

## Cisco Catalyst 6500 シリーズ スイッチの Cisco Catalyst OS および Cisco IOS の比較

バージョン 5.0 — EDCS-306654



### 目的

このホワイトペーパーでは、Cisco Catalyst® 6500 シリーズ スイッチで使用できる 2 つの OS (オペレーティング システム)、Catalyst Operating System (CatOS) ソフトウェアと Cisco IOS® ソフトウェアを比較し、Cisco Catalyst 6500 シリーズ スイッチにおける CatOS と Cisco IOS ソフトウェア (「ネイティブ」モデルともいう) のソフトウェア アーキテクチャ、動作、およびコンフィギュレーションについて説明します。

この文書は、Cisco Catalyst 6500 ソフトウェアで使用できるすべての機能を対象とはしていません。上記の両ソフトウェア モデルで使用頻度の高い機能について説明しています。\* また、この文書は、CatOS に詳しいユーザが、スーパーバイザ エンジンで Cisco IOS ソフトウェアに移行する場合のガイドとして使用することもできます。この文書は第 3 版です。

\* すべての機能およびサポートについては、Cisco CatOS バージョン 8.5.1 および Cisco IOS ソフトウェア リリース 12.2(18)SXF に関する文書を参照してください。これより前のリリースには、この文書で考慮されていない注意事項や未サポートの機能が存在する可能性があります。詳細については、リリース ノートを参照してください。

## はじめに

イントラネットおよびインターネットを使用するアプリケーションの急速な普及により、E コマースや E ラーニングなどの新しいビジネス モデルが注目を浴びています。インテリジェントな IP サービスを利用するこれらのアプリケーションによって、企業のイントラネットやサービス プロバイダーのインフラストラクチャは、業務コストの削減、情報フローの迅速化、および拡張性の高いサービスを実現する優れたツールに変わりつつあります。業界最大手のシスコシステムズはさまざまなソフトウェア オプションを提供することで、ネットワーク インフラストラクチャ全体でのサービスを可能にし、お客様が個々のネットワーク ニーズに応じてソフトウェアを選択できるようにしています。Cisco Catalyst 6500 シリーズ スイッチには、次の 2 つの OS モデルが用意されています。

- Cisco Catalyst 6500 シリーズのスーパーバイザ エンジンで Cisco CatOS を使用する場合、MSFC 用 Cisco IOS ソフトウェアを追加使用することにより、Cisco Catalyst 6500 でレイヤ 2/3/4 機能を実現します。スーパーバイザ エンジンで CatOS のみが稼働しているスイッチは、Policy Feature Card (PFC; ポリシー フィーチャ カード) の QoS (サービス品質)、セキュリティ、マルチキャスト、およびネットワーク管理といったレイヤ 2/3/4 機能を備えたレイヤ 2 フォワーディング デバイスで、ルーティング機能はありません。レイヤ 3 のルーティング機能は、Multilayer Switching Feature Card (MSFC; マルチレイヤ スwitチング フィーチャ カード) ルーティング エンジンの Cisco IOS ソフトウェア イメージによって提供されます。この MSFC は Supervisor 1A および 2 ではオプション、Supervisor 32 および 720 では標準搭載となっています。この文書では、スーパーバイザ エンジンの CatOS と MSFC の Cisco IOS ソフトウェアの組み合わせたものを「Hybrid (ハイブリッド)」OS と呼びます。この 2 つの OS は連携して動作し、レイヤ 2/3/4 のシステム機能を完全に提供します。

ハイブリッド モデルは、CatOS と Cisco IOS ソフトウェアの 2 つのオペレーティング イメージ、2 つのコンフィギュレーション、および 2 つのコマンド ラインに基づいて動作します。CatOS のデフォルト動作はスイッチです (すべてのポートが VLAN 1 でブリッジングされる)。また、Hybrid OS が稼働するスイッチはルータとして動作するようにも設定できます。

この動作モデルは、レイヤ 2 フォワーディング デバイスとして、IEEE 802.1X、インライン パワー、および音声 VLAN (仮想 LAN) ID を使用するワイヤリング クローゼットやアクセス レイヤ サービスを対象としています。MSFC ドータ モジュールが搭載されているデバイスは、ネットワークのディストリビューション レイヤに適しています。Supervisor Engine 720 (MSFC3 をデフォルトで搭載)、および Supervisor Engine 32 (MSFC2A をデフォルトで搭載) は Hybrid OS モデル対応なので、CatOS と MSFC 用 Cisco IOS を合わせて使用することができ、企業のコアにも適用できます。Hybrid OS モデルに 10 ギガビット イーサネット モジュールを組み合わせると、広い帯域幅を必要とする高速ネットワークにとって強力なソリューションとなります。

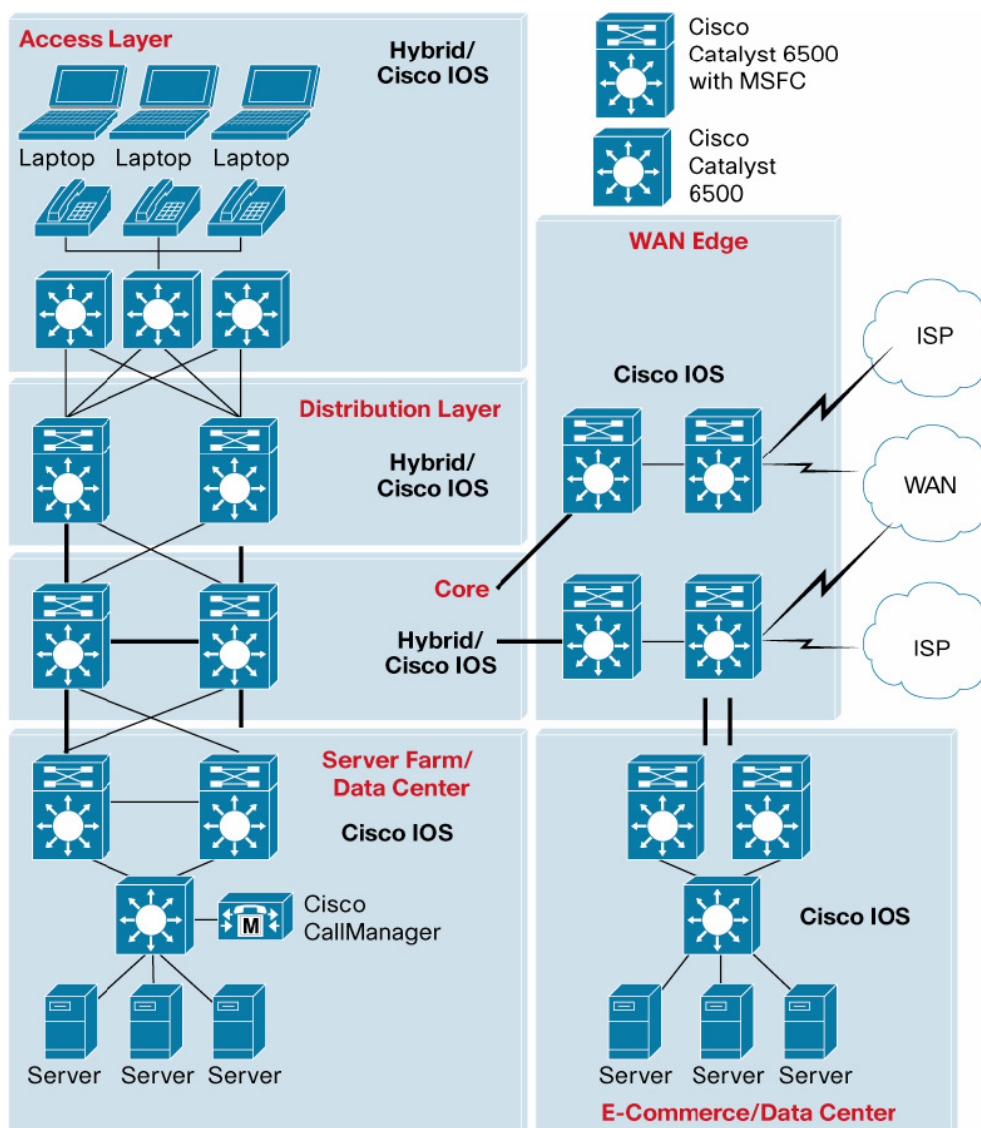
- Catalyst 6500 シリーズのスーパーバイザ エンジンで Cisco IOS ソフトウェアを稼働させる場合、単一の Cisco IOS イメージ、コンフィギュレーション、およびコマンド ラインを提供し、スイッチのレイヤ 2、3、および 4 すべての機能をサポートします。従来、Cisco IOS はルーティング プラットフォームのレイヤ 3 OS でしたが、Catalyst 6500 のスーパーバイザ エンジンにインストールする場合は、この機能がレイヤ 2 機能にまで拡張されます。Cisco IOS を使用する場合は、スーパーバイザ エンジンに MSFC ドータカードを搭載する必要があります (Supervisor Engine 32 および 720 にはデフォルトで搭載)。この文書では、「Cisco IOS」という用語は、Catalyst 6500 シリーズ スイッチのスーパーバイザ エンジンで使用される Cisco IOS ソフトウェアを意味します。

Cisco IOS ソフトウェアはデフォルトではルータとして動作します (すべてのポートがレイヤ 3 でシャットダウン状態になっています)。ただし、スイッチとして動作するようにインターフェイスを設定することもできます。

Cisco IOS オペレーティング モデルは、サービス プロバイダーや企業のデータセンターのバックボーンおよびディストリビューション レイヤ サービスを対象としています。このソフトウェア モデルをサービス モジュールと組み合わせて使用すると、統合型データ センタにとって強力なソリューションを実現できます。Cisco IOS ソフトウェアは、Catalyst 6500 シリーズ スイッチのスイッチング機能に Cisco IOS ソフトウェアのルーティング機能を組み合わせて、スイッチングとルーティングのすべての機能を実行する操作の容易な単一統合型 OS を実現します。

上記のソフトウェア動作モデルは、さまざまな要件に応じてネットワーク内で併用することができます。これらのモデルの機能は完全に同等ではないため、推奨モデルは求められる要件によって異なります。図 1 は、ネットワーク アーキテクチャにおいて、ハイブリッド モデルと Cisco IOS オペレーティング モデルを配置すべき場所を示しています。

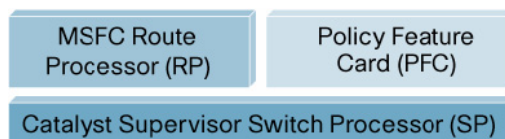
図 1 Cisco IOS ソフトウェアおよび Catalyst OS の配置



## アーキテクチャの比較

Cisco Catalyst 6500 は、レイヤ 2/3/4 の機能が統合された高性能デバイスです。使用するソフトウェア モデルに関係なく、スーパーバイザ エンジン ベースボード(スイッチ プロセッサ搭載)、PFC ドータカード、および MSFC(ルート プロセッサ)ドータカードでシステムのフォワーディング機能が実行されます(図 2)。

図 2 Cisco Catalyst 6500 のインテリジェンス コンポーネント



### スイッチ プロセッサの機能

すべてのシャーシ動作を制御する Switch Processor(SP; スイッチ プロセッサ)は、Supervisor 2 の 250 MHz R7000 CPU、Supervisor 32 の 400 MHz R7000 CPU、および Supervisor 720 の 600 MHz R7000 CPU で稼働します。シャーシ動作には、Online Insertion and Removal(OIR; ホットスワップ)イベントの検出、電源管理、環境管理、および冗長性管理などがあります。また SP が扱う処理には、各ライン カードに対する適切なライン カード ファームウェアのダウンロード、基本的なポート管理(ポートの設定、リンク ステータスの検出など)、およびその他のレイヤ 2 機能(スパンニングツリー、VLAN Trunking Protocol [VTP; VLAN トランキング プロトコル]、Internet Group Management Protocol [IGMP; インターネット グループ管理プロトコル] スヌーピング、Dynamic Trunking Protocol [DTP; ダイナミック トランキング プロトコル] など)があります。さらに SP は、システム初回起動時に CatOS または Cisco IOS のコンソール接続を提供します。

### ルート プロセッサの機能

Route Processor(RP; ルート プロセッサ)は、300 MHz R7000 CPU(MSFC2 および MSFC2A) または 600 MHz R7000 CPU(MSFC3)で稼働し、ルーティングや Cisco Express Forwarding (CEF)テーブルの作成といったレイヤ 3 機能を提供します。CEF はデフォルトのレイヤ 3 フォワーディング メカニズムです。RP は、Cisco Express Forwarding と隣接テーブルの生成とメンテナンスを行う一方で、この情報を PFC にプッシュして、ハードウェア フォワーディング、QoS、およびセキュリティ機能を実行します。また、RP には、IP アドレス解決(ARP)およびルーティング テーブル メンテナンスなどの機能もあります。

### Policy Feature Card(PFC)

PFC は、Application Specific Integrated Circuit(ASIC; 特定用途向け IC)でフォワーディングを行う装置です。PFC はハードウェア ベースの機能とサービスを高速に処理します(毎秒数千万パケット)。レイヤ 2 ブリッジング、レイヤ 3 ルーティング、アクセス制御、QoS マーキングおよびポリシング、NetFlow 統計情報、マルチキャストなどの機能は、PFC 内で実行されます。

### ソフトウェアの実行

Cisco IOS モードでは、両方の CPU(SP および RP)で全面的に Cisco IOS ソフトウェアが動作する必要があります。スイッチ内の見えないところで Catalyst ソフトウェアが実行されることはありません。また両方の CPU が使用する実行イメージは、IOS カーネルを完全に稼働させます。両方の CPU で Cisco IOS ソフトウェアを稼働させると、システム全体のパフォーマンスが向上します。ただし、MSFC に障害が発生した場合は、レイヤ 2/3/4 すべての機能が停止します。

反対に、CatOS は SP および PFC 上で動作し、レイヤ 2 フォワーディングおよびレイヤ 3/4 サービスを提供します。レイヤ 3 のフォワーディングおよびルーティング機能が必要な場合は、MSFC ドータカードを搭載し、RP 上で(Hybrid OS の一部として)Cisco IOS ソフトウェアを実行する必要があります。これにより、ハイブリッド構成の MSFC に障害が発生しても、レイヤ 2 および PFC の機能は影響を受けることなく動作し続けます。

### ソフトウェア機能のサポート

Cisco Catalyst 6500 シリーズの 2 つのソフトウェア モデル、CatOS と Cisco IOS の機能は、同一ではありません。以下に、使用頻度の高いプロトコルの CatOS および Cisco IOS ソフトウェアでのサポート状況を示します。Cisco IOS ソフトウェアの多くの機能はプラットフォームに依存しません(OSPF、BGP、PIM プロトコルなど)。このような場合、Hybrid OS の Cisco IOS の機能は Cisco IOS ソフトウェアでの機能と同じになります。

表 1 は、Cisco CatOS バージョン 8.3.1 および Cisco IOS ソフトウェア リリース 12.2(18)SXF(これには 12.1(26)E3 のすべての機能が含まれます)で利用できる使用頻度の高いソフトウェア機能を示しています。機能のサポートがハードウェアに依存する場合は、その旨が明記されています。

表 1 ソフトウェアの比較

ソフトウェア機能	CatOS	Cisco IOS
VLAN の範囲:最大 4096 の VLAN SVI(レイヤ 3 VLAN インターフェイス)	○	○
VLAN 間ルーティング	○	○
レイヤ 2 VLAN × 4096	○	○
プライベート VLAN	○	○
ダイナミック VLAN	○	
トランキング:IEEE 802.1Q、ISL	○	○
DTP、VTP	○	○
VTPv3	○	
IEEE 802.1Q トンネリング	○	○
レイヤ 2 プロトコルトンネリング	○	○
スパンニングツリー:PortFast、UplinkFast、BackboneFast、BPDU ガード、PRRST+、PVRST	○	○
IEEE 802.1s および 802.1w	○	○
ジャンボ フレーム	○	○
EtherChannel、Port Aggregation Protocol(PAgP)	○	○
EtherChannel、IEEE 802.3ad(LACP)	○	○
ローカル SPAN およびリモート SPAN(RSPAN)	○	○
マルチキャスト サービス:PIM、IGMP スヌーピング、RGMP、双方向 PIM	○	○
QoS マーキング、ポリシング、スケジューリング	○	○
QoS ACL	○	○
ルーティング ACL	○	○
VLAN ACL	○	○
Port-Based ACL(PACL)	○	
HSRP	○	○
VRRP	○	○
GLBP	○	○
IPv6		○

ソフトウェア機能	CatOS	Cisco IOS
Any Transport over MPLS (AToM) (PFC3bXL のみ)		○
Multiprotocol Label Switching (MPLS; マルチプロトコル ラベル スイッチング) (PFC3b および PFC3bXL のみ)		○
Cisco IOS サーバ ロードバランシング		○
ブロードキャスト抑制	○	○
プロトコル フィルタリング (Supervisor Engine 1A システムで Cisco IOS をサポートする場合のみ)	○	○
ポート セキュリティ	○	○
Secure Copy Protocol (SCP)	○	○
SSHv1 および SSHv2	○	○
SmartPort マクロ	○	
IEEE 802.1X および VLAN 割り当て	○	○
VLAN 割り当てに対する IEEE 802.1X 拡張機能	○	
Time Domain Reflectometer (TDR)	○	○
AutoQoS	○	
ARP インスペクション	○	○
ダイナミック ARP インスペクション	○	○
DHCP スヌーピング	○	○
IP ソース ガード	○	
Network-Based Application Recognition (NBAR)	○	○
ユーザ ベースのレート制限		○
Cisco Discovery Protocol (CDP)	○	○
NetFlow Data Export (NDE; NetFlow データ エクスポート)	○	○
Unidirectional Link Detection (UDLD; 単一方向リンク検出)	○	○
Cisco IP Phone の Voice VLAN ID (VVID; 音声 VLAN ID) およびインライン パワー	○	○
スーパーバイザの冗長性およびフェールオーバー	○	○
スーパーバイザのステートフル スイッチオーバー	○	○
MPLS、EoMPLS、MPLS VPN		○
Distributed Cisco Express Forwarding (dCEF)		○

### ハードウェアおよびライン カードのサポート

表 2 は、Cisco Catalyst 6500 シリーズのライン カードとサポートする OS の対応を示しています。

表 2 ハードウェア モジュール

シャーシ、スーパーバイザ、および PFC ドータカード	CatOS	Cisco IOS
WS-C6513、WS-C6509、WS-C6509-NEB、WS-C6509-NEB-A、WS-C6506、WS-C6503、OSR-7609-AC/DC、CISCO7603、CISCO7606、CISCO7609、WS-C6509	○	○
WS-SUP720	○	○
WS-SUP720-3B	○	○
WS-SUP720-3BXL	○	○
WS-SUP32-10GE-3B	○	○
WS-SUP32-GE-3B	○	○
WS-X6K-PFC3BXL	○	○
WS-X6K-S2U-MSFC2	○	○
WS-X6K-S2-MSFC2	○	○

シャーシ、スーパーバイザ、および PFC ドーターカード	CatOS	Cisco IOS
WS-X6K-S2-PFC2	○	N/A
WS-X6K-S1A-MSFC2	○	○
WS-X6K-SUP1A-MSFC	○	○
WS-X6K-SUP1A-PFC	○	N/A **
WS-X6K-SUP1A-2GE	○	N/A **
WS-X6K-SUP1-2GE	○	N/A **
<b>CEF720 シリーズ モジュールおよび XENPAK</b>		
WS-X6748-SFP	○	○
WS-X6748-GE-TX	○	○
WS-X6724-SFP	○	○
WS-X6704-10GE	○	○
WS-X6724-SFP	○	○
WS-X6748-GE-TX	○	○
WS-F6K-DFC3A		○
WS-X6700-DFC3		○
XENPAK-10GB-SR	○	○
XENPAK-10GB-LX4	○	○
XENPAK-10GB-CX4	○	○
XENPAK-10GB-LR	○	○
XENPAK-10GB-ER	○	○
スイッチング ファブリック モジュール		
WS-C6500-SFM	○	○
WS-X6500-SFM 2	○	○
<b>CEF256 および dCEF256 シリーズ モジュール</b>		
WS-F6K-DFC		○
WS-X6816-GBIC		○
WS-X6501-10GEX4	○	○
WS-X6502-10GE	○	○
WS-G6483	○	○
WS-G6488	○	○
WS-X6516-GBIC	○	○
WS-X6516A-GBIC	○	○
WS-X6516-GE-TX	○	○
WS-X6524-100FX-MM	○	○
WS-X6548-GE-TX/V	○	○
WS-X6548-RJ-21	○	○
WS-X6548-RJ-45	○	○
<b>クラシック モジュール</b>		
WS-X6416-GBIC	○	○
WS-X6416-GE-MT	○	○
WS-X6316-GE-TX	○	○
WS-X6408A-GBIC	○	○
WS-X6408-GBIC	○	○

シャーシ、スーパーバイザ、および PFC ドータカード	CatOS	Cisco IOS
WS-X6324-100FX-SM/MM	○	○
WS-X6224-100FX-MT	○	○
WS-X6348-RJ-21/V	○	○
WS-X6348-RJ-45/V	○	○
WS-X6148X2-RJ-45	○	○
WS-X6148-GE-TX/V	○	○
WS-X6148-RJ-45V	○	○
WS-X6148-RJ21V	○	○
WS-X6248-RJ-45	○	○
WS-X6248A-TEL	○	○
WS-X6248-TEL	○	○
WS-X6024-10FL-MT	○	○
<b>モジュール用音声ドータカード</b>		
WS-F6K-FE48X2-AF (WS-X6148X2-RJ-45 用)	○	○
WS-F6K-FE48-AF (WS-X6148-RJ-45 および WS-X6148-RJ-21 用)	○	○
WS-F6K-GE48-AF (WS-X6548-GE-TX および WS-X6148-GE-TX 用)	○	○
<b>サービス モジュールおよび音声モジュール</b>		
WS-X6624-FXS (EOS および EOL、2005 年 5 月 15 日)	○	
WS-X6608-T1/E1	○	
WS-X6381-IDS (EOS および EOL、2004 年 3 月 26 日)	○	○
WS-SVC-IDSM2-BUN-K9	○	○
WS-X6380-NAM (EOS 外部通知、2002 年 6 月 24 日)	○	○
WS-X6066-SLB-APC	○	○
WS-SVC-CSG-1	○	○
WS-SVC-CMM-6T1/E1	○	○
WS-SVC-NAM-1	○	○
WS-SVC-NAM-2	○	○
WS-SVC-FWM-1-K9	○	○
WS-SVC-CMM	○	○
WS-SVC-MWAM-1		○
WS-SVC-CSG-1	○	○
WS-SVC-PSD-1 (永続的ストレージ デバイス)		○
WS-SVC-IDSM2-K9	○	○
WS-SVC-SSL-1-K9	○	○
WS-SVC-IPSEC-1		○
WS-SVC-WLAN-1-K9		○
<b>その他のモジュール</b>		
WS-X6101-OC12-SMF/MMF	○	
WS-X6302-MSM	○	
<b>WAN モジュール</b>		
WS-X6582-2PA		○
WS-X6182-2PA	○	○
OSM-4GE-WAN		○

シャーシ、スーパーバイザ、および PFC ドータカード	CatOS	Cisco IOS
OSM-2+4GE-WAN+		○
OSM-4GE-WAN-GBIC	○	○
OSM-16OC3-POS-MM/SI/SL		○
OSM-2OC12-POS-MM/SI/SL	○	○
OSM-4OC12-POS-MM/SI/SL	○	○
OSM-4OC3-POS-SI	○	○
OSM-8OC3-POS-MM/SI/SL	○	○
OSM-16OC3-POS-MM/SI/SL	○	○
OSM-1OC48-POS-SS/SI/SL	○	○
OSM-1CHOC48/T3-SS/SI		○
OSM-4CHOC12/T3-MM/SI		○
OSM-2OC12-ATM-MM/SI		○
OSM-2OC12-POS-MM+/SI+		○
OSM-4OC12-POS-SI+		○
OSM-4OC3-POS-SI+/SL+		○
OSM-8OC3-POS-SI+		○
OSM-16OC3-POS-SI+		○
OSM-1OC48-POS-SS+/SI+/SL+		○
OSM-2OC12-ATM-MM+/SI+		○
OSM-2OC48/1DPT-SS/SI/SL		○
OSM-1CHOC12/T3-SI		○
OSM-12CT3/T1		○
OSM-2+4GE-WAN+		○

\*\* MSFC がない場合、IOS はサポートされません。

表 2 に示すように、大半のライン カードは CatOS と Cisco IOS ソフトウェアの両方でサポートされています。各ライン カードの具体的なソフトウェア情報については、<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/index.htm> にあるリリース ノートを参照してください。

### メモリ要件

Cisco IOS ソフトウェアと CatOS ソフトウェアのデフォルトのメモリ要件は同じです。Supervisor Engine 2 には、デフォルトで 128 MB の DRAM(512 MB にアップグレード可能)と 32 MB のブートフラッシュが搭載されています。MSFC2 には、128 MB の DRAM(512 MB にアップグレード可能)と 16 MB または 32 MB のブートフラッシュが搭載されています。Supervisor Engine 2 の 256 MB DRAM および MSFC2 の 256 MB DRAM は、部品番号 WS-X6K-S2U-MSFC2 で発注できます。Supervisor Engine 32 には、SP と RP の両方に 256 MB の DRAM(1 GB にアップグレード可能)と 512 MB の内蔵フラッシュカードが搭載されています。また、Supervisor Engine 720 には、SP と RP の両方にデフォルトで 512 MB の DRAM と 64 MB のブートフラッシュが搭載されています。

Cisco IOS ソフトウェア イメージはレイヤ 2 およびレイヤ 3 の統合イメージであるため、CatOS イメージよりも大きくなります。一部の 12.1E Cisco IOS イメージには 20 MB を超えるものもあるため、MEM-C6K-ATA-1-64M フラッシュカードを使って、Supervisor Engine 2 を備えたシステムごとに複数のイメージを保存する必要があります。

Supervisor Engine 720 および Supervisor 32 にメモリを追加する場合は、MEM-C6K-CPTFL64 M/128 M/256 M/512 M コンパクト フラッシュ カード(それぞれ 64 MB、128 MB、256 MB を搭載)を使用します。

Cisco IOS ソフトウェアには、ルーティング テーブルの容量に応じたメモリに関する注意事項があります(リリース ノートに記載)。詳しくは、Cisco Catalyst 6500 シリーズのリリース ノートを参照してください。

## 運用に関する比較

### イメージの管理

Hybrid OS を使用するシステムとスーパーバイザ エンジンで Cisco IOS を使用するシステムでは、イメージ名の表記法が異なります。それぞれのハードウェアに応じた適切なイメージを選択してください。以下の各項では、CatOS および Cisco IOS ソフトウェアの各種イメージ ファイルについて説明します。

#### Hybrid OS のオペレーティング システム ファイル

ハイブリッド モデルでは、2 種類の異なるイメージ ファイルが 2 つの異なる OS によって管理されます。CatOS イメージはスーパーバイザ ブートフラッシュまたはフラッシュ カードに保管されます(Supervisor 1A および Supervisor 2 の場合は PCMCIA、Supervisor Engine 32 と Supervisor Engine 720 の場合はコンパクト フラッシュ)。MSFC の Cisco IOS イメージは、MSFC ブートフラッシュに保管されます。**copy** コマンドを使用すると、アクティブ スーパーバイザおよびスタンバイ スーパーバイザ間でイメージを移動できます。また、TFTP アプリケーションを使用してイメージをスイッチにアップロードすることも可能です。ハイブリッドを実行する Cisco Catalyst 6500 システムは、表 3 に示すイメージ ファイルを使用します。

表 3 Hybrid OS のイメージ名

イメージ ファイル	説明
cat6000-supx	スーパーバイザ エンジンの CatOS イメージ(この場合、x は Sup2、Sup32、または Sup720)。スーパーバイザのブートフラッシュまたはフラッシュ カードに保管される
c6msfcx-boot-mz	レイヤ 3 ブート イメージ(この場合、x は MSFC または MSFC2)。MSFCx bootflash:のみに保管される。このイメージは、MSFC 上で Cisco IOS ソフトウェアを実行する場合は「必須」で、MSFC2 の場合は「推奨」
c6msfc-is-mz c6msfc2-is-mz c6msfc2a-ipbase_wan-mz c6msfc3-psv-mz	MSFC、MSFC2、MSFC2A、または MSFC3 用のレイヤ 3 イメージ(スーパーバイザ エンジンの CatOS イメージと併用)。MSFC bootflash:、sup-slot0:、sup-disk0:、または sup-disk1:に保管される

Hybrid OS と Cisco IOS ソフトウェアは、同じ MSFC ブート ヘルパー イメージ(c6msfc-boot)を使用します。このブート イメージは、MSFC ブートフラッシュの最初のファイルとして保管されます。ブート ヘルパー イメージは、ネットワーク インターフェイス コードおよびエンドホスト プロトコル コードを含む、機能の限られたシステム イメージです。

**注:** MSFC(1) からブート ヘルパーを削除することはできません。ブート ヘルパーは MSFC ブートフラッシュの最初のイメージとして使用されます。MSFC2、MSFC2A、および MSFC3 のハードウェアにはより性能の高い ROMMON \*\*\* 機能があるため、ブート イメージは必要ありません。ただし、万が一の場合に備えて、MSFC ブートフラッシュにブート イメージを保管しておくことを推奨します。MSFC2A または MSFC3 ではブート イメージは使用できません。

\*\*\* ROMMON は、CatOS や Cisco IOS ソフトウェアがシステムを制御できない場合にハードウェアの基本的な操作を行う低レベル ソフトウェアです。

### Cisco IOS ソフトウェアのオペレーティング システム ファイル

Cisco IOS ソフトウェアは、スーパーバイザのローカル デバイス上に単一のイメージとして保管する必要があります。これは、このイメージが 2 つのプロセッサ用にバンドルされたイメージで、SP が最初に起動するためです。このイメージは、スーパーバイザのブートフラッシュ (sup-bootflash:) またはフラッシュ カード (slot0:, または disk0:) のどちらかに保管しても構いませんが、MSFC ブートフラッシュには保管できません。Cisco IOS のシステム ファイルは、「c6supxy」で始まります。ここで、x はスーパーバイザのモデル番号、y は MSFC のモデル番号です。Supervisor Engine 32 および Supervisor Engine 720 の場合は、s(SUP)vw を使用します。ここで、SUP はスーパーバイザ エンジン、v は MSFC のバージョン、w は PFC のバージョンです。

表 4 Cisco IOS のイメージ名

イメージファイル	説明
c6sup11	レイヤ 2 ~ 4 がバンドルされたイメージ (Supervisor 1, MSFC2 用)
c6sup12	レイヤ 2 ~ 4 がバンドルされたイメージ (Supervisor 2, MSFC2 用)
c6sup22	レイヤ 2 ~ 4 がバンドルされたイメージ (Supervisor 2, MSFC2 用)
s3223	レイヤ 2 ~ 4 がバンドルされたイメージ (Supervisor 32, MSFC 2A, PFC3x 用)
s72033	レイヤ 2 ~ 4 がバンドルされたイメージ (Supervisor 720, MSFC 3, PFC3x 用)

**注:** フラッシュ カードは、CatOS と Cisco IOS ソフトウェアでは形式が異なるため、OS モデルを切り替える際にはフラッシュ カードをフォーマットする必要があります。

### ストレージ デバイス

Cisco IOS ソフトウェアの場合、アクティブ スーパーバイザのストレージ デバイスは、次のとおりです。

slot0:	アクティブ スーパーバイザのリニア フラッシュ カード
disk0:, disk1	アクティブ スーパーバイザの ATA フラッシュ カードまたはコンパクト フラッシュ カード
sup-bootflash:	アクティブ スーパーバイザの 16 MB、32 MB、または 64 MB (Sup720) オンボード フラッシュ
bootflash:	アクティブ MSFC の 16 MB、32 MB、または 64 MB (Sup720) オンボード フラッシュ
bootdisk:	アクティブ オンボード フラッシュ (Sup32)

新規イメージは、アクティブ スーパーバイザからスタンバイ スーパーバイザ、フラッシュ カード、RP ブートフラッシュ、または SP ブートフラッシュ/ブートディスクにコピーできます。スタンバイ ストレージ デバイスは、次のとおりです。

slaveslot0:	スタンバイ スーパーバイザのフラッシュ カード
slavesup-bootflash:	スタンバイ スーパーバイザの 16 MB、32 MB、または 64 MB (Sup720) オンボード フラッシュ
slavesup-bootdisk:	スタンバイ スーパーバイザの 64 MB (Sup32) オンボード フラッシュ
slavedisk0:	スタンバイ スーパーバイザのフラッシュ カード (Sup32 Sup720)
slavebootflash:	スタンバイ MSFC の 16 MB または 64 MB (Sup720) オンボード フラッシュ

次の例は、アクティブ スーパーバイザのフラッシュ カードからスタンバイ スーパーバイザのフラッシュにコピーする場合のコマンドです。

```
IOS# copy disk0:s72033-jk9sv-mz.122-18.SXD slavesup-disk0:
Destination filename [s72033-jk9sv-mz.122-18.SXD] ?
```

## Cisco Catalyst 6500 で稼働している OS の判別

ハイブリッドシステムで使用される Cisco IOS と Cisco IOS システムのコマンドラインは、外見上同じです。スイッチで稼働している OS を判別するには、Cisco IOS のコマンドラインから show version コマンドを入力します。Hybrid OS の IOS(レイヤ 3)機能にアクセスするには、コマンドラインから session 15(または 16)または switch console を入力します。コンソールが MSFC に切り替わると、Cisco IOS システムと Hybrid OS システムは外見上同じになります。

**ハイブリッドシステムの場合**

```
Router#show version
Cisco Internetwork Operating System Software
IOS (tm) MSFC2 Software (C6MSFC2-PSV-M), Version 12.1(19)E, EARLY DEPLOYMENT
RELEASE SOFTWARE (fc1)
```

**Cisco IOS システムの場合**

```
Router#show version
Cisco Internetwork Operating System Software
IOS (tm) c6sup2_rp Software (c6sup2_rp-PSV-M), Version 12.1(19)E, EARLY DEPLOYMENT
RELEASE SOFTWARE (fc1)
```

**Cisco IOS および Hybrid OS の起動プロセス**

Cisco IOS モデルおよび Hybrid OS モデルは自動的に起動するので、ユーザが起動プロセスを意識する必要はありません。ハイブリッドモデルの場合、SP と RP でそれぞれ異なる OS が起動するため、起動プロセスも別々になります。

Cisco IOS ソフトウェアの場合、SP と RP は両方とも Cisco IOS ソフトウェアをロードします。2つのプロセッサが動作する場合、ROMMON とブートフラッシュ デバイスも 2 つになります。最初に SP が ROMMON で起動し、Cisco IOS ソフトウェアの一部をロードします。SP が起動すると、次のプロセッサを起動するためにソフトウェア制御が RP に移ります。コンソール表示では、最初に SP の情報がスーパーバイザ エンジンの RJ-45 コンソール ポートに表示されます。Cisco IOS ソフトウェアが搭載された Cisco Catalyst 6500 では、起動中に制御が RP の CPU に移ります(次のコンソール表示を参照)。

```
System Bootstrap, Version 7.1(1) (Catalyst Supervisor ROMMON)
Copyright (c) 1994-2003 by cisco Systems, Inc.
c6k_sup2 processor with 262144 Kbytes of main memory

00:00:03: %OIR-6-CONSOLE:Changing console ownership to route processor

System Bootstrap, Version 12.1(19)E, RELEASE SOFTWARE (fc1) (MSFC or RP ROMMON)
Copyright (c) 2003 by cisco Systems, Inc.
Cat6k-MSFC2 platform with 524288 Kbytes of main memory
```

これ以降は、RP がシステムを制御します。ソフトウェアの観点から言えば、RP はプライマリ CPU として動作し、SP はセカンダリ CPU として動作します。ユーザがこれを意識する必要はありませんが、Cisco IOS ソフトウェアでは、すべてのコンフィギュレーション コマンドが RP の CPU を通じて直接入力されます。SP の機能に関するコマンドが入力されると、RP から SP に内部で受け渡されます。

CatOS の場合とは異なり、TFTP サーバからの Cisco IOS イメージのネット ブートはサポートされていません。これは、スーパーバイザのイメージが 2 つのプロセッサ用にバンドルされたイメージであるためです。ランタイム イメージ (c6sup<xy>-is-mz-<version>) は、SP (sup-bootflash) またはフラッシュ カード (slot0:, disk0:, disk1:) 上のローカル デバイスに保管する必要があります。

#### Cisco IOS ソフトウェアでの SP へのログイン

RP のコマンドラインから SP にログインして、レイヤ 2 に特化したデバッグを行うことができます。実行時に SP のデバッグおよびステータス確認を行う場合は、次のコマンドを使用します。レイヤ 2 ~ 4 の設定は、すべてメインの Cisco IOS コマンドラインから実行することに注意してください。

- **remote login** — remote login コマンド (Sup 2, Sup32, および Sup720 の場合は *remote login switch*) は CatOS の **session** コマンドに相当します。ホスト名は「hostname-sp」になります。SP からログアウトする場合には、Control-C ではなく **exit** コマンドを使用します。
- **remote command** — SP のコマンド出力を単発で確認する場合には、**remote command <command>** (Supervisor Engine 2, Supervisor Engine 32, および Supervisor Engine 720 の場合は **remote command switch <command>**) を使用します (下記を参照)。

**注:** remote command を使用する場合、ヘルプ機能 (*remote command show ?* など) は利用できません。

```
IOS#remote command sw show bootvar
IOS-sp#
BOOT variable = bootflash:c6sup22-psv-mz.121-11b.EX,1
CONFIG_FILE variable =
BOOTLDR variable does not exist
Configuration register is 0x2002
IOS#
```

#### スイッチの管理

Cisco Catalyst 6500 の管理ではダイレクト コンソール ケーブル接続が利用できます。他のネットワークベースの管理 (Telnet や SNMP など) を使用する場合は、スイッチにアクセスするための管理インターフェイスが必要になります。CatOS では、2 つの管理インターフェイス (sc0 および sc1) がシステムに用意されています。これらのインターフェイスには IP アドレスと VLAN を割り当てる必要があります (IP アドレスと VLAN が使用されている場合)。CatOS システムの IP ベースの管理は、すべて sc0 または sc1 インターフェイス アドレスに出力されます。Hybrid OS の場合は、sc0/sc1 インターフェイスに、ルーティング機能を持つ任意のレイヤ 3 VLAN インターフェイスを併せて使用します。

```
CatOS> (enable) show interface
s10:flags=51<UP,POINTOPOINT,RUNNING>
    slip 0.0.0.0 dest 0.0.0.0
sc0:flags=63<UP,BROADCAST,RUNNING>
    vlan 1 inet 10.1.1.54 netmask 255.255.255.0 broadcast 10.1.1.255
```

Cisco IOS ソフトウェアの場合、sc0/sc1 インターフェイスという概念は存在しません。Switch Virtual Interface (SVI; スイッチ仮想インターフェイス)を使用することで、スイッチをネットワークベースで管理できます (SVI については、あとの項で詳しく説明します)。作成されるすべてのレイヤ 2 VLAN に、SVI を対応付けることもできます。各 SVI には 1 つまたは複数の IP アドレスを設定できます。この IP アドレスは、SNMP または Telnet クライアントを使用して特定の VLAN 上のデバイスにアクセスする場合に使用します。次のコマンドを使用すると、システムを管理するための VLAN SVI と、それに対応する IP アドレスが表示されます。

```
IOS#show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	192.168.1.1	YES	manual	up	up
Vlan10	10.1.1.1	YES	manual	up	down

### スイッチのコンフィギュレーションの変更

CatOS ソフトウェアでは、コンフィギュレーションが変更されるとすぐに NVRAM に書き込まれます (ユーザによる操作は必要ありません)。CatOS のコンフィギュレーションは、すべて有効モード プロンプトから「set」コマンド シーケンスを使用して実行されます。特定のコマンドを消去するには、有効モード プロンプトから **clear** コマンドを入力します。

反対に、Cisco IOS ソフトウェアでは、**copy run start** (または **write memory**) コマンドが実行されない限り、NVRAM にコンフィギュレーションの変更が保存されることはありません。コンフィギュレーションを明示的に保存しない場合、システムをリロードすると、コンフィギュレーションの変更はすべて失われます。Cisco IOS のコマンドラインによる設定は、スーパーバイザまたは MSFC いずれの場合でも、コンフィギュレーション モード (config-t) で実行します。コマンドを解除する場合は、元のコマンドの **no** 形式を使用します。

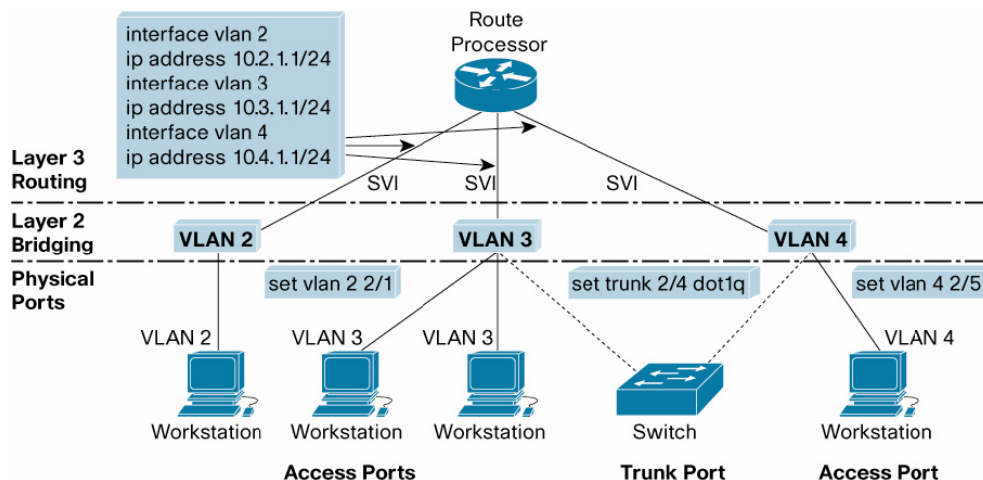
### ポートの動作

以下の項では、CatOS と Cisco IOS ソフトウェアのポート動作の違いについて説明します。

ハイブリッドの場合: MSFC 上で Cisco IOS ソフトウェアを使用する CatOS

ハイブリッド モデルでは、CatOS のレイヤ 2/4 機能と、MSFC 上にある Cisco IOS のレイヤ 3 フィーチャ セットが密接に統合されています。レイヤ 2 ポート (アクセス ポートやトランク ポートなど) と VLAN は、CatOS のコマンド セットを使用して設定し、レイヤ 3 の SVI は MSFC の Cisco IOS コマンド セットを使用して設定します。ポートは CatOS を使用してレイヤ 2 VLAN で設定されるため (**set vlan x <slot/port>**)、特定の VLAN に対する VLAN 間ルーティングを有効にするために、対応するレイヤ 3 SVI を作成する必要があります。SVI を作成するには、**interface vlan** コマンドを使用します。ハイブリッド モデルの場合、MSFC は物理インターフェイス (interface gig 1/1) ではなく、論理インターフェイス (interface vlan 10) 上で動作します。図 3 は、ハイブリッド モデルのポートの概念と、レイヤ 2 またはレイヤ 3 の機能を使用するための関連コマンドを示しています。

図 3 ハイブリッドモデルにおけるポートの概念



Cisco IOS ソフトウェア

Cisco IOS ソフトウェア モデルのポートの概念は、ハイブリッド ソフトウェア モデルと同じです。Cisco IOS モデルの場合、システムの設定はすべて単一のコマンドライン インターフェイスを通じて行われ、レイヤ 2 とレイヤ 3 の設定作業は区別されません。構文が異なる場合でも、レイヤ 2 ポートの概念(アクセス ポート、トランク ポート、およびレイヤ 3 VLAN インターフェイス [SVI] など)は依然として有効です。また、Cisco IOS ソフトウェアには、レイヤ 3 のルーテッド インターフェイスという概念があります。表 5 に、Cisco IOS の各種ポート タイプおよびインターフェイス タイプの概要を示します。詳細については、あとの項を参照してください。

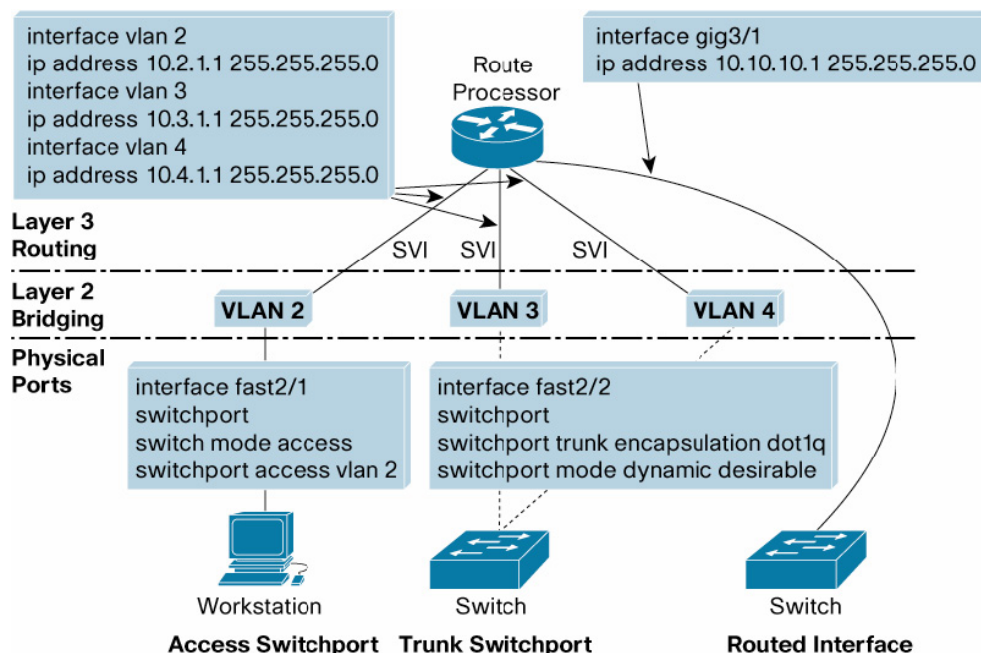
表 5 Cisco IOS のポートの概念

インターフェイス タイプ	目的	コンフィギュレーション例
ルーテッド インターフェイス	従来型の IOS ルーティング (各ポートが固有のネットワークを構成)	interface gigabitethernet 1/1 ip address 10.10.10.1 255.255.255.0 ipx network 1
ルーテッド SVI	1 つの VLAN に割り当てられたすべてのスイッチポートに対する単一のルーテッド インターフェイス	interface vlan 10 ip address 10.10.11.1 255.255.255.0 ipx network 2
レイヤ 2 VLAN	単一のレイヤ 2 ブロードキャストドメイン	vlan 10
アクセス スイッチ ポート インターフェイス	複数のレイヤ 2 ポートを単一の VLAN にまとめる	interface gigabitethernet 1/1 switchport switchport mode access switchport access vlan 10
トランク スイッチ ポート インターフェイス	異なる VLAN に属するレイヤ 2 ポートを構成する	Interface Gigabit Ethernet 1/1 Switchport switchport trunk encap dot1q switchport mode dynamic desirable

**注:** この文書では、「インターフェイス」と「ポート」という用語は同じ意味で使用されています。Cisco IOS のコマンドラインでは、ポートはインターフェイスと表され、CatOS のコマンドラインでは、一貫してポートという表現が使用されます。

図 4 は、レイヤ 2 またはレイヤ 3 の機能を使用する Cisco IOS の各種インターフェイス タイプとコマンドを示しています。

図 4 Cisco IOS モデルでのポートの概念



Cisco IOS では、モジュールのインターフェイス番号は 0 ではなく 1 から始まるため、スロット 2 に搭載されたラインカードの最初のインターフェイスは 2/1 となります。これは、CatOS で使用されるポート番号の表記法と同じです。

以下に、Cisco IOS ソフトウェアで使用される 3 つの主要なポートタイプについて説明します。

#### ルーテッド インターフェイス

Cisco IOS ソフトウェアでは、物理ポート レベル(この項で述べるルーテッド インターフェイス)または仮想ポート レベル(あとの項で述べる SVI)のいずれかの方法でレイヤ 3 インターフェイスを作成できます。Cisco IOS の場合、各物理ポートはデフォルトで(Cisco ルータと同じ)ルーテッド インターフェイスになります。スイッチ上のイーサネット ポート(ファスト イーサネット、ギガビット イーサネット、または 10 ギガビット イーサネット)はすべて `interface <interfacetype> <slot/port>` と表示され、デフォルトでシャットダウン状態になっています。この動作は CatOS とは異なります。CatOS では、すべてのポートが有効で、レイヤ 2 を認識し、デフォルトで VLAN 1 に所属し、ルーテッド インターフェイスをサポートしない設定になっています。Cisco IOS のルーテッド インターフェイスは、固有の IP サブネットまたは IPX ネットワーク上で構成する必要があります。これらのインターフェイスでは、Spanning-Tree Protocol (STP; スパニングツリー プロトコル)や DTP などのレイヤ 2 プロトコルは使用できません。

従来型の LAN ベース イーサネット ポートの場合、ルーテッド インターフェイスで IEEE 802.1Q カプセル化を区別するためのサブインターフェイスを作成することはできません。IEEE 802.1Q サブインターフェイスと同じ機能は、トランク ポート(あとの項を参照)で実現されます。

#### レイヤ 2 VLAN

同じ IP または IPX サブネットに複数のインターフェイスを配置する場合、ポートがレイヤ 2 ドメインや VLAN の一部として機能するように、ポートをルーテッド インターフェイスからレイヤ 2 ポートに変換する必要があります。ルーテッド インターフェイスを変換するには、最初にレイヤ 2 VLAN のエンティティを作成します。

VLAN ID を設定すると、レイヤ 2 ブロードキャストドメインまたはレイヤ 2 VLAN のインスタンスが作成されます。設定は、**vlan <vlan #>** コマンドを使用してグローバル コンフィギュレーション モードから行います。利用可能な VLAN ID は 1 ~ 4096 です。CatOS および Cisco IOS のどちらの場合でも、VLAN ID 1002 ~ 1005 は VTP のデフォルト VLAN で、ユーザによる設定変更はできません。

次の例は、CatOS および Cisco IOS で vlan 8 を作成する手順を示しています。

CatOS	Cisco IOS ソフトウェア
set vlan 8	IOS#configure terminal IOS(config)#vlan 8 IOS(config-vlan)#exit

CatOS および Cisco IOS ソフトウェアでは、4096 のレイヤ 2 VLAN を作成できるため、限られた数のシステム MAC アドレスを効率的に割り当てるために、MAC アドレス リダクション機能を有効にする必要があります。この機能を有効にするには、次のコマンドを使用します。

CatOS	Cisco IOS ソフトウェア
set spantree macreduction enable	IOS(config)# spanning-tree extend system-id

#### ルーテッド SVI

同一デバイス上の複数のポートが 1 つのサブネットに属する場合、VLAN を作成してこれらのポートをレイヤ 2 でグループ化します(上述のレイヤ 2 VLAN を参照)。一般に、これらのポートは別のサブネットまたは VLAN にトラフィックを送信する必要があります。この要件を実現するには、SVI を作成して VLAN 間ルーティングを可能にします。ハイブリッド ソフトウェア モデルの場合と同様に、Cisco IOS の SVI は **interface VLAN 1**、**interface VLAN 2** のように識別されます。これらのインターフェイスは、IP サブネットや IPX ネットワーク番号などのレイヤ 3 情報に関連付けられます。特定のレイヤ 2 VLAN に SVI が関連付けられていない場合、トラフィックはその VLAN 内でブリッジされますが、その VLAN との間でルーティングはされません。スイッチ ポートを VLAN に追加したり、VLAN から削除したりすると、そのポートは関連する SVI によって作成されたレイヤ 3 環境に自動的に加わります。Cisco IOS ソフトウェアでデバイスを管理する場合、ネットワーク アクセスを可能にするため SVI に IP アドレスを設定する必要があります。

#### アクセス スイッチポート

アクセス スイッチポートは、1 つの VLAN だけに属するレイヤ 2 ポートです。設定には **switchport** コマンドを使用して、インターフェイスをデフォルトのルーテッド インターフェイスからレイヤ 2 インターフェイスに変換します。ポートをレイヤ 3 ポートからレイヤ 2 ポートに変換すると、DTP や STP などのレイヤ 2 機能が有効になります。この **switchport** コマンドを有効にしないかぎり、スイッチポートに関連する他のいかなる設定も有効にできません。CatOS のポート動作と同様に、Cisco IOS のスイッチポートはデフォルトで VLAN 1 になります。スタティックなアクセス ポート(トランクのネゴシエーションを行わないポート)を作成する場合は、インターフェイス コンフィギュレーションから **switchport mode access** コマンドを入力します。その後、**switchport access vlan <vlan-id>** コマンドを使用して、特定の VLAN にこのアクセス ポートを割り当てます。次の例では、ポート 5/1 を VLAN 2 のアクセス ポートとして定義しています。

```
IOS# configure terminal
IOS(Config)# interface fastethernet5/1
IOS(Config-if)# switchport
IOS(Config-if)# switchport mode access
IOS(Config-if)# switchport access vlan 2
IOS(Config-if)# no shut
IOS(Config-if)# end
```

#### トランク スイッチポート

Cisco IOS ソフトウェアのトランク スイッチポートは、ISL または IEEE 802.1Q のカプセル化を使用して複数の VLAN をサポートするレイヤ 2 ポートです。このポートは、ISL または IEEE 802.1Q プロトコルをサポートする他のすべてのデバイスと完全な互換性があります。

ルーテッド インターフェイスをレイヤ 2 スイッチポートに変換すると、スイッチポートはデフォルトで *switchport mode dynamic desirable* になります。トランクのネゴシエーションを行う DTP を使用すると、このポートは隣接するレイヤ 2 デバイスとのトランクを構成できます。隣接インターフェイス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（デフォルトが *dynamic/desirable* であるため）。トランクはデフォルトでカプセル化のネゴシエーションを行います。隣接インターフェイスが ISL および IEEE 802.1Q カプセル化をサポートし、両方のインターフェイスがカプセル化タイプのネゴシエーションを行うように設定されている場合、トランクは ISL カプセル化を使用します。この動作は CatOS の場合と同じです。次の例は、IEEE 802.1Q カプセル化を行うようにトランクを設定する手順を示しています。

```
IOS# configure terminal
IOS(Config)# interface fastethernet 5/1
IOS(Config-if)# switchport
IOS(Config-if)# switchport trunk encapsulation dot1q
IOS(Config-if)# end
```

トランクのネゴシエーション ステートについては、次の URL で Cisco IOS のコンフィギュレーションガイドを参照してください。

[http://www.cisco.com/jp/service/manual\\_j/sw/cat60/iOSScg/chapter11/3999\\_08\\_11.shtml](http://www.cisco.com/jp/service/manual_j/sw/cat60/iOSScg/chapter11/3999_08_11.shtml)

**注：** 隣接デバイス間では、ダイナミック トランク ポートの設定を *desirable/auto* にすることが推奨されています。

IEEE 802.1Q トランク ポートのネイティブ VLAN を設定する場合は、**switchport trunk native vlan <vlan-id>** コマンドを使用します。インターフェイスから転送される VLAN を制御するには、*allowed* パラメータを使用します。また、リンク上で VTP プルーニングを制御するには、*pruning* パラメータを使用します。CatOS または Cisco IOS ソフトウェアいずれの場合も、VLAN 1 ではプルーニングを使用できません。ただし、Cisco IOS ソフトウェアおよび CatOS のどちらの場合も、VLAN 1 でトランク上のトラフィック伝送を無効にすることは可能です。

**no switchport** コマンドを入力すると、このスイッチポートに関連するすべてのコマンドがコンフィギュレーションから消去され、インターフェイス タイプはルーテッド インターフェイスに戻ります。た

だし、*switchport* を再度有効にすると、以前使用していたスイッチポートに関連するすべてのコマンドが再度有効になります。\*\*\*\*

\*\*\*\* これは、「no switchport」コマンドを実行してもリポートされないシステムに適用されます。

#### Cisco IOS のインターフェイス設定 (range コマンド)

すべてのインターフェイス タイプ(ルーテッド インターフェイス、SVI、またはスイッチポート)はグループ単位で設定できます。つまりポートのグループに対して、コンフィギュレーション パラメータを一度に適用することができます。Cisco IOS の **range** コマンドでは、**interface range** でポートの範囲を指定すると、複数のインターフェイスを同時に設定できます。指定するポートの範囲は、同一のラインカードまたは異なるラインカードで非連続に選択できます。次に、範囲設定の例を示します。

```
IOS(config)#int range fa3/1-48,gi1/1-2
IOS(config-if)# switchport
IOS(config-if)#switchport mode access
IOS(config-if)#switchport access vlan 2
IOS(config-if)# spanning-tree portfast
IOS(config-if)#no shut
```

**注:** 12.2(18)SXE 以前の IOS イメージの場合、ダッシュの前のスペースは必須です。また範囲は、カンマで区切って最大 5 つまで指定できます。カンマの前後にスペースを入れる必要はありません。

**range** コマンドは、ファスト イーサネット、ギガビット イーサネット、10 ギガビット イーサネットのインターフェイスで使用できます(上記を参照)。SVI が作成されている場合は、VLAN インターフェイスでも使用できます。

```
IOS(config)#int range vlan2 - 4
IOS(config-if)# description Floor 1 access VLANs
```

**インターフェイス レンジ マクロ**は、頻繁にグループ化されるポートを識別する場合に使用します。ポートの範囲はマクロで定義され、名前が付与されます。マクロが作成されると、各ポートを明示的に指定せずに、マクロ名を使用してポートのグループを指定できます。これは、同じポートグループ(すべての 10/100 サーバ ポートなど)の設定を頻繁に変更する場合に便利です。この機能は CatOS では利用できません。次の例では、ポート 3/1 ~ 3/8 に対して「servers」というインターフェイス レンジ マクロが定義されています。

```
IOS# configure terminal
IOS(config)#define interface-range servers fastethernet 3/1-8
IOS(config)#int range macro servers
IOS(config-if-range)#
To display the macro:
IOS# show running-config | include define
define interface-range servers fastethernet 3/1-8
```

## CatOS および Cisco IOS でのインターフェイスのモニタリング

インターフェイスをモニタリングする場合によく使用するコマンドは、次のとおりです。

```
CatOS> (enable) show port
```

Port	Name	Status	Vlan	Duplex	Speed	Type
1/1		connected	1	full	1000	1000BaseSX
1/2		notconnect	1	full	1000	No Connector
11/1		notconnect	1	auto	auto	10/100/1000
11/2		notconnect	1	auto	auto	10/100/1000
11/3		notconnect	1	auto	auto	10/100/1000
11/4		notconnect	1	auto	auto	10/100/1000
11/5		notconnect	1	auto	auto	10/100/1000
11/6		notconnect	1	auto	auto	10/100/1000
11/7		notconnect	1	auto	auto	10/100/1000
11/8		notconnect	1	auto	auto	10/100/1000

```
IOS#show interface status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Gi1/1		notconnect	routed	full	1000	No GBIC
Gi1/2		notconnect	routed	full	1000	No GBIC
Gi4/1		connected	1	full	1000	1000BaseSX
Gi4/2		disabled	routed	full	1000	1000BaseSX
Gi4/3		disabled	routed	full	1000	No GBIC
Gi4/4		disabled	routed	full	1000	1000BaseSX
Gi4/5		disabled	routed	full	1000	No GBIC
Gi4/6		disabled	routed	full	1000	No GBIC
Gi4/7		disabled	routed	full	1000	1000BaseSX
Gi4/8		disabled	routed	full	1000	1000BaseSX

### 機能の比較

以下の各項では、CatOS と Cisco IOS ソフトウェアの一般的な機能の違いについて説明します。ここでは、Cisco Catalyst 6500 でよく使用される一部の機能について、実装方法と CLI 構文の違いを説明するだけで、すべての機能や動作を網羅しているわけではありません。CatOS および Cisco IOS のすべての機能の詳細については、次の URL (英語) にある文書を参照してください。

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/index.htm>

### VLAN トランキンク プロトコル (VTP)

VTP は、レイヤ 2 ドメイン内のスイッチ間で VLAN 情報を管理する場合に使用します。VTP 管理は VTP サーバおよび VTP クライアントとして設定されたスイッチ間で行われ、ネットワーク内の共通の VLAN トポロジーの学習が行われます。デバイスは VTP トランスペアレント デバイスとして設定することもできます。VTP トランスペアレント デバイスは、VTP プロトコルに参加しませんが、VTP アドバタイズを転送することは可能です。CatOS と Cisco IOS ソフトウェアにおける VTP 機能の唯一の違いは、CatOS では VTP を完全に無効化できる点です (たとえば「off」モードの場合、デバイスは VTP アドバタイズを転送しません)。

Cisco IOS ソフトウェアの場合、VTP トランスペアレント、VTP クライアント、および VTP サーバ システムの VTP/VLAN 設定は、グローバル コンフィギュレーション モードで実行します。\*\*\*\*\* 次の例は、VTP ドメイン、VTP モード、および VLAN を定義して、ポートに適用する手順を示しています。

CatOS	Cisco IOS ソフトウェア
<code>set vtp domain ENG-CAMPUS</code>	IOS#configure terminal
<code>set vtp mode server</code>	IOS(config)#vtp mode server
<code>set vlan 8 name engineering</code>	IOS(config)#vtp domain ENG_CAMPUS
<code>set vlan 8 5/1-48</code>	IOS(config)#vlan 8
	IOS(config-vlan)#name engineering
	IOS(config)#interface range fastethernet 5/1-48
	IOS(config-if-range)#switchport
	IOS(config-if-range)#switchport mode access
	IOS(config-if-range)#switchport access vlan 8

\*\*\*\*\* VLAN または VTP は、VLAN データベース サブモードで設定する必要はありません。

#### Cisco IOS ソフトウェアにおける VTP の動作

CatOS では、コンフィギュレーションが変更されるとすぐに NVRAM に書き込まれます。反対に、Cisco IOS ソフトウェアでは、**copy run start** コマンドを実行しない限り、NVRAM にコンフィギュレーションの変更が保存されることはありません。VTP クライアントおよび VTP サーバのシステムでは、他の VTP サーバによる VTP の更新を即座に NVRAM に自動保存する必要があります。CatOS のデフォルト動作はこの VTP 更新要件を満たしていますが、Cisco IOS の更新モデルでは、更新操作を別に行う必要があります。

VLAN データベースは、VTP クライアントおよび VTR サーバの VTP 更新を即座に保存する方式として、Catalyst 6500 の Cisco IOS に導入されました。この VLAN データベースは、NVRAM 内に (vlan.dat という) 個別ファイルとして存在します。vlan.dat ファイルには VTP クライアントまたは VTP サーバ システムの VTP/VLAN 情報が格納され、**sh vtp status** を使用して情報を表示することができます。これらのシステムで **copy run start** コマンドを使用しても、NVRAM のスタートアップ コンフィギュレーション ファイルに VTP/VLAN の設定全体がバックアップされるわけではありません。

これは VTP トランスペアレントとして稼働するシステムには適用されません。VTP トランスペアレント システムで **copy run start** コマンドを使用すると、NVRAM のスタートアップ コンフィギュレーション ファイルに VTP/VLAN の設定全体がバックアップされます。

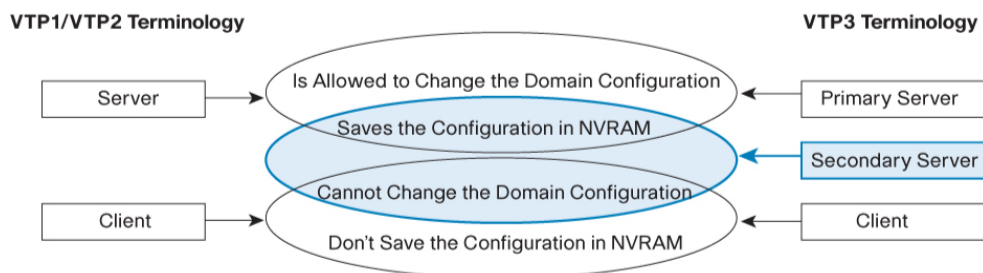
#### CatOS の VTPv3

CatOS は VTP の新バージョンである VTP Version 3 (VTPv3) をサポートしています。VTPv3 は 拡張範囲 VLAN (4096) のアドバタイズをサポートしています。この 4096 の VLAN 全体は、1 つのスイッチで一元的に設定を変更でき、変更が加えられるとネットワーク内の他のすべてのスイッチに自動的に反映されます。

また、VTPv3 では、誤って設定されたサーバや許可されていないサーバが導入された場合に、ドメインの設定が消失したり上書きされたりするリスクがありません。この機能は、プライマリ サーバとセカンダリ サーバという概念を導入し、ドメインの分割を可能にすることによって実現されました。ユーザはプライマリ サーバとして機能するサーバをスタティックに定義する必要があります。ドメインで使用できる VTP デバイスの説明は、次のとおりです。

- VTPv3 のプライマリ サーバは、VLAN の作成、変更、および削除と、それ以外のドメイン設定パラメータを指定できます。プライマリ サーバは、同一 VTP ドメイン内のスイッチに自らの VLAN 設定をアドパタイズし、トランク リンクを介して受信したアドパタイズに基づいて、自らの VLAN 設定を他のスイッチと同期させます（既存の VTP バージョンと同じ）。
- VTPv3 のセカンダリ サーバは、本来のクライアントとサーバの中間的な機能を備えています。ドメインの設定を保存することは可能ですが、変更することはできません。
- VTPv3 のクライアントはネットワークから設定を受信するだけで、設定の保存や変更はできません（既存の VTP バージョンと同じ）。

図 5



### Spanning Tree Protocol (STP) \*\*\*\*\*

Spanning-Tree Protocol (STP; スパニング ツリー プロトコル) は、複数のパスを経由してスイッチまたはブリッジを相互接続する際に、ループの発生を防止します。STP は、ループを検出するために他のスイッチと BPDU メッセージを交換することで 802.1D IEEE アルゴリズムを実装し、選択したブリッジ インターフェイスをシャットダウンしてループを解消します。このアルゴリズムにより、2 つのネットワーク デバイス間のアクティブ パスが 1 つだけになります。

Common Spanning-Tree (CST) では、VLAN の数に関係なく、ブリッジ型ネットワーク全体で 1 つのスパニングツリー インスタンスを想定しています。ネットワーク全体で保持されるスパニングツリー インスタンスが 1 つだけになるため、この実装により CPU 負荷が軽減されます。この実装は、ネットワークで必要なレイヤ 2 トポロジーが 1 つだけの場合に使用できます。

Multiple Instance STP (MISTP) (802.1s) は、数を減らしたスパニングツリー インスタンスに複数の VLAN をマッピングできる IEEE 標準です。このようなマッピングが可能なのは、ほとんどのネットワークで複数の論理トポロジーを必要としないためです。各インスタンスは、同じレイヤ 2 トポロジーを持つ複数の VLAN を処理します。

Per-VLAN Spanning Tree (PVST) は、ネットワークで構成された VLAN ごとにスパニングツリー インスタンスを保持します。PVST は ISL トランキングを使用して、VLAN トランクのフォワーディングとブロッキングを同時に行います。PVST は各 VLAN を個別のネットワークとみなすため、スパニングツリー ループを発生させることなく、トランク上の VLAN をフォワーディングすることで、レイヤ 2 のトラフィックのロードバランシングを実行できます。PVST+ (他の利点については後述します) は、802.1Q トランキング テクノロジーに同じ機能を提供し、シスコ スイッチでのみサポートされています。

Rapid Spanning Tree Protocol (RSTP; 高速スパニング ツリー プロトコル) は、スパニングツリー プロトコル (802.1D 規格) を改良したもので、トポロジーの変更後に高速のスパニングツリー コンバージェンスを実現します。この規格には、Cisco PortFast、UplinkFast、および BackboneFast と同等の機能も含まれており、ネットワークの再コンバージェンスをより高速に行います。

ここでは、基本的な STP 構成、PVST+(802.1D)、IEEE 802.1s(MST)、IEEE 802.1w(RSTP)、および Rapid PVST+について、CatOS と Cisco IOS の設定上の相違点を説明します。

\*\*\*\*\* [http://www.cisco.com/en/US/partner/tech/tk389/tk621/tsd\\_technology\\_support\\_protocol\\_home.html](http://www.cisco.com/en/US/partner/tech/tk389/tk621/tsd_technology_support_protocol_home.html)

#### 基本的な STP 構成

CatOS	Cisco IOS ソフトウェア
set spantree root 10 dia 5 hello 2	IOS(config)# spanning-tree vlan 10 root primary dia 5 hello 2
set spantree root sec 11 dia 5 hello 2	IOS(config)# spanning-tree vlan 11 root sec dia 5 hello 2
set spantree priority 4096 10,11	IOS(config)# spanning-tree vlan 10 pri 4096 IOS(config)# spanning-tree vlan 11 pri 4096

#### PVST+の拡張機能

PVST+では、シスコ独自のプロトコル(UplinkFast、BackboneFast、および PortFast など)を PVST+プロトコルに統合し、コンバージェンス時間を高速化することで、基本的なスパニングツリーアルゴリズムを拡張しています。

スパニングツリー UplinkFast を使用すると、ダイレクト ルート リンクに障害が発生した場合、レイヤ 2 ネットワークでのコンバージェンスが高速化されます。あるブリッジからルート ブリッジへのリンクがダウンすると、ブリッジは通常のスパニングツリー タイマーが切れるのを待たずに、ただちにブロッキング ポートをフォワーディング ポートに変更します。これにより、コンバージェンス時間が 50 秒から 3 ~ 5 秒、または 1 秒以内に短縮されます。

レイヤ 2 ネットワークで間接障害が発生すると、スパニングツリー BackboneFast は「maximum age」タイマーの値(デフォルトで 20 秒)を使用してコンバージェンス時間を短縮します。

また、スパニングツリー PortFast では、アクセス ポートがリスニング ステートおよびラーニング ステートを経由することなく、ただちにフォワーディング ステートになります。この機能は、1 台のワークステーション、IP フォン、またはサーバなどに接続されているスイッチ ポートで使用されます。この機能を使用すると、これらの装置はスパニングツリーのコンバージェンスを待たずに、ただちにネットワークに接続されます。通常、アクセス ポートは接続デバイスから Bridge Protocol Data Unit(BPDU; ブリッジ プロトコル データ ユニット)を送受信しないため、CatOS および Cisco IOS のどちらの場合でも、PortFast モードは非トランキング アクセス ポートおよびトランク ポートでサポートされます。

次の例は、上述の PVST+の拡張機能に関連する設定作業です。

CatOS	Cisco IOS ソフトウェア
set spantree uplinkfast enable	IOS(config)# spanning-tree uplinkfast
set spantree backbonefast enable	IOS(config)# spanning-tree backbonefast
set spantree portfast 3/1 enable	IOS(config)# int range fa3/1 IOS(config-if)# switchport IOS(config-if)# spanning-tree portfast

#### Rapid PVST+

Rapid PVST+は IEEE 802.1w 規格に準拠しており、PVST+の既存の設定を使用して STP のコンバージェンスを高速化します。Rapid PVST+では、トポロジーが変更されると、エントリがポート単位ですぐに消去されます。このモードでは、Rapid Spanning Tree Protocol(IEEE 802.1w)に UplinkFast および BackboneFast の機能が含まれているため、両者の設定は無視されます。

CatOS	Cisco IOS ソフトウェア
Set spantree mode rapid-pvst+	IOS(config)#spanning-tree mode rapid-pvst

#### IEEE 802.1s(MST)

Multiple Spanning Tree (MST) は IEEE 802.1s に準拠しており、IEEE 802.1w の Rapid Spanning Tree (RST) アルゴリズムを複数のスパンニングツリーに拡張しています。この拡張によって、コンバージェンスが PVST+よりも高速化されると同時に、VLAN 環境における高速コンバージェンスとロードバランシングの両方が可能になります。

MST を使用すると、トランク上に複数のスパンニングツリーを作成して、データトラフィック用に複数のフォワーディングパスを確保できます。この場合、1つの障害がスパンニングツリーの他のインスタンスに直接影響することがないため、耐障害性が向上します。また、複数の VLAN をスパンニングツリーの1つのインスタンスにまとめることによって、システムの CPU 負荷が大幅に減少します。

MST の設定に関する CatOS と Cisco IOS の大きな違いは、Cisco IOS の MST コンフィギュレーション サブモードです。このモードは、MST のコンフィギュレーションを入力および表示する場合に使用します。

CatOS	Cisco IOS ソフトウェア
Set spantree mst config name MST revision 1 Set spantree mst <b>instance</b> vlan <b>vlan</b> Set spantree mst config commit Set spantree mode mst	IOS(config)#spanning-tree mode mst IOS(config)#spanning-tree mst configuration IOS(config-mst)#name MST revision 1 instance 1 vlan 3

#### IEEE 802.1w(Rapid PVST+)

RSTP は、1台のスイッチを選択してスパンニングツリーのルートとして動作させることにより、ネットワークの再コンバージェンス時間を短縮します。これは、IEEE 802.1D ではなく、IEEE 802.1w に準拠しています。Rapid PVST+の設定は PVST+と同様ですが、次の構文が追加されています。

CatOS	Cisco IOS ソフトウェア
Set spantree mode rapid-pvst+ Set spantree link-type mod/port point-to-point	IOS(config)#spanning-tree mode rapid-pvst

**注:** CatOS のコマンド構文は **rapid-pvst+** を使用し、Cisco IOS は **rapid-pvst** を使用します。

#### ルートガードおよびBPDUガードの設定

ポートベースの BPDU ガードは、ポート上の BPDU をモニタします。アクセスポート上で BPDU が検出されると、BPDU ガードが設定されたインターフェイスはシャットダウンされます。PortFast が設定されたインターフェイスが BPDU を受信すると、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。BPDU ガード機能では、管理者が手動でインターフェイスを再度有効にするか、またはエラーディセーブル機能を使用して自動的にインターフェイスを再度有効にする必要があるため、無効な設定に対する安全な対処が可能になります。

スパンニングツリーのルートガード機能は、インターフェイスを強制的に指定ポートにします。また、このインターフェイスを経由してアクセス可能なデバイスがルートブリッジになろうとすると、ルートガード機能はそのインターフェイスを root-inconsistent (ブロッキング) ステートにします。

Cisco IOS ソフトウェアが BPDU ガードとルート ガード機能をサポートしているのは、スイッチポート上だけです。主な設定の相違点については、次のコンフィギュレーション ダイアログを参照してください。

CatOS	Cisco IOS ソフトウェア
<pre>set spantree bpdu-guard 3/1 enable set spanning-tree guard root 1/1 show spantree summary</pre>	<pre>IOS(config)# int range fast3/1 IOS(config-if)# switchport IOS(config-if)# spanning-tree portfast bpduguard IOS(config-if)# spanning-tree guard root IOS# show spanning-tree summary</pre>

### EtherChannel

CatOS および Cisco IOS ソフトウェアの 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、ネットワーク内での帯域幅集約およびリンク復元機能を実現します。Catalyst 6500 では、EtherChannel ごとに最大 8 つのイーサネット インターフェイスをすべて同一速度で設定できます (10、100、1000、または 10000 Mbps)。EtherChannel グループには、任意のライン カードを組み合わせてポートを追加できます。

### EtherChannel の動作

Cisco IOS ソフトウェアで EtherChannel を設定する手順は 2 段階です。まず **channel-group** にポートを割り当て、次に仮想的な **interface port-channel** を設定します。仮想的な **interface port-channel** は、物理インターフェイスと同じように動作します。CatOS および Cisco IOS どちらの場合も、ポート チャネル インターフェイスのすべての設定はポート チャネルの物理インターフェイスに伝えられます。たとえば、ポート チャネル インターフェイスを閉じると、そのポート チャネル上のすべての物理ポートがシャットダウンされます。EtherChannel の全ポートのパラメータを変更する場合は、コンフィギュレーションをポート チャネル インターフェイスに適用する必要があります。Cisco IOS ソフトウェアでは物理インターフェイスの設定が可能ですが、このコンフィギュレーションはポート チャネル バンドルには伝播されません。バンドル内のインターフェイスが同じでない場合、チャンネルは形成されません。

CatOS	Cisco IOS ソフトウェア
<pre>set port channel 3/1-8 1 desirable</pre>	<pre>interface range gigabit 3/1-8 switchport channel-group 1 mode desirable no shut interface port-channel 1 switchport trunk encapsulation dot1q no shut</pre>

CatOS は最大 128 の EtherChannel グループをサポートし、Cisco IOS ソフトウェアは最大 64 の EtherChannel グループをサポートしています (Cisco IOS 12.2(18)SXE 以降では 128 の Etherchannel グループがサポートされています)。

### EtherChannel のネゴシエーション

Cisco IOS および CatOS の EtherChannel は PAgP と LACP の両方をサポートしています。PAgP や LACP を使用すると、他のデバイスとのポート チャネルを自動的に作成できます。PAgP はシスコ独自のチャンネル ネゴシエーション プロトコルであり、LACP は IEEE 802.3ad で定義されたチャンネル ネゴシエーションの規格です。これらのプロトコルのネゴシエーション モードはほとんど同じです。Cisco IOS ソフトウェアと CatOS ソフトウェアではネゴシエーション キーワードは同じで

す。PAgP および LACP の設定の詳細については、次の URL からコンフィギュレーション ガイドを参照してください。

- [http://www.cisco.com/jp/service/manual\\_j/sw/cat60/iosscg/chapter13/3999\\_08\\_13.shtml](http://www.cisco.com/jp/service/manual_j/sw/cat60/iosscg/chapter13/3999_08_13.shtml)
- [http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw\\_7\\_3/config\\_gd/channel.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_7_3/config_gd/channel.htm)

#### PAgP 設定の例

CatOS	Cisco IOS ソフトウェア
<pre>set channelprotocol pagp set port channel 3/1-8 1 desirable</pre>	<pre>interface range gigabit 3/1-8 switchport channel-protocol pagp channel-group 1 mode desirable interface port-channel 1 switchport trunk encapsulation dot1q no shut</pre>

#### LACP 設定の例

CatOS	Cisco IOS ソフトウェア
<pre>set channelprotocol lacp set port channel 3/1-8 1 desirable</pre>	<pre>interface range gigabit 3/1-8 switchport channel-protocol lacp channel-group 1 mode active interface port-channel 1 switchport trunk encapsulation dot1q no shut</pre>

CatOS では、チャンネル プロトコルはモジュール単位で設定します。つまり、1 つのモジュール上のすべてのチャンネル ポートは、同じネゴシエーション プロトコルを使用する必要があります。Cisco IOS ソフトウェアでは、チャンネル プロトコルはポート単位で設定できます。

#### EtherChannel のロード シェアリング

EtherChannel では、複数のロードバランシング アルゴリズムを使ってポートにトラフィックを分散させることができます。この機能は、EtherChannel にレイヤ 2 またはレイヤ 3 のポートやインターフェイスが含まれているかどうかに関係なく利用できます。CatOS および Cisco IOS ソフトウェアで使用できるオプションは同じです(下記を参照)。

CatOS	Cisco IOS ソフトウェア
<pre>set port channel all distribution ? ip          Channel distribution ip mac        Channel distribution mac session    Channel distribution session set port channel all distribution ip ? source     Channel distribution source destination Channel distribution dest both      Channel distribution both</pre>	<pre>port-channel load-balance ? dst-ip      Dst IP Addr dst-mac     Dst Mac Addr dst-port    Dst TCP/UDP Port src-dst-ip  Src XOR Dst IP Addr src-dst-mac Src XOR Dst Mac Addr src-dst-port Src-Dst TCP/UDP Port src-ip      Src IP Addr src-mac     Src Mac Addr src-port    Src TCP/UDP Port</pre>

### EtherChannel のタイプ

Cisco IOS ソフトウェアには、レイヤ 2 およびレイヤ 3 の EtherChannel が存在します。Cisco IOS ソフトウェアの場合、レイヤ 2 EtherChannel にはスイッチ ポートとして設定されたポートを追加できます。また、レイヤ 3 EtherChannel にはスイッチポートと SVI の組み合わせ(またはルーテッド インターフェイス)のみを追加できます。CatOS はルーテッド ポートをサポートしておらず、SVI のみをサポートしているため、CatOS にはレイヤ 3 EtherChannel の 1 タイプしか存在しません。

#### レイヤ 2 EtherChannel

すべてのインターフェイスは共通の **channel-group** にグループ化され、続いて **interface port-channel** がスイッチポートとして設定されます。物理インターフェイス上で **channel-group** コマンドが有効になると、チャンネル プロトコル(PAgP または LACP)は *Port-Channel 1* インターフェイスを自動的に作成します。

CatOS	Cisco IOS ソフトウェア
<pre>set port channel 3/1-8 1 desirable set trunk 3/1-8 dot1q</pre>	<pre>interface range fa3/1 - 8 no shut channel-group 1 mode desirable interface port-channel 1 switchport switchport trunk encap dot1q no shut</pre>

**注:** デフォルトでは PAgP ネゴシエーション

#### SVI を使用したレイヤ 3 EtherChannel

SVI を使用したレイヤ 3 EtherChannel は、ルーティング機能を実現するレイヤ 3 SVI を追加で使用し、レイヤ 2 EtherChannel と同じように作成されます。この方法では、トランスポートを提供するレイヤ 2 VLAN、および VLAN の終端とルーティングを提供する SVI を使用してレイヤ 3 EtherChannel を構成します。

CatOS	Cisco IOS ソフトウェア
<pre><b>Catalyst OS config:</b> set port channel 3/1-8 2 desirable set spantree portfast 3/1-8 set vlan 10 3/1-8 <b>MSFC config:</b> int vlan 10 ip address 10.10.10.1 255.255.255.0</pre>	<pre>interface range fa3/1 - 8 no shut channel-group 1 mode desirable interface port-channel 1 switchport switchport mode access no shut int vlan 10 ip address 10.10.10.1 255.255.255.0</pre>

#### レイヤ 3 EtherChannel

本来のレイヤ 3 EtherChannel は IP サブネットのみで特定され、レイヤ 2 VLAN は無関係です。前述のルーテッド インターフェイスと同様に、これは Cisco IOS ソフトウェアだけで通用する概念です。次の例は、レイヤ 3 EtherChannel を設定する際に使用するコマンドラインの構文です。

CatOS	Cisco IOS ソフトウェア
<p>Catalyst OS には該当するコマンドなし</p>	<pre>int range fa3/1-8 channel-group 1 mode desirable interface port-channel 1 ip address 10.10.10.1 255.255.255.0</pre>

Cisco IOS システムの EtherChannel では、次の **show** コマンドが役立ちます。

- **show etherchannel summary** を使用すると、Cisco IOS システムのすべての EtherChannel ステートおよびポートが表示されます。

```

cat6k#show etherchannel summary
Flags:D - down    P - in port-channel
      I - stand-alone s - suspended
      H - Hot-standby (LACP only)
      R - Layer3   S - Layer2
      U - in use   f - failed to allocate aggregator

      u - unsuitable for bundling
Number of channel-groups in use: 2
Number of aggregators: 2

Group Port-channel Protocol Ports
-----+-----+-----+-----
1   Po1(SD)      LACP   Fa3/13(P) Fa3/14(P) Fa3/15(P) Fa3/16(P)
273 Po273(SD) -
cat6k#

```

- **show interfaces etherchannel** を使用すると、チャンネル ステータスに関係なく、EtherChannel に割り当てられたチャンネルグループに属するすべてのインターフェイスが表示されます。表示したインターフェイスのステータスが 1 つだけの場合は、**show interfaces <mod>/<port> etherchannel** を使用すると特定のインターフェイスのチャンネル ステータスだけが表示されるため、いくつもの出力画面をスクロールせずに済みます。

```

IOS1#sh int gi8/15 etherchannel
Port state = Up Mstr In-Bndl
Channel group = 2          Mode = Desirable-S1    Gcchange = 0
Port-channel = Po2        GC = 0x00020001      Pseudo port-channel = Po2
Port index = 1           Load = 0x55
Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.         P - Device learns on physical port.
Timers: H - Hello timer is running.        Q - Quit timer is running.
        S - Switching timer is running.     I - Interface timer is running.

Local information:
Port      Flags State   Timers Interval  Count  Priority Method  Ifindex
Gi8/15   SC   U6/S7          30s      1      128    Any    33

Partner's information:
Port      Partner          Partner          Partner          Partner  Group
Name      Device ID       Port            Age  Flags  Cap.
Gi8/15   cat6k-3-ios     0050.808a.a200 Gi4/3  11s  SC    20001

Age of the port in the current state:00h:00m:42s

```

## Identity Based Networking Services (IBNS) — IEEE 802.1X 認証

IEEE 802.1X は、クライアント/サーバ ベースのアクセス制御および認証プロトコルであり、パブリックにアクセス可能なポート経由で不正な装置が LAN に接続されるのを防ぎます。802.1X は、スイッチ ポートに接続されたユーザを認証した上で、スイッチまたは LAN のサービスを使用できるようにします。装置が認証されるまでの間、802.1X はデバイスが接続されているポート経由での Extensible Authentication Protocol over LAN (EAPOL) トラフィックだけを許可します。認証に成功すると、すべてのトラフィックをポート経由で送受信することができます。

CatOS および Cisco IOS はいずれも IEEE 802.1X のポートベース認証、802.1X 複数ホストモード(仕様で定義済み)、および RADIUS サーバを使用する IEEE 802.1X の VLAN 割り当てをサポートしています。CatOS ではこのほかに、次の 802.1X 拡張機能もサポートしています。

- **補助 VLAN 用に設定されたポートでの 802.1X 認証**
- **ゲスト VLAN 用の 802.1X 認証** — この機能を使用すると、802.1X 非対応のホストが 802.1X 認証を使用するネットワークにアクセスできます。
- **ポート セキュリティを使用した 802.1X 認証** — 802.1X は MAC アドレス数を定義するポート セキュリティ機能に対応し、特定のポート上で認証を行います。他のすべての MAC アドレスを経由して接続するユーザのアクセスは拒否されます。
- **802.1X 複数認証モード** — 管理者は、複数のホストが 802.1X ポートにアクセスできるように複数の認証を指定することができます。ホストはすべて個別に認証されます。

例: `Set port dot1x mod/port multiple-authentication enable`

- **802.1X 単一方向制御ポート** — 管理者は、802.1X 対応ポートで Wake-On LAN 機能を使用して、定期的なシステム バックアップやホストのソフトウェア アップグレードを実行できます。この 802.1X 拡張機能を使用すると、802.1X ポートでトラフィックを発信専用を設定できます。
- **ACL(アクセス制御リスト)割り当て機能を備えた 802.1X** — この拡張機能を使うと、ユーザおよびユーザの RADIUS サーバでの認証に基づいて、ACL ポリシーをポートにダイナミックに割り当てることができます。
- **802.1X ユーザ ディストリビューション** — この機能を使用すると、同一「グループ名」の認証済みユーザを複数の VLAN に均等に割り当てて、負荷分散を行うことができます。
- **802.1X RADIUS アカウンティングおよびトラッキング** — スイッチのアカウント情報情報を RADIUS サーバに転送します。また管理者は、RADIUS サーバから、ユーザ アクセスを制御したり(ユーザがネットワークにアクセスできる時刻など)、所定のユーザ グループ内で任意の時刻に認証されるユーザの最大数を制御したりすることができます。
- **802.1X 認証 ID/ポート記述間マッピング** — この機能を有効にすると、管理者はユーザが認証されるポートに対し、ポート記述を割り当てることができます。この記述を表示するには、「show port」を実行します。この機能は RADIUS サーバ上で設定されます。
- **RADIUS の DNS 解決** — 管理者は、IP アドレスに加えて(または IP アドレスの代わりに)サーバの DNS 名を設定できます。RADIUS サーバでサブネットが変更されてもすぐに解決されるため、スイッチを設定しなおす必要はありません。

RADIUS サーバは、スイッチで 802.1X を有効にする前に指定する必要があります。その後、802.1X をグローバルで有効にして、最後に個々のポートのコンソールから有効にします(下記を参照)。下記には、複数のホストで設定を行う場合の構文も記載されています。

CatOS	Cisco IOS ソフトウェア
<b>Globally:</b> Set dot1x system-auth-control enable <b>Per Port:</b> Set port dot1x mod/port port-control auto <b>Multiple Host:</b> Set port dot1x mod/port multiple-host enable	<b>Globally:</b> Router(config)# dot1x system-auth-control Router(config)# interface type1 <slot/port>  <b>Interface Commands:</b> Router(config-if)# dot1x port-control auto Router(config-if)# dot1x host-mode multi-host

Catalyst 6500 における IEEE 802.1X の設定の詳細については、次の URL を参照してください。  
[http://www.cisco.com/jp/service/manual /sw/cat60/iosscg/chapter47/3999\\_08\\_47.shtml](http://www.cisco.com/jp/service/manual /sw/cat60/iosscg/chapter47/3999_08_47.shtml)

### シスコのセキュリティ ツールキットの機能

シスコのセキュリティ ツールキット(12.2(18)SXE 以降の CatOS IOS のみでサポート)は、DoS や man-in-the-middle (MiM) 攻撃の緩和に役立ちます。セキュリティ ツールキットは、DHCP スヌーピング、Dynamic ARP Inspection (DAI; ダイナミック ARP インスペクション)、IP ソースガードの 3 つの機能で構成されています。

DHCP スヌーピングは、特定の DoS 攻撃(DHCP ログ サーバ攻撃)を防御します。この種の攻撃では、ログ サーバはサーバ自身をネットワークに追加して、DHCP Discover や IP アドレスの DHCP Request に応答します。DHCP スヌーピングは、ポートを trusted (信頼する)または untrusted (信頼しない)に設定することにより、この種の攻撃を防ぎます。すべての untrusted ポートでは、DHCP Discover および DHCP Request の送信しかできません。逆に、trusted ポートでは、すべての DHCP トラフィック(IP アドレスの Request や Offer を含む)の送受信が可能です。

すべてのホストに接続されているポート、または未知のデバイスに接続されているすべてのポートでは、ポートの DHCP を untrusted に設定する必要があります。この場合、サーバが untrusted ポートに接続すると、サーバは要求元ホストに IP アドレスを発行できません。

また、DHCP スヌーピングでは DHCP スヌーピング テーブルが使用されます。DHCP スヌーピング テーブルには、クライアントの MAC アドレス、IP アドレス、リース期間、およびポート上の untrusted ホストの VLAN が格納されます。このテーブルは DAI などの他の機能でも、ポートに接続されているユーザがネットワークを攻撃するのを防ぐために使用されます。DAI はすべてのホストの IP アドレスと MAC アドレスの対応関係を検証することによって、ネットワークを保護します。次の例では、VLAN 20 で dhcp-snooping が有効になります。また、この VLAN のすべてのポートはデフォルトで untrusted です。

CatOS	Cisco IOS ソフトウェア
Console>(enable)set security acl ip snoopname permit dhcp-snooping Console>(enable)set security acl ip snoopname permit ip any any Console>(enable)commit security acl snoopname Console>(enable)set security acl map snoopname 20	Router(config)# ip dhcp snooping Router(config)# ip dhcp snooping vlan 20

「DAI」はネットワーク内の ARP パケットを検証します。DAI を使用すると、ネットワーク管理者は (DHCP スヌーピング バインディング テーブルの記録に基づいて)、MAC アドレスと IP アドレスの対応関係が不正な ARP パケットを遮断、記録、および廃棄できます。DAI は一部の MiM 攻撃を防御します。次の例では、VLAN 20 のポート 4/2 からのすべての ARP トラフィックに対して DAI を有効にします (4/2 が untrusted に設定されているため)。

CatOS
<pre>Console&gt;(enable)set security acl arp-inspection dynamic enable 20 Console&gt;(enable)set port arp-inspection 4/2 trust disable</pre>
Cisco IOS ソフトウェア
<pre>Router(config)# ip arp inspection vlan 20 Router(config)# interface FastEthernet 4/2 Router(config-if)# no ip arp inspection trust</pre>

IP ソース ガードは、(Sup720 および Sup32 上の)CatOS でのみサポートされている機能で、特定のポートの DHCP スヌーピング バインディング テーブルに記録されている IP アドレスのみを許容することによって、IP スプーフィングを防止します。当初は、DHCP スヌーピングによって捕捉される DHCP パケットを除いて、ポート上のすべてのトラフィックがブロックされます。クライアントが DHCP の IP アドレスを受け取ると、PACL (ポートベース ACL) がその IP アドレスからのトラフィックを許可するポートにインストールされます。送信元 IP アドレスが PACL 許可リストに存在しない IP アドレスは除かれます。このようにして、ユーザがネイバの IP アドレスになりすまそうとするのを防ぎます。

IP ソース ガードを設定するには、ポートのセキュリティ ACL をポートベース モードにして、DHCP スヌーピングを有効にする必要があります。次の例では、ポート 4/2 で IP ソース ガードが有効になり、VLAN 10 で DHCP スヌーピングを有効にするセキュリティ ACL の「dhcpsnoop」が有効になります。

CatOS
<pre>Console&gt;(enable)set port security-acl 4/2 port-based Console&gt;(enable)set port dhcp-snooping 4/2 source-guard enable Console&gt;(enable)set security-acl ip dhcpsnoop permit dhcp-snooping Console&gt;(enable)set security-acl ip dhcpsnoop permit any any Console&gt;(enable)commit security-acl dhcpsnoop Console&gt;(enable)set security acl map dhcpsnoop 10</pre>

### Secure Copy Protocol (SCP)

Secure Copy Protocol (SCP) は現在、CatOS と IOS でサポートされています。SCP を使用すると、暗号イメージ ファイルを安全にコピーできます。SCP は Secure Shell (SSH; セキュア シェル) を使用します。SCP を使用すると、ネットワーク管理者は暗号化チャネルを経由して、システムとの間で SCP をコピーできます。

### Time Domain Reflectometer (TDR)

Time Domain Reflectometer (TDR; タイム ドメイン反射率計) を使用すると、ケーブル プラントのトラブルシューティングが可能になるため、スイッチの運用サポートが容易になります。48 ポート 10/100/1000 RJ-45 モジュールと 6148A 10/100 モジュールのポート インターフェイスに内蔵された TDR を使用すると、ネットワーク管理者は離れた場所からケーブルの損傷や不具合を識別できます。TDR テストはケーブルに信号を送信します。TDR では、ポート インターフェイスに組み込ま

れたインテリジェントな DSP を使用して、エコーが戻ってくる時間を測定し、損傷箇所までの距離を算出します。

オンライン テストである TDR を実行すると、ポートに接続されたワイヤ ペアと損傷箇所までの距離 (損傷がある場合) が表示されます。実行コマンドは、次のとおりです。

CatOS	Cisco IOS ソフトウェア
Console>(enable)test cable-diagnostics tdr 3/1 Console>(enable)show port tdr 3/1	IOS#test cable-diagnostics tdr interface g3/1 IOS#show cable-diagnostics tdr interface g3/1

## ACL

Hybrid OS が稼働する Catalyst 6500 シリーズは、次のタイプの ACL をサポートしています。

- IOS の Routing ACL (RACL; ルーティング ACL) — VLAN 間のルーテッドトラフィックのアクセス制御を行います。IOS の標準および拡張 ACL はルータ インターフェイスの入力と出力で設定され、ルーティングされるパケットに適用されます。IOS の ACL を使用する場合は、Catalyst 6500 シリーズに PFC と MSFC の両方を搭載する必要があります。
- VLAN ACL (VACL) — IP または IPX プロトコルのレイヤ 3 またはレイヤ 4 情報に基づいてアクセス制御を行います。VACL は VLAN 上で (ブリッジングおよびルーティングされる) すべてのパケットに適用され、任意の VLAN インターフェイスで設定できます。VACL は特定の物理スイッチ ポートに対してトラフィックを安全にフィルタリングおよびリダイレクトするために使用されます。VACL の方向 (入力または出力) は定義されません。VACL 機能を使用する場合は PFC が必要です。
- QoS ACL — ポートまたは VLAN への着信時に、マーキングまたはポリシングを適用すべき入力トラフィックを識別する場合に使用します。QoS ACL 機能を使用する場合は PFC が必要です。
- PACL \*\*\*\*\* — 通常、複数のポートで構成される VLAN ではなく、物理ポートにマッピングされるアクセス リストです。VACL と同様に、PACL はレイヤ 2 およびレイヤ 3 によって転送されるパケットに適用されます。Catalyst 6500 でサポートされるのは、入力側の PACL だけです。

Hybrid OS での IOS RACL の実装方法は、Cisco IOS (Catalyst 6500 または他の IOS ルータ) の場合と同じです。CatOS と Cisco IOS ソフトウェアの QoS ACL については、このホワイトペーパーの QoS の項で説明します。ここでは、CatOS と Cisco IOS ソフトウェアでの VACL 実装方法の相違点、および CatOS での PACL 実装方法について説明します。

### VLAN Access Control List (VACL)

CatOS の場合、セキュリティ ACL ステートメントを設定すると VACL が作成されます。このステートメントは、セキュリティ ポリシーの match パラメータと action パラメータを設定する場合に使用されます。

Cisco IOS における VACL の設定は、従来型の IOS ACL の実装方法に基づいています。つまり、VACL は IOS の access-list コマンドを使用して、トラフィックのマッチング パラメータを定義します。ここから、すべての設定 (ACL リファレンスおよびアクションなど) を「VLAN アクセスマップ」コンフィギュレーション モードで実行します。Cisco IOS の action は CatOS には存在しない CLI の概念ですが、ほぼ同様のキャプチャ、ログ、およびリダイレクト機能を提供します。これらのオプションの仕様については、ユーザ マニュアルを参照してください。次に、VACL の設定に関する CatOS と Cisco IOS の一般的な相違点を示します。

\*\*\*\*\* PACL は、PFC3a 以降を搭載した CatOS バージョン 8.3 以降が稼働する Sup 720 のみでサポートされています。

CatOS	Cisco IOS ソフトウェア
<pre>set vlan 10 set security acl ip sample permit ip any any commit security acl sample set security acl map sample 10</pre>	<pre>vlan 10 access-list 101 permit ip any any vlan access-map sample match ip address 101 action forward vlan filter sample vlan-list 10</pre>

**注:** IOS で VACL を作成すると、VLAN インターフェイスの SVI が自動的に作成されます。このインターフェイスが必要な場合、VACL を正常に動作させるために、インターフェイスを設定したり「UP」状態にしたりする必要はありません。

CatOS では、ACL を作成、変更、または削除すると、変更はメモリ内の編集バッファに一時的に保管されます。CatOS で ACL を有効にするには、ACL をコミットする必要があります。反対に Cisco IOS ソフトウェアでは、編集バッファは使用されません。IOS でポリシーを作成した場合には、VLAN またはインターフェイスにマッピングして ACL を有効にする必要があります。

#### VACL キャプチャ

VACL キャプチャは VACL の便利な拡張機能です。この機能は基本的に、指定されたフローと一致するパケットをキャプチャして、キャプチャ ポートから送信するポート ミラーリング機能です。VACL を作成すると、コピーを作成して分析(ネットワーク アナライザなどを使用)用の宛先ポートに送信するトラフィックを識別できます。この機能は、キャプチャされるトラフィックのパフォーマンスには影響しません。元のデータは目的どおりにデバイスを通過します。VACL キャプチャは、ネットワークのトラブルシューティングや分析に精度の高いツールとして機能するだけでなく、従来の Switched Port Analyzer (SPAN; スイッチド ポート アナライザ)に代わる拡張性の高い機能を実現します。

CatOS	Cisco IOS ソフトウェア
<pre>set vlan 10 set security acl ip cap_acl permit ip any any capture commit security acl cap_acl set security acl map cap_acl 10 set security acl capture-ports 1/1</pre>	<pre>vlan 10 access-list 101 permit ip any any vlan access-map cap_acl match ip address 101 action forward capture vlan filter sample vlan-list 10 int gigabitethernet 1/1 switchport capture</pre>

#### Port-Based Access Control List (PACL)

PACL (Sup720 および Sup32 上の CatOS のみでサポート)は、物理ポートにマッピングされるアクセス リストです。PACL には、ポート単位で設定可能な 3 つの動作モード(ポートベース、VLAN ベース、およびマージ モード)があります。ポートベース モードでは、PACL は既存の VACL および Cisco IOS ACL よりも優先されます。VLAN モードでは、VACL および IOS ACL が PACL よりも優先されます。マージ モードでは、入力側の PACL、VACL、および IOS ACL がマージされます (VLAN ベース モードはデフォルト モードです)。

PACL を設定する場合は、モードを指定する必要があります。次の例では、ポートベース モードでポート 2/1 に PACL を設定し、ポート 2/2 に ACL「pacl\_acl」をマッピングします。

CatOS
<pre>set port security-acl 2/1 port-based set security acl ip pacl_acl permit ip any any commit security acl pacl_acl set security acl map pacl_acl 2/2</pre>

## QoS

QoS という用語は、ネットワーク トラフィックの差別化と優先制御を行う各種機能を包括する概念です。これらの機能には、トラフィックの分類、マーキング、ポリシング、輻輳回避、およびスケジューリングなどがあります。Catalyst 6500 シリーズでは、QoS 機能は PFC(レイヤ 3 マーキング、ポリシング、および一部の分類機能に対応)とライン カード(輻輳回避、スケジューリング、および残りの分類機能に対応)で実行されます。CatOS の場合、PFC 非搭載のスーパーバイザでは、レイヤ 2 のみの QoS 分類とマーキングが実行できます。PFC と MSFC を搭載した Cisco IOS および Hybrid OS では、レイヤ 2/3/4 のすべての QoS 機能がサポートされます。

ここでは、QoS 機能の概要は省略し、次の設定例に関する CatOS と Cisco IOS ソフトウェアの違いについて説明します。

- インターフェイスの QoS 設定
- QoS ポリシーの設定

どちらの OS でも、QoS はデフォルトで無効になっています。Catalyst 6500 で QoS 機能を実行する場合は、最初に QoS をグローバルで有効に設定します。

CatOS	Cisco IOS ソフトウェア
set qos enable	Router(config)# mls qos

### インターフェイスの QoS 設定

#### 信頼状態

着信フレームの一部のフィールド(CoS、IP precedence、または DSCP など)を信頼(Trust)するようにポートを設定できます。次に、設定の例を示します。

CatOS	Cisco IOS ソフトウェア
set port qos 3/1 trust trust-cos	Router(config)# interface gigabitethernet 3/1 Router(config-if)# mls qos trust cos

CatOS および Cisco IOS は、IP フォンの音声トラフィックとワークステーションのデータ トラフィックを区別する拡張信頼機能をサポートしています。

#### デフォルトのポート CoS

スイッチには、特定のポートに着信するすべてのトラフィックに CoS 値を設定する機能が用意されています。この機能は、どちらの OS でもサポートされています。

CatOS	Cisco IOS ソフトウェア
set port qos 3/1 cos 3	Router(config)# interface gigabitethernet 3/1 Router(config-if)# mls qos cos 3

#### ポートベースおよび VLAN ベースの QoS モード

QoS ポリシーを適用できるのは、ポート単位または VLAN 単位のいずれかです。QoS はデフォルトではポート単位で機能します。この場合、QoS ポリシーはすべて特定のポートに適用されます。VLAN に適用されるポリシーは、ポートベースとして設定されているポートの入力トラフィックには影響しません。ポリシーを VLAN にマッピングする場合、VLAN ポリシーを適用する VLAN 内の各ポートでは、QoS が VLAN ベースであることをインターフェイスに通知する必要があります。目的のインターフェイスで次のコマンドを実行すると、デフォルト QoS がポートベースから VLAN ベースに変更されます。

CatOS	Cisco IOS ソフトウェア
set port qos 3/1 vlan-based	Router(config)# interface gigabitethernet 3/1 Router(config-if)# mls qos vlan-based

#### CoS/キュー マッピング

ここでは、標準受信キューおよび標準送信キューにおける CoS 値のキューまたはスレッシュホールドに対するマッピングについて説明します。Cisco IOS の場合、標準受信キューの設定では *rcv-queue* キーワードが使用され、ラウンドロビン送信キューでは *wrr-queue* キーワードが使用され、プライオリティキューでは *priority-queue* キーワードが使用されます。

CatOS の場合、CoS/キュー マッピングはキュー タイプごとに設定されます(つまり、すべての 1p2q2t ポートの設定が同じになります)。Cisco IOS の場合、CoS/キュー マッピングはインターフェイスごとに設定され、設定の変更は同一のポート ASIC で管理されるすべてのポートに反映されます(ASIC とポート間の配置はライン カードによって異なりますが、変更に関する警告は CLI によって出力されます)。次の例では、802.1p の値 5 を完全優先キュー(rx および tx)にマッピングし、802.1p の値 0 および 1 をロー プライオリティ キューの最初のスレッシュホールドにマッピングします。

CatOS	Cisco IOS ソフトウェア
set qos map 1p1q4t rx 2 1 cos 5 set qos map 1p2q2t tx 1 1 cos 0.1 set qos map 1p2q2t tx 3 1 cos 5	interface gigabitethernet 3/1 rcv-queue cos-map 2 1 5 wrr-queue cos-map 1 1 0 1 priority-queue cos-map 1 5

#### キュー サイズ

ポート単位のバッファ総量は固定されています。ただし、大半のイーサネット ポートでは、キュー単位のパケット バッファの割り当てを設定することが可能です。具体的には、従来型のファスト イーサネット、すべてのギガビット イーサネット、およびすべての 10 ギガビット イーサネットのラインカードで送信バッファの割り当てを変更できます。受信バッファの割り当ては、ファブリック対応のファスト イーサネット ポート(6548、6524 ライン カード)および 10 ギガビット イーサネット ポート(6501、6502 ライン カード)で設定できます。

CatOS	Cisco IOS ソフトウェア
set qos txq-ratio 1p2q2t 10 90 set qos rxq-ratio 1p1q0t 10 90	interface gigabitethernet 3/1 wrr-queue queue-limit 10 90 interface fastethernet 4/1 rcv-queue queue-limit 10 90

#### WRR スケジューリング

Weighted Round-Robin(WRR; 重み付けラウンドロビン)スケジューリングは、出力ポートから送信するトラフィックの優先制御を行います。優先制御は関係する各キューの相対的な重み付けに基づいて処理され、プライオリティの高いキューはプライオリティの低いキューよりも先に処理されます。WRR スケジューリング機能は、すべてのイーサネット ライン カードの送信キューでサポートされています。次の例は、ギガビット イーサネット ポートの場合を表しています。CoS/キュー マッピングと同様に、WRR スケジューリングは ASIC 単位で設定されます。

CatOS	Cisco IOS ソフトウェア
set qos wrr 1p2q2t 30 70	interface gigabitethernet 3/1 wrr-queue bandwidth 30 70

### QoS ポリシーの設定

QoS ポリシーの設定は、Cisco IOS ソフトウェアと CatOS では大きく異なっています。CatOS の場合、QoS ACL ステートメントは、マーキングとポリシングのすべての match パラメータと action パラメータを設定する場合に使用されます。Cisco IOS の QoS は、Modular QoS CLI (MQC; モジュラ QoS CLI) 構文を使用した分類、マーキング、およびポリシングをサポートしています。

Cisco IOS ポリシーはトラフィック クラス (*class-map* ステートメントを使用) を使用して、対象のトラフィックを識別します。これらのトラフィック クラスはさまざまなタイプのトラフィック フローに対して定義できます。たとえば IP トラフィック、IPX トラフィック、および MAC トラフィックに対して異なるクラスを設定できます。各トラフィック クラスは、IOS ベースの ACL またはクラスの match ステートメントを使用してトラフィックを識別します。*policy-map* (ポリシーマップ) には一致したトラフィックの処理方法 (マーキング、ポリシング、信頼など) が設定されます。ポリシーマップで定義されたポリシーは、**service-policy** コマンドを使用してインターフェイスにマッピングされます。

例については以下を参照してください。

### ACL による信頼

ポート上のすべてのトラフィックを信頼状態に設定する (上記を参照) には、もう一つの方法として、特定の QoS ACL と一致するトラフィックを信頼するように QoS ポリシーを作成することも可能です。この機能は CatOS および Cisco IOS ソフトウェアの両方で使用できます。次の例は、CatOS の QoS ACL 構文と Cisco IOS の MQC 構文 (上記を参照) の設定上の相違点を分かりやすく示しています。この例は、ギガビット イーサネット ポート 3/1 に着信するすべてのトラフィックに関して、ACL を使用して CoS を信頼する機能を比較しています。

CatOS	Cisco IOS ソフトウェア
<pre>set qos acl ip CatOS trust-cos any commit qos acl CatOS set qos acl map CatOS 3/1</pre>	<pre>access-list 101 permit ip any any policy-map IOS class IOS access-group 101 trust cos interface gigabitethernet 3/1 service-policy input IOS</pre>

CatOS ACL を作成、変更、または削除すると、変更はメモリ内の編集バッファに一時的に保管されます。CatOS で ACL を有効にするには、ACL をコミットする必要があります。Cisco IOS ソフトウェアでは、編集バッファは使用されません。IOS でポリシーを作成した場合は、ポートまたは VLAN にマッピングしてポリシーを有効にする必要があります。ポリシーを「UP」状態のインターフェイスにマッピングすると、ASIC ハードウェアに必要な情報が書き込まれ、該当するポリシーが有効になります。

### ポリサー

ポリシング機能は、主にトラフィックを設定された速度にレート制限する場合に使用します。トラフィックが設定された速度を超過した場合、トラフィックを廃棄するか、またはより低いプライオリティに変更することができます。この機能は、サービスレベル アグリーメントの遵守やセキュリティ保護を実現する場合に役立ちます。ポリサーは集約ポリサーまたはマイクロフロー ポリサーのどちらでも構いません。集約ポリサーは、クラスまたはクラス グループ内のすべてのトラフィックを 1 つの集約レートにレート制限します。マイクロフロー ポリサーは、トラフィック クラスの各フロー (一意の SA/DA MAC アドレス、SA/DA IP アドレス、TCP/UDP ポート番号、User-Based Rate Limiting [UBRL] を使用した一意の SA または DA) を個別のレートにレート制限します。シャーシ単位で設定できるマイクロフローの総数は 63、集約の総数は 1023 です (OS には依存しません)。

CatOS の場合、最初にポリシング パラメータ(rate、burst、および関連するアクションなど)をポリサー ステートメントで定義します。ポリシングされるトラフィックを識別し、該当するポリサーを参照する QoS ACL を設定します。その後、通常の ACL の設定と同様に、QoS ACL をコミットしてポートまたは VLAN に適用する必要があります。

Cisco IOS ソフトウェアの場合、最初に ACL を定義します。ポリシング パラメータは、2 種類のコンフィギュレーション モードのうちいずれかを使用して定義します。これは実行するポリサーのタイプによって異なります(詳細はあとの項を参照)。

**集約ポリサー**

Catalyst ソフトウェアで定義できる集約ポリサーは、共有集約ポリサーとインターフェイス別集約ポリサーの 2 種類です。

共有集約ポリサー(名前付き集約ポリサーともいう)は、インターフェイスまたは VLAN のグループに適用されて、すべてのインターフェイスまたはクラスのトラフィックを累積方式でポリシングします。共有集約ポリサーは、4 つの異なるインターフェイスの組み合わせに 100 Mbps のレート制限を適用する場合などに使用されます。このポリサーは、CatOS および Cisco IOS ソフトウェアの両方でサポートされています。次の例は、両者の設定を比較したものです。

CatOS	Cisco IOS ソフトウェア
<pre>set qos policer aggregate ag1 rate 1000000 burst 32 drop set qos acl ip ag_acl trust-dscp aggregate ag1 any set qos acl map ag_acl 3/5</pre>	<pre>access-list 101 permit ip any any mls qos aggregate-policer ag1 10000000 4625 conform-action transmit exceed- action drop policy-map limit-named class class-ag1 access-group 101 police aggregate ag1 interface fastethernet 3/5 service-policy input limit-named</pre>

**注:** CatOS の場合、レートは Kbps 単位で、バーストは Kb 単位です。Cisco IOS ソフトウェアの場合、レートは bps 単位で、バーストはバイト単位です。この違いはすべてのポリサー タイプに適用されます。

インターフェイス別集約ポリサーは、インターフェイスおよびトラフィック クラスに個々に適用されます。このポリサーは複数のインターフェイスに適用できますが、各インターフェイスのポリシングは個別に実行されます。インターフェイス別集約ポリサーは、4 つの異なるインターフェイスにそれぞれ 100 Mbps のレート制限を適用する場合などに使用されます。これらのポリサーは、Cisco IOS ソフトウェアでのみサポートされています。\*\*\*\*\*

CatOS	Cisco IOS ソフトウェア
<p>Catalyst OS には該当するコマンドなし</p>	<pre>access-list 101 permit ip any any policy-map limit-interface class class-ag1 access-group 101 <b>police</b> 10000000 4625 conform-action transmit exceed-action drop interface fastethernet 3/5 service-policy input limit-interface</pre>

\*\*\*\*\* CatOS でも同様の機能を実現できますが、インターフェイスごとに固有のポリサーを設定する必要があります。Cisco IOS のインターフェイス別ポリサーでは、ポリサーの定義は一度だけですが、適用は個々に行う必要があります。

Supervisor Engine 2 および 720 で稼働する Cisco IOS ソフトウェアは、分散フォワーディング システム (1 つまたは複数の Distributed Forwarding Card [DFC] が搭載されたシステム) でのポート単位のポリシングをサポートしています。分散システムでは、VLAN 単位の集約ポリシングはサポートされていません。

#### マイクロフロー ポリサー

Cisco IOS ソフトウェアの場合、マイクロフロー ポリサーの有効化はスイッチ上でグローバルに実行する必要があります。この操作は CatOS では必要ありません。**police flow** コマンドを使用すると、Cisco IOS ソフトウェアのマイクロフロー ポリシングの設定が表示されます。残りの設定は、Cisco IOS ソフトウェアにおけるインターフェイス別集約ポリサーの設定と同様です。

CatOS	Cisco IOS ソフトウェア
<pre>set qos policer microflow mfl rate 1000000 burst 32 drop set qos acl ip mf_acl trust-dscp microflow mfl any commit qos acl mf_acl set qos acl map mf_acl 3/5</pre>	<pre>mls qos flow-policing access-list 101 permit ip any any Policy-map limit-flow class limit-flow access-group 101 <b>police flow 200 15 confirm-action</b> <b>transmit exceed-action drop</b> interface fastethernet 3/5 service-policy input limit-flow</pre>

#### UBRL (Cisco IOS が稼働する Sup 32 および Sup 720 専用)

User-Based Rate Limiting (UBRL) 機能は、Supervisor Engine 32 および Supervisor Engine 720 のみでサポートされています。UBRL は、多数の送信元 IP アドレスまたは宛先 IP アドレスを、個々のレートに制限するマイクロフロー ポリシング機能です。UBRL を設定すると、2 つの ACL を使用するだけで、数多くのユーザをサポートできます。UBRL がサポートされているのは Cisco IOS だけです。次の例では、ユーザグループ内の各ユーザの (サブネット 192.168.0.0/16 宛) トラフィックを、それぞれ 1 Mbps にレート制限する UBRL を示しています。

CatOS	Cisco IOS ソフトウェア
非サポート	<pre>Access-list 101 permit ip any 192.168.0.0 0.0.255.255 Class-map 1Mbps-rate Match access-group 101 Policy-map Outbound Class 1Mbps-rate Police <b>flow mask src-only</b> 1000000 ... Int gig 3/1 Service-policy input Outbound</pre>

#### ACL によるマーキング

ACL と一致する特定のトラフィック クラスに対して、フレーム内のプライオリティ フィールド (CoS、DSCP、または ToS) を設定することができます。この方法を使用すると、ユーザはデフォルトのポート CoS 値によるマーキングよりも詳細で多様な設定が可能になります。

PFC QoS (IOS Release 12.1(12c)E1) で、信頼できないトラフィックのポリシー マップ クラス マーキングを行うには、**set ip dscp** および **set ip precedence** ポリシー マップ クラス コマンドを使用します。

次の表は、各 OS の設定パラメータの違いを比較したものです。

CatOS	Cisco IOS ソフトウェア
<pre>set qos acl ip CatOS dscp 24 any commit qos acl CatOS set qos acl map CatOS 3/1</pre>	<pre>access-list 101 permit ip any any policy-map IOS class IOS access-group 101 set ip dscp 24 interface gigabitethernet 3/1 service-policy input IOS</pre>

### AutoQoS

AutoQoS (CatOS のみでサポート) は、音声ポートで推奨される AVVID の設定に必要な QoS の設定を簡素化するマクロです。このマクロは、次の 2 つのコンポーネントに分けられます。

- **グローバルな自動 QoS コマンド (set qos auto)** — インターフェイスに限定されない、スイッチ全体での QoS 関連設定を処理します。
- **ポート固有の自動 QoS コマンド (set port qos mod/port autoqos)** — 特定のポートが目的のトラフィック タイプを反映するように、すべての着信 QoS パラメータを設定します。

次の例では、AutoQoS を有効にして、すべての着信 CoS および DSCP マーキングを信頼するように設定します。最後の例では、ポート 3/1 に Cisco IP Phone の入力 QoS が設定されています。

CatOS
<pre>set qos autoqos set port qos 3/1 autoqos trust cos set port qos 3/1 autoqos trust dscp set port qos 3/1 autoqos voip ciscoipphone</pre>

**注:** AutoQoS マクロ コマンドの詳細については、次の URL (英語) を参照してください。

[http://www.cisco.com/en/US/partner/products/hw/switches/ps708/products\\_configuration\\_guide\\_chapter09186a0080121d11.html-22805](http://www.cisco.com/en/US/partner/products/hw/switches/ps708/products_configuration_guide_chapter09186a0080121d11.html-22805)

### SPAN

SPAN は、スイッチ上の物理インターフェイスおよび論理インターフェイスで発着信されるトラフィックをミラーリングするトラブルシューティング分析機能です。SPAN セッションとは、モニタ対象の一連の SPAN 送信元ポートまたは VLAN と、ミラーリングされたトラフィックが送信される SPAN 宛先ポートを関連付けたものです。SPAN 宛先ポートはどの VLAN にも属さず、スパンニングツリーにも加わりません。10M 100M 1G または 10G ポートは、SPAN 送信元または SPAN 宛先ポートとして設定できます (ファブリック対応および DFC 対応ライン カードを含む)。

CatOS と Cisco IOS ソフトウェアでは、SPAN の実装方式が異なります。CatOS は最大 2 つの入力専用 SPAN セッションまたは入力/出力 SPAN セッション、および 4 つの出力専用 SPAN セッションをサポートできます。Cisco IOS ソフトウェアは、送信元インターフェイスでの入出力トラフィックを含む 2 つの SPAN セッションをサポートします。異なる SPAN セッションに含まれる一連の送信元インターフェイスは、重複していても異なっても構いません。SPAN 送信元にはスイッチポートとルーテッド ポートの両方を設定できます。異なる SPAN セッションには、重複のない一連の異なる宛先インターフェイスを含める必要があります。

入力 SPAN (Rx) は、送信元ポートが受信したネットワークトラフィックを、宛先ポートで分析するためにコピーします。出力 SPAN (Tx) は、送信元ポートが送信したネットワークトラフィックをコピーします。設定オプション「both」は、送信元ポートが受信および送信するネットワークトラフィックを宛

先ポートにコピーします。Cisco IOS ソフトウェアでは、128 の出力ソースまたは「both」ソースと最大 128 の入力ポートを送信元ポートとしてモニタできます。\*\*\*\*\* 最大で 64 の SPAN 宛先インターフェイスがサポートされます。

\*\*\*\*\* IOS 12.2(18)SXE 以降

次の例では、ポート 5/1 ~ 2 を SPAN 送信元、ポート 5/3 を SPAN 宛先として設定します。

CatOS	Cisco IOS ソフトウェア
set span 5/1,5/2 5/3 rx create	monitor session 1 source int f5/1-2 rx monitor session 1 dest int f5/3

### Remote SPAN (RSPAN)

Remote SPAN (RSPAN) は、SPAN のほとんどの機能に加えて、ネットワーク内の複数のスイッチに分散された送信元ポートおよび宛先ポートに対するサポートも備えています。RSPAN のトラフィックは、ユーザが指定したその RSPAN セッション専用の RSPAN VLAN を使用して、関係するすべてのスイッチに伝送されます。

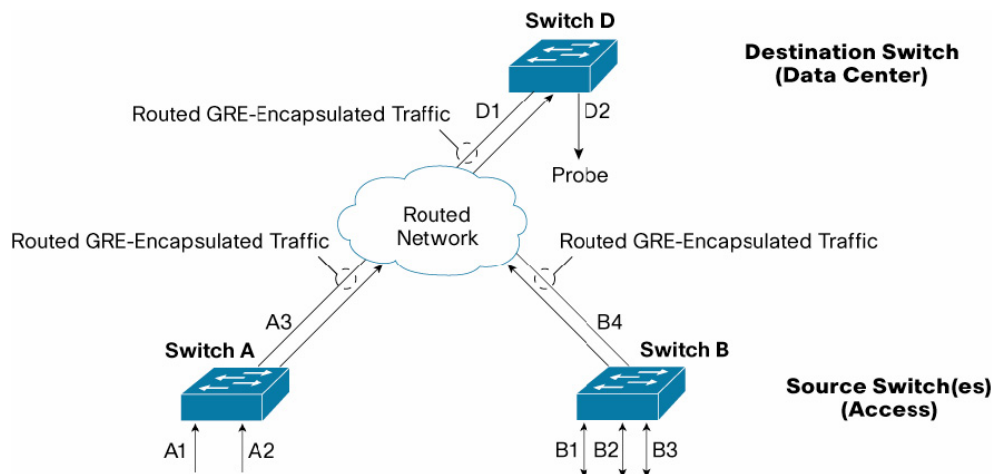
スイッチ単位で共存できる RSPAN セッションと SPAN セッションは最大 30 です。次の例では、VLAN 10 を RSPAN VLAN として、VLAN 5 を RSPAN 送信元ポートとして設定し、着信トラフィックと発信トラフィックの両方をモニタします。

CatOS	Cisco IOS ソフトウェア
Set vlan 10 rspan Set rspan source 5 10 both Set rspan destination 3/1 10 Show rspan	IOS(config)#vlan 10 IOS(config-vlan)#remote-span IOS(config)#monitor session 1 source vlan 5 both IOS(config)#monitor session 1 destination remote-vlan 10 IOS#sh monitor session 1

### カプセル化された Remote SPAN (ERSPAN)

12.2(18)SXE で導入された RSPAN により、Catalyst 6500 は Supervisor Engine 32 および Supervisor Engine 720 で GRE のハードウェア アクセラレーションを利用して、レイヤ 3 の境界を越えてネットワークをモニタリングできます。ERSPAN はリモート ネットワークのレイヤ 2 トラフィックをモニタし、すべてのレイヤ 2 ネットワークでネットワーク プローブの重複した要求を排除することでリソースを節約します。

図 6



ERSPAN と SPAN は、マルチキャスト フレームや Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) フレームなど、すべてのトラフィックをモニタできます。これらのフレームでは、RSPAN は BPDU モニタリングをサポートしていません。ERSPAN の設定例を次に示します。

CatOS	Cisco IOS ソフトウェア
該当なし	<pre>IOS(config)# monitor session 3 type erspan-source IOS(config-mon-erspan-src)# source interface gigabitethernet 4/1 IOS(config-mon-erspan-src)# destination IOS(config-mon-erspan-src-dst)# ip address 10.1.1.1 IOS(config-mon-erspan-src-dst)# origin ip address 10.10.1.1 IOS(config-mon-erspan-src-dst)# erspan-id 101</pre>

### ジャンボ フレーム

ジャンボ フレーム機能では、スイッチ上でデフォルト値よりも大きなイーサネット MTU サイズ (1500 バイト) が 1 つ使用できます。MTU は 1500 ~ 10240 バイトの間で設定でき、デフォルト (推奨) MTU は 9216 バイトです。ジャンボ フレームはハードウェアでスイッチングされるため、イーサネット、ファスト イーサネット、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 インターフェイスのパフォーマンスに影響を与えることはありません。これらのインターフェイスには、ルーテッド インターフェイス、アクセス スイッチ、トランク スイッチポート、または EtherChannel を使用できます (隣接デバイスによる制約に注意)。ジャンボ フレームは VLAN インターフェイス (SVI) でサポートされています。ただし、これが適用できるのはソフトウェアによってスイッチングされるトラフィックだけです。原則として (OS に関係なく)、ジャンボ フレームは特定の VLAN 内の全ポートで有効にするか、または全ポートで無効にします。

次の例は、CatOS と Cisco IOS ソフトウェアでのジャンボ フレームの設定を示しています。

CatOS	Cisco IOS ソフトウェア
<pre>Set port jumbo gil/1-2 enable Show port jumbo (to show)</pre>	<pre>int range gil/1-2 mtu 9216 show interface gil/1 (to show)</pre>

上記のコマンドを使用すると、ギガビット インターフェイス上で 9216 バイトの MTU が有効になります。この場合、IP MTU サイズも自動的に変更されます。ただし、反対に `ip mtu 9216` を使用して IP MTU を大きくしても、インターフェイスの MTU サイズは大きくなりません。

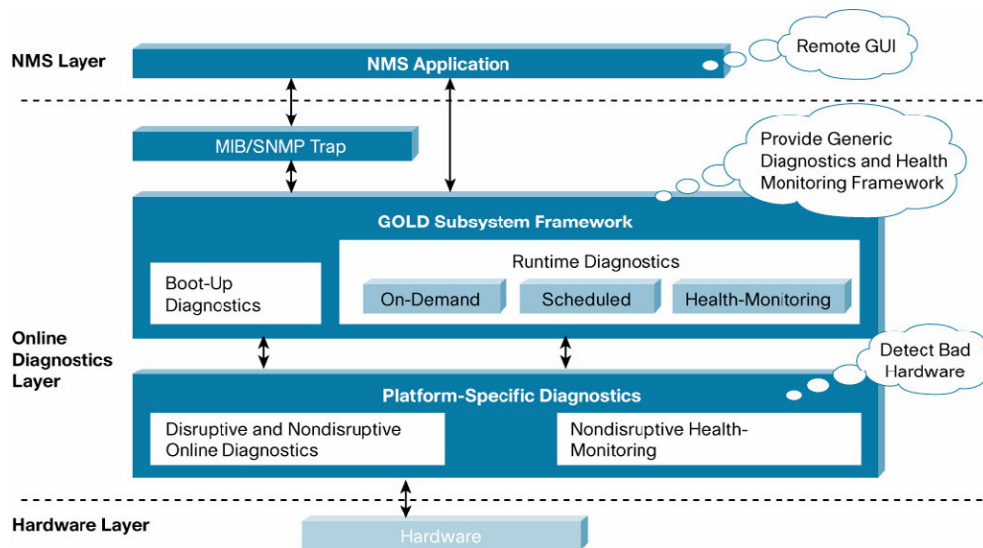
### ハイ アベイラビリティ

Catalyst 6500 のハイ アベイラビリティは、プラットフォームの主要な差別化要因の 1 つで、障害を解消し、最高の稼働率を実現します。Non Stop Forwarding (NSF) や Stateful Switchover (SSO) のような機能と Generic Online Diagnostics (GOLD) を組み合わせることで、Catalyst 6500 は、パケット処理とシステム間障害検出機能を併用して、優れた信頼性と稼働時間を実現します。

#### Generic Online Diagnostics (GOLD)

GOLD は、ハードウェア コンポーネントの状態を確認し、システム データとコントロール プレーンに適した動作を検証します。システムのブート時に有効になるテストもあれば、システムの動作中に有効になるテストもあります。図 7 に示すように、テストはブートアップ診断とランタイム診断の 2 つのカテゴリに分けられます。複数のテストを並行して実行することもできます。

図7 ブートアップ診断とランタイム診断



GOLD の詳細については、次の URL を参照してください。

- [http://www.cisco.com/jp/product/hs/switches/cat6500/prodlit/c6500gold\\_wp.shtml](http://www.cisco.com/jp/product/hs/switches/cat6500/prodlit/c6500gold_wp.shtml)
- <http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/diags.htm>

IOS と CatOS における GOLD 機能の実装の比較を次に示します。

CatOS	Cisco IOS ソフトウェア
<pre>set diagnostic bootup level ?   bypass          Bypass level   complete        Complete level   minimal         Minimal level</pre>	<pre>diagnostic bootup level ?   complete Complete level   minimal Minimal level</pre>
<pre>set diagnostic ondemand iterations 2</pre>	<pre>diagnostic ondemand iterations 2</pre>
<pre>set diagnostic ondemand action-on-failure stop</pre>	<pre>diagnostic ondemand action-on-failure stop</pre>
<pre>diagnostic start module 2 test 2</pre>	<pre>diagnostic start module 2 test 2</pre>
CatOS	Cisco IOS ソフトウェア
<pre>Console&gt; (enable) set diagnostic schedule module 2 test 1 weekly MON 03:00</pre>	<pre>Router(config)#diagnostic schedule module 2 test 1 weekly MON 03:00</pre>

## スーパーバイザの冗長性

Cisco IOS ソフトウェアと CatOS は、Catalyst 6500 シャーシ内でコンポーネントレベルの冗長性を実現する冗長スーパーバイザ エンジンの構成をサポートしています。ただし、Cisco IOS ソフトウェアと CatOS では、スーパーバイザ エンジンの冗長性を実現する動作モデルが異なります。

CatOS の場合、スーパーバイザの冗長性はハイ アベイラビリティ機能に基づいています。この機能を使用すると、スーパーバイザが二重化されたシステムで、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 エンジン間のプロトコル ステートを同期できます。アクティブ スーパーバイザに障害が発生すると、スタンバイ スーパーバイザは、スイッチ上で動作するプロトコルの正確な最新情報を使ってシステムの動作を引き継ぐことができます。これにより、スーパーバイザは 1 ~ 3 秒でフェールオーバーできるため、レイヤ 2、レイヤ 3、およびレイヤ 4 のプロトコルに関してネットワークを再コンバージェンスする必要はありません。ハイブリッド ソフトウェアでは、ルータ機能を担う MSFC エンジンに冗長構成にすることも可能です。ハイブリッド構成におけるハイ アベイラビリティの詳細については、[http://www.cisco.com/jp/product/hs/switches/cat6500/prodlit/c6500ha\\_wp.shtml](http://www.cisco.com/jp/product/hs/switches/cat6500/prodlit/c6500ha_wp.shtml) のホワイトペーパーを参照してください。

Catalyst 6500 の Cisco IOS ソフトウェアは、Route Processor Redundancy (RPR) (Enhanced High System Availability [EHSA] ともいう)、Route Processor Redundancy Plus (RPR+)、および Non Stop Forwarding with Stateful Switchover (NSF/SSO) をサポートしています。この動作モードでは、一方のスーパーバイザ/MSFC だけが動作して、もう一方はスタンバイ モードになります。アクティブおよびスタンバイ状態のスーパーバイザを確認するには、**show module** コマンドを使用します。障害を素早く検出するために、アクティブとスタンバイの間ではハートビート メッセージが交換されます。RPR および RPR+ 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 エンジン間でプロトコル ステートの同期は行いませんが、SSO はプロトコル ステートを同期します。次に、スーパーバイザの冗長性に関して、RPR、RPR+、および SSO で同等の特性を説明します。

Cisco IOS ソフトウェアの場合、スーパーバイザと MSFC はそれぞれ異なる機能とプロトコル(レイヤ 2 およびレイヤ 3)を処理します。ただしシステム上は、スーパーバイザと MSFC 両方のエンジンが正常に動作している必要があります。RPR/RPR+/SSO モードでスーパーバイザまたは MSFC どちらか一方に障害が発生すると、アクティブ スーパーバイザからスタンバイ スーパーバイザ/MSFC へのスイッチオーバーが行われます。CatOS の場合、一方の MSFC に障害が発生してもスーパーバイザは通常動作を継続できるため、スーパーバイザがスイッチオーバーする必要はありません。ただし、MSFC フェールオーバーのみが発生し、Catalyst OS が稼働するアクティブな PFC と Switch Processor (SP) がスロット 1 で完全に機能し、Route Processor (RP)/MSFC がスロット 2 で完全に機能するクロス モデルが許容される可能性があります。

スーパーバイザ/MSFC が冗長化されたハイブリッド システムでは、同一のシャーシ内に 2 つのアクティブ MSFC をオプションで搭載できます(デュアル ルータ モードという)。この構成では、2 つのアクティブ MSFC 間で Hot Standby Router Protocol (HSRP) が内部的に使用されます。Cisco IOS ソフトウェアでは、スタンバイ MSFC が完全に機能しないため、2 つの MSFC 間で HSRP を内部的に実行することができません。Cisco IOS ソフトウェアでは、RPR、RPR+、または NSF/SSO のどのモードを使用する場合でも、Cisco Catalyst 6500 からネットワーク内の他のルータへの外部 HSRP がサポートされています。

RPR または RPR+を使用するスーパーバイザ エンジン間のプロトコル冗長性はステートフルではありません。SSO 冗長性モードは、IOS のスーパーバイザ エンジン間でステートフルなプロトコル冗長性を提供しますが、Cisco Catalyst OS のハイ アベイラビリティ モードと同等の機能です。

次に、スーパーバイザの冗長性に関して、RPR、RPR+、および NSF/SSO の特性を説明します。

#### Route Processor Redundancy (RPR)

RPR を有効にすると、アクティブなスーパーバイザおよび MSFC が動作して、パケット フォワーディングと各種機能がすべて処理されます。スタンバイ スーパーバイザおよび MSFC はリセット状態ではありませんが、すべてのサブシステムが起動しているわけではありません。スタンバイ スーパーバイザはギガビット アップリンク ポートが動作するところまで起動しますが、スーパーバイザまたは MSFC 上でプロトコルは稼働していません。

アクティブ スーパーバイザに障害が発生すると、RPR がその機能停止を検出して、スイッチオーバーを実行します。ライン カードの電源のオフ/オン、スーパーバイザと MSFC の完全な起動、およびすべてのレイヤ 2/3 プロトコルの初期化が実行されます。EHSA でシステムがトラフィックのフォワーディングを開始するのに必要なフェールオーバー時間は約 90 秒です。実際のフェールオーバー時間は、構成の規模や複雑さによって異なります。

RPR では、アクティブ スーパーバイザとスタンバイ スーパーバイザ間で、スタートアップ コンフィギュレーションとブート変数の同期が行われます。

#### Route Processor Redundancy Plus (RPR+)

RPR+を有効にすると、アクティブなスーパーバイザおよび MSFC が動作して、パケット フォワーディングと各種機能がすべて処理されます。スタンバイ スーパーバイザと MSFC は完全に起動して、スタンバイ状態で動作します。RPR+ は RPR の拡張機能です。スタンバイ スーパーバイザが完全に起動しているため、RPR+では RPR よりも迅速なスーパーバイザのフェールオーバーが可能です。また、スーパーバイザのフェールオーバー時にライン カードの状態が維持されるため、フェールオーバー時間が短縮されます。ただし、ポートの状態は維持されないため、他のデバイスとの接続にフラッピングが発生します。

RPR+でシステムがトラフィックのフォワーディングを開始するのに必要なフェールオーバー時間は約 30 秒です。実際のフェールオーバー時間は、構成の規模や複雑さによって異なります。

#### Nonstop Forwarding with Stateful Switchover (NSF/SSO)

Cisco IOS ソフトウェアと CatOS の両方で NSF with SSO がサポートされています。主な差別化要因は、これらの機能が IOS に最初に導入されるときよりも高度な形式で適用される場所とその方法にあります。SSO は RPR+ 機能を拡張し、スーパーバイザ エンジンに障害が発生した場合にレイヤ 2 プロトコルの透過的なフェールオーバーを提供します。SSO はレイヤ 2 プロトコルに対してステートフルです。Policy Feature Card (PFC; ポリシー フィーチャ カード) および Distributed Forwarding Card (DFC) ハードウェア テーブルは、スイッチオーバーの前後で保持されます。これにより、レイヤ 2 とレイヤ 4 で透過的なフェールオーバーが可能になります。NSF は SSO と連携して、スイッチオーバー後のレイヤ 3 の整合性を保持します。アクティブなスーパーバイザの障害が発生したルータでは、既知のルートを使用してデータ パケットのフォワーディングを続行する一方で、ルーティング プロトコル情報が復旧および検証されます。このフォワーディングは、ピアリング アレンジメントをフェールオーバー時に復旧させるグレースフル リスタート メカニズムを利用することで続行されるため、不要なルート フラップやネットワークの不安定化を防ぐことができます。

NSF/SSO の場合、フェールオーバー時間は 0 ~ 3 秒です。NSF/SSO の詳細については、次の URL を参照してください。

[http://www.cisco.com/jp/product/hs/switches/cat6500/prodlit/nfwssc6500\\_ds.shtml](http://www.cisco.com/jp/product/hs/switches/cat6500/prodlit/nfwssc6500_ds.shtml)

### Hot Standby Router Protocol (HSRP)

Hot Standby Router Protocol (HSRP; ホットスタンバイ ルータ プロトコル) は、IP ネットワークにネットワーク冗長性を提供し、ネットワーク エッジ デバイスまたはアクセス回線で、ユーザ トラフィックが最初のホップ障害から迅速かつ透過的に復旧できるようにします。HSRP は、2 つ以上のシスコ ルーティング デバイス間で共有されるレイヤ 2 およびレイヤ 3 の仮想アドレスを提供して、ネットワークの耐障害性を確保します。選出アルゴリズムを使用して、静的に割り当てられた仮想 IP アドレスとレイヤ 2 MAC アドレスを組み合わせることで、障害からの透過的な復旧が可能になります。

[http://www.cisco.com/support/ja/index/Technologies/Hot\\_Standby\\_Router\\_Protoc\\_268435984.html](http://www.cisco.com/support/ja/index/Technologies/Hot_Standby_Router_Protoc_268435984.html)

### Virtual Router Redundancy Protocol (VRRP)

Virtual Router Redundancy Protocol (VRRP) は、シスコ独自の Hot Standby Router Protocol (HSRP) とよく似た機能を提供します。VRRP は、スタティックなデフォルト ルーティング環境に付きもののシングルポイント オブ フェイラーを解消するように設計されています。VRRP では、LAN 上のいずれかの VRRP ルータに、仮想ルータの役割をダイナミックに割り当てる選出プロトコルが定義されます。仮想ルータに割り当てられる IP アドレスを制御する VRRP ルータはマスターと呼ばれ、これらの IP アドレス宛に送信されるパケットのフォワーディングを行います。この選出プロセスでは、マスターが利用できなくなった場合、フォワーディングを行うデバイスのダイナミックなフェールオーバーが可能です。エンドホストは、LAN 上の仮想ルータの IP アドレスをデフォルトのファースト ホップ ルータとして使用できます。VRRP を使う利点は、すべてのエンドホストにダイナミック ルーティングやルータ ディスカバリ プロトコルを設定しなくても、デフォルト パスのアベイラビリティが向上することです。

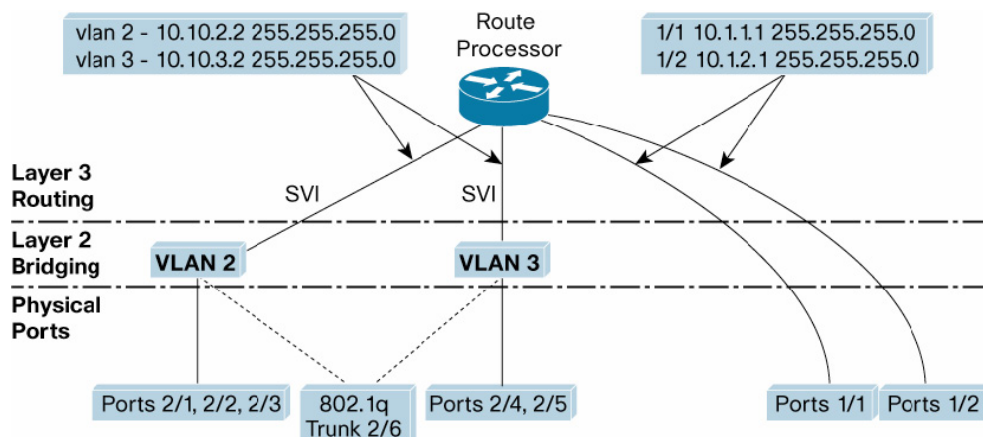
### Gateway Load Balancing Protocol (GLBP)

Gateway Load Balancing Protocol (GLBP) は、1 つの仮想 IP アドレスと複数の仮想 MAC アドレスを使用して、複数のゲートウェイ間での負荷分散を可能にします。このプロトコルは、HSRP や VRRP に似ています。GLBP を使用すると、冗長ルータ間でのパケットの負荷分散を実現できるだけでなく、障害の発生したルータや回線からデータトラフィックを保護できます。

### 付録 A: Cisco IOS ソフトウェアおよび CatOS の設定例の比較

ここでは、次のサンプル トポロジー (図 8) を使用して、完全な Cisco IOS モードの設定と CatOS の設定を比較します。

図 8 サンプル ネットワーク トポロジー による 設定 例



ステップ 1. スイッチおよびルータに名前を設定し、プロンプト、時刻、およびパスワードを設定します。

CatOS	Cisco IOS ソフトウェア
<pre>enable set system name cat6k-switch set enablepass set ip dns domain example.com set ip dns server a.b.c.d</pre>	<pre>Enable configure terminal hostname cat6k-switch enable password &lt;&gt; ip domain-name example.com ip name-server a.b.c.d end</pre>

ステップ 2. VTP をトランスパアレントに設定し、ステータスを確認します。

CatOS	Cisco IOS ソフトウェア
<pre>set vtp mode transparent show vtp domain</pre>	<pre>configure terminal vtp mode transparent end write memory show vtp status</pre>

ステップ 3. VLAN を作成し、ステータスを確認します。

CatOS	Cisco IOS ソフトウェア
<pre>set vlan 2 name Marketing set vlan 3 name Finance show vlan</pre>	<pre>configure terminal vlan 2 name Marketing vlan 3 name Finance end write memory show vlan</pre>

ステップ 4. ギガビット イーサネット アップリンクをルーテッド インターフェイスとして設定します。ギガビット イーサネット アップリンク 1/1 および 1/2 は、残りのネットワークと接続するために使用します。これらのポートはレイヤ 3 ルーティングの機能しか必要としないため、Cisco IOS ソフトウェアでは、以下のような単純なルーテッド インターフェイス コマンドを使用します。

CatOS	Cisco IOS ソフトウェア
<pre>Catalyst OS config: set vlan 89 1/1 set vlan 90 1/2 MSFC config: int vlan 89  ip address 10.1.1.1 255.255.255.0 no shut int vlan 90  ip address 10.1.2.1 255.255.255.0 no shut end write memory</pre>	<pre>configure terminal interface gigabitethernet 1/1 ip address 10.1.1.1 255.255.255.0 no shut interface gigabitethernet1/2 ip address 10.1.2.1 255.255.255.0 no shut end write memory</pre>

**注:** この例の VLAN 89 および 90 は無作為に選んだ値です。

ステップ 5. ポート 2/1 ~ 3 を VLAN 2 のクライアント接続用アクセス ポートとして使用するよう設定し、ポート 2/4 ~ 5 を VLAN 3、すべてのポートを速度 100 の全二重モードに設定します。

CatOS	Cisco IOS ソフトウェア
<pre>set vlan 2 2/1-3 set vlan 3 2/4-5 set port speed 2/1-5,100 set port duplex 2/1-5 full show port</pre>	<pre>Configure terminal interface range fastethernet 2/1-3 switchport switchport mode access switchport access vlan 2 speed 100 duplex full interface range fastethernet 2/4-5 switchport switchport mode access switchport access vlan 3 speed 100 duplex full end write memory show interface status</pre>

ステップ 6. トランク スイッチポートを設定します。3 つの VLAN は、すべてポート 2/6 を使って Catalyst B (レイヤ 2 Catalyst) に接続されます。トランクは IEEE 802.1Q のカプセル化を使用し、デフォルトで VLAN 1 になります。

CatOS	Cisco IOS ソフトウェア
<pre>set trunk 2/6 dot1q set trunk 2/6 desirable</pre>	<pre>interface fastethernet 2/6 switchport switchport mode dynamic desirable switchport trunk encapsulation dot1q</pre>

ステップ 7. **オプション設定**: Catalyst 6500 スイッチはデフォルトでトランク上のすべての VLAN を許可します。VLAN 50 ~ 100 のリストをトランクから削除します。

CatOS	Cisco IOS ソフトウェア
clear trunk 2/6 50-100	switchport trunk allowed vlan remove 50-100

ステップ 8. **ルーテッド SVI の設定**: ステップ 4 で、ギガビット イーサネット インターフェイスがルーテッド アップリンクとして設定されています。このステップでは、両方の VLAN にルーティング サービスを提供する 2 つの SVI インターフェイス (VLAN 間インターフェイス) を設定します。この設定では、VLAN 2 および VLAN 3 に HSRP を使用し、IPX ネットワーク番号も設定します。

CatOS	Cisco IOS ソフトウェア
<pre> Routing is done on MSFC: interface vlan2 ip address 10.10.2.2 255.255.255.0 standby 1 timers 1 3 standby 1 priority 200 preempt standby 1 ip 10.10.2.6 ipx network 20  interface vlan3 ip address 10.10.3.2 255.255.255.0 standby 1 timers 1 3 standby 1 priority 200 preempt standby 1 ip 10.10.3.6 ipx network 30                     </pre>	<p>論理的な SVI インターフェイスは MSFC の場合とまったく同じです。左記の設定をそのまま使用できます。</p>

## 付録 B: CatOS および Cisco IOS ソフトウェアのコマンド対応表

CatOS	Cisco IOS ソフトウェア
reset system	Reload
Session	Remote login
Set system name	Hostname
Set test diaglevel	Diagnostic level
Set boot config-register	Config-register
Set boot system flash	Boot system flash
Set module power down/up	Power enable module
Set port disable	Shutdown (interface mode)
set port duplex	Duplex
set port flowcontrol send [desired   off   on]	flowcontrol send [desired   off   on]
set port flowcontrol receive [desired   off   on]	flowcontrol receive [desired   off   on]
set port negotiation <mod/port> enable/disable	speed nonegotiate
set port speed	Speed
set cam	mac-address-table
Set port jumbo	Mtu 9216
set port channel	channel-group <group> mode (interface mode)
set trunk (default mode is auto)	switchport mode trunk (vlan database command)
set udld	Udld
set vlan <vlan id> port	1) switchport 2) switchport mode access 3) switchport access vlan <>
set vtp	Vtp
Set spanntree backbonefast	Spanning-tree backbonefast
Set spanntree enable/disable	Spanning-tree vlan
Set spanntree portfast	Spanning-tree portfast
set qos enable	mls qos
Set port dot1qtunnel	Switchport mode dot1qtunnel
show cam dynamic	show mac-address-table dynamic
show channel info or show port channel	show etherchannel summary
show mac	show interface counters
show port <slot/port>	show interface <type slot/port>
show mls cef	show mls cef
show port	show interface status
Show port capabilities	Show interface capabilities
show span	show monitor
show spanntree	show spanning-tree
show qos	show mls qos
show trace	show debugging
show trunk or show port trunk	show interfaces trunk
show udld	show udld
show vlan	show vlan

CatOS	Cisco IOS ソフトウェア
show vtp domain	show vtp status
clear cam	clear mac-address-table

### 付録 C: 変更手順

Cisco Catalyst 6000 シリーズ スイッチで、ハイブリッドからネイティブの IOS にソフトウェアを変更する手順については、次の URL を参照してください。

英語:

[http://www.cisco.com/en/US/partner/products/hw/switches/ps708/products\\_tech\\_note09186a008015bfa6.shtml](http://www.cisco.com/en/US/partner/products/hw/switches/ps708/products_tech_note09186a008015bfa6.shtml)

日本語 (自動翻訳): <http://www.cisco.com/support/ja/473/catos-ios-conversion-6500k.shtml>

Cisco Catalyst 6000 シリーズ スイッチで、ネイティブの IOS からハイブリッドにソフトウェアを変更する手順については、次の URL を参照してください。

英語:

[http://www.cisco.com/en/US/partner/products/hw/switches/ps700/products\\_tech\\_note09186a00801350b8.shtml](http://www.cisco.com/en/US/partner/products/hw/switches/ps700/products_tech_note09186a00801350b8.shtml)

日本語 (自動翻訳): <http://www.cisco.com/support/ja/473/ios-catos-convert-cat65k.shtml>

©2007 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。(0704R)

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。



**シスコシステムズ株式会社**

〒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)

<http://www.cisco.com/jp/go/contactcenter>

0120-092-255 (通話料無料)

電話受付時間：平日10:00～12:00、13:00～17:00

**お問い合わせ先**