能性がある場合、再認証をイネーブルのままにしておくことを推奨します。クライアントの接続をハブから切り離すと、ポートに link down や EAP logoff イベントが送信されない場合があります。

802.1X 制限 VLAN として動作する際、ポートに設定されたホスト モードに関係なく、ポートはシングルホスト モードで機能します。認証に失敗したクライアントだけが、そのポートでアクセスを許可されます。例外として、MDA モードで設定されたポートは、制限 VLAN からの音声サプリカントを認証できます。

RSPAN VLAN または音声 VLAN を除き、任意のアクティブ VLAN を 802.1X 制限 VLAN として設定することができます。制限 VLAN 機能はルーテッド ポートやトランク ポートではサポートされておらず、アクセス ポートでだけサポートされています。

この機能はポート セキュリティと連動します。ポートが認証されると、すぐに MAC アドレスがポート セキュリティに提供されます。ポート セキュリティがその MAC アドレスを許可しない場合、またはセキュア アドレス カウントが最大数に達している場合、ポートは無許可になり、errdisable ステートに移行します。

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 ガードなどの他のポート セキュリティ機能は、制限 VLAN 上で独立して設定できます。

詳細については、「制限付き VLAN の設定」（P.83-46）を参照してください。

アクセス不能認証バイパスを使用した 802.1X 認証

スイッチが設定済み RADIUS サーバに到達できず、ホストが認証できない場合、クリティカル ポートに接続されたホストにネットワーク アクセスできるようスイッチを設定できます。クリティカル ポートは、アクセス不能認証バイパス機能がイネーブルになっています。この機能はクリティカル認証または AAA 失敗ポリシーとも呼ばれます。

この機能がイネーブルの場合、スイッチはクリティカル ポートに接続されたホストの認証を行う際に、RADIUS サーバのステータスを確認します。利用可能なサーバが 1 つあれば、スイッチはホストを認証できます。ただし、すべての RADIUS サーバが利用不可能な場合は、スイッチはホストへのネットワーク アクセスを許可して、ポートを認証ステートの特別なケースであるクリティカル認証ステートにします。

アクセス不能認証バイパス機能の動作は、ポートの許可ステートにより異なります。

- クリティカル ポートに接続されているホストが認証を試行する際にポートが無許可ですべてのサーバが利用できない場合、スイッチはユーザ指定のクリティカル VLAN 内でポートをクリティカル認証ステートにします。
- ポートが許可済みで、再認証が行われた場合、スイッチは現在の VLAN（事前に RADIUS サーバにより割り当てられた）でクリティカル ポートをクリティカル認証ステートにします。
- 認証交換時に RADIUS サーバが使用不能になった場合、現在の交換はタイム アウトになり、スイッチは次の認証試行時にクリティカル ポートをクリティカル認証ステートにします。

ホストを認証できる RADIUS サーバが利用可能な場合、クリティカル認証ステートのすべてのクリティカル ポートは自動的に再認証されます。

アクセス不能認証バイパスは、次の機能と相互に作用します。

- ゲスト VLAN : アクセス不能認証バイパスは、ゲスト VLAN と互換性があります。ゲスト VLAN が 8021.x ポートでイネーブルの場合、この機能は次のように相互に作用します。
  - スイッチが EAP Request/Identity フレームへの応答を受信しないとき、または EAPOL パケットがクライアントによって送信されないときに、少なくとも 1 つの RADIUS サーバが使用できれば、スイッチはクライアントにゲスト VLAN を割り当てます。
  - すべての RADIUS サーバが利用不能でクライアントがクリティカル ポートに接続されている場合、スイッチはクライアントを認証して、ユーザ指定のクリティカル VLAN 内でクリティカル ポートをクリティカル認証ステートにします。

  - すべての RADIUS サーバが使用できず、クライアントがクリティカル ポートに接続されていない場合、ゲスト VLAN が設定されていても、スイッチはクライアントにゲスト VLAN を割り当てられません。
  - すべての RADIUS サーバが使用できず、クライアントがクリティカル ポートに接続されていて、すでにゲスト VLAN が割り当てられている場合、スイッチはそのポートをゲスト VLAN に保持します。
- 制限付き VLAN：ポートがすでに制限付き VLAN で許可されていて RADIUS サーバが使用できない場合、スイッチはクリティカル ポートを制限付き VLAN でクリティカル認証ステートにします。
- 802.1X アカウンティング：RADIUS サーバが利用不能な場合でもアカウンティングには影響しません。
- プライベート VLAN：プライベート VLAN ホスト ポートにアクセス不能認証バイパスを設定できます。アクセス VLAN は、セカンダリ VLAN でなければなりません。
- 音声 VLAN：アクセス不能認証バイパスは音声 VLAN と互換性がありますが、RADIUS 設定済み VLAN またはユーザ指定のアクセス VLAN は、音声 VLAN と異なっていなければなりません。
- Remote Switched Port Analyzer（RSPAN）：アクセス不能認証バイパスの RADIUS 設定またはユーザ指定のアクセス VLAN として RSPAN VLAN を指定しないでください。

音声 VLAN ポートを使用した 802.1X 認証

マルチ VLAN アクセス ポート（MVAP）は、2 つの VLAN に属しているポートです。音声 VLAN ポートは、ポートの音声トラフィックとデータ トラフィックを異なる VLAN に分離することのできる MVAP です。音声 VLAN ポートは、2 つの VLAN ID に関連付けされています。

- IP Phone との間で音声トラフィックをやりとりする音声 VLAN ID（VVID）。VVID は、ポートに接続された IP Phone を設定するために使用されます。
- 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。

ポートの許可ステートにかかわらず、IP Phone は音声トラフィックに対して VVID を使用します。これにより、802.1X 認証から独立して IP Phone が動作することができます。

シングル ホスト モードでは、IP Phone だけが音声 VLAN で許可されます。マルチ ホスト モードでは、サプリカントが PVID で認証された後、追加のクライアントがトラフィックを音声 VLAN 上で送信できます。マルチ ホスト モードがイネーブルの場合、サプリカント認証は PVID と VVID の両方に影響します。

IP Phone を認識するために、スイッチは、ポートの許可ステートに関係なく、ポート上の CDP トラフィックを許可します。リンクがあるとき、音声 VLAN ポートはアクティブになり、IP Phone からの最初の CDP メッセージを受け取るとデバイスの MAC アドレスが表示されます。Cisco IP Phone は、他のデバイスから受け取った CDP メッセージをリレーしません。その結果、複数の IP Phone が直列に接続されている場合、スイッチは直接接続されている 1 台の IP Phone のみを認識します。音声 VLAN ポートで 802.1X 認証がイネーブルの場合、スイッチは 2 ホップ以上離れた認識されない IP Phone からのパケットをドロップします。

802.1X 認証がポートでイネーブルになっている場合、音声 VLAN と同じポート VLAN を設定できません。

（注） 音声 VLAN が設定され、Cisco IP Phone が接続されているアクセス ポートで 802.1X 認証をイネーブルにした場合、Cisco IP Phone のスイッチへの接続が最大 30 秒間失われます。

音声 VLAN 設定の詳細については、第 18 章「Cisco IP Phone のサポート」を参照してください。

ポート セキュリティを使用した 802.1X 認証

シングルホスト モードまたはマルチホスト モードのいずれかで、802.1X ポートとポート セキュリティを設定できます。（**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にポート セキュリティも設定する必要があります）。ポート上でのポート セキュリティと 802.1X 認証をイネーブルにすると、802.1X 認証によってポートが認証され、ポート セキュリティによって、クライアントのものを含むすべての MAC アドレスのネットワーク アクセスが管理されます。その場合、802.1X ポートを介してネットワークにアクセス可能なクライアント数またはクライアント グループを制限することができます。

たとえば、スイッチにおいて、802.1X 認証とポート セキュリティの間には次のような相互作用があります。

- クライアントが認証され、ポート セキュリティ テーブルがいっぱいになっていない場合、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。追加されると、ポートが通常どおりアクティブになります。

  クライアントが認証されて手動でポート セキュリティが設定された場合、セキュア ホスト テーブル内のエントリは保証されます。

  クライアントが認証されてもポート セキュリティ テーブルがいっぱいの場合、セキュリティ違反が発生します。これは、セキュア ホストの最大数がスタティックに設定されているか、またはセキュア ホスト テーブルでのクライアントがエージング アウトした場合に発生します。クライアントのアドレスがエージング アウトした場合、そのクライアントのセキュア ホスト テーブル内でのエントリは他のホストに取って代わられます。

  いずれかのホストでセキュリティ違反が発生した場合、ポートは errdisable ステートになり、ただちにシャットダウンされます。

  セキュリティ違反発生時の動作は、ポート セキュリティ違反モードによって決まります。詳細については、「ポートでのポート セキュリティ違反モードの設定」（P.85-6）を参照してください。

- **no 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 コマンドを使用して、802.1X クライアント アドレスをポート セキュリティ テーブルから手動で削除する場合、**dot1x re-authenticate interface** *type slot/port* 特権 EXEC コマンドを使用して 802.1X クライアントを再認証する必要があります。
- 802.1X クライアントがログオフすると、ポートが未認証ステートに変更され、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 エントリがクリアされます。ここで通常の認証が実行されます。
- ポートが管理上のシャットダウン状態になると、ポートは未認証ステートになり、ダイナミック エントリはすべてセキュア ホスト テーブルから削除されます。
- ポート セキュリティと音声 VLAN は、シングルホスト モードまたはマルチホスト モードのいずれの場合でも 802.1X ポート上で同時に設定可能です。ポート セキュリティは、Voice VLAN Identifier（VVID）および Port VLAN Identifier（PVID）の両方に適用されます。

スイッチ上でポート セキュリティをイネーブルにする手順については、「ポート セキュリティの設定方法」（P.85-5）を参照してください。

ACL 割り当てとリダイレクト URL を使用した 802.1X 認証

概要

ACL およびリダイレクト URL などのホスト単位のポリシーは、802.1X、MAB、または Web ベース認証交換の終了時に RADIUS Access-Accept パケットで認証サーバ（AS）からスイッチにダウンロードできます。

ホスト単位のポリシーは、認証中に次のようにアクティブ化されます。

- ダウンロード可能 ACL（DACL）は Cisco Secure ACS に定義され、VSA を使用して ACS からスイッチにダウンロードされます。
- Filter-ID ACL はスイッチ上に定義され、ACL 名だけが RADIUS Filter-ID 属性を使用して AS からスイッチにダウンロードされます。
- リダイレクション URL と ACL 名は、VSA を使用して ACS からスイッチにダウンロードされます。リダイレクション ACL はスイッチ上に定義されます。

ホスト単位のポリシーの設定については、「DACL またはリダイレクト URL に関するスイッチの設定」（P.83-53）を参照してください。

Cisco Secure ACS を使用したダウンロード可能 ACL

ホスト認証が成功したあと、Cisco Secure ACS は、VSA を使用して ACL をスイッチにダウンロードすることができます。スイッチは DACL を、ホストが接続されているポート上のデフォルト ACL と結合します。DACL 定義は認証サーバ上にあるので、この機能により、集中型のポリシー管理が可能になります。

DACL の定義方法については、Cisco Secure ACS で次の 2 つの方法が提供されています。

- ダウンロード可能 IP ACL

  DACL のダウンロードは ACS の設定で [Assign IP ACL] を選択することでイネーブルになり、DACL は ACS の [Downloadable IP ACL Content] メニューで定義されます。DACL のサイズには制限がありません。

- ユーザ単位の ACL

  ACS は CiscoSecure-Defined-ACL [009\001 cisco-av-pair] VSA を使用して DACL を送信できます。DACL 全体が 1 つの RADIUS パケットで送信されるので、最大サイズは RADIUS パケットの最大サイズである 4096 バイトに制限されます。DACL は次の形式を使用して ACS 上に定義する必要があります。

  protocol:inacl#*sequence_number*=*ace*

  次に例を示します。

  ```
  ip:inacl#10=permit ip any 67.2.2.0 0.0.0.255
  ```

DACL の使用時には、次の注意事項が適用されます。

- すべての ACE の送信元アドレスは ANY として定義しておく必要があります。
- ポートの 802.1X ホスト モードが MDA またはマルチ認証の場合、DACL は認証済みホストの IP アドレスを送信元アドレスとして使用するように変更されます。ホスト モードがシングルホストまたはマルチホストの場合、送信元アドレスは ANY として設定され、ダウンロードされた ACL またはリダイレクトがポート上のすべての装置に適用されます。

- ホストの認証中に DACL が提供されなかった場合、ポートに設定されたデフォルトのスタティック ACL がホストに適用されます。音声 VLAN ポートでは、ポートのデフォルトのスタティック ACL だけが電話に適用されます。

Filter-ID ACL

ホスト認証が成功したあと、認証サーバは VSA ではなく、RADIUS Filter-Id 属性（属性 [11]）を使用して、次の形式でスイッチに拡張 ACL 名だけを提供することができます。

acl_name.in

末尾の「.in」は、ACL が受信方向に適用される必要があることを示します。

この方法では、ACL はスイッチ上に定義しておく必要があります。スイッチは、Filter-ID 属性値を、ローカルに設定された ACL の中で Filter-ID と同じ名前または番号を持つものと照合します（たとえば、Filter-ID=101.in は拡張番号付き ACL 101 と一致し、Filter-ID= guest.in は名前付き拡張 ACL「guest」と一致します）。その後は指定された ACL がポートに適用されます。ACL 定義はスイッチ上にあるので、この機能により、ポリシーのローカル バリエーションが可能になります。

Filter-ID ACL の使用時には、次の注意事項が適用されます。

- DACL 使用時の注意事項は Filter-ID ACL にも当てはまります。
- Filter-ID 属性は、番号（100 ～ 199、または 2000 ～ 2699）または名前になります。

リダイレクト URL

ホスト認証が成功したあと、Cisco Secure ACS は、VSA を使用して、認証済みホストからの HTTP または HTTPS 要求を代行受信およびリダイレクトするための情報をスイッチにダウンロードすることができます。ACS はリダイレクション ACL および URL をダウンロードします。ホストからの HTTP または HTTPS 要求が、ダウンロードされた ACL と一致した場合、ホストの Web ブラウザはダウンロードされたリダイレクション URL にリダイレクトされます。

ACS は次の cisco-av-pair VSA を使用してリダイレクションを設定します。

- url-redirect-acl

  この AV ペアは、リダイレクトする HTTP または HTTPS トラフィックを指定する ACL の名前または番号を示します。ACL はスイッチ上に定義しておく必要があり、送信元アドレスは ANY として定義しておく必要があります。この結果、リダイレクト ACL 内の許可エントリに一致するトラフィックがリダイレクトされます。

- url-redirect

  この AV ペアには、Web ブラウザのリダイレクト先となる HTTP または HTTPS URL が含まれます。

ACL のスタティック共有

複数のインターフェイスに同じ PACL および VLAN ベース機能がある場合、スタティック共有機能により、同じ ACL セットを使用するすべてのポートの TCAM 内の PACL および継承された VLAN ベース機能の ACL のコピーが 1 つ格納され、より多くの ACL 用に TCAM の領域を開放します。次のいずれかのイベントが発生したときに、スイッチは自動的にスタティック共有用に設定またはイネーブルにされたすべてのインターフェイスを評価します。

- インターフェイスが設定されたとき。
- インターフェイス上でステートの変化が発生したとき。

次の注意事項および制約事項を考慮してください。

- スタティック共有は、IPv6 をサポートするように設定されたインターフェイスではサポートされません。
- スタティック共有は NAC または 802.1X DACL 機能が設定されたアクセス モードのスイッチ ポートでだけサポートされます。
- スタティック共有は、QoS（VLAN ベースの QoS を除く）がイネーブルになっているスイッチ ポートではサポートされません。
- 802.1X を DACL とともに使用する際には、ポートが認証サーバの応答によってダイナミックに設定されたときにスタティック共有の評価が開始されるのを回避するために、**platform hardware acl dynamic setup static** コマンドを実行することを推奨します。スタティック共有の評価は、ポート/ホストのリンクアップ時間に影響を及ぼす場合があります。
- フォールバック認証がアクティブになっている 802.1X インターフェイスは、フォールバック認証がイネーブルでない、またはアクティブでないインターフェイスと一緒にスタティック共有グループを形成できません。

ポート ディスクリプタを使用した 802.1X 認証

RADIUS サーバ上で Cisco ベンダー固有属性（VSA）**aaa:supplicant-name** を設定すると、説明文を 802.1X クライアントの認証情報と関連付けることができます。ポート上でクライアントの 802.1X 認証が正常に進行している間に、スイッチは RADIUS サーバから Access-Accept パケットの一部として説明情報を受信し、ポートに対して **show interface users** コマンドが入力されたときに、この情報を表示します。ポートが複数の認証済みホストをサポートするモードの場合は、すべての認証済みホストの識別情報がポートの説明とともに表示されます。

MAC 認証バイパスを使用した 802.1X 認証

MAC 認証バイパス機能を使用し、クライアント MAC アドレス（図 83-4（P.83-12）を参照）に基づいてクライアントを許可するようにスイッチを設定できます。たとえば、プリンタなどの装置に接続されている 802.1X ポートで、この機能をイネーブルにすることができます。

クライアントからの EAPOL 応答の待機中に 802.1X 認証がタイムアウトした場合、スイッチは MAC 認証バイパスを使用してクライアントを許可しようとします。

MAC 認証バイパス機能が 802.1X ポートでイネーブルの場合、スイッチはクライアント ID として MAC アドレスを使用します。認証サーバには、ネットワーク アクセスを許可されたクライアント MAC アドレスのデータベースがあります。スイッチは、802.1X ポート上のクライアントを検出したあとで、クライアントからのイーサネット パケットを待機します。スイッチは、MAC アドレスに基づいたユーザ名およびパスワードを持つ RADIUS-access/request フレームを認証サーバに送信します。認証に成功すると、スイッチはクライアントにネットワークへのアクセスを許可します。許可が失敗した場合、ゲスト VLAN が設定されていれば、スイッチはポートをゲスト VLAN に割り当てます。

リンクの存続時間内に EAPOL パケットがインターフェイス上で検出された場合、スイッチは、そのインターフェイスに接続されているデバイスが 802.1X 対応サプリカントであることを確認し、（MAC 認証バイパス機能ではなく）802.1X 認証を使用してインターフェイスを認証します。インターフェイスのリンク ステータスがダウンした場合、EAPOL 履歴はクリアされます。

スイッチがすでに MAC 認証バイパスを使用してポートを許可し、802.1X サプリカントを検出している場合、スイッチはポートに接続されているクライアントを許可します。再認証が発生した際、Termination-Action RADIUS 属性が DEFAULT であるために前のセッションが終了した場合、スイッチは 802.1X 認証を優先再認証プロセスとして使用します。

MAC 認証バイパスで許可されたクライアントを再認証することができます。再認証プロセスは、802.1X で認証されたクライアントと同様です。再認証中に、ポートは前に割り当てられた VLAN に残ります。再認証に成功した場合、スイッチはポートを同じ VLAN 内に保持します。再認証に失敗した場合、ゲスト VLAN が設定されていればポートにゲスト VLAN を割り当てます。

再認証が Session-Timeout RADIUS 属性（属性 [27]）と Termination-Action RADIUS 属性（属性 [29]）に基づいており、Termination-Action RADIUS 属性（属性 [29]）のアクションが初期化の場合、（属性値は DEFAULT）、MAC 認証バイパス セッションが終了して、再認証中に接続が切断されます。MAC 認証バイパスがイネーブルで 802.1X 認証がタイムアウトした場合、スイッチは MAC 認証バイパス機能を使用して再許可を開始します。これらの AV ペアの詳細については、RFC 3580「IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines」を参照してください。

MAC 認証バイパスは、次の機能と相互に作用します。

- 802.1X 認証：802.1X 認証がポートでイネーブルの場合にだけ、MAC 認証バイパスをイネーブルにできます。
- ゲスト VLAN：クライアントの MAC アドレス ID が無効な場合、ゲスト VLAN が設定されていれば、スイッチは VLAN にクライアントを割り当てます。
- 制限付き VLAN：802.lx ポートに接続されているクライアントが MAC 認証バイパスで認証されている場合には、この機能はサポートされません。
- ポート セキュリティ：「ポート セキュリティを使用した 802.1X 認証」（P.83-23）を参照してください。
- 音声 VLAN：「音声 VLAN ポートを使用した 802.1X 認証」（P.83-22）を参照してください。
- VLAN メンバーシップ ポリシー サーバ（VMPS）：802.1X および VMPS は相互に排他的です。
- プライベート VLAN：クライアントをプライベート VLAN に割り当てられます。
- Network Admission Control（NAC）レイヤ 2 IP 検証：例外リスト内のホストを含む、802.1X ポートが MAC 認証バイパスで認証されたあとにこの機能が有効になります。

Network Admission Control レイヤ 2 IEEE 802.1X 検証

Network Admission Control（NAC）レイヤ 2 IEEE 802.1X 検証は、デバイスにネットワーク アクセスを許可する前に、エンドポイント システムまたはクライアントのウイルス対策の状態または*ポスチャ*を確認します。NAC レイヤ 2 IEEE 802.1X 検証は、認証済みポートを指定の VLAN に割り当てることでポリシーの適用を実行します。これにより、レイヤ 2 で不適切なポスチャのホストを区分および隔離します。

NAC レイヤ 2 IEEE 802.1X 検証の設定は、RADIUS サーバ上でポスチャ トークンを設定する必要があることを除いて、802.1X ポートベース認証の設定に似ています。**show dot1x** 特権 EXEC コマンドを使用して、クライアントのポスチャを表示する NAC ポスチャ トークンを表示することができます。NAC レイヤ 2 IEEE 802.1X 検証の設定については、「NAC レイヤ 2 IEEE 802.1X 検証の設定」（P.83-51）を参照してください。

NAC の詳細については、『*Network Admission Control Software Configuration Guide*』を参照してください。

NAC エージェントレス監査のサポート

MAB サポートが Cisco NAC 監査アーキテクチャに追加されています。これは、Cisco Trust Agent（CTA）を実行しておらず、NAC クエリーに応答できないクライアントのアンチウイルス ポスチャをチェックするために外部監査サーバを使用するものです。エージェントレス クライアントのアンチウイルス ポスチャを監査およびレポートするためには、NAC 監査サーバはクライアントの IP アドレス

と、そのクライアントがスイッチに接続するための一意のセッション ID を持っている必要があります。エージェントレス クライアントのための NAC 監査アーキテクチャをサポートするには、スイッチはクライアントの IP アドレスをスヌーピングし、エージェントレス クライアント用に一意のセッション ID を作成して割り当て、この情報を RADIUS サーバに渡して NAC 監査サーバと共有できるようにする必要があります。

MAB はレイヤ 2 で動作するので、MAB オーセンティケータは通常、サプリカントの IP アドレスを認識していません。また、サプリカントが最初にオーセンティケータと接触する際、サプリカントには IP アドレスがない可能性があります。DHCP が割り当てた IP アドレスを必要とするサプリカントは、認証の前に DHCP サーバへのアクセスを許可される必要があります。MAB オーセンティケータがサプリカントの IP アドレスを学習できるようにするには、スイッチ上で ARP と DHCP スヌーピングをイネーブルにする必要があります。IP アドレスと一意のセッション ID 情報を NAC 監査サーバと共有できるようにするには、特定の RADIUS 属性の送信をイネーブルにする必要があります。「NAC エージェントレス監査のサポートの設定」（P.83-52）を参照してください。

クライアントの IP アドレスと一意のセッション ID は、次の RADIUS *cisco-av-pair* ベンダー固有属性（VSA）を使用して、RADIUS Access-Request および Access-Accept 内で共有されます。

- Cisco-AVPair="identity-request=*ip-address*"

  ip-address は、ARP または DHCP スヌーピングを使用してスイッチが取得したクライアントの IP アドレスです。

- Cisco-AVPair="audit-session-id=*audit session id string*"

  audit session id string は、スイッチによってネットワーク アクセス サーバ（NAS）の IP アドレス、セッション カウント、およびセッション開始タイムスタンプから引き出された一意の 96 ビット ID の UTF-8 エンコーディングです。

Wake-on-LAN を使用した 802.1X 認証

802.1X 認証と Wake-on-LAN（WoL）機能では、スイッチがマジック パケットと呼ばれる特別なイーサネット フレームを受信したときに、休止状態の PC を起動することができます。この機能は、管理者が休止状態のシステムへ接続しなければならない場合に役立ちます。

WoL を使用するホストが 802.1X ポートを介して接続されていてホストの電源がオフの場合、802.1X ポートは無許可になります。無許可になったポートは EAPOL パケットしか送受信できないため、WoL マジック パケットはホストに届きません。さらに PC が休止状態になると、PC が認証されなくなるため、スイッチ ポートは閉じたままになります。

スイッチが WoL 機能を有効にした 802.1X 認証を使用している場合、スイッチはマジック パケットを含むトラフィックを無許可の 802.1X ポートに転送します。ポートが無許可の間、スイッチは EAPOL パケット以外の入力トラフィックをブロックし続けます。ホストはパケットを受信できますが、パケットをネットワーク内にある他のデバイスに送信できません。

（注）　PortFast がポートでイネーブルになっていないと、そのポートは強制的に双方向ステートになります。

authentication 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 ステートに変わります。ポートは、ホストにパケットを送信できますが、受信はできません。

authentication 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、そのポートのアクセスが双方向で制御されます。ポートは、ホストとの間でパケットを送受信しません。

MAC 移動

あるスイッチ ポートで MAC アドレスが認証されると、そのアドレスは同じスイッチの別の認証マネージャ対応ポートでは許可されません。スイッチが同じ MAC アドレスを別の認証マネージャ対応ポートで検出すると、そのアドレスは許可されなくなります。

場合によっては、MAC アドレスを同じスイッチ上のポート間で移動する必要があります。たとえば、認証ホストとスイッチ ポート間に別のデバイス（ハブまたは IP Phone など）がある場合、ホストをデバイスから接続して、同じスイッチの別のポートに直接接続する必要があります。

デバイスが新しいポートで再認証されるように、MAC 移動をグローバルにイネーブルにできます。ホストが別のポートに移動すると、最初のポートのセッションが削除され、ホストは新しいポートで再認証されます。

MAC アドレスがあるポートから別のポートに移動すると、スイッチは元のポートで認証済みセッションを終了し、新しいポートで新しい認証シーケンスを開始します。ポート セキュリティの動作は、MAC 移行を設定したときと同じです。

（注）
- MAC 移動はすべてのホスト モードでサポートされます。（認証ホストは、ポートでイネーブルにされているホスト モードに関係なく、スイッチの任意のポートに移動できます）。
- MAC 移動はポート セキュリティでサポートされます。
- MAC 移動の機能は、音声およびデータ ホストの両方に適用されます。
- オープン認証モードでは、MAC アドレスは、新しいポートでの許可を必要とせずに、元のポートから新しいポートへただちに移動します。

詳細については、「MAC 移動のイネーブル化」（P.83-54）を参照してください。

MAC 置換

MAC 置換機能は、ホストが、別のホストがすでに認証済みであるポートに接続しようとすると発生する違反に対処するように設定できます。

（注）
- Mac 置換機能は、マルチ認証モードで違反がトリガーされないので、そのモードのポートではサポートされません。
- Mac 置換機能は、マルチ ホスト モードでは最初のホストだけが認証を必要とするため、そのモードのポートではサポートされていません。

replace キーワードを指定して **authentication violation** インターフェイス コンフィギュレーション コマンドを設定すると、マルチドメイン モードのポートでの認証プロセスは、次のようになります。

- 既存の認証済み MAC アドレスを使用するポートで新しい MAC アドレスが受信されます。
- 認証マネージャは、ポート上の現在のデータ ホストの MAC アドレスを、新しい MAC アドレスで置き換えます。
- 認証マネージャは、新しい MAC アドレスに対する認証プロセスを開始します。
- 認証マネージャによって新しいホストが音声ホストであると判断された場合、元の音声ホストは削除されます。

ポートがオープン認証モードになっている場合、MAC アドレスはただちに MAC アドレス テーブルに追加されます。

詳細については、「MAC 置換のイネーブル化」（P.83-55）を参照してください。

Network Edge Access Topology（NEAT）を使用した 802.1x サプリカントおよびオーセンティケータ スイッチ

NEAT は、ワイヤリング クローゼットの外側の領域（会議室など）に ID を拡大します。これにより、任意のタイプのデバイスをポートで認証できます。

- 802.1x スイッチ サプリカント：802.1x サプリカント機能を使用することで、別のスイッチのサプリカントとして機能するようにスイッチを設定できます。この設定は、たとえば、スイッチがワイヤリング クローゼット外にあり、トランク ポートを介してアップストリーム スイッチに接続される場合に役に立ちます。802.1x スイッチ サプリカント機能を使用して設定されたスイッチは、セキュアな接続のためにアップストリーム スイッチで認証します。

  サプリカント スイッチが認証に成功すると、ポート モードがアクセスからトランクに変更されます。

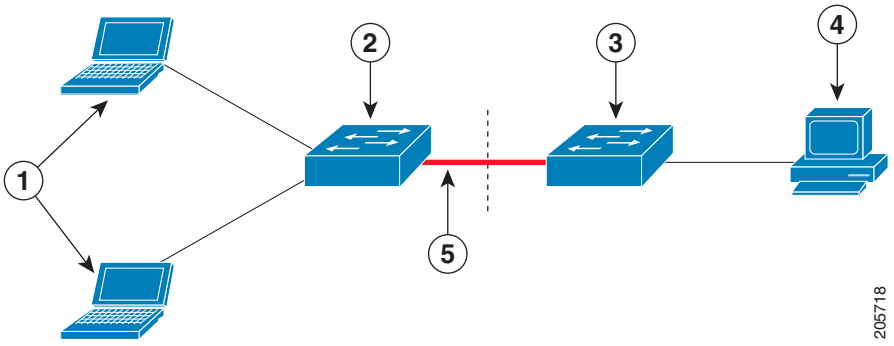
- アクセス VLAN は、オーセンティケータ スイッチで設定されている場合、認証が成功した後にトランク ポートのネイティブ VLAN になります。

1 つ以上のサプリカント スイッチに接続するオーセンティケータ スイッチ インターフェイスで MDA または multiauth モードをイネーブルにできます。オーセンティケータ スイッチのインターフェイスで、マルチホスト モードがサポートされないため、MDA モードでは音声クライアントはサポートされません。

すべてのホスト モードで機能するように **dot1x supplicant force-multicast** グローバル コンフィギュレーション コマンドを Network Edge Access Topology（NEAT）のサプリカント スイッチで使用します。

- ホスト許可：許可済み（サプリカントでスイッチに接続する）ホストからのトラフィックだけがネットワークで許可されます。これらのスイッチは、Client Information Signalling Protocol（CISP）を使用して、サプリカント スイッチに接続する MAC アドレスをオーセンティケータ スイッチに送信します（図 83-7 を参照してください）。
- 自動イネーブル化：オーセンティケータ スイッチでのトランク コンフィギュレーションを自動的にイネーブル化します。これにより、サプリカント スイッチから着信する複数の VLAN のユーザ トラフィックが許可されます。ACS で cisco-av-pair を *device-traffic-class=switch* として設定します （この設定は *group* または *user* 設定で行うことができます）。

図 83-7　CISP を使用したオーセンティケータまたはサプリカント スイッチ



1	ワークステーション（クライアント）	2	サプリカント スイッチ（ワイヤリング クローゼット外）
3	オーセンティケータ スイッチ	4	Access Control Server（ACS）
5	トランク ポート		

詳細については、「NEAT オーセンティケータとサプリカント スイッチの設定」（P.83-55）を参照してください。

802.1X ポートベース認証のデフォルト設定

機能	デフォルト設定
802.1X イネーブル ステートの切り換え	ディセーブル
ポート単位の 802.1X イネーブル ステート	ディセーブル（force-authorized） ポートはクライアントとの 802.1X ベース認証を行わずに、通常のトラフィックを送受信します。
AAA	ディセーブル
RADIUS サーバ • IP アドレス • UDP 認証ポート • キー	 • 指定なし • 1812 • 指定なし
ホスト モード	シングル ホスト モード
制御方向	双方向制御
定期的な再認証	ディセーブル
再認証の間隔（秒）	3600 秒
再認証の回数	2 回（ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再開する回数）
待機時間	60 秒（スイッチがクライアントとの認証情報の交換に失敗した後、待機状態を続ける秒数）
再送信時間	30 秒（スイッチが要求を再送信するまでに、EAP 要求/アイデンティティ フレームに対するクライアントからの応答を待機する秒数）
最大再送信回数	2 回（スイッチが認証プロセスを再開する前に、EAP 要求/アイデンティティ フレームを送信する回数）
クライアント 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へ中継する場合、スイッチがクライアントへ要求を再送信するまでに、応答を待機する時間）。
認証サーバ タイムアウト時間	30 秒（クライアントからの応答を認証サーバへ中継する場合、スイッチが認証サーバへ応答を再送信するまでに、返答を待機する時間）。
無活動タイムアウト	ディセーブル
ゲスト VLAN	指定なし

機能	デフォルト設定
アクセス不能認証バイパス	ディセーブル
制限付き VLAN	指定なし
オーセンティケータ（スイッチ）モード	指定なし
MAC 認証バイパス	ディセーブル **（注）** EAP を使った MAC 認証バイパスがインターフェイス上でイネーブルになっている場合は、その後にインターフェイス上で実行される **default interface** コマンドによってディセーブルになることはありません。

802.1X ポートベース認証の設定方法

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、AAA をイネーブルにして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、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から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、定義された方式をすべて試し終わるまで繰り返されます。このサイクルのいずれかの時点で認証が失敗した場合には、認証プロセスは中止され、その他の認証方式が試みられることはありません。

VLAN 割り当てを可能にするには、AAA 認証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してスイッチを設定する必要があります。

802.1X AAA 処理は、次のようになります。

1. ユーザがスイッチのポートに接続します。
2. 認証が実行されます。
3. RADIUS サーバ設定に基づいて、VLAN 割り当てが適宜イネーブルになります。
4. スイッチが開始メッセージをアカウンティング サーバに送信します。
5. 必要に応じて再認証が実行されます。
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。
7. ユーザがポートから切断します。
8. スイッチが停止メッセージをアカウンティング サーバに送信します。

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	`Router(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 2	`Router(config)# aaa authentication dot1x {default} method1 [method2...]`	802.1x ポート ベース認証方式リストを作成します。 **aaa authentication** コマンドに名前付きリストが指定されていない場合に使用す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状況で使用され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。 *method1* には、**group radius** キーワードを入力して、認証用のすべての RADIUS サーバ リストを使用できるようにします。 **group radius** キーワード以外にもコマンドラインのヘルプ ストリングに表示されますが、サポートされていません。
ステップ 3	`Router(config)# dot1x system-auth-control`	802.1x ポートベースの認証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 4	`Router(config)# aaa authorization network {default} group radius`	（任意）VLAN 割り当てなど、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 RADIUS 許可を使用するようにスイッチを設定します。
ステップ 5	`Router(config)# radius-server host ip-address`	RADIUS サーバの IP アドレスを指定します。
ステップ 6	`Router(config)# radius-server key string`	スイッチと RADIUS サーバ上で動作する RADIUS デーモンとの間で使用される認証および暗号キーを指定します。
ステップ 7	`Router(config)# interface type slot/port`	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 8	`Router(config-if)# switchport mode access`	前の手順で RADIUS サーバを設定した場合に限り、ポートをアクセス モードに設定します。
ステップ 9	`Router(config-if)# authentication port-control auto`	インターフェイスでのポートベース認証をイネーブルにします。 コマンドの **no** 形式を使用すると、インターフェイスでのポートベース認証がディセーブルになります。
ステップ 10	`Router(config-if)# dot1x pae authenticator`	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 11	`Router(config)# end`	特権 EXEC モードに戻ります。

次に、ギガビット イーサネット ポート 5/1 で AAA と 802.1X をイネーブルにする例を示します。

```
Router(config)# aaa new-model
Router(config)# aaa authentication dot1x default group radius
Router(config)# dot1x system-auth-control
Router(config)# interface gigabitethernet 5/1
Router(config-if)# authentication port-control auto
Router(config-if)# dot1x pae authenticator
Router(config-if)# end
```

次に、設定を確認する例を示します。

```
Router# show dot1x all

Sysauthcontrol              Enabled
Dot1x Protocol Version            2

Dot1x Info for GigabitEthernet1/7
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
```

スイッチ/RADIUS サーバ間通信の設定

RADIUS セキュリティ サーバは、次のいずれかによって識別されます。

- ホスト名
- ホスト IP アドレス
- ホスト名と特定の UDP ポート番号
- IP アドレスと特定の UDP ポート番号

IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、同一 IP アドレスのサーバ上にある複数の UDP ポートに RADIUS 要求を送信できるようになります。同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（たとえば認証など）を設定した場合、2 番めに設定されたホスト エントリは、最初に設定されたホスト エントリのフェールオーバー バックアップとして動作します。RADIUS ホスト エントリは、設定した順序に従って試行されます。

RADIUS サーバ パラメータを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`Router(config)# ip radius source-interface` *interface_name*	RADIUS パケットが、指定されたインターフェイスの IP アドレスを含むように指定します。
ステップ 2	`Router(config)# radius-server host` {*hostname* | *ip_address*}	スイッチに RADIUS サーバ ホスト名や IP アドレスを設定します。 複数の RADIUS サーバを使用する場合は、このコマンドを再度入力します。
ステップ 3	`Router(config)# radius-server key` *string*	スイッチと、RADIUS サーバで動作する RADIUS デーモン間で使用される認証および暗号キーを設定します。

- *hostname* または *ip_address* には、リモート RADIUS サーバのホスト名または IP アドレスを指定します。
- 別のコマンドラインには、**key** *string* を指定します。
- **key** *string* には、スイッチと、RADIUS サーバ上で動作する RADIUS デーモンとの間で使用する認証および暗号キーを指定します。キーは、RADIUS サーバで使用する暗号キーに一致するテキスト ストリングでなければなりません。
- **key** *string* を指定する場合、キーの途中および末尾のスペースが利用されます。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。キーは RADIUS デーモンで使用する暗号に一致している必要があります。
- **radius-server host** グローバル コンフィギュレーション コマンドを使用して、タイムアウト、再送信回数、暗号キーの値を、すべての RADIUS サーバにグローバルに設定できます。これらのオプションをサーバ単位で設定するには、**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。

（注）　RADIUS サーバ上でも、いくつかの値を設定する必要があります。これらの設定値としては、スイッチの IP アドレス、およびサーバとスイッチの双方で共有するキー ストリングがあります。詳細については、RADIUS サーバのマニュアルを参照してください。

次に、スイッチで RADIUS サーバ パラメータを設定する例を示します。

```
Router(config)# ip radius source-interface Vlan80
Router(config)# radius-server host 172.120.39.46
```

```
Router(config)# radius-server key rad123
```

802.1X オーセンティケータのホスト モードの設定

802.1X 対応ポートは、「802.1X ホスト モード」（P.83-13）の説明にあるように、単一クライアントまたは複数クライアントに対してアクセスを許可することができます。

802.1X 許可ポートのホスト 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	`Router(config)# interface type slot/port`	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 2	`Router(config-if)# authentication port-control auto`	インターフェイスでのポートベース認証をイネーブルにします。
ステップ 3	`Router(config-if)# dot1x pae authenticator`	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 4	`Router(config-if)# authentication host-mode host_mode`	ホスト モードを設定します。*host_mode* の値は次のとおりです。 • **single-host**：許可ポートで単一の認証済みホスト（クライアント）を許可します。 • **multi-host**：1 つのクライアントが認証されると、許可ポートで複数のクライアントを許可します。 • **multi-domain**：単一の IP Phone と単一のデータ クライアントを許可ポートで独立して認証できるようにします。 • **multi-auth**：単一の IP Phone と複数のデータ クライアントを許可ポートで独立して認証できるようにします。
ステップ 5	`Router(config-if)# authentication open`	（任意）認証前オープン アクセスをイネーブルにします。
ステップ 6	`Router(config-if)# end`	特権 EXEC モードに戻ります。

次に、ギガビット イーサネット インターフェイス 5/1 で 802.1X をイネーブルにし、複数のホストを許可する例を示します。

```
Router(config)# interface gigabitethernet 5/1
Router(config-if)# authentication port-control auto
Router(config-if)# dot1x pae authenticator
Router(config-if)# authentication host-mode multi-host
```

フォールバック認証のイネーブル化

マルチ認証モードのポートでは、MAB と Web ベース認証のいずれかまたは両方を、802.1X 以外のホスト（EAPOL に応答しないホスト）用のフォールバック認証方式として設定できます。認証方式の順序とプライオリティを設定します。

MAB の設定方法の詳細については、「MAC 認証バイパスの設定」（P.83-50）を参照してください。

Web ベース認証の設定方法の詳細については、第 84 章「Web ベース認証」を参照してください。

フォールバック認証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	`Router(config)# ip admission name rule-name proxy http`	Web ベース認証の認証ルールを設定します。
ステップ 2	`Router(config)# fallback profile profile-name`	Web ベース認証のフォールバック プロファイルを作成します。
ステップ 3	`Router(config-fallback-profile)# ip access-group rule-name in`	Web ベース認証前にネットワーク トラフィックに適用するデフォルト ACL を指定します。
ステップ 4	`Router(config-fallback-profile)# ip admission name rule-name`	IP 許可ルールをプロファイルに関連付け、Web ベース認証で接続するクライアントがこのルールを使用するように指定します。
ステップ 5	`Router(config-fallback-profile)# 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	`Router(config)# interface type slot/port`	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 7	`Router(config-if)# authentication port-control auto`	ポートで認証をイネーブルにします。
ステップ 8	`Router(config-if)# authentication order method1 [method2] [method3]`	（任意）使用される認証方式のフォールバック順序を指定します。*method* の 3 つの値のデフォルト順序は、**dot1x**、**mab**、および **webauth** です。また、指定した順序は、最大から最小まで、再認証の方式の相対的なプライオリティも決定します。
ステップ 9	`Router(config-if)# authentication priority method1 [method2] [method3]`	（任意）使用される認証方式の相対プライオリティを上書きします。*method* の 3 つの値は、プライオリティのデフォルト順序で、**dot1x**、**mab**、および **webauth** です。
ステップ 10	`Router(config-if)# authentication event fail action next-method`	認証が失敗した場合には設定された次の認証方式が使用されるように指定します。
ステップ 11	`Router(config-if)# mab [eap]`	MAC 認証バイパスをイネーブルにします。任意の **eap** キーワードは、RADIUS 認証中に EAP 拡張機能が使用されるように指定します。
ステップ 12	`Router(config-if)# authentication fallback profile-name`	指定されたプロファイルを使用した Web ベースの認証をイネーブルにします。
ステップ 13	`Router(config-if)# authentication violation [shutdown | restrict]`	（任意）セキュリティ違反が発生した場合のポートのディスポジションを設定します。デフォルトでは、ポートはシャットダウンされます。**restrict** キーワードが設定した場合、ポートはシャットダウンされませんが、違反した MAC アドレスに対するトラップ エントリが設定され、その MAC アドレスからのトラフィックはドロップされます。
ステップ 14	`Router(config-if)# authentication timer inactivity {seconds | server}`	（任意）MAB および 802.1X に対する無活動タイムアウト値を設定します。デフォルトでは、ポートに対する無活動の長さはディセーブルにされています。 • *seconds*：無活動タイムアウトの期間を指定します。範囲は 1 ～ 65535 秒です。 • server：無活動タイムアウト期間の値が認証サーバから取得されるように指定します。

	コマンド	目的
ステップ 15	`Router(config-if)# authentication timer restart seconds`	（任意）無許可ポートの認証を試行するために認証プロセスを再開するまでの期間を指定します。 • *seconds*：再起動期間を指定します。範囲は 1 ～ 65535 秒です。
ステップ 16	`Router(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 17	`Router(config)# ip device tracking`	Web ベース認証に必要な IP デバイス トラッキング テーブルをイネーブルにします。
ステップ 18	`Router(config)# exit`	特権 EXEC モードに戻ります。

次に、MAB への 802.1X フォールバックをイネーブルにし、続いて、802.1X がイネーブルにされたポートで Web ベース認証をイネーブルにする例を示します。

```
Router(config)# ip admission name rule1 proxy http
Router(config)# fallback profile fallback1
Router(config-fallback-profile)# ip access-group default-policy in
Router(config-fallback-profile)# ip admission rule1
Router(config-fallback-profile)# exit
Router(config)# interface gigabit1/1
Router(config-if)# switchport mode access
Router(config-if)# authentication port-control auto
Router(config-if)# dot1x pae authenticator
Router(config-if)# authentication order dot1x mab webauth
Router(config-if)# mab eap
Router(config-if)# authentication fallback fallback1
Router(config-if)# exit
Router(config)# ip device tracking
Router(config)# exit
```

定期的な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。再認証を行うまでの期間を手動で指定するか、RADIUS サーバで指定されたセッションタイムアウト期間を使用することができます。期間を指定せずに再認証をイネーブルにする場合、再認証を行う間隔は 3600 秒です。

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	`Router(config)# interface type slot/port`	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 2	`Router(config-if)# authentication periodic`	クライアントの定期的な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に設定されています。

	コマンド	目的
ステップ 3	`Router(config-if)# authentication timer reauthenticate [seconds | server]`	以下のキーワードを使用して再認証の間隔（秒）を指定します。 • *seconds* : 1 ～ 65535 の範囲で秒数を設定します。デフォルトは 3600 秒です。 • **server** : Session-Timeout RADIUS 属性（属性 [27]）および Termination-Action RADIUS 属性（属性 [29]）の値に基づいて秒数を設定します。 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 4	`Router(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。

```
Router(config)# interface gigabitethernet 5/1
Router(config-if)# authentication periodic
Router(config-if)# authentication timer reauthenticate 4000
```

入力を確認します。

```
Router# show dot1x interface type slot/port
```

手動によるポート接続クライアントの再認証

特定のポートに接続するクライアントを手動で再認証するには、次の作業を行います。

コマンド	目的
`Router# dot1x re-authenticate interface type slot/port`	ポートに接続するクライアントを手動で再認証します。 **（注）** 再認証は、すでに認証されているポートのステータスには影響しません。

次に、ギガビット イーサネット ポート 5/1 に接続されているクライアントを手動で再認証する例を示します。

```
Router# dot1x re-authenticate interface gigabitethernet 5/1
```

入力を確認します。

```
Router# show dot1x all
```

ポート接続クライアント認証の初期化

ポートに接続されているクライアントの認証を初期化するには、次の作業を行います。

コマンド	目的
Router# **dot1x initialize interface** *type slot/port*	ポートに接続されているクライアントの認証を初期化します。 **（注）** 認証の初期化により、既存の認証をディセーブルにしてから、ポートに接続されているクライアントを認証します。

次に、ギガビット イーサネット ポート 5/1 に接続されているクライアントに対する認証を初期化する例を示します。

```
Router# dot1x initialize interface gigabitethernet 5/1
```

入力を確認します。

```
Router# show dot1x all
```

802.1X クライアント情報のグローバルな削除

スイッチ上のすべてのインターフェイスからすべての既存サプリカントを完全に削除するには、次の作業を行います。

コマンド	目的
Router# **clear dot1x all**	すべてのポートに接続されているすべてのクライアントの 802.1X クライアント情報を削除します。

次に、すべてのポートに接続されているすべてのクライアントの 802.1X クライアント情報を削除する例を示します。

```
Router# clear dot1x all
```

インターフェイスからの 802.1X クライアント情報の削除

すべての既存サプリカントをスイッチのいずれかのインターフェイスまたはすべてのインターフェイスから完全に削除するには、次の作業を行います。

コマンド	目的
Router# **clear dot1x interface** *type slot/port*	指定したポートに接続されているクライアントの 802.1X クライアント情報を削除します。

次に、ギガビット イーサネット ポート 5/1 に接続されているクライアントの 802.1X クライアント情報を削除する例を示します。

```
Router# clear dot1x interface gigabitethernet 5/1
```

認証セッションのクリア

すべての認証セッションまたは選択した認証セッションをクリアするには、次の作業を行います。

コマンド	目的
Router# **clear authentication sessions** [**handle** *handle*] [**interface** *interface*] [**mac** *mac*] [**method** *method*]	現在の認証セッションをクリアします。オプションを指定しない場合、現在のすべてのアクティブ セッションがクリアされます。キーワードを追加したり組み合わせたりすることで、特定のセッションや一部のセッションをクリアすることができます。

次に、ギガビット イーサネット ポート 5/1 に接続されているすべての MAB 認証セッションをクリアする例を示します。

```
Router# clear authentication sessions interface gigabitethernet 5/1 method mab
```

802.1X タイムアウトの変更

インターフェイス コンフィギュレーション モードで **dot1x timeout {attribute}** *seconds* コマンド形式を使用して複数の 802.1X タイムアウト属性を変更することができます。ここでは、待機時間タイムアウトを変更する方法について詳細に説明し、次に同じコマンド形式を使用して他の 802.1X タイムアウトを変更する方法について説明します。

待機時間の設定

スイッチはクライアントを認証できなかった場合に、所定の時間だけアイドル状態を続け、その後再び認証を試みます。**dot1x timeout quiet-period** インターフェイス コンフィギュレーション コマンドがその待ち時間を制御します。認証が失敗する理由としては、クライアントが無効なパスワードを提示した場合などが考えられます。デフォルトよりも小さい値を入力することによって、ユーザへの応答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	Router(config)# **interface** *type slot/port*	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 2	Router(config-if)# **dot1x timeout quiet-period** *seconds*	クライアントとの認証のやり取りに失敗した場合に、スイッチが待機状態のままでいる秒数を設定します。 指定できる範囲は 0 ～ 65535 秒です。デフォルトは 60 秒です。
ステップ 3	Router(config-if)# **end**	特権 EXEC モードに戻ります。

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。

```
Router(config)# interface gigabitethernet 5/1
Router(config-if)# dot1x timeout quiet-period 30
```

スイッチからクライアントへの再送信時間の設定

クライアントはスイッチからの EAP 要求/アイデンティティ フレームに対し、EAP 応答/アイデンティティ フレームで応答します。スイッチはこの応答を受信しなかった場合、一定期間（再送信時間と呼ばれる）待機した後フレームを再送信します。

（注）　このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

スイッチが要求を再送信する前にクライアントからの EAP 要求/アイデンティティ フレームに対する応答を待機する時間を変更するには、インターフェイス コンフィギュレーション モードで **dot1x timeout tx-period** *seconds* コマンドを使用します。指定できる範囲は 1 ～ 65535 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** コマンドを使用します。

次の例では、要求を再送信する前に、スイッチが EAP 要求/アイデンティティ フレームに対するクライアントからの応答を待機する秒数を 60 秒に設定する方法を示します。

```
Router(config)# interface gigabitethernet 5/1
Router(config-if)# dot1x timeout tx-period 60
```

スイッチとクライアント間の EAP 要求フレーム再送信時間の設定

クライアントは EAP 要求フレームを受信したことをスイッチに通知します。スイッチがこの通知を受信できなかった場合、スイッチは所定の時間だけ待機した後、フレームを再送信します。

スイッチが通知を待機する時間を設定するには、インターフェイス コンフィギュレーション モードで **dot1x timeout supp-timeout** *seconds* コマンドを使用します。指定できる範囲は 1 ～ 65535 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 supp-timeout** コマンドを使用します。

次に、EAP 要求フレームのスイッチ/クライアント間再送信時間を 25 秒に設定する例を示します。

```
Router(config)# interface gigabitethernet 5/1
Router(config-if)# dot1x timeout supp-timeout 25
```

スイッチ/認証サーバ間のレイヤ 4 パケット再送信時間の設定

認証サーバは、レイヤ 4 パケットを受信するたびにスイッチに通知します。スイッチがパケット送信後に通知を受信できない場合、スイッチは所定の時間だけ待機した後、パケットを再送信します。

スイッチから認証サーバへのレイヤ 4 パケットの再送信値を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface` *type slot/port*	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 2	`Router(config-if)# dot1x timeout server-timeout` *seconds*	スイッチ/認証サーバ間のレイヤ 4 パケットの再送信値を設定します。*seconds* の範囲は 1 ～ 65535 秒です。デフォルトは 30 です。
ステップ 3	`Router(config-if)# end`	特権 EXEC モードに戻ります。

次に、スイッチ/認証サーバ間のレイヤ 4 パケットの再送信時間を 25 秒に設定する例を示します。

```
Router(config)# interface gigabitethernet 5/1
Router(config-if)# dot1x timeout server-timeout 25
```

スイッチ/クライアント間フレーム再送信回数の設定

スイッチ/クライアント間再送信時間を変更できるだけでなく、（クライアントから応答が得られなかった場合に）スイッチが認証プロセスを再起動する前に、クライアントに EAP 要求/アイデンティティ フレームを送信する回数を変更できます。

（注）　このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

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	`Router(config)# interface type slot/port`	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 2	`Router(config-if)# dot1x max-req count`	スイッチが認証処理を再開するまでに、クライアントへ EAP 要求/アイデンティティ フレームを送信する回数を変更できます。指定できる範囲は 1 ～ 10 です。デフォルトは 2 です。
ステップ 3	`Router(config-if)# end`	特権 EXEC モードに戻ります。

次に、スイッチが認証プロセスを再起動する前に、EAP 要求/アイデンティティ要求を送信する回数を 5 に設定する例を示します。

```
Router(config)# interface gigabitethernet 5/1
Router(config-if)# dot1x max-req 5
```

再認証回数の設定

ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再開する回数を変更することもできます。

（注）　このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

再認証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	`Router(config)# interface type slot/port`	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 2	`Router(config-if)# dot1x max-reauth-req count`	ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再開する回数を設定します。指定できる範囲は 0 ～ 10 です。デフォルトは 2 です。
ステップ 3	`Router(config-if)# end`	特権 EXEC モードに戻ります。

次の例では、ポートが無許可ステートに移行する前に、スイッチが認証プロセスを再起動する回数を 4 に設定する方法を示します。

```
Router(config)# interface gigabitethernet 5/1
Router(config-if)# dot1x max-reauth-req 4
```

IEEE 802.1X アカウンティングの設定

802.1X アカウンティングによる AAA システム アカウンティングをイネーブルにすることにより、ログ用のアカウンティング RADIUS サーバにシステム リロード イベントを送信することができます。その後、すべてのアクティブ 802.1X セッションがクローズしていることをサーバが判別できます。

RADIUS は信頼性の低い UDP トランスポート プロトコルを使用するため、ネットワーク状態が良好でないと、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。設定した回数のアカウンティング要求の再送信後、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、次のメッセージが表示されます。

```
Accounting message %s for session %s failed to receive Accounting Response.
```

このストップ メッセージが正常に送信されない場合、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.
```

（注） ロギングの開始、停止、仮のアップデート メッセージ、タイム スタンプなどのアカウンティング タスクを実行するように、RADIUS サーバを設定する必要があります。これらの機能をオンにするには、RADIUS サーバの [Network Configuration] タブの [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] タブの [CVS RADIUS Accounting] をイネーブルにします。

スイッチ上で AAA をイネーブルにしたあとで 802.1X アカウンティ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	`Router(config)# aaa accounting dot1x default start-stop group radius`	すべての 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 2	`Router(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（すべての RADIUS サーバのリストを使用）、スイッチがリロードするときにシステム 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。

	コマンド	目的
ステップ 3	`Router(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	`Router# show running-config`	入力を確認します。

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** 特権 EXEC コマンドを使用します。

次に、802.1X アカウンティングを設定する例を示します。最初のコマンドは、アカウンティングの UDP ポートとして 1813 を指定して、RADIUS サーバを設定します。

```
Router(config)# radius-server host 172.120.39.46 auth-port 1812 acct-port 1813 key rad123
Router(config)# aaa accounting dot1x default start-stop group radius
Router(config)# aaa accounting system default start-stop group radius
```

VLAN ユーザ分散の設定

複数の VLAN を含む VLAN グループを定義できます。さらに、VLAN ロード バランシングのために、802.1X 認証中のユーザに対する応答の一部として VLAN グループ名を提供するように RADIUS サーバを設定できます。提供された VLAN グループ名が定義済みの VLAN グループ名の中に見つかった場合、新たに認証されたユーザは、VLAN グループ内でユーザ追加数が最も少ない VLAN に配置されます。

VLAN グループを設定するには、次の作業を行います。

コマンド	目的
`Router(config)# vlan group` *group-name* `vlan-list` *vlan-list*	VLAN グループを作成するか、既存の VLAN グループに VLAN を追加します。 • *group-name* : VLAN グループの名前です。名前は最大 32 文字で、文字から始める必要があります。 • **vlan-list** *vlan-list* : VLAN グループに属する VLAN です。グループのメンバは、単一の VLAN ID、VLAN ID のリスト、または VLAN ID の範囲として指定できます。複数のエントリはハイフン（-）またはカンマ（,）で区切ります。

次に、VLAN 7 ～ 9 と 11 を VLAN グループにマッピングする例を示します。

```
Router(config)# vlan group ganymede vlan-list 7-9,11
```

ゲスト VLAN の設定

ゲスト VLAN を設定すると、サーバが EAP 要求/アイデンティティ フレームに対する応答を受信しない場合、802.1X 対応でないクライアントはゲスト VLAN に配置されます。802.1X 対応であっても、認証に失敗したクライアントはネットワーク アクセスを許可されません。ゲスト VLAN として動作する際、ポートに設定されたホスト モードに関係なく、ポートはマルチホスト モードで機能します。

ゲスト VLAN 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)# interface type slot/port`	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 2	`Router(config-if)# switchport mode {access | private-vlan host}`	ポートをアクセス モードに、またはプライベート VLAN ホスト ポートとして設定します。ルーテッド ポートおよびトランク ポートはゲスト VLAN をサポートしません。
ステップ 3	`Router(config-if)# authentication port-control auto`	ポートで認証をイネーブルにします。
ステップ 4	`Router(config-if)# authentication event no-response action authorize vlan vlan-id`	アクティブ VLAN をゲスト VLAN として指定します。指定できる範囲は 1 ～ 4094 です。 内部 VLAN（ルーテッド ポート）、RSPAN VLAN、プライベート プライマリ PVLAN、または音声 VLAN を除き、任意のアクティブ VLAN をゲスト VLAN として設定できます。
ステップ 5	`Router(config-if)# {dot1x pae authenticator | mab}`	ポート認証方式を 802.1X にするか、または MAC アドレス バイパスにするかを指定します。
ステップ 6	`Router(config-if)# end`	特権 EXEC モードに戻ります。

次に、802.1X ゲスト VLAN として VLAN 2 をイネーブルにする例を示します。

```
Router(config)# interface gigabitethernet 5/1
Router(config-if)# authentication port-control auto
Router(config-if)# authentication event no-response action authorize vlan 2
Router(config-if)# dot1x pae authenticator
```

次に、スイッチにクライアント通知タイムアウトとして 3 秒を設定し、要求を再送信する前にスイッチがクライアントからの EAP 要求/アイデンティティ フレームに対する応答を待機する秒数として 15 を設定し、802.1X ポートが DHCP クライアントに接続されているときに 802.1X ゲスト VLAN として VLAN 2 をイネーブルにする例を示します。

```
Router(config-if)# dot1x timeout supp-timeout 3
Router(config-if)# dot1x timeout tx-period 15
Router(config-if)# authentication event no-response action authorize vlan 2
Router(config-if)# dot1x pae authenticator
```

制限付き VLAN の設定

スイッチに制限付き VLAN を設定すると、認証サーバが有効なユーザ名とパスワードを受信しなかった場合、802.1X 準拠のクライアントが制限付き VLAN に移動します。制限 VLAN として動作する際、ポートに設定されたホスト モードに関係なく、ポートはシングルホスト モードで機能します。

制限 VLAN 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)# interface type slot/port`	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 2	`Router(config-if)# switchport mode {access | private-vlan host}`	ポートをアクセス モードに、またはプライベート VLAN ホスト ポートとして設定します。ルーテッド ポートおよびトランク ポートはゲスト VLAN をサポートしません。
ステップ 3	`Router(config-if)# authentication port-control auto`	ポートでのポートベース認証をイネーブルにします。
ステップ 4	`Router(config-if)# authentication event fail [retry retries] action authorize vlan vlan-id`	アクティブ VLAN を制限 VLAN として指定します。*vlan-id* の範囲は 1 ～ 4094 です。 （任意）**retry** キーワードは、ポートを制限 VLAN に移動する前に許可される認証試行回数を指定します。
ステップ 5	`Router(config-if)# end`	特権 EXEC モードに戻ります。

制限 VLAN をディセーブルにして削除するには、**authentication event fail** コマンドまたは **dot1x auth-fail** コマンドの **no** 形式を使用します。ポートは無許可ステートに戻ります。

ユーザが制限 VLAN に割り当てられる前に許可される認証試行最大回数を設定できます。**authentication event fail** [**retry** *retries*] **action authorize vlan** コマンドで **retry** キーワードを使用すると、試行回数を設定できます。*retries*（認証試行の許容回数）の範囲は 1 ～ 5 です。デフォルトは 2 回です。

次に、制限 VLAN として VLAN 2 をイネーブルにし、3 回の試行失敗後にホストを割り当てる例を示します。

```
Router(config)# interface gigabitethernet 5/1
Router(config-if)# authentication port-control auto
Router(config-if)# authentication event fail retry 3 action authorize vlan 2
Router(config-if)# dot1x pae authenticator
```

アクセス不能認証バイパス機能の設定

アクセス不能認証バイパス機能（クリティカル認証または AAA 失敗ポリシーとも呼ばれます）を設定できます。

ポートをクリティカル ポートとして設定して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、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# radius-server dead-criteria time` *time* **tries** *tries*	（任意）RADIUS サーバが利用不能または*停止*と見なされるときを判別するのに使用される条件を設定します。 指定できる *time* の範囲は 1 ～ 120 秒です。スイッチは、デフォルトの *seconds* 値を 10 ～ 60 秒の間で動的に決定します。 指定できる *tries* の範囲は 1 ～ 100 です。スイッチは、デフォルトの *tries* パラメータを 10 ～ 100 の間で動的に決定します。
ステップ 2	`Router(config)# radius-server deadtime` *minutes*	（任意）RADIUS サーバに要求が送信されない分数を設定します。指定できる範囲は 0 ～ 1440 分（24 時間）です。デフォルト値は 0 分です。

	コマンド	目的
ステップ 3	`Router(config)# radius-server host ip-address [acct-port udp-port] [auth-port udp-port] [key string] [test username name [idle-time time] [ignore-acct-port] [ignore-auth-port]]`	（任意）以下のキーワードを使用して RADIUS サーバのパラメータを設定します。 • **acct-port** *udp-port* : RADIUS アカウンティング サーバの UDP ポートを指定します。UDP ポート番号の範囲は 0 ～ 65536 です。デフォルト値は 1646 です。 • **auth-port** *udp-port* : RADIUS 認証サーバの UDP ポートを指定します。UDP ポート番号の範囲は 0 ～ 65536 です。デフォルト値は 1645 です。 （注） RADIUS アカウンティング サーバの UDP ポートと RADIUS 認証サーバの UDP ポートを非デフォルト値に設定します。 • **key** *string* : スイッチと RADIUS デーモンとの間のすべての RADIUS 通信で使用する認証および暗号キーを指定します。 （注） **radius-server key** {**0** *string* | **7** *string* | *string*} グローバル コンフィギュレーション コマンドを使用しても認証および暗号キーを設定できます。 • **test username** *name* : RADIUS サーバ ステータスの自動化テストをイネーブルにして、使用されるユーザ名を指定します。 • **idle-time** *time* : スイッチがテスト パケットをサーバに送信した後の間隔を分数で設定します。指定できる範囲は 1 ～ 35791 分です。デフォルトは 60 分（1 時間）です。 • **ignore-acct-port** : RADIUS サーバのアカウンティング ポートでのテストをディセーブルにします。 • **ignore-auth-port** : RADIUS サーバの認証ポートでのテストをディセーブルにします。
ステップ 4	`Router(config)# dot1x critical eapol`	（任意）スイッチがクリティカル ポートを正常に認証すると、スイッチが EAPOL 成功メッセージを送信するように指定します。
ステップ 5	`Router(config-if)# authentication critical recovery delay milliseconds`	（任意）使用できない RADIUS サーバが使用できるようになったときに、スイッチがクリティカル ポートを再初期化するために待機する回復遅延期間を設定します。指定できる範囲は 1 ～ 10000 ミリ秒です。デフォルトは 1000 ミリ秒です（ポートが毎秒再初期化可能になります）。
ステップ 6	`Router(config)# interface type slot/port`	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。

	コマンド	目的
ステップ 7	`Router(config-if)# authentication event server dead action authorize [vlan vlan-id]`	アクセス不能認証バイパス機能をイネーブルにして、AAA サーバに到達できない場合に、指定した VLAN 上のポートが許可されるようにします。VLAN を指定しない場合は、アクセス VLAN が使用されます。 （注）　**vlan** キーワードは、スイッチ ポートでだけ使用できます。
ステップ 8	`Router(config-if)# authentication event server alive action reinitialize`	アクセス不能認証バイパス回復機能を設定し、回復アクションとして、認証サーバが使用可能になったときにポートを認証するように指定します。
ステップ 9	`Router(config-if)# end`	特権 EXEC モードに戻ります。

RADIUS サーバのデフォルト設定に戻すには、**no radius-server dead-criteria**、**no radius-server deadtime**、および **no radius-server host** グローバル コンフィギュレーション コマンドを使用します。アクセス不能認証バイパスのデフォルト設定に戻すには、**no dot1x critical** {**eapol**} 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。アクセス不能認証バイパスをディセーブルにするには、**no authentication event server dead action authorize**（または **no dot1x critical**）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、アクセス不能認証バイパス機能を設定する例を示します。

```
Router(config)# radius-server dead-criteria time 30 tries 20
Router(config)# radius-server deadtime 60
Router(config)# radius-server host 1.1.1.2 acct-port 1550 auth-port 1560 key abc1234 test
username user1 idle-time 30
Router(config)# dot1x critical eapol
Router(config)# authentication critical recovery delay 2000
Router(config)# interface gigabitethernet 0/1
Router(config-if)# authentication event server dead action authorize vlan 123
Router(config-if)# authentication event server alive action reinitialize
```

MAC 認証バイパスの設定

インターフェイス上で MAC 認証バイパスを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface type slot/port`	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 2	`Router(config-if)# authentication port-control {auto | force-authorized | force-unauthorized}`	ポートでの 802.1X 認証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。 • **auto**：認証が成功するまで EAPOL トラフィックだけを許可します。 • **force-authorized**：すべてのトラフィックを許可し、認証は不要です。 • **force-unauthorized**：どのトラフィックも許可しません。

	コマンド	目的
ステップ 3	`Router(config-if)# mab [eap]`	インターフェイス上で MAC 認証バイパスをイネーブルにします。 • （任意）**eap** キーワードを使用して、スイッチが許可に EAP を使用するように設定します。 • EAP を使った MAC 認証バイパスがインターフェイス上でイネーブルになっている場合は、その後にインターフェイス上で実行される **default interface** コマンドによってディセーブルになることはありません。 • MAC 認証バイパスをルーテッド ポートで使用するために、MAC アドレス ラーニングがポートでイネーブルになっていることを確認してください。
ステップ 4	`Router(config-if)# end`	特権 EXEC モードに戻ります。

次に、ポートで MAC 認証バイパスをイネーブルにする例を示します。

```
Router(config)# interface gigabitethernet 5/1
Router(config-if)# authentication port-control auto
Router(config-if)# mab
```

NAC レイヤ 2 IEEE 802.1X 検証の設定

NAC レイヤ 2 IEEE 802.1X 検証を設定できます。これは、RADIUS サーバを使用した 802.1X 認証とも呼ばれます。NAC レイヤ 2 IEEE 802.1X の設定は 802.1X の設定と同じですが、RADIUS サーバでポスチャ トークンと VLAN 割り当てを設定する手順が追加されます。

NAC レイヤ 2 IEEE 802.1X 検証を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface` *type slot/port*	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 2	`Router(config-if)# authentication port-control auto`	インターフェイスでのポートベース認証をイネーブルにします。
ステップ 3	`Router(config-if)# authentication periodic`	クライアントの定期的な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に設定されています。

	コマンド	目的
ステップ 4	`Router(config-if)# authentication timer reauthenticate [seconds | server]`	以下のキーワードを使用して再認証の間隔（秒）を指定します。 • *seconds*：1 ～ 65535 の範囲で秒数を設定します。デフォルトは 3600 秒です。 • **server**：Session-Timeout RADIUS 属性（属性 [27]）および Termination-Action RADIUS 属性（属性 [29]）の値に基づいて秒数を設定します。 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 5	`Router(config-if)# end`	特権 EXEC モードに戻ります。

次に、NAC レイヤ 2 IEEE 802.1X 検証を設定する例を示します。

```
Router(config)# interface gigabitethernet 5/1
Router(config)# authentication port-control auto
Router(config-if)# authentication periodic
Router(config-if)# authentication timer reauthenticate server
```

NAC エージェントレス監査のサポートの設定

エージェントレス クライアントのための NAC 監査アーキテクチャをサポートするには、スイッチは認証中の 802.1X クライアントの IP アドレスをスヌーピングし、エージェントレス クライアント用に一意のセッション ID を作成して割り当て、この情報を RADIUS サーバに渡して NAC 監査サーバと共有できるようにする必要があります。スイッチがこの情報を取得して共有できるようにするには、スイッチ上で ARP と DHCP スヌーピングをイネーブルにし、特定の RADIUS 属性の送信をイネーブルにする必要があります。

NAC エージェントレス監査をサポートするための RADIUS およびトラッキング設定を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# radius-server attribute 8 include-in-access-req`	access-request または accounting-request パケットで Framed-IP-Address RADIUS 属性（属性 [8]）を送信するようにスイッチを設定します。
ステップ 2	`Router(config)# radius-server vsa send authentication`	認証段階でスイッチによって生成される RADIUS Access-Request 内のベンダー固有属性（VSA）（特に audit-session-id）を認識して使用するようにネットワーク アクセス サーバを設定します。
ステップ 3	`Router(config)# radius-server vsa send accounting`	後続の RADIUS Accounting-Request に VSA を含めることができるようにします。
ステップ 4	`Router(config)# ip device tracking`	IP デバイス トラッキング テーブルをイネーブルにします。

DACL またはリダイレクト URL に関するスイッチの設定

接続されたホストの認証中に RADIUS サーバからの DACL またはリダイレクト URL を受け入れるようにスイッチ 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	`Router# 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	`Router(config)# radius-server vsa send authentication`	認証段階でスイッチによって生成される RADIUS Access-Request 内のベンダー固有属性（VSA）を認識して使用するようにネットワーク アクセス サーバを設定します。 （注）　この手順は、リダイレクト URL を使用する場合、または DACL が Filter-ID 属性ではなく VSA を使用してダウンロードされる場合にだけ必要となります。
ステップ 3	`Router(config)# ip device tracking`	IP デバイス トラッキング テーブルをイネーブルにします。
ステップ 4	`Router(config)# ip access-list extended` *dacl-name*	VSA または Filter-ID 属性によって参照される ACL を設定します。 （注）　この手順は、RADIUS サーバで定義され、VSA を使用してダウンロードされる DACL には必要ありません。
ステップ 5	`Router(config-std-nacl)# {permit | deny} ...`	ACL を定義します。 （注）　送信元アドレスは ANY にする必要があります。
ステップ 6	`Router(config-std-nacl)# 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	`Router(config)# ip access-list extended` *acl-name*	ポート用のデフォルト ACL を定義します。
ステップ 8	`Router(config-std-nacl)# {permit | deny} ...`	ACL を定義します。
ステップ 9	`Router(config-std-nacl)# 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 10	`Router(config)# interface` *type slot/port*	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 11	`Router(config-if)# ip access-group` *acl-name* `in`	インターフェイスでデフォルトのスタティック ACL を適用します。
ステップ 12	`Router(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。

次に、ダウンロード ポリシーのスイッチを設定する例を示します。

```
Router# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# radius-server vsa send authentication
Router(config)# ip device tracking
Router(config)# ip access-list extended my_dacl
Router(config-ext-nacl)# permit tcp any host 10.2.3.4
Router(config-ext-nacl)# exit
Router(config)# ip access-list extended default_acl
Router(config-ext-nacl)# permit ip any any
Router(config-ext-nacl)# exit
Router(config)# interface fastEthernet 2/13
Router(config-if)# ip access-group default_acl in
```

```
Router(config-if)# exit
```

WoL を使った 802.1X 認証の使用

Wake-on-LAN（WoL）を使った 802.1X 認証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	`Router(config)# interface type slot/port`	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 2	`Router(config-if)# authentication control-direction {both | in}`	ポートでの WoL を使った 802.1X 認証をイネーブルにし、以下のキーワードを使用してポートを双方向または単一方向に設定します。 • **both**：ポートを双方向に設定します。ポートは、ホストにパケットを送受信できません。デフォルトでは、ポートは双方向です。 • **in**：ポートを単方向に設定します。ポートは、ホストにパケットを送信できますが、受信はできません。
ステップ 3	`Router(config-if)# end`	特権 EXEC モードに戻ります。

WoL を使った 802.1X 認証をディセーブルにするには、**no authentication control-direction**（または **no dot1x control-direction**）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、WoL を使った 802.1X 認証をイネーブルにし、ポートを双方向に設定する例を示します。

```
Router(config)# interface gigabitethernet 5/1
Router(config-if)# authentication control-direction both
```

MAC 移動のイネーブル化

スイッチで MAC 移動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	`Router# 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	`Router(config)# authentication mac-move permit`	スイッチで MAC 移動をイネーブルにします。
ステップ 3	`Router(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	`Router# show running-config`	（任意）入力を確認します。
ステップ 5	`Router# 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。

次の例では、スイッチで MAC 移動をグローバルにイネーブルにする方法を示します。

```
Router(config)# authentication mac-move permit
```

MAC 置換のイネーブル化

インターフェイスの MAC 置換をイネーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`Router# 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	`Router(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	`Router(config-if)# authentication violation {protect | replace | restrict | shutdown}`	インターフェイス上で MAC 置換をイネーブルにするには、**replace** キーワードを使用します。ポートが現在のセッションを削除し、新しいホストを使用して認証を開始します。 他のキーワードは、次のような機能があります。 • **protect**：ポートは、システム メッセージを生成せずに、予期しない MAC を使用するパケットをドロップします。 • **restrict**：違反パケットが CPU によってドロップされ、システム メッセージが生成されます。 • **shutdown**：ポートは、予期しない MAC アドレスを受信すると errdisable になります。
ステップ 4	`Router(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	`Router# show running-config`	入力を確認します。
ステップ 6	`Router# 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 MAC 置換をイネーブルにする例を示します。

```
Router(config)# interface gigabitethernet2/2
Router(config-if)# authentication violation replace
```

NEAT オーセンティケータとサプリカント スイッチの設定

- 「NEAT オーセンティケータの設定」（P.83-56）
- 「NEAT サプリカントの設定」（P.83-56）

（注）
- NEAT では、1 台のスイッチがサプリカントとして設定され、オーセンティケータ スイッチに接続する必要があります。
- 概要については、「Network Edge Access Topology（NEAT）を使用した 802.1x サプリカントおよびオーセンティケータ スイッチ」（P.83-30）を参照してください。
- cisco-av-pairs 値は、ACS で「device-traffic-class=switch」として設定されている必要があります。これは、サプリカントが正常に認証されたあとでトランクとしてインターフェイスを設定します。

NEAT オーセンティケータの設定

オーセンティケータとして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	`Router# 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	`Router(config)# cisp enable`	CISP をイネーブルにします。
ステップ 3	`Router(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 4	`Router(config-if)# switchport mode access`	ポート モードを **access** に設定します。
ステップ 5	`Router(config-if)# authentication port-control auto`	ポート認証モードを auto に設定します。
ステップ 6	`Router(config-if)# dot1x pae authenticator`	インターフェイスをポート アクセス エンティティ（PAE）オーセンティケータとして設定します。
ステップ 7	`Router(config-if)# spanning-tree portfast`	単一ワーク ステーションまたはサーバに接続されたアクセス ポート上で PortFast をイネーブルにします。
ステップ 8	`Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 9	`Router# show running-config interface` *interface-id*	設定を確認します。
ステップ 10	`Router# 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、スイッチを 802.1x オーセンティケータとして設定する例を示します。

```
Router# configure terminal
Router(config)# cisp enable
Router(config)# interface gigabitethernet1/1
Router(config-if)# switchport mode access
Router(config-if)# authentication port-control auto
Router(config-if)# dot1x pae authenticator
Router(config-if)# spanning-tree portfast trunk
```

NEAT サプリカントの設定

サプリカントとして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	`Router# 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	`Router(config)# cisp enable`	CISP をイネーブルにします。
ステップ 3	`Router(config)# dot1x credentials` *profile*	802.1x クレデンシャル プロファイルを作成します。これは、サプリカントとして設定されるポートに接続する必要があります。
ステップ 4	`Router(config)# username` *suppswitch*	ユーザ名を作成します。
ステップ 5	`Router(config)# password` *password*	新しいユーザ名のパスワードを作成します。

	コマンド	目的
ステップ 6	Router(config)# **dot1x supplicant force-multicast**	ユニキャスト パケットまたはマルチキャスト パケット受信した場合に、スイッチにマルチキャスト EAPOL パケット*だけ*を送信するように強制すると、NEAT はすべてのホスト モードのサプリカント スイッチで機能できます。
ステップ 7	Router(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 8	Router(config-if)# **switchport trunk encapsulation dot1q**	ポートをトランク モードに設定します。
ステップ 9	Router(config-if)# **switchport mode trunk**	インターフェイスを VLAN トランク ポートとして設定します。
ステップ 10	Router(config-if)# **dot1x pae supplicant**	インターフェイスをポート アクセス エンティティ（PAE）サプリカントとして設定します。
ステップ 11	Router(config-if)# **dot1x credentials** *profile-name*	802.1x クレデンシャル プロファイルをインターフェイスに対応付けます。
ステップ 12	Router(config-if)# **end**	特権 EXEC モードに戻ります。
ステップ 13	Router# **show running-config interface** *interface-id*	設定を確認します。
ステップ 14	Router# **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。

次の例では、スイッチをサプリカントとして設定する方法を示します。

```
Router# configure terminal
Router(config)# cisp enable
Router(config)# dot1x credentials test
Router(config)# username suppswitch
Router(config)# password myswitch
Router(config)# dot1x supplicant force-multicast
Router(config)# interface gigabitethernet1/1
Router(config-if)# switchport trunk encapsulation dot1q
Router(config-if)# switchport mode trunk
Router(config-if)# dot1x pae supplicant
Router(config-if)# dot1x credentials test
Router(config-if)# end
```

ポート上での 802.1X 認証のディセーブル化

no dot1x pae 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、ポートでの 802.1X 認証をディセーブルにすることができます。

ポートでの 802.1X 認証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	Router(config)# **interface** *type slot/port*	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 2	Router(config-if)# **no dot1x pae authenticator**	ポートでの 802.1X 認証をディセーブルにします。
ステップ 3	Router(config-if)# **end**	特権 EXEC モードに戻ります。

802.1X をポートでイネーブルにするもののポートに接続されているクライアントを許可できないようにする 802.1X Port Access Entity（PAE）オーセンティケータとしてポートを設定するには、**dot1x pae authenticator** 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。

次にポートでの 802.1X 認証をディセーブルにする例を示します。

```
Router(config)# interface gigabitethernet 5/1
Router(config-if)# no dot1x pae authenticator
```

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	`Router(config)# interface type slot/port`	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 2	`Router(config-if)# 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	`Router(config-if)# end`	特権 EXEC モードに戻ります。

次に、ポートの 802.1X 認証設定をデフォルト値にリセットする例を示します。

```
Router(config)# interface gigabitethernet 3/27
Router(config-if)# dot1x default
```

認証のステータスおよび情報の表示

- 「802.1X ステータスの表示」（P.83-58）
- 「認証の方式およびステータスの表示」（P.83-59）
- 「MAC 認証バイパスのステータスの表示」（P.83-62）

802.1X ステータスの表示

スイッチのグローバルな 802.1X 管理ステータスおよび動作ステータスを表示したり、個別のポートの 802.1X 設定を表示したりするには、次の作業を行います。

コマンド	目的
`Router# show dot1x [all | interface type slot/port]`	スイッチのグローバルな 802.1X 管理ステータスおよび動作ステータスを表示します。 （任意）**all** キーワードを使用して、802.1X 認証を使用するすべてのインターフェイスのグローバルな 802.1X ステータスと 802.1X 設定を表示します。 （任意）**interface** キーワードを使用して、特定のインターフェイスの 802.1X 設定を表示します。

次に、グローバルな 802.1X ステータスを表示する例を示します。

```
Router# show dot1x
Sysauthcontrol              Disabled
Dot1x Protocol Version            2
Critical Recovery Delay         100
Critical EAPOL              Disabled

Router#
```

次に、802.1X 認証を使用するすべてのインターフェイスのグローバルな 802.1X ステータスと 802.1X 設定を表示する例を示します。

```
Router# show dot1x all
Sysauthcontrol              Disabled
Dot1x Protocol Version            2
Critical Recovery Delay         100
Critical EAPOL              Disabled

Dot1x Info for GigabitEthernet3/27
----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = FORCE_AUTHORIZED
ControlDirection          = Both
HostMode                  = SINGLE_HOST
ReAuthentication          = Disabled
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = 3600 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
RateLimitPeriod           = 0

Router#
```

認証の方式およびステータスの表示

認証の方式およびステータスを表示するには、次のいずれかの作業を行います。

コマンド	目的
Router# **show authentication registrations**	登録済みのすべての方式の詳細を表示します。
Router# **show authentication interface** *interface*	特定のインターフェイスの認証情報を表示します。
Router# **show authentication method** *method*	指定した方式を使用して許可された現在の認証セッションを一覧表示します。
Router# **show authentication sessions** [**handle** *handle*] [**interface** *interface*] [**mac** *mac*] [**method** *method*] [**session-id** *session-id*]	現在の認証セッションに関する情報を表示します。オプションを指定しない場合、現在のすべてのアクティブ セッションが一覧表示されます。キーワードを追加したり組み合わせたりすることで、特定のセッションや一部のセッションに関する詳細情報を表示することができます。

表 83-2　認証セッションのステート

ステート	説明
Idle	セッションが初期化されました。方式はまだ実行されていません。
Running	このセッションの方式が実行中です。
No methods	このセッションの結果を出した方式はありません。
Authc Success	ある方式で、このセッションの認証成功の結果が提供されました。
Authc Failed	ある方式で、このセッションの認証失敗の結果が提供されました。
Authz Success	このセッションでは、すべての機能が正常に適用されました。
Authz Failed	このセッションで、機能の適用に失敗しました。

表 83-3　認証方式のステート

ステート	説明
Not run	指定した方式はこのセッションで実行されていません。
Running	このセッションの方式が実行中です。
Failed over	この方式は失敗しました。次の方式が結果を出すことが予期されています。
Success	この方式は、セッションの成功した認証結果を提供しました。
Authc Failed	この方式は、セッションの失敗した認証結果を提供しました。

次に、登録済みの認証方式を表示する例を示します。

```
Router# show authentication registrations
Auth Methods registered with the Auth Manager:
  Handle  Priority  Name
    3        0       dot1x
    2        1       mab
    1        2       webauth
```

次に、特定のインターフェイスに関する認証の詳細を表示する例を示します。

```
Router# show authentication interface gigabitethernet 1/23
Client list:
  MAC Address     Domain   Status              Handle          Interface
  0123.4567.abcd  DATA     Authz Success  0xE0000000  GigabitEthernet1/23

Available methods list:
  Handle  Priority  Name
    3        0      dot1x
    2        1      mab
Runnable methods list:
  Handle  Priority  Name
    2        0      mab
    3        1      dot1x
```

次に、スイッチ上のすべての認証セッションを表示する例を示します。

```
Router# show authentication sessions

Interface  MAC Address     Method   Domain   Status         Session ID
Gi1/48     0015.63b0.f676  dot1x    DATA     Authz Success  0A3462B1000000102983C05C
Gi1/5      000f.23c4.a401  mab      DATA     Authz Success  0A3462B10000000D24F80B58
Gi1/5      0014.bf5d.d26d  dot1x    DATA     Authz Success  0A3462B10000000E29811B94
```

次に、指定の認証方式を使用して許可されたセッションを表示する例を示します。

```
Router# show authentication method dot1x
Interface  MAC Address     Method   Domain   Status         Session ID
Gi1/48     0015.63b0.f676  dot1x    DATA     Authz Success  0A3462B1000000102983C05C
Gi1/5      0014.bf5d.d26d  dot1x    DATA     Authz Success  0A3462B10000000E29811B94
```

次に、インターフェイス上のすべての認証セッションを表示する例を示します。

```
Router# show authentication sessions interface gigabitethernet 1/47

Interface:  GigabitEthernet1/47
          MAC Address:  Unknown
           IP Address:  Unknown
               Status:  Authz Success
               Domain:  DATA
       Oper host mode:  multi-host
     Oper control dir:  both
        Authorized By:  Guest Vlan
          Vlan Policy:  20
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A3462C80000000000002763C
      Acct Session ID:  0x00000002
               Handle:  0x25000000

Runnable methods list:
       Method   State
       mab      Failed over
       dot1x    Failed over

---------------------------------------

            Interface:  GigabitEthernet1/47
          MAC Address:  0005.5e7c.da05
           IP Address:  Unknown
            User-Name:  00055e7cda05
               Status:  Authz Success
               Domain:  VOICE
       Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A3462C8000000010002A238
      Acct Session ID:  0x00000003
               Handle:  0x91000001

Runnable methods list:
       Method   State
       mab      Authc Success
       dot1x    Not run
```

次に、指定のセッション ID の認証セッションを表示する例を示します。

```
Router# show authentication sessions session-id 0B0101C70000004F2ED55218
```

```
              Interface:  GigabitEthernet9/2
            MAC Address:  0000.0000.0011
             IP Address:  20.0.0.7
               Username:  johndoe
                 Status:  Authz Success
                 Domain:  DATA
        Oper host mode:  multi-host
      Oper control dir:  both
         Authorized By:  Critical Auth
           Vlan policy:  N/A
       Session timeout:  N/A
          Idle timeout:  N/A
     Common Session ID:  0B0101C70000004F2ED55218
       Acct Session ID:  0x00000003
                Handle:  0x91000001

Runnable methods list:
       Method   State
       mab      Authc Success
       dot1x    Not run
```

次に、指定の認証方式によって許可されたすべてのクライアントを表示する例を示します。

```
Router# show authentication sessions method mab

No Auth Manager contexts match supplied criteria

Router# show authentication sessions method dot1x

Interface  MAC Address     Domain   Status         Session ID
Gi9/2      0000.0000.0011  DATA     Authz Success  0B0101C70000004F2ED55218
```

MAC 認証バイパスのステータスの表示

MAB のステータスを表示するには、次の作業を行います。

コマンド	目的
Router# **show mab** {**all** | **interface** *type slot/port*} [*detail*]	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関する MAB 認証の詳細を表示します。

表 83-4　MAB 認証ステート

ステート	説明
INITIALIZE	許可セッションは初期化されています。
ACQUIRING	セッションはクライアントの MAC アドレスを取得中です。
AUTHORIZING	セッションは MAC ベースの許可を待機中です。
TERMINATE	許可セッションの結果が取得されました。

次に、単一のインターフェイスに関する簡単な MAB ステータスを表示する例を示します。

```
Router# show mab interface fa1/1

MAB details for GigabitEthernet1/1
```

```
-------------------------------------
Mac-Auth-Bypass           = Enabled
Inactivity Timeout        = None
```

次に、単一のインターフェイスに関する詳細な MAB ステータスを表示する例を示します。

```
Router# show mab interface fa1/1 detail

MAB details for GigabitEthernet1/1
-------------------------------------
Mac-Auth-Bypass           = Enabled
Inactivity Timeout        = None

MAB Client List
---------------
Client MAC                = 000f.23c4.a401
MAB SM state              = TERMINATE
Auth Status               = AUTHORIZED
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

CHAPTER 84

Web ベース認証

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

Web ベース認証の前提条件

なし。

Web ベース認証の制約事項

- Web ベース認証は入力だけの機能です。
- Web ベース認証は、アクセス ポートだけで設定できます。Web ベース認証は、トランク ポート、EtherChannel メンバ ポート、またはダイナミック トランク ポートではサポートされていません。

- Web ベース認証を設定する前に、インターフェイスでデフォルトの ACL を設定する必要があります。レイヤ 2 インターフェイスのポート ACL を設定するか、レイヤ 3 インターフェイスの Cisco IOS ACL を設定します。
- レイヤ 2 インターフェイス上では、スタティック ARP キャッシュ割り当てのあるホストを認証できません。これらのホストは ARP メッセージを送信しないため、Web ベース認証機能で検出されません。
- デフォルトでは、スイッチの IP 装置追跡機能はディセーブルにされています。Web ベース認証を使用するには、IP デバイスのトラッキング機能をイネーブルにする必要があります。
- スイッチ上で HTTP サーバを実行するために、IP アドレスを少なくとも 1 つ設定する必要があります。また、各ホスト IP アドレスに到達するようにルートを設定する必要もあります。HTTP サーバは、ホストに HTTP ログイン ページを送信します。
- STP トポロジの変更によってホスト トラフィックが別のポートに着信する場合、2 ホップ以上離れたホストではトラフィックの中断が発生することがあります。これは、レイヤ 2（STP）トポロジの変更後に ARP および DHCP アップデートが送信されないことがあるためです。
- Web ベース認証は、ダウンロード可能ホスト ポリシーとして VLAN 割り当てをサポートしません。
- Cisco IOS Release 15.1SY では、RADIUS サーバからのダウンロード可能 ACL（DACL）がサポートされます。
- IPv6 トラフィックについては、Web ベース認証はサポートされていません。

Web ベース認証について

Web ベース認証の概要

Web ベース認証機能は、認証、許可、アカウンティング（AAA）システムの一部として機能できる Web ベース認証（Web 認証プロキシとも呼ばれる）を実装します。

Web ベースの認証機能を使用して、IEEE 802.1X サプリカントを実行していないホスト システムでエンドユーザを認証できます。レイヤ 2 およびレイヤ 3 インターフェイスで Web ベース認証機能を設定することができます。

ユーザが HTTP セッションを開始する際に、Web ベースの認証機能がホストからの入力 HTTP パケットを代行受信して、HTML ログイン ページをユーザに送信します。ユーザは資格情報を入力します。Web ベース認証はこの資格情報を認証のために AAA サーバに送信します。認証が成功すると、Web ベース認証がログイン成功 HTML ページをホストに送信し、AAA サーバによって返されたアクセス ポリシーが適用されます。

認証に失敗すると、Web ベース認証がログイン失敗 HTML ページをユーザに送信し、ログイン試行を再試行するようにユーザに要求します。ユーザが失敗ログイン試行の最大数を超過すると、Web ベース認証がログイン期限切れ HTML ページをホストに送信し、ユーザは待機する間ウォッチ リストに配置されます。

デバイスの役割

Web ベースの認証では、図 84-1 に示すように、ネットワーク上の装置にはそれぞれ特定のロールがあります。

図 84-1　Web ベースの認証装置のロール

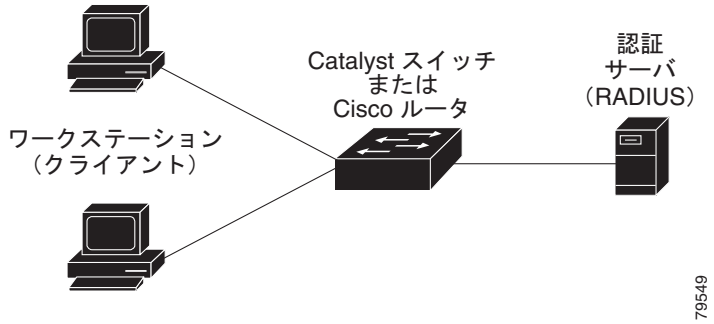


図 84-1 に示す特定の役割は、次のとおりです。

- *クライアント*：LAN およびスイッチ サービスへのアクセスを要求し、スイッチからの要求に応答するデバイス（ワークステーション）。このワークステーションでは、Java Script がイネーブルに設定された HTML ブラウザが実行されている必要があります。
- *認証サーバ*：実際にクライアントの認証を行います。認証サーバはクライアントの識別情報を確認し、そのクライアントに LAN およびスイッチ サービスへのアクセスを許可すべきかどうかをスイッチに通知します。
- *スイッチ*：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。スイッチはクライアントと認証サーバとの仲介デバイス（プロキシ）として動作し、クライアントに識別情報を要求し、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。

ホストの検出

スイッチは、検出されたホストに関する情報を格納するために、IP デバイス トラッキング テーブルを維持します。

（注） デフォルトでは、スイッチの IP 装置追跡機能はディセーブルにされています。Web ベース認証を使用するには、IP デバイスのトラッキング機能をイネーブルにする必要があります。

レイヤ 3 インターフェイスの場合、インターフェイス上に Web ベース認証が設定されると（またはインターフェイスがサービス中になると）、Web ベース認証が HTTP 代行受信 ACL を設定します。

レイヤ 2 インターフェイスの場合、次のメカニズムを使用して Web ベース認証が IP ホストを検出します。

- ARP ベース トリガー : ARP リダイレクト ACL により、Web ベース認証は固定 IP アドレスまたは動的に取得された IP アドレスを持つホストを検出できます。
- ダイナミック ARP インスペクション
- DHCP スヌーピング : スイッチがホストの DHCP バインディング エントリを作成するときに Web ベース認証が通知されます。

セッションの作成

Web ベース認証により、新しいホストが検出されると、次のようにセッションが作成されます。

- 例外リストをチェックします。

  ホスト IP が例外リストに含まれている場合、例外リスト エントリからのポリシーが適用され、セッションが確立されていると見なされます。

- 認証バイパスをチェックします。

  ホスト IP が例外リストにない場合、Web ベース認証は Nonresponsive Host（NRH; 非応答ホスト）要求をサーバに送信します。

  サーバ応答が Access Accepted である場合、このホスト用の許可がバイパスされます。セッションが確立されていると見なされます。

- HTTP 代行受信 ACL を設定します。

  NRH 要求に対するサーバ応答が Access Rejected である場合、HTTP 代行受信 ACL がアクティブになり、セッションはホストからの HTTP トラフィックを待機します。

認証プロセス

Web ベース認証がイネーブルの場合、次のイベントが発生します。

- ユーザが HTTP セッションを開始します。
- HTTP トラフィックが代行受信され、認証が開始されます。スイッチは、ユーザにログイン ページを送信します。ユーザがログイン ページにユーザ名とパスワードを入力すると、スイッチは認証サーバにそのエントリを送信します。
- クライアント ID が有効で、認証に成功した場合、スイッチは認証サーバからユーザのアクセス ポリシーをダウンロードしてアクティブにします。ログインの成功ページがユーザに送信されます
- 認証に失敗した場合は、スイッチはログインの失敗ページを送信します。ユーザがログインを再試行し、最大ログイン試行回数を超過すると、スイッチはログイン期限切れページを送信し、ホストがウォッチ リストに配置されます。ウォッチ リストのタイムアウト後、ユーザは認証プロセスを再試行することができます。
- 認証サーバがスイッチに応答せず、AAA 失敗ポリシーが設定されている場合、スイッチはホストに失敗アクセス ポリシーを適用します。ログインの成功ページがユーザに送信されます

ホストがレイヤ 2 インターフェイスの ARP プローブに応答しない場合やホストがレイヤ 3 インターフェイスでアイドル タイムアウト中にトラフィックを送信しない場合、スイッチはクライアントを再認証します。

- この機能は、ダウンロードされたタイムアウト、またはローカルに設定されたセッション タイムアウトを適用します。
- Termination-Action が RADIUS である場合、この機能は、サーバに NRH 要求を送信します。Termination-Action は、サーバからの応答に含まれます。
- 終了処理がデフォルトの場合、セッションが停止されて適用されたポリシーが削除されます。

AAA 失敗ポリシー

AAA 失敗ポリシーは、AAA サーバが使用できない場合、ユーザをネットワークに接続するか、または接続を維持するための方式です。クライアントの Web ベース認証が必要なときに AAA サーバにアクセスできない場合、ユーザを拒否する（つまり、ネットワークへのアクセスを提供しない）代わりに、管理者はユーザに適用できるデフォルト AAA 失敗ポリシーを設定できます。

このポリシーは次の理由で便利です。

- AAA が使用不可能である場合、アクセスが制限されることはあっても、ネットワークへの接続は維持できます。
- AAA サーバが再び利用できるようになると、ユーザは再検証を受けることが可能であり、ユーザの通常アクセス ポリシーを AAA サーバからダウンロードできます。

（注）　AAA サーバの停止時には、ユーザに既存のポリシーが関連付けられていない場合に限り、AAA 失敗ポリシーが適用されます。通常、ユーザ セッションで再認証が必要なときに AAA サーバが利用不可能な場合は、ユーザに対して現在有効なポリシーが維持されます。

AAA 失敗ポリシーが有効な間は、セッション ステートは AAA ダウンとして維持されます。

認証プロキシ Web ページのカスタマイゼーション

スイッチの内部 HTTP サーバは、Web ベース認証プロセスの間、認証を行うクライアントに送信する 4 つの HTML ページをホストします。この 4 つのページにより、サーバはユーザに次の 4 つの認証プロセスのステートを通知できます。

- ログイン：ユーザのクレデンシャルが要求された
- 成功：ログインに成功
- 失敗：ログインに失敗
- 期限切れ：ログインに何度も失敗したためログイン セッションが期限切れになった

4 つのデフォルト内部 HTML ページの代わりにカスタム HTML ページを使用したり、認証成功後にユーザがリダイレクトされる URL を指定して内部成功ページを効率的に置き換えたりできます。

その他の機能と Web ベース認証の相互作用

- 「ポート セキュリティ」（P.84-6）
- 「ゲートウェイ IP」（P.84-6）

- 「ACL」（P.84-6）
- 「IP ソース ガード」（P.84-6）
- 「EtherChannel」（P.84-6）
- 「スイッチオーバー」（P.84-7）

ポート セキュリティ

Web ベース認証とポート セキュリティは、同じポートに設定できます。（**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にポート セキュリティを設定します）。ポート セキュリティおよび Web ベース認証をポートでイネーブルにする際に、Web ベース認証がポートを認証し、ポート セキュリティでクライアントのものを含むすべての MAC アドレスのネットワーク アクセスを管理します。この場合、このポートを介してネットワークへ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。

ポート セキュリティをイネーブルにする手順については、「ポート セキュリティの設定方法」（P.85-5）を参照してください。

ゲートウェイ IP

Web ベース認証が VLAN のスイッチ ポートに設定されている場合、レイヤ 3 VLAN インターフェイス上にゲートウェイ IP を設定できません。

Web ベース認証はゲートウェイ IP と同じレイヤ 3 インターフェイスに設定できます。ソフトウェアで、両方の機能のホスト ポリシーが適用されます。GWIP ホスト ポリシーは、Web ベース認証のホスト ポリシーに優先されます。

ACL

VLAN ACL または Cisco IOS ACL をインターフェイス上に設定する場合、ACL がホスト トラフィックに適用されるのは Web ベース認証ホスト ポリシーが適用されたあとだけです。

レイヤ 2 Web ベース認証では、ポートに接続されたホストからの入力トラフィックについて、Port ACL（PACL; ポート ACL）をデフォルトのアクセス ポリシーとして設定する必要があります。認証後、Web ベース認証のホスト ポリシーは、PACL に優先されます。

MAC ACL と Web ベース認証を同じインターフェイスに設定することはできません。

アクセス VLAN に設定済み VACL キャプチャのあるポート上に Web ベース認証は設定できません。

IP ソース ガード

同じインターフェイスでの IP ソース ガードと Web ベース認証の設定はサポートされていません。

同じインターフェイスで IP ソース ガードと Web ベース認証を設定できます。DHCP スヌーピングがアクセス VLAN でもイネーブルである場合は、2 つの機能間の競合を回避するためにグローバル コンフィギュレーション モードで **platform acl tcam override dynamic dhcp-snooping** コマンドを入力する必要があります。IP ソース ガードと Web ベース認証が組み合わされているときは、その他の VLAN ベース機能はサポートされません。

EtherChannel

Web ベース認証は、レイヤ 2 EtherChannel インターフェイス上に設定できます。Web ベース認証設定は、すべてのメンバ チャネルに適用されます。

スイッチオーバー

RPR 冗長モードでは、スイッチオーバー中は現在認証されているホストに関する情報が保持されます。ユーザは再認証する必要がありません。

デフォルトの Web ベース認証の設定

機能	デフォルト設定
AAA	ディセーブル
RADIUS サーバ • IP アドレス • UDP 認証ポート • キー	 • 指定なし • 1812 • 指定なし
無活動タイムアウトのデフォルト値	3600 秒
無活動タイムアウト	イネーブル

Web ベース認証の設定方法

- 「デフォルトの Web ベース認証の設定」（P.84-7）
- 「Web ベース認証設定時の作業一覧」（P.84-8）
- 「認証ルールとインターフェイスの設定」（P.84-8）
- 「AAA 認証の設定」（P.84-9）
- 「スイッチ/RADIUS サーバ通信の設定」（P.84-9）
- 「HTTP サーバの設定」（P.84-11）
- 「Web ベース認証のパラメータ設定」（P.84-14）
- 「Web ベース認証のキャッシュ エントリの削除」（P.84-15）

Web ベース認証設定時の作業一覧

認証ルールとインターフェイスの設定

Web 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	`Router(config)# ip admission name name proxy http`	Web ベース許可の認証ルールを設定します。
ステップ 2	`Router(config)# interface type slot/port`	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、Web ベース認証をイネーブルにする入力レイヤ 2 またはレイヤ 3 インターフェイスを指定します。
ステップ 3	`Router(config-if)# ip access-group name`	デフォルト ACL を適用します。
ステップ 4	`Router(config-if)# ip admission name`	指定されたインターフェイスに Web ベース認証を設定します。
ステップ 5	`Router(config-if)# authentication order method1 [method2] [method3]`	（任意）使用される認証方式のフォールバック順序を指定します。*method* の 3 つの値のデフォルト順序は、**dot1x**、**mab**、および **webauth** です。 方式を省略すると、インターフェイス上でその方式がディセーブルになります。
ステップ 6	`Router(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 7	`Router(config)# ip device tracking`	IP デバイス トラッキング テーブルをイネーブルにします。
ステップ 8	`Router(config)# end`	特権 EXEC モードに戻ります。

この例では、ポート 5/1 上で 802.1X 認証または MAB 認証をディセーブルにしながら、Web ベースの認証をイネーブルにする方法を示します。

```
Router(config)# ip admission name webauth1 proxy http
Router(config)# interface gigabitethernet 5/1
Router(config-if)# ip admission webauth1
Router(config-if)# authentication order webauth
Router(config-if)# exit
Router(config)# ip device tracking
```

次に、設定を確認する例を示します。

```
Router# show ip admission configuration
Authentication Proxy Banner not configured
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
```

```
Authentication global init state time is 2 minutes
Authentication Proxy Watch-list is disabled

Authentication Proxy Rule Configuration
 Auth-proxy name webauth1
    http list not specified inactivity-time 60 minutes

Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

AAA 認証の設定

Web ベース認証をイネーブルにするには、AAA をイネーブルにして認証方式を指定する必要があります。次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# aaa new-model`	AAA 機能をイネーブルにします。
ステップ 2	`Router(config)# aaa authentication login default group {tacacs+ | radius}`	ログイン時の認証方法のリストを定義します。
ステップ 3	`Router(config)# aaa authorization auth-proxy default group {tacacs+ | radius}`	Web ベース許可の許可方式リストを作成します。
ステップ 4	`Router(config)# tacacs-server host {hostname | ip_address}`	AAA サーバを指定します。RADIUS サーバの場合は、「スイッチ /RADIUS サーバ通信の設定」（P.84-9）を参照してください。
ステップ 5	`Router(config)# tacacs-server key {key-data}`	スイッチと TACACS サーバとの間で使用される許可および暗号キーを設定します。

次の例では、AAA をイネーブルにする方法を示します。

```
Router(config)# aaa new-model
Router(config)# aaa authentication login default group tacacs+
Router(config)# aaa authorization auth-proxy default group tacacs+
```

スイッチ /RADIUS サーバ通信の設定

RADIUS セキュリティ サーバは、次のいずれかによって識別されます。

- ホスト名
- ホスト IP アドレス
- ホスト名と特定の UDP ポート番号
- IP アドレスと特定の UDP ポート番号

IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、同一 IP アドレスのサーバ上にある複数の UDP ポートに RADIUS 要求を送信できるようになります。同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（たとえば認証）を設定した場合、2 番めに設定されたホスト エントリは、最初に設定されたホスト エントリのフェールオーバー バックアップとして動作します。RADIUS ホスト エントリは、設定した順序に従って選択されます。

RADIUS サーバ パラメータを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`Router(config)# ip radius source-interface interface_name`	RADIUS パケットが、指定されたインターフェイスの IP アドレスを含むように指定します。
ステップ 2	`Router(config)# radius-server host {hostname | ip-address} test username username`	リモート RADIUS サーバのホスト名または IP アドレスを指定します。 **test username** *username* は、RADIUS サーバ接続の自動テストをイネーブルにするオプションです。指定された *username* は有効なユーザ名である必要はありません。 **key** オプションは、スイッチと RADIUS サーバとの間で使用する認証および暗号キーを指定します。 複数の RADIUS サーバを使用する場合は、このコマンドを再入力します。
ステップ 3	`Router(config)# radius-server key string`	スイッチと、RADIUS サーバで動作する RADIUS デーモン間で使用される認証および暗号キーを設定します。
ステップ 4	`Router(config)# radius-server vsa send authentication`	RADIUS サーバからの ACL のダウンロードをイネーブルにします。
ステップ 5	`Router(config)# radius-server dead-criteria tries num-tries`	RADIUS サーバに対する未応答の伝送数を指定します。この数を超えると RADIUS サーバが停止していると見なされます。指定できる *num-tries* の範囲は 1 ～ 100 です。

- 別のコマンドラインには、**key** *string* を指定します。
- **key** *string* には、スイッチと、RADIUS サーバ上で動作する RADIUS デーモンとの間で使用する認証および暗号キーを指定します。キーは、RADIUS サーバで使用する暗号キーに一致するテキスト ストリングでなければなりません。
- **key** *string* を指定する場合、キーの途中および末尾のスペースが利用されます。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。キーは RADIUS デーモンで使用する暗号に一致している必要があります。
- **radius-server host** グローバル コンフィギュレーション コマンドを使用して、タイムアウト、再送信回数、暗号キーの値を、すべての RADIUS サーバにグローバルに設定できます。これらのオプションをサーバ単位で設定するには、**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。

（注） RADIUS サーバ上でも、いくつかの値を設定する必要があります。これらの設定値としては、スイッチの IP アドレス、サーバとスイッチの双方で共有するキー ストリング、およびダウンロード可能 ACL があります。詳細については、RADIUS サーバのマニュアルを参照してください。

次に、スイッチで RADIUS サーバ パラメータを設定する例を示します。

```
Router(config)# ip radius source-interface Vlan80
Router(config)# radius-server host 172.120.39.46 test username user1
Router(config)# radius-server key rad123
Router(config)# radius-server dead-criteria tries 2
```

HTTP サーバの設定

Web ベース認証を使用するには、スイッチで HTTP サーバをイネーブルにする必要があります。このサーバは HTTP または HTTPS のいずれかについてイネーブルにできます。サーバ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 モードで次のいずれかの作業を行います。

コマンド	目的
`Router(config)# ip http server`	HTTP サーバをイネーブルにします。Web ベース認証機能は、HTTP サーバを使用してホストと通信し、ユーザ認証を行います。
`Router(config)# ip http secure-server`	HTTPS をイネーブルにします。

任意でカスタム認証プロキシ Web ページを設定したり、ログイン成功時のリダイレクション URL を指定したりできます。詳細については、次を参照してください。

- 認証プロキシ Web ページのカスタマイズ
- 成功ログインに対するリダイレクション URL の指定

認証プロキシ Web ページのカスタマイズ

Web ベース認証中に、スイッチの内部デフォルト HTML ページの代わりに、ユーザに表示される 4 つの代替 HTML ページを出力するオプションがあります。

カスタム認証プロキシ Web ページを使用するように指定するには、カスタム HTML ファイルをスイッチの内部ディスクまたはフラッシュ メモリに保存してから、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
ステップ 1	`Router(config)# ip admission proxy http login page file device:login-filename`	デフォルトのログイン ページの代わりに使用するカスタム HTML ファイルの、スイッチのメモリ ファイル システムの場所を指定します。*device:* はディスクまたはフラッシュ メモリのいずれかです（例：disk0:）。
ステップ 2	`Router(config)# ip admission proxy http success page file device:success-filename`	デフォルトのログイン成功ページの代わりに使用するカスタム HTML ファイルのメモリ ファイル システムの場所を指定します。
ステップ 3	`Router(config)# ip admission proxy http failure page file device:fail-filename`	デフォルトのログイン失敗ページの代わりに使用するカスタム HTML ファイルの場所を指定します。
ステップ 4	`Router(config)# ip admission proxy http login expired page file device:expired-filename`	デフォルトのログイン期限切れページの代わりに使用するカスタム HTML ファイルの場所を指定します。

- カスタム Web ページ機能をイネーブルにするには、4 つのすべてのカスタム HTML ファイルを指定する必要があります。4 つ未満のファイルが指定されている場合は、内部デフォルト HTML ページが使用されます。
- この 4 つのカスタム HTML ファイルはスイッチのディスクまたはフラッシュに存在している必要があります。
- イメージ ファイルのサイズには 256 KB の制限があります。
- すべてのイメージ ファイルに、「web_auth_」で始まるファイル名を付ける必要があります（例：「logo.jpg」ではなく、「web_auth_logo.jpg」）。

- すべてのイメージ ファイルの名前は、33 文字以上にすることができません。
- カスタム ページ上のイメージは、アクセス可能な HTTP サーバ上になければなりません。HTTP サーバにアクセスできるように、アドミッション ルール内に代行受信 ACL を設定する必要があります。
- カスタム ページからのすべての外部リンクでは、アドミッション ルール内で代行受信 ACL を設定する必要があります。
- 外部リンクまたは画像に必要なすべての名前解決では、有効な DNS サーバにアクセスするためにアドミッション ルール内で代行受信 ACL を設定する必要があります。
- カスタム Web ページ機能がイネーブルである場合、設定された auth-proxy-banner は使用されません。
- カスタム Web ページ機能がイネーブルである場合、成功ログイン機能のリダイレクション URL は利用不可能です。
- カスタム ファイルの指定を解除するには、このコマンドの **no** 形式を使用します。

カスタム ログイン ページはパブリック Web 形式であるため、このページについて次の注意事項に留意してください。

- ログイン形式では、ユーザ名およびパスワードのユーザ入力を受け入れて、そのデータを **uname** および **pwd** として POST する必要があります。
- カスタム ログイン ページは、ページ タイムアウト、暗号化されたパスワード、冗長送信の防止など、Web フォームに対するベスト プラクティスに従う必要があります。

次に、カスタム認証プロキシ Web ページを設定する例を示します。

```
Router(config)# ip admission proxy http login page file disk1:login.htm
Router(config)# ip admission proxy http success page file disk1:success.htm
Router(config)# ip admission proxy http fail page file disk1:fail.htm
Router(config)# ip admission proxy http login expired page file disk1:expired.htm
```

次に、カスタム認証プロキシ Web ページの設定を確認する例を示します。

```
Router# show ip admission configuration

Authentication proxy webpage
 Login page           : disk1:login.htm
 Success page         : disk1:success.htm
 Fail Page            : disk1:fail.htm
 Login expired Page   : disk1:expired.htm

Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Session ratelimit is 100
Authentication Proxy Watch-list is disabled
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

成功ログインに対するリダイレクション URL の指定

ユーザが認証に成功したあとにリダイレクトされる URL を指定するオプションがあり、内部成功 HTML ページを効率的に置き換えることができます。

成功ログインのリダイレクション URL を指定するには、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
Router(config)# **ip admission proxy http success redirect** *url-string*	デフォルトのログイン成功ページの代わりにユーザをリダイレクトする URL を指定します。

ログイン成功時のリダイレクション URL を設定する場合、次の注意事項に従ってください。

- カスタム認証プロキシ Web ページ機能がイネーブルである場合、リダイレクション URL 機能はディセーブルに設定され、CLI で利用できなくなります。リダイレクションはカスタム ログイン成功ページ内で実行できます。
- リダイレクション URL 機能がイネーブルである場合、設定された auth-proxy-banner は使用されません。
- リダイレクション URL の指定を解除するには、このコマンドの **no** 形式を使用します。

次に、ログイン成功時のリダイレクション URL を設定する例を示します。

```
Router(config)# ip admission proxy http success redirect www.cisco.com
```

次に、ログイン成功時のリダイレクション URL を確認する例を示します。

```
Router# show ip admission configuration

Authentication Proxy Banner not configured
Customizable Authentication Proxy webpage not configured
HTTP Authentication success redirect to URL: http://www.cisco.com
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Watch-list is disabled
Authentication Proxy Max HTTP process is 7
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

AAA 失敗ポリシーの設定

AAA 失敗ポリシーを設定するには、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
ステップ 1	Router(config)# **ip admission name** *rule-name* **proxy http event timeout aaa policy identity** *identity_policy_name*	AAA 失敗ルールを作成し、AAA サーバにアクセスできない場合にセッションに適用されるアイデンティティ ポリシーを関連付けます。 スイッチ上のルールを削除するには、**no ip admission name** *rule-name* **proxy http event timeout aaa policy identity** 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 2	Router(config)# **ip admission ratelimit aaa-down** *number_of_sessions*	（任意）AAA サーバが稼働状態に戻ったときに AAA サーバのフラッディングを回避するために、AAA ダウン ステートのホストからの認証試行をレート制限できます。

次に、AAA 失敗ポリシーを適用する例を示します。

```
Router(config)# ip admission name AAA_FAIL_POLICY proxy http event timeout aaa policy
identity GLOBAL_POLICY1
```

次に、AAA ダウン ステートで接続されているホストがあるかどうかを判別する例を示します。

```
Router# show ip admission cache
Authentication Proxy Cache
 Client IP 209.165.201.11 Port 0, timeout 60, state ESTAB (AAA Down)
```

次に、ホスト IP アドレスに基づいて特定のセッションに関する詳細情報を表示する例を示します。

```
Router# show ip admission cache 209.165.201.11
Address              : 209.165.201.11
MAC Address          : 0000.0000.0000
Interface            : Vlan333
Port                 : 3999
Timeout              : 60
Age                  : 1
State                : AAA Down
AAA Down policy      : AAA_FAIL_POLICY
```

Web ベース認証のパラメータ設定

失敗できるログイン試行回数の最大値を設定します。失敗した試行回数がこの値を超えると、クライアントは待機期間中、ウォッチ リストに載せられます。

Web ベース認証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	Router(config)# **ip admission max-login-attempts** *number*	失敗ログイン試行の最大回数を設定します。指定できる範囲は 1 ～ 2147483647 です。デフォルトは 5 です。
ステップ 2	Router(config)# **end**	特権 EXEC モードに戻ります。

次の例では、失敗ログイン試行の最大回数を 10 に設定する方法を示します。

```
Router(config)# ip admission max-login-attempts 10
```

Web ベース認証のキャッシュ エントリの削除

既存のセッション エントリを削除するには、次のいずれかの作業を行います。

コマンド	目的
Router# **clear ip auth-proxy cache** {* | *host ip address*}	認証プロキシ エントリを削除します。キャッシュ エントリすべてを削除するには、アスタリスクを使用します。シングル ホストのエントリを削除するには、具体的な IP アドレスを入力します。
Router# **clear ip admission cache** {* | *host ip address*}	認証プロキシ エントリを削除します。キャッシュ エントリすべてを削除するには、アスタリスクを使用します。シングル ホストのエントリを削除するには、具体的な IP アドレスを入力します。

次に、特定の IP アドレスのクライアントに対する Web ベース認証セッションを削除する例を示します。

```
Router# clear ip auth-proxy cache 209.165.201.1
```

Web ベース認証ステータスの表示

すべてのインターフェイスまたは特定のポートの Web ベース認証設定を表示するには、次の作業を行います。

コマンド	目的
Router# **show fm ip-admission l2http** [**all** | **interface** *type slot/port*]	Web ベース認証設定を表示します。 （任意）**all** キーワードを使用して、Web ベース認証を使用するすべてのインターフェイスを表示します。 （任意）特定のインターフェイスに対する Web ベース認証設定を表示するには、キーワード **interface** を使用します。

次に、グローバルな Web ベース認証のステータスだけを表示する例を示します。

```
Router# show fm ip-admission l2http all
```

次に、インターフェイス GigabitEthernet 3/27 の Web ベース認証を表示する例を示します。

```
Router# show fm ip-admission l2http interface gigabitethernet 3/27
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

ポート セキュリティ

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

ポート セキュリティの前提条件

なし。

ポート セキュリティの制約事項

- ポート セキュリティがデフォルト設定の場合に、errdisable ステートからすべてのセキュア ポートを回復させるには、**errdisable recovery cause psecure-violation** グローバル コンフィギュレーション コマンドを入力します。または、**shutdown** および **no shut down** 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、手動でセキュア ポートを再びイネーブルに戻すことができます。
- ダイナミックに学習されたすべてのセキュア アドレスを消去するには、**clear port-security dynamic** 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。
- 無許可の MAC アドレスは、特定のビット セットとともに学習されます。このビット セットにより、このアドレスから送信されるトラフィック、およびこのアドレス宛てに送信されるトラフィックはいずれもドロップされます。**show mac address-table** コマンドを使用すると、無許可の MAC アドレスを表示できますが、ビット ステートは表示されません （CSCeb76844）。
- スティッキ MAC アドレスがダイナミックに学習されたあとに、このアドレスを保持して、起動またはリロード後にポートに設定されるようにするには、**write memory** または **copy running-config startup-config** コマンドを入力して、アドレスを startup-config ファイルに保存する必要があります。
- ポート セキュリティは、Private VLAN（PVLAN; プライベート VLAN）ポートをサポートします。
- ポート セキュリティは、IEEE 802.1Q トンネル ポートをサポートします。
- ポート セキュリティは、スイッチド ポート アナライザ（SPAN）宛先ポートをサポートしません。
- ポート セキュリティは、EtherChannel ポートチャネル インターフェイスへのアクセスおよびトランキングをサポートします。
- ポート セキュリティと 802.1X ポートベース認証は同じポート上に設定できます。
- ポート セキュリティは、非交渉トランクをサポートします。
  - ポート セキュリティは、次のコマンドで設定したトランクだけをサポートします。

    switchport
    switchport trunk encapsulation
    switchport mode trunk
    switchport nonegotiate

  - セキュア アクセス ポートをトランクとして再設定すると、ポート セキュリティは、アクセス VLAN でダイナミックに学習されたこのポートのすべてのスティッキおよびスタティック セキュア アドレスを、トランクのネイティブ VLAN 上のスティッキまたはスタティック セキュア アドレスに変換します。ポート セキュリティによって、アクセス ポートの音声 VLAN 上のすべてのセキュア アドレスが削除されます。
  - セキュア トランクをアクセス ポートとして再設定すると、ポート セキュリティは、ネイティブ VLAN で学習されたすべてのスティッキおよびスタティック アドレスを、アクセス ポートのアクセス VLAN で学習されたアドレスに変換します。ポート セキュリティによって、ネイティブ VLAN 以外の VLAN で学習されたすべてのアドレスが削除されます。

（注） ポート セキュリティは、**switchport trunk native vlan** コマンドで設定した VLAN ID を使用します。

- 隣接スイッチ間で実行されている冗長リンクがある場合は、これらのスイッチに接続されているポートでポート セキュリティをイネーブルにする際に注意が必要です。これは、ポート セキュリティ違反が原因でポート セキュリティによってポートが errdisable に設定されるためです。

ポート セキュリティについて

ダイナミックに学習される MAC アドレスとスタティック MAC アドレスによるポート セキュリティ

ダイナミックに学習される MAC アドレス、およびスタティック MAC アドレスを使用したポート セキュリティでは、ポートへのトラフィック送信を許可する MAC アドレスを制限することで、ポートの入力トラフィックを制限できます。セキュア ポートにセキュア MAC アドレスを割り当てると、ポートは、定義されたアドレスのグループ外に送信元アドレスがある入力トラフィックを転送しません。セキュア MAC アドレスの数を 1 つに制限し、単一のセキュア MAC アドレスを割り当てると、そのポートに接続されているデバイスはそのポートの全帯域を使用できます。

次のいずれかの場合に、セキュリティ違反が発生します。

- ポート セキュリティは、セキュア MAC アドレスがセキュア ポートで最大数に達した場合に、識別されたどのセキュア MAC アドレスとも入力トラフィックの送信元 MAC アドレスが異なると、設定された違反モードを適用します。
- あるセキュア ポートで設定または学習されたセキュア MAC アドレスを持つトラフィックが、同一 VLAN 内の別のセキュア ポートにアクセスしようとすると、設定された違反モードが適用されます。

（注）　特定のセキュア ポートでセキュア MAC アドレスが設定または学習されたあと、同一 VLAN 上の別のポートでポート セキュリティがセキュア MAC アドレスを検出したときに発生する一連のイベントは、MAC 移動の違反と呼ばれます。

違反モードの詳細については、「ポートでのポート セキュリティ違反モードの設定」（P.85-6）を参照してください。

ポートにセキュア MAC アドレスの最大数を設定すると、ポート セキュリティによって、次のいずれかの方法でアドレス テーブルにセキュア アドレスが組み込まれます。

- すべてのセキュア MAC アドレスを、**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 コマンドを使用してスタティックに設定できます。
- 接続されているデバイスの MAC アドレスで、ポートがセキュア MAC アドレスをダイナミックに設定するようにすることができます。
- アドレス数をいくつかスタティックに設定し、残りのアドレスがダイナミックに設定されるようにすることができます。

ポートがリンクダウン状態になると、ダイナミックに学習されたアドレスはすべて削除されます。

起動、リロード、またはリンクダウン状態のあとは、ポートが入力トラフィックを受信するまで、ポート セキュリティは、ダイナミックに学習された MAC アドレスをアドレス テーブルに読み込みません。

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た時点で、アドレス テーブルにはない MAC アドレスからのトラフィックをポートが受信すると、セキュリティ違反となります。

protect、restrict、または shutdown の違反モードのいずれかにポートを設定できます。「ポート セキュリティの設定方法」（P.85-5）を参照してください。

アドレスの最大数を 1 に設定し、接続されたデバイスの MAC アドレスを設定すると、そのデバイスにはポートの全帯域幅が保証されます。

スティッキ MAC アドレスによるポート セキュリティ

スティッキ MAC アドレスを使用するポート セキュリティには、スタティック MAC アドレスによるポート セキュリティと同様の多数の利点がありますが、さらに、スティッキ MAC アドレスはダイナミックに学習できます。スティッキ MAC アドレスを使用したポート セキュリティでは、リンクダウン状態の発生中も、ダイナミックに学習された MAC アドレスを維持します。

write memory または **copy running-config startup-config** コマンドを入力すると、スティッキ MAC アドレスによるポート セキュリティは、ダイナミックに学習された MAC アドレスを startup-config ファイルに保存します。したがって、起動後または再起動後に、ポートが入力トラフィックからアドレスを学習する必要がありません。

IP Phone でのポート セキュリティ

図 85-1　　IP Phone を介して接続した装置

装置はスイッチに直接接続されていないため、スイッチでは、装置の接続が切断されている場合に、ポート リンクが失われていることを物理的に検出できません。最近の Cisco IP Phone は、Cisco Discovery Protocol（CDP）でホストの存在を示す Type Length Value（TLV）を送信して、接続されている装置のポートのリンク ステートの変更をスイッチに通知します。スイッチはホスト存在 TLV を認識します。ポート セキュリティでは、IP Phone のデータ ポートでのリンク ダウンを知らせる、ホストの存在を示す TLV 通知を受け取るとすぐに、スタティック MAC アドレス、スティッキ MAC アドレス、およびダイナミックに学習された MAC アドレスがすべてアドレス テーブルから削除されます。削除されたアドレスは、ダイナミックに学習されるかまたは設定された場合に限り、再び追加されます。

デフォルトのポート セキュリティ設定

機能	デフォルト設定
ポート セキュリティ	ディセーブル

機能	デフォルト設定
セキュア MAC アドレスの最大数	1.
違反モード	shutdown。セキュア MAC アドレスが最大数を超過した場合、ポートはシャットダウンし、SNMP トラップ通知が送信されます。

ポート セキュリティの設定方法

ポート セキュリティのイネーブル化

トランクでのポート セキュリティのイネーブル化

ポート セキュリティは、非交渉トランクをサポートします。

注意　セキュア アドレス数はデフォルトで 1 であり、違反に対するデフォルト アクションはポートのシャットダウンであるため、トランクでポート セキュリティをイネーブルにする前に、このポートのセキュア MAC アドレスの最大数を設定します（「ポートでのセキュア MAC アドレスの最大数の設定」（P.85-7）を参照）。

トランクでポート セキュリティ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	`Router(config)# interface {type slot/port | port-channel 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	`Router(config-if)# switchport`	ポートをレイヤ 2 ポートとして設定します。
ステップ 3	`Router(config-if)# switchport trunk encapsulation {isl | dot1q}`	カプセル化を 802.1Q として設定します。
ステップ 4	`Router(config-if)# switchport mode trunk`	無条件にポートをトランクに設定します。
ステップ 5	`Router(config-if)# switchport nonegotiate`	DTP を使用しないようにトランクを設定します。
ステップ 6	`Router(config-if)# switchport port-security`	トランクでポート セキュリティをイネーブルにします。
ステップ 7	`Router(config-if)# do show port-security interface type slot/port | include Port Security`	設定を確認します。

次に、ギガビット イーサネット ポート 5/36 を非交渉トランクとして設定し、ポート セキュリティをイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 5/36
Router(config-if)# switchport
Router(config-if)# switchport mode trunk
Router(config-if)# switchport nonegotiate
Router(config-if)# switchport port-security
Router(config-if)# do show port-security interface gigabitethernet 5/36 | include Port
Security
Port Security              : Enabled
```

アクセス ポートでのポート セキュリティのイネーブル化

アクセス ポートでポート セキュリティ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	Router(config)# **interface** {*type slot/port* | **port-channel** *channel_number*}	設定するインターフェイスを選択します。 **（注）** ポートは、トンネル ポートまたは PVLAN ポートとして使用できます。
ステップ 2	Router(config-if)# **switchport**	ポートをレイヤ 2 ポートとして設定します。
ステップ 3	Router(config-if)# **switchport mode access**	ポートをレイヤ 2 アクセス ポートとして設定します。 **（注）** デフォルト モード（dynamic desirable）のポートは、セキュア ポートとして設定できません。
ステップ 4	Router(config-if)# **switchport port-security**	ポートのポート セキュリティをイネーブルにします。
ステップ 5	Router(config-if)# **do show port-security interface** *type slot/port* **| include Port Security**	設定を確認します。

次に、ギガビット イーサネット ポート 5/12 でポート セキュリティをイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 5/12
Router(config-if)# switchport
Router(config-if)# switchport mode access
Router(config-if)# switchport port-security
Router(config-if)# do show port-security interface gigabitethernet 5/12 | include Port Security
Port Security              : Enabled
```

ポートでのポート セキュリティ違反モードの設定

ポートでポート セキュリティの違反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	Router(config)# **interface** {*type slot/port* | **port-channel** *channel_number*}	設定する LAN ポートを選択します。

	コマンド	目的
ステップ 2	`Router(config-if)# switchport port-security violation {protect | restrict | shutdown}`	（任意）違反モード、およびセキュリティ違反が検出されたときのアクションを設定します。
ステップ 3	`Router(config-if)# do show port-security interface type slot/port | include violation_mode`	設定を確認します。*violation_mode* の値は、**protect**、**restrict**、または **shutdown** です。

- **protect**：十分な数のセキュア MAC アドレスを削除して MAC アドレス数が最大値を下回るまで、PFC は送信元アドレスが不明なパケットをドロップします。
- **restrict**：十分な数のセキュア MAC アドレスを削除して MAC アドレス数が最大値を下回るまで、PFC は送信元アドレスが不明なパケットをドロップし、Security Violation カウンタを増分させます。
- **shutdown**：インターフェイスをただちに errordisable ステートにして、SNMP トラップ通知を送信します。

（注）　errdisable ステートからセキュア ポートを回復するには、**errdisable recovery cause** *violation_mode* 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。または、**shutdown** および **no shut down** 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、手動でセキュア ポートを再びイネーブルに戻すことができます。

次に、ギガビット イーサネット ポート 5/12 のセキュリティ違反モードを protect に設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 5/12
Router(config-if)# switchport port-security violation protect
Router(config-if)# do show port-security interface gigabitethernet 5/12 | include Protect
Violation Mode             : Protect
```

次に、ギガビット イーサネット ポート 5/12 のセキュリティ違反モードを restrict に設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 5/12
Router(config-if)# switchport port-security violation restrict
Router(config-if)# do show port-security interface gigabitethernet 5/12 | include Restrict
Violation Mode             : Restrict
```

ポートでのセキュア MAC アドレスの最大数の設定

セキュア MAC アドレスの最大数をポートに設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {type slot/port | port-channel 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	`Router(config-if)# switchport port-security maximum number_of_addresses vlan {vlan_ID | vlan_range}`	ポートに対し、セキュア MAC アドレスの最大数を設定します（デフォルトは 1）。 （注）　VLAN ごとの設定は、トランクだけでサポートされます。

- *number_of_addresses* の有効範囲は 1 ～ 4,097 です。
- ポート セキュリティは、トランクをサポートします。
  - トランクでは、トランクおよびトランク上のすべての VLAN に対して、セキュア MAC アドレスの最大数を設定できます。
  - セキュア MAC アドレスの最大数は、1 つの VLAN、または特定の VLAN 範囲に対して設定できます。
  - 特定の VLAN 範囲は、一組の VLAN 番号をダッシュ（-）でつなげて入力します。
  - 複数の VLAN 番号をカンマで区切って入力することも、一組の VLAN 番号をダッシュでつなげて入力することもできます。

次に、ギガビット イーサネット ポート 5/12 に対し、セキュア MAC アドレスの最大数を 64 に設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 5/12
Router(config-if)# switchport port-security maximum 64
Router(config-if)# do show port-security interface gigabitethernet 5/12 | include Maximum
Maximum MAC Addresses      : 64
```

スティッキ MAC アドレスによるポート セキュリティのポートでのイネーブル化

スティッキ MAC アドレスによるポート セキュリティをポート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	Router(config)# **interface** {*type slot/port* | **port-channel** *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	Router(config-if)# **switchport port-security mac-address sticky**	スティッキ MAC アドレスによるポート セキュリティをポートでイネーブルにします。

- **switchport port-security mac-address sticky** コマンドを入力すると、次のようになります。
  - ポートでダイナミックに学習されたすべてのセキュア MAC アドレスは、スティッキ セキュア MAC アドレスに変換されます。
  - スタティックなセキュア MAC アドレスは、スティッキ MAC アドレスに変換されません。
  - 音声 VLAN でダイナミックに学習されたセキュア MAC アドレスは、スティッキ MAC アドレスに変換されません。
  - ダイナミックに学習された新規のセキュア MAC アドレスは、スティッキ アドレスとなります。
- **no switchport port-security mac-address sticky** コマンドを入力すると、ポート上のすべてのスティッキ セキュア MAC アドレスは、ダイナミックなセキュア MAC アドレスに変換されます。

- スティッキ MAC アドレスがダイナミックに学習されたあとに、このアドレスを保持して、起動またはリロード後にポートに設定されるようにするには、**write memory** または **copy running-config startup-config** コマンドを入力して、アドレスを startup-config ファイルに保存する必要があります。

次に、スティッキ MAC アドレスによるポート セキュリティをギガビット イーサネット ポート 5/12 でイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 5/12
Router(config-if)# switchport port-security mac-address sticky
```

ポートでのスタティック セキュア MAC アドレスの設定

スタティック セキュア MAC アドレスをポートに設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** {*type slot/port* | **port-channel** *channel_number*}	設定する LAN ポートを選択します。
ステップ 2	Router(config-if)# **switchport port-security mac-address sticky** *mac_address* [**vlan** *vlan_ID*]	ポートに対し、スタティック MAC アドレスをセキュア アドレスとして設定します。 **（注）** VLAN ごとの設定は、トランクだけでサポートされます。
ステップ 3	Router(config-if)# **end**	コンフィギュレーション モードを終了します。

- スティッキ MAC アドレスによるポート セキュリティをイネーブルにしている場合に、スティッキ セキュア MAC アドレスを設定できます（「スティッキ MAC アドレスによるポート セキュリティのポートでのイネーブル化」（P.85-8）を参照）。
- **switchport port-security maximum** コマンドでポートに設定するセキュア MAC アドレスの最大数により、設定可能なセキュア MAC アドレスの数が定義されます。
- 最大数より少ないセキュア MAC アドレスを設定すると、残りの MAC アドレスはダイナミックに学習されます。
- トランクでは、ポート セキュリティがサポートされます。
  - トランクでは、VLAN 内でスタティック セキュア MAC アドレスを設定できます。
  - トランクでは、スタティック セキュア MAC アドレスに対応するように VLAN を設定していない場合、このアドレスは **switchport trunk native vlan** コマンドで設定した VLAN でセキュアとなります。

次に、ギガビット イーサネット ポート 5/12 で MAC アドレス 1000.2000.3000 をセキュア アドレスとして設定し、その設定を確認する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 5/12
Router(config-if)# switchport port-security mac-address 1000.2000.3000
Router(config-if)# end
Router# show port-security address
          Secure Mac Address Table
------------------------------------------------------------

Vlan    Mac Address       Type                  Ports
```

```
----    -----------       ----                 -----
   1    1000.2000.3000    SecureConfigured      Gi5/12
```

ポートでのセキュア MAC アドレスのエージング設定

（注）
- スタティック セキュア MAC アドレスおよびスティッキ セキュア MAC アドレスは、期限切れとなりません。
- **absolute** キーワードを使用してエージング タイプを設定すると、ダイナミックに学習されるすべてのセキュア アドレスは、エージング タイムを過ぎると期限切れとなります。**inactivity** キーワードを使用してエージング タイプを設定すると、エージング タイムは、ダイナミックに学習されたすべてのセキュア アドレスが期限切れとなるまでの非アクティブ期間として定義されます。

ポートでのセキュア MAC アドレスのエージング タイプの設定

セキュア MAC アドレスのエージング タイムをポートに設定できます。セキュア MAC アドレスのエージング タイプをポートに設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** {*type slot/port* | **port-channel** *channel_number*}	設定する LAN ポートを選択します。
ステップ 2	Router(config-if)# **switchport port-security aging type** {**absolute** | **inactivity**}	セキュア MAC アドレスのエージング タイプをポートに設定します（デフォルトは absolute）。

次に、ギガビット イーサネット ポート 5/12 のエージング タイプを inactivity に設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 5/12
Router(config-if)# switchport port-security aging type inactivity
Router(config-if)# do show port-security interface gigabitethernet 5/12 | include Type
Aging Type                : Inactivity
```

ポートでのセキュア MAC アドレスのエージング タイムの設定

セキュア MAC アドレスのエージング タイムをポートに設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** {*type slot/port* | **port-channel** *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	Router(config-if)# **switchport port-security aging time** *aging_time*	セキュア MAC アドレスのエージング タイムをポートに設定します。*aging_time* の有効範囲は 1 ～ 1440 分です（デフォルトは 0）。

次に、ギガビット イーサネット ポート 5/1 のセキュア MAC アドレス 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。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 5/1
Router(config-if)# switchport port-security aging time 120
Router(config-if)# do show port-security interface gigabitethernet 5/12 | include Time
Aging Time                 : 120 mins
```

ポート セキュリティの設定の確認

ポート セキュリティ設定を表示するには、次のコマンドを入力します。

コマンド	目的
Router# **show port-security** [**interface** {{**vlan** *vlan_ID*} | {*type slot/port*}}] [**address**]	スイッチまたは指定され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。

- ポート セキュリティでは、**vlan** キーワードはトランクだけでサポートされます。
- **address** キーワードを入力してセキュア MAC アドレスを表示すると、各アドレスのエージング情報（スイッチに対するグローバル情報、またはインターフェイスごとの情報）が表示されます。
- 次の値が表示されます。
  - 各インターフェイスで許可されるセキュア MAC アドレスの最大数
  - インターフェイスに設定されたセキュア MAC アドレスの数
  - 発生したセキュリティ違反の数
  - 違反モード

次に、インターフェイスを入力しない場合の **show port-security** コマンドの出力例を表示します。

```
Router# show port-security
Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                    (Count)        (Count)      (Count)
-------------------------------------------------------------------------------

     Gi5/1           11            11            0            Shutdown
     Gi5/5           15            5             0            Restrict
     Gi5/11          5             4             0            Protect
-------------------------------------------------------------------------------

Total Addresses in System: 21
Max Addresses limit in System: 128
```

次に、特定のインターフェイスに対する **show port-security** コマンドの出力例を示します。

```
Router# show port-security interface gigabitethernet 5/1
Port Security: Enabled
Port status: SecureUp
Violation mode: Shutdown
Maximum MAC Addresses: 11
Total MAC Addresses: 11
Configured MAC Addresses: 3
Aging time: 20 mins
Aging type: Inactivity
SecureStatic address aging: Enabled
Security Violation count: 0
```

次に、**show port-security address** 特権 EXEC コマンドの出力例を示します。

```
Router# show port-security address
          Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                  Ports   Remaining Age
                                                          (mins)
----    -----------       ----                  -----   -------------
   1    0001.0001.0001    SecureDynamic         Gi5/1       15 (I)
   1    0001.0001.0002    SecureDynamic         Gi5/1       15 (I)
   1    0001.0001.1111    SecureConfigured      Gi5/1       16 (I)
   1    0001.0001.1112    SecureConfigured      Gi5/1       -
   1    0001.0001.1113    SecureConfigured      Gi5/1       -
   1    0005.0005.0001    SecureConfigured      Gi5/5       23
   1    0005.0005.0002    SecureConfigured      Gi5/5       23
   1    0005.0005.0003    SecureConfigured      Gi5/5       23
   1    0011.0011.0001    SecureConfigured      Gi5/11      25 (I)
   1    0011.0011.0002    SecureConfigured      Gi5/11      25 (I)
------------------------------------------------------------------------
Total Addresses in System: 10
Max Addresses limit in System: 128
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

PART 14

合法的傍受

合法的傍受

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

合法的傍受の前提条件

- セキュア シェル（SSH）、たとえば、s72033-adventerprisek9-mz をサポートする実行イメージを実行している必要があります。合法的傍受は SSH をサポートしないイメージではサポートされません。
- 最高アクセス レベル（レベル 15）でスイッチにログインしている必要があります。レベル 15 のアクセス権でログインするには、**enable** コマンドを入力し、スイッチに対して定義された最高レベルのパスワードを指定します。
- コマンドライン インターフェイス（CLI）では、コマンドをグローバル コンフィギュレーション モードで発行する必要があります。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の合法的傍受をグローバルに設定できます。
- スイッチの時刻とメディエーション デバイスの時刻は同期する必要があります。スイッチとメディエーション デバイスの両方でネットワーク タイム プロトコル（NTP）を使用します。
- （任意）スイッチがメディエーション デバイスとの通信に使用するインターフェイスについて、ループバック インターフェイスを使用すると役立つ場合があります。ループバック インターフェイスを使用しない場合、スイッチ上の複数の物理インターフェイスで、ネットワーク障害を処理するために、メディエーション デバイスを設定する必要があります。

合法的傍受の制約事項

一般的な設定の制約事項

- VSS モードは合法的傍受をサポートしていません。
- ネットワーク管理者が、ノードに合法的傍受が展開されることを期待する場合、最適化された ACL ロギング（OAL）、VLAN アクセス コントロール リスト（VACL）キャプチャ、または侵入検知システム（IDS）をそのノードに設定しないでください。ノードに合法的傍受を展開すると、OAL、VACL キャプチャおよび IDS で予期しない動作が発生します。
- スイッチのパフォーマンスを維持するために、合法的傍受はアクティブ コールの 0.2 % 以下に制限されます。たとえば、スイッチが 4000 コールを処理している場合、それらのコールのうち 8 つのセッションを傍受できます。
- CISCO-IP-TAP-MIB は仮想ルーティングおよび転送（VRF）の OID citapStreamVRF をサポートしません。
- キャプチャされたトラフィックは、ルート プロセッサ上の CPU 使用率を保護するためにレート制限されています。レート制限は 8500 pps です。
- インターフェイス インデックスは、プロビジョニング中に合法的傍受をイネーブルにするインデックスを選択するためだけに使用されます。0 に設定すると、合法的傍受がすべてのインターフェイスに適用されます。
- （任意）スイッチとメディエーション デバイスの両方のドメイン名が、ドメイン ネーム システム（DNS）に登録されていることがあります。
- メディエーション デバイスには、アクセス ファンクション（AF）が必要です。
- メディエーション デバイスを、CISCO-TAP2-MIB ビューにアクセスできる SNMP ユーザ グループに追加する必要があります。グループに追加するユーザとして、メディエーション デバイスのユーザ名を指定します。

  メディエーション デバイスを CISCO-TAP2-MIB ユーザとして追加するときに、メディエーション デバイスの許可パスワードを指定する必要があります。パスワードの長さは、最低 8 文字である必要があります。
- 1 つのインターフェイスを合法的傍受処理専用にします。たとえば、QoS またはルーティングなどのプロセッサ集約的タスクを実行するインターフェイスを設定することはできません。
- IPv4 ユニキャスト トラフィックだけでサポートされます。また、傍受されるトラフィックでは、トラフィックが入力インターフェイスと出力インターフェイスの両方で IPv4 である必要があります。たとえば、合法的傍受では出力側が MPLS で入力側が IPv4 の場合、トラフィックを傍受できません。
- IPv4 マルチキャスト、IPv6 ユニキャスト、および IPv6 マルチキャスト フローはサポートされません。
- レイヤ 2 インターフェイスではサポートされません。ただし、合法的傍受は、レイヤ 2 インターフェイスを通して伝達される VLAN 上のトラフィックを傍受できます。
- 他のパケット内でカプセル化されるパケット（たとえば、トンネリング パケットまたは Q-in-Q パケット）に対してはサポートされていません。
- Q-in-Q パケットではサポートされません。合法的傍受のレイヤ 2 タップのサポートはありません。

- レイヤ 3 またはレイヤ 4 の書き換えの対象となるパケット（たとえば、ネットワーク アドレス変換（NAT）または TCP 反射式）に対してはサポートされていません。
- 入力方向では、後でパケットがドロップされる場合（たとえば、レート制限またはアクセス コントロール リスト（ACL）の **deny** ステートメントが原因で）、スイッチがパケットを傍受および複製します。出力方向では、パケットがドロップされる場合（たとえば、ACL による）、複製されません。
- 合法的傍受の ACL は、インターフェイスの入力および出力方向の両方に対して内部的に適用されます。
- 特定のユーザからのトラフィックを傍受するためには、一般的な構成は 2 つのフロー（各方向の 1 つずつ）から成ります。
- ハードウェア レート制限の対象のパケットは、合法的傍受で次のように処理されます。
  - レート リミッタによってドロップされるパケットは、傍受または処理されません。
  - レート リミッタを通過するパケットは、傍受および処理されます。
- 複数の LEA が 1 つのメディエーション デバイスを使用しており、それぞれが同じターゲットに対して傍受を実行している場合、スイッチは 1 つのパケットをメディエーション デバイスに送信します。各 LEA 用にパケットを複製するのは、メディエーション デバイスの役割です。
- 合法的傍受は、次の 1 つ以上のフィールドの組み合わせと一致する値の IPv4 パケットを傍受できます。
  - 宛先の IP アドレスとマスク
  - 宛先ポート範囲
  - 送信元 IP アドレスおよびマスク
  - 送信元ポート範囲
  - プロトコル ID

MIB ガイドライン

次の Cisco MIB が合法的傍受処理に使用されます。これらの MIB を合法的傍受 MIB の SNMP ビューに含めて、メディエーション デバイスがスイッチを通過するトラフィックに対する傍受を設定および実行できるようにします。

- CISCO-TAP2-MIB：両方のタイプの合法的傍受（通常およびブロードバンド）に必要です。
- CISCO-IP-TAP-MIB：レイヤ 3（IPv4）ストリームの傍受に必要です。通常およびブロードバンドの両方の合法的傍受でサポートされます。
- CISCO-IP-TAB-MIB では、次の機能に関して制限があります。
  - 次の機能の 1 つまたはすべてが設定され、機能しており、かつ合法的傍受がイネーブルの場合、合法的傍受が優先され、機能は次のように動作します。
    - 最適化された ACL ロギング（OAL）：機能しません。
    - VLAN アクセス コントロール リスト（VACL）キャプチャ：適切に動作しません。
    - 侵入検知システム（IDS）：適切に動作しません。

    この機能は、合法的傍受をディセーブルにした後または設定解除した後に開始されます。
  - IDS ではトラフィックを自分でキャプチャできませんが、合法的傍受によって傍受されたトラフィックだけはキャプチャします。

合法的傍受に関する情報

注意　このガイドは、合法的傍受の実装の法的義務に対応するものではありません。サービス プロバイダーには、そのネットワークが、適用される合法的傍受の法令および規制に適合することを保証する責任があります。法的な助言を求め、果たすべき義務を明確にすることを推奨します。

合法的傍受の概要

合法的傍受は、裁判所または行政機関による命令を根拠として、司法当局（LEA）が個人（ターゲット）に対して電子監視を実施できるようにするプロセスです。合法的傍受プロセスを容易にするために、特定の法律および規制によって、サービス プロバイダー（SP）およびインターネット サービス プロバイダー（ISP）に対して、許可された電子監視を明示的にサポートするようにネットワークを実装することが定められています。

監視は、音声、データ、およびマルチサービス ネットワークによる従来のテレコミュニケーションおよびインターネット サービスに対する傍受を使用して実行されます。LEA は、ターゲットのサービス プロバイダーに傍受を要求します。サービス プロバイダーには、その個人が送受信するデータ通信を傍受する責任があります。サービス プロバイダーは、ターゲットの IP アドレスを使用して、ターゲットのトラフィック（データ通信）を処理しているエッジ スイッチを判別します。次に、サービス プロバイダーは、ターゲットのトラフィックがスイッチを通過するときにそれを傍受し、傍受したトラフィックのコピーをターゲットに気付かれずに LEA に送信します。

合法的傍受機能は、米国内のサービス プロバイダーによる合法的傍受のサポート方法を定めた Communications Assistance for Law Enforcement Act（CALEA）をサポートしています。現在、合法的傍受は次の規格によって定義されています。

- Telephone Industry Association（TIA）仕様 J-STD-025
- Packet Cable Electronic Surveillance Specification（PKT-SP-ESP-101-991229）

シスコの合法的傍受ソリューションの詳細については、シスコの代理店にご連絡ください。

（注）　合法的傍受機能は、音声と日付の傍受を含む CISCO-IP-TAB-MIB のオブジェクト citapStreamprotocol の定義に従って IPv4 プロトコルの傍受をサポートします。

合法的傍受の利点

- 複数の LEA が相互に知られることなく同じターゲットに対して合法的傍受を実行できます。
- スイッチでの加入者サービスには影響しません。
- 入力と出力の両方向の傍受をサポートします。

- レイヤ 1 およびレイヤ 3 トラフィックの傍受をサポートします。レイヤ 2 トラフィックは、VLAN 上の IP トラフィックとしてサポートされます。
- 単一の物理インターフェイスを共有する個々の加入者の傍受をサポートします。
- ターゲットに気付かれません。ネットワーク管理者も通話者もパケットがコピーされていることや通話が傍受されていることに気付きません。
- 簡易ネットワーク管理プロトコル バージョン 3（SNMPv3）および View-based Access Control Model（SNMP-VACM-MIB）や User-based Security Model（SNMP-USM-MIB）などのセキュリティ機能を使用して、合法的傍受情報およびコンポーネントへのアクセスを制限します。
- 合法的傍受に関する情報を、最高特権を持つユーザ以外のユーザから秘匿します。管理者は、特権ユーザが法的傍受情報にアクセスできるアクセス権を設定する必要があります。
- 傍受を実行するための 2 つの保護されたインターフェイスがあります。1 つは傍受の設定用、もう 1 つは傍受したトラフィックの LEA への送信用です。

ボイスのための CALEA

音声用の法執行のための通信援助法（CALEA）によって、Voice over IP（VoIP）で伝送される音声会話の合法的傍受が認められています。スイッチは音声ゲートウェイ デバイスではありませんが、VoIP パケットはサービス プロバイダー ネットワークのエッジにあるスイッチを通過します。

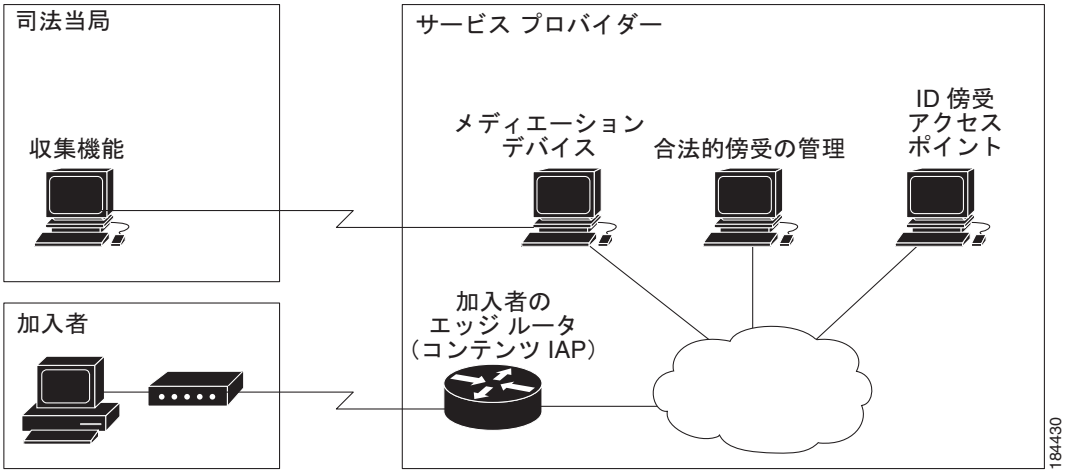
ある通話に注意を要すると認定された政府機関が判断した場合、ボイスのための CALEA は、会話を構成する IP パケットをコピーし、詳細な分析に適したモニタリング デバイスに重複パケットを送信します。

合法的傍受に使用されるネットワーク コンポーネント

- メディエーション デバイス
- 合法的傍受の管理
- 傍受アクセス ポイント
- コンテンツの傍受アクセス ポイント

合法的傍受処理については、「合法的傍受処理」（P.86-7）を参照してください。

図 86-1　　合法的傍受の概要



メディエーション デバイス

メディエーション デバイス（サードパーティ ベンダーから提供される）は、合法的傍受処理のほとんどを処理します。メディエーション デバイスは次の処理を行います。

- 合法的傍受の設定およびプロビジョニングに使用されるインターフェイスを提供します。
- 他のネットワーク デバイスに対して、合法的傍受を設定および実行する要求を生成します。
- 傍受したトラフィックを LEA が要求する形式（国によって異なる）に変換し、傍受したトラフィックのコピーをターゲットに気付かれずに LEA に送信します。

（注）　複数の LEA が同じターゲットに対して傍受を実行している場合、メディエーション デバイスは LEA ごとに傍受したトラフィックのコピーを作成する必要があります。メディエーション デバイスには、障害のために中断された合法的傍受を再開する役割もあります。

合法的傍受の管理

合法的傍受の管理（LIA）は、合法的傍受に認証インターフェイスや盗聴要求および管理を提供します。

傍受アクセス ポイント

傍受アクセス ポイント（IAP）は、合法的傍受に情報を提供するデバイスです。次の 2 つのタイプの IAP があります。

- Identification（ID）IAP : 傍受のための傍受関連情報（IRI）（ターゲットのユーザ名、システム IP アドレスなど）または、Voice over IP のコール エージェントを提供する認証、許可、アカウンティング（AAA）サーバなどのデバイス。IRI は、ターゲットのトラフィックが通過するコンテンツ IAP（スイッチ）をサービス プロバイダーが判別する場合に有用です。
- コンテンツ IAP : スイッチなどのターゲットのトラフィックが通過するデバイス。コンテンツ IAP は次の処理を行います。

- 司法命令で指定された期間、ターゲットが送受信するトラフィックを傍受します。傍受が気付かれないように、スイッチは宛先へのトラフィックの転送を継続します。
- 傍受したトラフィックのコピーを作成し、ユーザ データグラム プロトコル（UDP）パケットにカプセル化し、ターゲットに気付かれずにメディエーション デバイスにパケットを転送します。IP オプション ヘッダーはサポートされません。

（注）　コンテンツ IAP は、傍受したトラフィックの単一のコピーをメディエーション デバイスに送信します。複数の LEA が同じターゲットに対して傍受を実行している場合、メディエーション デバイスは LEA ごとに傍受したトラフィックのコピーを作成する必要があります。

コンテンツの傍受アクセス ポイント

コンテンツ IAP は、関連するデータ ストリームを傍受し、コンテンツを複製し、その後メディエーション デバイスに複製されたコンテンツを送信します。メディエーション デバイスは ID IAP およびコンテンツ IAP からデータを受信し、国別の要件に応じて必要な形式に情報を変換し、司法当局（LEA）に転送します。

合法的傍受処理

監視を実行する司法命令または令状を取得したあと、LEA はターゲットのサービス プロバイダーに監視を要求します。サービス プロバイダーの担当者は、メディエーション デバイスで実行される管理機能を使用して合法的傍受を設定し、ターゲットの電子トラフィックを（司法命令で定義された）特定の期間モニタリングします。

傍受を設定したあとは、ユーザの介入は必要ありません。管理機能が他のネットワーク デバイスと通信し、合法的傍受を設定および実行します。合法的傍受では、次の一連のイベントが発生します。

1. 管理機能は、ID IAP と通信して傍受関連情報（IRI）（ターゲットのユーザ名、システムの IP アドレスなど）を取得し、ターゲットのトラフィックが通過するコンテンツ IAP（スイッチ）を判別します。
2. ターゲットのトラフィックを処理するスイッチを特定したあと、管理機能は SNMPv3 の **get** および **set** 要求をスイッチの管理情報ベース（MIB）に送信し、合法的傍受を設定および有効化します。CISCO-TAP2-MIB は、加入者単位の傍受を提供する、サポートされた合法的傍受 MIB です。
3. 合法的傍受中に、スイッチは次の処理を行います。
   a. 着信および発信トラフィックを調べ、合法的傍受要求の指定と一致するトラフィックを傍受します。
   b. 傍受したトラフィックのコピーを作成し、ターゲットが疑いを持たないように元のトラフィックを宛先に転送します。
   c. 傍受したトラフィックを UDP パケットにカプセル化し、そのパケットをターゲットに気付かれずにメディエーション デバイスに転送します。

（注）　ターゲットのトラフィックの傍受および複製のプロセスによって、トラフィック ストリームに検出可能な遅延が発生することはありません。

4. メディエーション デバイスは、傍受したトラフィックを必要な形式に変換し、LEA で実行される収集機能に送信します。傍受したトラフィックはここに格納されて処理されます。

（注）　司法命令で許可されていないトラフィックをスイッチが傍受した場合、メディエーション デバイスは余分なトラフィックをフィルタで除外し、司法命令で許可されたトラフィックだけを LEA に送信します。

5. 合法的傍受の期間が終了すると、スイッチはターゲットのトラフィックの傍受を停止します。

合法的傍受 MIB

- CISCO-TAP2-MIB：合法的傍受処理に使用されます。
- CISCO-IP-TAP-MIB：レイヤ 3（IPv4）トラフィックを傍受する場合に使用されます。

CISCO-TAP2-MIB

CISCO-TAP2-MIB には合法的傍受を制御する SNMP 管理オブジェクトが含まれています。メディエーション デバイスはこの MIB を使用して、トラフィックがスイッチを通過するターゲットに対して合法的傍受を設定および実行します。

CISCO-TAP2-MIB には、スイッチで実行される合法的傍受に情報を提供する複数のテーブルが含まれています。

- cTap2MediationTable：スイッチで現在、合法的傍受を実行している各メディエーション デバイスに関する情報が含まれています。各テーブル エントリは、スイッチがメディエーション デバイスと通信するために使用する情報（デバイスのアドレス、傍受したトラフィックを送信するインターフェイス、傍受したトラフィックの送信に使用するプロトコルなど）を提供します。
- cTap2StreamTable：傍受するトラフィックを特定するために使用する情報が含まれています。各テーブル エントリには、合法的傍受のターゲットに関連するトラフィック ストリームを特定するために使用するフィルタへのポインタが含まれています。フィルタに一致するトラフィックが傍受およびコピーされて、対応するメディエーション デバイス アプリケーション（cTap2MediationContentId）に送信されます。

  cTap2StreamTable テーブルには、傍受されたパケット数のカウント、および傍受する必要があったが傍受されずにドロップされたパケットのカウントも含まれています。
- cTap2DebugTable：合法的傍受のエラーをトラブルシューティングするためのデバッグ情報が含まれています。

CISCO-TAP2-MIB には、合法的傍受イベントの複数の SNMP 通知も含まれています。MIB オブジェクトの詳細については、MIB 自体を参照してください。

CISCO-TAP2-MIB 処理

（メディエーション デバイスで実行される）管理機能によって、SNMPv3 の **set** および **get** 要求がスイッチの CISCO-TAP2-MIB に対して発行され、合法的傍受が設定および開始されます。このために、管理機能によって次の処理が実行されます。

1. cTap2MediationTable のエントリを作成し、スイッチが傍受を実行するメディエーション デバイスと通信する方法を定義します。

（注）　cTap2MediationNewIndex オブジェクトによって、メディエーション テーブル エントリの一意のインデックスが提供されます。

2. cTap2StreamTable にエントリを作成し、傍受するトラフィック ストリームを特定します。
3. cTap2StreamInterceptEnable を true(1) に設定し、傍受を開始します。スイッチは、傍受期間（cTap2MediationTimeout）が終了するまでストリーム内のトラフィックを傍受します。

CISCO-IP-TAP-MIB

CISCO-IP-TAP-MIB には、スイッチを通過する IPv4 トラフィック ストリームでの合法的傍受を設定および実行するための SNMP 管理オブジェクトが含まれています。この MIB は、CISCO-TAP2-MIB の拡張です。

CISCO-IP-TAP-MIB を使用して、次の 1 つ以上のフィールドの組み合わせと一致する値の IPv4 パケットを傍受するようにスイッチでの合法的傍受を設定できます。

- 宛先の IP アドレスとマスク
- 宛先ポート範囲
- 送信元 IP アドレスおよびマスク
- 送信元ポート範囲
- プロトコル ID

CISCO-IP-TAP-MIB 処理

データが傍受されると、2 つのストリームが作成されます。1 つ目のストリームは、ターゲット IP アドレスから他の IP アドレスに任意のポートを使用して送信されるパケット用です。2 つ目のストリームは、他のアドレスからターゲット IP アドレスに任意のポートを使用してルーティングされるパケットに対して作成されます。VoIP では、2 つのストリームが作成されます。1 つ目はターゲットからの RTP パケット用であり、2 つ目はターゲットへの RTP パケット用です。これらのパケットは、特定の送信元および宛先 IP アドレス、および RTP ストリームを設定するために使用される SDP 情報に指定されたポートを使用します。

合法的傍受サポートの設定方法

セキュリティに関する注意事項

- 合法的傍受の SNMP 通知は、メディエーション デバイス ポート上の UDP ポート 161（SNMP のデフォルトのポート 162 ではなく）に送信されます。手順については、「合法的傍受のための SNMP 通知のイネーブル化」（P.86-12）を参照してください。
- 合法的傍受 MIB にアクセスできるユーザは、メディエーション デバイス、およびスイッチでの合法的傍受について知る必要があるシステム管理者だけにします。また、これらのユーザには、合法的傍受 MIB にアクセスするための authPriv または authNoPriv アクセス権が必要です。NoAuthNoPriv アクセス権を持つユーザは、合法的傍受 MIB にアクセスできません。

- SNMP-VACM-MIB を使用して合法的傍受 MIB を含むビューを作成することはできません。
- デフォルトの SNMP ビューでは次の MIB は除外されています。

  CISCO-TAP2-MIB
  CISCO-IP-TAP-MIB
  SNMP-COMMUNITY-MIB
  SNMP-USM-MIB
  SNMP-VACM-MIB

「合法的傍受の制約事項」（P.86-2）と「合法的傍受の前提条件」（P.86-1）も参照してください。

合法的傍受 MIB へのアクセス

機密に関係するため、シスコの合法的傍受 MIB は合法的傍受機能をサポートするソフトウェア イメージだけで使用できます。これらの MIB には、Network Management Software MIBs Support ページ（http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml）からはアクセスできません。

合法的傍受 MIB へのアクセスの制限

合法的傍受 MIB へのアクセスは、メディエーション デバイスおよび合法的傍受について知る必要があるユーザだけに許可する必要があります。これらの MIB へのアクセスを制限するには、次の作業を実行する必要があります。

1. シスコの合法的傍受 MIB を含むビューを作成します。
2. このビューへの読み取りおよび書き込みアクセス権を持つ SNMP ユーザ グループを作成します。このユーザ グループに割り当てられたユーザだけが、MIB の情報にアクセスできます。
3. シスコの合法的傍受ユーザ グループにユーザを追加して、MIB および合法的傍受に関する情報にアクセスできるユーザを定義します。このグループのユーザとして、メディエーション デバイスを追加してください。追加しないと、スイッチで合法的傍受を実行できません。

（注）　シスコの合法的傍受 MIB ビューへのアクセスは、メディエーション デバイス、およびスイッチでの合法的傍受について知る必要があるシステム管理者だけに制限する必要があります。MIB にアクセスするには、スイッチ上でレベル 15 のアクセス権がユーザに必要です。

SNMPv3 の設定

次の手順を実行するには、スイッチで SNMPv3 が設定されている必要があります。次の資料を参照してください。

http://www.cisco.com/en/US/docs/ios-xml/ios/snmp/configuration/15-sy/snmp-15-sy-book.html

合法的傍受 MIB の制限付き SNMP ビューの作成

シスコの合法的傍受 MIB を含む SNMP ビューを作成し、ユーザを割り当てるには、グローバル コンフィギュレーション モードでレベル 15 のアクセス権を使用して、CLI で次の手順を実行します。コマンドの例については、「設定例」（P.86-11）を参照してください。

（注）　次の手順のコマンド構文には、各作業の実行に必要なキーワードだけが示されています。コマンド構文の詳細については、前の項（「SNMPv3 の設定」）に記載されているマニュアルを参照してください。

ステップ 1　スイッチで SNMPv3 が設定されていることを確認します。手順については、「SNMPv3 の設定」（P.86-10）に記載されているマニュアルを参照してください。

ステップ 2　CISCO-TAP2-MIB を含む SNMP ビューを作成します（*view_name* は、MIB 用に作成するビューの名前です）。この MIB は、通常とブロードバンドの両方の合法的傍受に必要です。

```
Router(config)# snmp-server view view_name ciscoTap2MIB included
```

ステップ 3　次の MIB の 1 つまたは両方を SNMP ビューに追加して、IPv4 ストリームに対する傍受のサポートを設定します（*view_name* は、ステップ 2 で作成したビューの名前です）。

```
Router(config)# snmp-server view view_name ciscoIpTapMIB included
```

ステップ 4　合法的傍受 MIB ビューにアクセスできる SNMP ユーザ グループ（*groupname*）を作成し、ビューに対するこのグループのアクセス権を定義します。

```
Router(config)# snmp-server group groupname v3 noauth read view_name write view_name
```

ステップ 5　作成したユーザ グループにユーザを追加します（*username* はユーザ、*groupname* はユーザ グループ、*auth_password* は認証パスワード）。

```
Router(config)# snmp-server user username groupname v3 auth md5 auth_password
```

（注）　SNMP ユーザ グループにメディエーション デバイスを追加してください。追加しないと、スイッチで合法的傍受を実行できません。合法的傍受 MIB ビューへのアクセスは、メディエーション デバイス、およびルータでの合法的傍受について知る必要があるシステム管理者だけに制限する必要があります。

これで、メディエーション デバイスは合法的傍受 MIB にアクセスして、SNMP の **set** および **get** 要求を発行し、スイッチ上で合法的傍受を設定および実行できるようになります。

SNMP 通知をメディエーション デバイスに送信するためのスイッチの設定方法については、「合法的傍受のための SNMP 通知のイネーブル化」（P.86-12）を参照してください。

設定例

次のコマンドは、メディエーション デバイスが合法的傍受 MIB にアクセスできるようにする方法の例です。

```
Router(config)# snmp-server view tapV ciscoTap2MIB included
Router(config)# snmp-server view tapV ciscoIpTapMIB included
```

1. 適切な合法的傍受 MIB（CISCO-TAP2-MIB および CISCO-IP-TAP-MIB）を含むビュー（tapV）を作成します。
2. tapV ビューの MIB への読み取り、書き込み、および通知アクセス権を持つユーザ グループ（tapGrp）を作成します。
3. メディエーション デバイス（ss8user）をユーザ グループに追加し、パスワード（ss8passwd）を使用して MD5 認証を指定します。

4. （任意）管理用に 24 文字の SNMP エンジン ID（123400000000000000000000 など）をスイッチに割り当てます。エンジン ID を指定しない場合は、自動的に生成されます。上記の例の最後の行に示されているように、エンジン ID の後ろのゼロは省略できることに注意してください。

（注）　エンジン ID を変更すると、SNMP ユーザ パスワードおよびコミュニティ ストリングに影響します。

合法的傍受のための SNMP 通知のイネーブル化

SNMP では、合法的傍受イベントの通知が自動的に生成されます（表 86-1 を参照）。これは、cTap2MediationNotificationEnable オブジェクトのデフォルト値が true(1) であるためです。

メディエーション デバイスに合法的傍受通知を送信するようにスイッチを設定するには、グローバル コンフィギュレーション モードでレベル 15 のアクセス権を使用して、次の CLI コマンドを発行します（*MD-ip-address* はメディエーション デバイスの IP アドレス、*community-string* は通知要求とともに送信するパスワードに似たコミュニティ ストリング）。

```
Router(config)# snmp-server host MD-ip-address community-string udp-port 161 snmp
Router(config)# snmp-server enable traps snmp authentication linkup linkdown coldstart
warmstart
```

- 合法的傍受では、**udp-port** は 161 である必要があります。162（SNMP のデフォルト）ではありません。
- 2 つ目のコマンドは、メディエーション デバイスに RFC 1157 通知を送信するようにスイッチを設定します。これらの通知は、認証の失敗、リンク ステータス（アップまたはダウン）、およびスイッチ再起動を示します。

表 86-1　合法的傍受イベントの SNMP 通知

通知	意味
cTap2MIBActive	スイッチは、CISCO-TAP2-MIB に設定されたトラフィック ストリームのパケットを傍受する準備ができています。
cTap2MediationTimedOut	合法的傍受が終了しました（cTap2MediationTimeout の期限切れのためなど）。
cTap2MediationDebug	cTap2MediationTable のエントリに関するイベントの場合、介入が必要になります。
cTap2StreamDebug	cTap2StreamTable のエントリに関するイベントの場合、介入が必要になります。

SNMP 通知のディセーブル

no snmp-server enable traps コマンドを入力して、SNMP 通知をディセーブルにできます。

合法的傍受通知をディセーブルにするには、SNMPv3 を使用して CISCO-TAP2-MIB オブジェクト cTap2MediationNotificationEnable を false(2) に設定します。SNMPv3 を通じて合法的傍受の通知を再度イネーブルにするには、オブジェクトに true（1）を再設定します。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

PART 15

付録

オンライン診断テスト

（注）

- オンライン診断テストの設定については、第 15 章「オンライン診断」を参照してください。
- オンライン診断テストをイネーブルにする前に、コンソール ロギングをイネーブルにしてすべての警告メッセージを表示してください。
- また、コンソールを介して接続している場合には、中断を伴うテストだけを実行するようにしてください。中断を伴うテストが完了すると、コンソールにシステムをリロードして通常の動作に戻すよう指示するメッセージが表示されます（確実にこの警告に従ってください）。
- テストの実行中、ポートを内部的にループしてストレス テストを行いますが、外部トラフィックがテスト結果に影響を与えることがあるため、すべてのポートがシャットダウンされます。スイッチを正常な稼働に戻すために、スイッチをリロードしなければなりません。スイッチをリロードするコマンドを入力すると、コンフィギュレーションを保存するかどうかを聞かれます。
- コンフィギュレーションは保存しないでください。
- 他のモジュール上でテストを実行している場合、テストが開始され、完了したら、モジュールをリセットする必要があります。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

グローバル ヘルス モニタリング テスト

TestAsicSync

このテストは、定期的にバスとポートの同期 ASIC のステータスを確認します。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	ディセーブルにしないでください。
デフォルト値：	オン
最初のリリース：	15.0(1)SY。
修正措置：	モジュールをリセットします。モジュールが 10 回連続して失敗した場合、または 3 回連続してリセットされた場合、電源が切断されます。
ハードウェア サポート：	すべてのモジュール。

TestEARLInternalTables

このテストでは、PFC と DFC のハードウェア テーブルに対する整合性検査を実行することにより、それらのハードウェア テーブルの大部分の問題を検出します。このテストは、5 分ごとに実行されます。

PFC のテストに失敗すると、次のいずれかが行われます。

- 冗長スーパーバイザ エンジンへのフェールオーバー
- 冗長スーパーバイザ エンジンが搭載されていない場合は、スーパーバイザ エンジンのシャットダウン

DFC のテストに失敗すると、次のいずれかが行われます。

- 最大で 2 回までの DFC 搭載モジュールのリセット
- 3 回めの失敗のあとにシャットダウン

CallHome がシステムに設定されている場合は、CallHome メッセージが生成されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	ディセーブルにしないでください。
デフォルト値：	オン
最初のリリース：	15.0(1)SY。
修正措置：	影響するモジュールをリセットします。
ハードウェア サポート：	PFC および DFC。

TestErrorCounterMonitor

このテストは、モジュール内に保持されているエラー カウンタに定期的にポーリングを行って、システム内の各モジュールで発生するエラーおよび中断をモニタします。エラー数がしきい値を超えた場合、エラーカウンタ ID、ポート番号、合計障害数、連続障害数、およびエラー カウンタの重大度を含む詳細情報とともに、Syslog メッセージが表示されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	ディセーブルにしないでください。CPU 使用率の急上昇中、このテストは精度を維持するために自動的にディセーブルになります。
デフォルト値：	オン
最初のリリース：	15.0(1)SY。
修正措置：	そのポートで検出されたエラーカウンタを示す Syslog メッセージを表示します。
ハードウェア サポート：	スーパーバイザ エンジンを含むすべてのモジュール

TestIntPortLoopback

このテストでは、スイッチング モジュールの内部ポートを使用してノンディスラプティブ ループバック テストを実行します。これは、ファブリック チャネルの障害およびポート ASIC の障害を検出するために使用できます。このテストは TestFabricCh0Health に似ています。このテストは、15 秒ごとに実行されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	このテストをオフにしないでください。ヘルス モニタリング テストとして使用してください。
デフォルト値：	オン
最初のリリース：	15.0(1)SY。
修正措置：	10 回連続して失敗すると、モジュールがリセットされます。3 回連続してリセットされると、モジュールの電源が切断されます。
ハードウェア サポート：	WS-X6148E-GE-45AT、WS-X6148A-GE-TX、WS-X6148A-GE-45AF、WS-X6148-FE-SFP、WS-X6148A-RJ-45、WS-X6148A-45AF。

TestL3TcamMonitoring

このテストは、レイヤ 3 パケット スイッチングを確認し、診断用のルックアップ キーを使用して FIB と CL TCAM の両方の状態をモニタします。このテストは、中断を伴わず、15 秒ごとに定期的に実行されます。10 回連続で失敗した場合は致命的として扱われ、モジュールは実行中にリロードされます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	ディセーブルにしないでください。
デフォルト値：	オン
最初のリリース：	15.0(1)SY。
修正措置：	モジュールが 10 回連続して失敗すると、モジュールは実行中にリロードされます。
ハードウェア サポート：	スーパーバイザ エンジン。

TestLtlFpoeMemoryConsistency

このテストでは、LTL および FPOE メモリが正常に動作していることを確認します。このテストは、15 秒ごとに実行されます。エラーが検出された場合は、自己修正が適用されます。自己修正に失敗した場合、モジュールをリセットする修正措置がトリガーされます。モジュールが 3 回連続してリセット

されると、モジュールの電源がオフになります。自己修正に成功した場合、修正措置は実行されません。短時間に多くの自己修正が実行されると（300 秒未満に 4 回以上の自己修正）、モジュールはリセットされます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	ディセーブルにしないでください。
デフォルト値：	オン
最初のリリース：	15.0(1)SY。
修正措置：	このテストに失敗すると、モジュールはリセットされます。リセットを 2 回行ったあとに電源がオフになります。
ハードウェア サポート：	スーパーバイザ エンジンを含むすべてのモジュール

TestMacNotification

このテストは、DFC 搭載モジュールとスーパーバイザ エンジン間のデータおよび制御パスを確認します。このテストは、また、レイヤ 2 MAC アドレス テーブルにおいてレイヤ 2 MAC アドレスの一貫性を保ちます。テストは、6 秒ごとに実行されます。テストが連続して 10 回失敗すると、起動時または実行時にモジュールがリセットされます（デフォルト）。3 回連続してリセットされると、モジュールの電源が切断されます。このテストは、15 秒ごとに実行されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	ディセーブルにしないでください。
デフォルト値：	オン
最初のリリース：	15.0(1)SY。
修正措置：	モジュールをリセットします。モジュールが 10 回連続して失敗した場合、または 3 回連続してリセットされた場合、電源が切断されます。
ハードウェア サポート：	DFC が装備されたモジュール

TestPortTxMonitoring

このテストは、定期的に各ポートの送信カウンタをポーリングします。テストでは syslog メッセージが表示され、設定されている間隔および障害しきい値に対してアクティビティが見られない場合、エラーによってポートがディセーブルになります。間隔およびしきい値を設定するには、**diagnostic monitor interval** コマンドおよび **diagnostic monitor threshold** コマンドを入力します。テストでパ

ケットを調達することはありませんが、定期的にパケットを送信する CDP プロトコルを利用します。CDP プロトコルがディセーブルになっている場合、そのポートに対するポーリングは行われません。テストは 75 秒ごとに実行され、障害しきい値はデフォルトで 5 に設定されています。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	ディセーブルにしないでください。
デフォルト値：	オン
最初のリリース：	15.0(1)SY。
修正措置：	障害の発生したポートを示す Syslog メッセージを表示します。エラーにより、障害の発生したポートはディセーブルになります。
ハードウェア サポート：	スーパーバイザ エンジンを含むすべてのモジュール

TestScratchRegister

このテストは、レジスタに値を書き込み、これらのレジスタからその値を読み取ることで、特定用途向け集積回路（ASIC）のヘルスをモニタします。テストは、30 秒ごとに実行されます。テストが連続して 5 回失敗すると、スーパーバイザ エンジンをテストしている場合はスーパーバイザ エンジンがスイッチオーバー（またはリセット）し、モジュールをテストしている場合はモジュールの電源が切断されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	ディセーブルにしないでください。
デフォルト値：	オン
最初のリリース：	15.0(1)SY。
修正措置：	誤作動しているスーパーバイザ エンジンをリセットするか、モジュールの電源を切断します。
ハードウェア サポート：	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、DFC 搭載モジュール、WS-X6148A-GE-TX、WS-X6148A-GE-45AF、WS-X6148-FE-SFP、WS-X6148A-RJ-45、WS-X6148A-45AF。

TestSnrMonitoring

このテストは、ポートの SNR（信号対雑音比）マージンをモニタします。この値は -12.7 dB ～ +12.7 dB の範囲で変わります。テストは、SNR を比較するために、次の 2 種類のしきい値レベルを使用します。

- +1.0 dB のマイナーしきい値
- 0.0 dB のメジャーしきい値

SNR 値がマイナーしきい値を下回ると、テストはマイナー警告メッセージを記録します。SNR 値がメジャーしきい値を下回ると、テストはメジャー警告メッセージを記録します。同様に、リカバリ メッセージは、SNR が 2 つのしきい値レベルを回復する場合に記録されます。テストのデフォルト間隔は 30 秒で、高速モニタリングの場合は 10 秒に設定できます。TestSnrMonitoring はブートアップ テストではなく、オンデマンドで実行できません。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	ディセーブルにしないでください。
デフォルト値：	オン
最初のリリース：	15.0(1)SY。
修正措置：	なし。
ハードウェア サポート：	WS-X6816-10T-2T、WS-X6716-10T。

TestUnusedPortLoopback

このテストは、実行時のスーパーバイザ エンジンとモジュールのネットワーク ポート間のデータ パスを定期的に検証します。このテストでは、レイヤ 2 のパケットはテスト ポートおよびスーパーバイザ エンジンのインバンド ポートに関連付けられた VLAN にフラッディングされます。パケットはテスト ポート内をループ バックして、同じ VLAN のスーパーバイザ エンジンに戻ります。このテストは TestLoopback に類似していますが、未使用（管理上停止）ネットワーク ポートとポート ASIC あたり 1 個の未使用ポート上でだけ実行されます。このテストは、現在の ASIC にノンディスラプティブ ループバック テストがないため、代用として使用します。このテストは、60 秒ごとに実行されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	ディセーブルにしないでください。CPU 使用率の急上昇中、このテストは精度を維持するために自動的にディセーブルになります。
デフォルト値：	オン
最初のリリース：	
修正措置：	障害の発生したポートを示す Syslog メッセージを表示します。スーパーバイザ エンジン以外のモジュールでは、すべてのポート グループに障害が発生した場合（たとえば、ポート ASIC ごとに少なくとも 1 つのポートで、すべてのポート ASIC の障害しきい値より多く障害が発生した場合）、デフォルトのアクションではモジュールがリセットされ、リセットを 2 回行ったあとにモジュールの電源を切断します。
ハードウェア サポート：	スーパーバイザ エンジンを含むすべてのモジュール。

ポート単位のテスト

TestActiveToStandbyLoopback

このテストは、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 エンジンのネットワーク ポート間のデータ パスを検証します。このテストでは、テスト ポートおよびアクティブ スーパーバイザ エンジンのインバンド ポートだけで構成されている VLAN にレイヤ 2 パケットがフラッ

ディングします。テスト パケットはターゲット ポートにループバックし、バスにフラッディングバックします（フラッディングされた VLAN では、アクティブ スーパーバイザ エンジンのインバンド ポートだけが待ち受けます）。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ループバック ポートの場合は、ディスラプティブです。中断する時間は、通常、1 秒未満です。中断時間は、ループバック ポートの設定（スパニングツリー プロトコルなど）によって異なります。
推奨事項：	ダウンタイムにスケジューリングします。
デフォルト値：	起動時または OIR を行ったあとに実行します。
最初のリリース：	15.0(1)SY。
修正措置：	ポートでループバック テストが失敗する場合、エラーによってポートがディセーブルになります。すべてのポートが失敗する場合は、スタンバイ スーパーバイザ エンジンをリセットします。
ハードウェア サポート：	スタンバイ スーパーバイザ エンジンだけ

TestCCPLoopback

このテストでは、コントロール プレーンのデータ パスをチェックします。このテストは、スーパーバイザ エンジンからワイヤレス サービス モジュール（WiSM2）のサービス ポートまたはハイ アベイラビリティ ポートに、オンライン診断パケットを送信します。TestCCPLoopback はテスト パケットがループ バックするかどうかを確認します。テストが失敗する場合、エラーを示すために、Syslog メッセージが表示されます。このテストは、ヘルス モニタリング、オンデマンド、予定されていたテストとしても実行できます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	ディセーブルにしないでください。
デフォルト値：	オン
最初のリリース：	15.0(1)SY1。
修正措置：	5 回連続して失敗したあとで Syslog メッセージが表示されます。
ハードウェア サポート：	WS-SVC-WISM2-K9。

TestDataPortLoopback

このテストは、スーパーバイザのインバンド ポートからファイアウォールまたは NAM サービス モジュールのデータ ポートに、データ パケットのパスを確認するためにパケットを送信します。パケットはハードウェアのスーパーバイザにループ バックされます。パケットがスーパーバイザから返されない場合、不良パスを特定するために、ハードウェア カウンタがポーリングされます。このテストは、45 秒ごとに実行されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	ディセーブルにしないでください。テストが連続して 10 回失敗した場合、モジュールがリセットされます。テストが常に失敗する場合、モジュールの電源がオフになります。
デフォルト値：	オン
最初のリリース：	15.0(1)SY1。
修正措置：	なし。
ハードウェア サポート：	WS-SVC-ASA-SM1-K9 および WS-SVC-NAM3-6G-K9。

TestDCPLoopback

このテストでは、データ プレーンのデータ パスをチェックします。このテストは、スーパーバイザ エンジンからワイヤレス サービス モジュール（WiSM2）のデータ ポートに、オンライン診断パケットを送信します。このテストでは、テスト パケットがループ バックするかどうかを確認します。テストが失敗する場合、エラーを示すために、Syslog メッセージが表示されます。このテストは、ヘルス モニタリング、オンデマンド、予定されていたテストとしても実行できます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	ディセーブルにしないでください。
デフォルト値：	オン
最初のリリース：	15.0(1)SY1。
修正措置：	5 回連続して失敗したあとで Syslog メッセージが表示されます。
ハードウェア サポート：	WS-SVC-WISM2-K9。

TestL2CTSLoopback

このテストは、スーパーバイザ エンジンのインバンド ポートから Ganita ASIC 内の各ポートに送信されたレイヤ 2 イーサネット パケットのカプセル化を提供します。このテストは、カプセル開放後に、元の内容とともに、スーパーバイザ エンジンのインバンド ポートにレイヤ 2 イーサネット パケットを返信します。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ディスラプティブ
推奨事項：	このテストは起動時に自動的に実行されます。オンデマンド テストもサポートされています。
デフォルト値：	オフ デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	スーパーバイザ エンジン。

TestL3CTSLoopback

このテストは、スーパーバイザ エンジンのインバンド ポートから Ganita ASIC 内の各ポートに送信されたレイヤ 3 IPv4 パケットのカプセル化を提供し、カプセル開放後に、元の内容とともに、スーパーバイザ エンジンのインバンド ポートにレイヤ 3 IPv4 パケットを返信します。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ディスラプティブ
推奨事項：	このテストは起動時に自動的に実行されます。オンデマンド テストもサポートされています。
デフォルト値：	オフ デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	スーパーバイザ エンジン。

TestLoopback

このテストは、スーパーバイザ エンジンとモジュールのネットワーク ポート間のデータ パスを検証します。このテストでは、テスト ポートおよびスーパーバイザ エンジンのインバンド ポートだけで構成されている VLAN にレイヤ 2 パケットがフラッディングします。パケットはポートにループバックし、同一 VLAN 上のスーパーバイザ エンジンに戻ります。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ループバック ポートの場合は、ディスラプティブです。中断する時間は、通常、1 秒未満です。中断時間は、ループバック ポートの設定（スパニングツリー プロトコルなど）によって異なります。
推奨事項：	ダウンタイムにスケジューリングします。
デフォルト値：	起動時または Online Insertion and Removal（OIR; ホットスワップ）を行ったあとに実行します。
最初のリリース：	15.0(1)SY。
修正措置：	ポートでループバック テストが失敗する場合、エラーによってポートがディセーブルになります。すべてのポートが失敗する場合は、モジュールをリセットします。
ハードウェア サポート：	スーパーバイザ エンジンを含むすべてのモジュール

TestMediaLoopback

このテストでは、Medianet のようなトラフィックのデータ パスを検証します。インデックス転送 UDP パケットは、テスト対象の MediaNet インターフェイスに送信されます。パケットはモジュールのインバンド ポートにループ バックされ、転送されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ディスラプティブ
推奨事項：	ディセーブルにしないでください。
デフォルト値：	オフ
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	WS-X6816-10T-2T、WS-X6716-10T、WS-X6816-10G-2T、WS-X6716-10GE、WS-X6848-SFP-2T、WS-X6748-SFP、WS-X6824-SFP-2T、WS-X6724-SFP、WS-X6848-TX-2T、WS-X6748-GE-TX。

TestMgmtPortsLoopback

このテストは、スーパーバイザのインバンド ポートからファイアウォールまたは NAM サービス モジュールに、バックプレーン ポートの状態を確認するためにパケットを送信します。パケットはハードウェアのスーパーバイザにループ バックされます。パケットがスーパーバイザから返されない場合、

サービス アプリケーションはパケットのステータスが照会され、サービス モジュールが指定するアクションによっては、syslog メッセージが表示され、モジュールがリセットされます。このテストは、30 秒ごとに実行されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	ディセーブルにしないでください。障害がファイアウォール モジュール内の場合は、どのポートがテストに失敗したかを示す syslog が出力されます。他のデータパスの問題が原因でテストが 10 回連続して失敗する場合、モジュールがリセットされます。テストが常に失敗する場合、モジュールの電源がオフになります。
デフォルト値：	オン
最初のリリース：	15.0(1)SY1。
修正措置：	なし。
ハードウェア サポート：	WS-SVC-ASA-SM1-K9 および WS-SVC-NAM3-6G-K9。

TestNetflowInlineRewrite

このテストは、NetFlow 検索操作、ACL の許可/拒否機能、およびポート ASIC のインライン書き換え機能を検証します。テスト パケットは、NetFlow テーブル検索を通じて書き換え情報を取得します。パケットがターゲット ポートに到着すると、VLAN および送信元/宛先 MAC アドレスが書き換えられます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ループバック ポートの場合は、ディスラプティブです。中断する時間は、通常、1 秒未満です。中断時間は、ループバック ポートの設定（スパニングツリー プロトコルなど）によって異なります。
推奨事項：	ダウンタイムにスケジューリングします。このテストは、起動時にだけ実行します。
デフォルト値：	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	スーパーバイザ エンジンを含むすべてのモジュール

TestNonDisruptiveLoopback

このテストは、スーパーバイザ エンジンとモジュールのネットワーク ポート間のデータ パスを検証します。このテストでは、レイヤ 2 パケットがテスト ポートのグループを含む VLAN にフラッディングされます。テスト ポート グループは、ポート ASIC チャネル当たり 1 つのポートで構成されています。

テスト ポート グループの各ポートは、パケットを中断せずにループバックし、スーパーバイザ エンジンのインバンド ポートに送り返します。テスト ポート グループの複数のポートが同時にテストされます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	ディセーブルにしないでください。
デフォルト値：	オン
最初のリリース：	15.0(1)SY。
修正措置：	連続して 10 回失敗すると、エラーによってポートがディセーブルになります。1 つのテスト サイクルですべてのポートがテストに失敗すると、エラーによってチャネルがディセーブルになります。すべてのチャネルが失敗する場合は、モジュールをリセットします。
ハードウェア サポート：	WS-X6148-FE-SFP、WS-X6148A-GE-TX、WS-X6148A-RJ-45。

TestNPLoopback

このテストでは、データ パスにエラーがないか ACE30 モジュールのデータ パスを確認します。このテストは起動時に実行され、デフォルト設定は、15 秒ごとに実行されるヘルス モニタリング テストです。TestNPLoopback が失敗すると、障害が発生したネットワーク プロセッサを示す SCP（Switch-Module Configuration Protocol）メッセージが ACE30 モジュールに送信されます。SCP メッセージを受信すると、ACE30 は修正処置を実行します。TestNPLoopback テストが 10 回連続して失敗すると、ACE30 モジュールがリセットされます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	ディセーブルにしないでください。
デフォルト値：	オン
最初のリリース：	15.0(1)SY1。
修正措置：	障害コードのテストに失敗したポートについて ACE30 に通知するために syslog メッセージが表示されます。障害コードに応じて、修正措置を取るかどうかを ACE30 が決定します。ACE30 の推奨措置は、コア ダンプをすべてのネットワーク プロセッサから収集し、ACE30 モジュールをリセットすることです。
ハードウェア サポート：	ACE30-MOD-K9。

TestTransceiverIntegrity

このセキュリティ テストは、トランシーバがサポートされていることを確認するためにトランシーバの活性挿抜（OIR）またはモジュールの起動時にトランシーバ上で実行されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	なし
デフォルト値：	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
最初のリリース：	15.0(1)SY。
修正措置：	エラーによってポートがディセーブルになります。
ハードウェア サポート：	トランシーバを使用するすべてのモジュール

PFC レイヤ 2 テスト

TestBadBpduTrap

このテストは、TestTrap テストと TestBadBpdu テストを組み合わせたものです（「DFC レイヤ 2 テスト」（P.A-17）を参照）。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	レイヤ 2 フォワーディング エンジンの学習機能で問題が発生している場合、このテストをオンデマンドで実行して、レイヤ 2 の学習機能を検証します。このテストは、ヘルス モニタリング テストとしても使用できます。
デフォルト値：	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	スーパーバイザ エンジンだけ

TestDontConditionalLearn

このテストは、TestDontLearn テストと TestConditionalLearn テストを組み合わせたものです（「DFC レイヤ 2 テスト」（P.A-17）を参照）。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	レイヤ 2 フォワーディング エンジンの学習機能で問題が発生している場合、このテストをオンデマンドで実行して、レイヤ 2 の学習機能を検証します。このテストは、ヘルス モニタリング テストとしても使用できます。
デフォルト値：	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	DFC が装備されたモジュール

TestMatchCapture

このテストは、TestProtocolMatchChannel テストと TestCapture テストを組み合わせたものです（「DFC レイヤ 2 テスト」（P.A-17）を参照）。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	このテストをオンデマンドで実行して、レイヤ 2 の学習機能を検証します。このテストは、ヘルス モニタリング テストとしても使用できます。
デフォルト値：	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	スーパーバイザ エンジンだけ

TestNewIndexLearn

このテストは、TestNewLearn テストと TestIndexLearn テストを組み合わせたものです（「DFC レイヤ 2 テスト」（P.A-17）を参照）。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	レイヤ 2 フォワーディング エンジンの学習機能で問題が発生している場合、このテストをオンデマンドで実行して、レイヤ 2 の学習機能を検証します。このテストは、ヘルス モニタリング テストとしても使用できます。
デフォルト値：	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	スーパーバイザ エンジンだけ

DFC レイヤ 2 テスト

TestBadBpdu

このテストは、スイッチ プロセッサに対するパケットのトラップまたはリダイレクトの機能を検証します。このテストは、レイヤ 2 フォワーディング エンジンの Trap 機能が正常に動作していることを確認します。スーパーバイザ エンジンでテストを実行する場合、スーパーバイザ エンジンのインバンド ポートから診断パケットが送信され、スーパーバイザ エンジンのレイヤ 2 フォワーディング エンジンを使用してパケット検索を実行します。DFC 搭載モジュールの場合、スーパーバイザ エンジンのイン

バンド ポートからスイッチ ファブリックを介して診断パケットが送信され、DFC ポートの 1 つからループバックされます。BPDU 機能は、レイヤ 2 フォワーディング エンジンによる診断パケット検索の実行時に検証されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ループバック ポートの場合は、ディスラプティブです。中断する時間は、通常、1 秒未満です。中断時間は、ループバック ポートの設定（スパニングツリー プロトコルなど）によって異なります。
推奨事項：	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
デフォルト値：	オフ
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	DFC が装備されたモジュール

TestCapture

このテストは、レイヤ 2 フォワーディング エンジンのキャプチャ機能が正常に動作していることを確認します。キャプチャ機能は、マルチキャスト レプリケーションで使用されます。スーパーバイザ エンジンでテストを実行する場合、スーパーバイザ エンジンのインバンド ポートから診断パケットが送信され、スーパーバイザ エンジンのレイヤ 2 フォワーディング エンジンを使用してパケット検索を実行します。DFC 搭載モジュールの場合、スーパーバイザ エンジンのインバンド ポートからスイッチ ファブリックを介して診断パケットが送信され、DFC ポートの 1 つからループバックされます。Capture 機能は、レイヤ 2 フォワーディング エンジンによる診断パケット検索の実行時に検証されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ループバック ポートの場合は、ディスラプティブです。中断する時間は、通常、1 秒未満です。中断時間は、ループバック ポートの設定（スパニングツリー プロトコルなど）によって異なります。
推奨事項：	ダウンタイムにスケジューリングします。
デフォルト値：	オフ
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	DFC が装備されたモジュール

TestConditionalLearn

このテストは、特定の条件下でレイヤ 2 送信元 MAC アドレスを学習する機能を検証します。スーパーバイザ エンジンでテストを実行する場合、スーパーバイザ エンジンのインバンド ポートから診断パケットが送信され、スーパーバイザ エンジンのレイヤ 2 フォワーディング エンジンを使用してパケット検索を実行します。DFC 搭載モジュールの場合、スーパーバイザ エンジンのインバンド ポートから

スイッチ ファブリックを介して診断パケットが送信され、DFC ポートの 1 つからループバックされます。Conditional Learn 機能は、レイヤ 2 フォワーディング エンジンによる診断パケット検索の実行時に検証されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ループバック ポートの場合は、ディスラプティブです。中断する時間は、通常、1 秒未満です。中断時間は、ループバック ポートの設定（スパニングツリー プロトコルなど）によって異なります。
推奨事項：	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
デフォルト値：	オフ
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	DFC が装備されたモジュール

TestDontLearn

このテストは、新しい送信元 MAC アドレスが学習されないときに、新しい送信元 MAC アドレスが MAC アドレス テーブルに読み込まれていないことを確認します。このテストは、レイヤ 2 フォワーディング エンジンの「学習しない」機能が正常に動作していることを確認します。DFC 搭載モジュールの場合、診断パケットはスーパーバイザ エンジンのインバンド ポートからスイッチ ファブリックを介して送信され、DFC 対応モジュール上のいずれかのポートからループ バックされます。「学習しない」機能は、レイヤ 2 フォワーディング エンジンによる診断パケット検索の実行時に検証されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ループバック ポートの場合は、ディスラプティブです。中断する時間は、通常、1 秒未満です。中断時間は、ループバック ポートの設定（スパニングツリー プロトコルなど）によって異なります。
推奨事項：	ダウンタイムにスケジューリングします。
デフォルト値：	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	DFC が装備されたモジュール

TestIndexLearn

このテストは、既存の MAC アドレス テーブル エントリが更新可能であることを確認します。このテストは、レイヤ 2 フォワーディング エンジンの Index Learn 機能が正常に動作していることを確認します。スーパーバイザ エンジンでテストを実行する場合、スーパーバイザ エンジンのインバンド ポートから診断パケットが送信され、スーパーバイザ エンジンのレイヤ 2 フォワーディング エンジンを使用してパケット検索を実行します。DFC 搭載モジュールの場合、スーパーバイザ エンジンのインバンド

ポートからスイッチ ファブリックを介して診断パケットが送信され、DFC ポートの 1 つからループバックされます。Index Learn 機能は、レイヤ 2 フォワーディング エンジンによる診断パケット検索の実行時に検証されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ループバック ポートの場合は、ディスラプティブです。中断する時間は、通常、1 秒未満です。中断時間は、ループバック ポートの設定（スパニングツリー プロトコルなど）によって異なります。
推奨事項：	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
デフォルト値：	オフ
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	DFC が装備されたモジュール

TestNewLearn

このテストは、レイヤ 2 フォワーディング エンジンのレイヤ 2 送信元 MAC アドレスの学習機能を検証します。スーパーバイザ エンジンの場合、スーパーバイザ エンジンのインバンド ポートから診断パケットが送信され、レイヤ 2 フォワーディング エンジンが診断パケットから新しい送信元 MAC アドレスを学習していることが確認されます。DFC 搭載モジュールの場合、スーパーバイザ エンジンのインバンド ポートからスイッチ ファブリックを介して診断パケットが送信され、DFC 対応モジュールの 1 つのポートからループバックされます。レイヤ 2 学習機能は、レイヤ 2 フォワーディング エンジンによる診断パケット検索の実行時に検証されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ループバック ポートの場合は、ディスラプティブです。中断する時間は、通常、1 秒未満です。中断時間は、ループバック ポートの設定（スパニングツリー プロトコルなど）によって異なります。
推奨事項：	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
デフォルト値：	オフ
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	DFC が装備されたモジュール

TestPortSecurity

このテストでは、セキュア MAC アドレスが別のポートからのパケットを送信する場合、CPU にパケットをリダイレクトする機能を検証します。スーパーバイザ エンジンの場合、診断パケットはスーパーバイザ エンジンのインバンド ポートから送信され、ポート セキュリティ機能は、レイヤ 2 フォワーディング エンジンによる診断パケット検索の実行時に検証されます。DFC を搭載したモジュールの場合、診断パケットはスーパーバイザ エンジンのインバンド ポートからファブリックを介して送信され、DFC 搭載モジュールの 1 つのポートでループ バックされます。ポート セキュリティ機能は、レイヤ 2 フォワーディング エンジンによる診断パケット検索の実行時に検証されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ディスラプティブ
推奨事項：	なし。
デフォルト値：	オフ
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	スーパーバイザ エンジンおよび DFC 搭載モジュール。

TestProtocolMatchChannel

このテストは、レイヤ 2 フォワーディング エンジンの特定のレイヤ 2 プロトコルを照合する機能を検証します。スーパーバイザ エンジンでテストを実行する場合、スーパーバイザ エンジンのインバンド ポートから診断パケットが送信され、スーパーバイザ エンジンのレイヤ 2 フォワーディング エンジンを使用してパケット検索を実行します。DFC 搭載モジュールの場合、スーパーバイザ エンジンのインバンド ポートからスイッチ ファブリックを介して診断パケットが送信され、DFC ポートの 1 つからループバックされます。Match 機能は、レイヤ 2 フォワーディング エンジンによる診断パケットのルックアップ中に確認されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ループバック ポートの場合は、ディスラプティブです。中断する時間は、通常、1 秒未満です。中断時間は、ループバック ポートの設定（スパニングツリー プロトコルなど）によって異なります。
推奨事項：	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
デフォルト値：	オフ
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	DFC が装備されたモジュール

TestStaticEntry

このテストは、レイヤ 2 MAC アドレス テーブルにスタティック エントリを読み込む機能を検証します。DFC 搭載モジュールの場合、スーパーバイザ エンジンのインバンド ポートからスイッチ ファブリックを介して診断パケットが送信され、DFC ポートの 1 つからループバックされます。Static Entry 機能は、レイヤ 2 フォワーディング エンジンによる診断パケット検索の実行時に検証されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ループバック ポートの場合は、ディスラプティブです。中断する時間は、通常、1 秒未満です。中断時間は、ループバック ポートの設定（スパニング ツリー プロトコルなど）によって異なります。
推奨事項：	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
デフォルト値：	オフ
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	DFC が装備されたモジュール

TestTrap

このテストは、スイッチ プロセッサに対するパケットのトラップまたはリダイレクトの機能を検証します。このテストは、レイヤ 2 フォワーディング エンジンの Trap 機能が正常に動作していることを確認します。スーパーバイザ エンジンでテストを実行する場合、スーパーバイザ エンジンのインバンド ポートから診断パケットが送信され、スーパーバイザ エンジンのレイヤ 2 フォワーディング エンジンを使用してパケット検索を実行します。DFC 搭載モジュールの場合、スーパーバイザ エンジンのインバンド ポートからスイッチ ファブリックを介して診断パケットが送信され、DFC ポートの 1 つからループバックされます。Trap 機能は、レイヤ 2 フォワーディング エンジンによる診断パケット検索の実行時に検証されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ループバック ポートの場合は、ディスラプティブです。中断する時間は、通常、1 秒未満です。中断時間は、ループバック ポートの設定（スパニング ツリー プロトコルなど）によって異なります。
推奨事項：	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
デフォルト値：	オフ
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	DFC が装備されたモジュール

PFC レイヤ 3 テスト

TestAclDeny

このテストは、レイヤ 2 およびレイヤ 3 フォワーディング エンジンの ACL 拒否機能が正常に動作していることを確認します。テストでは、入力、出力、レイヤ 2 リダイレクト、レイヤ 3 リダイレクト、およびレイヤ 3 ブリッジなどの各種の ACL 拒否シナリオを使用して、ACL 拒否機能が正常に動作しているかどうかを調べます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ディスラプティブ
推奨事項：	このテストをオンデマンドで実行します。
デフォルト値：	オン
最初のリリース：	15.0(1)SY。
修正措置：	自動 ASIC リセット（復旧用）
ハードウェア サポート：	スーパーバイザ エンジンおよび DFC 搭載モジュール。

TestAclPermit

このテストは、ACL 許可機能が正常に動作していることを確認します。特定の診断パケットを許可する ACL エントリが ACL TCAM にインストールされています。診断パケットが ACL TCAM エントリに一致し、適切に許可および転送されていることを確認するために、スーパーバイザ エンジンから対応する診断パケットが送信され、レイヤ 3 フォワーディング エンジンで検索されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ディスラプティブ
推奨事項：	このテストをオンデマンドで実行します。
デフォルト値：	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	スーパーバイザ エンジンおよび DFC 搭載モジュール。

TestAclRedirect

このテストは、レイヤ 3 フォワーディング エンジンの ACL リダイレクト機能を確認します。このテストでは、入力および出力のレイヤ 3 リダイレクトを確認します。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	このテストをオンデマンドで実行します。
デフォルト値：	オフ デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	スーパーバイザ エンジンおよび DFC 搭載モジュール。

TestDQUP

このテストは、診断パケットが QoS エントリと一致したときに、DQUP および PUP パケットを生成できるかどうかを確認します。このテストでは DQUP および PUP パケットを受信し、DQUP および PUP に含まれている情報が正しいことを確認します。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ディスラプティブ
推奨事項：	DQUP および PUP が正常に動作していないと考えられる場合は、このテストをオンデマンドで実行します。
デフォルト値：	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	スーパーバイザ エンジンおよび DFC 搭載モジュール。

TestInbandEdit

このテストは、レイヤ 3 フォワーディング エンジンの InbandEdit パケットを確認します。診断 NetFlow エントリおよび隣接エントリを 1 つずつ作成するために、InbandEdit 診断パケット 1 つが送信され、書き換えられた MAC および VLAN に基づいてこの InbandEdit パケットが転送されることを確認するために、診断パケットが 1 つ送信されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ディスラプティブ
推奨事項：	テストは、起動時に自動的に実行されます。オンデマンドもサポートされています。
デフォルト値：	このテストは、デフォルトでは、起動時に実行されます。
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	スーパーバイザ エンジンおよび DFC 搭載モジュール。

TestIPv4FibShortcut

このテストでは、次を確認します。

- レイヤ 3 フォワーディング エンジンの IPv4 FIB フォワーディングが正常に動作しているかどうかを確認します。1 つの診断 IPv4 FIB と隣接エントリがインストールされています。診断パケットが送信され、書き換えられた MAC および VLAN 情報に応じて診断パケットが転送されていることが確認されます。
- FIB TCAM および隣接デバイスが機能しているかどうかを確認します。各 FIB TCAM デバイスに FIB エントリが 1 つインストールされています。診断パケットが送信され、TCAM デバイスにインストールされた FIB TCAM エントリによって診断パケットがスイッチングされていることが確認されます。これは、完全な TCAM デバイス テストではありません。各 TCAM デバイスにはエントリが 1 つしかインストールされていません。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	ルーティング機能で問題が発生している場合は、このテストをオンデマンドで実行して、レイヤ 3 フォワーディング機能を検証します。このテストは、ヘルス モニタリング テストとしても使用できます。
デフォルト値：	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	スーパーバイザ エンジンおよび DFC 搭載モジュール。

TestIPv6FibShortcut

このテストは、レイヤ 3 フォワーディング エンジンの IPv6 FIB フォワーディングが正常に動作していることを確認します。1 つの診断 IPv6 FIB と隣接エントリがインストールされています。診断 IPv6 パケットが送信され、書き換えられた MAC および VLAN 情報に応じて診断パケットが転送されていることが確認されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	ルーティング機能で問題が発生している場合は、このテストをオンデマンドで実行して、レイヤ 3 フォワーディング機能を検証します。このテストは、ヘルス モニタリング テストとしても使用できます。
デフォルト値：	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	スーパーバイザ エンジンおよび DFC 搭載モジュール。

TestL3Capture2

このテストでは、レイヤ 3 フォワーディング エンジンのレイヤ 3 キャプチャ（キャプチャ 2）機能が正常に動作している確認します。このキャプチャ機能は、ACL ロギングおよび VACL ロギングに使用されます。1 つの診断 FIB およびキャプチャ 2 ビット セット付きの隣接エントリがインストールされています。診断パケットが送信され、キャプチャ ビット情報に応じて診断パケットが転送されていることが確認されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	このテストは、ヘルス モニタリング テストとしても使用できます。ACL または VACL ロギングを使用している場合は、ヘルス モニタリング テストとして使用してください。
デフォルト値：	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	スーパーバイザ エンジンおよび DFC 搭載モジュール。

TestMPLSFibShortcut

このテストでは、次を確認します。

- レイヤ 3 フォワーディング エンジンの MPLS フォワーディングが正常に動作していることを確認します。1 つの診断 MPLS FIB と隣接エントリがインストールされています。診断 MPLS パケットが送信され、隣接エントリの MPLS ラベルに応じて診断パケットが転送されていることが確認されます。
- レイヤ 3 フォワーディング エンジンの EoMPLS フォワーディングを確認します。1 つの診断 EoMPLS レイヤ 2 FIB と隣接エントリがインストールされています。診断レイヤ 2 パケットがフォワーディング エンジンに送信され、MPLS ラベルおよびカプセル化されたレイヤ 2 パケットに応じて転送されていることが確認されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	このテストは、ヘルス モニタリング テストとしても使用できます。MPLS トラフィックをルーティングする場合は、ヘルス モニタリング テストとして使用してください。
デフォルト値：	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	スーパーバイザ エンジンおよび DFC 搭載モジュール。

TestNATFibShortcut

このテストは、NAT 隣接情報に基づいてパケットを書き換える機能（宛先 IP アドレスの書き換え）を確認します。1 つの診断 NAT FIB と隣接エントリがインストールされています。診断パケットが送信され、書き換えられた IP アドレスに応じて診断パケットが転送されていることが確認されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	このテストは、ヘルス モニタリング テストとしても使用できます。宛先 IP アドレスが書き換えられている場合は、ヘルス モニタリング テストとして使用してください（たとえば、NAT を使用している場合）。
デフォルト値：	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	スーパーバイザ エンジンおよび DFC 搭載モジュール。

TestNetflowShortcut

このテストは、レイヤ 3 フォワーディング エンジンの NetFlow フォワーディング機能が正常に動作していることを確認します。1 つの診断 NetFlow エントリと隣接エントリがインストールされています。診断パケットが送信され、書き換えられた MAC および VLAN 情報に応じて診断パケットが転送されていることが確認されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ループバック ポートの場合は、ディスラプティブです。中断時間は、500 ミリ秒です。
推奨事項：	NetFlow が正常に動作していないと考えられる場合は、このテストをオンデマンドで実行します。
デフォルト値：	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	スーパーバイザ エンジンおよび DFC 搭載モジュール。

TestRBAcl

このテストは、レイヤ 3 フォワーディング エンジンのロール ベース ACL（RBACL）機能を確認します。このテストは src_ip/dest_ip の代わりに SGT と DGT を使用して、ACL 検索の結果を取得します。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	テストは、起動時に自動的に実行されます。オンデマンド テストおよびヘルス モニタリング テストもサポートされています。
デフォルト値：	このテストは、デフォルトでは、起動時に実行されます。
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	スーパーバイザ エンジンおよび DFC 搭載モジュール。

DFC レイヤ 3 テスト

TestAclDeny

このテストは、レイヤ 2 およびレイヤ 3 フォワーディング エンジンの ACL 拒否機能が正常に動作していることを確認します。テストでは、入力および出力レイヤ 2 リダイレクト、レイヤ 3 リダイレクト、およびレイヤ 3 ブリッジなどの各種の ACL 拒否シナリオを使用します。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ループバック ポートの場合は、ディスラプティブです。中断する時間は、通常、1 秒未満です。中断時間は、ループバック ポートの設定（スパニングツリー プロトコルなど）によって異なります。
推奨事項：	ACL を使用している場合は、ダウンタイムにスケジューリングします。
デフォルト値：	オフ
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	スーパーバイザ エンジンおよび DFC 搭載モジュール。

TestAclPermit

このテストは、ACL 許可機能が正常に動作していることを確認します。特定の診断パケットを許可する ACL エントリが ACL TCAM にインストールされています。診断パケットが ACL TCAM エントリに一致し、正常に許可および転送されていることを確認するために、スーパーバイザ エンジンから対応する診断パケットが送信され、レイヤ 3 フォワーディング エンジンで検索されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ループバック ポートの場合は、ディスラプティブです。中断する時間は、通常、1 秒未満です。中断時間は、ループバック ポートの設定（スパニングツリー プロトコルなど）によって異なります。
推奨事項：	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
デフォルト値：	オフ
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	スーパーバイザ エンジンおよび DFC 搭載モジュール。

TestAclRedirect

このテストは、レイヤ 3 フォワーディング エンジンの ACL リダイレクト機能を確認します。このテストでは、入力および出力のレイヤ 3 リダイレクトを確認します。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	このテストをオンデマンドで実行します。
デフォルト値：	オフ デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	DFC が装備されたモジュール

TestInbandEdit

このテストは、レイヤ 3 フォワーディング エンジンの InbandEdit パケットを確認します。診断 NetFlow エントリおよび隣接エントリを 1 つずつ作成するために、InbandEdit 診断パケット 1 つが送信され、書き換えられた MAC および VLAN に応じてこの InbandEdit パケットが転送されることを確認するために、診断パケットが 1 つ送信されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ディスラプティブ
推奨事項：	テストは、起動時に自動的に実行されます。オンデマンドもサポートされています。
デフォルト値：	オフ
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	DFC が装備されたモジュール

TestIPv4FibShortcut

このテストでは次を確認します。

- レイヤ 3 フォワーディング エンジンの IPv4 FIB フォワーディングが正常に動作しているかどうかを確認します。1 つの診断 IPv4 FIB と隣接エントリがインストールされています。診断パケットが送信され、書き換えられた MAC および VLAN 情報に応じて診断パケットが転送されていることが確認されます。
- FIB TCAM および隣接デバイスが機能しているかどうかを確認します。各 FIB TCAM デバイスに FIB エントリが 1 つインストールされています。診断パケットが送信され、TCAM デバイスにインストールされた FIB TCAM エントリによって診断パケットがスイッチングされていることが確認されます。これは、完全な TCAM デバイス テストではありません。各 TCAM デバイスにはエントリが 1 つしかインストールされていません。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ループバック ポートの場合は、ディスラプティブです。中断する時間は、通常、1 秒未満です。中断時間は、ループバック ポートの設定（スパニングツリー プロトコルなど）によって異なります。
推奨事項：	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
デフォルト値：	オフ
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	スーパーバイザ エンジンおよび DFC 搭載モジュール。

TestIPv6FibShortcut

このテストは、レイヤ 3 フォワーディング エンジンの IPv6 FIB フォワーディング機能が正常に動作していることを確認します。1 つの診断 IPv6 FIB と隣接エントリがインストールされています。診断 IPv6 パケットが送信され、書き換えられた MAC および VLAN 情報に応じて診断パケットが転送されていることが確認されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ループバック ポートの場合は、ディスラプティブです。中断する時間は、通常、1 秒未満です。中断時間は、ループバック ポートの設定（スパニングツリー プロトコルなど）によって異なります。
推奨事項：	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
デフォルト値：	オフ
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	スーパーバイザ エンジンおよび DFC 搭載モジュール。

TestL3Capture2

このテストでは、レイヤ 3 フォワーディング エンジンのレイヤ 3 キャプチャ（キャプチャ 2）機能が正常に動作している確認します。このキャプチャ機能は、ACL ロギングおよび VACL ロギングに使用されます。1 つの診断 FIB およびキャプチャ 2 ビット セット付きの隣接エントリがインストールされています。診断パケットが送信され、キャプチャ ビット情報に応じて診断パケットが転送されていることが確認されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ループバック ポートの場合は、ディスラプティブです。中断する時間は、通常、1 秒未満です。中断時間は、ループバック ポートの設定（スパニングツリー プロトコルなど）によって異なります。
推奨事項：	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
デフォルト値：	オフ
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	スーパーバイザ エンジンおよび DFC 搭載モジュール。

TestMPLSFibShortcut

このテストでは、次を確認します。

- レイヤ 3 フォワーディング エンジンの MPLS フォワーディングが正常に動作していることを確認します。1 つの診断 MPLS FIB と隣接エントリがインストールされています。診断 MPLS パケットが送信され、隣接エントリの MPLS ラベルに応じて診断パケットが転送されていることが確認されます。
- レイヤ 3 フォワーディング エンジンの EoMPLS フォワーディングを確認します。1 つの診断 EoMPLS レイヤ 2 FIB と隣接エントリがインストールされています。診断レイヤ 2 パケットがフォワーディング エンジンに送信され、MPLS ラベルおよびカプセル化されたレイヤ 2 パケットに応じて転送されていることが確認されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ループバック ポートの場合は、ディスラプティブです。中断する時間は、通常、1 秒未満です。中断時間は、ループバック ポートの設定（スパニングツリー プロトコルなど）によって異なります。
推奨事項：	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
デフォルト値：	オフ
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	スーパーバイザ エンジンおよび DFC 搭載モジュール。

TestNATFibShortcut

このテストは、NAT 隣接情報に基づいてパケットを書き換える機能（宛先 IP アドレスの書き換えなど）を確認します。1 つの診断 NAT FIB と隣接エントリがインストールされています。診断パケットがフォワーディング エンジンに送信され、診断パケットが書き換えられた IP アドレスに従って転送されていることが確認されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ループバック ポートの場合は、ディスラプティブです。中断する時間は、通常、1 秒未満です。中断時間は、ループバック ポートの設定（スパニングツリー プロトコルなど）によって異なります。
推奨事項：	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
デフォルト値：	オフ
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	スーパーバイザ エンジンおよび DFC 搭載モジュール。

TestNetflowShortcut

このテストは、レイヤ 3 フォワーディング エンジンの NetFlow フォワーディング機能が正常に動作していることを確認します。1 つの診断 NetFlow エントリと隣接エントリがインストールされています。診断パケットが送信され、書き換えられた MAC および VLAN 情報に応じて診断パケットが転送されていることが確認されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ループバック ポートの場合は、ディスラプティブです。中断する時間は、通常、1 秒未満です。
推奨事項：	NetFlow が正常に動作していないと考えられる場合は、このテストをオンデマンドで実行します。
デフォルト値：	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	スーパーバイザ エンジンおよび DFC 搭載モジュール。

TestRBAcl

このテストは、レイヤ 3 フォワーディング エンジンのロール ベース ACL（RBACL）機能を確認します。このテストは src_ip/dest_ip の代わりに SGT と DGT を使用して、ACL 検索の結果を取得します。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	テストは、起動時に自動的に実行されます。オンデマンド テストおよびヘルス モニタリング テストもサポートされています。
デフォルト値：	オフ
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	DFC が装備されたモジュール

レプリケーション エンジン テスト

TestEgressSpan

このテストは、両方の SPAN キューに対する書き換えエンジンの出力 SPAN レプリケーション機能が正常に動作していることを確認します。

属性	説明
ディスラプティブまたはノンディスラプティブ：	両方の SPAN セッションで、ディスラプティブです。中断する時間は、通常、1 秒未満です。
推奨事項：	このテストをオンデマンドで実行します。
デフォルト値：	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	スーパーバイザ エンジン、DFC 搭載モジュール。

TestIngressSpan

このテストは、ポート ASIC が入力 SPAN のパケットにタグ付けできることを確認します。このテストは、両方の SPAN キューに対する書き換えエンジンの入力 SPAN 操作が正常に動作していることも確認します。

属性	説明
ディスラプティブまたはノンディスラプティブ：	両方の SPAN セッションで、ディスラプティブです。モジュール上のループバック ポートの場合も、ディスラプティブです。中断時間は、ループバック ポートの設定（スパニングツリー プロトコルなど）によって異なります。
推奨事項：	このテストをオンデマンドで実行します。
デフォルト値：	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	スーパーバイザ エンジンおよび DFC 搭載モジュール。

TestL3VlanMet

このテストは、レプリケーション エンジンのマルチキャスト機能が正常に動作していることを確認します。レプリケーション エンジンは、2 つの異なる VLAN に診断パケットのマルチキャスト レプリケーションを実行するように設定されています。テストでは、スーパーバイザ エンジンのインバンド ポートから診断パケットが送信されたあと、レプリケーション エンジンに設定された 2 つの VLAN のインバンド ポートに 2 つのパケットが送り返されていることを確認します。

属性	説明
ディスラプティブまたはノンディスラプティブ：	スーパーバイザ エンジンの場合は、ノンディスラプティブです。 DFC が装備されたモジュールの場合は、ディスラプティブです。ループバック ポートで中断される時間は、通常、1 秒未満です。
推奨事項：	このテストをオンデマンドで実行して、レプリケーション エンジンのマルチキャスト レプリケーション機能をテストします。
デフォルト値：	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	スーパーバイザ エンジンおよび DFC 搭載モジュール。

ファブリック テスト

TestFabricCh0Health

このテストは、10 ギガビット モジュール上のファブリック チャネル 0 に対する入力および出力データ パスのヘルスを常にモニタします。テストは、5 秒ごとに実行されます。10 連続の失敗で修正不能であると診断され、モジュールがリセットされます。3 連続のリセット サイクルによって、ファブリックのスイッチオーバーが実行される場合があります。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	このテストをオフにしないでください。ヘルス モニタリング テストとして使用してください。
デフォルト値：	オン
最初のリリース：	15.0(1)SY。
修正措置：	10 回連続して失敗すると、モジュールがリセットされます。3 回連続してリセットされると、モジュールの電源が切断されます。
ハードウェア サポート：	WS-X6704-10GE。

TestFabricCh1Health

このテストは、10 ギガビット モジュール上のファブリック チャネル 1 に対する入力および出力データ パスのヘルスを常にモニタします。テストは、5 秒ごとに実行されます。10 連続の失敗で修正不能であると診断され、モジュールがリセットされます。3 連続のリセット サイクルによって、ファブリックのスイッチオーバーが実行される場合があります。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	このテストをオフにしないでください。ヘルス モニタリング テストとして使用してください。
デフォルト値：	オン
最初のリリース：	15.0(1)SY。
修正措置：	10 回連続して失敗すると、モジュールがリセットされます。3 回連続してリセットされると、モジュールの電源が切断されます。
ハードウェア サポート：	WS-X6704-10GE モジュール

TestFabricExternalSnake

このテストは、通常の OIR の起動時診断テスト段階でだけ、シャーシアクティブ スーパーバイザ エンジンで実行されます。このテストは、スーパーバイザ エンジンのインバンド ポートを介してテスト パケットを生成します。テスト データ パスには、ポート ASIC、スーパーバイザ エンジン内の書き換えエンジン ASIC、およびファブリック ASIC が含まれます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ディスラプティブ
推奨事項：	スーパーバイザ エンジンがオンラインになると、シャーシ アクティブ スーパーバイザ エンジンについてはオンデマンド診断によるこのテストがサポートされますが、シャーシ スタンバイ スーパーバイザ エンジンではサポートされません。
デフォルト値：	オフ
最初のリリース：	15.0(1)SY。
修正措置：	テストが失敗するということは重大な診断エラーであるため、スーパーバイザ エンジンがパワー リセットされます。
ハードウェア サポート：	アクティブ スーパーバイザ エンジン。

TestFabricFlowControlStatus

このテストでは、各ファブリック チャネルのフロー制御状態を検出するために、スイッチ ファブリック ASIC レジスタを読み取ります。フロー制御イベントは診断イベント キューに記録されます。デフォルトでは、このテストはヘルス モニタ テストとしてディセーブルです。イネーブルにすると、このテストは 15 秒ごとに実行されます。このテストでは、スロット単位またはチャネル単位のレート減少、現在のファブリック チャネル使用率、ピーク ファブリック チャネル使用率、および SP の CPU 使用率を入力方向と出力方向の両方で報告します。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	ヘルス モニタリング テストとして使用してください。ファブリック チャネルに問題があると考えられる場合、このテストを使用します。
デフォルト値：	オフ
最初のリリース：	15.0(1)SY。
修正措置：	フロー制御イベントは診断イベント ログに記録されます。
ハードウェア サポート：	スーパーバイザ エンジン。

TestFabricInternalSnake

このテストは、スーパーバイザ エンジンおよびファブリック スイッチング ASIC を搭載したモジュールでサポートされます。このテストは、ファームウェアがファブリック ASIC 全体を初期設定する起動中に、ファームウェア INIT シーケンス コードによって実行されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ディスラプティブ
推奨事項：	スーパーバイザ エンジンがオンラインになると、シャーシ スタンバイ スーパーバイザ エンジンについてはオンデマンド診断によるこのテストがサポートされますが、シャーシ アクティブ スーパーバイザ エンジンではサポートされません。ファブリック スイッチング ASIC を搭載したモジュールの場合、このテストは起動時診断でのみサポートされています。
デフォルト値：	オフ
最初のリリース：	15.0(1)SY。
修正措置：	テストに失敗すると、ファームウェア INIT シーケンスは失敗し、テスト対象のスーパーバイザ エンジンまたはモジュールはパワー リセットされます。
ハードウェア サポート：	スーパーバイザ エンジンおよびファブリック対応モジュール。

TestFabricVlanLoopback

このテストは、ハードウェアによって提供されるキューごとの VLAN ループバック機能を使用して、テスト対象のモジュールのインバンド ポートと、このインバンド ポートとの間で送受信されるトラフィックのスイッチングを処理するローカル ファブリック ポートの間のデータ パスを確認します。事前にプログラムされた VLAN ループバック レジスタと一致する VLAN を持つローカル ファブリック ポートの入力キューに、インバンド ポートからのテスト パケットが到着すると、テスト パケットはファブリックを通過し、同じファブリック ポートの出力キューにループバックし、このテスト パケットをインバンド ポートに返送します。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	テストは、起動時に自動的に実行されます。オンデマンドもサポートされています。このテストは、ローカル ファブリック チャネルとインバンド ポートの間のデータ パスの確認に使用するか、デバッグに使用します。
デフォルト値：	オフ
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	スーパーバイザ エンジンおよび DFC 搭載モジュール。

TestSynchedFabChannel

このテストは、モジュールおよびファブリック両方のファブリック同期化ステータスを定期的に確認します。ファブリック対応モジュールだけで使用できます。このテストはパケット スイッチング テストではないので、データ パスを伴いません。テストでは、モジュールとファブリックに SCP コントロール メッセージが送信されて、同期化ステータスの照会が行われます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	このテストをオフにしないでください。ヘルス モニタリング テストとして使用してください。
デフォルト値：	オン
最初のリリース：	15.0(1)SY。
修正措置：	5 回連続して失敗すると、モジュールがリセットされます。3 連続のリセット サイクルによって、モジュールの電源が切断されます。失敗の種類に応じて、ファブリックのスイッチオーバーが起動される場合があります。
ハードウェア サポート：	すべてのファブリック対応モジュール

完全メモリ テスト

- 「TestAclQosTcam」（P.A-41）
- 「TestAsicMemory」（P.A-41）
- 「TestEarlMemOnBootup」（P.A-42）

（注） メモリ テストを実行したあとにスーパーバイザ エンジンを再起動する必要があるため、他のモジュールでメモリ テストを実行してから、スーパーバイザ エンジンでメモリ テストを実行してください。オンデマンド オンライン診断テストの実行に関する詳細については、「オンデマンド オンライン診断の設定」（P.15-3）を参照してください。

TestAclQosTcam

このテストは、すべてのビットをテストし、PFC 上の ACL と QoS TCAM の両方の場所を確認します。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ディスラプティブ 約 1 時間、中断します。
推奨事項：	このテストを使用するのは、ハードウェアに問題があると考えられる場合、またはハードウェアをライブ ネットワークに設置する前だけにしてください。テストを行っているモジュールのバックグラウンドでトラフィックを実行しないでください。このテストの実行後に、スーパーバイザ エンジンを再起動する必要があります。
デフォルト値：	オフ
最初のリリース：	15.0(1)SY。
修正措置：	なし。
ハードウェア サポート：	スーパーバイザ エンジンを含むすべてのモジュール

TestAsicMemory

このテストは、アルゴリズムを使用して、モジュール上のメモリをテストします。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ディスラプティブ。約 1 時間、中断します。
推奨事項：	このテストを使用するのは、ハードウェアに問題があると考えられる場合、またはハードウェアをライブ ネットワークに設置する前だけにしてください。テストを行っているモジュールのバックグラウンドでトラフィックを実行しないでください。このテストの実行後に、スーパーバイザ エンジンを再起動する必要があります。
デフォルト値：	オフ
最初のリリース：	15.0(1)SY。
修正措置：	なし
ハードウェア サポート：	スーパーバイザ エンジンを含むすべてのモジュール

TestEarlMemOnBootup

このテストは起動時に実行され、すべてのビットと、Generic Memory Testing Logic（GMTL）でサポートされている EARL メモリの場所をテストします。EARL メモリは、起動時の初期化中にドライバによってテストされます。このテストでは、起動時テストの結果をドライバから取得して表示します。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	なし。
デフォルト値：	オフ
最初のリリース：	15.0(1)SY。
修正措置：	なし
ハードウェア サポート：	スーパーバイザ エンジンおよび DFC 搭載モジュール。

サービス モジュール テスト

TestPcLoopback

このテストでは、スーパーバイザと NAM サービス モジュール間の最も長いデータ パスを確認します。パケットはスーパーバイザからモジュールに送信され、PC によってスーパーバイザ エンジンにループバックされます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ディスラプティブ
推奨事項：	このテストは、起動時に自動的に実行されます。
デフォルト値：	オン
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	WS-SVC-NAM-1、WS-SVC-NAM-2。

TestPortASICLoopback

このテストでは、NAM サービス モジュールの ASIC ポートの状態を確認します。パケットはスーパーバイザ エンジンから送信され、ASIC でループ バックされます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ディスラプティブ
推奨事項：	このテストは、起動時に自動的に実行されます。
デフォルト値：	オン
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	WS-SVC-NAM-1、WS-SVC-NAM-2。

ストレス テスト

TestEobcStressPing

このテストは、スーパーバイザ エンジンとのモジュールの EOBC リンクのストレスをテストします。このテストは、スーパーバイザ エンジンがいくつかの sweep-ping プロセス（デフォルトでは 1 つ）を開始したときに起動します。sweep-ping プロセスは、20,000 SCP-ping パケットでモジュールの ping を処理します。各 packet-ping がタイムアウトする前にすべての 20,000 パケットが応答する場合（2 秒）、テストが正常に完了しています。テストが失敗する場合は、テスト時の EOBC バス上のトラフィック バーストを考慮して、5 回まで再試行できます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ディスラプティブ。数分間、中断します。
推奨事項：	このテストは、ネットワークに設置する前にハードウェア品質を調べるために使用します。
デフォルト値：	オフ
最初のリリース：	15.0(1)SY。
修正措置：	なし
ハードウェア サポート：	スーパーバイザ エンジン。

TestMicroburst

このテストは、連続失敗回数がしきい値に到達しない限り、ポート ASIC のパケット マイクロバーストをモニタし、SEA に記録します。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	ディセーブルにしないでください。
デフォルト値：	オン
最初のリリース：	15.0(1)SY。
修正措置：	なし
ハードウェア サポート：	スーパーバイザ エンジン 2T および DFC 搭載スイッチング モジュール。

TestNVRAMBatteryMonitor

このテストは、スーパーバイザ エンジンの NVRAM バッテリのステータスをモニタし、すべてのバッテリ ステータス変更を OBFL に記録します。バッテリ電圧が 3 日連続して特定のしきい値を下回ると、syslog が出力されます。NVRAM バッテリ ステータスの変更履歴を確認するには、**show logging onboard** コマンドを使用し、「NVRAM battery power」を調べます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	これは、1 時間ごとに実行される自動ヘルス モニタリング テストです。起動時に実行されず、オンデマンドで実行できません。
デフォルト値：	オン
最初のリリース：	15.0(1)SY。
修正措置：	このテストは、スーパーバイザ エンジンの NVRAM バッテリのステータスをモニタし、オンボード障害ロギング（OBFL）にバッテリ ステータス変更を記録します。**show logging onboard** コマンドの出力では、「NVRAM battery power」情報は NVRAM バッテリ ステータス履歴です。72 回連続して失敗すると、syslog にモジュールの交換が推奨されます。
ハードウェア サポート：	スーパーバイザ エンジン 2T。

TestTrafficStress

このテストは、モジュール上のすべてのポートを各ペアに設定して、スイッチと搭載されているモジュールでストレス テストを実行します。設定後、ペア間で相互にパケットが送信されます。パケットがスイッチを所定の期間通過できるように設定されると、テストによってパケットがドロップされていないことが確認されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ディスラプティブ。数分間、中断します。
推奨事項：	このテストは、ネットワークに設置する前にハードウェア品質を調べるために使用します。
デフォルト値：	オフ
最初のリリース：	15.0(1)SY。
修正措置：	なし
ハードウェア サポート：	スーパーバイザ エンジン。

一般的なテスト

ScheduleSwitchover

このテストは、オンライン診断スケジューリング機能を使用して、いつでもユーザがスイッチオーバーを起動できるようになっています。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ディスラプティブ
推奨事項：	ダウンタイムにこのテストをスケジューリングし、スイッチオーバー後のスタンバイ スーパーバイザ エンジンへの継承機能をテストします。
デフォルト値：	オフ
最初のリリース：	15.0(1)SY。
修正措置：	なし
ハードウェア サポート：	スーパーバイザ エンジン。

TestCFRW

このテストは、スーパーバイザ エンジンの CompactFlash ディスクを確認します。このテストは、システムの起動時またはディスクが挿入されるたびに実行されます。スロットにある各ディスクに 128 バイトの一時ファイルが書き込まれ、そのファイルから読み取りが行われます。コンテンツの読み取りがチェックされると、一時ファイルは削除されます。また、このテストは CLI からも実行できます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	ディセーブルにしないでください。トラフィックは影響を受けません。
デフォルト値：	オン
最初のリリース：	15.0(1)SY。
修正措置：	障害の発生したコンパクトフラッシュをフォーマットまたは交換します。
ハードウェア サポート：	リムーバブル CompactFlash デバイス。

TestFirmwareDiagStatus

このテストは、モジュールの起動時にファームウェアによって実行されるパワーオン診断テストの結果を表示します。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	このテストは起動時にだけ実行できます。
デフォルト値：	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
最初のリリース：	15.0(1)SY。
修正措置：	なし。システム メッセージ ガイドを参照してください。
ハードウェア サポート：	すべてのモジュール。

TestOBFL

このテストでは、オンボード障害ロギング機能を確認します。このテスト中、診断メッセージはモジュールに記録されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	このテストは起動時に自動的に実行され、オンデマンドで実行できません。
デフォルト値：	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
最初のリリース：	15.0(1)SY。
修正措置：	なし
ハードウェア サポート：	スーパーバイザ エンジン、DFC 搭載スイッチング モジュール、WS-SVC-WISM2。

TestRwEngineOverSubscription

これは、デフォルトでイネーブルではないヘルス モニタリング テストです。このテストは、モジュールで 1 秒ごとに実行され、書き換えエンジンがドロップ カウンタを取得することによってオーバーサブスクライブ状態になり、設定されているしきい値を超えた場合 syslog メッセージを生成するかどうかを確認します。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	このテストは、ヘルス モニタリング テストとしてだけ動作します。
デフォルト値：	オフ
最初のリリース：	15.0(1)SY。
修正措置：	なし
ハードウェア サポート：	スーパーバイザ エンジン、DFC 搭載モジュール。

TestVDB

このテストは、PoE 搭載モジュールで使用できます。このテストは、PoE ドーター カードで実行する診断テストの結果を問い合わせます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	このテストは、起動時に自動的に実行されます。
デフォルト値：	オフ
最初のリリース：	15.0(1)SY。
修正措置：	なし
ハードウェア サポート：	PoE ドーター カードを備えたモジュール。

クリティカル リカバリ テスト

- 「TestTxPathMonitoring」（P.A-48）

（注）　次のテストは、クリティカル リカバリ テストとも見なされます。

- 「TestFabricCh0Health」（P.A-37）
- 「TestFabricCh1Health」（P.A-37）
- 「TestSynchedFabChannel」（P.A-40）

TestTxPathMonitoring

このテストは、スーパーバイザ エンジンおよびサポートされているモジュールの各ポートに、ASIC 同期化を確認し、関連する問題を修正するために、インデックス誘導型パケットを定期的に送信します。テストは、2 秒ごとに実行されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ
推奨事項：	デフォルト設定を変更しないでください。
デフォルト値：	オン
最初のリリース：	15.0(1)SY。
修正措置：	なし（自己再生）
ハードウェア サポート：	スーパーバイザ エンジンおよび DFC 搭載モジュール。

ViSN テスト

TestRslHm

このテストでは、リモート スイッチとコア スイッチの間のデータおよび制御リンクをモニタします。診断パケットがリモート スイッチのスーパーバイザ エンジンのインバンド ポートからコア スイッチのスーパーバイザ エンジンのインバンド ポートに送信され、逆データ パス上で ping が実行されます。これは、リモート スイッチとアクティブおよびスタンバイ両方のコア スイッチ間の各 RSL リンクをテストします。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ノンディスラプティブ ヘルス モニタリング テスト。
推奨事項：	ディセーブルにしないでください。
デフォルト値：	オン
最初のリリース：	15.0(1)SY。
修正措置：	なし。詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート：	VSL 対応モジュール。

TestVSActiveToStandbyLoopback

このテストでは、仮想スイッチ リンクを通じた完全なデータ パスをテストする唯一の GOLD テストです。このテストでは、ループバック ポイントとしてスタンバイ仮想スイッチのスーパーバイザ エンジンのアップリンク ポートを選択し、アクティブ仮想スイッチのスーパーバイザ エンジンのインバンド ポートからシステムに VLAN フラッド パケットを送信します。アクティブおよびスタンバイ仮想スイッチのすべての VSL モジュールおよび VSL インターフェイスの FPOE および LTL VLAN フラッディング領域の設定によって、パケットは VSL 経由でスタンバイ仮想スイッチのスーパーバイザ エンジンのアップリンク ポートに到着し、そこからループ バックします。パケットは、スタンバイとアクティブ仮想スイッチの FPOE および LTL のプリコンフィギュレーションにより、アクティブ スーパーバイザ エンジンのインバンド ポートに戻ります。テスト障害が発生すると、エラー チェックが、アクティブおよびスタンバイ仮想スイッチの SP CPU、ファブリック フロー制御、およびその他のエラーのために実行されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ディスラプティブ
推奨事項：	このテストを実行する前に、すべてのヘルス モニタリング テストをディセーブルにしてください。このテストは、オンデマンド診断テストに対してだけ実行されます。
デフォルト値：	オフ
最初のリリース：	15.0(1)SY。
修正措置：	なし
ハードウェア サポート：	VSL 対応モジュール。

TestVslBridgeLink

このテストは、モジュールの起動時に VSL 対応モジュールおよびスーパーバイザ エンジンに診断カバレッジを提供します。このテストのデータ パスは、ローカルおよびリモート ブリッジのインバンド ポートに対応する 1 個のポートだけをループバック ポイントとして選択します。ハードウェアのブリッジ リンク機能を確認するために、診断パケットはスーパーバイザ エンジンのインバンド ポートから VSL モジュールのループバック ポイントに送信され、パケットは 2 つのファブリック データ パス コンプレックス間のブリッジ リンクを通過します。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ディスラプティブ
推奨事項：	このテストは、起動時に自動的に実行されます。
デフォルト値：	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
最初のリリース：	15.0(1)SY。
修正措置：	なし
ハードウェア サポート：	VSL 対応モジュール。

TestVslLocalLoopback

このテストでは、VSL リンク インターフェイスがアップ状態になる前に VSL モジュールの各ポートのハードウェア機能を確認します。このテストのデータ パスは、VSL モジュールによって抑制されます。診断パケットは、VSL モジュールのローカル インバンド ポートから各ポートに、ループバック テストを実行するために送信されます。このテストは、モジュールの起動時にのみ実行されます。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ディスラプティブ
推奨事項：	このテストは起動時に自動的に実行され、オンデマンドで実行できません。
デフォルト値：	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
最初のリリース：	15.0(1)SY。
修正措置：	なし
ハードウェア サポート：	VSL 対応モジュール。

TestVslStatus

このテストは、VSLP プロトコルで検出したステータス変更をレポートします。リンクの何らかの問題が VSLP プロトコルによって検出されると、リンク ステータスが変更され、その結果が適宜更新されます。このテストは、VSLP プロトコルによって要求されたハードウェアのステータスを確認するために、ループバック テストを起動します。

属性	説明
ディスラプティブまたはノンディスラプティブ：	ディスラプティブ
推奨事項：	このテストは、VSL モジュールがオンラインになると有効です。
デフォルト値：	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
最初のリリース：	15.0(1)SY。
修正措置：	なし
ハードウェア サポート：	VSL 対応モジュール。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

12.2SX QoS 設定からの移行

（注）
- この付録では、コマンドの移行時に発生する問題について説明します。移行が完了してから、設定に適用する変更を選択した場合の影響については説明しません。
- CLI で何らかの **mls qos** コマンドを入力すると警告が出ますが、無視されます。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

コマンドの移行

表 B-1　プラットフォーム固有グローバル コマンドの移行

12.2SX コマンドとコメント	移行アクション	SY のコマンドとコメント
`mls qos` • 他の設定を入力していない場合は、**mls qos** コマンドによって、キューイングとマーキングにおける大幅な変更が可能です。 • この付録に記載されている他の 12.2SX QoS コマンドの変換は、移行されるコンフィギュレーション ファイルに、その **mls qos** コマンドが含まれている場合に行われます。	変換	**`auto qos default`** 入力キューイング ポリシーが対応付けられていないポートで入力キューイングを設定します。出力キューイング ポリシーが対応付けられていないポートで出力キューイングを設定します。 • 設定に **mls qos marking ignore port-trust** コマンドが含まれていない場合は、移行により、サービス ポリシーが対応付けられていない各ポートのデフォルト以外の設定が実装されます。 – 信頼できない各ポートでは、リリース 12.2SX のデフォルト ポート ステート（「信頼できない」であり、これによりトラフィックをマーキング）を複製するために、移行によって、**platform qos trust none remark** インターフェイス コマンドが適用されます。これにより、すべての非 MPLS トラフィックがマーキングされます。 – 信頼できる各ポートでは、移行によって同等の **platform qos trust** インターフェイス コマンドが適用されます（**platform qos trust dscp** はデフォルトであるため、**mls qos trust dscp** コマンドで設定されたポートでは不要）。 **（注）** • **auto qos default** グローバル コンフィギュレーション コマンドは、QoS をグローバルにイネーブルにしません。SY には、QoS をイネーブルまたはディセーブルにするグローバル コマンドはありません。 • インターフェイスに対応付けられたサービス ポリシーは、そのインターフェイスの QoS 設定を定義します。一部の policy-map コマンドで必要な手動設定の詳細については、「プラットフォーム固有 policymap コマンドの移行」の表を参照してください。

表 B-1　プラットフォーム固有グローバル コマンドの移行 （続き）

12.2SX コマンドとコメント	移行アクション	SY のコマンドとコメント
`no mls qos` • これは、リリース 12.2SX のデフォルトです。 • 設定済みポリシーは無効で、すべての QoS ラベルは保持されます。	無視	• 同等の SY なし。SY のデフォルトの設定不可能状態に対応します。 • すべての設定済みポリシーは、有効です。 • IPv4 および IPv6 トラフィックの場合、受信した DSCP 値は保持され、受信した CoS は無視されて、受信した DSCP に基づく CoS 値がトラフィックに割り当てられます。 • MPLS トラフィックの場合、受信した EXP は保持され、受信した CoS は無視されて、受信した EXP に基づく CoS 値がトラフィックに割り当てられます。 • DSCP 値がないトラフィックの場合は、受信した CoS が保持されます。
`mls qos queueing-only` • 任意の設定済みサービス ポリシーに関係なく、ポリシングおよびマーキングをディセーブルにします（すべての入力 QoS ラベルを保持）。	変換	`platform qos queueing-only` • サービス ポリシーが設定されたポートを除き、ポリシングおよびマーキングをディセーブルにします（すべての入力 QoS ラベルを保持）。 • 入力キューイング ポリシーが対応付けられていないポートで入力キューイングを設定します。出力キューイング ポリシーが対応付けられていないポートで出力キューイングを設定します。
`no mls qos rewrite ip dscp`	変換	`no platform qos rewrite ip dscp` • このコマンドは、サービス ポリシー内の **set discard-class** コマンドまたは **set cos** コマンドを使用して設定されるポートごとの DSCP の透過性で、できるだけ早く置き換えてください。
`mls qos marking ignore port-trust` • リリース 12.2SX では、**mls qos marking ignore port-trust** が設定されている場合を除き、信頼できるポートでの policy trust コマンドは無視されます。	無視	同等の SY なし。SY のデフォルト状態に対応します。 • Cisco IOS Release 15.1SY では、設定されていれば、policy trust コマンドが常に反映され、設定済みのインターフェイス コマンドに関係なく、信頼できるポートで有効になります。 • 任意の設定済み 12.2SX **port trust** コマンドを無視できることを示すインジケータとして使用されます。
`mls qos marking statistics` • リリース 12.2SX では、1,023 個の集約ポリサーをサポートしており、このコマンドを設定すると、unpoliced トラフィック クラスのマーキング統計を提供するために、使用可能なポリサー カウントの一部が使用されます。	変換	**`platform qos marking statistics`** • リリース SY では、16,383 個の集約ポリサーをサポートしており、このコマンドを設定すると、unpoliced トラフィック クラスのマーキング統計を提供するために、使用可能なポリサー カウントの一部が使用されます。

表 B-1 プラットフォーム固有グローバル コマンドの移行 （続き）

12.2SX コマンドとコメント	移行アクション	SY のコマンドとコメント
mls qos police serial	無視	同等の SY なし。SY のデフォルトの設定不可能状態に対応します。
mls qos police redirected	無視	同等の SY なし。SY のデフォルトの設定不可能状態に対応します。
mls qos map cos-dscp	変換	table-map cos-discard-class-map
mls qos map dscp-cos	変換	table-map discard-class-cos-map
mls qos map dscp-exp	変換	table-map discard-class-exp-map
mls qos map exp-dscp	変換	table-map exp-discard-class-map
mls qos map ip-prec-dscp mls qos map precedence-dscp	変換	table-map precedence-discard-class-map
mls qos map policed-dscp normal-burst	変換	table-map policed-discard-class norm-burst-map
mls qos map policed-dscp max-burst	変換	table-map policed-discard-class max-burst-map
mls qos aggregate-policer • リリース 12.2SX では、最大 1,023 個の集約ポリサーの設定をサポートしています。police コマンド以外の一部の PFC QoS コマンドは、このカウントに含まれます。	変換	platform qos aggregate-policer • Cisco IOS Release 15.1SY では、最大 16,383 個の集約ポリサーの設定をサポートしています。police コマンド以外の一部の PFC QoS コマンドは、このカウントに含まれます。
mls qos protocol	変換	platform qos protocol • DoS の防止。
mls qos statistics-export	変換	platform qos statistics-export • QoS 統計情報のエクスポート。
mac packet-classify use vlan	無視	同等の SY なし。SY のデフォルトの設定不可能状態に対応します。
mls qos tunnel gre input uniform-mode	無視	同等の SY なし。SY のデフォルトの設定不可能状態に対応します。

表 B-2　Platform-Specific Interface-Mode コマンドの移行

12.2SX コマンドとメモ	移行アクション	SY のコマンドとメモ
`mls qos vlan-based` • **mls qos vlan-based** インターフェイス コマンドが設定されている場合、設定されたポートの信頼状態は、マーキングに影響します。	変換	`platform qos vlan-based` • **platform qos vlan-based** インターフェイス コマンドが設定されている場合、設定されたポートの信頼状態は、マーキングに影響しません。 • レイヤ 3 VLAN インターフェイスに対応付けられたサービス ポリシーは、**platform qos vlan-based** インターフェイス コマンドが設定されているポートの QoS を定義します。 • **platform qos vlan-based** インターフェイス コマンドで設定されたポートに対応付けられたサービス ポリシーは無視されます。
`mls qos trust cos` • **mls qos trust cos** インターフェイス コマンドが設定されている場合は、**no mls qos rewrite ip dscp** 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ない限り、入力 DSCP 値は CoS/DSCP マップの定義に従って書き換えられます。 • **mls qos trust cos** インターフェイス コマンドを設定すると、適用可能な policy trust コマンドも設定されている場合に、トラフィックをマーキングします。	変換	`platform qos trust cos` • **platform qos vlan-based** インターフェイス コマンドが設定されている場合は無視されます。 • 入力サービス ポリシーがポートに適用されており、**platform qos vlan-based** インターフェイス コマンドが設定されていない場合は無視されます。 • 入力 DSCP 値を書き換えません。
`mls qos trust dscp` • **mls qos trust dscp** インターフェイス コマンドを設定すると、適用可能な policy trust コマンドも設定されている場合に、トラフィックをマーキングします。	無視	同等の SY なし。SY のデフォルトの設定不可能状態に対応します。
`mls qos trust precedence` • **mls qos trust precedence** インターフェイス コマンドを設定すると、適用可能な policy trust コマンドも設定されている場合に、トラフィックをマーキングします。	無視	同等の SY なし。SY のデフォルト状態に対応します。入力 DSCP の下位 3 ビットはゼロにされません。
`no mls qos trust`	変換	`platform qos trust none remark` • **platform qos vlan-based** インターフェイス コマンドが設定されている場合は無視されます。 • 入力サービス ポリシーがポートに適用されており、**platform qos vlan-based** インターフェイス コマンドが設定されていない場合は無視されます。
`mls qos trust extend`	変換	`platform qos trust extend` • IP フォンのサポート。

表 B-2 Platform-Specific Interface-Mode コマンドの移行 （続き）

12.2SX コマンドとメモ	移行アクション	SY のコマンドとメモ
`mls qos trust device`	変換	`platform qos trust device` • IP フォンのサポート。
`mls qos mpls trust experimental`	変換	`platform qos mpls trust experimental`
`mls qos dscp-mutation`	変換	`platform qos dscp-mutation`
`mls qos exp-mutation`	変換	`platform qos exp-mutation`
`mls qos statistics-export`	変換	`platform qos statistics-export` • QoS 統計情報のエクスポート。
`mls qos bridged`	無視	同等の SY なし。マイクロフロー ポリシング設定の必要に応じて、自動的にイネーブルまたはディセーブルにします。
`mac packet-classify` • 入力トラフィックと出力トラフィックの両方に影響します。 • インターフェイスの制限リストに設定できます。	変換	`mac packet-classify input` • 入力トラフィックだけに影響します。 • **mac packet-classify output** コマンドは、出力トラフィックだけに影響します。
`mls qos loopback`	変換	`platform qos loopback`
`mls qos queue-mode mode-dscp`	変換	`platform qos queue-mode mode-dscp`
`mls qos cos` • トラフィックがマーキングされていると、元の入力 CoS 値が上書きされます。	変換	`platform qos cos` • 元の入力 CoS 値は、引き続き認識されます。 – IPv4 と IPv6 のトラフィックの場合、デフォルトでは、入力 CoS 値が DSCP 値で上書きされます。 – タグ付けされていない他のトラフィックの場合、デフォルトでは、設定されているポート CoS 値ではなく、入力 CoS 値が使用されます。 – 元の入力 CoS 値の代わりに、**platform qos cos** インターフェイス コマンドで設定された値を使用するには、**platform qos cos override** インターフェイス コマンドを使用します。

`wrr-queue bandwidth`
`wrr-queue cos-map`
`wrr-queue dscp-map`
`wrr-queue queue-limit`
`wrr-queue random-detect`
`wrr-queue threshold`
	変換	`wrr-queue bandwidth`
		`wrr-queue cos-map`
		`wrr-queue dscp-map`
		`wrr-queue queue-limit`
		`wrr-queue random-detect`
		`wrr-queue threshold`
		（注） これらのコマンドは、**platform qos queueing-only** または **auto qos default** 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だけ有効です。

表 B-2　Platform-Specific Interface-Mode コマンドの移行 （続き）

12.2SX コマンドとメモ	移行アクション	SY のコマンドとメモ

`rcv-queue bandwidth`
`rcv-queue cos-map`
`rcv-queue queue-limit`
`rcv-queue random-detect`
`rcv-queue threshold`
	変換	`rcv-queue bandwidth`
		`rcv-queue cos-map`
		`rcv-queue queue-limit`
		`rcv-queue random-detect`
		`rcv-queue threshold`
		
		（注）　これらのコマンドは、**platform qos queueing-only** または **auto qos default** 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だけ有効です。

`priority-queue cos-map`
`priority-queue queue-limit`
	変換	`priority-queue cos-map`
		`priority-queue queue-limit`
		
		（注）　これらのコマンドは、**platform qos queueing-only** または **auto qos default** 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だけ有効です。

`mls qos channel-consistency`	変換	`platform qos channel consistency` （注）　**auto qos default** 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にされます。

表 B-3　プラットフォーム固有 policymap コマンドの移行

12.2SX コマンド	移行アクション	SY コマンド
次の 12.2SX policy-map コマンドは SY 設定に伝播されますが、手動で置き換える必要があります。 • **trust dscp**: デフォルト。任意です。 • **trust ip precedence** または **trust precedence** : ポリシングの conform アクションとして **set dscp precedence** policy-map コマンドまたは **set-dscp-transmit precedence** で置き換えます。 • **trust cos**: ポリシングの conform アクションとして **set dscp cos** policy-map コマンドまたは **set-dscp-transmit cos** で置き換えます。		
`no trust`	無視	同等の SY なし。
`set {dscp | precedence} value`	変換	`set {dscp | precedence} value`
`police ... {exceed| violate} policed-dscp`	変換	`police ... {exceed| violate} policed-dscp`
`police flow ...`	変換	`police flow ...`
`police aggregate ...`	変換	`police aggregate ...`

グローバル コンフィギュレーション コマンドのキューイング パラメータ

次のキューイング パラメータは、**auto qos default** または **platform qos queueing-only** 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有効です。

キューイング パラメータ	デフォルト値		
1q2t ingress queue bandwidth allocation ratios	N/A		
1q2t ingress queue limits	N/A		
1q2t strict-priority ingress queue	N/A		
1q2t standard ingress queue	しきい値 1	CoS	0、1、2、3、4
		DSCP	サポート対象外
		テールドロップ	80%
		WRED ドロップ	サポート対象外
	しきい値 2	CoS	5、6、7
		DSCP	サポート対象外
		テールドロップ	100%（設定はできません）
		WRED ドロップ	サポート対象外

キューイング パラメータ （続き）	デフォルト値 （続き）		
1q8t ingress queue bandwidth allocation ratios	N/A		
1q8t ingress queue limits	N/A		
1q8t strict-priority ingress queue	N/A		
1q8t standard ingress queue	しきい値 1	CoS	0
		DSCP	サポート対象外
		テールドロップ	50 %
		WRED ドロップ	サポート対象外
	しきい値 2	CoS	なし
		DSCP	サポート対象外
		テールドロップ	50 %
		WRED ドロップ	サポート対象外
	しきい値 3	CoS	1、2、3、4
		DSCP	サポート対象外
		テールドロップ	60 %
		WRED ドロップ	サポート対象外
	しきい値 4	CoS	なし
		DSCP	サポート対象外
		テールドロップ	60 %
		WRED ドロップ	サポート対象外
	しきい値 5	CoS	6 および 7
		DSCP	サポート対象外
		テールドロップ	80%
		WRED ドロップ	サポート対象外
	しきい値 6	CoS	なし
		DSCP	サポート対象外
		テールドロップ	80%
		WRED ドロップ	サポート対象外
	しきい値 7	CoS	5
		DSCP	サポート対象外
		テールドロップ	100 %
		WRED ドロップ	サポート対象外
	しきい値 8	CoS	なし
		DSCP	サポート対象外
		テールドロップ	100 %
		WRED ドロップ	サポート対象外

キューイング パラメータ （続き）	デフォルト値 （続き）		
1p1q4t ingress queue bandwidth allocation ratios	N/A		
1p1q4t ingress queue limits	N/A		
1p1q4t strict-priority ingress queue		CoS	5
		DSCP	サポート対象外
		テールドロップ	100%（設定はできません）
		WRED ドロップ	サポート対象外
1p1q4t standard ingress queue	しきい値 1	CoS	0 および 1
		DSCP	サポート対象外
		テールドロップ	50 %
		WRED ドロップ	サポート対象外
	しきい値 2	CoS	2 および 3
		DSCP	サポート対象外
		テールドロップ	60 %
		WRED ドロップ	サポート対象外
	しきい値 3	CoS	4
		DSCP	サポート対象外
		テールドロップ	80%
		WRED ドロップ	サポート対象外
	しきい値 4	CoS	6 および 7
		DSCP	サポート対象外
		テールドロップ	100 %
		WRED ドロップ	サポート対象外
1p1q8t ingress queue bandwidth allocation ratios	N/A		
1p1q8t ingress queue limits	N/A		
1p1q8t strict-priority ingress queue		CoS	5
		DSCP	サポート対象外
		テールドロップ	100%（設定はできません）
		WRED ドロップ	サポート対象外

キューイング パラメータ （続き）	デフォルト値 （続き）		
1p1q8t standard ingress queue	しきい値 1	CoS	0
		DSCP	サポート対象外
		テールドロップ	ディセーブル、70%
		WRED ドロップ	イネーブル、ロー：40%、ハイ：70%
	しきい値 2	CoS	1
		DSCP	サポート対象外
		テールドロップ	ディセーブル、70%
		WRED ドロップ	イネーブル、ロー：40%、ハイ：70%
	しきい値 3	CoS	2
		DSCP	サポート対象外
		テールドロップ	ディセーブル、80%
		WRED ドロップ	イネーブル、ロー：50%、ハイ：80%
	しきい値 4	CoS	3
		DSCP	サポート対象外
		テールドロップ	ディセーブル、80%
		WRED ドロップ	イネーブル、ロー：50%、ハイ：80%
	しきい値 5	CoS	4
		DSCP	サポート対象外
		テールドロップ	ディセーブル、90%
		WRED ドロップ	イネーブル、ロー：60%、ハイ：90%
	しきい値 6	CoS	6
		DSCP	サポート対象外
		テールドロップ	ディセーブル、90%
		WRED ドロップ	イネーブル、ロー：60%、ハイ：90%
	しきい値 7	CoS	7
		DSCP	サポート対象外
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：70%、ハイ：100%
2q8t ingress queue bandwidth allocation ratios	90:10		
2q8t ingress queue limits	ロー プライオリティ：80%		
	ハイ プライオリティ：20%		
2q8t strict-priority ingress queue	N/A		

キューイング パラメータ （続き）	デフォルト値 （続き）		
2q8t standard ingress queue 2（ハイ プライオリティ）	しきい値 1	CoS	5
		DSCP	サポート対象外
		テールドロップ	100 %
		WRED ドロップ	サポート対象外
	しきい値 2 ～ 8	CoS	なし
		DSCP	サポート対象外
		テールドロップ	100 %
		WRED ドロップ	サポート対象外
2q8t standard ingress queue 1（ロー プライオリティ）	しきい値 1	CoS	0 および 1
		DSCP	サポート対象外
		テールドロップ	70%
		WRED ドロップ	サポート対象外
	しきい値 2	CoS	2 および 3
		DSCP	サポート対象外
		テールドロップ	80%
		WRED ドロップ	サポート対象外
	しきい値 3	CoS	4
		DSCP	サポート対象外
		テールドロップ	90 %
		WRED ドロップ	サポート対象外
	しきい値 4	CoS	6 および 7
		DSCP	サポート対象外
		テールドロップ	100 %
		WRED ドロップ	サポート対象外
	しきい値 5 ～ 8	CoS	なし
		DSCP	サポート対象外
		テールドロップ	100 %
		WRED ドロップ	サポート対象外
8q4t ingress queue bandwidth allocation ratios	90:0:0:0:0:0:0:10		
8q4t ingress queue limits	ロー プライオリティ：80%		
	中間キュー：0%		
	ハイ プライオリティ：20%		
8q4t strict-priority ingress queue	N/A		

キューイング パラメータ （続き）	デフォルト値 （続き）		
8q4t standard ingress queue 8（ハイ プライオリティ）	しきい値 1	CoS	5
		DSCP	40、46
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
	しきい値 2	CoS	なし
		DSCP	なし
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
	しきい値 3	CoS	なし
		DSCP	なし
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
	しきい値 4	CoS	なし
		DSCP	なし
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
8q4t standard ingress queue 7（中間プライオリティ）	しきい値 1	CoS	なし
		DSCP	なし
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
	しきい値 2	CoS	なし
		DSCP	なし
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
	しきい値 3	CoS	なし
		DSCP	なし
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
	しきい値 4	CoS	なし
		DSCP	なし
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%

キューイング パラメータ （続き）	デフォルト値 （続き）		
8q4t standard ingress queue 6（中間プライオリティ）	しきい値 1	CoS	なし
		DSCP	48 ～ 63
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
	しきい値 2	CoS	なし
		DSCP	なし
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
	しきい値 3	CoS	なし
		DSCP	なし
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
	しきい値 4	CoS	なし
		DSCP	なし
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
8q4t standard ingress queue 5（中間プライオリティ）	しきい値 1	CoS	なし
		DSCP	32、34 ～ 38
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
	しきい値 2	CoS	なし
		DSCP	なし
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
	しきい値 3	CoS	なし
		DSCP	なし
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
	しきい値 4	CoS	なし
		DSCP	なし
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%

キューイング パラメータ （続き）	デフォルト値 （続き）		
8q4t standard ingress queue 4（中間プライオリティ）	しきい値 1	CoS	なし
		DSCP	24、30
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
	しきい値 2	CoS	なし
		DSCP	28
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
	しきい値 3	CoS	なし
		DSCP	26
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
	しきい値 4	CoS	なし
		DSCP	なし
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
8q4t standard ingress queue 3（中間プライオリティ）	しきい値 1	CoS	なし
		DSCP	22
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
	しきい値 2	CoS	なし
		DSCP	20
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
	しきい値 3	CoS	なし
		DSCP	18
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
	しきい値 4	CoS	なし
		DSCP	なし
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%

キューイング パラメータ （続き）	デフォルト値 （続き）		
8q4t standard ingress queue 2（中間プライオリティ）	しきい値 1	CoS	なし
		DSCP	14
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
	しきい値 2	CoS	なし
		DSCP	12
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
	しきい値 3	CoS	なし
		DSCP	10
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
	しきい値 4	CoS	なし
		DSCP	なし
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%

キューイング パラメータ （続き）	デフォルト値 （続き）		
8q4t standard ingress queue 1（最小プライオリティ）	しきい値 1	CoS	0 および 1
		DSCP	0 ～ 9、11、13、15 ～ 17、19、21、23、25、27、29、31、33、39、41 ～ 45、47
		テールドロップ	ディセーブル、70%
		WRED ドロップ	イネーブル、ロー：40%、ハイ：70%
	しきい値 2	CoS	2 および 3
		DSCP	なし
		テールドロップ	ディセーブル、80%
		WRED ドロップ	イネーブル、ロー：40%、ハイ：80%
	しきい値 3	CoS	4
		DSCP	なし
		テールドロップ	ディセーブル、90%
		WRED ドロップ	イネーブル、ロー：50%、ハイ：90%
	しきい値 4	CoS	6 および 7
		DSCP	なし
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：50%、ハイ：100%
8q8t ingress-queue bandwidth allocation ratios	90:0:0:0:0:0:0:10		
8q8t ingress-queue limits	最小プライオリティ：80%		
	中間キュー：0%		
	最大プライオリティ：20%		
8q8t strict-priority ingress queue	N/A		
8q8t standard ingress queue 8（最大プライオリティ）	しきい値 1	CoS	5
		DSCP	サポート対象外
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
	しきい値 2 ～ 8	CoS	なし
		DSCP	サポート対象外
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%

キューイング パラメータ （続き）	デフォルト値 （続き）		
8q8t standard ingress queues 2–7 （中間プライオリティ）	しきい値 1 ～ 8	CoS	なし
		DSCP	サポート対象外
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
8q8t standard ingress queue 1 （最小プライオリティ）	しきい値 1	CoS	0 および 1
		DSCP	サポート対象外
		テールドロップ	ディセーブル、70%
		WRED ドロップ	イネーブル、ロー：40%、ハイ：70%
	しきい値 2	CoS	2 および 3
		DSCP	サポート対象外
		テールドロップ	ディセーブル、80%
		WRED ドロップ	イネーブル、ロー：40%、ハイ：80%
	しきい値 3	CoS	4
		DSCP	サポート対象外
		テールドロップ	ディセーブル、90%
		WRED ドロップ	イネーブル、ロー：50%、ハイ：90%
	しきい値 4	CoS	6 および 7
		DSCP	サポート対象外
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：50%、ハイ：100%
	しきい値 5 ～ 8	CoS	なし
		DSCP	サポート対象外
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：50%、ハイ：100%
1p7q2t ingress-queue bandwidth allocation ratios	5:255		
1p7q2t ingress-queue limits	標準キュー 1（最小プライオリティ）：50%		
	標準キュー 2：20%		
	標準キュー 3：15%		
	標準キュー 4 ～ 7：0%		
	完全優先：15%		

キューイング パラメータ （続き）	デフォルト値 （続き）		
1p7q2t strict-priority ingress queue		CoS	5
		DSCP	40、46
		テールドロップ	100%（設定はできません）
		WRED ドロップ	サポート対象外
1p7q2t standard ingress queue 7（中間プライオリティ）	しきい値 1	CoS	なし
		DSCP	なし
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
	しきい値 2	CoS	なし
		DSCP	なし
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
1p7q2t standard ingress queue 6（中間プライオリティ）	しきい値 1	CoS	なし
		DSCP	48 ～ 63
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
	しきい値 2	CoS	なし
		DSCP	なし
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
1p7q2t standard ingress queue 5（中間プライオリティ）	しきい値 1	CoS	なし
		DSCP	32、34 ～ 38
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
	しきい値 2	CoS	なし
		DSCP	なし
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%

キューイング パラメータ （続き）	デフォルト値 （続き）		
1p7q2t standard ingress queue 4 （中間プライオリティ）	しきい値 1	CoS	なし
		DSCP	24、30
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
	しきい値 2	CoS	なし
		DSCP	26、28
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
1p7q2t standard ingress queue 3 （中間プライオリティ）	しきい値 1	CoS	6 および 7
		DSCP	22
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：70%、ハイ：100%
	しきい値 2	CoS	なし
		DSCP	18、20
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：70%、ハイ：100%
1p7q2t standard ingress queue 2 （中間プライオリティ）	しきい値 1	CoS	2
		DSCP	14
		テールドロップ	ディセーブル、70%
		WRED ドロップ	イネーブル、ロー：40%、ハイ：70%
	しきい値 2	CoS	3 および 4
		DSCP	10、12
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：70%、ハイ：100%

キューイング パラメータ （続き）	デフォルト値 （続き）		
1p7q2t standard ingress queue 1（最小プライオリティ）	しきい値 1	CoS	0
		DSCP	0 ～ 9、11、13、15 ～ 17、19、21、23、25、27、29、31、33、39、41 ～ 45、47
		テールドロップ	ディセーブル、70%
		WRED ドロップ	イネーブル、ロー：40%、ハイ：70%
	しきい値 2	CoS	1
		DSCP	なし
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：70%、ハイ：100%
1p3q8t egress-queue bandwidth allocation ratios	100:150:200		
1p3q8t egress-queue limits	ロー プライオリティ：50%		
	ミディアム プライオリティ：20%		
	ハイ プライオリティ：15%		
	完全優先：15%		
1p3q8t strict-priority egress queue		CoS	5
		DSCP	サポート対象外
		テールドロップ	100%（設定はできません）
		WRED ドロップ	サポート対象外
1p3q8t standard egress queue 3（ハイ プライオリティ）	しきい値 1	CoS	6 および 7
		DSCP	サポート対象外
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：70%、ハイ：100%
	しきい値 2 ～ 8	CoS	なし
		DSCP	サポート対象外
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：70%、ハイ：100%

キューイング パラメータ （続き）	デフォルト値 （続き）		
1p3q8t standard egress queue 2 （ミディアム プライオリティ）	しきい値 1	CoS	2
		DSCP	サポート対象外
		テールドロップ	ディセーブル、70%
		WRED ドロップ	イネーブル、ロー：40%、ハイ：70%
	しきい値 2	CoS	3 および 4
		DSCP	サポート対象外
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：70%、ハイ：100%
	しきい値 3 ～ 8	CoS	なし
		DSCP	サポート対象外
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：70%、ハイ：100%
1p3q8t standard egress queue 1 （最小プライオリティ）	しきい値 1	CoS	0
		DSCP	サポート対象外
		テールドロップ	ディセーブル、70%
		WRED ドロップ	イネーブル、ロー：40%、ハイ：70%
	しきい値 2	CoS	1
		DSCP	サポート対象外
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：70%、ハイ：100%
	しきい値 3	CoS	なし
		DSCP	サポート対象外
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：70%、ハイ：100%
	しきい値 4	CoS	なし
		DSCP	サポート対象外
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：70%、ハイ：100%
	しきい値 5 ～ 8	CoS	なし
		DSCP	サポート対象外
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：50%、ハイ：100%

キューイング パラメータ （続き）	デフォルト値 （続き）		
1p7q4t egress-queue bandwidth allocation ratios	100:150:200:0:0:0:0:0		
1p7q4t egress-queue limits	標準キュー 1（最小プライオリティ）：50%		
	標準キュー 2：20%		
	標準キュー 3：15%		
	標準キュー 4 ～ 7：0%		
	完全プライオリティ キュー：15%		
1p7q4t strict-priority egress queue		CoS	5
		DSCP	40、46
		テールドロップ	100%（設定はできません）
		WRED ドロップ	サポート対象外
1p7q4t standard egress queue 7 （中間プライオリティ）	しきい値 1	CoS	なし
		DSCP	なし
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
	しきい値 2	CoS	なし
		DSCP	なし
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
	しきい値 3	CoS	なし
		DSCP	なし
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
	しきい値 4	CoS	なし
		DSCP	なし
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%

キューイング パラメータ （続き）	デフォルト値 （続き）		
1p7q4t standard egress queue 6 （中間プライオリティ）	しきい値 1	CoS	なし
		DSCP	48 ～ 63
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
	しきい値 2	CoS	なし
		DSCP	なし
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
	しきい値 3	CoS	なし
		DSCP	なし
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
	しきい値 4	CoS	なし
		DSCP	なし
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
1p7q4t standard egress queue 5 （中間プライオリティ）	しきい値 1	CoS	なし
		DSCP	32、34 ～ 38
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
	しきい値 2	CoS	なし
		DSCP	なし
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
	しきい値 3	CoS	なし
		DSCP	なし
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
	しきい値 4	CoS	なし
		DSCP	なし
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%

キューイング パラメータ （続き）	デフォルト値 （続き）		
1p7q4t standard egress queue 4（中間プライオリティ）	しきい値 1	CoS	なし
		DSCP	24、30
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
	しきい値 2	CoS	なし
		DSCP	28
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
	しきい値 3	CoS	なし
		DSCP	26
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
	しきい値 4	CoS	なし
		DSCP	なし
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
1p7q4t standard egress queue 3（中間プライオリティ）	しきい値 1	CoS	なし
		DSCP	22
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：70%、ハイ：100%
	しきい値 2	CoS	なし
		DSCP	20
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：70%、ハイ：100%
	しきい値 3	CoS	なし
		DSCP	18
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：70%、ハイ：100%
	しきい値 4	CoS	なし
		DSCP	なし
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：70%、ハイ：100%

キューイング パラメータ （続き）	デフォルト値 （続き）		
1p7q4t standard egress queue 2 （中間プライオリティ）	しきい値 1	CoS	なし
		DSCP	14
		テールドロップ	ディセーブル、70%
		WRED ドロップ	イネーブル、ロー：40%、ハイ：70%
	しきい値 2	CoS	なし
		DSCP	12
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：70%、ハイ：100%
	しきい値 3	CoS	なし
		DSCP	10
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：70%、ハイ：100%
	しきい値 4	CoS	なし
		DSCP	なし
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：70%、ハイ：100%

キューイング パラメータ （続き）	デフォルト値 （続き）		
1p7q4t standard egress queue 1（最小プライオリティ）	しきい値 1	CoS	0 および 1
		DSCP	0 ～ 9、11、13、15 ～ 17、19、21、23、25、27、29、31、33、39、41 ～ 45、47
		テールドロップ	ディセーブル、70%
		WRED ドロップ	イネーブル、ロー：40%、ハイ：70%
	しきい値 2	CoS	2 および 3
		DSCP	なし。
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：70%、ハイ：100%
	しきい値 3	CoS	4
		DSCP	なし。
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：70%、ハイ：100%
	しきい値 4	CoS	6 および 7
		DSCP	なし。
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：70%、ハイ：100%
1p7q8t egress-queue bandwidth allocation ratios	100:150:200:0:0:0:0		
1p7q8t egress-queue limits	標準キュー 1（最小プライオリティ）：50%		
	標準キュー 2：20%		
	標準キュー 3：15%		
	標準キュー 4 ～ 7：0%		
	完全優先：15%		
1p7q8t strict-priority egress queue		CoS	5
		DSCP	サポート対象外
		テールドロップ	100%（設定はできません）
		WRED ドロップ	サポート対象外
1p7q8t standard egress queues 4–7（中間および最高プライオリティ）	しきい値 1 ～ 8	CoS	なし
		DSCP	サポート対象外
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：100%、ハイ：100%

キューイング パラメータ （続き）	デフォルト値 （続き）		
1p7q8t standard egress queue 3 （中間プライオリティ）	しきい値 1	CoS	6 および 7
		DSCP	サポート対象外
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：70%、ハイ：100%
	しきい値 2 ～ 8	CoS	なし
		DSCP	サポート対象外
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：100%、ハイ：100%
1p7q8t standard egress queue 2 （中間プライオリティ）	しきい値 1	CoS	2
		DSCP	サポート対象外
		テールドロップ	ディセーブル、70%
		WRED ドロップ	イネーブル、ロー：40%、ハイ：70%
	しきい値 2	CoS	3 および 4
		DSCP	サポート対象外
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：70%、ハイ：100%
	しきい値 3 ～ 8	CoS	なし
		DSCP	サポート対象外
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：70%、ハイ：100%
1p7q8t standard egress queue 1 （最小プライオリティ）	しきい値 1	CoS	0
		DSCP	サポート対象外
		テールドロップ	ディセーブル、70%
		WRED ドロップ	イネーブル、ロー：40%、ハイ：70%
	しきい値 2	CoS	1
		DSCP	サポート対象外
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：70%、ハイ：100%
	しきい値 3 ～ 8	CoS	なし
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：70%、ハイ：100%

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

数字

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

あ

い

え

お

か

き

く

け

こ

さ

し

す

せ

そ

た

つ

て

と

な

に

ね

は

ひ

ふ

ほ

ま

み

む

め

も

ゆ

よ

ら

り

る

れ

ろ

©2008 Cisco Systems, Inc. All rights reserved.
Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。
本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。
「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R)
この資料の記載内容は2008年10月現在のものです。
この資料に記載された仕様は予告なく変更する場合があります。

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