アドミニストレーション ガイド

Cisco Sx250 シリーズ マネージド スイッチ、
ファームウェア リリース 2.4.x、バージョン 0.3

Table of Contents

Contents

1

クイック スタート ガイド

ここで説明する内容は次のとおりです。

作業を開始する前に

デバイス設置作業を開始する前に、次の項目を用意していることを確認してください。

- ネットワーク デバイス接続用の RJ-45 イーサネット ケーブル。10 G ポートには、カテゴリ 6a 以上のケーブルが必要です。その他すべてのポートには、カテゴリ 5e 以上のケーブルが必要です。
- スイッチ管理用のコンソール ポートを使用するためのコンソール ケーブル。
- ハードウェア設置用の工具。スイッチに同梱されているラックマウント キットには、デスクトップ配置用のゴム製の脚 4 本、ラックマウント用ブラケット 2 つ、ネジ 12 本が含まれています。付属のネジを無くしてしまった場合は、次のサイズのネジを代わりに使用してください。
  - ネジ山の直径:6.9 mm
  - ネジ山の表面から根元までの長さ:5.9 mm

- 軸径:3.94 mm

- Web ベースのインターフェイスまたはコンソール ポートを使用してスイッチを管理するために、Internet Explorer(バージョン 9.0、10.0、11.0)、Firefox(バージョン 36.0、37.0 以降)、または Chrome(バージョン 40、41、42 以降)が使えるコンピュータ。

ラックへのスイッチのマウント

スイッチは標準規格サイズの 19 インチ(約 48 cm)幅のラックにマウントできます。スイッチには高さ 1 ラック ユニット(RU)、すなわち 1.75 インチ(44.45 mm)のスペースが必要です。

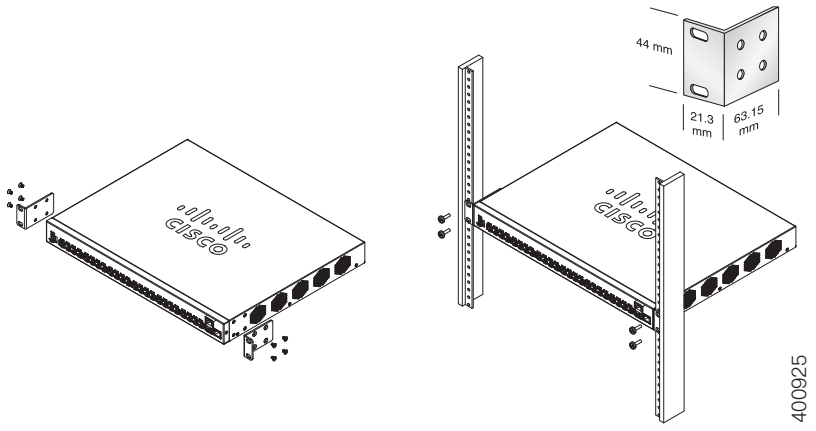
注意 安定性を確保するために、最も重いデバイスから順に下から上へとラックに載せていきます。重いデバイスをラックの一番上に載せると、不安定になり、転倒する可能性があります。

スイッチを 19 インチの標準シャーシに取り付けます。

ステップ 1 付属のブラケットの 1 つをスイッチの側面に据え、ブラケットの 4 つの穴がネジ穴と合うようにします。付属のネジを 4 本使用して固定します。

ステップ 2 前述の手順を繰り返して、スイッチの反対側に別のブラケットを取り付けます。

ステップ 3 ブラケットが確実に取り付けられたら、スイッチを標準の 19 インチ ラックに設置する準備ができました。



Power over Ethernet の考慮事項

警告　スイッチは、設備外部へのルーティングは行われない PoE ネットワークにのみ接続されるよう意図されています。

PoE をサポートしているのは一部のデバイスだけです。PoE をサポートしているモデルは次のようにモデル番号の最後に P が付きます。SF250-48HP。

PoE フィールドは、すべての関連ページにその説明がありますが、PoE をサポートしているデバイス上でのみサポートされます。

スイッチが Power over Ethernet（PoE）モデルのいずれかである場合は、次の所要電力を考慮してください。

表 1　Power Over Ethernet モデルのスイッチ

SKU 名	説明	PoE PD チップセット タイプ	PoE PSE チップセット タイプ	PoE PD AF/AT/60W	PoE PSE AF/AT/60W
SF250-24P	SF250-24P 24 ポート 10/100 PoE スマート スイッチ	なし	3*69208**M**（0x4B42）	なし	AF/AT
SF250-48HP	SF250-48HP 48 ポート 10/100 PoE スマート スイッチ	なし	6* PD69208（0x4AC2）/ 6*69208**M**（0x4B42）（2.2.7 現在）	なし	AF/AT
SG250-08HP	SG250-08HP 8 ポート ギガビット PoE スマート スイッチ	なし	1*69208**M**（0x4B42）	なし	AF/AT
SG250-10P	SG250-10P 10 ポート ギガビット PoE スマート スイッチ	2x PD70210 + 2x PD70222 + 1?x LX7309	1* PD69208（0x4AC2）/ 1*69208**M**（0x4B42）	AF/AT/60W	AF/AT
SG250-26HP	SG250-26HP 26 ポート ギガビット PoE スマート スイッチ	なし	3* PD69208（0x4AC2）/ 3*69208**M**（0x4B42）	なし	AF/AT

表 1　Power Over Ethernet モデルのスイッチ（続き）

SKU 名	説明	PoE PD チップセット タイプ	PoE PSE チップセット タイプ	PoE PD AF/AT/60W	PoE PSE AF/AT/60W
SG250-26P	SG250-26P 26 ポート ギガビット PoE スマート スイッチ	なし	3* PD69208（0x4AC2）/ 3*69208**M**（0x4B42）	なし	AF/AT
SG250-50HP	SG250-50HP 50 ポート ギガビット PoE スマート スイッチ	なし	6*69208**M**（0x4B42）	なし	AF/AT
SG250-50P	SG250-50P 50 ポート ギガビット PoE スマート スイッチ	なし	6*69208**M**（0x4B42）	なし	AF/AT
SG250X-24P	SG250X-24P 24 ポートギガビット PoE 対応および 4 ポート 10 ギガビットスマートスイッチ	NA	3*69208**M**（0x4B42）	NA	AF/AT
SG250X-48P	SG250X-48P 48 ポート ギガビット PoE 対応および 4 ポート 10 ギガビット スマート スイッチ	NA	6*69208**M**（0x4B42）	NA	AF/AT

注　60 ワット PoE は、イーサネット Plus 標準の IEEE 給電を 2 倍に拡張し、ポートごとに 60 ワットを給電します。

注意　PoE 供給能力のあるスイッチを接続するときには、次の点を考慮してください。
PoE モデルのスイッチは、接続先 PD（受電デバイス）に DC で給電可能な PSE（給電側機器）です。このようなデバイスには VoIP 電話機、IP カメラ、ワイヤレス アクセス ポイントが含まれます。PoE スイッチは、先行標準のレガシー PoE 受電デバイスを検出して給電できます。レガシー PoE のサポートが原因で、PSE として動作する PoE スイッチが（他の PoE スイッチを含む）接続先 PSE を誤ってレガシー PD として検出して給電する可能性があります。
PoE スイッチは PSE であるため AC で給電されるべきですが、誤検出により別の PSE からレガシー PD として給電される可能性があります。このような状態が発生した場合、PoE スイッチが正しく機能しない可能性があり、接続先 PD に正しく電力を供給できない場合があります。

誤検出を防ぐには、PSE への接続に使用される PoE スイッチ上のポートで PoE を無効にしてください。また、PSE デバイスを PoE スイッチに接続する前に、まず PSE デバイスに給電する必要があります。あるデバイスが PD として誤検出される場合には、そのデバイスを PoE ポートから切断し、AC 電源によって電力を再供給した後で、PoE ポートに再接続してください。

スイッチの設定

作業を開始する前に

本スイッチにアクセスして管理するには、Web ベースのインターフェイスを使用して IP ネットワーク経由で行う方法と、コンソール ポートを使用してスイッチのコマンドライン インターフェイスで行う方法の 2 つの方法があります。コンソール ポートを使用するには、ユーザに高度な知識が求められます。

次の表に、スイッチを最初に設定するときに使用されるデフォルト設定を示します。

パラメータ	デフォルト値
Username	**cisco**
Password	**cisco**
LAN IP	**192.168.1.254**

Web ベースのインターフェイスを使用したスイッチの設定

Web ベースのインターフェイスからスイッチにアクセスするには、スイッチが使用している IP アドレスを知る必要があります。スイッチは工場出荷時設定の IP アドレス 192.168.1.254 とサブネット /24 を使用します。

スイッチが工場出荷時設定の IP アドレスを使用している場合、システム LED は連続的に点滅します。DHCP サーバから割り当てられた IP アドレスをスイッチが使用している場合、または管理者がスタティック IP アドレスを設定した場合、システム LED はグリーンで点灯した状態になります（DHCP はデフォルトで有効）。

ネットワーク接続を介してスイッチを管理している場合、DHCP サーバまたは手動でスイッチの IP アドレスを変更すると、スイッチへのアクセスが失われます。Web ベースのインターフェイスを使用するためには、スイッチが使用している新しい IP アドレスをブラウザに入力する必要があります。スイッチをコンソール ポート接続で管理している場合には、リンクは維持されます。

スイッチを Web ベースのインターフェイスを使用して設定するには、次の操作を実行します。

ステップ 1 コンピュータとスイッチの電源をオンにします。

ステップ 2 Cisco 350-550 XG スイッチの場合は、コンピュータを前面パネルにある OOB ポートに接続します。その他のすべてのスイッチの場合は、コンピュータを任意のネットワーク ポートに接続します。

ステップ 3 コンピュータの IP 構成を設定します。

a. スイッチがデフォルトのスタティック IP アドレス 192.168.1.254/24 を使用している場合、コンピュータの IP アドレスに、192.168.1.2 ～ 192.168.1.253 の範囲内で未使用の IP アドレスを選択する必要があります。

b. IP アドレスが DHCP によって割り当てられる場合、DHCP サーバが実行中で、スイッチとコンピュータから接続可能であることを確認します。各デバイスが DHCP サーバから割り当てられた新しい IP アドレスを検出するために、デバイスを一旦切断して再接続することが必要な場合があります。

注 お使いのコンピュータで IP アドレスを変更する方法は、そのアーキテクチャやオペレーティング システムの種類によって異なります。お使いのコンピュータのヘルプとサポート機能を使用して「IP アドレスの設定」について検索してください。

ステップ 4 Web ブラウザ ウィンドウを開きます。デバイスに接続したときに、ActiveX プラグインをインストールするよう求められた場合は、指示に従ってプラグインのインストールを許可します。

ステップ 5 アドレスバーにスイッチの IP アドレスを入力し、Enter キーを押します。たとえば **http://192.168.1.254** です。

ステップ 6 ログイン ページが表示されたら、Web ベースのインターフェイスで使用する言語を選択して、ユーザ名とパスワードを入力します。

デフォルトのユーザ名は **cisco** です。デフォルトのパスワードは **cisco** です。ユーザ名とパスワードはどちらも大文字と小文字を区別します。

ステップ 7 [ログイン] をクリックします。

デフォルトのユーザ名とパスワードで初めてログインする場合、[パスワードの変更] ページが表示されます。新しいパスワード作成のルールがページに表示されます。

ステップ 8 新しいパスワードを入力して確認します。

注 パスワード複雑度は、デフォルトで有効になっています。パスワードは、デフォルトの複雑性ルールに準拠する必要があります。または、[パスワード強度の強制] オプションの横にある [無効] をオンにして一時的に無効にすることもできます。

ステップ 9 [適用] をクリックします。

注意 Web ベースのインターフェイスを終了する前に、[保存] アイコンをクリックして設定の変更内容を必ず保存してください。設定を保存する前に終了した場合、変更内容はすべて失われます。

[はじめに] ページが開きます。これで、スイッチを設定する準備が整いました。詳細については、『アドミニストレーション ガイド』またはヘルプ ページを参照してください。

ブラウザについての制約事項

管理ステーションで複数の IPv6 インターフェイスを使用している場合、IPv6 リンクローカル アドレスではなく IPv6 グローバル アドレスを使用して、ブラウザからデバイスにアクセスしてください。

コンソール ポートを使用したスイッチの設定

コンソール ポートを使用してスイッチを設定するには、次の操作を実行します。

ステップ 1 付属のコンソール ケーブルを使用して、コンピュータをスイッチのコンソール ポートに接続します。

ステップ 2 コンピュータで HyperTerminal などのコンソール ポート ユーティリティを実行します。

ステップ 3 次のパラメータを使用してユーティリティを設定します。

- 115200 bits per second
- 8 data bits
- no parity

- 1 stop bit
- no flow control

ステップ 4 ユーザ名とパスワードを入力します。デフォルトのユーザ名は **cisco**、デフォルトのパスワードは **cisco** です。ユーザ名とパスワードはどちらも大文字と小文字を区別します。

デフォルトのユーザ名とパスワードで初めてログインする場合、次のメッセージが表示されます。

```
Please change your password from the default settings.Please change the
password for better protection of your network.Do you want to change the
password (Y/N) [Y]?
```

ステップ 5 **Y** と入力して、新しい管理者パスワードを設定します。

注 パスワード複雑度は、デフォルトで有効になっています。パスワードは、デフォルトの複雑性ルールを満たす必要があります。

注意 終了する前に、設定の変更内容が保存されたことを確認してください。

これで、スイッチを設定する準備が整いました。ご使用のスイッチの『CLI Guide』を参照してください。

注 ネットワークで DHCP を使用していない場合、スイッチの IP アドレスのタイプを**スタティック**に設定し、スタティック IP アドレスおよびサブネット マスクを変更してネットワーク トポロジに合わせてください。そうしないと、複数のスイッチが工場出荷時設定の同じ IP アドレス 192.168.1.254 を使用することになります。

USB ポート

USB ポートは、外部ストレージ（disk-on-key）デバイスの接続に使用できます。このポートは、コンフィギュレーション、SYSLOG、およびイメージ ファイルを保持できます。USB ポートは FAT32 ファイル システムを完全にサポートし、NTFS ファイル システムを部分的に（読み取りのみ）サポートします。

相対パスと完全修飾パスの両方を使用できます。

システムは、GUI 経由の USB ポート上の次のユーザ アクションをサポートします。

- USB コンテンツの表示
- USB 経由のファイルのコピー（TFTP を使用した場合と同じ）
- USB ファイルの内容の削除、名前の変更、および表示

スイッチの機能

この項では、スイッチを習熟するためにスイッチの外観について説明します。

製品モデル

利用可能な製品モデルを次に示します。

表 2　製品モデル

SKU 名	説明
SF250-24	SF250-24 24 ポート 10/100 スマート スイッチ
SF250-24P	SF250-24P 24 ポート 10/100 PoE スマート スイッチ
SF250-48	SF250-48 48 ポート 10/100 スマート スイッチ
SF250-48HP	SF250-48HP 48 ポート 10/100 PoE スマート スイッチ
SG250-08	SG250-08 8 ポート ギガビット スマート スイッチ
SG250-08HP	SG250-08HP 8 ポート ギガビット PoE スマート スイッチ
SG250-10P	SG250-10P 10 ポート ギガビット PoE スマート スイッチ
SG250-18	SG250-18 18 ポート ギガビット スマート スイッチ
SG250-26	SG250-26 26 ポート ギガビット スマート スイッチ

表 2　製品モデル(続き)

SKU 名	説明
SG250-26HP	SG250-26HP 26 ポート ギガビット PoE スマート スイッチ
SG250-26P	SG250-26P 26 ポート ギガビット PoE スマート スイッチ
SG250-50	SG250-50 50 ポート ギガビット スマート スイッチ
SG250-50HP	SG250-50HP 50 ポート ギガビット PoE スマート スイッチ
SG250-50P	SG250-50P 50 ポート ギガビット PoE スマート スイッチ
SG250X-24	SG250X-24 24 ポートギガビットおよび 4 ポート 10 ギガビット スマート スイッチ
SG250X-24P	SG250X-24P 24 ポートギガビット PoE 対応および 4 ポート 10 ギガビット スマート スイッチ
SG250X-48	SG250X-48 48 ポート ギガビットおよび 4 ポート 10 ギガビット スマート スイッチ
SG250X-48P	SG250X-48P 48 ポート ギガビット PoE 対応および 4 ポート 10 ギガビット スマート スイッチ

前面パネル

ポート、LED、およびリセット ボタンは、以下の図に示すようにスイッチの前面パネルに配置されています。すべての SKU が下に表示されるわけではありません。代表的なグループが表示されています。

TBD

SF240_24P

SG250-10P

デバイスの前面パネルに配置されているコンポーネントを次に示します。

- USB ポート：USB ポートはスイッチと USB デバイスを接続します。これにより、接続した USB デバイスを利用して、コンフィギュレーション ファイル、ファームウェア イメージ、および Syslog ファイルの保存と復元が可能になります。
- RJ-45 イーサネット ポート：RJ-45 イーサネット ポートを使用して、コンピュータ、プリンタ、アクセス ポイントなどのネットワーク デバイスをスイッチに接続します。
- Multigigabit Ethernet Ports：（青色で強調）これらのポートは Cat 5e ケーブルで 100 Mbps、1 Gbps、および 2.5 Gbps のスピードをサポートします。全世界で導入されているケーブルの多くは、100 m で 1 Gbps に制限されています。Cisco Multigigabit Ethernet により、ケーブルを交換しなくても、同じインフラストラクチャ上で最大 2.5 Gbps のスピードが可能になります。
- 60 ワット PoE ポート：黄色で示されています。60 ワット PoE ポートは PoE 給電を 2 倍に拡張し、60 ワットを給電します。250 デバイスと SF350-48P デバイスには装備されていません。

- SFP+ ポート（存在する場合）：Small Form-Factor Pluggable Plus（SFP+）は、スイッチを他のスイッチとリンクするためのモジュール用の接続ポイントです。これらのポートは一般に、ミニ 10 ギガビット インターフェイス コンバータ ポートとも呼ばれます。このガイドでは SFP+ という用語を使います。
- SFP+ ポートは、シスコの SFP 1G 光モジュール（MGBSX1、MGBLH1、MGBT1）に加えて、他社ブランドのモジュールとも互換性があります。
- シスコ スイッチでサポートされている Cisco SFP+ 10 G 光ファイバ モジュールは次のとおりです。SFP-10G-SR、SFP-10G-LR、SFP-10G-SR-S、および SFP-10G-LR-S。
- シスコ スイッチでサポートされている、スタック構成用の Cisco SFP+ 銅ケーブル モジュールは次のとおりです。SFP-H10GB-CU1M、SFP-H10GB-CU3M、および SFP-H10GB-CU5M。
- SFP+ ポートは、コンビネーション ポートとなっており、もう 1 つの RJ-45 ポートと共有されます。SFP+ がアクティブな場合、隣接した RJ-45 ポートは無効になります。
- 一部の SFP インターフェイスは、コンボ ポートと呼ばれる、もう 1 つの RJ-45 ポートと共有されます。SFP がアクティブな場合、隣接した RJ-45 ポートは無効になります。
- 対応する RJ-45 ポートの LED は、SFP インターフェイスのトラフィックに応答するとグリーンで点灯します。
- OOB ポート（存在する場合）：OOB（Out of Band）ポートは、管理インターフェイスとしてのみ使用できる CPU のイーサネット ポートです。OOB ポートとインバンド レイヤ 2 インターフェイス間のブリッジングはサポートされていません。これは 250 デバイスにはありません。

前面パネル LED

デバイスには次のグローバル LED が装備されています。

- Master：（グリーン）この LED は、スイッチがスタック マスターであるときに点灯します。
- System：（グリーン）この LED はスイッチの電源がオンになると点灯し、ブート中、セルフテストの実行中、または IP アドレスの取得中は点滅します。LED がグリーンで点滅する場合、スイッチでハードウェア障害、ファームウェア障害、またはコンフィギュレーション ファイルのエラーが検出されています。
- Stack ID：（グリーン）スイッチがスタック構成のとき、スタック ID に対応する番号の LED が点灯します。

ポート LED は以下のとおりです。

- LINK/ACT:(グリーン)各ポートの左側に配置されています。この LED は、対応するポートと別のデバイス間のリンクが検出されると点灯し、ポートがトラフィックを渡している間は点滅します。
- XG:(グリーン)10 G ポートの右側に配置されています。この LED は、別のデバイスがこのポートに接続されていて、電源がオンになっており、かつデバイス間で 10 Gbps のリンクが確立されているときに点灯します。LED が消灯している場合は、接続速度が 10 Gbps を下回っているか、ポートに何も接続されていないかのいずれかです。
- Gigabit:(グリーン) OOB ポートの右側に配置されています。この LED は、別のデバイスがポートに接続されていて、電源がオンになっており、かつデバイス間で 1000 Mbps のリンクが確立されているときに点灯します。LED が消灯している場合は、接続速度が 1000 Mbps を下回っているか、ポートに何も接続されていないかのいずれかです。
- SFP+(存在する場合):(グリーン)10 G ポートの右側に配置されています。この LED は、共有ポートを介して接続されていると点灯し、ポートがトラフィックを渡している間は点滅します。
- PoE(存在する場合):(オレンジ)ポートの右側に配置されています。この LED が点灯している場合、対応するポートに接続されたデバイスに電力が供給されていることを示します。

リセット ボタン

スイッチの前面パネルのリセットボタンの開口部に、ピンまたはペーパー クリップを挿入することにより、スイッチをリセットできます。リセット ボタンを使用して、スイッチを再起動またはリセットするには、次の手順に従います。

- スイッチを再起動するには、リセット ボタンを 10 秒未満押し続けます。
- スイッチを工場出荷時設定に復元するには、次の手順に従います。
  - ネットワークからスイッチを切断するか、ネットワーク上のすべての DHCP サーバを無効にします。
  - 電源を投入して、リセット ボタンを 10 秒以上押し続けます。

背面パネル

背面パネルには次のボタンがあります。

- 電源:スイッチを AC 電源に接続します。
- コンソール:シリアル ケーブルをコンピュータのシリアル ポートに接続し、端末エミュレーション プログラムを使用して設定できるようにします。

2

一般情報

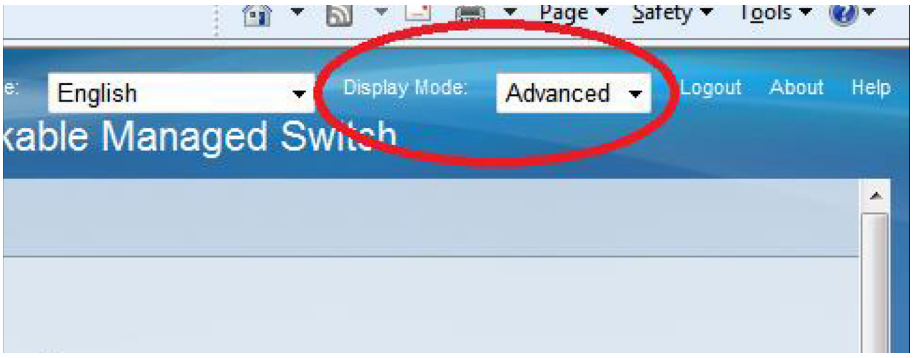
ここで説明する内容は次のとおりです。

基本表示モードと拡張表示モード

製品はさまざまな機能をサポートしているため、WEB GUI には何百もの設定ページと表示ページが含まれています。これらのページは次の表示モードに分割されています。

- [基本]:コンフィギュレーション オプションの基本サブセットが使用可能です。コンフィギュレーション オプションのいずれかが不足している場合は、デバイス ヘッダーで [拡張] モードを選択します。
- [拡張]:コンフィギュレーション オプションがすべて使用可能です。

下の図のように、モード間を移動します。



ユーザが基本から拡張に切り替えると、ブラウザでページがリロードされます。ただし、リロード後は、ユーザは同じページに留まります。

ユーザが拡張から基本に切り替えると、ブラウザでページがリロードされます。ページが基本モードでも存在する場合は、ユーザが同じページに留まります。ページが基本モードでは存在しない場合は、ブラウザでユーザが使用していたフォルダの最初のページがロードされます。フォルダが存在しない場合は、[はじめに] ページが表示されます。

拡張コンフィギュレーションが存在し、ページが基本モードでロードされる場合は、ページ レベルのメッセージがユーザに表示されます（たとえば、2 台の RADIUS サーバが設定されていても、基本モードでは 1 台のサーバしか表示できません。また、802.1X 認証に時間範囲が設定されていても、基本モードでは時間範囲を表示できません）。

モードを切り替えると、ページ上で行われたすべての設定（適用なし）が削除されます。

クイック スタート デバイス設定

クイック初期セットアップは、「VLAN 設定ウィザード」で説明されている設定ウィザードを使用するか、[はじめに] ページのリンクを使用して次のように実行できます。

カテゴリ	リンク名（ページ上）	リンク ページ
初期セットアップ	管理アプリケーションおよびサービスの変更	TCP/UDP サービス
	デバイス IP アドレスの変更	IPv4 インターフェイス
	VLAN の作成	VLAN 設定
	ポート設定	ポート設定
デバイス ステータス	システム サマリー	システムの要約
	ポート統計情報	インターフェイス
	RMON 統計情報	統計情報
	ログの表示	RAM メモリ
クイック アクセス	デバイス パスワードの変更	ユーザ アカウント

カテゴリ	リンク名（ページ上）	リンク ページ
	デバイス ソフトウェアのアップグレード	ファームウェア操作
	デバイス コンフィギュレーションのバックアップ	ファイル操作
	MAC ベース ACL の作成	MAC ベース ACL の作成
	IP ベース ACL の作成	IPv4 ベース ACL の作成
	QoS の設定	QoS プロパティ
	SPAN の設定	スイッチド ポート アナライザ（SPAN）

[はじめに] ページには、シスコの Web ページに移動する 2 つのホット リンクが用意されています。[サポート] リンクをクリックすると、デバイスの製品サポート ページに移動します。[フォーラム] リンクをクリックすると、[サポート コミュニティ] ページに移動します。

インターフェイス命名規則

GUI 内で、インターフェイスは次の要素を連結して表示されます。

- **インターフェイスのタイプ:** 次のタイプのインターフェイスは、さまざまなタイプのデバイスに存在します。
  - **ファスト イーサネット（10/100 ビット）:FE** と表示されます。
  - **ギガビット イーサネット ポート（10/100/1000 ビット）:GE** と表示されます。
  - **アウトオブバンド ポート:OOB** と表示されます。
  - **LAG（ポート チャネル）:LAG** と表示されます。
  - **VLAN:VLAN** と表示されます。
  - **トンネル:Tunnel** と表示されます。
- **インターフェイス番号:** ポート、LAG、トンネル、または VLAN ID。

ウィンドウ ナビゲーション

ここでは、Web ベースのスイッチ設定ユーティリティの機能を説明します。

アプリケーション ヘッダー

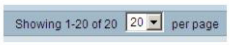
各ページにアプリケーション ヘッダーが表示されます。次のアプリケーション リンクが含まれています。

アプリケーション リンク名	説明
	[保存] アプリケーション リンクの左側にある赤く点滅する X アイコンは、実行コンフィギュレーションの変更がまだスタートアップ コンフィギュレーション ファイルに保存されていないことを示しています。赤い X アイコンの点滅は、[コンフィギュレーションのコピー/保存] ページで無効にできます。 [コンフィギュレーションのコピー/保存] ページを表示するには、[保存] をクリックします。デバイスのスタートアップ コンフィギュレーション ファイル タイプに実行コンフィギュレーション ファイルをコピーして、保存します。この保存の後は、赤い X アイコンと [保存] アプリケーション リンクは表示されなくなります。デバイスをリブートすると、スタートアップ コンフィギュレーション ファイル タイプが実行コンフィギュレーションにコピーされ、実行コンフィギュレーション内のデータに従ってデバイス パラメータが設定されます。
[ユーザ名]	デバイスにログインしているユーザの名前が表示されます。デフォルトのユーザ名は **cisco** です。(デフォルトのパスワードは **cisco** です)。
[ホスト名]	[システム設定] ページで割り当てられたホスト名を表示します。ホスト名の長さが 20 文字を超えている場合は、最初の 20 文字とその後に省略記号(...)が表示されます。切り捨てられたホスト名にカーソルを合わせると、完全なホスト名を示すツールチップが表示されます。

アプリケーション リンク名	説明
[言語メニュー]	このメニューには、次のオプションがあります。 • [言語の選択]: メニューに表示される言語の中から 1 つ選択します。この言語は、Web ベースの設定ユーティリティの言語になります。 • [言語のダウンロード]:デバイスに新しい言語を追加します。 注 言語ファイルをアップグレードするには、[ファームウェア/言語のアップグレード/バックアップ] ページを使用します。
[ログアウト]	クリックすると、Web ベースのスイッチ設定ユーティリティからログアウトします。
[バージョン情報]	クリックすると、デバイス名とデバイスのバージョン番号が表示されます。
[ヘルプ]	クリックすると、オンライン ヘルプが表示されます。
	重大度のレベルが [重要] より高い SYSLOG メッセージが記録されると、SYSLOG アラート ステータス アイコンが表示されます。[RAM メモリ] ページを開くには、このアイコンをクリックします。このページにアクセスした後は、SYSLOG アラート ステータス アイコンは表示されなくなります。アクティブな SYSLOG メッセージがない場合にこのページを表示するには、[ステータスと統計情報] > [ログの表示] > [RAM メモリ] の順にクリックします。

管理ボタン

システムのさまざまなページに表示され、よく使用されるボタンを次の表に示します。

ボタン名	説明
	プルダウン メニューを使用して、ページごとにエントリ数を設定します。
	必須フィールドを示します。
[追加]	クリックすると、関連する [追加] ページが表示され、テーブルにエントリを追加できます。情報を入力し、[適用] をクリックして、実行コンフィギュレーションに保存します。[閉じる] をクリックし、メインページに戻ります。[コンフィギュレーションのコピー/保存] ページを表示して、デバイスのスタートアップ コンフィギュレーション ファイル タイプに実行コンフィギュレーションを保存するには、[保存] をクリックします。
[適用]	クリックすると、変更がデバイスの実行コンフィギュレーションに適用されます。デバイスを再起動すると、実行コンフィギュレーションは、スタートアップ コンフィギュレーション ファイル タイプか別のファイル タイプに保存していない限り、失われます。[コンフィギュレーションのコピー/保存] ページを表示して、デバイスのスタートアップ コンフィギュレーション ファイル タイプに実行コンフィギュレーションを保存するには、[保存] をクリックします。
[キャンセル]	クリックすると、ページ上で行われた変更がリセットされます。
[クリア]	ページ上の情報をクリアします。
[フィルタのクリア]	クリックすると、表示される情報を選択するためのフィルタがクリアされます。
[すべてのインターフェイスカウンタのクリア]	クリックすると、すべてのインターフェイスの統計情報カウンタがクリアされます。

ボタン名	説明
[インターフェイス カウンタのクリア]	クリックすると、選択したインターフェイスの統計情報カウンタがクリアされます。
[ログのクリア]	ログ ファイルをクリアします。
[テーブルのクリア]	テーブル エントリをクリアします。
[閉じる]	メインページに戻ります。実行コンフィギュレーションに適用されていない変更があった場合、メッセージが表示されます。
[設定のコピー]	テーブルには、通常、コンフィギュレーション設定を含む 1 つ以上のエントリが含まれます。各エントリを個別に変更するのではなく、次のように、1 つのエントリを変更し、そのエントリを選択して複数のエントリにコピーすることができます。 1. コピーするエントリを選択します。[設定のコピー] をクリックすると、ポップアップが表示されます。 2. [コピー先] フィールドに宛先エントリ番号を入力します。 3. 変更を保存するには、[適用] をクリックします。メインページに戻るには、[閉じる] をクリックします。
[削除]	テーブルのエントリを選択して [削除] をクリックすると、そのエントリが削除されます。
[詳細]	クリックすると、選択したエントリに関連付けられている詳細が表示されます。
[編集]	エントリを選択し、[編集] をクリックします。[編集] ページが表示され、エントリを変更できます。 1. [適用] をクリックし、実行コンフィギュレーションに変更を保存します。 2. [閉じる] をクリックし、メインページに戻ります。
[実行]	クエリ フィルタリング条件を入力し、[実行] をクリックします。ページに結果が表示されます。
[更新]	[更新] をクリックすると、カウンタ値が更新されます。
[テスト]	[テスト] をクリックすると、関連するテストが実行されます。

ボタン名	説明
[デフォルトの復元]	工場出荷時のデフォルトを復元する場合に、[デフォルトに戻す] をクリックします。
[デフォルトの取り消し（Cancel Defaults）]	工場出荷時のデフォルトを復元する場合に、[デフォルトの取り消し（Cancel Defaults）] をクリックします。

検索ファシリティ

検索機能によって、関連する GUI ページを容易に特定することができます。

キーワードの検索結果には、関連するページへのリンクだけでなく、関連するヘルプページへのリンクも表示されます。

検索機能にアクセスするには、キーワードを入力して、虫めがねアイコンをクリックします。

3

ダッシュボード

ダッシュボードは 8 個の四角形の集合で、初めは空ですが、さまざまなタイプの情報を入力できます

使用可能なモジュールからモジュールを選択し、グリッドに配置できます。現在表示されているモジュールの設定をカスタマイズすることもできます。

ダッシュボードを読み込むと、ダッシュボードに選択したモジュールがグリッドの所定の場所に読み込まれます。モジュールのデータは、モジュールのタイプに応じた間隔で定期的に更新されます。モジュールによっては、この間隔を設定することができます。

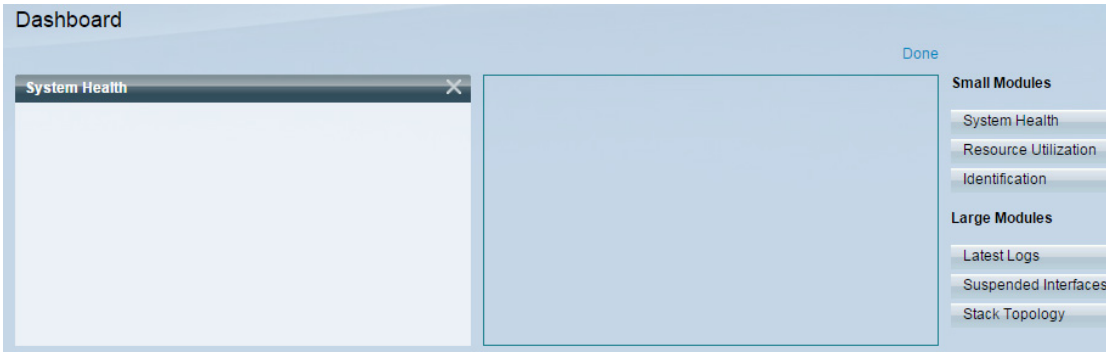
この章では以下のトピックを取り上げます。

- グリッド管理
- システム ヘルス
- リソース使用率
- 識別
- ポート使用率
- PoE 使用率
- 最新のログ
- 一時停止されたインターフェイス
- トラフィック エラー

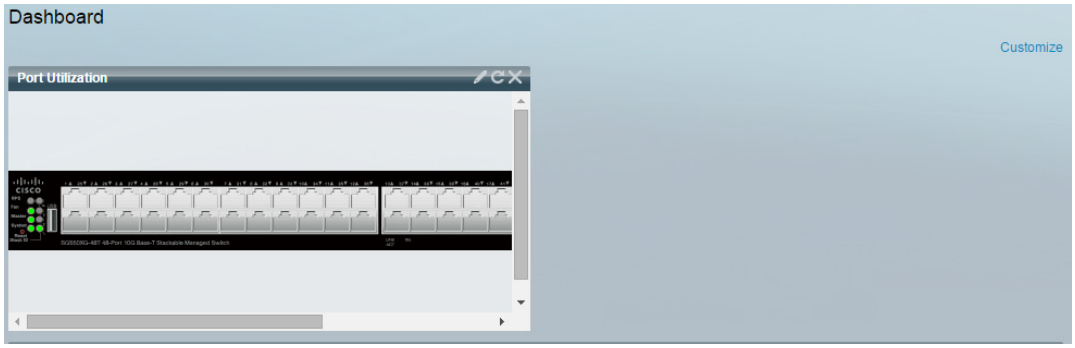
グリッド管理

ダッシュボードは複数のモジュールで構成されますが、同時に表示できるのは 1 つのモジュールのサブセットだけです。

ダッシュボードを開くと、グリッドのワイヤ フレーム ビューが表示されます（下図参照（下のスクリーン キャプチャでは 2 つの四角形だけ表示 ））。



現在非表示になっているモジュールを表示するには、ダッシュボードの右上にある [カスタマイズ] をクリックします（下図参照）。



右側にあるモジュールのリストからモジュールを選択し、グリッド内の任意のスペースにドラッグ アンド ドロップして、グリッドにモジュールを追加します。

モジュールは次のグループに分かれています。

- **スモール モジュール**は 1 つの四角形を占有するモジュールです。
- **ラージ モジュール**は 2 つの四角形を占有するモジュールです。

現在占有されているスペースにモジュールをドラッグすると、新しいモジュールが古いモジュールに置き換わります。

グリッド内のモジュールの配置を再調整するには、使用しているグリッド位置から別の位置へドラッグします。このモジュールは、未使用の場所にドロップすることも、同じサイズのモジュールによって使用されている場所にドロップすることもできます。選択した場所が使用済みの場合、モジュールの位置が入れ替わります。

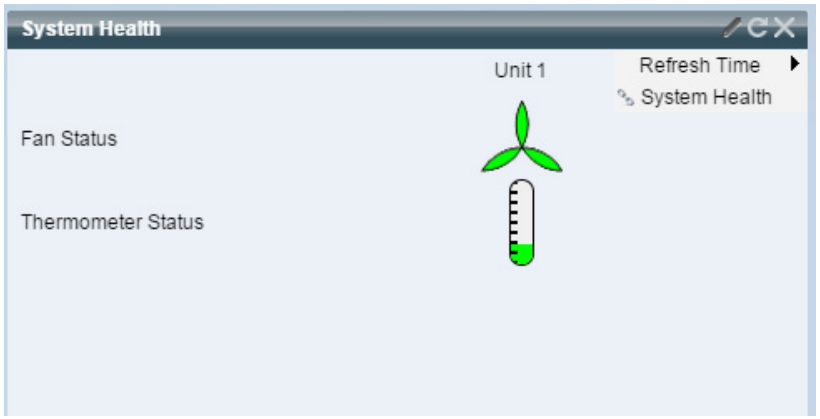
右隅にある [完了] をクリックした場合にだけ、関連する情報がモジュールに読み込まれますダッシュボードに含まれる各モジュールのタイトル バーには、モジュールのタイトルと 3 つのボタンが表示されます。

これらのボタンの機能は次のとおりです。

- 鉛筆 :コンフィギュレーション オプション(モジュールによって異なる)を開きます。
- 更新 :情報を更新します。
- X:モジュールをダッシュボードから削除します。

システム ヘルス

このモジュールは、スタンドアロン デバイスのデバイス温度(そのような情報が入手可能な場合)を表示します。(下図参照)。



次のアイコンが表示されます。

- [ファンステータス]:1 つのファンが故障し、冗長ファンでバックアップされている場合は黄色。ファンが動作中の場合は緑色。ファンが故障している場合は赤色。
- [温度計ステータス]
  - *適正温度*:緑色(温度計の目盛:ほぼ 0)。
  - *警告発生温度*:黄色(温度計の目盛:半分)。
  - *危険温度*:赤色(温度計の目盛:最大)。

次のコンフィギュレーション オプション(右上の鉛筆アイコン)が使用可能です。

- [リフレッシュ時間]:表示されたオプションのいずれかを選択します。

リソース使用率

このモジュールには、さまざまなシステム リソースの利用状況がパーセント表示の横棒グラフ形式で表示されます、次のリソースを監視できます。

- [マルチキャストグループ]:定義可能な上限数に対する、実際に存在するマルチキャスト グループのパーセンテージ。
- [MAC アドレス テーブル]:使用中の MAC アドレス テーブルのパーセンテージ。
- [TCAM]:QoS エントリと ACL エントリによる TCAM の使用率。
- [CPU]:CPU の使用率。

リソース使用率が 80 % を超えると、その横棒が赤色になります。

横棒上にカーソルをポイントすると、使用率の数値情報(使用済みリソース/最大使用可能リソース)を表すツールチップが表示されます。

次のコンフィギュレーション オプション(右隅)が使用可能です。

- [リフレッシュ時間]:表示されたオプションのいずれかを選択します。
- [マルチキャストグループ]:クリックすると [MAC グループ アドレス] が開きます。
- [MAC アドレステーブル]:クリックすると [ダイナミック アドレス] が開きます。
- [TCAM 使用率情報]:クリックすると [ハードウェア リソース使用率] が開きます。
- [CPU 使用率情報]:クリックすると [CPU 利用率] が開きます。

識別

このモジュールには、デバイス（下図参照）に関する基本情報が表示されます。

次のフィールドが表示されます。

- [システムの説明]：デバイスの説明を表示します。
- [ホスト名]：[システム設定] ページで入力した情報かデフォルトの情報が使用されます。[開始ウィザード] で追加することもできます。
- [ファームウェア バージョン]：デバイス上で実行している現在のファームウェア バージョン。
- [MAC アドレス]：デバイスの MAC アドレス。
- [シリアル番号]：デバイスのシリアル番号。
- [システム ロケーション]：デバイスの物理的な場所を入力します。
- [システム コンタクト先]：連絡先の担当者名を入力します。
- [総有効電力]：デバイスに使用可能な電力量。
- [現在の電力消費量]：デバイスで消費される電力量。

次のコンフィギュレーション オプション（右隅）が使用可能です。

- [リフレッシュ時間]：表示されたオプションのいずれかを選択します。
- [システム設定]：クリックすると [システム設定] が開きます。
- [システムの要約]：クリックすると [システムの要約] が開きます。

ポート使用率

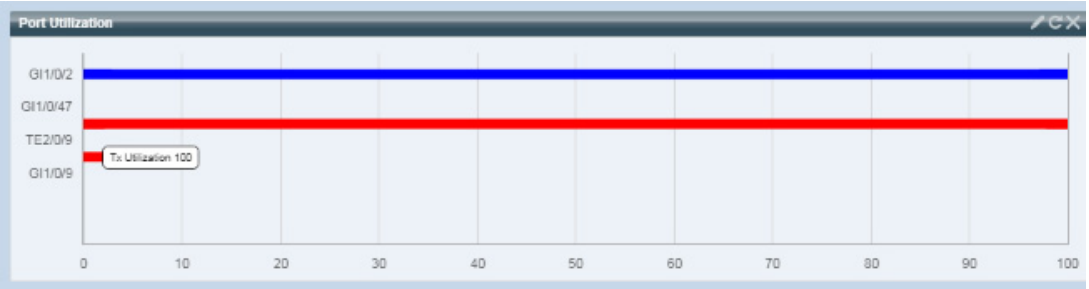
このモジュールには、デバイス上のポートがデバイス ビューまたはチャート ビューのどちらかで表示されます。ビューはコンフィギュレーション オプション（右上の鉛筆アイコン）で選択されます。

- **表示モード - デバイス ビュー**

  デバイスが表示されます。ポートにマウスを合わせるとそのポートに関する情報が表示されます。

- **表示モード - チャート ビュー**

  ポートのリストが表示されます。ポート使用率がバー形式で表示されます。



  ポートごとに、以下のポート使用率情報が表示されます。

  送信—%（赤色）

  受信—%（青色）

- [リフレッシュ時間]：表示されたオプションのいずれかを選択します。
- [インターフェイスの統計情報]：[ステータスと統計情報] > [インターフェイス] ページへのリンク。

PoE 使用率

このモジュールには、次の図のように、PoE の利用状況がグラフィック形式で表示されます。(下図参照)。

このモジュールには 0 ～ 100 の値のダイヤルが付いたゲージが表示されます。ダイヤルのトラップしきい値から 100 までの範囲は赤色です。計器の中央に、実際の PoE 使用率がワット単位で表示されます。

それぞれの横棒は、デバイスの PoE 使用率を 0 ～ 100 の範囲で表します。PoE 使用率がトラップしきい値を超えると、横棒が赤色になります。それ以外の場合、横棒は緑色です。

横棒上にカーソルをポイントすると、そのデバイスの実際の PoE 使用率をワット単位で表すツールチップが表示されます。

追加のビューはコンフィギュレーション オプション(右上の鉛筆アイコン)で選択できます。

- [リフレッシュ時間]:表示されたオプションのいずれかを選択します。
- [PoE グローバル プロパティ]:[ポート管理] -> [PoE] -> [プロパティ] ページへのリンク。
- [PoE ポート設定]:[ポート管理] -> [PoE] -> [設定] ページへのリンク。

最新のログ

このモジュールには、システムにより SYSLOG としてログに書き込まれた、最新の 5 つのイベントに関する情報が表示されます（下図参照）。

次のコンフィギュレーション オプション（右隅）が使用可能です。

- [重大度しきい値]:「ログ設定」を参照。
- [リフレッシュ時間]: 表示されたオプションのいずれかを選択します。
- [ログの表示]: クリックすると [RAM メモリ] が開きます。

注　詳細については、「ログの表示」を参照してください。

一時停止されたインターフェイス

このモジュールには、中断されたインターフェイスがデバイス ビューまたはテーブル ビューのどちらかで表示されます。ビューはコンフィギュレーション オプション（右上の鉛筆アイコン）で選択されます。

- **デバイス ビュー**

  このビューには、デバイスが表示されます。下図を参照してください。

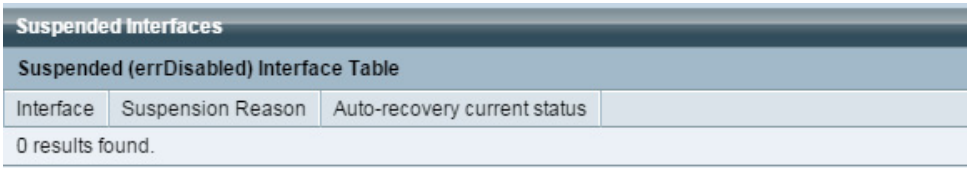
  デバイス内の中断されたポートすべてが赤色で表示されます。

中断されたポートにカーソルをポイントすると、次の情報を含むツールチップが表示されます。

- ポート名。
- ポートが LAG のメンバーである場合、ポートの LAG ID。
- 中断されている場合は、保留理由。

- **テーブル ビュー**

  情報が表形式で表示されます（下図参照）。



  次のフィールドが表示されます。

  - [インターフェイス]: 中断されたポートまたは LAG
  - [保留理由]: インターフェイスが中断された理由
  - [現在のステータスの自動修復]: 中断の原因となった機能に対して自動修復が有効になっているかどうか。

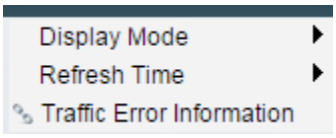
次のコンフィギュレーション オプション（右隅）が使用可能です。

- [表示モード]:[デバイスビュー] または [テーブルビュー] のどちらかを選択します。
- [リフレッシュ時間]: 表示されたオプションのいずれかを選択します。
- [エラー復旧設定]: クリックすると [エラー回復設定] が開きます。

トラフィック エラー

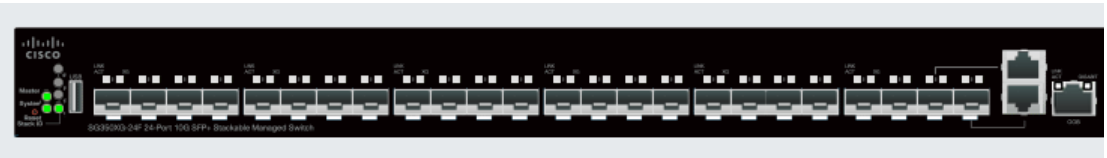
このモジュールには、RMON 統計情報に関してカウントされたさまざまなタイプのエラー パケットの数が表示されます。ビューはコンフィギュレーション オプション（右上の鉛筆アイコン）で選択されます。

鉛筆アイコンから次を選択できます。



- **表示モード - デバイス ビュー**

  デバイス モジュール モードの場合、デバイスのダイアグラムが表示されます（下図参照）。



  デバイス内の中断されたポートすべてが赤色で表示されます。

  中断されたポートにカーソルをポイントすると、次の情報を含むツールチップが表示されます。

  - ポート名。
  - ポートが LAG のメンバーである場合、ポートの LAG ID。
  - ポート上でログに書き込まれた最新のエラーの詳細情報。

- **表示モード - テーブル ビュー**

  - [インターフェイス]：ポートの名前。
  - [最後のトラフィック エラー]：ポート上で発生したトラフィック エラーとエラーが発生した最後の時刻。

- [リフレッシュ時間]：いずれかのリフレッシュレートを選択します。
- [トラフィックエラー情報]：リンクをクリックすると、[統計情報] ページが開きます。

4

設定ウィザード

ここでは、次の設定ウィザードについて説明します。

具体的な内容は、次のとおりです。

- 開始ウィザード
- VLAN 設定ウィザード
- ACL ウィザード

開始ウィザード

このウィザードは、デバイスの初期設定を支援します。

ステップ 1 [設定ウィザード] > [開始ウィザード] の順にクリックします。

ステップ 2 [ウィザードを起動] をクリックしてから、[次へ] をクリックします。

ステップ 3 次のフィールドを入力します。

- [システム ロケーション]:デバイスの物理的な場所を入力します。
- [システム コンタクト先]:連絡先の担当者名を入力します。
- [ホスト名]:このデバイスのホスト名を選択します。これは CLI コマンドのプロンプトで使用されます。
  - [デフォルトを使用]:これらのスイッチのデフォルト ホスト名(システム名)は、*switch123456* で、123456 は 16 進数のデバイス MAC アドレスの下位 3 バイトになります。
  - [ユーザ定義]:ホスト名を入力します。文字、数字、およびハイフンのみ使用できます。ホスト名の開始または終了はハイフンにできません。その他の記号、句読点、ブランクも使用できません(RFC1033、1034、1035 の規定により)。

ステップ 4 [次へ] をクリックします。

ステップ 5 次のフィールドを入力します。

- [インターフェイス]:システムの IP インターフェイスを選択します。
- [送信元 IP インターフェイス]:次のいずれかのオプションを選択します。
  - [DHCP]:デバイスが DHCP サーバから IP アドレスを受信する場合に選択します。
  - [スタティック]:デバイスの IP アドレスを手動で入力する場合に選択します。

[送信元 IP インターフェイス] として [スタティック] を選択した場合は、次のフィールドに値を入力します。

- [IP アドレス]:インターフェイスの IP アドレス。
- [ネットワークマスク]:このアドレスの IP マスク。
- [管理デフォルトゲートウェイ]:デフォルト ゲートウェイの IP アドレスを入力します。
- [DNS サーバ]:DNS サーバの IP アドレスを入力します。

ステップ 6 [次へ] をクリックします。

ステップ 7 次のフィールドを入力します。

- [ユーザ名]:1 ～ 20 文字の新しいユーザ名を入力します。UTF-8 文字は使用できません。
- [パスワード]:パスワードを入力します(UTF-8 文字は使用できません)。パスワードの強度と複雑度が定義されている場合、ユーザ パスワードは、パスワード強度で設定されたポリシーに従う必要があります。
- [パスワードの確認]:パスワードを再び入力します。
- [パスワード強度]:パスワードの強度が表示されます。パスワードの強度と複雑度に関するポリシーは、[パスワード強度] ページで設定します。
- [現在のユーザ名とパスワードを維持する]:現在のユーザ名とパスワードを維持する場合に選択します。

ステップ 8 [次へ] をクリックします。

ステップ 9 次のフィールドを入力します。

- [クロックソース]:次のいずれかのオプションを選択します。
  - [手動設定]:デバイス システム時刻を入力する場合に選択します。これを選択した場合、[日付] と [時刻] を入力します。

- [デフォルトSNTP サーバ]:デフォルト SNTP サーバを使用する場合に選択します。

注 デフォルト SNTP サーバは名前で定義されるため、DNS を設定して動作可能にする必要があります(DNS サーバを設定して到達可能にする)。これは、[DNS 設定] で行います。

- [手動 SNTP サーバ]:SNTP サーバの IP アドレスを入力する場合に選択します。

ステップ 10 [次へ] をクリックして、入力したコンフィギュレーションの概要を表示します。

ステップ 11 [適用] をクリックして、構成データを保存します。

VLAN 設定ウィザード

このウィザードは、VLAN の設定を支援します。このウィザードを実行するたびに、単一の VLAN 上でポート メンバーシップを設定できます。最初のステップは、トランク ポート モード(タグ付きとタグなしのトランク ポートを設定する)が対象で、その後で、アクセス ポート モードを設定します。

ステップ 1 [設定ウィザード] > [VLAN 設定ウィザード] の順にクリックします。

ステップ 2 [ウィザードを起動] をクリックしてから、[次へ] をクリックします。

ステップ 3 トランク ポートとして設定するポートを選択します(グラフ表示内の必要なポートをクリックすることによって)。すでにトランク ポートとして設定されているポートが事前に選択されます。

ステップ 4 [次へ] をクリックします。

ステップ 5 次のフィールドを入力します。

- [VLAN ID]:設定する VLAN を選択します。既存の VLAN または**新しい VLAN** を選択できます。
- [新しい VLAN ID]:新しい VLAN の VLAN ID を入力します。
- [VLAN 名]:オプションで、VLAN 名を入力します。

ステップ 6 VLAN のタグなしメンバーとして設定するトランク ポートを選択します(グラフ表示内の必要なポートをクリックすることによって)。このステップで選択されなかったトランク ポートは、VLAN のタグ付きメンバーになります。

ステップ 7 [次へ] をクリックします。

ステップ 8 VLAN のアクセス ポートにするポートを選択します。VLAN のアクセス ポートは、VLAN のタグなしメンバーです(グラフ表示内の必要なポートをクリックすることによって)。

ステップ 9 [次へ] をクリックして、入力した情報の概要を表示します。

ステップ 10 [適用] をクリックします。

ACL ウィザード

新しい ACL を作成するには、次のようにします。

ステップ 1 [設定ウィザード] > [ACLウィザード] の順にクリックします。

ステップ 2 [次へ] をクリックします。

ステップ 3 次のフィールドを入力します。

- [ACL名]:新しい ACL の名前を入力します。
- [ACLタイプ]:ACL のタイプを選択します。[IPv4] または [MAC]。

ステップ 4 [次へ] をクリックします。

ステップ 5 次のフィールドを入力します。

- [一致したときのアクション]:オプションのいずれかを選択します。
  - [トラフィックの許可]:ACE 条件に一致するパケットを転送します。
  - [トラフィックの拒否]:ACE 条件に一致するパケットをドロップします。
  - [インターフェイスのシャットダウン]:ACE 条件に一致するパケットをドロップし、パケットが受信されたポートを無効にします。このポートは、[エラー回復設定] ページから再アクティブ化できます。

ステップ 6 MAC ベース ACL の場合は、次のフィールドに値を入力します。

- [送信元MACアドレス]:すべての送信元アドレスを許可する場合は [任意] を選択します。送信元アドレスを入力するか送信元アドレスの範囲を指定する場合は [ユーザ定義] を選択します。
- [送信元MAC値]:送信元 MAC アドレスの照合に使用する MAC アドレスを入力します。必要に応じて、マスクも入力します。

- [送信元MACワイルドカードマスク]:MAC アドレスの範囲を定義するためのマスクを入力します。
- [宛先 MAC アドレス]:すべての宛先アドレスを許可する場合は [任意] を選択します。宛先アドレスを入力するか宛先アドレスの範囲を指定する場合は [ユーザ定義] を選択します。
- [宛先MAC値]:宛先 MAC アドレスの照合に使用する MAC アドレスを入力します。必要に応じて、マスクも入力します。
- [宛先 MAC ワイルドカード マスク]:MAC アドレスの範囲を定義するためのマスクを入力します。このマスクは、サブネット マスクなどの他のマスクとは異なる点にご注意ください。このマスクでは、**1** に設定したビットの値はマスクせず、**0** に指定したビットの値はマスクします。

  注 0000 0000 0000 0000 0000 0000 1111 1111 というマスクを例に説明します。0 になっているビットの一致は照合され、1 になっているビットの一致は照合されません。1 を 10 進数の整数に変換し、4 つずつの 0 をまとめて 0 として記述する必要があります。この例では、1111 1111 = 255 で、マスクは 0.0.0.255 と記述されます。
- [時間範囲名]:[時間範囲] を選択した場合、使用する時間範囲を選択します。時間範囲は [システム時刻の設定] セクションで定義します。このフィールドは、[時間範囲] が事前に定義されている場合にのみ表示されます。

ステップ 7 IPv4 ベース ACL の場合は、次のフィールドに値を入力します。

- [プロトコル]:特定のプロトコルに基づく ACL を作成するための次のオプションのいずれかを選択します。
  - [任意(IP)]:すべての IP プロトコル パケットを受け入れます。
  - [TCP]:伝送制御プロトコル パケットを受け入れます。
  - [UDP]:ユーザ データグラム プロトコル パケットを受け入れます。
  - [ICMP]:ICMP プロトコル パケットを受け入れます。
  - [IGMP]:IGMP プロトコル パケットを受け入れます。
- [TCP/UDP 用の送信元ポート]:ドロップダウン リストからポートを選択します。
- [TCP/UDP 用の宛先ポート]:ドロップダウン リストからポートを選択します。
- [送信元 IP アドレス]:すべての送信元アドレスを許可する場合は [任意] を選択します。送信元アドレスを入力するか送信元アドレスの範囲を指定する場合は [ユーザ定義] を選択します。
- [送信元 IP 値]:送信元 IP アドレスの照合に使用する IP アドレスを入力します。

- [送信元 IP ワイルドカード マスク]:IP アドレスの範囲を定義するためのマスクを入力します。このマスクは、サブネット マスクなどの他のマスクとは異なる点にご注意ください。このマスクでは、1 に設定したビットの値はマスクせず、0 に指定したビットの値はマスクします。
- [宛先 IP アドレス]:すべての送信元アドレスを許可する場合は [任意] を選択します。送信元アドレスを入力するか送信元アドレスの範囲を指定する場合は [ユーザ定義] を選択します。
- [宛先IP値]:送信元 IP アドレスの照合に使用する IP アドレスを入力します。
- [宛先IPワイルドカードマスク]:IP アドレスの範囲を定義するためのマスクを入力します。このマスクは、サブネット マスクなどの他のマスクとは異なる点にご注意ください。このマスクでは、1 に設定したビットの値はマスクせず、0 に指定したビットの値はマスクします。
- [時間範囲名]:[時間範囲] を選択した場合、使用する時間範囲を選択します。時間範囲は [システム時刻の設定] セクションで定義します。このフィールドは、[時間範囲] が事前に定義されている場合にのみ表示されます。

ステップ 8 [次へ] をクリックします。

ステップ 9 ACL と ACE を作成することを確認します。

ACL ルールの詳細が表示されます。別のルールを追加するには、[このACLに別のルールを追加する] をクリックします。

ステップ 10 [次へ] をクリックして、ACL バインディング情報を入力します。

- [バインディングタイプ]:ACL をバインドするための次のオプションのいずれかを選択します。
  - [物理インターフェイスのみ]:ACL をポートにバインドします。この場合は、ACL をバインドするポートをクリックします。
  - [VLAN のみ]:ACL を VLAN にバインドします。[ACLをバインドするVLANのリストの入力] フィールドに VLAN のリストを入力します。
  - [バインディングなし]:ACL をバインドしません。

[適用] をクリックします。

5

ステータスと統計情報

ここでは、デバイスの統計情報を表示する方法について説明します。

具体的な内容は、次のとおりです。

- システムの要約
- CPU 利用率
- インターフェイス
- Etherlike
- ポート使用率
- GVRP
- 802.1X EAP
- ACL
- ハードウェア リソース使用率
- ヘルスと電力
- スイッチド ポート アナライザ(SPAN)
- 診断
- RMON
- ログの表示

システムの要約

[システムの要約] ページには、デバイスのグラフ、デバイスの状態、ハードウェア情報、ファームウェア バージョン情報、一般的な PoE ステータスなどが表示されます。

システム情報を表示するには、[ステータスと統計情報] > [システムの要約] の順にクリックします。

システム情報

- [システムの説明]:システムの説明。
- [システム ロケーション]:デバイスの物理的な場所。この値を入力するには、[編集] をクリックし、[システム設定] ページに移動します。
- [システムコンタクト先]:コンタクト先の担当者名。この値を入力するには、[編集] をクリックし、[システム設定] ページに移動します。
- [ホスト名]:デバイスの名前。この値を入力するには、[編集] をクリックし、[システム設定] ページに移動します。デフォルトでは、デバイスのホスト名は、*switch* という単語と、デバイス MAC アドレスの下位 3 バイト(16 進数値の右側 6 桁)を連結したものになります。
- [システムオブジェクトID]:エンティティに含まれるネットワーク管理サブシステムの一意のベンダー ID(SNMP で使用される)。
- [システム稼動時間]:最後の再起動から経過した時間。
- [現在時刻]:現在のシステム時刻。
- [基本 MAC アドレス]:デバイスの MAC アドレス。
- [ジャンボフレーム]:ジャンボ フレームのサポート状態。このサポートは、[ポート設定] ページで有効または無効にできます。

  注 ジャンボ フレームを動作させるには、有効にした後、デバイスを再起動する必要があります。

ソフトウェア情報

- [ファームウェア バージョン]:アクティブ イメージのファームウェア バージョン番号。
- [ファームウェアのMD5チェックサム]:アクティブ イメージの MD5 チェックサム。

  注 次の 3 つのフィールドは、デバイス上の言語ごとに 1 回ずつ計 2 回表示される可能性があります。

- [ロケール]:第 1 言語のロケール。(常に英語に設定されています)。
- [言語バージョン]:第 1 言語または英語の言語パッケージ バージョン。
- [言語の MD5 チェックサム]:言語ファイルの MD5 チェックサム。

TCP/UDP サービスのステータス

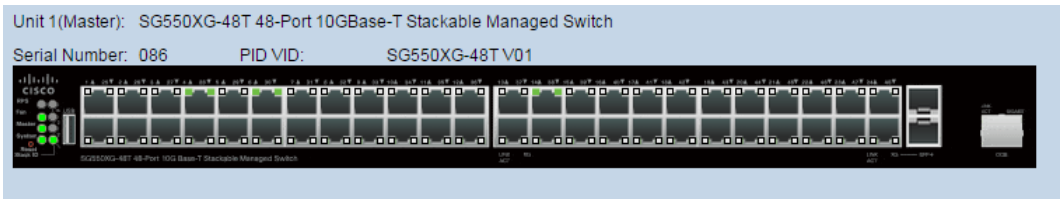
次のフィールドをリセットするには、[編集] をクリックして [TCP/UDP サービス] ページを開きます。

- [HTTP サービス]:HTTP の状態(有効または無効)。
- [HTTPS サービス]:HTTPS の状態(有効または無効)。
- [SNMP サービス]:SNMP の状態(有効または無効)。
- [Telnet サービス]:Telnet の状態(有効または無効)。
- [SSH サービス]:SSH の状態(有効または無効)。

PoE 電源情報(デバイス サポート PoE)

- [PoE電源情報]:[詳細] をクリックすると、[PoE のプロパティ] ページに直接リンクします。このページには、PoE 電源情報が表示されます。
- [最大有効PoE電力(W)]:スイッチにより給電可能な最大電力。
- [PoE電力消費合計(W)]:接続されている PoE デバイスに給電された合計 PoE 電力。
- [PoE 電源モード]:ポート制限またはクラス制限。

下の図のように、ユニットがグラフィカルに表示されます。



ポート上にカーソルを移動するとその名前が表示されます。

デバイスに関する次の情報が表示されます。

- [シリアル番号]:シリアル番号。
- [PID VID]:ポート番号とバージョン ID。

CPU 利用率

デバイスの CPU は、管理インターフェイスを処理するエンドユーザ トラフィックに加えて、次のタイプのトラフィックを処理します。

- 管理トラフィック
- プロトコル トラフィック
- スヌーピング トラフィック

トラフィックが過剰に発生すると CPU に負荷がかかり、デバイスの通常の動作に支障をきたす場合があります。デバイスは、セキュア コア テクノロジー（SCT）機能を使用することにより、受信したトラフィックの合計量に関係なく、管理トラフィックとプロトコル トラフィックの受信および処理を確実に実行できます。デバイスでは SCT はデフォルトで有効になっており、無効にできません。

他の機能との干渉は発生しません。

CPU 利用率を表示するには、次のようにします。

ステップ 1 [ステータスと統計情報] > [CPU利用率] の順にクリックします。

[CPU 入力レート] フィールドには、CPU に対する 1 秒あたりの入力フレーム レートが表示されます。

ウィンドウに、デバイス上の CPU 使用率を示すグラフが表示されます。X 軸はサンプル番号、Y 軸は利用率になります。

ステップ 2 [CPU利用率] チェックボックスがオンになっていることを確認します。

ステップ 3 統計情報が更新されるまでの**リフレッシュ レート**（秒単位の時間）を選択します。指定した間隔で新しいサンプルが作成されます。

デバイス上の CPU 使用率を示すグラフを含むウィンドウが表示されます。

インターフェイス

[インターフェイス] ページには、トラフィック統計情報がポート別に表示されます。情報のリフレッシュ レートを選択できます。

このページは、送受信されるトラフィック量とその分散(ユニキャスト、マルチキャスト、ブロードキャスト)を分析するのに便利です。

イーサネット統計情報を表示したり、リフレッシュ レートを設定したりするには、次のようにします。

ステップ 1 [ステータスと統計情報] > [インターフェイス] の順にクリックします。

ステップ 2 パラメータを入力します。

- [インターフェイス]: イーサネット統計情報を表示するインターフェイスを選択します。
- [リフレッシュレート]: インターフェイス イーサネット統計情報がリフレッシュされるまでの時間を選択します。

[受信統計情報] には、着信パケットについての情報が表示されます。

- [合計バイト(オクテット)]: 受信されたオクテット数。不良パケットと FCS オクテットが含まれますが、フレーミング ビットは含まれません。
- [ユニキャストパケット]: 受信された正常なユニキャスト パケット数。
- [マルチキャストパケット]: 受信済みの正常なマルチキャスト パケット数。
- [ブロードキャストパケット]: 受信済みの正常なブロードキャスト パケット数。
- [エラーがあるパケット]: 受信済みのエラーのあるパケット数。

[送信統計情報] には、送信パケットについての情報が表示されます。

- [合計バイト(オクテット)]: 送信されたオクテット数。不良パケットと FCS オクテットが含まれますが、フレーミング ビットは含まれません。
- [ユニキャストパケット]: 送信済みの正常なユニキャスト パケット数。
- [マルチキャストパケット]: 送信済みの正常なマルチキャスト パケット数。
- [ブロードキャストパケット]: 送信済みの正常なブロードキャスト パケット数。

ステップ 3 テーブル ビューまたはグラフィック ビューに統計情報カウンタを表示するには、次のようにします。

- テーブル ビューにすべてのポートを表示するには、[すべてのインターフェイス統計情報の表示] をクリックします。
- これらの結果をグラフィック形式で表示するには、[インターフェイス履歴グラフの表示] をクリックします。このビューでは、表示する結果の [期間] と表示する統計情報のタイプを選択できます。たとえば、[過去 5 分間] と [ユニキャスト パケット] を選択した場合は、過去 5 分間に受信されたユニキャスト パケットの数が表示されます。

Etherlike

[Etherlike] ページには、Etherlike MIB 規格定義に従って統計情報がポート別に表示されます。情報のリフレッシュ レートを選択できます。このページには、トラフィックを中断する可能性のある物理レイヤ（レイヤ 1）のエラーについての詳細な情報が表示されます。

Etherlike 統計を表示したり、リフレッシュ レートを設定したりするには、次のようにします。

ステップ 1 [ステータスと統計情報] > [Etherlike] の順にクリックします。

ステップ 2 パラメータを入力します。

- [インターフェイス]: イーサネット統計情報を表示する特定のインターフェイスを選択します。
- [リフレッシュ レート]: Etherlike 統計情報がリフレッシュされるまでの時間を選択します。

選択したインターフェイスのフィールドが表示されます。

注 次のフィールドのいずれかにエラーの数（0 以外）が表示された場合は、[最終更新] 時刻が表示されます。

- [フレームチェックシーケンス(FCS)エラー]: Cyclic Redundancy Check（CRC; 巡回冗長検査）に失敗した受信フレーム数。
- [単一コリジョン フレーム]: 単一コリジョンに含まれるが、正常に送信できたフレーム数。

- [レイトコリジョン]:データの最初の 512 ビットの後に検出されたコリジョン。
- [過剰コリジョン]:過剰コリジョンが原因で拒否された送信回数。
- [オーバーサイズパケット]:2000 オクテットを超える受信パケット。
- [内部MAC受信エラー]:受信側のエラーにより拒否されたフレーム。
- [受信済みポーズフレーム]:受信されたフロー制御ポーズ フレーム。このフィールドは、XG ポートに対してのみサポートされます。ポート速度が 1 G の場合は、受信済みポーズ フレーム カウンタが作動しません。
- [送信済みポーズフレーム]:選択されたインターフェイスから送信されたフロー制御ポーズ フレーム。

ステップ 3 テーブル ビューに統計情報カウンタを表示するには、[すべてのインターフェイス統計情報の表示] をクリックしてすべてのポートをテーブル ビューに表示します。

ポート使用率

[ポート使用率] ページには、ポートあたりのブロードバンド(着信と発信の両方)の使用率が表示されます。

ポート使用率を表示するには、次のようにします。

ステップ 1 [ステータスと統計情報] > [ポート使用率] の順にクリックします。

ステップ 2 インターフェイス イーサネット統計情報がリフレッシュされるまでの時間を示す [リフレッシュレート] を入力します。

ポートごとに次のフィールドが表示されます。

- [インターフェイス]:ポートの名前。
- [Tx使用率]:発信パケットに使用される帯域幅の量。
- [Rx使用率]:着信パケットに使用される帯域幅の量。

ポート上の一定期間の使用率推移のグラフを表示するには、ポートを選択して、[インターフェイス履歴グラフの表示] をクリックします。さらに、次のフィールドが表示されます。

- [期間]:時間の単位を選択します。グラフには、この時間の単位にわたるポート使用率が表示されます。

GVRP

[GVRP] ページには、ポートとの間で送受信された GARP VLAN 登録プロトコル（GVRP）フレームに関する情報が表示されます。GVRP は、スイッチ上での VLAN 情報の自動コンフィギュレーション用の規格ベースのレイヤ 2 ネットワーク プロトコルです。これは、802.1Q-2005 の 802.1ak 修正で定義されています。

ポートの GVRP 統計情報は、そのポートで GVRP がグローバルに有効になっている場合にのみ表示されます。[GVRP 設定] ページを参照してください。

GVRP 統計を表示したり、リフレッシュ レートを設定したりするには、次のようにします。

ステップ 1 [ステータスと統計情報] > [GVRP] の順にクリックします。

ステップ 2 パラメータを入力します。

- [インターフェイス]:GVRP 統計情報を表示する特定のインターフェイスを選択します。
- [リフレッシュレート]:GVRP ページがリフレッシュされるまでの時間を選択します。

[アトリビュート（カウンタ）] には、さまざまなパケット タイプのカウンタがインターフェイス別に表示されます。これらは、[受信済み] パケットと [送信済み] パケットに関して表示されます。

- [Join Empty]:受信または送信された GVRP の Join Empty パケット数。
- [Empty]:受信または送信された GVRP の Empty パケット数。
- [Leave Empty]:受信または送信された GVRP の Leave Empty パケット数。
- [Join In]:受信または送信された GVRP の Join In パケット数。
- [Leave In]:受信または送信された GVRP の Leave In パケット数。

- [Leave All]:受信または送信された GVRP の Leave All パケット数。

[GVRPエラー統計情報] セクションには、GVRP エラー カウンタが表示されます。

- [無効なプロトコルID]:無効なプロトコル ID エラー。
- [無効なアトリビュートタイプ]:無効なアトリビュート ID エラー。
- [無効なアトリビュート値]:無効なアトリビュート値エラー。
- [無効なアトリビュート長]:無効なアトリビュート長エラー。
- [無効なイベント]:無効なイベント。

ステップ 3 統計情報カウンタをクリアするには、[すべてのインターフェイス統計情報の表示] をクリックしてすべてのポートを 1 つのページに表示します。

802.1X EAP

[802.1x EAP] ページには、送信または受信された Extensible Authentication Protocol (EAP; 拡張認証プロトコル) フレームについての情報が表示されます。802.1X 機能を設定するには、[プロパティ] ページ ([セキュリティ] > [802.1x]) を参照してください。

EAP 統計情報を表示したり、リフレッシュ レートを設定したりするには、次のようにします。

ステップ 1 [ステータスと統計情報] > [802.1x EAP] の順にクリックします。

ステップ 2 統計情報を取得するためにポーリングするインターフェイスを選択します。

ステップ 3 EAP 統計情報がリフレッシュされるまでの時間を示すリフレッシュ レートを選択します。

選択したインターフェイスに対する値が表示されます。

- [受信済み EAPOL EAP フレーム]:ポートで受信された有効な EAPOL フレーム。
- [受信済み EAPOL 開始フレーム]:ポートで受信された有効な EAPOL 開始フレーム。
- [受信済みEAPOLログオフフレーム]:ポートで受信した EAPOL ログオフ フレーム。
- [受信済み EAPOL 通知フレーム]:ポートで受信された EAPOL 通知フレーム。

- [受信済み EAPOL 通知要求フレーム]:ポートで受信された EAPOL 通知要求フレーム。
- [受信済み EAPOL 無効フレーム]:ポートで受信された EAPOL 無効フレーム。
- [受信済み EAPOL EAP パケット長エラー フレーム]:このポートで受信された、パケット本体の長さが無効な EAPOL フレーム。
- [受信済み未認識 CKN を含む MKPDU フレーム]:このポートで受信された、未認識 CKN を含む EAP フレーム。
- [受信済み MKPDU 無効フレーム]:ポートで受信された MKPDU 無効フレーム。
- [最終EAPOLフレームバージョン]:一番新しく受信した EAPOL フレームに関連付けられていたプロトコル バージョン番号。
- [最終EAPOLフレーム送信元]:一番新しく受信した EAPOL フレームに関連付けられていた送信元 MAC アドレス。
- [送信済み EAPOL EAP サプリカント フレーム]:ポートで送信された EAPOL EAP サプリカント フレーム。
- [送信済み EAPOL 開始フレーム]:ポートで送信された EAPOL 開始フレーム。
- [送信済み EAPOL ログオフ フレーム]:ポートで送信された EAPOL ログオフ フレーム。
- [送信済み EAPOL 通知フレーム]:ポートで送信された EAPOL 通知フレーム。
- [送信済み EAPOL 通知要求フレーム]:ポートで送信された EAPOL 通知要求フレーム。
- [送信済み EAPOL EAP オーセンティケータ フレーム]:ポートで送信された EAP オーセンティケータ フレーム。
- [送信済み CKN を含まない EAPOL MKA フレーム]:ポートで送信された CKN を含まない MKA フレーム。

ステップ 4 統計情報カウンタをクリアするには、次のようにします。

- すべてのインターフェイスのカウンタを表示するには、[すべてのインターフェイス統計情報の表示] をクリックします。
- すべてのインターフェイスのカウンタをクリアするには、[インターフェイス カウンタのクリア] をクリックします。

ACL

ACL ロギング機能が有効になっている場合、ACL ルールと一致するパケットに対して情報 SYSLOG メッセージが生成されます。

ACL に基づいてパケットが転送または拒否されたインターフェイスを表示するには、次のようにします。

ステップ 1 [ステータスと統計情報] > [ACL] の順にクリックします。

ステップ 2 ページが更新されるまでのリフレッシュ レート（秒単位）を選択します。指定した間隔で新しいインターフェイスのグループが作成されます。

次の情報が表示されます。

- [グローバルトラップパケットカウンタ]: リソース不足が原因でグローバルにトラップされたパケットの数。
- [トラップ パケット – Port/LAG ベース]: ACL ルールに基づいてパケットが転送または拒否されたインターフェイス。
- [トラップ パケット – VLAN ベース]: ACL ルールに基づいてパケットが転送または拒否された VLAN。

ステップ 3 統計情報カウンタを管理するには、[カウンタのクリア] をクリックしてすべてのインターフェイスのカウンタをクリアします。

ハードウェア リソース使用率

このページには、ACL（アクセス コントロール リスト）や サービス品質（QoS）など、システムが使用するリソースが表示されます。

一部のアプリケーションは、初回起動時にルールを割り振ります。さらに、システム ブート時に初期化されるプロセスは、起動プロセス中にそれらのルールの一部を使用します。

ハードウェア リソース利用率を表示するには、[ステータスと統計情報] > [ハードウェアリソース使用率] をクリックします。

次のフィールドが表示されます。

- [ACLとQoSのルール]
  - [使用中]: ACL および QoS ルールで使用される TCAM エントリの数。
  - [最大]: ACL および QoS ルールで使用可能な TCAM エントリの数。

さまざまなプロセス間での割り振りを変更する方法を表示するには、「ハードウェア リソース」セクションを参照してください。

ヘルスと電力

[ヘルスと電力] ページは、すべての関連デバイスの温度ステータス、電源ステータス、およびファン ステータスをモニタします。モデルにより、デバイスのファンの個数は異なります。ファンがないモデルも存在します。

ファン

デバイスによっては、その動作にファンが不可欠な場合があります。ファンがないと、デバイスの温度が高くなりすぎて自動的にシャットダウンします。ファンは可動部品のため、故障することがあります。システムには冗長ファンが取り付けられています。このファンは、システム ファンのいずれかが故障しない限り、作動しません。作動した場合は、冗長ファンがデバイスの環境モニタリングの一部になります。

冗長ファンは 1 日 1 分以上作動させることをお勧めします。

デバイスによっては、ハードウェアを過熱から保護するための温度センサーが備わっています。その場合、デバイスが過熱しクール ダウンする間に、デバイスは次のアクションを実行します。

イベント	アクション
最低 1 つの温度センサーが警告しきい値を超える	次の処理が生成されます。 • Syslog メッセージ • SNMP トラップ
最低 1 つの温度センサーが危険しきい値を超える	次の処理が生成されます。 • Syslog メッセージ • SNMP トラップ 次のアクションが実行されます。 • システム LED がオレンジ色に点灯します（ハードウェアがサポートしている場合）。 • ポートの無効化：危険温度を超えた状態が 2 分以上続くと、すべてのポートがシャットダウンします。 • （PoE をサポートするデバイスの場合）電力消費量を減らし、熱放出を抑えるために、PoE 回路が無効になります。
危険しきい値超過後のクール ダウン時間（すべてのセンサーが警告しきい値より 2 °C 以上低い値になるまで）。	すべてのセンサーが警告しきい値より 2 度低い値までクール ダウンすると、PHY が再び有効になり、すべてのポートが復旧します。 ファン ステータスが [OK] になると、ポートが有効になります。 （PoE をサポートするデバイスの場合）PoE 回路が有効になります。

[ヘルスと電力] フィールド

デバイスのヘルス パラメータを表示するには、[ステータスと統計情報] > [ヘルスと電力] の順にクリックします。

注 デバイスに関連するフィールドのみが表示されます。

このセクションには、Green Ethernet 機能や LED 無効化機能によって、またポートをダウンさせる（物理的にまたは時間範囲設定によって）ことによってデバイスで節約される電力が表示されます。

PoE 節約には、特定の時刻（通常は、PoE ネットワーク要素が使用されていないとき）にポートへの PoE をシャットダウンする PoE 時間範囲機能を使用することにより節約される電力の合計が表示されます。

次の情報が表示されます（フィールドの順序はデバイスによって異なる場合があります）。

[環境における節約（Environmental Savings）]

- [ファンステータス]：次の値が使用できます。
  - [OK]：ファンが正常に動作している。
  - [障害]：ファンが正常に動作していません。
  - [N/A]：ファン ID が特定のモデルに適合していません。
- [センサーステータス]：次の値が表示されます。
  - [OK]：センサーが正常に動作しています。
  - [障害]：センサーが正常に動作していません。
  - [N/A]：センサー ID が特定のモデルに適合していません。
- [温度]：オプションは次のとおりです。
  - [OK]：温度が警告しきい値未満の場合。
  - [警告]：温度が警告しきい値と危険しきい値の間の場合。
  - [危険]：温度が危険しきい値を超えている場合。
  - [N/A]：該当なし。

- [メイン電源ステータス]: メイン電源に関して以下のいずれかが表示されます。

  [アクティブ]: 電源は使用中です。

  [障害]: メイン電源で障害が発生しました。

省電力

- [現在の Green Ethernet およびポート電力節約]: 現在、すべてのポートで節約されている電力量。
- [累積 Green Ethernet およびポート電力節約]: デバイスの電源がオンになって以降、すべてのポートで節約されている電力の累積量。
- [予測年間 Green Ethernet およびポート電力節約]: 1 週間でデバイス上で節約される電力量の予想。この値は、前の週の節約量に基づいて計算されます。
- [現在の PoE 電力節約]: PD が接続されているポートで、時間範囲機能のために PoE が動作しないことにより節約された PoE 電力の現在量。
- [累積 PoE 電力節約]: デバイスの電源がオンになって以降、PD が接続されているポートで、時間範囲機能のために PoE が動作しないことにより節約された PoE 電力の累積量。
- [予測年間 PoE 電力節約]: デバイスの電源がオンになって以降、PD が接続されているポートで、時間範囲機能のために PoE が動作しないことにより節約される PoE 電力の年間予想量。この予想は、前の週の節約量に基づきます。

イーサネット電源テーブル(デバイスで PD ポートがサポートされている場合のみ表示されます)。次のフィールドが表示されます。

- [ポート名]: ポートの番号。
- [PD ステータス]: 次の値のいずれかが表示されます。
  - [接続]: PD ポートが、電力を供給している PSE デバイスに接続されています。
  - [未接続]: PD ポートが PSE デバイスに接続されていません。
- [ネゴシエーション モード]: 次の値のいずれか。
  - [自動]: CDP または LLDP ネゴシエーションが電力レベルの決定に使用されます。
  - [802.3AF の強制]: 両側で AF 電力標準を使用します。
  - [802.3AT の強制]: 両側で AT 電力標準を使用します。

- [60W の強制]：両側で 60W の電力を使用します。

• [電力予算]：実際にポートに割り当てられた電力量。

スイッチド ポート アナライザ（SPAN）

ポート ミラーリングやポート モニタリングとも呼ばれる SPAN 機能は、ネットワーク アナライザで分析されるネットワーク トラフィックを選択します。ネットワーク アナライザは、Cisco SwitchProbe デバイスにすることも、その他のリモート モニタリング（RMON）プローブにすることもできます。

ネットワーク デバイスでは、ポート ミラーリングにより、1 つのデバイス ポート、複数のデバイス ポート、または VLAN 全体で受信されるネットワーク パケットのコピーが、デバイスの別のポートのネットワーク モニタリング接続に送信されます。この機能は、通常、侵入検知システムなど、ネットワーク トラフィックのモニタリングを必要とする場合に使用されます。モニタリング ポートに接続されたネットワーク アナライザはデータ パケットを処理します。

デバイスは、セッションあたり最大 4 つのインターフェイスをミラーリングできます。

ネットワーク ポートが受信し、ミラーリング対象の VLAN に割り当てられているパケットは、そのパケットが最終的にトラップまたは破棄される場合であっても、アナライザ ポートにミラーリングされます。送信（Tx）ミラーリング機能がアクティブな場合、デバイスから送信されるパケットはミラーリングされます。

ミラーリングにより、送信元ポートからのトラフィックがすべてアナライザ（宛先）ポートで受信されるというわけではありません。アナライザ ポートがサポートできる以上のデータが送信された場合、一部のデータが失われる可能性があります。

SPAN セッションの宛先

モニタリング セッションは、1 つ以上の送信元ポートと単一の宛先ポートで構成されます。

宛先ポートを追加するには、次のようにします。

ステップ 1 [ステータスと統計情報] > [SPAN] > [セッション宛先] の順にクリックします。

すでに定義されている宛先が表示されます。

ステップ 2 [追加] をクリックします。

ステップ 3 次のフィールドを入力します。

- [セッション ID]: セッション ID を選択します。これは送信元ポートのセッション ID に一致している必要があります。
- [ポート]: トラフィックのコピー先となるポート番号を選択します。

  これはアナライザ ポートです。Wireshark を実行している PC など、ネットワーク アナライザがこのポートに接続されます。
- [ネットワークトラフィック]: モニタリングされるトラフィック以外のトラフィックがポート上で可能であることを有効にする場合に選択します。

ステップ 4 [適用] をクリックします。

SPAN セッションの送信元

デバイス上に 1 つ以上の SPAN 送信元を設定する必要があります。

ミラーする送信元ポートを設定するには、次のようにします。

ステップ 1 [ステータスと統計情報] > [SPAN] > [セッションの送信元] の順にクリックします。

ステップ 2 [追加] をクリックします。

ステップ 3 [セッション ID] からセッション番号を選択します。これはすべての送信元ポートと宛先ポートで同じである必要があります。

ステップ 4 トラフィックがアナライザ ポート（**送信元インターフェイス**）に送信されるポートまたは VLAN を選択します。

ステップ 5 [モニタタイプ] フィールドで、ミラーするトラフィックのタイプとして、着信、発信、またはその両方を選択します。

- [TxおよびRx]: 着信パケットと発信パケットの両方に対するポート ミラーリング。
- [Rx]: 着信パケットに対するポート ミラーリング。
- [Tx]: 発信パケットに対するポート ミラーリング。

ステップ 6 [適用] をクリックします。ミラーリング用の送信元インターフェイスが設定されます。

診断

ここでは、ポート ミラーリングの設定、ケーブル テストの実行、およびデバイス動作情報の表示について説明します。

具体的な内容は、次のとおりです。

- カッパー ポート テスト
- 光モジュール ステータス
- テクニカル サポート情報

カッパー ポート テスト

[カッパーテスト] ページには、カッパー ケーブルに対して Virtual Cable Tester（VCT）によって実行された統合ケーブル テストの結果が表示されます。

VCT によって、2 つのタイプのテストが実行されます。

- Time Domain Reflectometry（TDR; タイム ド メイン反射率計）テクノロジーは、ポートに取り付けられているカッパー ケーブルの品質と特性をテストします。長さ 140 m までのケーブルをテストできます。テスト結果は、[カッパー テスト] ページの [テスト結果] ブロックに表示されます。
- DSP ベース テストは、アクティブな XG リンクに対して実行され、ケーブルの長さを測定します。これらの結果は、[カッパー テスト] ページの [詳細情報] ブロックに表示されます。このテストはリンク速度が 10 G の場合にのみ実行できます。

カッパー ポート テスト実行時の前提条件

テストを実行する準備として、次のようにします。

- （必須）ショート リーチ モードの無効化（[プロパティ] ページを参照）
- （任意）EEE の無効化（[プロパティ] ページを参照）

ケーブル テスト（VCT）を実行する際には、CAT6a データ ケーブルをご使用ください。

テスト結果の精度は、詳細テストの場合に +/- 10 のエラー範囲、基本テストの場合に +/- 2 のエラー範囲になります。

注意 ポートはテスト時、停止状態となり、通信は中断されます。テスト後、ポートは稼動状態に戻ります。Web ベースのスイッチ設定ユーティリティの実行に使用しているポートに対してカッパー ポート テストを実行することは、その間このデバイスと通信できなくなるので、推奨できません。

ポートに取り付けられているカッパー ケーブルをテストするには、次のようにします。

ステップ 1 [ステータスと統計情報] > [診断] > [カッパーテスト] の順にクリックします。

ステップ 2 テストを実行するポートを選択します。

ステップ 3 [カッパーテスト] をクリックします。

ステップ 4 メッセージが表示された場合、リンクが停止状態になることを了承する場合は [OK] をクリックし、テストを中止する場合は [キャンセル] をクリックします。

[テスト結果] ブロックに次のフィールドが表示されます。

- [最終更新]: ポートに対して最後のテストが実行された時刻。
- [テスト結果]: ケーブル テストの結果。選択項目は次のとおりです。
  - [OK]: ケーブルはテストに合格しました。
  - [ケーブルなし]: ケーブルがポートに接続されていません。
  - [開放ケーブル]: ケーブルの一方の側しか接続されていません。
  - [短絡ケーブル]: ケーブルにショートが発生しています。
  - [テスト結果不明]: エラーが発生しました。
- [障害個所までの距離]: 障害が検出されたケーブル位置からポートまでの距離。
- [動作ポート ステータス]: ポートの状態（アップまたはダウン）が表示されます。

[詳細情報] ブロックに次の情報が表示されます（ページを開くたびに情報が更新されます）。

- [ケーブル長]: 長さの目安を提供します。
- [ペア]: テスト中のケーブル ワイヤ ペア。
- [ステータス]: ワイヤ ペアのステータス。赤は障害が発生していることを示し、緑は正常な状態を示します。
- [チャネル]: ケーブル チャネル。ワイヤのタイプ（ストレート ケーブルまたはクロス ケーブル）を示します。

- [極性]: 自動極性検出と修正機能がワイヤ ペアに対して有効になっているかどうかを示します。
- [ペア スキュー]: ワイヤ ペア間の遅延差。

光モジュール ステータス

[光モジュールステータス] ページには、Small Form-factor Pluggable（SFP）トランシーバにより報告される動作状況が表示されます。

サポートされている GE SFP（1000 Mbps）トランシーバは次のとおりです。

- MGBBX1: 1000BASE-BX-20U SFP トランシーバ（シングルモード ファイバ対応、波長 1310 nm）は、最大 40 km までサポートします。
- MGBLH1: 1000BASE-LH SFP トランシーバ（シングルモード ファイバ対応、波長 1310 nm）は、最大 40 km までサポートします。
- MGBLX1: 1000BASE-LX SFP トランシーバ（シングルモード ファイバ対応、波長 1310 nm）は、最大 10 km までサポートします。
- MGBSX1:1000BASE-SX SFP トランシーバ（マルチモード ファイバ対応、波長 850 nm）は、最大 550 m までサポートします。
- MGBT1: 1000BASE-T SFP トランシーバ（カテゴリ 5 カッパー ワイヤ対応）は最大 100 m までサポートします。

サポートされている XG SFP+（10,000 Mbps）トランシーバは次のとおりです。

- Cisco SFP-10GSR
- Cisco SFP-10GLRM
- Cisco SFP-10GLR

サポートされている XG パッシブ ケーブル（Twinax/DAC）は次のとおりです。

- Cisco SFP-H10GCU1m
- Cisco SFP-H10GCU3m
- Cisco SFP-H10GCU5m

光テスト結果を表示するには、[ステータスと統計情報] > [診断] > [光モジュールステータス] の順にクリックします。

このページには次のフィールドが表示されます。

- [ポート]:SFP が接続しているポート番号。
- [説明]:光トランシーバの説明。
- [シリアル番号]:光トランシーバのシリアル番号。
- [PID]:VLAN ID。
- [VID]:光トランシーバの ID。
- [温度]:SFP の動作温度(摂氏)。
- [電圧]:SFP の動作電圧。
- [電流]:SFP の電流消費量。
- [出力電力]:送出される光電力。
- [入力電力]:受け取る光電力。
- [トランスミッタ障害]:リモート SFP から報告される信号損失。値は [TRUE]、[FALSE]、および [N/S](信号なし)になります。
- [信号消失]:ローカル SFP から報告される信号損失。値は [TRUE] か [FALSE] になります。
- [データ レディ]:SFP が動作しています。値は [TRUE] か [FALSE] になります。

テクニカル サポート情報

このページでは、デバイス ステータスの詳細なログが提供されます。この情報は、テクニカル サポートがユーザの問題解決を支援する場合に非常に役に立ちます。その理由は、単一のコマンドで複数の show コマンド(debug コマンドを含む)の出力が得られるためです。

デバッグに役立つテクニカル サポート情報を表示するには、次のようにします。

ステップ 1 [ステータスと統計情報] > [診断] > [テクニカルサポート情報] の順にクリックします。

ステップ 2 [生成] をクリックします。

さまざまな **show** CLI コマンドからの情報が表示されます。

注　このコマンドからの出力の生成にはしばらく時間がかかる場合があります。情報が生成されたら、[技術サポート データの選択] をクリックすることにより、画面上のテキスト ボックスからコピーすることができます。

RMON

RMON（リモート ネットワーキング モニタリング）を使用すると、デバイスの SNMP エージェントがトラフィック統計情報の監視を一定期間行い、トラップを SNMP マネージャに送信することによって、プロアクティブな対応をすることができます。ローカル SNMP エージェントは、実際のリアルタイムのカウンタを、事前定義されたしきい値と比較してアラームを生成するので、SNMP 中央管理プラットフォームでポーリングする必要がなくなります。ネットワークのベース ラインを基準とした相対幅を持つ適切なしきい値が設定されていれば、これはプロアクティブな管理において効果的なメカニズムとなります。

RMON を使用すると、SNMP マネージャがデバイスを頻繁にポーリングして情報を得る必要がなくなるため、マネージャとデバイス間のトラフィックを減らすことができますし、デバイスがイベント発生時にイベントを報告するため、マネージャがタイムリーなステータス レポートを取得できるようになります。

この機能により、次のアクションを実行できるようになります。

- 現在の統計情報（カウンタ値がクリアされたとき以降）を表示する。一定期間、これらのカウンタ値を収集して、収集データのテーブルを表示することもできます。収集された各セットは、[履歴] タブに 1 行で表示されます。
- 「特定のレイト コリジョン数に達した」など、カウンタ値に関して興味を引く変化を定義して（アラームを定義）、このイベントが発生したときに実行するアクションを定義する（ログ、トラップ、またはその両方）。

統計情報

[統計情報] ページには、パケット サイズについての詳細情報および物理レイヤ エラーについての情報が表示されます。表示される情報は、RMON 規格に基づいています。オーバー サイズ パケットは、次の基準を満たすイーサネット フレームとして定義されます。

- パケットの長さが MRU バイト サイズより長い。
- コリジョン イベントが検出されていない。

- レイト コリジョン イベントが検出されていない。
- 受信した (Rx) エラー イベントが検出されていない。
- 有効な CRC がパケットにある。

RMON 統計情報を表示したり、リフレッシュ レートを設定したりするには、次のようにします。

ステップ 1 [ステータスと統計情報] > [RMON] > [統計情報] の順にクリックします。

ステップ 2 イーサネット統計情報を表示するインターフェイスを選択します。

ステップ 3 インターフェイス統計情報がリフレッシュされるまでの時間を示すリフレッシュ レートを選択します。

選択したインターフェイスに関する以下の統計情報が表示されます。

注 次のフィールドのいずれかにエラーの数(0 以外)が表示された場合は、[最終更新] 時刻が表示されます。

- [受信済みバイト]:受信されたオクテット数。不良パケットと FCS オクテットが含まれますが、フレーミング ビットは含まれません。
- [ドロップイベント]:ドロップされたパケット数。
- [受信済みパケット]:マルチキャスト パケットとブロードキャスト パケットを含む、受信済みの正常なパケット数。
- [受信済みブロードキャストパケット]:受信済みの正常なブロードキャスト パケット数。この数にはマルチキャスト パケットは含まれません。
- [受信済みマルチキャストパケット]:受信済みの正常なマルチキャスト パケット数。
- [CRC &アラインメントエラー]:発生した CRC とアラインメント エラー数。
- [アンダーサイズパケット]:受信済みアンダーサイズ パケット数(64 オクテット未満)。
- [オーバーサイズ パケット]:受信済みオーバーサイズ パケット数(2000 オクテット超過)。
- [フラグメント]:受信済みフラグメント(フレーミング ビットを含まず、FCS オクテットを含む、64 オクテット未満のパケット)の数。

- [ジャバー]:1632 オクテットを超える受信済みパケット数。この数にはフレーミング ビットは含まれず、FCS オクテットは含まれます。この FCS オクテットには、オクテットの整数(FCS エラー)を持つ不良 Frame Check Sequence(FCS; フレーム チェック シーケンス)、または非整数オクテット(アラインメント エラー)を持つ不良 FCS のいずれかが含まれます。ジャバー パケットは、次の基準を満たすイーサネット フレームとして定義されます。
  - パケットのデータ長が MRU より長い。
  - 無効な CRC がパケットにある。
  - 受信した (Rx) エラー イベントが検出されていない。
- [コリジョン]:受信済みコリジョン数。ジャンボ フレームが有効である場合、ジャバー フレームのしきい値はジャンボ フレームの最大サイズまで引き上げられます。
- [64 バイト フレーム]:送信または受信された 64 バイトを格納するフレーム数。
- [65 ～ 127 バイト フレーム]:送信または受信された 65 ～ 127 バイトを格納するフレーム数。
- [128 ～ 255 バイト フレーム]:送信または受信された 128 ～ 255 バイトを格納するフレーム数。
- [256 ～ 511 バイト フレーム]:送信または受信された 256 ～ 511 バイトを格納するフレーム数。
- [512 ～ 1023 バイト フレーム]:送信または受信された 512 ～ 1023 バイトを格納するフレーム数。
- [1024 バイト以上のフレーム]:送信または受信された 1024 ～ 2000 バイトを格納するフレーム、およびジャンボ フレームの数。

ステップ 4 テーブル ビューまたはグラフィック ビューにカウンタを表示するには、次のようにします。

- テーブル ビューにすべてのポートを表示するには、[すべてのインターフェイス統計情報の表示] をクリックします。
- これらの結果をグラフィック形式で表示するには、[グラフィックビュー] をクリックします。このビューでは、表示する結果の [期間] と表示する統計情報のタイプを選択できます。

RMON の履歴

RMON 機能を使用すると、インターフェイスごとに統計情報をモニタできます。

[履歴] ページでは、サンプリング頻度、保存するサンプル数、およびデータ収集元ポートを定義できます。

データは、サンプリングされてから保存され、[履歴テーブル] をクリックして表示できる [履歴テーブル] ページに表示されます。

RMON 制御情報を入力するには、次のようにします。

ステップ 1 [ステータスと統計情報] > [RMON] > [履歴] の順にクリックします。このページに表示されるフィールドは、下にある [RMON 履歴の追加] ページで定義されます。このページにあり、[追加] ページで定義されていないフィールドは次のものだけです。

- [現在のサンプル数]:RMON は、規格により、要求されたすべてのサンプルを許可するのではなく、要求ごとにサンプル数を制限するようになっています。したがって、このフィールドは、要求に対して実際に許可されたサンプル数(要求値以下)を表します。

ステップ 2 [追加] をクリックします。

ステップ 3 パラメータを入力します。

- [新規履歴エントリ]:新しい [履歴] テーブル エントリ番号が表示されます。
- [送信元インターフェイス]:履歴サンプルを取得するインターフェイスのタイプを選択します。
- [最大保持サンプル数]:保存されるサンプル数を入力します。
- [サンプリング間隔]:ポートからサンプルが収集された秒数を入力します。フィールド範囲は 1 ～ 3600 です。
- [オーナー]:RMON 情報を要求した RMON ステーションまたはユーザを入力します。

ステップ 4 [適用] をクリックします。エントリが [履歴制御テーブル] ページに追加され、実行コンフィギュレーション ファイルが更新されます。

ステップ 5 実際の統計情報を表示するには、[履歴テーブル](下に説明)をクリックします。

RMON 統計情報テーブル

[履歴] ページには、インターフェイス固有の統計情報ネットワーク サンプリングが表示されます。サンプルは、上で説明されている [履歴制御テーブル] で構成されています。

RMON 履歴統計情報を表示するには、次のようにします。

ステップ 1 [ステータスと統計情報] > [RMON] > [履歴] の順にクリックします。

ステップ 2 [履歴テーブル] をクリックします。

ステップ 3 [履歴エントリ番号] ドロップ ダウン メニューから、オプションでサンプルのエントリ番号を選択して表示します。

選択したサンプルのフィールドが表示されます。

- [オーナー]:履歴テーブル エントリのオーナー。
- [サンプル番号]:統計情報はこのサンプルから取得されます。
- [ドロップイベント]:サンプリング中にネットワーク リソース不足によりドロップされたパケット数。これは、ドロップ パケットが検出された回数を表します。ただしドロップされたパケットの正確な数を表さない場合があります。
- [受信済みバイト]:受信されたオクテット数。不良パケットと FCS オクテットが含まれますが、フレーミング ビットは含まれません。
- [受信済みパケット]:不良パケット、マルチキャスト パケット、ブロードキャスト パケットを含む受信済みパケット。
- [ブロードキャストパケット]:正常なブロードキャスト パケット数。この数にはマルチキャスト パケットは含まれません。
- [マルチキャストパケット]:受信済みの正常なマルチキャスト パケット数。
- [CRCアラインメントエラー]:発生した CRC とアライン メント エラー数。
- [アンダーサイズパケット]:受信済みアンダーサイズ パケット数(64 オクテット未満)。
- [オーバーサイズ パケット]:受信済みオーバーサイズ パケット数(2000 オクテット超過)。
- [フラグメント]:受信済みフラグメント(フレーミング ビットを含まず、FCS オクテットを含む、64 オクテット未満のパケット)の数。

- [ジャバー]:2000 オクテットを超える受信済みパケット合計数。この数にはフレーミング ビットは含まれず、FCS オクテットは含まれます。この FCS オクテットには、オクテットの整数(FCS エラー)を持つ不良 Frame Check Sequence (FCS; フレーム チェック シーケンス)、または非整数オクテット(アラインメント エラー)を持つ不良 FCS のいずれかが含まれます。
- [コリジョン]:受信済みコリジョン数。
- [利用率]:インターフェイスが処理できる、最大トラフィックと比較した現在のインターフェイス トラフィックの割合。

RMON イベント制御

アラームをトリガーするオカレンスや、発生する通知のタイプを制御できます。これは次のように実行されます。

- [イベント] ページ:アラームがトリガーされたときに発生するアクションを設定します。これは、ログとトラップのどのような組み合わせでも構いません。
- [アラーム] ページ:アラームをトリガーするオカレンスを設定します。

RMON イベントを定義するには、次のようにします。

ステップ 1 [ステータスと統計情報] > [RMON] > [イベント] の順にクリックします。

このページには、事前に定義されたイベントが表示されます。

このページのフィールドは、[時間] フィールドを除き、[RMONイベントの追加] ダイアログボックスによって定義されます。

- [時間]:イベントの時刻を表示します。(これは、親ウィンドウの読み取り専用テーブルであり、定義できません。)

ステップ 2 [追加] をクリックします。

ステップ 3 パラメータを入力します。

- [イベントエントリ]:新しいエントリのイベント エントリ インデックス番号が表示されます。
- [コミュニティ]:トラップが送信されるときに含める SNMP コミュニティ ストリングを入力します(任意)。トラップがネットワーク管理ステーションに届くようにするには、[通知受信者] ページを使用してコミュニティを定義する必要があることに注意してください。

- [説明]: イベントの名前を入力します。この名前は、アラームをイベントに付加する場合に [RMON アラームの追加] ページで使用されます。
- [通知タイプ]: このイベントの結果のアクションのタイプを選択します。次の値から選択します。
  - [なし]: アラームの発生時に行われるアクションはありません。
  - [ログ（イベント ログ テーブル）]: アラームの発生時、イベント ログ テーブルにログ エントリを追加します。
  - [トラップ（SNMP マネージャと Syslog サーバ）]: アラームの発生時、リモート ログ サーバにトラップを送信します。
  - [ログとトラップ]: アラームの発生時、イベント ログ テーブルにログ エントリを追加し、リモート ログ サーバにトラップを送信します。
- [オーナー]: イベントを定義したデバイスまたはユーザを入力します。

ステップ 4 [適用] をクリックします。RMON イベントは、実行コンフィギュレーション ファイルに保存されます。

ステップ 5 [イベント ログ テーブル] をクリックして、発生してログに書き込まれたアラームのログを表示します（以下の説明を参照）。

RMON イベント ログ

[イベント] ページには、発生したイベント（アクション）のログが表示されます。次の 2 つのイベントのタイプがログに書き込まれます: *ログ*または*ログとトラップ*。イベントがアラームにバインドされ（[RMON アラーム] ページを参照）、アラーム条件が発生した場合に、そのイベントのアクションが実行されます。

ステップ 1 [ステータスと統計情報] > [RMON] > [イベント] の順にクリックします。

ステップ 2 [イベント ログ テーブル] をクリックします。

イベントを表示する特定のインターフェイスをフィルタで選択できます。

このページには次のフィールドが表示されます。

- [イベント エントリ番号]: イベントのログ エントリ番号。
- [ログ番号]: ログ番号（イベント内）。
- [ログ時刻]: ログ エントリが入力された時刻。

- [説明]:アラームをトリガーしたイベントの説明。

RMON アラーム

RMON アラームは、エージェントが保守するカウンタまたはその他の SNMP オブジェクト カウンタに対して例外イベントを生成するために、しきい値とサンプリング間隔を設定するためのメカニズムを備えています。アラームには、上昇しきい値と下降しきい値の両方を設定する必要があります。上昇しきい値を超えた後、対になっている下降しきい値を超えるまでは、上昇イベントは生成されません。下降アラームが実行された後、上昇しきい値を超えると次のアラームが実行されます。

1 つ以上のアラームが 1 つのイベントにバインドされます。イベントは、アラームの発生時に実行するアクションを示します。

アラーム カウンタは、絶対値またはカウンタ値の変化(デルタ)のいずれかで監視できます。

RMON アラームを入力するには、次のようにします。

ステップ 1 [ステータスと統計情報] > [RMON] > [アラーム] の順にクリックします。

すでに定義されているアラームがすべて表示されます。フィールドについては、下記の [RMON アラームの追加] ページで説明されています。これらのフィールドに加え、以下のフィールドが表示されます。

- [カウンタ値]:最後のサンプリング期間の統計値が表示されます。

ステップ 2 [追加] をクリックします。

ステップ 3 パラメータを入力します。

- [アラームエントリ]:アラーム エントリ番号が表示されます。
- [インターフェイス]:RMON 統計情報の表示対象となるインターフェイスのタイプを選択します。
- [カウンタ名]:測定される発生タイプを示す MIB 変数を選択します。
- [サンプルタイプ]:アラームを生成するサンプリング方法を選択します。次のオプションがあります。
  - [絶対]:しきい値を超えると、アラームが生成されます。
  - [デルタ]:現在値から最後のサンプリング値を減算します。値間の差がしきい値と比較されます。しきい値を超えていると、アラームが生成されます。

- [上昇しきい値]: 上昇しきい値アラームをトリガーする値を入力します。
- [上昇イベント]: 上昇イベントがトリガーされたときに実行するイベントを選択します。イベントは、[RMON イベント制御] ページで設定します。
- [下降しきい値]: 下降しきい値アラームをトリガーする値を入力します。
- [下降イベント]: 下降イベントがトリガーされたときに実行するイベントを選択します。
- [始動アラーム]: アラームの生成を開始する最初のイベントを選択します。上昇は、低い値のしきい値から高い値のしきい値に向けてしきい値を超えることで定義されます。
  - [上昇アラーム]: 上昇値が上昇しきい値アラームをトリガーします。
  - [下降アラーム]: 下降値が下降しきい値アラームをトリガーします。
  - [上昇および下降]: 上昇値と下降値の両方がアラームをトリガーします。
- [間隔]: アラーム間隔を秒単位で入力します。
- [オーナー]: アラームを受信するユーザまたはネットワーク管理システムの名前を入力します。

ステップ 4 [適用] をクリックします。RMON アラームは、実行コンフィギュレーション ファイルに保存されます。

ログの表示

デバイスは、次のログに記録することができます。

- RAM へのログ（リブート時にクリア）
- フラッシュ メモリへのログ（ユーザ コマンドでのみクリア）

重大度により各ログに書き込まれるメッセージを設定できます。メッセージは、外部 SYSLOG サーバ上のログを含む、複数のログに送信することができます。

RAM メモリ

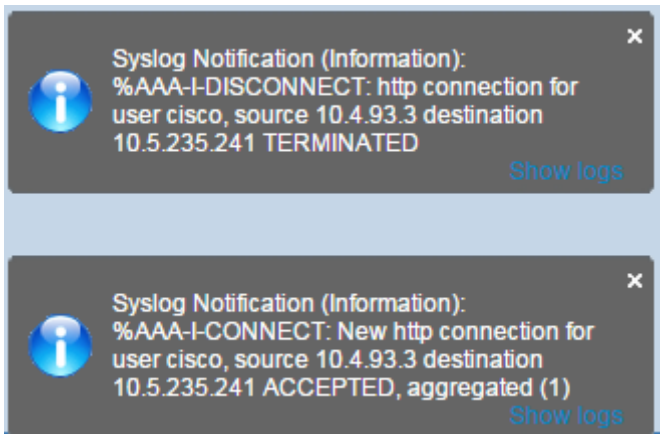
[RAM メモリ] ページには、RAM（キャッシュ）に保存されたすべてのメッセージが時間順に表示されます。エントリは、[ログ設定] ページ内のコンフィギュレーションに従って、RAM ログに保存されます。

ポップアップ SYSLOG 通知

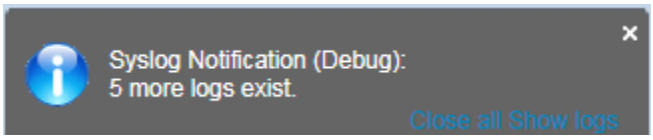
新しい SYSLOG メッセージが RAM ログ ファイルに書き込まれると、Web GUI にその内容に関する通知が表示されます。

Web GUI は 10 秒ごとに RAM ログをポーリングします。過去 10 秒間に作成されたすべての SYSLOG に関する通知ポップアップが画面右下に表示されます。

通知ポップアップが表示されます以下を参照してください。



表示されるポップアップ通知が 8 件以上の場合、サマリー ポップアップが表示されます。このポップアップには、表示されていない SYSLOG 通知の数が示されます。また、次に示すように、表示されたすべてのポップアップを閉じるためのボタンも表示されます。



ログ エントリを表示するには、[ステータスと統計情報] > [ログの表示] > [RAM メモリ] の順にクリックします。

ページの上部に以下が表示されます。

- [アラートアイコン点滅]: 無効と有効を切り替えます。
- [ポップアップ Syslog 通知]: 前述したようにポップアップ SYSLOG の受信を有効にします。
- [現在のロギングしきい値]: 生成するロギングのレベルを指定します。フィールド名の横の [編集] をクリックすると、これを変更できます。

このページには、各ログ ファイルについての次のフィールドが含まれています。

- [ログ インデックス]: ログ エントリ番号。
- [ログ時刻]: メッセージが生成された時刻。
- [重大度]: イベントの重大度。
- [説明]: イベントについて説明するメッセージ テキスト。

ログ メッセージをクリアするには、[ログのクリア] をクリックします。メッセージがクリアされます。

フラッシュ メモリ

[フラッシュ メモリ] ページには、フラッシュ メモリに保存されたメッセージが時間順に表示されます。ログの最小重大度は [ログ設定] ページで設定します。フラッシュ ログはデバイスの再起動時に保持されます。ログは手動でクリアできます。

フラッシュ ログを表示するには、[ステータスと統計情報] > [ログの表示] > [フラッシュ メモリ] の順にクリックします。

[現在のロギングしきい値] は、生成されるロギングのレベルを指定します。フィールド名の横の [編集] をクリックすると、これを変更できます。

このページには、各ログ ファイルに関する次のフィールドが含まれています。

- [ログ インデックス]: ログ エントリ番号。
- [ログ時刻]: メッセージが生成された時刻。
- [重大度]: イベントの重大度。
- [説明]: イベントについて説明するメッセージ テキスト。

メッセージをクリアするには、[ログのクリア] をクリックします。メッセージがクリアされます。

6

管理

この項では、システム情報の表示方法と、デバイスでのさまざまなオプションの設定方法について説明します。

具体的な内容は、次のとおりです。

- システム設定
- ユーザ アカウント
- アイドルセッションタイムアウト
- 時間設定
- システム ログ
- ファイル管理
- プラグアンドプレイ(PNP)
- リブート
- ディスカバリ - Bonjour
- ディスカバリ - LLDP
- ディスカバリ - CDP
- デバイスの特定
- Ping
- トレースルート

システム設定

システム設定を入力するには、次のようにします。

ステップ 1 [各種管理] > [システム設定] の順にクリックします。

ステップ 2 システム設定を表示または変更します。

- [システムの説明]:デバイスの説明を表示します。
- [システム ロケーション]:デバイスの物理的な場所を入力します。
- [システム コンタクト先]:連絡先の担当者名を入力します。
- [ホスト名]:このデバイスのホスト名を選択します。これは CLI コマンドのプロンプトで使用されます。
  - [デフォルトを使用]:これらのスイッチのデフォルト ホスト名(システム名)は、*switch123456* で、123456 は 16 進数のデバイス MAC アドレスの下位 3 バイトになります。
  - [ユーザ定義]:ホスト名を入力します。文字、数字、およびハイフンのみ使用できます。ホスト名の開始または終了はハイフンにできません。その他の記号、句読点、ブランクも使用できません(RFC1033、1034、1035 の規定により)。
- [カスタムバナー設定]:次のバナーを設定できます。
  - [ログイン バナー]:ここに入力するテキストはログイン前のログイン ページに表示されます。[プレビュー] をクリックすると、結果を表示できます。
  - [ウェルカム バナー]:ここに入力するテキストはログイン後のログイン ページに表示されます。[プレビュー] をクリックすると、結果を表示できます。

  注 Web ベースのコンフィギュレーション ユーティリティからログイン バナーを定義すると、CLI インターフェイス(コンソール、Telnet、および SSH)のバナーもアクティブになります。

  バナーには最大で 1000 文字を含めることができます。510 文字より後は、<Enter> を押して続行してください。

ステップ 3 [適用] をクリックし、実行コンフィギュレーション ファイルに値を保存します。

ユーザ アカウント

[ユーザアカウント] ページでは、デバイスへのアクセス（読み取り専用または読み取り/書き込み）を許可される追加のユーザを入力したり、既存のユーザのパスワードを変更したりできます。

レベル 15 ユーザを下記の説明に従って追加すると、既定のユーザはシステムから削除されます。

注　パスワード リカバリについては、メニュー CLI とパスワード リカバリを参照してください。

新しいユーザを追加するには、次のようにします。

ステップ 1　[各種管理] > [ユーザアカウント] をクリックします。

このページには、システムで定義されたユーザと、各ユーザの特権レベルが表示されます。

ステップ 2　ユーザを新しく追加するために [追加] をクリックするか、既存のユーザを修正するために [編集] をクリックします。

ステップ 3　パラメータを入力します。

- [ユーザ名]：1 ～ 20 文字の新しいユーザ名を入力します。UTF-8 文字は使用できません。
- [パスワード]：パスワードを入力します（UTF-8 文字は使用できません）。パスワードの強度と複雑度が定義されている場合、ユーザ パスワードは、パスワード強度で設定されたポリシーに従う必要があります。
- [パスワードの確認]：パスワードを再び入力します。
- [パスワード強度メーター]：パスワードの強度が表示されます。パスワードの強度と複雑度に関するポリシーは、[パスワード強度] ページで設定します。
- [ユーザレベル]：追加/編集されるユーザの特権レベルを選択します。
  - [読み取り専用CLIアクセス (1)]：ユーザは GUI にアクセスできません。単に、デバイス構成を変更しない CLI コマンドにアクセスできるだけです。
  - [読み取り/制限付き書き込みCLIアクセス (7)]：ユーザは GUI にアクセスできません。デバイス構成を変更する一部の CLI コマンドにアクセスできるだけです。詳しくは、*『CLI Reference Guide』*を参照してください。
  - [読み取り/書き込み管理アクセス (15)]：ユーザは GUI にアクセスでき、デバイスの設定を行うことができます。

ステップ 4 [適用] をクリックします。ユーザがデバイスの実行コンフィギュレーション ファイルに追加されます。

アイドルセッションタイムアウト

[アイドルセッションタイムアウト] では、タイムアウトが発生するまでに管理セッションがアイドル状態を継続できる時間を設定します。タイムアウトが発生した場合、次のセッションのいずれかを再構築するには、再度ログインする必要があります。

- [HTTPセッションタイムアウト]
- [HTTPSセッションタイムアウト]
- [Telnetセッションタイムアウト]
- [SSHセッションタイムアウト]

さまざまなタイプのセッションのアイドル セッション タイムアウトを設定するには、次のようにします。

ステップ 1 [各種管理] > [アイドルセッションタイムアウト] の順にクリックします。

ステップ 2 対応するリストから各セッション タイプのタイムアウトを選択します。デフォルトのタイムアウト値は 10 分です。

ステップ 3 [適用] をクリックして、デバイスのコンフィギュレーションを設定します。

時間設定

「各種管理:時刻設定」を参照してください。

システム ログ

ここでは、複数の個別のログをデバイスで生成できるようにするためのシステム ログ機能について説明します。各ログは、システム イベントを記述するメッセージの集まりです。

デバイスは、次のローカル ログを生成します。

- コンソール インターフェイスに送信されるログ。
- RAM 内のログ イベントの巡回リストに書き込まれるログ。デバイスの再起動時に消去されます。
- フラッシュ メモリに保存される巡回ログ ファイルに書き込まれるログ。再起動後も保持されます。

加えて、SNMP トラップおよび SYSLOG メッセージの形式で、リモート SYSLOG サーバにメッセージを送信することができます。

このセクションの内容は、次のとおりです。

ログ設定

重大度別にロギングされるイベントを選択することができます。各ログ メッセージは、重大度の最初のアルファベットで示されます（ただし *「緊急 (Emergency)」*のみアルファベット F を使用するので例外）。このアルファベットは両側がダッシュ (-) で連結されています。たとえば、ログ メッセージ「%INIT-I-InitCompleted: … 」の重大度は **I** で、これは *「情報」*を意味します。

イベントの重大度は、高いものから順に次のとおりです。

- [緊急]: システムが使用不能です。
- [アラート]: アクションが必要です。
- [重大]: システムに重大な状況が発生しています。
- [エラー]: システムがエラー状態にあります。
- [警告]: システム警告が発生しました。
- [通知]: システムは適切に動作していますが、システム通知が発生しています。

- [情報]:デバイス情報。
- [デバッグ]:イベントに関する詳細情報。

RAM ログおよびフラッシュ ログに対して重大度を選択できます。これらのログはそれぞれ、[RAM メモリ] ページと [フラッシュ メモリ] ページに表示されます。

ログに保存する重大度を選択することにより、それより重大度の高いイベントはすべて、自動的にログに保存されることになります。それより低い重大度のイベントはログに保存されません。

たとえば、[警告] が選択された場合、**警告**およびこれより高いすべての重大度(緊急、アラート、重要、エラー、および警告)がログに保存されます。**警告**より低い重大度(通知、情報、およびデバッグ)のイベントはログに保存されません。

グローバル ログ パラメータを設定するには、次のようにします。

ステップ 1 [各種管理] > [システムログ] > [ログ設定] の順にクリックします。

ステップ 2 パラメータを入力します。

- [ロギング]:これを選択するとメッセージ ロギングが有効になります。
- [Syslog アグリゲータ]:これを選択すると SYSLOG メッセージとトラップの集約が有効になります。これが有効になると、同一かつ連続する SYSLOG メッセージとトラップが、指定された最大集約時間にわたって集約され、単一のメッセージで送信されます。集約メッセージは、到着順に送信されます。各メッセージには、集約された回数が示されます。
- [最大集約時間]:SYSLOG メッセージが集約される間隔を入力します。
- [発信元 ID]:この設定により、SYSLOG メッセージに発信元 ID を追加できます。次のオプションがあります。
  - [なし]:SYSLOG メッセージに発信元 ID を含めません。
  - [ホスト名]:システム ホスト名を SYSLOG メッセージに含めます。
  - [IPv4アドレス]:送信元インターフェイスの IPv4 アドレスを SYSLOG メッセージに含めます。
  - [IPv6 アドレス]:送信元インターフェイスの IPv6 アドレスを SYSLOG メッセージに含めます。
  - [ユーザ定義]:SYSLOG メッセージに含める記述を入力します。
- [RAM メモリロギング]:RAM に記録するメッセージの重大度を選択します。

- [フラッシュメモリロギング]:フラッシュ メモリに記録するメッセージの重大度を選択します。
- [適用] をクリックします。実行コンフィギュレーション ファイルが更新されます。

リモート ログの設定

[リモートログサーバ] ページでは、ログ メッセージの送信先となるリモート SYSLOG サーバを定義できます。各サーバについて、受け取るメッセージの重大度を設定できます。

SYSLOG サーバを定義するには、次のようにします。

ステップ 1 [各種管理] > [システムログ] > [リモートログサーバ] の順にクリックします。

ステップ 2 次のフィールドを入力します。

- [IPv4 発信元インターフェイス]:SYSLOG サーバに送られる SYSLOG メッセージの発信元 IPv4 アドレスとして使われる IPv4 アドレスを持つ送信元インターフェイスを選択します。
- [IPv6 発信元インターフェイス]:SYSLOG サーバに送られる SYSLOG メッセージの送信元 IPv6 アドレスとして使われる IPv6 アドレスを持つ送信元インターフェイスを選択します。

  注 [自動] オプションが選択されている場合、システムは、発信インターフェイスで定義された IP アドレスからソース IP アドレスを取得します。

すでに設定されたログ サーバごとに情報が記述されます。[追加] ページ内のフィールドについては以下で説明します。

ステップ 3 [追加] をクリックします。

ステップ 4 パラメータを入力します。

- [サーバ指定方法]: リモート ログ サーバを IP アドレスで識別するか、名前で指定するかを選択します。
- [IP バージョン]:サポートする IP 形式を選択します。

- [IPv6 アドレス タイプ]:IPv6 アドレス タイプを選択します(IPv6 が使用される場合)。次のオプションがあります。
  - [リンク ローカル]:IPv6 アドレスによって、単一ネットワーク リンク上のホストが一意に識別されます。リンク ローカル アドレスのプレフィックス部は FE80::/10 です。このタイプのアドレスはルーティング不能であり、ローカル ネットワーク内で通信する場合にのみ使用できます。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。
  - [グローバル]:IPv6 アドレスは、他のネットワークから認識可能かつアクセス可能なグローバル ユニキャスト IPV6 タイプになります。
- [リンクローカルインターフェイス]:リストからリンク ローカル インターフェイスを選択します(IPv6 アドレス タイプとしてリンク ローカルが選択されている場合)。
- [ログサーバの IP アドレス/名前]:ログ サーバの IP アドレスまたはドメイン名を入力します。
- [UDP ポート]:ログ メッセージの送信先となる UDP ポートを入力します。
- [ファシリティ]:リモート サーバに送信されるシステム ログの出力元のファシリティの値を選択します。サーバに割り当てられるファシリティ値は 1 つだけです。ファシリティコードが 2 度割り当てられると、最初のファシリティ値は上書きされます。
- [説明]:サーバの説明を入力します。
- [最小重大度]:サーバに送信されるシステム ログ メッセージの最小重大度を選択します。

ステップ 5 [適用] をクリックします。[リモート ログ サーバの追加] ページが閉じ、SYSLOG サーバが追加されて、実行コンフィギュレーション ファイルが更新されます。

ファイル管理

「各種管理:ファイル管理」を参照してください。

プラグアンドプレイ(PNP)

新しいネットワーク デバイスの設置やデバイスの交換を手作業で行うと、費用と時間がかかり、誤りが発生しやすくなります。通常、新しいデバイスは最初に中心的な準備施設に送られ、そこでデバイスを開梱し、ステージング ネットワークに接続し、適切なライセンス、設定、イメージを使って更新します。その後、デバイスを梱包して実際の設置場所に運びます。これらの手順が完了した後、専門的な担当者が設置場所まで出向いて設置作業を行う必要があります。デバイスが NOC/データ センター自体に設置される場合でも、デバイスの数が非常に多くて専門家が不足する可能性があります。このすべての問題のために、デプロイが遅れ、運用コストがさらに増えます。

Cisco Plug-n-Play ソリューションを使用すると、ネットワーク デバイスのデプロイ/設置に関連するコストを減らし、設置のスピードを上げ、セキュリティを損なわずにより簡単にデプロイできます。Cisco Plug-n-Play ソリューションを使用すると、さまざまなデプロイ シナリオやデプロイ場所でスイッチをゼロ タッチ インストールすることができます。

PNP 設定

PNP を設定するには、次のようにします。

注　この機能はデフォルトで有効になっています。

ステップ 1　[管理] > [PNP] > [PNP 設定] をクリックします。

ステップ 2　次のフィールドに情報を入力して、PNP を設定します。

- [PNP 状態]:デフォルトで有効になっています。

[PNP トランスポート]:PNP エージェント セッション情報とパラメータを定義します。

- [設定の定義]:使用するトランスポート プロトコル、PNP サーバ アドレス、および使用する TCP ポートに関する設定情報を取得するためのオプションとして、次のいずれかを選択します。
  - [デフォルト設定]:このオプションを選択すると、DHCP オプション 43 から PNP 設定が取得されます。DHCP オプション 43 から一部または全部の情報が得られない場合、次のデフォルト値が使用されます:デフォルト トランスポート プロトコル HTTP、PNP サーバの DNS 名 "pnpserver"、ポートは HTTP に関連します。

    [デフォルト設定] オプションを選択すると、[PNP トランスポート] セクションのすべてのフィールドがグレー表示になります。

- [手動設定]:PNP トランスポートに使用する TCP ポートとサーバを手動で設定します。

- [TCP ポート]:TCP ポートの番号。システムにより次のように自動入力されます:80（HTTP 用）
- [サーバ指定方法]:PNP サーバを IP アドレスで指定するか、それとも名前で指定するかを選択します。
- [IP バージョン]:サポートする IP 形式を選択します。
- [サーバ IPv6 アドレス タイプ]:IP バージョン タイプが IPv6 である場合は、次のいずれかのオプションを選択します。
  - [リンク ローカル]:IPv6 アドレスによって、単一ネットワーク リンク上のホストが一意に識別されます。リンク ローカル アドレスのプレフィックス部は **FE80** です。このタイプのアドレスはルーティング不能であり、ローカル ネットワーク内で通信する場合にのみ使用できます。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。
  - [グローバル]:IPv6 アドレスは、他のネットワークから認識可能かつアクセス可能なグローバル ユニキャスト IPV6 タイプになります。
- [リンク ローカル インターフェイス]:送信元 IPv6 アドレス タイプが [リンク ローカル] である場合は、どこから IPv6 アドレスを受け取るかを選択します。
- [サーバの IP アドレス/名前]:PNP サーバの IP アドレスまたはドメイン名を入力します。

PNP ユーザ

- [ユーザ定義]:サーバに送られる PNP パケットに含まれるユーザ情報。次のいずれかのオプションを選択します。
  - [デフォルト値]:このオプションを選択すると、PNP ユーザ名とパスワードの設定が DHCP オプション 43 から取得されます。このオプションを選択すると、ユーザ名とパスワードのフィールドがグレー表示になります。
  - [手動設定]:PNP ユーザ名とパスワードを手動で設定するにはこれを選択します。
- [ユーザ名]:PNP パケットに含めるユーザ名。
- [パスワード]:暗号化形式またはプレーンテキスト形式のパスワード。

[PNP 動作設定]:次のパラメータを入力します。

- [再接続間隔]:接続が失われた後、セッションの再接続を試行するまでの間隔（秒数）。
- [ディスカバリ タイムアウト]:PNP サーバのディスカバリに失敗した後、ディスカバリを再試行するまでの待機時間（秒数）を指定します。
- [タイムアウト指数因子]:指数を使ってディスカバリ試行をトリガーする値。前のタイムアウト値を指数で乗算し、その結果をタイムアウトとして適用します（値がタイムアウト最大値より小さい場合）。
- [ディスカバリ タイムアウト最大値]:タイムアウトの最大値。[ディスカバリ タイムアウト] 値よりも大きくなければなりません。
- [ウォッチドッグ タイムアウト]:アクティブな PNP セッション中（たとえばファイル ダウンロード処理中）に PnP またはファイル サーバからの応答を待つ間隔。

ステップ 3 [適用] をクリックします。パラメータが、実行コンフィギュレーション ファイルにコピーされます。

暗号化されたパスワードを表示するには、[機密データを平文で表示] をクリックします。

PNP セッション

この画面には、現在有効になっている PNP パラメータの値が表示されます。該当する場合、パラメータのソースが括弧で示されます。

PNP パラメータについての情報を表示するには、次のようにします。

ステップ 1 [管理] > [PNP] > [PNP セッション] をクリックします。

次のフィールドが表示されます。

- [管理ステータス]:PNP が有効になっているかどうか。
- [動作ステータス]:PNP が動作中かどうか。
- [PNP エージェント状態]:アクティブな PNP セッションが存在するかどうかを示します。可能な値は、[ディスカバリ待機]、[ディスカバリ]、[準備未完了]、[無効]、[セッション]、[セッション待機] です。
- [トランスポートプロトコル]:PNP エージェント セッション情報を表示します。
- [TCP ポート]:PNP セッションの TCP ポート。

- [サーバ IP アドレス]:PNP サーバの IP アドレス。
- [ユーザ名]:PNP パケットで送信されるユーザ名。
- [パスワード MD5]:PNP パケットで送信されるパスワード。
- [ディスカバリ タイムアウト]:設定済みのディスカバリ タイムアウト
- [セッション間隔タイムアウト]:設定済みのセッション間隔タイムアウト(PNP エージェント状態が「待機中」の場合にのみ表示されます)。
- [残りのタイムアウト]:残っているタイムアウトの値。

注 [再開] ボタンをクリックすると、ただちに PnP エージェントが次のように待機状態を終了します。

- エージェントがディスカバリ待機中状態の場合は、ディスカバリ状態に設定されます。
- エージェントが PnP セッション待機中状態の場合は、PnP セッション状態に設定されます。

リブート

ジャンボ フレームのサポートを有効にするなど、コンフィギュレーションを変更した場合、その変更を有効にするためにシステムをリブートしなければならないことがあります。ただし、デバイスをリブートすると、実行コンフィギュレーションが削除されるので、デバイスをリブートする前に、実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存しておくことが重要です。[適用] をクリックしても、コンフィギュレーションはスタートアップ コンフィギュレーションに保存されません。ファイルおよびファイル タイプの詳細については、「システム ファイル」の項をご覧ください。

[ファイル操作] ページを使用するか、ウィンドウの上にある [保存] をクリックして、デバイス設定をバックアップできます。同じページを使用して、リモート デバイスからコンフィギュレーションをアップロードすることもできます。

将来の時刻にリブートするようにリブート時刻を設定しておくとよい場合があります。次のようなケースが考えられます。

- ユーザがリモート デバイス上でアクションを実行しており、そのアクションのミスが原因でリモート デバイスへの接続が失われる可能性がある場合。リブートをあらかじめスケジュールしておけば、指定した時間の経過後に動作設定が復元され、リモート デバイスへの接続を復元することができます。これらのアクションが正常に終了した場合は、遅延リブートを手動でキャンセルできます。

- デバイスのリロードによってネットワーク接続が失われる場合。遅延リブートを使用することにより、ユーザにとって都合のよい時間（深夜など）にリブートをスケジュールできます。

デバイスをリブートするには、次のようにします。

ステップ 1 [各種管理] > [リブート] の順にクリックします。

ステップ 2 [リブート] ボタンをクリックし、デバイスをリブートします。

- [リブート]：デバイスをリブートします。デバイスをリブートすると実行コンフィギュレーション内の保存されていない情報は破棄されてしまうので、ウィンドウの右上隅にある [保存] をクリックして、起動中に現在のコンフィギュレーションが保持されるようにする必要があります。[保存] オプションが表示されない場合は、実行コンフィギュレーションがスタートアップ コンフィギュレーションと一致しており、保存する必要がないことを意味しています。

  次のオプションが選択できます。

  - [即時]：すぐにリブートします。
  - [日付]：スケジュールするリブートの日付（月/日）、および時間（時間と分）を入力します。ソフトウェアのリロードがスケジュールされ、指定した時刻（24 時間形式）に実行されます。月と日を指定すると、指定した日時にリロードを実行するようにスケジュールされます。月と日を指定しない場合は、その日（指定時刻が現在時より後の時刻である場合）か、翌日（指定時刻が現在時より前の時刻である場合）の指定時刻にリロードが実行されます。00 時 00 分を指定すると、午前 0 時にリロードがスケジュールされます。リロードは 24 日以内に行われる必要があります。

  注 このオプションを使用するには、システム時刻が手動もしくは SNTP で設定されている必要があります。

  注 リブートがスケジュールされている場合は、[リブートのキャンセル] をクリックしてスケジュールされたリブートをキャンセルします。

  - [以内]：指定した時間および分以内にリブートを実行します。指定できる最大時間は 24 日です。

- [工場出荷時設定に戻す]：工場出荷時のデフォルト設定を使用してデバイスをリブートします。このプロセスでアクティブ イメージ、ミラー コンフィギュレーション、およびローカリゼーション ファイルを除くすべてが消去されます。
- [スタートアップコンフィギュレーションファイルのクリア]：次にデバイスを起動する際に、そのデバイスのスタートアップ コンフィギュレーションをクリアする場合、オンにします。

ディスカバリ - Bonjour

「Bonjour」を参照してください。

ディスカバリ - LLDP

「ディスカバリ - LLDP」を参照してください。

ディスカバリ - CDP

「ディスカバリ - CDP」を参照してください。

デバイスの特定

この機能は、ネットワーク内の特定のデバイス上のすべてのネットワーク ポート LED を点滅させることにより、そのデバイスを物理的に特定できるようにします。この機能は、複数のデバイスが相互接続された部屋の中でのデバイスの特定に役立ちます。この機能がアクティブになっている場合は、デバイス上のすべてのネットワーク ポート LED が設定された期間（デフォルトは 1 分間）点滅します。

ステップ 1 [管理] > [デバイスの特定] の順にクリックします。

ステップ 2 次のフィールドに値を入力します。

- [時間]: ポートの LED を点滅させる時間（秒単位）を入力します。
- [残り時間]; このフィールドは、この機能がアクティブになっている場合にのみ表示されます。ここには、LED が点滅する残り時間が表示されます。

ステップ 3 [ユニット ID]この機能をアクティブにするには、[開始] をクリックします。

この機能がアクティブになると、[開始] ボタンが [停止] ボタンに変わります。このボタンを使用すれば、定義されたタイマーが切れる前に LED の点滅を停止できます。

Ping

Ping ユーティリティは、リモート ホストに到達できるかどうかをテストし、デバイスから宛先デバイスに送信したパケットが往復に要した時間を計測します。

Ping は、Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）エコー リクエスト パケットを対象ホストに送信し、pong とも呼ばれる ICMP 応答を待機することで動作します。往復にかかった時間が計測され、すべてのパケット ロスが記録されます。

ホストを ping するには、次のようにします。

ステップ 1 [各種管理] > [Ping] の順にクリックします。

ステップ 2 次のフィールドに情報を入力して Ping を設定します。

- [ホスト指定方法]: 送信元インターフェイスを IP アドレスで指定するか、名前で指定するかを選択します。このフィールドは、次に説明する、[送信元 IP] フィールドに表示されるインターフェイスに影響を及ぼします。
- [IP バージョン]: 送信元インターフェイスを IP アドレスで指定する場合は、IPv4 または IPv6 を選択し、選択した形式で入力することを示します。
- [ソース IP]: 送信元インターフェイスを選択します。この IPv4 アドレスが、宛先との通信で送信元 IPv4 アドレスとして使用されます。[ホスト指定方法] フィールドに [名前] を指定した場合、ドロップダウン フィールドにはすべての IPv4 および IPv6 アドレスが表示されます。[ホスト指定方法] フィールドに [IP アドレス] を指定した場合、[IP バージョン] フィールドで指定したタイプの既存の IP アドレスのみが表示されます。

  注 [自動] オプションを選択した場合、宛先アドレスを基に、システムが送信元アドレスを計算します。

- [送信先IPv6 アドレスタイプ]: 次のいずれかのオプションを選択します。
  - [リンク ローカル]: IPv6 アドレスによって、単一ネットワーク リンク上のホストが一意に識別されます。リンク ローカル アドレスのプレフィックス部は **FE80** です。このタイプのアドレスはルーティング不能であり、ローカル ネットワーク内で通信する場合にのみ使用できます。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。
  - [グローバル]: IPv6 アドレスは、他のネットワークから認識可能かつアクセス可能なグローバル ユニキャスト IPV6 タイプになります。

- [リンクローカルインターフェイス]:IPv6 アドレス タイプが [リンクローカル] である場合は、どこから IPv6 アドレスを受け取るかを選択します。
- [宛先 IP アドレス/名前]:ping 対象デバイスのアドレスまたはホスト名。IP アドレスかホスト名かは、[ホスト指定方法] によって決まります。
- [ping 間隔]:システムが ping パケット間で待機する時間。ping は、成功したかどうかにかかわらず、[ping 回数] フィールドで設定した回数繰り返されます。デフォルトの間隔を使用するか、特定の値を指定します。
- [ping 回数]:ping 操作を実行する回数。デフォルト値を使用するか、特定の値を指定します。
- [ステータス]:ping が正常に実行されたかどうかが表示されます。

ステップ 3 ホストを ping するには、[ping の実行] をクリックします。Ping のステータスが表示され、メッセージのリストにメッセージが追加されて、Ping 操作の結果が示されます。

ステップ 4 このページの [Pingカウンタとステータス] セクションに Ping の結果が表示されます。

- [送信済みパケット数]:ping によって送信されたパケット数
- [受信済みパケット数]:ping によって受信されたパケット数
- [パケットロス]:ping プロセス中に消失したパケットの割合
- [最低ラウンドトリップ時間]:パケットが戻るまでの最短時間
- [最大ラウンドトリップ時間]:パケットが戻るまでの最長時間
- [平均ラウンドトリップ時間]:パケットが戻るまでの平均時間
- [ステータス]:失敗か成功か

トレースルート

トレースルートは、IP パケットをターゲット ホストに送信し、デバイスに戻すことにより、パケットが転送される IP ルートを検出します。[トレースルート] ページには、デバイスとターゲット ホスト間の各ホップ、および各ホップのラウンドトリップ時間が表示されます。

ステップ 1 [各種管理] > [トレースルート] の順にクリックします。

ステップ 2 次のフィールドに情報を入力して、トレースルートを設定します。

- [ホスト指定方法]:ホストを IP アドレスで指定するか、名前で指定するかを選択します。

- [IP バージョン]:ホストを IP アドレスで指定する場合は、IPv4 または IPv6 を選択し、選択した形式で入力することを示します。
- [ソース IP]:送信元インターフェイスを選択します。この IPv4 アドレスが、通信メッセージの送信元 IPv4 アドレスとして使用されます。[ホスト指定方法] フィールドに [名前] を指定した場合、ドロップダウン フィールドにはすべての IPv4 および IPv6 アドレスが表示されます。[ホスト指定方法] フィールドに [IP アドレス] を指定した場合、[IP バージョン] フィールドで指定したタイプの既存の IP アドレスのみが表示されます。
- [ホストの IP アドレス/名前]:ホスト アドレスまたは名前を入力します。
- [TTL]:トレースルートで許可する最大ホップ数を入力します。送信したフレームが無限ループに入るのを防ぐために使用します。トレースルート コマンドは、宛先に到達するか、設定した値に達すると終了します。デフォルト値(30)を使用する場合は [デフォルトを使用] を選択します。
- [タイムアウト]:システムがフレームの損失を宣言する前に、フレームが戻るのを待機する時間を入力するか、[デフォルトを使用] を選択します。

ステップ 3 [トレースルートのアクティブ化] をクリックします。処理が実行されます。

ページが表示され、ラウンド トリップ時間(RTT)、および各トリップのステータスが次のフィールドに表示されます。

- [インデックス]:ホップの数が表示されます。
- [ホスト]:宛先までのルートにある停止位置が表示されます。

[ラウンドトリップ時間(1-3)]:第 1 フレームから第 3 フレームまでのラウンドトリップ時間(ミリ秒単位)、および第 1 から第 3 までの操作のステータスが表示されます。

7

各種管理:ファイル管理

ここでは、システム ファイルの管理方法について説明します。

具体的な内容は、次のとおりです。

- システム ファイル
- ファームウェア操作
- ファイル操作
- ファイル ディレクトリ
- DHCP 自動コンフィギュレーション/イメージ更新

システム ファイル

システム ファイルとは、コンフィギュレーション情報やファームウェア イメージなどの情報を格納したファイルです。

通常、**flash://system/** フォルダに含まれるファイルはシステム ファイルです。

これらのファイルを使用してさまざまなアクションが実行されます。たとえば、デバイス ブートの元となるファームウェア ファイルの選択、デバイス内部でのさまざまなタイプのコンフィギュレーション ファイルのコピー、外部サーバなどの外部デバイスとの間のファイルのコピーなどです。

デバイス上のコンフィギュレーション ファイルはそれぞれのタイプによって定義され、そのデバイスの設定やパラメータ値を格納します。

デバイス上の他のファイルには、ファームウェア ファイル、ログ ファイルがあり、これらは*動作ファイル*と呼ばれます。

コンフィギュレーション ファイルはテキスト ファイルであり、PC などの外部デバイスにコピーした後、メモ帳などのテキスト エディタで編集できます。

ファイルおよびファイル タイプ

デバイス上に存在するファイルのタイプの例を次に説明します。

- **実行コンフィギュレーション**:デバイスが動作するために現在使用しているパラメータが含まれています。デバイスのパラメータ値を変更すると、このファイルが変更されます。

  デバイスがリブートされると、実行コンフィギュレーションは失われます。

  デバイスに対して加えた変更を保持するには、実行コンフィギュレーションをスタートアップ コンフィギュレーションか、他のファイル タイプに保存する必要があります。

- **スタートアップ コンフィギュレーション**:別のコンフィギュレーション（通常は実行コンフィギュレーション）をスタートアップ コンフィギュレーションにコピーすることにより保存されるパラメータ値。

  スタートアップ コンフィギュレーションはフラッシュに保存され、デバイスがリブートしても保持されます。デバイスがリブートすると、スタートアップ コンフィギュレーションは RAM にコピーされ、実行コンフィギュレーションとして認識されます。

- **ミラー コンフィギュレーション**:次の状況が生じている場合にデバイスによって作成されるスタートアップ コンフィギュレーションのコピー。

  - デバイスが 24 時間続けて稼動している。
  - 24 時間、実行コンフィギュレーションの内容が変更されていない。
  - スタートアップ コンフィギュレーションと実行コンフィギュレーションが同じである。

  スタートアップ コンフィギュレーションからミラー コンフィギュレーションへのコピーはシステムによってのみ行われます。ただし、ミラー コンフィギュレーションから別のファイル タイプや別のデバイスに手動でコピーすることはできます。

  実行コンフィギュレーションをミラーコンフィギュレーションに自動的にコピーするオプションは、[ファイル ディレクトリ] ページで無効にできます。

- **バックアップ ファイル**:システム シャットダウンからの保護や、特定の運用状態の維持のために、ファイルを手動でコピーしたもの。たとえば、ミラー コンフィギュレーション、スタートアップ コンフィギュレーション、および実行コンフィギュレーションを、バックアップ ファイルにコピーできます。バックアップはフラッシュ内か、PC または USB ドライブ上に存在し、デバイスがリブートしても保持されます。

- **ファームウェア**:デバイスの動作と機能を制御するプログラム。より一般的にはイメージと呼ばれます。
- **言語ファイル**:Web ベースのコンフィギュレーション ユーティリティのウィンドウを、選択した言語で表示できるようにする辞書。
- **ロギング ファイル**:フラッシュ メモリ内に保存される SYSLOG メッセージ。

ファームウェア操作

[ファームウェア操作] ページは次の用途に使用できます。

- ファームウェア イメージの更新またはバックアップ
- アクティブ イメージのスワップ

次のファイル転送方法がサポートされています。

- ブラウザの機能を使用する HTTP/HTTPS
- USB
- TFTP サーバを必要とする TFTP
- SCP サーバを必要とする Secure Copy Protocol（SCP）

デバイスには 2 つのファームウェア イメージが保存されています。一方のイメージは*アクティブ イメージ*となり、もう一方のイメージは*非アクティブ イメージ*となります。

デバイスのファームウェアを更新すると、新しいファームウェアが非アクティブ イメージを必ず上書きします。デバイスに新しいファームウェアをアップロードすると、次に起動する際には新しいバージョンが使用されます。リブート後、元のバージョンは非アクティブ バージョンになります。

HTTP/HTTPS または USB を使用してファームウェアを更新またはバックアップするには、次のようにします。

ステップ 1 [各種管理] > [ファイル管理] > [ファームウェア操作] の順にクリックします。

次のフィールドが表示されます。

- [アクティブなファームウェアファイル]:現在のアクティブなファームウェア ファイルを表示します。

- [アクティブなファームウェアバージョン]:現在のアクティブなファームウェア ファイルのバージョンを表示します。

ステップ 2 次のフィールドを入力します。

- [操作タイプ]:[ファームウェアの更新] または[ファームウェアのバックアップ]を選択します。
- [コピー方法]:[HTTP/HTTPS] または [USB] を選択します。
- [ファイル名]:更新するファイルの名前を入力します(HTTP/HTTPS によるバックアップは該当せず)。

ステップ 3 [適用] をクリックします。

ステップ 4 [リブート] をクリックします。

TFTP を使用してファームウェアを更新またはバックアップするには、次のようにします。

ステップ 1 [各種管理] > [ファイル管理] > [ファームウェア操作] の順にクリックします。

次のフィールドが表示されます。

- [アクティブなファームウェアファイル]:現在のアクティブなファームウェア ファイルを表示します。
- [アクティブなファームウェアバージョン]:現在のアクティブなファームウェア ファイルのバージョンを表示します。

ステップ 2 次のフィールドを入力します。

- [操作タイプ]:[ファームウェアの更新] または[ファームウェアのバックアップ]を選択します。
- [コピー方法]:[TFTP] を選択します。
- [サーバ指定方法]:TFTP サーバを IP アドレスで指定するか、名前で指定するかを選択します。

[サーバ指定方法] がアドレス指定の場合:

- [IP バージョン]:([サーバ指定方法] がアドレス指定の場合)このサーバに IPv4 アドレスと IPv6 アドレスのどちらを使用するかを選択します。

- [IPv6 アドレス タイプ]：IPv6 アドレス タイプを選択します（IPv6 が使用される場合）。次のオプションがあります。
  - [リンク ローカル]：IPv6 アドレスによって、単一ネットワーク リンク上のホストが一意に識別されます。リンク ローカル アドレスのプレフィックス部は FE80 です。このタイプのアドレスはルーティング不能であり、ローカル ネットワーク内で通信する場合にのみ使用できます。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。
  - [グローバル]：IPv6 アドレスは、他のネットワークから認識可能かつアクセス可能なグローバル ユニキャスト IPV6 タイプになります。
- [リンクローカルインターフェイス]：リストからリンク ローカル インターフェイスを選択します（IPv6 が使用される場合）。
- [サーバの IP アドレス/名前]：TFTP サーバの IP アドレスまたは名前を入力します。どちらでも構いません。
- （更新）[ソース]：ソース ファイル名を入力します。
- （バックアップ）[宛先]：バックアップ ファイル名を入力します。

ステップ 3 操作を開始するには、[適用] をクリックします。

SCP を使用してファームウェアを更新またはバックアップするには、次のようにします。

ステップ 1 [各種管理] > [ファイル管理] > [ファームウェア操作] の順にクリックします。

次のフィールドが表示されます。

- [アクティブなファームウェアファイル]：現在のアクティブなファームウェア ファイルを表示します。
- [アクティブなファームウェアバージョン]：現在のアクティブなファームウェア ファイルのバージョンを表示します。

ステップ 2 次のフィールドを入力します。

- [操作タイプ]：[ファームウェアの更新] または [ファームウェアのバックアップ] を選択します。
- [コピー方法]：[SCP] を選択します。

ステップ 3 **リモート SSH サーバ認証**による SSH サーバ認証（デフォルトでは無効）を有効にするには、[編集] をクリックします。そうすると、[SSH サーバ認証] ページに移動するので、ここで SSH サーバを設定します。

ステップ 4 このページに戻ります。

ステップ 5 [SSH クライアント認証] を実行するには、次のメソッドのいずれかを選択します。

- [SSH クライアントシステムクレデンシャルの使用]：固定 SSH ユーザ クレデンシャルを設定します。[SSH ユーザ認証] ページに移動するには、[システムクレデンシャル] をクリックします。このページで、恒久的に使用するユーザとパスワードを設定できます。
- [SSH クライアントのワンタイムクレデンシャルを使用]：次の値を入力します。
  - [ユーザ名]：今回のコピー アクションに使用するユーザ名を入力します。
  - [パスワード]：今回のコピーに使用するパスワードを入力します。

  注 ワンタイム クレデンシャルに使用するユーザ名とパスワードは、コンフィギュレーション ファイルに保存されません。

ステップ 6 次のフィールドを入力します。

- [サーバ指定方法]：SCP サーバを IP アドレスで指定するか、ドメインの名前で指定するかを選択します。

[サーバ指定方法] がアドレス指定の場合：

- [IP バージョン]：IPv4 と IPv6 のどちらのアドレスを使用するかを選択します。
- [IPv6 アドレス タイプ]：IPv6 アドレス タイプを選択します（IPv6 が使用される場合）。次のオプションがあります。

  [リンク ローカル]：IPv6 アドレスによって、単一ネットワーク リンク上のホストが一意に識別されます。リンク ローカル アドレスのプレフィックス部は **FE80** です。このタイプのアドレスはルーティング不能であり、ローカル ネットワーク内で通信する場合にのみ使用できます。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。

  [グローバル]：IPv6 アドレスは、他のネットワークから認識可能かつアクセス可能なグローバル ユニキャスト IPv6 タイプになります。
- [リンクローカルインターフェイス]：リストからリンク ローカル インターフェイスを選択します。

- [サーバの IP アドレス/名前]:SCP サーバの IP アドレスまたはドメイン名を入力します。どちらでも構いません。
- (更新)[ソース]:ソース ファイル名を入力します。
- (バックアップ)[宛先]:バックアップ ファイル名を入力します。

ステップ 7 [適用] をクリックします。ファイル、パスワード、サーバ アドレスがすべて正しい場合は、次のいずれかの結果になります。

- SSH サーバ認証が([SSH サーバ認証] ページで)有効になっており、SCP サーバが信頼された場合、その操作は成功します。SCP サーバが信頼されない場合、操作は失敗し、エラーが表示されます。
- SSH サーバ認証が有効でない場合は、どの SCP サーバに対しても操作は成功します。

イメージ ファイルを切り替えるには:

ステップ 1 [各種管理] > [ファイル管理] > [ファームウェア操作] の順にクリックします。

次のフィールドが表示されます。

- [アクティブなファームウェアファイル]:現在のアクティブなファームウェア ファイルを表示します。
- [アクティブなファームウェアバージョン]:現在のアクティブなファームウェア ファイルのバージョンを表示します。

ステップ 2 次のフィールドが表示されます。

- [操作タイプ]:[イメージの切り替え] を選択します。
- [リブート後のアクティブイメージ]:リブート後にアクティブにするファームウェア ファイルを選択します。
- [リブート後のアクティブイメージバージョン番号]:リブート後のファームウェア ファイルのバージョンが表示されます。

ステップ 3 [適用] をクリックします。新しいファームウェアを使用してすぐにリロードする場合は、成功メッセージが表示された後で [リブート] をクリックします。

ファイル操作

[ファイル操作] ページからは次の操作を行えます。

- デバイスのコンフィギュレーション ファイルやログを外部デバイスにバックアップする。
- 外部デバイスからデバイスにコンフィギュレーション ファイルを復元する。
- コンフィギュレーション ファイルを複製する。

コンフィギュレーション ファイルを実行コンフィギュレーションに復元すると、インポートされたファイルは、元のファイルにはなかったコンフィギュレーション コマンドを*追加*し、既存のコンフィギュレーション コマンド内のパラメータ値を*上書き*します。

コンフィギュレーション ファイルをスタートアップ コンフィギュレーションに復元すると、新しいファイルによって元のファイルが*置換*されます。

スタートアップ コンフィギュレーションに復元する場合は、その復元されたスタートアップ コンフィギュレーションを実行コンフィギュレーションとして使用するためにデバイスをリブートする必要があります。デバイスをリブートするには、「リブート」で説明されているプロセスを使用します。

いずれかのウィンドウで [適用] をクリックすると、デバイスのコンフィギュレーション設定に加えた変更内容が実行コンフィギュレーションに*のみ*保存されます。

注意 実行コンフィギュレーションをスタートアップ コンフィギュレーションか別のコンフィギュレーション ファイルにコピーしていない場合、デバイスをリブートすると、最後にファイルがコピーされた後に加えられた変更はすべて失われます。

次の組み合わせによる内部ファイル タイプのコピーが可能です。

- 実行コンフィギュレーションから、スタートアップ コンフィギュレーション、または他のバックアップ ファイルへのコピー。
- スタートアップ コンフィギュレーションから、実行コンフィギュレーション、または他のバックアップ ファイルへのコピー。
- バックアップ ファイルから、実行コンフィギュレーション、またはスタートアップ コンフィギュレーションへのコピー。
- ミラー コンフィギュレーションから、実行コンフィギュレーション、スタートアップ コンフィギュレーション、またはバックアップ ファイルへのコピー。

次の項でこれらの操作について説明します。

HTTP/HTTPS、USB、または内部フラッシュを使用してシステム コンフィギュレーション ファイルを更新するには、次のようにします。

ステップ 1 [各種管理] > [ファイル管理] > [ファイル操作] の順にクリックします。

ステップ 2 次のフィールドを入力します。

- [操作タイプ]:[更新ファイル] を選択します。
- [宛先ファイルタイプ]:更新するコンフィギュレーション ファイル タイプを 1 つ選択します。
- [コピー方法]:[HTTP/HTTPS]、[USB]、または [内部フラッシュ] を選択します。
- [ファイル名]:更新元になるファイル（ソース ファイル）の名前を入力します。

ステップ 3 操作を開始するには、[適用] をクリックします。

TFTP を使用してシステム コンフィギュレーション ファイルを更新するには、次のようにします。

ステップ 1 [各種管理] > [ファイル管理] > [ファイル操作] の順にクリックします。

ステップ 2 次のフィールドを入力します。

- [操作タイプ]:[更新ファイル] を選択します。
- [宛先ファイルタイプ]:更新するコンフィギュレーション ファイル タイプを 1 つ選択します。
- [コピー方法]:[TFTP] を選択します。
- [サーバ指定方法]:TFTP サーバを IP アドレスで指定するか、ドメイン名で指定するかを選択します。

  [サーバ指定方法] がアドレス指定の場合:

  - [IP バージョン]:IPv4 と IPv6 のどちらのアドレスを使用するかを選択します。

    [サーバ指定方法] でサーバを名前で選択するように指定した場合、IP バージョン関連のオプションを選択する必要はありません。

- [IPv6 アドレス タイプ]：IPv6 アドレス タイプを選択します（IPv6 が使用される場合）。次のオプションがあります。

  [リンク ローカル]：IPv6 アドレスによって、単一ネットワーク リンク上のホストが一意に識別されます。リンク ローカル アドレスのプレフィックス部は **FE80** です。このタイプのアドレスはルーティング不能であり、ローカル ネットワーク内で通信する場合にのみ使用できます。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。

  [グローバル]：IPv6 アドレスは、他のネットワークから認識可能かつアクセス可能なグローバル ユニキャスト IPV6 タイプになります。

- [リンクローカルインターフェイス]：リストからリンク ローカル インターフェイスを選択します。

- [サーバの IP アドレス/名前]：TFTP サーバの IP アドレスまたは名前を入力します。
- [ソース]：更新ファイル名を入力します。

ステップ 3 操作を開始するには、[適用] をクリックします。

SCP を使用してシステム コンフィギュレーション ファイルを更新するには、次のようにします。

ステップ 1 [各種管理] > [ファイル管理] > [ファイル操作] の順にクリックします。

ステップ 2 次のフィールドを入力します。

- [操作タイプ]：[更新ファイル] を選択します。
- [宛先ファイルタイプ]：更新するコンフィギュレーション ファイル タイプを 1 つ選択します。
- [コピー方法]：[SCP] を選択します。

ステップ 3 **リモート SSH サーバ認証**による SSH サーバ認証（デフォルトでは無効）を有効にするには、[編集] をクリックします。そうすると、[SSH サーバ認証] ページに移動するので、ここで SSH サーバを設定します。

ステップ 4 このページに戻ります。

ステップ 5 [SSH クライアント認証] を実行するには、次のメソッドのいずれかを選択します。

- [SSH クライアントシステムクレデンシャルの使用]：固定 SSH ユーザ クレデンシャルを設定します。[SSH ユーザ認証] ページに移動するには、[システムクレデンシャル] をクリックします。このページで、恒久的に使用するユーザとパスワードを設定できます。
- [SSH クライアントのワンタイムクレデンシャルを使用]：次の値を入力します。
  - [ユーザ名]：今回のコピー アクションに使用するユーザ名を入力します。
  - [パスワード]：今回のコピーに使用するパスワードを入力します。

  注 ワンタイム クレデンシャルに使用するユーザ名とパスワードは、コンフィギュレーション ファイルに保存されません。
- [サーバ指定方法]：SCP サーバを IP アドレスで指定するか、ドメインの名前で指定するかを選択します。

  [サーバ指定方法] がアドレス指定の場合：
  - [IP バージョン]：IPv4 と IPv6 のどちらのアドレスを使用するかを選択します。
  - [IPv6 アドレス タイプ]：IPv6 アドレス タイプを選択します（IPv6 が使用される場合）。次のオプションがあります。

    [リンク ローカル]：IPv6 アドレスによって、単一ネットワーク リンク上のホストが一意に識別されます。リンク ローカル アドレスのプレフィックス部は **FE80** です。このタイプのアドレスはルーティング不能であり、ローカル ネットワーク内で通信する場合にのみ使用できます。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。

    [グローバル]：IPv6 アドレスは、他のネットワークから認識可能かつアクセス可能なグローバル ユニキャスト IPV6 タイプになります。
  - [リンクローカルインターフェイス]：リストからリンク ローカル インターフェイスを選択します。
- [サーバの IP アドレス/名前]：SCP サーバの IP アドレスまたは名前を入力します。
- [ソース]：ソース ファイル名を入力します。

ステップ 6 操作を開始するには、[適用] をクリックします。

HTTP/HTTPS を使用してシステム コンフィギュレーション ファイルをバックアップするには、次のようにします。

ステップ 1 [各種管理] > [ファイル管理] > [ファイル操作] の順にクリックします。

ステップ 2 次のフィールドを入力します。

- [操作タイプ]:[バックアップファイル] を選択します。
- [ソースファイルタイプ]:バックアップするコンフィギュレーション ファイル タイプを 1 つ選択します。
- [コピー方法]:[HTTP/HTTPS] を選択します。
- [機密データの処理]:機密データをバックアップ ファイルに含める方法を選択します。次のオプションが選択できます。
  - [除外]:機密データをバックアップに含めません。
  - [暗号化]:機密データを暗号化してバックアップに含めます。
  - [プレーンテキスト]:機密データをプレーンテキスト形式でバックアップに含めます。

  注 使用可能な機密データ オプションは、現在のユーザの SSD ルールによって決まります。詳細については、「SSD ルール」のページを参照してください。

ステップ 3 操作を開始するには、[適用] をクリックします。

USB または内部フラッシュを使用してシステム コンフィギュレーション ファイルをバックアップするには、次のようにします。

ステップ 1 [各種管理] > [ファイル管理] > [ファイル操作] の順にクリックします。

ステップ 2 次のフィールドを入力します。

- [操作タイプ]:[バックアップファイル] を選択します。
- [ソースファイルタイプ]:バックアップするコンフィギュレーション ファイル タイプを 1 つ選択します。
- [コピー方法]:[USB]、または [内部フラッシュ] を選択します。
- [ファイル名]:宛先バックアップ ファイルの名前を入力します。

- [機密データの処理]:機密データをバックアップ ファイルに含める方法を選択します。次のオプションが選択できます。
  - [除外]:機密データをバックアップに含めません。
  - [暗号化]:機密データを暗号化してバックアップに含めます。
  - [プレーンテキスト]:機密データをプレーンテキスト形式でバックアップに含めます。

  注 使用可能な機密データ オプションは、現在のユーザの SSD ルールによって決まります。詳細については、「SSD ルール」のページを参照してください。

ステップ 3 操作を開始するには、[適用] をクリックします。

TFTP を使用してシステム コンフィギュレーション ファイルをバックアップするには、次のようにします。

ステップ 1 [各種管理] > [ファイル管理] > [ファイル操作] の順にクリックします。

ステップ 2 次のフィールドを入力します。

- [操作タイプ]:[バックアップファイル] を選択します。
- [ソースファイルタイプ]:バックアップするファイルのタイプを選択します。
- [コピー方法]:[TFTP] を選択します。
- [サーバ指定方法]:TFTP サーバを IP アドレスで指定するか、ドメイン名で指定するかを選択します。

  [サーバ指定方法] がアドレス指定の場合:
  - [IP バージョン]:IPv4 と IPv6 のどちらのアドレスを使用するかを選択します。

    [サーバ指定方法] でサーバを名前で選択するように指定した場合、IP バージョン関連のオプションを選択する必要はありません。
  - [IPv6 アドレス タイプ]:IPv6 アドレス タイプを選択します（IPv6 が使用される場合）。次のオプションがあります。

[リンク ローカル]:IPv6アドレスによって、単一ネットワーク リンク上のホストが一意に識別されます。リンク ローカル アドレスのプレフィックス部は **FE80** です。このタイプのアドレスはルーティング不能であり、ローカル ネットワーク内で通信する場合にのみ使用できます。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。

[グローバル]:IPv6 アドレスは、他のネットワークから認識可能かつアクセス可能なグローバル ユニキャスト IPV6 タイプになります。

- [リンクローカルインターフェイス]:リストからリンク ローカル インターフェイスを選択します。

- [サーバの IP アドレス/名前]:TFTP サーバの IP アドレスまたは名前を入力します。
- [宛先]:バックアップ ファイル名を入力します。
- [機密データの処理]:機密データをバックアップ ファイルに含める方法を選択します。次のオプションが選択できます。
  - [除外]:機密データをバックアップに含めません。
  - [暗号化]:機密データを暗号化してバックアップに含めます。
  - [プレーンテキスト]:機密データをプレーンテキスト形式でバックアップに含めます。

  注 使用可能な機密データ オプションは、現在のユーザの SSD ルールによって決まります。詳細については、[セキュア機密データ管理] > [SSD ルール] ページをご覧ください。

ステップ 3 操作を開始するには、[適用] をクリックします。

SCP を使用してシステム コンフィギュレーション ファイルをバックアップするには、次のようにします。

ステップ 1 [各種管理] > [ファイル管理] > [ファイル操作] の順にクリックします。

ステップ 2 次のフィールドを入力します。

- [操作タイプ]:[バックアップファイル] を選択します。
- [ソースファイルタイプ]:バックアップするファイルのタイプを選択します。
- [コピー方法]:[SCP] を選択します。

- [リモートSSH サーバ認証]: リモート SSH サーバ認証の現在の状態。[編集] をクリックして [SSH サーバ認証] に移動し、設定を変更します。

[SSH クライアント認証]: クライアント認証は、次のいずれかの方法で実行できます。

- [SSH クライアントシステムクレデンシャルの使用]: 固定 SSH ユーザ クレデンシャルを設定します。[SSH ユーザ認証] ページに移動するには、[システムクレデンシャル] をクリックします。このページで、恒久的に使用するユーザとパスワードを設定できます。
- [SSH クライアントのワンタイムクレデンシャルを使用]: 次の値を入力します。
  - [ユーザ名]: 今回のコピー アクションに使用するユーザ名を入力します。
  - [パスワード]: 今回のコピーに使用するパスワードを入力します。
- [サーバ指定方法]: SCP サーバを IP アドレスで指定するか、ドメインの名前で指定するかを選択します。
- [IP バージョン]: IPv4 と IPv6 のどちらのアドレスを使用するかを選択します。
- [IPv6 アドレス タイプ]: IPv6 アドレス タイプを選択します（IPv6 が使用される場合）。次のオプションがあります。
  - [リンク ローカル]: IPv6 アドレスによって、単一ネットワーク リンク上のホストが一意に識別されます。リンク ローカル アドレスのプレフィックス部は **FE80** です。このタイプのアドレスはルーティング不能であり、ローカル ネットワーク内で通信する場合にのみ使用できます。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。
  - [グローバル]: IPv6 アドレスは、他のネットワークから認識可能かつアクセス可能なグローバル ユニキャスト IPV6 タイプになります。
- [リンクローカルインターフェイス]: リストからリンク ローカル インターフェイスを選択します。
- [サーバの IP アドレス/名前]: SCP サーバの IP アドレスまたは名前を入力します。
- [宛先]: バックアップ ファイル名を入力します。
- [機密データの処理]: 機密データをバックアップ ファイルに含める方法を選択します。次のオプションが選択できます。
  - [除外]: 機密データをバックアップに含めません。
  - [暗号化]: 機密データを暗号化してバックアップに含めます。

- [プレーンテキスト]:機密データをプレーンテキスト形式でバックアップに含めます。

注 使用可能な機密データ オプションは、現在のユーザの SSD ルールによって決まります。詳細については、[セキュア機密データ管理] > [SSD ルール] ページをご覧ください。

ステップ 3 操作を開始するには、[適用] をクリックします。

システム コンフィギュレーション ファイルをタイプの異なるコンフィギュレーション ファイルにコピーするには、次のようにします。

ステップ 1 [各種管理] > [ファイル管理] > [ファイル操作] の順にクリックします。

ステップ 2 次のフィールドを入力します。

- [操作タイプ]:[重複] を選択します。
- [ソースファイル名]:コピーするコンフィギュレーション ファイル タイプを 1 つ選択します。
- [宛先ファイル名]:宛先コンフィギュレーション ファイルの名前を入力します。

ステップ 3 操作を開始するには、[適用] をクリックします。

ファイル ディレクトリ

[ファイルディレクトリ] ページには、システム内に存在するシステム ファイルが表示されます。

ステップ 1 [各種管理] > [ファイル管理] > [ファイルディレクトリ] の順にクリックします。

ステップ 2 必要に応じて、[自動ミラーコンフィギュレーション] を有効にします。これにより、ミラー コンフィギュレーション ファイルが自動的に作成されるようになります。ミラー コンフィギュレーション ファイルがある場合、この機能を無効にすると、そのファイルが削除されます。ミラー ファイルの説明、およびミラー コンフィギュレーション ファイルを自動作成しないほうがよいかもしれない状況については、システム ファイルをご覧ください。

ステップ 3 ファイルとディレクトリを表示するドライブを選択します。次のオプションが選択できます。

- [フラッシュ]:管理ステーションのルート ディレクトリに含まれるすべてのファイルを表示します。
- [USB]:USB ドライブ上のファイルを表示します。

ステップ 4 [実行] をクリックすると、以下のフィールドが表示されます。

- [ファイル名]:ファイルタイプに応じて、システム ファイルのタイプ、またはファイルの実際の名前。
- [パーミッション]:ユーザに付与されたファイルに対する読み取り/書き込みアクセス許可。
- [サイズ]:ファイル サイズ。
- [最終変更日]:ファイルが変更された日時。
- [フル パス]:ファイルのパス。

DHCP 自動コンフィギュレーション/イメージ更新

自動コンフィギュレーション/イメージ更新機能により、ネットワーク内のスイッチの設定と、そのファームウェアのアップグレードを自動で行うことができます。管理者はこのプロセスを使用して、ネットワーク内のこれらのデバイスのコンフィギュレーションとファームウェアをリモートから最新の状態に保つことができます。

この機能は次の部分で構成されています。

- [自動イメージ更新]:ファームウェア イメージをリモート TFTP/SCP サーバから自動的にダウンロードします。自動コンフィギュレーション/イメージ更新プロセスの終了時に、このファームウェア イメージに従ってデバイスがリブートします。
- [自動コンフィギュレーション]:コンフィギュレーション ファイルをリモート TFTP/SCP サーバから自動的にダウンロードします。自動コンフィギュレーション/イメージ更新プロセスの終了時に、このコンフィギュレーション ファイルに従ってデバイスがリブートします。

注 自動イメージ更新と自動コンフィギュレーションが両方ともリクエストされた場合は、自動イメージ更新が先に実行され、リブートしてから、自動コンフィギュレーションが実行されます。その後、最終的なリブートが実行されます。

この機能を使用するには、デバイスのコンフィギュレーション ファイルとファームウェア イメージの場所と名前を使用して、ネットワーク内の DHCP サーバを設定します。ネットワーク内のデバイスは、既定では DHCP クライアントとして設定されます。DHCP サーバによってデバイスに IP アドレスが割り当てられるとき、デバイスはコンフィギュレーション ファイルとファームウェア イメージに関する情報も受け取ります。コンフィギュレーション ファイルかファームウェア イメージが、現在デバイスで使用しているものと異なる場合、そのファイルまたはイメージをダウンロードしてから、デバイスはリブートします。ここでは、これらのプロセスについて説明します。

自動更新/コンフィギュレーションにより、最新のコンフィギュレーション ファイルとファームウェア イメージを使用してネットワーク内のデバイスを最新に保つことができるだけでなく、ネットワークへのデバイスのクイック インストールも可能となります。これは、開封直後のデバイスは、システム管理者が手動で介入しなくても、コンフィギュレーション ファイルとソフトウェア イメージをネットワークから取得するように設定されているためです。デバイスは、初めて IP アドレスを DHCP サーバに要求するとき、DHCP サーバが指定したコンフィギュレーション ファイルとイメージ（またはその一方）をダウンロードし、それに従ってリブートを実行します。

自動コンフィギュレーション プロセスは、RADIUS サーバ キーや SSH/SSL キーなどの機密情報を含むコンフィギュレーション ファイルのダウンロードをサポートしています。これには、Secure Copy Protocol（SCP）とセキュア機密データ（SSD）機能が使用されます（SSH クライアント認証、およびセキュリティ：セキュア機密データ管理をご覧ください）。

ダウンロード プロトコル（TFTP または SCP）

コンフィギュレーション ファイルとファームウェア イメージは、TFTP サーバか SCP サーバのどちらかからダウンロードできます。

使用するプロトコルを次のように設定します。

- [ファイル拡張子に基づく自動]：（デフォルト）このオプションを選択した場合、ユーザが設定するファイル拡張子を持つファイルは SCP を使用して（SSH 経由で）ダウンロードされ、その他の拡張子を持つファイルは TFTP を使用してダウンロードされます。たとえば、指定したファイル拡張子が *.xyz* の場合、拡張子が *.xyz* のファイルは SCP を使用してダウンロードされ、他の拡張子を持つファイルは TFTP を使用してダウンロードされます。デフォルトの拡張子は .scp です。
- [TFTP のみ]：コンフィギュレーション ファイル名の拡張子が何であれ、TFTP 経由でダウンロードが行われます。
- [SCP のみ]：コンフィギュレーション ファイル名の拡張子が何であれ、SCP 経由（SSH を使用）でダウンロードが行われます。

SSH クライアント認証

SCP は SSH ベースです。デフォルトで、リモート SSH サーバ認証は無効になっているため、デバイスはリモート SSH サーバをすべてそのまま受け入れます。リモート SSH サーバ認証を有効にすると、信頼済みサーバ リストに含まれるサーバのみが使用されるようにできます。

[SSH クライアント認証] のパラメータは、クライアント（デバイス）が SSH サーバにアクセスするのに必要です。デフォルトの SSH クライアント認証パラメータは次のとおりです。

- [SSH認証方式]: ユーザ名/パスワード
- [SSH ユーザ名]: anonymous
- [SSHパスワード]: anonymous

注 [SSH クライアント認証] のパラメータは、ファイルを手動でダウンロードする際（つまり、DHCP 自動設定/イメージ更新機能を使用しないダウンロード）にも使用できます。

自動コンフィギュレーション/イメージ更新プロセス

DHCP 自動コンフィギュレーションでは、受信した DHCP メッセージから取得したコンフィギュレーション サーバの名前とアドレス、およびコンフィギュレーション ファイルの名前とパスがあれば、それらが使用されます。加えて、DHCP イメージ更新では、メッセージ内にファームウェアの間接ファイル名が含まれていれば、そのファイル名が使用します。この情報は、DHCPv4 サーバから受信する**オファー** メッセージと、DHCPv6 サーバから受信する**情報応答**メッセージの中で [DHCP オプション] として指定されています。

この情報が DHCP サーバ メッセージ内に含まれていない場合は、[DHCP 自動コンフィギュレーション/イメージ更新] ページで設定されているバックアップ情報が使用されます。

[自動コンフィギュレーション/イメージ更新] プロセスがトリガーされると（自動コンフィギュレーション/イメージ更新のトリガーを参照）、次に示す一連のイベントが発生します。

自動イメージ更新の開始

- スイッチは、受信した DHCP メッセージに、オプション 125（DHCPv4）、およびオプション 60（DHCPv6）の間接ファイル名があれば、それを使用します。
- DHCP サーバがファームウェア イメージ ファイルの間接ファイル名を送信しなかった場合は、（[DHCP 自動コンフィギュレーション/イメージ更新] ページの）バックアップ間接イメージファイル名が使用されます。
- スイッチは、間接イメージ ファイルをダウンロードし、その中から TFTP/SCP サーバのイメージ ファイル名を抽出します。
- スイッチは、TFTP サーバのイメージ ファイルのバージョンと、スイッチのアクティブ イメージのバージョンを比較します。
- 両者のバージョンが異なる場合、新しいバージョンが非アクティブ イメージにロードされ、リブートが実行されて、この非アクティブ イメージがアクティブ イメージになります。
- SCP プロトコルを使用している場合は、再起動が実行されることを通知する SYSLOG メッセージが生成されます。
- SCP プロトコルを使用している場合は、自動更新プロセスが完了したことを確認する SYSLOG メッセージが生成されます。
- TFTP プロトコルを使用している場合は、このコピー プロセスによって SYSLOG メッセージが生成されます。

自動コンフィギュレーションの開始

- このデバイスは、TFTP/SCP サーバの名前とアドレス、およびコンフィギュレーション ファイルの名前とパス（DHCPv4 オプション：66、150、および 67、DHCPv6 オプション：59 および 60）を使用します（受信した DHCP メッセージに含まれている場合）。
- DHCP サーバによってこれらの情報が送信されなかった場合は、（[DHCP 自動コンフィギュレーション/イメージ更新] ページの）バックアップ サーバの IP アドレス/名前とバックアップ コンフィギュレーション ファイル名が使用されます。
- 新しいコンフィギュレーション ファイルの名前が、デバイス上で使用されていたコンフィギュレーション ファイルの名前と異なる場合、またはデバイスがまだ設定されていなかった場合は、新しいコンフィギュレーション ファイルが使用されます。
- 自動コンフィギュレーション/イメージ更新のプロセスの終了時に、新しいコンフィギュレーション ファイルを使用してデバイスがリブートされます。

- このコピー プロセスによって SYSLOG メッセージが生成されます。

オプションが未設定の場合

- DHCP サーバが DHCP オプションで TFTP/SCP サーバ アドレスを送信せず、バックアップ TFTP/SCP サーバ アドレス パラメータが設定されなかった場合、次の処理が実行されます。
  - **SCP**：自動コンフィギュレーション プロセスは中止されます。
  - **TFTP**：デバイスは、限定されたブロードキャスト アドレス（IPv4 の場合）、またはその IP インターフェイス上にあるすべてのノード アドレス（IPv6 の場合）に対して TFTP 要求メッセージを送信します。その後、最初に応答した TFTP サーバを使用して、自動コンフィギュレーション/イメージ更新のプロセスを続行します。

ダウンロード プロトコルの選択

- コピー プロトコル（SCP/TFTP）をダウンロード プロトコル（TFTP または SCP）の説明に従って選択します。

SCP

- SCP を使用してダウンロードする場合、次のどちらかが当てはまるなら、デバイスは指定した SCP/SSH サーバをすべて（認証なしで）許可します。
  - SSH サーバ認証プロセスが無効である。出荷時設定のままのデバイス（開封直後のデバイスなど）でコンフィギュレーション ファイルをダウンロードできるようにするため、SSH サーバ認証はデフォルトで無効になっています。
  - その SSH サーバが SSH 信頼済みサーバリストに設定されている。

  SSH サーバ認証プロセスが有効な場合、その SSH サーバが SSH 信頼済みサーバ リストにないと、自動コンフィギュレーション プロセスは中止されます。
- その情報が使用できる場合は、SCP サーバへのアクセスが実行され、そこからコンフィギュレーション ファイルやイメージがダウンロードされます。

自動コンフィギュレーション/イメージ更新のトリガー

DHCPv4 経由の自動コンフィギュレーション/イメージ更新は、次の条件が満たされた場合にトリガーされます。

- デバイスの IP アドレスがリブート時に動的に割り当てられるか更新された場合。または、管理アクションにより明示的に更新されるか、リース期間の終了により自動的に更新された場合。明示的な更新は、[IPv4インターフェイス] ページでアクティブ化できます。
- 自動イメージ更新が有効な場合は、DHCP サーバから間接イメージ ファイルを受信するか、バックアップ間接イメージ ファイル名が設定されたときに、自動イメージ更新プロセスがトリガーされます。「間接」という言葉は、それがイメージそのものではなく、イメージへのパス名を保持しているファイルであることを表しています。
- 自動コンフィギュレーションが有効な場合は、DHCP サーバからコンフィギュレーション ファイル名を受信したとき、または、バックアップ コンフィギュレーション ファイル名が設定されたときに、自動コンフィギュレーション プロセスがトリガーされます。

DHCPv6 経由の自動設定/イメージ更新は、次の条件が満たされた場合にトリガーされます。

- DHCPv6 サーバがデバイスに情報を送信する場合。次のケースが考えられます。
  - IPv6 が有効なインターフェイスが、DHCPv6 ステートレス コンフィギュレーション クライアントとして定義されたとき。
  - DHCPv6 メッセージをサーバから受信したとき（例：ユーザが [IPv6 インターフェイス] ページで [再起動] ボタンをクリックしたとき）。
  - DHCPv6 情報がデバイスによって更新されたとき。
  - ステートレス DHCPv6 クライアントを有効にして、デバイスを再起動した後。
- DHCPv6 サーバ パケットにコンフィギュレーション ファイル名オプションが含まれている場合。
- DHCP サーバから間接イメージ ファイル名が提供されたとき、または、バックアップ間接イメージ ファイル名が設定されたときに、自動イメージ更新プロセスがトリガーされます。「間接」という言葉は、それがイメージそのものではなく、イメージへのパス名を保持しているファイルであることを表しています。

DHCP 自動コンフィギュレーション/イメージ更新

デバイスを DHCP クライアントとして設定するには、[DHCP 自動コンフィギュレーション/イメージ更新] ページを使用します。

システムのデフォルトは次のとおりです。

- 自動コンフィギュレーション：無効。
- 自動イメージ更新：無効。
- デバイスは DHCP クライアントとして有効。
- リモート SSH サーバ認証：有効。

開始する前に

この機能を使用するには、デバイスが DHCPv4 クライアントか DHCPv6 クライアントとして設定されている必要があります。デバイスで定義される DHCP クライアントのタイプは、デバイスで定義されるインターフェイスのタイプと関連があります。

自動コンフィギュレーションの準備

DHCP サーバと TFTP/SCP サーバを準備するには、次のようにします。

TFTP/SCP サーバ

- コンフィギュレーション ファイルを作業ディレクトリに置きます。このファイルは、デバイスからコンフィギュレーション ファイルをコピーして作成できます。デバイスがブートされると、このファイルが実行コンフィギュレーション ファイルになります。

DHCP サーバ

次のオプションを使用して DHCP サーバを設定します。

- DHCPv4:
  - 66（単一のサーバ アドレス）、または 150（サーバ アドレスのリスト）
  - 67（コンフィギュレーション ファイル名）
- DHCPv6
  - オプション 59（サーバ アドレス）
  - オプション 60（コンフィギュレーション ファイル名と間接イメージ ファイル名を、カンマで区切って指定）

自動イメージ更新の準備

DHCP サーバと TFTP/SCP サーバを準備するには、次のようにします。

TFTP/SCP サーバ

1. メイン ディレクトリにサブ ディレクトリを作成します。ここにソフトウェア イメージ ファイルを置きます。
2. ファームウェア バージョンのパスと名前が含まれた間接ファイルを作成します（例：cisco\cisco-version.ros が含まれた indirect-cisco.txt ファイル）。
3. この間接ファイルを TFTP/SCP サーバのメイン ディレクトリにコピーします。

DHCP サーバ

次のオプションを使用して DHCP サーバを設定します。

- DHCPv4：オプション 125（間接ファイル名）
- DHCPv6：オプション 60（コンフィギュレーション ファイル名と間接イメージ ファイル名を、カンマで区切って指定）

DHCP クライアントのワーク フロー

ステップ 1 [DHCP 自動コンフィギュレーション/イメージ更新] ページで、自動コンフィギュレーションのパラメータと自動イメージ更新のパラメータ（またはどちらか一方）を設定します。

ステップ 2 [IP コンフィギュレーション] > [IPv4 インターフェイス] ページで [IP アドレス タイプ] を [ダイナミック] に設定します。[IPv4 インターフェイス] ページで [IP アドレス タイプ] を [ダイナミック] に設定し、[Ipv6 インターフェイス] ページでデバイスをステートレス DHCPv6 クライアントとして定義します。

Web コンフィギュレーション

自動コンフィギュレーションや自動更新を設定するには、次のようにします。

ステップ 1 [各種管理] > [ファイル管理] > [DHCP 自動設定/イメージ更新] の順にクリックします。

ステップ 2 値を入力します。

- [DHCP 経由の自動コンフィギュレーション]：このフィールドを選択すると、DHCP 自動コンフィギュレーションが有効になります。この機能はデフォルトで無効になっていますが、このページで有効にすることもできます。

- [ダウンロードプロトコル]:次のいずれかを選択します。
  - [ファイル拡張子に基づく自動]:これを選択すると、自動コンフィギュレーションで、コンフィギュレーション ファイルの拡張子に応じて TFTP プロトコルか SCP プロトコルが使用されます。このオプションを選択する場合、コンフィギュレーション ファイルの拡張子を必ず指定しなければならないわけではありません。指定されていない場合は、次に示すように、デフォルトの拡張子が使用されます。
  - [SCP のファイル拡張子]:[ファイル拡張子に基づく自動] を選択した場合、ファイル拡張子をここで指定できます。この拡張子を持つファイルはすべて、SCP を使用してダウンロードされます。拡張子を入力しなかった場合は、デフォルトの拡張子 **.scp** が使用されます。
  - [TFTP のみ]:これを選択すると、自動コンフィギュレーションには TFTP プロトコルのみが使用されます。
  - [SCP のみ]:これを選択すると、自動コンフィギュレーションには SCP プロトコルのみが使用されます。
- [DHCP を使用したイメージ自動更新]:このフィールドを選択すると、DHCP サーバからファームウェア イメージを更新できるようになります。この機能はデフォルトで無効になっていますが、このページで有効にすることもできます。
- [ダウンロードプロトコル]:次のいずれかを選択します。
  - [ファイル拡張子に基づく自動]:これを選択すると、イメージ ファイルの拡張子に応じて TFTP プロトコルか SCP プロトコルが自動更新で使用されます。このオプションを選択する場合、イメージ ファイルの拡張子を必ず指定しなければならないわけではありません。指定されていない場合は、次に示すように、デフォルトの拡張子が使用されます。
  - [SCP のファイル拡張子]:[ファイル拡張子に基づく自動] を選択した場合、ファイル拡張子をここで指定できます。この拡張子を持つファイルはすべて、SCP を使用してダウンロードされます。拡張子を入力しなかった場合は、デフォルトの拡張子 **.scp** が使用されます。
  - [TFTP のみ]:これを選択すると、自動更新には TFTP プロトコルのみが使用されます。
  - [SCP のみ]:これを選択すると、自動更新には SCP プロトコルのみが使用されます。

- [SCP の SSH 設定]：SCP をコンフィギュレーション ファイルのダウンロードに使用する場合は、次のいずれかを選択します。
- [リモート SSH サーバ認証]：[有効/無効] リンクをクリックすると、[SSH サーバ認証] ページに移動します。このページで、ダウンロードに使用する SSH サーバの認証を有効にし、必要に応じて、信頼済み SSH サーバを入力できます。
- [SSH クライアント認証]：[システムクレデンシャル] リンクをクリックし、[SSH ユーザ認証] ページでユーザ クレデンシャルを入力します。
- [バックアップサーバ定義]：バックアップ サーバを IP アドレス で設定するか、名前で設定するかを選択します。

ステップ 3 [サーバ指定方法] がアドレス指定の場合：

- [IP バージョン]：IPv4 と IPv6 のどちらのアドレスを使用するかを選択します。
- [IPv6 アドレス タイプ]：IPv6 アドレス タイプを選択します（IPv6 が使用される場合）。次のオプションがあります。
  - [リンク ローカル]：IPv6 アドレスによって、単一ネットワーク リンク上のホストが一意に識別されます。リンク ローカル アドレスのプレフィックス部は FE80 です。このタイプのアドレスはルーティング不能であり、ローカル ネットワーク内で通信する場合にのみ使用できます。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。
  - [グローバル]：IPv6 アドレスは、他のネットワークから認識可能かつアクセス可能なグローバル ユニキャスト IPV6 タイプになります。
- [リンクローカルインターフェイス]：リストからリンク ローカル インターフェイスを選択します（IPv6 が使用される場合）。

ステップ 4 次のオプション情報を入力します。この情報は、DHCP サーバから必要な情報が提供されなかった場合に使用されます。

- [バックアップサーバの IP アドレス/名前]：バックアップサーバの IP アドレスか名前を入力します。
- [バックアップコンフィギュレーションファイル名]：バックアップ コンフィギュレーション ファイル名を入力します。
- [バックアップ間接イメージ ファイル名]：使用する間接イメージ ファイル名を入力します。これは、イメージへのパスが含まれたファイルです。間接イメージ ファイル名の例：indirect-cisco.scp。このファイルには、ファームウェア イメージのパスと名前が含まれています。

次のフィールドが表示されます。

- [最終自動コンフィギュレーション/イメージのサーバ IP アドレス]:最後にバックアップを実行したサーバのアドレス。
- [最後に自動コンフィギュレーションで使用したファイル名]:最後のコンフィギュレーション ファイル名を入力します。

ステップ 5 [適用] をクリックします。パラメータが、実行コンフィギュレーション ファイルにコピーされます。

8

各種管理:時刻設定

同期されたシステム クロックは、ネットワーク上のすべてのデバイス間で基準時刻になります。ネットワーク時刻の同期化は非常に重要です。ネットワークの管理、セキュリティ保護、計画、およびデバッグのすべての局面で、イベント発生の判断が必要になるためです。クロックが同期化されていなければ、セキュリティ違反やネットワーク使用率の追跡時に、デバイス間でログ ファイルを正しく関連付けられなくなります。

また、時刻が同期化されていれば、共有ファイル システムに混乱が生じるのを減らすこともできます。ファイル システムがどのマシン上にあるかに関係なく、変更時間が一貫していることが重要だからです。

以上の理由により、ネットワーク上のすべてのデバイスで設定される時刻が正確であることが必要です。

注 このデバイスは、Simple Network Time Protocol(SNTP; 簡易ネットワーク タイム プロトコル)に対応しています。このプロトコルを有効にすると、デバイスは、SNTP サーバ時刻から取得した時刻でデバイス時刻を動的に同期します。デバイスは SNTP クライアントとしてのみ動作し、他のデバイスにタイム サービスを提供することはできません。

ここでは、システムの時刻、時間帯、および Daylight Savings Time(DST; 夏時間)を設定するときのオプションについて説明します。具体的な内容は、次のとおりです。

- システム時刻の設定
- SNTP モード
- システムの時刻
- SNTP ユニキャスト
- SNTP マルチキャスト/エニーキャスト
- SNTP 認証
- 時間範囲
- 繰り返し時間範囲

システム時刻の設定

システムの時刻を設定する方法としては、ユーザが手動で設定する方法、SNTP サーバを使用して動的に設定する方法、および GUI を実行している PC から同期化する方法があります。SNTP サーバを選択した場合、手動で設定した時刻は、サーバとの通信が確立したときに上書きされます。

デバイスでは、起動プロセスの実行中に、時刻、時間帯、および DST が必ず設定されます。これらのパラメータは、GUI を実行している PC、SNTP、または手動で設定した値から取得されます。ただし、取得に失敗した場合は、工場出荷時の初期状態になります。

時刻

次の方法により、デバイスのシステム時刻を設定することができます。

- [手動]:ユーザの操作で時刻を設定する必要があります。
- [PCから]:ブラウザの情報を使用して、PC から時刻を受信できます。

  コンピュータから取得した時刻の設定は、実行コンフィギュレーション ファイルに保存されます。リブート後にコンピュータから取得した時刻をデバイスで使用できるようにするため、実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーする必要があります。リブート後、時刻は、デバイスへの初回 WEB ログイン時に設定されます。

  この機能を初めて構成したときに、時刻が未設定であった場合、デバイスでは、PC から取得した時刻が設定されます。

  この時刻設定方法は、HTTP 接続と HTTPS 接続のどちらでも有効です。
- [SNTP]:SNTP タイム サーバから時刻を受信できるようになります。SNTP を使用すると、クロック ソースとして SNTP サーバを使用して、ミリ秒まで、デバイスのネットワーク時刻の正確な同期化を行うことができます。SNTP サーバを指定する場合、ホスト名でサーバを識別することを選択すると、GUI で次の 3 つの選択候補が提示されます。
  - time-a.timefreq.bldrdoc.gov
  - time-b.timefreq.bldrdoc.gov
  - time-c.timefreq.bldrdoc.gov

上記の時刻ソースのいずれかに基づいて時刻が設定されると、以後、ブラウザによって時刻は再設定されません。

注　SNTP は、推奨されている時刻設定方法です。

時間帯と夏時間（DST）

時間帯と DST は、次の方法によりデバイスに設定できます。

- DHCP サーバを使用したデバイスのダイナミック設定。この場合、次のように設定されます。
  - ダイナミック DST が有効で使用可能な場合、常に、DST の手動設定より優先されます。
  - サーバからソース パラメータが提供されない場合、またはダイナミック設定がユーザによって無効になっている場合、手動設定が使用されます。
  - 時間帯と DST のダイナミック設定は、IP アドレスのリース時間が切れても続行します。
- 手動で設定した時間帯と DST が実際に使用されるのは、ダイナミック設定が無効になっているか失敗した場合のみです。

  注 ダイナミック時間帯の設定を適用するには、DHCP サーバは、DHCP オプション 100 を指定する必要があります。

SNTP モード

デバイスは、次のいずれかの方法で、SNTP サーバからシステム時刻を受け取ることができます。

- [クライアントブロードキャスト受信(パッシブモード)]：SNTP サーバは時刻をブロードキャストし、デバイスはこれらのブロードキャストをリッスンします。デバイスがこのモードである場合、ユニキャスト SNTP サーバを定義する必要はありません。
- [クライアントブロードキャスト送信(アクティブモード)]：デバイスは、SNTP クライアントとして、SNTP 時刻の更新を定期的に要求します。このモードは、次のいずれかの方法で機能します。
  - [SNTPエニーキャストクライアントモード]：デバイスのブロードキャスト時刻は、サブネットですべての SNTP サーバにパケットを要求し、応答を待機します。
  - [ユニキャストSNTP サーバモード]：デバイスはユニキャスト クエリーを、手動設定された SNTP サーバ リストに送信し、応答を待機します。

デバイスは、上記のすべてのモードを同時にアクティブにできます。最も近いストラタム（参照クロックからの距離）に基づくアルゴリズムに従って、SNTP サーバから受信された最適なシステム時刻が選択されます。

システムの時刻

[システムの時刻] ページを使用して、システム時刻のソースを選択します。ソースが手動である場合は、ここに時刻を入力できます。

注意　システムの時刻を手動で設定し、デバイスを再起動した場合は、手動時刻設定を再入力する必要があります。

システムの時刻を定義するには、次のようにします。

ステップ 1　[各種管理] > [時間設定] > [システムの時刻] の順にクリックします。

次のフィールドが表示されます。

- [実際の時刻（システム時刻源）]：デバイスのシステム時刻。ここには、DHCP 時間帯が表示されます。ユーザ定義の時間帯の頭字語が定義されている場合はそれが表示されます。
- [最後に同期されたサーバ]：システム時刻を最後に取得したときの SNTP サーバのアドレス、ストラタム、およびタイプ。

ステップ 2　次のパラメータを指定します。

- [クロックソース設定]：システム クロックの設定に使用するソースを選択します。
  - [メインクロックソース(SNTP サーバ)]：これが有効になっている場合、システムの時刻は SNTP サーバから取得されます。この機能を使用するには、[SNTP マルチキャスト/エニーキャスト] ページで SNTP サーバへの接続も設定する必要があります。（任意）[SNTP 認証] ページを使用して、SNTP セッションを強制認証します。
  - [代替クロックソース(アクティブ HTTP/HTTPS セッションを介した PC)]：HTTP プロトコルを使用して設定コンピュータから日付と時刻を設定する場合に選択します。

  注 RIP MD5 認証を機能させるには、[クロックソース設定] を上記のいずれかに設定する必要があります。
- [手動設定]：日付と時刻を手動で設定します。SNTP サーバなどの代替時刻ソースがない場合は、現地時間が使用されます。
  - [日付]：システム日付を入力します。
  - [現地時間]：システム時刻を入力します。

- [時間帯設定]：現地時間は、DHCP サーバまたは時間帯のオフセットを介して使用されます。
  - [DHCP から時間帯を取得]：DHCP サーバからの時間帯と DST のダイナミック設定を有効にします。これらのパラメータを設定できるかどうかは、DHCP パケットから検出される情報によって異なります。このオプションを有効にした場合、*デバイスで DHCP クライアントを有効にする必要があります。*

    注 DHCP クライアントは、ダイナミック時間帯の設定を指定するオプション 100 をサポートします。
  - [DHCP からの時間帯]：DHCP サーバから設定された時間帯の頭字語を表示します。この頭字語は、[実際の時刻] フィールドに表示されます
  - [時間帯のオフセット]：*Greenwich Mean Time*（GMT; グリニッジ標準時）と現地時間との差を選択します。たとえば、パリの時間帯のオフセットは GMT +1、ニューヨークの時間帯のオフセットは GMT – 5 になります。
  - [時間帯の頭字語]：この時間帯を表す名前を入力します。この頭字語は、[実際の時刻] フィールドに表示されます。
- [サマータイム設定]：DST の定義方法を選択します。
  - [夏時間]：夏時間を有効にする場合に選択します。
  - [時間設定のオフセット]：GMT からのオフセットの分数を 1 ～ 1440 の範囲で入力します。デフォルトは 60 です。
  - [夏時間タイプ]：次のいずれかをクリックします。

    [米国]：米国で使用されている日付に基づいて DST が設定されます。

    [欧州]：欧州連合およびこの規格を採用しているその他の国で使用されている日付に基づいて DST が設定されます。

    [日付指定]：DST は手動で設定されます。通常は、米国とヨーロッパ諸国以外の国用です。次のパラメータを指定します。

    [繰り返し]：DST を毎年同じ日付に発生させます。

[日付指定] を選択すると、DST の開始と終了をカスタマイズできるようになります。

- [開始]：DST が開始する日付と時刻。
- [終了]：DST が終了する日付と時刻。

ステップ 3 [繰り返し] を選択すると、DST の開始と終了を個別にカスタマイズできるようになります。

- [開始]: 毎年 DST が開始する日付。
  - [曜日]: 毎年 DST が開始する曜日。
  - [週]: 毎年 DST が開始する月の週。
  - [月]: 毎年 DST が開始する月。
  - [時刻]: 毎年 DST が開始する時刻。
- [終了]: 毎年 DST が終了する日付。たとえば、DST を当地毎年 10 月の第 4 週目の金曜日 AM 5:00 に終了するとします。次のパラメータを指定します。
  - [曜日]: 毎年 DST が終了する曜日。
  - [週]: 毎年 DST が終了する月の週。
  - [月]: 毎年 DST が終了する月。
  - [時刻]: 毎年 DST が終了する時刻。

ステップ 4 [適用] をクリックします。システムの時刻値が、実行コンフィギュレーション ファイルに書き込まれます。

SNTP ユニキャスト

最大 16 台のユニキャスト SNTP サーバを設定できます。

注 ユニキャスト SNTP サーバを名前で指定するには、最初にデバイスで DNS サーバを設定する必要があります（「DNS 設定」を参照してください）。

ユニキャスト SNTP サーバを追加するには、次のようにします。

ステップ 1 [各種管理] > [時間設定] > [SNTP ユニキャスト] の順にクリックします。

ステップ 2 次のフィールドを入力します。

- [SNTP クライアントユニキャスト]: これを選択すると、SNTP で事前定義されたユニキャスト クライアントをユニキャスト SNTP サーバと共にデバイスで使用できます。

- [IPv4 送信元インターフェイス]：SNTP サーバとの通信に使用するメッセージのソース IPv4 アドレスとして使用する IPv4 アドレスの IPv4 インターフェイスを選択します。
- [IPv6 送信元インターフェイス]：SNTP サーバとの通信に使用するメッセージのソース IPv6 アドレスとして使用する IPv6 アドレスの IPv6 インターフェイスを選択します。

  注 [自動] オプションが選択されている場合、システムは、発信インターフェイスで定義された IP アドレスからソース IP アドレスを取得します。

このページには、各ユニキャスト SNTP サーバについての次の情報が表示されます。

- [SNTP サーバ]：SNTP サーバの IP アドレス。ストラタム レベルによって、優先サーバまたはホスト名が選択されます。
- [ポール間隔]：ポーリングが有効か無効かを示します。
- [認証キーID]：SNTP サーバとデバイス間の通信に使用されるキー認証。
- [ストラタムレベル]：参照クロックからの距離を数値で示します。ポーリング間隔が有効になっていない場合、SNTP サーバはプライマリ サーバ（ストラタム レベル 1）に設定できません。
- [ステータス]：SNTP サーバのステータス。表示される値は次のとおりです。
  - [アップ]：SNTP サーバは現在正常に動作しています。
  - [ダウン]：SNTP サーバは現在使用できません。
  - [不明]：SNTP サーバの状態が不明です。
  - [処理中]：SNTP サーバへの接続は現在処理中です。
- [最後の応答]：前回この SNTP サーバからの応答が受信された日時。
- [オフセット]：ローカル クロックを基準としたサーバのクロック推定オフセット（ミリ秒）。ホストは、RFC 2030 で説明されているアルゴリズムを使ってこのオフセット値を決定します。
- [遅延]：ローカル クロックとサーバ クロック間のネットワーク パスにおける、ローカル クロックを基準としたサーバ クロックの推定ラウンド トリップ遅延（ミリ秒）。ホストは、RFC 2030 で説明されているアルゴリズムを使ってこの遅延値を決定します。
- [ソース]：SNTP サーバの定義方法（たとえば、手動、DHCPv6 サーバからなど）。
- [インターフェイス]：パケットを受信するインターフェイス。

ステップ 3 ユニキャスト SNTP サーバを追加するには、[SNTPクライアントユニキャスト] を有効にします。

ステップ 4 [追加] をクリックします。

注 すべてのユーザ定義の SNTP サーバを削除するには、[デフォルトサーバの復元] をクリックします。

ステップ 5 次のパラメータを指定します。

- [サーバ指定方法]：SNTP サーバを IP アドレスで識別するか、リストから既知の SNTP サーバを名前で選択するかのいずれかを選択します。

  注 既知の SNTP サーバを指定するには、デバイスがインターネットに接続し、DNS サーバで設定されているか、DNS サーバが DHCP により識別されるように設定されている必要があります。(「DNS 設定」を参照してください)

- [IP バージョン]：IP アドレスのバージョンとして以下を選択します。[バージョン6] または [バージョン4]。

- [IPv6 アドレス タイプ]：IPv6 アドレス タイプを選択します(IPv6 が使用される場合)。次のオプションがあります。

  - [リンク ローカル]：IPv6 アドレスによって、単一ネットワーク リンク上のホストが一意に識別されます。リンク ローカル アドレスのプレフィックス部は **FE80** です。このタイプのアドレスはルーティング不能であり、ローカル ネットワーク内で通信する場合にのみ使用できます。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。

  - [グローバル]：IPv6 アドレスは、他のネットワークから認識可能かつアクセス可能なグローバル ユニキャスト IPV6 タイプになります。

- [リンクローカルインターフェイス]：リストからリンク ローカル インターフェイスを選択します(IPv6 アドレス タイプとしてリンク ローカルが選択されている場合)。

- [SNTP サーバの IP アドレス/名前]：SNTP サーバの IP アドレッサ名を入力します。この形式は、選択されているアドレス タイプによって異なります。

- [ポール間隔]：選択すると、システムの時刻情報を取得するために SNTP サーバのポーリングが有効になります。ポーリング対象のすべての NTP サーバがポーリングされ、クロックは、ストラタム レベル(参照クロックからの距離)が一番低い、アクセス可能なサーバから選択されます。ストラタムが一番低いサーバがプライマリ サーバと見なされます。次に低いストラタムのサーバがセカンダリ サーバと見なされ、それよりストラタムが低いサーバがその下に

位置します。プライマリ サーバがダウンしている場合、デバイスはポーリング設定が有効になっているすべてのサーバをポーリングし、その中でストラタムが一番低いプライマリ サーバを新たに選択します。

- [認証]：認証を有効にする場合、このチェックボックスを選択します。
- [認証キーID]：認証が有効な場合、キー ID の値を選択します。（認証キーの作成は、[SNTP 認証] ページを使用して行います。）

ステップ 6 [適用] をクリックします。STNP サーバが追加され、メインページに戻ります。

SNTP マルチキャスト/エニーキャスト

デバイスは、アクティブ モード/パッシブ モードにすることができます（詳しくは、「SNTP モード」を参照してください）。

サブネット上ですべてのサーバからの SNTP パケットの受信を有効にしたり、SNTP サーバへの時刻要求の送信を有効にしたりするには、次のようにします。

ステップ 1 [各種管理] > [時間設定] > [SNTP マルチキャスト/エニーキャスト] の順にクリックします。

以下のオプションから選択します。

- [SNTP IPv4 マルチキャスト クライアント モード（クライアント ブロードキャスト受信）]：サブネット上の任意の SNTP サーバから、システム時刻の IPv4 マルチキャスト送信を受信する場合に選択します。
- [SNTP IPv6 マルチキャスト クライアント モード（クライアント ブロードキャスト受信）]：サブネット上の任意の SNTP サーバから、システム時刻の IPv6 マルチキャスト送信を受信する場合に選択します。
- [SNTP IPv4 エニーキャスト クライアント モード（クライアント ブロードキャスト送信）]：システムの時刻情報を要求する SNTP IPv4 同期パケットを送信する場合に選択します。パケットは、サブネット上のすべての SNTP サーバに送信されます。
- [SNTP IPv6 エニーキャスト クライアント モード（クライアント ブロードキャスト送信）]：システムの時刻情報を要求する SNTP IPv6 同期パケットを送信する場合に選択します。パケットは、サブネット上のすべての SNTP サーバに送信されます。

ステップ 2 [適用] をクリックし、設定を実行コンフィギュレーション ファイルに保存します。

SNTP 認証

SNTP クライアントは、HMAC-MD5 を使用して応答を認証できます。SNTP サーバはキーと関連付けられており、キーは応答自体とともに MD5 機能への入力として使用されます。MD5 の結果も応答パケットに組み込まれます。

[SNTP認証] ページでは、認証が必要な SNTP サーバとの通信に使用する認証キーを設定できます。

認証キーは、使用している SNTP サーバのタイプに応じて、独立したプロセスで SNTP サーバに作成されます。詳細については、SNTP サーバのシステム管理者に確認してください。

ワークフロー

ステップ 1 後述する [SNTP 認証] ページで認証を有効にします。

ステップ 2 後述する [SNTP 認証] ページでキーを作成します。

ステップ 3 [SNTP ユニキャスト] ページで、このキーを SNTP サーバと関連付けます。

SNTP 認証を有効にして、キーを定義するには、次のようにします。

ステップ 1 [各種管理] > [時間設定] > [SNTP 認証] の順にクリックします。

ステップ 2 デバイスと SNTP サーバ間の SNTP セッションの認証が必要な場合は、[SNTP 認証] を選択します。

ステップ 3 [適用] をクリックしてデバイスを更新します。

ステップ 4 [追加] をクリックします。

ステップ 5 次のパラメータを指定します。

- [認証キー ID]: この SNTP 認証キーを内部的に識別するための番号を入力します。
- [認証キー(暗号化)]: 認証に使用するキーを暗号化形式で入力します（最大 8 文字）。SNTP サーバは、デバイスと同期化するために、このキーを送信する必要があります。

- [認証キー(プレーン テキスト)]:認証に使用するキーをプレーン テキスト形式で入力します(最大 8 文字)。SNTP サーバは、デバイスと同期化するために、このキーを送信する必要があります。
- [信頼済みキー]:デバイスが、この認証キーを使って、SNTP サーバからのみ同期化情報を受信できるようにする場合に選択します。

ステップ 6 [適用] をクリックします。SNTP 認証パラメータが、実行コンフィギュレーション ファイルに書き込まれます。

時間範囲

時間範囲を定義して、以下のタイプのコマンドと関連付けることにより、その時間範囲のみコマンドを適用することができます。

- ACL
- 8021X ポート認証
- ポート設定
- 時間ベースの PoE

時間範囲には以下の 2 つのタイプがあります。

- [絶対]:このタイプの時間範囲は、特定の日付または即時に開始し、特定の日付で終了するか、無制限に実行されます。これは、[時間範囲] ページで作成されます。繰り返し要素をそれに追加することができます。
- [繰り返し]:このタイプの時間範囲には、絶対範囲に追加される時間範囲要素が含まれており、繰り返しに基づいて開始および終了します。これは、[繰り返し時間範囲] ページで定義されます。

時間範囲に絶対範囲と繰り返し範囲の両方が含まれる場合、関連するコマンドの動作は、絶対開始時刻と繰り返し時間範囲の両方に達した場合にのみアクティブ化されます。関連するコマンドの動作は、いずれかの時間範囲に達した時点で非アクティブ化されます。

このデバイスでサポートされる絶対時間範囲は最大 10 個です。

すべての時間仕様はローカル時刻として解釈されます(夏時間はこれに影響しません)。その時間範囲エントリを目的の時刻に確実に実行するために、システム時刻を設定する必要があります。

時間範囲機能は、以下の目的で使用できます。

- 一例として、ネットワークへのコンピュータのアクセスをビジネス時間だけに制限し、その後にネットワーク ポートをロックし、残りのネットワークのアクセスをブロックします(「ポート設定」および「リンクアグリゲーション」を参照してください)。
- 指定した期間だけに PoE 操作を制限します。

絶対時間範囲

絶対時間範囲を定義するには、次のようにします。

ステップ 1 [各種管理] > [時間設定] > [時間範囲] の順にクリックします。

既存の時間範囲が表示されます。

ステップ 2 新規の時間範囲を追加するには、[追加] をクリックします。

ステップ 3 次のフィールドを入力します。

- [時間範囲名]:新規の時間範囲名を入力します。
- [絶対開始時間]:開始時間を定義するには、以下を入力します。
  - [即時]:時間範囲を即時に開始する場合に選択します。
  - [日付]、[時刻]:時間範囲の開始日時を入力します。
- [絶対終了時間]:開始時間を定義するには、以下を入力します。
  - [無期限]:時間範囲を終了させない場合に選択します。
  - [日付]、[時刻]:時間範囲の終了日時を入力します。

ステップ 4 [適用] をクリックします。

ステップ 5 繰り返しの時間範囲を追加するには、[繰り返し時間範囲] をクリックします。

繰り返し時間範囲

繰り返し時間要素は、絶対時間範囲に追加できます。これにより、絶対範囲内の特定の期間に操作が制限されます。

繰り返しの時間範囲要素を絶対時間範囲に追加するには、次のようにします。

ステップ 1 [各種管理] > [時間設定] > [繰り返し時間範囲] の順にクリックします。

既存の繰り返し時間範囲が表示されます（特定の絶対時間範囲ごとにフィルタされます。）

ステップ 2 繰り返し範囲を追加する絶対時間範囲を選択します。

ステップ 3 新規の繰り返し時間範囲を追加するには、[追加] をクリックします。

ステップ 4 次のフィールドを入力します。

- [繰り返し開始時刻]：時間範囲の繰り返しが開始する日時を入力します。
- [繰り返し終了時刻]：時間範囲の繰り返しが終了する日時を入力します。

ステップ 5 [適用] をクリックします。

ステップ 6 [時間範囲] をクリックして [絶対時間範囲] ページにアクセスします。

9

各種管理:ディスカバリ(検出)

ここでは、検出処理の設定について説明します。

具体的な内容は、次のとおりです。

- Bonjour
- LLDP および CDP
- ディスカバリ - LLDP
- ディスカバリ - CDP

Bonjour

Bonjour クライアントであるこのデバイスからは、直接接続している IP サブネットに Bonjour ディスカバリ プロトコル パケットが定期的にブロードキャストされます。これにより、このデバイスの存在およびこのデバイスが提供するサービス(HTTP、HTTPS など)がアドバタイズされます。(このデバイスが提供するサービスの有効/無効は、[セキュリティ] > [TCP/UDPサービス] ページから切り替えることができます)。この結果、このデバイスがネットワーク管理システムやサードパーティ製アプリケーションから*検出*できるようになります。デフォルトでは、管理 VLAN 上で Bonjour が有効になって実行されています。

デバイスがレイヤ 2 システム モードの場合、Bonjour ディスカバリはグローバルに有効になり、Bonjour アドバタイズメントが管理 VLAN に送信されます。このデバイスは、管理者がオンにしたすべてのサービスを [サービス] ページのコンフィギュレーションに基づいてアドバタイズします。

Bonjour ディスカバリと IGMP を両方とも有効にした場合、[IPマルチキャストグループアドレスの追加] ページに Bonjour の IP マルチキャスト アドレスが表示されます。

Bonjour ディスカバリを無効にした場合、デバイスはどのタイプのサービスもアドバタイズしなくなり、ネットワーク管理アプリケーションからのサービス要求への応答もしなくなります。

Bonjour ディスカバリはグローバルにしか有効にできず、ポートごとや VLAN ごとに有効にすることはできません。管理者が有効にしたサービスは、デバイスによってアドバタイズされます。

Bonjour ディスカバリと IGMP を両方とも有効にした場合、[IPマルチキャストグループアドレスの追加] ページに Bonjour の IP マルチキャスト アドレスが表示されます。

Bonjour ディスカバリを無効にした場合、デバイスはサービスのアドバタイズも、ネットワーク管理アプリケーションからのサービス要求への応答もしなくなります。

デフォルトでは、管理 VLAN のメンバーになっているすべてのインターフェイスで Bonjour が有効になっています。

Bonjour を設定するには、次のようにします。

ステップ 1 [各種管理] > [ディスカバリ - Bonjour] の順にクリックします。

ステップ 2 [有効] を選択し、Bonjour ディスカバリをグローバルに有効にします。

ステップ 3 特定のインターフェイスで Bonjour を有効にするには、[追加] をクリックします。

ステップ 4 インターフェイスを選択します。インターフェイスに IP アドレスが割り当てられている場合は、そのアドレスが表示されます。

ステップ 5 [適用] をクリックし、実行コンフィギュレーション ファイルを更新します。

注 インターフェイスで Bonjour を無効にするには、[削除] をクリックします（削除の場合、[適用] をクリックするなどの追加の操作はありません）。

LLDP および CDP

LLDP（Link Layer Discovery Protocol）、および CDP（Cisco Discovery Protocol）は、直接接続された LLDP および CDP 対応のネイバーが、自身とそれぞれの機能をアドバタイズするためのリンク層プロトコルです。デフォルトでは、デバイスはそのすべてのインターフェイスに定期的に LLDP/CDP アドバタイズメントを送信し、着信 LLDP および CDP パケットをプロトコルの要求に従って処理します。LLDP と CDP では、アドバタイズメントは TLV（Type, Length, Value）としてパケット内にエンコードされます。

CDP/LLDP の設定に関する注意点は次のとおりです。

- CDP/LLDP の有効または無効は、グローバルに設定することもポートごとに設定することもできます。ポートの CDP/LLDP 機能は、CDP/LLDP がグローバルに有効な場合のみ使用できます。
- CDP/LLDP がグローバルに有効な場合、デバイスは、CDP/LLDP が無効なポートの着信 CDP/LLDP パケットをフィルタリングします。
- CDP/LLDP がグローバルに無効な場合、デバイスの構成によって、すべての着信 CDP/LLDP パケットの廃棄、VLAN 対応フラッディング、または VLAN 非対応フラッディングを実行できます。VLAN 対応のフラッディングでは、着信 CDP/LLDP パケットは、入力ポートを除き、パケットを受信する VLAN にフラッディングされます。VLAN 非対応のフラッディングでは、着信 CDP/LLDP パケットは、入力ポートを除くすべてのポートにフラッディングされます。デフォルトでは、CDP/LLDP がグローバルに無効な場合は、CDP/LLDP パケットは廃棄されます。着信 CDP および LLDP パケットの廃棄またはフラッディングは、それぞれ [CDP のプロパティ] ページと [LLDP のプロパティ] ページで設定できます。
- Auto Smartport では、CDP または LLDP、もしくは両方を有効にする必要があります。Auto Smartport は、インターフェイスから受信した CDP/LLDP アドバタイズメントに基づいてインターフェイスを自動的に設定します。
- IP 電話などの CDP および LLDP エンド デバイスは、CDP および LLDP アドバタイズメントから音声 VLAN 設定を学習します。デフォルトでは、デバイスは、デバイスに設定された音声 VLAN に基づいて CDP および LLDP アドバタイズメントを送信できるようになっています。詳細については、「音声 VLAN」を参照してください。

注 CDP/LLDP は、ポートが LAG のメンバーであるかどうかを区別しません。複数のポートが 1 つの LAG のメンバーである場合、CDP/LLDP はそのポートが LAG のメンバーであるという事実を考慮せずに各ポートにパケットを送信します。

CDP/LLDP の動作は、インターフェイスの STP ステータスとは無関係です。

802.1x ポート アクセス コントロールがインターフェイスで有効な場合、デバイスは、インターフェイスが認証および承認されている場合にのみ、そのインターフェイスとの間で CDP/LLDP パケットを送受信します。

ポートがミラーリングの対象の場合、CDP/LLDP はそのポートをダウンしたものと見なします。

注 CDP および LLDP は、直接接続された CDP/LLDP 対応のデバイスが自身とそれぞれの機能をアドバタイズするためのリンク層プロトコルです。CDP/LLDP 対応のデバイスが直接接続されておらず、CDP/LLDP 非対応のデバイスと分離している展開では、CDP/LLDP 非対応のデバイスが受信した CDP/LLDP パケットをフラッディングする場合にのみ、CDP/LLDP 対応のデバイスは他のデバイスからアドバタイズメントを受信できます。CDP/LLDP 非対応のデバイスが VLAN 対応フラッディングを実行する場合、CDP/LLDP 対応のデバイスは、同じ VLAN 内に存在する場合のみ、互いにアドバタイズメントを受信できます。CDP/LLDP 非対応のデバイスが CDP/LLDP パケットをフラッディングする場合、CDP/LLDP 対応のデバイスは複数のデバイスからアドバタイズメントを受信することがあります。

ディスカバリ - LLDP

ここでは、LLDP の設定方法を説明します。具体的な内容は、次のとおりです。

- LLDP の概要
- LLDP 設定のワークフロー
- LLDP のプロパティ
- ポート設定
- LLDP MED ネットワーク ポリシー
- LLDP MED ポート設定
- LLDP ポート ステータス
- LLDP ローカル情報
- LLDP ネイバー情報
- LLDP 統計情報
- LLDP 過負荷

LLDP の概要

LLDP は、ネットワーク マネージャがマルチベンダー環境でのネットワーク管理のトラブルシューティングや強化を実行するためのプロトコルです。LLDP では、ネットワーク デバイスが、自身を他のデバイスにアドバタイズする方法、および検出された情報を格納する方法が標準化されています。

LLDP を使用した場合、各デバイスの ID、設定情報、および機能が近隣デバイスにアドバタイズされます。受信側デバイスでは、これらのデータが管理情報ベース（MIB）に格納されます。ネットワーク管理システムでは、これらの MIB データベースに照会することによって、ネットワークのトポロジがモデル化されます。

LLDP はリンク層プロトコルです。デフォルトで、デバイスは、プロトコルの要求に従ってすべての着信 LLDP パケットの終了、および処理を実行します。

LLDP プロトコルには、LLDP Media Endpoint Discovery（LLDP-MED; LLDP メディア エンドポイント検出）という拡張機能があります。LLDP-MED を利用すれば、VoIP 電話やテレビ電話などのメディア エンドポイント デバイスとの間で情報を送受信できます。LLDP-MED の詳細については、「LLDP MED ネットワーク ポリシー」をご覧ください。

LLDP 設定のワークフロー

LLDP 機能を使用して実行できる作業の例と推奨される手順を次に示します。LLDP を設定するためのより詳細なガイドラインは、LLDP/CDP に関するセクションを参照してください。LLDP の設定に関するページは、「LLDP および CDP」セクションからアクセスできます。

1. [LLDP のプロパティ] ページを使用して、LLDP 更新情報の送信間隔などの LLDP グローバル パラメータを入力します。
2. [ポート設定] ページを使用して、ポートごとに LLDP を設定します。このページでは、LLDP PDU の送受信、SNMP 通知の送信、アドバタイズする TLV の指定、デバイスの管理アドレスのアドバタイズについて、インターフェイスを設定できます。
3. [LLDP MED ネットワーク ポリシー] ページを使用して、LLDP MED ネットワーク ポリシーを作成します。
4. [LLDP MED ポート設定] ページを使用して、LLDP MED ネットワーク ポリシーとオプションの LLDP-MED TLV を必要なインターフェイスにバインドします。
5. Auto Smartport で LLDP デバイスの機能を検出する場合は、[プロパティ] ページで LLDP を有効にします。
6. [LLDP 過負荷] ページを使用して、過負荷情報を表示します。

LLDP のプロパティ

[プロパティ] ページでは、LLDP の一般パラメータを入力して、機能をグローバルに有効/無効にしたり、タイマーを設定したりすることができます。

LLDP のプロパティ値を設定するには、次のようにします。

ステップ 1 [各種管理] > [ディスカバリ - LLDP] > [プロパティ] の順にクリックします。

ステップ 2 パラメータを入力します。

- [LLDP ステータス]:選択するとデバイス上の LLDP が有効になります(デフォルトで有効)。
- [LLDP フレーム処理]:LLDP が有効でない場合は、選択した基準に一致するパケットを受信したときに実行する処理を次の中から選択します。
  - [フィルタリング]:パケットを削除します。
  - [フラッディング]:VLAN メンバーすべてにパケットを転送します。
- [TLV アドバタイズ間隔]:LLDP アドバタイズメント更新データの送信間隔(単位:秒)を入力するか、デフォルトを使用します。
- [トポロジ変更 SNMP 通知間隔]:SNMP 通知を実行する最短の時間間隔を入力します。
- [ホールド係数]:LLDP パケットを破棄せずに保持する時間を、[TLV アドバタイズ間隔] の値の倍数で入力します。たとえば、[TLV アドバタイズ間隔] の値が 30 秒であり、[ホールド係数] の値が 4 である場合、LLDP パケットは 120 秒後に破棄されます。
- [再初期化遅延]:LLDP 有効/無効サイクルの後、LLDP を無効にしてから再初期化するまでの間隔(単位:秒)を入力します。
- [送信遅延]:LLDP ローカル システム MIB の内容が変更されたときに LLDP フレームを送信する間隔(単位:秒)を入力します。
- [シャーシ ID アドバタイズメント]:LLDP メッセージのアドバタイズメントに関して、次のオプションのいずれかを選択します。
  - [MAC アドレス]:デバイスの MAC アドレスをアドバタイズします。
  - [ホスト名]:デバイスのホスト名をアドバタイズします。

ステップ 3 LED-MED の [プロパティ] の [Fast Startリピート回数] フィールドに、LLDP-MED Fast Start 機能の初期化時に LLDP パケットを送信する回数を入力します。LLDP-MED Fast Start 機能は、新しいエンドポイント デバイスがデバイスにリンクしたときに初期化されます。LLDP MED の詳細については、「LLDP MED ネットワーク ポリシー」セクションを参照してください。

ステップ 4 [適用] をクリックします。LLDP プロパティが実行コンフィギュレーション ファイルに追加されます。

ポート設定

[LLDP ポート設定] ページでは、ポートごとに LLDP や SNMP 通知を有効にしたり、LLDP PDU に送信される TLV を入力できます。

[LLDP MED ポート設定] ページで、アドバタイズされる LLDP-MED TLV を選択できます。また、デバイスの管理アドレス TLV も設定できます。

ポートの LLDP 情報を設定するには、次のようにします。

ステップ 1 [管理] > [ディスカバリ - LLDP] > [ポート設定] の順にクリックします。

このページには、ポートの LLDP 情報が表示されます。

ステップ 2 ポートを選択して、[編集] をクリックします。

このページには、次のフィールドが表示されます。

- [インターフェイス]: 編集するポートを選択します。
- [管理ステータス]: このポートの LLDP 発行オプションを選択します。値は次のとおりです。
  - [Txのみ]: 発行はしますが検出はしません。
  - [Rx のみ]: 検出はしますが発行はしません。
  - [Tx および Rx]: 発行も検出も行います。
  - [無効]: このポート上で LLDP を無効にします。
- [SNMP 通知]: トポロジの変更があったときに、SNMP 通知を受信者（たとえば、SNMP 管理システム）に送信する場合は、[有効] を選択します。

  通知送信間隔は、[LLDP のプロパティ] ページの [トポロジ変更 SNMP 通知間隔] フィールドで指定します。[SNMPv1,2 通知受信者] を使用して、SNMP 通知の受信者を定義します。

- [選択済みのオプション TLV]：デバイスが発行する情報を選択するには、[使用可能なオプション TLV] リストからその TLV をここへ移動します。選択可能な TLV は次のとおりです。
  - [ポートの説明]：ポートに関する情報（例：製造元、製品名、ハードウェア バージョン、ソフトウェア バージョン）。
  - [システム名]：システムに割り当てられている名前（英数字）。この値は sysName オブジェクトと同じです。
  - [システムの説明]：ネットワーク エンティティの説明（英数字）。システムの名前、および、このデバイスでサポートされているハードウェア、オペレーティング システム、ネットワーキング ソフトウェアの各バージョンが含まれます。この値は sysDescr オブジェクトと同じです。
  - [システム機能]：デバイスの主な機能、およびそれらの機能がデバイス上で有効になっているかどうか。機能は 2 オクテットで表されます。ビット 0 ～ 7 はそれぞれ、その他、リピータ、ブリッジ、WLAN AP、ルータ、電話、DOCSIS ケーブル デバイス、ステーションを意味します。ビット 8 ～ 15 は予約されています。
  - [802.3 MAC-PHY]：送信元デバイスの、設定可能な通信方式（全二重/半二重）およびビット レート、ならびに、現在の通信方式およびビット レート。また、現在の設定がオート ネゴシエーションと手動ネゴシエーションのどちらによって決定されたかも示します。
  - [802.3 Power via MDI]：MDI 経由で伝送される最大電力。
  - [802.3リンクアグリゲーション]：LLDP PDU 送信元ポートに関連付けられているリンクを集約できるかどうかを示します。また、現在リンクが集約されているかどうかも示し、集約されている場合はその集約ポート ID も表示します。
  - [802.3最大フレームサイズ]：MAC/PHY の実装における許容最大フレーム サイズ。
  - [MDI 経由の 4 線式電源]：（60W PoE をサポートする PoE ポートに関連）60 ワットの電力を可能にする Power over Ethernet をサポートするために定義されたシスコ独自の TLV（標準サポートは最大 30 ワット）。

管理アドレスのオプション TLV

- [アドバタイズメント モード]:デバイスの IP 管理アドレスをアドバタイズする方法を次の中から 1 つ選択します。
  - [自動アドバタイズ]:アドバタイズする管理アドレスを、デバイスのすべての IP アドレスからソフトウェアが自動的に選択するように指定します。複数の IP アドレスがある場合、ソフトウェアはダイナミック IP アドレスの中から最下位の IP アドレスを選択します。ダイナミック アドレスがない場合、ソフトウェアはスタティック IP アドレスの中から最も小さい IP アドレスを選択します。
  - [なし]:管理 IP アドレスをアドバタイズしません。
  - [手動アドバタイズ]:アドバタイズする管理 IP アドレスを選択します。
- [IP アドレス]:[手動アドバタイズ] を選択した場合、表示される IP アドレスの中から管理 IP アドレスを選択します。

802.1 VLANおよびプロトコル

- [PVID]:TLV で PVID をアドバタイズする場合に選択します。
- [ポートおよびプロトコル VLAN ID]:ポートで有効になっているプロトコルベースの VLAN を入力します。
- [VLAN ID]:アドバタイズする VLAN を選択します。
- [プロトコル ID]:アドバタイズするプロトコルを選択します。
- [選択済みプロトコル ID]:[プロトコル ID] ボックスで使用するプロトコルを選択して、それらを [選択済みプロトコル ID] ボックスに移動します。

ステップ 3 関連情報を入力し、[適用] をクリックします。ポート設定が、実行コンフィギュレーション ファイルに書き込まれます。

LLDP MED ネットワーク ポリシー

LLDP Media Endpoint Discovery（LLDP-MED; LLDP メディア エンドポイント検出）は LLDP の拡張機能で、メディア エンドポイント デバイスをサポートする次の付加機能を提供します。

- 音声やビデオなどのリアルタイム アプリケーションのネットワーク ポリシーをアドバタイズおよび検出することができます。
- デバイスの位置を検出して、位置データベースを作成することができます。たとえば Voice over Internet Protocol（VoIP）の場合、IP 電話位置情報を使用して、Emergency Call Service（E-911）にかかってきた電話の位置を特定することができます。
- トラブルシューティング情報。次の場合、LLDP MED はネットワーク管理者にアラートを送信します。
  - ポート速度や通信方式（全二重 / 半二重）が一致していない。
  - QoS ポリシーの設定が不適切である。

LLDP MED ネットワーク ポリシーの設定

LLDP-MED ネットワーク ポリシーは、音声やビデオなどの特定のリアルタイム アプリケーションに関連するコンフィギュレーション設定のセットです。ネットワーク ポリシーが設定されている場合は、接続された LLDP メディア エンドポイント デバイス宛の発信 LLDP パケットにこのポリシーを含めることができます。メディア エンドポイント デバイスは、受信したネットワーク ポリシーの指定に従ってトラフィックを送信する必要があります。たとえば、VoIP 電話に対し、VoIP トラフィックについて次の処理を指示するネットワーク ポリシーを作成できます。

- VLAN 10 の音声トラフィックをタグ付きパケットとして、802.1p プライオリティ 5 で送信する。
- DSCP 46 で音声トラフィックを送信する。

ネットワーク ポリシーをポートにバインドするには、[LLDP MED ポート設定] ページを使用します。管理者は、複数のネットワーク ポリシーと、ポリシーの送信先インターフェイスを手動で設定できます。管理者には、手動で VLAN を作成し、ネットワーク ポリシーとバインドされたインターフェイスに従って VLAN のポート メンバーシップを指定する責任があります。

管理者は、デバイスによって維持されている音声 VLAN に基づいて、音声アプリケーションのネットワーク ポリシーを自動的に生成しアドバタイズするようにデバイスを設定することもできます。デバイスが音声 VLAN を維持する方法の詳細は、自動音声 VLAN に関する項を参照してください。

LLDP MED ネットワーク ポリシーを作成するには、次のようにします。

ステップ 1 [各種管理] > [ディスカバリ - LLDP] > [LLDP MED ネットワークポリシー] の順にクリックします。

このページには、作成済みのネットワーク ポリシーが表示されます。

ステップ 2 デバイスが、維持している音声 VLAN に基づいて音声アプリケーションのネットワーク ポリシーを自動的に生成およびアドバタイズするように設定する場合は、[音声アプリケーションの LLDP MED ネットワーク ポリシー] で [自動] を選択します。

注 このボックスがオンの場合、手動で音声ネットワーク ポリシーを設定することはできません。

ステップ 3 [適用] をクリックし、この設定を実行コンフィギュレーション ファイルに追加します。

ステップ 4 新たにポリシーを定義するには、[追加] をクリックします。

ステップ 5 値を入力します。

- [ネットワーク ポリシー番号]: 作成するポリシーの番号を選択します。
- [アプリケーション]: 定義されるネットワーク ポリシーの対象となるアプリケーションのタイプ（トラフィックのタイプ）を選択します。
- [VLAN ID]: トラフィックの送信先 VLAN ID を入力します。
- [VLAN タイプ]: トラフィックをタグ付きにするかどうかを選択します。
- [ユーザ プライオリティ]: このネットワーク ポリシーで設定したトラフィックに適用するトラフィック プライオリティを選択します。これは、CoS 値です。
- [DSCP 値]: ネイバーから送信されるアプリケーション データに割り当てる DSCP 値を選択します。この値により、ネイバーからデバイスに送信するアプリケーション トラフィックにマークする方法をネイバーに通知できます。

ステップ 6 [適用] をクリックします。ネットワーク ポリシーが作成されます。

注 [LLDP MED ポート設定] ページを使用して、発信 LLDP パケットに関する手動で定義したネットワーク ポリシーを含めるには、インターフェイスを手動で設定する必要があります。

LLDP MED ポート設定

[LLDP MED ポート設定] ページでは、インターフェイスに対して発信する LLDP アドバタイズメントに含める LLDP-MED TLV およびネットワーク ポリシーを選択できます。ネットワーク ポリシーは、[LLDP MED ネットワークポリシー] ページを使用して設定します。

注 [音声アプリケーションの LLDP-MED ネットワーク ポリシー]（[LLDP MED ネットワーク ポリシー] ページ）が [自動] で、自動音声 VLAN が動作している場合、デバイスは、LLDP-MED が有効で音声 VLAN のメンバーあるすべてのポートについて、音声アプリケーションの LLDP-MED ネットワーク ポリシーを自動的に生成します。

各ポートで LLDP-MED を設定するには、次のようにします。

ステップ 1 [各種管理] > [ディスカバリ - LLDP] > [LLDP MED ポート設定] の順にクリックします。

このページには、すべてのポートに関する以下の LLDP MED 設定が表示されます（[編集] ページで説明されていないフィールドのみ一覧表示されます）。

- [ユーザ定義ネットワークポリシー]: トラフィックのタイプ（アプリケーションと呼ばれる）に関するポリシーが定義されます。これはLLDP MED ネットワーク ポリシーで定義されます。この場合は、ポート上のポリシーに関する次の情報が表示されます。
  - [アクティブ]: トラフィックのタイプがポート上でアクティブになっているかどうか。
  - [アプリケーション]: ポリシーを定義するトラフィックのタイプ。
- [ロケーション]: ロケーション TLV が送信されるかどうか。
- [PoE]: POE-PSE TLV が送信されるかどうか。
- [インベントリ]: インベントリ TLV が送信されるかどうか。

ステップ 2 ページ上部のメッセージは、音声アプリケーションの LLDP MED ネットワーク ポリシーが自動的に生成されるかどうかを示しています（LLDP の概要を参照）。モードを変更するリンクをクリックします。

ステップ 3 追加の LLDP MED TLV や、ユーザ定義 LLDP MED ネットワーク ポリシーをポートに関連付けるには、必要なものを選択して、[編集] をクリックします。

ステップ 4 パラメータを入力します。

- [インターフェイス]: 設定するインターフェイスを選択します。
- [LLDP MED ステータス]: このポート上で LLDP MED を有効にするか無効にするかを選択します。

- [SNMP 通知]:トポロジの変更があった場合、MED をサポートするエンド ステーション（たとえば、SNMP 管理システム）が検出されたときにポートごとに SNMP 通知を送信するかどうかを選択します。
- [選択したオプション TLV]:デバイスが発行できる TLV を選択するには、必要な TLV を [使用可能なオプション TLV] の一覧から [選択したオプション TLV] の一覧に移動させます。
- [選択したネットワークポリシー]:発行する LLDP MED ポリシーを選択するには、必要なポリシーを [使用可能なネットワークポリシー] の一覧から [選択したネットワークポリシー] の一覧に移動させます。これらは、[LLDP MED ネットワーク ポリシー] ページで作成されたものです。ユーザが定義したネットワーク ポリシーをアドバタイズメントに含めるには、[使用可能なオプション TLV] から [ネットワークポリシー] を選択する必要があります。

  注 次に示すフィールドの値は、LLDP-MED 規格（ANSI-TIA-1057_final_for_publication.pdf）で定められているデータ形式に従い、16 進数で正確に入力する必要があります。

  - [デバイス場所の座標]:LLDP を使用して発行する座標を入力します。
  - [デバイス場所の住所]:LLDP を使用して発行する住所を入力します。
  - [デバイス場所の ECS ELIN]:LLDP を使用して発行する、Emergency Call Service（ECS）の ELIN の場所を入力します。

ステップ 5 [適用] をクリックします。LLDP MED ポート設定が、実行コンフィギュレーション ファイルに書き込まれます。

LLDP ポート ステータス

[LLDP ポートステータス] ページには、各ポートの LLDP グローバル情報が表示されます。

ステップ 1 LLDP ポート ステータスを表示するには、[各種管理] > [ディスカバリ - LLDP] > [LLDP ポートステータス] の順にクリックします。

すべてのポートの情報が表示されます。

ステップ 2 特定のポートに送信される LLDP および LLDP-MED の TLV の詳細情報を表示するには、ポートを選択して、[LLDP ローカル情報の詳細] をクリックします。

ステップ 3 特定のポートから受信する LLDP および LLDP-MED の TLV の詳細情報を表示するには、ポートを選択して、[LLDP ネイバー情報の詳細] をクリックします。

- **LLDP ポート ステータス グローバル情報**
- [シャーシ ID サブタイプ]：シャーシ ID のタイプ（例：MAC アドレス）。
- [シャーシ ID]：シャーシの ID。シャーシ ID サブタイプが MAC アドレスである場合は、デバイスの MAC アドレスが表示されます。
- [システム名]：デバイスの名前。
- [システムの説明]：デバイスの説明（英数字）。
- [サポートされているシステム機能]：デバイスの主要機能（例：ブリッジ、WLAN AP、ルータ）。
- [有効なシステム機能]：デバイスで有効になっている主要機能。
- [ポート ID サブタイプ]：表示されるポート ID のタイプ。
- **LLDP ポート ステータス テーブル**
- [インターフェイス]：ポート ID。
- [LLDP ステータス]：LLDP 発行オプション。
- [LLDP MED ステータス]：有効または無効。
- [ローカル PoE（電力タイプ、電源、電力プライオリティ、電力値）]：アドバタイズされるローカル PoE 情報。
- [リモート PoE（電力タイプ、電源、電力プライオリティ、電力値）]：ネイバーによってアドバタイズされる PoE 情報。
- [ネイバー数]：検出されたネイバー数。
- [第 1 デバイスのネイバー機能]：ネイバーの主要機能（例：ブリッジ、ルータ）。

LLDP ローカル情報

ポートからアドバタイズされている LLDP ローカル ポート ステータスを表示するには、次のようにします。

ステップ 1 [各種管理] > [ディスカバリ - LLDP] > [LLDP ローカル情報] の順にクリックします。

ステップ 2 LLDP ローカル情報を表示するインターフェイスを選択します。

このページには、選択したインターフェイスに関する次のフィールドが表示されます。

[グローバル]

- [シャーシ ID サブタイプ]: シャーシ ID のタイプ。(例: MAC アドレス)。
- [シャーシ ID]: シャーシの ID。シャーシ ID サブタイプが MAC アドレスである場合は、デバイスの MAC アドレスが表示されます。
- [システム名]: デバイスの名前。
- [システムの説明]: デバイスの説明(英数字)。
- [サポートされているシステム機能]: デバイスの主要機能(例: ブリッジ、WLAN AP、ルータ)。
- [有効なシステム機能]: デバイスで有効になっている主要機能。
- [ポート ID サブタイプ]: 表示されるポート ID のタイプ。
- [ポート ID]: ポートの ID。
- [ポートの説明]: ポートに関する情報(例: 製造元、製品名、ハードウェア バージョン、ソフトウェア バージョン)。

[管理アドレス]

ローカル LLDP エージェントのアドレス テーブルが表示されます。他のリモート マネージャはこのアドレスを使用して、ローカル デバイスに関する情報を取得できます。アドレスは次の要素で構成されています。

- [IPv4 アドレス]: 管理用途に最も適した IPv4 戻りアドレス。
- [IPv6 グローバル アドレス]: 管理用途に最も適した IPv6 戻りグローバル アドレス。
- [IPv6 リンク ローカル アドレス]: 管理用途に最も適した IPv6 戻りリンク ローカル アドレス。

[MAC/PHY の詳細]

- [自動ネゴシエーション対応]:ポート速度の自動ネゴシエーションがサポートされているかどうか。
- [自動ネゴシエーション有効]:ポート速度の自動ネゴシエーションがアクティブかどうか。
- [自動ネゴシエーションアドバタイズ機能]:ポート速度の自動ネゴシエーション機能（例:1000BASE-T 半二重モード、100BASE-TX 全二重モード）。
- [動作 MAU タイプ]:Medium Attachment Unit（MAU）のタイプ。MAU では物理層の機能が実行されます。たとえば、イーサネット インターフェイスのコリジョン検出から入ってきたデータに対するデジタル データ変換、ネットワーク（例:100BASE-TX 全二重モード）へのビット挿入などの処理が実行されます。

[802.3の詳細]

- [802.3 最大フレーム サイズ]:サポートされている IEEE 802.3 フレーム サイズの最大値。

[802.3リンクアグリゲーション]

- [アグリゲーション機能]:インターフェイスを集約できるかどうか。
- [アグリゲーション ステータス]:現在、インターフェイスが集約されているかどうか。
- [アグリゲーション ポート ID]:アドバタイズされている集約インターフェイス ID。

[802.3 Power via MDI]

- [MDI 電源対応ポート クラス]:アドバタイズされている電源対応ポート クラス。
- [PSE MDI 電源対応]:ポートで MDI 電源がサポートされているかどうか。
- [PSE MDI 電源状態]:ポートで MDI 電源が有効になっているかどうか。
- [PSE 電源ペア制御機能]:ポートで電源ペア制御がサポートされているかどうか。
- [PSE 電源ペア]:ポートでサポートされている電源ペア制御タイプ。
- [PSE 電力クラス]:アドバタイズされている、ポートの電力クラス。
- [電力タイプ]:ポートに接続された POD デバイスのタイプ。

- [電源]:ポートの電源。
- [電力プライオリティ]:ポートの電力のプライオリティ。
- [PD 要求電力値]:PSE から PD に割り当てられた電力量。
- [PSE 割り当て電力値]:給電側機器(PSE)に割り当てられた電力量。

[802.3 Energy Efficient Ethernet (EEE)](デバイスが EEE をサポートする場合)

- [ローカル Tx]:低電力アイドル(LPI モード)を抜けた後、データの送信を開始するまで、送信リンク パートナーが待機する時間(単位:マイクロ秒)。
- [ローカル Rx]:受信リンク パートナーが要求する、低電力アイドル(LPI モード)後にデータを送信するまでに、送信リンク パートナーが待機する時間(単位:マイクロ秒)。
- [リモート Tx エコー]:リモート リンク パートナーの Tx 値に対するローカル リンク パートナーのリフレクション。
- [リモート Rx エコー]:リモート リンク パートナーの Rx 値に対するローカル リンク パートナーのリフレクション。

[MDI 経由の 4 線式電源]

- [4 ペア PoE サポート済み]:システムとポートが 4 ペア線の有効化をサポートしていることを示します(この HW 能力を持っている特定のポートにのみ当てはまる)。
- [予備ペア検出/分類必要]:4 ペア線が必要なことを示します。
- [PD 予備ペア所望状態]:POD デバイスが 4 ペア能力を有効にするように要求していることを示します。
- [PD 予備ペア動作状態]:4 ペア能力が有効か無効かを示します。

[MEDの詳細]

- [サポートされている機能]:ポート上でサポートされている MED 機能。
- [現在の機能]:ポート上で有効になっている MED 機能。
- [デバイス クラス]:LLDP-MED エンドポイント デバイス クラス。表示されるデバイス クラスは次のとおりです。
  - [エンドポイントクラス1]:汎用エンドポイント クラス。基本的な LLDP サービスを提供します。

- [エンドポイントクラス2]：メディア エンドポイント クラス。クラス 1 のすべての機能に加え、メディア ストリーミング機能を提供します。
- [エンドポイントクラス3]：通信デバイス クラス。クラス 1 およびクラス 2 のすべての機能に加え、位置、911、レイヤ 2 デバイス サポート、デバイス情報管理の各機能を提供します。

- [PoE デバイス タイプ]：ポートの PoE タイプ（例：PD）。
- [PoE 電源]：ポートの電源。
- [PoE 電力プライオリティ]：ポートの電力のプライオリティ。
- [PoE 電力値]：ポートの電力値。
- [ハードウェアリビジョン]：ハードウェアのバージョン。
- [ファームウェア リビジョン]：ファームウェアのバージョン。
- [ソフトウェア リビジョン]：ソフトウェアのバージョン。
- [シリアル番号]：デバイスのシリアル番号。
- [製造業者名]：デバイスの製造業者名。
- [モデル名]：デバイスのモデル名。
- [アセット ID]：アセット ID。

[場所の情報]

- [住所]：住所。
- [座標]：マップ座標（緯度、経度、および標高）。
- [ECS ELIN]：Emergency Call Service（ECS）の Emergency Location Identification Number（ELIN）。

[ネットワークポリシーテーブル]

- [アプリケーション タイプ]：ネットワーク ポリシーのアプリケーション タイプ（例：音声）。
- [VLAN ID]：ネットワーク ポリシーが定義されている VLAN の ID。
- [VLAN タイプ]：ネットワーク ポリシーが定義されている VLAN のタイプ。表示されるフィールド値は次のとおりです。
  - [タグ付き]：ネットワーク ポリシーはタグ付き VLAN 用に定義されています。

- [タグなし]：ネットワーク ポリシーはタグなし VLAN 用に定義されています。

- [ユーザ プライオリティ]：ネットワーク ポリシーのユーザ プライオリティ。
- [DSCP]：ネットワーク ポリシーの DSCP。

ステップ 3 ページの下部にある [LLDP ポート ステータス テーブル] をクリックすると、[LLDP ポート ステータス テーブル] に詳細が表示されます（ポート設定を参照）。

LLDP ネイバー情報

[LLDPネイバー情報] ページには、ネイバー デバイスから受信した情報が表示されます。

タイムアウトになると、情報は削除されます。ネイバーの TTL TLV で表される時間内に、そのネイバーから LLDP PDU が 1 件も受信されなかった場合、タイムアウトになります。

LLDP ネイバー情報を表示するには、次のようにします。

ステップ 1 [各種管理] > [ディスカバリ - LLDP] > [LLDP ネイバー情報] の順にクリックします。

ステップ 2 LLDP ネイバー情報を表示するインターフェイスを選択します。

このページには、選択したインターフェイスに関する次のフィールドが表示されます。

- [ローカル ポート]：ネイバーが接続されているローカル ポートの番号。
- [シャーシ ID サブタイプ]：シャーシ ID のタイプ（例：MAC アドレス）。
- [シャーシ ID]：802 LAN 近隣デバイスのシャーシの ID。
- [ポート ID サブタイプ]：表示されるポート ID のタイプ。
- [ポート ID]：ポートの ID。
- [システム名]：発行されたデバイスの名前。
- [存続可能時間]：このネイバーの情報が削除されるまでの時間間隔（単位：秒）。

ステップ 3 ローカル ポートを選択し、[詳細] をクリックします。

[LLDP ネイバー情報] ページには、次のフィールドが含まれています。

[ポートの詳細]

- [ローカル ポート]:ポート番号。
- [MSAP エントリ]:デバイスのメディア サービス アクセスポイント（MSAP）のエントリ番号。

[基本内容]

- [シャーシ ID サブタイプ]:シャーシ ID のタイプ（例:MAC アドレス）。
- [シャーシ ID]:802 LAN 近隣デバイスのシャーシの ID。
- [ポート ID サブタイプ]:表示されるポート ID のタイプ。
- [ポート ID]:ポートの ID。
- [ポートの説明]:ポートに関する情報（例:製造元、製品名、ハードウェア バージョン、ソフトウェア バージョン）。
- [システム名]:発行されるシステムの名前。
- [システムの説明]:ネットワーク エンティティの説明（英数字）。システムの名前、および、このデバイスでサポートされているハードウェア、オペレーティング システム、ネットワーキング ソフトウェアの各バージョンが含まれます。この値は sysDescr オブジェクトと同じです。
- [サポートされているシステム機能]:このデバイスの主要機能。機能は 2 オクテットで表されます。ビット 0 ～ 7 はそれぞれ、その他、リピータ、ブリッジ、WLAN AP、ルータ、電話、DOCSIS ケーブル デバイス、ステーションを意味します。ビット 8 ～ 15 は予約されています。
- [有効なシステム機能]:デバイスで有効になっている主要機能。

[管理アドレステーブル]

- [アドレス サブタイプ]:管理アドレスのサブタイプ（例:MAC、IPv4）。
- [アドレス]:管理アドレス。
- [インターフェイス サブタイプ]:ポートのサブタイプ。
- [インターフェイス番号]:ポート番号。

[MAC/PHY の詳細]

- [自動ネゴシエーション対応]:ポート速度の自動ネゴシエーションがサポートされているかどうか。表示されるフィールド値は [TRUE] または [FALSE] です。
- [自動ネゴシエーション有効]:ポート速度の自動ネゴシエーションがアクティブかどうか。表示されるフィールド値は [TRUE] または [FALSE] です。
- [自動ネゴシエーション アドバタイズ機能]:ポート速度の自動ネゴシエーション機能（例:1000BASE-T 半二重モード、100BASE-TX 全二重モード）。
- [動作 MAU タイプ]:Medium Attachment Unit（MAU）のタイプ。MAU では物理層の機能が実行されます。たとえば、イーサネット インターフェイスから入ってきたデータに対して、デジタル データ変換、コリジョン検出、ビット挿入などの処理が実行され、ネットワーク（例:100BASE-TX 全二重モード）に送出されます。

[802.3 Power via MDI]

- [MDI 電源対応ポート クラス]:アドバタイズされている電源対応ポート クラス。
- [PSE MDI 電源対応]:ポートで MDI 電源がサポートされているかどうか。
- [PSE MDI 電源状態]:ポートで MDI 電源が有効になっているかどうか。
- [PSE 電源ペア制御機能]:ポートで電源ペア制御がサポートされているかどうか。
- [PSE 電源ペア]:ポートでサポートされている電源ペア制御タイプ。
- [PSE 電力クラス]:アドバタイズされている、ポートの電力クラス。
- [電力タイプ]:ポートに接続された POD デバイスのタイプ。
- [電源]:ポートの電源。
- [電力プライオリティ]:ポートの電力のプライオリティ。
- [PD 要求電力値]:受電デバイスから要求された電力量。
- [PSE 割り当て電力値]:PSE から PD に割り当てられた電力量。

[MDI 経由の 4 線式電源]

- [4 ペア PoE サポート済み]:システムとポートが 4 ペア線の有効化をサポートしていることを示します(この HW 能力を持っている特定のポートにのみ当てはまる)。
- [予備ペア検出/分類必要]:4 ペア線が必要なことを示します。
- [PD 予備ペア所望状態]:POD デバイスが 4 ペア能力を有効にするように要求していることを示します。
- [PD 予備ペア動作可能状態]:4 ペア能力が有効か無効かを示します。

[802.3の詳細]

- [802.3 最大フレーム サイズ]:ポートでサポートされている、アドバタイズされる最大フレーム サイズ。

[802.3リンクアグリゲーション]

- [アグリゲーション機能]:ポートを集約できるかどうか。
- [アグリゲーション ステータス]:現在、ポートが集約されているかどうか。
- [アグリゲーション ポート ID]:アドバタイズされている集約ポート ID。

[802.3 Energy Efficient Ethernet (EEE)]

- [リモート Tx]:低電力アイドル(LPI モード)を抜けた後、データの送信を開始するまで、送信リンク パートナーが待機する時間(単位:マイクロ秒)。
- [リモート Rx]:受信リンク パートナーが要求する、低電力アイドル(LPI モード)後にデータを送信するまでに、送信リンク パートナーが待機する時間(単位:マイクロ秒)。
- [ローカル Tx エコー]:リモート リンク パートナーの Tx 値に対するローカル リンク パートナーのリフレクション。
- [ローカル Rx エコー]:リモート リンク パートナーの Rx 値に対するローカル リンク パートナーのリフレクション。

[MEDの詳細]

- [サポートされている機能]:ポート上で有効になっている MED 機能。
- [現在の機能]:ポートからアドバタイズされている MED TLV。
- [デバイス クラス]:LLDP-MED エンドポイント デバイス クラス。表示されるデバイス クラスは次のとおりです。
  - [エンドポイント クラス 1]:汎用エンドポイント クラス。基本的な LLDP サービスを提供します。
  - [エンドポイント クラス 2]:メディア エンドポイント クラス。クラス 1 のすべての機能に加え、メディア ストリーミング機能を提供します。
  - [エンドポイント クラス 3]:通信デバイス クラス。クラス 1 およびクラス 2 のすべての機能に加え、位置、911、レイヤ 2 スイッチ サポート、デバイス情報管理の各機能を提供します。
- [PoE デバイス タイプ]:ポートの PoE タイプ（例:PD/PSE）。
- [PoE 電源]:ポートの電源。
- [PoE 電力プライオリティ]:ポートの電力のプライオリティ。
- [PoE 電力値]:ポートの電力値。
- [ハードウェアリビジョン]:ハードウェアのバージョン。
- [ファームウェア リビジョン]:ファームウェアのバージョン。
- [ソフトウェア リビジョン]:ソフトウェアのバージョン。
- [シリアル番号]:デバイスのシリアル番号。
- [製造業者名]:デバイスの製造業者名。
- [モデル名]:デバイスのモデル名。
- [アセット ID]:アセット ID。

[802.1 VLANおよびプロトコル]

- [PVID]:アドバタイズされているポートの VLAN ID。

[PPVID]

[PPVID テーブル]

- [VID]：プロトコルの VLAN ID。
- [サポート済み]：サポートされている、ポートおよびプロトコルの VLAN ID。
- [有効]：有効になっている、ポートおよびプロトコルの VLAN ID。

[VLAN ID]

[VLAN ID テーブル]

- [VID]：ポートおよびプロトコルの VLAN ID。
- [VLAN 名]：アドバタイズされている VLAN 名。

[プロトコル ID テーブル]

- [プロトコル ID]：アドバタイズされているプロトコル ID。

[場所の情報]

ANSI-TIA-1057 規格の 10.2.4 項に従って、次のデータ構造を 16 進数で入力します。

- [住所]：住所。
- [座標]：位置マップ座標（緯度、経度、および標高）。
- [ECS ELIN]：デバイスの Emergency Call Service（ECS）の Emergency Location Identification Number（ELIN）。
- [不明]：不明なロケーション情報。

[ネットワークポリシーテーブル]

- [アプリケーション タイプ]：ネットワーク ポリシーのアプリケーション タイプ（例：音声）。
- [VLAN ID]：ネットワーク ポリシーが定義されている VLAN の ID。
- [VLAN タイプ]：ネットワーク ポリシーが定義されている VLAN のタイプ（タグ付きまたはタグなし）。
- [ユーザ プライオリティ]：ネットワーク ポリシーのユーザ プライオリティ。
- [DSCP]：ネットワーク ポリシーの DSCP。

ステップ 4 ポートを選択し、[LLDP ポート ステータス テーブル] をクリックすると、[LLDP ポート ステータス テーブル] に詳細が表示されます。

LLDP 統計情報

[LLDP 統計情報] ページには、ポートごとの LLDP 統計情報が表示されます。

LLDP 統計情報を表示するには、次のようにします。

ステップ 1 [各種管理] > [ディスカバリ - LLDP] > [LLDP 統計情報] の順にクリックします。

次のフィールドが各ポートに対して表示されます。

- [インターフェイス]: インターフェイスの ID。
- [Tx フレーム（合計）]: 送信されたフレームの合計数。
- [Rx フレーム]
  - [合計]: 受信したフレームの合計数。
  - [廃棄済み]: 受信したフレームのうち、廃棄されたフレームの数。
  - [エラー]: 受信したフレームのうち、エラーになったフレームの数。
- [Rx TLV]
  - [廃棄済み]: 受信した TLV のうち、廃棄された TLV の数。
  - [未認識]: 受信した TLV のうち、認識されなかった TLV の数。
- [ネイバーの情報削除回数]: このインターフェイス上でネイバーがエージアウトされた回数。

ステップ 2 最新の統計情報を表示するには、[更新] をクリックします。

LLDP 過負荷

LLDP では、LLDP TLV および LLDP-MED TLV として情報を LLDP パケットに追加します。LLDP 過負荷は、LLDP パケット内の総情報量がインターフェイスでサポートされている最大 PDU サイズを超えたときに発生します。

[LLDP 過負荷] ページには、LLDP/LLDP-MED 情報のバイト数、追加の LLDP 情報に使用可能なバイト数、および各インターフェイスの過負荷ステータスが表示されます。

LLDP 過負荷情報を表示するには、次のようにします。

ステップ 1 [各種管理] > [ディスカバリ - LLDP] > [LLDP 過負荷] の順にクリックします。

このページには次の情報がポートごとに表示されます。

- [インターフェイス]: ポート ID。
- [使用中の合計バイト数]: 各パケットの LLDP 情報の合計バイト数。
- [使用可能な残りのバイト数]: 各パケットで追加の LLDP 情報用に残っている利用可能な合計バイト数。
- [ステータス]: TLV が送信されているか、それとも過負荷状態になっているか。

ステップ 2 特定のポートの過負荷状態を詳細表示するには、そのポートを選択して [詳細] をクリックします。

このページには、このポートから送信された各 TLV に関する次の情報が表示されます。

- [LLDP 必須 TLV]
  - [サイズ（バイト）]: 必須 TLV の合計バイト数。
  - [ステータス]: 必須 TLV グループが送信されているか、過負荷状態になっているか。
- [LLDP MED 機能]
  - [サイズ（バイト）]: LLDP MED 機能パケットの合計バイト数。
  - [ステータス]: LLDP MED 機能パケットが送信されたか、過負荷状態であったか。
- [LLDP MED の場所]
  - [サイズ（バイト）]: LLDP MED 位置パケットの合計バイト数。

  - [ステータス]：LLDP MED 位置パケットが送信されたか、過負荷状態であったか。

- [LLDP MED ネットワークポリシー]
  - [サイズ（バイト）]：LLDP MED ネットワーク ポリシー パケットの合計バイト数。
  - [ステータス]：LLDP MED ネットワーク ポリシー パケットが送信されたか、過負荷状態であったか。
- [LLDP MED 拡張PoE]
  - [サイズ（バイト）]：MDI 経由 LLDP MED 拡張電力パケットの合計バイト数。
  - [ステータス]：MDI 経由 LLDP MED 拡張電力パケットが送信されたか、過負荷状態であったか。
- [802.3 TLV]
  - [サイズ（バイト）]：LLDP MED 802.3 TLV パケットの合計バイト数。
  - [ステータス]：LLDP MED 802.3 TLV パケットが送信されたか、過負荷状態であったか。
- [LLDP オプションTLV]
  - [サイズ（バイト）]：LLDP MED オプション TLV パケットの合計バイト数。
  - [ステータス]：LLDP MED オプション TLV パケットが送信されたか、過負荷状態であったか。
- [LLDP MED コンポーネント]
  - [サイズ（バイト）]：LLDP MED インベントリ TLV パケットの合計バイト数。
  - [ステータス]：LLDP MED インベントリ パケットが送信されたか、過負荷状態であったか。
- [合計]
  - [合計（バイト）]：各パケットの LLDP 情報の合計バイト数。
  - [使用可能な残りのバイト数]：各パケットで追加の LLDP 情報用に未送信のまま残っている利用可能な合計バイト数。

ディスカバリ - CDP

ここでは、CDP の設定方法を説明します。

具体的な内容は、次のとおりです。

- CDP のプロパティ
- CDP インターフェイス設定
- CDP ローカル情報
- CDP ネイバー情報
- CDP 統計情報

CDP のプロパティ

LLDP と同様に、Cisco Discovery Protocol（CDP）は、直接接続されたネイバーが自身とそれぞれの機能を互いにアドバタイズするためのリンク層プロトコルです。LLDP とは異なり、CDP はシスコ独自のプロトコルです。

CDP を設定する手順

次に、デバイスに CDP を設定する手順の例を示します。CDP を設定するための詳細なガイドラインは、LLDP/CDP に関するセクションで参照できます。

ステップ 1 CDP の [プロパティ] ページを使用して、CDP グローバル パラメータを入力します。

ステップ 2 [CDP インターフェイス設定] ページを使用して、インターフェイスごとに CDP を設定します。

ステップ 3 Auto Smartport で CDP デバイスの機能を検出する場合は、[プロパティ] ページで CDP を有効にします。

CDP を使用して Smartport 機能に対応するデバイスを識別する方法については、Smartport タイプをご覧ください。

CDP の一般パラメータを入力するには、次のようにします。

ステップ 1 [各種管理] > [ディスカバリ - CDP] > [プロパティ] の順にクリックします。

ステップ 2 パラメータを入力します。

- [CDP ステータス]:選択するとデバイス上の CDP が有効になります。
- [CDP フレーム処理]:CDP が有効でない場合は、選択した基準に一致するパケットを受信したときに実行する処理を次の中から選択します。
  - [ブリッジング]:VLAN に基づいてパケットを転送します。
  - [フィルタリング]:パケットを削除します。
  - [フラッディング]:入力ポートを除くすべてのポートに着信 CDP パケットを転送する VLAN 非対応のフラッディング。
- [CDP 音声 VLAN アドバタイズメント]:選択すると、CDP が有効で、音声 VLAN のメンバーであるすべてのポートで、デバイスが CDP を使用して音声 VLAN をアドバタイズできるようになります。音声 VLAN は、[音声 VLAN プロパティ] ページから設定します。
- [CDP 必須 TLV の検証]:選択すると、必須 TLV を含まない着信 CDP パケットは廃棄され、無効なエラー カウンタが増加します。
- [CDP バージョン]:使用する CDP のバージョンを選択します。
- [CDP 保留時間]:CDP パケットを廃棄するまで待機する時間を、[TLV アドバタイズ間隔] の値の倍数で入力します。たとえば、[TLV アドバタイズ間隔] の値が 30 秒であり、[ホールド係数] の値が 4 である場合、LLDP パケットは 120 秒後に破棄されます。次のオプションが選択できます。
  - [デフォルトを使用]:デフォルトの時間（180 秒）を使用します。
  - [ユーザ定義]:時間を秒単位で入力します。
- [CDP 転送速度]:CDP アドバタイズメント更新データの送信間隔を秒単位で入力します。次のオプションが選択できます。
  - [デフォルトを使用]:デフォルトのレート（60 秒）を使用します。
  - [ユーザ定義]:レートを秒単位で入力します。
- [デバイス ID 形式]:デバイス ID のフォーマットを選択します（MAC アドレスまたはシリアル番号）。次のオプションが選択できます。
  - [MAC アドレス]:デバイスの MAC アドレスをデバイス ID として使用します。

- [シリアル番号]:デバイスのシリアル番号をデバイス ID として使用します。
- [ホスト名]:デバイスのホスト名をデバイス ID として使用します。

- [送信元インターフェイス]:フレームの TLV で使用される IP アドレス。次のオプションが選択できます。
  - [デフォルトを使用]:発信インターフェイスの IP アドレスを使用します。
  - [ユーザ定義]:アドレス TLV 内のインターフェイス([インターフェイス] フィールドに表示)の IP アドレスを使用します。
- [インターフェイス]:[送信元インターフェイス] で [ユーザ定義] が選択された場合は、インターフェイスを選択します。
- [Syslog 音声 VLAN 不一致]:オンにすると、音声 VLAN の不一致が検出されたときに SYSLOG メッセージが送信されます。これは、着信フレーム内の音声 VLAN 情報が、ローカル デバイスがアドバタイズしている情報と一致していないことを示しています。
- [Syslog ネイティブ VLAN 不一致]:オンにすると、ネイティブ VLAN の不一致が検出されたときに SYSLOG メッセージが送信されます。これは、着信フレーム内のネイティブ VLAN 情報が、ローカル デバイスがアドバタイズしている情報と一致していないことを示しています。
- [Syslog デュプレックス不一致]:オンにすると、デュプレックス情報が一致しないときに SYSLOG メッセージが送信されます。これは、着信フレーム内のデュプレックス情報が、ローカル デバイスがアドバタイズしている情報と一致していないことを示しています。

ステップ 3 [適用] をクリックします。LLDP のプロパティ値が設定されます。

CDP インターフェイス設定

LLDP およびリモート ログ サーバ通知をポートごとにアクティブにしたり、LLDP PDU に組み込む TLV を選択したりするには、[インターフェイス設定] ページを使用します。

これらのプロパティ値を設定することにより、LLDP 対応デバイスに送信する情報のタイプを選択できます。

アドバタイズする LLDP-MED TLV は、[LLDP MED ポート設定] ページで選択できます。

CDP インターフェイス設定を定義するには、次のようにします。

ステップ 1 [各種管理] > [ディスカバリ - CDP] > [インターフェイス設定] の順にクリックします。

このページには、各インターフェイスに関する次の CDP 情報が表示されます。

- [CDP ステータス]: ポートに対する CDP 発行オプション。
- [レポートが CDP ネイバーと競合しています]: [編集] ページで有効または無効になっているレポート オプションのステータスを表示します（音声 VLAN、ネイティブ VLAN、デュプレックス）。
- [ネイバー数]: 検出されたネイバー数。

ページ下部に 4 つのボタンがあります。

- [設定のコピー]: 選択すると、ポート間でコンフィギュレーションがコピーされます。
- [編集]: フィールドは後述のステップ 2 で説明されています。
- [CDP ローカル情報の詳細]: [CDP ローカル情報] ページに移動します。
- [CDP ネイバー情報の詳細]: [CDP ネイバー情報] ページに移動します。

ステップ 2 ポートを選択して、[編集] をクリックします。

このページには、次のフィールドが表示されます。

- [インターフェイス]: 定義するインターフェイスを選択します。
- [CDP ステータス]: ポートで CDP 発行オプションを有効にするか無効にするかを選択します。

  注 次の 3 つのフィールドは、デバイスが管理ステーションにトラップを送信するように設定されている場合に使用可能となります。

- [Syslog 音声 VLAN 不一致]: 選択すると、音声 VLAN の不一致が検出されたときに SYSLOG メッセージが送信されるようになります。これは、着信フレーム内の音声 VLAN 情報が、ローカル デバイスがアドバタイズしている情報と一致していないことを示しています。
- [Syslog ネイティブ VLAN 不一致]: 選択すると、ネイティブ VLAN の不一致が検出されたときに SYSLOG メッセージが送信されるようになります。これは、着信フレーム内のネイティブ VLAN 情報が、ローカル デバイスがアドバタイズしている情報と一致していないことを示しています。

- [Syslog デュプレックス不一致]：選択すると、デュプレックス情報の不一致が検出されたときに SYSLOG メッセージが送信されるようになります。これは、着信フレーム内のデュプレックス情報が、ローカル デバイスがアドバタイズしている情報と一致していないことを示しています。

ステップ 3 関連情報を入力し、[適用] をクリックします。ポート設定が、実行コンフィギュレーションに書き込まれます。

CDP ローカル情報

ローカル デバイスに関する CDP プロトコルによってアドバタイズされる情報を表示するには、次のようにします。

ステップ 1 [各種管理] > [ディスカバリ - CDP] > [CDP ローカル情報] の順にクリックします。

ステップ 2 ローカル ポートを選択すると、次のフィールドが表示されます。

- [インターフェイス]：ローカル ポート数。
- [CDP 状態]：CDP が有効かどうかを表示します。
- [デバイス ID TLV]
  - [デバイス ID タイプ]：デバイス ID TLV でアドバタイズされるデバイス ID のタイプ。
  - [デバイス ID]：デバイス ID TLV でアドバタイズされるデバイス ID。
- [システム名TLV]
  - [システム名]：デバイスのシステム名。
- [アドレスTLV]
  - [アドレス1-3]：デバイス アドレス TLV でアドバタイズされる IP アドレス。
- [ポート TLV]
  - [ポート ID]：ポート TLV でアドバタイズされるポートの ID。
- [機能の TLV]
  - [機能]：ポート TLV でアドバタイズされる機能。

- [バージョン TLV]
  - [バージョン]:デバイスが稼動しているソフトウェアのリリースに関する情報。
- [プラットフォーム TLV]
  - [プラットフォーム]:プラットフォーム TLV でアドバタイズされるプラットフォームの ID。
- [ネイティブ VLAN TLV]
  - [ネイティブ VLAN]:ネイティブ VLAN TLV でアドバタイズされるネイティブ VLAN ID。
- [全/半二重 TLV]
  - [デュプレックス]:全二重 TLV または半二重 TLV でアドバタイズされるポートのデュプレックスが半二重か全二重か。
- [アプライアンス TLV]
  - [アプライアンス ID]:アプライアンス TLV でアドバタイズされる、ポートに接続されたデバイスのタイプ。
  - [アプライアンス VLAN ID]:アプライアンスによって使用されるデバイス上の VLAN（例:アプライアンスが IP 電話の場合は、音声 VLAN）。
- [拡張信頼 TLV]
  - [拡張信頼]:有効な場合、そのポートは信頼できることを示しています。つまり、パケットの送信元となるホストまたはサーバが信頼でき、それ自体でパケットにマーキングできることを意味します。この場合、このようなポートで受信されたパケットは、再度マーキングされることはありません。無効な場合は、ポートが信頼できないことを示しています。この場合、次のフィールドが関係します。
- [信頼できないポートの CoS TLV]
  - [信頼できないポートの CoS]:ポートの [拡張信頼] が無効な場合、このフィールドにはレイヤ 2 CoS 値、つまり 802.1D/802.1p プライオリティ値が表示されます。これは、信頼できないポートで受信されたすべてのパケットに、デバイスが再度マーキングする CoS 値です。
- [使用可能な電力 TLV]
  - [要求ID]:最新の電力要求 ID が、電力要求 TLV で最後に受信した [要求ID] フィールドに反映されます。インターフェイスが最後にアップした時点以降に電力要求 TLV を受信しなかった場合は、0 になります。

- [電源管理ID]：次のイベントのいずれかが発生するたびに、値が 1 つ（または、0 を避けるため 2 つ）増加します。

  [有効電力] または [管理電力レベル] が変わった。

  最後に受信した設定値と異なる [要求ID] フィールド値を持つ電力要求 TLV を受信した（または、最初の値を受信したとき）。

  インターフェイスがダウンした。

- [有効電力]：ポートが消費する電力量。
- [管理電力レベル]：電力消費量 TLV についての、POD デバイスに対するサプライヤの要求を表示します。デバイスはこのフィールドに常に [設定なし] と表示します。

• [MDI（UPOE）TLV 経由の 4 線式電源]

  この TLV がサポートされているかどうかが表示されます。

- [4 ペア PoE サポート済み]：PoE がサポートされているかどうかが表示されます。
- [予備ペア検出/分類必要]：この分類が必要かどうかが表示されます。
- [PD 予備ペア所望状態]：PD 予備ペアが必要な状態が表示されます。
- [PD 予備ペア動作状態]：PSE 予備ペアの状態が表示されます。

CDP ネイバー情報

[CDP ネイバー情報] ページには、ネイバー デバイスから受信した CDP 情報が表示されます。

タイムアウトになると、情報は削除されます。ネイバーの TTL TLV で表される時間内に、そのネイバーから CDP PDU が 1 件も受信されなかった場合、タイムアウトになります。

CDP ネイバー情報を表示するには、次のようにします。

ステップ 1 [各種管理] > [ディスカバリ - CDP] > [CDP ネイバー情報] の順にクリックします。

ステップ 2 フィルタを選択するには、[フィルタ] チェックボックスをオンにし、ローカル インターフェイスを選択して、[実行] をクリックします。

フィルタがトリガーされ、[フィルタのクリア] が有効になります。

ステップ 3 フィルタ処理を停止するには、[フィルタのクリア] をクリックします。

[CDP ネイバー情報] ページには、リンク パートナー（ネイバー）に関する次のフィールドが表示されます。

- [デバイス ID]：ネイバーのデバイス ID。
- [システム名]：ネイバーのシステム名。
- [ローカル インターフェイス]：ネイバーが接続されているローカル ポートの番号。
- [アドバタイズメント バージョン]：CDP プロトコル バージョン。
- [存続可能時間（秒）]：このネイバーの情報が削除されるまでの時間間隔（単位：秒）。
- [機能]：ネイバーによってアドバタイズされる機能。
- [プラットフォーム]：ネイバーのプラットフォーム TLV からの情報。
- [ネイバー インターフェイス]：ネイバーの発信インターフェイス。

ステップ 4 デバイスを選択し、[詳細] をクリックします。

このページには、ネイバーに関する次のフィールドが表示されます。

- [デバイス ID]：近隣デバイス ID の ID。
- [システム名]：近隣デバイス ID の名前。
- [ローカルインターフェイス]：フレームが到達する際に経由するポートのインターフェイス番号。
- [アドバタイズメントバージョン]：CDP のバージョン。
- [存続可能時間]：このネイバーの情報が削除されるまでの時間間隔（単位：秒）。
- [機能]：このデバイスの主要機能。機能は 2 オクテットで表されます。ビット 0 ～ 7 はそれぞれ、その他、リピータ、ブリッジ、WLAN AP、ルータ、電話、DOCSIS ケーブル デバイス、ステーションを意味します。ビット 8 ～ 15 は予約されています。
- [プラットフォーム]：ネイバーのプラットフォームの ID。
- [ネイバーインターフェイス]：フレームが到達する際に経由するネイバーのインターフェイス番号。
- [ネイティブ VLAN]：ネイバーのネイティブ VLAN。
- [アプリケーション]：ネイバー上で実行中のアプリケーション名。

- [デュプレックス]:ネイバー インターフェイスが半二重か全二重か。
- [アドレス]:ネイバーのアドレス。
- [使用電力]:インターフェイスでネイバーによって消費される電力量。
- [バージョン]:ネイバーのソフトウェアのバージョン。
- [電力要求]:ポートに接続された PD によって要求される電力。
- [電力要求リスト]:各 PD は、サポートされる電力レベル（最大 3 つ）からなるリストを送信できます。
- [使用可能な電力]
  - [要求 ID]:最新の電力要求 ID が、電力要求 TLV で最後に受信した [要求ID] フィールドに反映されます。インターフェイスが最後にアップした時点以降に電力要求 TLV を受信しなかった場合は、0 になります。
  - [電源管理 ID]:次のイベントのいずれかが発生するたびに、値が 1 つ（または、0 を避けるため 2 つ）増加します。

    [有効電力] フィールドまたは [管理電力レベル] フィールドの値が変わった。

    最後に受信した設定値と異なる [要求 ID] フィールド値を持つ電力要求 TLV を受信した（または、最初の値を受信したとき）。

    インターフェイスがダウンした。
  - [有効電力]:ポートが消費する電力量。
  - [管理電力レベル]:電力消費量 TLV についての、POD デバイスに対するサプライヤの要求を表示します。デバイスはこのフィールドに常に [設定なし] と表示します。
- [MDI 経由の 4 線式電源]
  - [4 ペア PoE サポート済み]:システムとポートが 4 ペア線の有効化をサポートしていることを示します（この HW 能力を持っている特定のポートにのみ当てはまる）。
  - [予備ペア検出/分類必要]:4 ペア線が必要なことを示します。
  - [PD 予備ペア所望状態]:POD デバイスが 4 ペア能力を有効にするように要求していることを示します。
  - [PD 予備ペア動作状態]:4 ペア能力が有効か無効かを示します。

注 [テーブルのクリア] ボタンをクリックすると、CDP からの場合は、接続されていたデバイスがすべて切断され、Auto Smartport が有効な場合は、すべてのポート タイプがデフォルトに変更されます。

CDP 統計情報

[CDP 統計情報] ページには、ポートとの間で送受信された CDP フレームに関する情報が表示されます。CDP パケットは、スイッチ インターフェイスに接続されたデバイスから受信され、Smartport 機能用に使用されます。詳細については、「ディスカバリ - CDP」を参照してください。

ポートの CDP 統計情報は、ポートで CDP がグローバルで有効になっている場合にのみ表示されます。これは、[CDP のプロパティ] ページ、および [CDP インターフェイス設定] ページで行います。

CDP 統計情報を表示するには、次のようにします。

ステップ 1 [各種管理] > [ディスカバリ - CDP] > [CDP 統計情報] の順にクリックします。

各インターフェイスについて、次のフィールドが表示されます。

[受信パケットおよび送信パケット]

- [バージョン 1]:受信または送信した CDP バージョン 1 のパケット数。
- [バージョン 2]:受信または送信した CDP バージョン 2 のパケット数。
- [合計]:受信または送信した CDP パケットの合計数。

[CDPエラー統計情報] には、CDP エラー カウンタが表示されます。

- [無効なチェックサム]:無効なチェックサム値とともに受信したパケットの数。
- [その他のエラー]:無効なチェックサム以外のエラーとともに受信したパケットの数。
- [最大数を超えるネイバー]:空き容量がないためパケット情報をキャッシュに格納できなかった回数。

ステップ 2 すべてのインターフェイスのカウンタを完全にクリアするには、[すべてのインターフェイスカウンタのクリア] をクリックします。1 つのインターフェイスのカウンタを完全にクリアするには、そのインターフェイスを選択し、[インターフェイス カウンタのクリア] をクリックします。

10

ポート管理

ここでは、ポートの設定、リンク アグリゲーション、および Green Ethernet 機能について説明します。

具体的な内容は、次のとおりです。

- ワークフロー
- ポート設定
- エラー回復設定
- ループバック検出設定
- リンクアグリゲーション
- PoE
- Green Ethernet

ワークフロー

ポートを設定するには、次のようにします。

1. [ポート設定] ページでポートを設定します。
2. [LAG 管理] ページで、Link Aggregation Group（LAG; リンク アグリゲーション グループ）プロトコルを有効にするか無効にするかを設定し、また、各 LAG にメンバー ポートを追加します。デフォルトでは、すべての LAG は空になっています。
3. [LAG 設定] ページで、LAG のイーサネット パラメータ値（速度、自動ネゴシエーションなど）を設定します。
4. [LACP] ページで、ダイナミック LAG のメンバーまたはメンバー候補になっているポートの LACP パラメータ値を設定します。
5. [プロパティ] ページで、[Green Ethernet] および [802.3 Energy Efficient Ethernet] を設定します。

6. [ポート設定] ページで、ポートごとの Green Ethernet エネルギー モードおよび 802.3 Energy Efficient Ethernet を設定します。
7. デバイスで PoE がサポートされていて有効になっている場合、ポート管理: PoE の説明に従ってデバイスを設定します。

ポート設定

[ポート設定] ページには、ポートのグローバル設定情報およびポートごとの設定情報が表示されます。このページでポートを選択し、[ポート設定の編集] ページでそのポートを設定することができます。

ポート情報を設定するには、次のようにします。

ステップ 1 [ポート管理] > [ポート設定] をクリックします。

すべてのポートに対してポート設定が表示されます。

ステップ 2 次のフィールドを入力します。

- [リンクフラップ防止]: ネットワークの中断を最小化する場合に選択します。有効になっている場合は、このコマンドが、自動的に、リンク フラップ イベントが発生しているポートを無効にします。
- [ジャンボフレーム]: 最大 9 KB のパケットをサポートする場合に選択します。[ジャンボ フレーム] を有効にしなかった場合（デフォルト）、サポートされる最大パケット サイズは 2,000 バイトになります。9 KB を超えるパケットを受信すると、受信ポートがシャットダウンする可能性があることに注意してください。また、10 KB を超えるパケットを送信すると、受信ポートがシャットダウンする可能性があることに注意してください。

  ジャンボ フレームを有効にするには、この機能を有効にした後でデバイスをリブートする必要があります。

ステップ 3 [適用] をクリックし、グローバル設定情報を更新します。

ジャンボ フレーム設定の変更内容が反映されるのは、[ファイル操作] ページで実行コンフィギュレーションをスタートアップ コンフィギュレーション ファイルに明示的に保存し、デバイスをリブートした後のみです。

ステップ 4 ポートの設定情報を更新するには、目的のポートを選択し、[編集] をクリックします。

ステップ 5 次のパラメータを変更します。

- [インターフェイス]: ポート番号を選択します。

- [ポートの説明]:ポートのユーザ定義名またはコメントを入力します。

> **注：** [インターフェイス] と [ポートの説明] は、メイン ページの [ポート] 列に表示されます。

- [ポートタイプ]:ポートのタイプおよび速度を表示します。次のオプションがあります。
  - [カッパー ポート]:コンボ ポートでない、標準のポート。10 M、100 M、1000 M(タイプ:カッパー)、および 10 G。
  - [コンボ ポート]:カッパー CAT6a ケーブルまたは *SFP ファイバ ギガビット インターフェイス*のどちらかで接続されたコンボ ポート。
  - /SX550X/SX350X

  注 コンボ ポートの両方のポートが使用されている場合は、SFP Fiber が優先されます。
- [管理ステータス]:デバイスのリブート時にこのポートをアクティブ化する場合は [アップ]、アクティブ化しない場合は [ダウン] を選択します。
- [動作ステータス]:ポートが現在アクティブ化されているかどうかが表示されます。ポートがエラーのためにアクティブ化されていない場合、エラーの説明が表示されます。
- [リンクステータスSNMPトラップ]:ポートのリンク ステータスへの変更を通知する SNMP トラップの生成を有効にするには、このフィールドを選択します。
- [時間範囲]:ポートをアクティブ化する時間範囲を有効にするには、このフィールドを選択します。時間範囲がアクティブでない場合、ポートは停止されます。時間範囲が設定されている場合、ポートが管理者によりアクティブ化されている場合のみ有効です。
- [時間範囲名]:時間範囲を指定するプロファイルを選択します。OOB ポートとは無関係です。時間範囲がまだ定義されていない場合、[時間範囲] ページに移動するには [編集] をクリックします。OOB ポートとは無関係です。
- [動作時間範囲の状態]:時間範囲が現在アクティブ化されているかいないかを表示します。
- [自動ネゴシエーション]:このポート上で自動ネゴシエーションを有効にするには、このフィールドを選択します。自動ネゴシエーションを有効にした場合、送信速度、デュプレックス モード、フロー制御の各情報が、このポートからポート リンク パートナーにアドバタイズされます。

- [動作自動ネゴシエーション]: このポートの現在の自動ネゴシエーション ステータスが表示されます。
- [管理ポート速度]: ポートの速度を設定します。使用できる速度はポート タイプによって決まります。[管理速度] を選択できるのは、自動ネゴシエーションを無効にしている場合のみです。
- [動作ポート速度]: 自動ネゴシエーションによって決定された現在のポート速度が表示されます。
- [管理デュプレックスモード]: (非 XG ポートの場合にのみ表示) ポートのデュプレックス モードを選択します。このフィールド値を選択できるのは、自動ネゴシエーションが無効になっており、ポート速度が 10 M または 100 M に設定されている場合のみです。ポート速度が 1 G の場合、モードは常に全二重です。次のオプションがあります。
  - [半二重]: デバイスとクライアントの間で双方向通信を同時に行うことができません。
  - [全二重]: デバイスとクライアントの間で双方向通信を同時に行うことができます。
- [動作デュプレックスモード]: (非 XG ポート上でのみ表示) ポートの現在のデュプレックス モードが表示されます。
- [自動アドバタイズメント]: 自動ネゴシエーションが有効な場合に、このポートからアドバタイズする通信機能を選択します。

  注 すべてのデバイスに対してすべてのオプションが関連するわけではない点に注意してください。

  次のオプションがあります。
  - [最大機能]: すべてのポート速度と両方のデュプレックス モード。
  - [10 半二重]: 10 Mbps のスピードで半二重モード (XG デバイス上には表示されません)。
  - [10 全二重]: 10 Mbps のスピードで全二重モード (XG デバイス上には表示されません)。
  - [100 半二重]: 100 Mbps のスピードで半二重モード (XG デバイス上には表示されません)。
  - [100全二重]: 100 Mbps のスピードで全二重モード。
  - [1000 全二重]: 1000 Mbps のスピードで全二重モード。

- [動作アドバタイズメント]: このポートのネイバーに現在送信されている機能が表示されます。表示されるオプションは、[管理アドバタイズメント] フィールドの選択項目と同じです。
- [プリファレンス モード]: 自動ネゴシエーションが有効になっている場合にのみ使用できます。自動ネゴシエーション動作のための、インターフェイスのマスタースレーブ モードを選択します。次のいずれかのオプションを選択します。
  - [スレーブ]: デバイス ポートが自動ネゴシエーション プロセスにおいてスレーブであるプリファレンスを用いてネゴシエーションを開始します。
  - [マスター]: デバイス ポートが自動ネゴシエーション プロセスにおいてマスターであるプリファレンスを用いてネゴシエーションを開始します。
- [ネイバーアドバタイズメント]: このネイバー デバイス(リンク パートナー)からアドバタイズする機能を選択します。
- [バックプレッシャ]: (非 XG ポート上でのみサポート) このポートにおけるバック プレッシャ モードを選択します。バック プレッシャとは、デバイスが輻輳状態のときにパケット受信速度を下げる方式のことであり、半二重通信モードでのみ使用できます。このオプションを選択すると、信号を混雑させ、リモート ポートからパケットが送信されないようにします。
- [フロー制御]: 802.3x フロー制御を有効にするか無効にするかを選択します。または、ポートでフロー制御の自動ネゴシエーションを有効にするかを選択します(全二重モードの場合のみ)。コンボ ポートではフロー制御自動ネゴシエーションを有効にすることはできません。
- [MDI/MDIX]: このポートの *Media Dependent Interface*(MDI)/*Media Dependent Interface with Crossover* (MDIX) ステータスを選択します。

  次のオプションがあります。
  - [MDIX]: 送信と受信のペアを入れ替える場合、このフィールドを選択します。
  - [MDI]: ストレート ケーブルを使用してこのデバイスをステーションに接続する場合、この項目を選択します。
  - [自動]: 他のデバイスとの接続において正しいピン割り当てが自動検出されるようにこのデバイスを設定する場合、このフィールドを選択します。
- [動作MDI/MDIX]: 現在の MDI/MDIX 設定情報が表示されます。
- [LAG のメンバー]: ポートが LAG のメンバーである場合、LAG 番号が表示されます。それ以外の場合、このフィールドには何も表示されません。

ステップ 6 [適用] をクリックします。ポート設定が、実行コンフィギュレーション ファイルに書き込まれます。

エラー回復設定

このページでは、エラー条件が原因でシャットダウンしたポートを、自動回復間隔が経過した後に自動で再アクティブ化する設定を有効にできます。

エラー回復を設定するには、次の手順を実行します。

ステップ 1 [ポート管理] > [エラー回復設定] をクリックします。

ステップ 2 次のフィールドを入力します。

- [自動回復間隔]: 有効にされている場合、ポートがシャットダウンしてから自動エラー回復までの遅延時間を指定します。
- [自動 ErrDisable 回復]
  - [ポートセキュリティ]: ポート セキュリティ違反のためにポートがシャットダウンした際に自動エラー回復が有効になるようにするには、このフィールドを選択します。
  - [802.1x 単一ホスト違反]: ポートが 802.1x によりシャットダウンされた際に自動エラー回復が有効になるようにするには、このフィールドを選択します。
  - [ACL 拒否]: ACL 動作による自動エラー回復機能を有効にするには、これを選択します。
  - [STP ループバックガード]: STP ループバック ガードによりポートがシャットダウンした際に自動回復を有効にします。
  - [ループバック検出]: ループバック検出によるポートのシャットダウンのエラー回復機能を有効にするには、このフィールドを選択します。
  - [ストーム制御]: ストーム制御によるポートのシャットダウンのエラー回復機能を有効にするには、このフィールドを選択します。
  - [リンクフラップ防止]: ネットワークの中断を最小化する場合に選択します。有効になっている場合は、このコマンドが、自動的に、リンク フラップ イベントが発生しているポートを無効にします。

ステップ 3 [適用] をクリックし、グローバル設定情報を更新します。

ポートを手動で再アクティブ化するには、次の手順を実行します。

ステップ 1 [ポート管理] > [エラー回復設定] をクリックします。

アクティブ化されていないインターフェイスのリストと、その [保留理由] が表示されます。

ステップ 2 再アクティブ化するインターフェイスを選択します。

ステップ 3 [再アクティブ化] をクリックします。

ループバック検出設定

ループバック検出(LBD)は、ループ保護が有効にされているポートからループ プロトコル パケットを送信することにより、ループに対する保護を提供します。スイッチがループ プロトコル パケットを送信し、次いで同じパケットを受信する場合、スイッチはパケットを受信したポートをシャット ダウンします。

ループバック検出は STP とは独立して動作します。ループが検出された後、ループを受信したポートはシャットダウン状態に置かれます。トラップが送信され、イベントが記録されます。ネットワーク マネージャは、LBD パケットの送信間隔を設定する検出間隔を定義することができます。

ループバック検出プロトコルは、次のようなループ状況を検出することができます。

- **ワイヤのショート**:すべての受信トラフィックをループバックするポート。
- **直接マルチポート ループ**:スイッチが、複数のポートにより他のスイッチに接続されており、STP が無効にされています。
- **LAN セグメント ループ**:スイッチが、ループがある LAN セグメントに、1 つまたは複数のポートにより接続されています。

LBD の動作

LBD プロトコルは、定期的にループバック検出パケットをブロードキャストします。スイッチは、自身の LBD パケットを受信すると、ループを検出します。

あるポートに対して LBD をアクティブにするには、次の条件が真でなければなりません。

- LBD がグローバルで有効になっている。
- LBD がそのポートに対して有効になっている。
- ポート動作ステータスがアクティブになっている。
- ポートが、STP フォワーディング ステートまたは無効状態にある（MSTP インスタンス フォワーディング ステート、インスタンス 0）。

LBD フレームは、LBD アクティブ ポートの最高プライオリティ キューに送信されます（LAG の場合、LBD は LAG の各アクティブポート メンバーに送信されます）。

ループが検出されると、スイッチは次の動作を実行します。

- 受信ポートまたは LAG をエラー無効状態に設定する。
- 適切な SNMP トラップを発行する。
- 適切な SYSLOG メッセージを生成する。

デフォルト設定とコンフィギュレーション

ループバック検出はデフォルトでは有効ではありません。

他の機能との連携

ループバック検出が有効にされているポートで STP が有効にされている場合、そのポートは STP フォワーディング ステートになければなりません。

LBD の設定

LBD を有効にして設定するには、次の手順を実行します。

ステップ 1 [ループバック検出設定] ページで、[ループバック検出] をシステム全体で有効にします（後述）。

ステップ 2 [ループバック検出設定] ページで、アクセス ポートに対して [ループバック検出] を有効にします（後述）。

ステップ 3 [エラー回復設定] ページで、ループバック検出の自動回復機能を有効にします。

ループバック検出を設定するには、次の手順を実行します。

ステップ 1 [ポート管理] > [ループバック検出設定] をクリックします。

ステップ 2 機能を有効にするには、[ループバック検出] グローバル フィールドで [有効] を選択します。

ステップ 3 [検出間隔] を入力します。これは LBD パケット送信の間隔です。

ステップ 4 [適用] をクリックし、実行コンフィギュレーション ファイルにコンフィギュレーションを保存します。

[ループバック検出状態] に関連して、各インターフェイスに対して次のフィールドが表示されます。

- [管理]:ループバック検出が有効になっています。
- [動作]:ループバック検出が有効になっていますが、インターフェイスに対してアクティブ化されていません。

ステップ 5 フィルタ内の [インターフェイスタイプが次に等しい] フィールドで、ポートまたは LAG に対して LBD を有効にするかどうかを選択します。

ステップ 6 LBD を有効にするポートまたは LAG を選択し、[編集] をクリックします。

ステップ 7 選択したポートまたは LAG の [ループバック検出状態] フィールドで [有効] を選択します。

ステップ 8 [適用] をクリックし、実行コンフィギュレーション ファイルにコンフィギュレーションを保存します。

リンクアグリゲーション

ここでは、LAG の設定方法について説明します。具体的な内容は、次のとおりです。

リンク アグリゲーションの概要

Link Aggregation Control Protocol（LACP; リンク アグリゲーション制御プロトコル）は IEEE 802.3az で規定されている規格です。複数の物理ポートを束ね、1 つの論理チャネル（LAG）として扱うことができます。LAG を作成した場合、2 つのデバイス間において、帯域幅が広がり、ポートの柔軟性が高まり、また、リンクを冗長構成にすることができます。

作成できる LAG のタイプは次の 2 つです。

- [スタティック]：LAG 内のポートを手動で設定します。LACP が無効になっている場合、LAG は静的に作成されます。スタティック LAG に割り当てられるポートのグループは、常にアクティブ メンバーになります。LAG を手動で作成した場合、LACP オプションを追加したり削除したりするには、その LAG を編集してメンバーを削除する必要があります（メンバーは適用前に再追加できます）。その後、[LACP] ボタンを使用して編集できるようになります。
- [ダイナミック]：LACP が有効になっている場合、LAG は動的に作成されます。ダイナミック LAG に割り当てられるポートのグループは、候補ポートになります。LACP によって、LAG のどの候補ポートをアクティブ メンバー ポートにするかが決定されます。非アクティブ候補ポートはスタンバイ ポートになります。つまり、アクティブ メンバー ポートに障害が発生した場合、*スタンバイ* ポートが代わりに使用されます。

ロード バランシング

LAG に転送されたトラフィックは、アクティブ メンバー ポート間で負荷分散されます。この結果、LAG のすべてのアクティブ メンバー ポートの合計帯域幅に近い帯域幅を効果的に利用できます。

LAG のアクティブ メンバー ポート間でトラフィックをロード バランシングする処理は、ハッシュに基づく分散機能によって管理されます。この機能により、レイヤ 2 またはレイヤ 3 のパケット ヘッダー情報に基づいてユニキャストおよびマルチキャスト トラフィックが分散されます。

このデバイスで使用できるロード バランシング モードは次の 2 種類です。

- **MAC アドレスを基準**:すべてのパケットの送信元 MAC アドレスと宛先 MAC アド レスに基づいて負荷分散されます。
- **IP アドレスと MAC アドレスを基準**:IP パケットの場合は、送信元 IP アドレスと宛先 IP アドレス、非 IP パケットの場合は、送信元 MAC アドレスと宛先 MAC アドレスに基づいて負荷分散されます。

LAG 管理

LAG は通常、1 つの論理ポートとして扱われます。たとえば、LAG のポート属性(状態、速度など)は通常のポートに似ています。

デバイスは、8 個の LAG と LAG あたり最大 8 個のポートをサポートします。

LAG の特徴は次のとおりです。

- LAG 内の各ポートのメディア タイプはすべて同じでなければなりません。
- LAG 内のポートは、別の LAG に追加しないようにしてください。
- 1 つのスタティック LAG には最大 8 個のポートを追加できます。1 つのダイナミック LAG には最大 16 個の候補ポートを追加できます。
- ポートを LAG に追加すると、LAG の設定情報がポートに適用されます。そのポートを LAG から削除すると、そのポートの元々の設定情報が再度適用されます。
- Spanning Tree Protocol(STP)などのプロトコルでは、LAG 内のすべてのポートが 1 つのポートとして扱われます。

デフォルト設定とコンフィギュレーション

デフォルトで、ポートは LAG のメンバーではなく、LAG の一部になる候補でもありません。

スタティック LAG およびダイナミック LAG を設定する手順

LAG を手動で作成した場合、LACP オプションを追加したり削除したりするには、その LAG を編集してメンバーを削除する必要があります。これで、[LACP] ボタンを使用して編集できるようになります。

スタティック LAG を設定するには、次のようにします。

1. LAG で LACP を無効にしてスタティックにします。[ポート リスト] フィールドに表示されているポートを選択して [LAG メンバー] フィールドに移動し、最大 8 個のメンバー ポートをスタティック LAG に追加します。LAG のロード バランシング アルゴリズムを選択します。これらの処理を [LAG 管理] ページで実行します。
2. [LAG 設定] ページで、LAG のさまざまな設定（速度、フロー制御など）を行います。

ダイナミック LAG を設定するには、次のようにします。

1. LAG で LACP を有効にします。[LAG 管理] ページで、[ポート リスト] フィールドに表示されているポートを選択して [LAG メンバー] リストに移動し、最大 16 個の候補ポートをダイナミック LAG に追加します。
2. [LAG 設定] ページで、LAG のさまざまな設定（速度、フロー制御など）を行います。
3. [LACP] ページで、LAG 内のポートの LACP プライオリティおよびタイムアウトを設定します。

LAG 管理

[LAG 管理] ページには、LAG のグローバル管理情報と LAG ごとの管理情報が表示されます。このページでは、LAG のグローバル管理情報を設定できます。また、[LAG メンバーシップの編集] ページで LAG を選択し、LAG ごとの管理情報を設定することもできます。

LAG のロード バランシング アルゴリズムを選択するには、次のようにします。

ステップ 1 [ポート管理] > [リンクアグリゲーション] > [LAG 管理] をクリックします。

ステップ 2 [ロードバランスアルゴリズム] で次のいずれかを選択します。

- [MAC アドレス]:すべてのパケットの送信元 MAC アドレスと宛先 MAC アドレスに基づいて、ロード バランシングを実行します。

- [IP/MAC アドレス]:IP パケットの場合は、送信元 IP アドレスと宛先 IP アドレス、非 IP パケットの場合は、送信元 MAC アドレスと宛先 MAC アドレスに基づいてロード バランシングを実行します。

ステップ 3 [適用] をクリックします。ロード バランス アルゴリズムが実行コンフィギュレーション ファイルに保存されます。

LAG 内のメンバー ポートまたは候補ポートを定義するには、次のようにします。

ステップ 1 LAG を選択し、[編集] をクリックします。

各 LAG に対して、次のフィールドが表示されます([編集] ページにないフィールドのみ説明します)。

- [リンクステート]:ポートがアクティブ化されているかどうか。
- [アクティブ メンバー]:LAG のアクティブ ポート。
- [スタンバイ メンバー]:この LAG の候補ポート。

ステップ 2 次のフィールドに値を入力します。

- [LAG]:LAG 番号を選択します。
- [LAG 名]:LAG 名またはコメントを入力します。
- [LACP]:選択した LAG で LACP を有効にする場合に選択します。このフィールドを選択した場合、LAG はダイナミック LAG になります。このフィールドを有効にできるのは、次のフィールドでポートを LAG に移動した場合だけです。
- [ポート リスト]:LAG に追加するポートを [ポート リスト] フィールドで選択し、[LAG メンバー] フィールドに移動します。1 つのスタティック LAG には最大 8 個、1 つのダイナミック LAG には最大 16 個の候補ポートを追加できます。これらが候補ポートです。

ステップ 3 [適用] をクリックします。LAG メンバーシップが実行コンフィギュレーション ファイルに保存されます。

LAG 設定

[LAG 設定] ページには、すべての LAG の現在の設定情報が表示されます。[LAG 設定の編集] ページでは、選択した LAG の情報の設定、また、一時停止されている LAG の再アクティブ化を行うことができます。

LAG 設定を構成したり一時停止されている LAG を再アクティブ化したりするには、次のようにします。

ステップ 1 [ポート管理] > [リンクアグリゲーション] > [LAG 設定] をクリックします。

システム内の LAG が表示されます。

ステップ 2 LAG を選択し、[編集] をクリックします。

ステップ 3 次のフィールドに値を入力します。

- [LAG]:LAG 番号を選択します。
- [LAGタイプ]:この LAG を構成しているポートのタイプが表示されます。
- [説明]:LAG 名またはコメントを入力します。
- [管理ステータス]:選択した LAG をアクティブ化する場合は [アップ]、アクティブ化しない場合は [ダウン] を選択します。
- [動作ステータス]:LAG が現在アクティブ化されているかどうかが表示されます。
- [リンクステータスSNMPトラップ]:ポートのリンク ステータスに変更を通知する SNMP トラップの生成を有効にするには、このフィールドを選択します。
- [時間範囲]:ポートをアクティブ化する時間範囲を有効にするには、このフィールドを選択します。時間範囲がアクティブでない場合、ポートは停止されます。時間範囲が設定されている場合、ポートが管理者によりアクティブ化されている場合のみ有効です。
- [時間範囲名]:時間範囲を指定するプロファイルを選択します。時間範囲がまだ定義されていない場合、[時間範囲] ページに移動するには [編集] をクリックします。
- [動作時間範囲の状態]:時間範囲が現在アクティブ化されているかいないかを表示します。

- [管理自動ネゴシエーション]:LAG で自動ネゴシエーションを有効にするか無効にするかを選択します。自動ネゴシエーションは、リンク相手との間で実行されます。自動ネゴシエーションを有効にした場合、自身の伝送速度とフロー制御が相手にアドバタイズされます。フロー制御のアドバタイズは、デフォルトでは [無効] になっています。アグリゲートされているリンクの両側で自動ネゴシエーションを有効にするか、または、両側で自動ネゴシエーションを無効にしてリンク速度を同じにすることを推奨します。
- [動作自動ネゴシエーション]:現在の自動ネゴシエーションのステータスが表示されます。
- [管理速度]:LAG 内のポートの速度を選択します。
- [動作LAG速度]:LAG の現在の速度が表示されます。
- [管理アドバタイズメント]:この LAG からアドバタイズする通信機能を選択します。次のオプションがあります。
  - [最大機能]:すべての LAG 速度と両方のデュプレックス モード。
  - [10 全二重]:10 Mbps のスピードのアドバタイズで全二重モード。
  - [100 全二重]:100 Mbps のスピードのアドバタイズで全二重モード。
  - [1000 全二重]:1000 Mbps のスピードのアドバタイズで全二重モード。
- [動作アドバタイズメント]:管理アドバタイズメントのステータスが表示されます。この LAG からその機能がネイバー LAG にアドバタイズされ、ネゴシエーション プロセスが開始します。表示される値は、[管理アドバタイズメント] フィールドの選択項目と同じです。
- [管理フロー制御]:[フロー制御] を [有効] または [無効] に設定するか、LAG で [フロー制御] の [自動ネゴシエーション] を有効にします。
- [動作フロー制御]:現在の [フロー制御] のステータスが表示されます。

ステップ 4 [適用] をクリックします。実行コンフィギュレーション ファイルが更新されます。

LACP

ダイナミック LAG では LACP が有効になっており、LAG で定義されているすべての候補ポート上で動作します。

LACP におけるプライオリティとルール

候補ポートが 9 個以上追加されているダイナミック LAG では、LACP システム プライオリ ティと LACP ポート プライオリティの両方を使用して、どの候補ポートがアクティブ メンバ ポートになるかが決定されます。

選択された候補ポートは、すべて同じリモート デバイスに接続されます。ローカル スイッチとリモート スイッチのどちらにも LACP システム プライオリティが設定されます。

LACP ポート プライオリティがローカル デバイスとリモート デバイスのどちらから選ばれるかを決定するために、次のアルゴリズムが使用されます。ローカル LACP プライオリティは、リモート LACP システム プライオリティと比較されます。プライオリティが最も低いデバイスによって、LAG の候補ポートが選択されます。両者のプライオリティが同じである場合は、両者の MAC アドレスが比較されます。MAC アドレスが最も小さいデバイスのプライオリティによって、LAG の候補ポートが決定されます。

ダイナミック LAG には、同じタイプのイーサネット ポートを最大 16 個追加できます。アクティブにできるポートとスタンバイ モードにできるポートは、それぞれ最大 8 個です。ダイナミック LAG 内に 9 個以上のポートがある場合、このリンクの制御エンドであるデバイスでは、ポート プライオリティに基づいて、この LAG に割り当てるポート、および、ホットスタンバイ モードにするポートが決定されます。もう一方のデバイス(このリンクの非制御エンド)で設定されているポート プライオリティは無視されます。

次の追加ルールを使用して、ダイナミック LACP のアクティブ ポートまたはスタンバイ ポートが選択されます。

- 伝送速度が最速アクティブ メンバー ポートと異なるリンクや、半二重モードで動作しているリンクは、スタンバイ モードになります。ダイナミック LAG 内のアクティブ ポートは、すべて同じボー レートで動作します。
- リンクの LACP ポート プライオリティの値が現在のアクティブ メンバー ポートより小さく、アクティブ メンバー ポートの数がすでに上限数に達している場合、このリンクは非アクティブになり、スタンバイ モードに移行します。

リンク パートナーを持たない LACP

LACP が LAG を作成するには、両方のリンク エンドのポートが LACP に対して設定されなければなりません。つまり、ポートが LACP PDU を送信し、受信した PDU を処理しなければなりません。

しかしながら、1 つのリンク パートナーが LACP に対して一時的に設定されていないことがあります。そのような状況の一例は、リンク パートナーがデバイス上にあり、自動コンフィギュレーション プロトコルを使用して自身のコンフィギュレーションを受信するプロセスの最中である場合です。このデバイスのポートはまだ LACP に対して設定されていません。LAG リンクがアクティブ化できない場合、デバイスの設定を実行することはできません。同じような状況は、デュアル NIC ネットワークブート コンピュータ（例、PXE）でも起こり得ます。これは、起動後でなければ LAG コンフィギュレーションを受信することができません。

いくつかの LACP 設定ポートが設定され、リンクが 1 つ以上のポートでアクティブ化されたもののそれらのポートに対してリンク パートナーからの LACP 応答がない場合、アクティブ化されたリンクを持つ最初のポートは LACP LAG に追加され、アクティブ化されます（他のポートは非候補になります）。このようにして、ネイバー デバイスは、たとえば DHCP を使用して IP アドレスを取得し、自動コンフィギュレーションを使用して自身のコンフィギュレーションを取得します。

LACP 設定

[LACP] ページを使用して、LAG の候補ポートを設定し、ポートごとに LACP パラメータを設定します。

LAG に対してアクティブ メンバー ポートの上限数（8）を超える候補ポートが追加されていて、かつ各候補ポートの特性が同じである場合、プライオリティが最も高いポートがデバイスのダイナミック LAG からアクティブ ポートとして選択されます。

注 LACP 設定情報は、ダイナミック LAG のメンバーでないポートでは関係ありません。

LACP 設定を定義するには、次のようにします。

ステップ 1 [ポート管理] > [リンクアグリゲーション] > [LACP] をクリックします。

ステップ 2 [LACP システムプライオリティ] を入力します。

ステップ 3 ポートを選択して、[編集] をクリックします。

ステップ 4 次のフィールドに値を入力します。

- [ポート]: タイムアウト値とプライオリティを設定するポートの番号を選択します。

- [LACP ポートプライオリティ]: このポートの LACP プライオリティを入力します。
- [LACP タイムアウト]: 連続する LACP PDU の送受信の時間間隔です。相手デバイスから定期的に送信される LACP PDU を待つ時間（[ロング]/[ショート]）を、表示される LACP タイムアウトの設定から選択します。

ステップ 5 [適用] をクリックします。実行コンフィギュレーション ファイルが更新されます。

PoE

ここでは、PoE 機能を使用する方法について説明します。

具体的な内容は、次のとおりです。

- 概要
- PoE のプロパティ
- 設定
- 統計情報
- Green Ethernet の概要

概要

PoE デバイスとは、ネットワーク トラフィックの中断、物理ネットワークの更新、または ネットワーク インフラストラクチャの変更を行うことなく、既存のカッパー ケーブルを介して、接続先の受電装置（PD）に電力を供給する給電側機器（PSE）です。

特徴

PoE には次の機能があります。

- 有線 LAN 上のすべてのデバイスに 110/220 V AC 電源を確保する必要がなくなる。
- すべてのネットワーク デバイスを電源の近くに置く必要がなくなる。
- ケーブル システムを社内で二重に配置する必要がなくなるため、設置コストを大幅に削減できる。

Power over Ethernet は、イーサネット LAN に接続する比較的低出力の装置を配置する企業ネットワークで使用できます。たとえば、次のような装置があります。

- IP 電話
- ワイヤレス アクセス ポイント
- IP ゲートウェイ
- 音声およびビデオ リモート モニタリング デバイス

動作

PoE は次のステージで実装されます。

- **検出**:カッパー ケーブルに特殊パルスを送信します。PoE デバイスが相手側にある場合、そのデバイスがこのパルスに応答します。
- **分類**:検出ステージの後、給電側機器(PSE)と受電装置(PD)の間でネゴシエーションが開始します。ネゴシエーション中、PD は、自分が消費する最大電力を示すクラスを指定します。
- **電力消費**:分類ステージが完了した後、PSE は PD に電力を供給します。PoE 対応であっても分類が存在しない PD は、クラス 0(最大)と想定されます。PD が、規格で許可されている以上の電力を消費しようとすると、PSE はポートへの給電を停止します。

PoE は 2 つのモードをサポートしています。

- **ポート制限**:デバイスが供給に同意する最大電力は、分類ステージの結果にかかわらず、システム管理者が設定する値に制限されます。
- **クラス電力制限**:デバイスが供給に同意する最大電力は、分類ステージの結果によって決まります。つまり、クライアントの要求により設定されます。

PoE デバイス

アップリンク ポートは、1 または 2 つの PD ポートを備えた受電デバイス(PD)として機能します。8 ポート デバイスでは、最上位ポートが PD になります(PD ポートは給電側機器(PSE)機能を備えていません)。2 つの PD ポートが存在する場合は、それらを 1 つの PSE に接続することをお勧めします。両方の PD ポートに同じ電力標準(両方が AF、両方が AT、または両方が 60W PoE)から電力が供給されていれば、両方のポートが機能します。

さまざまな SKU とその PoE の詳細については、Power Over Ethernet モデルのスイッチを参照してください。

PoE 設定における考慮事項

PoE の設定をする際は、以下を考慮してください。

- PSE が供給できる電力量。
- PD が実際に消費しようとする電力量。

次の項目を設定できます。

- PSE から PD に給電できる最大電力。
- モード。デバイス稼動中に、クラス電力制限からポート制限へ、またはその反対へモードを変更できます。ポート制限モードで設定されたポート別電力値は保持されます。

  注 デバイスの動作中にモードをクラス制限からポート制限に（またはその逆に）変更すると、PD が強制的にリブートされます。
- ポート別数値制限（mW 単位）により許可される最大ポート制限（ポート制限モード）。
- PD が許容されている以上の電力を消費しようとした場合に生成されるトラップと、トラップが生成される最大電力割合。

PoE 対応ハードウェアが自動的に PD クラスを検出し、各ポートに接続されているデバイスのクラスに従い、電力制限を検出します（クラス制限モード）。

接続中に、（デバイスがクラス制限モードかポート制限モードかにかかわらず）設定済みの割り当てによって可能な量を超える電力を PD がデバイスに要求した場合、デバイスは次のことを行います。

- PoE ポート リンクのアップ/ダウン状態を維持します。
- PoE ポートへの給電を停止します。
- 電力停止の理由をログに記録します。
- SNMP トラップを生成します。

PoE のプロパティ

注　この項は PoE をサポートするデバイスのみに関連します。

PoE の [プロパティ] ページでは、PoE モードとしてポート制限またはクラス制限のいずれかを選択し、PoE トラップの生成を指定できます。

これらの設定は事前に入力されています。PD が実際に接続されて電力が消費されているとき、消費されている電力が許可されている最大電力よりずっと小さい場合があります。

リブート、初期化、およびシステム コンフィギュレーション中は、PD の損傷を避けるために出力電力はオフになります。

デバイスで PoE を設定し、現在の電力消費量を監視するには、次のようにします。

ステップ 1　[ポート管理] > [PoE] > [プロパティ] をクリックします。

ステップ 2　次のフィールドに値を入力します。

- [電力モード]: 次のいずれかのオプションを選択します。
  - [クラス制限]: 分類ステージの結果として、デバイスのクラスによりポート別最大電力量が決まります。
  - [ポート制限]: ユーザが、ポートごとの最大電力量を設定します。

  注　ポート制限からクラス制限に（またはその逆に）変更する場合には、PoE ポートを無効にし、電力設定を変更した後でポートを有効にする必要があります。
- [トラップ]: トラップを有効または無効にします。トラップを有効にする場合は、SNMP もまた有効にして、少なくとも 1 つの通知受信者を設定する必要があります。
- [電力トラップしきい値]: 消費量しきい値（電力制限のパーセンテージ）を入力します。電力がこの値を超えると、アラームが発生します。
- [ソフトウェア バージョン]: PoE チップのソフトウェア バージョンが表示されます。

それぞれのデバイスまたはスタックの全装置に関して、次のカウンタが表示されます。

- [定格電力]: デバイスが、接続している全 PD に給電できる電力総量。
- [消費電力]: PoE ポートが現在消費している電力量。
- [有効電力]: 定格電力から消費電力量を差し引いた値。

- [PSE チップセットとハードウェア リビジョン]:PoE チップセットとハードウェア リビジョン番号。

ステップ 3 [適用] をクリックして、PoE プロパティを保存します。

設定

[設定] ページには、システムの PoE 情報が表示され、PoE モードがポート制限の場合にインターフェイス上で PoE を有効にしたり、現在の電力消費量やポート別最大電力を監視したりすることができます。

注 デバイスで特定の期間にわたって PoE を設定することができます。この機能を使用して、PoE が有効になる曜日と時間帯をポートごとに定義できます。時間範囲がアクティブでないときには、PoE が無効になります。この機能を使用するには、まず [時間範囲] ページで時間範囲を定義しておく必要があります。

このページは、ポートあたりの電力を指定されたワット数に制限します。これらの設定をアクティブにするには、システムが PoE ポート制限モードになっている必要があります。このモードは、[PoE のプロパティ] ページで設定されます。

ポートで消費される電力がポート制限値を超えると、ポート電力はオフになります。

PoE プライオリティの例

想定:48 のポートを持つデバイスが合計 375 ワットを供給しているとします。

管理者は、すべてのポートに最大 30 ワットを割り当てるよう設定しています。48 のポートに 30 ワットを掛けると 1440 ワットになり、これは多すぎます。デバイスは各ポートに十分な電力を供給できないため、プライオリティに従って電力を供給します。

管理者は各ポートのプライオリティを設定して、受電可能な電力量を割り当てます。

これらのプライオリティは、PoE の [設定] ページで指定します。

PoE をサポートするデバイス モデルと、PoE ポートに割り当て可能な最大電力については、「システム設定」の説明を参照してください。

PoE ポート制限を設定するには、次のようにします。

ステップ 1 [ポート管理] > [PoE] > [設定] をクリックします。

ポートと関連する PoE 情報が表示されます。これらのフィールドは [編集] ページで説明されます。ただし、次のフィールドを除きます。

- [管理電力割り当て(mW)]:割り当てることができる電力量を入力します。
- [動作ステータス]:PoE がポートで現在アクティブかどうかが表示されます。
- [PoE 標準]:サポートされている PoE のタイプが表示されます(60W PoE および 802.3 AT PoE など)。

ステップ 2 ポートを選択して、[編集] をクリックします。

ステップ 3 次のフィールドを入力します。

- [インターフェイス]:設定するポートを選択します。
- [管理ステータス]:ポートでの PoE を有効または無効にします。
- [時間範囲]:ポートでの PoE を有効にする場合に選択します。
- [時間範囲名]:[時間範囲] が有効になっている場合、使用する時間範囲を選択します。時間範囲は [時間範囲] ページで定義されます。新規の時間範囲を定義するには、[編集] をクリックします。
- [プライオリティレベル]:電力供給が低くなったときに使用するポートのプライオリティ(低、高、または重要)を選択します。たとえば、電力供給率が 99% であるとき、ポート 1 のプライオリティが高で、ポート 3 のプライオリティが低の場合、ポート 1 は電力を受け、ポート 3 は電力を受けられないことがあります。
- [管理電力割り当て]:PoE の [プロパティ] ページで電力モードとしてポート制限を設定した場合にのみ、このフィールドが表示されます。電力モードがポート制限モードである場合、ポートに割り当てる電力(ミリワット単位)を入力します。
- [4 ペアの強制]:電源に予備ペアを強制する場合に選択します。これにより、CDP/LLDP PoE ネゴシエーションをサポートしない PD に 60 ワット PoE を使用できます。
- [最大電力割り当て]:PoE の [プロパティ] ページで設定した電力モードがポート制限モードである場合にのみ、このフィールドが表示されます。このポートで許可される電力の最大量が表示されます。
- [ネゴシエートされる電力]:デバイスに割り当てられる電力。

- [電力ネゴシエーションプロトコル]:ネゴシエートされる電力を決定するプロトコル。
- [電力消費]:設定(クラス制限)で割り当てられたミリワット単位の電力量が表示されます。
- [クラス]:発生する電力のクラスが表示されます。

[設定(クラス制限)] ページには、システムの PoE 情報が表示され、インターフェイス上で PoE を有効にしたり、現在の電力消費量やポート別最大電力制限を監視したりすることができます。

注 デバイスで特定の期間にわたって PoE を設定することができます。この機能を使用して、PoE が有効になる曜日と時間帯をポートごとに定義できます。時間範囲がアクティブでないときには、PoE が無効になります。この機能を使用するには、まず [時間範囲] ページで時間範囲を定義しておく必要があります。

このページは、接続された PD のクラスに基づいて、ポートあたりの電力を制限します。これらの設定をアクティブにするには、システムが PoE クラス制限モードになっている必要があります。このモードは、PoE の [プロパティ] ページで設定されます。

ポートで消費される電力がクラス制限値を超えると、ポート電力はオフになります。

PoE プライオリティの例

PoE をサポートするデバイス モデルと、PoE ポートに割り当て可能な最大電力については、「システム設定」の説明を参照してください。

PoE クラス制限を設定するには、次のようにします。

ステップ 1 [ポート管理] > [PoE] > [設定(クラス制限)] の順にクリックします。

ポートと関連する PoE 情報が表示されます。これらのフィールドは [編集] ページで説明されます。ただし、次のフィールドを除きます。

- [PoE 標準]:サポートされている PoE のタイプが表示されます(60W PoE および 802.3 AT PoE など)。
- [動作ステータス]:PoE がポートで現在アクティブかどうかが表示されます。

ステップ 2 ポートを選択して、[編集] をクリックします。

ステップ 3 次のフィールドに値を入力します。

- [インターフェイス]:設定するポートを選択します。
- [管理ステータス]:ポートでの PoE を有効または無効にします。

- [プライオリティレベル]:電力供給が低くなったときに使用するポートのプライオリティ(低、高、または重要)を選択します。たとえば、電力供給率が 99% であるとき、ポート 1 のプライオリティが高で、ポート 3 のプライオリティが低の場合、ポート 1 は電力を受け、ポート 3 は電力を受けられないことがあります。
- [4 ペアの強制]:拡張電源を提供する場合にこの機能を有効にします。
- [電力消費]:割り当てられたミリワット単位の電力量が表示されます。設定(クラス制限)
- [クラス]:デバイスの最大電力レベルを示す、デバイスのクラスが表示されます。

クラス	デバイス ポートから送られる最大電力
0	30.0 ワット
1	4.0 ワット
2	7.0 ワット
3	15.4 ワット
4	30.0 ワット

- [最大電力割り当て]:PoE の [プロパティ] ページで設定した電力モードがポート制限モードである場合にのみ、このフィールドが表示されます。このポートで許可される電力の最大量が表示されます。
- [ネゴシエートされる電力]:デバイスに割り当てられる電力。
- [電力ネゴシエーションプロトコル]:ネゴシエートされる電力を決定するプロトコル。

ステップ 4 [適用] をクリックします。ポートの PoE 設定が実行コンフィギュレーション ファイルに書き込まれます。

統計情報

このページには、一定期間の平均電力消費を表す電力消費傾向が表示されます。これは、PoE 動作のモニタリングとデバッグに有効です。

デバイスは、一定期間の PoE ポート消費値(ワット単位)を保存しています。そのため、指定された日/週/月の期間の平均 PoE 消費の計算および表示が可能になるとともに、傾向の検出が可能になります。インターフェイスごとの情報とデバイス全体の情報が提供されます。

PoE 消費値は 1 分ごとに測定されます。日次統計情報、週次統計情報、および月次統計情報は、リブートしても消えないようにフラッシュ メモリに保存されます。

ポート/デバイスあたりの平均 PoE 消費のサンプルを以下に示します。

期間内の PoE 消費測定値の合計/サンプリング期間の時間（分）

デバイス上の PoE 消費傾向を表示して、表示用の設定を定義するには、以下のようにします。

ステップ 1 [ポート管理] > [PoE] > [統計情報] をクリックします。

ステップ 2 [ユニット] フィールドと [ポート] フィールドでポートを選択します。

ステップ 3 [リフレッシュ レート] を選択します。

ステップ 4 選択したインターフェイスに関する次のフィールドが表示されます。

[消費履歴]

- [過去 1 時間の平均消費]：過去 1 時間のすべての PoE 消費測定値の平均。
- [過去 1 日の平均消費]：過去 1 日のすべての PoE 消費測定値の平均。
- [過去 1 週間の平均消費]：過去 1 週間のすべての PoE 消費測定値の平均。

[PoE イベント カウンタ]

- [過負荷カウンタ]：検出された過負荷状態の数。
- [ショート カウンタ]：検出されたショート状態の数。
- [拒否カウンタ]：検出された拒否状態の数。
- [未検出カウンタ]：検出された未検出状態の数。
- [無効な署名カウンタ]：検出された無効な署名状態の数。

次の操作をメインページで実行することができます。

- [イベント カウンタのクリア]：表示されたイベント カウンタをクリアします。
- [すべてのインターフェイス統計情報の表示]：すべてのインターフェイスに関する上記統計情報を表示します。
- [インターフェイス履歴グラフの表示]：カウントをグラフ形式で表示します。
- [リフレッシュ]：表示されたカウンタをリフレッシュします。

[すべてのインターフェイス統計情報の表示] をクリックすると、次の操作を実行できます。

- [イベント カウンタのクリア]:表示されたイベント カウンタをクリアします。
- [インターフェイス統計情報の表示]:選択されたインターフェイスに関する上記統計情報を表示します。
- [インターフェイス履歴グラフの表示]:選択されたインターフェイスに関するカウンタをグラフ形式で表示します。
- [リフレッシュ]:表示されたカウンタをリフレッシュします。

[インターフェイス履歴グラフの表示] をクリックすると、次の操作を実行できます。

- [インターフェイス統計情報の表示]:選択されたインターフェイスに関するグラフ統計情報を表形式で表示します。[期間] を時間、日、週、または年で入力します。
- [すべてのインターフェイス統計情報の表示]:すべてのインターフェイスに関する上記統計情報を表形式で表示します。[期間] を時間、日、週、または年で入力します。
- [イベント カウンタのクリア]:カウンタをクリアします。

Green Ethernet

ここでは、デバイスの電力を減らすために設計された Green Ethernet 機能について説明します。

内容は次のとおりです。

Green Ethernet の概要

Green Ethernet は、環境に配慮してデバイスの電力消費量を減らす機能の総称です。Green Ethernet は EEE と異なり、すべてのデバイスで Green Ethernet エネルギー検出が有効になります。EEE ではギガバイト ポートのみが有効になります。

Green Ethernet 機能では、次の方法で全体的な電力消費量を減らすことができます。

- [エネルギー検出モード]:非アクティブ リンク上のポートは非アクティブ モードに移行します。これにより、ポートの管理ステータスを「アップ」にしたまま電力を節約することができます。非アクティブ モードから完全動作モードに戻るのに要する時間は非常に短く、ユーザが意識することはありません。フレームが欠落することもありません。このモードは、GE ポートと FE ポートのどちらでも使用できます。このモードはデフォルトで無効になっています。
- [ショートリーチモード]:短いケーブルで電力が削減されます。ケーブル長が解析されると、そのケーブル長に合わせて電力消費量が調整されます。ケーブルが Tengigabit ポートの場合は 30 m、その他のタイプのポートの場合は 50 m よりも短い場合、そのケーブル上でフレームを送信する際の電力消費量が減少します。これにより、電力を節約することができます。このモードは、RJ-45 ポートでのみ使用できます。コンボ ポートでは使用できません。このモードはデフォルトで無効になっています。

これらの Green Ethernet 機能の他に、GE ポートをサポートするデバイスには **802.3az Energy Efficient Ethernet（EEE）**もあります。EEE を使用すると、ポートにトラフィックが流れていない場合の電力消費を抑えることができます。詳細については、「802.3az Energy Efficient Ethernet 機能」を参照してください（GE モデルでのみ利用可能です）。

EEE はデフォルトでグローバルに有効になっています。あるポートで EEE が有効な場合、ショート リーチ モードを無効にする必要があります。同様に、ユーザはショート リーチ モードを有効にする前に EEE を無効にする必要があります。XG インターフェイスではショート リーチが常に有効であり、EEE 設定に関する制限はありません。

これらのモードは、ポートごとに設定され、ポートの LAG メンバーシップは考慮されません。

デバイスの LED は電力を消費します。ほとんどの時間、デバイスは誰もいない部屋にありますので、LED を点灯するのはエネルギーの無駄遣いです。Green Ethernet 機能により、必要のないときはポートの LED（リンク、速度および PoE）を無効にし、必要になったとき（デバッグ、追加のデバイスを接続するなど）に LED を有効にすることができます。

[システムの要約] ページでは、デバイス ボードの写真に表示される LED は LED 無効化の影響を受けません。

電力節約量、現在の電力消費量、および累積節電量を監視できます。合計電力節約量は、Green Ethernet 機能を利用していない場合のその物理インターフェイスの電力消費量に対するパーセント値で表示されます。

表示される節電量は、Green Ethernet に関連するものに限られます。EEE に節約されたエネルギーの量は表示されません。

ポート LED の無効化による電力節約

ポート LED の無効化機能により、デバイスの LED が消費する電力を節約することができます。デバイスはしばしば誰もいない部屋にありますので、LED を点灯するのはエネルギーの無駄遣いです。Green Ethernet 機能により、必要のないときはポートの LED（リンク、速度および PoE）を無効にし、必要になったとき（デバッグ、追加のデバイスを接続するなど）に LED を有効にすることができます。

[システムの要約] ページでは、デバイス ボードの写真に表示される LED は LED 無効化の影響を受けません。

ポート LED は、[プロパティ] ページで無効化することができます。

802.3az Energy Efficient Ethernet 機能

ここでは、802.3az Energy Efficient Ethernet（EEE）機能について説明します。

具体的な内容は、次のとおりです。

- 802.3az EEE の概要
- アドバタイズ機能のネゴシエーション
- 802.3Az EEE のリンク レベル検出
- 802.3az EEE の可用性
- デフォルト コンフィギュレーション
- 機能間の連携
- 802.3az EEE を設定する手順

802.3az EEE の概要

802.3az EEE は、リンクのトラフィックが流れていないときに電力を削減するように設計されています。Green Ethernet では、ポートが非アクティブ化されているときに電力が削減されます。802.3az EEE では、ポートがアクティブ化されていてもトラフィックがない場合に電力が削減されます。

802.3az EEE はアウトオブバンド ポートではサポートされません。

注 リモート リンク パートナー ステータスを表示できるのは、リンク速度が 1 G または 10 G の場合のみです。

802.3az EEE を使用すると、トラフィックが流れていないときに、リンクの両側のシステムではそれぞれの機能の一部を無効にして電力を削減することができます。

802.3az EEE では、100 Mbps および 1000 Mbps の IEEE 802.3 MAC 動作をサポートしています。

両方のデバイスで最適なパラメータの組み合わせを選択するために、LLDP が使用されます。リンク パートナーで LLDP がサポートされない場合、または LLDP が無効な場合、802.3az EEE はそのまま動作しますが、最適な動作モードにはならない可能性があります。

802.3az EEE 機能は、Low Power Idle（LPI）モードと呼ばれるポート モードで実装されます。トラフィックが流れていないときにこの機能が有効であれば、ポートは LPI モードに入り、電力消費が大幅に削減されます。

802.3az EEE が機能するには、接続の両側（デバイスのポートおよび接続しているデバイス）で 802.3az EEE がサポートされている必要があります。トラフィックが流れていないときは、両側から電力を削減しようとしていることを示す信号を送信されます。両側からの信号を受信すると、ポートが LPI ステータスであること（および非アクティブ化ステータスではないこと）がキープ アライブ信号で示され、電力が削減されます。

ポートを LPI モードのままにするには、キープ アライブ信号を両側から継続的に受信する必要があります。

アドバタイズ機能のネゴシエーション

802.3az EEE サポートは、自動ネゴシエーション段階でアドバタイズされます。自動ネゴシエーションにより、リンクされたデバイスは、リンクの他端側デバイスでサポートされる機能（動作モード）を検出したり、共通の機能を判断したり、結合操作用に自身を設定したりすることができます。自動ネゴシエーションは、リンクアップ時、管理のコマンド発行時、またはリンク エラーの検出時に実行されます。リンク確立プロセス時に、両方のリンク パートナーがそれぞれの 802.3az EEE 機能を交換します。自動ネゴシエーションがデバイスで有効になっている場合は、ユーザの操作なしで自動的に自動ネゴシエーションが行われます。

注　ポートで自動ネゴシエーションが有効でない場合、EEE は無効です。唯一の例外として、リンク速度が 1 GB または 10 G の場合は、自動ネゴシエーションが無効であっても、EEE が有効なままになります。

802.3Az EEE のリンク レベル検出

これらの機能の他に、802.3az EEE の機能および設定も、IEEE 規格 802.1AB プロトコル（LLDP）の Annex G で定義されている組織固有の TLV に基づいたフレームを使用してアドバタイズされます。LLDP は、自動ネゴシエーション完了後に、802.3az EEE の動作をさらに最適化するために使用されます。802.3az EEE TLV は、システムのウェイクアップ期間と更新期間を微調整するために使用されます。

802.3az EEE の可用性

EEE をサポートする製品の詳細な一覧については、リリース ノートを参照してください。

デフォルト コンフィギュレーション

デフォルトでは、802.3az EEE および EEE LLDP は、グローバルおよびポートごとに有効です。

機能間の連携

802.3az EEE と他の機能との連携について次に説明します。

- ポートで自動ネゴシエーションが有効でない場合、802.3az EEE 動作ステータスは無効です。このルールの例外として、リンク速度が 1 GB の場合は、自動ネゴシエーションが無効であっても、EEE が有効なままになります。
- 802.3az EEE が有効でポートがアクティブ化されている場合、ポートの最大ウェイク アップ時間値に従って、ただちに動作を開始します。
- GE ポートのポート速度が 10 Mbit に変更されると、802.3az EEE は無効になります。これは、GE モデルでのみサポートされています。

802.3az EEE を設定する手順

ここでは、802.3az EEE 機能を設定し、カウンタを表示する方法について説明します。

ステップ 1　[ポート管理] > [ポート設定] ページを開いて、ポートで自動ネゴシエーションが有効になっていることを確認します。

a. ポートを選択し、[ポート設定の編集] ページを開きます。

b. [自動ネゴシエーション] フィールドを選択して、有効にします。

ステップ 2 [プロパティ] ページで、[802.3 Energy Efficient Ethernet (EEE)] がグローバルに有効であることを確認します(デフォルトで有効です)。このページには、エネルギーの節約量も表示されます。

ステップ 3 [ポート設定] ページを開いて、ポートで 802.3az EEE が有効になっていることを確認します。

a. ポートを選択し、[ポート設定の編集] ページを開きます。

b. ポートの [802.3 Efficient Energy Ethernet(EEE)] モードを確認します(デフォルトで有効です)。

c. [802.3 Energy Efficient Ethernet (EEE) LLDP] で、LLDP を通じて 802.3az EEE 機能のアドバタイズメントを有効にするか無効にするかを選択します(デフォルトで有効です)。

ステップ 4 ローカル デバイスの 802.3 EEE 関連情報を表示するには、[LLDP ローカル情報] ページを開き、[802.3 Energy Efficient Ethernet (EEE)] ブロックで情報を表示します。

ステップ 5 リモート デバイスの 802.3az EEE 情報を表示するには、[LLDP ネイバー情報] ページを開き、[802.3 Energy Efficient Ethernet (EEE)] ブロックで情報を表示します。

プロパティ

[プロパティ] ページでは、デバイスの Green Ethernet モードを表示および設定できます。また、現在の電力節約量を表示できます。

Green Ethernet および EEE を有効にして電力節約量を表示するには、次のようにします。

ステップ 1 [ポート管理] > [Green Ethernet] > [プロパティ] をクリックします。

ステップ 2 次のフィールドに値を入力します。

- [エネルギー検出モード]: このモードを有効にする場合は、このチェックボックスをオンにします。この設定は一部の XG デバイスではサポートされていません。
- [ショートリーチ]: (非 XG デバイスの場合) この機能を有効にする場合はこのチェックボックスをオンにします。
- [ポート LED]: ポート LED を有効にするには、このフィールドを選択します。無効になっている場合、リンク ステータス、アクティビティ等は表示されません。
- [802.3 Energy Efficient Ethernet (EEE)]: EEE モードをグローバルに有効または無効にします。

ステップ 3 [累積節電量] 情報をリセットするには、[節電カウンタのリセット] をクリックします。

ステップ 4 [適用] をクリックします。Green Ethernet プロパティは、実行コンフィギュレーションファイルに書き込まれます。

ポート設定

[ポート設定] ページには、ポートごとの現在の Green Ethernet モードおよび EEE モードが表示され、[ポート設定の編集] ページで Green Ethernet を設定できるようにします。ポートで Green Ethernet のいずれかのモードを使用するには、[プロパティ] ページでそのモードをグローバルで有効にしておく必要があります。

EEE 設定は、GE ポートを搭載するデバイスでのみ表示されます。EEE は、ポートが自動ネゴシエーションに設定されている場合のみ動作します。例外として、ポートが 1 GB 以上の速度の場合は、自動ネゴシエーションが無効であっても、EEE が動作し続けます。

ショート リーチおよびエネルギー検出の機能は XG デバイスで常に有効であり、無効にすることはできません。FE または GE ポートを持つデバイスで、これらの機能は有効または無効にすることができます。

ポートごとの Green Ethernet 情報を設定するには、次のようにします。

ステップ 1 [ポート管理] > [Green Ethernet] > [ポート設定] をクリックします。

[ポート設定] ページには、次のフィールドが表示されます。

- [グローバルパラメータステータス]: 以下が表示されます。
  - [エネルギー検出モード]: このモードが有効であるかどうか。
  - [ショートリーチモード]: このモードが有効であるかどうか。
  - [802.3 Energy Efficient Ethernet (EEE)モード]: このモードが有効であるかどうか。

次のフィールドが各ポートに対して表示されます。

注 一部の SKU ではいくつかのフィールドが表示されない場合があります。

- [ポート]: ポート番号。
- [エネルギー検出]: このポートのエネルギー検出機能の状態。
  - [管理]: エネルギー検出が有効になっているかどうかが表示されます。

- [動作]:エネルギー検出がローカル ポート上で現在動作しているかどうかが表示されます。これは、有効であるかどうか(管理ステータス)、ローカル ポートで有効であるかどうか、およびローカル ポートで動作しているかどうかを示す機能です。
- [理由]:エネルギー検出が有効になっているのに動作していない理由が表示されます。

• [ショートリーチ]:このポートのショート リーチ機能の状態。

- [管理]:ショート リーチが有効になっているかどうかが表示されます。
- [動作]:ショート リーチがローカル ポート上で現在動作しているかどうかが表示されます。これは、有効であるかどうか(管理ステータス)、ローカル ポートで有効であるかどうか、およびローカル ポートで動作しているかどうかを示す機能です。
- [理由]:ショート リーチが有効になっているのに動作していない理由が表示されます。
- [ケーブル長]:ケーブルの長さ。

• [802.3 Energy Efficient Ethernet (EEE)]:EEE 機能に関するポートの状態です。

- [管理]:EEE が有効になっているかどうかが表示されます。
- [動作]:EEE がローカル ポートで現在動作しているかどうかが表示されます。これは、有効であるかどうか(管理ステータス)、ローカル ポートで有効であるかどうか、およびローカル ポートで動作しているかどうかを示す機能です。
- [LLDP 管理]:LLDP 経由の EEE カウンタのアドバタイズが有効になっているかどうかが表示されます。
- [LLDP 動作]:LLDP 経由の EEE カウンタのアドバタイズが現在動作しているかどうかが表示されます。
- [リモートでの EEE サポート]:EEE がリンク パラメータでサポートされているかどうかが表示されます。EEE は、ローカルとリモートの両方のリンク パラメータでサポートされている必要があります。

ステップ 2 [ポート] を選択して、[編集] をクリックします。

ステップ 3 (XG デバイス用のみ) このポートで [エネルギー検出] モードを有効にするか無効にするかを選択します。

ステップ 4 (XG デバイス用のみ)デバイスに GE ポートが搭載されている場合に、このポートで [ショートリーチ] モードを有効にするか無効にするかを選択します。

ステップ 5 このポートで [802.3 Energy Efficient Ethernet (EEE)] モードを有効にするか無効にするかを選択します。

ステップ 6 このポートで [802.3 Energy Efficient Ethernet（EEE）LLDP] モード（LLDP 経由の EEE 機能のアドバタイズメント）を有効にするか無効にするかを選択します。

ステップ 7 [適用] をクリックします。Green Ethernet ポート設定は、実行コンフィギュレーションファイルに書き込まれます。

11

Smartport

ここでは、Smartport 機能について説明します。

具体的な内容は、次のとおりです。

概要

Smartport 機能を使用すると、必要に応じて共通のコンフィギュレーションを保存して共有できるようになります。同じ Smartport マクロを複数のインターフェイスに適用することで、共通する一連のコンフィギュレーションをインターフェイス間で共有します。

Smartport マクロをインターフェイスに適用する場合には、マクロ名を指定するか、マクロに関連付けられているSmartport タイプを指定します。Smartport タイプ別に、Smartport マクロをインターフェイスに適用する方法として、次の 2 種類の方法があります。

- **Static Smartport**：ユーザが手動で Smartport タイプをインターフェイスに割り当てます。この操作により、対応する Smartport マクロがインターフェイスに適用されます。

- **Auto Smartport**：Auto Smartport では、インターフェイスにデバイスが接続された時点で、コンフィギュレーションが適用されます。インターフェイスからデバイスが検出されると、接続しているデバイスの Smartport タイプに対応する Smartport マクロ（割り当て済みの場合）が自動的に適用されます。

Smartport 機能はさまざまなコンポーネントで構成され、デバイスの他の機能と連携します。各コンポーネントと機能については、次の項で説明します。

- Smartport、Smartport タイプ、および Smartport マクロについては、この項で説明します。
- 音声 VLAN と Smartport については、「音声 VLAN」で説明します。
- Smartport の LLDP/CDP については、それぞれ「ディスカバリ - LLDP」セクションと「ディスカバリ - CDP」セクションで説明します。

さらに、一般的なワークフローについては、「Smartport の共通タスク」セクションで説明します。

Smartport とは

Smartport は、組み込み マクロを適用できるインターフェイスです。これらのマクロは、デバイスで通信要件をサポートするための設定作業を省力化するとともに、さまざまなタイプのネットワーク デバイスの機能を活用できるようにするための手段として設計されています。ネットワーク アクセスと QoS の要件は、IP 電話、プリンタ、ルータ、アクセス ポイント（AP）など、インターフェイスの接続先に応じて異なります。

Smartport タイプ

Smartport タイプは、Smartport に接続しているか、接続対象のデバイスのタイプを指します。このデバイスでは、次の Smartport タイプがサポートされています。

- プリンタ
- デスクトップ
- ゲスト
- サーバ
- ホスト
- IP カメラ
- IP 電話

- IP 電話 + デスクトップ
- スイッチ
- ルータ
- ワイヤレス アクセス ポイント

Smartport タイプには、インターフェイスに接続したデバイスのタイプを示す名前が設定されています。Smartport タイプごとに、2 種類の Smartport マクロが用意されています。1 つは、通常のマクロであり、対象のコンフィギュレーションを適用する機能があります。もう 1 つのマクロは、「アンチマクロ」と呼ばれるもので、インターフェイスが別の Smartport タイプに変化したときに、通常のマクロによって実行されたコンフィギュレーションをすべて取り消す機能があります。

次の表は、Smartport タイプと Auto Smartport の関係を示しています。

Smartport タイプ	Auto Smartport によるサポート	Auto Smartport によるサポート（デフォルト）
不明	いいえ	いいえ
デフォルト	いいえ	いいえ
プリンタ	いいえ	いいえ
デスクトップ	いいえ	いいえ
ゲスト	いいえ	いいえ
サーバ	いいえ	いいえ
ホスト	はい	いいえ
IP カメラ	いいえ	いいえ
IP 電話	はい	はい
IP 電話 + デスクトップ	はい	はい
スイッチ	はい	はい
ルータ	はい	いいえ
ワイヤレス アクセス ポイント	はい	はい

特殊な Smartport タイプ

特殊な Smartport タイプとして、[デフォルト] と [不明] の 2 つがあります。この 2 つのタイプはマクロとは関連付けられていませんが、Smartport に関するインターフェイスの状態を表すために用意されています。

この特殊な Smartport タイプについて、次に説明します。

- **デフォルト**

  Smartport タイプが（まだ）割り当てられていないインターフェイスには、Smartport ステータス [デフォルト] が設定されています。

  Auto Smartport によって Smartport タイプがインターフェイスに割り当てられて、インターフェイスが永続的に Auto Smartport として設定されていない場合は、次の条件に該当すると、Smartport タイプが [デフォルト] に再初期化されます。

  - リンクの停止/稼動を切り替える操作がインターフェイスで実行された。
  - デバイスが再起動された。
  - 指定した時間、デバイスからの CDP および LLDP アドバタイズメントが検出されず、インターフェイスに接続しているデバイスがすべて期限切れ状態になっている。

- **不明**

  Smartport マクロがインターフェイスに適用されて、エラーが発生した場合、インターフェイスにはステータス [不明] が割り当てられます。この場合、Smartport および Auto Smartport 機能は、エラーを修正して、Smartport ステータスをリセットするリセット操作（[インターフェイス設定] ページで実行）を適用するまで、インターフェイスに対して機能しません。

  トラブルシューティング時のヒントについては、「Smartport の共通タスク」のワークフロー部分を参照してください。

注 このセクション全体を通して、TTL 経由の LLDP および CDP メッセージの説明で「期限切れ」という用語を使用しています。最新の CDP パケットと LLDP パケットの両方の TTL が 0 に低下する前に、「Auto Smartport が有効」、「永続性ステータスが無効」、「インターフェイスで CDP メッセージと LLDP メッセージがもはや受信されていない」という条件をすべて満たした場合、アンチマクロが実行され、Smartport タイプはデフォルトに戻ります。

Smartport マクロ

Smartport マクロは、特定のネットワーク デバイスに応じてインターフェイスを設定する スクリプトです。

Smartport マクロとグローバル マクロを混同しないでください。グローバル マクロはデバイス全体を設定するのに対して、Smartport マクロの適用範囲は対象のインターフェイスに限定されます。

マクロのソースは、、[タイプ設定] ページの [マクロソースの表示] ボタンをクリックすることにより、検索することができます。

マクロと対応するアンチマクロは、ペアで各 Smartport タイプに割り当てられています。マクロはコンフィギュレーションを適用するのに対して、アンチマクロはそのコンフィギュレーションを削除します。

次のような名前で、2 つの Smartport マクロがペアになっています。

- macro_name（例：printer）
- no_macro_name（例：no_printer、Smartport マクロ printer のアンチ Smartport マクロ）

各デバイス タイプの組み込み Smartport マクロのリストについては、「組み込み Smartport マクロ」を参照してください。

インターフェイスへの Smartport タイプの適用

Smartport タイプがインターフェイスに適用されたときに、関連付けられている Smartport マクロの Smartport タイプとコンフィギュレーションは、実行コンフィギュレーション ファイルに保存されます。管理者が実行コンフィギュレーション ファイルをスタートアップ コンフィギュレーション ファイルに保存した場合、リブート後、デバイスでは次の要領で、Smartport タイプと Smartport マクロがインターフェイスに適用されます。

- スタートアップ コンフィギュレーション ファイルでインターフェイスの Smartport タイプを指定していない場合、Smartport タイプは [デフォルト] に設定されます。
- スタートアップ コンフィギュレーション ファイルでスタティック Smartport タイプを指定している場合、インターフェイスの Smartport タイプは該当するスタティック タイプに設定されます。

- スタートアップ コンフィギュレーション ファイルで、Auto Smartport によって動的に割り当てられた Smartport タイプを指定している場合
  - Auto Smartport のグローバルな動作状態、インターフェイスの Auto Smartport 状態、永続性ステータスがすべて [有効] の場合、Smartport タイプは該当するダイナミック タイプに設定されます。
  - これ以外の場合、対応するアンチマクロが適用されて、インターフェイスのステータスは [デフォルト] に設定されます。

マクロ エラーとリセット操作

インターフェイスの既存のコンフィギュレーションと Smartport マクロの間に競合がある場合、Smartport マクロでエラーが発生する可能性があります。

Smartport マクロのエラーが発生すると、次のパラメータを含む SYSLOG メッセージが送信されます。

- ポート番号
- Smartport タイプ
- マクロでエラーが発生した CLI コマンドの行番号

Smartport マクロのエラーがインターフェイスで発生した場合、インターフェイスのステータスは [不明] に設定されます。エラーの理由は、[インターフェイス設定] ページの [診断の表示] ポップアップに表示されます。

問題の原因を確認して、既存のコンフィギュレーションまたは Smartport マクロを修正したら、リセット操作を実行し、インターフェイスをリセットしてから、Smartport タイプを再適用（[インターフェイス設定] ページ）する必要があります。トラブルシューティング時のヒントについては、「Smartport の共通タスク」のワークフロー部分を参照してください。

Smartport 機能の動作

Smartport マクロをインターフェイスに適用する場合には、マクロに関連付けられている Smartport タイプを指定します。

CDP と LLDP 経由で検出できないデバイスに対応する Smartport タイプに対してサポートが提供されているので、これらの Smartport タイプは対象のインターフェイスに静的に割り当てる必要があります。具体的には、[インターフェイス設定] ページに移動し、対象のインターフェイスのラジオ ボタンを選択して、[編集] をクリックします。次に、割り当てる Smartport タイプを選択して、必要に応じてパラメータを調整してから、[適用] をクリックします。

Smartport タイプ別に、Smartport マクロをインターフェイスに適用する方法として、次の 2 種類の方法があります。

- **Static Smartport**

  手動で Smartport タイプをインターフェイスに割り当てます。対応する Smartport マクロがインターフェイスに適用されます。[インターフェイス設定] ページから Smartport タイプをインターフェイスに手動で割り当てることができます。

- **Auto Smartport**

  インターフェイスからデバイスが検出されると、接続しているデバイスの Smartport タイプに対応する Smartport マクロ（存在する場合）が自動的に適用されます。Auto Smartport は、デフォルトでグローバルに有効になっています。また、インターフェイス レベルでも有効になっています。

どちらの場合でも、Smartport タイプがインターフェイスから削除されるときには、関連付けられているアンチマクロが実行されます。同様に、アンチマクロの実行により、すべてのインターフェイス コンフィギュレーションが削除されます。

Auto Smartport

Auto Smartport で Smartport タイプをインターフェイスに自動的に割り当てるには、Auto Smartport を設定できるように、Auto Smartport 機能をグローバルに有効にすると同時に、関連するインターフェイスで有効にする必要があります。デフォルトでは、Auto Smartport は有効になっており、すべてのインターフェイスを設定できる状態です。各インターフェイスに割り当てられている Smartport タイプは、それぞれのインターフェイスで受信された CDP および LLDP パケットによって判別されます。

- 複数のデバイスがインターフェイスに接続されている場合、可能であれば、すべてのデバイスに適したコンフィギュレーション プロファイルがインターフェイスに適用されます。

- デバイスが期限切れ(他のデバイスからアドバタイズを受信していない状態)である場合、インターフェイス コンフィギュレーションはその永続性ステータスに従って変更されます。永続性ステータスが有効である場合、インターフェイス コンフィギュレーションは保持されます。有効でない場合、Smartportタイプは [デフォルト] に戻ります。

Auto Smartport の有効化

Auto Smartport は、次の方法により [プロパティ] ページでグローバルに有効にできます。

- [有効]: Auto Smartport を手動で有効にして、すぐに動作状態に移行します。
- [自動音声 VLAN で有効化]: 自動音声 VLAN が有効で動作している場合に、Auto Smartport を動作可能にします。[自動音声 VLAN ごとに有効にする] がデフォルト設定です。

注 Auto Smartport をグローバルに有効にすることに加えて、Auto Smartport を対象のインターフェイスでも有効にする必要があります。デフォルトでは、Auto Smartport はすべてのインターフェイスで有効になっています。

自動音声 VLAN を有効にする場合の詳細については、「音声 VLAN」を参照してください。

Smartport タイプの識別

Auto Smartport が [プロパティ] ページでグローバルに有効になっていると同時に、インターフェイス([インターフェイス設定] ページ)で有効になっている場合、デバイスでは、接続しているデバイスの Smartport タイプに基づいて、Smartport マクロがインターフェイスに適用されます。Auto Smartport では、接続しているデバイスからアドバタイズされる CDP および LLDP に基づいて、そのデバイスの Smartport タイプが導出されます。

たとえば、IP 電話をポートに接続した場合、その機能をアドバタイズする CDP または LLDP パケットが送信されます。この CDP および LLDP パケットの受信後、デバイスでは、電話に適した Smartport タイプが導出され、IP 電話が接続されるインターフェイスに、対応する Smartport マクロが適用されます。

永続的な Auto Smartport がインターフェイスで有効になっている場合を除き、接続しているデバイスの期限切れ、リンク ダウン、リブート、または接続されたデバイスが競合機能を受信した場合、その Smartport タイプと、Auto Smartport によって適用されるコンフィギュレーションは削除されます。指定した時間、デバイスから CDP および LLDP のアドバタイズメントが検出されなかった場 合、期限切れとして扱われます。

CDP/LLDP 情報による Smartport タイプの識別

デバイスでは、CDP/LLDP 機能に基づいて、ポートに接続しているデバイスのタイプが検出されます。

次の表はこのマッピングを示しています。

CDP 機能と Smartport タイプのマッピング

機能名	CDP ビット	Smartport タイプ
ルータ	0x01	ルータ
TB ブリッジ	0x02	ワイヤレス アクセス ポイント
SR ブリッジ	0x04	無視
スイッチ	0x08	スイッチ
ホスト	0x10	ホスト
IGMP 条件付きフィルタリング	0x20	無視
リピータ	0x40	無視
VoIP 電話	0x80	ip_phone
リモート管理デバイス	0x100	無視
CAST 電話ポート	0x200	無視
2 ポート MAC リレー	0x400	無視

LLDP 機能と Smartport タイプのマッピング

機能名	LLDP ビット	Smartport タイプ
その他	1	無視
リピータ IETF RFC 2108	2	無視
MAC ブリッジ IEEE 規格 802.1D	3	スイッチ
WLAN アクセス ポイント IEEE 規格 802.11 MIB	4	ワイヤレス アクセス ポイント
ルータ IETF RFC 1812	5	ルータ
電話 IETF RFC 4293	6	ip_phone

LLDP 機能と Smartport タイプのマッピング（続き）

機能名	LLDP ビット	Smartport タイプ
DOCSIS ケーブル デバイス IETF RFC 4639 および IETF RFC 4546	7	無視
ステーション専用 IETF RFC 4293	8	ホスト
C-VLAN コンポーネント。VLAN ブリッジ IEEE 規格 802.1Q	9	スイッチ
S-VLAN コンポーネント。VLAN ブリッジ IEEE 規格 802.1Q	10	スイッチ
2 ポート MAC リレー（TPMR）IEEE 規格 802.1Q	11	無視
予約済み	12-16	無視

注 IP 電話とホストのビットのみが設定されている場合、Smartport タイプは ip_phone_desktop になります。

複数のデバイスをポートに接続している場合

デバイスでは、接続しているデバイスから CDP および LLDP パケットでアドバタイズされている機能に基づいて、そのデバイスの Smartport タイプが導出されます。

複数のデバイスが単一のインターフェイスを介してデバイスに接続されている場合、Auto Smartport では、正しい Smartport タイプを割り当てるため、各機能のアドバタイズメントはそのインターフェイスから受信されたものとして扱われます。この割り当ては、次のアルゴリズムに基づいています。

- インターフェイス上のすべてのデバイスが同じ機能をアドバタイズしている場合（競合が存在しない状況）、一致する Smartport タイプがインターフェイスに適用されます。
- いずれかのデバイスがスイッチである場合、Smartport タイプとして [スイッチ] が使用されます。
- いずれかのデバイスが AP である場合、Smartport タイプとして [ワイヤレスアクセスポイント] が使用されます。
- いずれかのデバイスが IP 電話であり、別のデバイスがホストである場合、Smartport タイプとして ip_phone_desktop が使用されます。

- いずれかのデバイスが IP 電話 + デスクトップであり、別のデバイスが IP 電話またはホストである場合、Smartport タイプとして ip_phone_desktop が使用されます。
- 上記以外のケースでは、Smartport タイプとして [デフォルト] が使用されます。

LLDP/CDP の詳細については、それぞれ「ディスカバリ - LLDP」セクションと「ディスカバリ - CDP」セクションを参照してください。

永続的な Auto Smartport インターフェイス

インターフェイスの永続性ステータスが有効である場合、接続しているデバイスの期限切れ、インターフェイスの停止、およびデバイスのリブートが発生しても、そのインターフェイスの Smartport タイプと、Auto Smartport によって動的に適用済みのコンフィギュレーションは、インターフェイスでそのまま使用されます(コンフィギュレーションは保存されているという前提)。接続しているデバイスに別の Smartport タイプが Auto Smartport で検出される場合を除き、インターフェイスの Smartport タイプとコンフィギュレーションは変更されません。インターフェイスの永続性ステータスが無効である場合、そこに接続しているデバイスの期限切れ、インターフェイスの停止、またはデバイスのリブートが発生すると、インターフェイスの Smartport タイプはデフォルトに戻ります。インターフェイスの永続性ステータスを有効にすると、無効のときに発生していたデバイス検出の遅延は発生しなくなります。

注 インターフェイスに適用されている Smartport タイプの永続性は、インターフェイスに適用された Smartport タイプによる実行コンフィギュレーションがスタートアップコンフィギュレーション ファイルに保存されている場合にのみ、複数回リブートを実行した後でも有効です。

エラー処理

Smartport マクロをインターフェイスに適用する処理でエラーが発生した場合、問題点を [インターフェイス設定] ページで確認し、[インターフェイス設定] ページからエラーを修正した後で、ポートをリセットしてマクロを再適用できます。

デフォルト コンフィギュレーション

Smartport は常に使用可能な状態です。デフォルトでは、Auto Smartport は自動音声 VLAN によって有効になっています。CDP と LLDP の両方に基づいて、接続しているデバイスの Smartport タイプが検出され、Smartport タイプ（IP 電話、IP 電話 + デスクトップ、スイッチ、ワイヤレス アクセス ポイント）が判別されます。

音声の工場出荷時の初期状態の説明については、「音声 VLAN」を参照してください。

他の機能との関係

Auto Smartport はデフォルトで有効になっており、無効にすることができます。テレフォニー OUI は、Auto Smartport および自動音声 VLAN とは同時に使用できません。テレフォニー OUI を有効にする前に、Auto Smarport を無効にしてください。

Smartport の共通タスク

この項では、Smartport および Auto Smartport を設定する際の共通タスクについて説明します。

ワークフロー 1：Auto Smartport をデバイスでグローバルに有効にして、ポートに Auto Smartport を設定するには、次の手順を実行します。

ステップ 1 デバイスで Auto Smartport 機能を有効にするため、[プロパティ] ページを開きます。[管理 Auto Smartport] を [有効] または [自動音声 VLAN で有効化] に設定します。

ステップ 2 デバイスで処理する対象（接続しているデバイスからの CDP および LLDP アドバタイズメント）を選択します。

ステップ 3 [Auto Smartportデバイス検出] フィールドで、検出するデバイスのタイプを選択します。

ステップ 4 [適用] をクリックします。

ステップ 5 Auto Smartport 機能を 1 つまたは複数のインターフェイスで有効にするため、[インターフェイス設定] ページを開きます。

ステップ 6 インターフェイスを選択し、[編集] をクリックします。

ステップ 7 [Smartport 適用] フィールドで [Auto Smartport] を選択します。

ステップ 8 必要に応じて、[永続性ステータス] チェックボックスをオンまたはオフにします。

ステップ 9 [適用] をクリックします。

ワークフロー 2: インターフェイスを Static Smartport として設定するには、次の手順を実行します。

ステップ 1 インターフェイス上の Smartport 機能を有効にするため、[インターフェイス設定] ページを開きます。

ステップ 2 インターフェイスを選択し、[編集] をクリックします。

ステップ 3 [Smartport 適用] フィールドで、インターフェイスに適用する Smartport タイプを選択します。

ステップ 4 必要に応じて、マクロ パラメータを設定します。

ステップ 5 [適用] をクリックします。

ワークフロー 3: Smartport マクロのパラメータのデフォルト値を調整するには、次の手順を実行します。

この手順により、次の操作を実行できます。

- マクロ ソースを表示する。
- パラメータのデフォルト値を変更する。
- パラメータのデフォルト値を工場出荷時設定に復元する。

ステップ 1 [タイプ設定] ページを開きます。

ステップ 2 [Smartport タイプ] を選択します。

ステップ 3 選択した Smartport タイプに関連付けられている現在の Smartport マクロを表示するため、[マクロ ソースの表示] をクリックします。

ステップ 4 [編集] をクリックし、新しいウィンドウを開きます。このウィンドウで、その Smartport タイプにバインドされているマクロのパラメータのデフォルト値を変更することができます。各パラメータのデフォルト値は、選択した Smartport タイプ（該当する場合）が Auto Smartport でインターフェイスに適用される場合に使用されます。

ステップ 5 [編集] ページで、フィールドの値を変更します。

ステップ 6 パラメータを変更した場合は、[適用] をクリックしてマクロを返します。

ワークフロー 4:エラーが発生した Smartport マクロを再実行するには、次の手順を実行します。

ステップ 1 [インターフェイス設定] ページで、Smartport タイプが [不明] であるインターフェイスを選択します。

ステップ 2 [診断の表示] をクリックし、問題を確認します。

ステップ 3 トラブルシューティングを実行して、問題を解決します。以下のトラブルシューティングのヒントを検討してください。

ステップ 4 [編集] をクリックします。開いた新しいウィンドウで、[リセット] をクリックし、インターフェイスをリセットします。

ステップ 5 Smartport マクロをインターフェイス上で実行するには、メインページに戻り、[再適用](スイッチ、ルータ、AP 以外のデバイスの場合)または、[Smartportマクロの再適用](スイッチ、ルータ、または AP の場合)を使用してマクロを再適用します。

次の方法でも、単一または複数の [不明] インターフェイスをリセットできます。

ステップ 1 [インターフェイス設定] ページで、[ポートタイプが次に等しい] チェックボックスをオンにします。

ステップ 2 [不明] を選択し、[実行] をクリックします。

ステップ 3 [すべての不明な Smartport のリセット] をクリックします。次に、上で説明したようにマクロを再適用します。

ヒント マクロが失敗する原因は、マクロを適用する前のインターフェイスのコンフィギュレーションとの衝突(ほとんどの場合、セキュリティおよびストーム制御の設定で発生)である場合があります。また、ユーザ定義マクロ内の不適切なポート タイプ、入力ミス、または不適切なコマンド、あるいは、無効なパラメータ設定などが原因である場合もあります。マクロの適用前にパラメータのタイプや範囲はチェックされないので、パラメータに不正な値や無効な値が含まれていると、マクロの適用時に、ほぼ確実にエラーが発生します。

Web ベースのインターフェイスを使用した Smartport の設定

Smartport 機能は、[Smartport] > [プロパティ] の [Smartportタイプ設定] および [インターフェイス設定] ページで設定します。

音声 VLAN の設定については、「音声 VLAN」を参照してください。

LLDP/CDP の設定については、それぞれ「ディスカバリ - LLDP」セクションと「ディスカバリ - CDP」セクションで説明します。

プロパティ

Smartport 機能をグローバルに設定するには、次のようにします。

ステップ 1 [Smartport] > [プロパティ] の順にクリックします。

ステップ 2 パラメータを入力します。

- [管理 Auto Smartport]: Auto Smartport をグローバルに有効にするか無効にするかを選択します。次のオプションが選択できます。
  - [無効]: デバイスで Auto Smartport を無効にする場合に選択します。
  - [有効]: デバイスで Auto Smartport を有効にする場合に選択します。
  - [自動音声 VLAN で有効化]: Auto Smartport を有効にしますが、自動音声 VLAN も有効で動作している場合にのみ、Auto Smartport を動作状態に移行します。[自動音声 VLAN ごとに有効にする] がデフォルト設定です。
- [動作Auto Smartport]: Auto Smartport ステータスが表示されます。
- [Auto Smartportデバイス検出方式]: 接続しているデバイスの Smartport タイプを検出する際に使用する着信パケットのタイプ (CDP か LLDP、またはこの両方) を選択します。Auto Smartport でデバイスの識別を可能にするため、少なくとも 1 つのタイプを選択する必要があります。
- [動作CDP ステータス]: CDP の動作ステータスが表示されます。Auto Smartport で CDP アドバタイズメントに基づいて Smartport タイプを検出する場合、CDP を有効にします。
- [動作LLDP ステータス]: LLDP の動作ステータスが表示されます。Auto Smartport で LLDP/LLDP-MED アドバタイズメントに基づいて Smartport タイプを検出する場合、LLDP を有効にします。

- [Auto Smartportデバイス検出]:Auto Smartport で Smartport タイプをインターフェイスに割り当て可能にするデバイスのタイプを選択します。未選択の場合、Auto Smartport では、その Smartport タイプをどのインターフェイスにも割り当てません。

ステップ 3 [適用] をクリックします。この操作により、デバイスでグローバル Smartport パラメータが設定されます。

タイプ設定

[Smartport タイプ設定] ページでは、Smartport タイプ設定の編集や、マクロ ソースの表示を実行できます。

デフォルトでは、各 Smartport タイプは組み込み Smartport マクロのペアと関連付けられています。マクロとアンチマクロの詳細については、「Smartport タイプ」を参照してください。組み込みマクロおよびユーザ定義マクロには、パラメータを設定できます。組み込みマクロには、最大 3 つのパラメータを設定できます。

Auto Smartport によって適用された Smartport タイプの各パラメータを [Smartportタイプ設定] ページで編集することで、各パラメータのデフォルト値を設定します。このデフォルト値は、Auto Smartport によって使用されます。

注 Auto Smartport タイプを変更すると、Auto Smartport によってそのタイプが割り当てられているインターフェイスに、新しい設定が適用されます。この場合、無効なマクロをバインドしたり、無効なデフォルト パラメータ値を設定したりすると、この Smartport タイプのすべてのポートについて、ステータスが [不明] になります。

ステップ 1 [Smartport] > [Smartport タイプ設定] の順にクリックします。

ステップ 2 Smartport タイプに関連付けられている Smartport マクロを表示するため、Smartport タイプを選択して、[マクロ ソースの表示] をクリックします。

ステップ 3 マクロのパラメータを変更するには、Smartport タイプを選択して、[編集] をクリックします。

ステップ 4 次のフィールドを入力します。

- [ポートタイプ]:Smartport タイプを選択します。
- [マクロ名]:現在 Smartport タイプに関連付けられている Smartport マクロ名が表示されます。

- [マクロ パラメータ]:マクロ内の 3 つのパラメータに対して、次のフィールドを表示します。
  - [パラメータ名]:マクロ内のパラメータ名です。
  - [パラメータ値]:マクロ内の現在のパラメータ値です。この値はここで変更することができます。
  - [パラメータの説明]:パラメータの説明です。

ステップ 5 [適用] をクリックし、実行コンフィギュレーションに変更を保存します。Smartport タイプに関連付けられている Smartport マクロおよびそのパラメータ値が変更された場合、Auto Smartport では、Auto Smartport によって現在 Smartport タイプで割り当てられているインターフェイスに、マクロが自動的に適用されます。Auto Smartport では、Smartport タイプが静的に割り当てられたインターフェイスに、変更内容は適用されません。

注 タイプとの関連付けが設定されていないので、マクロ パラメータを検証する方法はありません。したがって、この時点では、エントリはすべて有効になります。ただし、Smartport タイプがインターフェイスに割り当てられて、関連付けられているマクロが適用されたときに、パラメータ値が無効な場合、エラーの原因になる可能性があります。

インターフェイス設定

次のタスクを実行するには、[インターフェイス設定] ページを使用します。

- マクロ パラメータのインターフェイス固有の値で、特定の Smartport タイプをインターフェイスに静的に適用する。
- インターフェイスで Auto Smartport を有効にする。
- 適用時にエラーが発生し、Smartport タイプを [不明] に変化させた Smartport マクロを診断する。
- Smartport マクロが失敗した後、すべてのインターフェイスまたは次のタイプのインターフェイスに再適用する。スイッチ、ルータ、および AP。[適用] をクリックする前に、必要な修正を実施しておく必要があります。トラブルシューティング時のヒントについては、「Smartport の共通タスク」のワークフロー部分を参照してください。

- Smartport マクロをインターフェイスに再適用する。環境によっては、Smartport マクロを再適用して、インターフェイスのコンフィギュレーションを最新の状態にできると便利です。たとえば、スイッチの Smartport マクロをデバイスのインターフェイスで再適用すると、そのインターフェイスは、最後のマクロ適用後に作成された VLAN のメンバーになります。再適用によってインターフェイスに影響が現れるかどうか判別するには、デバイスの現在の構成とマクロの定義内容を十分に把握している必要があります。
- [不明] インターフェイスをリセットする。これにより [不明] のインターフェイスのモードをデフォルトに設定します。

Smartport マクロを適用するには、次のようにします。

ステップ 1 [Smartport] > [インターフェイス設定] の順にクリックします。

インターフェイスのグループに関連付けられた最後の Smartport マクロを再適用するには、次のオプションのいずれかをクリックします。

- [すべてのスイッチ、ルータ、およびワイヤレスアクセスポート]:すべてのインターフェイスにマクロを再適用します。
- [すべてのスイッチ]:スイッチとして定義されたすべてのインターフェイスにマクロを再適用します。
- [すべてのルータ]:ルータとして定義されたすべてのインターフェイスにマクロを再適用します。
- [すべてのワイヤレスアクセスポート]:アクセス ポイントとして定義されたすべてのインターフェイスにマクロを再適用します。

  特定のインターフェイスに関連付けられた Smartport マクロを再適用するには、そのインターフェイス(アップしている必要がある)を選択して [再適用] をクリックし、そのインターフェイスに適用されていた最後のマクロを再適用します。

  [再適用] アクションにより、新しく作成したすべての VLAN にインターフェイスも追加されます。

ステップ 2 Smartport 診断

Smartport マクロのエラーが発生した場合、インターフェイスの Smartport タイプは [不明] になります。タイプが [不明] のインターフェイスを選択して、[診断の表示] をクリックします。この操作により、マクロ適用時のエラーの原因になったコマンドが表示されます。トラブルシューティング時のヒントについては、「Smartport の共通タスク」のワークフロー部分を参照してください。問題を訂正した後、マクロの再適用に進みます。

ステップ 3 すべての [不明] のインターフェイスをデフォルト タイプにリセットします。

- [Smartportタイプが次に等しい] チェックボックスを選択します。
- [不明] を選択します。
- [実行] をクリックします。
- [すべての不明な Smartport のリセット] をクリックします。次に、上で説明したようにマクロを再適用します。これにより、タイプが [不明] のすべてのインターフェイスがリセットされます。つまり、すべてのインターフェイスがデフォルト タイプに戻ります。マクロか現在のインターフェイス コンフィギュレーション、またはこの両方のエラーの修正が終わったら、新しいマクロを適用できます。

注 タイプが [不明] のインターフェイスをリセットしても、エラーが発生したマクロによって実行されたコンフィギュレーションはリセットされません。この場合、手動で消去する必要があります。

Smartport タイプをインターフェイスに割り当てるか、インターフェイスで Auto Smartport をアクティブ化するには、次のようにします。

ステップ 1 インターフェイスを選択し、[編集] をクリックします。

ステップ 2 次のフィールドを入力します。

- [インターフェイス]:ポートまたは LAG を選択します。
- [Smartportタイプ]:ポート/LAG に現在割り当てられている Smartport タイプが表示されます。
- [Smartport 適用]:[Smartport 適用] プルダウンから Smartport タイプを選択します。
- [Smartport 適用方式]:Auto Smartport を選択した場合、Auto Smartport で、接続しているデバイスから受信された CDP および LLDP アドバタイズメントに基づいて、Smartport タイプが自動的に割り当てられると同時に、対応する Smartport マクロが適用されます。Smartport タイプを静的に割り当てて、対応する Smartport マクロをインターフェイスに適用するには、対象の Smartport タイプを選択します。
- [永続性ステータス]:永続性ステータスを有効にする場合、これを選択します。有効にした場合、インターフェイスの停止やデバイスのリブートが発生しても、インターフェイスへの Smartport タイプの関連付けはそのまま使用されます。永続性が適用されるのは、インターフェイスの [Smartport適用] が Auto Smartport である場合に限定されます。インターフェイスで永続性を有効にすると、無効のときに発生していたデバイス検出の遅延は発生しなくなります。

- [マクロ パラメータ]:マクロ内の最大 3 つのパラメータに対して、次のフィールドが表示されます。
  - [パラメータ名]:マクロ内のパラメータ名です。
  - [パラメータ値]:マクロ内の現在のパラメータ値です。この値はここで変更することができます。
  - [パラメータの説明]:パラメータの説明です。

ステップ 3 インターフェイスのステータスが(マクロの適用が成功しなかった結果として)[不明]の場合、そのインターフェイスをデフォルトに設定するには、[リセット] をクリックします。マクロはメインページで再適用することができます。

ステップ 4 変更内容を更新して Smartport タイプをインターフェイスに割り当てるには、[適用]をクリックします。

組み込み Smartport マクロ

各 Smartport タイプの組み込みマクロのペアについて、次に説明します。Smartport タイプごとに、インターフェイスを設定するマクロと、コンフィギュレーションを削除するアンチ マクロが用意されています。

次の Smartport タイプのマクロ コードが提供されています。

- desktop
- printer
- guest
- server
- host
- ip_camera
- ip_phone
- ip_phone_desktop
- switch
- router
- ap

desktop

```
[desktop]
#interface configuration, for increased network security and reliability when
connecting a desktop device, such as a PC, to a switch port.
#macro description Desktop
#macro keywords $native_vlan $max_hosts
#
#macro key description:   $native_vlan: The untag VLAN which will be
configured on the port
#                        $max_hosts: The maximum number of allowed devices on
the port
#Default Values are
#$native_vlan = Default VLAN
#$max_hosts = 10
#
#the port type cannot be detected automatically
#
#the default mode is trunk
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_desktop

```
[no_desktop]
#macro description No Desktop
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

printer

```
[printer]
#macro description printer
#macro keywords $native_vlan
#
#macro key description: $native_vlan: The untag VLAN which will be configured
on the port
#Default Values are
#$native_vlan = Default VLAN
#
#the port type cannot be detected automatically
#
switchport mode access
switchport access vlan $native_vlan
#
#single host
port security max 1
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_printer

```
[no_printer]
#macro description No printer
#
no switchport access vlan
no switchport mode
#
no port security
no port security mode
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

guest

```
[guest]
#macro description guest
#macro keywords $native_vlan
#
#macro key description:  $native_vlan: The untag VLAN which will be
configured on the port
#Default Values are
#$native_vlan = Default VLAN
#
#the port type cannot be detected automatically
#
switchport mode access
switchport access vlan $native_vlan
#
#single host
port security max 1
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_guest]]

```
[no_guest]
#macro description No guest
#
no switchport access vlan
no switchport mode
#
no port security
no port security mode
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

server

```
[server]
#macro description server
#macro keywords $native_vlan $max_hosts
#
#macro key description:   $native_vlan: The untag VLAN which will be
configured on the port
#                         $max_hosts: The maximum number of allowed devices on
the port
#Default Values are
#$native_vlan = Default VLAN
#$max_hosts = 10
#
#the port type cannot be detected automatically
#
#the default mode is trunk
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_server

```
[no_server]
#macro description No server
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
#
spanning-tree portfast auto
#
@
```

host

```
[host]
#macro description host
#macro keywords $native_vlan $max_hosts
#
#macro key description:   $native_vlan: The untag VLAN which will be
configured on the port
#                         $max_hosts: The maximum number of allowed devices on
the port
#Default Values are
#$native_vlan = Default VLAN
#$max_hosts = 10
#
#the port type cannot be detected automatically
#
#the default mode is trunk
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_host

```
[no_host]
#macro description No host
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

ip_camera

```
[ip_camera]
#macro description ip_camera
#macro keywords $native_vlan
#
#macro key description:  $native_vlan: The untag VLAN which will be
configured on the port
#Default Values are
#$native_vlan = Default VLAN
#
switchport mode access
switchport access vlan $native_vlan
#
#single host
port security max 1
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_ip_camera

```
[no_ip_camera]
#macro description No ip_camera
#
no switchport access vlan
no switchport mode
#
no port security
no port security mode
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

ip_phone

```
[ip_phone]
#macro description ip_phone
#macro keywords $native_vlan $voice_vlan $max_hosts
#
#macro key description:   $native_vlan: The untag VLAN which will be
configured on the port
#                          $voice_vlan: The voice VLAN ID
#                        $max_hosts: The maximum number of allowed devices on
the port
#Default Values are
#$native_vlan = Default VLAN
#$voice_vlan = 1
#$max_hosts = 10
#
#the default mode is trunk
smartport switchport trunk allowed vlan add $voice_vlan
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_ip_phone

```
[no_ip_phone]
#macro description no ip_phone
#macro keywords $voice_vlan
#
#macro key description:   $voice_vlan: The voice VLAN ID
#
#Default Values are
#$voice_vlan = 1
#
smartport switchport trunk allowed vlan remove $voice_vlan
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
```

```
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

ip_phone_desktop

```
[ip_phone_desktop]
#macro description ip_phone_desktop
#macro keywords $native_vlan $voice_vlan $max_hosts
#
#macro key description:   $native_vlan: The untag VLAN which will be
configured on the port
#                          $voice_vlan: The voice VLAN ID
#                        $max_hosts: The maximum number of allowed devices on
the port
#Default Values are
#$native_vlan = Default VLAN
#$voice_vlan = 1
#$max_hosts = 10
#
#the default mode is trunk
smartport switchport trunk allowed vlan add $voice_vlan
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_ip_phone_desktop

```
[no_ip_phone_desktop]
#macro description no ip_phone_desktop
#macro keywords $voice_vlan
#
#macro key description:   $voice_vlan: The voice VLAN ID
#
#Default Values are
#$voice_vlan = 1
#
smartport switchport trunk allowed vlan remove $voice_vlan
no smartport switchport trunk native vlan
```

```
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

switch

```
[switch]
#macro description switch
#macro keywords $native_vlan $voice_vlan
#
#macro key description:  $native_vlan: The untag VLAN which will be
configured on the port
#                        $voice_vlan: The voice VLAN ID
#Default Values are
#$native_vlan = Default VLAN
#$voice_vlan = 1
#
#the default mode is trunk
smartport switchport trunk allowed vlan add all
smartport switchport trunk native vlan $native_vlan
#
spanning-tree link-type point-to-point
#
@
```

no_switch

```
[no_switch]
#macro description No switch
#macro keywords $voice_vlan
#
#macro key description:   $voice_vlan: The voice VLAN ID
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no spanning-tree link-type
#
@
```

router

```
[router]
#macro description router
#macro keywords $native_vlan $voice_vlan
#
#macro key description:  $native_vlan: The untag VLAN which will be
configured on the port
#                        $voice_vlan: The voice VLAN ID
#
#Default Values are
#$native_vlan = Default VLAN
#$voice_vlan = 1
#
#the default mode is trunk
smartport switchport trunk allowed vlan add all
smartport switchport trunk native vlan $native_vlan
#
smartport storm-control broadcast level 10
smartport storm-control broadcast enable
#
spanning-tree link-type point-to-point
#
@
```

no_router

```
[no_router]
#macro description No router
#macro keywords $voice_vlan
#
#macro key description:   $voice_vlan: The voice VLAN ID
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
#
no spanning-tree link-type
#
@
```

ap

```
[ap]
#macro description ap
#macro keywords $native_vlan $voice_vlan
#
#macro key description:  $native_vlan: The untag VLAN which will be
configured on the port
```

12

VLAN 管理

ここで説明する内容は次のとおりです。

- 標準 VLAN
- GVRP 設定
- 音声 VLAN

VLAN は、接続しているブリッジ型ネットワークの物理 LAN セグメントには関係なく、VLAN に関連付けられたデバイスがイーサネット MAC レイヤ上で互いに通信できる、ポートの論理グループです。

VLAN について

各 VLAN には、1 から 4094 の値で一意の VLAN ID（VID）が設定されます。ブリッジ型ネットワーク内のデバイスのポートが、VLAN にデータを送信したり VLAN からデータを受信できる場合、VLAN のメンバーになります。あるポートから VLAN に向かうすべてのパケットに VLAN タグが付いていない場合、そのポートは VLAN のタグなしメンバーになります。あるポートから VLAN に向かうすべてのパケットに VLAN タグが付いている場合、そのポートは VLAN のタグ付きメンバーになります。タグなし VLAN については、1 つのポートは 1 つのタグなし VLAN にしかメンバーとして所属できませんが、タグ付き VLAN については、複数のタグ付き VLAN のメンバーになることができます。

VLAN アクセス モードのポートは 1 つの VLAN のみのメンバーになれます。一般モードまたはトランク モードのポートは、1 つ以上の VLAN のメンバーになれます。

VLAN はセキュリティとスケーラビリティの問題を解決します。VLAN からのトラフィックは VLAN 内で通信され、VLAN 内のデバイスが終端になります。また、これらのデバイスの位置を物理的に変更することなく、デバイスを論理的に接続することにより、ネットワーク構成が簡単になります。

フレームが VLAN タグ付きである場合、4 バイトの VLAN タグが各イーサネット フレームに追加されます。タグには、1 から 4094 までの VLAN ID と、0 から 7 までの VLAN Priority Tag（VPT）が含まれます。VPT の詳細については、「サービス品質」を参照してください。

フレームが VLAN 対応デバイスに到着すると、フレーム内の 4 バイトの VLAN タグに応じて、VLAN に分類されます。

フレームに VLAN タグが含まれていない場合またはフレームが優先タグのみの場合、そのフレームは、受信した入力ポートに設定されている PVID（ポート VLAN 識別子）に基づいて VLAN に分類されます。

入力フィルタリングが有効になっており、入力ポートが、パケットが所属する VLAN のメンバーでない場合、そのフレームは入力ポートで破棄されます。VLAN タグ内の VID が 0 の場合のみ、そのフレームは優先タグ付きと見なされます。

VLAN に所属するフレームはその VLAN 内で通信されます。これは、ターゲット VLAN のメンバーの出力ポートだけにフレームを送信または転送することにより可能になります。出力ポートは、VLAN のタグ付きメンバーにでもタグなしのメンバーにでもなれます。

出力ポートで次のことが行われます。

- 出力ポートがターゲット VLAN のタグ付きメンバーであり、元のフレームに VLAN タグが付いていない場合、フレームに VALN タグを追加します。
- 出力ポートがターゲット VLAN のタグなしメンバーであり、元のフレームに VLAN タグが付いている場合、フレームから VALN タグを削除します。

VLAN の役割

デバイス VLAN は静的にしか作成できません。

VLAN によっては、別の役割を持つものもあります。

- 音声 VLAN：詳細については、「音声 VLAN」を参照してください。
- ゲスト VLAN：[プロパティ] ページで設定します。
- デフォルト VLAN：VLAN1.
- 管理 VLAN詳細については、「IP 情報の設定」を参照してください。

QinQ

Q-in-Q を使用すると、サービス プロバイダー ネットワークとカスタマー ネットワークとを分離できます。デバイスは、ポートベースの C タグ付きサービス インターフェイスをサポートするプロバイダー ブリッジです。

QinQ では、デバイスがサービス タグ（S タグ）と呼ばれる ID タグを追加して、プロバイダー ネットワークにパケットを転送します。S タグは、カスタマー VLAN タグを維持しながら、さまざまなカスタマーの間のトラフィックを分離するために使用されます。

カスタマー トラフィックは、元々 C タグ付きだったかタグなしであったかには関係なく、TPID 0x8100 の S タグを使用してカプセル化されます。S タグがあることで、ブリッジングが S タグ VID（S-VID）のみに基づくプロバイダー ブリッジ ネットワーク内の集約としてこのトラフィックを扱うことができます。

S タグは、トラフィックがネットワーク サービス プロバイダーのインフラストラクチャを経由して転送される間は維持され、その後、出力デバイスによって削除されます。

Q-in-Q には、カスタマーのエッジ デバイスを設定する必要がないという別の利点もあります。

QinQ は [インターフェイス設定] ページで有効にします。

標準 VLAN

ここでは、さまざまなタイプの VLAN を設定する際に使用する GUI ページについて説明します。ここでは、以下について説明します。

- 標準 VLAN の概要
- VLAN 設定
- インターフェイス設定
- VLAN へのポート
- ポート VLAN メンバーシップ

標準 VLAN の概要

VLAN を設定する手順

VLAN を設定するには、次のようにします。

ステップ 1 VLAN 設定の説明に従って、必要な VLAN を作成します。

ステップ 2 「インターフェイス設定」の説明に従って、ポートの VLAN 関連コンフィギュレーションを設定し、インターフェイスで QinQ を有効にします。

ステップ 3 「VLAN へのポート」または「ポート VLAN メンバーシップ」の説明に従って、VLAN にインターフェイスを割り当てます。

ステップ 4 「ポート VLAN メンバーシップ」の説明に従って、すべてのインターフェイスの現在の VLAN ポート メンバーシップを確認します。

デフォルト VLAN 設定

デバイスは自動的に VLAN 1 をデフォルト VLAN として作成し、すべてのポートのデフォルト インターフェイス ステータスが「アクセス」になり、すべてのポートがデフォルト VLAN のタグなしメンバーとして設定されます。

デフォルト VLAN には次の特徴があります。

- デフォルト VLAN は、独立した、スタティックでもダイナミックでもない VLAN で、すべてのポートがタグなしメンバーになります。
- 削除はできません。
- ラベルは指定できません。
- 自動的に、OUI 対応音声 VLAN 用の音声 VLAN として使用されます。
- ポートがどの VLAN のメンバーでもなくなると、デバイスは自動的にそのポートをデフォルト VLAN のタグなしメンバーに設定します。VLAN が削除されたり、ポートが VLAN から削除されると、ポートはその VLAN のメンバーでなくなります。

VLAN 設定

VLAN は作成できますが、その VLAN が手動または動的に少なくとも 1 つのポートに接続されるまで有効にはなりません。ポートは必ず 1 つ以上の VLAN に所属している必要があります。

250 シリーズのデバイスでは、デフォルト VLAN を含めて、最大 256 の VLAN をサポートします。

各 VLAN には、1 から 4094 の値で一意の VID を設定する必要があります。VID 4095 はデバイスで廃棄 VLAN として予約されています。廃棄 VLAN に分類されるパケットはすべて入力時に廃棄され、ポートに転送されません。

VLAN を作成するには、次のようにします。

ステップ 1 [VLAN 管理] > [VLAN 設定] の順にクリックします。

定義済みのすべての VLAN の情報が表示されます。これらのフィールドは、[追加] ページで定義されるものです。次のフィールドは、[追加] ページに表示されません。

- [発信元]: この VLAN の作成方法。
  - [スタティック]: ユーザ定義の VLAN。
  - [デフォルト]: デフォルト VLAN。

ステップ 2 新しい VLAN を追加するには、[追加] をクリックします。

このページから、1 つの VLAN または複数の VLAN を作成できます。

ステップ 3 VLAN を 1 つだけ作成する場合は、[VLAN] ラジオ ボタンを選択し、[VLAN ID] と、任意で、[VLAN 名] を入力します。

複数の VLAN を作成する場合は、[範囲] ラジオ ボタンを選択し、[開始VID] と [終了 VID] を入力して、作成する VLAN の範囲を指定します。[範囲] 機能を使用する場合、1 回に作成できる VLAN の最大数は 100 個です。

注 一部の VLAN は、システムが内部的に使用するために必要であり、ユーザが作成または設定することはできません。システムは内部で以下の VLAN を使用する必要があります。

- イーサネット ポートまたはポート チャネル(LAG)上で直接定義された IP インターフェイスごとに 1 つの VLAN。
- IPv6 トンネルごとに 1 つの VLAN。
- 802.1x 用の 1 つの VLAN。

IPv6 トンネル用と 802.1x 用の VLAN は事前に割り当てられるのに対して、イーサネット ポート/ポート チャネルの IP 設定用の VLAN は IP 設定が適用されたときに割り当てられます。内部 VLAN は、最大の空き VLAN(デフォルトは VLAN 4094)から順に割り当てられます。

ステップ 4 新しい VLAN に次のフィールドを追加します。

- [VLANインターフェイス状態]: VLAN をシャットダウンするかどうかを選択します。シャットダウンされた状態の VLAN は、上位レベルとの間でメッセージの送受信を行いません。たとえば、IP インターフェイスが設定されている VLAN をシャットダウンすると、VLAN へのブリッジングは継続されますが、スイッチは VLAN 上で IP トラフィックを送受信できなくなります。

- [リンクステータスSNMPトラップ]:SNMP トラップのリンクステータス生成を有効にするかどうかを選択します。

ステップ 5 VLAN を作成するには、[適用] をクリックします。

インターフェイス設定

[インターフェイス設定] ページでは、すべてのインターフェイスの VLAN 関連パラメータのコンフィギュレーションが表示され、それらの設定を行うことができます。

VLAN 設定を行うには、次のようにします。

ステップ 1 [VLAN 管理] > [インターフェイス設定] の順にクリックします。

ステップ 2 インターフェイス タイプ(ポートまたは LAG)を選択し、[実行] をクリックします。ポートまたは LAG とその VLAN パラメータが表示されます。

ステップ 3 ポートまたは LAG を設定するには、ポートまたは LAG を選択して、[編集] をクリックします。

ステップ 4 次のフィールドに値を入力します。

- [インターフェイス]:ポートか LAG を選択します。
- [スイッチポート モード]:レイヤ 2 とレイヤ 3 のどちらかを選択します。
- [インターフェイスVLANモード]:VLAN のインターフェイス モードを選択します。次のオプションがあります。
  - [全般]:インターフェイスは、IEEE 802.1q 規格で定義されているすべての機能をサポートします。インターフェイスは、1 つ以上の VLAN のタグ付きまたはタグなしメンバーになれます。
  - [アクセス]:インターフェイスは、1 つの VLAN のタグなしメンバーになります。このモードのポートはアクセス ポートと呼ばれます。
  - [トランク]:インターフェイスは、最大 1 つの VLAN のタグなしメンバーと、0 個以上の VLAN のタグ付きメンバーになります。このモードのポートはトランク ポートと呼ばれます。
  - [カスタマー]:このオプションを選択すると、インターフェイスが QinQ モードになります。それにより、ユーザがプロバイダー ネットワーク上で独自の VLAN 配置(PVID)を使用できるようになります。デバイスに 1 つ以上のカスタマー ポートがある場合、デバイスは QinQ モードになります。「QinQ」を参照してください。

- [フレーム タイプ]: (一般モードでのみ使用可能) インターフェイスで受信可能なフレームのタイプを選択します。設定したフレーム タイプでないフレームは入力時に破棄されます。選択項目は次のとおりです。
  - [すべて通過]: インターフェイスはすべてのフレーム タイプ (タグなしフレーム、タグ付きフレーム、プライオリティ タグ付きフレーム) を受け入れます。
  - [タグ付きのみ通過]: インターフェイスはタグ付きフレームのみを受け入れます。
  - [タグなしのみ通過]: インターフェイスはタグなしフレームとプライオリティ フレームのみ受け入れます。
- [入力フィルタリング]: (一般モードのみ) 入力フィルタリングを有効にするには、これを選択します。入力フィルタリングが有効になると、インターフェイスは、そのインターフェイスがメンバーになっていない VLAN に分類されるすべての着信フレームを破棄します。入力フィルタリングは、一般ポートで有効または無効にできます。アクセス ポートとトランク ポートでは常に有効になります。

ステップ 5 [適用] をクリックします。パラメータが、実行コンフィギュレーション ファイルに書き込まれます。

VLAN へのポート

[VLAN へのポート] ページと [ポート VLAN メンバーシップ] ページには、ポートの VLAN メンバーシップがさまざまな表現で表示されます。VLAN にメンバーシップを追加したり、VLAN からメンバーシップを削除するには、これらのページを使用します。

ポートが、禁止されているデフォルト VLAN メンバーシップを持っている場合、そのポートにその他の VLAN のメンバーシップを設定することはできません。そのポートには内部 VID の 4095 が割り当てられます。

パケットを適切に転送するには、エンド ノード間のパスで VLAN トラフィックを運ぶ VLAN 対応の中間デバイスを手動で設定する必要があります。

2 つの VLAN 対応デバイス間のタグなしポート メンバーシップは、仲介する VLAN 対応デバイスがない場合、同じ VLAN になっている必要があります。つまり、2 つのデバイス間にあるポートの PVID は、そのポートと VLAN 間でタグなしパケットの送受信を行う場合、同じである必要があります。同じになっていない場合、VLAN 間を行き来するトラフィックがリークする可能性があります。

VLAN タグ付きフレームは、VLAN 対応や VLAN 非対応の他のネットワーク デバイスを通過できます。宛先エンド ノードが VLAN 未対応であり、VLAN からのトラフィックを受信する場合、最後の VLAN 対応デバイスが（ある場合）、宛先 VLAN のフレームをタグなしのエンド ノードに送信する必要があります。

特定の VLAN 内のポートを表示して設定するには、[VLAN へのポート] ページを使用します。

ポートまたは LAG を VLAN にマップするには、次のようにします。

ステップ 1 [VLAN 管理] > [VLAN へのポート] の順にクリックします。

ステップ 2 VLAN とインターフェイス タイプ（ポートまたは LAG）を選択し、[実行] をクリックして、ポートの VLAN 関連特性を表示または変更します。

各ポートまたは LAG のポート モードに、[インターフェイス設定] ページから設定した現在のポート モード（アクセス、トランク、全般、プライベート - ホスト、プライベート - プロミスキャス、またはカスタマー）が表示されます。

各ポートまたは LAG に、VLAN への現在の登録が表示されます。

次のフィールドが表示されます。

- [VLANモード]: VLAN 内のポートのタイプが表示されます。
- [メンバーシップ タイプ]: 次のいずれかのオプションを選択します。
  - [禁止]: このインターフェイスは、GVRP 登録からであっても VLAN に参加できません。ポートがその他の VLAN のメンバーでない場合、ポートに対してこのオプションを有効にすると、このポートは、内部 VLAN 4095（予約 VID）のポートになります。
  - [除外済み]: インターフェイスは現在 VLAN のメンバーではありません。VLAN を新しく作成するとき、これがすべてのポートと LAG のデフォルトになります。
  - [タグ付き]: このインターフェイスは、VLAN のタグ付きメンバーです。
  - [タグなし]: このインターフェイスは、VLAN のタグなしメンバーです。VLAN のフレームはインターフェイス VLAN にタグなしで送信されます。
- [PVID]: インターフェイスの PVID を VLAN の VID に設定する場合は、これを選択します。PVID はポート単位の設定です。

ステップ 3 [適用] をクリックします。インターフェイスが VLAN に割り当てられ、実行コンフィギュレーション ファイルに書き込まれます。

別の VLAN ID を選択することによって、引き続き、別の VLAN のポート メンバーシップを表示または設定できます。

ポート VLAN メンバーシップ

[ポート VLAN メンバーシップ] ページには、デバイス上のすべてのポートとともに、各ポートが所属する VLAN のリストが表示されます。

インターフェイスのポートベース認証方式が 802.1x であり、[管理ポート制御] が [自動] の場合は、次のようになります。

- ポートは、認証されるまで、ゲスト VLAN および未認証 VLAN を除くすべての VLAN から除外されます。[ポートへのVLAN] ページで、このポートには大文字の P がマークされます。
- ポートは、認証されると、設定された VLAN でメンバーシップを受け取ります。

注 VLAN IS モードがサポートされます。これは、さまざまな VLAN モードのポート VLAN メンバーシップを事前に設定できることを意味します。ポートが特定の VLAN モードになると、コンフィギュレーションがアクティブになります。別のモードに変更すると、変更前のモードの設定が保存され、インターフェイス上でそのモードが再アクティブ化されたときにその設定が再適用されます。

ポートを 1 つ以上の VLAN に割り当てるには、次のようにします。

ステップ 1 [VLAN 管理] > [ポートVLANメンバーシップ] の順にクリックします。

ステップ 2 インターフェイス タイプ (ポートまたは LAG) を選択し、[実行] をクリックします。選択したタイプのすべてのインターフェイスについて次のフィールドが表示されます。

- [LAG]: ポート ID または LAG ID。
- [モード]: [インターフェイス設定] ページで選択されたインターフェイス VLAN モード。
- [管理 VLAN]: インターフェイスがメンバーになる可能性のあるすべての VLAN を表示するドロップダウン リスト。
- [動作 VLAN]: インターフェイスが現在メンバーになっているすべての VLAN を表示するドロップダウン リスト。
- [LAG]: 選択したインターフェイスが [ポート] の場合、このインターフェイスがメンバーになっている LAG が表示されます。

ステップ 3 ポートを選択し、[VLAN への参加] ボタンをクリックします。

ステップ 4 次のフィールドに値を入力します。

- [インターフェイス]:ポートか LAG を選択します。
- [現在の VLAN モード]:[インターフェイス設定] ページで選択したポート VLAN モードが表示されます。
- [アクセス モード メンバーシップ(アクティブ)]
  - [アクセス VLAN ID]:ポートがアクセス モードになっている場合は、この VLAN のメンバーになります。
- [トランク モード メンバーシップ]
  - [ネイティブ VLAN ID]:ポートがトランク モードになっている場合は、この VLAN のメンバーになります。
  - [タグ付き VLAN]:ポートがトランク モードになっている場合は、これらの VLAN のメンバーになります。次のオプションが選択できます。

    [すべての VLAN]:ポートがトランク モードになっている場合は、すべての VLAN のメンバーになります。

    [ユーザ定義]:ポートがトランク モードになっている場合は、ここに入力された VLAN のメンバーになります。
- [一般モード メンバーシップ]
  - [タグなし VLAN]:ポートが一般モードになっている場合は、この VLAN のタグなしメンバーになります。
  - [タグ付き VLAN]:ポートが一般モードになっている場合は、これらの VLAN のタグ付きメンバーになります。
  - [禁止VLAN]:ポートが一般モードになっている場合は、インターフェイスが GVRP 登録からであっても VLAN に参加できません。ポートがその他の VLAN のメンバーでない場合、ポートに対してこのオプションを有効にすると、このポートは、内部 VLAN 4095(予約 VID)のポートになります。
  - [一般 PVID]:ポートが一般モードになっている場合は、これらの VLAN のメンバーになります。
- [カスタマー モード メンバーシップ]
  - [カスタマー VLAN ID]:ポートがカスタマー モードになっている場合は、この VLAN のメンバーになります。

ステップ 5 ポートを選択して、[詳細] をクリックし、次のフィールドを表示します。

- [管理 VLAN]:ポートはこれらの VLAN 用に設定されます。

- [動作 VLAN]:ポートは現在これらの VLAN のメンバーです。

ステップ 6 [適用] をクリックします([VLAN への参加] の場合)。設定が修正され、実行コンフィギュレーション ファイルに書き込まれます。

GVRP 設定

隣接する VLAN 対応デバイスは、Generic VLAN Registration Protocol(GVRP)を使用して、相互に VLAN 情報を交換できます。GVRP は Generic Attribute Registration Protocol(GARP)に基づいており、ブリッジ型ネットワークに VLAN 情報を伝達します。

インターフェイスで GVRP を有効にするには、全般モードで設定する必要があります。

GVRP を使用してポートが VLAN に参加すると、[ポート VLAN メンバーシップ] ページで明示的に禁止されていない限り、このポートはタグ付きダイナミック メンバーとしてその VLAN に追加されます。VLAN が存在しない場合、([GVRP 設定] ページで)このポートに対して [ダイナミック VLAN 作成] が有効にされていれば、VLAN が動的に作成されます。

GVRP は、各ポート上だけでなくグローバルに有効化する必要があります。有効化されると、GVRP によって GARP パケット データ単位(GPDU)が送受信されます。定義済みであっても非アクティブな VLAN の情報は伝達されません。VLAN 情報を伝達するには、その VLAN が少なくとも 1 つのポート上でアクティブである必要があります。

デフォルトで、GVRP はグローバルにもポートでも無効です。

GVRP 設定

インターフェイスの GVRP 設定を定義するには、次のようにします。

ステップ 1 [VLAN 管理] > [GVRP 設定] の順にクリックします。

ステップ 2 GVRP をグローバルに有効にするために、[GVRP グローバルステータス] を選択します。

ステップ 3 [適用] をクリックし、グローバルな GVRP のステータスを設定します。

ステップ 4 インターフェイス タイプ(ポートまたは LAG)を選択し、[実行] をクリックして、そのタイプのインターフェイスをすべて表示します。

ステップ 5 ポートの GVRP 設定を定義するために、ポートを選択し、[編集] をクリックします。

ステップ 6 次のフィールドに値を入力します。

- [インターフェイス]:編集するインターフェイス(ポートまたは LAG)を選択します。
- [GVRP状態]:このインターフェイス上で GVRP を有効にすることを選択して指定します。
- [ダイナミックVLAN作成]:このインターフェイス上でのダイナミック VLAN 作成を有効にすることを選択して指定します。
- [GVRP登録]:このインターフェイス上で GVRP を使用した VLAN 登録を有効にすることを選択して指定します。

ステップ 7 [適用] をクリックします。GVRP 設定が変更され、実行コンフィギュレーション ファイルに書き込まれます。

音声 VLAN

LAN では、IP 電話、VoIP エンドポイント、音声システムなどの音声デバイスは、同じ VLAN 内に配置されます。この VLAN は、音声 VLAN と呼ばれます。音声デバイスが別々の音声 VLAN 内にある場合、通信を行うには IP(レイヤ 3)ルータが必要です。

ここで説明する内容は次のとおりです。

- 音声 VLAN の概要
- 音声 VLAN 設定
- テレフォニー OUI

音声 VLAN の概要

ここで説明する内容は次のとおりです。

- ダイナミック音声 VLAN モード
- 自動音声 VLAN、Auto Smartport、CDP、および LLDP
- 音声 VLAN の QoS
- 音声 VLAN の制限事項
- 音声 VLAN のワークフロー

適切な設定を使用した典型的な音声展開シナリオは、次のとおりです。

- **UC3xx/UC5xx がホストされている場合:**すべてのシスコ製電話および VoIP エンドポイントがこの展開モデルに対応しています。このモデルの場合、UC3xx/UC5xx、シスコ製電話機、および VoIP エンドポイントは、同じ音声 VLAN 内にあります。UC3xx/UC5xx のデフォルト音声 VLAN は VLAN 100 です。
- **サードパーティ製 IP PBX がホストされている場合:**Cisco SBTG CP-79xx、SPA5xx 電話機、および SPA8800 エンドポイントがこの展開モデルに対応しています。このモデルの場合、電話機で使用される VLAN は、ネットワーク構成によって決まります。音声とデータの VLAN は別々の場合も同じ場合もあります。電話機と VoIP エンドポイントは、構内 IP PBX に登録されます。
- **IP Centrex/ITSP がホストされている場合:**Cisco CP-79xx、SPA5xx 電話機、および SPA8800 エンドポイントがこの展開モデルに対応しています。このモデルの場合、電話機で使用される VLAN は、ネットワーク構成によって決まります。音声とデータの VLAN は別々の場合も同じ場合もあります。電話機と VoIP エンドポイントは、「クラウド」内の構外 SIP プロキシに登録されます。

VLAN の観点からすると、上記のモデルは VLAN 対応環境および VLAN 非対応環境の両方で動作します。VLAN 対応環境で、音声 VLAN は設置時に設定された多くの VLAN のうちのいずれかです。VLAN 非対応環境でのシナリオは、VLAN が 1 つだけの VLAN 対応環境と同等です。

デバイスは VLAN 対応スイッチとして常に動作します。

デバイスは、単一の音声 VLAN をサポートします。デフォルトで、音声 VLAN は VLAN 1 です。音声 VLAN のデフォルトは、VLAN 1 です。手動で別の音声 VLAN に設定できます。また、自動音声 VLAN が有効な場合は、動的に学習することもできます。

ポートを音声 VLAN に手動で追加するには、「VLAN インターフェイスの設定」の説明に従って基本 VLAN コンフィギュレーションを使用するか、音声関連の Smartport マクロをポートに手動で適用します。デバイスがテレフォニー OUI モードの場合、または Auto Smartport が有効な場合は、動的にポートを追加することもできます。

ダイナミック音声 VLAN モード

デバイスは 2 種類のダイナミック音声 VLAN モードをサポートしています。それは、テレフォニー OUI（組織固有識別子）モード、および自動音声 VLAN モードです。これら 2 つのモードは、音声 VLAN や音声 VLAN ポート メンバーシップの構成に影響を与えます。2 つのモードは相互に排他的です。

- **テレフォニー OUI**

  テレフォニー OUI モードでは、音声 VLAN は手動設定の VLAN である必要があり、デフォルト VLAN に設定することはできません。

デバイスがテレフォニー OUI モードで、ポートが音声 VLAN への参加候補として手動で設定される場合、送信元 MAC アドレスが設定済みテレフォニー OUI のいずれかと一致するパケットをデバイスが受信すると、デバイスはこのポートを音声 VLAN に動的に追加します。OUI は、イーサネット MAC アドレスの先頭 3 バイトです。テレフォニー OUI の詳細については、「テレフォニー OUI」を参照してください。

- **自動音声 VLAN**

  自動音声 VLAN モードでは、音声 VLAN はデフォルト音声 VLAN、手動構成、外部デバイス（UC3xx/5xx など）からの学習結果、または CDP や VSDP で音声 VLAN をアドバタイズするスイッチからの学習結果のいずれかを使用できます。VSDP は、音声サービスのディスカバリ用に Cisco で定義されたプロトコルです。

  テレフォニー OUI モードではテレフォニー OUI に基づいて音声デバイスを検出しますが、自動音声 VLAN モードはそれとは異なり、Auto Smartport に基づいてポートを音声 VLAN に動的に追加します。Auto Smartport が有効な場合、CDP や LLDP-MED を介して電話またはメディア エンドポイントとしてアドバタイズするポートに接続されたデバイスを検出すると、そのポートを音声 VLAN に追加します。

音声エンドポイント

音声 VLAN が適切に機能するには、シスコ製電話や VoIP エンドポイントなどの音声デバイスが音声トラフィックを送受信する音声 VLAN に割り当てられている必要があります。たとえば次のシナリオが考えられます。

- 電話やエンドポイントは、音声 VLAN で静的に構成されています。
- 電話やエンドポイントは、TFTP サーバからダウンロードするブート ファイルで音声 VLAN を取得できます。DHCP サーバでは、IP アドレスを電話に割り当てるときにブート ファイルと TFTP サーバを指定できます。
- 電話機やエンドポイントは、ネイバーの音声システムおよびスイッチから受け取る CDP および LLDP-MED のアドバタイズメントから音声 VLAN の情報を取得できます。

デバイスは、接続する音声デバイスが音声 VLAN のタグ付きパケットを送信することを前提とします。音声 VLAN がネイティブ VLAN でもあるポートでは、音声 VLAN のタグなしパケットも使用可能です。

自動音声 VLAN、Auto Smartport、CDP、および LLDP

デフォルト

工場出荷時のデフォルトにより、CDP、LLDP、LLDP-MED、Auto Smartport モード、および信頼できる DSCP による基本 QoS が有効になります。すべてのポートは、デフォルトの音声 VLAN であるデフォルトの VLAN 1 のメンバーです。

音声 VLAN のトリガー

[ダイナミック音声VLAN] のモードが [自動音声 VLAN の有効化] に設定されている場合、1 つ以上のトリガーが発生した場合に限り、自動音声 VLAN が動作状態になります。トリガーになりうるものとしては、スタティック音声 VLAN コンフィギュレーション、ネイバー CDP アドバタイズメントで受信した音声 VLAN 情報、Voice VLAN Discovery Protocol (VSDP) で受信した音声 VLAN 情報などがあります。必要に応じて、トリガーを待機せず、直ちに自動音声 VLAN モードを動作させることもできます。

Auto Smartport が有効である場合、自動音声 VLAN モードに従い、自動音声 VLAN が動作状態になると Auto Smartport が有効になります。必要に応じて、自動音声 VLAN とは無関係に動作するよう Auto Smartport を設定できます。

注 ここに示すデフォルト コンフィギュレーション リストは、出荷時に自動音声 VLAN をサポートしているファームウェア バージョンを使用するスイッチに適用されます。また、自動音声 VLAN をサポートするファームウェア バージョンにアップグレードした、未構成のスイッチにも適用されます。

注 デフォルトおよび音声 VLAN トリガーは、音声 VLAN を含まないインストールや、設定済みのスイッチには影響しないように設計されています。自動音声 VLAN や Auto Smartport は、必要に応じて展開に合わせて手動で無効や有効にすることができます。

自動音声 VLAN

自動音声 VLAN は音声 VLAN の維持を行いますが、音声 VLAN ポート メンバーシップを維持するには Auto Smartport に依存します。自動音声 VLAN は、動作時に次の機能を実行します。

- 直接接続されたネイバー デバイスからの CDP アドバタイズメントで、音声 VLAN の情報を検出します。
- 複数のネイバー スイッチやルータ（シスコ ユニファイド コミュニケーション（UC）デバイスなど）がそれぞれの音声 VLAN をアドバタイズしている場合、MAC アドレスが最も小さいデバイスからの音声 VLAN が使用されます。

注 デバイスを Cisco UC デバイスに接続するには、UC デバイスがポートの CDP で音声 VLAN をアドバタイズするように、*switchport voice vlan* コマンドを使用して UC デバイスのポートを設定することが必要になる場合があります。

- 音声 VLAN 関連パラメータは、Voice VLAN Discovery Protocol（VSDP; 音声 VLAN 検出プロトコル）を使用して他の自動音声 VLAN 対応スイッチと同期されます。デバイス自体は、常に、認識されているプライオリティの最も高いソースからの音声 VLAN を使用して構成されます。プライオリティは、音声 VLAN 情報を提供するソースのソース タイプおよび MAC アドレスに基づきます。ソース タイプのプライオリティは、高いほうから順に、静的 VLAN コンフィギュレーション、CDP アドバタイズメント、変更されたデフォルト VLAN に基づくデフォルト コンフィギュレーション、デフォルト音声 VLAN です。数値の小さい MAC アドレスのほうが数値の大きい MAC アドレスよりもプライオリティが高くなります。
- 音声 VLAN は、プライオリティがさらに高いソースからの新しい音声 VLAN が検出されるか、自動音声 VLAN がユーザによって再起動されるまで維持されます。再起動されると、デバイスは音声 VLAN をデフォルト音声 VLAN にリセットし、自動音声 VLAN 検出を再起動します。
- 新しい音声 VLAN が設定されるか検出されると、デバイスはその音声 VLAN を自動作成し、既存の音声 VLAN のポート メンバーシップすべてを新しい音声 VLAN に置き換えます。これにより、既存の音声セッションが中断または終了することがあります。ネットワーク トポロジが変更されたと見なされるためです。

Auto Smartport は CDP/LLDP を使用して、ポートから音声エンドポイントが検出されたときにも音声 VLAN のポート メンバーシップを維持します。

- CDP および LLDP が有効な場合、デバイスは CDP パケットと LLDP パケットを定期的に送信して、使用する音声 VLAN を音声エンドポイントにアドバタイズします。
- ポートに接続しているデバイスが CDP や LLDP を使用して自身を音声エンドポイントとしてアドバタイズすると、Auto Smartport により対応する Smartport マクロがポートに適用され、ポートが音声 VLAN に自動的に追加されます（競合する機能や優れた機能をアドバタイズするポートからのデバイスが他にない場合）。デバイスが自身を電話としてアドバタイズする場合、デフォルト Smartport マクロは phone です。デバイスが自身を電話およびホスト、または電話およびブリッジとしてアドバタイズする場合、デフォルト Smartport マクロは phone+desktop です。

音声 VLAN の QoS

音声 VLAN は、LLDP-MED ネットワーク ポリシーを使用して CoS/802.1p 設定や DSCP 設定を伝達できます。LLDP-MED のデフォルトでは、アプライアンスが LLDP-MED パケットを送信する場合に、音声 QoS 設定を使用して応答するように設定されます。MED をサポートするデバイスは、LLDP-MED 応答で受け取った CoS/802.1p 値および DSCP 値と同じ値を使用して音声トラフィックを送信します。

ユーザは、音声 VLAN と LLDP-MED の間の自動更新を無効にしたり、独自のネットワーク ポリシーを使用したりできます。

OUI モードでは、デバイスで OUI に基づく音声トラフィックのマッピングおよびリマーキング（CoS/802.1p）を追加設定できます。

デフォルトでは、すべてのインターフェイスが CoS/802.1p 信頼モードです。デバイスは、音声ストリームで見つかった CoS/802.1p 値に基づいてサービス品質を適用します。テレフォニー OUI 音声ストリームでは、サービス品質をオーバーライドできるのに加え、必要に応じて音声ストリームの 802.1p をリマークできます。これは [テレフォニー OUI] で希望の CoS/802.1p 値を指定したり、リマーキング オプションを使用したりすることにより、これを実行できます。

音声 VLAN の制限事項

次のような制限事項があります。

- 音声 VLAN は 1 つしかサポートされません。
- 音声 VLAN として定義された VLAN は削除できません。

テレフォニー OUI の場合は、さらに次の制限事項が適用されます。

- 音声 VLAN は Smartport を有効にできません。
- 音声 VLAN の QoS 決定は、ポリシー決定以外のその他の QoS 決定より優先されます。
- 現在の音声 VLAN に候補ポートがない場合のみ、新しい VLAN ID を音声 VLAN に設定できます。
- 候補ポートのインターフェイス VLAN は、一般モードまたはトランク モードである必要があります。
- 音声 VLAN の QoS は、音声 VLAN に参加している候補ポートとスタティック ポートに適用されます。
- 音声フローは、転送データベース（FDB）がその MAC アドレスを学習できる場合に受け入れられます。（FDB に空きスペースがない場合、アクションは発生しません）。

音声 VLAN のワークフロー

自動音声 VLAN、Auto Smartport、CDP、および LLDP のデバイス デフォルト設定は、大半の音声展開シナリオに対応します。ここでは、デフォルト コンフィギュレーションが適用されないときに音声 VLAN を展開する方法について説明します。

ワークフロー 1: 自動音声 VLAN を設定するには、次のようにします。

ステップ 1 [音声 VLAN プロパティ] ページを開きます。

ステップ 2 音声 VLAN ID を選択します。VLAN ID 1 には設定できません（ダイナミック音声 VLAN の場合、この手順は必要ありません）。

ステップ 3 [ダイナミック音声VLAN] を [自動音声 VLAN の有効化] に設定します。

ステップ 4 [自動音声VLAN アクティブ化] の方式を選択します。

注 現在、デバイスがテレフォニー OUI モードの場合は、無効にしてから自動音声 VLAN を設定する必要があります。

ステップ 5 [適用] をクリックします。

ステップ 6 「Smartport の共通タスク」の項の説明に従って、Smartport を設定します。

ステップ 7 「ディスカバリ - LLDP」および「ディスカバリ - CDP」の説明に従って、LLDP/CDP を設定します。

ステップ 8 [インターフェイス設定] ページで、適切なポートの Smartport 機能を有効にします。

注 手順 7 および手順 8 は、デフォルトで有効な設定です。必要に応じて設定してください。

ワークフロー 2: テレフォニー OUI 方式を設定するには、次のようにします。

ステップ 1 [VLAN 管理] > [音声VLAN] > [プロパティ] ページを開きます。[ダイナミック音声 VLAN] を [テレフォニーOUIの有効化] に設定します。

注 現在、デバイスが自動音声 VLAN モードの場合は、無効にしてからテレフォニー OUI を有効にする必要があります。

ステップ 2 [テレフォニー OUI テーブル] ページでテレフォニー OUI を設定します。

ステップ 3 [テレフォニー OUI インターフェイス] ページで、ポートの [テレフォニー OUI VLAN メンバーシップ] を設定します。

音声 VLAN 設定

ここでは、音声 VLAN の設定方法について説明します。具体的な内容は、次のとおりです。

- 音声 VLAN プロパティ
- 自動音声 VLAN 設定
- テレフォニー OUI

音声 VLAN プロパティ

音声 VLAN の [プロパティ] ページで次の操作を行います。

- 音声 VLAN の現在の設定内容を表示します。
- 音声 VLAN の VLAN ID を設定します。
- 音声 VLAN の QoS を設定します。
- 音声 VLAN モード（テレフォニー OUI または自動音声 VLAN）を設定します。
- 自動音声 VLAN がトリガーされる方法を設定します。

音声 VLAN プロパティを表示して設定するには、次のようにします。

ステップ 1 [VLAN 管理] > [音声VLAN] > [プロパティ]の順にクリックします。

- デバイスで設定された音声 VLAN 設定は、[音声VLAN 設定] の [管理ステータス] ブロックに表示されます。
- 音声 VLAN 展開に実際に適用されている音声 VLAN 設定は、[音声VLAN 設定] の [動作ステータス] ブロックに表示されます。

ステップ 2 次の [管理ステータス] フィールドに値を入力します。

- [音声VLAN ID]：音声 VLAN にする VLAN を入力します。

  注 音声 VLAN ID、CoS/802.1p、DSCP のすべてまたはいずれかを変更すると、デバイスは、管理音声 VLAN をスタティック音声 VLAN としてアドバタイズします。外部音声 VLAN によってトリガーされる [自動音声VLAN アクティブ化] オプションを選択した場合は、デフォルト値のままにしておく必要があります。

- [CoS/802.1p]：音声ネットワーク ポリシーとして LLDP-MED で使用される CoS/802.1p 値を選択します。詳細については、[各種管理] > [ディスカバリ] > [LLDP] > [LLDP MED ネットワークポリシー] をご覧ください。

- [DSCP]:音声ネットワーク ポリシーとして LLDP-MED で使用される DSCP 値を選択します。詳細については、[各種管理] > [ディスカバリ] > [LLDP] > [LLDP MED ネットワークポリシー] をご覧ください。

次の [動作ステータス] フィールドが表示されます。

- [音声VLAN ID]:音声 VLAN。
- [CoS/802.1p]:音声ネットワーク ポリシーとして LLDP-MED で使用される値。詳細については、[各種管理] > [ディスカバリ] > [LLDP] > [LLDP MED ネットワークポリシー] をご覧ください。
- [DSCP]:音声ネットワーク ポリシーとして LLDP-MED で使用される値。

次の [ダイナミック音声VLAN 設定] フィールドが表示されます。

- [ダイナミック音声 VLAN]:次のいずれかの方法で音声 VLAN 機能を無効または有効にするにはこのフィールドを選択します。
  - [自動音声 VLAN の有効化]:ダイナミック音声 VLAN を自動音声 VLAN モードで有効にします。
  - [テレフォニーOUIの有効化]:ダイナミック音声 VLAN をテレフォニー OUI モードで有効にします。
  - [無効]:自動音声 VLAN またはテレフォニー OUI を無効にします。
- [自動音声 VLAN のアクティブ化]:自動音声 VLAN が有効な場合は、自動音声 VLAN をアクティブ化するためのオプションを次の中から選択します。
  - [即時]:有効にすると、デバイスでただちに自動音声 VLAN がアクティブになり、動作状態になります。
  - [外部音声VLANトリガーを使用]:音声 VLAN をアドバタイズするデバイスをデバイスが検出した場合にのみ、デバイス上の自動音声 VLAN がアクティブになり、動作状態になります。

  注 音声 VLAN ID、CoS/802.1p、DSCP のすべてまたはいずれかを手動でデフォルト値から再設定すると、外部ソースから学習した自動音声 VLAN よりもプライオリティが高いスタティック音声 VLAN になります。

ステップ 3 [適用] をクリックします。VLAN のプロパティは、実行コンフィギュレーション ファイルに書き込まれます。

自動音声 VLAN 設定

自動音声 VLAN モードが有効な場合は、[自動音声 VLAN] ページを使用して、関連のグローバル パラメータおよびインターフェイス パラメータを表示します。

このページの [自動音声 VLAN の再起動] をクリックして、自動音声 VLAN を手動で再起動することもできます。少し待った後、音声 VLAN はデフォルト音声 VLAN にリセットされ、LAN 内の自動音声 VLAN 対応スイッチすべてで自動音声 VLAN 検出および同期化プロセスが再起動します。

注 [ソースタイプ] が [非アクティブ] の状態の場合、音声 VLAN をデフォルトの音声 VLAN にリセットする処理のみが実行されます。

自動音声 VLAN パラメータを表示するには、次のようにします。

ステップ 1 [VLAN 管理] > [音声VLAN] > [自動音声VLAN] の順にクリックします。

このページの [動作状態] ブロックに、現在の音声 VLAN およびそのソースに関する情報が表示されます。

- [自動音声VLANステータス]: 自動音声 VLAN が有効かどうかが表示されます。
- [音声VLAN ID]: 現在の音声 VLAN の ID。
- [ソース タイプ]: 音声 VLAN がルート デバイスによって検出されたソースのタイプを表示します。
- [CoS/802.1p]: 音声ネットワーク ポリシーとして LLDP-MED で使用される CoS/802.1p 値が表示されます。
- [DSCP]: 音声ネットワーク ポリシーとして LLDP-MED で使用される DSCP 値が表示されます。
- [ルートスイッチ MAC アドレス]: 自動音声 VLAN のルート デバイスの MAC アドレス。自動音声 VLAN ルート デバイスは、この音声 VLAN を検出している、またはこの音声 VLAN が設定されているデバイスであり、この音声 VLAN の学習元のデバイスです。
- [スイッチ MAC アドレス]: デバイスの基本 MAC アドレス。デバイスの [スイッチ MAC アドレス] が [ルート スイッチ MAC アドレス] である場合、そのデバイスは自動音声 VLAN ルート デバイスです。
- [音声 VLAN ID 変更時間]: 音声 VLAN の最終更新時刻。

ステップ 2 [自動音声 VLAN の再起動] をクリックして、音声 VLAN をデフォルト音声 VLAN にリセットし、LAN 内の自動音声 VLAN 対応スイッチすべてで自動音声 VLAN 検出を再起動します。

[音声VLANローカルソーステーブル] には、デバイスで設定されている音声 VLAN、および、直接接続されたネイバー デバイスによってアドバタイズされた音声 VLAN の設定が表示されます。次のフィールドが含まれています。

- [インターフェイス]: 音声 VLAN 設定が受信または設定されたインターフェイスを表示します。[N/A] が表示される場合、その設定はデバイスそれ自体で行われています。インターフェイスが表示される場合、音声設定がネイバーから受信されています。
- [送信元 MAC アドレス]: 音声設定の受信元 UC の MAC アドレス。
- [ソース タイプ]: 音声設定の受信元 UC のタイプ。次のオプションが選択できます。
  - [デフォルト]: デバイスのデフォルト音声 VLAN 設定。
  - [スタティック]: デバイス上に定義されている、ユーザ定義の音声 VLAN 設定。
  - [CDP]: 音声 VLAN 設定をアドバタイズした UC は、CDP を実行しています。
  - [LLDP]: 音声 VLAN 設定をアドバタイズした UC は、LLDP を実行しています。
  - [音声 VLAN ID]: アドバタイズまたは設定された音声 VLAN の ID。
- [音声 VLAN ID]: 現在の音声 VLAN の ID。
- [CoS/802.1p]: 音声ネットワーク ポリシーとして LLDP-MED で使用される、アドバタイズまたは設定された CoS/802.1p 値。
- [DSCP]: 音声ネットワーク ポリシーとして LLDP-MED で使用される、アドバタイズまたは設定された DSCP 値。
- [最適なローカルソース]: この音声 VLAN がデバイスによって使用されたかどうかが表示されます。次のオプションが選択できます。
  - [はい]: デバイスはこの音声 VLAN を使用して他の自動音声 VLAN 対応スイッチと同期化します。この音声 VLAN は、よりプライオリティの高いソースが検出されない限り、ネットワークの音声 VLAN として機能します。ベスト ローカル ソースになるローカル ソースは 1 つだけです。
  - [いいえ]: この音声 VLAN は最適なローカル ソースではありません。

ステップ 3 [更新] をクリックして、ページの情報を更新します。

テレフォニー OUI

OUI は、Institute of Electrical and Electronics Engineers, Incorporated（IEEE; 電気電子学会）登録機関により割り当てられます。IP 電話製造元数には制限があり、既知のものなので、既知の OUI 値を使用すると、関連フレームおよびそのフレームを受信するポートは自動的に音声 VLAN に割り当てられます。

OUI グローバル テーブルには最大 128 OUI まで格納できます。

ここで説明する内容は次のとおりです。

- テレフォニー OUI テーブル
- テレフォニー OUI インターフェイス

テレフォニー OUI テーブル

[テレフォニーOUI] ページで、テレフォニー OUI の QoS プロパティを設定します。また、自動メンバーシップ エージング タイムを設定することもできます。テレフォニー アクティビティがないまま指定した時間が経過すると、ポートは音声 VLAN から削除されます。

[テレフォニー OUI] ページを使用して、既存の OUI を表示し、新しい OUI を追加します。

テレフォニー OUI を設定したり新しい音声 VLAN OUI を追加したりするには、次のようにします。

ステップ 1 [VLAN 管理] > [音声VLAN] > [テレフォニーOUI]の順にクリックします。

[テレフォニーOUI] ページには、次のフィールドが含まれています。

- [テレフォニーOUIの動作ステータス]:OUI が音声トラフィックの識別に使用されているかどうかを表示します。
- [CoS/802.1p]:音声トラフィックに割り当てる CoS キューを選択します。
- [CoS/802.1p の再マーキング]:出力トラフィックを再マーキングするかどうかを選択します。
- [自動メンバーシップ エージング タイム]:ポートで検出された電話の MAC アドレスすべてが期限切れになった後、音声 VLAN からそのポートを削除するまでの遅延時間を入力します。

ステップ 2 [適用] をクリックし、これらの値でデバイスの実行コンフィギュレーションを更新します。

[テレフォニーOUIテーブル] が表示されます。

- [テレフォニー OUI]:OUI 用に予約されている MAC アドレスの先頭 6 桁。
- [説明]:ユーザが割り当てた OUI の説明。

ステップ 3 [デフォルトOUIの復元] をクリックすると、ユーザが作成した OUI はすべて削除され、デフォルトの OUI のみがテーブルに残ります。復元が完了するまでは、OUI 情報が正確でない場合があります。復元には数秒かかる場合があります。数秒後に、このページを閉じてから開き直して、ページを更新します。

OUI をすべて削除するには、一番上のチェックボックスを選択します。すべての OUI が選択されるので、[削除] をクリックすると、すべて削除できます。その後で、[デフォルトOUIの復元] をクリックすると、システムが既知の OUI を復元します。

ステップ 4 OUI を新規に追加するには、[追加] をクリックします。

ステップ 5 次のフィールドに値を入力します。

- [テレフォニー OUI]:新しい OUI を入力します。
- [説明]:OUI の名前を入力します。

ステップ 6 [適用] をクリックします。OUI がテレフォニー OUI テーブルに追加されます。

テレフォニー OUI インターフェイス

QoS アトリビュートは、次のいずれかのモードで、音声パケットにポートごとに割り当てられます。

- [すべて]:そのインターフェイスで受信され、音声 VLAN に分類されるすべての着信フレームに、その音声 VLAN に設定されているサービス品質(QoS)値が適用されます。
- [テレフォニー送信元MACアドレス]:音声 VLAN に分類され、設定済みテレフォニー OUI と一致する送信元 MAC アドレスに OUI が含まれている着信フレームに、その音声 VLAN 用に設定されている QoS 値が適用されます。

[テレフォニーOUIインターフェイス] ページを使用して、OUI ID に基づいて音声 VLAN にインターフェイスを追加し、音声 VLAN の OUI QoS モードを設定します。

インターフェイスでテレフォニー OUI を設定するには、次のようにします。

ステップ 1 [VLAN 管理] > [音声VLAN] > [テレフォニーOUIインターフェイス]の順にクリックします。

[テレフォニーOUIインターフェイス] ページには、すべてのインターフェイスの音声 VLAN OUI パラメータが含まれています。

ステップ 2 テレフォニー OUI ベースの音声 VLAN の候補ポートとしてインターフェイスを設定するには、[編集] をクリックします。

ステップ 3 次のフィールドに値を入力します。

- [インターフェイス]: インターフェイスを選択します。
- [テレフォニー OUI VLAN メンバーシップ]: 有効にすると、そのインターフェイスがテレフォニー OUI ベースの音声 VLAN の候補ポートになります。設定済みテレフォニー OUI のいずれかと一致するパケットが受信されると、ポートは音声 VLAN に追加されます。
- [音声VLAN QoSモード] (メイン ページの [テレフォニーOUI QoSモード]): 次のオプションのいずれかを選択します。
  - [すべて]: この音声 VLAN に分類されるすべてのパケットに QoS 属性が適用されます。
  - [テレフォニー送信元 MAC アドレス]: IP 電話からのパケットのみに QoS 属性が適用されます。

ステップ 4 [適用] をクリックします。OUI が追加されます。

13

スパニング ツリー

このセクションでは、スパニング ツリー プロトコル（STP）（IEEE802.1D および IEEE802.1Q）について説明します。具体的な内容は、次のとおりです。

- STP の種類
- STP のステータスとグローバル設定
- STP インターフェイス設定
- RSTP インターフェイス設定
- マルチ スパニング ツリーの概要
- MSTP プロパティ
- MSTP インスタンスへの VLAN
- MSTP インスタンス設定
- MSTP インターフェイス設定

STP の種類

STP は、リンクを選択的にスタンバイ モードに設定してループを回避することで、レイヤ 2 のブロードキャスト ドメインをブロードキャスト ストームから保護します。スタンバイ モードになっているリンク上では、ユーザ データの転送が一時的に停止します。トポロジが変更されてデータ転送が可能になると、リンクは自動的に有効化されます。

ホスト間に代替パスが存在する場合、ループが発生します。ループは、スイッチが同じパケットを永久に中継することになり、宛先にパケットが届かなかったり、ブロードキャスト/マルチキャスト ストームを引き起こしたり、ネットワーク効率が低下したりします。

STP を使用すると、ネットワーク上のエンド ステーション間に 1 本の固有のパスが生成され、ループが解消されるので、スイッチと相互接続リンクがツリー トポロジになります。

このデバイスでサポートされているスパニング ツリー プロトコルのバージョンは次のとおりです。

- 従来の STP では、任意の 2 台のエンド ステーション間に生成されるパスが 1 本のみになるため、ループが解消されます。
- Rapid STP（RSTP; 高速 STP）では、ネットワーク トポロジが検出され、スパニング ツリーが構成されるまでの収束時間が短くなります。ネットワーク トポロジが元々ツリー構造になっている場合、RSTP は非常に効果的であり、収束に要する時間が短くなる可能性があります。RSTP はデフォルトで有効になっています。
- 多重 STP（MSTP）：MSTP は RSTP に基づきます。レイヤ 2 のループを検知し、関係するポートからトラフィックが送信されないようにすることでループを軽減します。レイヤ 2 ドメイン単位にループが存在するため、STP ループを排除するためにポートがブロックされたときに、この状況になる可能性があります。トラフィックは、ブロックされていないポートに転送され、ブロックされているポートには転送されません。この場合は、ブロックされているポートが常に使用されないため、帯域幅が効率的に消費されません。
- MSTP では、この問題を解決するため、インスタンスごとにループを個別に検知して軽減できるように、複数の STP インスタンスが有効になります。これにより、ポートは 1 つ以上の STP インスタンスに対してブロックされますが、他の STP インスタンスに対してはブロックされなくなります。複数の VLAN が複数の STP インスタンスに関連付けられている場合は、それらのトラフィックが関連する MST インスタンスの STP ポート状態に基づいて中継されます。帯域幅利用率が改善されます。

STP のステータスとグローバル設定

[STP ステータス & グローバル設定] ページには、STP、RSTP、または MSTP を有効にするためのパラメータが含まれています。

各モードを設定するには、[STP インターフェイス設定] ページ、[RSTP インターフェイス設定] ページ、および [MSTP プロパティ] ページをそれぞれ使用します。

STP のステータスとグローバル設定を設定するには、次のようにします。

ステップ 1 [スパニングツリー] > [STP ステータス&グローバル設定] の順にクリックします。

ステップ 2 パラメータを入力します。

[グローバル設定]:

- [スパニングツリー状態]:選択すると、デバイスで有効になります。
- [STP ループバックガード]:選択すると、デバイスでループバック ガードが有効になります。
- [STP動作モード]:STP モードを選択します。
- [BPDU処理]:ポートまたはデバイス上で STP が無効になっている場合のブリッジ プロトコル データ ユニット(BPDU)パケットの管理方法を選択します。BPDU は、スパニング ツリー情報を送信する目的で使用されます。
  - [フィルタリング]:インターフェイス上でスパニング ツリーが無効になっている場合に BPDU パケットをフィルタリングします。
  - [フラッディング]:インターフェイス上でスパニング ツリーが無効になっている場合に BPDU パケットをフラッディングします。
- [パスコストデフォルト値]:STP ポートにデフォルト パス コストを割り当てる際に使用する方法を選択します。インターフェイスに割り当てられるデフォルトのパス コストは、このフィールドで選択した方法によって変わります。
  - [ショート]:ポートのパス コストとして 1 ～ 65,535 の範囲の値を入力します。
  - [ロング]:ポートのパス コストとして 1 ～ 200,000,000 の範囲の値を入力します。

[ブリッジ設定]:

- [プライオリティ]:ブリッジ プライオリティ値を入力します。スイッチ間で BPDU が交換された後、プライオリティ値が最も小さいデバイスがルート ブリッジになります。すべてのスイッチのプライオリティ値が同じである場合は、MAC アドレスに基づいてルート ブリッジが決まります。このプライオリティ値は、4096 の倍数にしてください。たとえば、4096、8192、12288 などの値を入力します。
- [ハロータイム]:ルート ブリッジが設定メッセージを待機する時間間隔を秒数で入力します。
- [最大経過時間]:このデバイスが設定メッセージを待機する時間を秒数で入力します。この時間内に設定メッセージが届かない場合、デバイス自体の設定情報が再定義されます。
- [転送遅延]:ブリッジがラーニング ステートを維持する時間を秒数で入力します。この時間を過ぎると、ブリッジからパケットが転送されます。詳細については、「STP インターフェイス設定」を参照してください。

[指定ルート]:

- [ブリッジID]:このデバイスのブリッジ プライオリティ値と MAC アドレスを結合した値。
- [ルートブリッジID]:ルート ブリッジのプライオリティ値と MAC アドレスを結合した値。
- [ルートポート]:このブリッジからルート ブリッジへの最小のコスト パスを提供するポート。(これはブリッジがルートでない場合に重要です。)
- [ルートパスコスト]:このブリッジからルートまでのパスのコスト。
- [トポロジ変更回数]:STP トポロジが今までに変更された回数。
- [最後のトポロジ変更からの経過時間]:最後にトポロジが変更されてからの経過時間。日/時間/分/秒の形式で表示されます。

ステップ 3 [適用] をクリックします。STP グローバル設定が実行コンフィギュレーション ファイルに書き込まれます。

STP インターフェイス設定

[STP インターフェイス設定] ページでは、ポート単位の STP 情報を設定するや、代表ブリッジなどのプロトコルによって学習された情報を表示することができます。

入力された定義設定は、すべての種類の STP プロトコルで有効です。

インターフェイス単位の STP 情報を設定するには、次のようにします。

ステップ 1 [スパニングツリー] > [STP インターフェイス設定] の順にクリックします。

ステップ 2 インターフェイスを選択し、[編集] をクリックします。

ステップ 3 パラメータを入力します。

- [インターフェイス]: スパニング ツリーを設定するポートまたは LAG を選択します。
- [STP]: このポートに対して STP を有効または無効にします。
- [エッジポート]: このポートに対してファスト リンクを有効または無効にします。ポートに対してファスト リンク モードを有効にした場合、そのポートはリンクアップすると自動的にフォワーディング ステートに設定されます。ファスト リンクを有効にすると、STP プロトコルにおける収束処理が最適化されます。次のオプションがあります。
  - [有効]: ファスト リンクをすぐに有効にします。
  - [自動]: このインターフェイスがアクティブになってから数秒後に、ファスト リンクを有効にします。この場合、ファスト リンクが有効になる前にループが解消されます。
  - [無効]: ファスト リンクを無効にします。

  注 値を [自動] に設定することを推奨します。このようにすると、このデバイスにホストが接続されたときにポートがファスト リンク モードに設定され、別のデバイスに接続されたときには通常の STP ポートとして設定されます。これはループの回避に役立ちます。

  エッジ ポートは MSTP モードでは動作しません。
- [BPDU処理]: ポート上またはデバイス上で STP が無効になっている場合の BPDU パケットの処理方法を選択します。BPDU は、スパニング ツリー情報を送信する目的で使用されます。
  - [グローバル設定を使用]: [STP のステータスとグローバル設定] ページで定義した設定を使用する場合に選択します。

  - [フィルタリング]: インターフェイス上でスパニング ツリーが無効になっている場合に BPDU パケットをフィルタリングします。
  - [フラッディング]: インターフェイス上でスパニング ツリーが無効になっている場合に BPDU パケットをフラッディングします。
- [パスコスト]: ルート パス コストにおけるこのポートのコストを入力するか、または、このシステムによって生成されたデフォルトのコストを使用します。
- [プライオリティ]: このポートのプライオリティ値を入力します。このスイッチの 2 つのポートがループに接続されている場合、このプライオリティ値がポートの選択に影響を及ぼします。プライオリティは 0 ～ 240 の範囲の値で、16 の倍数である必要があります。
- [ポート状態]: このポートの現在の STP 状態が表示されます。
  - [無効]: このポートに対して STP は現在無効になっています。トラフィックが転送され、MAC アドレスが学習されます。
  - [ブロッキング]: このポートは現在ブロックされており、BPDU データ以外のトラフィックを転送したり、MAC アドレスを学習したりすることはできません。
  - [リスニング]: このポートはリスニング モードになっています。トラフィックを転送したり、MAC アドレスを学習したりすることはできません。
  - [ラーニング]: このポートは学習モードになっています。トラフィックを転送することはできませんが、新しい MAC アドレスを学習することはできます。
  - [フォワーディング]: このポートはフォワーディング モードになっています。トラフィックを転送したり、新しい MAC アドレスを学習したりすることができます。
- [代表ブリッジID]: 代表ブリッジのブリッジ プライオリティ値と MAC アドレスが表示されます。
- [指定ポートID]: 選択したポートのプライオリティ値とインターフェイスが表示されます。
- [指定コスト]: STP トポロジに属しているポートのコストが表示されます。コストが小さいポートは、STP でループが検出されたときにブロックされる可能性が低くなります。
- [フォワーディングへの移行]: このポートが**ブロッキング**状態から**フォワーディング**状態に移行した回数が表示されます。
- [速度]: このポートの速度が表示されます。

- [LAG]: このポートが所属している LAG が表示されます。ポートが LAG のメンバーである場合、ポートの設定情報よりも LAG の設定情報が優先されます。

ステップ 4 [適用] をクリックします。インターフェイス設定が実行コンフィギュレーション ファイルに書き込まれます。

RSTP インターフェイス設定

高速スパニング ツリー プロトコル(RSTP)を使用した場合、転送ループが解消されるため、通常の STP 収束処理がより高速になります。

[RSTP インターフェイス設定] ページでは、ポート単位で RSTP を設定できます。このページで設定した情報は、グローバル STP モードが RSTP に設定されている場合に有効になります。

RSTP 設定を入力するには、次のようにします。

ステップ 1 [スパニングツリー] > [STP ステータス&グローバル設定] の順にクリックします。

ステップ 2 [RSTP] を有効にします。

ステップ 3 [スパニングツリー] > [RSTP インターフェイス設定] の順にクリックします。[RSTP インターフェイス設定] ページが表示されます。

ステップ 4 ポートを選択します。

注 [プロトコル移行のアクティブ化] は、テスト対象のブリッジ パートナーに接続しているポートを選択した場合にのみ使用可能になります。

ステップ 5 STP によってリンク パートナーが検出された場合、[プロトコル移行のアクティブ化] をクリックし、プロトコル移行テストを実行します。このテストにより、まだ STP を使用しているリンク相手が存在しているかどうか、また、存在する場合は RSTP または MSTP のどちらに移行したかが判明します。リンク相手が STP リンクにまだ存在している場合、引き続き STP を使用してそのリンク相手と通信します。そうではなく、すでに RSTP または MSTP に移行されている場合は、デバイスが RSTP または MSTP を使用して通信します。

ステップ 6 インターフェイスを選択し、[編集] をクリックします。

ステップ 7 パラメータを入力します。

- [インターフェイス]: インターフェイスを設定し、RSTP を設定するポートまたは LAG を指定します。

- [ポイントツーポイント管理ステータス]:ポイントツーポイント リンクのステータスを指定します。全二重と定義されているポートは、ポイントツーポイント ポート リンクであると見なされます。
  - [有効]:RSTP が有効になっている場合、このポートは RSTP エッジ ポートになり、通常 2 秒以内にフォワーディング モードに移行します。
  - [無効]:このポートは、RSTP のためのポイントツーポイントとは見なされません。つまり、このポート上では、STP は高速ではなく通常速度で動作します。
  - [自動]:RSTP BPDU を使用して、デバイスのステータスを自動的に決定します。
- [ポイントツーポイント動作ステータス]:[ポイントツーポイント管理ステータス] を [自動] に設定した場合、ポイントツーポイントの動作ステータスが表示されます。
- [ロール]:STP パスを構成するために、STP によってこのポートに割り当てられているロールが表示されます。表示されるロールは次のとおりです。
  - [ルート]:パケットをルート ブリッジに転送するためのコスト パスが最も低いロール。
  - [指定]:このスイッチを LAN に接続するためのインターフェイス。LAN からルート ブリッジまでのコスト パスが最小です。
  - [代替]:ルート ポートからルート ブリッジへの代替パスに使用されます。
  - [バックアップ]:スパニング ツリーのリーフへの指定ポート パスに対するバック アップ パスに使用されます。これは、2 つのポートがポイントツーポイント リンクによってループに接続されている場合に割り当てられます。また、バックアップ ポートは、共有セグメントへの接続が LAN 上に複数確立されている場合にも割り当てられます。
  - [無効]:このポートはスパニング ツリーに属していません。
- [モード]:現在のスパニング ツリーのモードを表示します。従来の STP または RSTP です。
- [ファストリンク動作ステータス]:このインターフェイスに対するファスト リンク(エッジ ポート)のステータス(有効、無効、または自動)が表示されます。値は次のとおりです。
  - [有効]:ファスト リンクが有効になっています。
  - [無効]:ファスト リンクが無効になっています。

- [自動]: このインターフェイスがアクティブになってから数秒後に、ファスト リンク モードが有効になります。

• [ポート ステータス]: 特定のポートの RSTP ステータスが表示されます。

- [無効]: このポートに対して STP は現在無効になっています。
- [廃棄]: このポートは現在廃棄/ブロックされており、トラフィックを転送したり、MAC アドレスを学習したりすることはできません。
- [リスニング]: このポートはリスニング モードになっています。トラフィックを転送したり、MAC アドレスを学習したりすることはできません。
- [ラーニング]: このポートは学習モードになっています。トラフィックを転送することはできませんが、新しい MAC アドレスを学習することはできます。
- [フォワーディング]: このポートはフォワーディング モードになっています。トラフィックを転送したり、新しい MAC アドレスを学習したりすることができます。

ステップ 8 [適用] をクリックします。実行コンフィギュレーション ファイルが更新されます。

マルチ スパニング ツリーの概要

Multiple Spanning Tree Protocol（MSTP）は、複数の異なる VLAN 上のさまざまなドメインの間の STP ポートの状態を分離するために使用されます。たとえば、VLAN A のループにより、ポート A がある STP インスタンスでブロックされている場合に、同じポートを別の STP インスタンスでフォワーディング ステートにすることができます。[MSTP プロパティ] ページでは、グローバル MSTP 設定を定義できます。

MSTP を設定するには、次のようにします。

ステップ 1 「*STP のステータスとグローバル設定*」ページで説明するように、[STP 動作モード] を [MSTP] に設定します。

ステップ 2 MSTP インスタンスを定義します。各 MSTP インスタンスは、ループフリー トポロジを計算して作成し、インスタンスにマップする VLAN からのパケットをブリッジします。「MSTP インスタンスへの VLAN」セクションを参照してください。

ステップ 3 どの VLAN のどの MSTP インスタンスをアクティブにするか決定し、それらの MSTP インスタンスをそれぞれ VLAN に関連付けます。

ステップ 4 MSTP の属性を次のように設定します。

- *MSTP プロパティ*
- MSTP インスタンス設定
- *MSTP インスタンスへの VLAN*

MSTP プロパティ

グローバル MSTP は、VLAN グループごとに別個のスパニング ツリーを設定し、各スパニング ツリー インスタンス内の可能な代替パスの 1 つを除くすべてをブロックします。MSTP は複数 MST インスタンス(MSTI)を実行できる MST リージョンの構成を有効にします。複数リージョンとその他の STP ブリッジは、単一の共通スパニング ツリー(CST)を使用して相互接続されます。

MSTP BPDU が RSTP ブリッジによって RSTP BPDU として解釈できるという点で、MSTP は RSTP ブリッジと完全に互換性があります。これを使用すると、設定を変更しないで RSTP ブリッジとの互換性が有効になるだけでなく、MSTP リージョン自体の内部にある MSTP ブリッジの数に関係なく、MSTP リージョンの外部にある RSTP ブリッジで、リージョンが単一の RSTP ブリッジとして認識されるようになります。

複数のスイッチを同じ MST リージョンに配置するには、VLAN から MST インスタンスへの同じマッピング、同じ設定リビジョン番号、同じリージョン名を持っている必要があります。

同じ MST リージョン内に配置するスイッチは、別の MST リージョンのスイッチによって分離されることはありません。分離されると、リージョンは 2 つの分離したリージョンになります。

このマッピングは、[MSTP インスタンスへの VLAN] ページで実行できます。

システムが MSTP モードで動作している場合にこのページを使用します。

MSTP を定義するには、次のようにします。

ステップ 1 [スパニングツリー] > [STP ステータス&グローバル設定] の順にクリックします。

ステップ 2 MSTP を有効にします。

ステップ 3 [スパニングツリー] > [MSTP プロパティ] の順にクリックします。

ステップ 4 パラメータを入力します。

- [リージョン名]:MSTP リージョン名を定義します。

- [リビジョン]:現在の MST 設定のリビジョンを識別する符号なしの 16 ビットの数値を定義します。フィールドの範囲は 0 ～ 65535 です。
- [最大ホップ]:BPDU を廃棄する前に特定のリージョンで発生するホップの合計数を設定します。BPDU を廃棄すると、ポート情報が期限切れになります。フィールドの範囲は 1 ～ 40 です。
- [ISTマスター]:リージョン マスターを表示します。

ステップ 5 [適用] をクリックします。MSTP プロパティが定義され、実行コンフィギュレーション ファイルが更新されます。

MSTP インスタンスへの VLAN

[MSTP インスタンスへの VLAN] ページでは、各 VLAN をマルチ スパニング ツリー インスタンス(MSTI)にマップできます。デバイスを同じリージョンに配置するには、VLAN から MSTI への同じマッピングを持っている必要があります。

注 同じ MSTI を複数の VLAN にマップできますが、各 VLAN には 1 つの MST インスタンスしかアタッチできません。

このページ(およびすべての MSTP ページ)の設定は、システムの STP モードが MSTP である場合に適用されます。

インスタンス ゼロに加えて、最大で 16 個の MST インスタンスを定義できます。

MST インスタンスの 1 つに明示的にマップされていない VLAN では、デバイスが CIST(Core and Internal Spanning Tree)インスタンスに自動的にマップします。CIST インスタンスは、MST インスタンス 0 です。

VLAN を MST インスタンスにマップするには、次のようにします。

ステップ 1 [スパニングツリー] > [MSTP インスタンスへの VLAN] の順にクリックします。

[MSTP インスタンスへの VLAN] ページには、次のフィールドがあります。

- [MSTP インスタンス ID]:すべての MST インスタンスが表示されます。
- [VLAN]:MST インスタンスに属するすべての VLAN が表示されます。

ステップ 2 VLAN を MSTP インスタンスに追加するには、MST インスタンスを選択して、[編集] をクリックします。

ステップ 3 パラメータを入力します。

- [MSTP インスタンス ID]:MST インスタンスを選択します。
- [VLAN]:この MST インスタンスにマップされる VLAN を定義します。
- [アクション]:VLAN を MST インスタンスに**追加**(マップ)するか**削除**するかを定義します。

ステップ 4 [適用] をクリックします。MSTP VLAN のマッピングが定義され、実行コンフィギュレーション ファイルが更新されます。

MSTP インスタンス設定

[MSTP インスタンス設定] ページでは、MST インスタンスごとにパラメータを設定して表示できます。これは、*STP ステータスとグローバル設定を設定する作業*をインスタンス単位で行う機能と同等です。

MSTP インスタンス設定を入力するには、次のようにします。

ステップ 1 [スパニングツリー] > [MSTP インスタンス設定] の順にクリックします。

ステップ 2 パラメータを入力します。

- [インスタンス ID]:表示して定義する MST インスタンスを選択します。
- [含まれるVLAN]:選択したインスタンスにマップされる VLAN を表示します。デフォルトのマッピングでは、すべての VLAN が Common and Internal Spanning Tree(CIST) インスタンス 0 にマップされています。
- [ブリッジプライオリティ]:選択された MST インスタンスに対するこのブリッジのプライオリティを設定します。
- [代表ルートブリッジ ID]:MST インスタンスに対するルート ブリッジのプライオリティと MAC アドレスが表示されます。
- [ルートポート]:選択されたインスタンスのルート ポートを表示します。
- [ルートパスコスト]:選択されたインスタンスのルート パス コストを表示します。
- [ブリッジ ID]:選択されたインスタンスにおけるこのデバイスのブリッジ プライオリティと MAC アドレスが表示されます。

- [残存ホップ]:次の宛先まで残っているホップの数を表示します。

ステップ 3 [適用] をクリックします。MST インスタンス構成が定義され、実行コンフィギュレーション ファイルが更新されます。

MSTP インターフェイス設定

[MSTP インターフェイス設定] ページでは、すべての MST インスタンスに対してポートの MSTP 設定を行い、MST インスタンス単位の代表ブリッジなど、プロトコルによって現在学習されている情報を表示できます。

MST インスタンスでポートを設定するには、次のようにします。

ステップ 1 [スパニングツリー] > [MSTP インターフェイス設定] の順にクリックします。

ステップ 2 パラメータを入力します。

- [インスタンスが次に等しい]:設定する MSTP インスタンスを選択します。
- [インターフェイスタイプが次に等しい]:ポートまたは LAG のリストを表示するかどうかを選択します。

ステップ 3 [実行] をクリックします。インスタンスのインターフェイスに対する MSTP パラメータが表示されます。

ステップ 4 インターフェイスを選択し、[編集] をクリックします。

ステップ 5 パラメータを入力します。

- [インスタンス ID]:設定する MST インスタンスを選択します。
- [インターフェイス]:MSTI 設定の定義対象となるインターフェイスを選択します。
- [インターフェイスプライオリティ]:指定されたインターフェイスと MST インスタンスのポート プライオリティを設定します。
- [パスコスト]:[ユーザ定義] テキストボックスのルート パス コストにポートのコストを指定するか、[デフォルトを使用] を選択してデフォルト値を使用します。

- [ポート状態]:特定の MST インスタンスの特定のポートの MSTP ステータスを表示します。パラメータは次のように定義されます。
  - [無効]:STP は現在無効です。
  - [廃棄]:このインスタンスのポートは現在廃棄/ブロックされており、BPDU データ以外のトラフィックを転送したり、MAC アドレスを学習したりすることはできません。
  - [リスニング]:このインスタンスのポートはリスニング モードになっています。トラフィックを転送したり、MAC アドレスを学習したりすることはできません。
  - [ラーニング]:このインスタンスのポートは学習モードになっています。トラフィックを転送することはできませんが、新しい MAC アドレスを学習することはできます。
  - [フォワーディング]:このインスタンスのポートはフォワーディング モードになっています。トラフィックを転送したり、新しい MAC アドレスを学習したりすることができます。
  - [境界]:このインスタンスのポートは境界ポートになっています。インスタンス 0 から状態を継承し、[STP インターフェイス設定] ページで確認できます。
- [ポート ロール]:STP パスを構成するために MSTP アルゴリズムによって割り当てられた、ポート単位のポートまたは LAG ロール、あるいはインスタンス単位の LAG を表示します。
  - [ルート]:このインターフェイスを経由してパケットを転送すると、ルート デバイスにパケットを転送するコスト パスが最小になります。
  - [指定ポート]:このブリッジを LAN に接続するためのインターフェイス。MST インスタンスに対する LAN からルート ブリッジまでのルート コスト パスが最小です。
  - [代替]:このインターフェイスは、ルート ポートからルート デバイスへの代替パスに使用されます。
  - [バックアップ]:このインターフェイスは、スパニング ツリーのリーフへの指定ポート パスに対するバックアップ パスに使用されます。バックアップ ロールは、2 つのポートがポイントツーポイント リンクによってループに接続されている場合に割り当てられます。また、バックアップ ポートは、共有セグメントへの接続が LAN 上に複数確立されている場合にも発生します。
  - [無効]:このインターフェイスはスパニング ツリーに属していません。

- [境界]: このインスタンスのポートは境界ポートになっています。インスタンス 0 から状態を継承し、[STP インターフェイス設定] ページで確認できます。

- [モード]: 現在のインターフェイス スパニング ツリーのモードを表示します。
  - リンク パートナーが MSTP または RSTP を使用している場合、表示されるポート モードは RSTP になります。
  - リンク パートナーが STP を使用している場合、表示されるポート モードは STP になります。
- [タイプ]: このポートの MST タイプが表示されます。
  - [境界]: 境界ポートは、MST ブリッジをリモート リージョンの LAN にアタッチします。ポートが境界ポートの場合、リンクの反対側のデバイスが RSTP モードと STP モードのどちらで動作しているかどうかも示します。
  - [内部]: ポートが内部ポートです。
- [代表ブリッジ ID]: リンクまたは共有 LAN をルートに接続するブリッジの ID 番号を表示します。
- [指定ポート ID]: リンクまたは共有 LAN をルートに接続する代表ブリッジのポート ID 番号を表示します。
- [指定コスト]: STP トポロジに属しているポートのコストが表示されます。コストが小さいポートは、STP でループが検出されたときにブロックされる可能性が低くなります。
- [残存ホップ]: 次の宛先まで残っているホップを表示します。
- [フォワーディングへの移行]: このポートがフォワーディング ステートから廃棄ステートに移行した回数が表示されます。

ステップ 6 [適用] をクリックします。実行コンフィギュレーション ファイルが更新されます。

14

MAC アドレス テーブルの管理

このセクションでは、MAC アドレスをシステムに追加する方法について説明します。具体的な内容は、次のとおりです。

- スタティック アドレス
- ダイナミック アドレス

MAC アドレスにはスタティック（静的）とダイナミック（動的）の 2 種類があります。MAC アドレスは、その種類に応じて、*スタティック アドレス* テーブルまたは *ダイナミック アドレス* テーブルに、VLAN 情報およびポート情報と共に格納されます。

スタティック アドレスはユーザによって構成されるため、期限切れになりません。

デバイスに到着するフレーム内に表示される新しい送信元 MAC アドレスは、ダイナミック アドレス テーブルに追加されます。構成可能な一定期間にわたって、この MAC アドレスが保持されます。この有効期間に達する前に、同じ送信元 MAC アドレスを持つ別のフレームがデバイスに到着しない場合、この MAC エントリは期限切れになり、テーブルから削除されます。

デバイスにフレームが到着するとき、デバイスはスタティックまたはダイナミック テーブル内に一致する宛先 MAC アドレス エントリがないか検索します。一致が見つかった場合、そのフレームは、テーブルで指定されたポートで出力されるようマークが付けられます。テーブル内に見つからない MAC アドレスに送信されるフレームは、該当する VLAN 上の全ポートに伝送/ブロードキャストされます。このようなフレームを、不明なユニキャスト フレームといいます。

デバイスでは、最大 8,000 個のスタティックおよびダイナミック MAC アドレスがサポートされます。

スタティック アドレス

スタティック MAC アドレスは、デバイス上の特定の物理インターフェイスおよび VLAN に割り当てられます。そのアドレスが別のインターフェイスで見つかった場合、それは無視され、アドレス テーブルには書き込まれません。

スタティック アドレスを定義するには、次のようにします。

ステップ 1 [MAC アドレステーブル] > [スタティックアドレス] の順にクリックします。

[スタティックアドレス] ページには、現在定義されているスタティック アドレスが含まれます。

ステップ 2 [追加] をクリックします。

ステップ 3 パラメータを入力します。

- [VLAN ID]: ポートの VLAN ID を選択します。
- [MAC アドレス]: インターフェイス MAC アドレスを入力します。
- [インターフェイス]: エントリのインターフェイス(ポート、または LAG)を選択します。
- [ステータス]: エントリの処理方法を選択します。次のオプションがあります。
  - [固定]: システムはこの MAC アドレスを決して削除しません。スタートアップ コンフィギュレーションでスタティック MAC アドレスを保存すると、それは再起動後も保持されます。
  - [リセット時に削除]: デバイスがリセットされると、スタティック MAC アドレスは削除されます。
  - [タイムアウト時に削除]: 期限が切れると、MAC アドレスは削除されます。
  - [セキュア]: インターフェイスが従来のロック モードである場合、MAC アドレスが保護されます(「ポート セキュリティ」を参照)。

ステップ 4 [適用] をクリックします。新しいエントリがテーブルに表示されます。

ダイナミック アドレス

ダイナミック アドレス テーブル(ブリッジング テーブル)には、デバイスに入ってくるフレームの発信元アドレスを監視することにより得られる MAC アドレスが含まれます。

このテーブルのオーバーフローを防いで新しい MAC アドレスを追加する余地を残すために、対応するトラフィックが一定期間(エージング タイム)にわたって受信されないアドレスは削除されます。

ダイナミック アドレスの設定

ダイナミック アドレスのエージング タイム(有効期限)を設定するには、次のようにします。

ステップ 1 [MAC アドレステーブル] > [ダイナミックアドレス設定] の順にクリックします。

ステップ 2 [エージング タイム] を入力します。エージング タイムは、ユーザ設定値から、その値の 2 倍から 1 を引いた値までになります。たとえば、300 秒と入力した場合、エージング タイムは 300 ～ 599 秒になります。

ステップ 3 [適用] をクリックします。エージング タイムが更新されます。

ダイナミック アドレス

ダイナミック アドレスを照会するには、次のようにします。

ステップ 1 [MAC アドレステーブル] > [ダイナミックアドレス] の順にクリックします。

ステップ 2 [フィルタ] ブロックで、次の照会条件を入力できます。

- [VLAN ID]:テーブルで照会する VLAN ID を入力します。
- [MAC アドレス]:テーブルで照会する MAC アドレスを入力します。
- [インターフェイス]:テーブルで照会するインターフェイスを選択します。照会で特定のポート、または LAG を検索することができます。

ステップ 3 [実行] をクリックします。ダイナミック MAC アドレス テーブルが照会され、照会結果が表示されます。

ステップ 4 すべてのダイナミック MAC アドレスを削除するには、[テーブルのクリア] をクリックします。

15

マルチキャスト

ここでは、マルチキャスト転送機能について説明します。具体的な内容は次のとおりです。

- マルチキャスト転送の概要
- プロパティ
- MAC グループ アドレス
- IP マルチキャスト グループ アドレス
- IPv4 マルチキャスト コンフィギュレーション
- IPv6 マルチキャスト コンフィギュレーション
- IGMP/MLD スヌーピング IP マルチキャスト グループ
- マルチキャスト ルータ ポート
- すべて転送
- 未登録マルチキャスト

マルチキャスト転送の概要

マルチキャスト転送機能を利用すれば、「1 対多」型の情報配信を行うことができます。マルチキャスト転送が役に立つのは、情報を多数のクライアントに配信する場合です。各クライアントは、コンテンツ全体を受信する必要はありません。典型的な用途の 1 つにケーブル テレビがあります。ケーブル テレビの場合、クライアントは配信の途中でチャネルの視聴を開始し、配信が終わる前に視聴をやめることができます。

データは受信対象ポートにのみ送信されます。そのため、リンク上の帯域幅とホスト リソースを節約できます。

デフォルトでは、すべてのマルチキャスト フレームが VLAN のすべてのポートにフラッディングされます。プロパティ ページでブリッジ マルチキャスト フィルタリング ステータスを有効にすると、対象ポートにのみマルチキャスト フレームを転送し、それ以外のポートへのマルチキャストはフィルタリング(ドロップ)して、それらのポートにマルチキャスト フレームを転送しないようにすることができます。

フィルタリングを有効にした場合、マルチキャスト フレームは、マルチキャスト転送データベース(MFDB)で定義されている対象 VLAN 上のポートのサブセットに転送されます。マルチキャスト フィルタリングは、すべてのトラフィックに適用されます。

マルチキャスト メンバーを表す一般的な方法は(S,G)表記です。「S」はマルチキャスト ストリーム データの(単一の)送信元、「G」は IPv4 または IPv6 のグループ アドレスを意味します。あるマルチキャスト クライアントが、特定のマルチキャスト グループの任意の送信元からマルチキャスト トラフィックを受信できる場合、これは(*,G)として保存されます。

マルチキャスト フレームの転送方法として、以下のいずれか 1 つを設定できます。

- [MAC グループアドレス]: イーサネット フレーム内の宛先 MAC アドレスに基づいて転送されます。

  注 1 つまたは複数の IP マルチキャスト グループ アドレスが 1 つの MAP アドレスにマッピングされる可能性があります。つまり、MAC グループ アドレスに基づく転送の場合、IP マルチキャスト ストリームが、そのストリームの受信対象でないポートに転送される可能性があります。

- [IP グループアドレス]:IP パケットの宛先 IP アドレスに基づいて転送されます(*,G)。

- [送信元固有 IP グループアドレス]:IP パケットの宛先 IP アドレスと送信元 IP アドレスの両方に基づいて転送されます(S,G)。

IGMPv3 と MLDv2 では、(S,G)がサポートされていますが、IGMPv1/2 と MLDv1 では、(*.G)のみがサポートされています。

このデバイスでは、スタティック マルチキャスト グループ アドレスとダイナミック マルチ キャスト グループ アドレスを合わせて最大 256 個登録できます。

各 VLAN に対して、いずれか 1 つのフィルタリング オプションだけを設定できます。

マルチキャスト転送を行うための一般的な構成

マルチキャスト ルータが IP サブネット間でマルチキャスト パケットをルーティングするのに対し、マルチキャスト対応レイヤ 2 スイッチは、LAN 内または VLAN 内の登録済みノードにマルチキャスト パケットを転送します。

マルチキャスト転送を行うための一般的な構成要素は、プライベート/パブリック IP ネットワーク間でマルチキャスト ストリームを転送するルータ、IGMP/MLD スヌーピング機能を備えたデバイス、およびマルチキャスト ストリームを受信するマルチキャスト クライアントです。この構成では、ルータが IGMP/MLD クエリーを定期的に送信します。

マルチキャストの動作

レイヤ 2 マルチキャスト サービスでは、レイヤ 2 スイッチが、特定のマルチキャスト アドレス宛の 1 つのフレームを受信します。スイッチ上で、各受信対象ポートに送信するため、フレームが複製されます。

IGMP/MLD スヌーピングが有効になっているデバイスは、マルチキャスト ストリームのフレームを受信すると、IGMP/MLD 参加メッセージを使用してマルチキャスト ストリームを受信するよう登録されたすべてのポートにそのマルチキャスト フレームを転送します。

システム上では、各 VLAN に対するマルチキャスト グループのリストが保持されており、各ポートが受信すべきマルチキャスト情報が管理されています。マルチキャスト グループおよびその受信ポートは、静的（スタティック）に設定することも、IGMP または MLD プロトコル スヌーピングを使って動的（ダイナミック）に学習させることもできます。

マルチキャスト登録（IGMP/MLD スヌーピング）

マルチキャスト登録とは、マルチキャスト登録プロトコルを待機して、それに応答するプロセスのことです。使用可能なプロトコルは、IPv4 の場合は IGMP、IPv6 の場合は MLD です。

デバイス上で、ある VLAN に対して IGMP/MLD スヌーピングが有効になっている場合、デバイスに接続されている VLAN およびネットワーク上のマルチキャスト ルータから受信される IGMP/MLD パケットが解析されます。

ホストが IGMP/MLD メッセージを使用してマルチキャスト ストリーム（あるいは特定ソースからのマルチキャスト ストリーム）を受信するよう登録しているということをデバイスが学習すると、その登録情報がデバイスの MFDB に追加されます。

サポートされているバージョンは次のとおりです。

- IGMP v1、v2、v3
- MLD v1、v2

注 このデバイスは、スタティック VLAN に対する IGMP/MLD スヌーピングのみをサポートしています。ダイナミック VLAN に対する IGMP/MLD スヌーピングはサポートしていません。

IGMP/MLD スヌーピングがグローバルに、または特定の VLAN に対して有効になっている場合、すべての IGMP/MLD パケットが CPU に転送されます。CPU では着信パケットが解析され、次の情報が特定されます。

- VLAN 上のマルチキャスト グループへの参加を要求しているポート、および、参加先の VLAN とマルチキャスト グループ。
- IGMP/MLD クエリーを生成しているマルチキャスト ルータ（Mrouter）に接続しているポート。
- PIM、DVMRP、または IGMP/MLD クエリー プロトコルを受信しているポート。

これらの VLAN が [IGMP/MLD スヌーピング IP マルチキャスト グループ] ページに表示されます。

特定のマルチキャスト グループへの参加を要求するポートから、IGMP/MLD 報告メッセージが送信されます。この報告メッセージの中で、ホストがどのグループへの参加を要求しているかが指定されます。この結果、マルチキャスト転送データベースに転送エントリが作成されます。

IGMP スヌーピング クエリア

マルチキャスト ルータが存在しない場合にスヌーピング スイッチのレイヤ 2 マルチキャスト ドメインをサポートするために、IGMP/MLD スヌーピング クエリアが使用されます。たとえば、ローカル サーバによってマルチキャスト コンテンツが提供されても、そのネットワーク上のルータ（存在する場合）がマルチキャストをサポートしないことがあります。

デバイスを、バックアップの IGMP クエリアとして設定したり、正規の IGMP クエリアが存在しない場合に IGMP クエリアとなるよう設定したりすることができます。デバイスは全機能を備えた IGMP クエリアではありません。

IGMP クエリアとして有効になっているデバイスは、マルチキャスト ルータから IGMP トラフィック（クエリー）が検出されない状態が 60 秒経過した後、機能を開始します。他の IGMP クエリアが存在する場合、デバイスは、標準的なクエリア選択プロセスの結果に基づいて、クエリーの送信を停止することも、停止しないこともあります。

IGMP/MLD クエリア アクティビティの速度は、IGMP/MLD スヌーピングが有効になったスイッチと整合する必要があります。スヌーピング テーブル エージング タイムに整合する速度で、クエリーが送信される必要があります。エージング タイムより低い速度でクエリーが送信される場合、サブスクライバはマルチキャスト パケットを受信できません。この操作は [IGMP/MLD スヌーピング IP マルチキャスト グループ] ページで行います。

IGMP/MLD クエリア選出メカニズムが無効になっている場合、IGMP/MLD スヌーピング クエリアは有効化後に一般クエリー メッセージを送る操作を 60 秒間遅らせます。他のクエリアが存在しない場合は、一般クエリー メッセージを送信し始めます。他のクエリアが検出されると、一般クエリー メッセージの送信を停止します。

IGMP/MLD スヌーピング クエリアは、次の間隔で別のクエリアの機能を検出した場合に一般クエリー メッセージの送信を再開します。

クエリー パッシブ間隔 = ロバストネス X クエリー間隔 + 0.5 X クエリー応答間隔

注 VLAN に IPM マルチキャスト ルータが存在する場合は、IGMP/MLD クエリア選出メカニズムを無効にすることを推奨します。

マルチキャスト アドレスの特徴

マルチキャスト アドレスには次の特徴があります。

- IPv4 のマルチキャスト アドレス範囲は、224.0.0.0 ～ 239.255.255.255 です。
- IPv6 のマルチキャスト アドレス範囲は、FF00:/8 です。
- IP マルチキャスト グループ アドレスをレイヤ 2 マルチキャスト アドレスにマッピングするには、次のようにします。
  - IPv4 の場合、IPv4 アドレスの下位 23 ビットを 01:00:5e というプレフィックスの後ろに追加します。標準では、IP アドレスの上位 9 ビットは無視されます。また、マッピングに使用される下位 23 ビットは互いに同じであるため、上位 9 ビットの値だけが異なる IP アドレスは、同じレイヤ 2 アドレスにマッピングされます。たとえば、234.129.2.3 は 01:00:5e:01:02:03 というレイヤ 2 マルチ キャスト グループ アドレスにマッピングされます。最大 32 個の IP マルチキャスト グループ アドレスを、同じレイヤ 2 アドレスにマッピングできます。
  - IPv6 の場合、IPv6 マルチキャスト アドレスの下位 32 ビットを 33:33 というプレフィックスの後ろに追加します。たとえば、IPv6 マルチキャスト アドレス FF00:1122:3344 はレイヤ 2 マルチキャスト アドレス 33:33:11:22:33:44 に マッピングされます。

IGMP/MLD プロキシ

IGMP/MLD プロキシは単純な IP マルチキャスト プロトコルです。

IGMP/MLD プロキシを使用して、エッジ ボックスなどのデバイス上のマルチキャスト トラフィックを複製することで、これらのデバイスの設計と実装が大幅に簡略化される可能性があります。Protocol Independent Multicast（PIM）、ディスタンス ベクター マルチキャスト ルーティング プロトコル（DVMRP）などの複雑なマルチキャスト ルーティング プロトコルをサポートしないことにより、デバイスのコストだけでなく運用上のオーバーヘッドも削減されます。別の利点は、コア ネットワーク ルータで使用されるマルチキャスト ルーティング プロトコルにプロキシ デバイスが依存しないことです。そのため、任意のマルチキャスト ネットワークにプロキシ デバイスを簡単に展開できます。

IGMP/MLD プロキシ ツリー

IGMP/MLD プロキシは、（PIM などの）堅牢なマルチキャスト ルーティング プロトコルの実行を必要としない単純なツリー トポロジで機能します。グループ メンバーシップ情報とプロキシ グループ メンバーシップ情報の学習に基づく単純な IPM ルーティング プロトコルを使用し、その情報に基づいてマルチキャスト パケットを転送するだけで十分です。

各プロキシ デバイスでのアップストリーム インターフェイスとダウンストリーム インターフェイスを指定することにより、手動でツリーを設定する必要があります。さらに、プロキシ ツリー トポロジに適用する IP アドレス指定スキームを設定する際は、プロキシ デバイスが IGMP/MLD クエリア選出で確実に選出されてマルチキャスト トラフィックを転送できるように設定する必要があります。ツリー内にプロキシ デバイス以外の他のマルチキャスト ルータが存在してはならず、ツリーのルートはより広範なマルチキャスト インフラストラクチャに接続されるべきです。

IGMP/MLD に基づく転送を行うプロキシ デバイスには、1 つのアップストリーム インターフェイスと 1 つ以上のダウンストリーム インターフェイスがあります。これらの指定は明示的に行われます。各インターフェイスのタイプを決定するプロトコルは存在しません。プロキシ デバイスはダウンストリーム インターフェイスで IGMP/MLD のルータ部分を実行し、アップストリーム インターフェイスで IGMP/MLD のホスト部分を実行します。

ただ 1 つのツリーを使用できます。

転送ルールとクエリア

次のように転送ルールが適用されます。

- アップストリーム インターフェイスで受信されたマルチキャスト パケットが以下に転送されます。
  - アップストリーム インターフェイス上
  - パケットを要求しているすべてのダウンストリーム インターフェイス上（ただし、プロキシ デバイスがそのインターフェイス上のクエリアである場合のみ）
- ダウンストリーム インターフェイスで受信されたマルチキャスト パケットは、プロキシ デバイスがそのインターフェイスのクエリアでない場合、ドロップされます。
- プロキシ デバイスがクエリアであるダウンストリーム インターフェイスで受信されたマルチキャスト パケットは、アップストリーム インターフェイスに転送され、パケットを要求するすべてのダウンストリーム インターフェイスにも転送されます（ただしプロキシ デバイスがそれらのインターフェイス上のクエリアである場合のみ）。

ダウンストリーム インターフェイスの保護

デフォルトでは、IGMP/MLD ツリーのインターフェイスに到達する IP マルチキャスト トラフィックが転送されます。ダウンストリーム インターフェイスに到達する IP マルチキャスト トラフィックの転送を無効にすることができます。これはグローバルに行うことも、特定のダウンストリーム インターフェイスに対して行うこともできます。

プロパティ

マルチキャスト フィルタリングを有効にしてフォワーディング方式を選択するには、次のようにします。

ステップ 1 [マルチキャスト] > [プロパティ] をクリックします。

ステップ 2 パラメータを入力します。

- [ブリッジマルチキャストフィルタリングステータス]: これを選択するとフィルタリングが有効になります。

- [VLAN ID]:フォワーディング(転送)方式の設定対象となる VLAN ID を選択します。
- [IPv6 用フォワーディング方式]:IPv6 アドレス用に、次のいずれかの転送方式を設定します。
  - [MAC グループアドレス]:MAC マルチキャスト グループ アドレスに従ってパケットを転送します。
  - [IP グループアドレス]:IPv6 マルチキャスト グループ アドレスに従ってパケットを転送します。
  - [送信元固有 IP グループアドレス]:送信元 IPv6 アドレスおよび IPv6 マルチキャスト グループ アドレスに従ってパケットを転送します。VLAN 上に IPv6 アドレスが設定されている場合、IPv6 マルチキャストの動作転送方式は IP グループ アドレスになります。

  注 IPv6 IP グループ アドレスと送信元固有 IP グループ アドレス モードの場合、デバイスは宛先マルチキャスト アドレスの 4 バイトと送信元アドレスの一致のみをチェックします。宛先マルチキャスト アドレスの場合、グループ ID の最後の 4 バイトが照合されます。送信元アドレスの場合、最後の 3 バイトと最後のバイトから 5 番目が照合されます。
- [IPv4 用フォワーディング方式]:IPv4 アドレス用に、次のいずれかの転送方式を設定します。
  - [MAC グループアドレス]:MAC マルチキャスト グループ アドレスに従ってパケットを転送します。
  - [IP グループアドレス]:IPv4 マルチキャスト グループ アドレスに従ってパケットを転送します。
  - [送信元固有 IP グループアドレス]:送信元 IPv4 アドレスおよび IPv4 マルチキャスト グループ アドレスに従ってパケットを転送します。VLAN 上に IPv4 アドレスが設定されている場合、IPv4 マルチキャストの動作転送方式は IP グループ アドレスになります。

ステップ 3 [適用] をクリックします。実行コンフィギュレーション ファイルが更新されます。

MAC グループ アドレス

[MAC グループ アドレス] ページでは、次の操作が可能です。

- 特定の VLAN ID または特定の MAC アドレス グループに関する情報を、マルチキャスト転送データベース(MFDB)から照会して表示できます。この情報は、IGMP/MLD スヌーピング機能によって動的に取得されたもの、または手動で設定したものです。
- 宛先 MAC アドレスに基づく静的な転送情報を設定するスタティック エントリを MFDB に追加したり、エントリを削除したりすることができます。
- 各 VLAN ID および MAC アドレス グループのメンバーであるポート/LAG のリストを表示したり、トラフィックをその VLAN ID および MAC アドレス グループに転送するかどうかを設定できます。

MAC マルチキャスト グループを定義および表示するには、次のようにします。

ステップ 1 [マルチキャスト] > [MAC グループアドレス] をクリックします。

ステップ 2 フィルタ パラメータを入力します。

- [VLAN ID が次に等しい]: 表示するグループの VLAN ID を設定します。
- [MAC グループアドレスが次に等しい]: 表示するマルチキャスト グループの MAC アドレスを設定します。MAC グループ アドレスを指定しない場合、選択した VLAN のすべての MAC グループ アドレスがこのページに含まれます。

ステップ 3 [実行] をクリックすると、MAC マルチキャスト グループが下部に表示されます。

このページと、[IP マルチキャスト グループ アドレス] ページの両方で作成されたエントリが表示されます。IP マルチキャスト グループ アドレス ページで作成されたエントリは、IP アドレスが MAC アドレスに変換されます。

ステップ 4 [追加] をクリックして、スタティック MAC グループ アドレスを追加します。

ステップ 5 パラメータを入力します。

- [VLAN ID]: 新しいマルチキャスト グループの VLAN ID を定義します。
- [MAC グループアドレス]: 新しいマルチキャスト グループの MAC アドレスを定義します。

ステップ 6 [適用] をクリックすると、MAC マルチキャスト グループが実行コンフィギュレーション ファイルに保存されます。

グループ内のインターフェイスに関する登録情報を設定および表示するには、アドレスを選択して [詳細] をクリックします。

このページにあるフィールドは次のとおりです。

- [VLAN ID]: マルチキャスト グループの VLAN ID。
- [MAC グループ アドレス]: グループの MAC アドレス。

ステップ 7 ポートまたは LAG を、[フィルタ]:[インターフェイスタイプ] メニューから選択します。

ステップ 8 [実行] をクリックすると、VLAN のポートまたは LAG のメンバーシップが表示されます。

ステップ 9 各インターフェイスをマルチキャスト グループに関連付ける方法を選択します。

- [スタティック]: インターフェイスがスタティック メンバーとしてマルチキャスト グループに関連付けられます。
- [ダイナミック]: IGMP/MLD スヌーピングの結果としてインターフェイスがマルチキャスト グループに追加されたことを示します。
- [禁止]: このポートがこの VLAN 上のこのマルチキャスト グループに参加できないことを指定します。
- [なし]: このポートが現在、この VLAN 上のこのマルチキャスト グループのメンバーでないことを指定します。

ステップ 10 [適用] をクリックします。実行コンフィギュレーション ファイルが更新されます。

注 [IP マルチキャスト グループ アドレス] ページで作成されたエントリを選択しても、このページでは削除できません。

IP マルチキャスト グループ アドレス

[IP マルチキャストグループアドレス] ページは [MAC グループアドレス] ページに似ていますが、マルチキャスト グループは IP アドレスで識別される点が異なります。

[IP マルチキャストグループアドレス] ページでは、IP マルチキャスト グループを照会したり追加したりできます。

IP マルチキャスト グループを定義および表示するには、次のようにします。

ステップ 1 [マルチキャスト] > [IP マルチキャストグループアドレス] をクリックします。

スヌーピング機能によって学習されたすべての IP マルチキャスト グループ アドレスがこのページに含まれます。

ステップ 2 フィルタリングに必要なパラメータを入力します。

- [VLAN ID が次に等しい]:表示するグループの VLAN ID を定義します。
- [IP バージョンが次に等しい]:IPv6 または IPv4 を選択します。
- [IP マルチキャストグループアドレスが次に等しい]:表示するマルチキャスト グループの IP アドレスを定義します。この値は、転送モードが(S,G)の場合にのみ意味を持ちます。
- [送信元 IP アドレスが次に等しい]:送信元デバイスの IP アドレスを定義します。モードが (S,G) である場合は、送信側 S を入力します。この値と IP グループ アドレスの組み合わせが、表示されるマルチキャスト グループ ID (S,G) になります。モードが (*.G) である場合は「*」と入力します。これは、マルチキャスト グループが宛先でのみ定義されることを意味します。

ステップ 3 [実行] をクリックします。結果が下部に表示されます。

ステップ 4 [追加] をクリックして、スタティック IP マルチキャスト グループ アドレスを追加します。

ステップ 5 パラメータを入力します。

- [VLAN ID]:追加するグループの VLAN ID を定義します。
- [IP バージョン]:IP アドレス タイプを選択します。
- [IP マルチキャストグループアドレス]:新しいマルチキャスト グループの IP アドレスを定義します。
- [送信元固有]:特定の送信元がエントリに含まれることを示し、[送信元 IP アドレス] フィールドのアドレスを追加します。このフィールドを選択しなかった場合、このエントリは(*,G)として定義されます。つまり、送信元 IP アドレスが任意であることを意味します。
- [送信元 IP アドレス]:含める送信元アドレスを定義します。

ステップ 6 [適用] をクリックします。IP マルチキャスト グループが新規に作成され、デバイスが更新されます。

ステップ 7 IP グループ アドレスの登録情報を設定および表示するには、アドレスを選択して [詳細] をクリックします。

ウィンドウの上部に、選択された VLAN ID、IP バージョン、IP マルチキャスト グループ アドレス、および送信元 IP アドレスが読み取り専用で表示されます。フィルタ タイプを選択できます。

- [インターフェイスタイプが次に等しい]:ポートまたは LAG のどちらを表示するかを選択します。

ステップ 8 インターフェイスごとに、関連付けタイプを選択します。選択項目は次のとおりです。

- [スタティック]: インターフェイスがスタティック メンバーとしてマルチキャスト グループに関連付けられます。
- [ダイナミック]: インターフェイスがダイナミック メンバーとしてマルチキャスト グループに関連付けられます。
- [禁止]: このポートがこの VLAN 上のこのグループに参加できないことを指定します。
- [なし]: このポートが現在、この VLAN 上のこのマルチキャスト グループのメンバーでないことを示します。[スタティック] または [禁止] が選択されるまでは、デフォルトで [なし] が選択されています。

ステップ 9 [適用] をクリックします。実行コンフィギュレーション ファイルが更新されます。

IPv4 マルチキャスト コンフィギュレーション

次のページで、IPv4 マルチキャスト コンフィギュレーションを設定します。

- IGMP スヌーピング
- IGMP VLAN 設定

IGMP スヌーピング

選択的な IPv4 マルチキャスト転送を可能にするには、([プロパティ] ページで) ブリッジ マルチキャスト フィルタリング機能を有効にするとともに、([IGMP スヌーピング] ページで) グローバルに、および該当する VLAN ごとに IGMP スヌーピングを有効にする必要があります。

IGMP スヌーピングを有効にし、このデバイスを VLAN での IGMP スヌーピング クエリアとして指定するには、次のようにします。

ステップ 1 [マルチキャスト] > [IPv4 マルチキャストコンフィギュレーション] > [IGMP スヌーピング] をクリックします。

IGMP スヌーピングをグローバルで有効にした場合、デバイスでネットワーク トラフィックが監視され、マルチキャスト トラフィックの受信を要求したホストが特定されます。デバイスで IGMP スヌーピングが実行されるのは、IGMP スヌーピングとブリッジ マルチキャスト フィルタリングの両方が有効になっている場合だけです。

IGMP スヌーピング テーブルが表示されます。表示されたフィールドの説明が下の [編集] ページに表示されます。加えて、次のフィールドが表示されます。

- [IGMP スヌーピングステータス]:IGMP スヌーピングが有効になっているかどうか([管理]) とそれが実際に VLAN 上で動作しているかどうか([動作]) を表示します。
- [IGMP クエリア ステータス]:IGMP クエリアが有効になっているかどうか([管理]) と、それが実際に VLAN 上で動作しているかどうか([動作]) を表示します。

次の機能を有効または無効にします。

- [IGMP スヌーピングステータス]: これを選択すると、すべてのインターフェイスで IGMP スヌーピングがグローバルに有効になります。
- [IGMP クエリア ステータス]: これを選択すると、すべてのインターフェイスで IGMP クエリアがグローバルに有効になります。

ステップ 2 インターフェイス上で IGMP を設定するには、スタティック VLAN を選択して [編集] をクリックします。次のフィールドを入力します。

- [IGMP スヌーピングステータス]: これを選択すると、VLAN で IGMP スヌーピングが有効になります。デバイスでネットワーク トラフィックが監視され、マルチキャスト トラフィックの受信を要求したホストが特定されます。デバイスで IGMP スヌーピングが実行されるのは、IGMP スヌーピングとブリッジ マルチキャスト フィルタリングの両方の機能が有効になっている場合だけです。
- [マルチキャストルータポート自動学習]: これを選択すると、マルチキャスト ルータの自動学習が有効になります。
- [即時脱退]: これを選択すると、スイッチは、脱退メッセージを送信してきたインターフェイスを転送テーブルから削除する際、まず最初に MAC に基づく一般クエリーをそのインターフェイスに送らなくても削除できるようになります。ホストから IGMP グループ脱退メッセージを受け取った場合、システムはテーブル エントリからそのホストのポートを削除します。マルチキャスト ルータからの IGMP クエリーを中継した後、マルチキャスト クライアントから IGMP メンバーシップ報告を受け取らなければ、エントリを定期的に削除します。この機能を有効にすると、デバイス ポートに送信される不要な IGMP トラフィックをブロックするのにかかる時間が短縮されます。

- [最終メンバー クエリー カウンタ]:このデバイスがクエリアとして選出されている場合に、グループ メンバーがこれ以上存在しないとデバイスが判断する基準となる、MLD グループ固有のクエリーの送信回数。この値に達すると、デバイスはグループ メンバーがこれ以上存在しないと見なします。
  - [クエリーロバストネスの使用(x)]:この値は、[MLD VLAN 設定] ページで設定されます。括弧内の数字は現在のクエリー ロバストネス値です。
  - [ユーザ定義]:ユーザ定義値を入力します。
- [IGMP クエリア ステータス]:選択すると、この機能が有効になります。マルチキャスト ルータが存在しない場合には、この機能が必要です。
- [IGMPクエリアバージョン]:IGMP クエリアの選出を有効にするか、無効にするか。IGMP クエリア選出メカニズムが有効になっている場合、IGMP スヌーピング クエリアは、RFC3810 で指定された標準的な IGMP クエリア選出メカニズムをサポートします。

  IGMP クエリア選出メカニズムが無効になっている場合、IGMP スヌーピング クエリアは、有効化された後に一般クエリー メッセージの送信を 60 秒間遅らせ、他のクエリアがなければ一般クエリー メッセージを送信し始めます。他のクエリアを検出すると、一般クエリー メッセージの送信を停止します。IGMP スヌーピング クエリアは、次に示すクエリー パッシブ間隔で別のクエリアの機能を検出した場合、一般クエリー メッセージの送信を再開します。ロバストネス * (クエリー間隔) + 0.5 * クエリー応答間隔
- [IGMPクエリアバージョン]:デバイスがクエリアとして選出された場合に使用する IGMP バージョンを選択します。送信元固有の IP マルチキャスト転送を行うスイッチやマルチキャスト ルータが VLAN 内に存在する場合は、IGMPv3 を選択してください。それ以外の場合は IGMPv2 を選択します。
- [クエリアソース IP アドレス]:送信されるメッセージで使われる、デバイスの送信元インターフェイスを選択します。MLD では、システムによってこのアドレスが自動選択されます。

  注 [自動] オプションが選択されている場合、システムは、発信インターフェイスで定義された IP アドレスからソース IP アドレスを取得します。

ステップ 3 [適用] をクリックします。実行コンフィギュレーション ファイルが更新されます。

注 IGMP スヌーピング タイマー設定(クエリー ロバストネス(堅牢性)、クエリー間隔など)を変更しても、すでに作成済みのタイマーに対しては影響を及ぼしません。

IGMP VLAN 設定

特定の VLAN における IGMP を設定するには、次のようにします。

ステップ 1 [マルチキャスト] > [IPv4 マルチキャストコンフィギュレーション] > [IGMP VLAN 設定] をクリックします。

IGMP が有効になっているそれぞれの VLAN について、次のフィールドが表示されます。

- [クエリー ロバストネス]: リンクで想定されるパケット損失数を入力します。
- [クエリー間隔](秒): このデバイスがクエリアとして選出された場合に使用される、一般クエリーの送信間隔。
- [クエリー最大応答間隔](秒): 定期的な一般クエリーに挿入される最大応答コードを計算するために使われる遅延時間。
- [最終メンバー クエリー間隔(ミリ秒)]: 選出されたクエリアから送られたグループ固有のクエリーの最大応答時間値をデバイスが読み込めない場合に使用される最大応答遅延を入力します。

  しきい値より小さい TTL 値を持つマルチキャスト パケットは、インターフェイスで転送されません。

  デフォルト値は 0 で、すべてのマルチキャスト パケットがインターフェイスで転送されることを意味します。

  値 256 は、どのマルチキャスト パケットもインターフェイスで転送されないことを意味します。

  境界ルータでのみ TTL しきい値を設定してください。逆に言うと、TTL しきい値が設定されたルータは自動的に境界ルータになります。

ステップ 2 インターフェイスを選択し、[編集] をクリックします。上記で説明されたフィールドの値を入力します。

ステップ 3 [適用] をクリックします。実行コンフィギュレーション ファイルが更新されます。

IPv6 マルチキャスト コンフィギュレーション

次のページで、IPv6 マルチキャスト コンフィギュレーションを設定します。

- MLD スヌーピング
- MLD VLAN 設定

MLD スヌーピング

選択的な IPv6 マルチキャスト転送を可能にするには、(プロパティ ページで)ブリッジ マルチキャスト フィルタリング機能を有効にするとともに、MLD スヌーピング ページでグローバルおよび該当する VLAN ごとに MLD スヌーピングを有効にする必要があります。

MLD スヌーピングを有効にして VLAN でそれを設定するには、次のようにします。

ステップ 1 [マルチキャスト] > [IPv6 マルチキャストコンフィギュレーション] > [MLD スヌーピング] をクリックします。

MLD スヌーピング ステータスをグローバルで有効にした場合、デバイス上でネットワーク トラフィックが監視され、マルチキャスト トラフィックの受信を要求したホストが特定されます。デバイスで MLD スヌーピングが実行されるのは、MLD スヌーピングとブリッジ マルチキャスト フィルタリングの両方が有効になっている場合だけです。

MLD スヌーピング テーブルが表示されます。表示されたフィールドの説明が下の [編集] ページに表示されます。加えて、次のフィールドが表示されます。

- [MLD スヌーピング ステータス]:MLD スヌーピングが有効になっているかどうか([管理]) とそれが実際に VLAN 上で動作しているかどうか([動作]) を表示します。
- [MLD クエリア ステータス]:MLD クエリアが有効になっているかどうか([管理]) と、それが実際に VLAN 上で動作しているかどうか([動作]) を表示します。

ステップ 2 次の機能を有効または無効にします。

- [MLD スヌーピング ステータス]: これを選択すると、すべてのインターフェイスで MLD スヌーピングがグローバルに有効になります。
- [MLD クエリア ステータス]: これを選択すると、すべてのインターフェイスで MLD クエリアがグローバルに有効になります。

ステップ 3 インターフェイスでの MLD プロキシを設定するには、スタティック VLAN を選択して [編集] をクリックします。次のフィールドを入力します。

- [MLD スヌーピング ステータス]: これを選択すると、VLAN で MLD スヌーピングが有効になります。デバイスでネットワーク トラフィックが監視され、マルチキャスト トラフィックの受信を要求したホストが特定されます。デバイスで MLD スヌーピングが実行されるのは、MLD スヌーピングとブリッジ マルチキャスト フィルタリングの両方の機能が有効になっている場合だけです。
- [マルチキャスト ルータ ポート自動学習]: これを選択すると、マルチキャスト ルータの自動学習が有効になります。
- [即時脱退]: これを選択すると、スイッチは、脱退メッセージを送信してきたインターフェイスを転送テーブルから削除する際、まず最初に MAC に基づく一般クエリーをそのインターフェイスに送らなくても削除できるようになります。ホストから MLD グループ脱退メッセージを受け取った場合、システムはテーブル エントリからそのホストのポートを削除します。マルチキャスト ルータからの MLD クエリーを中継した後、マルチキャスト クライアントから MLD メンバーシップ報告を受け取らなければ、エントリを定期的に削除します。この機能を有効にすると、デバイス ポートに送信される不要な MLD トラフィックをブロックするのにかかる時間が短縮されます。
- [最終メンバー クエリー カウンタ]: このデバイスがクエリアとして選出されている場合に、グループ メンバーがこれ以上存在しないとデバイスが判断する基準となる、MLD グループ固有のクエリーの送信回数。この値に達すると、デバイスはグループ メンバーがこれ以上存在しないと見なします。
  - [クエリー ロバストネスの使用(x)]: この値は、[MLD VLAN 設定] ページで設定されます。括弧内の数字は現在のクエリー ロバストネス値です。
  - [ユーザ定義]: ユーザ定義値を入力します。
- [MLD クエリア ステータス]: 選択すると、この機能が有効になります。マルチキャスト ルータが存在しない場合には、この機能が必要です。
- [MLD クエリア選出]: MLD クエリアの選出を有効にするか、無効にするか。MLD クエリア選出メカニズムが有効になっている場合、MLD スヌーピング クエリアは、RFC3810 で指定された標準的な MLD クエリア選出メカニズムをサポートします。

  MLD クエリア選出メカニズムが無効になっている場合、MLD スヌーピング クエリアは、有効化された後に一般クエリー メッセージの送信を 60 秒間遅らせ、他のクエリアがなければ一般クエリー メッセージを送信し始めます。他のクエリアを検出すると、一般クエリー メッセージの送信を停止します。MLD スヌーピング クエリアは、次に示すクエリー パッシブ間隔で別のクエリアの機能を検出した場合、一般クエリー メッセージの送信を再開します。ロバストネス * (クエリー間隔) + 0.5 * クエリー応答間隔

- [MLD クエリアバージョン]:デバイスがクエリアとして選出された場合に使用される MLD バージョンを選択します。送信元固有の IP マルチキャスト転送を行うスイッチやマルチキャスト ルータが VLAN 内に存在する場合は、MLDv2 を選択してください。それ以外の場合は MLDv1 を選択します。

ステップ 4 [適用] をクリックします。実行コンフィギュレーション ファイルが更新されます。

注 MLD スヌーピング タイマー設定(クエリー ロバストネス(堅牢性)、クエリー間隔など)を変更しても、すでに作成済みのタイマーに対しては影響を及ぼしません。

MLD VLAN 設定

特定の VLAN における MLD を設定するには、次のようにします。

ステップ 1 [マルチキャスト] > [IPv6 マルチキャストコンフィギュレーション] > [MLD VLAN 設定] をクリックします。

MLD が有効になっているそれぞれの VLAN について、次のフィールドが表示されます。

- [インターフェイス名]:MLD 情報が表示されている対象の VLAN。
- [クエリー ロバストネス]:リンクで想定されるパケット損失数を入力します。
- [クエリー間隔](秒):このデバイスがクエリアとして選出された場合に使用される、一般クエリーの送信間隔。
- [クエリー最大応答間隔](秒):定期的な一般クエリーに挿入される最大応答コードを計算するために使われる遅延時間。
- [最終メンバー クエリー間隔(ミリ秒)]:選出されたクエリアから送られたグループ固有のクエリーの最大応答時間値をデバイスが読み込めない場合に使用される最大応答遅延を入力します。

ステップ 2 VLAN を設定するには、それを選択して [編集] をクリックします。上記に説明されているフィールドに入力します。

ステップ 3 [適用] をクリックします。実行コンフィギュレーション ファイルが更新されます。

IGMP/MLD スヌーピング IP マルチキャスト グループ

[IGMP/MLD スヌーピング IP マルチキャストグループ] ページには、IGMP/MLD メッセージから学習された IPv4 および IPv6 のグループ アドレスが表示されます。

このページに表示される情報は、[MAC グループ アドレス] ページの情報と異なる場合があります。たとえば、システムが MAC に基づくグループに従ってフィルタリングを行っている状況で、あるポートがマルチキャスト グループ 224.1.1.1 および 225.1.1.1 への参加を要求していて、その両方のグループが同じ MAC マルチキャスト アドレス 01:00:5e:01:01:01にマップされているとします。この場合、MAC マルチキャストのページにはエントリが 1 つしか表示されませんが、[IGMP/MLD IP マルチキャストグループ] ページにはエントリが 2 つ表示されます。

IP マルチキャスト グループを照会するには、次のようにします。

ステップ 1 [マルチキャスト] > [IGMP/MLD スヌーピング IP マルチキャスト グループ] をクリックします。

ステップ 2 検索するスヌーピング グループのタイプを設定します(IGMP または MLD)。

ステップ 3 次のクエリー フィルタ基準の一部または全部を指定します。

- [グループアドレスが次に等しい]:照会するマルチキャスト グループの MAC アドレスまたは IP アドレスを定義します。
- [送信元アドレスが次に等しい]:照会する送信側アドレスを指定します。
- [VLAN ID が次に等しい]:照会する VLAN ID を指定します。

ステップ 4 [実行] をクリックします。マルチキャスト グループごとに次のフィールドが表示されます。

- [VLAN ID]:VLAN の ID。
- [グループアドレス]:マルチキャスト グループの MAC アドレスまたは IP アドレス。
- [送信元アドレス]:指定したすべてのグループ ポートに対する送信側アドレス。
- [含まれるポート]:マルチキャスト ストリームの宛先ポートのリスト。
- [除外ポート]:このグループに含まれないポートのリスト。
- [互換モード]:IP グループ アドレスに関してデバイスが受信したホスト登録情報の最も古い IGMP/MLD バージョン。

マルチキャスト ルータ ポート

マルチキャスト ルータ ポートとは、マルチキャスト ルータが接続されているポートのことです。マルチキャスト ストリームおよび IGMP/MLD 登録メッセージを転送するときに、デバイスは(1 つ以上の)マルチキャスト ルータ ポート番号を含めます。マルチキャスト ルータ上でマルチキャスト ストリームを順次転送し、登録メッセージを他のサブネットに伝達するには、マルチキャスト ルータ ポートを設定する必要があります。

マルチキャスト ルータ ポートの静的な設定、または動的な設定の確認を行うには、次のようにします。

ステップ 1 [マルチキャスト] > [マルチキャストルータポート] をクリックします。

ステップ 2 次のクエリー フィルタ基準の一部または全部を指定します。

- [VLAN ID が次に等しい]: 記述されるルータ ポートの VLAN ID を選択します。
- [IP バージョンが次に等しい]: マルチキャスト ルータでサポートされている IP バージョンを選択します。
- [インターフェイスタイプが次に等しい]: ポートまたは LAG のどちらを表示するかを選択します。

ステップ 3 [実行] をクリックします。クエリー基準に一致するインターフェイスが表示されます。

ステップ 4 ポートまたは LAG ごとに、関連付けタイプを選択します。選択項目は次のとおりです。

- [スタティック]: このポートをマルチキャスト ルータ ポートとして静的に設定します。
- [ダイナミック]: (表示のみ) このポートは MLD/IGMP クエリーによってマルチキャスト ルータ ポートとして動的に設定されます。マルチキャスト ルータ ポートの動的学習を有効にするには、[IGMP スヌーピング] ページ、または、[MLD スヌーピング] ページを使用します。
- [禁止]: このポートで IGMP/MLD クエリーが受信された場合でも、このポートをマルチキャスト ルータ ポートとして設定しません。ポートで [禁止] が有効になっている場合、このポートでのマルチキャスト ルータの学習は行われません(つまり、このポートでのマルチキャスト ルータ ポート自動学習が無効になります)。
- [なし]: このポートは現在、マルチキャスト ルータ ポートではありません。

ステップ 5 [適用] をクリックしてデバイスを更新します。

すべて転送

ブリッジ マルチキャスト フィルタリングが有効になっている場合は、登録済みマルチキャスト グループへのマルチキャスト パケットが IGMP スヌーピングと MLD スヌーピングに基づいてポートに転送されます。ブリッジ マルチキャスト フィルタリングが無効になっている場合は、すべてのマルチキャスト パケットが対応する VLAN にフラッディングされます。

[すべて転送] ページでは、特定の VLAN からマルチキャスト ストリームを受信するポートや LAG を設定します。この機能を利用するには、マルチキャスト アドレスの特徴 ページでブリッジ マルチキャスト フィルタリングを有効にする必要があります。無効になっている場合、すべてのマルチキャスト トラフィックがデバイス上のポートにフラッディングされます。

ポートに接続されているデバイスで IGMP または MLD がサポートされていない場合、そのポートに対して全マルチキャスト転送を静的に(手動で)設定できます。

IGMP メッセージと MLD メッセージを除くマルチキャスト パケットは、必ず、[すべて転送] として定義されたポートに転送されます。この設定は、選択した VLAN のメンバーであるポートにのみ影響を与えます。

全マルチキャスト転送を設定するには、次のようにします。

ステップ 1 [マルチキャスト] > [すべて転送] をクリックします。

ステップ 2 次の項目を定義します。

- [VLAN ID が次に等しい]: 表示するポート/LAG の VLAN ID。
- [インターフェイスタイプが次に等しい]: ポートまたは LAG のどちらを表示するかを定義します。

ステップ 3 [実行] をクリックします。すべてのポート /LAG のステータスが表示されます。

ステップ 4 以下を使用して、「すべて転送」として設定するポート/LAG を選択します。

- [スタティック]: このポートはすべてのマルチキャスト ストリームを受信します。
- [禁止]: IGMP/MLD スヌーピングにより、マルチキャスト グループに参加するポートとして指定されている場合でも、このポートはマルチキャスト ストリームを受信できません。
- [なし]: このポートは現在、「すべて転送」ポートではありません。

ステップ 5 [適用] をクリックします。実行コンフィギュレーション ファイルが更新されます。

未登録マルチキャスト

この機能を使用すると、要求(登録)されたマルチキャスト グループだけを受信することができます。ネットワークで送信されるその他の(未登録の)マルチキャストは受信されません。

未登録マルチキャスト フレームは、通常 VLAN 上のすべてのポートに転送されます。

未登録マルチキャスト ストリームを受信または拒否(フィルタリング)するポートを選択できます。この設定は、そのポートがメンバーである(またはメンバーになる予定の)すべての VLAN に対して有効です。

未登録マルチキャスト設定を定義するには、次のようにします。

ステップ 1 [マルチキャスト] > [登録解除済みマルチキャスト] をクリックします。

ステップ 2 [インターフェイスタイプが次に等しい] を選択して、ポートまたは LAG を表示します。

ステップ 3 [実行] をクリックします。

ステップ 4 次の項目を定義します。

- [ポート/LAG]:ポートまたは LAG の ID を表示します。
- 選択したインターフェイスの転送ステータスが表示されます。表示される値は次のとおりです。
  - [フォワーディング]:選択したインターフェイスへの、未登録マルチキャスト フレームのフォワーディングを有効にします。
  - [フィルタリング]:選択したインターフェイスでの、未登録マルチキャスト フレームのフィルタリング(拒否)を有効にします。

ステップ 5 [適用] をクリックします。設定値が保存され、実行コンフィギュレーション ファイルが更新されます。

16

IP コンフィギュレーション

IP インターフェイスのアドレスは、ユーザが手動で割り当てるか、または、DHCP サーバから自動的に割り当てられます。このセクションでは、デバイスの IP アドレスを手動で、またはデバイスを DHCP クライアントにして定義することについて説明します。

ここで説明する内容は次のとおりです。

概要

ジャンボ フレームが無効である場合、トラフィックに関する L3 トラフィック MTU は 1518 バイトに制限されます。

ジャンボ フレームが有効である場合、トラフィックに関する L3 トラフィック MTU は 9000 バイトに制限されます。

工場出荷時の IPv4 インターフェイス設定では、デフォルト VLAN は *DHCPv4* です。つまり、デバイスは DHCPv4 クライアントとして動作し、起動時にデバイスから DHCPv4 要求が送信されます。

DHCPv4 サーバから、IPv4 アドレスが含まれている DHCPv4 応答が受信された場合、デバイスから Address Resolution Protocol（ARP; アドレス解決プロトコル）パケットが送信されます。これにより、一意の IP アドレスが割り当てられます。「IPv4 アドレスが使用中である」という内容の DHCP 応答が受信された場合は、デバイスからその DHCP サーバに DHCPDECLINE メッセージが送信され、続いて、DHCPDISCOVER パケットが再度送信され、DHCP サーバ検出プロセスがやり直されます。

60 秒以内に DHCPv4 応答が受信されなかった場合、デバイスから DHCPDISCOVER クエリーが引き続き送信されると共に、デフォルトの IPv4 アドレス192.168.1.254/24 が使用されます。

同じ IP サブネット上で複数のデバイスによって同じ IP アドレスが使用されている場合、IP アドレス衝突が発生します。IP アドレス衝突が発生した場合、DHCP サーバ上、または、IP アドレスがデバイスと衝突するデバイス上、あるいはその両方で、管理作業を行う必要があります。

デフォルト VLAN に関する IP アドレス割り当てルールは次のとおりです。

- デバイスにスタティック IPv4 アドレスが設定されていない場合、DHCPv4 サーバから応答が受信されるまで、デバイスから DHCPv4 クエリーが送信され続けます。
- デバイスの IP アドレスが変更された場合、Gratuitous ARP パケットがデバイスから VLAN に送信され、IP アドレスが衝突していないかどうかが検査されます。このルールは、デバイスの IP アドレスがデフォルト値に戻された場合にも適用されます。
- DHCP サーバから新しい一意の IP アドレスが割り当てられると、システム ステータス LED が緑で点灯します。スタティック IP アドレスを割り当てた場合も、システム ステータス LED は緑で点灯します。IP アドレス割り当て処理中、および出荷時設定の IP アドレス（192.168.1.254）が使用されている場合、システム ステータス LED は点滅します。
- リース期間終了前にクライアントが DHCPREQUEST メッセージを送信してリース期間を更新しなければならない場合、同様のルールが適用されます。
- 出荷時設定では、スタティック IP アドレスも DHCP サーバから割り当てられた IP アドレスも使用できない場合、デフォルトの IP アドレスが使用されます。デフォルト以外の IP アドレスが使用可能になると、その IP アドレスが自動的に使用されます。デフォルトの IP アドレスは、常に管理 VLAN 上にあります。

デバイスには複数の IP アドレスを設定できます。各 IP アドレスを、指定されたポート、LAG、または VLAN に割り当てることができます。これらの IP アドレスは [IPv4 インターフェイス] ページと [Ipv6 インターフェイス] ページで設定します。デバイスには、対応するインターフェイスからそのすべての IP アドレスにアクセスできます。

事前に定義されたデフォルト ルートは提供されません。デバイスをリモート管理するには、デフォルト ルートを定義する必要があります。DHCP 割り当てのすべてのデフォルト ゲートウェイがデフォルト ルートとして保存されます。さらに、デフォルト ルートを手動で定義することもできます。これは、[IPv4 スタティック ルート] ページと [IPv6 ルータ] ページで定義します。

このガイドでは、デバイスに設定または割り当てられている IP アドレスは、すべて、管理 IP アドレスとして参照しています。

ループバック インターフェイス

概要

ループバック インターフェイスは、動作状態が常にオンになっている仮想インターフェイスです。リモート IP アプリケーションと通信する際にこの仮想インターフェイスで設定されている IP アドレスがローカル アドレスとして使用される場合、リモート アプリケーションまでの実際のルートが変更されたとしても、通信は中断されません。

ループバック インターフェイスの動作状態は常にオンです。IP アドレス（IPv4 か IPv6 のいずれか）を定義し、その IP アドレスを、リモート IP アプリケーションとの IP 通信のローカル IP アドレスとして使用します。リモート アプリケーションが、スイッチのアクティブ（ループバック以外の）IP インターフェイスのいずれか 1 つからアクセス可能である限り、通信はそのまま維持されます。一方、リモート アプリケーションとの通信でいずれかの IP インターフェイスの IP アドレスが使用される場合、その IP インターフェイスがダウンすると通信が終了することになります。

ループバック インターフェイスではブリッジ機能がサポートされておらず、VLAN のメンバーになることはできませんし、レイヤ 2 プロトコルを有効にすることもできません。

IPv6 リンクのローカル インターフェイス ID は 1 です。

ループバック インターフェイスの設定

IPv4 ループバック インターフェイスを設定するには、IPv4 インターフェイスでループバック インターフェイスを追加します。

IPv6 ループバック インターフェイスを設定するには、IPv6 アドレスでループバック インターフェイスを追加します。

IPv4 の管理およびインターフェイス

ここで説明する内容は次のとおりです。

- IPv4 インターフェイス
- IPv4 スタティック ルート
- IPv4 転送テーブル
- RIPv2

- ARP
- ARP プロキシ
- UDP リレー/IP ヘルパー
- DHCP /リレー

IPv4 インターフェイス

Web ベースのコンフィギュレーション ユーティリティを使用してデバイスを管理するには、IPv4 デバイス管理 IP アドレスが定義されていて、かつ、その IP アドレスを知っている必要があります。デバイスの IP アドレスは、手動で割り当てることも、DHCP サーバから自動的に割り当てることもできます。

[IPv4インターフェイス] ページは、デバイス管理用の IP アドレスを設定するために使用します。この IP アドレスは、ポート、LAG、VLAN、ループバック インターフェイス、またはアウトオブバンド インターフェイスに対して設定できます。

デバイスに複数の IP アドレス(インターフェイス)を設定できます。これにより、さまざまなインターフェイス間のトラフィック ルーティングと、リモート ネットワークへのトラフィック ルーティングがサポートされます。一般に(デフォルトでは)ルーティング機能はハードウェアにより実行されます。ハードウェア リソースを使い尽くした場合、またはハードウェアでルーティング テーブルのオーバーフローが発生した場合は、IP ルーティングはソフトウェアにより実行されます。

ハードウェア ルーティングでは、ワイヤ スピードの Layer 3 トラフィック転送が実現しますが、ソフトウェア ルーティングは CPU のキャパシティや、ソフトウェアが実行している他のタスクにより制限されます。

注 デバイスのソフトウェアは、1 つのポートまたは LAG に設定されているすべての IP アドレスに 1 つずつ VLAN ID (VID) を割り当てます。4094 以降で未使用の VID のうち最初のものが採用されます。

IPv4 アドレスを設定するには、次のようにします。

ステップ 1 [IP コンフィギュレーション] > [IPv4 の管理およびインターフェイス] > [IPv4 インターフェイス] をクリックします。

次のフィールドを入力します。

- [IPv4 ルーティング]: IPv4 ルーティングを有効にするには、[有効] ボックスをオンにします(デフォルトで有効になっています)。

- [ハードウェアベースのルーティング]:ハードウェア ベースのルーティングが現在アクティブであるか、またはソフトウェア ベースのルーティングがアクティブであるかを表示します。

ハードウェア ベースのルーティングがアクティブではない場合に有効にするには、[ハードウェアベースのルーティングの再アクティブ化] をクリックします。ハードウェア ベースのルーティングのアクティブ化は、現在のルーティング コンフィギュレーションをサポートするのに使用可能なハードウェア リソースに応じて決まります。

ステップ 2 [適用] をクリックします。パラメータが、実行コンフィギュレーション ファイルに保存されます。

[IPv4 インターフェイス テーブル] に次のフィールドが表示されます。

- [インターフェイス]:IP アドレスが定義されているインターフェイス。これはアウトオブバンド ポートにすることもできます。
- [IP アドレスタイプ]:使用可能なオプションを以下に示します。
  - [DHCP]:DHCP サーバから受信したもの。
  - [スタティック]:手動で入力したもの。スタティック インターフェイスはユーザが作成した非 DHCP インターフェイスです。
  - [デフォルト]:設定の実行前からデフォルトでデバイス上に存在するデフォルト アドレス。
- [IP アドレス]:インターフェイスに設定されている IP アドレス。
- [マスク]:設定されている IP アドレス マスク。
- [ステータス]:IP アドレス重複チェックの結果。
  - [暫定]:IP アドレス重複チェックの最終結果はありません。
  - [有効]:IP アドレスのコリジョン チェックが完了しており、IP アドレスのコリジョンは検出されませんでした。
  - [妥当な重複]:IP アドレス重複チェックが完了しており、IP アドレスの重複が検出されました。
  - [重複]:デフォルト IP アドレスの、IP アドレスの重複が検出されました。
  - [遅延]:DHCP クライアントが始動時に有効なら、DHCP アドレス検出のための時間を取るため、IP アドレスの割り当ては 60 秒間遅延されます。
  - [未受信]:DHCP アドレス関連。DHCP クライアントによる検出プロセスの開始時には、実アドレス取得の前にダミー IP アドレス 0.0.0.0 が割り当てられます。このダミー アドレスのステータスは「未受信」です。

ステップ 3 [追加] をクリックします。

ステップ 4 次のいずれかのフィールドを選択します。

- [インターフェイス]: この IP コンフィギュレーションに関連するインターフェイスとしてポート、LAG、ループバック、または VLAN を選択し、リストからインターフェイスを選択します。
- [IP アドレスタイプ]: 次のいずれかのオプションを選択します。
  - [ダイナミック IP アドレス]: IP アドレスを DHCP サーバから受け取ります。
  - [スタティック IP アドレス]: IP アドレスを入力します。

ステップ 5 [スタティック IP アドレス] が選択されている場合は、次のフィールドに入力します。

- [IP アドレス]: インターフェイスの IP アドレスを入力します。
- **マスク**
  - [ネットワークマスク]: このアドレスの IP マスク。
  - [プレフィックス長]: IPv4 プレフィックスの長さ。

ステップ 6 [適用] をクリックします。IPv4 アドレス設定が実行コンフィギュレーション ファイルに書き込まれます。

IPv4 スタティック ルート

このページでは、デバイス上の IPv4 スタティック ルートの設定と表示を実行できます。トラフィックのルーティング時、ネクスト ホップはプレフィックスの最長一致に従って決定されます(LPM アルゴリズム)。1 つの宛先 IPv4 アドレスが、IPv4 スタティック ルート テーブルの複数のルートに一致する可能性があります。デバイスで使用されるのは、サブネット マスクが最も高いルート、つまりプレフィックス最長一致です。複数のデフォルト ゲートウェイが同じメトリック値で定義されている場合は、設定されているすべてのデフォルト ゲートウェイのうち最も低い IPv4 アドレスが使用されます。

IP スタティック ルートを定義するには、次のようにします。

ステップ 1 [IP コンフィギュレーション] > [IPv4 の管理およびインターフェイス] > [IPv4 スタティック ルート] の順にクリックします。

IPv4 スタティック ルート テーブルが表示されます。エントリごとに次のフィールドが表示されます。

- [送信先 IP プレフィックス]:宛先 IP アドレス プレフィックス。
- [プレフィックス長]:宛先 IP の IP ルート プレフィックス。
- [ルート タイプ]:ルートは拒否ルート、リモート ルートのうちどれか。
- [ネクスト ホップ ルータ IP アドレス]:ルート上のネクスト ホップ IP アドレスまたは IP エイリアス。
- [メトリック]:このホップのコスト(低い値ほど良い)。
- [送信インターフェイス]:このルートの送信インターフェイス。

注 ルーティング エントリの IP SLA オブジェクト トラッキング ID を定義すると、指定されたネクスト ホップ経由でリモート ネットワークへの接続がチェックされます。接続が存在しない場合は、オブジェクト トラック ステータスがダウンに設定され、ルータが転送テーブルから削除されます(「IP コンフィギュレーション」の項で詳細を確認してください)。

ステップ 2 [追加] をクリックします。

ステップ 3 次のフィールドに値を入力します。

- [送信先 IP プレフィックス]:宛先 IP アドレス プレフィックスを入力します。
- [マスク]:以下を選択して入力します。
  - [ネットワーク マスク]:マスク形式の、宛先 IP の IP ルート プレフィックス(ルート ネットワーク アドレス内のビット数)。
  - [プレフィックス長]:IP アドレス形式の、宛先 IP の IP ルート プレフィックス。
- [ルート タイプ]:ルート タイプを選択します。
  - [拒否]:ルートを拒否し、すべてのゲートウェイを通じた宛先ネットワークへのルーティングを停止します。これにより、このルートの宛先 IP が指定されたフレームが着信した場合、ドロップされます。この値を選択すると、以下の制御が無効になります。ネクスト ホップ IP アドレス、メトリック、および IP SLA トラック。

- [リモート]:このルートがリモート パスであることを示します。

- [ネクストホップルータ IP アドレス]:ルート上のネクスト ホップ ルータ IP アドレスまたは IP エイリアスを入力します。

  注 デバイスが DHCP サーバから IP アドレスを取得する場合、直接接続 IP サブネットを通じてスタティック ルートを設定することはできません。

- [メトリック]:ネクスト ホップへの管理距離を入力します。範囲は 1～255 です。

ステップ 4 [適用] をクリックします。IP スタティック ルートが、実行コンフィギュレーション ファイルに保存されます。

IPv4 転送テーブル

IPv4 転送テーブルを表示するには、次のようにします。

ステップ 1 [IP コンフィギュレーション] > [IPv4 の管理およびインターフェイス] > [IPv4 転送テーブル] の順にクリックします。

IPv4 転送テーブルが表示されます。エントリごとに次のフィールドが表示されます。

- [送信先 IP プレフィックス]:宛先 IP アドレス プレフィックス。
- [プレフィックス長]:宛先 IP の IP ルート プレフィックスの長さ。
- [ルート タイプ]:ルートはローカル ルート、拒否ルート、リモート ルートのうちどれか。
- [ネクスト ホップ ルータ IP アドレス]:ネクスト ホップ IP アドレス。
- [ルート オーナー]:以下のオプションのうちのいずれか 1 つ。
  - [デフォルト]:デフォルト システム コンフィギュレーションによって設定されたルート。
  - [スタティック]:手動で作成されたルート。
  - [ダイナミック]:IP ルーティング プロトコルによって作成されたルート。
  - [DHCP]:DHCP サーバから受け取ったルート。
  - [直接接続]:デバイスが接続されるサブネット。
- [メトリック]:このホップのコスト(低い値ほど良い)。

- [管理ステータス]: ネクスト ホップまでの管理距離（低い値ほど良い）。これは、スタティック ルートには関係ありません。
- [送信インターフェイス]: このルートの送信インターフェイス。

ARP

このデバイスには、直接接続されている IP サブネット上にある既知のデバイスがすべて登録された、Address Resolution Protocol（ARP）テーブルが保持されています。直接接続されている IP サブネットとは、デバイスの IPv4 インターフェイスが接続されているサブネットのことです。デバイスでローカル デバイスにパケットを送信またはルーティングすることが必要な場合、ARP テーブルが検索され、そのデバイスの MAC アドレスが取得されます。ARP テーブルには、スタティック アドレスとダイナミック アドレスの両方が登録されます。スタティック アドレスとは、手動で割り当てられたアドレスのことであり、有効期間がありません。デバイス上では、受信された ARP パケットからダイナミック アドレスが生成されます。ダイナミック アドレスには有効期間が設定されています。

注 生成されたトラフィックの転送に加えて、ルーティングでもマッピング情報が使用されます。

ARP テーブルを定義するには、次のようにします。

ステップ 1 [IP コンフィギュレーション] > [IPv4 の管理およびインターフェイス] > [ARP] をクリックします。

ステップ 2 パラメータを入力します。

- [ARP エントリのエージング アウト]: ARP テーブル内でダイナミック アドレスを保持する期間（単位: 秒）を入力します。テーブルに登録されている期間が ARP エントリのエージング アウトの時間を超えると、そのダイナミック アドレスは期限切れになります。期限切れになったダイナミック アドレスは ARP テーブルから削除されます。再学習された場合のみ、再登録されます。
- [ARP テーブル エントリのクリア]: システムから削除する ARP エントリのタイプを選択します。
  - [すべて]: すべてのスタティック アドレスとすべてのダイナミック アドレスを今すぐ削除します。
  - [ダイナミック]: すべてのダイナミック アドレスを今すぐ削除します。
  - [スタティック]: すべてのスタティック アドレスを今すぐ削除します。
  - [標準エージング アウト]: [ARP エントリのエージング アウト] で指定した期間に基づいてダイナミック アドレスを削除します。

ステップ 3 [適用] をクリックします。ARP グローバル設定が実行コンフィギュレーション ファイルに書き込まれます。

ARP テーブルに表示されるフィールドは次のとおりです。

- [インターフェイス]:IP デバイスが存在する直接接続されている IP サブネットに対する、IPv4 インターフェイス。
- [IP アドレス]:IP デバイスの IP アドレス。
- [MAC アドレス]:IP デバイスの MAC アドレス。
- [ステータス]:エントリが手動で入力されたか、動的に学習されたか。

ステップ 4 [追加] をクリックします。

ステップ 5 パラメータを入力します。

- [IP バージョン]:このホストでサポートされている IP アドレス形式。サポートされているのは IPv4 だけです。
- [インターフェイス]:IPv4 インターフェイスをポート、LAG、または VLAN 上に設定することができます。デバイス上で設定されている IPv4 インターフェイスのリストから、目的のインターフェイスを選択します。
- [IP アドレス]:ローカル デバイスの IP アドレスを入力します。
- [MAC アドレス]:ローカル デバイスの MAC アドレスを入力します。

ステップ 6 [適用] をクリックします。ARP エントリが、実行コンフィギュレーション ファイルに保存されます。

ARP プロキシ

プロキシ ARP のテクニックは、特定の IP サブネット上のデバイスにより、ネットワーク上にないネットワーク アドレスについて問い合わせる ARP クエリーに応答するために使用されます。

注 ARP プロキシ機能は、デバイスが L3 モードの場合にのみ使用できます。

ARP プロキシでは、トラフィックの宛先が認識されており、応答で別の MAC アドレスが提供されます。別のホストの ARP プロキシとして動作すると、LAN トラフィックの宛先を効率的にそのホストに向けられます。一般的には、そのようにして検出されたトラフィックは、別のインターフェイスを使用して、またはトンネルを使用して、プロキシによって意図された宛先へルーティングされます。

プロキシの動作のために異なる IP アドレスを求める ARP クエリー要求が出されて、ノードが自分の MAC アドレスで応答するというプロセスは、パブリッシングと呼ばれることがあります。

すべての IP インターフェイス上で ARP プロキシを有効にするには、次のようにします。

ステップ 1 [IP コンフィギュレーション] > [IPv4 の管理およびインターフェイス] > [ARP プロキシ] をクリックします。

ステップ 2 [ARP プロキシ] を選択することにより、リモート ノードを求める ARP 要求に対してデバイスが、デバイス MAC アドレスで応答できるようにします。

ステップ 3 [適用] をクリックします。ARP プロキシが有効になり、実行コンフィギュレーション ファイルが更新されます。

UDP リレー/IP ヘルパー

一般にスイッチは、IP サブネット間の IP ブロードキャスト パケットのルーティングを行いません。しかし、この機能によりデバイスは、IPv4 インターフェイスから受け取った特定の UDP ブロードキャスト パケットを、特定の宛先 IP アドレスにリレーできるようになります。

特定の UDP ポートを宛先とする UDP パケットを特定の IPv4 インターフェイスから受け取った場合のリレー処理を設定するには、UDP リレーを追加します。

ステップ 1 [IP コンフィギュレーション] > [IPv4 の管理およびインターフェイス] > [UDP リレー/IP ヘルパー] をクリックします。

ステップ 2 [追加] をクリックします。

ステップ 3 デバイスが UDP ブロードキャスト パケットを、設定されている UDP 宛先ポートに基づいてリレーする先の [送信元 IP インターフェイス] を選択します。そのインターフェイスは、デバイス上で設定されている IPv4 インターフェイスのうちの 1 つでなければなりません。

ステップ 4 デバイスがリレーするパケットの [UDP 宛先ポート] の番号を入力します。ドロップダウン リストからウェルノウン ポートを 1 つ選択するか、またはポート ラジオ ボタンをクリックして手動で番号を入力します。

ステップ 5 UDP パケット リレーを受信する [宛先 IP アドレス] を入力します。このフィールドが 0.0.0.0 の場合、UDP パケットは破棄されます。このフィールドが 255.255.255.255 の場合、UDP パケットはすべての IP インターフェイスにフラッディングされます。

ステップ 6 [適用] をクリックします。UDP リレー設定が実行コンフィギュレーション ファイルに書き込まれます。

DHCP /リレー

ここで説明する内容は次のとおりです。

- 概要
- プロパティ

DHCPv4 リレーの概要

DHCP リレーは、DHCP パケットを DHCP サーバにリレーします。

デバイスは、IP アドレスが設定されていない VLAN から受信した DHCP メッセージをリレーすることができます。IP アドレスのない VLAN 上で DHCP リレーが有効になっているなら、常にオプション 82 が自動的に挿入されます。この挿入は特定の VLAN においてなされるものであり、オプション 82 挿入のグローバル管理状態には影響しません。

正規の DHCP リレーの場合、

- DHCP リレーを有効にします。

プロパティ

DHCP リレーを設定するには、次のようにします。

ステップ 1 [IP コンフィギュレーション] > [IPv4 の管理およびインターフェイス] > [DHCP スヌーピング/リレー] > [プロパティ] をクリックします。

次のフィールドを入力します。

- [DHCPリレー]: DHCP リレーを有効にする場合に選択します。

ステップ 2 [適用] をクリックします。設定が実行コンフィギュレーション ファイルに書き込まれます。

ステップ 3 DHCP サーバを定義するには、[追加] をクリックします。

ステップ 4 DHCP サーバの IP アドレスを入力し、[適用] をクリックします。設定が実行コンフィギュレーション ファイルに書き込まれます。

インターフェイス設定

すべてのインターフェイスまたは VLAN で DHCP リレーを有効化できます。DHCP リレーを機能させるには、VLAN またはインターフェイスに IP アドレスを設定する必要があります。

特定のインターフェイス上で DHCP リレーを有効にするには、次のようにします。

ステップ 1 [IP コンフィギュレーション] > [IPv4 の管理およびインターフェイス] > [DHCP リレー] > [インターフェイス設定] をクリックします。

ステップ 2 インターフェイス上で DHCP リレーを有効にするには、[追加] をクリックします。

ステップ 3 有効にするインターフェイスと機能を選択します。[DHCP リレー]。

ステップ 4 [適用] をクリックします。設定が実行コンフィギュレーション ファイルに書き込まれます。

IPv6 の管理およびインターフェイス

ここで説明する内容は次のとおりです。

- 概要
- IPv6 グローバル コンフィギュレーション
- Ipv6 インターフェイス
- IPv6 トンネル
- IPv6 アドレス
- IPv6 ルータの設定
- IPv6 デフォルト ルータ リスト
- IPv6 ネイバー
- IPv6 プレフィックス リスト
- IPv6 ルータ
- DHCPv6 リレー

概要

Internet Protocol version 6（IPv6）は、パケット交換インターネットワーク用のネットワーク層プロトコルです。IPv6 は、広く普及している IPv4 の後継プロトコルとして策定されました。

IPv6 ではアドレス長が 32 ビットから 128 ビットに拡張されたので、アドレス割り当ての柔軟性が大幅に向上しています。IPv6 アドレスは、4 桁の 16 進数のグループ 8 個で記述します（たとえば、FE80:0000:0000:0000:0000:9C00:876A:130B）。すべての桁が 0 であるグループを「::」に置き換えた、短縮形で記述することもできます（たとえば、FE80::9C00:876A:130B）。

IPv4 しか使用できないネットワーク上で IPv6 ノードどうしが通信するには、途中でマッピングする技術が必要です。この技術をトンネルと呼びます。トンネルを使用すれば、IPv6 にしか対応していないホストでも IPv4 サービスを利用できます。また、孤立した IPv6 ホストおよび IPv6 ネットワークが IPv4 インフラストラクチャ上で他の IPv6 ノードと通信できます。

トンネルでは、ISATAP または手動メカニズムのどちらかが使用されます（IPv6 トンネルを参照）。トンネルでは、IPv4 ネット ワークが仮想 IPv6 ローカル リンクとして扱われ、各 IPv4 アドレスがこのローカル リンク上の IPv6 アドレスにマッピングされます。

このデバイスでは、IPv6 フレームを検出する際、フレームの EtherType が IPv6 であるかどうかが検査されます。

IPv4 ルーティングの場合と同じ方法で、デバイスの MAC アドレスに宛てられたものの、デバイスには認識されていない IPv6 アドレスに宛てられたフレームは、ネクスト ホップ デバイスに転送されます。そのデバイスは、ターゲット端末であるか、または宛先により近いルータの場合があります。転送メカニズムにより、（実質的に）未変更の受信された L3 パケットを含む L2 フレームが再構築され、ネクスト ホップ デバイスの MAC アドレスが宛先 MAC アドレスとなります。

システムによりスタティック ルーティングおよびネイバー ディスカバリのメッセージ（IPv4 ARP メッセージに類似のもの）が使用されて、適切な転送テーブルとネクスト ホップ アドレスが構築されます。

ルートは、2 つのネットワーク デバイスの間の経路を定義するものです。ユーザによって追加されるルーティング エントリはスタティックであり、ユーザが明示的に削除するまでシステムによって保持されて使用されます。それらは、ルーティング プロトコルでは変更されません。スタティック ルートを更新する必要がある場合、それはユーザによって明示的に実行されなければなりません。ネットワーク内にルーティング ループが発生しないようにすることはユーザの責任です。

スタティック IPv6 ルートは、以下のいずれかです。

- 直接接続。この場合、宛先はデバイス上のインターフェイスに直接接続され、パケット宛先（インターフェイス）がネクスト ホップ アドレスとして使用されます。
- 再帰的。ネクスト ホップのみ指定され、発信インターフェイスはそのネクスト ホップから派生します。

同じように、ネクスト ホップ デバイス（直接接続エンド システムを含む）の MAC アドレスは、ネットワーク ディスカバリを使用して自動的に派生します。しかしこれは、ネイバー テーブルに手動でエントリを追加することにより、ユーザによってオーバーライドおよび補足されることがあります。

IPv6 グローバル コンフィギュレーション

IPv6 グローバル パラメータおよび DHCPv6 クライアントの設定値を定義するには、次のようにします。

ステップ 1 [IP コンフィギュレーション] > [IPv6 の管理とインターフェイス] > [IPv6グローバル コンフィギュレーション] をクリックします。

ステップ 2 次のフィールドに値を入力します。

- [IPv6 ルーティング]: これを選択すると、IPv6 ルーティングが有効になります。これが有効になっていない場合、デバイスは（ルータではなく）ホストとして動作し、管理パケットは受信できますが、パケットの送信はできなくなります。ルーティングが有効の場合、デバイスによる IPv6 パケット送信が可能です。

  IPv6 ルーティングを有効にすると、ネットワーク内のルータから送信された RA からオートコンフィグ操作を介してデバイス インターフェイスに割り当てられたすべてのアドレスが削除されます。
- [ICMPv6 レート制限間隔]: ICMP エラー メッセージの生成頻度を入力します。
- [ICMPv6 レート制限バケットサイズ]: 間隔ごとにデバイスから送信できる ICMP エラー メッセージの最大件数を入力します。
- [IPv6ホップ制限]: パケットを渡す先となる最終宛先までの途上にある中間ルータの最大数を入力します。パケットが別のルータに転送されるたびに、ホップ制限が小さくなっていきます。ホップ制限がゼロになった時点で、パケットが破棄されます。これにより、パケットが無限に転送され続ける事態が回避されます。

- [DHCPv6 クライアント設定]
  - [固有 ID (DUID) 形式]: これは、DHCP サーバによりクライアントを検索するために使用される DHCP クライアントの識別子です。以下の形式のいずれかを使用できます。

    [リンク レイヤ]: (デフォルト)。このオプションを選択した場合、デバイスの MAC アドレスが使用されます。

    [エンタープライズ番号]: このオプションを選択した場合、以下のフィールドを入力します。
  - [エンタープライズ番号]: ベンダーにより IANA によって管理されている民間企業番号が登録されています。
  - [ID]: ベンダー定義の 16 進ストリング (16 進文字 64 桁以下)。文字数が偶数でない場合、右端にゼロが追加されます。16 進文字は、2 文字ごとにピリオドまたはコロンで区切ることができます。
- [DHCPv6 固有 ID (DUID)]: 選択されている識別子が表示されます。

ステップ 3 [適用] をクリックします。IPv6 グローバル パラメータおよび DHCPv6 クライアントの設定値が更新されます。

Ipv6 インターフェイス

IPv6 インターフェイスは、ポート、LAG、VLAN、ループバック インターフェイス、またはトンネルに設定できます。

他のタイプのインターフェイスとは異なり、トンネル インターフェイスは [IPv6 トンネル] ページで最初に作成された後、そのページの中でトンネルに IPv6 インターフェイスが設定されます。

IPv6 インターフェイスを定義するには、次のようにします。

ステップ 1 [IP コンフィギュレーション] > [IPv6 の管理およびインターフェイス] > [IPv6 インターフェイス] をクリックします。

ステップ 2 パラメータを入力します。

- [IPv6 リンクローカルのデフォルトゾーン]: デフォルト ゾーンを定義する機能を有効にする場合に選択します。これは、指定されたインターフェイスなしで、またはデフォルト ゾーン 0 で着信するリンク ローカル パケットを発信するために使用するインターフェイスです。

- [IPv6 リンク ローカルのデフォルトゾーンインターフェイス]:デフォルト ゾーンとして使用するインターフェイスを選択します。これは、それ以前に定義されたトンネルまたはその他のインターフェイスにすることが可能です。

ステップ 3 [適用] をクリックして、デフォルト ゾーンを設定します。

IPv6 インターフェイス テーブルは次のフィールドと一緒に表示されます。

- [トンネル タイプ]:[手動]、[6 to 4]、および [ISATAP] 。

ステップ 4 [追加] をクリックして、インターフェイス IPv6 を有効にする新しいインターフェイスを追加します。

ステップ 5 次のフィールドを入力します。

- [IPv6 インターフェイス]:IPv6 アドレスの特定のポート、LAG、ループバック インターフェイス、または VLAN を選択します。

ステップ 6 インターフェイスを DHCPv6 クライアントとして設定して、インターフェイスが DHCPv6 サーバからSNTP コンフィギュレーションや DNS 情報などの情報を受信できるようにするには、以下の [DHCPv6 クライアント] フィールドを入力します。

- [DHCPv6 クライアント]: インターフェイス上で DHCPv6 クライアント(ステートレスおよびステートフル)を有効にする場合に選択します。
- [高速コメント]:アドレス割り当てとその他の設定に対する 2 メッセージ交換の使用を有効にする場合に選択します。これが有効になっている場合は、クライアントが要請メッセージに高速コミット オプションを含めます。
- [情報の最小更新時間]: この値は、更新時間値の最小値を規定するために使用されます。サーバから送信される更新時間オプションがこの値未満の場合、この値が使用されることになります。[無制限](サーバがこのオプションを送信するのでない限り更新されない)を選択するか、または [ユーザ定義] を選択して値を設定します。
- [情報更新時間]: この値は、DHCPv6 サーバから受信する情報をデバイスが更新する頻度を示します。このオプションがサーバから受信されない場合、ここに入力した値が使用されます。[無制限](サーバがこのオプションを送信するのでない限り更新されない)を選択するか、または [ユーザ定義] を選択して値を設定します。

ステップ 7 付加的な IPv6 パラメータを設定するには、以下のフィールドを入力します。

- [IPv6 アドレス自動コンフィギュレーション]: ネイバーによって送信されるルータ アドバタイズメントからの自動アドレス コンフィギュレーションを有効にする場合に選択します。

- [DAD 試行回数]: このインターフェイスのユニキャスト IPv6 アドレスに対して Duplicate Address Detection（DAD; 重複アドレス検出）処理を実行しているときに送信する、ネイバー送信要求メッセージの件数を入力します。DAD は、ユニキャスト IPv6 アドレスを新規に割り当てる前に、そのアドレスが重複していないかどうかを検査する処理です。DAD 処理中、新規アドレスは仮割り当て状態になります。「**0**」を入力した場合、このインターフェイスに対する DAD 処理は無効になります。「**1**」を入力した場合、メッセージは 1 回だけ送信されます。
- [ICMPv6 メッセージの送信]: 宛先到達不能メッセージを生成します。
- [IPv6 リダイレクト]: ICMP IPv6 リダイレクト メッセージの送信を有効にする場合に選択します。それらのメッセージは、他のデバイスに対して、そのデバイスにはトラフィックを送信せず、別のデバイスに送信するように通知します。

ステップ 8 [適用] をクリックし、選択したインターフェイス上での IPv6 処理を有効にします。正規の IPv6 インターフェイスには、次のアドレスが自動的に割り当てられます。

- リンク ローカル アドレス。インターフェイス ID 部はデバイスの MAC アドレスから生成され、EUI-64 形式になっています。
- すべてのノード リンク ローカル マルチキャスト アドレス（「FF02::1」）。
- 送信要求ノード マルチキャスト アドレス。形式は「FF02::1:FFXX:X」です。

ステップ 9 [再起動] ボタンを押して、DHCPv6 サーバから受信されるステートレス情報の更新を開始します。

ステップ 10 必要なら [IPv6 アドレス テーブル] をクリックし、インターフェイスに IPv6 アドレスを手動で割り当てます。このページについては、IPv6 アドレスセクションで説明されています。

ステップ 11 トンネルを追加するには、IPv6 トンネル テーブルの中で（[Ipv6 インターフェイス] ページでトンネルとして定義されている）インターフェイスを選択して、[IPv6 トンネル] をクリックします。「IPv6 トンネル」を参照してください。

DHCPv6 クライアント詳細

[詳細] ボタンを押すと、インターフェイスで DHCPv6 サーバから受信する情報が表示されます。

これは、選択されているインターフェイスが DHCPv6 ステートレス クライアントとして定義されている場合にアクティブです。

ボタンが押された場合、以下のフィールドが表示されます(DHCP サーバから受信された情報の場合)。

- [DHCP 動作モード]: ここには、以下の条件が満たされている場合に [有効] と表示されます。
  - インターフェイスが有効。
  - その上で IPv6 が有効。
  - その上で DHCPv6 クライアントが有効。
- [ステートフル サービス状態]: クライアントで DHCP サーバからステートフル コンフィギュレーション情報を受信するようにします。
- [ステートレス サービス状態]: クライアントで DHCP サーバからステートレス コンフィギュレーション情報を受信するようにします。
- [IPv6 アドレス IA NA]: IA ID にタグの C/IANAID、T1-C/T1、T2、- C/T2 の値が設定されます。T1 と T2 は、少なくとも 1 つのアドレスがインターフェイス上で受信されたときに使用可能になります。
- [DHCP サーバ アドレス]: DHCPv6 サーバのアドレス。
- [DHCP サーバ DUID]: DHCPv6 サーバの固有識別子。
- [DHCP サーバプリファレンス]: この DHCPv6 サーバの優先度。
- [情報の最小更新時間]: 上記参照。
- [情報更新時間]: 上記参照。
- [受信した情報更新時間]: DHCPv6 サーバから受信した更新時間。
- [残りの情報更新時間]: 次の更新までの残り時間。
- [DNS サーバ]: DHCPv6 サーバから受信した DNS サーバのリスト。
- [DNS ドメイン検索リスト]: DHCPv6 サーバから受信したドメインのリスト。
- [SNTP サーバ]: DHCPv6 サーバから受信した SNTP サーバのリスト。
- [POSIXタイムゾーン文字列]: DHCPv6 サーバから受信したタイムゾーン。
- [コンフィギュレーション サーバ]: DHCPv6 サーバから受信したコンフィギュレーション ファイルを含むサーバ。
- [コンフィギュレーション ファイル名]: DHCPv6 サーバから受信したコンフィギュレーション サーバ上のコンフィギュレーション ファイルのパス。

IPv6 トンネル

トンネルにより、IPv4 ネットワークを通じた IPv6 パケットの転送が可能になります。各トンネルには送信元 IPv4 アドレスがあり、手動トンネルの場合は宛先 IPv4 アドレスもあります。それらのアドレスの間では、IPv6 パケットがカプセル化されます。

ISATAP トンネル

デバイスは、1 つの Intra-Site Automatic Tunnel Addressing Protocol（ISATAP）トンネルをサポートしています。

ISATAP トンネルは、ポイントツーマルチポイント トンネルです。送信元アドレスは、デバイスの IPv4 アドレス（または IPv4 アドレスの 1 つ）です。

ISATAP トンネルを設定する際、宛先 IPv4 アドレスがルータにより提供されます。次のことに注意してください。

- リンク ローカル IPv6 アドレスが、ISATAP インターフェイスに割り当てられます。最初の IP アドレスが ISATAP インターフェイスに割り当てられると、その ISATAP インターフェイスがアクティブ化されます。
- ISATAP インターフェイスがアクティブ化されている場合、ISATAP と IPv4 がマッピングされ、DNS プロセスによって ISATAP ルータの IPv4 アドレスが解決されます。ISATAP DNS レコードが解決されない場合、ホスト マッピング テーブル内の、ISATAP ホストの名前とアドレスのマッピングが検索されます。
- ISATAP ルータの IPv4 アドレスが DNS プロセスで解決されない場合、ISATAP IP インターフェイスはアクティブ化されたままになります。DNS プロセスでアドレスが解決されるまで、ISATAP トラフィックを処理するためのデフォルト ルータは設定されません。

トンネルの設定

IPv6 トンネルを設定するには、次のようにします。

ステップ 1 [IP コンフィギュレーション] > [IPv6 の管理およびインターフェイス] > [IPv6トンネル] をクリックします。

ステップ 2 [ISATAPトンネルの作成] をクリックします。

ステップ 3 [トンネル番号] と [トンネル タイプ]:1 と ISATAP が表示されます。

ステップ 4 次のフィールドを入力します。

- [送信元 IPv4 アドレス]:トンネル インターフェイスのローカル(送信元)IPv4 アドレスを設定します。選択された IPv4 インターフェイスに割り当てられている IPv4 アドレス。この IPv4 アドレスは、ISATAP トンネル インターフェイスに割り当てる IPv6 アドレスの一部となります。IPv6 アドレスの上位 64 ビットはネットワーク プレフィックス部(「fe80::」)であり、下位 64 ビットは「0000:5EFE」と IPv4 アドレスで構成されます。
  - [自動]:トンネル インターフェイスで送信されるパケットの送信元アドレスとして設定済みのすべての IPv4 インターフェイスの中から、最も小さい IPv4 アドレスが自動選択されます。
  - [手動]:トンネル インターフェイス上で送信されるパケットの送信元アドレスとして使用する IPv4 アドレスを指定します。IPv4 アドレスが別のインターフェイスに移っても、トンネル インターフェイスのローカル アドレスは変わりません。

    注 デバイスの IPv4 アドレスが変化すると、トンネル インターフェイスのローカル アドレスも変化します。
  - [インターフェイス]:送信元インターフェイスを選択します。
- [ISATAP ルータ名]:特定の自動トンネル ルータ ドメイン名を表すグローバル ストリングを設定するには、以下のいずれかのオプションを選択します。
  - [デフォルトを使用]:常に ISATAP です。
  - [ユーザ定義]:ルータのドメイン名を入力します。

ステップ 5 パラメータを入力します。

- [ISATAP 送信要求間隔]:アクティブ化された ISATAP ルータが検出されない場合に、ISATAP ルータに送信要求メッセージを送信する間隔(秒数)を入力します。**デフォルト値**をそのまま使用するか、または**ユーザ定義値**を使用することができます。
- [ISATAP ロバストネス]:対ルータ送信要求クエリーの送信間隔を計算する際に使用されます。値が大きいほど、クエリー送信頻度が高くなります。**デフォルト値**をそのまま使用するか、または**ユーザ定義値**を使用することができます。

  注 IPv4 インターフェイスが動作していない場合、ISATAP トンネルは機能しません。

ステップ 6 [適用] をクリックし、実行コンフィギュレーション ファイルに ISATAP パラメータを保存します。

ステップ 7 ISATAP トンネルを削除するには、[ISATAP トンネルの削除] ボタンをクリックします。

IPv6 アドレス

IPv6 インターフェイスに IPv6 アドレスを割り当てるには、次のようにします。

ステップ 1 [IP コンフィギュレーション] > [IPv6 の管理およびインターフェイス] > [IPv6 アドレス] をクリックします。

ステップ 2 テーブルに対してフィルタ処理を実行するには、インターフェイス名を選択してから、[実行] をクリックします。このインターフェイスが [IPv6 アドレス テーブル] に表示されます。これらのフィールドは [追加] ページで説明されます。ただし、次のフィールドを除きます。

- [アドレス ソース]: アドレス ソース タイプのいずれかが表示されます。DHCP、システム、またはスタティック。
- [DAD ステータス]: 重複アクセス検出（Duplicate Access Detection）がアクティブかどうかと DAD 状態が表示されます。
- [優先ライフタイム]: 優先ライフタイムのエントリが表示されます。
- [有効なライフタイム]: 有効なライフタイムのエントリが表示されます。
- [有効期限]: 有効期限が表示されます。

ステップ 3 [追加] をクリックします。

ステップ 4 フィールドに値を入力します。

- [IPv6 インターフェイス]: IPv6 アドレスを定義するインターフェイスが表示されます。* が表示されている場合、それは、IPv6 インターフェイスが有効になっていないにもかかわらず、設定されていることを意味します。
- [IPv6 アドレス タイプ]: 追加する IPv6 アドレスのタイプを選択します。
  - [リンクローカル]: 単一ネットワーク リンク上のホストを一意に識別する IPv6 アドレス。リンク ローカル アドレスのプレフィックス部は **FE80** です。このタイプのアドレスはルーティング不能であり、ローカル ネットワーク内で通信する場合にのみ使用できます。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。

- [グローバル]:他のネットワークからも認識かつアクセス可能なグローバル ユニキャスト IPv6 タイプである IPv6 アドレス。
- [エニーキャスト]:IPv6 アドレスはエニーキャスト アドレスです。これは、多くの場合、異なる複数のノードに属する一連のインターフェイスに割り当てられるアドレスです。エニーキャスト アドレスに送信されるパケットは、エニーキャスト アドレスによって識別される最近接インターフェイス(使用されているルーティング プロトコルで定義)に配布されます。

注 IPv6 アドレスが ISATAP インターフェイス上にある場合、エニーキャストは使用できません。

- [IPv6 アドレス]:レイヤ 2 において、デバイスは単一の IPv6 インターフェイスをサポートします。インターフェイスには、デフォルトのリンク ローカル アドレスとマルチキャスト アドレスが割り当てられますが、それに加え、受信されたルータ アドバタイズメントに基づいて、グローバル アドレスが自動的に割り当てられます。1 つのインターフェ イスに割り当て可能なアドレスは最大 128 個です。各アドレスは、16 ビット値をコロンで区切った 16 進表記で入力する必要があります。

  さまざまなタイプのトンネルに、以下のタイプのアドレスを追加することができます。

  - [手動トンネルに]:グローバル アドレスまたはエニーキャスト アドレス
  - [ISATAPトンネルに]:EUI-6 によるグローバル アドレス
  - [6 to 4 トンネル]:なし
- [プレフィックス長]:グローバル IPv6 プレフィックス部の長さ。0 ～ 128 の範囲の値を入力します。この値は、プレフィックス(アドレスのネットワーク部)を構成する、アドレスの上位ビットの数を意味します。
- [EUI-64]:EUI-64 パラメータを使用して、デバイスの MAC アドレスに基づく EUI-64 形式を使用することによりグローバル IPv6 アドレスのインターフェイス ID 部を識別する場合に選択します。

ステップ 5 [適用] をクリックします。実行コンフィギュレーション ファイルが更新されます。

IPv6 ルータの設定

以下のセクションでは、IPv6 ルータの設定方法について説明します。具体的な内容は、次のとおりです。

- ルータ アドバタイズメント
- IPv6 プレフィックス

ルータ アドバタイズメント

IPv6 ルータは、そのプレフィックスを隣接デバイスにアドバタイズできます。この機能は、次のようにして、インターフェイスごとに有効にしたり抑止したりできます。

ステップ 1 [IP コンフィギュレーション] > [IPv6 の管理およびインターフェイス] > [IPv6 ルータ コンフィギュレーション] > [ルータアドバタイズメント] の順にクリックします。

ステップ 2 ルータ アドバタイズメント テーブルに示されているインターフェイスを構成するには、それを選択してから [編集] をクリックします。

ステップ 3 次のフィールドを入力します。

- [ルータ アドバタイズメントの抑制]: インターフェイス上で IPv6 ルータ アドバタイズメントの伝送を抑制する場合は、[はい] を選択します。この機能が抑制されていない場合は、以下のフィールドを入力します。
- [ルータ プリファレンス]: ルータのプリファレンスとして、[低]、[中] または [高] のいずれかを選択します。ルータ アドバタイズメント メッセージは、このフィールドで設定されているプリファレンスで送信されます。プリファレンスが設定されていない場合、[中] プリファレンスで送信されます。

プリファレンスとルータとの関連付けは、たとえば、1 つのリンク上の 2 つのルータが同等ではあるもののコストの異なるルーティングを提供し、ホストがルータの 1 つを優先することがポリシーで述べられている場合に便利です。

- [アドバタイズメント間隔オプションを含める]: アドバタイズメント オプションがこのシステムで使用されることを指示する場合に選択します。このオプションは、アクセスしてくるモバイル ノードに対して、そのノードがルータ アドバタイズメントを受け取る間隔を示します。ノードでは、移動検出アルゴリズムの中でこの情報を使用することがあります。
- [ホップ限度]: これはルータがアドバタイズする値です。ゼロ以外の場合、ホストによってホップ限度として使用されます。

- [マネージド アドレス コンフィギュレーション フラグ]:接続されているホストに対して、アドレスを取得するためステートフル自動コンフィギュレーションを使用するよう指示する場合、このフラグを選択します。ホストでは、ステートフルとステートレスのアドレス自動コンフィギュレーションを同時に使用する可能性があります。
- [他のステートフル コンフィギュレーション フラグ]:接続されているホストに対して、その他の(アドレス以外の)情報を取得するためステートフル自動コンフィギュレーションを使用するよう指示する場合、このフラグを選択します。

  注 マネージド アドレス コンフィギュレーション フラグが設定されている場合、接続されているホストでは、ステートフル自動コンフィギュレーションを使用することにより、このフラグの設定には関係なく、その他の(アドレス以外の)情報を取得することができます。
- [ネイバー要求再送信間隔]:アドレスを解決する場合、またはあるネイバーに到達可能であるかどうかを試す場合に、ネイバー送信要求メッセージをネイバーに送信する際の再送信と再送信の間の時間を決定します。
- [最大ルータ アドバタイズメント間隔]:ルータ アドバタイズメントの時間間隔の合計の最大値を入力します。

このコマンドを使用してルータをデフォルト ルータとして設定する場合、送信間隔は、IPv6 ルータ アドバタイズメントのライフタイム以下でなければなりません。他の IPv6 ノードとの同期を回避するため、実際に使用される間隔は、最小値と最大値の間の値からランダムに選択されます。

- [最小ルータアドバタイズメント間隔]:ルータ アドバタイズメントの時間間隔の合計の最小値を入力するか([ユーザ定義])、またはシステム デフォルトを使用する場合は [デフォルトを使用] を選択します。

  注 最小ルータ アドバタイズメント間隔は、最大ルータ アドバタイズメント間隔の 75% 以下でなければならず、かつ 3 秒以上でなければなりません。
- [ルータ アドバタイズメント ライフタイム]:このルータがデフォルト ルータとして有用であり続ける残り時間を秒数で入力します。値がゼロの場合、それはデフォルト ルータとして有用でなくなったことを示します。
- [到達可能時間]:リモート IPv6 ノードが到達可能であると見なされる時間の合計をミリ秒単位で入力するか([ユーザ定義])、またはシステム デフォルトを使用する場合は [デフォルトを使用] オプションを選択します。

ステップ 4 [適用] をクリックし、実行コンフィギュレーション ファイルにコンフィギュレーションを保存します。

IPv6 プレフィックス

デバイスのインターフェイスに対してアドバタイズするプレフィクスを定義するには

ステップ 1 [IP コンフィギュレーション] > [IPv6 の管理およびインターフェイス] > [IPv6 ルータコンフィギュレーション] > [IPv6 プレフィクス] の順にクリックします。

ステップ 2 必要なら、[フィルタ] フィールドを有効にし、[実行] をクリックします。フィルタにマッチするインターフェイスのグループが表示されます。

ステップ 3 インターフェイスを追加するには、[追加] をクリックします。

ステップ 4 プレフィックスを追加する、必要な IPv6 インターフェイスを選択します。

ステップ 5 次のフィールドを入力します。

- [プレフィックス アドレス]: IPv6 ネットワーク。この引数は、RFC 4293 で説明されている形式になっていなければならず、アドレスは、コロンとコロンの間に 16 ビット値を使用した 16 進数で指定します。
- [プレフィックス長]: IPv6 プレフィックスの長さ。アドレスのうち何桁の高次連続ビットがプレフィックス(アドレスのネットワーク部分)となるかを示す 10 進値。10 進値の前には、スラッシュ記号を付ける必要があります。
- [プレフィックス アドバタイズメント]: このプレフィックスをアドバタイズする場合に選択します。
- [有効なライフタイム]: このプレフィックスが有効であり続ける時間、つまり無効になるまでの残り時間(秒数)。無効になったプレフィックスから生成されるアドレスは、パケットの宛先または送信元アドレスになってはなりません。
  - [無制限]: フィールドを、無制限を表す 4,294,967,295 に設定する場合、この値を選択します。
  - [ユーザ定義]: 値を入力します。
- [優先ライフタイム]: このプレフィックスが優先であり続ける残りの時間(秒数)。この時間が経過した後、プレフィックスは、新たな通信において送信元アドレスとして使用されなくなります。しかし、そのようなインターフェイスで受信されるパケットは期待どおりに処理されます。優先ライフタイムは、有効なライフタイム以下でなければなりません。
  - [無制限]: フィールドを、無制限を表す 4,294,967,295 に設定する場合、この値を選択します。
  - [ユーザ定義]: 値を入力します。

- [自動コンフィギュレーション]:インターフェイス上でステートレス自動コンフィギュレーションを使用して IPv6 アドレスの自動コンフィギュレーションを有効にし、そのインターフェイス上で IPv6 処理を有効にします。アドレスは、ルータ アドバタイズメント メッセージで受信されるプレフィックスに応じて設定されます。
- [プレフィックス ステータス]:次のいずれかのオプションを選択します。
  - [オンリンク]:指定されたプレフィックスをオンリンクとして設定します。指定されたプレフィックスを含むアドレスにトラフィックを送信するノードでは、宛先が、リンクでローカルに到達可能であると見なします。オンリンク プレフィックスは、接続プレフィックス(L ビット設定)としてルーティング テーブル中に挿入されます。
  - [オンリンクなし]:指定されたプレフィックスをオンリンクでないものとして設定します。オンリンクなしのプレフィックスは、接続プレフィックスとしてルーティング テーブル中に挿入されますが、L ビットがクリアされてアドバタイズされます。
  - [オフリンク]:指定されたプレフィックスをオフリンクとして設定します。プレフィックスは、L ビットをクリアした状態でアドバタイズされます。プレフィックスは、接続プレフィックスとしてルーティング テーブル中に挿入されません。プレフィックスが接続プレフィックスとしてルーティング テーブル中にすでに存在する場合(たとえばプレフィックスが IPv6 アドレスの追加でも設定されていた場合)、それは削除されます。

ステップ 6 [適用] をクリックし、実行コンフィギュレーション ファイルにコンフィギュレーションを保存します。

IPv6 デフォルト ルータ リスト

[IPv6 デフォルト ルータ リスト] ページでは、デフォルトの IPv6 ルータのアドレスを設定および表示できます。このリストには、外部ネットワークとの間で送受信されるトラフィックを処理するための、このデバイスに対するデフォルト ルータになり得るルータが表示されます(空の場合もあります)。このリスト内のルータが無作為に選択されます。このデバイスでは、スタティック IPv6 デフォルト ルータを 1 台使用できます。ダイナミック デフォルト ルータとは、ルータ アドバタイズメントをこのデバイスの IPv6 インターフェイスに送信したルータのことです。

IP アドレスを追加または削除すると、次の処理が実行されます。

- IP インターフェイスを削除すると、デフォルト ルータの IP アドレスがすべて削除されます。ダイナミック IP アドレスを削除することはできません。
- ユーザ定義アドレスを複数個挿入しようとすると、アラート メッセージが表示されます。

- リンク ローカル アドレス(プレフィックスが「fe80:」)でないアドレスを挿入しようとすると、アラート メッセージが表示されます。

デフォルト ルータを定義するには、次のようにします。

ステップ 1 [IP コンフィギュレーション] > [IPv6 の管理とインターフェイス] > [IPv6 デフォルト ルータリスト] をクリックします。

このページには、次のフィールドがデフォルト ルータごとに表示されます。

- [発信インターフェイス]:デフォルト ルータが接続されている発信 IPv6 インターフェイス。
- [デフォルト ルータ IPv6 アドレス]:デフォルト ルータのリンク ローカル IP アドレス。
- [タイプ]:以下のオプションを含むデフォルト ルータ コンフィギュレーション。
  - [スタティック]:デフォルト ルータは、[追加] ボタンで手動でこのテーブルに追加されました。
  - [ダイナミック]:デフォルト ルータは動的に設定されました。
- [メトリック]:このホップのコスト。

ステップ 2 [追加] をクリックし、スタティック デフォルト ルータを追加します。

ステップ 3 次のフィールドを入力します。

- [ネクストホップタイプ]:パケット送信先となる次の宛先の IP アドレス。これは、以下のもので構成されます。
  - [グローバル]:他のネットワークからも認識かつアクセス可能なグローバル ユニキャスト IPv6 タイプである IPv6 アドレス。
  - [リンク ローカル]:単一ネットワーク リンク上のホストを一意に識別する IPv6 インターフェイスおよび IPv6 アドレス。リンク ローカル アドレスのプレフィックス部は **FE80** です。このタイプのアドレスはルーティング不能であり、ローカル ネットワーク内で通信する場合にのみ使用できます。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。
- [ポイントツーポイント][発信インターフェイス]:発信リンク ローカル インターフェイスが表示されます。
- [デフォルト ルータ IPv6 アドレス]:スタティック デフォルト ルータの IP アドレス。

- [メトリック]: このホップのコストを入力します。

ステップ 4 [適用] をクリックします。デフォルト ルータが、実行コンフィギュレーション ファイルに保存されます。

IPv6 ネイバー

[IPv6 ネイバー] ページでは、IPv6 インターフェイス上の IPv6 ネイバーのリストを設定および表示できます。IPv6 ネイバー テーブル（別名：IPv6 近隣探索キャッシュ）には、デバイスと同じ IPv6 サブネット上にある IPv6 ネイバーの MAC アドレスが表示されます。いわば、IPv4 の ARP テーブルの IPv6 版です。デバイスがネイバーと通信する際、この IPv6 ネイバー テーブルが使用され、その IPv6 アドレスに基づいて MAC アドレスが特定されます。

このページには、自動検出されたエントリと手動設定されたエントリが表示されます。エントリごとに、ネイバーが接続されているインターフェイス、ネイバーの IPv6 アドレスと MAC アドレス、エントリ タイプ（スタティックまたはダイナミック）、およびネイバーの状態が表示されます。

IPv6 ネイバーを定義するには、次のようにします。

ステップ 1 [IP コンフィギュレーション] > [IPv6 の管理およびインターフェイス] > [IPv6 ネイバー] をクリックします。

[テーブルのクリア] オプションを選択することにより、IPv6 ネイバーテーブル内の IPv6 アドレスの全部または一部を消去することができます。

- [スタティックのみ]: スタティック IPv6 アドレス エントリを削除します。
- [ダイナミックのみ]: ダイナミック IPv6 アドレス エントリを削除します。
- [すべてのダイナミックおよびスタティック]: スタティック IPv6 アドレス エントリとダイナミック IPv6 アドレス エントリを両方とも削除します。

隣接インターフェイスに関する次のフィールドが表示されます。

- [インターフェイス]: 隣接 IPv6 インターフェイス タイプ。
- [IPv6 アドレス]: ネイバーの IPv6 アドレス。
- [MACアドレス]: 指定された IPv6 アドレスにマップされる MAC アドレス。
- [タイプ]: 近隣探索キャッシュ情報エントリのタイプ（スタティックまたはダイナミック）。

- [状態]:IPv6 ネイバーの状態を指定します。値は次のとおりです。
  - [未完了]:アドレス解決中です。ネイバーからの応答はまだありません。
  - [到達可能]:ネイバーは到達可能であると認識されています。
  - [失効]:それまで認識されていたネイバーは到達不能になっています。トラフィックを送信する必要性が生じるまで、このネイバーの到達可能性は検査されません。
  - [遅延]:それまで認識されていたネイバーは到達不能になっています。このインターフェイスは、事前定義された遅延時間の間、[遅延] 状態になります。到達可能性確認応答が受信されない場合、状態が [プローブ] に変わります。
  - [プローブ]:ネイバーが到達不能になっており、到達可能性を検査するためのユニキャスト ネイバー宛送信要求プローブを送信中です。
- [ルータ]:ネイバーがルータかどうかを指定します([はい] または [いいえ])。

ステップ 2 ネイバーをテーブルに追加するには、[追加] をクリックします。

ステップ 3 次のフィールドが表示されます。

- [インターフェイス]:追加する隣接 IPv6 インターフェイスが表示されます。
- [IPv6 アドレス]:インターフェイスに割り当てられた IPv6 ネットワーク アドレスを入力します。このアドレスは、有効な IPv6 アドレスでなければなりません。
- [MAC アドレス]:指定された IPv6 アドレスにマップされる MAC アドレスを入力します。

ステップ 4 [適用] をクリックします。実行コンフィギュレーション ファイルが更新されます。

ステップ 5 IP アドレスのタイプを [スタティック] から [ダイナミック] に変更するには、アドレスを選択し、[編集] をクリックし、[IPv6 ネイバーの編集] ページを使用します。

IPv6 プレフィックス リスト

最初のホップ セキュリティが設定されている場合、IPv6 プレフィックスに基づくフィルタリングのルールを定義することが可能です。それらのリストは、[IPv6 プレフィックスリスト] ページで定義できます。

プレフィックス リストは、**permit** または **deny** キーワードにより、マッチング条件に基づいてプレフィックスを許可するか拒否するように設定することができます。暗黙の拒否は、どのプレフィックス リスト エントリにもマッチしないトラフィックに適用されます。

プレフィックス リスト エントリは、IP アドレスとビット マスクとで構成されます。IP アドレスとしては、クラスフル ネットワーク、サブネット、あるいは単一ホスト ルートのためのものが可能です。ビット マスクは 1 ～ 32 の数値です。

プレフィックス リストは、プレフィックス長の等号マッチ、または ge および le キーワード使用する場合の範囲内のマッチに基づいてトラフィックをフィルタ処理するように設定されています。

[より大きい] および [より小さい] のパラメータは、プレフィックス長の範囲を指定するために使用され、ネットワーク/長さ引数のみ使用する場合に比べてコンフィギュレーションの柔軟性が高くなります。[より大きい] と [より小さい] のどちらのパラメータも指定されていない場合、プレフィックス リストは等号マッチを使用して処理されます。[より大きい] パラメータのみ指定されている場合、範囲は [より大きい] に入力された値から 32 ビット長さの最大値までです。[より小さい] のみ指定されている場合、範囲はネットワーク/長さ引数に入力されている値から、[より小さい] までです。[より大きい] と [より小さい] の両方の引数が入力された場合、範囲は、[より小さい] と [より大きい] で使用されている値の間になります。

プレフィックス リストを作成するには、次のようにします。

ステップ 1 [IP コンフィギュレーション] > [IPv6 の管理およびインターフェイス] > [IPv6 プレフィックスリスト] の順にクリックします。

ステップ 2 [追加] をクリックします。

ステップ 3 次のフィールドを入力します。

- [リスト名]: 次のいずれかのオプションを選択します。
  - [既存のリストの使用]: プレフィックスの追加先となる定義済みリストを選択します。
  - [新しいリストの作成]: 作成する新しいリストの名前を入力します。

- [連続番号]:プレフィックス リスト内でのプレフィックスの場所を指定します。次のいずれかのオプションを選択します。
  - [自動番号付与]:新しい IPv6 プレフィックスを、プレフィックス リストの最後のエントリの後に入れます。連続番号は、最後の連続番号に 5 を加えたものと等しくなります。リストが空の場合、最初のプレフィックス リスト エントリに番号 5 が割り当てられ、それ以降のプレフィックス リスト エントリはそれぞれ 5 ずつインクリメントしていきます。
  - [ユーザ定義]:新しい IPv6 プレフィックスを、パラメータで指定される場所に入れます。その番号のエントリが存在する場合、新しいものによって置換されます。
- [ルール タイプ]:プレフィックス リストのためのルールを入力します。
  - [許可]:条件に一致するネットワークを許可します。
  - [拒否]:条件に一致するネットワークを拒否します。
  - [説明]:テキスト。
- [IPv6 プレフィックス]:IP ルート プレフィックス。
- [プレフィックス長]:IP ルート プレフィックス長。
- [より大きい]:マッチングに使用するプレフィックスの最小長。次のいずれかのオプションを選択します。
  - [限度なし]:マッチングにプレフィックスの最小長を使用しません。
  - [ユーザ定義]:マッチングするプレフィックス最小長。
- [より小さいい]:マッチングに使用するプレフィックスの最大長。次のいずれかのオプションを選択します。
  - [限度なし]:マッチングにプレフィックスの最大長を使用しません。
  - [ユーザ定義]:マッチングするプレフィックス最大長。
- [説明]:プレフィックス リストの説明を入力します。

ステップ 4 [適用] をクリックし、実行コンフィギュレーション ファイルにコンフィギュレーションを保存します。

IPv6 ルータ

IPv6 転送テーブルには、設定されているさまざまなルートが含まれています。それらのルートの 1 つはデフォルト ルート（IPv6 アドレスは「0」）です。このルートは、IPv6 デフォルト ルータ リストから選択されたデフォルト ルータを使用して、デバイスと同じ IPv6 サブネット上にない宛先デバイスにパケットを送信するものです。このテーブルには、デフォルト ルートの他に、ダイナミック ルートも登録されています。ダイナミック ルートとは、ICMP リダイレクト メッセージを使用して IPv6 ルータから受信された ICMP リダイレクト ルートのことです。デバイスで使用されているデフォルト ルータが、デバイスの通信先 IPv6 サブネットとの間でトラフィックをルーティングしているルータでない場合に、ICMP リダイレクト メッセージが送信されます。

IPv6 ルートを表示するには、次のようにします。

[IP コンフィギュレーション] > [IPv6 の管理およびインターフェイス] > [IPv6 ルート] をクリックします。

このページには次のフィールドが表示されます。

- [IPv6 プレフィックス]: 宛先 IPv6 サブネット アドレスの IP ルート アドレス プレフィックス。
- [プレフィックス長]: 宛先 IPv6 サブネット アドレスの IP ルート プレフィックス長。数値の前にスラッシュ (/) が付加されています。
- [発信インターフェイス]: パケットの転送に使用されるインターフェイス。
- [ネクスト ホップ]: パケット転送先アドレスのタイプ。通常は、隣接ルータのアドレスです。以下のタイプのいずれかです。
  - [リンク ローカル]: 単一ネットワーク リンク上のホストを一意に識別する IPv6 インターフェイスおよび IPv6 アドレス。リンク ローカル アドレスのプレフィックス部は **FE80** です。このタイプのアドレスはルーティング不能であり、ローカル ネットワーク内で通信する場合にのみ使用できます。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。
  - [グローバル]: 他のネットワークからも認識かつアクセス可能なグローバル ユニキャスト IPv6 タイプである IPv6 アドレス。
  - [ポイントツーポイント]: ポイントツーポイント トンネル。
- [メトリック]: このルートを、IPv6 ルート テーブル内にある同一宛先の他ルートと比較する際に使用される値。デフォルト ルートにはすべて同じ値が設定されています。

- [ライフタイム]:パケットの送信および再送信のタイムアウト時間。この時間内に送信または再送信されなかったパケットは破棄されます。
- [ルート タイプ]:宛先の接続方法、およびエントリの取得に使用される方式。値は次のとおりです。
  - *S (スタティック)*:エントリは、ユーザによって手動で設定されました。
  - *I (ICMP リダイレクト)*:エントリは、ICMP リダイレクト メッセージを使用して IPv6 ルータから受信された ICMP リダイレクト ダイナミック ルートです。
  - *ND (ルータ アドバタイズメント)*:エントリは、ルータ アドバタイズメント メッセージから取得されます。

ステップ 1 新しいルートを追加するには、[追加] をクリックして、前述のフィールドに値を入力します。加えて、次のフィールドに値を入力します。

- [IPv6 アドレス]:新しいルートの IPv6 アドレスを追加します。

ステップ 2 [適用] をクリックし、変更を保存します。

DHCPv6 リレー

ここで説明する内容は次のとおりです。

- グローバル宛先
- インターフェイス設定

DHCPv6 リレーは、DHCPv6 メッセージを DHCPv6 サーバにリレーするために使用されます。これは RFC 3315 の中で定義されています。

DHCPv6 クライアントが DHCPv6 サーバに直接接続されていない場合、この DHCPv6 クライアントの直接接続先の DHCPv6 リレー エージェント(デバイス)により、直接接続されている DHCPv6 クライアントから受信するメッセージがカプセル化され、それらが DHCPv6 サーバに転送されます。

その反対方向では、リレー エージェントにより、DHCPv6 からの受信パケットがカプセルから取り出され、DHCPv6 クライアントに向けてそれらが転送されます。

ユーザは、パケット転送先となるリスト DHCP サーバのリストを設定する必要があります。DHCPv6 サーバの 2 つのセットを設定できます。

- [グローバル宛先]:パケットは、常にそれらの DHCPv6 サーバにリレーされます。

- [インターフェイス リスト]: これは、DHCPv6 サーバのインターフェイスごとのリストです。あるインターフェイスで DHCPv6 パケットが受信された場合、そのパケットはインターフェイス リスト上のサーバ（存在する場合）と、グローバル宛先リスト上のサーバの両方にリレーされます。

他の機能との依存関係

DHCPv6 クライアントと DHCPv6 リレー機能は、1 つのインターフェイス上では相互に排他的です。

グローバル宛先

すべての DHCPv6 パケットのリレー先 DHCPv6 サーバのリストを設定するには、次のようにします。

ステップ 1 [IP コンフィギュレーション] > [IPv6 の管理およびインターフェイス] > [DHCPv6 リレー] > [グローバル宛先] をクリックします。

ステップ 2 デフォルト DHCPv6 サーバを追加するには、[追加] をクリックします。

ステップ 3 次のフィールドを入力します。

- [IPv6 アドレス タイプ]: クライアント メッセージ転送先の宛先アドレスのタイプを入力します。アドレス タイプは、[リンク ローカル]、[グローバル]、または [マルチキャスト]（All_DHCP_Relay_Agents_and_Servers）のいずれかです。
- [DHCPv6 サーバ IP アドレス]: パケット転送先の DHCPv6 サーバのアドレスを入力します。
- [IPv6 インターフェイス]: DHCPv6 サーバのアドレス タイプが [リンクローカル] または [マルチキャスト] の場合に、パケットが送信される宛先インターフェイスを入力します。このインターフェイスは、VLAN、LAG、またはトンネルです。

ステップ 4 [適用] をクリックします。実行コンフィギュレーション ファイルが更新されます。

インターフェイス設定

あるインターフェイス上で DHCPv6 リレーを有効にし、そのインターフェイス上で DHCPv6 パケット受信時にそれらのリレー先となる DHCPv6 サーバのリストを設定するには、次のようにします。

ステップ 1 [IP コンフィギュレーション] > [IPv6 の管理およびインターフェイス] > [DHCPv6 リレー] > [インターフェイス設定] の順にクリックします。

ステップ 2 あるインターフェイス上で DHCPv6 を有効にし、オプションとして、インターフェイスの DHCPv6 サーバを追加するには、[追加] をクリックします。

次のフィールドを入力します。

- [送信元インターフェイス]:DHCPv6 リレーを有効にするインターフェイス（ポート、LAG、VLAN、またはトンネル）を選択します。
- [グローバル宛先のみ使用]:パケットの転送先が DHCPv6 グローバル宛先サーバのみの場合に選択します。
- [IPv6 アドレス タイプ]:クライアント メッセージ転送先の宛先アドレスのタイプを入力します。アドレス タイプは、[リンク ローカル]、[グローバル]、または [マルチキャスト]（All_DHCP_Relay_Agents_and_Servers）のいずれかです。
- [DHCPv6 サーバ IP アドレス]:パケット転送先の DHCPv6 サーバのアドレスを入力します。
- [宛先IPv6 インターフェイス]:DHCPv6 サーバのアドレス タイプが [リンク ローカル] または [マルチキャスト] の場合に、パケットが送信されるインターフェイスを入力します。

ステップ 3 [適用] をクリックします。実行コンフィギュレーション ファイルが更新されます。

ドメイン ネーム システム

Domain Name System（DNS; ドメイン ネーム システム）は、ドメイン名を IP アドレスに変換するものです。これにより、ホストを探したりホストのアドレス指定をしたりすることができます。

このデバイスは、DNS クライアントとして、1 台以上の設定済み DNS サーバを使用することによってドメイン名を IP アドレスに変換します。

DNS 設定

[DNS 設定] ページを使用して、DNS 機能を有効にしたり、DNS サーバを設定したり、デバイスによって使用されるデフォルト ドメインを設定したりできます。

ステップ 1 [IP コンフィギュレーション] > [DNS] > [DNS 設定] の順にクリックします。

ステップ 2 基本モードでは、次のパラメータを入力します。

- [サーバ指定方法]:DNS サーバを定義するオプションとして、次のいずれか 1 つを選択します。
  - [IP アドレス別]:IP アドレスが DNS サーバに入力されます。
  - [無効]:DNS サーバが定義されません。
- [サーバ IP アドレス]:前述の [IP アドレス別] を選択した場合は、DNS サーバの IP アドレスを入力します。
- [デフォルト ドメイン名]:非修飾ホスト名を完成させるために使用する DNS ドメイン名を入力します。デバイスによりこれがすべての非完全修飾ドメイン名(NFQDN)に付加されて、それらが FQDN になります。

  注 非修飾名とドメイン名を区切る最初のピリオドは含めないようにしてください(cisco.com など)。

ステップ 3 拡張モードでは、次のパラメータを入力します。

- [DNS]:デバイスを DNS クライアントとして指定し、1 台以上の設定済み DNS サーバを使用して DNS 名を IP アドレスに解決できるようにする場合に選択します。
- [ポーリング再試行回数]:デバイスが DNS サーバが存在しないと判断するまで、DNS クエリーを DNS サーバに送信する回数を入力します。
- [ポーリング タイムアウト]:DNS クエリーに対する応答をデバイスが待機する秒数を入力します。
- [ポーリング間隔]:再試行回数に達した後、DNS クエリー パケットをデバイスが送信する頻度を秒数として入力します。
  - [デフォルトを使用]:デフォルト値を使用する場合に選択します。

    この値 = 2*(ポーリング再試行回数 + 1)* ポーリング タイムアウト
  - [ユーザ定義]:ユーザ定義値を入力する場合に選択します。

- [デフォルト パラメータ]:以下のデフォルト パラメータを入力します。
  - [デフォルト ドメイン名]:非修飾ホスト名を完成させるために使用する DNS ドメイン名を入力します。デバイスによりこれがすべての非完全修飾ドメイン名(NFQDN)に付加されて、それらが FQDN になります。

    注 非修飾名とドメイン名を区切る最初のピリオドは含めないようにしてください(cisco.com など)。
  - [DHCP ドメイン検索リスト]:[詳細] をクリックして、デバイス上で設定されている DNS サーバのリストを表示します。

ステップ 4 [適用] をクリックします。実行コンフィギュレーション ファイルが更新されます。

[DNS サーバテーブル] には、設定された DNS サーバごとに次の情報が表示されます。

- [DNS サーバ]:DNS サーバの IP アドレスを入力します。
- [プリファレンス]:サーバごとにプリファレンス値があります。その値が低いほど、使用される確率が高くなります。
- [送信元]:サーバの IP アドレスの送信元(スタティック、または DHCPv4、または DHCPv6)
- [インターフェイス]:サーバの IP アドレスのインターフェイス。

ステップ 5 定義できる DNS サーバは最大 8 台です。DNS サーバを追加するには、[追加] をクリックします。

ステップ 6 パラメータを入力します。

- [IP バージョン]:IPv6 の場合は [バージョン 6]、IPv4 の場合は [バージョン 4] を選択します。
- [IPv6 アドレス タイプ]:IPv6 アドレス タイプを選択します(IPv6 が使用される場合)。次のオプションがあります。
  - [リンク ローカル]:IPv6 アドレスによって、単一ネットワーク リンク上のホストが一意に識別されます。リンク ローカル アドレスのプレフィックス部は **FE80** です。このタイプのアドレスはルーティング不能であり、ローカル ネットワーク内で通信する場合にのみ使用できます。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。
  - [グローバル]:IPv6 アドレスは、他のネットワークから認識可能かつアクセス可能なグローバル ユニキャスト IPV6 タイプになります。

- [リンクローカルインターフェイス]:IPv6 アドレス タイプがリンク ローカルである場合、その受信元のインターフェイスを選択します。
- [DNS サーバ IP アドレス]:DNS サーバの IP アドレスを入力します。
- [プリファレンス]:ドメインの使用順序を決定する値を選択します。低い値から高い値へという順序で使用されます。これにより、DNS クエリー中に非修飾名が完成される順序が効率的に決定されます。

ステップ 7 [適用] をクリックします。DNS サーバが、実行コンフィギュレーション ファイルに保存されます。

検索リスト

検索リストには、ユーザ、[DNS 設定] ページ、および DHCPv4 と DHCPv6 のサーバから受信した動的エントリによって定義される 1 つのスタティック エントリが含まれる場合があります。

デバイス上で設定されたドメイン名を表示するには、[IP コンフィギュレーション] > [DNS] > [検索リスト] の順にクリックします。

デバイスに設定されている DNS サーバごとに次のフィールドが表示されます。

- [ドメイン名]:デバイスで使用できるドメインの名前。
- [送信元]:このドメインのサーバの IP アドレスの送信元(スタティック、または DHCPv4、または DHCPv6)
- [インターフェイス]:このドメインのサーバの IP アドレスのインターフェイス。
- [プリファレンス]:これは、ドメインの使用順序です。低い値から高い値へという順序で使用されます。これにより、DNS クエリー中に非修飾名が完成される順序が効率的に決定されます。

ホスト マッピング

ホスト名/IP アドレスのマッピングは、ホスト マッピング テーブル(DNS キャッシュ)に保存されています。

そのキャッシュには、以下のタイプのエントリが含まれる可能性があります。

- [スタティックエントリ]:これらは、手動でキャッシュに追加されたマッピング ペアです。スタティック エントリは 64 個まで可能です。

- [ダイナミックエントリ]: これらは、ユーザによって使用された結果としてシステムによって追加されたマッピング ペアか、または DHCP によってデバイスに設定された IP アドレスごとに 1 つエントリがあるマッピング ペアです。ダイナミック エントリは 256 個まで可能です。

名前解決処理では必ず、最初にこれらのスタティック エントリが検査されます。一致するエントリがない場合は、ダイナミック エン トリが検査されます。ここでも一致するエントリがない場合は、外部 DNS サーバに要求が送信されます。

1 つの DNS サーバの 1 つのホスト名に対して 8 個の IP アドレスがサポートされています。

ホスト名とその IP アドレスを追加するには、次のようにします。

ステップ 1 [IP コンフィギュレーション] > [DNS] > [ホスト マッピング] の順にクリックします。

ステップ 2 必要なら、[テーブルのクリア] オプションを選択して、ホスト マッピング テーブル内のエントリの全部または一部を消去できます。

- [スタティックのみ]: スタティック ホストを削除します。
- [ダイナミックのみ]: ダイナミック ホストを削除します。
- [すべてのダイナミックおよびスタティック]: スタティック ホストおよびダイナミック ホストを削除します。

ホスト マッピング テーブルに表示されるフィールドは次のとおりです。

- [ホスト名]: ユーザ定義ホスト名または完全修飾名。
- [IP アドレス]: ホスト IP アドレス。
- [IP バージョン]: ホスト IP アドレスの IP バージョン。
- [タイプ]: このエントリがキャッシュに対して [ダイナミック] かそれとも [スタティック] か。
- [ステータス]: ホストへのアクセス試行の結果が表示されます。
  - [OK]: 試行成功。
  - [ネガティブ キャッシュ]: 試行失敗。再試行しないでください。
  - [応答なし]: 応答はありませんが、将来システムによる再試行が可能です。
- [TTL（秒）]: これがダイナミック エントリの場合、これがキャッシュ内に保持される長さ。
- [残りのTTL（秒）]: これがダイナミック エントリの場合、これがキャッシュ内に保持される残りの長さ。

ステップ 3 ホスト マッピングを追加するには、[追加] をクリックします。

ステップ 4 パラメータを入力します。

- [IP バージョン]:IPv6 の場合は [バージョン 6]、IPv4 の場合は [バージョン 4] を選択します。
- [IPv6 アドレス タイプ]:IPv6 アドレス タイプを選択します(IPv6 が使用される場合)。次のオプションがあります。
  - [リンク ローカル]:IPv6 アドレスによって、単一ネットワーク リンク上のホストが一意に識別されます。リンク ローカル アドレスのプレフィックス部は **FE80** です。このタイプのアドレスはルーティング不能であり、ローカル ネットワーク内で通信する場合にのみ使用できます。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。
  - [グローバル]:IPv6 アドレスは、他のネットワークから認識可能かつアクセス可能なグローバル ユニキャスト IPV6 タイプになります。
- [リンクローカルインターフェイス]:IPv6 アドレス タイプがリンク ローカルである場合、その受信元のインターフェイスを選択します。
- [ホスト名]::ユーザ定義ホスト名または完全修飾名を入力します。ホスト名は ASCII 文字の A～Z(大文字と小文字は区別しない)、数字 0～9、下線文字、およびハイフンに制限されています。ピリオド (.) は、ラベルを区切るために使用されています。
- [IP アドレス]:単一のアドレス、または関連する 8 個以下の IP アドレスを入力します(IPv4 または IPv6)。

ステップ 5 [適用] をクリックします。設定値が、実行コンフィギュレーション ファイルに保存されます。

17

セキュリティ

ここでは、デバイスのセキュリティとアクセス コントロールについて説明します。このシステムにはさまざまなセキュリティ機能が備わっています。

ここで説明する各種のセキュリティ機能は、以下のとおりです。一部の機能は、複数の種類のセキュリティまたはアクセス コントロールに対して利用されています。そのため、このような機能は以下の一覧に 2 回出現します。

デバイスを管理する権限については、次の各項で説明します。

- パスワード強度
- 管理アクセス方式
- 管理アクセス認証
- SSL サーバ

デバイスの CPU を標的にした攻撃を防ぐ方法については、次の各項で説明します。

- TCP/UDP サービス
- ストーム制御
- アクセス制御

エンドユーザによるデバイス経由でのネットワーク アクセスを制御する方法については、次の各項で説明します。

- 管理アクセス方式
- RADIUS
- ポート セキュリティ

その他のネットワーク ユーザからの攻撃を防ぐ方法については、次の各項で説明します。これらの攻撃はデバイスを通過するものであり、デバイスを標的にしたものではありません。

- サービス拒絶防御
- SSL サーバ

- ストーム制御
- ポート セキュリティ
- アクセス制御

RADIUS

Remote Authorization Dial-In User Service（RADIUS）サーバは、802.1x または MAC に基づいてネットワーク アクセスを制御します。

デバイスは、RADIUS サーバを使用してセキュリティを一元管理できる RADIUS クライアントか、または RADIUS サーバとして設定できます。

RADIUS クライアント

組織のすべてのデバイスを対象として 802.1X または MAC に基づくネットワーク アクセスの一元的な制御を行うために、デバイスを使用して Remote Authorization Dial-In User Service（RADIUS）サーバを設置することができます。この方法により、組織内のすべてのデバイスに関する認証と認可を 1 つのサーバで扱うことができます。

デバイスを RADIUS クライアントとして設定すると、次のサービスのために RADIUS サーバを使用できます。

- 認証：ユーザ名およびユーザ定義のパスワードを使用して、デバイスにログオンする通常のユーザおよび 802.1X ユーザを認証する機能を提供します。
- 承認：ログイン時に実行されます。認証セッションが完了した後、認証済みのユーザ名を使って承認セッションが開始します。次に、RADIUS サーバはユーザの特権を確認します。

アカウンティング：RADIUS サーバを使用したログイン セッションのアカウンティングを有効にします。これにより、システム管理者は RADIUS サーバからアカウンティング レポートを生成できます。RADIUS サーバ アカウンティングに使用されるユーザ定義可能な TCP ポートは、RADIUS サーバ認証および承認に使われる TCP ポートと同じです。

デフォルト

この機能には、次のデフォルト設定が適用されます。

- デフォルトでは、デフォルト RADIUS サーバが定義されていません。

- RADIUS サーバを設定するとき、デフォルトではアカウンティング機能が無効になります。

RADIUS の手順

RADIUS サーバを使用するには、次のようにします。

ステップ 1 RADIUS サーバ上でデバイスのアカウントを開きます。

ステップ 2 [RADIUS] ページと [RADIUS サーバの追加] ページで、そのサーバおよび他のパラメータを設定します。

注 複数の RADIUS サーバがすでに構成されている場合、デバイスは、使用可能な RADIUS サーバに関する構成済みの優先度に基づき、デバイスで使用する RADIUS サーバを選択します。

RADIUS サーバのパラメータ値を設定するには、次のようにします。

ステップ 1 [セキュリティ] > [RADIUS クライアント] をクリックします。

ステップ 2 必要に応じてデフォルト RADIUS パラメータを入力します。[デフォルトパラメータ] で入力した値は、すべての RADIUS サーバに適用されます。([RADIUS サーバの追加] ページで) 特定の RADIUS サーバに関する値が入力されない場合、これらのフィールドの値がデバイスで使用されます。

- [リトライ回数]:RADIUS サーバに要求を送信する最大試行回数を入力します。この回数送信しても失敗する場合は、エラーが発生したと見なされます。
- [応答タイムアウト]:RADIUS サーバからの応答をデバイスが待つ時間 (単位:秒) を入力します。この時間が経過した後、クエリーを再試行するか、または次のサーバに切り替えます。
- [デッドタイム]:応答のない RADIUS サーバへのサービス要求がバイパスされるようになるまでの経過時間 (単位:分) を入力します。「0」を入力した場合、この RADIUS サーバはバイパスされません。
- [キーストリング]:デバイスと RADIUS サーバの間の認証と暗号化に使用されるデフォルトのキー ストリングを入力します。このキーは、RADIUS サーバ側で設定されているキーと一致していなければなりません。キーは、MD5 を使用して送信データを暗号化する際に使用されます。暗号化またはプレーンテキストのいずれかの形式でキーを入力できます。(別のデバイスからの) 暗号化キーストリングがない場合は、プレーンテキスト モードでキー ストリングを入力して [適用] をクリックします。暗号化キー ストリングが生成されて、表示されます。

デフォルト キー ストリングが定義済みであれば、それがオーバーライドされます。

- [送信元 IPv4 インターフェイス]:RADIUS サーバとの通信のためのメッセージで使用されるデバイス IPv4 送信元インターフェイスを選択します。
- [送信元 IPv6 インターフェイス]:RADIUS サーバとの通信のためのメッセージで使用されるデバイス IPv6 送信元インターフェイスを選択します。

  注 [自動] オプションが選択されている場合、システムは、発信インターフェイスで定義された IP アドレスからソース IP アドレスを取得します。

ステップ 3 [適用] をクリックします。実行コンフィギュレーション ファイル内で、デバイスの RADIUS デフォルト設定が更新されます。

RADIUS サーバを追加するには、[追加] をクリックします。

ステップ 4 RADIUS サーバごとに、フィールドに値を入力します。[RADIUS] ページで入力したデフォルト値を使用するには、[デフォルトを使用] を選択します。

- [サーバ指定方法]:RADIUS サーバを IP アドレスで指定するか、名前で指定するかを選択します。
- [IP バージョン]:RADIUS サーバの IP アドレスのバージョンを選択します。
- [IPv6 アドレス タイプ]:IPv6 アドレス タイプを選択します(IPv6 が使用される場合)。次のオプションがあります。
  - [リンク ローカル]:IPv6 アドレスによって、単一ネットワーク リンク上のホストが一意に識別されます。リンク ローカル アドレスのプレフィックス部は **FE80** です。このタイプのアドレスはルーティング不能であり、ローカル ネットワーク内で通信する場合にのみ使用できます。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。
  - [グローバル]:IPv6 アドレスは、他のネットワークから認識可能かつアクセス可能なグローバル ユニキャスト IPV6 タイプになります。
- [リンクローカルインターフェイス]:リストからリンク ローカル インターフェイスを選択します(IPv6 アドレス タイプとしてリンク ローカルが選択されている場合)。
- [サーバの IP アドレス/名前]:RADIUS サーバを IP アドレスまたは名前で入力します。

- [プライオリティ]:サーバのプライオリティを入力します。プライオリティにより、デバイスがユーザ認証のためにサーバと通信を試みる際の順序が決まります。デバイスは、プライオリティが最も高い RADIUS サーバを最初に試します。プライオリティは 0 が最高です。
- [キーストリング]:デバイスと RADIUS サーバとの間の通信を認証および暗号化するために使われるキー ストリングを入力します。このキーは、RADIUS サーバ側で設定されているキーと一致していなければなりません。**暗号化**または**プレーンテキスト**のいずれかの形式で入力できます。[デフォルトを使用] を選択した場合、デバイスはデフォルトのキー ストリングを使用して RADIUS サーバへの認証を試みます。
- [応答タイムアウト]:[ユーザ定義] を選択して、RADIUS サーバからの応答をデバイスが待つ時間(単位:秒)を入力します。この時間が経過した後、デバイスはクエリーを再試行するか、または(最大再試行回数に達していれば)次のサーバに切り替えます。[デフォルトを使用] を選択した場合、デバイスはデフォルトのタイムアウト値を使用します。
- [認証ポート]:認証要求用の RADIUS サーバ ポートの UDP ポート番号を入力します。
- [リトライ回数]:[ユーザ定義] を選択して、RADIUS サーバに要求を送る最大試行回数を入力します。この回数送信しても失敗する場合は、エラーが発生したと見なされます。[デフォルトを使用] を選択した場合、デバイスはリトライ回数のデフォルト値を使用します。
- [デッド タイム]:[ユーザ定義] を選択して、応答のない RADIUS サーバへのサービス要求がバイパスされるようになるまでの経過時間(単位:分)を入力します。[デフォルトを使用] を選択した場合、デバイスはデッド タイムのデフォルト値を使用します。「0」と入力した場合、デッド タイムは設定されません。
- [使用タイプ]:RADIUS サーバの認証タイプを入力します。次のオプションがあります。
  - [ログイン]:RADIUS サーバは、デバイスの管理を希望するユーザを認証する目的で使用されます。
  - [802.1X]:RADIUS サーバは 802.1x 認証用に使用されます。
  - [すべて]:RADIUS サーバは、デバイスの管理を希望するユーザの認証、および 802.1X 認証に使用されます。

ステップ 5 [適用] をクリックします。RADIUS サーバ定義が、デバイスの実行コンフィギュレーション ファイルに追加されます。

ステップ 6 ページ上で機密データをプレーンテキスト形式で表示するには、[機密データを平文で表示] をクリックします。

パスワード強度

デフォルトのユーザ名とパスワードは **cisco** および **cisco** です。デフォルトのユーザ名とパスワードで初めてログインすると、新しいパスワードを入力するように求められます。パスワード複雑度は、デフォルトで有効になっています。([パスワード強度] ページの [パスワードの複雑度の設定] が有効になっていて) パスワードの複雑さが不十分な場合は、別のパスワードを作成するように求められます。

ユーザ アカウントの作成方法については、「ユーザ アカウント」を参照してください。

デバイスにアクセスするユーザの認証にパスワードが使用されるため、単純なパスワードはセキュリティを危険にさらす可能性があります。そのため、パスワード複雑度要件がデフォルトで適用されており、必要に応じて設定を変更できます。

パスワード複雑度ルールを定義するには、次のようにします。

ステップ 1 [セキュリティ] > [パスワード強度] をクリックします。

ステップ 2 パスワードに関する次のエージング パラメータを入力します。

- [パスワードエージング]: これを選択した場合、[パスワードエージング時間] で指定した日数が経過するとユーザはパスワードを変更するよう要求されます。
- [パスワードエージング時間]: パスワードの有効日数を入力します。この日数が経過すると、パスワードを変更するよう要求されます。

  注 パスワード エージングは、長さゼロのパスワード (つまりパスワードなし) にも適用されます。

ステップ 3 パスワードの複雑度ルールを有効にするには、[パスワードの複雑度の設定] を選択します。

パスワード複雑度が有効な場合、新しいパスワードは次のデフォルト設定に従う必要があります。

- 長さは 8 文字以上にする。
- 3 つ以上の文字クラスの文字を含む (大文字、小文字、数字、標準キーボードで使用可能な特殊文字)。
- 現在のパスワードとは異なるパスワードにする。

- 同じ文字を 3 回以上続けて使用しない。
- ユーザ名や、その大文字小文字を入れ替えただけの派生形を繰り返したり逆にしたりして使用しない。
- 製造業者名や、その大文字小文字を入れ替えただけの派生形を繰り返したり逆にしたりして使用しない。

ステップ 4 [パスワードの複雑度の設定] が有効な場合は、次のパラメータを設定できます。

- [最小パスワード長]:パスワードの最小文字数を入力します。

  注 長さをゼロのパスワード(つまりパスワードなし)を使用できます。また、この場合でもパスワード エージングを割り当てることができます。

- [許容される文字の繰り返し]:1 つの文字を繰り返すことのできる回数を入力します。
- [文字クラスの最小数]:パスワードに含まれる必要のある文字クラスの数を入力します。文字クラスは、小文字(1)、大文字(2)、数字(3)、および記号または特殊文字(4)です。
- [新規パスワードは現在のパスワードとは異なっている必要があります]:これを選択した場合、パスワードの変更時に、新しいパスワードを現在のパスワードと同じ値にすることはできません。

ステップ 5 [適用] をクリックします。パスワード設定が実行コンフィギュレーション ファイルに書き込まれます。

注 ユーザ名/パスワード同等値の設定、および製造業者/パスワード同等値の設定は CLI で可能です。詳細については、*『CLI Reference Guide』*を参照してください。

管理アクセス方式

ここでは、さまざまな管理方式に関するアクセス ルールについて説明します。

具体的な内容は、次のとおりです。

- アクセス プロファイル
- プロファイル ルール

アクセス プロファイルによって、さまざまなアクセス方法でデバイスにアクセスするユーザを認証および承認する方法が決まります。アクセスプロファイルを使用して、特定のソースからの管理アクセスを制限することができます。

アクティブ アクセス プロファイルと管理アクセス認証方式の両方に合格したユーザだけが、デバイスに管理アクセスできます。

デバイス上では、一度に 1 つのアクセス プロファイルだけをアクティブにすることができます。

アクセス プロファイルは、1 つ以上のルールから構成されています。各ルールは、アクセス プロファイル内のプライオリティ順に（上から順に）実行されます。

各ルールはフィルタで構成されており、各フィルタは次の要素で構成されています。

- [アクセス方式]: デバイスにアクセスして管理するための方式。
  - Telnet
  - Secure Telnet（SSH）
  - Hypertext Transfer Protocol（HTTP; ハイパーテキスト転送プロトコル）
  - Secure HTTP（HTTPS）
  - Simple Network Management Protocol（SNMP; シンプル ネットワーク管理プロトコル）
  - 上記すべて
- [アクション]: インターフェイスまたは送信元アドレスへのアクセスを許可するか拒否するか。
- [インターフェイス]: Web ベースの設定ユーティリティへのアクセスを許可または拒否されるポート、LAG、または VLAN。
- [送信元 IP アドレス]: IP アドレスまたはサブネット。ユーザ グループによって、管理方式へのアクセスが異なる可能性があります。たとえば、あるユーザ グループは HTTPS セッションのみを使ってデバイス モジュールにアクセスでき、別のユーザ グループは HTTPS および Telnet の両方のセッションを使ってデバイス モジュールにアクセスできる場合があります。

アクセス プロファイル

[アクセスプロファイル] ページには、定義されているアクセス プロファイルが表示され、アクティブにする 1 つのアクセス プロファイルを選択できます。

ユーザがあるアクセス方式でデバイスにアクセスしようとすると、デバイスは、この方式によるデバイスへの管理アクセスがアクティブ アクセス プロファイルで明示的に許可されているかどうかを確認します。合致するルールが見つからない場合、アクセスは拒否されます。

アクティブ アクセス プロファイルに違反するデバイス アクセスが試行された場合、デバイスで SYSLOG メッセージが生成され、システム管理者にそのアクセス試行が通知されます。

詳細については、「プロファイル ルール」を参照してください。

[アクセスプロファイル] ページを使用してアクセス プロファイルを作成し、その最初のルールを追加します。アクセス プロファイルに 1 つのルールしか含めない場合は、それで終了です。プロファイルにルールを追加するには、[プロファイルルール]ページを使用します。

ステップ 1 [セキュリティ] > [管理アクセス方式] > [アクセスプロファイル]をクリックします。

このページには、アクティブ アクセス プロファイルと非アクティブ アクセス プロファイルを含むすべてのアクセス プロファイルが表示されます。

ステップ 2 アクティブなアクセス プロファイルを切り替えるには、[アクティブアクセスプロファイル] ドロップダウン メニューからプロファイルを選択し、[適用] をクリックします。選択したプロファイルがアクティブ アクセス プロファイルになります。

他のいずれかのアクセス プロファイルを選択した場合、「選択したアクセスプロファイルによっては Web ベースのデバイス設定ユーティリティから切断される可能性がある」という内容の注意メッセージが表示されます。

ステップ 3 アクティブ アクセス プロファイルを選択するには [OK] をクリックします。操作を中止するには、[キャンセル] をクリックします。

ステップ 4 [追加] をクリックして、[アクセスプロファイルの追加] ページを開きます。このページでは、新しいアクセス プロファイルとルール 1 つを設定できます。

ステップ 5 [アクセスプロファイル名] を入力します。この名前には最大で 32 文字を含めることができます。

ステップ 6 パラメータを入力します。

- [ルールプライオリティ]:ルールのプライオリティを入力します。パケットがルールの条件に一致した場合、ユーザ グループはデバイスへの管理アクセスを許可または拒否されます。プライオリティの高いルールから順に適用されるため、ルールのプライオリティは非常に重要です。最高のプライオリティは「1」です。
- [管理方式]:ルールを定義する対象となる管理方式を選択します。次のオプションがあります。
  - [すべて]:すべての管理方式をこのルールに割り当てます。

- [Telnet]:デバイスへのアクセスを要求しているユーザが Telnet アクセス プロファイル基準を満たす場合、そのユーザはアクセスを許可または拒否されます。
- [Secure Telnet(SSH)]:デバイスへのアクセスを要求しているユーザが SSH アクセス プロファイル基準を満たす場合、そのユーザはアクセスを許可または拒否されます。
- [HTTP]:デバイスへのアクセスを要求しているユーザが HTTP アクセス プロファイル基準を満たす場合、そのユーザは許可または拒否されます。
- [Secure HTTP(HTTPS)]:デバイスへのアクセスを要求しているユーザが HTTPS アクセス プロファイル基準を満たす場合、そのユーザは許可または拒否されます。
- [SNMP]:デバイスへのアクセスを要求しているユーザが SNMP アクセス プロファイル基準を満たす場合、そのユーザは許可または拒否されます。

- [アクション]:このルールに関連付けられる処理を選択します。次のオプションがあります。
  - [許可]:ユーザがこのプロファイルの設定に一致した場合、デバイスへのアクセスを許可します。
  - [拒否]:ユーザがこのプロファイルの設定に一致した場合、デバイスへのアクセスを拒否します。
- [インターフェイスに適用]:このルールに関連付けられるインターフェイスを選択します。次のオプションがあります。
  - [すべて]:すべてのポート、VLAN、および LAG に適用されます。
  - [ユーザ定義]:選択したインターフェイスに適用されます。
- [インターフェイス]:[ユーザ定義] を選択した場合は、インターフェイス番号を入力します。
- [送信元 IP アドレスに適用]:このアクセス プロファイルの適用対象となる送信元 IP アドレスのタイプを選択します。[送信元 IP アドレス] フィールドにはサブネットワークを入力できます。次のいずれかを選択します。
  - [すべて]:すべてのタイプの IP アドレスに適用されます。
  - [ユーザ定義]:フィールドで定義されたタイプの IP アドレスだけに適用されます。
- [IP バージョン]:送信元 IP アドレスのバージョンを入力します(バージョン 6 またはバージョン 4)。

- [IP アドレス]:送信元 IP アドレスを入力します。
- [マスク]:送信元 IP アドレスのサブネット マスクの形式を選択し、次のいずれかのフィールドに値を入力します。
  - [ネットワーク マスク]:送信元 IP アドレスが属するサブネットを選択し、サブネット マスクをピリオド区切りの 10 進表記で入力します。
  - [プレフィックス長]:[プレフィックス長] を選択し、送信元 IP アドレス プレフィックスを構成するビット数を入力します。

ステップ 7 [適用] をクリックします。アクセス プロファイルが実行コンフィギュレーション ファイルに書き込まれます。これで、このアクセス プロファイルをアクティブ アクセス プロ ファイルとして選択できます。

プロファイル ルール

アクセス プロファイルには最大 128 個のルールを含めることができます。これにより、デバイスにアクセスして管理することを許可されるユーザ、および使用できるアクセス方式を定めることができます。

アクセス プロファイル内の各ルールには、1 つのアクションおよび照合する基準(1 つ以上のパラメータ)が含まれます。各ルールにはプライオリティが設定されています。プライオリティが最も高いルールが最初に適用されます。入力パケットがルールの条件に合致した場合、そのルールの処理が実行されます。アクティブ アクセス プロファイル内のどのルールの条件にも合致しなかったパケットは、ドロップされます。

たとえば、IT 管理センターに割り当てられた IP アドレス以外のすべての IP アドレスからデバイスにアクセスできないように制限できます。このようにして、さらにデバイスを管理できるので、セキュリティの層を追加できます。

プロファイル ルールをアクセス プロファイルに追加するには、次のようにします。

ステップ 1 [セキュリティ] > [管理アクセス方式] > [プロファイルルール] をクリックします。

ステップ 2 [フィルタ] フィールドを選択し、次にアクセス プロファイルを選択します。[実行] をクリックします。

選択したアクセス プロファイルが [プロファイルルールテーブル] に表示されます。

ステップ 3 [追加] をクリックしてルールを追加します。

ステップ 4 パラメータを入力します。

- [アクセスプロファイル名]:アクセス プロファイルを選択します。

- [ルールプライオリティ]:ルールのプライオリティを入力します。パケットがルールの条件に一致した場合、ユーザ グループはデバイスへの管理アクセスを許可または拒否されます。プライオリティの高いルールから順に適用されるため、ルールのプライオリティは非常に重要です。
- [管理方式]:ルールを定義する対象となる管理方式を選択します。次のオプションがあります。
  - [すべて]:すべての管理方式をこのルールに割り当てます。
  - [Telnet]:デバイスへのアクセスを要求しているユーザが Telnet アクセス プロファイル基準を満たす場合、そのユーザはアクセスを許可または拒否されます。
  - [Secure Telnet(SSH)]:デバイスへのアクセスを要求しているユーザが Telnet アクセス プロファイル基準を満たす場合、そのユーザはアクセスを許可または拒否されます。
  - [HTTP]:HTTP アクセスをこのルールに割り当てます。デバイスへのアクセスを要求しているユーザが HTTP アクセス プロファイル基準を満たす場合、そのユーザは許可または拒否されます。
  - [Secure HTTP(HTTPS)]:デバイスへのアクセスを要求しているユーザが HTTPS アクセス プロファイル基準を満たす場合、そのユーザは許可または拒否されます。
  - [SNMP]:デバイスへのアクセスを要求しているユーザが SNMP アクセス プロファイル基準を満たす場合、そのユーザは許可または拒否されます。
- [アクション]:次のいずれかのオプションを選択します。
  - [許可]:このルールで定義されたインターフェイスおよび IP ソースからのユーザに対してデバイス アクセスを許可します。
  - [拒否]:このルールで定義されたインターフェイスおよび IP ソースからのユーザに対してデバイス アクセスを拒否します。
- [インターフェイスに適用]:このルールに関連付けられるインターフェイスを選択します。次のオプションがあります。
  - [すべて]:すべてのポート、VLAN、および LAG に適用されます。
  - [ユーザ定義]:選択したポート、VLAN、または LAG のみに適用されます。
- [インターフェイス]:インターフェイス番号を入力します。

- [送信元 IP アドレスに適用]: このアクセス プロファイルの適用対象となる送信元 IP アドレスのタイプを選択します。[送信元 IP アドレス] フィールドにはサブネットワークを入力できます。次のいずれかを選択します。
  - [すべて]: すべてのタイプの IP アドレスに適用されます。
  - [ユーザ定義]: フィールドで定義されたタイプの IP アドレスだけに適用されます。
- [IP バージョン]: 送信元アドレスとしてサポートされる IP バージョンを選択します（IPv6 または IPv4）。
- [IP アドレス]: 送信元 IP アドレスを入力します。
- [マスク]: 送信元 IP アドレスのサブネット マスクの形式を選択し、次のいずれかのフィールドに値を入力します。
  - [ネットワーク マスク]: 送信元 IP アドレスが属するサブネットを選択し、サブネット マスクをピリオド区切りの 10 進表記で入力します。
  - [プレフィックス長]: [プレフィックス長] を選択し、送信元 IP アドレス プレフィックスを構成するビット数を入力します。

ステップ 5 [適用] をクリックすると、このルールがアクセス プロファイルに追加されます。

管理アクセス認証

SSH、Telnet、HTTP、HTTPS など、さまざまな管理アクセス方式に認証方式を割り当てることができます。認証処理は、ローカルで、あるいは RADIUS サーバで実行可能です。

承認処理が有効になっている場合、ユーザの ID と読み取り/書き込み特権の両方が検証されます。承認処理が有効になっていない場合、ユーザの ID だけが検証されます。

使用される承認/認証方式は、認証方式の選択順序によって決まります。最初に選択した認証方式が使用不能の場合、次に選択した認証方式が使用されます。たとえば、[RADIUS]、[ローカル] の順に認証方式を選択した場合、設定されたすべての RADIUS サーバに対してプライオリティ順にクエリーが送られて応答がなければ、ユーザはローカルに承認/認証されます。

承認処理が有効になっている場合、認証方式が失敗するか、またはユーザの特権レベルが十分でないと、デバイスへのアクセスを拒否されます。言い換えると、ある認証方式で認証に失敗した場合、デバイスは認証の試行を停止します(そのまま続行して次の認証方式を使用することはありません)。

同様に、承認処理が無効になっていて、ある方式で認証に失敗した場合、デバイスは認証の試行を停止します。

アクセス方式に割り当てる認証方式を定義するには、次のようにします。

ステップ 1 [セキュリティ] > [管理アクセス認証] をクリックします。

ステップ 2 管理アクセス方式の [アプリケーション](タイプ)を入力します。

ステップ 3 [承認] を選択すると、下記で説明する方式のリストに従ってユーザの認証および承認の両方が有効になります。このフィールドを選択しない場合は、認証だけが実行されます。[承認] が有効になっている場合、ユーザの読み取り/書き込み特権が検査されます。この特権レベルは [ユーザ アカウント] ページで設定されます。

ステップ 4 矢印を使用して、[オプションの方式] 列と [選択した方式] 列の間で認証方式を移動します。最初に選択した認証方式が最初に使用されます。

- [RADIUS]:ユーザは RADIUS サーバで承認/認証されます。RADIUS サーバが 1 つ以上定義されている必要があります。Web ベースの設定ユーティリティへのアクセス権限が RADIUS サーバによって付与されるようにするには、RADIUS サーバが「cisco-avpair = shell:priv-lvl=15」を返す必要があります。
- [なし]:ユーザは承認/認証なしでデバイスへのアクセスを許可されます。
- [ローカル]:ユーザ名とパスワードは、ローカル デバイスに格納されているデータと照合されます。これらのユーザ名とパスワードは、[ユーザアカウント] ページで定義されます。

  注 [ローカル] または [なし] は、必ず最後の認証方式として選択する必要があります。[ローカル] または [なし] の後に選択した認証方式はすべて無視されます。

ステップ 5 [適用] をクリックします。選択した認証方式が、そのアクセス方式に割り当てられます。

SSL サーバ

ここではセキュア ソケット レイヤ(SSL)機能について説明します。

具体的な内容は、次のとおりです。

- SSL の概要
- SSL サーバ認証設定

SSL の概要

セキュア ソケット レイヤ(SSL)機能は、デバイスへの HTTPS セッションを開くために使用されます。

デバイス上に存在するデフォルト証明書を使って HTTPS セッションを開くことができます。

デフォルト証明書を使用するとき、ブラウザによっては、証明書が証明機関(CA)によって署名されていないという理由で警告が発生することがあります。信頼されている CA によって署名された証明書を使用するのがベスト プラクティスです。

ユーザ作成の証明書を使って HTTPS セッションを開くには、次のようにします。

1. 証明書を生成します。
2. 証明書を認定するよう CA に要請します。
3. 署名された証明書をデバイスにインポートします。

デフォルトでは、変更可能な証明書がデバイスに含まれています。

HTTPS はデフォルトで有効になっています。

SSL サーバ認証設定

デバイスにあるデフォルトの証明書を置換するために、新しい証明書を生成する必要が生じることがあります。

新しい証明書を作成するには、次のようにします。

ステップ 1 [セキュリティ] > [SSL サーバ] > [SSL サーバ認証設定] をクリックします。

SSL サーバ キー テーブル内に **SSL アクティブ証明書番号** 1 および 2 に関する情報が表示されます。次のフィールドのいずれかを選択します。

これらのフィールドは [編集] ページで定義されます。ただし次のフィールドを除きます。

- [有効期限の開始]:証明書が有効になる最初の日付を指定します。
- [有効期限の終了]:証明書が有効である最後の日付を指定します。
- [証明書ソース]:証明書がシステムによって生成されたか(自動生成)、それともユーザによって生成されたか(ユーザ定義)を指定します。

ステップ 2 アクティブな証明書を選択します。

ステップ 3 [証明書要求の生成] をクリックします。

ステップ 4 次のフィールドを入力します。

- [証明書ID]:アクティブな証明書を選択します。
- [共通名]:完全修飾デバイス URL または IP アドレスを指定します。これを指定しない場合、デフォルトとして(証明書の生成時に)最も低いデバイス IP アドレスになります。
- [組織単位]:組織単位または部署の名前を指定します。
- [組織名]:組織の名前を指定します。
- [ロケーション]:場所または市町村名を指定します。
- [都道府県]:州または都道府県の名前を指定します。
- [国]:国名を指定します。
- [証明書要求]:[証明書要求の生成] ボタンを押したときに作成されるキーを表示します。

ステップ 5 [証明書要求の生成] をクリックします。これにより、証明機関(CA)で入力する必要のあるキーが作成されます。[証明書要求] フィールドからこれをコピーします。

証明書をインポートするには、次のようにします。

ステップ 1 [セキュリティ] > [SSL サーバ] > [SSL サーバ認証設定] をクリックします。

ステップ 2 [証明書のインポート] をクリックします。

ステップ 3 次のフィールドを入力します。

- [証明書ID]:アクティブな証明書を選択します。
- [証明書ソース]:ユーザ定義の証明書であることを表示します。

- [証明書]:受信される証明書にコピーします。
- [RSAキーペアのインポート]:新しい RSA キーペアへのコピーを有効にするには、このフォールドを選択します。
- [公開キー]:RSA 公開キーにコピーします。
- [秘密キー(暗号化)]:暗号化形式で RSA 秘密キーにコピーするには、このフィールドを選択します。
- [秘密キー(プレーンテキスト)]:プレーンテキスト形式で RSA 秘密キーにコピーするには、このフィールドを選択します。

ステップ 4 [適用] をクリックして、実行コンフィギュレーションに変更を適用します。

ステップ 5 このキーを暗号化して表示するには、[機密データを暗号化して表示] をクリックします。このボタンをクリックした場合、暗号化形式で秘密キーが([適用] をクリックしたときに)コンフィギュレーション ファイルに書き込まれます。テキストが暗号化形式で表示されているときには、ボタンが [機密データを平文で表示] に変わり、再びプレーンテキストでテキストを表示できるようになります。

[詳細] ボタンをクリックすると、証明書と RSA キーペアが表示されます。これを使用して、証明書および RSA キーペアを他のデバイスにコピーします(コピー/貼り付けを使用)。[機密データを暗号化して表示] をクリックすると、秘密キーが暗号化形式で表示されます。

デバイスで新しい自己生成証明書を作成するには、次のようにします。

ステップ 1 [セキュリティ] > [SSL サーバ] > [SSL サーバ認証設定] をクリックします。

ステップ 2 証明書を選択して [編集] をクリックします。

ステップ 3 必要に応じて次のフィールドに入力します。

- [RSA キーの再生成]:RSA キーを再生成する場合に選択します。
- [キー長]:オプションから必要なキー長を選択します。
- [共通名]:共通名を入力します。
- [組織単位]:証明書の組織単位の名前を入力します。
- [場所]:証明書の組織単位の場所を入力します。
- [都道府県/州]:証明書の組織単位の都道府県/州を入力します。
- [国]:証明書の組織単位の国を入力します。
- [期間]:証明書を有効にする時間の長さを入力します。

ステップ 4 [適用] をクリックして、実行コンフィギュレーションに変更を適用します。

SSH クライアント

「セキュリティ:SSH クライアント」を参照してください。

TCP/UDP サービス

[TCP/UDP サービス] ページで、主にセキュリティを強化する目的で、デバイスのさまざまな TCP/UDP サービスを有効にすることができます。

デバイスで提供される TCP/UDP サービスは次のとおりです。

- **HTTP**:工場出荷時に有効に設定されています
- **HTTPS**:工場出荷時に有効に設定されています
- **SNMP**:工場出荷時に無効に設定されています
- **Telnet**:工場出荷時に無効に設定されています
- **SSH**:工場出荷時に無効に設定されています

このウィンドウには、アクティブな TCP 接続も表示されます。

TCP/UDP サービスを設定するには、次のようにします。

ステップ 1 [セキュリティ] > [TCP/UDP サービス] をクリックします。

ステップ 2 サービスが表示されたら、次の TCP/UDP サービスを有効または無効にします。

- [HTTP サービス]:HTTP サービスが有効/無効のどちらになっているかを示します。
- [HTTPS サービス]:HTTPS サービスが有効/無効のどちらになっているかを示します。
- [SNMP サービス]:SNMP サービスが有効/無効のどちらになっているかを示します。
- [Telnet サービス]:Telnet サービスが有効/無効のどちらになっているかを示します。

- [SSH サービス]:SSH サーバ サービスが有効/無効のどちらになっているかを示します。

ステップ 3 [適用] をクリックします。サービスが実行コンフィギュレーション ファイルに書き込まれます。

[TCP サービステーブル]に、各サービスについて次のフィールドが表示されます。

- [サービス名]:TCP サービスを提供するためにデバイスが使用するアクセス方式。
- [タイプ]:サービスが使用する IP プロトコル。
- [ローカル IP アドレス]:サービスを提供するためにデバイスが使用するローカル IP アドレス。
- [ローカルポート]:サービスを提供するためにデバイスが使用するローカル TCP ポート。
- [リモート IP アドレス]:サービスを要求しているリモート デバイスの IP アドレス。
- [リモートポート]:サービスを要求しているリモート デバイスの TCP ポート。
- [状態]:サービスのステータス。

UDP サービス テーブルに表示される情報は次のとおりです。

- [サービス名]:UDP サービスを提供するためにデバイスが使用するアクセス方式。
- [タイプ]:サービスが使用する IP プロトコル。
- [ローカル IP アドレス]:サービスを提供するためにデバイスが使用するローカル IP アドレス。
- [ローカルポート]:サービスを提供するためにデバイスが使用するローカル UDP ポート。
- [アプリケーションインスタンス]:UDP サービスのサービス インスタンス。(たとえば 2 つの送信元が同じ宛先にデータを送る場合。)

ストーム制御

ここでは、ストーム制御について説明します。具体的な内容は、次のとおりです。

- ストーム制御
- ストーム制御統計情報

ブロードキャスト フレーム、マルチキャスト フレーム、または Unknown ユニキャスト フレームが受信された場合、そのフレームが複製され、フレームのコピーがすべての該当出力ポートに送信されます。つまり実際には、該当 VLAN に属するすべてのポートに送信されます。このように、1 つの入力フレームに対して多数のコピーが生成されるので、トラフィック ストームが発生するおそれがあります。

ストーム防止機能を利用すると、デバイスに入ってくるフレームの数を制限し、この制限の対象としてカウントされるフレームのタイプを指定することができます。

ブロードキャスト フレーム、マルチキャスト フレーム、または不明なユニキャスト フレームのレートがユーザ定義のしきい値より高い場合、しきい値を超えて受信されたフレームは破棄されます。

ストーム制御

ストーム制御を定義するには、次のようにします。

ステップ 1 [セキュリティ] > [ストーム制御] > [ストーム制御設定] の順にクリックします。

ステップ 2 ポートを選択して [編集] をクリックします。

ステップ 3 パラメータを入力します。

- [インスタンス]: ストーム制御を有効にする対象のポートを選択します。

[不明なユニキャストストーム制御]

- [ストーム制御状態]: ユニキャスト パケットのストーム制御を有効にする場合に選択します。
- [レートしきい値]: 不明なパケットを転送できるようにする最大レートを入力します。この値は、**キロビット/秒**または使用可能な全帯域幅の**パーセンテージ**で入力できます。
- [トラップオンストーム]: ポート上でストームが発生したときにトラップを送信する場合に選択します。これが選択されていない場合は、トラップが送信されません。

- [シャットダウンオンストーム]:ポート上でストームが発生したときにポートをシャットダウンする場合に選択します。これが選択されていない場合は、余剰トラフィックが破棄されます。

[マルチキャスト ストーム制御]

- [ストーム制御状態]:マルチキャスト パケットのストーム制御を有効にする場合に選択します。
- [マルチキャストタイプ]:ストーム制御を実装する次のタイプのマルチキャスト パケットのいずれかを選択します。
  - [すべて]:ポート上のすべてのマルチキャスト パケットに対するストーム制御を有効にします。
  - [登録済みマルチキャスト]:ポート上の登録済みマルチキャスト アドレスに対するストーム制御のみを有効にします。
  - [登録解除済みマルチキャスト]:ポート上の登録解除済みマルチキャスト ストーム制御のみを有効にします。
- [レートしきい値]:不明なパケットを転送できるようにする最大レートを入力します。この値は、**キロビット/秒**または使用可能な全帯域幅の**パーセンテージ**で入力できます。
- [トラップオンストーム]:ポート上でストームが発生したときにトラップを送信する場合に選択します。これが選択されていない場合は、トラップが送信されません。
- [シャットダウンオンストーム]:ポート上でストームが発生したときにポートをシャットダウンする場合に選択します。これが選択されていない場合は、余剰トラフィックが破棄されます。

[ブロードキャスト ストーム制御]

- [ストーム制御状態]:ブロードキャスト パケットのストーム制御を有効にする場合に選択します。
- [レートしきい値]:不明なパケットを転送できるようにする最大レートを入力します。この値は、**キロビット/秒**または使用可能な全帯域幅の**パーセンテージ**で入力できます。
- [トラップオンストーム]:ポート上でストームが発生したときにトラップを送信する場合に選択します。これが選択されていない場合は、トラップが送信されません。
- [シャットダウンオンストーム]:ポート上でストームが発生したときにポートをシャットダウンする場合に選択します。これが選択されていない場合は、余剰トラフィックが破棄されます。

ステップ 4 [適用] をクリックします。ストーム制御が変更され、実行コンフィギュレーション ファイルが更新されます。

ストーム制御統計情報

ストーム制御統計情報を表示するには、次のようにします。

ステップ 1 [セキュリティ] > [ストーム制御] > [ストーム制御統計情報] の順にクリックします。

ステップ 2 インターフェイスを選択します。

ステップ 3 [リフレッシュレート] を入力します。統計情報の更新頻度を選択します。オプションは次のとおりです。

- [リフレッシュなし]:統計情報はリフレッシュされません。
- [15 秒]:統計情報は 15 秒ごとにリフレッシュされます。
- [30 秒]:統計情報は 30 秒ごとにリフレッシュされます。
- [60 秒]:統計情報は 60 秒ごとにリフレッシュされます。

不明なユニキャスト、マルチキャスト、およびブロードキャスト ストーム制御に関する次の統計情報が表示されます。

- [マルチキャストトラフィックタイプ]:(マルチキャスト トラフィックの場合のみ):[登録済み] または [未登録]。
- [通過したバイト数]:受信バイト数。
- [ドロップされたバイト数]:ストーム制御が原因でドロップされたバイト数。
- [最終ドロップ時刻]:最後のバイトがドロップされた時刻。

ステップ 4 すべてのインターフェイスのカウンタを完全にクリアするには、[すべてのインターフェイスカウンタのクリア] をクリックします。1 つのインターフェイスのカウンタを完全にクリアするには、そのインターフェイスを選択し、[インターフェイス カウンタのクリア] をクリックします。

ポート セキュリティ

注 ポート セキュリティは、802.1X が有効になっているポートまたは SPAN 宛先として定義されたポート上では有効にすることができません。

特定の MAC アドレスからのポート アクセスを制限することにより、ネットワークのセキュリティを強化できます。アクセスを制限したい送信元 MAC アドレスは、動的（ダイナミック）に学習させることも、静的（スタティック）に設定することもできます。

ポート セキュリティを設定すると、受信された MAC アドレスと学習された MAC アドレスが照合されます。ロックされているポートには、特定の MAC アドレスからのみアクセスできます。

ポート セキュリティには次の 4 つのモードがあります。

- [クラシックロック]:ポート上で学習済みのすべての MAC アドレスがロックされます。新しい MAC アドレスは学習されません。また、学習済み MAC アドレスがエージングしたり再学習されたりすることはありません。
- [限定ダイナミックロック]:デバイスは、許容最大アドレス数として設定された制限に達するまで MAC アドレスを学習します。制限に達すると、デバイスはそれ以上 MAC アドレスを学習しません。このモードでは、学習済み MAC アドレスがエージングしたり再学習されたりすることがあります。
- [無期限セキュア]:ポートに関連付けられている現在のダイナミック MAC アドレスを保持します（スタート コンフィギュレーション ファイルにコンフィギュレーションが保存されている間）。ポートの許容最大アドレス数に達するまで、新しい MAC アドレスを「無制限セキュア」対象として学習することができます。再学習とエージングは無効です。
- [リセット時にセキュア削除]:リセット後に、ポートに関連している現在のダイナミック MAC アドレスを削除します。ポートの許容最大アドレス数に達するまで、新しい MAC アドレスを「リセット時に削除」対象として学習することができます。再学習とエージングは無効です。

新しい MAC アドレスから届いたフレームがポート上で検出され、かつ、その MAC アドレスが承認されていない場合、（つまり、ポート セキュリティがクラシック ロック モードであり、届いた MAC アドレスがロックされている場合、または、ポート セキュリティが限定ダイナミック ロック モードであり、学習済み MAC アドレスが上限数に達している場合）、防御機構が働き、次のいずれかの処理が実行されます。

- フレームが廃棄される
- フレームが転送される
- ポートが停止する

安全な MAC アドレスから送信されたフレームが別のポートに届いた場合、そのフレームは転送されますが、そのポート上でその MAC アドレスが学習されることはありません。

これらの処理のいずれかを実行するのに加え、トラップを生成することができます。その際、トラップの生成頻度を下げて回数を減らし、スイッチが過負荷状態になるのを回避することができます。

ポート セキュリティを設定するには、次のようにします。

ステップ 1 [セキュリティ] > [ポートセキュリティ] をクリックします。

ステップ 2 変更対象となるインターフェイスを選択して、[編集] をクリックします。

ステップ 3 パラメータを入力します。

- [インターフェイス]: インターフェイス名を選択します。
- [インターフェイスステータス]: ポートをロックするには、このフィールドを選択します。
- [学習モード]: ポートのロックの種類を選択します。このフィールドの値を指定するには、[インターフェイスステータス]のロックを解除する必要があります。[学習モード] フィールドは、[インターフェイスステータス] フィールドがロックされている場合にのみ有効になります。[学習モード]の値を変更するには、[インターフェイスステータス]のロックをいったん解除する必要があります。変更後、[インターフェイスステータス]を元に戻すことができます。次のオプションがあります。
  - [クラシックロック]: すでに学習済みのアドレス数にかかわらず、ポートをただちにロックします。
  - [限定ダイナミックロック]: ポートに関連付けられている現在のダイナミック MAC アドレスを削除することで、ポートをロックします。このポートに対して設定した上限数に達するまで MAC アドレスが学習されます。また、MAC アドレスはエージングしたり再学習されたりすることがあります。
  - [無期限セキュア]: ポートに関連している現在のダイナミック MAC アドレスを保持し、([アドレスの最大許容数] で設定される) ポートの許容最大アドレス数に達するまで学習します。再学習とエージングは無効です。
  - [リセット時にセキュア削除]: リセット後に、ポートに関連している現在のダイナミック MAC アドレスを削除します。ポートの許容最大アドレス数に達するまで、新しい MAC アドレスを「リセット時に削除」対象として学習することができます。再学習とエージングは無効です。

- [アドレスの最大許容数]:学習モードとして [限定ダイナミックロック] を選択した場合、このポート上で学習できる MAC アドレスの最大数を入力します。数値 0 は、このポート上でスタティック MAC アドレスだけを設定できることを意味します。
- [違反時アクション]:ロックされているポートに届いたパケットに適用する処理を選択します。次のオプションがあります。
  - [廃棄]:学習されていない送信元から届いたパケットを廃棄します。
  - [転送]:不明な送信元からのパケットを転送します。MAC アドレスは学習されません。
  - [シャットダウン]:学習されていない送信元からのパケットを廃棄し、ポートをシャットダウンします。ポートが再アクティブ化されるか、デバイスがリブートされるまで、ポートはシャットダウンしたままになります。
- [トラップ]:ロックされているポートにパケットが届いたときにトラップを有効にするには、このフィールドを選択します。トラップは、ロックが侵害されようとしたことを通知するものです。クラシック ロック モードの場合、トラップの内容は、新たに受信された MAC アドレスです。限定ダイナミック ロック モードの場合、トラップの内容は、上限数を超過した分の新しい MAC アドレスです。
- [トラップ間隔]:トラップとトラップの間の最短経過時間を入力します(単位:秒)。

ステップ 4 [適用] をクリックします。ポート セキュリティが変更され、実行コンフィギュレーション ファイルが更新されます。

802.1X 認証

802.1X 認証については、「セキュリティ:802.1X 認証」という章の情報を参照してください。

サービス拒絶防御

サービス妨害(DoS)攻撃は、デバイスをユーザにとって使用不能にしようとするハッカーの妨害行為です。

DoS 攻撃は、大量の外部要求通信でデバイスを飽和させて、正当なトラフィックに応答できないようにします。このような攻撃により、デバイス CPU オーバーロードがよく発生します。

- Martian アドレス
- SYN フィルタリング
- SYN レート保護
- ICMP フィルタリング
- IP フラグメント フィルタリング

セキュア コア テクノロジー(SCT)

DoS 攻撃への対抗策としてデバイスで採用できる方式の 1 つは、SCT の使用です。デバイスでは SCT はデフォルトで有効になっており、無効にできません。

シスコ デバイスは拡張機能を備えたデバイスであり、エンドユーザ(TCP)トラフィックに加えて管理トラフィック、プロトコル トラフィックおよびスヌーピング トラフィックを扱います。

SCT を使用すると、受信されるトラフィックの総量にかかわらず、デバイスは管理トラフィックとプロトコル トラフィックを確実に受け取って処理することができます。これを実現するために、CPU への TCP トラフィックがレート制限されます。

他の機能との干渉は発生しません。

SCT は [セキュリティ スイート設定] ページ([詳細] ボタン)で監視できます。

DoS 攻撃の種類

たとえば次のように DoS 攻撃が発生する可能性があります。

- TCP SYN パケット:(しばしば送信者アドレスを偽装した)膨大な数の TCP SYN パケットによって攻撃が行われることがあります。これらのパケットが届くたびに、デバイスは TCP/SYN-ACK パケット(確認応答)を送り返し、送信者アドレスからの応答パケット(ACK パケットに対する応答)を待機することにより、ハーフオープン接続を生成します。しかし送信者アドレスが偽装され

ているため、応答は決して届きません。このようなハーフオープン接続のために、デバイスで作成できる接続数が飽和し、正当な要求への応答が妨げられます。加えて、CPU へのパケット数は潜在的に限定されており、攻撃トラフィックがこのパケット数を消費する可能性があります。

このようなパケットを [SYN保護] ページでブロックできます。

- TCP SYN-FIN パケット：新しい TCP 接続を作成するために SYN パケットが送られます。接続を閉じるために TCP FIN パケットが送られます。通常、1 つのパケット内に SYN と FIN の両方のフラグが設定されることは決してありません。したがって、そのようなパケットはデバイスに対する攻撃である可能性があり、ブロックすべきです。

  [SYN保護] ページでは、どんな現象を SYN 攻撃と見なすかを定義できます。デバイスがインターフェイスでそのような攻撃を検出した場合、このページにそれが報告されます。

DoS 攻撃に対する防御

*サービス妨害(DoS)*防御機能により、システム管理者は次のような方法で DoS 攻撃に対抗できます。

- TCP SYN 保護の有効化。この機能を有効にすると、SYN パケット攻撃が検出されたときにレポートが発行されます。1 秒あたりの SYN パケット数が、ユーザ設定しきい値を超えた場合に、SYN 攻撃であると識別されます。
- SYN-FIN パケットをブロックできます。

機能間の依存関係

この機能と他の機能の間に依存関係はありません。

デフォルト コンフィギュレーション

DoS 防御機能のデフォルトは次のとおりです。

- DoS 防御機能はデフォルトで無効になっています。
- SYN-FIN 保護機能はデフォルトで有効です（DoS 防御機能が無効になっている場合でも）。
- SYN 保護が有効になっている場合、デフォルトは「レポート」です。デフォルトしきい値は 1 秒あたり 30 SYN パケットです。
- その他のすべての DoS 防御機能はデフォルトで無効になっています。

セキュリティ スイート設定

注 DoS 攻撃防止機能をアクティブ化するには、その前に、すべての Access Control List (ACL; アクセス コントロール リスト)および拡張 QoS ポリシーをポートからアンバインドしておく必要があります。ポートで DoS 防御機能がアクティブ化されている間、ACL と拡張 QoS ポリシーは非アクティブ化されます。

DoS 防御機能のグローバル設定および SCT の監視を行うには、次のようにします。

ステップ 1 [セキュリティ] > [サービス拒絶防御] > [セキュリティスイート設定] をクリックします。

[CPU 保護メカニズム]:[有効] は、SCT が有効になっていることを示します。

ステップ 2 [CPU 利用率] の横の [詳細] をクリックすると [CPU 利用率] ページに移動し、CPU リソース利用率情報が表示されます。

ステップ 3 この機能を設定するには、[TCP SYN 保護] の横にある [編集] をクリックします。

ステップ 4 [DoS 防御] を選択するとこの機能が有効になります。

- [無効]: この機能が無効になります。
- [システムレベルの防御]: Stacheldraht(分散型)、Invasor(トロイの木馬)、および Back Orifice(トロイの木馬)による攻撃を防ぐ機能が有効になります。
- [システムレベルおよびインターフェイスレベルの防御]: Stacheldraht(分散型)、Invasor(トロイの木馬)、および Back Orifice(トロイの木馬)による攻撃を防ぐ機能が有効になります。

ステップ 5 [システムレベルの防御] または [システムレベルおよびインターフェイスレベルの防御] を選択した場合、次の [DoS防御] オプションの 1 つまたは複数を有効にしてください。

- [Stacheldraht(分散型)]: 送信元 TCP ポートが 16660 に等しい TCP パケットを破棄します。
- [Invasor(トロイの木馬)]: 宛先 TCP ポートが 2140 に等しく、送信元 TCP ポートが 1024 に等しい TCP パケットを破棄します。
- [Back Orifice(トロイの木馬)]: 宛先 UDP ポートが 31337 に等しく、送信元 UDP ポートが 1024 に等しい UDP パケットを破棄します。

ステップ 6 必要に応じて次の項目をクリックします。

- [Martian アドレス]:[編集] をクリックすると [Martian アドレス] ページに移動します。

- [SYN フィルタリング]:[編集] をクリックすると [SYN フィルタリング] ページに移動します。
- [SYN レート保護]:(レイヤ 2 のみ)[編集] をクリックすると [SYN レート保護] ページに移動します。
- [ICMP フィルタリング]:[編集] をクリックすると [ICMP フィルタリング] ページに移動します。
- [IIP フラグメント化]:[編集] をクリックすると [IP フラグメント フィルタリング] ページに移動します。

ステップ 7 [適用] をクリックします。サービス拒絶防御のセキュリティ スイート設定が実行コンフィギュレーション ファイルに書き込まれます。

SYN 保護

デバイスを攻撃するためにハッカーがネットワーク ポートを使用して SYN 攻撃を仕掛け、結果として TCP リソース(バッファ)と CPU パワーが消費される可能性があります。

CPU は SCT を使って保護されるため、CPU への TCP トラフィックは制限されます。しかし、高いレートの SYN パケットによって 1 つ以上のポートが攻撃された場合、CPU は攻撃者のパケットだけを受け取り、こうしてサービス拒否が発生します。

SYN 保護機能を使用すると、CPU は各ネットワーク ポートから CPU に入ってくる 1 秒ごとの SYN パケット数をカウントします。

この数値がしきい値より高い場合、SYSLOG メッセージが生成されますが、パケットはブロックされません。

SYN 保護を設定するには、次のようにします。

ステップ 1 [セキュリティ] > [サービス拒絶防御] > [SYN 保護] をクリックします。

ステップ 2 パラメータを入力します。

- [SYN-FIN パケットのブロック]:選択すると、この機能が有効になります。すべてのポートで、SYN と FIN の両方のフラグを持つすべての TCP パケットがドロップされます。
- [SYN 保護モード]:次の 3 つのモードから選択します。
  - [無効]:特定のインターフェイスでこの機能が無効になります。

- [レポート]:SYSLOG メッセージを生成します。しきい値を超えた場合、ポートのステータスが [攻撃済み] に変わります。
- [ブロックとレポート]:TCPSYN 攻撃が見つかった場合、システム宛ての TCP SYN パケットはドロップされて、ポートのステータスが [ブロック済み] に変わります。

- [SYN 保護しきい値]:(「自分への MAC を含む SYN を拒否」ルールがポートで適用されて)SYN パケットをブロックするようになる、1 秒あたりの SYN パケット数。
- [SYN 保護期間]:(「自分への MAC を含む SYN を拒否」ルールがポートからバインド解除されて)SYN パケットのブロックを解除するまでの秒数。

ステップ 3 [適用] をクリックします。SYN 保護が定義され、実行コンフィギュレーション ファイルが更新されます。

SYN 保護インターフェイス テーブルには、(ユーザからの要求に従って)ポートまたは LAG ごとに次のフィールドが表示されます。

- [現在のステータス]:インターフェイスのステータス。表示される値は次のとおりです。
  - [ノーマル]:このインターフェイスで攻撃は検出されませんでした。
  - [攻撃済み]:このインターフェイスで攻撃が検出されました。
- [最新の攻撃]:システムで最後に検出された SYN-FIN 攻撃の日付とシステム アクション(**レポート済み**)。

Martian アドレス

[Martian アドレス] ページでは、ネットワークで検出されると攻撃と見なされる IP アドレスを入力できます。このようなアドレスからのパケットは破棄されます。

デバイスは、IP プロトコルの観点から言うと不正なアドレスであるいくつかの予約済み Martian アドレスをサポートしています。サポートされる予約済み Martian アドレスは、

- [Martian アドレス] ページで不正と定義されているアドレス。
- ループバック アドレスなど、プロトコルの観点から不正と見なされるアドレス。次の範囲内のアドレスを含みます。
  - **0.0.0.0/8(ただし送信元アドレスとしての 0.0.0.0/32 を除く)**:このブロックのアドレスは、このネットワーク上の送信元ホストを参照します。

- **127.0.0.0/8**：インターネット ホスト ループバック アドレスとして使用されます。
- **192.0.2.0/24**：ドキュメンテーションおよびコード例で TEST-NET として使用されます。
- **224.0.0.0/4（送信元 IP アドレスとして）**：IPv4 マルチキャスト アドレス割り当てで使用されます。以前は「クラス D アドレス空間」と呼ばれていました。
- **240.0.0.0/4（ただし宛先アドレスとしての 255.255.255.255/32 を除く）**：予約済みアドレス範囲。以前は「クラス E アドレス空間」と呼ばれていました。

さらに、DoS 防御用に新しい Martian アドレスを追加することもできます。Martian アドレスを含むパケットは破棄されます。

Martian アドレスを定義するには、次のようにします。

ステップ 1 [セキュリティ] > [サービス拒絶防御] > [Martian アドレス] をクリックします。

ステップ 2 [予約済みのMartian アドレス] を選択して [適用] をクリックすると、システム レベル防御リストに予約済みの Martian アドレスが含まれるようになります。

ステップ 3 Martian アドレスを追加するには、[追加] をクリックします。

ステップ 4 パラメータを入力します。

- [IP バージョン]：サポートされる IP バージョンを示します。現在、IPv4 のみがサポートされています。
- [IP アドレス]：拒否する IP アドレスを入力します。表示される値は次のとおりです。
  - [予約済みリストから]：予約済みリストからウェルノウン IP アドレスを選択します。
  - [新規 IP アドレス]：IP アドレスを入力します。
- [マスク]：拒否する IP アドレスの範囲を定義するために IP アドレスのマスクを入力します。値は次のとおりです。
  - [ネットワークマスク]：ドット付き 10 進表記でのネットワーク マスク。
  - [プレフィックス長]：サービス拒絶防御を有効にする対象の IP アドレス範囲を定義するための IP アドレス プレフィックスを入力します。

ステップ 5 [適用] をクリックします。Martian アドレスが実行コンフィギュレーション ファイルに書き込まれます。

SYN フィルタリング

[SYN フィルタリング] ページでは、SYN フラグを含む、1 つ以上のポート宛ての TCP パケットをフィルタリングできます。

SYN フィルタを定義するには、次のようにします。

ステップ 1 [セキュリティ] > [サービス拒絶防御] > [SYN フィルタリング] をクリックします。

ステップ 2 [追加] をクリックします。

ステップ 3 パラメータを入力します。

- [インターフェイス]: フィルタを定義するインターフェイスを選択します。
- [IPv4アドレス]: フィルタを定義する対象の IP アドレスを入力するか、[すべてのアドレス] を選択します。
- [ネットワークマスク]: IP アドレス形式で、フィルタを有効にする対象のネットワーク マスクを入力します。次のいずれかを入力します。
  - [マスク]: ドット付き 10 進表記のネットワーク マスク。
  - [プレフィックス長]: サービス拒絶防御を有効にする対象の IP アドレス範囲を定義するための IP アドレス プレフィックスを入力します。
- [TCP ポート]: フィルタされる宛先 TCP ポートを次のように選択します。
  - [既知のポート]: リストからポートを選択します。
  - [ユーザ定義]: ポート番号を入力します。
  - [すべてのポート]: すべてのポートをフィルタするには、このフィールドを選択します。

ステップ 4 [適用] をクリックします。SYN フィルタが定義され、実行コンフィギュレーション ファイルが更新されます。

SYN レート保護

[SYN レート保護] ページでは、入力ポートで受信される SYN パケットの数を制限できます。これにより、パケット処理のために開かれる新しい接続の数をレート制限することで、サーバに対する SYN フラッドの影響を軽減できる可能性があります。

SYN レート保護を定義するには、次のようにします。

ステップ 1 [セキュリティ] > [サービス拒絶防御] > [SYN レート保護] をクリックします。

このページには、インターフェイスごとに、現在定義されている SYN レート保護が表示されます。

ステップ 2 [追加] をクリックします。

ステップ 3 パラメータを入力します。

- [インターフェイス]:レート保護を定義するインターフェイスを選択します。
- [IP アドレス]:SYN レート保護を定義する対象の IP アドレスを入力するか、[すべてのアドレス] を選択します。IP アドレスを入力する場合には、マスクまたはプレフィックス長のいずれかを入力してください。
- [ネットワークマスク]:送信元 IP アドレスのサブネット マスクの形式を選択し、次のいずれかのフィールドに値を入力します。
  - [マスク]:送信元 IP アドレスが属するサブネットを選択し、サブネット マスクをドット区切り 10 進表記で入力します。
  - [プレフィックス長]:[プレフィックス長] を選択し、送信元 IP アドレス プレフィックスを構成するビット数を入力します。
- [SYN レート制限]:受信してもよい SYN パケットの数を入力します。

ステップ 4 [適用] をクリックします。SYN レート保護が定義され、実行コンフィギュレーションが更新されます。

ICMP フィルタリング

[ICMP フィルタリング] ページでは、特定の送信元からの ICMP パケットをブロックできます。これにより、ICMP 攻撃が発生した場合にネットワークの負荷を減らすことができます。

ICMP フィルタリングを定義するには、次のようにします。

ステップ 1 [セキュリティ] > [サービス拒絶防御] > [ICMP フィルタリング] をクリックします。

ステップ 2 [追加] をクリックします。

ステップ 3 パラメータを入力します。

- [インターフェイス]:ICMP フィルタリングを定義するインターフェイスを選択します。
- [IP アドレス]:ICMP パケット フィルタリングをアクティブにする対象の IPv4 アドレスを入力するか、または [すべてのアドレス] を選択してすべての送信元アドレスからの ICMP パケットをブロックします。IP アドレスを入力する場合には、マスクまたはプレフィックス長のいずれかを入力してください。
- [ネットワークマスク]:送信元 IP アドレスのサブネット マスクの形式を選択し、次のいずれかのフィールドに値を入力します。
  - [マスク]:送信元 IP アドレスが属するサブネットを選択し、サブネット マスクをドット区切り 10 進表記で入力します。
  - [プレフィックス長]:[プレフィックス長] を選択し、送信元 IP アドレス プレフィックスを構成するビット数を入力します。

ステップ 4 [適用] をクリックします。ICMP フィルタリングが定義され、実行コンフィギュレーションが更新されます。

IP フラグメント フィルタリング

[IP フラグメント化] ページでは、フラグメント化された IP パケットをブロックできます。

フラグメント化された IP をブロックする機能を設定するには、次のようにします。

ステップ 1 [セキュリティ] > [サービス拒絶防御] > [IP フラグメントフィルタリング] をクリックします。

ステップ 2 [追加] をクリックします。

ステップ 3 パラメータを入力します。

- [インターフェイス]:IP フラグメンテーションを定義するインターフェイスを選択します。
- [IP アドレス]:フラグメント化された IP パケットをフィルタリングする対象の IP ネットワークを入力するか、または [すべてのアドレス] を選択してすべてのアドレスからの IP フラグメント化パケットをブロックします。IP アドレスを入力する場合には、マスクまたはプレフィックス長のいずれかを入力してください。
- [ネットワークマスク]:送信元 IP アドレスのサブネット マスクの形式を選択し、次のいずれかのフィールドに値を入力します。
  - [マスク]:送信元 IP アドレスが属するサブネットを選択し、サブネット マスクをドット区切り 10 進表記で入力します。
  - [プレフィックス長]:[プレフィックス長] を選択し、送信元 IP アドレス プレフィックスを構成するビット数を入力します。

ステップ 4 [適用] をクリックします。IP フラグメンテーションが定義され、実行コンフィギュレーション ファイルが更新されます。

18

セキュリティ:802.1X 認証

ここでは、802.1X 認証について説明します。

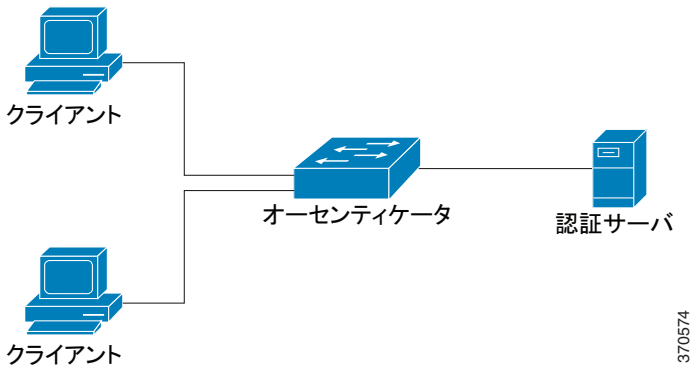
具体的な内容は、次のとおりです。

概要

802.1X 認証を使用すると、権限がないクライアントは、公衆アクセス可能なポート経由での接続が制限されます。802.1X 認証は、クライアント/サーバ モデルです。このモデルでは、ネットワーク デバイスは次の特定の役割を果たします。

- クライアントまたはサプリカント
- オーセンティケータ
- 認証サーバ

次の図で説明します。



ネットワーク デバイスは、ポートごとにクライアント/サプリカント、オーセンティケータ、またはその両方として使用することができます。

クライアントまたはサプリカント

クライアントまたはサプリカントとは、LAN へのアクセスを要求するネットワーク デバイスです。このクライアントはオーセンティケータに接続されます。

クライアントが認証に 802.1x プロトコルを使用する場合、クライアントは、802.1x プロトコルのサプリカントの部分と EAP プロトコルのクライアントの部分を実行します。

オーセンティケータ

オーセンティケータは、サプリカント ポートの接続先となる、ネットワーク サービスを提供するネットワーク デバイスです。

802.1x ベース認証では、オーセンティケータが 802.1x メッセージ（EAPOL パケット）から EAP メッセージを抽出し、RADIUS プロトコルを使用してこれを認証サーバに渡します。

ポートは認証モードに設定されます。詳細については、「ポート ホスト モード」を参照してください。

認証サーバ

認証サーバは、クライアントの実際の認証を実行します。デバイス用の認証サーバは、EAP 拡張機能を備えた RADIUS 認証サーバです。

オープンアクセス

オープン（モニタリング）アクセス機能は、実際の認証失敗と、802.1x 環境のコンフィギュレーションの誤りやリソース不足が原因で生じる失敗を区別するのに役立ちます。

オープン アクセスを使用することにより、システム管理者はネットワークに接続しているホストのコンフィギュレーション上の問題を容易に把握できるようになります。さらにこの機能は、不適切な状態を監視して、これらの問題を修正できるようにします。

オープン アクセスがインターフェイスで有効になっている場合、スイッチは RADIUS サーバから受け取った失敗をすべて成功と見なし、認証結果にかかわらず、インターフェイスに接続しているステーションにネットワークへのアクセスを許可します。

通常の動作では、認証が有効なポート上のトラフィックは認証と承認が正常に完了するまでブロックされますが、オープン アクセスにより、その動作が変更されます。デフォルトの認証動作では、Extensible Authentication Protocol over LAN（EAPoL）を除くすべてのトラフィックがブロックされます。ただし、オープン アクセスでは、認証（802.1X ベース、MAC ベース、および WEB ベース）が有効になっている場合でも、すべてのトラフィックに対する無制限のアクセスを許可するオプションが管理者に提供されます。

RADIUS アカウンティングが有効になっている場合、認証試行をログに記録し、監査証跡を使用して、ネットワークに接続しているユーザやシステムを把握できます。

エンド ユーザや、ネットワークに接続されたホストへの影響はありません。オープンアクセスは、[ポート認証] ページから有効化できます。

ポート認証状態

ポート認証状態により、クライアントにネットワークへのアクセス権が付与されるかどうかが決まります。

ポートの管理状態は [ポート認証] ページで設定できます。

次の値のいずれかを使用できます。

- [強制許可]

  ポート認証は無効で、ポートはスタティック設定に従い、認証を行わずにすべてのトラフィックを送信します。スイッチは、802.1x EAPOL 開始メッセージを受信すると、EAP 成功メッセージを格納した 802.1x EAP パケットを送信します。

デフォルトでは、この状態です。

- [強制無許可]

  ポート認証は無効で、ポートはゲスト VLAN および非認証 VLAN 経由ですべてのトラフィックを送信します。詳細については、「ホストおよびセッション認証」を参照してください。スイッチは、802.1x EAPOL 開始メッセージを受信すると、EAP 失敗メッセージを格納した 802.1x EAP パケットを送信します。

- [自動]

  ポート認証は、設定済みのポート ホスト モードおよびポートに設定されている認証方式に従って有効になります。

ポート ホスト モード

ポートは、次のポート ホストモードに設定できます([ホストおよびセッション認証]ページで設定)。

- [単一ホスト モード]

  許可されたクライアントが存在する場合にポートが許可されます。1 つのポートには 1 つのホストのみ許可されます。

  ポートが許可されておらず、ゲスト VLAN が有効な場合、タグのないトラフィックはゲスト VLAN に再マッピングされます。タグ付きトラフィックは、ゲスト VLAN か非認証 VLAN に所属する場合以外は、ドロップされます。ポートでゲスト VLAN が無効な場合、非認証 VLAN に所属するタグ付きトラフィックのみがブリッジされます。

  ポートが許可されると、許可されたホストからのトラフィックは、タグなしのものもタグ付きのものも、スタティック VLAN メンバーシップ ポート設定に従ってブリッジされます。その他のホストからのトラフィックはドロップされます。

  ユーザは、許可されたホストからのタグなしトラフィックが、認証プロセス中に RADIUS サーバによる割り当て済み VLAN に再マッピングされるように指定することもできます。タグ付きトラフィックは、RADIUS による割り当て済み VLAN か非認証 VLAN に所属する場合以外は、ドロップされます。ポート上の RADIUS VLAN 割り当ては、[ポート認証] ページで設定します。

- [複数ホスト モード]

  許可されたクライアントが少なくとも 1 つ存在する場合にポートが許可されます。

ポートが許可されておらず、ゲスト VLAN が有効な場合、タグのないトラフィックはゲスト VLAN に再マッピングされます。タグ付きトラフィックは、ゲスト VLAN か非認証 VLAN に所属する場合以外は、ドロップされます。ポートでゲスト VLAN が無効な場合、非認証 VLAN に所属するタグ付きトラフィックのみがブリッジされます。

ポートが許可されると、そのポートに接続されたすべてのホストからのトラフィックは、タグなしのものもタグ付きのものも、スタティック VLAN メンバーシップ ポート設定に従ってブリッジされます。

許可されたポートからのタグなしトラフィックが、認証プロセス中に RADIUS サーバによる割り当て済み VLAN に再マッピングされるように指定することもできます。タグ付きトラフィックは、RADIUS による割り当て済み VLAN か非認証 VLAN に所属する場合以外は、ドロップされます。ポート上の RADIUS VLAN 割り当ては、[ポート認証] ページで設定します。

- [複数セッション モード]

  単一ホスト モードや複数ホスト モードとは異なり、複数セッション モードのポートには認証ステータスがありません。認証ステータスは、ポートに接続している各クライアントに対して割り当てられます。

  非認証 VLAN に所属するタグ付きトラフィックは、ホストが許可されているどうかにかかわらず、常にブリッジされます。

  非認証 VLAN に所属していない未許可のホストのトラフィックは、タグ付きのものもタグなしのものも、VLAN で定義され有効な場合はゲスト VLAN に再マッピングされ、ゲスト VLAN がポートで無効な場合はドロップされます。

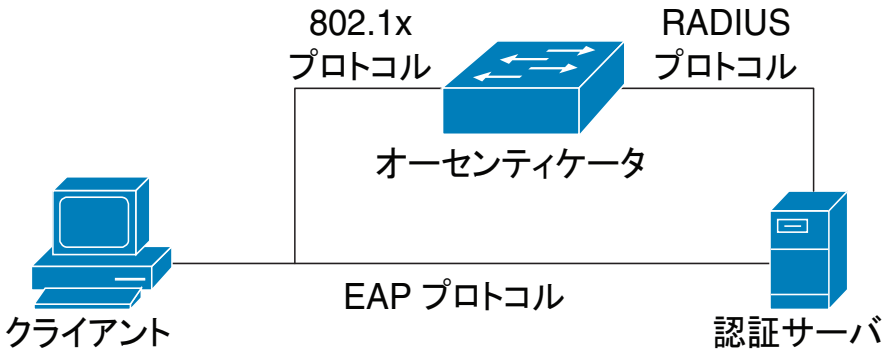
  許可されたポートからのタグなしトラフィックが、認証プロセス中に RADIUS サーバによる割り当て済み VLAN に再マッピングされるように指定することもできます。タグ付きトラフィックは、RADIUS による割り当て済み VLAN か非認証 VLAN に所属する場合以外は、ドロップされます。ポート上の RADIUS VLAN 割り当ては、[ポート認証] ページで設定します。

802.1x ベース認証

802.1x ベースのオーセンティケータは、透過的な EAP メッセージを 802.1x サプリカントと認証サーバ間でリレーします。サプリカントとオーセンティケータ間の EAP メッセージは 802.1x メッセージ内にカプセル化され、オーセンティケータと認証サーバ間の EAP メッセージは RADIUS メッセージ内にカプセル化されます。

次の図で説明します。

図 1　802.1x ベース認証



ゲスト VLAN

ゲスト VLAN は、サプリカント デバイスやポートを認証して許可する必要のないサービスへのアクセスを提供します。

ゲスト VLAN とは、未許可のクライアントに割り当てられている VLAN のことです。ゲスト VLAN、および非認証にする 1 つ以上の VLAN を、[プロパティ] ページから設定できます。

ゲスト VLAN は、設定されている場合、次の特徴を持つスタティック VLAN です。

- ゲスト VLAN は、既存のスタティック VLAN から手動で定義する必要があります。
- ゲスト VLAN は、音声 VLAN や非認証 VLAN としては使用できません。

ゲスト VLAN におけるホスト モード

ホスト モードは、ゲスト VLAN において次のように作動します。

- **単一ホスト モードと複数ホスト モード**

  未許可のポートで受信する、ゲスト VLAN に所属するトラフィックは、タグなしのものもタグ付きのものも、ゲスト VLAN 経由でブリッジされます。その他のトラフィックはすべて破棄されます。非認証 VLAN に所属するトラフィックは、この VLAN 経由でブリッジされます。

- **複数セッション モード**

  非認証 VLAN に所属せず、未許可のクライアントから受信したトラフィックは、タグなしのものもタグ付きのものも、TCAM ルールを使用してゲスト VLAN に割り当てられ、ゲスト VLAN 経由でブリッジされます。非認証 VLAN に所属するタグ付きトラフィックは、この VLAN 経由でブリッジされます。

  このモードは、ポリシーベース VLAN を持つ同一のインターフェイスには設定できません。

VLAN 名として tunnel-private-group ID 属性を指定する場合、この名前の VLAN をデバイス上で静的に設定する必要があります。この属性内の VLAN ID（2-4094）が使用された場合、サプリカントが認証された後で、VLAN が動的に作成されます。

このデバイスは、802.1X 規格で規定されている認証機構をサポートしており、802.1X サプリカントを認証および許可することができます。

違反モード

単一ホスト モードでは、許可済みのポート上の未許可ホストがインターフェイスにアクセスしようとしたときに実行するアクションを設定できます。この作業は [ホストおよびセッション認証] ページで行います。

次のオプションが選択できます。

- [制限]：サプリカント MAC アドレスとは異なる MAC アドレスを持つステーションがインターフェイスにアクセスしようとすると、トラップを生成します。トラップ間の最小時間は 1 秒です。これらのフレームは転送されますが、送信元アドレスは学習されません。
- [保護]：サプリカント アドレスとは異なる送信元アドレスを持つフレームを破棄します。
- [シャットダウン]：サプリカント アドレスとは異なる送信元アドレスを持つフレームを破棄し、ポートをシャットダウンします。

SNMP トラップを、設定可能な最小の時間間隔で送信するようにデバイスを設定することもできます。[秒] に 0 を指定すると、トラップは無効になります。最小の時間を指定しない場合、[制限] モードではデフォルトで 1 秒に設定され、その他のモードでは 0 に設定されます。

待機期間

待機時間とは、認証失敗情報交換後に、ポート（単一ホスト モードまたは複数ホスト モード）またはクライアント（複数セッション モード）が認証の試行を実行できない期間を指します。単一ホスト モードと複数ホスト モードの場合、この期間はポートごとに定義され、複数セッション モードの場合、この期間はクライアントごとに定義されます。待機時間中、スイッチは認証要求を承諾も開始もしません。

待機時間に入る前のログインの最大試行回数を指定することもできます。値として 0 を指定すると無制限にログインを試行できるようになります。

待機時間の長さとログインの最大試行回数は、[ポート認証] ページで設定できます。

一般的な作業

ワークフロー 1：ポート上で 802.1x 認証を有効にするには、次のようにします。

ステップ 1 [セキュリティ] > [802.1x 認証] > [プロパティ] の順にクリックして、802.1x 認証をグローバルに有効にします。

ステップ 2 ポートベース認証を有効にします。

ステップ 3 [認証方式] を選択します。

ステップ 4 [適用] をクリックします。実行コンフィギュレーション ファイルが更新されます。

ステップ 5 [セキュリティ] > [802.1x 認証] > [ホストとセッション] の順にクリックします。

ステップ 6 必要なポートを選択し、[編集] をクリックします。

ステップ 7 ホストの [認証モード] を設定します。

ステップ 8 [適用] をクリックします。実行コンフィギュレーション ファイルが更新されます。

ステップ 9 [セキュリティ] > [802.1x 認証] > [ポート認証] の順にクリックします。

ステップ 10 ポートを選択して、[編集] をクリックします。

ステップ 11 [管理ポート制御] フィールドを [自動] に設定します。

ステップ 12 認証方式を定義します。

ステップ 13 [適用] をクリックします。実行コンフィギュレーション ファイルが更新されます。

ワークフロー 2:トラップを設定するには、次のようにします。

ステップ 1 [セキュリティ] > [802.1x 認証] > [プロパティ] の順にクリックします。

ステップ 2 必要なトラップを選択します。

ステップ 3 [適用] をクリックします。実行コンフィギュレーション ファイルが更新されます。

ワークフロー 3:802.1x ベース認証、を設定するには、次のようにします。

ステップ 1 [セキュリティ] > [802.1x 認証] > [ポート認証] の順にクリックします。

ステップ 2 必要なポートを選択し、[編集] をクリックします。

ステップ 3 ポートに必要なフィールドを入力します。

このページのフィールドについては、「ポート認証」の説明を参照してください。

ステップ 4 [適用] をクリックします。実行コンフィギュレーション ファイルが更新されます。

ポート間で設定をコピーするには、[設定のコピー] ボタンを使用します。

ワークフロー 4:待機期間を設定するには、次のようにします。

ステップ 1 [セキュリティ] > [802.1x 認証] > [ポート認証] の順にクリックします。

ステップ 2 ポートを選択して、[編集] をクリックします。

ステップ 3 [待機期間] フィールドに待機時間を入力します。

ステップ 4 [適用] をクリックします。実行コンフィギュレーション ファイルが更新されます。

ワークフロー 5:ゲスト VLAN を設定するには、次のようにします。

ステップ 1 [セキュリティ] > [802.1x 認証] > [プロパティ] の順にクリックします。

ステップ 2 [ゲスト VLAN] フィールドで [有効] を選択します。

ステップ 3 [ゲスト VLAN ID] フィールドでゲスト VLAN を選択します。

ステップ 4 [ゲスト VLAN タイムアウト] を [即時] に設定するか、[ユーザ定義] フィールドに値を入力します。

ステップ 5 [適用] をクリックします。実行コンフィギュレーション ファイルが更新されます。

プロパティ

[プロパティ] ページを使用して、ポートまたはデバイスの認証をグローバルに有効にします。認証を使用するには、各ポートでグローバルにも個別にも認証を有効化する必要があります。

ポートベース認証を定義するには、次のようにします。

ステップ 1 [セキュリティ] > [802.1x 認証] > [プロパティ] の順にクリックします。

ステップ 2 パラメータを入力します。

- [ポートベース認証]：ポートベース認証を有効または無効にします。

  この認証を無効にすると、802.1x が無効になります。

- [認証方式]：ユーザの認証方式を選択します。次のオプションがあります。

  - [RADIUS、なし]：まず RADIUS サーバを使用してポート認証を実行します。RADIUS サーバから応答がない場合（例：サーバが停止している場合）、認証処理は実行されず、セッションが許可されます。
  - [RADIUS]：RADIUS サーバ上でユーザを認証します。認証処理が実行されなかった場合、セッションは許可されません。
  - [なし]：ユーザを認証しません。セッションは許可されます。

- [ゲスト VLAN]：選択すると、未許可のポートにゲスト VLAN を使用できるようになります。ゲスト VLAN が有効な場合、未許可のポートはすべて、[ゲスト VLAN ID] フィールドで選択した VLAN に自動的に参加します。後で許可されたポートはゲスト VLAN から削除されます。

  ゲスト VLAN は、他の VLAN と同様に、レイヤ 3 インターフェイス（IP アドレスが割り当てられた）として定義できます。ただし、ゲスト VLAN IP アドレス経由ではデバイス管理が使用できません。

- [ゲスト VLAN ID]：VLAN の一覧からゲスト VLAN を選択します。

- [ゲスト VLAN タイムアウト]：期間を [即時] として定義するか、[ユーザ定義] に値を入力します。この値は次にように使用されます。

  リンクアップ後にソフトウェアで 802.1x サプリカントが検出されない場合、または認証に失敗した場合、[ゲスト VLAN タイムアウト] で設定した時間の経過後に、そのポートがゲスト VLAN に追加されます。

  ポートの状態が許可から未許可に変わると、ゲスト VLAN タイムアウトが発生してから、そのポートがゲスト VLAN に追加されます。

- [トラップ設定]:トラップを有効にするには、次のオプションの中から 1 つ以上を選択します。
  - [802.1x認証失敗トラップ]:選択すると、802.1X 認証が失敗したときにトラップが生成されます。
  - [802.1x認証成功トラップ]:選択すると、802.1X 認証が成功したときにトラップが生成されます。

ステップ 3 [適用] をクリックします。802.1x のプロパティが実行コンフィギュレーション ファイルに書き込まれます。

ポート認証

[ポート認証] ページでは、各ポートのパラメータを設定できます。ホスト認証などのいくつかの設定は、ポートが [強制許可] 状態の間しか変更できないため、ポート制御を [強制許可] に変更してから設定を変更するようにお勧めします。設定が完了したら、ポート制御を元の状態に戻してください。

注 802.1x が設定されているポートを LAG のメンバーにすることはできません。802.1x とポート セキュリティは同じポート上で同時に有効にできません。あるインターフェイス上でポート セキュリティを有効にした場合は、[管理ポート制御] を [自動] モードに変更できません。

802.1X 認証を定義するには、次のようにします。

ステップ 1 [セキュリティ] > [802.1x 認証] > [ポート認証] の順にクリックします。

ステップ 2 このページには、すべてのポートに対する認証設定情報が表示されます。ポートを選択し、[編集] をクリックします。

ステップ 3 パラメータを入力します。

- [インターフェイス]:ポートを選択します。
- [現在のポート制御]:現在のポート許可状態が表示されます。状態が [許可] の場合は、そのポートが認証されているか、[管理ポート制御] が [強制許可] に設定されています。一方、状態が [無許可] の場合は、ポートが認証されていないか、[管理ポート制御] が [強制無許可] に設定されています。サプリカントをインターフェイス上で有効にすると、現在のポート制御がサプリカントになります。

- [管理ポート制御]：管理ポートの許可状態を選択します。次のオプションがあります。
  - [強制無許可]：インターフェイスの状態を未許可に移行して、インターフェイス アクセスを拒否します。デバイスが、このインターフェイスを介してクライアントに認証サービスを提供することはありません。
  - [自動]：そのデバイス上でのポートベースの認証と許可を有効にします。デバイスとクライアントの間で交換される認証情報に基づいて、インターフェイスの状態は許可になったり未許可になったりします。
  - [強制許可]：認証せずにインターフェイスを許可します。
- [ゲストVLAN]：未許可のポートに対するゲスト VLAN の使用を可能にする場合に選択します。ゲスト VLAN が有効な場合、未許可のポートは、[ポート認証] ページの [ゲストVLAN ID] フィールドで選択した VLAN に自動的に参加します。認証の失敗後、指定したポート上でゲスト VLAN がグローバルに有効になっている場合は、このゲスト VLAN がタグなし VLAN としてその未許可のポートに自動的に割り当てられます。
- [定期再認証]：選択すると、[再認証期間] で指定した間隔で、ポートの再認証試行が有効になります。
- [再認証期間]：選択したポートを再認証する間隔を入力します（単位：秒）。
- [即時再認証]：選択すると、ポートの再認証がすぐに有効になります。
- [認証状態]：定義されているポート認可状態が表示されます。次のオプションがあります。
  - [初期化]：起動処理中。
  - [強制許可]：ポート制御状態が [強制許可]（トラフィックの転送）に設定されています。
  - [強制無許可]：ポート制御状態が [強制無許可]（トラフィックの廃棄）に設定されています。

  注 [強制許可] でも [強制無許可] でもない場合、ポートは [自動] モードになっており、オーセンティケータには現在の認証状態が表示されます。ポートが認証されたら、その状態が [認証済み] と表示されます。
- [時間範囲]：選択すると、認証が指定した時間範囲に制限されます。
- [時間範囲名]：[時間範囲] を選択した場合、使用する時間範囲を選択します。時間範囲は [システム時刻の設定] セクションで定義します。

- [最大ホスト数]:このインターフェイスで使用できる、許可されたホストの最大数を入力します。[無制限] を選択して無制限にするか、[ユーザ定義] を選択して制限を設定します。
- [待機期間]:待機期間の長さを入力します。
- [EAP の再送信]:サプリカント（クライアント）からの、Extensible Authentication Protocol（EAP; 拡張認証プロトコル）要求/ID フレームに対する応答をデバイスが待機する時間を入力します（単位:秒）。この時間内に応答がない場合、要求が再送信されます。
- [最大 EAP 要求]:送信される EAP 要求の最大数を入力します。定義された期間内に応答が受信されなかった（サプリカント タイムアウト）場合は、認証プロセスが再開されます。
- [最大 EAP 再試行][サプリカントタイムアウト]:EAP 要求がサプリカントに再送信されるまでの経過時間を入力します（単位:秒）。
- [サーバタイムアウト]:デバイスが認証サーバに要求を再送信するまでの経過時間を入力します（単位:秒）。

ステップ 4 [サプリカント][適用] をクリックします。ポート設定が、実行コンフィギュレーションファイルに書き込まれます。

ホストおよびセッション認証

[ホストおよびセッション認証] ページでは、ポート上での 802.1X の動作モード、および違反検出時に実行する処理を設定できます。

これらのモードに関する説明は、「ポート ホスト モード」を参照してください。

ポートの 802.1X 詳細設定を定義するには、次のようにします。

ステップ 1 [セキュリティ] > [802.1x 認証] > [ホストおよびセッション認証] の順にクリックします。

このページには、すべてのポートの認証パラメータが表示されます。次のフィールドを除くすべてのフィールドは、[編集] ページに表示されます。

- [違反の数]:単一ホスト モードで、そのインターフェイスが、サプリカントの MAC アドレスとは異なる MAC アドレスを持つホストから受信したパケット数が表示されます。

ステップ 2 ポートを選択して、[編集] をクリックします。

ステップ 3 パラメータを入力します。

- [インターフェイス]:ホスト認証を有効にするポート番号を入力します。
- [ホスト認証]:いずれかのモードを選択します。これらのモードについては、上記の「ポート ホスト モード」の説明を参照してください。

[単一ホストの違反設定](ホスト認証が [単一ホスト] の場合にのみ表示されます)。

- [違反時アクション]:サプリカントの MAC アドレスとは異なる MAC アドレスを持つホストから、単一セッション モードか単一ホスト モードで受信したパケットに適用する処理を選択します。次のオプションがあります。
  - [保護(破棄)]:パケットを破棄します。
  - [制限(転送)]:パケットを転送します。
  - [シャットダウン]:パケットを破棄し、ポートをシャットダウンします。ポートは、再アクティブ化されるかデバイスが再起動するまで、シャットダウンした状態になります。
- [トラップ]:選択すると、トラップが有効になります。
- [トラップ間隔]:ホストにトラップを送信する頻度を定義します。このフィールドの値を指定できるのは、複数ホストが無効になっている場合だけです。

ステップ 4 [適用] をクリックします。設定が実行コンフィギュレーション ファイルに書き込まれます。

認証済みホスト

認証済みユーザの詳細を表示するには、[セキュリティ] > [802.1x 認証] > [認証済みホスト] の順にクリックします。

このページには次のフィールドが表示されます。

- [ユーザ名]：各ポートで認証されたサプリカント名。
- [ポート]：ポートの数。
- [セッション時間 (DD:HH:MM:SS)]：そのポートでのアクセスをサプリカントが認証および許可されていた時間の長さ。
- [認証サーバ]：RADIUS サーバ。
- [MACアドレス]：サプリカントの MAC アドレスが表示されます。

19

セキュリティ:セキュア機密データ管理

セキュア機密データ(SSD)とは、デバイスの機密データ(パスワードやキーなど)の保護を実現するためのアーキテクチャです。SSD では、機密データを管理するセキュアなソリューションを提供するために、パスフレーズ、暗号化、アクセス制御、およびユーザ認証を使用します。

SSD は、コンフィギュレーション ファイルの整合性を守り、設定プロセスを保護し、さらに SSD ゼロタッチ自動コンフィギュレーションをサポートするために拡張されています。

はじめに

SSD は、デバイスの機密データ(パスワードやキーなど)の保護、ユーザ資格情報および SSD ルールに基づき暗号化された機密データや機密データへのプレーンテキストでのアクセスの許可 / 拒否、機密データを含むコンフィギュレーション ファイルの改ざんからの保護を実施します。

さらに SSD では、機密データを含むコンフィギュレーション ファイルのセキュアなバックアップと共有を可能にします。

SSD は、機密データの保護を目的のレベルに設定する柔軟性を提供します。機密データの保護レベルには、保護のないプレーンテキストから、デフォルトのパスフレーズによる暗号化に基づく最小限の保護、ユーザ定義のパスフレーズによる暗号化に基づくより良好な保護まであります。

SSD は、認証および承認されたユーザに限り、SSD ルールに従って、機密データの読み取り権限を付与します。デバイスは、ユーザ認証プロセスを通して、ユーザの管理アクセスの認証と承認を行います。

管理者には、SSD を使用しているかどうかにかかわらず、ローカルの認証データベースを使用して認証プロセスを安全にすること、またはユーザ認証プロセスで使用する外部認証サーバへの通信を安全にすること、あるいはその両方を行うことをお勧めします。

すなわち SSD は、SSD ルール、SSD プロパティ、およびユーザ認証を使用してデバイスの機密データを保護するものです。またデバイスの SSD ルール、SSD プロパティ、およびユーザ認証の設定は、それ自体が SSD で守られた機密データです。

SSD 管理

SSD 管理には、機密データの処理およびセキュリティを定義するコンフィギュレーション パラメータのコレクションが含まれます。SSD コンフィギュレーション パラメータ自体は、機密データであり SSD によって守られています。

SSD のすべてのコンフィギュレーションは、適正な権限でのみユーザが利用できる SSD ページ経由で実行されます（「SSD ルール」を参照）。

SSD ルール

SSD ルールは、管理チャネル上のユーザ セッションに付与される読み取り権限およびデフォルトの読み取りモードを定義します。

SSD ルールは、ユーザおよび SSD 管理チャネルで一意に決まります。同一のユーザに異なる SSD ルールが存在する可能性がありますが、異なるチャネル向けです。逆に、同一のチャネルに異なるルールが存在する可能性がありますが、異なるユーザ向けです。

読み取り権限は、機密データを表示する方法を決定します。表示方法には、暗号化形式のみ、プレーンテキスト形式のみ、暗号化形式とプレーンテキスト形式の両方、または機密データを表示する権限なしがあります。SSD ルールは、それ自身を機密データとして保護するよう規定します。

デバイスは、合計で 32 の SSD ルールをサポートすることができます。

デバイスはユーザに、ユーザ ID/ユーザ資格情報およびユーザが機密データにアクセスする管理チャネルのタイプの組み合わせに最も良く適合する SSD ルールの SSD 読み取り権限を付与します。

デバイスには、一連の SSD ルールがデフォルトで付属します。管理者は、必要に応じて SSD ルールの追加、削除、および変更ができます。

注 デバイスは、SSD で定義されたすべてのチャネルをサポートしていない場合があります。

SSD ルールの要素

SSD ルールは次の要素を含みます。

- [ユーザタイプ]: サポートされるユーザ型を望ましい順に並べると次のようになります。(ユーザが複数の SSD ルールに一致する場合は、最も望ましいユーザ タイプが適用されます)。
  - [特定]: このルールは特定のユーザに適用されます。
  - [デフォルトユーザ(cisco)]: このルールはデフォルト ユーザ(cisco)に適用されます。
  - [レベル 15]: このルールは特権レベル 15 のユーザに適用されます。
  - [すべて]: このルールはすべてのユーザに適用されます。
- [ユーザ名]: ユーザ タイプが [特定] の場合、ユーザ名が必要です。
- [チャネル]: ルールが適用される SSD 管理チャネルのタイプ。サポートされるチャネルのタイプは次のとおりです。
  - [セキュア]: このルールがセキュアなチャネルのみに適用されるように指定します。デバイスによっては、次のセキュアなチャネルの一部またはすべてをサポートします。
    コンソール ポート インターフェイス、SCP、SSH、および HTTPS。
  - [セキュアでない]: このルールがセキュアでないチャネルのみに適用されるように指定します。デバイスによっては、次のセキュアでないチャネルの一部またはすべてをサポートします。
    Telnet、TFTP、および HTTP。
  - [セキュア XML SNMP]: このルールが XML over HTTPS またはプライバシー機能のある SNMPv3 のみに適用されるように指定します。デバイスが、セキュアな XML および SNMP チャネルのすべてをサポートする場合と一部しかサポートしない場合があります。

- [セキュアでないXML SNMP]:このルールが XML over HTTPS または SNMPv1/v2 およびプライバシー機能のない SNMPv3 のみに適用されるように指定します。デバイスが、セキュアな XML および SNMP チャネルのすべてをサポートする場合と一部しかサポートしない場合があります。

- [読み取り権限]:ルールと関連付けられた読み取り権限。次のものがあります。
  - (最低)[除外]:ユーザはあらゆる形式の機密データへのアクセスを許可されません。
  - (中間)[暗号化のみ]:ユーザは暗号化された機密データにのみアクセスを許可されます。
  - (高)[プレーンテキストのみ]:ユーザはプレーンテキストの機密データにのみアクセスを許可されます。ユーザに、SSD パラメータへの読み取り権限と書き込み権限がある場合もあります。
  - (最高)[両方]:ユーザは、暗号化およびプレーンテキストの権限の両方を持ち、暗号化された機密データおよびプレーンテキストの機密データへのアクセスが許可されます。ユーザに、SSD パラメータへの読み取り権限と書き込み権限がある場合もあります。

  各管理チャネルは特定の読み取り権限を許可します。これらを次にまとめます。

管理チャネル	許可される読み取り権限オプション
セキュア	両方、暗号化のみ
セキュアでない	両方、暗号化のみ
セキュア XML SNMP	除外、プレーンテキストのみ
セキュアでない XML SNMP	除外、プレーンテキストのみ

- [デフォルトの読み取りモード]:すべてのデフォルトの読み取りモードは、ルールの読み取り権限に従属します。次のオプションが存在しますが、読み取り権限によっては拒否されることがあります。ユーザのユーザ定義済み読み取り権限が、たとえば [除外] であり、さらにデフォルトの読み取りモードが [暗号化] の場合、ユーザ定義済みの読み取り権限が優先します。
  - [除外]:機密データの読み取りを許可しない。
  - [暗号化]:機密データは暗号化形式で提示されます。
  - [プレーンテキスト]:機密データはプレーンテキストで提示されます。

各管理チャネルは特定の読み取り推定を許可します。これらを次にまとめます。

読み取り権限	許可されるデフォルトの読み取りモード
除外	除外
暗号化のみ	* 暗号化
プレーンテキストのみ	* プレーンテキスト
両方	* プレーンテキスト、暗号化

* セッションの読み取りモードは、新しい読み取りモードが読み取り権限に違反しない場合には、[SSD プロパティ] ページで一時的に変更することができます。

注　次の点に注意してください。

- [セキュア XML SNMP] および [セキュアでない XML SNMP] 管理チャネルのデフォルトの読み取りモードは、読み取り権限と同じでなければなりません。
- 読み取り権限 [除外] は、[セキュアXML SNMP] および [セキュアでないXML SNMP] 管理チャネルにのみ許可されます。[除外] は、通常のセキュアなチャネルおよびセキュアでないチャネルには許可されません。
- セキュアおよびセキュアでない XML-SNMP 管理チャネルで機密データが [除外] になっている場合、機密データは 0 (null 文字列または数値 0) として提示されます。ユーザが機密データを表示させたい場合は、ルールをプレーンテキストに変更する必要があります。
- デフォルトでは、プライバシー機能のある SNMPv3 のユーザおよび XML-over-secure チャネル権限がある SNMPv3 ユーザは、レベル 15 ユーザと見なされます。
- セキュアでない XML および SNMP (SNMPv1、v2、およびプライバシー機能のない v3) チャネルの SNMP ユーザは、[すべて] のユーザと見なされます。
- SNMP コミュニティ名は、SSD ルールに一致するユーザ名としては使用されません。
- 特定の SNMPv3 ユーザによるアクセスは、SNMPv3 ユーザ名に一致するユーザ名で SSD ルールを設定することで制御できます。
- 読み取りアクセス許可 (プレーンテキストのみまたは両方) 付きのルールを 1 つ以上設置する必要があります。これは、このようなアクセス許可を持っているユーザだけが SSD ページにアクセスできるためです。

- ルールのデフォルトの読み取りモードおよび読み取り権限に対する変更が有効となると、すべてのアクティブな管理セッションの対象ユーザおよびチャネルには直ちに適用されます（変更を加えたセッションは、そのルールが適用可能な場合でも除外されます）。ルールが変更された場合（追加、削除、編集）、システムは対象となるすべての CLI/GUI セッションを更新します。

注 セッションに SSD ルールが適用されると、ログインはそのセッションから変更されます。そのユーザはログアウトしてから再度ログインして変更を確認する必要があります。

注 XML または SNMP コマンドが開始するファイル転送を実行している場合、使用されている基礎となるプロトコルは TFTP です。そのため、セキュアでないチャネル用の SSD ルールが適用されます。

SSD ルールおよびユーザ認証

SSD は、認証および承認されたユーザに限り、SSD ルールに従って SSD 権限を付与します。デバイスは、管理アクセスの認証と承認をユーザ認証プロセスに依存しています。不正アクセスからデバイスや機密データおよび SSD 設定を含むデータを守るために、デバイスのユーザ認証プロセスをセキュアにすることをお勧めします。ユーザ認証プロセスをセキュアにするために、ローカルの認証データベースを使用したり、RADIUS サーバなどの外部認証サーバを経由して通信をセキュアにできます。外部認証サーバとのセキュア通信の設定は機密データであり、SSD によって保護されています。

注 ローカルの認証データベースにあるユーザの資格情報は、すでに SSD と関係のない仕組みによって保護されています。

代替チャネルを使用するアクションをチャネルからユーザが発行した場合、デバイスは SSD ルールから、ユーザの資格情報および代替チャネルに一致する読み取り権限およびデフォルトの読み取りモードを適用します。たとえば、ユーザがセキュアなチャネルからログインして TFTP のアップロード セッションを開始した場合、セキュアでないチャネル（TFTP）上のユーザの SSD 読み取り権限が適用されます。

デフォルトの SSD ルール

デバイスには次の工場出荷時ルールがあります。

ルール キー		ルール アクション	
ユーザ	チャネル	読み取り権限	デフォルトの読み取りモード
レベル 15	セキュア XML SNMP	プレーンテキストのみ	プレーンテキスト
レベル 15	セキュア	両方	暗号化
レベル 15	セキュアでない	両方	暗号化
すべて	セキュアでない XML SNMP	除外	除外
すべて	セキュア	暗号化のみ	暗号化
すべて	セキュアでない	暗号化のみ	暗号化

デフォルト ルールは変更することができますが、削除することはできません。SSD のデフォルト ルールが変更されている場合には、復元することが可能です。

SSD デフォルト読み取りモード セッションのオーバーライド

システムは、ユーザの読み取り権限およびデフォルトの読み取りモードに基づいて、暗号化またはプレーンテキストとして機密データをセッションに含めます。

デフォルトの読み取りモードは、セッションの SSD 読み取り権限と競合しない限り、一時的にオーバーライドできます。この変更は、現在のセッションでただちに有効となり、次のいずれかが発生するまで有効です。

- ユーザが再度変更した。
- セッションが終了した。
- セッションのユーザに適用される SSD ルールの読み取り権限が変更され、セッションの現在の読み取りモードと互換性がなくなった。この場合、セッションの読み取りモードは SSD ルールのデフォルトの読み取りモードに戻ります。

SSD プロパティ

SSD プロパティは、SSD ルールと連動しながら、デバイスの SSD 環境を定義して制御する一連のパラメータです。SSD 環境は、次のプロパティから構成されます。

- 機密データの暗号化を制御するプロパティ。
- コンフィギュレーション ファイルのセキュリティの強度を制御するプロパティ。
- 機密データが現在のセッション内でどのように表示されるかを制御するプロパティ。

パスフレーズ

パスフレーズは、SSD 機能におけるセキュリティの仕組みの基本となるもので、機密データの暗号化および復号化のキーを生成するのに使用します。同じパスフレーズを持つデバイスは、そのパスフレーズから生成されたキーを使用してお互いの暗号化された機密データを復号化できます。

パスフレーズは次のルールに従う必要があります。

- [長さ]:8～16 文字。
- [文字クラス]:パスフレーズには、少なくとも 1 つの大文字、1 つの小文字、1 つの数字、1 つの特殊文字（例:#、$）が含まれなければなりません。

デフォルトおよびユーザ定義のパスフレーズ

すべてのデバイスには、デフォルトのすぐに使えるユーザにすぐ分かるパスフレーズが用意されています。デフォルトのパスフレーズは、コンフィギュレーション ファイルや CLI/GUI には一切表示されません。

セキュリティや保護をもっと改善したい場合、管理者はデバイスの SSD を設定して、デフォルトのパスフレーズではなくユーザ定義のパスフレーズを使用する必要があります。ユーザ定義のパスフレーズは十分に守られた秘密として取り扱われ、デバイスの機密データが侵害されないようにしなければなりません。

ユーザ定義のパスフレーズは、手動でプレーンテキストで設定することができます。またコンフィギュレーション ファイルから派生させることもできます。（「機密データ ゼロタッチ自動コンフィギュレーション」を参照してください）。デバイスは、常に暗号化されたユーザ定義のパスフレーズを表示します。

ローカル パスフレーズ

デバイスは、実行コンフィギュレーションのパスフレーズであるローカル パスフレーズを維持します。SSD は通常、ローカル パスフレーズから生成されるキーを使用して機密データの暗号化と復号化を実行します。

ローカル パスフレーズは、デフォルト パスフレーズとユーザ定義パスフレーズのどちらにでも設定できます。デフォルトでは、ローカル パスフレーズとデフォルト パスフレーズは同じになっています。コマンド ライン インターフェイス（利用できる場合）か Web ベースのインターフェイスのどちらかを使った管理者のアクションによって変更することができます。スタートアップ コンフィギュレーション ファイルがデバイスの実行コンフィギュレーションになると、パスフレーズはスタートアップ コンフィギュレーションファイルのものに自動的に変更されます。デバイスが工場出荷時設定にリセットされると、ローカル パスフレーズはデフォルト パスフレーズにリセットされます。

コンフィギュレーション ファイルのパスフレーズ制御

ファイルのパスフレーズ制御は、ユーザ定義のパスフレーズ、ユーザ定義のパスフレーズから生成されたキーによって暗号化される機密データに対する追加の保護を、テキストベースのコンフィギュレーション ファイルで提供します。

既存のパスフレーズ制御モードを次に示します。

- [制限なし]（デフォルト）：デバイスは、コンフィギュレーションファイルを生成する際にパスフレーズを含めます。これにより、コンフィギュレーション ファイルを受け取ったすべてのデバイスが、そのファイルからパスフレーズを知ることができるようになります。
- [制限あり]：デバイスは、パスフレーズをコンフィギュレーション ファイルにエクスポートされないようにします。[制限あり] モードは、コンフィギュレーション ファイルにある暗号化された機密データを、パスフレーズを持たないデバイスから保護します。このモードは、コンフィギュレーション ファイルにあるパスフレーズを見られたくない場合に使用します。

デバイスが工場出荷時設定にリセットされると、ローカル パスフレーズはデフォルト パスフレーズにリセットされます。その結果、デバイスは、管理セッション（GUI/CLI）から入力されたユーザ定義のパスフレーズに基づいて暗号化された任意の機密データ、または [制限あり] モードの任意のコンフィギュレーション ファイルにある機密データを復号化できなくなります。これには、デバイスが工場出荷時のデフォルトにリセットされる前にそのデバイス自体が作成したファイルを含みます。これはデバイスがユーザ定義のパスフレーズを使って手動で再設定されるまで維持されます。それ以外の場合、ユーザ定義のパスフレーズはコンフィギュレーション ファイルから取得されます。

コンフィギュレーションファイルの整合性の制御

ユーザは、[コンフィギュレーションファイルの整合性の制御] を使用してコンフィギュレーション ファイルを作成することにより、コンフィギュレーション ファイルを改ざんや変更から保護することができます。デバイスが、ユーザ定義のパスフレーズを [制限なしコンフィギュレーション ファイル パスフレーズ制御] で使用する場合は、[コンフィギュレーションファイルの整合性の制御] を有効にすることをお勧めします。

注意 整合性が保護されたコンフィギュレーション ファイルに何らかの変更が加えられた場合は、改ざんがあったと見なされます。

デバイスは、コンフィギュレーション ファイルの整合性が保護されているかどうかを、そのファイルの SSD 制御ブロックのファイル整合性制御コマンドを調べることによって判断します。ファイルの整合性が保護されていても、デバイスがそのファイルの整合性が完全ではないことを発見した場合には、デバイスはそのファイルを拒否します。それ以外の場合は、ファイルは受理されてその後の処理が行われます。

ファイルがスタートアップ コンフィギュレーション ファイルにダウンロードまたはコピーされた場合、デバイスはテキストベースのコンフィギュレーション ファイルの整合性を確認します。

読み取りモード

各セッションには読み取りモードがあります。読み取りモードは機密データがどのように表示されるかを決定します。読み取りモードは、機密データが通常のテキストとして表示される [プレーンテキスト] と、機密データが暗号化形式で表示される [暗号化] のどちらかです。

コンフィギュレーション ファイル

コンフィギュレーション ファイルにはデバイスのコンフィギュレーションがあります。デバイスには、実行コンフィギュレーション ファイル、スタートアップ コンフィギュレーション ファイル、ミラー コンフィギュレーション ファイル(オプション)、バックアップ コンフィギュレーション ファイルがあります。ユーザは、リモートのファイルサーバとの間でコンフィギュレーション ファイルを手動でアップロードおよびダウンロードすることができます。デバイスは、DHCP を使用した自動コンフィギュレーション ステージの間に、スタートアップ コンフィギュレーション ファイルをリモートのファイルサーバから自動的にダウンロードすることができます。リモートのファイルサーバに保存されているコンフィギュレーション ファイルは、リモート コンフィギュレーション ファイルと呼ばれます。

実行コンフィギュレーション ファイルは、現在デバイスが使用しているコンフィギュレーションを含みます。スタートアップ コンフィギュレーション ファイルにあるコンフィギュレーションは、リブート後に実行コンフィギュレーションになります。実行コンフィギュレーション ファイルおよびスタートアップ コンフィギュレーション ファイルは、内部形式でフォーマットされています。ミラー コンフィギュレーション ファイル、バックアップ コンフィギュレーション ファイル、リモート コンフィギュレーション ファイルは、テキストベースのファイルで、アーカイブ、記録、または復元用として維持されます。ソースのコンフィギュレーション ファイルをコピー、アップロード、およびダウンロードする際に 2 つのファイルのフォーマットが異なっている場合、デバイスは自動的にソースのコンテンツを宛先のフォーマットに変換します。

ファイル SSD インジケータ

実行コンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルをテキストベースのコンフィギュレーション ファイルにコピーする場合、デバイスは、ファイル SSD インジケータを生成してテキストベースのコンフィギュレーション ファイルに配置し、ファイルが暗号化された機密データ、プレーンテキストの機密データ、または機密データが除外されているもののいずれであるかを示します。

- SSD インジケータが存在する場合には、コンフィギュレーション ヘッダー ファイルになければなりません。
- SSD インジケータを含まないテキストベースのコンフィギュレーションは、機密データを含まないと見なされます。
- SSD インジケータは、テキストベースのコンフィギュレーション ファイルの SSD 読み取り権限を強制するために使用されますが、コンフィギュレーション ファイルを実行コンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルにコピーする際には無視されます。

ファイル中の SSD インジケータは、コピー中に、暗号化機密データ、プレーンテキスト機密データを含める、または機密データをファイルから除外するためにユーザの指示に従って設定されます。

SSD 制御ブロック

デバイスは、そのスタートアップ コンフィギュレーション ファイルまたは実行コンフィギュレーション ファイルからテキストベースのコンフィギュレーション ファイルを生成する際に、ユーザが機密データをファイルに含めるように要求した場合、SSD 制御ブロックをファイルに挿入します。この SSD 制御ブロックは、改ざんから保護されていて、ファイルを生成したデバイスの SSD ルールと SSD プロパティを含みます。SSD 制御ブロックは、それぞれ「ssd-control-start」で始まり、「ssd-control-end」で終わります。

スタートアップ コンフィギュレーション ファイル

デバイスは現在、実行コンフィギュレーション ファイル、バックアップ コンフィギュレーション ファイル、ミラー コンフィギュレーション ファイル、リモート コンフィギュレーション ファイルからスタートアップ コンフィギュレーション ファイルへのコピーをサポートしています。スタートアップ コンフィギュレーションにあるコンフィギュレーションは、リブート後に有効となり、実行コンフィギュレーション ファイルになります。ユーザは、SSD 読み取り権限および管理セッションの現在の SSD 読み取りモードに従って、スタートアップ コンフィギュレーション ファイルから暗号化またはプレーンテキストの機密データを取得することができます。

スタートアップ コンフィギュレーション ファイルの任意の形式の機密データへの読み取りアクセスは、スタートアップ コンフィギュレーション ファイルのパスフレーズとローカルのパスフレーズが異なる場合は除外されます。

SSD は、バックアップ コンフィギュレーション ファイル、ミラー コンフィギュレーション ファイル、リモート コンフィギュレーション ファイルをスタートアップ コンフィギュレーション ファイルへコピーする場合、次のルールを追加します。

- デバイスが工場出荷時のデフォルトにリセットされると、SSD ルールおよび SSD プロパティを含むすべてのコンフィギュレーションがデフォルトにリセットされます。
- ソースのコンフィギュレーション ファイルに暗号化された機密データが含まれるものの、SSD 制御ブロックがない場合、デバイスはソース ファイルを拒絶しコピーは失敗します。
- ソースのコンフィギュレーション ファイルに SSD 制御ブロックがない場合、スタートアップ コンフィギュレーション ファイルの SSD コンフィギュレーションはデフォルトにリセットされます。

- ソースのコンフィギュレーション ファイルの SSD 制御ブロックにパスフレーズがある場合、デバイスはソース ファイルを拒否し、ファイルに SSD 制御ブロックのパスフレーズから生成されたキーによって暗号化されたのではない暗号化された機密データがある場合、コピーは失敗します。
- ソースのコンフィギュレーション ファイルに SSD 制御ブロックがあり、そのファイルの SSD 整合性チェックまたはファイル整合性チェック、あるいはその両方が失敗した場合、デバイスはソース ファイルを拒否してコピーは失敗します。
- ソースのコンフィギュレーション ファイルの SSD 制御ブロックにパスフレーズがない場合、ファイル内のすべての暗号化された機密データは、ローカルのパスフレーズから生成されたキーまたはデフォルトのパスフレーズから生成されたキーのどちらかで暗号化される必要があります。ただし両方のキーを使うことはできません。それ以外の場合、ソース ファイルは拒否されてコピーは失敗します。
- デバイスは、ソースのコンフィギュレーション ファイルの SSD 制御ブロックのパスフレーズ、パスフレーズ制御、およびファイル整合性（ある場合）を、スタートアップ コンフィギュレーション ファイルへ設定します。スタートアップ コンフィギュレーション ファイルの設定は、ソースのコンフィギュレーション ファイルの機密データを暗号化するキーを生成するために使用するパスフレーズを用いて行われます。見あたらない SSD コンフィギュレーションは、デフォルトにリセットされます。
- ソースのコンフィギュレーション ファイルに SSD 制御ブロックがあり、そのファイルにプレーンテキスト、SSD 制御ブロックの SSD コンフィギュレーション以外の機密データがある場合、ファイルは受理されます。

実行コンフィギュレーション ファイル

実行コンフィギュレーション ファイルは、現在デバイスが使用しているコンフィギュレーションを含みます。ユーザは、SSD 読み取り権限および管理セッションの現在の SSD 読み取りモードに従って、実行コンフィギュレーション ファイルから暗号化またはプレーンテキストの機密データを取得することができます。ユーザは、バックアップ コンフィギュレーション ファイルまたはミラー コンフィギュレーション ファイルを、CLI、XML、SNMP などを介して他の管理アクション経由でコピーすることで実行コンフィギュレーション ファイルを変更することができます。

デバイスは、ユーザが実行コンフィギュレーションの SSD コンフィギュレーションを直接変更した場合、次のルールを適用します。

- 管理セッションを開いたユーザが、SSD 権限（[両方] または [プレーンテキストのみ] 読み取り権限のいずれか）を持っていない場合、デバイスはすべての SSD コマンドを拒否します。

- ソース ファイルからコピーした場合、ファイル SSD インジケータ、SSD 制御ブロック整合性、および SSD ファイル整合性は検査も強制もされません。
- ソース ファイルからコピーした場合、ソース ファイルのパスフレーズがプレーンテキストだとコピーは失敗します。パスフレーズが暗号化されていると、無視されます。
- パスフレーズを実行コンフィギュレーションに直接（ファイル コピーでなく）設定する場合は、コマンドのパスフレーズはプレーンテキストで入力しなければなりません。それ以外では、コマンドは拒否されます。
- 暗号化された機密データを使ったコンフィギュレーション コマンドは、ローカルのパスフレーズから生成されたキーで暗号化され、実行コンフィギュレーションに設定されます。それ以外は、コンフィギュレーション コマンドはエラーとなり、実行コンフィギュレーション ファイルには組み込まれません。

バックアップ コンフィギュレーション ファイルとミラー コンフィギュレーション ファイル

自動ミラー コンフィギュレーション サービスが有効な場合、デバイスは、スタートアップ コンフィギュレーション ファイルからミラー コンフィギュレーション ファイルを定期的に生成します。デバイスは、必ず暗号化された機密データでミラー コンフィギュレーション ファイルを生成します。そのため、ミラー コンフィギュレーション ファイルのファイル SSD インジケータは、常に暗号化された機密データを含むファイルであることを示します。

デフォルトでは、自動ミラー コンフィギュレーション サービスが有効になります。自動ミラー コンフィギュレーションを有効化または無効化するように設定するには、[各種管理] > [ファイル管理] > [ファームウェア操作] をクリックします。

次のように、SSD 読み取り権限、現在のセッションの読み取りモード、およびソースファイルのファイル SSD インジケータに従って、ユーザは、ミラー コンフィギュレーション ファイルおよびバックアップ コンフィギュレーション ファイル全体を表示、コピー、アップロードすることができます。

- ミラー コンフィギュレーション ファイルまたはバックアップ コンフィギュレーション ファイルにファイル SSD インジケータが存在しない場合、このファイルへのアクセスはすべてのユーザに許されます。
- [両方] の読み取り権限を持つユーザは、すべてのミラー コンフィギュレーション ファイルおよびバックアップ コンフィギュレーション ファイルにアクセスすることができます。しかし、現在のセッションの読み取りモードがファイル SSD インジケータと異なる場合、ユーザには、そのアクションは許可されないことを示すプロンプトが提示されます。

- [プレーンテキストのみ] 権限を持つユーザは、そのファイル SSD インジケータが [除外] または [プレーンテキストのみ] 機密データを示している場合、ミラー コンフィギュレーション ファイルおよびバックアップ コンフィギュレーション ファイルにアクセスすることができます。
- [暗号化のみ] 権限を持つユーザは、そのファイル SSD インジケータが [除外] または [暗号化] 機密データを示している場合、ミラー コンフィギュレーション ファイルおよびバックアップ コンフィギュレーション ファイルにアクセスすることができます。
- [除外] 権限を持つユーザは、そのファイル SSD インジケータが [暗号化] または [プレーンテキスト] 機密データを示している場合、ミラー コンフィギュレーション ファイルおよびバックアップ コンフィギュレーション ファイルにアクセスできません。

ユーザは、ファイル内の機密データ（存在する場合）と競合するファイル SSD インジケータを手動で変更することはできません。それ以外の場合、プレーンテキストの機密データは想定外に漏洩する可能性があります。

機密データ ゼロタッチ自動コンフィギュレーション

SSD ゼロタッチ自動コンフィギュレーションは、暗号化された機密データを持つ対象デバイスの自動コンフィギュレーションです。そのとき機密データの暗号化にそのキーが使われるパスフレーズを使って手動で事前に対象デバイスを設定する必要はありません。

デバイスは、デフォルトで有効となる自動コンフィギュレーションを現在サポートしています。自動コンフィギュレーションが有効であり、ファイル サーバとブート ファイルを指定する DHCP オプションを利用しているデバイスは、ファイル サーバからブート ファイル（リモート コンフィギュレーション ファイル）をスタートアップ コンフィギュレーション ファイルにダウンロードしてからリブートします。

注 ファイル サーバは、DHCP オプション 150 およびデバイス上の静的設定に加え、bootp siaddr および sname フィールドにより指定されます。

ユーザは、暗号化された機密データによって対象デバイスを安全に自動設定することができます。まずコンフィギュレーションを持つデバイスからの自動コンフィギュレーションで使用されるコンフィギュレーション ファイルを作成します。デバイスには次の設定と指定が必要です。

- ファイルの機密データの暗号化
- ファイル コンテンツの整合性の強制
- デバイスおよび機密データへのセキュアなアクセスを適正に制御する、セキュアな認証コンフィギュレーション コマンドと SSD ルールを含める

コンフィギュレーション ファイルがユーザのパスフレーズで生成されていて、SSD ファイルのパスフレーズ制御が [制限あり] の場合、結果のコンフィギュレーション ファイルを目的の対象デバイスに自動設定することが可能です。しかし、自動コンフィギュレーションがユーザ定義のパスフレーズを継承する場合、対象デバイスは、ファイルを生成したゼロタッチではないデバイスと同一のパスフレーズにより手動であらかじめ設定されている必要があります。

コンフィギュレーション ファイルを生成するデバイスが、[制限なし] パスフレーズ制御モードにある場合、デバイスはパスフレーズをファイルに含めます。結果としてユーザは、対象デバイスをパスフレーズであらかじめ手動で設定しなくても、すぐに使えるデバイスや工場出荷時デフォルトのデバイスを含む対象デバイスを、コンフィギュレーション ファイルで自動設定することができます。対象デバイスがパスフレーズを直接コンフィギュレーション ファイルから取得するため、ゼロタッチと呼ばれます。

注 すぐに使える状態または工場出荷時デフォルト状態のデバイスは、デフォルトの匿名ユーザを使用して SCP サーバにアクセスします。

SSD 管理チャネル

デバイスは、telnet、SSH、Web などの管理チャネル経由で管理することができます。SSD はチャネルを、そのセキュリティやプロトコルに基づいて次のタイプに分類します。セキュア、セキュアでない、セキュア XML SNMP、およびセキュアでない XML SNMP です。

次に、SSD が各管理チャネルを「セキュア」または「セキュアでない」のどちらと見なしているかを示します。「セキュアでない」と見なした場合、表はパラレル セキュア チャネルを示します。

管理チャネル	SSD 管理チャネル タイプ	パラレル セキュア管理チャネル
コンソール	セキュア	
Telnet	セキュアでない	SSH
SSH	セキュア	
GUI/HTTP	セキュアでない	GUI/HTTPS
GUI/HTTPS	セキュア	
XML/HTTP	セキュアでない XML SNMP	XML/HTTPS

管理チャネル	SSD 管理チャネル タイプ	パラレル セキュア管理チャネル
XML/HTTPS	セキュア XML SNMP	
SNMPv1/v2/v3 （プライバシー機能なし）	セキュアでない XML SNMP	セキュア XML SNMP
SNMPv3 （プライバシー機能あり）	セキュア XML SNMP （レベル 15 ユーザ）	
TFTP	セキュアでない	SCP
SCP （セキュア コピー）	セキュア	
HTTP ベースのファイル転送	セキュアでない	HTTPS ベースのファイル転送
HTTPS ベースのファイル転送	セキュア	

メニュー CLI とパスワード リカバリ

メニュー CLI インターフェイスは、読み取り権限が [両方] または [プレーンテキストのみ] のユーザだけに許可されます。その他のユーザは拒否されます。メニュー CLI 中の機密データは、常にプレーンテキストとして表示されます。

パスワード リカバリは現在、ブート メニューからアクティブ化され、ユーザは認証なしでターミナルにログオンできます。SSD がサポートされている場合、このオプションはローカルのパスフレーズがデフォルトのパスフレーズと同じ場合にのみ許可されます。デバイスがユーザ定義のパスフレーズで設定されている場合、ユーザはパスワードの復元をアクティブ化できません。

SSD の設定

SSD 機能は次のページで設定されます。

- SSD プロパティは、[SSD プロパティ] ページで設定します。
- SSD ルールは、[SSD ルール] ページで定義します。

SSD プロパティ

[プレーンテキストのみ] または [両方] の SSD 読み取り権限を持つユーザのみが SSD プロパティを設定できます。

グローバル SSD プロパティを設定するには次のようにします。

ステップ 1 [セキュリティ] > [セキュア機密データ管理] > [プロパティ]をクリックします。

次のフィールドが表示されます。

- [現在のローカルパスフレーズのタイプ]:デフォルトのパスフレーズまたはユーザ定義のパスフレーズのどちらが現在使用されているかを表示します。

ステップ 2 次の [永続的設定] フィールドを入力します。

- [コンフィギュレーション ファイルのパスフレーズの制御]:「コンフィギュレーション ファイルのパスフレーズ制御」で説明されたオプションを選択します。
- [コンフィギュレーションファイルの整合性の制御]: この機能を有効化するには、このフィールドを選択します。「コンフィギュレーションファイルの整合性の制御」を参照してください。

ステップ 3 現在のセッションの読み取りモードを選択します(SSD ルールの要素を参照)。

ステップ 4 [適用] をクリックします。設定値が、実行コンフィギュレーション ファイルに保存されます。

ローカルのパスフレーズを変更するには次のようにします。

ステップ 1 [ローカル パスフレーズの変更] をクリックしてから新しい [ローカル パスフレーズ] を入力します。

- [デフォルト]:デバイスのデフォルト パスフレーズを使用します。
- [ユーザ定義(プレーンテキスト)]:新しいパスフレーズを入力します。

- [パスフレーズの確認]：新しいパスフレーズを確認します。

ステップ 2 [適用] をクリックします。設定値が、実行コンフィギュレーション ファイルに保存されます。

SSD ルール コンフィギュレーション

[プレーンテキストのみ] または [両方] の SSD 読み取り権限を持つユーザのみが SSD ルールを設定できます。

SSD ルールを設定するには次のようにします。

ステップ 1 [セキュリティ] > [セキュア機密データ管理] > [SSD ルール] をクリックします。

現在定義されているルールが表示されます。[ルールタイプ] フィールドは、ルールがユーザ定義かデフォルトかを示します。

ステップ 2 新しいルールを追加するには、[追加].をクリックします。次のフィールドを入力します。

- [ユーザ]：ルールを適用するユーザを定義します。次のいずれかのオプションを選択します。
  - [特定のユーザ]：ルールを適用する特定のユーザ名を選択して入力します（このユーザは必ずしも定義されている必要はありません）。
  - [デフォルトユーザ（cisco）]：ルールがデフォルト ユーザに適用されることを示します。
  - [レベル15]：ルールが特権レベル 15 を持つすべてのユーザに適用されます。
  - [すべて]：ルールがすべてのユーザに適用されることを示します。
- [チャネル]：ルールが適用される入力チャネルのセキュリティ レベルを定義します。次のいずれかのオプションを選択します。
  - [セキュア]：ルールが、セキュアなチャネル（コンソール、SCP、SSH および HTTPS）にのみ適用されることを示します。SNMP と XML チャネルは含みません。
  - [セキュアでない]：ルールが、セキュアでないチャネル（Telnet, TFTP および HTTP）にのみ適用されることを示します。SNMP と XML チャネルは含みません。
  - [セキュアXML SNMP]：ルールが XML over HTTPS およびプライバシー機能のある SNMPv3 のみに適用されることを示します。

- [セキュアでないXML SNMP]:ルールが XML over HTTP または SNMPv1/v2 およびプライバシー機能のない SNMPv3、あるいはその両方のみに適用されることを示します。

- [読み取り権限]:ルールと関連する読み取り権限。次のものがあります。
  - [除外]:最も低い読み取り権限。ユーザはいかなるフォームでも機密データを取得することが許可されません。
  - [プレーンテキストのみ]:上記よりも高い読み取り権限。ユーザはプレーンテキストのみで機密データを取得することが許可されます。
  - [暗号化のみ]:中間の読み取り権限。ユーザは暗号化のみで機密データを取得することが許可されます。
  - [両方(プレーンテキストおよび暗号化)]:最も高い読み取り権限。ユーザは、暗号化およびプレーンテキストの権限の両方を持ち、暗号化された機密データおよびプレーンテキストの機密データの取得が許可されます。

- [デフォルトの読み取りモード]:すべてのデフォルトの読み取りモードは、ルールの読み取り権限に従属します。次のオプションが存在しますが、ルールの読み込み権限によっては拒否されることがあります。
  - [除外]:機密データの読み取りを許可しません。
  - [暗号化]:機密データは暗号化形式で提示されます。
  - [プレーンテキスト]:機密データはプレーンテキストで提示されます。

ステップ 3 [適用] をクリックします。設定値が、実行コンフィギュレーション ファイルに保存されます。

ステップ 4 次のアクションは選択したルールで実行されます。

- ルールの [追加]、[編集]、または [削除]、または [デフォルトへの復元]。
- [すべてのルールをデフォルトに戻す]:ユーザが変更したデフォルト ルールをデフォルト ルールに復元します。

20

セキュリティ:SSH サーバ

ここでは、デバイス上で SSH セッションを確立する方法について説明します。

具体的な内容は、次のとおりです。

概要

SSH サーバ機能を使用すれば、リモート ユーザは、デバイスに対して SSH セッションを確立することができます。これは、セッションが保護されることを除いて、Telnet セッションを確立する場合と同様です。

デバイスは、SSH サーバとして、パスワードと公開キーのどちらかでリモート ユーザを認証する SSH ユーザ認証をサポートします。一方、リモート ユーザは、SSH クライアントとして、デバイス公開キー(フィンガープリント)を使用してデバイスを認証することで SSH サーバ認証を実行することができます。

SSH サーバは次のモードで動作できます。

- **内部生成 RSA/DSA キー(デフォルト設定)**:RSA キーと DSA キーが生成されます。ユーザは、SSH サーバ アプリケーションにログオンして、デバイスの IP アドレスを入力し、デバイス上でセッションを開こうとしたときに自動的に認証されます。
- **公開キー モード**:ユーザはデバイス上で定義されます。彼らの RSA/DSA キーは、PuTTY などの外部の SSH サーバ アプリケーションで生成されます。公開キーがデバイス上で入力されます。こうして、ユーザは、外部の SSH サーバ アプリケーションを介してデバイス上で SSH セッションを開くことができます。

一般的な作業

ここでは、SSH サーバ機能を使用して実行される一般的な作業について説明します。

ワークフロー 1：SSH ユーザ認証を使用せずに SSH セッションを構築するために、次の手順を実行します。

ステップ 1 [TCP/UDP サービス] ページで SSH サーバを有効にします。

ステップ 2 [SSH ユーザ認証] ページでパスワードと公開キーによる SSH ユーザ認証を無効にします。

ステップ 3 PUTTY などの SSH クライアント アプリケーションからデバイスに対して SSH セッションを確立します。

ワークフロー 2：パスワードによる SSH ユーザ認証を使用して SSH セッションを構築するために、次の手順を実行します。

ステップ 1 [TCP/UDP サービス] ページで SSH サーバを有効にします。

ステップ 2 [SSH ユーザ認証] ページでパスワードによる SSH ユーザ認証を有効にします。

ステップ 3 PUTTY などの SSH クライアント アプリケーションからデバイスに対して SSH セッションを確立します。

ワークフロー 3：公開キーによる SSH ユーザ認証を使用して SSH セッションを構築するには、次の手順を実行します。管理認証のバイパスをするかどうかは任意です。

ステップ 1 [TCP/UDP サービス] ページで SSH サーバを有効にします。

ステップ 2 [SSH ユーザ認証] ページで公開キーによる SSH ユーザ認証を有効にします。公開キーは、SSH クライアント上で事前に作成しておく必要があり、SSH クライアントがデバイス上で SSH サーバに対する SSH セッションを確立するときに使用されます。

ステップ 3 必要に応じて、[SSH ユーザ認証] ページで管理認証をパスすることによる自動ログインを有効にします。

ステップ 4 [SSH ユーザ認証] ページで SSH ユーザ認証テーブルにユーザとその公開キーを追加します。

ステップ 5 PUTTY などの SSH クライアント アプリケーションからデバイスに対して SSH セッションを確立します。

SSH ユーザ認証

[SSH ユーザ認証] ページを使用して、公開キーまたはパスワードによる SSH ユーザ認証を有効にします。ユーザが公開キーを使用して SSH サーバを確立する場合は、ユーザ名と公開キーを SSH ユーザ認証テーブルに入力しておく必要があります。ユーザがパスワードを使用して SSH セッションを確立する場合は、ユーザ名とパスワードを管理アクセス権を持っているユーザのものにする必要があります。

ユーザを追加するためには、外部の SSH キー生成/クライアント アプリケーション（PuTTY など）でユーザの RSA または DSA キーを生成する必要があります。

自動ログイン

[SSH ユーザ認証] ページを使用して、ローカル ユーザ データベース内ですでに設定済みのユーザの SSH ユーザ名を作成する場合。次のように、**自動ログイン**機能を設定することによって、追加の認証を避けることができます。

- [有効]：ユーザがローカル データベース内で定義されており、そのユーザが公開キーを使用した SSH 認証をパスした場合は、ローカル データベースのユーザ名とパスワードによる認証が省略されます。

  注 この特定の管理方式（コンソール、Telnet、SSH など）用に設定された認証方式は *ローカル*にする（つまり、*RADIUS* や *TACACS+* ではない）必要があります。詳細については、「管理アクセス方式」を参照してください。

- [無効]：SSH 公開キーによる認証が成功したら、ユーザ名がローカル ユーザ データベース内で設定されている場合でも、[管理アクセス認証] ページで設定された認証方式によってユーザが再度認証されます。

このページはオプションです。SSH でユーザ認証を操作する必要はありません。

認証を有効にしてユーザを追加するには、次のようにします。

ステップ 1 [セキュリティ] > [SSH サーバ] > [SSH ユーザ認証] の順にクリックします。

ステップ 2 次のフィールドを選択します。

- [パスワードによる SSH ユーザ認証]：ローカル データベース内で設定されたユーザ名/パスワードを使用して SSH クライアント ユーザの認証を実行する場合に選択します（「ユーザ アカウント」を参照）。
- [公開キーによるSSH ユーザ認証]：公開キーを使用して SSH クライアント ユーザの認証を実行する場合に選択します。
- [自動ログイン]：このフィールドは、[公開キーによる SSH ユーザ認証] 機能が選択された場合に有効にすることができます。

ステップ 3 [適用] をクリックします。設定値が、実行コンフィギュレーション ファイルに保存されます。

設定されたユーザに関する次のフィールドが表示されます。

- [SSH ユーザ名]:ユーザのユーザ名。
- [キータイプ]:RSA キーか DSA キーか。
- [フィンガープリント]:公開キーから生成されるフィンガープリント。

ステップ 4 [追加] をクリックして、新しいユーザを追加し、次のフィールドに値を入力します。

- [SSH ユーザ名]:ユーザ名を入力します。
- [キータイプ]:[RSA] と [DSA] のどちらかを選択します。
- [公開キー]:このテキスト ボックスに、外部の SSH クライアント アプリケーション（PuTTY など）で生成された公開キーをコピーします。

ステップ 5 [適用] をクリックして、新しいユーザを保存します。

すべてのアクティブなユーザに関する次のフィールドが表示されます。

- [IP アドレス]:アクティブ ユーザの IP アドレス。
- [SSH ユーザ名]:アクティブ ユーザのユーザ名。
- [SSH バージョン]:アクティブ ユーザによって使用される SSH のバージョン。
- [暗号]:アクティブ ユーザの暗号。
- [認証コード]:アクティブ ユーザの認証コード。

SSH サーバ認証

リモート SSH クライアントは、SSH サーバ認証を実行することによって、想定された SSH ドライバへの SSH セッションが確立されていることを保証します。SSH サーバ認証を実行するには、リモート SSH クライアントにターゲット SSH サーバの SSH サーバ公開キー（またはフィンガープリント）のコピーが保存されている必要があります。

[SSH サーバ認証] ページで、SSH サーバとしてのデバイスの秘密/公開キーが生成/インポートされます。ユーザは、SSH セッションで SSH サーバ認証を実行する場合に、このデバイスの SSH サーバ公開キー（またはフィンガープリント）をアプリケーショ

ンにコピーする必要があります。公開/秘密 RSA キーおよび DSA キーは、デバイスが工場出荷時設定からブートしたときに自動的に生成されます。各キーは、該当するユーザ設定キーがユーザによって削除されたときも自動的に作成されます。

RSA または DSA キーを再生成する、または、別のデバイス上で生成された RSA/DSA キーをコピーするには、次のようにします。

ステップ 1 [セキュリティ] > [SSH サーバ] > [SSH サーバ認証] の順にクリックします。

キーごとに次のフィールドが表示されます。

- [キータイプ]:RSA または DSA。
- [キーソース]:[自動生成] または [ユーザ定義]。
- [フィンガープリント]:キーから生成されるフィンガープリント。

ステップ 2 RSA キーと DSA キーのどちらかを選択します。

ステップ 3 次のアクションのいずれかを実行します。

- [生成]:選択されたタイプのキーを生成します。
- [編集]:別のデバイスからのキーをコピーできるようにします。次のフィールドを入力します。
  - [キータイプ]:上記参照。
  - [公開キー]:公開キーを入力します。
  - [秘密キー]:[暗号化済み] または [プレーンテキスト] のどちらかを選択して、秘密キーを入力します。

  [機密データを暗号化して表示] または [機密データを平文で表示] をクリックすると、機密データの表示方法が設定されます。
- [削除]:キーを削除できるようにします。
- [詳細]:生成されたキーを表示できるようにします。[詳細] ウィンドウでは、[機密データを平文で表示] をクリックすることもできます。これをクリックすると、キーが暗号化形式ではなく、平文で表示されます。キーがすでに平文で表示されている場合は、[機密データを暗号化して表示] をクリックしてテキストを暗号化形式で表示することができます。

21

セキュリティ:SSH クライアント

このセクションでは、SSH クライアントとして動作するデバイスについて説明します。

具体的な内容は、次のとおりです。

- 概要
- SSH ユーザ認証
- SSH サーバ認証
- SSH サーバのユーザ パスワードの変更

概要

セキュア コピー (SCP) と SSH

セキュア シェルまたは SSH は、SSH クライアント(この場合はデバイス)と SSH サーバとの間で、セキュリティの確保されたチャネル上でデータを交換することを可能にするネットワーク プロトコルです。

SSH クライアントによりユーザは、ネットワークが 1 つ以上のスイッチで構成されていて、さまざまなシステム ファイルが 1 つの中央 SSH サーバに保管されている場合に、ネットワークの管理作業を実行できます。ネットワークを通じてコンフィギュレーション ファイルが転送される際、SSH プロトコルを利用するアプリケーションの 1 つであるセキュア コピー (SCP) により、ユーザ名/パスワードなどの機密データが盗まれないことが保証されます。

セキュア コピー (SCP) は、ファームウェア、ブート イメージ、コンフィギュレーション ファイル、言語ファイル、およびログ ファイルを、中央 SCP サーバからデバイスに安全に転送するために使用されます。

SSH において、デバイス上で実行される SCP は SSH クライアント アプリケーションであり、SCP サーバは SSH サーバ アプリケーションです。

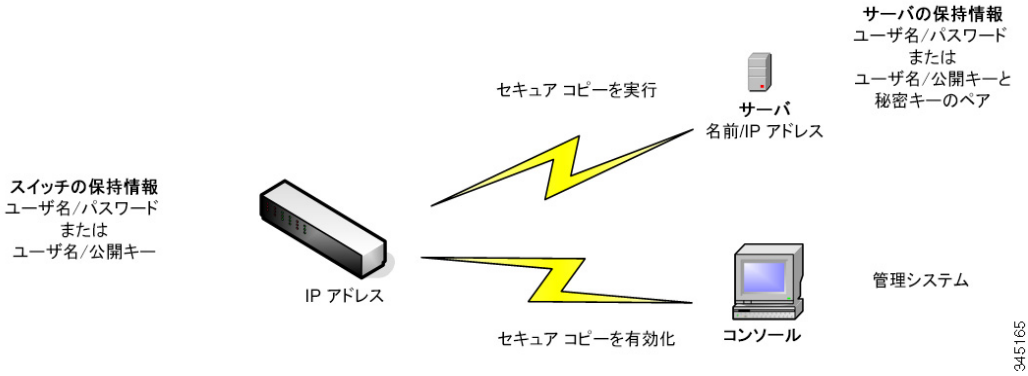
TFTP または HTTP を通じてファイルがダウンロードされる際、データ転送のセキュリティは確保されません。

SCP を通じてファイルがダウンロードされる場合、セキュリティが確保されたチャネルを通じて SCP サーバからデバイスに情報がダウンロードされます。そのセキュア チャネルの作成の前に、ユーザが操作を実行する許可を得るための認証が実行されます。

認証情報は、デバイス上でも SSH サーバ上でもユーザが入力する必要があります。ただし、このガイドではサーバの操作については説明しません。

SCP 機能を使用したネットワーク設定の典型的な処理について、以下の図に示します。

典型的なネットワーク設定処理



SSH サーバ認証

SSH クライアントとしてのデバイスは、信頼できる SSH サーバとのみ通信します。SSH サーバ認証が無効になっている場合（デフォルトの設定）、どの SSH サーバも信頼できるものと見なされます。SSH サーバ認証がオンの場合、ユーザは、信頼できるサーバのためのエントリを信頼 SSH サーバ テーブルに追加する必要があります。このテーブルには、SSH 信頼サーバごとに以下の情報が格納されます。最大 16 個のサーバについて、以下の情報が含まれます。

- サーバの IP アドレス/ホスト名
- サーバの公開キー フィンガープリント

SSH サーバ認証がオンの場合、デバイス上で実行されている SSH クライアントは、以下の認証プロセスを使用して SSH サーバの認証を実行します。

- 受信した SSH サーバ公開キーのフィンガープリントがデバイスにより計算されます。
- デバイスにより、SSH 信頼サーバ テーブルから SSH サーバの IP アドレス/ホスト名が検索されます。以下のいずれか 1 つが可能です。
  - 一致するものが検出された場合、サーバの IP アドレス/ホスト名とそのフィンガープリントの両方について、サーバが認証されます。
  - 一致する IP アドレス/ホスト名は検出されるものの、一致するフィンガープリントは見つからない場合、検索が続行されます。一致するフィンガープリントが見つからない場合、検索は完了し、認証は失敗します。
  - 一致する IP アドレス/ホスト名が見つからない場合、検索は完了し、認証は失敗します。
- 信頼サーバのリストの中に SSH サーバのエントリが見つからない場合、プロセスは失敗します。

即使用可能デバイス（出荷時設定のデバイス）の自動設定をサポートするため、デフォルトでは SSH サーバ認証が無効になっています。

SSH ユーザ認証

デバイス（SSH クライアント）が SSH サーバに対する SSH セッションを確立しようとしたときに、SSH サーバはさまざまな方法でクライアントを認証します。それらについて、以下に説明します。

パスワード

パスワード方式を使用するには、まず、ユーザ名/パスワードが SSH サーバ上で確立されていなければなりません。これは、デバイスの管理システムでは実行されません。ただし、サーバ上でユーザ名が確立された後に、デバイスの管理システムによりサーバパスワードを変更することは可能です。

その後、デバイス上でユーザ名/パスワードを作成する必要があります。デバイスが SSH サーバに対する SSH セッションを確立しようとしたときに、デバイスから提供されるユーザ名/パスワードがサーバ上のユーザ名/パスワードと一致する必要があります。

データは、セッション中にネゴシエートされるワンタイム対称キーを使用して暗号化できます。

管理対象の各デバイスには、それぞれ独自のユーザ名/パスワードが必要です。一方、スイッチについては、複数のスイッチで同じユーザ名/パスワードを使用できます。

パスワード方式は、デバイスでのデフォルトの方式です。

公開/秘密キー

SSH サーバによるクライアント認証に公開/秘密キー方式を使用するには、SSH クライアントであるデバイス上でユーザを作成して、公開/秘密キーのペアを生成/インポートします。その後で、SSH サーバ上で同じユーザを作成し、SSH クライアントで生成/入力された公開キー（またはフィンガープリント）を SSH サーバにコピーします。ユーザを作成して、公開キー（またはフィンガープリント）を SSH サーバにコピーする操作については、このガイドでは扱いません。

RSA と DSA のデフォルト キー ペアは、デバイス ブート時に生成されます。それらのキーのうちの 1 つが、SSH サーバからダウンロードするデータの暗号化のために使用されます。デフォルトでは RSA キーが使用されます。

ユーザがそれらのキーの一方または両方を削除した場合、それらは再生成されます。

公開/秘密キーは、暗号化されてデバイスのメモリに保管されます。キーはデバイスのコンフィギュレーション ファイルの一部であり、秘密キーは、暗号化された形またはプレーンテキストの形でユーザに対して表示可能です。

秘密キーを別のデバイスの秘密キーに直接コピーすることはできないため、秘密キーをデバイスからデバイスへコピーするインポート メソッドが存在します（「*キーのインポート*」を参照）。

キーのインポート

キー方式の場合、個々のデバイスに対して公開/秘密キーをそれぞれ別個に作成する必要があります。セキュリティ上の理由から、それらの秘密キーを、あるデバイスから別のデバイスに直接コピーすることはできません。

ネットワーク内に複数のスイッチがある場合、各公開/秘密キーを作成してからそれぞれ個別に SSH サーバにロードしなければならないため、全スイッチの公開/秘密キーを作成する処理には時間がかかります。

この処理を簡素化するため、暗号化された秘密キーをシステム内の全スイッチに安全な方法で転送することを可能にする付加的な機能があります。

デバイス上で秘密キーが作成される際は、それに関連する*パスフレーズ*を作成することも可能です。このパスフレーズは、秘密キーを暗号化して残りのスイッチにインポートするために使用されます。それにより、すべてのスイッチで同じ公開/秘密キーを使用することが可能になります。

デフォルト パスワード

デフォルトで、パスワードによる SSH ユーザ認証が有効になっており、ユーザ名/パスワードは「anonymous」です。

ユーザは、認証のための以下の情報を設定する必要があります。

- 使用する認証方式。
- ユーザ名/パスワードまたは公開/秘密キーのペア。

サポートされるアルゴリズム

デバイス（SSH クライアントとして動作）と SSH サーバの間の接続が確立済みの場合、クライアントと SSH サーバは、SSH トランスポート層で使用するアルゴリズムを決定するためにデータをやり取りします。

クライアント側では、以下のアルゴリズムがサポートされています。

- キー交換アルゴリズム-diffie-hellman
- 暗号化アルゴリズム
  - aes128-ctr
  - aes192-ctr
  - aes256-ctr
  - Chacha
  - Poly1305
- メッセージ認証コード アルゴリズム
  - hmac-sha1

注 圧縮アルゴリズムはサポートされていません。

作業を開始する前に

SCP 機能を使用するには、その前に、以下の操作を実行する必要があります。

- パスワード認証方式を使用する場合、SSH サーバ上でユーザ名/パスワードをセットアップする必要があります。
- 公開/秘密キー認証方式を使用する場合、SSH サーバ上で公開キーを保管する必要があります。

一般的な作業

ここでは、SSH クライアントとしてのデバイスで実行される共通タスクについて説明します。ここで参照されているページはすべて、メニュー ツリーのうち [SSH クライアント] の分岐の下にあるページです。

ワークフロー 1：SSH クライアントを設定し、リモート SSH サーバとの間でデータをやり取りするには、次の手順を実行します。

ステップ 1 パスワード方式と公開/秘密キー方式のどちらを使用するかを決定します。[SSH ユーザ認証] ページを使用します。

ステップ 2 パスワード方式が選択された場合、以下の手順を実行します。

a. 実際にセキュア データ転送をアクティブにする際、[SSH ユーザ認証] ページでグローバル パスワードを作成するか、[ファームウェア操作] または [ファイル操作] ページで一時パスワードを作成します。

b. SCP を使用し、[ファームウェア操作] ページの [SCP] オプションを選択することにより、ファームウェア、ブート イメージ、または言語ファイルをアップグレードします。このページでは、パスワードを直接入力するか、または [SSH ユーザ認証] ページで入力したパスワードを使用することができます。

c. SCP を使用し、[ファイル操作] ページの [SCP 経由(SSHを使用)] オプションを選択することにより、コンフィギュレーション ファイルをダウンロード/バックアップします。このページでは、パスワードを直接入力するか、または [SSH ユーザ認証] ページで入力したパスワードを使用することができます。

ステップ 3 リモート SSH サーバ上でユーザ名/パスワードをセットアップするか、パスワードを変更します。これはサーバに依存した作業であり、ここでは説明しません。

ステップ 4 公開/秘密キー方式を使用する場合は、以下の手順を実行します。

a. RSA と DSA のどちらのキーを使用するかを選択し、ユーザ名を作成した後、公開/秘密キーを生成します。

b. [詳細] ボタンをクリックすることにより、生成されたキーを表示し、ユーザ名と公開キーを SSH サーバに転送します。これはサーバに依存した作業であり、ここでは説明しません。

c. SCP を使用し、[ファームウェア操作] ページの [SCP] オプションを選択することにより、ファームウェアをアップグレード/バックアップします。

d. SCP を使用し、[ファイル操作] ページの [SCP] オプションを選択することにより、コンフィギュレーション ファイルをダウンロード/バックアップします。

ワークフロー 2：公開/秘密キーを 1 つのデバイスから別のデバイスにインポートするには、次の手順を実行します。

ステップ 1 [SSH ユーザ認証] ページで公開/秘密キーを生成します。

ステップ 2 [SSD プロパティ] ページで SSD のプロパティを設定し、新しいローカル パスフレーズを作成します。

ステップ 3 [詳細] をクリックして、生成された暗号化キーを表示し、それらを [詳細] ページから外部デバイスにコピーします（Begin および End フッタを含む）。公開キーと秘密キーを別個にコピーします。

ステップ 4 もう一方のデバイスにログオンし、[SSH ユーザ認証] ページを開きます。必要なキーのタイプを選択して [編集] をクリックします。公開/秘密キーを貼り付けます。

ステップ 5 [適用] をクリックして、公開/秘密キーを第 2 のデバイスにコピーします。

ワークフロー 3：SSH サーバ上でパスワードを変更するには、次の手順を実行します。

ステップ 1 [SSH サーバのユーザ パスワードの変更] ページでサーバを特定します。

ステップ 2 新しいパスワードを入力します。

ステップ 3 [適用] をクリックします。

SSH ユーザ認証

このページは、パスワード方式が選択されている場合は SSH ユーザ認証方式を選択したり、デバイス上のユーザ名とパスワードを設定したりするため、また、公開/秘密キー方式が選択されている場合は RSA または DSA キーを生成するために使用されます。

認証方式を選択し、ユーザ名/パスワード/キーを設定するには、次の手順を実行します。

ステップ 1 [セキュリティ] > [SSH クライアント] > [SSH ユーザ認証] をクリックします。

ステップ 2 [SSH ユーザ認証方式] を選択します。これは、セキュア コピー用に定義されているグローバルな方式です (SCP)。次のいずれかのオプションを選択します。

- [パスワード]：これはデフォルトの設定です。これが選択されている場合は、パスワードを入力するか、デフォルトのパスワードをそのまま受け入れます。

- [RSA公開キーによる]：これが選択されている場合、[SSH ユーザキーテーブル]のブロックで RSA の公開キーと秘密キーを作成します。
- [DSA公開キーによる]：これが選択されている場合、[SSH ユーザキーテーブル]のブロックで DSA の公開/秘密キーを作成します。

ステップ 3 （どの方式が選択されている場合でも）[ユーザ名] を入力するか、またはデフォルトのユーザ名をそのまま使用します。これは、SSH サーバで定義されているユーザ名と一致していなければなりません。

ステップ 4 [パスワード] 方式が選択されている場合は、パスワード（[暗号化] または [プレーンテキスト]）を入力するか、またはデフォルトの暗号化パスワードをそのまま受け入れます。

ステップ 5 次のいずれかの操作を実行します。

- [適用]：選択した認証方式が、そのアクセス方式に割り当てられます。
- [デフォルトのクレデンシャルの復元]：デフォルトのユーザ名とパスワード (anonymous) が復元されます。
- [機密データを平文で表示]：現在のページの秘密データがプレーンテキストとして表示されます。

[SSH ユーザキーテーブル]：各キーについて、以下のフィールドが含まれています。

- [キータイプ]：RSA または DSA。
- [キーソース]：[自動生成] または [ユーザ定義]。
- [フィンガープリント]：キーから生成されるフィンガープリント。

ステップ 6 RSA キーまたは DSA キーを処理するには、[RSA] か [DSA] を選択してから、以下の操作のいずれかを実行します。

- [生成]：新しいキーを生成します。
- [編集]：別のデバイスにコピー/ペーストするキーを表示します。
- [削除]：キーを削除します。
- [詳細]：キーを表示します。

SSH サーバ認証

SSH サーバ認証を有効にし、信頼できるサーバを定義するには、次の手順を実行します。

ステップ 1 [セキュリティ] > [SSH クライアント] > [SSH サーバ認証] をクリックします。

ステップ 2 [有効] を選択して、SSH サーバ認証を有効にします。

- [IPv4 送信元インターフェイス]：IPv4 SSH サーバとの通信に使用されるメッセージ用ソース IPv4 アドレスとして IPv4 アドレスを使用するソース インターフェイスを選択します。
- [IPv6 送信元インターフェイス]：IPv6 SSH サーバとの通信に使用されるメッセージ用ソース IPv6 アドレスとして IPv6 アドレスを使用するソース インターフェイスを選択します。

  注 [自動] オプションが選択されている場合、システムは、発信インターフェイスで定義された IP アドレスからソース IP アドレスを取得します。

ステップ 3 [適用] をクリックします。

ステップ 4 [追加] をクリックし、SSH 信頼サーバについての以下のフィールドを入力します。

- [サーバ指定方法]：SSH サーバを特定するための方法を 1 つ選択します。
  - [IP アドレス]：これが選択されている場合、以下のフィールドにサーバの IP アドレスを入力します。
  - [名前]：これが選択されている場合、[サーバの IP アドレス/名前] フィールドにサーバの名前を入力します。
- [IP バージョン]：IP アドレスで SSH サーバを指定することを選択した場合、その IP アドレスが IPv4 アドレスなのか、それとも IPv6 アドレスなのかを選択します。
- [IPv6 アドレスタイプ]：SSH サーバ IP アドレスが IPv6 アドレスの場合、IPv6 アドレス タイプを選択します。次のオプションがあります。
  - [リンク ローカル]：IPv6 アドレスによって、単一ネットワーク リンク上のホストが一意に識別されます。リンク ローカル アドレスのプレフィックス部は FE80 です。このタイプのアドレスはルーティング不能であり、ローカル ネットワーク内で通信する場合にのみ使用できます。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。

- [グローバル]：IPv6 アドレスは、他のネットワークから認識可能かつアクセス可能なグローバル ユニキャスト IPV6 タイプになります。

- [リンクローカルインターフェイス]：インターフェイスのリストからリンクローカル インターフェイスを選択します。
- [ログサーバの IP アドレス/名前]：[サーバ指定方法] での選択内容に応じて、SSH サーバの IP アドレスか、またはその名前のいずれかを入力します。
- [フィンガープリント]：SSH サーバのフィンガープリントを入力します（そのサーバからコピーしたもの）。

ステップ 5 [適用] をクリックします。信頼できるサーバの定義が、実行コンフィギュレーション ファイルに保存されます。

SSH サーバのユーザ パスワードの変更

SSH サーバ上でパスワードを変更するには、次のようにします。

ステップ 1 [セキュリティ] > [SSH クライアント] > [SSH サーバのユーザパスワードの変更] をクリックします。

ステップ 2 次のフィールドを入力します。

- [サーバ指定方法]：[IP アドレス] か [名前] のいずれかを選択することにより、SSH サーバを定義します。[ログサーバの IP アドレス/名前] フィールドに、サーバの名前またはサーバの IP アドレスを入力します。
- [IP バージョン]：IP アドレスで SSH サーバを指定することを選択した場合、その IP アドレスが IPv4 アドレスなのか、それとも IPv6 アドレスなのかを選択します。
- [IPv6 アドレス タイプ]：SSH サーバ IP アドレスが IPv6 アドレスの場合、IPv6 アドレス タイプを選択します。次のオプションがあります。

  - [リンク ローカル]：IPv6 アドレスによって、単一ネットワーク リンク上のホストが一意に識別されます。リンク ローカル アドレスのプレフィックス部は FE80 です。このタイプのアドレスはルーティング不能であり、ローカル ネットワーク内で通信する場合にのみ使用できます。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。

- [グローバル]：IPv6 アドレスは、他のネットワークから認識可能かつアクセス可能なグローバル ユニキャスト IPV6 タイプになります。

- [リンクローカルインターフェイス]：インターフェイスのリストからリンクローカル インターフェイスを選択します。
- [ログサーバの IP アドレス/名前]：[サーバ指定方法] での選択内容に応じて、SSH サーバの IP アドレスか、またはその名前のいずれかを入力します。
- [ユーザ名]：これは、サーバで定義されているユーザ名と一致していなければなりません。
- [古いパスワード]：これは、サーバで定義されているパスワードと一致していなければなりません。
- [新しいパスワード]：新しいパスワードを入力し、[パスワードの確認] フィールドでその確認入力をします。

ステップ 3 [適用] をクリックします。SSH サーバ上のパスワードが変更されます。

22

アクセス制御

アクセス コントロール リスト（ACL）機能は、セキュリティ メカニズムの一部です。ACL 定義は、特定のサービス品質（QoS）が付与されるトラフィック フローの定義に使用するメカニズムの 1 つです。詳細については、「サービス品質」を参照してください。

ネットワーク マネージャは、ACL を使用して入力トラフィックのパターン（フィルタとアクション）を定義できます。ACL がアクティブなポートまたは LAG 上のデバイスに届いたパケットは、エントリを許可または拒否されます。

ここで説明する内容は次のとおりです。

- 概要
- MAC ベース ACL の作成
- IPv4 ベース ACL の作成
- IPv6 ベース ACL の作成
- ACL バインディング

概要

アクセス コントロール リスト（ACL）は、分類フィルタとアクションの番号付きリストです。それぞれの分類規則とそのアクションを、アクセス コントロール要素（ACE）と呼びます。

各 ACE は、トラフィック グループを区別するフィルタと、それらのフィルタに関連付けられたアクションで構成されています。1 つの ACL には 1 つ以上の ACE が含まれることがあります。ACE は、入力フレームのコンテンツと照合されます。コンテンツがフィルタに一致するフレームには、DENY アクションか PERMIT アクションが適用されます。

さまざまなデバイスが次の数の ACL および ACE をサポートします。

デバイス	最大 ACL 数	最大 ACE 数
SG550XG/SX550X	2K	2K
Sx550X	3K	3K
SG350XG/SX350X	2K	2K
SG350 および Sx350	1K	1K
Sx250	512	512

単一ポートまたは単一 ACL で最大 256 の ACE を設定できます。

パケットが ACE フィルタに一致した場合、その ACE アクションが実行され、ACL 処理は中止されます。パケットが ACE フィルタに一致しない場合は、次の ACE アクションが処理されます。1 つの ACL に含まれるどの ACE とも一致しない場合、他にも ACL があれば、その ACL が同様に処理されます。

注 関連するすべての ACL に含まれるどの ACE とも一致しない場合、そのパケットは破棄されます(デフォルトのアクション)。このような場合、デフォルトでパケットが破棄されるため、ACE を ACL に明示的に追加し、必要なトラフィックが許可されるように設定する必要があります。必要なトラフィックには、デバイス自体に送信される、Telnet、HTTP、SNMP などの管理トラフィックが含まれます。たとえば、ACL の条件と一致しないパケットをすべて廃棄しないようにするには、最もプライオリティの低い ACE を ACL に明示的に追加して、すべてのトラフィックを許可する必要があります。

ACL がバインドされているポートで IGMP/MLD スヌーピングが有効になっている場合は、ACE フィルタをその ACL に追加して、IGMP/MLD パケットがデバイスに転送されるようにします。追加しない場合、IGMP/MLD スヌーピングはそのポートで失敗します。

最初に一致した ACE が適用されるため、ACL 内における ACE の順序は重要です。ACE は、先頭のものから順次処理されます。

ACL は、特定のトラフィック フローを許可または拒否するなどの方法により、セキュリティ目的で使用する場合があります。また、QoS 拡張モードにおけるトラフィックの分類や優先順位付けにも使用されます。

注 ポートには、ACL を使用したセキュリティか QoS 拡張ポリシーを設定できますが、両方を同時に設定することはできません。

1 つのポートに関連付けられる ACL は、原則として 1 つのみです。ただし例外として、IP ベース ACL と IPv6 ベース ACL は、両方とも 1 つのポートに関連付けることができます。

1 つのポートに複数の ACL を関連付けるには、1 つ以上のクラス マップを含むポリシーを使用する必要があります。

定義できる ACL のタイプは、フレーム ヘッダーのどの部分を検査対象とするかにより異なっており、次のとおりです。

- MAC ACL：レイヤ 2 フィールドのみを検査します。「Defining MAC-based ACLs」を参照してください。
- IP ACL：IP フレームのレイヤ 3 レイヤを検査します。「IPv4 ベース ACL」を参照してください。
- IPv6 ACL：IPv4 フレームのレイヤ 3 レイヤを検査します。「Defining IPv6-Based ACL」を参照してください。

ACL 内のフィルタと一致したフレームは、その ACL の名前と同じ名前を持つフローとして定義されます。拡張 QoS の場合、このフロー名を使用してこれらのフレームを参照でき、QoS をこれらのフレームに適用できます。

ACL ロギング

この機能により、ACE にロギング オプションを追加できます。この機能が有効になっている場合、ACE が許可または拒否したパケットはすべて、これに関連する情報 SYSLOG メッセージを生成します。

ACL ロギングが有効な場合、ACL をインターフェイスにバインドすることにより、ACL ロギングをインターフェイスごとに指定できます。この場合、このインターフェイスに関連付けられている許可 ACE または拒否 ACE と一致するパケットに対して、SYSLOG が生成されます。

フローは、同一の特徴を持つパケットのストリームとして、次のように定義されます。

- 「レイヤ 2 パケット」：同じ送信元と宛先の MAC アドレス
- 「レイヤ 3 パケット」：同じ送信元と宛先の IP アドレス
- 「レイヤ 4 パケット」：同じ送信元と宛先の IP および L4 ポート

新しいフローの場合は常に、特定のインターフェイスからトラップされた先頭のパケットにより情報 SYSLOG メッセージが生成されます。同じフローの追加パケットは CPU にトラップされますが、このフローに対する SYSLOG メッセージは、5 分につき 1 メッセージのみ生成されます。この SYSLOG により、過去 5 分以内に少なくとも 1 パケットはトラップされたことがわかります。

トラップされたパケットの処理後、これらのパケットは許可の場合は転送され、拒否の場合は破棄されます。

サポートされるフローの数は、ユニットあたり 150 フローです。

SYSLOG

SYSLOG メッセージには情報の重大度が示され、パケットが拒否ルールか許可ルールと一致したかどうかが記述されます。

- レイヤ 2 パケットの場合、SYSLOG には次の情報が含まれます（該当する場合）：送信元 MAC、宛先 MAC、イーサタイプ、VLAN ID、および CoS キュー。
- レイヤ 3 パケットの場合、SYSLOG には次の情報が含まれます（該当する場合）：ソース IP、宛先 IP アドレス、プロトコル、DSCP 値、ICMP タイプ、ICMP コード、および IGMP タイプ。
- レイヤ 4 パケットの場合、SYSLOG には次の情報が含まれます（該当する場合）：送信元ポート、宛先ポート、および TCP フラグ。

次に SYSLOG の例を示します。

- 非 IP パケットの場合：
  - 06-Jun-2013 09:49:56 %3SWCOS-I-LOGDENYMAC: gi0/1: deny ACE 00:00:00:00:00:01 -> ff:ff:ff:ff:ff:ff, Ethertype-2054, VLAN-20, CoS-4, trapped
- IP パケット（v4 および v6）の場合：
  - 06-Jun-2013 12:38:53 %3SWCOS-I-LOGDENYINET: gi0/1: deny ACE IPv4(255) 1.1.1.1 -> 1.1.1.10, protocol-1, DSCP-54, ICMP Type-Echo Reply, ICMP code-5 , trapped
- L4 パケットの場合：
  - 06-Jun-2013 09:53:46 %3SWCOS-I-LOGDENYINETPORTS: gi0/1: deny ACE IPv4(TCP) 1.1.1.1(55) -> 1.1.1.10(66), trapped

ACL の設定

ここでは、ACL の作成方法と、ルールの（ACE）の追加方法について説明します。

ACL の作成ワークフロー

ACL を作成してインターフェイスと関連付けるには、次の操作を実行します。

1. 次のタイプの ACL を 1 つ以上作成します。
   a. MAC ベース ACL：[MAC ベース ACL] ページと [MAC ベース ACE] ページを使用して作成
   b. IP ベース ACL：[IPv4 ベース ACL] ページと [IPv4 ベース ACE] ページを使用して作成
   c. IPv6 ベース ACL：[IPv6 ベース ACL] ページと [IPv6 ベース ACE] ページを使用して作成
2. [ACL バインディング(VLAN)] ページと [ACL バインディング(ポート)] ページを使用して、ACL をインターフェイスに関連付けます。

ACL の変更ワークフロー

使用していない ACL のみ、変更できます。ACL を変更するために、ACL をアンバインドする手順を次に示します。

1. ACL が QoS 拡張モード クラス マップには属しておらず、インターフェイスに関連付けられている場合、[ACL バインディング(VLAN)] *または* [ACL バインディング(ポート)] ページを使用してインターフェイスからアンバインドします。
2. ACL がクラス マップの一部になっていて、インターフェイスにバインドされていない場合、その ACL は変更できます。
3. ACL が、インターフェイスにバインドされているポリシーに含まれるクラス マップの一部になっている場合、アンバインドするには次に示す一連の手順を実行する必要があります。
   - [ポリシーバインディング] を使用して、クラス マップを含むポリシーをインターフェイスからアンバインドします。
   - [ポリシーの設定]（**編集**）を使用して、ACL を含むクラス マップをポリシーから削除します。
   - [クラスマッピングの定義] を使用して、ACL を含むクラス マップを削除します。

このようにして初めて、この項で説明しているとおり、ACL を変更できます。

MAC ベース ACL の作成

MAC ベース ACL は、レイヤ 2 フィールドに基づいてトラフィックをフィルタ処理するために使用します。MAC ベース ACL は、一致するかどうかすべてのフレームを検査します。

MAC ベース ACL は [MAC ベース ACL] ページで定義します。ルールは [MAC ベース ACE] ページで定義します。

MAC ベース ACL

MAC ベース ACL を定義するには、次のようにします。

ステップ 1 [アクセスコントロール] > [MAC ベースACL] の順にクリックします。

このページには、現在定義されているすべての MAC ベース ACL のリストが表示されます。

ステップ 2 [追加] をクリックします。

ステップ 3 [ACL名] フィールドに、新しい ACL の名前を入力します。ACL 名では大文字と小文字が区別されます。

ステップ 4 [適用] をクリックします。MAC ベース ACL が実行コンフィギュレーション ファイルに保存されます。

MAC ベース ACE

注 MAC ベースのルールは、それぞれ 1 つの TCAM ルールを使用します。TCAM 割り当てはペアで実行されることにご注意ください。たとえば、最初の ACE には 2 つの TCAM ルールが割り当てられ、2 番目の TCAM ルールの方は次の ACE に割り当てられます。

ルール（ACE）を ACL に追加するには、次のようにします。

ステップ 1 [アクセスコントロール] > [MAC ベース ACE] の順にクリックします。

ステップ 2 ACL を選択し、[実行] をクリックします。ACL に含まれる ACE が一覧表示されます。

ステップ 3 [追加] をクリックします。

ステップ 4 パラメータを入力します。

- [ACL名]:ACE を追加する ACL の名前が表示されます。
- [プライオリティ]:ACE のプライオリティを入力します。プライオリティが高い ACE が最初に処理されます。プライオリティは 1 が最高です。
- [アクション]:一致した場合に実行するアクションを選択します。次のオプションがあります。
  - [許可]:ACE 条件に一致するパケットを転送します。
  - [拒否]:ACE 条件に一致するパケットをドロップします。
  - [シャットダウン]:ACE 条件に一致するパケットをドロップし、パケットを受信したポートを無効にします。このポートは、[エラー回復設定] ページから再アクティブ化できます。
- [ロギング]:選択すると、ACL ルールと一致する ACL フローのロギングが有効になります。
- [時間範囲]:選択すると、ACL の使用時間が指定した時間範囲に制限されます。
- [時間範囲名]:[時間範囲] を選択した場合、使用する時間範囲を選択します。時間範囲は [システム時刻の設定] セクションで定義します。
- [宛先 MAC アドレス]:すべての宛先アドレスを許可する場合は [任意] を選択します。宛先アドレスを入力するか宛先アドレスの範囲を指定する場合は [ユーザ定義] を選択します。
- [宛先 MAC アドレス値]:宛先 MAC アドレスの照合に使用する MAC アドレスを入力します。必要に応じて、マスクも入力します。
- [宛先 MAC ワイルドカード マスク]:MAC アドレスの範囲を定義するためのマスクを入力します。このマスクは、サブネット マスクなどの他のマスクとは異なる点にご注意ください。このマスクでは、**1** に設定したビットの値はマスクせず、**0** に指定したビットの値はマスクします。

  注 0000 0000 0000 0000 0000 0000 1111 1111 というマスクを例に説明します。0 になっているビットの一致は照合され、1 になっているビットの一致は照合されません。1 を 10 進数の整数に変換し、4 つずつの 0 をまとめて 0 として記述する必要があります。この例では、1111 1111 = 255 で、マスクは 0.0.0.255 と記述されます。
- [送信元MACアドレス]:すべての送信元アドレスを許可する場合は [任意] を選択します。送信元アドレスを入力するか送信元アドレスの範囲を指定する場合は [ユーザ定義] を選択します。

- [送信元MACアドレス値]:送信元 MAC アドレスの照合に使用する MAC アドレスを入力します。必要に応じて、マスクも入力します。
- [送信元MACワイルドカードマスク]:MAC アドレスの範囲を定義するためのマスクを入力します。
- [VLAN ID]:照合する VLAN タグの VLAN ID セクションを入力します。
- [802.1p]:802.1p を使用する場合は [含める] を選択します。
- [802.1p値]:VPT タグに追加する 802.1p 値を入力します。
- [802.1p マスク]:VPT タグに適用するワイルドカード マスクを入力します。
- [イーサタイプ]:照合するフレームのイーサタイプを入力します。

ステップ 5 [適用] をクリックします。MAC ベース ACE が実行コンフィギュレーション ファイルに保存されます。

IPv4 ベース ACL の作成

IPv4 ベース ACL は、IPv4 パケットを検査する際に使用します。ARP などその他の種類のフレームは検査されません。

照合できるフィールドは次のとおりです。

- IP プロトコル(既知のプロトコルの場合は名前で照合可。または値で直接照合)
- TCP/UDP トラフィックの送信元ポート/宛先ポート
- TCP フレームのフラグの値
- ICMP および IGMP のタイプとコード
- 送信元 IP アドレスおよび宛先 IP アドレス(ワイルドカードを含む)
- DSCP/IP 優先度値

注 ACL は、フローごとに QoS 処理を実行する際のフロー定義の構成要素としても使用されます。

[IPv4 ベース ACL] ページから、システムに ACL を追加できます。ルールは [IPv4 ベース ACE] ページで定義します。

IPv6 ACL は [IPv6ベースACL] ページで定義します。

IPv4 ベース ACL

IPv4 ベース ACL を定義するには、次のようにします。

ステップ 1 [アクセス コントロール] > [IPv4 ベース ACL] の順にクリックします。

このページには、現在定義されている IPv4 ベース ACL がすべて表示されます。

ステップ 2 [追加] をクリックします。

ステップ 3 [ACL名] フィールドに、新しい ACL の名前を入力します。名前は大文字と小文字が区別されます。

ステップ 4 [適用] をクリックします。IPv4 ベース ACL が実行コンフィギュレーション ファイルに保存されます。

IPv4 ベース ACE

注 IPv4 ベースのルールは、それぞれ 1 つの TCAM ルールを使用します。TCAM 割り当てはペアで実行されることにご注意ください。たとえば、最初の ACE には 2 つの TCAM ルールが割り当てられ、2 番目の TCAM ルールの方は次の ACE に割り当てられます。

ルール（ACE）を IPv4 ベース ACL に追加するには、次のようにします。

ステップ 1 [アクセスコントロール] > [IPv4ベースACE] の順にクリックします。

ステップ 2 ACL を選択し、[実行] をクリックします。選択した ACL に対して現在定義されている IP ACE が表示されます。

ステップ 3 [追加] をクリックします。

ステップ 4 パラメータを入力します。

- [ACL名]：ACL の名前が表示されます。
- [プライオリティ]：プライオリティを入力します。プライオリティが高い ACE が最初に処理されます。
- [アクション]：ACE と一致するパケットに割り当てるアクションを選択します。選択項目は次のとおりです。
  - [許可]：ACE 条件に一致するパケットを転送します。
  - [拒否]：ACE 条件に一致するパケットをドロップします。

- [シャットダウン]:ACE 条件に一致するパケットをドロップし、パケットの宛先ポートを無効にします。ポートは [エラー回復設定] ページで再アクティブ化できます。

- [ロギング]:選択すると、ACL ルールと一致する ACL フローのロギングが有効になります。
- [時間範囲]:選択すると、ACL の使用時間が指定した時間範囲に制限されます。
- [時間範囲名]:[時間範囲] を選択した場合、使用する時間範囲を選択します。時間範囲は [システム時刻の設定] セクションで定義します。
- [プロトコル]:選択すると、特定のプロトコルまたはプロトコル ID に基づく ACE が作成されます。すべての IP プロトコルを受け入れるには、[任意(IPv4)] を選択します。それ以外の場合は、次のプロトコルのうちの 1 つを、[リストから選択] ドロップダウンリストから選択します。
  - [ICMP]:インターネット制御メッセージ プロトコル
  - [IGMP]:インターネット グループ管理プロトコル
  - [IP-in-IP]:IP-in-IP カプセル化
  - [TCP]:伝送制御プロトコル
  - [EGP]:外部ゲートウェイ プロトコル
  - [IGP]:内部ゲートウェイ プロトコル
  - [UDP]:ユーザ データグラム プロトコル
  - [HMP]:ホスト マッピング プロトコル
  - [RDP]:信頼性の高いデータグラム プロトコル。
  - [IDPR]:ドメイン間ポリシー ルーティング プロトコル
  - [IPV6]:IPv6 over IPv4 トンネリング
  - [IPV6:ROUT]:ゲートウェイ経由で IPv6 over IPv4 ルートに属するパケットを照合
  - [IPV6:FRAG]:IPv6 over IPv4 フラグメント ヘッダーに属するパケットを照合
  - [IDRP]:ドメイン間ルーティング プロトコル
  - [RSVP]:ReSerVation プロトコル
  - [AH]:認証ヘッダー

- [IPV6:ICMP]:インターネット制御メッセージ プロトコル
- [EIGRP]:Enhanced Interior Gateway Routing Protocol
- [OSPF]:Open Shortest Path First
- [IPIP]:IP-in-IP
- [PIM]:Protocol Independent Multicast
- [L2TP]:Layer 2 Tunneling Protocol
- [ISIS]:IGP 固有のプロトコル
- [照合するプロトコルID]:名前を選択するのではなく、プロトコル ID を入力します。

- [送信元 IP アドレス]:すべての送信元アドレスを許可する場合は [任意] を選択します。送信元アドレスを入力するか送信元アドレスの範囲を指定する場合は [ユーザ定義] を選択します。
- [送信元 IP アドレス値]:送信元 IP アドレスの照合に使用する IP アドレスを入力します。
- [送信元 IP ワイルドカード マスク]:IP アドレスの範囲を定義するためのマスクを入力します。このマスクは、サブネット マスクなどの他のマスクとは異なる点にご注意ください。このマスクでは、1 に設定したビットの値はマスクせず、0 に指定したビットの値はマスクします。

  注 0000 0000 0000 0000 0000 0000 1111 1111 というマスクを例に説明します。0 になっているビットの一致は照合され、1 になっているビットの一致は照合されません。1 を 10 進数の整数に変換し、4 つずつの 0 をまとめて 0 として記述する必要があります。この例では、1111 1111 = 255 で、マスクは 0.0.0.255 と記述されます。
- [宛先 IP アドレス]:すべての宛先アドレスを許可する場合は [任意] を選択します。宛先アドレスを入力するか宛先アドレスの範囲を指定する場合は [ユーザ定義] を選択します。
- [宛先 IP アドレス値]:宛先 IP アドレスの照合に使用する IP アドレスを入力します。
- [宛先IPワイルドカードマスク]:IP アドレスの範囲を定義するためのマスクを入力します。
- [送信元ポート]:次のいずれかを選択します。
  - [任意]:すべての送信元ポートに対して照合を実行します。

- [リストから1つ]:パケットを照合する TCP/UDP 送信元ポートを 1 つ選択します。このフィールドは、[リストから選択] ドロップダウン メニューで [800/6-TCP] または [800/17-UDP] が選択されている場合にのみアクティブになります。
- [番号で1つ]:パケットを照合する TCP/UDP 送信元ポートを 1 つ入力します。このフィールドは、[リストから選択] ドロップダウン メニューで [800/6-TCP] または [800/17-UDP] が選択されている場合にのみアクティブになります。
- [範囲]:パケットを照合する TCP/UDP 送信元ポートの範囲を選択します。設定可能なポート範囲は 8 種類あり、送信元ポートと宛先ポートで共有されています。TCP プロトコルと UDP プロトコルには、それぞれ 8 種類のポート範囲が設定されています。

- [宛先ポート]:使用可能な値のいずれかを選択します。値は、上述の [送信元ポート] フィールドと同じです。

  注 ACE の IP プロトコルを指定してからでなければ、送信元ポートや宛先ポートを入力できません。

- [TCP フラグ]:パケットのフィルタ処理に使用する TCP フラグを 1 つ以上選択します。フィルタ処理されたパケットは、転送されるかドロップされます。TCP フラグを使用してパケットをフィルタ処理すると、パケットをきめ細かく制御できるので、ネットワーク セキュリティが向上します。
- [タイプ オブ サービス]:IP パケットのサービス タイプ。
  - [任意]:任意のサービス タイプ。
  - [照合する DSCP]:照合する Differentiated Service Code Point(DSCP)
  - [照合する IP 優先度]:IP 優先度とは、適切な QoS を確実に提供するためにネットワークが使用する TOS(タイプ オブ サービス)のモデルです。このモデルでは、RFC 791 および RFC 1349 で説明されているとおり、IP ヘッダー内のサービス タイプ バイトで最も上位の 3 ビットを使用します。
- [ICMP]:ACL の IP プロトコルが ICMP である場合、フィルタリングに使用する ICMP メッセージ タイプを選択します。メッセージ タイプ名を選択するか、メッセージ タイプ番号を入力します。
  - [任意]:すべてのメッセージ タイプを受け入れます。
  - [リストから選択]:メッセージ タイプ名を選択します。
  - [照合するICMPタイプ]:フィルタリングに使用するメッセージ タイプ番号。

- [ICMPコード]:ICMP メッセージには、そのメッセージの処理方法を示すコード フィールドが設定されている場合があります。次のいずれかのオプションを選択して、このコードに基づいてフィルタリングするかどうかを設定します。
  - [任意]:すべてのコードを受け入れます。
  - [ユーザ定義]:フィルタリングに使用する ICMP コードを入力します。
- [IGMP]:ACL が IGMP に基づいている場合は、フィルタリングに使用する IGMP メッセージ タイプを選択します。メッセージ タイプ名を選択するか、メッセージ タイプ番号を入力します。
  - [任意]:すべてのメッセージ タイプを受け入れます。
  - [リストから選択]: メッセージ タイプ名を選択します。
  - [照合するIGMPタイプ]:フィルタリングに使用するメッセージ タイプ番号。

ステップ 5 [適用] をクリックします。IPv4 ベース ACE が実行コンフィギュレーション ファイルに保存されます。

IPv6 ベース ACL の作成

[IPv6 ベース ACL] ページでは、純粋な IPv6 ベース トラフィックを検査する IPv6 ACL を表示および作成できます。IPv6 ACL では、IPv6 over IPv4 パケットや ARP パケットは検査しません。

注 ACL は、フローごとに QoS 処理を実行する際のフロー定義の構成要素としても使用されます。

IPv6 ベース ACL

IPv6 ベース ACL を定義するには、次のようにします。

ステップ 1 [アクセス コントロール] > [IPv6 ベース ACL] の順にクリックします。

このウィンドウには、定義されている ACL とそのコンテンツのリストが表示されます。

ステップ 2 [追加] をクリックします。

ステップ 3 [ACL名] フィールドに、新しい ACL の名前を入力します。名前は大文字と小文字が区別されます。

ステップ 4 [適用] をクリックします。IPv6 ベース ACL が実行コンフィギュレーション ファイルに保存されます。

IPv6 ベース ACE

注 IPv6 ベースのルールは、それぞれ 2 つの TCAM ルールを使用します。

ステップ 1 [アクセス コントロール] > [IPv6 ベース ACE] の順にクリックします。

このウィンドウには、指定した ACL（ルールのグループ）に対する ACE（ルール）が表示されます。

ステップ 2 ACL を選択し、[実行] をクリックします。選択した ACL に対して現在定義されている IP ACE が表示されます。

ステップ 3 [追加] をクリックします。

ステップ 4 パラメータを入力します。

- [ACL名]：ACE を追加する ACL の名前が表示されます。
- [プライオリティ]：プライオリティを入力します。プライオリティが高い ACE が最初に処理されます。
- [アクション]：ACE と一致するパケットに割り当てるアクションを選択します。選択項目は次のとおりです。
  - [許可]：ACE 条件に一致するパケットを転送します。
  - [拒否]：ACE 条件に一致するパケットをドロップします。
  - [シャットダウン]：ACE 条件に一致するパケットをドロップし、パケットの宛先ポートを無効にします。ポートは [エラー回復設定] ページで再アクティブ化できます。
- [ロギング]：選択すると、ACL ルールと一致する ACL フローのロギングが有効になります。
- [時間範囲]：選択すると、ACL の使用時間が指定した時間範囲に制限されます。
- [時間範囲名]：[時間範囲] を選択した場合、使用する時間範囲を選択します。時間範囲については、「システムの時刻」の項で説明します。

- [プロトコル]:選択すると、特定のプロトコルに基づく ACE が作成されます。すべての IP プロトコルを受け入れるには、[任意(IPv6)] を選択します。

  それ以外の場合は、次のいずれかのプロトコルを選択します。

  - [TCP]:伝送制御プロトコル。2 台のホスト間で通信とデータ ストリームの交換を行うことができます。TCP を使用すると、確実にパケットが送達されるだけでなく、送信された順序どおりにパケットが伝送および受信されます。
  - [UDP]:ユーザ データグラム プロトコル。パケットを送信しますが、送達は保証されません。
  - [ICMP]:パケットをインターネット制御メッセージ プロトコル(ICMP)と照合します。

  または

  - [照合するプロトコル ID]:照合するプロトコルの ID を入力します。
- [送信元 IP アドレス]:すべての送信元アドレスを許可する場合は [任意] を選択します。送信元アドレスを入力するか送信元アドレスの範囲を指定する場合は [ユーザ定義] を選択します。
- [送信元 IP アドレス値]:送信元 IP アドレスの照合に使用する IP アドレスを入力します。必要に応じて、マスクも入力します。
- [送信元 IP プレフィックス長]:送信元 IP アドレスのプレフィックス長を入力します。
- [宛先 IP アドレス]:すべての宛先アドレスを許可する場合は [任意] を選択します。宛先アドレスを入力するか宛先アドレスの範囲を指定する場合は [ユーザ定義] を選択します。
- [宛先 IP アドレス値]:宛先 IP アドレスの照合に使用する IP アドレスを入力します。必要に応じて、マスクも入力します。
- [宛先 IP プレフィックス長]:IP アドレスのプレフィックス長を入力します。
- [送信元ポート]:次のいずれかを選択します。
  - [任意]:すべての送信元ポートに対して照合を実行します。
  - [リストから選択]:パケットを照合する TCP/UDP 送信元ポートを 1 つ選択します。このフィールドは、[IP プロトコル] ドロップダウン メニューで [800/6-TCP] または [800/17-UDP] が選択されている場合にのみアクティブになります。

- [番号]:パケットを照合する TCP/UDP 送信元ポートを 1 つ入力します。このフィールドは、[IP プロトコル] ドロップダウン メニューで [800/6-TCP] または [800/17-UDP] が選択されている場合にのみアクティブになります。

- [宛先ポート]:使用可能な値のいずれかを選択します。値は、上述の [送信元ポート] フィールドと同じです。

  注 ACL の IPv6 プロトコルを指定してからでなければ、送信元ポートや宛先ポートを設定できません。

- [フロー ラベル]:IPv6 フロー ラベル フィールドに基づいて IPv6 トラフィックを分類します。これは IPv6 パケット ヘッダーに含まれる 20 ビットのフィールドです。送信元ステーションでは IPv6 フロー ラベルを使用して、同じフローに属する複数のパケットにラベルを付けることができます。すべてのフロー ラベルを受け入れ可能な場合は [任意] を選択します。または [ユーザ定義] を選択して、ACL で受け入れる特定のフロー ラベルを入力します。

- [TCP フラグ]:パケットのフィルタ処理に使用する TCP フラグを 1 つ以上選択します。フィルタ処理されたパケットは、転送されるかドロップされます。TCP フラグを使用してパケットをフィルタ処理すると、パケットをきめ細かく制御できるので、ネットワーク セキュリティが向上します。フラグのタイプごとに、次のオプションのいずれかを選択します。

  - [設定]:フラグが SET の場合に照合します。
  - [設定解除]:フラグが Not SET の場合に照合します。
  - [設定しない]:TCP フラグを無視します。

- [タイプ オブ サービス]:IP パケットのサービス タイプ。

  - [任意]:任意のサービス タイプ。
  - [照合する DSCP]:照合する Differentiated Service Code Point(DSCP)
  - [照合する IP 優先度]:IP 優先度とは、適切な QoS を確実に提供するためにネットワークが使用する TOS(タイプ オブ サービス)のモデルです。このモデルでは、RFC 791 および RFC 1349 で説明されているとおり、IP ヘッダー内のサービス タイプ バイトで最も上位の 3 ビットを使用します。

- [ICMP]:ACL が ICMP に基づいている場合は、フィルタリングに使用する ICMP メッセージ タイプを選択します。メッセージ タイプ名を選択するか、メッセージ タイプ番号を入力します。すべてのメッセージ タイプを受け入れる場合は、[任意] を選択します。

  - [任意]:すべてのメッセージ タイプを受け入れます。

- [リストから選択]:ドロップダウン リストからメッセージ タイプ名を選択します。
- [照合するICMPタイプ]:フィルタリングに使用するメッセージ タイプ番号。

• [ICMPコード]:ICMP メッセージには、そのメッセージの処理方法を示すコード フィールドが設定されている場合があります。次のいずれかのオプションを選択して、このコードに基づいてフィルタリングするかどうかを設定します。

- [任意]:すべてのコードを受け入れます。
- [ユーザ定義]:フィルタリングに使用する ICMP コードを入力します。

ステップ 5 [適用] をクリックします。

ACL バインディング

ACL をインターフェイス(ポート、LAG、または VLAN)にバインドすると、その ACE ルールが、このインターフェイスに届いたパケットに適用されます。ACL 内のどの ACE にも一致しないパケットはデフォルトのルールと照合され、このルールにも一致しないパケットはドロップされます。

1 つのインターフェイスにバインドできる ACL は 1 つのみですが、インターフェイスをポリシー マップにまとめ、そのポリシー マップをインターフェイスにバインドすることで、複数のインターフェイスを同じ ACL にバインドできます。

インターフェイスにバインドした ACL は、バインド先または使用中のポートすべてから削除しない限り、編集、変更、削除できません。

注 インターフェイス(ポート、LAG、または VLAN)は、ポリシーや ACL にバインドできますが、ポリシーと ACL の両方に同時にバインドすることはできません。

注 同一のクラス マップでは、宛先 IPv6 アドレスがフィルタリング条件として設定されている IPv6 ACE と同時に MAC ACL を使用することはできません。

ACL バインディング(VLAN)

ACL を VLAN にバインドするには、次のようにします。

ステップ 1 [アクセスコントロール] > [ACL バインディング(VLAN)] の順にクリックします。

ステップ 2 VLAN を選択して、[編集] をクリックします。

必要な VLAN が表示されない場合は、新規に追加します。

ステップ 3 次のいずれかを選択します。

- [MAC ベースACL]: インターフェイスにバインドする MAC ベース ACL を選択します。
- [IPv4 ベース ACL]: インターフェイスにバインドする IPv4 ベース ACL を選択します。
- [IPv6 ベース ACL]: インターフェイスにバインドする IPv6 ベース ACL を選択します。
- [デフォルト アクション]: 次のいずれかのオプションを選択します。
  - [いずれも拒否]: ACL に一致しないパケットは拒否(ドロップ)されます。
  - [いずれも許可]: ACL に一致しないパケットは許可(転送)されます。

  注 [デフォルトアクション] は、IP ソース ガードがそのインターフェイス上でアクティブでない場合にのみ定義できます。

ステップ 4 [適用] をクリックします。ACL バインディングが変更され、実行コンフィギュレーション ファイルが更新されます。

注 ACL が選択されていない場合は、VLAN にバインド済みの ACL がバインド解除されます。

ACL バインディング(ポート)

ACL をポートまたは LAG にバインドするには、次のようにします。

ステップ 1 [アクセスコントロール] > [ACL バインディング(ポート)] の順にクリックします。

ステップ 2 インターフェイス タイプとして [ポート] または [LAG] を選択します。

ステップ 3 [実行] をクリックします。選択したインターフェイスの各タイプについて、そのタイプのインターフェイスすべてと、それらの現在の ACL のリスト([入力 ACL] と [出力 ACL])が表示されます。

- [インターフェイス]:ACL が定義されているインターフェイスの ID。
- [MAC ACL]:インターフェイスにバインドされている MAC タイプの ACL(存在する場合)。
- [IPv4 ACL]:インターフェイスにバインドされている IPv4 タイプの ACL(存在する場合)。
- [IPv6 ACL]:インターフェイスにバインドされている IPv6 タイプの ACL(存在する場合)。
- [デフォルトアクション]:ACL のルールのアクション([いずれもドロップ] または [いずれも許可])。

  注 1 つのインターフェイスからすべての ACL をアンバインドするには、そのインターフェイスを選択し、[クリア] をクリックします。

ステップ 4 インターフェイスを選択し、[編集] をクリックします。

ステップ 5 入力 ACL と出力 ACL に関する以下の内容を入力します。

[入力 ACL]

- [MAC ベース ACL]:インターフェイスにバインドする MAC ベース ACL を選択します。
- [IPv4 ベース ACL]:インターフェイスにバインドする IPv4 ベース ACL を選択します。
- [IPv6 ベース ACL]:インターフェイスにバインドする IPv6 ベース ACL を選択します。
- [デフォルト アクション]:次のいずれかのオプションを選択します。
  - [いずれも拒否]:ACL に一致しないパケットは拒否(ドロップ)されます。
  - [いずれも許可]:ACL に一致しないパケットは許可(転送)されます。

注 [デフォルトアクション] は、IP ソース ガードがそのインターフェイス上でアクティブでない場合にのみ定義できます。

[出力 ACL]

- [MAC ベース ACL]: インターフェイスにバインドする MAC ベース ACL を選択します。
- [IPv4 ベース ACL]: インターフェイスにバインドする IPv4 ベース ACL を選択します。
- [IPv6 ベース ACL]: インターフェイスにバインドする IPv6 ベース ACL を選択します。
- [デフォルト アクション]: 次のいずれかのオプションを選択します。
  - [いずれも拒否]: ACL に一致しないパケットは拒否(ドロップ)されます。
  - [いずれも許可]: ACL に一致しないパケットは許可(転送)されます。

  注 [デフォルトアクション] は、IP ソース ガードがそのインターフェイス上でアクティブでない場合にのみ定義できます。

ステップ 6 [適用] をクリックします。ACL バインディングが変更され、実行コンフィギュレーション ファイルが更新されます。

注 ACL が選択されていない場合は、インターフェイスにバインド済みの ACL がバインド解除されます。

23

サービス品質

サービス品質（QoS）機能をネットワーク全体に適用した場合、基準に従ってネットワーク トラフィックにプライオリティが設定され、重要なトラフィックが優先的に処理されます。

ここで説明する内容は次のとおりです。

QoS の機能とコンポーネント

QoS 機能は、ネットワークのパフォーマンスを最適化する目的で使用されます。

QoS を使用すると、次のことが可能です。

- 次の属性に基づいて着信パケットをトラフィック クラスに分類する。
  - デバイス コンフィギュレーション
  - 入力インターフェイス
  - パケット内容
  - これらの属性の組み合わせ

QoS には、以下のことが含まれます。

- **トラフィック分類**:着信パケットのそれぞれを、パケットの内容やポートに基づいて、特定のトラフィック フローに属するものとして分類します。分類は ACL(アクセス コントロール リスト)によって行われ、ACL の条件を満たすトラフィックだけが CoS または QoS 分類の対象になります。
- **ソフトウェア キューへの割り当て**:着信パケットが転送キューに割り当てられます。パケットは特定のキューに送信され、そのパケットが所属するトラフィック クラスの機能として処理されます。「キュー」を参照してください。
- **その他のトラフィック クラス処理属性**:QoS 機構が各種のクラス(帯域幅管理など)に適用されます。

QoS 動作

信頼されるヘッダー フィールドのタイプは [グローバル設定] ページで入力します。また、[CoS/802.1p 値のキューへのマッピング] ページ(信頼モードが CoS/802.1p の場合)または [DSCP 値のキューへのマッピング] ページ(信頼モードが DSCP の場合)で、そのフィールドの値ごとに、フレームが送信される出力キューが割り当てられます。

QoS モード

選択されている QoS モードは、システム内のすべてのインターフェイスに適用されます。

- **基本モード**：サービス クラス（CoS）。

  同じクラスのトラフィックはすべて、同じように処理されます。具体的には、着信フレーム内で示されている QoS 値に基づいて、出力ポート上の出力キューを決定するという 1 つの QoS アクションが実行されます。この QoS 値は、レイヤ 2 においては VLAN Priority Tag（VPT）802.1p 値、
  レイヤ 3 においては、IPv4 の場合は Differentiated Service Code Point（DSCP）値、IPv6 の場合はトラフィック クラス（TC）値です。デバイスが基本モードで動作している場合、外部デバイス上で割り当てられたこの QoS 値が信頼されます。この QoS 値によって、このパケットのトラフィック クラスと QoS が決定されます。

  信頼されるヘッダー フィールドは、[グローバル設定] ページで入力します。また、[CoS/802.1p 値のキューへのマッピング] ページ（信頼モードが CoS/802.1p の場合）または [DSCP 値のキューへのマッピング] ページ（信頼モードが DSCP の場合）で、そのフィールドの値ごとに、フレームが送信される出力キューが割り当てられます。

- **拡張モード**：フローごとのサービス品質（QoS）。

  拡張モードの場合、フローごとの QoS は、クラス マップやポリサーで構成されます。

  - クラス マップは、フローのトラフィックの種類を定義し、1 つ以上の ACL が含まれています。ACL に合致するパケットは、フローに属します。
  - ポリサーは、設定されている QoS をフローに適用します。フローの QoS 設定に含められるのは、出力キュー、DSCP または CoS/802.1p 値、およびプロファイル外の（超過）トラフィックに対するアクションです。

- **無効モード**：このモードでは、すべてのトラフィックが単一のベスト エフォート キューにマッピングされまるため、特に優先されるトラフィックのタイプはありません。

アクティブになるのは、一度に 1 つのモードのみです。システムが QoS 拡張モードで動作するように設定されているときには、QoS 基本モードの設定値はアクティブになりません。その逆も同じです。

モードが変更されると、以下のことが発生します。

- QoS 拡張モードからその他のモードに変更される場合、ポリシー プロファイル定義とクラス マップが削除されます。インターフェイスに直接適用されている ACL は、適用された状態のままになります。
- QoS 基本モードから拡張モードに変更される場合、基本モードでの QoS 信頼モードの設定は保持されません。
- QoS が無効にされた場合、シェーパーとキューの設定（WRR/SP 帯域幅の設定）はデフォルト値にリセットされます。

その他のすべてのユーザ設定は、そのまま維持されます。

QoS を設定する手順

QoS の一般パラメータを設定するには、次のようにします。

ステップ 1 [QoS プロパティ] ページで、システムの QoS モード（基本、拡張、または無効。詳しくは、QoS モードを参照）を選択します。以下の手順では、QoS を有効にしてあることを前提としています。

ステップ 2 [QoS プロパティ] ページで、各インターフェイスにデフォルトの CoS プライオリティを割り当てます。

ステップ 3 [キュー] ページで、各出力キューに対してスケジュール方式（完全優先または WRR）と WRR 帯域割り当て率を設定します。

ステップ 4 [DSCP 値のキューへのマッピング] ページで、各 IP DSCP/TC 値に出力キューを割り当てます。デバイスが DSCP 信頼モードで動作している場合、着信パケットはその DSCP/TC 値に基づいて出力キューに格納されます。

ステップ 5 各 CoS/802.1p プライオリティに出力キューを割り当てます。デバイスが CoS/802.1 信頼モードで動作している場合、すべての着信パケットは、その CoS/802.1p プライオリティに基づいて出力キューに格納されます。この作業は [CoS/802.1p 値のキューへのマッピング] ページで行います。

ステップ 6 レイヤ 3 トラフィックで必要とされる場合のみ、[DSCP 値のキューへのマッピング] ページで、各 DSCP/TC 値にキューを割り当てます。

ステップ 7 以下のページで、帯域幅とレート制限を設定します。

a. [キューあたりの出力シェーピング] ページで、各キューに対する出力シェーピングを設定します。

b. [帯域幅] ページで、各ポートに対する入力レート制限と出力シェーピング レートを設定します。

ステップ 8 以下のうちのいずれか 1 つを実行することにより、選択したモードを設定します。

a. *基本 QoS モードの設定手順*に記載されているように基本モードを設定します。

b. *拡張 QoS モードの設定手順*に記載されているように拡張モードを設定します。

QoS を設定する手順

QoS の一般パラメータを設定するには、次のようにします。

ステップ 1 [QoS プロパティ] ページで信頼モードを選択し、QoS を有効にします。次に、[インターフェイス設定] ページで、ポートに対する QoS を有効にします。

ステップ 2 [QoS プロパティ] ページで、各インターフェイスにデフォルトの CoS または DSCP プライオリティを割り当てます。

ステップ 3 [キュー] ページで、各出力キューに対してスケジュール方式（完全優先または WRR）と WRR 帯域割り当て率を設定します。

ステップ 4 [DSCP 値のキューへのマッピング] ページで、各 IP DSCP/TC 値に出力キューを割り当てます。デバイスが DSCP 信頼モードで動作している場合、着信パケットはその DSCP/TC 値に基づいて出力キューに格納されます。

ステップ 5 各 CoS/802.1p プライオリティに出力キューを割り当てます。デバイスが CoS/802.1 信頼モードで動作している場合、すべての着信パケットは、その CoS/802.1p プライオリティに基づいて出力キューに格納されます。この作業は [CoS/802.1p 値のキューへのマッピング] ページで行います。

ステップ 6 以下のページで、帯域幅とレート制限を設定します。

a. [キューあたりの出力シェーピング] ページで、各キューに対する出力シェーピングを設定します。

b. [帯域幅] ページで、各ポートに対する入力レート制限と出力シェーピング レートを設定します。

全般

ここで説明する内容は次のとおりです。

- QoS プロパティ
- キュー
- CoS/802.1p 値のキューへのマッピング
- DSCP 値のキューへのマッピング
- 帯域幅
- キューあたりの出力シェーピング
- VLAN 入力レート制限
- TCP 輻輳回避

QoS プロパティ

[QoS プロパティ] ページには、システムの QoS モード（基本、拡張、または無効：詳しくは、QoS モードの項を参照）を設定するためのいくつかのフィールドが含まれています。

QoS を有効にして、QoS モードを選択するには、次のようにします。

ステップ 1 [サービス品質] > [全般] > [QoS プロパティ] をクリックします。

ステップ 2 QoS モードを設定します。次のオプションが選択できます。

- [無効]：デバイス上で QoS は無効になります。
- [基本]：デバイス上で QoS は基本モードで有効になります。
- [拡張]：デバイス上で QoS は拡張モードで有効になります。

ステップ 3 デバイス上のすべてのポートとその CoS 情報を表示または修正するには、[ポート] を選択します。すべての LAG とその CoS 情報を表示または修正するには、[LAG] を選択します。その後、[実行] をクリックします。

すべてのポートまたは LAG に対して次のフィールドが表示されます。

- [インターフェイス]: インターフェイスのタイプ。
- [デフォルト CoS]: VLAN タグが設定されていない着信パケットに対するデフォルトの VPT 値。デフォルト CoS のデフォルト値は 0 です。デフォルトが関係するのは、タグなしフレームの場合のみ、かつ、システムが基本モードであり [グローバル設定] ページで [CoSを信頼] が選択されている場合のみです。

ステップ 4 [適用] をクリックします。実行コンフィギュレーション ファイルが更新されます。

インターフェイスの QoS を設定するには、インターフェイスを選択し、[編集] をクリックします。

ステップ 1 パラメータを入力します。

- [インターフェイス]: ポートまたは LAG を選択します。
- [デフォルトCoS]: VLAN タグが設定されていない着信パケットに割り当てる、デフォルト CoS（サービス クラス）値を選択します。

ステップ 2 [適用] をクリックします。このインターフェイスのデフォルト CoS 値が実行コンフィギュレーション ファイルに保存されます。

デフォルトの CoS 値を復元するには、[CoS デフォルトの復元] をクリックします。

キュー

デバイスでは、インターフェイスごとに 8 つのキューがサポートされます。キュー番号 8 は、最もプライオリティの高いキューです。キュー番号 1 は、最もプライオリティの低いキューです。

キュー内のトラフィックを処理する方式には、SP と WRR の 2 とおりがあります。

- [完全優先]: プライオリティが最も高いキュー内の出力トラフィックが最初に送出されます。それより低いキュー内のトラフィックは、プライオリティが最高のキューが空になった後に送出されます。つまり、プライオリティが最高のトラフィックは最大番号のキューに格納されます。

- [WRR]:WRR モードでは、キューから送出されるパケット数は、キューのウェイトに比例します。つまり、キューのウェイトが大きいほど、送出されるフレームの数が多くなります。たとえば、許容最大数の 4 個のキューがあり、4 個のキューすべてが WRR モードに設定されていて、デフォルトのウェイト設定が使用されている場合、すべてのキューが飽和状態になっていて輻輳が発生していると仮定すると、キュー 1 では帯域幅の 1/15、キュー 2 では 2/15、キュー 3 では 4/15、キュー 4 では 8/15 がそれぞれ使用されます。このデバイスで使用される WRR アルゴリズムの種類は、一般的な Deficit WRR（DWRR）ではなく Shaped Deficit WRR（SDWRR）です。

キューイング モードを選択するには、[キュー] ページを使用します。キューイング モードが SP の場合、プライオリティによって各キューの処理順序が決まります。まず、プライオリ ティが最高のキューから開始し、各キューが完了すると、プライオリティが次に高いキューに移ります。

キューイング モードが WRR の場合は、まず、キューからパケットが送出されます。そのキューに割り当てられた帯域幅がすべて使用されると、続いて、別のキュー内のパケットの送出が開始します。

プライオリティの低いキューを WRR モードに設定し、プライオリティの高いキューを SP モードに設定することもできます。この場合、SP モードのキュー内のトラフィックは常に、WRR モードのキュー内のトラフィックよりも先に送出されます。SP モードのキューが空になると、WRR モードのキュー内のトラフィックの送出が開始します。WRR モードの各キューに対する相対的なパケット送出割合は、各キューに割り当てられているウェイトによって決まります。

優先順位方式を選択し、WRR データを入力するには、次のようにします。

ステップ 1 [サービス品質] > [全般] > [キュー] をクリックします。

ステップ 2 パラメータを入力します。

- [キュー]:キュー番号が表示されます。
- [スケジューリング方式]:次のオプションのいずれかを選択します。
  - [完全優先]:選択したキューおよびそれよりプライオリティの高いすべてのキューのトラフィック スケジューリングは、厳密にそのキューのプライオリティに基づきます。
  - [WRR]:選択したキューのトラフィック スケジューリングは、WRR に基づきます。送出時間は、空でない WRR モードのキュー間で配分されます。つまり、それらのキューには出力記述子が設定されています。この配分が発生するのは、SP モードのキューが空になっている場合のみです。
  - [WRRウェイト]:WRR を選択した場合、このキューに割り当てる WRR ウェイトを入力します。

- [WRR帯域幅の %]: このキューに割り当てられている帯域幅の割合が表示されます。この値は、WRR ウェイトをパーセント値で表したものです。

ステップ 3 [適用] をクリックします。キューが設定され、実行コンフィギュレーション ファイルが更新されます。

CoS/802.1p 値のキューへのマッピング

[CoS/802.1p値のキューへのマッピング] ページでは、802.1p 値(プライオリティ)を出力キューにマッピングできます。[CoS/802.1p 値のキューへのマッピング テーブル] では、着信パケットの格納先となる出力キューが、そのパケットの VLAN タグ内の 802.1p 値に基づいて決定されます。タグが設定されていない着信パケットの場合、802.1p プライオリティが、入力ポートに割り当てられているデフォルトの CoS/802.1p プライオリティとなります。

キューが 8 個の場合のデフォルトのマッピングを、以下の表に示します。

CoS/802.1p 値とキューのマッピング([CoS/802.1p 値のキューへのマッピング])、キューのスケジュール方式と帯域割り当て([キュー] ページ)を調整することにより、ネットワークでのサービス品質目標を達成できます。

CoS/802.1p 値からキューへのマッピングは、以下のいずれかが存在する場合にのみ適用されます。

- デバイスが QoS 基本モードかつ CoS/802.1p 信頼モードである場合。
- デバイスが QoS 拡張モードであり、CoS/802.1p が信頼されているフローにパケットが属する場合

キュー 1 には最低のプライオリティが、350 および 550 ファミリのキュー 8 には最高のプライオリティが割り当てられます。

CoS 値を出力キューにマッピングするには、次のようにします。

ステップ 1 [サービス品質] > [全般] > [CoS/802.1p 値のキューへのマッピング] をクリックします。

ステップ 2 パラメータを入力します。

- [802.1p]: 出力キューに割り当てる 802.1p プライオリティ タグ値が表示されます。プライオリティは 0 が最低、7 が最高です。
- [出力キュー]: 802.1p プライオリティをマッピングする出力キューを選択します。サポートされる出力キュー数は、4 個または 8 個のいずれかです。キュー 4 またはキュー 8 がプライオリティの最も高い出力キューで、キュー 1 のプライオリティが最低です。

ステップ 3 それぞれの 802.1p プライオリティをマッピングする出力キューを選択します。

ステップ 4 [適用]、[キャンセル]、または [デフォルトの復元] をクリックします。801.1p プライオリティ値のキューへのマッピングがなされて実行コンフィギュレーション ファイルが更新されるか、入力された変更がキャンセルされるか、または以前に定義された値が復元されます。

DSCP 値のキューへのマッピング

[DSCP値のキューへのマッピング] ページでは、DSCP 値を出力キューにマッピングできます。[DSCP 値のキューへのマッピング テーブル] は、着信パケットの格納先となる出力キューが、そのパケットの DSCP 値に基づいて決定されます。着信パケットの VPT 値は変更されません。

DSCP 値とキューのマッピング、キューイング モード、および帯域割り当てを調整することにより、ネットワーク上でサービス品質目標を達成できます。

次の場合、DSCP 値とキューのマッピングを IP パケットに適用できます。

- デバイスが QoS 基本モードであり、かつ DSCP が信頼モードである場合。または、
- デバイスが QoS 拡張モードであり、パケットが DSCP 信頼であるフローに属する場合

非 IP パケットは、常にベスト エフォート キューに格納されます。

8 キュー システムでの DSCP からキューへのデフォルト マッピングを、以下の表に示します。7 が最高であり、8 はスタック コントロール用に使用されます。

DSCP	63	55	47	39	31	23	15	7
キュー	6	6	7	5	4	3	2	1
DSCP	62	54	46	38	30	22	14	6
キュー	6	6	7	5	4	3	2	1
DSCP	61	53	45	37	29	21	13	5
キュー	6	6	7	5	4	3	2	1
DSCP	60	52	44	36	28	20	12	4

キュー	6	6	7	5	4	3	2	1
DSCP	59	51	43	35	27	19	11	3
キュー	6	6	7	5	4	3	2	1
DSCP	58	50	42	34	26	18	10	2
キュー	6	6	7	5	4	3	2	1
DSCP	57	49	41	33	25	17	9	1
キュー	6	6	7	5	4	3	2	1
DSCP	56	48	40	32	24	16	8	0
キュー	6	6	6	7	6	6	1	1

8 キュー システムの場合の DSCP 値のキューへのデフォルトのマッピングを、以下の表に示します。8 が最高です。

DSCP	63	55	47	39	31	23	15	7
キュー	7	7	8	6	5	4	3	1
DSCP	62	54	46	38	30	22	14	6
キュー	7	7	8	6	5	4	3	1
DSCP	61	53	45	37	29	21	13	5
キュー	7	7	8	6	5	4	3	1
DSCP	60	52	44	36	28	20	12	4
キュー	7	7	8	6	5	4	3	1
DSCP	59	51	43	35	27	19	11	3
キュー	7	7	8	6	5	4	3	1
DSCP	58	50	42	34	26	18	10	2
キュー	7	7	8	6	5	4	3	1

DSCP	57	49	41	33	25	17	9	1
キュー	7	7	8	6	5	4	3	1
DSCP	56	48	40	32	24	16	8	0
キュー	7	7	7	8	7	7	1	2

DSCP をキューにマップするには、次のようにします。

ステップ 1 [サービス品質] > [全般] > [DSCP 値のキューへのマッピング] をクリックします。

[DSCP値のキューへのマッピング] ページには、[入力DSCP] フィールドが含まれています。このフィールドには着信パケットの DSCP 値、およびその関連クラスが表示されます。

ステップ 2 [出力キュー] で、DSCP 値をマッピングする出力キュー(トラフィック フォワーディング キュー)を選択します。

ステップ 3 [適用] をクリックします。実行コンフィギュレーション ファイルが更新されます。

帯域幅

[帯域幅] ページには、各インターフェイスに対する帯域幅情報が表示されます。

帯域幅情報を表示するには、次のようにします。

ステップ 1 [サービス品質] > [全般] > [帯域幅] をクリックします。

このページ内のフィールドは [編集] ページで説明されます。ただし、次のフィールドを除きます。

- [入力レート制限]:
  - [ステータス]:入力レート制限が有効になっているかどうかが表示されます。
  - [レート制限(キロビット/秒)]:ポートの入力レート制限が表示されます。
  - [%]:ポートの入力レート制限を合計ポート帯域幅で割った値が表示されます。
  - [CBS (バイト)]:データのバイトに含まれる入力インターフェイスの最大バースト データ サイズ。

- [出力シェーピング レート]:
  - [ステータス]:出力シェーピング レートが有効になっているかどうかが表示されます。
  - [CIR (キロビット/秒)]:出力インターフェイスの最大帯域幅が表示されます。
  - [CBS (バイト)]:データのバイトに含まれる出力インターフェイスの最大バースト データ サイズ。

ステップ 2 インターフェイスを選択し、[編集] をクリックします。

ステップ 3 [ポート] または [LAG] インターフェイスを選択します。

ステップ 4 選択したインターフェイスに関する次のフィールドの値を指定します。

- [入力レート制限]:入力レート制限を有効にする場合、このフィールドを選択します。具体的な値はその下のフィールドで定義します。(LAG とは無関係です)。
- [入力レート制限(キロビット/秒)]:このインターフェイスで使用できる最大帯域幅を入力します。(LAG とは無関係です)。
- [認定バーストサイズ(CBS)]:この入力インターフェイスに対する最大バースト データ サイズをバイトで入力します。この値は、使用帯域幅が一時的に許容制限を超えるとしても送信できるデータ量を意味します。このフィールドは、インターフェイスがポートの場合のみ利用可能です。(LAG とは無関係です)。
- [出力シェーピングレート]:このインターフェイスで出力シェーピングを有効にする場合、このフィールドを選択します。
- [認定情報レート(CIR)]:この出力インターフェイスで使用できる最大帯域幅を入力します。
- [出力認定バーストサイズ(CBS)]:この出力インターフェイスに対する最大バースト データ サイズをバイトで入力します。この値は、使用帯域幅が一時的に許容制限を超えるとしても送信できるデータ量を意味します。

ステップ 5 [適用] をクリックします。帯域幅設定値が、実行コンフィギュレーション ファイルに書き込まれます。

キューあたりの出力シェーピング

このデバイスでは、[帯域幅] ページでポート単位で入出力レートを制限できるだけでなく、選択した出力フレームの入出力レートをキュー単位、ポート単位で制限することもできます。出力レートを制限するには、出 力負荷をシェーピングします。

このデバイスでは、管理フレーム以外のすべてのフレームの出力レートを制限できます。レートが制限されていないパケットは、レート計算において無視されます。つまり、それらのパケットのサイズは合計レート制限に含まれません。

キュー単位出力レート シェーピングは、無効にすることもできます。

キュー単位出力シェーピングを定義するには、次のようにします。

ステップ 1 [サービス品質] > [全般] > [キューあたりの出力シェーピング] をクリックします。

[キューあたりの出力シェーピング] ページには、各キューに対するレート制限とバースト サイズが表示されます。

ステップ 2 インターフェイス タイプ（ポートまたは LAG）を選択し、[実行] をクリックします。

ステップ 3 ポートまたは LAG を選択し、[編集] をクリックします。

このページでは、インターフェイスごとに最大 8 個のキューに対して、出力シェーピングを有効にすることができます。

ステップ 4 [インターフェイス] を選択します。

ステップ 5 必要な各キューに対して、次のフィールドの値を入力します。

- [有効]: このキューに対して出力シェーピングを有効にする場合に選択します。
- [認定情報レート(CIR)]: 最大レート値（CIR）を入力します（単位：Kbps）。CIR は、送信できる平均データ量です。
- [認定バーストサイズ(CBS)]: 最大バースト サイズ（CBS）をバイトで入力します。CBS は、CIR を一時的に超えて送信できるデータ量を意味します。

ステップ 6 [適用] をクリックします。帯域幅設定値が、実行コンフィギュレーション ファイルに書き込まれます。

VLAN 入力レート制限

[VLAN 入力レート制限] ページで VLAN ごとにレート制限を実行すると、VLAN 上でのトラフィック制限が有効になります。VLAN 入力レート制限が設定されている場合、そのデバイス上のすべてのポートからの集約トラフィックが制限されます。

VLAN ごとのレート制限には、以下の制約が適用されます。

- システム内で定義されている他のトラフィック ポリシングよりも低い優先度になります。たとえば、QoS レート制限と VLAN レート制限がパケットに適用されていて、それらのレート制限が競合する場合、QoS レート制限が優先されます。
- これはデバイス レベルで適用され、そのデバイス内部ではパケット プロセッサ レベルで適用されます。デバイス上に複数のパケット プロセッサがある場合、設定されている VLAN レート制限値が、パケット プロセッサのそれぞれに独立して適用されます。ポート数が 24 個以下のデバイスの場合、パケット プロセッサは 1 個ですが、48 ポート以上のデバイスではパケット プロセッサが 2 個あります。

レート制限は、ユニット中のパケット プロセッサごと、そしてスタック中のユニットごとに別個に計算されます。

VLAN 入力レート制限を定義するには、次のようにします。

ステップ 1 [サービス品質] > [全般] > [VLAN 入力レート制限] をクリックします。

このページには、VLAN 入力レート制限の一覧表が表示されます。

ステップ 2 [追加] をクリックします。

ステップ 3 パラメータを入力します。

- [VLAN ID]: VLAN を選択します。
- [認定情報レート(CIR)]: VLAN への入力として受け入れ可能な最大平均データ量を、Kbps 単位で入力します。
- [認定バーストサイズ(CBS)]: この出力インターフェイスに対する最大バースト データ サイズをバイトで入力します。この値は、使用帯域幅が一時的に許容制限を超えるとしても送信できるデータ量を意味します。LAG の場合は入力できません。

ステップ 4 [適用] をクリックします。VLAN レート制限が追加され、実行コンフィギュレーション ファイルが更新されます。

TCP 輻輳回避

[TCP 輻輳回避] ページでは、TCP 輻輳回避アルゴリズムをアクティブにすることができます。このアルゴリズムは、さまざまな送信元が同じバイト カウントのパケットを送信しているためにノードで輻輳が発生している場合に、その輻輳ノードでの TCP グローバル同期を無効にするか、または回避します。

TCP 輻輳回避を設定するには、次のようにします。

ステップ 1 [サービス品質] > [全般] > [TCP 輻輳回避] をクリックします。

ステップ 2 [有効] をクリックして TCP 輻輳回避を有効にし、[適用] をクリックします。

QoS 基本モード

ここで説明する内容は次のとおりです。

- 概要
- グローバル設定
- インターフェイス設定

概要

QoS 基本モードでは、ネットワーク内の特定のドメインを信頼できるものとして定義できます。そのドメイン内では、必要となるサービスのタイプを表すために、パケットに 802.1p プライオリティや DSCP のマークが付けられます。そのドメイン内のノードでは、それらのフィールドを使用して、パケットが特定の出力キューに割り当てられます。初期パケット分類およびそれらのフィールドのマーキングは、信頼できるドメインの入力において実行されます。

基本 QoS モードの設定手順

基本 QoS モードを設定するには、次のようにします。

1. [QoS プロパティ] ページで、システムの基本モードを選択します。
2. [グローバル設定] ページで、信頼の動作を選択します。デバイスでは、CoS/802.1p 信頼モードおよび DSCP 信頼モードがサポートされています。CoS/802.1p 信頼モードでは、VLAN タグの 802.1p プライオリティが使用されます。DSCP 信頼モードでは、IP ヘッダーの DSCP 値が使用されます。

あるポートでは、例外として、着信 CoS マークを信頼しないことにする場合は、[インターフェイス設定] ページで、そのポートでの QoS 状態を無効にします。

グローバルに選択されている信頼モードを、ポートで有効または無効する場合は、[インターフェイス設定] ページを使用します。信頼モードなしでポートが無効にされている場合、その入力パケットはすべてベスト エフォートで転送されます。着信パケットの CoS/802.1p 値や DSCP 値が信頼できないポートでは、信頼モードを無効にするようお勧めします。そうしない場合、ネットワークのパフォーマンスが低下する可能性があります。

グローバル設定

[グローバル設定] ページには、デバイス上で信頼を有効にするための情報が含まれています（後述の [信頼モード] フィールドを参照）。QoS モードが基本モードの場合、この設定がアクティブになります。QoS ドメインに入ってくるパケットは、その QoS ドメインの境界で分類されます。

信頼設定を定義するには、次のようにします。

ステップ 1 [サービス品質] > [QoS 基本モード] > [グローバル設定] をクリックします。

ステップ 2 デバイスが基本モードになっているときに [信頼モード] を選択します。パケット CoS レベルおよび DSCP タグがそれぞれ別個のキューにマッピングされる場合、そのパケットの割り当て先キューは信頼モードによって決まります。

- [CoS/802.1p]: トラフィックは、VLAN タグの VPT フィールドに基づいて、またはポートごとのデフォルト CoS/802.1p 値に基づいて（着信パケットに VLAN タグがない場合）キューにマッピングされます。VPT とキューの実際のマッピングは、[CoS/802.1p 値のキューへのマッピング] ページで設定できます。
- [DSCP]: すべての IP トラフィックは、IP ヘッダーの DSCP フィールドに基づいてキューにマッピングされます。DSCP とキューの実際のマッピングは、[DSCP 値のキューへのマッピング] ページで設定できます。トラフィックが IP トラフィックではない場合、ベスト エフォート キューにマッピングされます。
- [CoS/802.1p、DSCP]: CoS/802.1p と DSCP のうち、いずれか設定されているほう。

ステップ 3 着信パケット中の元の DSCP 値を、DSCP オーバーライド テーブルに入力された新しい値でオーバーライドする場合は、[入力DSCP のオーバーライド] を選択します。[入力DSCP のオーバーライド] が有効にされると、デバイスで出力キューイングに新しい DSCP 値が使用されます。また、パケット中の元の DSCP 値も、新しい DSCP 値によって置き換えられます。

注 フレームは、元の DSCP 値ではなく書き換え後の新しい値を使用して出力キューにマッピングされます。

ステップ 4 [入力 DSCP のオーバーライド] を有効にした場合は、[DSCP オーバーライドテーブル] をクリックして DSCP を設定し直します。(**DSCP オーバーライド テーブル**を参照)。

ステップ 5 [DSCP 入力] には、着信パケットの DSCP 値が表示されます。これらの値を代替値に変更する必要があります。[DSCP 出力] の値を選択して、マッピングする発信値を指定します。

ステップ 6 [適用] をクリックします。実行コンフィギュレーション ファイルが新しい DSCP 値で更新されます。

インターフェイス設定

[インターフェイス設定] ページでは、デバイスのポートごとに QoS を設定できます。

- **インターフェイスに対して QoS 状態を無効にした場合**:そのポートの着信トラフィックはすべて、ベスト エフォート キューに格納されます。トラフィックの分類処理およびプライオリティ設定処理は実行されません。
- **ポートに対して QoS 状態を有効にした場合**:そのポートに届いたトラフィックは、システム規模でグローバルに設定された信頼モード (CoS/802.1p 信頼モードまたは DSCP 信頼モード) に基づいて処理されます。

各インターフェイスの QoS 設定を入力するには、次のようにします。

ステップ 1 [サービス品質] > [QoS 基本モード] > [インターフェイス設定] をクリックします。

ステップ 2 [ポート] または [LAG] を選択して、ポートまたは LAG のリストを表示します。

[QoS 状態] に、各インターフェイスの QoS 状態 (有効か無効か) が表示されます。

ステップ 3 インターフェイスを選択し、[編集] をクリックします。

ステップ 4 [ポート] または [LAG] インターフェイスを選択します。

ステップ 5 このインターフェイスの QoS 状態 (有効か無効か) をクリックして設定します。

ステップ 6 [適用] をクリックします。実行コンフィギュレーション ファイルが更新されます。

QoS 拡張モード

ここで説明する内容は次のとおりです。

概要

ACL に合致して着信が許可されたフレームは、暗黙的に、着信許可を出した ACL の名前がラベルとして付けられます。これらのフローには、拡張モード QoS アクションを適用できます。

QoS 拡張モードでは、フローごとの QoS をサポートするポリシーがデバイスにより使用されます。ポリシーとそのコンポーネントには、以下の特徴および関係性があります。

- ポリシーには 1 つ以上のクラス マップが含まれています。
- クラス マップは、関連する 1 つ以上の ACL でフローを定義します。クラス マップの中の許可（転送）アクションを伴う ACL ルール（ACE）のみに合致するパケットは、同じフローに属するものと見なされ、同じサービス品質が適用されます。そのようにして、1 つのポリシーに 1 つ以上のフローが含まれ、そのそれぞれにユーザ定義 QoS があります。
- クラス マップ（フロー）の QoS は関連するポリサーにより適用されます。ポリサーには、シングル ポリサーと集約ポリサーの 2 種類があります。それぞれのポリサーは、QoS 仕様により設定されます。シングル ポリサーは、そのポリサーの QoS 仕様に基づいて QoS を単一のクラス マップに、したがって単一のフローに適用します。集約ポリサーは、1 つ以上のクラス マップに、したがって 1 つ以上のフローに QoS を適用します。集約ポリサーは、異なる複数のポリシーからのクラス マップをサポート可能です。

- フローごとの QoS は、ポリシーを目的のポートにバインドすることによりフローに適用されます。1 つのポリシーとそのクラス マップを 1 つ以上のポートにバインドすることは可能ですが、各ポートは 1 つのポリシーにしかバインドできません。

備考:

- シングル ポリサーと集約ポリサーは、デバイスがレイヤ 2 モードの場合に利用可能です。
- ACL については、ポリシーに関係なく、1 つの ACL を 1 つ以上のクラス マップに対して設定可能です。
- クラス マップは 1 つのポリシーにのみ属することができます。
- シングル ポリサーを使用するクラス マップが複数ポートにバインドされている場合、各ポートがそれぞれシングル ポリサーの独自のインスタンスを持ち、互いに独立したポートでクラス マップ (フロー) に QoS を適用します。
- 集約ポリサーは、ポリシーおよびポートには関係なく、集約中のすべてのフローに QoS を適用します。

拡張 QoS 設定値は、3 つの部分で構成されます。

- マッチング ルールの定義。単一のルール グループに合致するすべてのフレームは、1 つの *フロー* と見なされます。
- ルールに合致する各フロー内のフレームに適用されるアクションの定義。
- ルールとアクションの組み合わせの、1 つ以上のインターフェイスへのバインド。

拡張 QoS モードの設定手順

拡張 QoS モードを設定するには、次のようにします。

1. [QoS プロパティ] ページで、システムの拡張モードを選択します。[グローバル設定] ページで、信頼モードを選択します。パケット CoS レベルおよび DSCP タグがそれぞれ別個のキューにマッピングされる場合、そのパケットの割り当て先キューは信頼モードによって決まります。
   - 内部 DSCP 値が着信パケットで使用されているものとは異なる場合、[アウトオブプロファイル DSCP リマーク] ページで、外部値を内部値にマッピングします。それにより、[DSCPリマーク テーブル] ページが表示されます。
2. 「ACL ワークフローの作成」の説明に従って、ACL を作成します。

3. ACL が定義されている場合は、[クラスマッピング] ページでクラス マップを作成して、ACL をクラス マップに関連付けます。
4. [ポリシーテーブル] ページでポリシーを作成し、[ポリシークラスマップ] ページでそのポリシーを 1 つ以上のクラス マップに関連付けます。また、必要なら、クラス マップをポリシーに関連付ける際にポリサーをそのクラス マップに割り当てることによって、QoS を指定することもできます。
   - **シングルポリサー**:[ポリシーテーブル] ページと[クラス マッピング] ページを使用して、クラス マップをシングル ポリサーに関連付けるポリシーを作成します。ポリシー内で、シングル ポリサーを定義します。
   - **集約ポリサー**:[集約ポリサー] ページで、フローごとに、合致するフレームすべてを同じポリサー(集約ポリサー)に送る QoS アクションを作成します。[ポリシーテーブル] ページで、クラス マップを集約ポリサーに関連付けるポリシーを作成します。
5. [ポリシーバインディング] ページで、ポリシーをインターフェイスにバインドします。

グローバル設定

[グローバル設定] ページには、デバイス上で信頼を有効にするための情報が含まれています。QoS ドメインに入ってくるパケットは、その QoS ドメインの境界で分類されます。

信頼設定を定義するには、次のようにします。

ステップ 1 [サービス品質] > [QoS 拡張モード] > [グローバル設定] をクリックします。

ステップ 2 デバイスが拡張モードになっているときに [信頼モード] を選択します。パケット CoS レベルおよび DSCP タグがそれぞれ別個のキューにマッピングされる場合、そのパケットの割り当て先キューは信頼モードによって決まります。

- [CoS/802.1p]:トラフィックは、VLAN タグの VPT フィールドに基づいて、またはポートごとのデフォルト CoS/802.1p 値に基づいて(着信パケットに VLAN タグがない場合)キューにマッピングされます。VPT とキューの実際のマッピングは、[CoS/802.1p 値のキューへのマッピング] ページで設定できます。
- [DSCP]:すべての IP トラフィックは、IP ヘッダーの DSCP フィールドに基づいてキューにマッピングされます。DSCP とキューの実際のマッピングは、[DSCP 値のキューへのマッピング] ページで設定できます。トラフィックが IP トラフィックではない場合、ベスト エフォート キューにマッピングされます。
- [CoS/802.1p、DSCP]:非 IP トラフィックに信頼 CoS モード、および IP トラフィックに信頼 DSCP を使用する場合に選択します。

ステップ 3 [デフォルト モードのステータス] フィールドで、インターフェイスのデフォルトの拡張モード QoS 信頼モード（信頼できるかどうか）を選択します。これにより、拡張 QoS で基本 QoS の機能が提供されるため、拡張 QoS でデフォルトで（ポリシーを作成することなく）CoS/DSCP を信頼できるようになります。

[QoS 拡張モード] で、[デフォルト モードのステータス] が [信頼できない] に設定されている場合、インターフェイスで設定されているデフォルトの CoS 値は無視され、すべてのトラフィックはキュー 1 に送られます。詳しくは、[サービス品質] > [QoS 拡張モード] > [グローバル設定] ページを参照してください。

インターフェイス上にポリシーがある場合、デフォルト モードは無効になり、ポリシー設定に従ったアクションになり、合致しないトラフィックはドロップされます。

ステップ 4 DSCP オーバーライド テーブルに従って、着信パケット中の元の DSCP 値を新しい値でオーバーライドする場合は、[入力DSCP のオーバーライド] を選択します。[入力 DSCP のオーバーライド] が有効にされると、デバイスで出力キューイングに新しい DSCP 値が使用されます。また、パケット中の元の DSCP 値も、新しい DSCP 値によって置き換えられます。

注 フレームは、元の DSCP 値ではなく書き換え後の新しい値を使用して出力キューにマッピングされます。

ステップ 5 [入力 DSCP のオーバーライド] を有効にした場合は、[DSCP オーバーライド テーブル] をクリックして DSCP を設定し直します。

DSCP オーバーライド テーブル

ステップ 1 次のフィールドを入力します。

- [DSCP 入力]: 着信パケットの DSCP 値が表示されます。これらの値を代替値に変更する必要があります。
- [DSCP 出力]: 発信値がマッピングされることを示す場合に DSCP 出力値を選択します。

ステップ 2 [適用] をクリックします。

アウトオブプロファイル DSCP リマーク

クラス マップ(フロー)にポリサーが割り当てられている場合、フロー内のトラフィック量が QoS で指定されている制限を超えた場合に実行されるアクションを指定できます。トラフィックのうち、フローが QoS 制限を超過する原因となった部分は、*アウトオブプロファイル パケット*と呼ばれます。

超過アクションがアウト オブ プロファイル DSCP の場合、デバイスにより、アウト オブ プロファイル IP パケットの元の DSCP 値が、アウト オブ プロファイル DSCP マッピング テーブルに基づく新しい値を使用してマッピングし直されます。デバイスは、新しい値を使用して、それらのパケットにリソースと出力キューを割り当てます。また、アウトオブプロファイル パケット中の元の DSCP 値も、新しい DSCP 値によって物理的に置き換えられます。

アウト オブ プロファイル DSCP 超過アクションを使用するには、アウト オブ プロファイル DSCP リマーク テーブルで DSCP 値を再マッピングします。そうしない場合、アクションは空になります。出荷時設定では、パケットはこのテーブルの DSCP 値により、その値そのものに再マッピングされるためです。

この機能により、信頼 QoS ドメイン間で切り替えられる着信トラフィックの DSCP タグが変更されます。あるドメインで使用されている DSCP 値が変更されると、そのタイプのトラフィックのプライオリティが、他のドメインで使用されている DSCP 値に対して設定され、同じタイプのトラフィックが識別されるようになります。

これらの設定値は、システムが QoS 拡張モードの場合にアクティブになり、一度アクティブになるとグローバルにアクティブになります。

例:サービスのレベルとして、シルバー、ゴールド、プラチナの 3 種類があり、それらのレベルを示すマークとして使用する DSCP 着信値がそれぞれ 10、20、30 だとします。このトラフィックが、別のサービス プロバイダー(同じ 3 種類のレベルのサービスがあるが、DSCP 値として 16、24、48 が使用されている)に転送されると、**アウト オブ プロファイル DSCP リマーク**により、着信値から発信値へのマッピングに従って、着信値が変更されます。

DSCP 値をマップするには、次のようにします。

ステップ 1 [サービス品質] > [QoS 拡張モード] > [アウト オブ プロファイル DSCP リマーク] をクリックします。このページで、デバイスを出入りするトラフィックの DSCP 値を設定することができます。

[DSCP 入力] には、着信パケットの DSCP 値が表示されます。これらの値を代替値に変更する必要があります。

ステップ 2 着信値のマッピング結果となる [DSCP 出力] 値を選択します。

ステップ 3 [適用] をクリックします。実行コンフィギュレーション ファイルが新しい DSCP リマーク テーブルにより更新されます。

ステップ 4 このインターフェイスの CoS 情報を工場出荷時設定に戻すには、[デフォルトの復元] を選択します。

クラス マッピング

クラス マップは、その上で定義された ACL(アクセス コントロール リスト)を使用してトラフィック フローを定義します。MAC ACL、IP ACL、および IPv6 ACL を組み合わせて、クラス マップを作成できます。クラス マップは、すべて合致か、いずれかが合致という形でパケット条件に合致するように設定されます。パケット合致は、ファースト フィット方式で判定されます。つまり、最初に合致したクラス マップに関連するアクションが、システムの実行するアクションになります。複数のパケットが同じクラス マップに合致する場合、それらのパケットは同じフローに属するものと見なされます。

注 クラス マップを定義しても、QoS には影響しません。そのクラス マップが使用されるようになるには、しなければならないことが他にもあります。

より複雑なルール セットが必要になる場合、複数のクラス マップを、ポリシーと呼ばれるスーパー グループにまとめることができます(ポリシー テーブルを参照)。

注 同一のクラス マップでは、宛先 IPv6 アドレスがフィルタリング条件として設定されている IPv6 ACE と同時に MAC ACL を使用することはできません。

[クラスマッピング] ページには、定義されているクラス マップと、そのそれぞれを構成する ACL のリストが表示されます。このページで、クラス マップを追加したり削除したりできます。

クラス マップを定義するには、次のようにします。

ステップ 1 [サービス品質] > [QoS 拡張モード] > [クラス マッピング] をクリックします。

クラス マップごとに、その上で定義された ACL がそれらの関係と一緒に表示されます。最大 3 つの ACL を [一致] と一緒に表示できます。[一致] は [And] または [Or] のどちらかにすることができます。これは、ACL 間の関係を示しています。クラス マップは、3 つの ACL を And または Or のどちらかで結合した結果になります。

ステップ 2 [追加] をクリックします。

1 つまたは 2 つの ACL を選択し、クラス マップの名前を指定すると、新しいクラス マップが追加されます。クラス マップの ACL が 2 個の場合、フレームがそれら ACL の両方に合致しなければならないのか、それとも選択された ACL のうちいずれか一方または両方に合致しなければならないのかを指定できます。

ステップ 3 パラメータを入力します。

- [クラスマップ名]:新しいクラス マップの名前を入力します。
- [一致ACLタイプ]:クラス マップで定義されているフローに属すると見なされるためにパケットが合致しなければならない条件。次のオプションがあります。
  - [IP]:パケットは、クラス マップの IP ベース ACL のいずれかに合致しなければなりません。
  - [MAC]:パケットは、クラス マップの MAC ベース ACL のいずれかに合致しなければなりません。
  - [IPおよびMAC]:パケットは、クラス マップの IP ベース ACL と MAC ベース ACL に合致しなければなりません。
  - [IPまたはMAC]:パケットは、クラス マップの IP ベース ACL または MAC ベース ACL のいずれかに合致しなければなりません。
- [IP]:クラス マップの IPv4 ベース ACL または IPv6 ベース ACL を選択します。
- [MAC]:クラス マップの MAC ベース ACL を選択します。
- [優先ACL]:パケットを IP ベース ACL と MAC ベース ACL のどちらと最初に照合するのかを選択します。

ステップ 4 [適用] をクリックします。実行コンフィギュレーション ファイルが更新されます。

集約ポリサー

事前定義ルール セットに合致するトラフィックのレートを測定し、ポートで許可されるファイル転送トラフィックのレートの制限などの制限を適用することができます。

これは、クラス マップの ACL を使用して目的のトラフィックを照合したり、ポリサーを使用して合致トラフィックに QoS を適用したりすることによって行えます。

ポリサーは、QoS 仕様により設定されます。ポリサーには、以下の 2 種類あります。

- **シングル(標準)ポリサー**:シングル ポリサーは、ポリサー QoS 仕様に基づいて QoS を単一のクラス マップに、つまりは単一のフローに適用します。シングル ポリサーを使用するクラス マップが複数ポートにバインドされている場合、各ポートがそれぞれシングル ポリサーの独自のインスタンスを持ち、本来は互いに独立しているポートでクラス マップ(フロー)に QoS を適用します。シングル ポリサーは、[ポリシーテーブル] ページで作成されます。

- **集約ポリサー**:集約ポリサーは、1 つ以上のクラス マップに、つまりは 1 つ以上のフローに QoS を適用します。集約ポリサーは、異なる複数のポリシーからのクラス マップをサポート可能です。集約ポリサーは、ポリシーおよびポートには関係なく、集約中のすべてのフローに QoS を適用します。集約ポリサーは、[集約ポリサー] ページで作成されます。

  集約ポリサーは、ポリサーを複数のクラスで共有する場合に定義されます。あるポートのポリサーを、別のデバイスの他のポリサーと共有することはできません。

各ポリサーは、以下のパラメータを組み合わせたそれぞれ独自の QoS 仕様により定義されます。

- 最大許容レート(認定情報レート、CIR)(単位:Kbps)。
- トラフィック量(入力認定バースト サイズ、CBS)(単位:バイト)。これは、定義されている最大レートを超える場合にも一時的なバーストとして通過を許可されるトラフィックです。
- 制限を超えるフレーム(アウトオブプロファイル トラフィック)に適用されるアクション。そのようなフレームは、そのまま通過させられるか、ドロップされるか、あるいは通過させられた上で新しい DSCP 値に再マッピングされて、そのデバイス内の以降のすべての処理ではプライオリティが低いフレームとなるようにマークされます。
- 指定されたレートとオプション アクションに基づいてトラフィック ポリシングを設定します。CIR と、これらのオプション値とアクションを入力します。

ポリサーをクラス マップに割り当てる処理は、クラス マップがポリシーに追加される時点で実行されます。ポリサーが集約ポリサーの場合は、[集約ポリサー] ページで、それを作成する必要があります。

集約ポリサーを定義するには、次のようにします。

ステップ 1 [サービス品質] > [QoS 拡張モード] > [集約ポリサー] をクリックします。

このページには、既存の集約ポリサーが表示されます。

ステップ 2 [追加] をクリックします。

ステップ 3 パラメータを入力します。

- [集約ポリサー名]:集約ポリサーの名前を入力します。
- [入力認定情報レート(CIR)]:最大帯域幅(単位:bps)。[帯域幅] ページにある説明を参照してください。

- [入力認定バーストサイズ(CBS)]:CIR を超えていても通過を許可される最大バースト サイズ(単位:バイト)を入力します。[帯域幅] ページにある説明を参照してください。
- [超過アクション]:CIR を超える着信パケットに対して実行するアクションを選択します。選択項目は次のとおりです。
  - [ドロップ]:定義されている CIR 値を超えるパケットはドロップされます。
  - [アウト オブ プロファイル DSCP]:定義されている CIR 値を超えるパケットの DSCP 値は、アウト オブ プロファイル DSCP リマーク テーブルに基づく値に再マップされます。

ステップ 4 [適用] をクリックします。実行コンフィギュレーション ファイルが更新されます。

ポリシー テーブル

[ポリシー テーブル マップ] ページには、システム内で定義されている拡張 QoS ポリシーのリストが表示されます。このページでは、ポリシーを作成したり削除したりすることもできます。インターフェイスにバインドされているポリシーだけがアクティブになります([ポリシーバインディング] ページを参照)。

各ポリシーは、以下のもので構成されます。

- ポリシーの中のトラフィック フローを定義する ACL の 1 つ以上のクラス マップ。
- ポリシーの中のトラフィック フローに QoS を適用する 1 つ以上の集約。

ポリシーが追加された後、[ポリシーテーブル] ページで、クラス マップを追加することができます。

QoS ポリシーを追加するには、次のようにします。

ステップ 1 [サービス品質] > [QoS 拡張モード] > [ポリシーテーブル] をクリックします。

このページには、定義されているポリシーのリストが表示されます。

ステップ 2 [ポリシークラスマップテーブル] をクリックして、[ポリシークラスマップ] ページを表示します。
または
[追加] をクリックして、[ポリシーテーブルの追加] ページを表示します。

ステップ 3 [新規ポリシー名] フィールドに、新しいポリシーの名前を入力します。

ステップ 4 [適用] をクリックします。QoS ポリシー プロファイルが追加され、実行コンフィギュレーション ファイルが更新されます。

ポリシー クラス マップ

ポリシーには、1 つ以上のクラス マップを追加することができます。クラス マップは、同じトラフィック フローに属すると見なされるパケットのタイプを定義します。

ポリシーにクラス マップを追加するには、次のようにします。

ステップ 1 [サービス品質] > [QoS 拡張モード] > [ポリシー クラス マップ] をクリックします。

ステップ 2 フィルタでポリシーを選択して、[実行] をクリックします。そのポリシーの中のすべてのクラス マップが表示されます。

ステップ 3 新しいクラス マップを追加するには、[追加] をクリックします。

ステップ 4 パラメータを入力します。

- [ポリシー名]: クラス マップの追加先ポリシーが表示されます。
- [クラス マップ名]: ポリシーに関連付ける既存のクラス マップを選択します。クラス マップは、[クラスマッピング] ページで作成されます。
- [アクションタイプ]: 合致するすべてのパケットの入力 CoS/802.1p や DSCP の値に関連するアクションを選択します。
  - [デフォルト信頼モードを使用する]: このオプションが選択されている場合は、デフォルト モード ステータスをグローバル信頼モードで使用します。デフォルト モード ステータスが「信頼できない」の場合は、入力 CoS/802.1p と DSCP の値を無視します。一致したパケットはベスト エフォートとして送信されます。
  - [常に信頼]: このオプションが選択されている場合は、デバイスがグローバル信頼モード ([グローバル設定] ページで選択) に基づいて一致したパケットを信頼します。デフォルト モード ステータス ([グローバル設定] ページで選択) は無視されます。
  - [設定]: このオプションが選択されている場合は、[新しい値] ボックスに入力された値を使用することにより、合致パケットの出力キューが以下のように判別されます。

    新しい値 (0..7) が CoS/802.1p プライオリティである場合、そのプライオリティ値と [CoS/802.1p値のキューへのマッピングテーブル] を使用して、すべての合致パケットの出力キューを判別します。

新しい値 (0..63) が DSCP である場合、新しい DSCP と [DSCP値のキューへのマッピングテーブル] を使用して、合致する IP パケットの出力キューを判別します。

そうでない場合、新しい値 (1..8) を、すべての合致パケットの出力キュー番号として使用します。

- [ポリシングタイプ]:ポリシーのポリサー タイプを選択します。次のオプションがあります。
  - [なし]:ポリシーは使用されません。
  - [シングル]:ポリシーのポリサーはシングル ポリサーです。
  - [集約]:ポリシーのポリサーは集約ポリサーです。

ステップ 5 [ポリシングタイプ] が [集約] の場合は、[集約ポリサー] を選択します。

ステップ 6 [ポリシングタイプ] が [シングル] である場合、以下の QoS パラメータを入力します。

- [入力認定情報レート(CIR)]:CIR を Kbps 単位で入力します。[帯域幅] ページにある説明を参照してください。
- [入力認定バーストサイズ(CBS)]:CBS をバイト単位で入力します。[帯域幅] ページにある説明を参照してください。
- [超過アクション]:CIR を超える着信パケットに割り当てるアクションを選択します。次のオプションがあります。
  - [ドロップ]:定義されている CIR 値を超えるパケットはドロップされます。
  - [アウト オブ プロファイル DSCP]:定義されている CIR 値を超える IP パケットは、アウト オブ プロファイル DSCP リマーク テーブルに由来する新しい DSCP を使用して転送されます。

ステップ 7 [適用] をクリックします。

ポリシー バインディング

[ポリシー バインディング] ページには、どのポリシー プロファイルがどのポートにバインドされているかが表示されます。ポリシーは入力ポリシーまたは出力ポリシーとしてインターフェイスにバインドできます。ポリシー プロファイルが特定のポートにバインドされている場合、それはそのポートでアクティブです。1 つのポートと 1 つの方向に設定できるポリシー プロファイルは 1 つのみですが、1 つのポリシーを複数のポートにバインドすることはできます。

ポリシーがポートにバインドされている場合、ポリシーで定義されているフローに属するトラフィックがフィルタリングされ、それに QoS が適用されます。

ポリシーを編集するには、まず、バインド先のすべてのポートからそのポリシーを削除する（アンバインド）必要があります。

注 ポートは、ポリシーか ACL のいずれかにバインドできますが、その両方にバインドすることはできません。

ポリシー バインディングを定義するには、次のようにします。

ステップ 1 [サービス品質] > [QoS 拡張モード] > [ポリシーバインディング] をクリックします。

ステップ 2 必要に応じて、[インターフェイスタイプ] を選択します。

ステップ 3 [実行] をクリックします。そのインターフェイスのポリシーが表示されます。

ステップ 4 [編集] をクリックします。

ステップ 5 入力ポリシー/インターフェイスに対して以下を選択します。

- [入力ポリシーバインディング]: 入力ポリシーをインターフェイスにバインドする場合に選択します。
- [ポリシー名]: バインドする入力ポリシーを選択します。
- [デフォルト アクション]: パケットがポリシーと一致した場合のアクションを選択します。
  - [いずれも拒否]: インターフェイス上のパケットがいずれかのポリシーと一致したら転送する場合に選択します。
  - [いずれも許可]: インターフェイス上のパケットがどのポリシーにも合致しないならそれらを転送する場合に選択します。

  注 [いずれも許可] を定義できるのは、IP ソース ガードがインターフェイス上でアクティブでない場合にのみです。

ステップ 6 出力ポリシー/インターフェイスに対して以下を選択します。

- [出力ポリシーバインディング]: 出力ポリシーをインターフェイスにバインドする場合に選択します。
- [ポリシー名]: バインドする出力ポリシーを選択します。
- [デフォルト アクション]: パケットがポリシーと一致した場合のアクションを選択します。
  - [いずれも拒否]: インターフェイス上のパケットがいずれかのポリシーと一致したら転送する場合に選択します。

- [いずれも許可]: インターフェイス上のパケットがどのポリシーにも合致しないならそれらを転送する場合に選択します。

注 [いずれも許可] を定義できるのは、IP ソース ガードがインターフェイス上でアクティブでない場合にのみです。

ステップ 7 [適用] をクリックします。QoS ポリシー バインディングが定義され、実行コンフィギュレーション ファイルが更新されます。

QoS 統計情報

これらのページでは、シングル ポリサーおよび集約ポリサーを管理したり、キュー統計情報を表示したりすることができます。

ポリサー統計

シングル ポリサーは、1 つのポリシー内の 1 つのクラス マップに割り当てられます。集約ポリサーは、1 つ以上のポリシー内の 1 つ以上のクラス マップに割り当てられます。

シングル ポリサー統計情報の表示

[シングルポリサー統計] ページでは、インターフェイスから受信したプロファイル内パケットおよびアウトオブプロファイル パケットのうち、ポリシーのクラス マップで定義されている条件を満たすものの数が示されます。

注 デバイスがレイヤ 3 モードの場合、このページは表示されません。

ポリサー統計情報を表示するには、次のようにします。

ステップ 1 [サービス品質] > [QoS 統計情報] > [シングルポリサー統計] をクリックします。

このページには次のフィールドが表示されます。

- [インターフェイス]: このインターフェイスに関する統計情報が表示されます。
- [ポリシー]: このポリシーに関する統計情報が表示されます。
- [クラスマップ]: このクラス マップに関する統計情報が表示されます。
- [プロファイル内バイト]: 受信したプロファイル内バイトの数。

- [アウトオブプロファイルバイト]:受信したアウトオブプロファイル バイトの数。

ステップ 2 [追加] をクリックします。

ステップ 3 パラメータを入力します。

- [インターフェイス]:統計情報を収集する対象のインターフェイスを選択します。
- [ポリシー名]:ポリシー名を選択します。
- [クラスマップ名]:クラス名を選択します。

ステップ 4 [適用] をクリックします。統計情報を求める付加的な要求が作成され、実行コンフィギュレーション ファイルが更新されます。

集約ポリサー統計情報の表示

集約ポリサー統計情報を表示するには、次のようにします。

ステップ 1 [サービス品質] > [QoS 統計情報] > [集約ポリサー統計] をクリックします。

このページには次のフィールドが表示されます。

- [集約ポリサー名]:統計の対象となるポリサー。
- [プロファイル内バイト]:受信されたプロファイル内パケットの数。
- [アウトオブプロファイルバイト]:受信されたアウトオブプロファイル パケットの数。

ステップ 2 [追加] をクリックします。

ステップ 3 統計情報表示の対象となる [集約ポリサー名]、作成済みの集約ポリサーの 1 つを選択します。

ステップ 4 [適用] をクリックします。統計情報を求める付加的な要求が作成され、実行コンフィギュレーション ファイルが更新されます。

キュー統計情報

[キュー統計情報] ページには、転送されたパケットや破棄されたパケットなどのキューに関する統計情報が、インターフェイスごと、キューごと、およびドロップ優先順位ごとに表示されます。

キュー統計情報を表示して、表示する統計情報（カウンタ セット）を定義するには、次のようにします。

ステップ 1 [サービス品質] > [QoS 統計情報] > [キュー統計情報] をクリックします。

このページには次のフィールドが表示されます。

- [リフレッシュレート]: インターフェイス イーサネット統計情報がリフレッシュされるまでの時間を選択します。オプションは次のとおりです。
  - [リフレッシュなし]: 統計情報はリフレッシュされません。
  - [15 秒]: 統計情報は 15 秒ごとにリフレッシュされます。
  - [30 秒]: 統計情報は 30 秒ごとにリフレッシュされます。
  - [60 秒]: 統計情報は 60 秒ごとにリフレッシュされます。

特定のユニットとインターフェイスを表示するには、フィルタでユニット/インターフェイスを選択して、[実行] をクリックします。

特定のインターフェイスを表示するには、フィルタでインターフェイスを選択して、[実行] をクリックします。

キュー統計情報テーブルに、各キューに関する次のフィールドが表示されます。

- [キュー]: パケットが転送またはテール ドロップされたキュー。
- [送信パケット数]: 送信されたパケットの数。
- [テール ドロップ パケット数]: テール ドロップされたパケットの割合。
- [送信バイト数]: 送信されたバイトの数。
- [テール ドロップ バイト数]: テール ドロップされたバイトの割合。

24

SNMP

このセクションでは、ネットワーク デバイスを管理する Simple Network Management Protocol（SNMP）機能について説明します。

具体的な内容は、次のとおりです。

概要

SNMP バージョンとワークフロー

デバイスは SNMP エージェントとして機能し、SNMPv1、v2、および v3 をサポートします。さらに、サポートされる MIB（Management Information Base）で定義されたトラップを使用して、システム イベントをトラップ レシーバに報告します。

SNMPv1 および v2

このシステムへのアクセスを制御するには、コミュニティ エントリのリストを定義します。各コミュニティ エントリは、*コミュニティ ストリング*とそのアクセス権限で構成されています。システムは、適切な権限と適切な動作が設定されたコミュニティを指定する SNMP メッセージにのみ応答します。

SNMP エージェントは、デバイスの管理に使用される変数のリストを維持します。これらの変数は、*Management Information Base*（MIB; 管理情報ベース）内で定義されています。

注 SNMPv3 の使用が推奨されています。他のバージョンにはセキュリティの脆弱性があるためです。

SNMPv3

SNMPv3 では、SNMPv1 および SNMPv2 の機能に加え、SNMPv1 および SNMPv2 の PDU にアクセス制御機構と新しいトラップ機構が適用されてます。また、SNMPv3 では次のような User Security Model（USM）も規定されています。

- **認証**：データの整合性が確保されます。また、データ送信元を認証できます。
- **プライバシー**：メッセージの内容が開示されないように保護することができます。*暗号ブロック連鎖*（CBC-DES）が暗号化に使用されます。SNMP メッセージでは、認証のみを有効にすることも、認証とプライバシーの両方を有効にすることもできます。認証を有効にせずにプライバシーのみを有効にすることはできません。
- **適時性**：メッセージ遅延攻撃やメッセージ再生攻撃を防ぐことができます。SNMP エージェントでは、受信メッセージのタイム スタンプとメッセージ着信時刻が比較されます。

SNMP ワークフロー

注 セキュリティ上の理由から、SNMP はデフォルトで無効になっています。SNMP 経由でデバイスを管理する前に、[TCP/UDP サービス] ページで SNMP を有効にしておく必要があります。

SNMP を設定する際の推奨手順を次に示します。

SNMPv1 または SNMPv2 を使用する場合:

ステップ 1 [コミュニティ] ページに移動して、[追加] をクリックします。コミュニティは、基本モードの場合はアクセス権限とビューに関連付けることができます。拡張モードの場合はグループに関連付けることができます。コミュニティのアクセス権限は次の 2 つの方法で定義できます。

- **基本モード**:コミュニティのアクセス権限は、読み取り専用、読み取りと書き込み、SNMP Admin のいずれかに設定できます。また、[ビュー] ページで定義されたビューを選択することによって、コミュニティへのアクセスを、特定の MIB オブジェクトのみに制限できます。
- **拡張モード**:コミュニティのアクセス権限は、[グループ] ページで定義されたグループによって定義されます。グループには、特定のセキュリティ モデルを設定できます。グループのアクセス権限は、読み取り、書き込み、および通知です。

ステップ 2 SNMP 管理ステーションを 1 つのアドレスに制限するのか、それともすべてのアドレスから SNMP 管理を許可するのかを選択します。SNMP 管理を 1 つのアドレスに制限する場合は、[IP アドレス] フィールドに SNMP 管理 PC のアドレスを入力します。

ステップ 3 [コミュニティストリング] フィールドに一意のコミュニティ ストリングを入力します。

ステップ 4 オプションで、[トラップ設定] ページを使用してトラップを有効にします。

ステップ 5 オプションで、[通知フィルタ] ページを使用して通知フィルタを定義します。

ステップ 6 [SNMPv1.2 通知受信者] ページで通知受信者を設定します。

SNMPv3 を使用する場合:

ステップ 1 [エンジン ID] ページで SNMP エンジンを定義します。一意のエンジン ID を作成するか、またはデフォルトのエンジン ID を使用します。エンジン ID 設定を適用すると、SNMP データベースがクリアされます。

ステップ 2 オプションで、[ビュー] ページで SNMP ビューを定義します。これを指定すると、コミュニティまたはグループで利用できる OID の範囲が制限されます。

ステップ 3 [グループ] ページを使用してグループを定義します。

ステップ 4 [ユーザ] ページを使用してユーザを定義します。ここで、ユーザをグループに関連付けることができます。SNMP エンジン ID が設定されていない場合、ユーザが作成されない可能性があります。

ステップ 5 オプションで、[トラップ設定] ページを使用してトラップを有効または無効にします。

ステップ 6 オプションで、[通知フィルタ] ページを使用して通知フィルタを定義します。

ステップ 7 オプションで、[SNMPv3 通知受信者] ページを使用して通知受信者を定義します。

サポートされる MIB

サポートされる MIB のリストについては、以下の URL にアクセスし、**Cisco MIBS** としてリストされているダウンロード エリアに移動してください。

www.cisco.com/cisco/software/navigator.html

モデル OID

250 ファミリの OID は次のとおりです。

SKU 名	説明	システムオブジェクト ID
F250-24	SF250-24 24 ポート 10/100 スマート スイッチ	9.6.1.98.24.1
SF250-24P	SF250-24P 24 ポート 10/100 PoE スマート スイッチ	9.6.1.98.24.5
SF250-48	SF250-48 48 ポート 10/100 スマート スイッチ	9.6.1.98.24.1
SF250-48HP	SF250-48HP 48 ポート 10/100 PoE スマート スイッチ	9.6.1.98.24.4
SG250-08	SG250-08 8 ポート ギガビット スマート スイッチ	9.6.1.97.8.3
SG250-08HP	SG250-08HP 8 ポート ギガビット PoE スマート スイッチ	9.6.1.97.8.4S
SG250-10P	SG250-10P 10 ポート ギガビット PoE スマート スイッチ	9.6.1.97.10.5

SKU 名	説明	システムオブジェクト ID
SG250-18	SG250-18 18 ポート ギガビット スマート スイッチ	9.6.1.97.18.1
SG250-26	SG250-26 26 ポート ギガビット スマート スイッチ	9.6.1.97.26.1
SG250-26HP	SG250-26HP 26 ポート ギガビット PoE スマート スイッチ	9.6.1.97.26.4
SG250-26P	SG250-26P 26 ポート ギガビット PoE スマート スイッチ	9.6.1.97.26.5
SG250-50	SG250-50 50 ポート ギガビット スマート スイッチ	9.6.1.97.50.1
SG250-50HP	SG250-50HP 50 ポート ギガビット PoE スマート スイッチ	9.6.1.97.50.4
SG250-50P	SG250-50P 50 ポート ギガビット PoE スマート スイッチ	9.6.1.97.50.5
SG250X-24	SG250X-24 24 ポートギガビットおよび 4 ポート 10 ギガビットスマートスイッチ	9.6.1.99.24.1
SG250X-24P	SG250X-24P 24 ポートギガビット PoE 対応および 4 ポート 10 ギガビットスマートスイッチ	9.6.1.99.24.5
SG250X-48	SG250X-48 48 ポート ギガビットおよび 4 ポート 10 ギガビット スマート スイッチ	9.6.1.99.48.1
SG250X-48P	SG250X-48P 48 ポート ギガビット PoE 対応および 4 ポート 10 ギガビット スマート スイッチ	9.6.1.99.48.5

プライベート オブジェクト ID は、enterprises(1).cisco(9).otherEnterprises(6).ciscosb(1).switch001(101) の下に配置されています。

エンジン ID

エンジン ID は、エンティティを一意に識別するために SNMPv3 エンティティで使用されます。SNMP エージェントは、正規の SNMP エンジンであると見なされます。つまり、エージェントは着信メッセージ（Get、GetNext、GetBulk、Set）に応答し、また、トラップ メッセージをマネージャに送信します。エージェントのローカル情報は、メッセージ内のフィールドにカプセル化されます。

各 SNMP エージェントは、SNMPv3 のメッセージ交換で使用されるローカル情報を維持します。デフォルトの SNMP エンジン ID は、企業番号とデフォルトの MAC アドレスで構成されます。このエンジン ID は、管理ドメイン内で一意である必要があります。つまり、1 つのネットワーク上には、同じエンジン ID を持つデバイスは複数台存在しません。

ローカル情報は、読み取り専用の 4 個の MIB 変数（snmpEngineId、snmpEngineBoots、snmpEngineTime、および snmpEngineMaxMessageSize）に格納されます。

注意　エンジン ID を変更すると、設定されていたユーザとグループはすべて消去されます。

SNMP エンジン ID を定義するには、次のようにします。

ステップ 1　[SNMP] > [エンジン ID] の順にクリックします。

ステップ 2　[ローカルエンジン ID] に使用するエンジン ID を選択します。

- [デフォルトを使用]：デバイスによって生成されたエンジン ID を使用する場合に選択します。デフォルトのエンジン ID は、デバイスの MAC アドレスを基にして生成されます。これは、規格ごとに次のように定義されています。
  - *第 1 ～ 4 オクテット*：第 1 ビットは「1」、第 2 ～ 4 ビットは IANA 企業番号です。
  - *第 5 オクテット*：3 に設定されます。これは、続くオクテットが MAC アドレスであることを意味します。
  - *第 6 ～ 11 オクテット*：デバイスの MAC アドレスです。
- [なし]：エンジン ID を使用しません。
- [ユーザ定義]：ローカル デバイスのエンジン ID を入力します。フィールド値は 16 進数文字列で入力します（**範囲：10 ～ 64**）。16 進数文字列の各バイトは 2 桁の 16 進数で表されます。

すべてのリモート エンジン ID とその IP アドレスは、リモート エンジン ID テーブルに表示されます。

ステップ 3 [適用] をクリックします。実行コンフィギュレーション ファイルが更新されます。

リモート エンジン ID テーブルには、エンジンとエンジン ID の IP アドレスの間のマッピングが表示されます。

エンジン ID の IP アドレスを追加するには、次のようにします。

ステップ 4 [追加] をクリックします。次のフィールドを入力します。

- [サーバ指定方法]: エンジン ID サーバを IP アドレスで指定するか、名前で指定するかを選択します。
- [IP バージョン]: サポートする IP 形式を選択します。
- [IPv6 アドレス タイプ]: IPv6 アドレス タイプを選択します（IPv6 が使用される場合）。次のオプションがあります。
  - [リンク ローカル]: IPv6 アドレスによって、単一ネットワーク リンク上のホストが一意に識別されます。リンク ローカル アドレスのプレフィックス部は **FE80** です。このタイプのアドレスはルーティング不能であり、ローカル ネットワーク内で通信する場合にのみ使用できます。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。
  - [グローバル]: IPv6 アドレスは、他のネットワークから認識可能かつアクセス可能なグローバル ユニキャスト IPV6 タイプになります。
- [リンクローカルインターフェイス]: リストからリンク ローカル インターフェイスを選択します（IPv6 アドレス タイプとしてリンク ローカルが選択されている場合）。
- [サーバの IP アドレス/名前]: ログ サーバの IP アドレスまたはドメイン名を入力します。
- [エンジン ID]: エンジン ID を入力します。

ステップ 5 [適用] をクリックします。実行コンフィギュレーション ファイルが更新されます。

ビュー

ビューとは、MIB サブツリーの集合を表すユーザ定義ラベルのことです。各サブツリー ID は、関連するサブツリーのルートの*オブジェクト ID*（OID）が使用されます。目的のサブツリーのルートを指定するには、既知の名前を使用するか、または、OID（「モデル OID」を参照）を入力します。

各サブツリーを定義中のビューに含めるか除外します。

[ビュー] ページでは、SNMP ビューを作成および編集できます。デフォルトのビュー（Default および DefaultSuper）を変更することはできません。

ビューをグループにアタッチするには、[グループ] ページを使用します。基本アクセス モードを使用するコミュニティにアタッチするには、[コミュニティ] ページを使用します。

SNMP ビューを定義するには、次のようにします。

ステップ 1 [SNMP] > [ビュー] の順にクリックします。

ビューごとに次のフィールドが表示されます。

- [オブジェクトIDサブツリー]: ビューに含めるかまたは含めない MIB ツリー内のノード。
- [オブジェクトIDサブツリービュー]: ノードを含めるか含めないか。

ステップ 2 [追加] をクリックして新しいビューを定義します。

ステップ 3 パラメータを入力します。

- [ビュー名]: 0 ～ 30 文字でビューの名前を入力します。
- [オブジェクトIDサブツリー]: 選択した SNMP ビューに含めるかまたは除外する MIB ツリー内のノードを選択します。オブジェクトの選択方法には次のものがあります。
  - [リストから選択]: MIB ツリー内を探索できます。選択されているノードの親または兄弟のレベルに移動するには、上矢印ボタンを押します。選択されているノードの子のレベルに移動するには、下矢印ボタンを押します。ノードからその兄弟ノードに移動するには、ビューでそのノードをクリックします。兄弟ノードがビューに表示されていない場合は、スクロールバーを使用します。
  - [ユーザ定義]: [リストから選択] オプションにない OID を入力します。

ステップ 4 [ビューに含める] を選択または選択解除します。これを選択した場合、選択された MIB がビューに組み込まれます。選択しなかった場合は、除外されます。

ステップ 5 [適用] をクリックします。

ステップ 6 ビューの設定を確認するために、[フィルタ] の[ビュー名] リストでユーザ定義ビューを選択します。デフォルトで存在するビューは次のとおりです。

- [デフォルト]:読み取りビューおよび読み取り/書き込みビュー用のデフォルトの SNMP ビュー。
- [DefaultSuper]:管理ビュー用のデフォルトの SNMP ビュー。

グループ

SNMPv1 および SNMPv2 では、SNMP フレームとともにコミュニティ ストリングが送信されます。コミュニティ ストリングは、SNMP エージェントへのアクセス権限を取得するためのパスワードの役割を果たします。ただし、フレームもコミュニティ ストリングも暗号化されません。そのため、SNMPv1 および SNMPv2 は安全ではありません。

SNMPv3 では、次のセキュリティ機構を設定できます。

- **認証**:デバイスで、SNMP ユーザが正規のシステム管理者であるかどうかを検査します。この検査は、フレームごとに実行されます。
- **プライバシー**:SNMP フレームで暗号化データを送信することができます。

それで、SNMPv3 では、次の 3 段階のセキュリティ レベルがあります。

- セキュリティなし(認証なし、プライバシーなし)
- 認証(認証あり、プライバシーなし)
- 認証およびプライバシー

SNMPv3 では、各ユーザが読み取りまたは書き込みをできる内容およびユーザが受け取る通知を制御する方法が提供されます。グループは、読み取り/書き込み権限およびセキュリティ レベルを定義します。グループが機能するのは、そのグループに SNMP ユーザまたはコミュニティが関連付けられている場合です。

注 グループにデフォルトでないビューを関連付けるには、まず [ビュー] ページでビューを作成します。

SNMP グループを作成するには、次のようにします。

ステップ 1 [SNMP] > [グループ] の順にクリックします。

このページには、既存の SNMP グループとそのセキュリティ レベルが含まれています。

ステップ 2 [追加] をクリックします。

ステップ 3 パラメータを入力します。

- [グループ名]: 新しいグループ名を入力します。
- [セキュリティモデル]: このグループに関連付ける SNMP バージョン（SNMPv1、SNMPv2、または SNMPv3）を選択します。

さまざまなセキュリティ レベルと組み合わせて 3 種類のビューを定義できます。各セキュリティ レベルごとに、以下のフィールドを入力して、読み取り、書き込み、通知用のビューを選択します。

- [有効]: セキュリティ レベルを有効にする場合にこのフィールドを選択します。
- [セキュリティレベル]: グループに関連付けるセキュリティ レベルを定義します。SNMPv1 と SNMPv2 は、認証とプライバシーのどちらもサポートしません。SNMPv3 を選択した場合は、次のいずれかを選択します。
  - [認証なし、プライバシーなし]: [認証] と [プライバシー] のどちらのセキュリティ レベルもグループに割り当てません。
  - [認証、プライバシーなし]: SNMP メッセージを認証し、SNMP メッセージの送信元を認証しますが、それらを暗号化しません。
  - [認証、プライバシー]: SNMP メッセージを認証し、それらを暗号化します。
- [ビュー]: ビューにグループの読み取り、書き込み、通知のアクセス権限を関連付けることにより、グループが読み取り、書き込み、および通知アクセス権限を持つ MIB ツリーの範囲が制限されます。
  - [読み取り]: 選択したビューに対する管理アクセス権限は、読み取り専用です。それ以外の場合、このグループに関連付けられたユーザまたはコミュニティは、SNMP 自体を制御する MIB を除くすべての MIB を読み取ることができます。
  - [書き込み]: 選択したビューに対する管理アクセス権限は、書き込みです。それ以外の場合、このグループに関連付けられたユーザまたはコミュニティは、SNMP 自体を制御する MIB を除くすべての MIB に書き込むことができます。

- [通知]:利用可能なトラップの内容を、選択したビューに含まれるものだけに制限します。それ以外の場合、トラップに含まれる内容に制限はありません。このフィールドは、SNMPv3 の場合のみ選択できます。

ステップ 4 [適用] をクリックします。SNMP グループは実行コンフィギュレーション ファイルに保存されます。

ユーザ

SNMP ユーザを定義するには、ログイン資格情報(ユーザ名、パスワード、および認証方式)、および、コンテキストとスコープを設定します。このコンテキストとスコープの中で、ユーザはグループおよびエンジン ID と関連付けられます。

設定されたユーザには、そのグループの属性が設定され、関連付けられたビュー内でアクセス権限が設定されます。

グループを使用した場合、ネットワーク管理者は、アクセス権限を 1 人のユーザではなくユーザのグループに割り当てることができます。

各ユーザは、1 つのグループにしか所属できません。

SNMPv3 ユーザを作成するには、次の条件が満たされている必要があります。

- このデバイス上でエンジン ID が設定されていること。この作業は [エンジン ID] ページで行います。
- SNMPv3 グループを使用できること。SNMPv3 グループを定義するには、[グループ] ページを使用します。

SNMP ユーザを表示したり、新規に定義したりするには、次のようにします。

ステップ 1 [SNMP] > [ユーザ] の順にクリックします。

このページには、既存のユーザが表示されます。このページ内のフィールドは [追加] ページで説明されます。ただし、次のフィールドを除きます。

- [IP アドレス]:エンジンの IP アドレスが表示されます。

ステップ 2 [追加] をクリックします。

このページでは、SNMP アクセス制御権限を SNMP ユーザに割り当てるための情報が提供されます。

ステップ 3 パラメータを入力します。

- [ユーザ名]:ユーザの名前を入力します。
- [エンジン ID]:このユーザが接続する SNMP エンティティが、ローカルとリモートのどちらであるかを選択します。ローカル SNMP エンジン ID を変更または削除すると、SNMPv3 ユーザ データベースが削除されます。インフォーム要求メッセージを受信したり情報を要求したりするには、ローカル ユーザとリモート ユーザの両方を作成する必要があります。
  - [ローカル]:ユーザはローカル デバイスに接続されます。
  - [リモート IP アドレス]:ユーザはローカル デバイスに加えて別の SNMP エンティティに接続されます。リモート エンジン ID が定義されている場合、リモート デバイスはインフォーム要求メッセージを受信しますが、情報を要求することはできません。

    リモート エンジン ID を入力します。
- [グループ名]:この SNMP ユーザを所属させる SNMP グループを選択します。SNMP グループは、[グループの追加] ページで定義します。

  注 削除されたグループに所属するユーザはそのまま残りますが、非アクティブになります。
- [認証方式]:認証方式を選択します。割り当てられたグループ名に応じて、認証方式が変わります。グループが認証を要求しない場合、そのユーザは、いずれの認証も設定することはできません。次のオプションがあります。
  - [なし]:ユーザ認証を行いません。
  - [MD5]:MD5 認証方式でキーを生成するために使用されるパスワード。
  - [SHA]:SHA(Secure Hash Algorithm)認証方式でキーを生成するために使用されるパスワード。
- [認証パスワード]:MD5 パスワードまたは SHA パスワードを使用して認証を行う場合は、ローカル ユーザ パスワードを [暗号化] または [プレーンテキスト] のいずれかに入力します。ローカル ユーザ パスワードは、ローカル データベースと照合されます。ASCII 文字 32 字以内で入力します。
- [プライバシー方式]:次のいずれかのオプションを選択します。
  - [なし]:プライバシー パスワードは暗号化されません。
  - [DES]:プライバシー パスワードは、DES(Data Encryption Standard)に従って暗号化されます。

- [プライバシーパスワード]:DES プライバシー方式が選択されている場合、16 バイトが必要です(DES 暗号化キー)。このフィールドは、ちょうど 32 文字の 16 進数でなければなりません。[暗号化] または [プレーンテキスト] モードを選択できます。

ステップ 4 [適用] をクリックし、設定を保存します。

コミュニティ

SNMPv1 および SNMPv2 におけるアクセス権限を管理するには、[コミュニティ] ページでコミュニティを定義します。コミュニティ名は、SNMP 管理ステーションとデバイスの間で共有されるパスワードのようなものです。これは、SNMP 管理ステーションを認証する目的で使用されます。

コミュニティを定義するのは、SNMPv1 と SNMPv2 の場合のみです。SNMPv3 では、コミュニティの代わりにユーザを使用します。ユーザはグループに所属し、そのグループにアクセス権限が割り当てられます。

[コミュニティ] ページでは、直接(基本モード)またはグループを介して(拡張モード)、コミュニティにアクセス権限が関連付けられます。

- **基本モード**:コミュニティのアクセス権限は、読み取り専用、読み取りと書き込み、SNMP Admin のいずれかに設定できます。また、[ビュー] ページで定義されたビューを選択することによって、コミュニティへのアクセスを、特定の MIB オブジェクトのみに制限できます。
- **拡張モード**:コミュニティのアクセス権限は、[グループ] ページで定義されたグループによって定義されます。グループには、特定のセキュリティ モデルを設定できます。グループのアクセス権限は、読み取り、書き込み、および通知です。

SNMP コミュニティを定義するには、次のようにします。

ステップ 1 [SNMP] > [コミュニティ] の順にクリックします。

このページには、設定された SNMP コミュニティとそのプロパティに関する表が表示されます。このページ内のフィールドは [追加] ページで説明されます。ただし、次のフィールドを除きます。

- [コミュニティタイプ]:コミュニティのモードが表示されます([基本] または [拡張])。

ステップ 2 [追加] をクリックします。

このページで、ネットワーク管理者は新しい SNMP コミュニティを定義および設定することができます。

ステップ 3 [SNMP 管理ステーション]:SNMP コミュニティにアクセスできる管理ステーションの IP アドレスを入力するには、[ユーザ定義] をクリックします。どの IP デバイスもこの SNMP コミュニティにアクセスできるようにするには、[すべて] をクリックします。

- [IP バージョン]:IPv4 または IPv6 を選択します。
- [IPv6 アドレスタイプ]:サポートされる IPv6 アドレス タイプを選択します（IPv6 が使用される場合）。次のオプションがあります。
  - [リンク ローカル]:IPv6 アドレスによって、単一ネットワーク リンク上のホストが一意に識別されます。リンク ローカル アドレスのプレフィックス部は **FE80** です。このタイプのアドレスはルーティング不能であり、ローカル ネットワーク内で通信する場合にのみ使用できます。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。
  - [グローバル]:IPv6 アドレスは、他のネットワークから認識可能かつアクセス可能なグローバル ユニキャスト IPV6 タイプになります。
- [リンクローカルインターフェイス]:IPv6 アドレス タイプがリンク ローカルの場合、VLAN と ISATAP のどちらから IPv6 アドレスを受け取るかを選択します。
- [IP アドレス]:SNMP 管理ステーションの IP アドレスを入力します。
- [コミュニティストリング]:デバイスに対する管理ステーションの認証に使用するコミュニティ名を入力します。
- [(コミュニティタイプ)基本]:このコミュニティ タイプでは、どのグループへも接続されません。選択できるのは、コミュニティ アクセス レベル（読み取り、読み取りと書き込み、または SNMP Admin）のみで、さらに任意で特定のビュー用に修飾することができます。デフォルトでは、MIB 全体に適用されます。これを選択した場合、次の各フィールドを入力します。
  - [アクセスモード]:このコミュニティのアクセス権限を選択します。次のオプションがあります。

    [読み取り専用]:管理アクセス権限は読み取り専用に制限されます。コミュニティに変更を加えることはできません。

[読み取りと書き込み]:管理アクセス権限は読み取りと書き込みです。デバイス コンフィギュレーションに変更を加えることはできますが、コミュニティに変更を加えることはできません。

[SNMP Admin]:ユーザは、すべてのデバイス コンフィギュレーション オプションにアクセスできます。また、コミュニティを修正するアクセス許可が与えられます。SNMP Admin は、SNMP MIB を除くすべての MIB の読み取りと書き込みと同等です。SNMP Admin は、SNMP MIB にアクセスする際に必要です。

- [ビュー名]:SNMP ビュー(アクセスが付与されている MIB サブツリーの集合)を選択します。

- [(コミュニティタイプ)拡張]:選択されたコミュニティに対してこのタイプを選択します。
  - [グループ名]:SNMP グループを選択します。このグループによってアクセス権限が決まります。

ステップ 4 [適用] をクリックします。SNMP コミュニティが定義され、実行コンフィギュレーションが更新されます。

トラップ設定

[トラップ設定] ページでは、デバイスから SNMP 通知を送信するかどうか、および、いつ通知を送信するかを設定できます。SNMP 通知の受信者を設定するには、[SNMPv1.2 通知受信者] ページまたは [SNMPv3 通知受信者] ページを使用します。

トラップ設定を定義するには、次のようにします。

ステップ 1 [SNMP] > [トラップ設定] の順にクリックします。

ステップ 2 このデバイスから SNMP 通知を送信できるように指定するには、[SNMP通知] で [有効] を選択します。

ステップ 3 SNMP 認証失敗時の通知を有効にするには、[認証通知] で [有効] を選択します。

ステップ 4 [適用] をクリックします。SNTP トラップ設定が実行コンフィギュレーション ファイルに書き込まれます。

通知受信者

RFC 1215 で規定されているように、トラップ メッセージは、システム イベントを報告するために生成されます。このシステムでは、サポート対象の MIB で定義されるトラップを生成できます。

トラップ受信者（通知受信者）は、デバイスからトラップ メッセージが送信されるネットワーク ノードです。通知受信者のリストを定義できます。

トラップ受信者エントリは、ノードの IP アドレス、および、トラップ メッセージに格納されるバージョンに対応する SNMP 資格情報で構成されています。トラップ メッセージの送信が必要なイベントが発生した場合、通知受信者テーブル内のすべてのノードに送信されます。

[SNMPv1.2 通知受信者] ページおよび [SNMPv3 通知受信者] ページでは、SNMP 通知の宛先、および、各宛先に送信する SNMP 通知の種類（トラップまたはインフォーム要求）を設定できます。[追加] ポップアップ ウィンドウおよび [編集] ポップアップ ウィンドウでは、通知の属性を設定できます。

SNMP 通知は、デバイスから SNMP 管理ステーションに送信されるメッセージであり、リンク アップ、リンク ダウンなど、何らかのイベントが発生したことを意味します。

特定の通知をフィルタリングすることもできます。これを行うには、[通知フィルタ] ページでフィルタを作成し、それを SNMP 通知受信者にアタッチします。通知フィルタを使用することにより、送信する通知の OID に基づいて、管理ステーションに送信する SNMP 通知の種類をフィルタリングできます。

SNMPv1.2 通知受信者

SNMPv1、v2 の受信者を定義するには、次のようにします。

ステップ 1 [SNMP] > [通知受信者 SNMPv1、2] の順にクリックします。

このページには、SNMPv1、v2 の受信者が表示されます。

ステップ 2 次のフィールドを入力します。

- [IPv4 送信元インターフェイスを通知する]：IPv4 SNMP サーバとの通信に使用するインフォーム要求メッセージ内で、IPv4 アドレスをソース IPv4 アドレスとして使用する送信元インターフェイスを選択します。
- [IPv6 送信元インターフェイスをトラップする]：IPv4 SNMP サーバとの通信に使用するトラップ メッセージ内で、IPv6 アドレスをソース IPv6 アドレスとして使用する送信元インターフェイスを選択します。

- [IPv6 送信元インターフェイスを通知する]:IPv4 SNMP サーバとの通信に使用するインフォーム要求メッセージ内で、IPv4 アドレスをソース IPv4 アドレスとして使用する送信元インターフェイスを選択します。
- [IPv6 送信元インターフェイスをトラップする]:IPv6 SNMP サーバとの通信に使用するトラップ メッセージ内で、IPv6 アドレスをソース IPv6 アドレスとして使用する送信元インターフェイスを選択します。

  注 [自動] オプションが選択されている場合、システムは、発信インターフェイスで定義された IP アドレスからソース IP アドレスを取得します。

ステップ 3 [追加] をクリックします。

ステップ 4 パラメータを入力します。

- [サーバ指定方法]:リモート ログ サーバを IP アドレスで指定するか、名前で指定するかを選択します。
- [IP バージョン]:IPv4 または IPv6 を選択します。
- [IPv6 アドレスタイプ]:[リンクローカル] または [グローバル] を選択します。
  - [リンク ローカル]:IPv6 アドレスによって、単一ネットワーク リンク上のホストが一意に識別されます。リンク ローカル アドレスのプレフィックス部は **FE80** です。このタイプのアドレスはルーティング不能であり、ローカル ネットワーク内で通信する場合にのみ使用できます。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。
  - [グローバル]:IPv6 アドレスは、他のネットワークから認識可能かつアクセス可能なグローバル ユニキャスト IPV6 タイプになります。
- [リンクローカルインターフェイス]:IPv6 アドレス タイプがリンク ローカルの場合、VLAN と ISATAP のどちらから IPv6 アドレスを受け取るかを選択します。
- [受信者の IP アドレス/名前]:トラップの送信先の IP アドレスまたはサーバ名を入力します。
- [UDP ポート]:受信デバイス側で通知に使用される UDP ポートを入力します。
- [通知タイプ]:トラップとインフォーム要求のどちらを送信するかを選択します。両方とも送信する必要がある場合は、受信者を 2 つ作成する必要があります。
- [タイムアウト]:デバイスがインフォーム要求を再送信するまでの待機時間を秒数で入力します。
- [リトライ回数]:デバイスがインフォーム要求を再送信する回数を入力します。

- [コミュニティ ストリング]:プルダウンからトラップ マネージャのコミュニティ ストリングを選択します。コミュニティ ストリング名は、[コミュニティ] ページにリストされた名前から生成されます。
- [通知バージョン]:トラップの SNMP バージョンを選択します。SNMPv1 と SNMPv2 のいずれかをトラップのバージョンとして使用できます。一度に有効にできるのは 1 つのバージョンのみです。
- [通知フィルタ]:管理ステーションに送信する SNMP 通知の種類をフィルタリングする場合に選択します。フィルタは、[通知フィルタ] ページで作成します。
- [フィルタ名]:トラップに含める情報を定義した SNMP フィルタ ([通知フィルタ] ページで定義) を選択します。

ステップ 5 [適用] をクリックします。SNTP 通知受信者設定が実行コンフィギュレーション ファイルに書き込まれます。

SNMPv3 通知受信者

SNMPv3 の受信者を定義するには、次のようにします。

ステップ 1 [SNMP] > [通知受信者 SNMPv3] の順にクリックします。

このページには、SNMPv3 の受信者が表示されます。

- [IPv4 送信元インターフェイスを通知する]:IPv4 SNMP サーバとの通信に使用するインフォーム要求メッセージ内で、IPv4 アドレスをソース IPv4 アドレスとして使用する送信元インターフェイスを選択します。
- [IPv6 送信元インターフェイスをトラップする]:IPv4 SNMP サーバとの通信に使用するトラップ メッセージ内で、IPv6 アドレスをソース IPv6 アドレスとして使用する送信元インターフェイスを選択します。
- [IPv6 送信元インターフェイスを通知する]:IPv4 SNMP サーバとの通信に使用するインフォーム要求メッセージ内で、IPv4 アドレスをソース IPv4 アドレスとして使用する送信元インターフェイスを選択します。
- [IPv6 送信元インターフェイスをトラップする]:IPv6 SNMP サーバとの通信に使用するトラップ メッセージ内で、IPv6 アドレスをソース IPv6 アドレスとして使用する送信元インターフェイスを選択します。

ステップ 2 [追加] をクリックします。

ステップ 3 パラメータを入力します。

- [サーバ指定方法]:リモート ログ サーバを IP アドレスで指定するか、名前で指定するかを選択します。
- [IP バージョン]:IPv4 または IPv6 を選択します。
- [IPv6 アドレス タイプ]:IPv6 アドレス タイプを選択します(IPv6 が使用される場合)。次のオプションがあります。
  - [リンク ローカル]:IPv6 アドレスによって、単一ネットワーク リンク上のホストが一意に識別されます。リンク ローカル アドレスのプレフィックス部は **FE80** です。このタイプのアドレスはルーティング不能であり、ローカル ネットワーク内で通信する場合にのみ使用できます。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。
  - [グローバル]:IPv6 アドレスは、他のネットワークから認識可能かつアクセス可能なグローバル ユニキャスト IPV6 タイプになります。
- [リンクローカルインターフェイス]:プルダウン リストからリンク ローカル インターフェイスを選択します(IPv6 アドレス タイプとしてリンク ローカルが選択されている場合)。
- [受信者の IP アドレス/名前]:トラップの送信先の IP アドレスまたはサーバ名を入力します。
- [UDP ポート]:受信デバイス側で通知に使用される UDP ポートを入力します。
- [通知タイプ]:トラップとインフォーム要求のどちらを送信するかを選択します。両方とも送信する必要がある場合は、受信者を 2 つ作成する必要があります。
- [タイムアウト]:デバイスがインフォーム要求またはトラップを再送信するまでの待機時間を秒数で入力します。タイムアウト:範囲:1 ～ 300、デフォルト:15
- [リトライ回数]:デバイスがインフォーム要求を再送信する回数を入力します。リトライ回数:範囲:1 ～ 255、デフォルト:3
- [ユーザ名]:ドロップダウン リストから SNMP 通知送信先ユーザを選択します。通知を受け取るには、このユーザが [ユーザ] ページで定義されていて、そのエンジン ID がリモートである必要があります。
- [セキュリティ レベル]:パケットに適用する認証のレベルを選択します。

注 このセキュリティ レベルは、選択したユーザ名によって異なります。このユーザ名が認証なしとして設定された場合、[セキュリティレベル] の選択肢は [認証なし] のみです。ただし、[ユーザ] ページでこのユーザ名に認証およびプライバシーが割り当てられた場合、この画面のセキュリティ レベルの選択肢は、認証なし、認証のみ、または認証とプライバシーのいずれかになります。

次のオプションがあります。

- [認証なし]:パケットに対して認証処理も暗号化処理も実行されません。
- [認証]:パケットに対して認証処理は実行されますが、暗号化処理は実行されません。
- [プライバシー]:パケットに対して認証処理と暗号化処理の両方が実行されます。

- [通知フィルタ]:管理ステーションに送信する SNMP 通知の種類をフィルタリングする場合に選択します。フィルタは、[通知フィルタ] ページで作成します。
- [フィルタ名]:トラップに含める情報を定義した SNMP フィルタ([通知フィルタ] ページで定義)を選択します。

ステップ 4 [適用] をクリックします。SNTP 通知受信者設定が実行コンフィギュレーション ファイルに書き込まれます。

通知フィルタ

[通知フィルタ] ページでは、SNMP 通知フィルタ、および、検査される OID を設定できます。通知フィルタを作成したら、[SNMPv1.2 通知受信者] ページおよび [SNMPv3 通知受信者] ページで、通知受信者にアタッチすることができます。

通知フィルタを使用することにより、送信する通知の OID に基づいて、管理ステーションに送信する SNMP 通知の種類をフィルタリングできます。

通知フィルタを定義するには、次のようにします。

ステップ 1 [SNMP] > [通知フィルタ] の順にクリックします。

[通知フィルタ] ページでは、フィルタごとに通知情報が表示されます。[フィルタ名] を使用して、このテーブル内の通知エントリをフィルタリングすることができます。

ステップ 2 [追加] をクリックします。

ステップ 3 パラメータを入力します。

- [フィルタ名]:0 ～ 30 文字で名前を入力します。
- [オブジェクトIDサブツリー]:選択した SNMP フィルタに含めるかまたは除外する MIB ツリー内のノードを選択します。オブジェクトの選択方法には次のものがあります。
  - [リストから選択]:MIB ツリー内を探索できます。選択されているノードの親または兄弟のレベルに移動するには、上矢印ボタンを押します。選択されているノードの子のレベルに移動するには、下矢印ボタンを押します。ノードからその兄弟ノードに移動するには、ビューでそのノードをクリックします。兄弟ノードがビューに表示されていない場合は、スクロールバーを使用します。
  - [オブジェクトID] を使用する場合、[フィルタに含める] オプションが選択されていると 、**入力したオブジェクト ID** がビューに表示されます。

ステップ 4 [フィルタに含める] を選択または選択解除します。これを選択した場合、選択された MIB がフィルタに組み込まれます。選択しなかった場合は、除外されます。

ステップ 5 [適用] をクリックします。SNMP ビューが定義され、実行コンフィギュレーションが更新されます。