



## 製品概要

---

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

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



(注)

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

[http://www.cisco.com/en/US/products/hw/switches/ps4324/prod\\_release\\_note09186a0080758ff3.html](http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_release_note09186a0080758ff3.html)

---

## レイヤ 2 ソフトウェアの機能

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

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

### 802.1Q およびレイヤ 2 プロトコル トンネリング

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

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

### CDP

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

CDP の設定手順については、[第 24 章「CDP の設定」](#)を参照してください。

## EtherChannel バンドル

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

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

## ジャンボ フレーム

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

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

## LLDP

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

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

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

## Multiple Spanning-Tree

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

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

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

## PVRST+

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

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

## QoS

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

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

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

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

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

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

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

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

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

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

## Resilient Ethernet Protocol

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

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

## STP

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

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

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

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

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

## Stateful Switchover

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

- ステートフル IGMP スヌーピング

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

- ステートフル DHCP スヌーピング

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

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

## SVI 自動ステート

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

## UBRL

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

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

## UDLD

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

UDLD については、[第 26 章「UDLD の設定」](#) を参照してください。

## 単一方向イーサネット

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

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

## VLAN

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

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

次の VLAN 関連の機能もサポートされます。

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



- プライベート VLAN — プライベート VLAN は、通常の VLAN の機能を持ち、スイッチ上の他のポートからレイヤ 2 をある程度分離させるポートセットです。  
プライベート VLAN については、第 36 章「PVLAN の設定」を参照してください。
- プライベート VLAN トランク ポート — プライベート VLAN トランク ポートを使用すると、プライベート VLAN 上のセカンダリ ポートが複数のセカンダリ VLAN を実行します。
- プライベート VLAN 混合モード トランク ポート — プライベート VLAN 混合モード トランクを使用すると、混合モード ポートを 802.1Q トランク ポートに拡大し、複数のプライマリ VLAN (したがって、複数のサブネット) を伝送します。プライベート VLAN 混合モード トランクは一般的に、別のプライマリ VLAN 上で異なるサービスまたはコンテンツを独立サブスクライバに提供するために使用します。セカンダリ VLAN は、プライベート VLAN 混合モード トランク上で伝送できません。
- ダイナミック VLAN メンバシップ — ダイナミック VLAN メンバシップの、ポートに接続されたデバイスの送信元 MAC に基づいて、VLAN にスイッチ ポートを動的に割り当てることができます。ネットワーク内にあるスイッチの 1 つのポートからネットワーク内にある別のスイッチのポートにホストを移動する場合、そのスイッチはそのホストに適切な VLAN を新しいポートへ動的に割り当てます。VLAN Management Policy Server (VMPS; VLAN マネジメント ポリシー サーバ) クライアント機能を使用すると、ダイナミック アクセス ポートを VMPS クライアントに変換できます。VMPS クライアントは VQP クエリーを使用して VMPS サーバと通信し、ポートに接続するホストの MAC アドレスに基づいてポートに VLAN を割り当てられます。

## レイヤ 3 ソフトウェアの機能

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

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

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

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

### CEF

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

CEF の設定手順については、第 28 章「CEF の設定」を参照してください。

### HSRP

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

HSRP の設定については、次の URL を参照してください。

[http://www.cisco.com/en/US/products/ps6350/products\\_configuration\\_guide\\_chapter09186a008042fbb3.html](http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a008042fbb3.html)

### SSO 認識 HSRP

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



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

## IP ルーティング プロトコル

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

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

## BGP

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

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

## BGP ルートマップの継続

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

## EIGRP

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

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



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



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

## GLBP

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

GLBP の詳細については、次の URL を参照してください。

[http://www.cisco.com/en/US/products/ps6350/products\\_configuration\\_guide\\_chapter09186a008042fb97.html](http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a008042fb97.html)

## IGRP

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

## IS-IS

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

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

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

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

## OSPF

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

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

## RIP

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

## VRRP

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

## マルチキャスト サービス

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

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

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

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

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

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

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

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

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

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

PIM-SSM マッピングの詳細については、次の URL を参照してください。

[http://www.cisco.com/en/US/docs/ios/12\\_3t/12\\_3t2/feature/guide/gtssmma.html#wp1171997](http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gtssmma.html#wp1171997)

## NSF/SSO

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

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

## ISSU

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

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

## PBR

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

PBR の詳細については、第 32 章「PBR の設定」を参照してください。

## UDLR

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

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

## VRF-Lite

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

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



## 管理機能

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

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

### Cisco Network Assistant および組み込み CiscoView

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

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

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

### DHCP

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

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

DHCP サーバの設定の詳細については、次の URL を参照してください。

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

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

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

## 強制 10/100 自動ネゴシエーション

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

## インテリジェントな電源管理

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

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

## MAC アドレス通知

MAC アドレス通知機能により、Catalyst 4500 シリーズ スイッチによって学習され、エージングアウトし、スイッチから削除された MAC アドレスが監視されます。通知は CISCO-MAC-NOTIFICATION MIB 経由で送信または取得されます。これは一般的に、ホストが移動するたびに MAC アドレス通知イベントを収集する中央ネットワーク管理アプリケーションによって使用されます。潜在的な DoS 攻撃 (サービス拒絶攻撃) または man-in-the-middle 攻撃を通知するよう、ユーザ設定可能な MAC テーブル利用率しきい値を定義できます。

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

## MAC 通知 MIB

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

## NetFlow 統計情報

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

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

## SSH

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

## SNMP

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

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

SNMP の詳細については、第 47 章「SNMP の設定」を参照してください。

## SPAN および RSPAN

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

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

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

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

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

## VRRP

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

VRRP の詳細については、次の URL を参照してください。

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hiap\\_c/ch20/haipvrrp.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hiap_c/ch20/haipvrrp.htm)

## WCCP

Web Content Communication Protocol (WCCP) バージョン 2 レイヤ 2 (L2) リダイレクションにより、Catalyst 4500 シリーズ スイッチはレイヤ 2/MAC アドレス書き換えを使用して、コンテンツ要求を直接接続されたコンテンツ エンジンに透過的にリダイレクトします。WCCPv2 L2 リダイレクションはスイッチング ハードウェアで高速化されるので、Generic Routing Encapsulation (GRE; 総称ルーティング カプセル化) を使用したレイヤ 3 (L3) リダイレクションよりも効率的です。キャッシュ クラスタのコンテンツ エンジンは、頻繁にアクセスされるコンテンツを透過的に保存し、同じコンテンツに関する連続した要求に応じます。この結果、オリジナルのコンテンツ サーバから同一コンテンツを繰り返し伝送する必要がなくなります。これはポートまたはダイナミック サービスのある HTTP および非 HTTP トラフィックの透過的なリダイレクションをサポートします (Web キャッシング、HTTPS キャッシング、FTP [ファイル転送プロトコル] キャッシング、プロキシ キャッシング、メディア キャッシング、およびストリーミング サービスなど)。WCCPv2 L2 リダイレクションは一般的に、地域サイトまたは支店などのネットワーク エッジで透過的なキャッシングを可能にします。WCCPv2 L2 リダイレクションは、PBR または VRF-Lite が設定された同じ入力 インターフェイスでイネーブルにできません。L2 リダイレクションのための ACL ベースの分類はサポートされません。

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

## セキュリティ機能

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

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

### 802.1X ID ベースのネットワーク セキュリティ

このセキュリティ機能の内容は、次のとおりです。

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

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

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

## DAI

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

DAI の詳細については、第 41 章「DAI の設定」を参照してください。

## DHCP スヌーピング

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

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

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

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ip\\_c/ipcprt1/1cddhcp.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ip_c/ipcprt1/1cddhcp.htm)

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

## フラッディング ブロック

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

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



## ハードウェアベースのコントロールプレーンポリシング

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

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

## スタティックホストのためのIPSG

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

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

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

## IPSG

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

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

## ローカル認証、RADIUS、および TACACS+ 認証

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

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/secur\\_c/scprtl/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/secur_c/scprtl/index.htm)

## NAC

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

- NAC レイヤ 2 IP 検証

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

レイヤ 2 IP 検証の詳細については、次の URL を参照してください。

[http://www.cisco.com/en/US/products/hw/switches/ps4324/prod\\_configuration\\_guide09186a00805764fd.html](http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_configuration_guide09186a00805764fd.html)

- NAC レイヤ 2 802.1X 認証

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

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

## ACL によるネットワーク セキュリティ

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

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

次のセキュリティ機能がサポートされています。

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

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

## ポート セキュリティ

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

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

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

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

## ストーム制御

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

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

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

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

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

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

## ユーティリティ

### レイヤ 2 traceroute

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

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

### TDR

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

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

### デバッグ機能

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

- **platform**
- **debug platform**

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

## Metro の機能

### Resilient Ethernet Protocol

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

詳細については、次の URL を参照してください。

[http://www.cisco.com/en/US/products/hw/switches/ps5532/products\\_configuration\\_guide\\_chapter09186a0080878947.html](http://www.cisco.com/en/US/products/hw/switches/ps5532/products_configuration_guide_chapter09186a0080878947.html)

