CHAPTER 1

製品概要

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

（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_notes_list.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 トンネリング、VLAN マッピング、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 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。

サービス プロバイダー VLAN にカスタマー VLAN をマッピングするには、カスタマー ネットワークに接続されたトランク ポート上で VLAN マッピング（または VLAN ID トランスレーション）を設定できます。ポートに入るパケットは、パケットのポート番号と元のカスタマー VLAN-ID（C-VLAN）に基づいて、サービス プロバイダーの VLAN（S-VLAN）にマッピングされます。

802.1Q トンネリングおよび VLAN マッピングの設定については、第 28 章「802.1Q トンネリング、VLAN マッピング、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。

Cisco IOS Auto SmartPort マクロ

Cisco IOS Auto SmartPort マクロは、ポートで検出されたデバイス タイプに基づいてポートを動的に設定します。スイッチは、ポート上で新しいデバイスを検出すると、適切な Cisco IOS Auto SmartPort マクロを適用します。ポート上でリンク ダウン イベントが発生した場合、スイッチはそのマクロを削除します。たとえば、ポートに Cisco IP Phone を接続した場合は、Cisco IOS Auto SmartPorts により

自動的に IP Phone マクロが適用されます。IP Phone マクロが適用されると、遅延に影響されやすい音声トラフィックを正しく処理できるように QoS（Quality Of Service）、セキュリティ機能、および専用の音声 VLAN がイネーブルになります。

SmartPort マクロの設定については、第 20 章「Cisco IOS Auto SmartPort マクロの設定」を参照してください。

Cisco Discovery Protocol

Cisco Discovery Protocol（CDP）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、Cisco スイッチとルータは MAC 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 はデータリンク層上でのみ実行され、異なるネットワーク層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、簡易ネットワーク管理プロトコル（SNMP）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 29 章「CDP の設定」を参照してください。

Cisco Group Management Protocol（CGMP）サーバ

CGMP サーバはマルチキャスト 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だけに転送されます。

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 25 章「EtherChannel およびリンク ステート トラッキングの設定」を参照してください。

イーサネット CFM

イーサネット CFM は、サービスインスタンスごと（VLAN ごと）のエンドツーエンド イーサネット レイヤ OAM プロトコルで、予防的な接続の監視、障害検証、および障害切り離しの機能を備えています。エンドツーエンドには、プロバイダー エッジ間（PE-to-PE）デバイス、またはカスタマー エッジ間（CE-to-CE）デバイスを含みます。イーサネット CFM は、IEEE 802.1ag で仕様が定められており、イーサネット ネットワークのレイヤ 2 ping、レイヤ 2 traceroute、およびエンドツーエンド接続チェックの標準です。

CFM の詳細については、第 64 章「イーサネット OAM と CFM の設定」を参照してください。

イーサネット OAM プロトコル

イーサネット Operation, Administration, and Maintenance（OAM; 運用管理および保守）は、イーサネット インフラストラクチャ全体のコンテキスト内の管理機能を向上するために、イーサネット ネットワークの設置、監視、およびトラブルシューティングを行うためのプロトコルです。イーサネット OAM は、ネットワークまたはネットワークの一部（特定のインターフェイス）の全二重ポイントツーポイント イーサネット リンクまたは疑似ポイントツーポイント イーサネット リンク上に実装できます。

OAM の詳細については、第 64 章「イーサネット OAM と CFM の設定」を参照してください。

Flex Link および MAC アドレス テーブル移動更新

Flex Link は、レイヤ 2 インターフェイス（スイッチ ポートまたはポート チャネル）のペアで、一方のインターフェイスが他方のインターフェイスのバックアップとして機能するように設定されています。この機能は、Spanning Tree Protocol（STP; スパニングツリー プロトコル）の代替ソリューションです。Flex Link は、通常、お客様がスイッチで STP を実行しない場合のサービス プロバイダーまたは企業ネットワークに設定されます。

MAC アドレス テーブル移動更新により、プライマリ（転送）リンクがダウンしてスタンバイ リンクがトラフィックの転送を開始したときに、スイッチは高速双方向コンバージェンスを提供できます。

Flex Link および MAC アドレス テーブル移動更新の詳細については、第 22 章「Flex Link および MAC アドレス テーブル移動更新機能の設定」を参照してください。

Flexible NetFlow（Supervisor Engine 7-E および 7L-E のみ）

フローは、パケット フィールドを含む場合があるキー フィールド属性、パケット ルーティング属性、および入出力インターフェイス情報の一意のセットとして定義されます。NetFlow 機能は、フローを、機能キー フィールドの値が同じ一連のパケットとして定義します。Flexible NetFlow（FNF）を使用すれば、さまざまなフロー属性が指定されたフロー レコードを収集し、オプションで転送もできます。NetFlow 収集は、IP、IPv6、およびレイヤ 2 トラフィックをサポートします。

Flexible NetFlow の設定については、第 63 章「Flexible NetFlow の設定」を参照してください。

インターネット グループ管理プロトコル（IGMP）スヌーピング

IGMP スヌーピングは、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、マルチキャスト トラフィックを要求するホストが接続されたポートにのみ転送されます。

IGMPv3 のサポートによって、IGMPv3 ホストまたはルータが存在する場合に、マルチキャスト トラフィック フラッディングが抑制されます。IGMPv3 スヌーピングは、IGMPv3 クエリーおよびメンバーシップ レポート メッセージをリッスンして、ホストとマルチキャスト グループの関連付けを維持します。また、スイッチからマルチキャスト データをそれが必要なポートにだけ伝播させることができます。IGMPv3 スヌーピングは、IGMPv1 および IGMPv2 と完全な相互運用性があります。

明示的ホスト トラッキング（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ーシップ情報の追跡、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 クエリアは、VLAN で IGMP スヌーピングをサポートするために必要なレイヤ 2 機能です。VLAN では、マルチキャスト トラフィックでルーティングが必要ではないため、PIM および IGMP は設定されていません。

SSO をサポートするステートフル IGMP スヌーピングは、スイッチオーバーが発生したときに、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 メンバーシップを認識するように、アクティブ スーパーバイザ エンジンによって学習された IGMP 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が軽減されます。

IGMP スヌーピングの設定手順については、第 26 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 マルチキャスト BSR および BSR スコープ ゾーンのサポート

PIM-SM 対応のブートストラップ ルータ（BSR）プロトコルは、グループと RP のマッピング情報をドメイン全体に迅速に配布するためのダイナミック適応メカニズムを備えています。IPv6 BSR 機能を使用すると、到達不能になった RP が検出され、マッピング テーブルが変更されます。これにより、到達不能な RP が今後使用されなくなり、新しいテーブルがドメイン全体に迅速に配布されるようになります。

BSR では、管理用スコープのマルチキャストを使用してネットワークでグループと RP のマッピングを配布することによって、限定スコープ ゾーンをサポートしています。ユーザは、ドメイン内の管理用スコープ領域ごとに候補 BSR と一連の候補 RP を設定できます。

BSR および BSR スコープ ゾーンのサポートについては、Catalyst 4500 シリーズ スイッチでのサポートに関する次の警告がある次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_pim/configuration/15-0sy/ip6-mcast-bsr.html

- 「IPv6 BSR: Scoped Zone Support」セクションでは、ある段落が次のように始まります。

  C-RP にスコープが設定されていない場合、その C-RP は、スコープ ゾーンのグループ範囲を含む、スコープ ゾーンの選択された BSR から BSM を受信することによって、管理用スコープ ゾーンの有無およびそのグループ範囲を検出します。

  C-RP にスコープはもう設定できません。そのため、文は次のように読むべきです。

  C-RP は、スコープ ゾーンのグループ範囲を含む、スコープ ゾーンの選択された BSR から BSM を受信することによって、管理用スコープ ゾーンの有無およびそのグループ範囲を検出します。

- 「Configuring a BSR and Verifying BSR Information」セクションの「Summary Steps」および「Detailed Steps」のステップ 3 において、C-BSR を設定するコマンドは、次のようにリストされています。

  ipv6 pim [**vrf** *vrf-name*] **bsr candidate bsr** *ipv6-address* [*hash-mask-length*] [**priority** *priority-value*]

  scope scope-value および「新しい」オプション（**accept-rp-candidate** *access-list-name*）は、元の構文が誤って除外したため、このリリースでサポートされます。

  ipv6 pim [**vrf** *vrf-name*] **bsr candidate bsr** *ipv6-address* [*hash-mask-length*] [**priority** *priority-value*] [**scope** *scope-value*] [**accept-rp-candidate** *access-list-name*]

- 「Sending PIM RP Advertisements to the BSR」セクションの「Summary Steps」および「Detailed Steps」のステップ 3 において、キーワード **scope** *scope-value* は削除すべきです。**scope** キーワードは C-RP 用にもう存在しません。

- 「Configuring BSR for Use Within Scoped Zones」セクションに、複数の変更が適用されます。

次の段落は、

候補 RP でスコープが指定されている場合、このデバイスは指定されたスコープの BSR に自身を C-RP 専用としてアドバタイズします。スコープとともにグループ リストが指定されている場合は、そのグループ リストと同じスコープが指定されたアクセス リスト内のプレフィックスだけがアドバタイズされます。

次のように読むべきです。

候補 RP は、それが処理するさまざまな範囲を、それぞれの選定された BSR にアドバタイズします。グループ リストが指定されている場合は、グループ リストのプレフィックスごとに、選定されたスコープ BSR がプレフィックスのスコープにあることを確認します。見つからない場合、プレフィックスは選定された非スコープ BSR が存在すればそこに通知されます。

注：プレフィックスはスコープ固有でない場合（たとえば、FF00::/8）、非スコープ BSR だけに通知されます。候補 RP はグループ リストが設定されていない場合、プレフィックス FF00::/8 だけを持つグループ リストが設定されているかのように動作します。

「Summary Steps」で、ステップ 3 と 4 は次のように読むべきです。

ipv6 pim [**vrf** *vrf-name*] **bsr candidate bsr** *ipv6-address* [*hash-mask-length*] [**priority** *priority-value*] [**scope** *scope-value*] [**accept-rp-candidate** *access-list-name*]

ipv6 pim [**vrf** *vrf-name*] **bsr candidate rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**interval** *seconds*] [**bidir**]

「Details Steps」で、ステップ 3 は次のように読むべきです。

ipv6 pim [**vrf** *vrf-name*] **bsr candidate bsr** *ipv6-address* [*hash-mask-length*] [**priority** *priority-value*] [**scope** *scope-value*] [**accept-rp-candidate** *access-list-name*]

例：

```
Device(config)# ipv6 pim bsr candidate bsr 2001:DB8:1:1:4 scope 6
```

「Details Steps」で、ステップ 4 は次のように読むべきです。

ipv6 pim [**vrf** *vrf-name*] **bsr candidate rp** *ipv6-address* [**group-list** ***access-list-name***] [**priority** *priority-value*] [**interval** *seconds*] [**bidir**]

例：

```
Device(config)# ipv6 pim bsr candidate rp 2001:DB8:1:1:1 group-list list
```

- 「Configuring BSR Devices to Announce Scope-to-RP Mappings」セクションで、キーワード **scope** *scope-value* は「Summary Steps」および「Detail Steps」両方のステップ 3 から削除すべきです。
- 「Additional References」セクションで、FC 5059 を参照すると役立ちます。

IPv6 Multicast Listen Discovery（MLD）と Multicast Listen Discovery 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、および隣接ノードの対象となるマルチキャスト パケットを検出します。MLD スヌーピングは、MLD v1 と MLD v2 の 2 種類のバージョンでサポートされます。ネットワーク スイッチでは、MLD スヌーピングを使用してマルチキャスト トラフィックのフラッディングを抑制し、IPv6 マルチ キャスト データを VLAN 内のすべてのポートにフラッディングされるのではなくデータを受信するポートのリストに転送します。これにより、ネットワーク デバイスの負荷を軽減し、リンクで不要な帯域幅を最小化し、IPv6 マルチ キャスト データを効率的に配信できます。

マルチキャスト サービスの設定方法については、第 36 章「IP マルチキャストの設定」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 イーサネット 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 フレーム機能はポート単位でレイヤ 2 およびレイヤ 3 インターフェイスで設定できます。この機能は、次のハードウェアでだけサポートされます。

- WS-X4306-GB：すべてのポート
- WS-X4232-GB-RJ：ポート 1 と 2
- WS-X4418-GB：ポート 1 と 2
- WS-X4412-2GB-TX：ポート 13 と 14
- WS-4648-RJ45V-E
- WS-X4648+RJ45V+E
- WS-X4706-10GE ラインカード
- スーパーバイザ エンジン アップリンク ポート

ジャンボ フレームについては、第 8 章「インターフェイスの設定」を参照してください。

Link Aggregation Control Protocol

LACP では、LAN ポート間で LACP パケットを交換することによって、EtherChannel の自動作成をサポートしています。LACP パケットが交換されるのは、passive および active モードのポート間に限られます。このプロトコルは、LAN ポート グループの機能を動的に「学習」して、他の LAN ポートに通知します。正確に一致するイーサネット リンクを特定すると、それらを 1 つの EtherChannel にグループ分けします。その後で、その EtherChannel が単一のブリッジ ポートとしてスパニングツリーに追加されます。

Cisco IOS XE 3.1.0SG における Cisco IOS XE IP Application Services 機能

ここでは、Cisco IOS XE 3.1.0SG でサポートされている IP Application Services ソフトウェア機能について説明します。機能マニュアルへのリンクが掲載されています。

機能ガイドには、複数の機能に関する情報が含まれている場合があります。機能ガイドで特定の機能に関する情報を検索する場合は、巻末の機能情報表を参照してください。

機能ガイドには、さまざまなソフトウェア リリースとプラットフォームでサポートされている機能が掲載されています。ご使用のシスコ ソフトウェア リリースまたはプラットフォームで、機能ガイドに記載されたすべての機能がサポートされているとは限りません。そのガイドでどの機能がソフトウェア リリースでサポートされるかについては、機能ガイドの最後にある機能情報の表を参照してください。プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは不要です。

IEEE 802.3ad Link Aggregation Control Protocol（LACP）

http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_lnkbndl.html

ギガビット インターフェイス用の LACP（802.3ad）

http://www.cisco.com/en/US/docs/ios/ios_xe/cether/configuration/guide/ce_lnkbndl_xe.html

Link Layer Discovery Protocol

非シスコ 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 LLDP をサポートしています。Link Layer Discovery Protocol（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ネイバー ディスカバリ プロトコルです。このプロトコルはデータ リンク層で動作するため、異なるネットワーク層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できます。

LLDP は一連の属性をサポートし、これらを使用してネイバー デバイスを検出します。属性には、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 30 章「LLDP、LLDP-MED、およびロケーション サービスの設定」を参照してください。

リンクステート トラッキング

リンクステート トラッキングは、トランク フェールオーバーとも呼ばれ、複数のインターフェイスのリンクステートをバインドする機能です。たとえば、リンクステート トラッキングをサーバ NIC アダプタ チーミング機能とともに使用すると、ネットワークで冗長性が実現されます。サーバ ネットワーク アダプタが、チーミングと呼ばれるプライマリまたはセカンダリ関係で設定され、プライマリ インターフェイスでリンクが消失した場合、接続はセカンダリ インターフェイスに透過的に変更されます。

リンク ステート トラッキングの設定については、第 25 章「EtherChannel およびリンク ステート トラッキングの設定」を参照してください。

ロケーション サービス

ロケーション サービス機能を使用すると、スイッチに接続されているデバイスについて、スイッチから Cisco Mobility Services Engine（MSE）に、ロケーションおよび接続のトラッキング情報を提供できます。トラッキングされたデバイスは、ワイヤレス エンドポイント、ワイヤード エンドポイント、またはワイヤード スイッチやワイヤード コントローラになります。スイッチは、暗号化された Network Mobility Services Protocol（NMSP）のロケーションおよび接続の通知を介して、デバイスのリンク アップとリンク ダウンのイベントを MSE に通知します。

LLDP の設定手順については、第 30 章「LLDP、LLDP-MED、およびロケーション サービスの設定」を参照してください。

マルチ スパニングツリー

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

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

MST の設定手順については、第 21 章「STP および MST の設定」を参照してください。

Per-VLAN ラピッド スパニングツリー

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

PVRST+ の設定手順については、第 21 章「STP および MST の設定」を参照してください。

Quality of Service

（注）　Catalyst 4900M、Catalyst 4948E、Supervisor Engine 6-E および Supervisor Engine 6L-E の QoS 機能は同等です。

Quality of Service（QoS）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 の機能をサポートします。

- 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。電話が検出されない場合、信頼境界機能がハイ プライオリティ キューの誤使用を避けるためにスイッチ ポートの信頼設定をディセーブルにします。

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 機能の導入を簡略にします。

Cisco Modular QoS コマンドライン インターフェイス

Cisco Modular QoS CLI（MQC）は、Cisco IOS ソフトウェア QoS を実装す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 機能の設定に関する MQC に従います。MQC は、新しい機能およびテクノロジーの手法の迅速な展開をイネーブルにし、帯域幅、遅延、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向上ジッタとパケット損失に関連するネットワーク パフォーマンスの管理が容易になります。豊富な拡張 QoS 機能が、Cisco MQC を使用してイネーブルになります。

Two-Rate Three-Color ポリシング

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 DiffServ コード ポイント（DSCP）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、多くの場合、ネットワークに出入りするトラフィックのレートを制限するためにネットワークのエッジのインターフェイスで設定されます。この機能を使用すると、ユーザが定義した基準に準拠するトラフィックはインターフェイスを介して送信できますが、これらの基準を超える、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ます。

QoS および Auto-QoS については、第 41 章「Quality of Service 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、スパニングツリー プロトコル（STP）に代わるプロトコルとして、ネットワーク ループの制御、リンク障害の処理、コンバージェンス時間の改善を実現します。REP は、セグメントに接続されているポートのグループを制御することで、セグメントがブリッジング ループを作成するのを防ぎ、セグメント内のリンク障害に応答します。REP は、より複雑なネットワークを構築するための基盤を提供し、VLAN ロード バランシングをサポートします。

REP については、第 23 章「Resilient Ethernet Protocol の設定」を参照してください。

SmartPort マクロ

SmartPort マクロは、一般的な設定を保存したり、共有する作業を簡単に実行するための方法を提供します。SmartPort マクロを使用すると、ネットワーク内のスイッチの位置に基づいて機能および設定をイネーブルにしたり、ネットワーク中に多数の設定を導入したりできます。

SmartPort マクロの設定については、第 19 章「SmartPort マクロの設定」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 21 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 24 章「オプションの STP 機能の設定」を参照してください。

ステートフル スイッチオーバー

ステートフル スイッチオーバー（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 メンバー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 IGMP 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 DHCP データを認識し、セキュリティ機能が間断なく提供されるように、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 の詳細については、第 12 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 SVI も通常停止します。SVI が「アップまたはダウン」状態であることを判断するときにいくつかのポートを考慮しないようにネットワークを設計できます。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して機能し、その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。

単一方向リンク検出

単方向リンク検出（UDLD）は、光ファイバまたは銅製イーサネット ケーブルで接続されたデバイスで、ケーブルの物理構成をモニタして、単方向リンクを検出できるようにします。

標準 UDLD では、単方向リンクを検出できる時間は、タイマーがどのように設定されているかによって数秒から数分まで異なります。リンク ステータス メッセージは 2 秒ごとに交換されます。Fast UDLD では、1 秒未満で（これもタイマーの設定によって異なります）単一方向リンクを検出できます。リンク ステータス メッセージは 200 ミリ秒ごとに交換されます。

UDLD および Fast UDLD の詳細については、第 31 章「UDLD 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な方法で、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 トランキング プロトコル（VTP）、およびダイナミック VLAN メンバーシップの詳細については、第 16 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 の詳細については、第 43 章「プライベート VLAN 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 無差別トランク ポート：プライベート VLAN 無差別トランクを使用すると、無差別ポートを 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 無差別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加入者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 無差別トランク上で伝送できません。
- ダイナミック VLAN メンバーシップ：ダイナミック VLAN メンバーシップの、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 に新しいポートを動的に割り当てます。VLAN メンバーシップ ポリシー サーバ（VMPS）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。

仮想スイッチング システム

ネットワーク オペレータは、冗長ペアとしてスイッチを設定し、リンクをプロビジョニングすることにより、ネットワークの信頼性を高めます。冗長ネットワーク要素や冗長リンクにより、ネットワークの設計や操作が複雑になることがあります。仮想スイッチングを使用すると、ネットワーク要素の数が減り、複雑な冗長スイッチおよびリンクの管理が隠され、ネットワークが単純化されます。

VSS では、1 つのネットワーク要素に Catalyst 4500 または 4500-X シリーズ スイッチのペアを結合します。VSS によって管理される冗長リンクは、外部的には 1 つのポート チャネルとして機能します。Cisco Release IOS XE 3.4.0SG 以降、Catalyst 4500 または 4500-X シリーズ スイッチは、VSS をサポートします。

（注）　Smart Install ディレクタは、VSS ではサポートされません。

VSS については、第 5 章「Virtual Switching System の設定」を参照してください。

Virtual Switch System クライアント

Catalyst 4500 シリーズ スイッチは拡張 PAgP をサポートします。Catalyst 4500 シリーズ スイッチが PAgP EtherChannel で Catalyst 6500 シリーズの Virtual Switch System（VSS）に接続されている場合は、Catalyst 4500 シリーズ スイッチが、自動的に、デュアルアクティブ検出用のこの EtherChannel 上で拡張 PAgP を使用して、VSS クライアントになります。この VSS クライアント機能は、Catalyst 4500 シリーズ スイッチのパフォーマンスに影響を与えることはなく、ユーザによる設定も必要ありません。

VSS については、第 25 章「EtherChannel およびリンク ステート トラッキングの設定」を参照してください。

Y.1731（AIS および RDI）

Y.1731 ETH-AIS（Ethernet Alarm Indication Signal）機能および ETH-RDI（Ethernet Remote Defect Indication）機能は、大規模なネットワークのサービス プロバイダー向けに障害およびパフォーマンス管理を提供します。

ETH-AIS は、サーバ（サブ）レイヤで障害状態を検出した後のアラームを抑制します。スパニングツリー プロトコル（STP）環境内で提供される独立した復元機能のため、ETH-AIS が STP 環境で適用されることはありません。この場合、AIS は設定可能で、管理者は AIS を STP 環境またはそれ以外でイネーブルおよびディセーブルにする方法について説明します。

ETH-RDI は、MEP が障害状態が発生したピア MEP と通信する際に使用します。ETH-RDI が使用されるのは、ETH-CC 送信がイネーブルになっている場合のみです。

Y.1731 については、第 65 章「Y.1731 の設定（AIS および RDI）」を参照してください。

レイヤ 3 ソフトウェアの機能

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

従来のソフトウェアベースのスイッチと比較すると、レイヤ 3 スイッチは、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）を使用することにより、より多くのパケットをより高速に処理します。

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

双方向フォワーディング検出

（注）　Catalyst 4500E でのサポートは限定的です。Cisco IOS Release IOS 15.1(1)SG 以降では、双方向フォワーディング検出（BFD）は Catalyst 4900M および Catalyst 4948E イーサネット スイッチでだけサポートされます。

双方向フォワーディング検出（BFD）プロトコル。BFD はあらゆるメディア タイプ、カプセル化、トポロジ、およびルーティング プロトコルの高速転送パス障害検出回数を提供するように設計された検出プロトコルです。これにはマルチ ホップ BFD セッションの設定方法の説明が含まれます。BFD は高速転送パス障害検出に加えて、ネットワーク管理者に一貫した障害検出方法を提供します。

BFD の設定については、第 38 章「双方向フォワーディング検出の設定」を参照してください。

シスコ エクスプレス フォワーディング

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

CEF の設定手順については、第 34 章「シスコ エクスプレス フォワーディングの設定」を参照してください。

デバイス センサー

デバイス センサーは、Cisco Discovery Protocol（CDP）、Link Layer Discovery Protocol（LLDP）、および DHCP などのプロトコルを使用して、ネットワーク デバイスからデバイスのエンドポイント情報を取得して、クライアントがこの情報を利用できるようにします。デバイス センサーには、組み込みの Device Classifier（ローカル アナライザ）、Auto SmartPort（ASP）、Medianet Services Interface（MSI）プロキシ、および EnergyWise などの内部クライアントがあります。デバイス センサーには、RADIUS アカウンティングを使用してエンドポイントのデータを受信 / 分析する外部クライアント、Identity Services Engine（ISE）もあります。ISE と統合した場合、デバイス センサーは集中ポリシー管理機能とデバイスのプロファイリング機能を提供します。

デバイス センサーの詳細については、第 45 章「802.1X ポートベース認証の設定」を参照してください。

EIGRP スタブ ルーティング

EIGRP スタブ ルーティング機能は、すべてのイメージで使用でき、エンド ユーザの近くにルーテッド トラフィックを移動することでリソースの利用率を低減させます。

IP ベース イメージには EIGRP スタブ ルーティングだけが含まれています。IP サービス イメージには、完全な EIGRP ルーティングが含まれています。

EIGRP スタブ ルーティングを使用するネットワークでは、IP トラフィックがユーザに到達するには、ルート EIGRP スタブ ルーティングを設定しているスイッチを通過する必要があります。スイッチは、ユーザ インターフェイスとして設定されているインターフェイスまたは他のデバイスに接続されているインターフェイスにルーテッド トラフィックを送信します。

EIGRP スタブ ルーティングの設定手順については、第 33 章「レイヤ 3 インターフェイスの設定」を参照してください。

拡張オブジェクト トラッキング

拡張オブジェクト トラッキング機能を導入しなくても、Hot Standby Router Protocol（HSRP; ホット スタンバイ ルータ プロトコル）に単純なトラッキング メカニズムが内蔵されています。このメカニズムでは、インターフェイスの回線プロトコルの状態しか追跡することができません。インターフェイスのラインプロトコル ステートがダウンになった場合、ルータの HSRP 優先度は削減され、より高い優先度のもう 1 つの HSRP ルータがアクティブになることができます。

EOT 機能は、HSRP からトラッキング メカニズムを分離して、別のスタンドアロン トラッキング プロセスを生成します。このプロセスは、別の Cisco IOS プロセスだけでなく、HSRP でも使用することができます。この機能を使用すると、インターフェイスのラインプロトコル ステートに加えて他のオブジェクトも追跡できます。

HSRP、Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）、Gateway Load Balancing Protoco（GLBP）などのクライアント プロセスで、トラッキング オブジェクトに対する興味を登録し、追跡対象オブジェクトの状態が変化したときに通知を受け取るようにすることができます。

EOT の詳細については、次の URL を参照してください。

拡張オブジェクト トラッキングのプラットフォーム固有の情報については、第 58 章「拡張オブジェクト トラッキングの設定」を参照してください。

拡張オブジェクト トラッキ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-xml/ios/ipapp/configuration/12-4t/iap-eot.html

GLBP

Gateway Load Balancing Protocol（GLBP）機能は、LAN 上の 1 つのデフォルト ゲートウェイで設定された 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 ルータを連結し、IP パケットの転送負荷を共有しながら単一の仮想ファースト ホップ IP ルータを提供します。GLBP デバイスはパケット転送の役割、リソースの使用状況の最適化を共有し、コストを削減します。LAN 上にあるその他のルータは、冗長化された GLBP ルータとして動作できます。このルータは、既存のフォワーディング ルータが機能しなくなった場合にアクティブになります。これにより、ネットワークの復元力が向上し、管理上の負担が軽減されます。

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/docs/ios/ipapp/configuration/guide/ipapp_glbp_ps6350_TSD_Products_Configuration_Guide_Chapter.html

Cisco IOS XE 3.1.0SG における Cisco IOS XE IP Application Services 機能

ここでは、Cisco IOS XE 3.1.0SG でサポートされている IP Application Services ソフトウェア機能について説明します。機能マニュアルへのリンクが掲載されています。

機能ガイドには、複数の機能に関する情報が含まれている場合があります。機能ガイドで特定の機能に関する情報を検索する場合は、巻末の機能情報表を参照してください。

機能ガイドには、さまざまなソフトウェア リリースとプラットフォームでサポートされている機能が掲載されています。ご使用のシスコ ソフトウェア リリースまたはプラットフォームで、機能ガイドに記載されたすべての機能がサポートされているとは限りません。そのガイドでどの機能がソフトウェア リリースでサポートされるかについては、機能ガイドの最後にある機能情報の表を参照してください。プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは不要です。

Gateway Load Balancing Protocol（GLBP）、GLBP MD5 認証

http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_glbp.html

HSRP

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

HSRP の設定については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_hsrp_ps6350_TSD_Products_Configuration_Guide_Chapter.html

Cisco IOS XE IP Application Services：Cisco IOS XE 3.1.0SG における HSRP 機能

ここでは、Cisco IOS XE 3.1.0SG でサポートされている IP Application Services の HSRP ソフトウェア機能について説明します。機能マニュアルへのリンクが掲載されています。

機能ガイドには、複数の機能に関する情報が含まれている場合があります。機能ガイドで特定の機能に関する情報を検索する場合は、巻末の機能情報表を参照してください。

機能ガイドには、さまざまなソフトウェア リリースとプラットフォームでサポートされている機能が掲載されています。ご使用のシスコ ソフトウェア リリースまたはプラットフォームで、機能ガイドに記載されたすべての機能がサポートされているとは限りません。そのガイドでどの機能がソフトウェア リリースでサポートされるかについては、機能ガイドの最後にある機能情報の表を参照してください。プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは不要です。

HSRP：Hot Standby Router Protocol（ホットスタンバイ ルータ プロトコル）

http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_hsrp.html

HSRP MD5 認証

http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_hsrp.html

ICMP Redirect に対する HSRP サポート

http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_hsrp.html

IP Precedence アカウンティング

http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_ipserv.html

ISSU：HSRP

http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_hsrp.html

SSO：HSRP

http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_hsrp.html

SSO 対応 HSRP

SSO 対応 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 ルータとして機能を引き継ぎます。これは NSF/SSO で提供される信頼性およびアベイラビリティをさらにレイヤ 3 に拡張します。SSO 対応 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.1-18）
- 「EIGRP」（P.1-18）
- 「IS-IS」（P.1-19）
- 「OSPF」（P.1-19）
- 「RIP」（P.1-20）

BGP

ボーダー ゲートウェイ プロトコル（BGP）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、これにはクラスレス ドメイン間ルーティング（CIDR）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 内部のネットワーク クラスの概念をエミュレートし、IP プレフィックスのアドバタイズをサポートします。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。

BGP 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_4t/ip_route/configuration/guide/t_brbbas.html

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 は拡散更新アルゴリズム（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層サポートの各機能を備えています。ネットワーク トポロジが変更されると、EIGRP はトポロジ テーブルで宛先までの新しい適切なルートを確認します。テーブルにこのようなルートが見つかると、EIGRP はルーティング テーブルをただちに更新します。ユーザは EIGRP が IPX パケットのルーティング用に提供する高速コンバージェンスと部分的更新を使用できます。

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

（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）　カスタマーは、IPv6 プレフィックスをルーティングするように Enhanced Interior Gateway Routing Protocol（EIGRP）を設定できます。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。

EIGRP 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/ps6630/products_ios_protocol_option_home.html

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 Open Shortest Path First（OSPF）ルーティング プロトコルに厳密に準拠しています。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でだけリレーされます。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 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/ps6632/products_ios_protocol_option_home.html

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。リンクステート情報が累積すると、ルータは、Shortest Path First（SPF）アルゴ

リズムを使用して各ノードへの最短パスを計算します。この他の OSPF の機能には、等コスト マルチパス ルーティングや上位層の 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*の概念を使用します。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。

OSPF 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/tech/tk365/tk480/tsd_technology_support_sub-protocol_home.html

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）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。

RIP 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/tech/tk365/tk554/tsd_technology_support_sub-protocol_home.html

インサービス ソフトウェア アップグレード

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 Cisco 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インサービス ソフトウェア アップグレード（ISSU）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 または IOS XE 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。

Cisco IOS ISSU の詳細については、第 6 章「Cisco IOS インサービス ソフトウェア アップグレード プロセスの設定」を参照してください。

Cisco IOS XE ISSU の詳細については、第 7 章「Cisco IOS XE インサービス ソフトウェア アップグレード プロセスの設定」を参照してください。

IPv6

IPv6 は、エンドツーエンドのセキュリティ、Quality of Service（QoS）、グローバルに一意なアドレスなどのサービスを提供します。IPv6 アドレス スペースによって、プライベート アドレスの必要性が低下し、ネットワーク エッジの境界ルータで Network Address Translation（NAT; ネットワーク アドレス変換）処理を行う必要性も低下します。

Catalyst 4500 シリーズ スイッチでサポートされている IPv6 サービスの詳細については、第 53 章「IPv6 のサポート」を参照してください。

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。

- ANCP クライアント : ANCP マルチキャストを使用すると、ANCP（IGMP ではなく）または CLI のダイレクト スタティック コンフィギュレーションを使用して Catalyst 4500 スイッチ上のマルチキャスト トラフィックを制御できます。
- 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だけに転送されます。
- インターネット グループ管理プロトコル（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、マルチキャスト トラフィックを要求するホストが接続されたポートにのみ転送されます。

  IGMPv3 のサポートによって、IGMPv3 ホストまたはルータが存在する場合に、マルチキャスト トラフィック フラッディングが抑制されます。IGMPv3 スヌーピングは、IGMPv3 クエリーおよびメンバーシップ レポート メッセージをリッスンして、ホストとマルチキャスト グループの関連付けを維持します。また、スイッチからマルチキャスト データをそれが必要なポートにだけ伝播させることができます。IGMPv3 スヌーピングは、IGMPv1 および IGMPv2 と完全な相互運用性があります。

  明示的ホスト トラッキング（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ーシップ情報の追跡、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 クエリアは、VLAN で IGMP スヌーピングをサポートするために必要なレイヤ 2 機能です。VLAN では、マルチキャスト トラフィックでルーティングが必要ではないため、PIM および IGMP は設定されていません。

  IGMP スヌーピングの設定手順については、第 26 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 Listen Discovery（MLD）と Multicast Listen Discovery スヌーピング : MLD は、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）の存在を検出し、隣接ノードに関係するマルチキャスト デバイスを検出するのに IPv6 マルチキャスト パケットが使用するプロトコルです。MLD スヌーピングは、MLD v1 と MLD v2 の 2 種類のバージョンでサポートされます。ネットワーク スイッチでは、MLD スヌーピングを使用してマルチキャスト トラフィックのフラッディングを抑制し、IPv6 マルチ キャスト データを VLAN 内のすべてのポートにフラッディングされるのではなくデータを受信するポートのリストに転送します。これにより、ネットワーク デバイスの負荷を軽減し、リンクで不要な帯域幅を最小化し、IPv6 マルチ キャスト データを効率的に配信できます。

  マルチキャスト サービスの設定方法については、第 27 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 はさらに、完全に独立したマルチキャスト ルーティング テーブルを作成する代わりに、ユニキャスト ルーティング テーブルを使用して Reverse Path Forwarding（RPF）チェック機能を実行します。

PIM-SSM マッピングについては、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

- IP マルチキャスト ロード分割（S、G、およびネクスト ホップを使用する等コスト マルチパス（ECMP））：
  IP マルチキャスト ロード分割では、ソース アドレスとグループ アドレスに基づいた、およびソース アドレスとグループ アドレスとネクスト ホップ アドレスに基づいたロード分割のサポートを追加して、より柔軟なサポートを ECMP マルチキャスト ロード分割に導入しています。この機能により、多数のストリームをグループに送信するデバイスまたは多数のチャネルをブロードキャストするデバイス（IPTV サーバや MPEG ビデオ サーバなど）からのマルチキャスト トラフィックを、等コスト パスの全域にわたってより効果的にロード共有できます。

マルチキャスト サービスの設定方法については、第 36 章「IP マルチキャストの設定」を参照してください。

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。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、およびシスコ エクスプレス フォワーディング（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。

（注）　IP ベース イメージでは、NSF は EIGRP スタブ ルーティングと OSPF でサポートされます。

（注）　Enterprise Services イメージでは、NSF は RIP を除くすべてのルーティング プロトコルでサポートされています。

（注）　LAN ベース イメージは NSF をサポートしません。

NSF/SSO の詳細については、第 12 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。

ルーテッド アクセスの OSPF

ルーテッド アクセスの OSPF は、お客様がレイヤ 3 ルーティングの機能をアクセス クローゼットまたはワイヤリング クローゼットに拡張できるようにするために、特別に設計されています。

（注）　OSPF for Routed Access は、OSPFv2 インスタンスと OSPFv3 インスタンスをそれぞれ 1 つずつと、最大 200 のダイナミックに学習されるルートをサポートします。

ワイヤリング クローゼット（スポーク）が、すべての非ローカルのトラフィックをディストリビューション レイヤに転送するディストリビューション スイッチ（ハブ）に接続された、キャンパス環境の標準的なトポロジ（ハブおよびスポーク）では、ワイヤリング クローゼット スイッチが、完全なルーティング テーブルを保持する必要がありません。理想的には、ディストリビューション スイッチは、エリア間および外部ルートに到達するためのデフォルト ルートをワイヤリング クローゼット スイッチに送信します（OSPF スタブまたは完全なスタブ エリア設定）。

詳細については、次のリンクを参照してください。

http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/routed-ex.html

Cisco IOS Release 12.2(53)SG では、IP ベース イメージはルーテッド アクセスの OSPF をサポートします。ルート制限のない複数の OSPFv2 および OSPFv3 インスタンスが必要な場合は、Enterprise Services イメージが必要です。また、VRF-Lite 機能をイネーブルにするためにも Enterprise Services は必要です。

ポリシーベース ルーティング

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。ポリシーベース ルーティング（PBR）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 ポートなど、パケットに関連したその他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。

リリース IOS XE 3.4.0SG および IOS 15.1(2)SG 以降では、PBR 再帰ネクスト ホップ機能は再帰ネクスト ホップ IP アドレスの設定をイネーブルにするためにルート マップを拡張します。再帰ネクスト ホップ IP アドレスは、直接接続されていないサブネットにすることができます。ルーティング テーブルは、設定されている再帰ネクスト ホップ経由でルーティングされるようにパケットを送信する直接接続されたネクスト ホップを見つけるために検索されます。

PBR の詳細については、第 39 章「ポリシーベース ルーティングの設定」を参照してください。

ユニキャスト Reverse Path Forwarding

ユニキャスト Reverse Path Forwarding（ユニキャスト RPF）機能は、検証可能な送信元 IP アドレスが不足している IP パケットを廃棄することで、間違ったまたは偽造（スプーフィングされた）送信元 IP アドレスがネットワークに流れて発生する問題を軽減するのに役立ちます。

URPF については、第 35 章「uRPF の設定」を参照してください。

単方向リンク ルーティング

単方向リンク ルーティング（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。

単方向リンク ルーティング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/en/US/docs/ios/12_1/iproute/configuration/guide/1cdudlr.html

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 VPN Routing/Forwarding（VRF; VPN ルーティング/転送）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 40 章「VRF-Lite の設定」を参照してください。

Virtual Router Redundancy Protocol

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、マルチベンダーのファーストホップ ゲートウェイ冗長配置で使用されます。

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/en/US/docs/ios/ipapp/configuration/guide/ipapp_vrrp_ps6441_TSD_Products_Configuration_Guide_Chapter.html

管理機能

Catalyst 4500 シリーズ スイッチは CLI を使用して、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。

- 「Supervisor Engine 7-E および Supervisor Engine 7L-E のファイル システム管理」（P.1-31）
- 「Supervisor Engine 6-E、Supervisor Engine 6L-E、Catalyst 4948E および Catalyst 4900M の FAT 管理システム」（P.1-31）
- 「強制 10/100 自動ネゴシエーション」（P.1-32）
- 「インテリジェントな電源管理」（P.1-32）
- 「MAC アドレス通知」（P.1-32）
- 「MAC 通知 MIB」（P.1-32）
- 「NetFlow 統計情報」（P.1-32）
- 「NetFlow-lite」（P.1-33）
- 「Power over Ethernet」（P.1-33）
- 「セキュア シェル」（P.1-33）
- 「簡易ネットワーク管理プロトコル」（P.1-33）
- 「SPAN および RSPAN」（P.1-34）
- 「Universal Power over Ethernet」（P.1-34）
- 「Web Content Coordination Protocol」（P.1-34）
- 「Wireshark」（P.1-35）
- 「XML-PI」（P.1-35）

Cisco Call Home

Call Home を使用すると、E メールベースおよび Web ベースで重大なシステム イベントの通知を行えます。ポケットベル サービス、通常の電子メール、または XML ベースの自動解析アプリケーションとの適切な互換性のために、さまざまなメッセージの形式が使用できます。この機能の一般的な利用方法には、ネットワーク サポート エンジニアのダイレクト ページング、ネットワーク オペレーション センターへの電子メール通知、サポート Web サイトへの XML 配信、Cisco Smart Call Home サービスを利用したシスコ Technical Assistance Center（TAC）の直接ケース生成などがあります。

Call Home 機能では、設定、診断、環境条件、コンポーネント、システム イベントについての情報を含むアラート メッセージを送信できます。

Call Home の詳細については、第 66 章「Call Home の設定」を参照してください。

Cisco Energy Wise

Cisco EnergyWise はシスコ スイッチング ソリューションに追加されたエネルギー管理テクノロジーで、企業のインフラストラクチャ全体にわたるエネルギー消費量の測定、報告、削減を支援します。EnergyWise の管理インターフェイスを使用すると、ネットワークを統合ファブリックとして使用して、ネットワーク管理アプリケーションをエンドポイントと通信させたり、相互に通信させたりできます。

詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/switches/lan/energywise/phase2/ios/configuration/guide/ew_v2.html

http://www.cisco.com/en/US/docs/switches/lan/energywise/phase2_5/ios/release/notes/ol23554.html#wp604941

Cisco IOS IP Service Level Agreement

Cisco IOS IP Service Level Agreement（SLA; サービス レベル契約）により、シスコのお客様は、アクティブなトラフィック（連続的で信頼性がある予測可能な形式でのトラフィックの発生）をモニタリングして、IP アプリケーション向けの IP サービス レベルを分析できます。Cisco IOS SLA を使用すると、サービス プロバイダーのお客様はサービス レベル契約の検討と提供が可能になり、企業のお客様はサービス レベルの検証、外部委託しているサービス レベル契約の検証、およびネットワーク パフォーマンスの把握ができるようになります。Cisco IOS IP SLA は、ネットワーク アセスメントを実行することで Quality of Service（QoS）の検証、新しいサービス導入の簡易化、ネットワーク トラブルシューティングの補助を可能にします。

Cisco IOS IP SLA のプラットフォーム固有の情報については、第 67 章「Cisco IOS IP SLA 動作の設定」を参照してください。

Cisco IOS IP SLA の詳細については、次の URL の『*Cisco IOS IP SLAs Configuration Guide, Release 12.4T*』を参照してください。
http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/12_4t/sla_12_4t_book.html

Catalyst 4500 シリーズ スイッチでは、Cisco IOS IP SLA ビデオ動作を使用する組み込みのトラフィック シミュレータもサポートして、Telepresence、IPTV、IP ビデオ サーベイランス カメラなど、さまざまなビデオ アプリケーションの合成トラフィックを生成します。次の目的のために、このシミュレータ ツールを使用できます。

- ネットワーク パフォーマンス要件の厳しいアプリケーションを導入する前にネットワーク アセスメントを行うため。
- 導入後のネットワーク関連のパフォーマンスの問題を Cisco IOS Mediatrace と連携してトラブルシューティングするため。

このトラフィック シミュレータには、複数のテストを同時または定期的に、長期にわたって実行できる高性能なスケジューラが含まれています。（Enterprise Services フィーチャ セットを実行しているスイッチでのみサポートされます）。

この機能の設定については、次の URL にある『*Configuring Cisco IOS IP SLAs Video Operations*』を参照してください。

http://www.cisco.com/en/US/docs/ios-xml/ios/ipsla/configuration/12-2se/sla_video.html

Cisco メディア サービス プロキシ

メディア サービス プロキシ（MSP）機能は、ネットワークのさまざまなメディア エンド ポイントを自動的に特定し、適切なメディア サービスを提供します。これは、適切なデバイスをそれぞれに対応するネットワーク サービスに自動的に接続するレイヤとして機能します。

MSP はネットワーク中心のモデルに従います。このモデルでは、アクセス スイッチおよびルータはデバイスとフローに関する情報を、Cisco Discovery Protocol（以前の CDP）および DHCP などのメカニズムを使用することによって、または Session Initiation Protocol（SIP）および H.323 などの主要なプロトコル パケットのスヌーピングによって学習します。情報の学習を達成するために、エンドポイントへ変更を加える必要はありません。情報が収集された後、MSP がネットワーク デバイスに適切なサービスを提供します。

次に、MSP の利点を示します。

- ネットワークのデバイスおよびフローの自動識別。
- エンドポイントへの適切なサービスの適用。

• 管理者のための設定制御（それによってサービスの手動による設定および管理が減少します）。たとえば、保証帯域幅を必要とするビデオ アプリケーションのためにネットワークにリソース予約プロトコル（RSVP）を設定します。

（注）　システムは MSP およびフロー メタデータがイネーブルの状態で 512 を超える SIP フローに拡張することはできません。

この機能の設定については、次のマニュアルを参照してください。

http://www.cisco.com/en/US/docs/ios-xml/ios/msp/configuration/15-1sg/med-ser-prxy.html

http://www.cisco.com/en/US/docs/ios-xml/ios/msp/configuration/xe-3sg/med-ser-prxy-xe.html

Cisco Medianet AutoQoS

Cisco Medianet AutoQoS はスイッチでの QoS のイネーブル化のプロセスを容易にするためのデフォルト設定を提供します。さまざまなプラットフォーム間で QoS の機能と動作に違いがあるため、このプロセスは困難な場合があります。この機能は、Catalyst 4500 の AutoQoS 機能を拡張して、ビデオ トラフィックやその他の種類のトラフィックをサポートします。

AutoQoS の目的は、QoS をサポートするネットワークの設定中にお客様が引き受けなければならない作業を簡略化することです。これは、さまざまなトラフィック クラスを処理するために QoS 設定を自動化して行われます。Medianet の AutoQoS には、所定の設定を実装するために既存の CLI コマンドを呼び出すマクロとして機能するコマンドが用意されています。特定のインターフェイスに接続されているデバイス（PC、別のスイッチ、IP カメラなど）のタイプを指定する必要があります。Medianet の AutoQoS は、そのインターフェイスにデフォルトの QoS 設定を適用します。これは必要に応じて後で微調整が可能です。

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

Cisco Medianet フロー メタデータ

フロー メタデータは他のデータを限定するデータです。フロー メタデータは、ネットワークに流れるメディア ストリームのタイプ、性質と特性についてネットワークに認識させることによりインテリジェント ネットワークをサポートするのを支援します。また、フロー メタデータでは、ネットワークがメディア ストリームにポリシーを適用できるようになります。Medianet システムにわたって、フロー メタデータは、さまざまな Medianet サービスにより首尾一貫して生成、転送、保存、および取得され、その作用を受けます。

フロー メタデータ インフラストラクチャは、1 コンポーネントからのデータを、ネットワーク要素の間だけでなく、同じネットワーク要素の別のコンポーネントが使用できるようにするフレームワークを提供します。

フロー メタデータは、Cisco IOS Release 15.1(1)SG よりも前のリリースでサポートされます。フロー メタデータは、ネットワーク内のフローを記述するデータです。このフロー メタデータは属性とともに 5 タプル フローを記述します。ネットワーク要素は、エンドポイントによって生成されたフロー メタデータに基づいてアクションを実行できます。

フロー メタデータ インフラストラクチャは、プロデューサとコンシューマという 2 つの主要コンポーネントで構成されています。

- フロー メタデータ プロデューサはフロー メタデータの任意のソースです。プロデューサは、特定のフローのすべての属性を伝播します。プロデューサはネットワーク内の任意の場所（エンドポイント、プロキシ エージェント、または中間ノード）に存在することができます。現在、エンドポ

イントによって生成されるフロー メタデータがサポートされます。プロデューサはフロー メタデータ属性をシグナリングするための RSVP などの特定の転送プロトコルを使用して、コントロール プレーン データベースと呼ばれるデータベースに情報を格納します。その情報をコンシューマが使用できます。

- フロー メタデータ コンシューマはプロデューサが提供するフロー タプルとフロー メタデータを使用する任意のネットワーク要素です。フロー タプルとフロー メタデータは、転送インフラストラクチャを介して異なるネットワーク要素のコンシューマへ、メディア パスに沿って伝播することもできます。

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/en/US/docs/ios-xml/ios/mdata/configuration/xe-3sg/metadata-framework.html

http://www.cisco.com/en/US/docs/ios-xml/ios/mdata/configuration/15-1sg/metadata-framework.html

フロー メタデータ コマンドの詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios-xml/ios/qos/command/qos-cr-book.html

Cisco IOS Mediatrace と Performance Monitor

Cisco IOS Mediatrace は、IP フローのパスをネットワーク管理者が検出できるようにしてパフォーマンスの低下の問題を切り分けてトラブルシューティングを行う場合や、経路上のノードでモニタリング機能を動的にイネーブルにする際や、ネットワークホップバイホップ ベースで情報を収集するのに役立ちます。この情報には、特に、フロー統計情報のほか、着信および発信インターフェイス、CPU、およびメモリの使用率情報、さらに IP ルートまたは Cisco IOS Mediatrace のモニタリング状態の変更が含まれます。

詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios-xml/ios/media_monitoring/configuration/15-1sg/mm-pasv-mon.html

http://www.cisco.com/en/US/docs/ios-xml/ios/media_monitoring/configuration/xe-3sg/mm-pasv-mon.html

http://www.cisco.com/en/US/docs/ios/media_monitoring/command/reference/mm_book.html

http://www.cisco.com/en/US/docs/ios-xml/ios/media_monitoring/configuration/15-1sg/mm-mediatrace.html

http://www.cisco.com/en/US/docs/ios-xml/ios/media_monitoring/configuration/xe-3sg/mm-mediatrace.html

Cisco IOS Mediatrace および Performance Monitor の設定時の注意事項は次のとおりです。

- ビデオ モニタリングは、物理ポート上でのみサポートされます。

Catalyst 4500 シリーズ スイッチでの Cisco IOS Mediatrace と Performance Monitor の制約事項は、次のとおりです。

- どちらの機能も、入力トラフィックをモニタするようにだけ設定できます。
- Supervisor Engine 6-E、Supervisor 6L-E、Catalyst 4900M および Catalyst 4948E では、パケットはカプセル化で CEure および rxSPAN セッションの両方によってモニタすることはできません。最初に適用されたコンフィギュレーションが優先されます。

- インターフェイスで受信されたすべてのパケットをモニタできるわけではありません。入力インターフェイスによって受信された後で、パケットは転送の判断ができなくなるか、または設定されたセキュリティ機能（IP ソース ガードなど）が原因でさまざまな段階でドロップされる可能性があります。スイッチは、スイッチ近くのパケットを監視しようとしますが、入力分類段階の前にドロップされていないパケットのみモニタ可能です。
- CPU 使用率は高いトラフィック レートをモニタするときに影響を受けます。内部で決定されたしきい値を超過すると、モニタ対象のパケットは元のパケットがハードウェアでそのまま転送されますがドロップされます。リリース IOS XE 3.3.0SG および IOS 15.1(1) SG 以降、モニタ対象のパケットは、次のいずれかが当てはまる場合、ドロップされることがあります。
  - パケット レートがフローごとに 512 PPS を超えている。
  - モニタ トラフィックの合計帯域幅が 10Mbps を超えている。
  - リソースが新しく監視されるパケットのエンキューに不十分である。

  モニタ対象のパケットがドロップされた場合、フロー レコードに *collect monitor event* が含まれていれば、*monitor event* は TRUE に設定されます。1 分間、新しいドロップがなければ、*monitor event* は FALSE に設定されますが、新しいモニタ間隔が開始されるまで、**show performance monitor status** の出力に反映されません。

  monitor event はグローバル フラグです。これは、「monitor event」を TRUE に設定するトリガーとなるすべてのパケットが、その監視間隔のすべてのモニタされたフローに関してドロップされることを意味します。メトリックが連続パケットの収集に依存していれば、そのメトリックの精度は *monitor event* が TRUE の場合に影響を受ける可能性があります。

Cisco Network Assistant

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任意の場所で管理します。グラフィカル ユーザ インターフェイスを使用すると、コマンドライン インターフェイス 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。

Cisco Network Assistant の詳細については、第 15 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。

Dynamic Host Control Protocol

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

  http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_dhcp_rdmp_ps6350_TSD_Products_Configuration_Guide_Chapter.html

Easy Virtual Network

Easy Virtual Network（EVN）は、ネットワークのエンドツーエンドの仮想化を実現する IP ベースの仮想化テクノロジーです。単一の IP インフラストラクチャを使用して、トラフィック パスが相互に独立した状態で、個別の仮想ネットワークを提供できます。Easy Virtual Network を設定して、複数の仮想 IP ネットワークを設定します。

EVN 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-xml/ios/evn/configuration/xe-3s/evn-xe-3s-book.html

次の制約事項/機能の相互作用が適用されます。

- マルチキャスト

  送信元と受信側が異なる VRF にある VRF をマルチキャスト トラフィックが通過するとき、マルチキャスト カウンタは受信側の VRF について増加しません。

- NetFlow

  EVN トランク インターフェイスに設定されている場合、NetFlow はすべての VRF のトラフィック情報をキャプチャしますが、その VRF 情報を維持しません。

- SPAN

  - EVN トランク インターフェイスが SPAN 送信元として設定されている場合、EVN トランクによって搬送されるすべての VRF に属するトラフィックがスパンされます。デフォルトでは、VNET タグは保持されません。これを維持するには、**encapsulation dot1q** オプションで SPAN 宛先を設定します。
  - EVN トランクの特定の VRF に属するトラフィックをスパンするには、対応する VNET タグを vlan_ids として持つ **filter vlan** を SPAN セッションに設定し、**filter vlan** で指定された VLAN を設定します。
  - すべてのインターフェイス上の特定の VRF のトラフィックをスパンするには、VNET タグを vlan_ids として持つ SPAN 送信元として **vlan** を設定し、送信元として指定された VLAN を設定します。
  - CPU が SPAN 送信元として設定されている場合、スパンされる送信パケットはデフォルトでタグ付けされます。**encapsulation dot1q** オプションが SPAN セッションで設定されている場合、スパンされた CPU 送信パケットは二重タグ付きです。

  SPAN セッションの設定については、第 56 章「SPAN および RSPAN の設定」を参照してください。

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。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。

（組み込み CiscoView 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）。

組み込まれている Event Manager

Embedded Event Manager（EEM）は、イベント検出と回復を Cisco IOS 内部で直接行うための分散型でカスタマイズされた手法です。EEM はイベントをモニタし、モニタ対象イベントが発生したり、しきい値に達したりすると、情報提供や訂正などの必要な EEM 処理を実行します。EEM ポリシーは、イベントおよびイベントが発生した場合に行う処理を定義するエンティティです。

EEM については、次の URL を参照してください。

http://www.cisco.com/en/US/products/ps6815/products_ios_protocol_group_home.html

イーサネット管理ポート

イーサネット管理ポートは、PC を接続するレイヤ 3 ホスト ポートで、*Fa1 または fastethernet1 ポート*とも呼ばれます。ネットワークの管理に、スイッチ コンソール ポートの代わりとしてイーサネット管理ポートを使用できます。スイッチ スタックを管理するときに、PC を Catalyst 4500 シリーズ スイッチのイーサネット管理ポートに接続します。

イーサネット管理ポートの詳細については、第 8 章「インターフェイスの設定」の「イーサネット管理ポートの使用」を参照してください。

Supervisor Engine 7-E および Supervisor Engine 7L-E のファイル システム管理

IOS XE 3.1.0SG の format コマンドは、標準的な IOS 形式と比較して若干変更されました。その理由は、後者が ext2 形式をサポートしないためです。

IOS XE 3.1.0SG での USB フラッシュでは、3 つのオプション形式、つまり FAT16、FAT32 および EXT2 があります。

```
Switch# format usb0: ?
   FAT16  FAT16 filesystem type
   FAT32  FAT32 filesystem type
   ext2   ext2 filesystem type
```

IOS XE 3.1.0SG での SD カードでは、デフォルト形式は FAT16 です。

```
Switch# format slaveusb0: ?
    FAT16  FAT16 filesystem type
   FAT32  FAT32 filesystem type
   ext2   ext2 filesystem type
```

Supervisor Engine 6-E、Supervisor Engine 6L-E、Catalyst 4948E および Catalyst 4900M の FAT 管理システム

FAT ファイル システムは、デバイス ディスクおよびフラッシュ上のファイルの管理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り、フラッシュ間でイメージの削除、追加、および転送を容易に行うことができます。

強制 10/100 自動ネゴシエーション

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

インテリジェントな電源管理

この機能はシスコ製の受電デバイスと連動し、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 準拠の受電デバイス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デバイス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 14 章「Power over Ethernet（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 アドレスがモニタリングされます。通知は CISCO-MAC-NOTIFICATION MIB を使用して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 攻撃または中間者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モニタリングします。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

（注）　NetFlow は、Catalyst 4900M、Catalyst 4948E、Supervisor Engine 6-E、および Supervisor Engine 6L-E でサポートされません。これは、Supervisor Engine 7-E および Supervisor Engine 7L-E だけでサポートされます。

NetFlow 統計情報は、グローバル トラフィックのモニタリング機能で、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提供します。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 61 章「NetFlow の設定」を参照してください。

NetFlow-lite

（注）　NetFlow-lite は Catalyst 4948E および Catalyst 4948E-F イーサネット スイッチでのみサポートされます。

NetFlow-lite 機能は、スイッチのインターフェイスにすることができるモニタリング ポイントでの入力パケット サンプリングに基づいています。NetFlow のサンプリング パケットをエクスポートすることにより、デバイスで切り替えられるトラフィックが可視化されます。入力パケットをサンプリングするレートは設定可能で、幅広いサンプリング レートがサポートされます。各サンプリング済みパケットはデータ パスに個別の NetFlow データ レコードとしてエクスポートされます。NetFlow V9 および V10（IPFIX）のエクスポート形式がサポートされています。

NetFlow 統計情報の詳細については、第 62 章「NetFlow-lite の設定」を参照してください。

Power over Ethernet

Power over Ethernet（PoE）は、LAN スイッチング インフラストラクチャが、銅線イーサネット ケーブル経由でエンドポイント（「受電デバイス」）に電力を提供できるようにします。かつて「インライン パワー」と呼ばれていたこの機能は、2000 年にシスコによって、新しく登場した IP テレフォニー配置をサポートするために開発されました。

IP 電話は動作に電力を必要とし、Power over Ethernet は、スケーラブルで管理可能な電力配信をサポートし、IP テレフォニー配置を簡略化します。ワイヤレス ネットワーキングが登場したときに、Power over Ethernet はローカル電源アクセスが存在しなかった場所のワイヤレス デバイスへの電力供給を開始しました。

Power over Ethernet の詳細については、第 14 章「Power over Ethernet（PoE）の設定」を参照してください。

セキュア シェル

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。

簡易ネットワーク管理プロトコル

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 60 章「SNMP の設定」を参照してください。

SPAN および RSPAN

スイッチド ポート アナライザ（SPAN）は、ネットワーク アナライザまたはリモート モニタリング（RMON）プローブによってポート上の解析用トラフィックをモニタリングします。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 56 章「SPAN および RSPAN の設定」を参照してください。

リモート 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 56 章「SPAN および RSPAN の設定」を参照してください。

Universal Power over Ethernet

IEEE 802.3 Power over Ethernet（PoE）標準は、30 W の Data Terminal Equipment（DTE）によって供給できる最大電力を設定します。この電力は ISO/IEC 11801:1995 に規定されているクラス D またはそれ以上のケーブル配線の 4 本のツイスト ペア導体から 2 ペアにより供給されます。

Cisco® Universal Power over Ethernet（UPOE）は、標準のイーサネット ケーブル配線インフラストラクチャ（クラス D またはそれ以上）により最大 60 W の電力を供給する機能を提供するように、IEEE 802.3 PoE 標準を拡張するシスコ独自のテクノロジーです。

UPOE の詳細については、第 14 章「Power over Ethernet（PoE）の設定」の「Universal PoE の設定」を参照してください

Web Content Coordination Protocol

（注）　WCCP バージョン 1 はサポート*されません*。

Web Content Communication Protocol（WCCP）バージョン 2 レイヤ 2 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 および MAC アドレス書き換えを使用して、直接接続されたコンテンツ エンジンにコンテンツ要求を透過的にリダイレクトできるようになります。WCCPv2 レイヤ 2 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ため、総称ルーティング カプセル化（GRE）を使用したレイヤ 3 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、ファイル転送プロトコル（FTP）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 レイヤ 2 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のために展開されます。WCCPv2 レイヤ 2 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。レイヤ 2 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ていません。

WCCP については、第 70 章「WCCP バージョン 2 サービスの設定」を参照してください。

Wireshark

（注）　Wireshark は Supervisor Engine 7-E、Supervisor Engine 7L-E、および Catalyst 4500X-32 だけでサポートされます。

Cisco IOS XE Release 3.3.0SG と IP Base および Enterprise Services フィーチャ セット以降、Catalyst 4500 シリーズ スイッチは、Wireshark をサポートします。これは、複数のプロトコルをサポートし、グラフィカル ユーザ インターフェイスおよびテキストベース ユーザ インターフェイスで情報を提供する以前 Ethereal と呼ばれていたパケット アナライザ プログラムです。Wireshark は個々のインターフェイスで適用されるかイネーブルにされます。グローバルなパケット キャプチャはサポートされません。

Wireshark については、第 57 章「Wireshark の設定」を参照してください。

XML-PI

eXtensible Markup Language Programmatic Interface（XML-PI）Release 1.0 は、Network Configuration Protocol（NETCONF）を使用します。このリリースは、テクノロジーや外部の XML/CLI ゲートウェイを必要とせず、実行コンフィギュレーションと **show** コマンド出力をキーワード レベルに下げて収集する新しいデータ モデルを提供します。XML-PI を使用すれば、任意の数のネットワーク デバイスを同時に管理する XML ベースのネットワーク管理アプリケーションを開発できます。

詳細については、次のリンクを参照してください。

http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_xmlpi_v1.html

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.1-36）
- 「Cisco TrustSec のセキュリティ アーキテクチャ」（P.1-37）
- 「Cisco TrustSec MACsec の暗号化」（P.1-38）
- 「ダイナミック ARP インスペクション（DAI）」（P.1-38）
- 「DHCP スヌーピング」（P.1-38）
- 「フラッディング ブロック」（P.1-39）
- 「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.1-39）

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。

- ゲスト VLAN に対する 802.1X 認証：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。
- 802.1X 認証失敗オープン割り当て：デバイスが 802.1X 経由の自己認証に失敗した（たとえば、パスワードが間違っていた）場合に対処するようにスイッチを設定できます。
- ACL 割り当てを使用した 802.1X 認証：ホストの 802.1X または MAB 認証中に、ACL などのホスト単位ポリシーをダウンロードして、RADIUS サーバからスイッチに URL をリダイレクトします。
- ユーザ単位 ACL とフィルタ ID ACL を使用した 802.1X 認証：サードパーティ製 AAA サーバを使用して ACL ポリシーを強制できます。
- 802.1X コンバージェンス：802.1X 設定および実装内のスイッチング ビジネス ユニット間に一貫性をもたらします。
- 802.1X プロトコル：スイッチ ポートに接続されたホストをスイッチ サービスにアクセスする前に認証するための手段を提供します。
- 802.1X RADIUS アカウンティング：ネットワーク デバイスの使用を追跡できます。
- Network Edge Access Topology（NEAT）を使用した 802.1X サプリカントおよびオーセンティケータ スイッチ：ワイヤリング クローゼット（会議室など）外の領域に識別を拡張します。NEAT は、エンドホスト（PC またはシスコ IP Phone）に対して 802.1X オーセンティケータとして動作するスイッチが保護されていない場所（ワイヤリング クローゼット外）に配置されている配置シナリオ用に設計されています。オーセンティケータ スイッチは常に信頼できるわけではありません。
- 認証失敗 VLAN 割り当てを使用した 802.1X：ポート単位で認証失敗ユーザにアクセスを提供することができます。認証失敗ユーザは、802.1X には対応できるが認証サーバ内に有効な資格情報を持たないエンド ホストか、またはユーザ側の認証ポップアップ ウィンドウでユーザ名とパスワードの組み合わせが入力されていないエンド ホストです。

- アクセス不能認証バイパスを使用した 802.1X：AAA サーバが到達不能または応答しない場合に適用されます。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。
- ポート セキュリティを使用した 802.1X：単一ホスト モードと複数ホスト モードのどちらかで 802.1X ポート上のポート セキュリティを可能にします。ポート上でポート セキュリティと 802.1X をイネーブルにすると、802.1X がポートを認証し、ポート セキュリティがそのポートで許可される MAC アドレスの数（クライアントの MAC アドレスを含む）を管理します。
- MAC 認証バイパスを使用した 802.1X：プリンタなどの 802.1X サプリカント機能のないエージェントレス デバイスへのネットワーク 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。
- RADIUS によるセッション タイムアウトを使用した 802.1X：スイッチで使用される再認証タイムアウトを、ローカルに設定されたものと RADIUS によるもののどちらにするかを指定できます。
- 単方向制御ポートを使用した 802.1X：Wake-on-LAN（WoL）マジック パケットを許可されていない 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転送できます。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信するために使用されます。
- 違反モードを使用した 802.1X：この機能により、違反に対する応答に基づいて shutdown、restrict、または replace モードのいずれかとして 802.1X セキュリティ違反動作を設定することができます。
- VLAN 割り当てを使用した 802.1X 認証：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。
- VLAN ユーザ分散を使用した 802.1X：動的に VLAN ID または VLAN 名を割り当てる方法の代替方法で、この機能は VLAN グループ名を割り当てます。これにより、複数の VLAN で同じグループに属している（かつ共通の VLAN グループ名によって特徴付けられている）ユーザを分散できます。これは通常、非常に大規模なブロードキャスト ドメインの作成を避けるために行います。
- 音声 VLAN を使用した 802.1X 認証：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。
- マルチドメイン認証：この機能により、データ デバイスと IP Phone（Cisco または Cisco 以外）などの音声デバイスの両方が、データ ドメインと音声ドメインに分割される同一スイッチ ポートで認証できるようになります。
- RADIUS 許可の変更：この機能は、RFC 5176 で定義された Change of Authorization（CoA）拡張機能をプッシュ モードで採用して、外部の認証、許可、アカウンティング（AAA）またはポリシー サーバからのセッションのダイナミック再設定ができるようにします。

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 45 章「802.1X ポートベース認証の設定」を参照してください。

Cisco TrustSec のセキュリティ アーキテクチャ

Cisco TrustSec のセキュリティ アーキテクチャは、信頼できるネットワーク デバイスのドメインを確立することによってセキュア ネットワークを構築します。ドメイン内の各デバイスは、そのピアによって認証されます。ドメイン内のデバイス間リンクでの通信は、暗号化、メッセージ整合性検査、データパス リプレイ防止メカニズムを組み合わせたセキュリティで保護されます。Cisco TrustSec は、ネットワークに入るようにセキュリティ グループ（SG）がパケットを分類するために認証中に取得したデバイスおよびユーザ クレデンシャルを使用します。このパケット分類は、Cisco TrustSec ネット

ワークへの入力時にパケットにタグ付けされることにより維持されます。タグによってパケットはデータ パス全体を通じて正しく識別され、セキュリティおよびその他のポリシー基準が適用されます。このタグは、セキュリティ グループ タグ（SGT）と呼ばれ、エンドポイント デバイスが SGT に応じてトラフィックをフィルタリングできるようにすることにより、アクセス コントロール ポリシーをネットワークに強制できます。

詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/trustsec.html

Cisco TrustSec MACsec の暗号化

（注）　® Catalyst® 4500-X シリーズ スイッチは、Cisco TrustSec® テクノロジーをサポートしますが、TrustSec MACsec の暗号化をサポートしていません。

MACsec（Media Access Control Security）は 2 台の MACsec 対応デバイス間のパケットの認証と暗号化の IEEE 802.1AE 規格です。Catalyst 4500 シリーズ スイッチは、スイッチとホスト デバイス間の暗号化に、ダウンリンク ポートでの MACsec Key Agreement（MKA）による 802.1AE 暗号化をサポートします。また、スイッチは、Cisco TrustSec ネットワーク デバイス アドミッション コントロール（NDAC）および Security Association Protocol（SAP）キー交換を使用して MACsec リンク層スイッチ間セキュリティをサポートします。リンク層セキュリティはスイッチ間のパケット認証とスイッチ間の MACsec 暗号化の両方を含みます（暗号化は任意です）。

TrustSec MACsec の暗号化の詳細については、第 44 章「MACsec の暗号化設定」を参照してください。

ダイナミック ARP インスペクション（DAI）

ダイナミック ARP インスペクション（DAI）は、すべてのアドレス解決プロトコル（ARP）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 50 章「ダイナミック ARP インスペクションの設定」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メンテナンス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 サーバの間でファイアウォールに似た役割を果たします。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。

SSO をサポートする DHCP スヌーピングは、スイッチオーバー発生時に、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 DHCP データを認識して、セキュリティのメリットが失われないように、アクティブ スーパーバイザ エンジンから冗長スーパーバイザ エンジンに DHCP スヌーピング データを伝播します。

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」の章を参照してください。

http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_dhcp_rdmp_ps6350_TSD_Products_Configuration_Guide_Chapter.html

DHCP スヌーピングの設定手順については、第 51 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 54 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、すべての Catalyst 4500 スーパーバイザ エンジンで使用できます。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。

レイヤ 2 制御パケット QoS を使用して、物理ポートまたは VLAN に着信する制御パケットをポリシングすることが可能で、これは、レイヤ 2 制御パケットに QoS を適用できます。

コントロール プレーン ポリシングおよびレイヤ 2 制御パケット QoS については、第 49 章「コントロール プレーン ポリシングおよびレイヤ 2 制御パケット QoS 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ネイバー 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 51 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。

スタティック ホスト用 IP ソース ガード

この機能により、ARP パケットを使用してスタティック 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 ホスト用 IP ソース ガード（IPSG）により、DHCP ホストおよびスタティック ホスト両方の（デバイスのトラッキング データベースと DHCP スヌーピング バインディング データベースの両方において）ポートごと MAC アドレスごとに複数のバインディングを実行できます。この機能では、制限を超えるとアクションを実行できます。

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 51 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。

IPv6 ファースト ホップ セキュリティ

（注） IPv6 ファースト ホップ セキュリティは SUP-6、SUP6L-E、4948E、SUP-7E、SUP7L-E、4500X-32 および 4500X-16 プラットフォームでサポートされます。

IPv6 FHS は、大きな L2 ドメインで見られる特定のスケーラビリティの問題に対処するため、および IPv6 対応ネットワークのリンク動作を保護するために設計された機能のセットです。

IPv6 FHS は DoS または情報の盗難になる可能性のある次のタイプの攻撃または誤設定エラーに対する有効な対策を提供します。

- ルータ偽装（MiM 攻撃）
- アドレスの盗難
- アドレス スプーフィング
- リモート アドレス解決キャッシュの枯渇（DoS 攻撃）

このような攻撃は悪意のある、あるいは誤って設定されたユーザから発生し、レイヤ 2 ドメイン内のユーザやネットワーク全般に対する重大な中断の原因となる可能性があります。

サポートされる機能は次のとおりです。

- RA Guard
- NDP インスペクション
- ND ごとのキャッシュ制限値
- IPv6 デバイス トラッキング
- DAD プロキシ
- ポートごとのアドレス制限値
- IPv6 アドレス収集

- DHCPv6 Guard
- 宛先ガード
- Lightweight DHCPv6 リレー エージェント（LDRA）

（注）　セカンダリ VLAN で IPv6 FHS を設定することはできません。プライマリ VLAN の設定からポリシーが継承されます。したがって、プライマリ VLAN で適用されるポリシーはすべて関連付けられたセカンダリ VLAN で自動的にプログラムされます。ただし、適用されるポリシーは常に VLAN レベルの設定よりも優先されます。

FHS の概要については、次の URL を参照してください。

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6553/aag_c45-707354.pdf

FHS を実装する方法の詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-4t/ip6-first-hop-security.html

ローカル認証、RADIUS、および TACACS+ 認証

ローカル認証、Remote Authentication Dial-In User Service（RADIUS; リモート認証ダイヤルイン ユーザ サービス）、および Terminal Access Controller Access Control System Plus（TACACS+; ターミナル アクセス コントローラ アクセス システム プラス）認証方式は、スイッチに対するアクセスをコントロールします。詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_cfg_authentifcn_ps6350_TSD_Products_Configuration_Guide_Chapter.html

ネットワーク アドミッション コントロール

ネットワーク アドミッション コントロールは次の 2 つの機能で構成されます。

- NAC レイヤ 2 IP 検証

  NAC レイヤ 2 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 レイヤ 2 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 ステートや 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/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.1/configuration/guide/nac_conf.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 レイヤ 2 IP と同様に、NAC レイヤ 2 802.1X 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 45 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 MAC アクセス コントロール リスト（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。

Catalyst 4500 シリーズ スイッチでは、次の 3 つの ACL タイプがサポートされています。

- TCP、User Datagram Protocol（UDP）、Internet Group Management Protocol（IGMP）、Internet Control Message Protocol（ICMP）などの IP トラフィックをフィルタリングする IP ACL
- IPv6 ACL
- イーサネット アドレスおよび EtherType に基づいて一致する MAC ACL

スイッチは、トラフィックをフィルタリングする ACL の次の用途をサポートします。

- 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。
- VLAN 間でルーテッド トラフィックのアクセスを制御するために、レイヤ 3 インターフェイスに適用されたルータ ACL。
- すべてのパケット（ブリッジド パケットおよびルーテッド パケット）のアクセスを制御するための VLAN ACL または VLAN マップ。

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 52 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（プライベート 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 48 章「ポート セキュリティの設定」を参照してください。

PPPoE 中継エージェント

アクセス スイッチにイーサネット経由で接続されているエンド ホストをサービス プロバイダー BRAS が区別するのを支援するために、PPPoE 中継エージェント（PPPoE IA）が加入者と BRAS の間に配置されます。アクセス スイッチでは、PPPoE IA により異なるユーザのイーサネット フレームに適切にタグ付けすることで加入者線識別が可能になります （タグには、いずれの加入者がスイッチおよび VLAN に接続されているかなどの特定の情報が記載されています)。ポートごと VLAN ごとにすべての PPPoE Active Discovery（PAD）メッセージをインターセプトすることによって、PPPoE IA はホストと BRAS 間のミニセキュリティ ファイアウォールとして機能します。これは、信頼できないポートから代行受信される PAD メッセージの確認、ポート単位の PAD メッセージ レート制限の実行、PAD メッセージに対する VSA タグの挿入および削除など、特定のセキュリティ機能を提供します。

PPPoE IA については、第 46 章「PPPoE 中継エージェントの設定」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 にフラッディングすると発生し、過剰なトラフィックが生み出され、ネットワーク パフォーマンスを低下させます。プロトコルスタック実装またはネットワーク設定のエラーが、ブロードキャスト ストームの原因になります。マルチキャストおよび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 Release 12.2(40) SG 以降の Catalyst 4500 シリーズ スイッチでは、ポート単位のブロードキャスト トラフィックおよびマルチキャスト トラフィックの抑制が可能です。

ブロードキャスト抑制の設定手順については、第 55 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

Unicast Reverse-path Forwarding（uRPF; ユニキャスト RPF）機能は、検証可能な送信元 IP アドレスが不足している IP パケットを廃棄することで、間違ったまたは偽造（スプーフィングされた）送信元 IP アドレスがネットワークに流れて発生する問題を軽減するのに役立ちます。uRPF が IP ルーティング テーブルと整合性の取れた有効な送信元アドレスを持つパケットだけを転送することによって、DoS 攻撃および DDoS 攻撃をそらします。これにより、お客様のネットワーク、ISP、および残りのインターネットが保護されます。uRPF をストリクト モードで使用する場合は、ルータが戻りパケットの転送に使用するインターフェイスでパケットを受信する必要があります。uRPF ストリクト 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。

ブロードキャスト抑制の設定手順については、第 35 章「uRPF の設定」を参照してください。

ユーティリティ

サポートされているユーティリティは次のとおりです。

レイヤ 2 traceroute

レイヤ 2 traceroute を使用すれば、スイッチでパケットが送信元デバイスから宛先デバイスまでの間に通過する物理パスを識別できます。レイヤ 2 traceroute は、ユニキャストの送信元および宛先 MAC アドレスのみをサポートします。

レイヤ 2 traceroute については、第 9 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

タイム ドメイン反射率計（TDR）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 9 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、次のコマンド 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。

Web ベース認証

Web ベース認証機能（別名 Web 認証プロキシ）を使用して、IEEE 802.1X サプリカントを実行していないホスト システムでエンド ユーザを認証できます。HTTP セッションを開始すると、この機能により、ホストからの入力 HTTP パケットが代行受信され、ユーザに HTML ログイン ページが送信されます。資格情報を入力します。資格情報は、Web ベース認証機能により、認証のために AAA サーバに送信されます。認証に成功した場合、Web ベース認証は、ログインの成功を示す HTML ページをホストに送信し、AAA サーバから返されたアクセス ポリシーを適用します。

Web ベース認証の詳細については、第 47 章「Web ベース認証の設定」を参照してください。

Cisco IOS 15.1(2) SG および Cisco IOS XE 3.4SG でサポートされる新規のソフトウェア機能および変更されたソフトウェア機能

このマニュアルでは、Cisco IOS Release 15.1(2) SG および Cisco IOS XE Release 3.4SG でサポートされる新規のソフトウェア機能および変更されたソフトウェア機能の一覧を示します。

BFD C ビットのサポート - RFC5882

双方向フォワーディング検出（BFD）RFC 5880 は必須のセクションおよびオプションの認証セクションがある BFD 制御パケットを定義します。BFD 制御パケットの必須セクションには、BFD の結末がコントロール プレーンに依存しているか無関係であるかを判断する 1 ビット（C ビット）があります。ピアがリモート接続の検出に対してファスト フォールオーバー機能で対応している、BGP などのクライアントは、この C ビット サポートを使用して、BGP グレースフル リスタートが BGP セッションに対する BFD ファスト フォールオーバー サポートとともにイネーブルの場合にノンストップ フォワーディング（NSF）を行うためにより確定的なメカニズムを提供します。BGP に対する BFD C ビット サポートは BGP neighbor コマンドを使用して現在サポートされています。neighbor コマンドの詳細については、次を参照してください。

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/command/irg-cr-book.html

BGP - 拡張リフレッシュ

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-1sg/irg_enhan_route_refresh.html

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/xe-3sg/irg_enhan_route_refresh.html

BGP の整合性チェッカ

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-1sg/irg-consistency-check.html

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/xe-3sg/irg-consistency-check.html

DHCP - DHCPv6 ガード

http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_dhcp/configuration/15-1sg/ip6-dhcpv6-guard.html

DHCPv6 リレー - Lightweight DHCPv6 リレー エージェント

Lightweight DHCPv6 リレー エージェント（LDRA）は、リレー エージェント情報がリンク層ブリッジング（非ルーティング）機能を実行するアクセス ノードによって挿入されるようにします。レイヤ 2 集約ネットワークでは、アクセス ノードが集約を処理する場合に、DHCPv6 サーバまたは DHCP リレー エージェントは DHCP クライアントがネットワークにどのように接続されているかを通常認識しません。LDRA は、クライアントの識別に DHCPv6 サーバによって使用されるように、インターフェイス ID オプションなどのリレー エージェント情報がアクセス ノードによって挿入されるようにします。

FTP IPv6 のサポート

http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6_nman/configuration/15-1sg/ip6-tftp-supp.html

IPSLA 4.0 - IP v6 Phase2

次のリンクでこの機能は構成されます。

http://www.cisco.com/en/US/docs/ios-xml/ios/ipsla/configuration/15-1sg/sla_dns.html

http://www.cisco.com/en/US/docs/ios-xml/ios/ipsla/configuration/15-1sg/sla_ftp.html

http://www.cisco.com/en/US/docs/ios-xml/ios/ipsla/configuration/15-1sg/sla_http.html

http://www.cisco.com/en/US/docs/ios-xml/ios/ipsla/configuration/15-1sg/sla_icmp_pathecho.html

http://www.cisco.com/en/US/docs/ios-xml/ios/ipsla/configuration/15-1sg/sla_icmp_pathjitter.html

http://www.cisco.com/en/US/docs/ios-xml/ios/ipsla/configuration/xe-3sg/sla_dns.html

http://www.cisco.com/en/US/docs/ios-xml/ios/ipsla/configuration/xe-3sg/sla_ftp.html

http://www.cisco.com/en/US/docs/ios-xml/ios/ipsla/configuration/xe-3sg/sla_http.html

http://www.cisco.com/en/US/docs/ios-xml/ios/ipsla/configuration/xe-3sg/sla_icmp_pathecho.html

http://www.cisco.com/en/US/docs/ios-xml/ios/ipsla/configuration/xe-3sg/sla_icmp_pathjitter.html

IPSLA マルチキャストのサポート

http://www.cisco.com/en/US/docs/ios-xml/ios/ipsla/configuration/15-1sg/sla_mcast_suppt.html

http://www.cisco.com/en/US/docs/ios-xml/ios/ipsla/configuration/xe-3sg/sla_mcast_suppt.html

IPv6 ネイバー ディスカバリ ネイバー インスペクション

http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6_fhsec/configuration/15-1sg/ip6-nd-inspect.html

IPv6 ネイバー ディスカバリ マルチキャスト抑制

http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6_fhsec/configuration/15-1sg/ip6-nd-mcast-supp.html

IPv6 ルータ アドバタイズメント（RA）ガード

http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6_fhsec/configuration/15-1sg/ip6-ra-guard.html

ISSU - IPv4 マルチキャスト

http://www.cisco.com/en/US/docs/ios-xml/ios/ha/configuration/15-1sg/ha-config-performing-inservice-software-upgrade.html

ISSU - IPv6 マルチキャスト

http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_resil/configuration/15-sg/imc_high_availability.html

http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_resil/configuration/xe-3sg/imc_high_availability.html

NSF/SSO - IPv6 マルチキャスト

http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_resil/configuration/15-sg/imc_high_availability.html

http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_resil/configuration/xe-3sg/imc_high_availability.html

NTPv4 MIB

http://www.cisco.com/en/US/docs/ios-xml/ios/bsm/configuration/15-1sg/bsm-ntp4-mib.html

http://www.cisco.com/en/US/docs/ios-xml/ios/bsm/configuration/xe-3sg/bsm-ntp4-mib.html

NTPv4 オーファン モードのサポート、信頼できるキー設定の範囲

http://www.cisco.com/en/US/docs/ios-xml/ios/bsm/configuration/15-1sg/bsm-time-calendar-set.html

OSPFv3 アドレス ファミリ

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/15-mt/ip6-route-ospfv3-add-fam.htmll

OSPFv3 VRF-Lite/PE-CE

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/command/iro-cr-book.html

リバース SSH 拡張

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_ssh/configuration/15-mt/sec-rev-ssh-enhanmt.html

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_ssh/configuration/xe-3sg/sec-rev-ssh-enhanmt.html

SSH バージョン 2 クライアント サポート

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_ssh/configuration/15-1mt/Secure_Shell_Version_2_Support.htmll

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_ssh/configuration/xe-3sg/sec-secure-shell-v2.html

SSH キーボード インタラクティブ認証

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_secure_shell_v2.html

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_ssh/configuration/xe-3sg/sec-secure-shell-v2.html

SSHv2 の拡張機能

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_secure_shell_v2.html

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_ssh/configuration/xe-3sg/sec-secure-shell-v2.html

RSA キーの SSHv2 拡張機能

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_secure_shell_v2.html

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_ssh/configuration/xe-3sg/sec-secure-shell-v2.html

TFTP IPv6 のサポート

http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6_nman/configuration/15-1sg/ip6-tftp-supp.html

IPv6 での OSPF の TTL セキュリティ サポート

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/xe-3sg/iro-ttl-sec-ospfv3.html

WebUI の WSMA 機能拡張

http://www.cisco.com/en/US/docs/ios-xml/ios/wsma/configuration/15-1sg/wsma.html

http://www.cisco.com/en/US/docs/ios-xml/ios/wsma/configuration/xe-3sg/wsma.html

WSMA および XML-PI の機能拡張

http://www.cisco.com/en/US/docs/ios-xml/ios/wsma/configuration/15-1sg/wsma.html

http://www.cisco.com/en/US/docs/ios-xml/ios/wsma/configuration/xe-3sg/wsma.html