アドミニストレーション ガイド

Cisco Small Business

SG200 シリーズ 8 ポート スマート スイッチ

目　次

第 1 章 : はじめに 8

Web ベースのスイッチ設定ユーティリティの開始 8

ユーティリティの起動 9

ログイン 9

ログアウト 10

クイック スタート デバイス コンフィギュレーション 10

ウィンドウ ナビゲーション 11

アプリケーション ヘッダー 11

その他のリソース 12

ナビゲーション ウィンドウ 13

管理ボタン 13

第 2 章 : 統計情報の表示 16

システムの要約 16

システムの要約の表示 16

システム設定の指定 19

インターフェイス統計情報 20

Etherlike 統計情報 21

802.1X EAP 統計情報 22

IPv6 DHCP 統計情報 23

RADIUS 統計情報 24

統計情報 25

ログ 26

RAM メモリ ログ 27

フラッシュ メモリ ログ 28

第 3 章 : 各種管理 30

システム設定の指定 31

管理インターフェイス 32

IPv4 管理インターフェイスの設定 32

IPv6 管理インターフェイスの設定 34

IPv6 アドレスの追加 35

IPv6 デフォルト ルータ テーブル 36
IPv6 ネイバーの表示と追加 36
ユーザ アカウントの管理 37
ユーザの追加 37
ユーザ パスワードの変更 39
ユーザの削除 39
管理サービスの有効化 40
アイドル セッション タイムアウトの設定 40
ログイン セッション 41
ログイン履歴 41
時間設定 42
システムの時刻の設定 42
SNTP 設定の指定 44
SNTP 認証の設定 47
システム ログ 49
ログ設定の指定 49
リモート ログ サーバの設定 50
ファイル管理 51
ファームウェアと言語ファイルのアップグレードとバックアップ 53
コンフィギュレーション ファイルとログファイルのダウンロードとバックアップ 54
コンフィギュレーション ファイルのダウンロードによる設定の復元 55
コンフィギュレーション ファイルとログのバックアップ 56
コンフィギュレーションの削除 57
コンフィギュレーション ファイルのコピーと保存 58
DHCP 自動コンフィギュレーション 59
概要 59
DHCP サーバのメッセージの詳細 60
代替 TFTP サーバとファイル名 61
コンフィギュレーション ファイルのダウンロードの詳細 61
DHCP 自動コンフィギュレーションの設定 64
HTTP 経由でのファームウェア リカバリ 66
スイッチのリブート 67
ホストの Ping 68

制御パケットの転送の設定 69
診断 70
カッパー ポートのテスト 70
ポート ミラーリングの設定 71
CPU/ メモリ利用率 73
Bonjour の有効化 74
LLDP-MED 75
グローバル LLDP-MED プロパティの設定 75
ポートでの LLDP-MED の設定 76
LLDP-MED ポート ステータスの詳細 78
LLDP-MED ネイバー情報 79
DHCP クライアント ベンダー オプションの設定 81

第 4 章 : ポートの管理 83

ポート設定の指定 83
リンク アグリゲーション 85
LAG の設定 85
LAG 情報の設定 86
LACP 情報の設定 87
PoE の設定 88
PoE プロパティの設定 89
PoE ポート設定の指定 90
Green Ethernet 92
Green Ethernet プロパティの設定 93
Green Ethernet ポート設定の指定 94

第 5 章 : VLAN 管理 96

VLAN の作成 97
VLAN インターフェイスの設定 98
インターフェイス VLAN モードの変更 100
VLAN メンバシップの設定 101
VLAN へのポートの設定 102

ポート VLAN メンバシップの設定 103
デフォルト VLAN の設定 104
音声とメディア 105
テレフォニー OUI の表示と追加 106
OUI ベースの音声とメディアの設定 106
SIP/H323 ベースの音声とメディアの設定 107
メディア VLAN 108
自動 VoIP セッション 110

第 6 章 : スパニング ツリー 111

スパニング ツリーの概要 111
STP のステータスとグローバル情報の設定 112
グローバル情報とブリッジの設定 112
STP インターフェイスの設定 114
RSTP インターフェイス設定 116

第 7 章 : MAC アドレス テーブル 118

スタティック MAC アドレスの設定 118
ダイナミック アドレスのエージング タイムの設定 120
ダイナミック MAC アドレス 120

第 8 章 : マルチキャスト 122

マルチキャスト プロパティ 123
すべての VLAN でのマルチキャスト転送モードの設定 123
個々の VLAN でのマルチキャスト プロパティの設定 124
MAC グループ アドレスの設定 124
MAC グループ アドレス テーブルの表示 125
スタティックな MAC グループ アドレス テーブル エントリの追加 125
MAC アドレス グループ ポート メンバシップの設定 126
IGMP スヌーピングの設定 126
MLD スヌーピングの設定 128
IGMP マルチキャスト ルータ インターフェイスの設定 130

MLD マルチキャスト ルータ インターフェイスの設定 131

第 9 章 : IP コンフィギュレーション 132

ARP テーブル 132

ドメイン ネーム システム 133

DNS サーバの設定 133

グローバル DNS の設定 133

DNS サーバの追加 134

ホスト名マッピング 134

スタティック DNS マッピングの設定 134

ダイナミック DNS エントリの表示と削除 135

第 10 章 : セキュリティ 136

RADIUS 136

グローバル RADIUS の設定 137

RADIUS サーバの追加 137

パスワード強度 139

管理アクセス プロファイル ルール 140

アクセス プロファイルとルールの設定 140

アクセス プロファイルおよびルールの修正と削除 142

認証方式 143

ストーム制御 144

ポート セキュリティ 145

ポート セキュリティの有効化 146

セキュア MAC アドレスの表示と設定 147

802.1X 148

802.1X プロパティ値の設定 149

ポート PAE 機能の変更 150

ポート認証の設定 150

サプリカント ポート認証の設定 152

認証済みホストの表示 153

第 11 章 : Quality of Service 154

QoS プロパティ 155

キューの定義 156

キュー設定の推奨事項 157

キューの設定 157

CoS/802.1p プライオリティのキューへのマッピング 158

IP Precedence のキューへのマッピング 159

DSCP 値のキューへのマッピング 160

レート制限プロファイルの定義 161

レート制限プロファイルのインターフェイスへの適用 162

トラフィック シェーピング 163

1

はじめに

この章では、Web ベースのスイッチ設定ユーティリティの概要について説明します。具体的な内容は次のとおりです。

- 「Web ベースのスイッチ設定ユーティリティの開始」
- 「クイック スタート デバイス コンフィギュレーション」
- 「ウィンドウ ナビゲーション」

Web ベースのスイッチ設定ユーティリティの開始

ここでは、Web ベースのスイッチ設定ユーティリティ内の移動方法について説明します。

ブラウザには次の制約事項があります。

- Internet Explorer 8 を使用している場合は、ブラウザ ウィンドウを開いて、次の設定を行います。

  [ツール] > [インターネット オプション] の順にクリックし、[セキュリティ] タブを選択します。[ローカル イントラネット] を選択して、[サイト] をクリックします。[詳細設定] をクリックして、[追加] をクリックします。スイッチのイントラネット アドレス（http://<ip-address>）をローカル イントラネット ゾーンに追加します。IP アドレスをサブネット IP アドレスとして指定して、サブネット内のすべてのアドレスをローカル イントラネット ゾーンに追加することもできます。

- Internet Explorer 6 を使用している場合、IPv6 アドレスで直接スイッチにアクセスすることはできません。ただし、Domain Name System（DNS; ドメイン ネーム システム）サーバを使用して、IPv6 アドレスを含むドメイン名を作成し、そのドメイン名を IPv6 アドレスの代わりにアドレス バーに指定することはできます。

- 管理ステーションに複数の IPv6 インターフェイスがある場合、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、ブラウザからスイッチにアクセスしてください。

ユーティリティの起動

Web ベースのスイッチ設定ユーティリティを開くには、次の手順に従います。

ステップ 1 Web ブラウザを開きます。

ステップ 2 ブラウザのアドレス バーに、設定するスイッチの IP アドレスを入力し、Enter キーを押します。[ログイン] ページが開きます。

ログイン

Web ベースのスイッチ設定ユーティリティにログインするには、次の手順に従います。

ステップ 1 ユーザ名とパスワードを入力します。工場出荷時の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。

注：工場出荷時のデフォルト設定でスイッチが起動すると、Web ベースのスイッチ設定ユーティリティがデフォルトの言語で表示されます。ログインした後に、[ファームウェア / 言語のアップグレード / バックアップ] ページを使用して追加の言語をダウンロードできます。

ステップ 2 これが、デフォルト ユーザ名（**cisco**）とデフォルト パスワード（**cisco**）を使用した初めてのログインである場合、またはパスワードの有効期限が切れている場合、[パスワードの変更] ページが開きます。新しいパスワードを入力して、確認のために再入力し、[適用] をクリックして、[閉じる] をクリックします。新しいパスワードが保存されます。('、"、%、? の各文字はサポートされていません)。

ステップ 3 [ログイン] をクリックします。

ログインが成功すると、[はじめに] ページが開きます。

間違ったユーザ名またはパスワードを入力すると、エラー メッセージが表示され、[ログイン] ページのままになります。

[起動時にこのページを表示しない] を選択し、ログインのたびに [はじめに] ページが表示されないようにします。このオプションを選択すると、[はじめに] ページの代わりに [システムの要約] ページが開きます。

ログアウト

デフォルトで、ユーザは 10 分間非アクティブな状態が続くとアプリケーションから自動的にログアウトされるようになっています。デフォルトのタイムアウト時間を変更する手順については、**「アイドル セッション タイムアウトの設定」**を参照してください。

ページ右上隅の [ログアウト] をクリックして、いつでもログアウトすることができます。

注意 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 タイプにコピーされていない限り、スイッチをリブートすると、前回ファイル タイプが保存された以降の変更はすべて失われます。ログオフする前に、そのセッションで行った変更が保持されるように、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 ファイル タイプに保存しておくことを推奨します。

[保存] ボタンの左に赤い X アイコンが表示されている場合、実行コンフィギュレーションが変更されており、かつそれらがスタートアップ コンフィギュレーション ファイル タイプにまだ保存されていないことを示しています。

[保存] をクリックすると、ページが表示されます（**「コンフィギュレーション ファイルとログファイルのダウンロードとバックアップ」**を参照）。スタートアップ コンフィギュレーション ファイル タイプにコピーすることにより、実行コンフィギュレーションを保存します。この保存の後、赤い **X** アイコンと [保存] ボタンが表示されなくなります。

クイック スタート デバイス コンフィギュレーション

クイック ナビゲーションにより、簡単にデバイス コンフィギュレーションを実行できるように、[はじめに] ページには、使用頻度の高いページへのリンクが用意されています。

[はじめに] ページのリンク

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]	[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 の作成]
	[ポート設定]	[ポート設定]

[はじめに] ページのリンク （続き）

カテゴリ	リンク名（ページ上）	リンク ページ
[デバイス ステータス]	[システムの要約]	[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]
	[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 / 言語のアップグレード / バックアップ]
	[デバイスコンフィギュレーションのバックアップ]	[コンフィギュレーション / ログのダウンロード / バックアップ]
	[QoS の設定]	[QoS プロパティ]
	[ポートミラーリングの設定]	[ポートミラーリング]

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について説明します。

アプリケーション ヘッダー

すべてのページにアプリケーション ヘッダーが表示されます。次のボタンが含まれています。

ボタン

ボタン名	説明
	Syslog アラート ステータス ボタン（赤い円に **X**）は、重大度が重要より上の新しい Syslog メッセージが記録されると表示されます。クリックすると、[ステータスと統計情報] > [ログの表示] > [RAM メモリ ログ] ページが開きます。このページにアクセスした後は、Syslog アラート ステータス ボタンは表示されなくなります。

ボタン （続き）

ボタン名	説明
	[保存] ボタンの左側にある赤い **X** アイコンは、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。 このボタンをクリックすると、[コンフィギュレーション / ログのダウンロード / バックアップ] ページが表示されます。スタートアップ コンフィギュレーション ファイル タイプにコピーすることにより、実行コンフィギュレーションを保存します。この保存の後、赤い **X** アイコンと [保存] ボタンが表示されなくなります。スイッチをリブートすると、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スイッチ パラメータが設定されます。
<ユーザ名>	スイッチにログインしているユーザの名前です。デフォルト ユーザ名は **cisco** です。
[言語] メニュー	言語を選択するか、新しい言語ファイルをデバイスにロードします。メニューに必要な言語が表示されていれば、その言語を選択します。表示されていない場合、[言語のダウンロード] を選択します。新しい言語の追加の詳細については、[ファームウェア / 言語のアップグレード / バックアップ] ページを参照してください。
[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、スイッチのタイプと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。

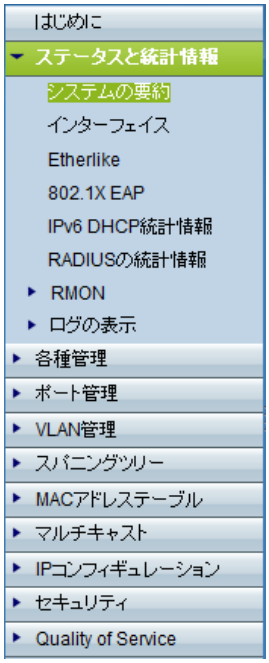
その他のリソース

[はじめに] ページの次のリンクを使用して、スイッチの使用に関する追加情報やサポート情報にアクセスすることができます。

- **[サポート]**：Cisco Small Business マネージド スイッチのサポート Web ページが表示されます。
- **[フォーラム]**：Cisco Small Business Support Community の Web ページが表示されます。

ナビゲーション ウィンドウ

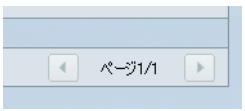
ナビゲーション ウィンドウは各ページの左側にあります。最上位レベルのカテゴリをクリックすると、関連ページへのリンクが表示されます。左側に矢印が表示されているリンクはサブカテゴリで、展開すると関連ページのリンクが表示されます。



管理ボタン

さまざまなページに表示されるよく使用されるボタンを次の表に示します。

管理ボタン

ボタン名	説明
	ページ数と現在表示しているページによっては、これらの機能を使用してテーブルのページをナビゲートすることができます。[I<] をクリックすると最初のページ、[<] をクリックすると前のページ、[>] をクリックすると次のページ、[>I] をクリックすると最後のページに進みます。特定のページを選択するには、[ページ <number> / <number>] ドロップダウン リストを使用します。

管理ボタン （続き）

ボタン名	説明
	各ページに表示するテーブル エントリの数を選択します。
	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] をクリックします。[閉じる] をクリックし、メインページに戻ります。 **注：**行った変更は実行コンフィギュレーションにだけ適用されます。スイッチのリブート時に、実行コンフィギュレーションは失われます。行った変更をスタートアップ コンフィギュレーションに保存するには、[保存] をクリックします。詳細については、**「コンフィギュレーション ファイルのコピーと保存」**を参照してください。
[適用]	クリックすると、選択したページで入力した変更が適用されます。 **注：**行った変更は実行コンフィギュレーションにだけ適用されます。スイッチのリブート時に、実行コンフィギュレーションは失われます。行った変更をスタートアップ コンフィギュレーションに保存するには、[保存] をクリックします。詳細については、**「コンフィギュレーション ファイルのコピーと保存」**を参照してください。
[キャンセル]	クリックすると、ページで行った変更が取り消され、以前に適用されていた値にリセットされます。
[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になります。
[インターフェイスカウンタのクリア]	クリックすると、選択されたインターフェイスの統計情報カウンタがクリアになります。
[ログのクリア]	クリックすると、ログ ファイルが消去されます。
[テーブルのクリア]	クリックすると、テーブル エントリが消去されます。
[閉じる]	クリックすると、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。

管理ボタン （続き）

ボタン名	説明
[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て、これを複数のエントリにコピーすることができます。 ▪ コピーするエントリを選択します。[設定のコピー] をクリックします。 ▪ 宛先エントリ番号を入力します。 ▪ [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。 ▪ [閉じる] をクリックし、メインページに戻ります。
[削除]	削除するエントリをテーブルから選択し、[削除] をクリックします。エントリが削除されます。
[詳細]	クリックすると、メインページで選択されたエントリと関連付けられている詳細が表示されます。
[編集]	編集するエントリを選択し、[編集] をクリックして開きます。[編集] ページが開くので、ここでエントリを変更できます。 ▪ [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。 ▪ [閉じる] をクリックし、メインページに戻ります。
[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。
[フィルタのクリア]	[フィルタのクリア] をクリックすると、デフォルトの基準でページにデータが再表示されます。
[実行]	[実行] をクリックすると、選択した基準を使用して、ページに表示されるデータがフィルタリングされます。
[ソート ボタン]	テーブルの下部に「このテーブルはソート可能です」というメッセージが表示された場合、各列見出しがソート ボタンとして機能します。列見出しをクリックすると、選択した列の内容に基づいて、レコードが昇順でソートされます。ソートの適用後には、列見出しに矢印が表示されます。この矢印をクリックして、ソート順序を逆にすることができます。

2

統計情報の表示

この章では、スイッチの統計情報を表示する方法について説明します。

この章で説明する項目は次のとおりです。

- 「システムの要約」
- 「インターフェイス統計情報」
- 「Etherlike 統計情報」
- 「802.1X EAP 統計情報」
- 「IPv6 DHCP 統計情報」
- 「統計情報」
- 「ログ」

システムの要約

[システムの要約]ページには、ハードウェア モデルの説明、ソフトウェア バージョン、言語パック、システム アップ タイムなどの基本的な情報が表示されます。

システムの要約の表示

システム情報を表示するには、ナビゲーション ウィンドウで [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。または、[はじめに] ページの [デバイスステータス] の [システムの要約] をクリックします。

[システムの要約] ページには、次の情報が表示されます。

- **[システムの説明]**：システムの説明。
- **[システムロケーション]**：スイッチの物理的な位置。[システム設定] ページを表示してこの値を入力するには、[編集] をクリックします。

- **[システムコンタクト先]**：担当者の名前。[システム設定] ページを表示してこの値を入力するには、[編集] をクリックします。
- **[ホスト名]**：スイッチの名前。[システム設定] ページを表示してこの値を入力するには、[編集] をクリックします。デフォルトのホスト名は、**switch** に続けて基本 MAC アドレスの最後の 3 オクテットが付いた名前になります。たとえば、MAC アドレスが 010203040506 のスイッチのデフォルトのホスト名は、**switch040506**（16 進数値の右側 6 桁）になります。
- **[システムアップタイム]**：最後のリブートから経過した時間。
- **[現在の時刻]**：現在のシステム時刻。
- **[基本 MAC アドレス]**：スイッチ MAC アドレス。

ハードウェアとファームウェアのバージョン情報

スイッチの次のハードウェアおよびファームウェア情報が表示されます。

- **[シリアル番号]**：スイッチのシリアル番号。
- **[PID VID]**：ポート番号とバージョン ID。
- **[最大有効電力]（W）**：（PoE スイッチのみ）PoE ポートにより給電可能な最大電力。
- **[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。
- **[ブートバージョン]**：ブート コードのバージョン。
- **[ブートの MD5 チェックサム]**：ブート コードの MD5 チェックサム。

また、スイッチのグラフにより、各スイッチ ポートの設定を確認することができます。[ポート設定] ページを表示するには、ポートをクリックします。

[TCP/UDP サービス]

このテーブルには、TCP または UDP を使用する各サービスの情報が表示されます。

- **[サービス名]**：HTTP など、よく使用されるサービス名（使用できる場合）。
- **[タイプ]**：このサービスに使用される転送プロトコル（TCP または UDP）。
- **[ポート]**：サービスの Internet Assigned Numbers Authority（IANA; インターネット割り当て番号局）ポート番号。
- **[IP アドレス]**：スイッチのこのサービスに接続されているリモート デバイスの IP アドレス（存在する場合）。

- **[リモートポート]**: このサービスと通信しているあらゆるリモート デバイスの IANA ポート番号。
- **[状態]**：サービスの状態。UDP の場合、アクティブ状態になっている接続のみがテーブルに表示されます。アクティブ状態になっている場合、スイッチとクライアントまたはサーバ間で接続が確立されています。TCP の状態は、次のとおりです。
  - **[リッスン]**：サービスは、接続要求をリスニングしています。
  - **[アクティブ]**：接続セッションが確立されていて、パケットが送受信されています。
  - **[接続状態]**：スイッチとサーバまたはクライアント（このプロトコルに関する各デバイスの役割によって決まります）間で接続セッションが確立されています。

[言語パックテーブル]

このテーブルには、スイッチで使用可能な言語に関する情報が表示されます。言語は、管理者が設定ユーティリティにログインしたときに選択できます。

デフォルトの言語は英語で、この言語パックがソフトウェアに組み込まれています。[ファームウェア / 言語のアップグレード / バックアップ] ページを使用して、追加の言語パックをダウンロードすることができます。言語ファイルは、シスコのファームウェア ダウンロード ページから入手できます。

[言語パックテーブル] には、使用可能な各言語の次の情報が表示されます。

- **[言語]**：言語名。
- **[ロケール]**：言語および国または地域を示す Internet Engineering Task Force（IETF）ロケール コード。
- **[バージョン]**：言語ファイルのバージョン。
- **[MD5 チェックサム]**：ファイルの整合性を確認するのに使用する 128 ビット ハッシュ コード。
- **[ファイルタイプ]**：次のいずれかの値を示します。
  - **[組み込み]**：ソフトウェア内で提供されているデフォルトの言語。この言語は、個別のファイルとしてダウンロードすることはできません。
  - **[外部]**：スイッチにダウンロードされ、ログイン時に選択可能な言語ファイル。
- **[ファイルサイズ]**：ファイルのサイズ（KB 単位）。

- **[デフォルト]**：[はい] と表示されている場合は、スイッチをリブートしたときに Web ベースのスイッチ設定ユーティリティのログイン ページがこの言語で表示されることを示します。
- **[ステータス]**：[アクティブ] または [非アクティブ] と表示されます。ログイン時に、ユーザは言語を選択できます。選択した言語がアクティブな言語になります。

システム設定の指定

システム設定を設定するには、次の手順に従います。

ステップ 1 [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。[システム設定] ページが開きます。

ステップ 2 [編集] をクリックして、次の設定を変更します。

- **[システムロケーション]**：スイッチの物理的な位置を入力します。
- **[システムコンタクト先]**：担当者の名前を入力します。
- **[ホスト名]**：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、RFC1034、RFC1035 の規定により）。デフォルトのホスト名は、switch に続けて基本 MAC アドレスの最初の 3 バイトが付いた名前になります。たとえば、MAC アドレスが 010203040506 のスイッチのデフォルトのホスト名は、switch010203 になります。

ステップ 3 [適用] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

インターフェイス統計情報

受信パケットと送信パケットの統計情報を表示するには、[インターフェイス] ページを使用します。このページを表示するには、ナビゲーション ウィンドウで [ステータスと統計情報] > [インターフェイス] の順にクリックするか、[はじめに] ページの [デバイスステータス] の [ポート統計情報] をクリックします。

統計情報を表示するインターフェイス（ポートまたは LAG）を選択し、統計情報のリフレッシュ レートを選択します。選択したインターフェイスの次の情報が表示されます。

- **[合計バイト (オクテット)]**：前回スイッチがリフレッシュされてから、選択されたインターフェイスで送信または受信されたオクテットの合計数。
- **[ユニキャストパケット]**：前回スイッチがリフレッシュされてから、選択されたインターフェイスで送信または受信されたユニキャスト パケットの合計数。
- **[マルチキャストパケット]**：前回スイッチがリフレッシュされてから、選択されたインターフェイスで送信または受信されたマルチキャスト パケットの合計数。
- **[ブロードキャストパケット]**：前回スイッチがリフレッシュされてから、選択されたインターフェイスで送信または受信されたブロードキャスト パケットの合計数。
- **[エラーがあるパケット]**：前回スイッチがリフレッシュされてから、選択されたインターフェイスで送信または受信された、エラーがあるパケットの合計数。
- **[STP BPDU]**：前回スイッチがリフレッシュされてから、選択されたインターフェイスで送信または受信された Spanning Tree Protocol（STP; スパニング ツリー プロトコル）Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）の合計数。
- **[RSTP BPDU]**：前回スイッチがリフレッシュされてから、選択されたインターフェイスで送信または受信された Rapid Spanning Tree Protocol（RSTP; 高速スパニング ツリー プロトコル）BPDU の合計数。

統計情報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] をクリックすると、選択されたインターフェイスのすべてのカウンタが 0 にリセットされます。
- [すべてのインターフェイスカウンタのクリア] をクリックすると、すべてのインターフェイスのすべてのカウンタが 0 にリセットされます。

Etherlike 統計情報

システムは、ポートと LAG に関する統計情報を RFC2665 に従って収集して報告します。

このページを表示するには、ナビゲーション ウィンドウで [ステータスと統計情報] > [Etherlike] の順にクリックします。

統計情報を表示するインターフェイス（ポートまたは LAG）を選択し、統計情報のリフレッシュ レートを選択します。これらの統計情報は、前回ページがリフレッシュされてからの累積的な情報です。選択したインターフェイスの次の情報が表示されます。

- **[フレームチェックシーケンス (FCS) エラー]**：受信された FCS エラー。
- **[単一コリジョンフレーム]**：受信された信号コリジョン フレーム エラー。
- **[レイトコリジョン]**：受信されたレイト コリジョン フレーム。
- **[過剰コリジョン]**：受信された過剰コリジョン フレーム。
- **[複数のコリジョン]**：受信された複数コリジョン フレーム。
- **[オーバーサイズパケット]**：サイズが 1518 オクテット（フレーミング ビットは含まず、FCS オクテットを含む）を超えていること以外には形式が正常な受信パケット。
- **[内部 MAC 受信エラー]**：LAG またはインターフェイスで受信された内部 MAC エラー。
- **[アラインメントエラー]**：アラインメント エラーを伴う受信パケット。
- **[受信済みポーズフレーム]**：LAG またはインターフェイスで受信されたポーズ フレーム。
- **[送信済みポーズフレーム]**：LAG またはインターフェイスから送信されたポーズ フレーム。

統計情報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] をクリックすると、選択されたインターフェイスのすべてのカウンタが 0 にリセットされます。
- [すべてのインターフェイスカウンタのクリア] をクリックすると、すべてのインターフェイスのすべてのカウンタが 0 にリセットされます。

802.1X EAP 統計情報

スイッチ ポートは、ネットワーク アクセスの制御に IEEE 802.1X Extensible Authentication Protocol（EAP; 拡張認証プロトコル）を使用するように設定できます（「802.1X」を参照）。[802.1X EAP] ページを使用して、ポートで受信された EAP パケットに関する情報を表示できます。

[802.1X EAP] ページを表示するには、ナビゲーション ウィンドウで [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 1 統計情報を表示する [ポート] を選択します。

ステップ 2 統計情報の [リフレッシュレート] を選択します。これらの統計情報は、前回ページがリフレッシュされてからの累積的な情報です。

選択したインターフェイスの次の情報が表示されます。

- **[受信済み EAPOL フレーム]**：ポートで受信された有効な Extensible Authentication Protocol over LAN（EAPOL; EAP over LAN）フレーム。
- **[送信済み EAPOL フレーム]**：ポートを通じて送信された 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 EAPOL 開始フレーム。
- **[受信済み EAPOL ログオフフレーム]**：ポートで受信された EAPOL ログオフ フレーム。
- **[受信済み無効 EAPOL フレーム]**：このポートで受信された認識されない EAPOL フレーム。
- **[受信済み 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。

統計情報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] をクリックすると、選択されたインターフェイスのすべてのカウンタが 0 にリセットされます。
- [すべてのインターフェイスカウンタのクリア] をクリックすると、すべてのインターフェイスのすべてのカウンタが 0 にリセットされます。

IPv6 DHCP 統計情報

スイッチは、IPv6 インターフェイス経由で管理したり、管理 IPv6 アドレスを Dynamic Host Configuration Protocol（DHCPv6）経由で受信するように設定することができます。管理インターフェイスでの IPv6 と DHCP の設定については、**「管理インターフェイス」**を参照してください。[IPv6 DHCP 統計情報] ページを使用して、送受信された DHCPv6 パケットに関する情報を表示できます。

このページを表示するには、ナビゲーション ウィンドウで [ステータスと統計情報] > [IPv6 DHCP 統計情報] の順にクリックします。

ページのリフレッシュ レートを選択します。ページには次の統計情報が表示されます。これらの統計情報は、前回ページがリフレッシュされてからの累積的な情報です。

- [受信済み DHCPv6 アドバタイズメントパケット]
- [受信済み DHCPv6 応答パケット]
- [廃棄された受信済み DHCPv6 アドバタイズメントパケット]
- [廃棄された受信済み DHCPv6 応答パケット]
- [受信済みの DHCPv6 不正パケット]
- [受信済み DHCPv6 パケットの合計数]
- [送信済み DHCPv6 要請パケット]
- [送信済み DHCPv6 要求パケット]
- [送信済み DHCPv6 更新パケット]
- [送信済み DHCPv6 再結合パケット]
- [送信済み DHCPv6 解放パケット]
- [送信済み DHCPv6 パケットの合計数]

[カウンタのクリア] をクリックすると、すべてのカウンタが 0 にリセットされます。

RADIUS 統計情報

スイッチは、ユーザ認証用に RADIUS サーバと通信するように設定できます。[RADIUS 統計情報] ページを表示するには、ナビゲーション ウィンドウで [ステータスと統計情報] > [RADIUS 統計情報] の順にクリックします。

リストから RADIUS サーバを選択して、ページのリフレッシュ レートを選択します。ページには次の統計情報が表示されます。これらの統計情報は、前回ページがリフレッシュされてからの累積的な情報です。

- **[アクセス要求]**：RADIUS サーバに送信された認証要求パケット数。
- **[アクセス再送信]**：RADIUS サーバに再送信された認証要求パケット数。
- **[アクセス許可]**：RADIUS サーバに受け入れられた認証要求パケット数。
- **[アクセス拒否]**：RADIUS サーバに拒否された認証要求パケット数。
- **[アクセスチャレンジ]**：RADIUS サーバからスイッチに送信されたアクセス チャレンジ パケット数。
- **[不正なアクセス応答]**：RADIUS サーバからの不正応答パケット数。
- **[不正なオーセンティケータ]**：無効なメッセージ オーセンティケータ属性が含まれていた認証要求パケット数。
- **[保留中の要求]**：サーバに送信されたが応答のない認証要求パケット数。
- **[タイムアウト]**：サーバから応答がないためにタイムアウトになった認証要求パケット数。
- **[不明なタイプ]**：スイッチが受信した不明なタイプの RADIUS パケット数。
- **[ドロップされたパケット]**：スイッチがドロップした RADIUS パケット数。

[すべての統計情報のクリア] をクリックすると、すべてのカウンタが 0 にリセットされます。

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。

統計情報を表示するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで [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 統計情報を表示するポートまたは LAG を選択します。

ステップ 3 ページのリフレッシュ レートを選択します。

選択したインターフェイスの次の情報が表示されます。

- **[受信済みバイト]**：前回スイッチがリフレッシュされてから、インターフェイスで受信されたオクテット。この数には、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]**：前回スイッチがリフレッシュされてから、インターフェイスでパケットがドロップされた回数。
- **[受信済みパケット]**：前回スイッチがリフレッシュされてから、インターフェイスで受信されたパケット。この数には、不良パケット、マルチキャストおよびブロードキャスト パケットが含まれます。
- **[受信済みブロードキャストパケット]**：前回スイッチがリフレッシュされてから、インターフェイスで受信された良好なブロードキャスト パケット。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]**：前回スイッチがリフレッシュされてから、インターフェイスで受信された良好なマルチキャスト パケット。
- **[CRC& アラインメントエラー]**：前回スイッチがリフレッシュされてから、インターフェイスで発生した CRC エラーとアライメント エラー。
- **[アンダーサイズパケット]**：前回スイッチがリフレッシュされてから、インターフェイスで受信されたアンダーサイズ パケット（64 オクテット未満）。
- **[オーバーサイズパケット]**：前回スイッチがリフレッシュされてから、インターフェイスで受信されたオーバーサイズ パケット（1518 オクテット超）。
- **[フラグメント]**：前回スイッチがリフレッシュされてから、インターフェイスで受信されたフラグメント（64 オクテット未満のパケット。これには、フレーミング ビットは含まれず、フレーム チェック シーケンス オクテットは含まれます）。

- **[ジャバー]**：サイズが 1518 オクテットを超えていて、サンプリング セッション中に FCS エラーのあった受信済みパケット。
- **[コリジョン]**：前回スイッチがリフレッシュされてから、インターフェイスで受信されたコリジョン。
- **[64 バイトフレーム]**：前回スイッチがリフレッシュされてから、インターフェイスで受信された 64 バイトのフレーム。
- **[65 ～ 127 バイトフレーム]**：前回スイッチがリフレッシュされてから、インターフェイスで受信された 65 ～ 127 バイトのフレーム。
- **[128 ～ 255 バイトフレーム]**：前回スイッチがリフレッシュされてから、インターフェイスで受信された 128 ～ 255 バイトのフレーム。
- **[256 ～ 511 バイトフレーム]**：前回スイッチがリフレッシュされてから、インターフェイスで受信された 256 ～ 511 バイトのフレーム。
- **[512 ～ 1023 バイトフレーム]**：前回スイッチがリフレッシュされてから、インターフェイスで受信された 512 ～ 1023 バイトのフレーム。
- **[1024 ～ 1518 バイトフレーム]**：前回スイッチがリフレッシュされてから、インターフェイスで受信された 1024 ～ 1518 バイトのフレーム。

ログ

スイッチは、システムの状態を識別したり、スイッチ動作中に発生した問題を診断するのに役立つメッセージを生成します。メッセージは、プラットフォーム上で発生したイベント、障害、エラーや、設定の変更に応じて生成されます。

これらのメッセージのログは RAM とフラッシュ メモリに保存されます。フラッシュ ログ内のエントリは、RAM 内のログとは異なり、プラットフォームをリブートした後も保存されたままになります。

ログ メニュー項目にアクセスするには、ナビゲーション ウィンドウで [ステータスと統計情報] > [ログの表示] の順にクリックします。ログ メニューには、次のページが含まれています。

- **「RAM メモリ ログ」**
- **「フラッシュ メモリ ログ」**

RAM メモリ ログ

[RAM メモリ] ページを使用して、ログが記録された時刻、ログの重大度、ログの説明など、特定の RAM（キャッシュ）ログ エントリに関する情報を表示することができます。

このページを表示するには、ナビゲーション ウィンドウで [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。

（注） テーブルに含まれているエントリ数が最大数の場合は、このページが表示されるまでに最大 45 秒かかることがあります。

[RAM メモリログテーブル] のフィールドは次のとおりです。

- **[ログインデックス]**：ログ エントリの ID 番号。
- **[ログ時刻]**：ログが RAM メモリ ログ テーブルに記録された時刻。
- **[重大度]**：ログの重大度。次のいずれかになります。
  - **緊急（0）**：システム使用不可能。
  - **アラート（1）**：ただちに処理を実行する必要あり。
  - **重要（2）**：致命的な状態。
  - **エラー（3）**：エラー状態。
  - **警告（4）**：警告状態。
  - **通知（5）**：正常であるが注意を要する状態。
  - **情報（6）**：情報メッセージ。
  - **デバッグ（7）**：イベントに関する詳細情報。

  [ログ設定] ページを使用して、ログに記録する重大度レベルを選択できます。
- **[コンポーネント]**：ログ エントリを生成したソフトウェア コンポーネントまたはサービス。
- **[説明]**：ログの説明。

[ログのクリア] をクリックして、RAM からすべてのログ エントリを削除することができます。

フラッシュ メモリ ログ

ログ ファイルには、ログが記録された時刻、ログの重大度、ログの説明など、特定のログ エントリに関する情報が含まれています。いくつかのタイプのログがサポートされていて、システムは各タイプの最大 3 つのバージョンを保存します。

フラッシュ ログを表示するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで [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。

ステップ 2 リストからログ タイプを選択します。

- **[デフォルト]**：スタートアップ ログおよび動作ログからのエントリ。
- **[スタートアップ]**：システムの再起動時に作成されたログ エントリ。
- **[動作]**：システム動作中に作成されたログ エントリ。

ステップ 3 表示するログ バージョンを選択します。

バージョン 1 のログには最新のログ、つまり直近に作成されたログ ファイルで、バージョン 2 のログは次に新しいログ ファイル、バージョン 3 のログは最も古いログ ファイルです。特定のタイプの新しいログが作成されると、バージョン 3 のログが削除され、バージョン 1 のログがバージョン 2、バージョン 2 のログがバージョン 3 に名前が変更されます。

異なるバージョンとログを選択した場合、新しいログが自動的に [フラッシュメモリログ テーブル] に表示されます。テーブルに含まれているエントリ数が最大数の場合は、このページが表示されるまでに最大 45 秒かかることがあります。

[フラッシュメモリログテーブル] には、次のフィールドがあります。

- **[ログインデックス]**：ログ エントリの ID 番号。
- **[ログ時刻]**：ログがフラッシュ メモリ ログ テーブルに記録された時間。
- **[重大度]**：ログの重大度。次のいずれかになります。
  - **アラート（1）**：ただちに処理を実行する必要あり。
  - **重要（2）**：致命的な状態。
  - **エラー（3）**：エラー状態。
  - **警告（4）**：警告状態。
  - **通知（5）**：正常であるが注意を要する状態。

- **情報（6）**：情報メッセージ。
- **デバッグ（7）**：イベントに関する詳細情報。

[ログ設定] ページを使用して、ログに記録する重大度レベルを選択できます。

- **[コンポーネント]**：ログ エントリを生成したソフトウェア コンポーネント。
- **[説明]**：ログの説明。

（注） [ログのクリア] をクリックして、フラッシュ メモリからすべてのログ エントリを削除することができます。[ログのバックアップ] をクリックして、[コンフィギュレーション/ログのダウンロード/バックアップ] ページを開くことができます。ここでは、TFTP または HTTP を使用して、TFTP サーバまたはネットワーク ロケーションにログ ファイルをバックアップすることができます。詳細については、**「コンフィギュレーション ファイルとログのバックアップ」**を参照してください。

3

各種管理

この章では、グローバル システム設定の指定方法と診断の実行方法について説明します。

この章で説明する項目は次のとおりです。

- 「システム設定の指定」
- 「管理インターフェイス」
- 「ユーザ アカウントの管理」
- 「管理サービスの有効化」
- 「アイドル セッション タイムアウトの設定」
- 「ログイン セッション」
- 「ログイン履歴」
- 「時間設定」
- 「システム ログ」
- 「ファイル管理」
- 「スイッチのリブート」
- 「ホストの Ping」
- 「制御パケットの転送の設定」
- 「診断」
- 「Bonjour の有効化」
- 「LLDP-MED」
- 「DHCP クライアント ベンダー オプションの設定」

システム設定の指定

[システム設定] ページで、ネットワーク内のスイッチを識別する情報を設定できます。

システム設定を指定するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで [各種管理] > [システム設定] の順にクリックします。

[システムの説明] はファームウェアにハードコードされています。

ステップ 2 パラメータを入力します。

- **[システムロケーション]**：スイッチの物理的なロケーションの説明。
- **[システムコンタクト先]**：スイッチの担当者の名前。
- **[ホスト名]**：この管理対象ノードに管理上割り当てられた名前。規定により、これはノードの完全修飾ドメイン名です。デフォルトのホスト名は、**switch** に続けてスイッチの MAC アドレスの末尾 6 桁の 16 進数が付加された名前になります。ホスト名ラベルには、アルファベット、数字、およびハイフンのみを指定できます。ホスト名ラベル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。

ステップ 3 [適用] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

管理インターフェイス

スイッチの管理インターフェイスにより、ネットワーク上の管理ステーションから Web ベースのスイッチ設定ユーティリティにアクセスすることができます。スイッチは、管理トラフィックをスイッチ上の他のトラフィックから分離する管理 VLAN の構成をサポートしています。

管理インターフェイスには、IPv4 アドレスまたは IPv6 アドレスを割り当てることができます。アドレスは、スタティックに設定することも、DHCP/BOOTP サーバを通じて取得することもできます。

[各種管理] > [管理インターフェイス] メニューで使用可能な設定ページの詳細については、次のトピックを参照してください。

- **「IPv4 管理インターフェイスの設定」**
- **「IPv6 管理インターフェイスの設定」**
- **「IPv6 ネイバーの表示と追加」**

IPv4 管理インターフェイスの設定

[IPv4 インターフェイス] ページを使用して、管理 VLAN と IPv4 アドレスを設定できます。

IPv4 管理インターフェイスを設定するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで [各種管理] > [管理インターフェイス] > [IPv4 インターフェイス] の順にクリックします。

ステップ 2 リストから管理 VLAN を選択します。

Web ベースのスイッチ設定ユーティリティにアクセスするには、ポートが管理 VLAN のメンバでなければなりません。デフォルトでは、VLAN 1 が管理 VLAN として設定されていて、すべてのスイッチ ポートが VLAN 1 のメンバとして設定されています。

少なくとも 1 つのポートが管理 VLAN のメンバとして設定されている必要があります。[メンバポート] リストには、選択した管理 VLAN の現在のすべてのメンバが表示されます。

管理 VLAN を変更した場合、以前の管理 VLAN のメンバの管理アクセスを継続するには、以前の管理 VLAN のすべてのメンバを新しい VLAN に再割り当てする必要があります。

ステップ 3 [IPアドレスタイプ] で、次のいずれかのオプションを選択します。

- **[DHCP]**：管理インターフェイスは、IPv4 アドレスを DHCP サーバから取得します。
- **[Bootp]**：管理インターフェイスは、IPv4 アドレスを BOOTP サーバから取得します。
- **[スタティック]**：[IPアドレス] フィールドに割り当てられている管理インターフェイスの IPv4 アドレス。

  デフォルトでは、DHCP が有効で、スイッチは DHCP サーバに IP アドレスを要求します。サーバから IP アドレスを取得できない場合、スイッチは工場出荷時のスタティック IP アドレスにフォールバックします。この場合、[System] LED が連続的に点滅します。スイッチは DHCP サーバからの IP アドレスの取得を試行し続けます。工場出荷時のスタティック IP アドレスは 192.168.1.254/24 で、デフォルトゲートウェイは 192.168.1.1 です。

  [IP アドレスタイプ] を [スタティック] に設定した場合は、次の項目を指定します。

  - **[IP アドレス]**：IPv4 アドレスを入力します。
  - **[マスク]**：32 ビット ネットワーク マスクを入力します（例：255.255.255.0）。または、[プレフィクス長] を選択して、ネットワーク プレフィクス（例：24）を構成するビット数（0 ～ 32）を指定します。
  - **[デフォルトゲートウェイ]**：[ユーザ定義] を選択して、管理パケット用のデフォルト ゲートウェイ IP アドレスを指定します。
    または、[なし] を選択して、管理パケットがサブネットの外部に転送されないようにします。
- **[動作デフォルトゲートウェイ]**：現在使用されているデフォルト ゲートウェイ。

ステップ 4 [適用] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

注意 管理 IP アドレスと [IPアドレスタイプ] を変更すると、現在の管理セッションが終了します。[管理 VLAN] とそのポート メンバシップを変更すると、スイッチとの通信が中断され、現在の管理セッションが終了します。

IPv6 管理インターフェイスの設定

[IPv6 インターフェイス] ページを使用して、IPv6 を介した Web ベースのスイッチ設定ユーティリティへのアクセスを有効にできます。スイッチは、IPv6 アドレスを動的（ダイナミック）に学習するように設定することも、IPv6 アドレスを静的（スタティック）に設定することもできます。

IPv6 管理アクセスを有効にするには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで [各種管理] > [管理インターフェイス] > [IPv6 インターフェイス] の順にクリックします。

ステップ 2 次の設定を行います。

- **[IPv6 モード]**：選択すると、IPv6 管理アクセスが有効になります。
- **[IPv6 アドレス自動コンフィギュレーション]**：選択すると、スイッチは、アドレスのリンク ローカル部分にポートの MAC アドレスを使用して、EUI-64 形式でリンク ローカル アドレスを自動設定できるようになります。スイッチは、ルータのアドバタイズメントを待ち受けして、アドレスのグローバル部分を検出して自動設定します。
- **[DHCPv6]**：選択すると、スイッチは DHCPv6 サーバから IPv6 アドレスを取得できるようになります。
- **[IPv6 ゲートウェイ]**：スイッチが、サブネット外部のデバイス宛の IPv6 パケットを送信しなければならない、IPv6 ルータのリンク ローカル アドレスを入力します。

ステップ 3 [適用] をクリックします。変更内容が実行コンフィギュレーションに保存されます。[キャンセル] をクリックして、変更内容をクリアすることができます。

IPv6 アドレスの追加

[IPv6 アドレステーブル] には、スイッチに現在設定されているスタティック アドレスが表示されます。このテーブルは次のフィールドで構成されています。

- **[IPv6 アドレス]**：IPv6 グローバル アドレス形式での IPv6 アドレス。
- **[DAD ステータス]**：Duplicate Address Detection（DAD; 重複アドレス検出）のステータス。スイッチに IPv6 アドレスを設定する場合、スイッチは、実際にアドレスを割り当てる前に近隣探索を行い、ネットワーク上でそのアドレスが使用されているかどうかを検出します。
  - アドレスがすでに使用されている場合、そのアドレスの DAD ステータスは [True] になります。この場合、そのアドレスを管理アクセスに使用することはできません。
  - アドレスが一意であることが判明した場合、そのアドレスの DAD ステータスは [False] になります。この場合、そのアドレスを管理アクセスに使用することができます。

複数の IPv6 アドレスを設定することができます。各アドレスに異なるプレフィクスを指定して、異なるサブネット上のステーションからスイッチを管理できるようにする必要があります。これにより、あるサブネットへのルートで障害が発生した場合に、別のサブネットからスイッチを管理することができます。

スタティック IPv6 アドレスを追加するには、次の手順に従います。

ステップ 1 [追加] をクリックします。

ステップ 2 IPv6 アドレスに続けて、スラッシュ（/）、プレフィクス長を入力します。

ステップ 3 アドレスが EUI-64 形式に従っている場合は [EUI-64] を選択します。最初の 3 ～ 5 のオクテットは Organizationally Unique Identifier（OUI; 組織固有識別子）で、残りのオクテットは一意に割り当てられたアドレスです。

ステップ 4 [適用] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

IPv6 デフォルト ルータ テーブル

IPv6 の管理を有効にした場合、スイッチは IPv6 近隣探索プロセスを使用して、ローカル IPv6 サブネット外部のデバイスと通信するためのデフォルト ルータを識別します。IPv6 ネットワークのデフォルト ルータの機能は、IPv4 ネットワークのデフォルト ルータとほぼ同じです。

[IPv6 デフォルトルータテーブル] には、各 IPv6 管理アドレスのデフォルト ルータの IP アドレスが表示されます。デフォルト ルータのアドレスは、サブネット上の IPv6 インターフェイスのリンク ローカル アドレスで構成されています。

IPv6 ネイバーの表示と追加

IPv6 管理が有効になっている場合、スイッチは接続されているリンク上の IPv6 対応デバイスを識別します。スイッチは、最大 1,000 個のダイナミック IPv6 ネイバーの検出をサポートしていて、IPv6 ネイバーのスタティック設定をサポートしています。

[IPv6 ネイバー] ページには、ダイナミックに検出されたネイバーとスタティックに設定されたネイバーが表示され、スタティック ホストを追加することができます。

[IPv6 ネイバーテーブル] を表示するには、ナビゲーション ウィンドウで [各種管理] > [管理インターフェイス] > [IPv6 ネイバー] の順にクリックします。

[IPv6 ネイバーテーブル] には、各ダイナミック エントリの次のフィールドが表示されます。

- **[IPv6 アドレス]**：ネイバーの IPv6 アドレス。
- **[MAC アドレス]**：ネイバーの MAC アドレス。
- **[状態]**：ネイバーの状態。次の状態は、ダイナミック エントリの状態です。
  - **[到達可能]**：事前に設定された時間内に、ネイバーへの転送パスが正常に機能していることを示す確認を受信しました。到達可能状態の場合、パケット送信時にデバイスは特別な処理を行いません。
  - **[遅延]**：転送パスが正常に機能していることを示す確認を前回受信してから、事前に設定された時間を超過しました。
- **[経過時間]**：エントリがキャッシュに追加されてから経過した時間（秒）。
- **[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）。

[ダイナミックネイバーのクリア] をクリックして、テーブルをクリアすることができます。

スタティック IPv6 ネイバーの追加

スイッチは最大 16 個のスタティック IPv6 ネイバー エントリをサポートしています。スタティック ネイバーを追加するには、次の手順に従います。

ステップ 1 [追加] をクリックします。

ステップ 2 IPv6 グローバル アドレスを入力します（プレフィクス長は入力しません）。

ステップ 3 ネイバーの 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。変更内容が実行コンフィギュレーションに保存されます。

ユーザ アカウントの管理

スイッチには、デフォルトで 1 名の管理ユーザが設定されています。

- ユーザ名：**cisco**
- パスワード：**cisco**

[ユーザアカウント] ページを使用して、最大 5 名の追加ユーザを設定したり、ユーザ パスワードを変更することができます。

ユーザの追加

ユーザを新規に追加するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで [各種管理] > [ユーザアカウント] の順にクリックします。

[ユーザアカウントテーブル] に、現在設定されているユーザが表示されます。

ステップ 2 [追加] をクリックします。

ステップ 3 英数字 1 ～ 32 文字のユーザ名を入力します。ユーザ名には、0 ～ 9 の数字と a ～ z のアルファベット（大文字または小文字）を使用することができます。

ステップ 4 1 ～ 64 文字（文字数は**「パスワード強度」**設定によって異なります）のパスワードを入力し、確認のためパスワードを再度入力します （'、"、%、? の各文字はサポートされていません）。

パスワードを入力するに従って、パスワードの強度を示す垂直バーの数と色が次のように変化します。

- 赤：パスワードが最小限の複雑度要件を満たしていません。[最小値未満] というテキストがメーターの右側に表示されます。
- オレンジ：パスワードは最小限の複雑度要件を満たしていますが、パスワードの強度が低くなっています。[弱い] というテキストがメーターの右側に表示されます。
- 緑：パスワードの強度が高いことを示しています。[強い] というテキストがメーターの右側に表示されます。

[適用] ボタンは、強度メーターがオレンジ色になり、確認のためのパスワードが入力されるまで、使用可能になりません。

ユーザを追加する場合、パスワードの強度チェック機能を一時的に無効にすることで、強度チェック条件を満たさないパスワードを設定することができます。[パスワード強度の適用を無効にする] をクリックして、警告が表示されたら [OK] をクリックします。

すべてのユーザのパスワード強度チェック機能を無効にしたり、その特性を設定するには、[パスワード強度] ページを使用します。

ステップ 5 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

ユーザ パスワードの変更

ユーザ パスワードを変更するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで [各種管理] > [ユーザアカウント] の順にクリックします。

ステップ 2 設定するユーザを選択して、[編集] をクリックします。

ステップ 3 1 ～ 64 文字（文字数は**「パスワード強度」**設定によって異なります）のパスワードを入力し、確認のためパスワードを再度入力します （'、"、%、? の各文字はサポートされていません）。

パスワードを入力するに従って、パスワードの強度を示す垂直バーの数と色が変化します。赤色のバーは、パスワードの強度が低いことを示します。オレンジ色のバーはパスワードの強度がより高く、緑色のバーはパスワードの強度が最も高いレベルであることを示しています。

パスワードを変更する場合、パスワードの強度チェック機能を一時的に無効にすることで、強度チェック条件を満たさないパスワードを設定することができます。[パスワード強度の適用を無効にする] をクリックして、警告が表示されたら [OK] をクリックします。

すべてのユーザのパスワード強度チェック機能を無効にしたり、その特性を設定するには、[パスワード強度] ページを使用します。

ステップ 4 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

ユーザの削除

デフォルトのユーザ（通常、**cisco** ユーザ ID）を除くすべてのユーザを削除できます。

ユーザを削除するには、[ユーザアカウントテーブル] でユーザ名を選択して [削除] をクリックします。

管理サービスの有効化

[管理サービス] ページを使用して、Web ベースのスイッチ設定ユーティリティへの HTTP 接続用の TCP ポート番号を設定できます。

HTTP 接続のデフォルトのポート番号は、一般的な IANA ポート番号 80 です。異なる HTTP ポート番号を設定するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで [各種管理] > [管理サービス] の順にクリックします。

ステップ 2 使用する論理ポート番号を 1025 ～ 65535 の範囲で入力します。デフォルトはポート 80 です。

ステップ 3 [適用] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

アイドル セッション タイムアウトの設定

指定した時間、非アクティブな状態が続くと、ユーザは自動的に管理インターフェイスからログ オフされます。タイムアウト後、ユーザは再認証される必要があります。

[アイドルセッションタイムアウト] ページを使用して、タイムアウト時間を設定することができます。このページを表示するには、ナビゲーション ウィンドウで [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。

HTTP セッションの非アクティブ タイムアウト時間は、1 ～ 60 分に設定できます。デフォルト値は 10 分です。

値を変更した場合は、[適用] をクリックして、行った変更を実行コンフィギュレーションに保存します。

ログイン セッション

[ログインセッション] ページには、アクティブな管理ログイン セッションが表示されます。このページを表示するには、ナビゲーション ウィンドウで [各種管理] > [ログインセッション] の順にクリックします。

このページには、現在ログインしている各ユーザの次の情報が表示されます。

- **[ID]**：ログイン セッションに対してシステムが生成した ID。
- **[ユーザ名]**：ユーザがログインするのに使用した名前。
- **[接続元]**：ホストの IP アドレス。
- **[アイドル時間]**：このユーザの前回のアクティビティから経過した時間。
- **[セッション時間]**：このユーザがログインして経過した時間。
- **[セッションタイプ]**：管理セッションで使用中のプロトコル（HTTP）。

ログイン履歴

[ログイン履歴] ページを使用して、管理ソフトウェアへの以前のログインに関するデータを表示できます。このページを表示するには、ナビゲーション ウィンドウで [各種管理] > [ログイン履歴] 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。

- **[ログイン時刻]**：ユーザがログインした日時。
- **[ユーザ名]**：ユーザがログインするのに使用した名前。
- **[プロトコル]**：ユーザがソフトウェアを設定するのに使用しているプロトコル。HTTP、Telnet、シリアル、SSH、または SNMP のいずれかになります。
- **[ロケーション]**：ホストの IP アドレス。

時間設定

メッセージ ログなどのスイッチ ソフトウェア イベント用のネットワーク同期型タイムスタンプ サービスを提供するのに、システム クロックが使用されます。システム クロックを手動で設定することも、サーバからクロック データを取得する Simple Network Time Protocol（SNTP）クライアントとしてスイッチを設定することもできます。

[各種管理] > [時間設定] メニューで使用可能な設定ページについては、次のトピックを参照してください。

- 「システムの時刻の設定」
- 「SNTP 設定の指定」
- 「SNTP 認証の設定」

システムの時刻の設定

[システムの時刻] ページを使用して、システムの時刻を手動で設定したり、システムが時間設定を SNTP サーバから取得するように設定することができます。このページを表示するには、ナビゲーション ウィンドウで [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。

デフォルトでは、時刻はスイッチでローカルに設定されています。

（注） システムの実際の時刻、日付、時間帯情報、および夏時間のステータスがページの下部に表示されます。

クロック設定のローカル指定

時間設定をローカルに設定するには、次の手順に従います。

ステップ 1 [システムの時刻] ページで [ローカル設定を使用] を選択します。

ステップ 2 スイッチが時間帯を DHCP サーバから取得するようにするには、[時間帯ソース - DHCP] を選択します。

ステップ 3 スイッチにアクセスするのに使用しているコンピュータからスイッチが時間設定を取得するようにするには、[コンピュータの日付 / 時刻を設定] を選択します。

または、このフィールドをクリアして、次の時間設定を指定することもできます。

- **[日付]**：日付を mm/dd/yyyy の形式で入力します。たとえば、2010 年 1 月 1 日の場合は 01/01/2010 と入力します。

- **[現地時間]**：現在の時刻を HH:mm:ss の形式で入力します。たとえば、午後 10 時の場合は 22:00:00 と入力します （時刻が 24 時間形式の場合は、ヒント テキストに HH と表示され、12 時間形式の場合は hh と表示されます）。
- **[GMT 時間帯のオフセット]**：現地の時間帯と Greenwich Mean Time（GMT; グリニッジ標準時）との時刻差を選択します。

ステップ 4 [時間帯の省略形] フィールドに、設定を識別するためのオプションの略語を 4 文字以内で指定します。このフィールドは、参照情報としてのみ使用されます （'、"、%、? の各文字はサポートされていません）。

ステップ 5 [夏時間] を選択して、Daylight Savings Time（DST; 夏時間）を設定します（現地の時間帯で該当する場合）。選択した場合は、次のフィールドを設定します。

- **[米国]/[欧州]/[その他]**：[米国] または [欧州] を選択して、米国またはヨーロッパで使用されている値に設定された DST オフセットに設定します。または、[その他] を選択して、手動で設定します。手動で設定する場合は、次回の DST 期間のみの設定を指定することも、毎年繰り返される DST 期間の設定を指定することもできます。
- **[DST 時間帯の省略形]**：設定を識別するためのオプションの略語を 4 文字以内で指定します。このフィールドは、参照情報としてのみ使用されます （'、"、%、? の各文字はサポートされていません）。
- **[夏時間のオフセット]**：DST の開始時にクロックを進める時間（分）を指定します。
- **[開始]/[終了]**：DST の開始および終了日時を指定します。
- **[繰り返し]**：毎年繰り返される DST 期間を指定する場合に選択します。各年の DST の開始日および終了日である曜日と週数を選択します。

ステップ 6 [適用] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

SNTP クライアントとしてのスイッチの設定

スイッチの SNTP 設定を指定して、スイッチが SNTP サーバから時刻を取得するように設定することもできます。

スイッチが SNTP サーバから時刻を取得するように設定するには、次の手順に従います。

ステップ 1 [システムの時刻] ページで、[SNTP サーバを使用] を選択します。

ステップ 2 スイッチの SNTP クライアント動作モードを設定します。

- **[ユニキャスト]**：設定されているユニキャスト SNTP サーバにのみユニキャスト SNTP 要求を送信するようにスイッチを設定します。この機能を有効にするには、少なくとも 1 つのユニキャスト SNTP サーバを追加する必要があります。

- **[ブロードキャスト]**：SNTP サーバからブロードキャストされる SNTP メッセージから時間設定を取得するようにスイッチを設定します。

ステップ 3 [適用] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

ステップ 4 **「SNTP 設定の指定」**および**「SNTP 認証の設定」**に従って、ポーリング間隔、ユニキャスト サーバ アドレス、スイッチが SNTP サーバにアクセスするのに必要な認証情報などの追加の SNTP 設定を指定します。

SNTP 設定の指定

スイッチは、Simple Network Time Protocol（SNTP; 簡易ネットワーク タイム プロトコル）をサポートしています。SNTP により、ネットワーク デバイスの時刻がミリ秒単位で正確に同期されます。時刻同期は、ネットワーク SNTP サーバによって実行されます。スイッチは SNTP クライアントとしてのみ動作し、他のシステムにタイム サービスを提供することはできません。

[SNTP 設定] ページを表示するには、ナビゲーション ウィンドウで [各種管理] > [時間設定] > [SNTP 設定] の順にクリックします。

SNTP 設定の指定

ステップ 1 [システムの時刻] ページで [SNTP サーバを使用] オプションが選択されていて、必要に応じてユニキャストまたはブロードキャスト モードが選択されていることを確認します。

ステップ 2 [SNTP 設定] ページで、次の設定を行います。

- **[クライアントポート]**：スイッチで SNTP クライアント用に使用する論理ポート番号。デフォルトは、このサービス用の一般的な IANA ポート番号である 123 です。
- **[ユニキャストポール間隔]**：スイッチが同期メッセージを SNTP サーバに送信する間隔。このフィールドは、SNTP の受信方法として [ユニキャスト] を選択している場合のみ編集することができます。3 ～ 16 の値を入力します。実際の間隔（秒）は、指定した値の 2 乗になります。たとえば、4 と入力した場合、ポーリング間隔は 16 秒になります。

ステップ 3 [適用] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

アクティブ サーバ プロパティとグローバル パラメータの表示

[SNTP 設定] ページには、スイッチが最後に時間設定を取得した SNTP サーバ（存在する場合）の次のプロパティが表示されます。また、このページにはグローバル（設定不可）パラメータも表示されます。

アクティブ サーバ：

- **[サーバホストアドレス]**：SNTP サーバの IP アドレス。
- **[サーバタイプ]**：サーバが使用している IP プロトコル バージョン（IPv4 または IPv6）。
- **[サーバストラタム]**：参照クロックからの距離を識別する SNTP サーバの階層レベル。
- **[サーバリファレンス ID]**：このサーバが使用している参照クロックを識別する 32 ビット コード。
- **[サーバモード]**：サーバの動作モード。
  - **[ユニキャスト]**：SNTP サーバは、SNTP クライアントからのユニキャスト要求を待ち受けます。
  - **[ブロードキャスト]**：SNTP サーバは、SNTP クライアントにブロードキャスト メッセージを定期的に送信します。
  - **[予約済み]**：SNTP サーバから応答を受信していません。サーバから応答を受信すると、いずれかの有効な状態（ブロードキャストまたはユニキャスト）に変わります。

グローバル パラメータ：

- **[SNTP クライアントバージョン]**：スイッチがサポートしている最も大きい SNTP プロトコル バージョン。
- **[最終更新時刻]**：最新の SNTP 更新を受信した時刻。
- **[最終ユニキャスト試行時刻]**：スイッチが最後に SNTP ユニキャスト サーバとの同期を試行した時刻。
- **[クライアントモード]**：設定されている SNTP クライアント モード（ユニキャストまたはブロードキャスト）。このモードの設定については、**「システムの時刻の設定」**を参照してください。
- **[サーバの最大エントリ]**：スイッチに設定可能な最大サーバ数。

- **[サーバの現在のエントリ]**：現在システムに設定されていて、[ユニキャスト SNTP サーバテーブル] に表示されている SNTP サーバの数。
- **[ブロードキャスト数]**：スイッチが SNTP サーバから受信した SNTP ブロードキャスト パケット数。

SNTP サーバの追加と変更

[ユニキャスト SNTP サーバテーブル] には、設定した各 SNTP サーバの次の情報が表示されます。

- **[SNTP サーバ]**：SNTP サーバの IP アドレスまたはホスト名。
- **[認証キー ID]**：SNTP サーバと通信するのに必要な暗号化キー。
- **[最終試行時刻]**：スイッチが最後に SNTP ユニキャスト サーバとの同期を試行した時刻。
- **[ステータス]**：SNTP サーバの動作ステータス。表示される値は次のとおりです。
  - **[成功]**：クライアントは、このサーバから時刻を取得することができました。
  - **[要求のタイムアウト]**：クライアントの要求がタイムアウトになりました。
  - **[不良な日付エンコード]**：サーバから不正な日付形式を受け取りました。
  - **[サポートされていないバージョン]**：サーバは、スイッチに設定されている SNTP バージョンをサポートしていません。
  - **[非同期のサーバ]**：スイッチの時刻がサーバと同期されていません。
  - **[サーバ Kiss Of Death]**：SNTP サーバが Kiss of Death（KoD）パケットで応答し、トラフィックの急激な増加またはその他のエラー状態により、スイッチに対してサーバに要求を送信しないように指示しました。
  - **[その他]**：ステータスを判断できませんでした。
- **[最後の応答]**：SNTP サーバから最後に応答が合った時刻。
- **[バージョン]**：サーバが使用している SNTP プロトコル バージョン。
- **[ポート]**：プロトコル ポート番号（SNTP 用の一般的なポート番号は 123）。
- **[ポーリングモード]**：スイッチがこのサーバに SNTP 要求を送信するように設定されているかどうか（有効または無効）。
- **[ユニキャスト合計要求数]**：スイッチがユニキャスト サーバに行った同期要求の総数。

サーバの設定を編集するには、チェックボックスをオンにして選択し、[編集] をクリックします。サーバを削除するには、チェックボックスをオンにして選択し、[削除] をクリックします。サーバを新規追加するには、[追加] をクリックして、設定を入力します。詳細については、次の説明を参照してください。

SNTP サーバを追加するには、次の手順に従います。

ステップ 1 [追加] をクリックします。

ステップ 2 パラメータを入力します。

- **[SNTP サーバ]**：IPv4 アドレスまたはドメイン名を入力します。ドメイン名を使用する場合は、スイッチで DNS サービスが有効になっていることを確認してください（**「ドメイン ネーム システム」**を参照）。
- **[認証キー]**：SNTP サーバと通信する際に認証が必要な場合は [有効] を選択します。
- **[認証キー ID]**：認証を使用する場合は、リストから認証キー ID を選択します。認証キーの設定方法については、**「SNTP 認証の設定」**を参照してください。
- **[ポーリングモード]**：スイッチがこのサーバに要求を送信できるようにするには [有効] を選択します。
- **[ポート]**：SNTP メッセージ ヘッダー内に指定する UDP ポート番号を指定します。デフォルトでは、ポート番号は一般的な IANA 値である 123 になっています。
- **[バージョン]**：サーバがサポートしている最も大きい SNTP バージョン（1 ～ 4）を指定します。

ステップ 3 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

SNTP 認証の設定

スイッチが STNP サーバへの認証に使用する識別情報が含まれた暗号化キーを設定するには、[SNTP 認証] ページを使用します。このページを使用して、SNTP 認証サービスを有効にすることもできます。

スイッチが使用可能な SNTP サーバを定義する場合、サーバが認証を使用するかどうかと、サーバが使用する認証キーを指定します。

（注） SNTP 認証を有効にするには、少なくとも 1 つの信頼済み認証キーを設定する必要があります。設定しないと、「SNTP 認証を有効にできませんでした」というメッセージが表示されます。

認証キーを設定して、このサービスを有効にするには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで [各種管理] > [時間設定] > [SNTP 認証] の順にクリックします。

[SNTP 認証テーブル] に、現在設定されている各認証キーと、キーが信頼済みキーとして現在使用できるかどうかが表示されます。

ステップ 2 [有効] を選択して、時刻を同期する前にスイッチが SNTP サーバの認証を行うように要求します。

ステップ 3 [適用] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

ステップ 4 [SNTP 認証テーブル] で、[追加] をクリックして、キーをリストに追加します。

ステップ 5 パラメータを入力します。

- **[認証キー ID]**：キー番号。システムで SNTP サーバを定義するときに、認証に使用するキーを指定します。
- **[認証キー]**：キーの値。値は、サーバとの間で送受信する SNTP メッセージの暗号化と複合化で使用する暗号鍵です。
- **[信頼済みキー]**：このキーが信頼済みキーであるかどうかを示します。信頼済みキーのみを使用できます。SNTP 認証サービスを有効にするには、少なくとも 1 つの信頼済みキーを設定する必要があります。

  キーは、ユニキャスト SNTP サーバでのみ使用されます。キーは、信頼済みとして有効になっている場合のみ、SNTP サーバを認証するのに使用されます。スイッチで設定されているが、信頼済みとして指定されていないキーは使用されません。管理者は、別のときに使用する目的で、信頼されていないキーを追加することができます。

ステップ 6 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

システム ログ

スイッチは、イベント、障害、エラー、設定変更などに応じてメッセージを生成します。これらのメッセージは、システム メモリにローカルに保存され、監視または長期アーカイブ用の 1 つまたは複数の集中的な収集場所に転送されます。

[各種管理] > [システムログ] メニューで使用可能な設定ページの詳細については、次のトピックを参照してください。

- 「ログ設定の指定」
- 「リモート ログ サーバの設定」

ログ設定の指定

[ログ設定] ページを使用して、ログをグローバルに有効にしたり、一時的なメモリ（RAM）および永続的なメモリ（フラッシュ）に記録するイベント タイプを定義することができます。フラッシュ メモリ内のログ メッセージは、リブート後も維持されます。ログがいっぱいになると、最も古いイベントが自動的に削除され、新しいエントリで置き換えられます。

ログ設定を指定するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで [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 システムで実行するログのタイプを有効にします。

- **[ログ集約]**：有効にすると、同じタイプの複数のログが 1 つのログ メッセージに組み合わされます。設定されている時間内に複数の同じログ メッセージを連続的に受信した場合、これらのメッセージは 1 つのログ メッセージに集約されます。
- **[ログ集約間隔]**：[ログ集約] を有効にした場合は、間隔を秒単位で指定します。この間隔内に受信した連続するメッセージは、1 つのログ メッセージに集約されます。15 ～ 120 秒の範囲で指定します。
- **[RAM メモリロギング]**：選択すると、RAM へのロギングが有効になります。
- **[フラッシュメモリロギング]**：選択すると、フラッシュ メモリへのロギングが有効になります。
- **[フラッシュログサイズ]**：フラッシュ メモリのログに保存するログ メッセージの最大数を入力します。

ステップ 3 各ログ タイプのイベントの重大度が記録されるようにします。重大度は、高いものから順に次のとおりです。

- **緊急**：システムが使用できません。
- **アラート**：何らかの措置が必要です。
- **重要**：システムは危機的な状況です。
- **エラー**：システムがエラー状況です。
- **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**：イベントの詳細情報が提供されます。

（注）：重大度を選択した場合、その重大度以上のイベントが自動的にロギングの対象として選択されます。

ステップ 4 [適用] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

リモート ログ サーバの設定

スイッチの Syslog メッセージ送信先とする、1 つまたは複数のリモート ログ サーバを定義することができます。ログ サーバを定義して、サーバに送信するログ イベントの重大度を設定するには、[リモートログサーバ] ページを使用します。

Syslog 動作を有効にして、リモート ログ サーバを設定するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで [各種管理] > [リモートログサーバ] の順にクリックします。

ステップ 2 [Syslog ロギング] モードの [有効] をクリックして、次の設定を指定します。

- **[ファシリティ]**：このスイッチからの Syslog メッセージの分類を識別する値をリストから選択します。これらの値（ローカル 0 ～ ローカル 7）の意味は、ネットワーク管理者が決定します。
- **[ローカルポート]**：スイッチの IANA ポート番号を指定します。デフォルトは、Syslog プロトコル用の一般的なポート番号である 514 です。

ステップ 3 [リモートログサーバテーブル] で [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。

- **[ログサーバ]**：ログの送信先であるサーバの IPv4 アドレスまたはホスト名。
- **[UDP ポート]**：リモート サーバが Syslog プロトコルに使用する論理 UDP ポート番号。デフォルトは、一般的な IANA Syslog ポート番号である 514 です。
- **[最小重大度]**：この重大度以上の項目のみがリモート サーバに送信されます。重大度については、**「ログ設定の指定」**を参照してください。

ステップ 5 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

ファイル管理

ファイル管理機能を使用して、ファームウェアのアップグレードやバックアップ、言語ファイルの更新、設定の変更内容の保存、スイッチ内の設定ファイルのコピー、自動コンフィギュレーション機能の設定を行うことができます。

（注） スイッチでダウンロードまたはアップロード処理が進行中の場合、不明な変更からスイッチを保護できるように、転送が完了するまでスイッチへのすべての管理アクセスが遮断されます。

[ファイル管理] メニューで使用可能な設定ページの詳細については、次のトピックを参照してください。

- **「ファームウェアと言語ファイルのアップグレードとバックアップ」**
- **「コンフィギュレーション ファイルとログファイルのダウンロードとバックアップ」**
- **「コンフィギュレーションの削除」**
- **「コンフィギュレーション ファイルのコピーと保存」**
- **「DHCP 自動コンフィギュレーション」**
- **「HTTP 経由でのファームウェア リカバリ」**

ファイルとファイル タイプ

スイッチ上には、次のタイプのコンフィギュレーション ファイルと動作ファイルがあります。

- **実行コンフィギュレーション**：スイッチが動作するために現在使用しているパラメータ。パラメータ値が変わるときにコンフィギュレーション インターフェイスの 1 つを使用することによりユーザにより変更できるのはこのファイル タイプのみで、リブート後も保持されるようにするには、スタートアップ コンフィギュレーションなどの別のファイル タイプに手動で保存する必要があります。

  スイッチのリブート時に、実行コンフィギュレーションは失われます。スイッチをリブートすると、フラッシュに保存されているスタートアップ コンフィギュレーションが RAM に保存されている実行コンフィギュレーションにコピーされます。

- **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たパラメータ値。

  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、スイッチがリブートしても保持されます。スイッチがリブートすると、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になります。

- **バックアップ コンフィギュレーション**：システム シャットダウンからの保護や特定の動作状態保持のために、パラメータ定義を手動でコピーしたもの。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、または実行コンフィギュレーションをバックアップ コンフィギュレーション ファイルにコピーできます。バックアップ コンフィギュレーションは、フラッシュ内に保存され、デバイス リブート時にも保持されます。

- **ミラー コンフィギュレーション**：次の状態の後、スイッチが作成するスタートアップ コンフィギュレーションのコピー。

  - スイッチが 24 時間連続稼動。
  - 24 時間以内に実行コンフィギュレーションが変更されたが、保存されていない。

  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スイッチによってのみ行われます。ミラー コンフィギュレーションを別のファイル タイプまたは別のデバイスにコピーすることは手動でできます。

- **ファームウェア**：オペレーティング システム。より一般的にはイメージと呼ばれます。

- **ブート コード**：基本システム スタートアップを制御し、ファームウェア イメージを起動します。

- **言語ファイル**：選択された言語でウィンドウを表示するためのディクショナリ。

- **フラッシュ ログ**：フラッシュ メモリ内に保存される SYSLOG メッセージ。

ファームウェアと言語ファイルのアップグレードとバックアップ

[ファームウェア / 言語のアップグレード / バックアップ] ページを使用して、次のことが可能です。

- サーバから新しいイメージをダウンロードして、ファームウェアをアップグレードする。
- サーバから新しいブート ファイルをダウンロードして、ブート コードをアップグレードする。
- サーバから新しいファイルをダウンロードして、言語ファイルを更新する。言語ファイルにより、Web ベースのスイッチ設定ユーティリティの言語オプションが決まります。ログイン時に表示言語を選択できます。
- ファームウェア イメージをサーバにバックアップする。

常に英語がデフォルトの言語になります。

（注） コンフィギュレーション ファイルをバックアップまたは復元することもできます。詳細については、**「コンフィギュレーション ファイルとログファイルのダウンロードとバックアップ」**を参照してください。

ファームウェアをアップグレードまたはバックアップしたり、ブート コードや言語ファイルを更新するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで [各種管理] > [ファイル管理] > [ファームウェア / 言語のアップグレード / バックアップ] 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。

- **[転送方式]**：ダウンロード先またはアップロード元のサーバ タイプに対応する、ファイル転送で使用するプロトコル（TFTP または HTTP）を選択します。
- **[保存するアクション]**：スイッチにファイルをダウンロードするには [アップグレード] を選択し、スイッチからサーバへファイルをコピーするには [バックアップ] を選択します。
- **[ファイルタイプ]**：アップグレードまたはバックアップするファイルのタイプを選択します（ファームウェア イメージのみをバックアップできます）。
  - **[ファームウェアイメージ]**：スイッチのすべての機能とインターフェイスを制御するソフトウェア。
  - **[ブートコード]**：初期のシステム ブートアップを制御するソフトウェア。
  - **[言語パック]**：ユーザがログイン ページで指定した言語でシステム インターフェイスを表示できるようにするファイル。

- **[TFTP サーバ]**（TFTP のみ）：TFTP サーバの IP アドレスを指定します。
- **[ソースファイル名]**：TFTP 経由でアップグレードする場合は、パスを含めてファイル名を入力します。HTTP 経由でアップグレードする場合は、コンピュータでファイルを参照して選択します。
- **[宛先ファイル名]**：TFTP 経由でバックアップする場合は、パスを含めてファイル名を入力します。このフィールドは、HTTP 経由でのバックアップでは表示されません。

ステップ 3 [適用] をクリックして、アップグレードまたはバックアップを開始します。進捗状況バーに、ファイル転送のステータスが示されます。標準的なイメージ転送の所要時間は 5 ～ 6 分です。

警告 イメージやブート コード ファイルをスイッチにダウンロードしているときに、スイッチの電源が遮断されないようにしてください。ファイルのダウンロード中に電源障害が発生すると、永続的なメモリ内のファイルの内容が失われます。

ブート コード ファイルのダウンロード中に停電が発生すると、スイッチがブートできなくなります。このような場合は、Cisco Small Business Support Center にサポートを要請してください。

イメージのダウンロード中に停電が発生すると、イメージはロードされませんが、ブート ローダは引き続き動作可能な状態になります。機能するイメージのダウンロード方法については、**「HTTP 経由でのファームウェア リカバリ」**を参照してください。

コンフィギュレーション ファイルとログファイルのダウンロードとバックアップ

[コンフィギュレーション / ログのダウンロード / バックアップ] ページを使用して、保存されているコンフィギュレーション ファイルをスイッチにダウンロードして、以前に保存した設定を復元したり、現在のコンフィギュレーション ファイルをネットワーク ロケーションにバックアップすることができます。また、次のページを参照して、ログ ファイルをバックアップすることもできます。

- コンフィギュレーション ファイルのダウンロードによる設定の復元
- コンフィギュレーション ファイルとログのバックアップ

コンフィギュレーション ファイルのダウンロードによる設定の復元

コンフィギュレーション ファイルをスイッチにダウンロードして、以前にバックアップしたファイルを復元するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで [各種管理] > [ファイル管理] > [コンフィギュレーション/ログのダウンロード/バックアップ] の順にクリックします。

ステップ 2 [転送方式] を選択します（HTTP または TFTP）。

ステップ 3 [保存するアクション] で [アップグレード] を選択して、以降の手順で指定するファイルをダウンロードします。

ステップ 4 次のパラメータを入力します。

- **[TFTP サーバ]**（TFTP のみ）：TFTP サーバの IP アドレスを指定します。IP コンフィギュレーションで DNS が有効になっている場合は、サーバ名を指定します（「ドメイン ネーム システム」を参照）。
- **[ソースファイル名]**：TFTP の場合は、パスを含めてファイル名を指定します。HTTP の場合は、コンピュータでファイルを参照して選択します。
- **[宛先ファイルタイプ]**：次のいずれかのオプションを選択します。
  - **[スタートアップコンフィギュレーション]**：指定したコンフィギュレーション ファイルが有効な場合は、現在のスタートアップ コンフィギュレーション ファイルが置き換えられます。リブート時にそれがアクティブなコンフィギュレーション ファイルになります。
  - **[バックアップコンフィギュレーション]**：指定したファイルで、現在のバックアップ コンフィギュレーション ファイルが置き換えられます。

ステップ 5 [適用] をクリックして、アップグレードを開始します。進捗状況バーにアップグレードのステータスが示されます。

注意 コンフィギュレーション ファイルをスイッチにダウンロードしているときに、スイッチの電源が途絶えないようにしてください。コンフィギュレーション ファイルのダウンロード中に電源障害が発生すると、ファイルが失われ、プロセスをやり直さなければならなくなります。

コンフィギュレーション ファイルとログのバックアップ

コンフィギュレーション ファイルまたはログをバックアップするには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで [各種管理] > [ファイル管理] > [コンフィギュレーション/ログのダウンロード/バックアップ] の順にクリックします。

ステップ 2 [転送方式] を選択します（HTTP または TFTP）。

ステップ 3 [保存するアクション] で [バックアップ] を選択します。

ステップ 4 パラメータを入力します。

- **[TFTP サーバ]**（TFTP のみ）：TFTP サーバの IP アドレスを指定します。IP コンフィギュレーションで DNS が有効になっている場合は、サーバのドメイン名を指定します（「ドメイン ネーム システム」を参照）。
- **[宛先ファイル名]**（TFTP のみ）：保存されているファイルの名前を、TFTP サーバ上でのパスを含めて指定します。
- **[ソースファイルタイプ]**：コンフィギュレーション ファイル タイプを選択します。
  - **[実行コンフィギュレーション]**：現在の管理セッションで適用したすべての変更内容を含む、最新の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]**：フラッシュ メモリに保存されているコンフィギュレーション ファイル。このファイルには、RAM に適用したがまだスイッチに保存されていないコンフィギュレーションの変更内容は含まれていません。
  - **[バックアップコンフィギュレーション]**：バックアップとして使用する、スイッチに保存されている追加のコンフィギュレーション ファイル。管理者は、バックアップ 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 タイプにコピーし、スイッチをリブートしてバックアップ コンフィギュレーション ファイルを使用することができます。
  - **[ミラーコンフィギュレーション]**：実行コンフィギュレーションが 24 時間以上変更されていない場合、それがミラー コンフィギュレーション ファイル タイプに自動的に保存され、新しいミラー ファイルが使用可能であることを示す、重大度が**アラート**のログメッセージが生成されます。この機能により管理者は、スタートアップ コンフィギュレーション ファイル タイプに保存する前に以前のバージョンのコンフィギュレーションを確認したり、ミラー コンフィギュレーション ファイル タイプを別のコンフィギュレーション ファイル タイプにコピーすることができます。スイッチがリブートすると、ミラー コンフィギュレーションは工場出荷時のデフォルト パラメータにリセットされます。
  - **[フラッシュログ]**：フラッシュ メモリに保存されたイベントのログ。

- **[操作ログ]**：スイッチの RAM 内にあり、フラッシュ メモリに保存されていないイベントのログ。
- **[スタートアップログ]**：スタートアップ メッセージのログ。

ステップ 5 [適用] をクリックします。

HTTP 経由でのバックアップの場合、ファイルの保存場所を指定するように求められます。進捗状況バーに、ファイル転送のステータスが示されます。

コンフィギュレーションの削除

[コンフィギュレーションの削除] ページでは、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 コンフィギュレーションを削除できます。スタートアップ コンフィギュレーション ファイルとバックアップ コンフィギュレーション ファイルを両方とも削除した場合、スイッチはリブート時にデフォルトのコンフィギュレーション ファイルを使用します。

スタートアップ コンフィギュレーション ファイルまたはバックアップ コンフィギュレーション ファイルを削除するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで [各種管理] > [ファイル管理] > [コンフィギュレーションの削除] の順にクリックします。

ステップ 2 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 コンフィギュレーション ファイル タイプを選択します。

ステップ 3 [適用] をクリックします。

コンフィギュレーション ファイルのコピーと保存

[コンフィギュレーションのコピー / 保存] ページでは、ファイル システム内のファイルをコピーできます。たとえば、バックアップ 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 ファイルにコピーして、スイッチを次回ブートしたときにそれが使用されるようにすることができます。

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 ファイルにコピーするには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで [各種管理] > [ファイル管理] > [コンフィギュレーションのコピー / 保存] の順にクリックします。

ステップ 2 [ソースファイル名] を選択します。

- **[実行コンフィギュレーション]**：現在の管理セッションで適用したすべての変更内容を含む、最新の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]**：スイッチが前回のブート時に使用したコンフィギュレーション ファイル タイプ。このファイルには、適用したがまだスイッチに保存されていないコンフィギュレーションの変更内容は含まれていません。
- **[バックアップコンフィギュレーション]**：スイッチに保存されているバックアップ コンフィギュレーション ファイル タイプ。
- **[ミラーコンフィギュレーション]**：実行コンフィギュレーションが 24 時間以上変更されていない場合、それがミラー コンフィギュレーション ファイル タイプに自動的に保存され、新しいミラー コンフィギュレーション ファイルが使用可能であることを示す、重大度が**アラート**のログメッセージが生成されます。ミラー コンフィギュレーション ファイルは、スイッチがスタートアップ コンフィギュレーション ファイル タイプまたはバックアップ コンフィギュレーション ファイル タイプでブートできないときに使用することができます。そのような場合、管理者はミラー 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 タイプまたはバックアップ コンフィギュレーション ファイル タイプにコピーしてリブートすることができます。

ステップ 3 [宛先ファイル名] で、コピーするファイルで上書きするファイル タイプを選択します。

- **[スタートアップコンフィギュレーション]**：スイッチが前回のブート時に使用したコンフィギュレーション ファイル タイプ。このファイルには、適用したがまだスイッチに保存されていないコンフィギュレーションの変更内容は含まれていません。
- **[バックアップコンフィギュレーション]**：スイッチに保存されているバックアップ コンフィギュレーション ファイル タイプ。

ステップ 4 [適用] をクリックして、コピーを開始します。

完了すると、「コピー操作に成功しました。」というメッセージがウィンドウに表示されます。

DHCP 自動コンフィギュレーション

コンフィギュレーションを容易に展開およびアップグレードできるように、スイッチは DHCP での自動コンフィギュレーションをサポートしています。この機能により、ブート時にデバイス ストレージでコンフィギュレーション ファイルが見つからなかった場合、または新しいコンフィギュレーション ファイルがダウンロード可能な場合に、スイッチの自動コンフィギュレーションが可能になります。

（注） 自動コンフィギュレーション機能を使用するには、DHCP または BOOTP サーバ、TFTP サーバ、DNS サーバ（必要な場合）を含む、ネットワーク内の他のデバイスが正しく設定されている必要があります。

概要

スタートアップ時に、スイッチは DCHP サーバと通信して IP アドレスと他の情報を取得します。自動コンフィギュレーションが有効になっている場合、スイッチは、DHCP サーバから受け取った TFTP サーバとスタートアップ コンフィギュレーション ファイル名に応じて、スタートアップ コンフィギュレーション ファイルもダウンロードすることがあります。自動コンフィギュレーションはデフォルトで有効になっています。

DHCP 自動コンフィギュレーションは、自動コンフィギュレーションが有効になっている状態でスイッチがリブートし、次のいずれかの条件が満たされた場合に開始されます。

1. TFTP サーバとスタートアップ コンフィギュレーションに関する情報が DHCP サーバから受信され、自動コンフィギュレーションによって以前にコンフィギュレーション ファイルがダウンロードされていない。
2. TFTP サーバとスタートアップ コンフィギュレーションに関する情報が DHCP サーバから受信され、コンフィギュレーション ファイル名が以前の DHCP メッセージでアドバタイズされたファイル名と異なる。
3. スタートアップ コンフィギュレーション ファイルが存在せず、TFTP サーバまたはスタートアップ コンフィギュレーションに関する情報が DHCP サーバから受信されていない。

条件 1 および 2 に該当する場合、スイッチはファイルをフラッシュ メモリに保存します。その後のスタートアップで、スイッチは保存されているファイル名と、最新の DHCP メッセージのオプション 66/67 に指定されている名前を比較します。名前が異なる場合は、新しいファイルをダウンロードして、フラッシュ メモリに書き込みます。

（注） システムが初めてブートしたとき、スイッチはスタートアップ コンフィギュレーション ファイルをまだダウンロードしていないため、スイッチには DHCP サーバから受信したコンフィギュレーション ファイルの特定の名前がありません。これらのオプションが DHCP メッセージで受信されると、そのファイル名が保存され、ダウンロード処理が開始されます。

条件 3 に該当する場合、**「デフォルト ネットワーク コンフィギュレーション ファイル」**で説明されているように、スイッチは TFTP サーバとスタートアップ コンフィギュレーション ファイルを検索します。

DHCP サーバのメッセージの詳細

次のフィールドが BOOTP または DHCP サーバによって返され、スイッチによって処理される可能性があります。

- TFTP サーバからダウンロードするコンフィギュレーション ファイルの名前（ブートファイルまたはオプション 67）。
- ブートファイル取得元の TFTP サーバの識別情報。

  TFTP サーバの IP アドレスは、DHCP の応答内の複数のソースから推論することができます。スイッチは、次の条件に基づいて選択を行います。条件は、優先度の高い順に示しています。

  1. DHCP または BOOTP の応答内の **sname** フィールド
  2. DHCP の応答内の **TFTP server name (option 66)** フィールド
  3. DHCP の応答内の **TFTP server address (option 150)** フィールド
  4. DHCP または BOOTP の応答内の **siaddr** フィールド

  sname またはオプション 66 の値のみがスイッチに返された場合は、TFTP サーバの IP アドレスを解決するのに DNS サーバが必要です。スイッチに IP アドレスが割り当てられた後、ホスト名が割り当てられていない場合、自動コンフィギュレーションは対応するホスト名の DNS 要求を送信します。

代替 TFTP サーバとファイル名

[DHCP 自動コンフィギュレーション] ページで、代替 TFTP サーバを設定して、DHCP サーバによって提供されたサーバまたはファイル名が見つからない場合に使用するファイル名を設定できます。次の処理が行われます。

1. スイッチはユニキャスト メッセージを DHCP を通じて特定された TFTP サーバ（提供された場合）に送信します。
2. DHCP 情報が提供されなかった場合、あるいはサーバまたはファイル名が見つからない場合、サーバは代替情報（設定されている場合）を使用します。
3. 代替情報が設定されていない場合、あるいはサーバまたはファイル名が見つからない場合、スイッチは DHCP を通じて特定された TFTP サーバにブロードキャスト メッセージを送信します。

コンフィギュレーション ファイルのダウンロードの詳細

スイッチは、まずホスト固有のコンフィギュレーション ファイルのダウンロードを試行します。これが不可能な場合、[デフォルトのネットワーク構成モード] が有効になっていれば、コンフィギュレーション ファイル <hostname>.cfg をダウンロードします。

ホスト固有のコンフィギュレーション ファイル

スイッチは、ホスト固有のコンフィギュレーション ファイルのダウンロードを試行します。このファイル名は、DHCP/BOOTP サーバからの応答内でブートファイル名として指定されているか、DHCP 自動コンフィギュレーションのバックアップ コンフィギュレーション ファイルとして設定されています。スイッチは、指定されたブートファイル用の 3 つのユニキャスト TFTP 要求を行います。ユニキャストの試行が失敗したか、TFTP サーバ アドレスが提供されなかった場合、スイッチは使用可能なあらゆる TFTP サーバに対して、指定されたブートファイルに関する 3 つのブロードキャスト要求を行います。スイッチは、コンフィギュレーション ファイルを取得すると、コンフィギュレーションにエラーがないか検証します。検証が正常に完了すると、スイッチは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 タイプにコピーし、コンフィギュレーション ファイル名を不揮発性メモリに保存して、ユニットをリブートします。

（注） ブートファイル名は *.cfg である必要があります。

デフォルト ネットワーク コンフィギュレーション ファイル

[デフォルトのネットワーク構成モード] が有効になっている場合、次のいずれかの条件が満たされたときにスイッチはコンフィギュレーション ファイル <hostname>.cfg をダウンロードします。

- ホスト固有のコンフィギュレーション ファイルが指定されていない、または設定されていない。
- ホスト固有のコンフィギュレーション ファイルが TFTP サーバに存在しない。
- ダウンロード中に障害が発生した。

コンフィギュレーション ファイル内のホスト名を解決するために、スイッチはまず TFTP サーバから fp-net.cfg をダウンロードします。fp-net.cfg ファイルは、デフォルト ネットワーク コンフィギュレーション ファイルと呼ばれ、1 つまたは複数の「IP アドレス - ホスト名」のマッピングが含まれています。スイッチは、IP アドレスを使用してマッピングからホスト名を判断します。マッピングがない場合、スイッチは逆引き（逆 DNS ルックアップ）を行ってホスト名を見つけます。

fp-net.cfg ファイルの例を次に示します。

```
config
  ...
  ip host switch_to_setup 192.168.1.10
  ip host another_switch 192.168.1.11
  ... <other hostname definitions>
exit
```

ホスト名が判明すると、スイッチは「*<hostname>*.cfg」という名前のファイルの TFTP 要求を発行します。*<hostname>* はスイッチのホスト名の最初の 8 文字です。

スイッチは IP アドレスを使用して、逆引き（逆 DNS ルックアップ）を行います。たとえば、スイッチの IP アドレスが 192.168.1.10 の場合、ホスト名は **switch_t.cfg**（上記の例の最初の 8 文字）になります。

デフォルトのスイッチ名は、switch に 16 進数のアドレスの末尾 6 桁が付加された名前になります。マッピング ファイルには、**ip host switchD99FA5 192.168.1.10** などのホスト名が含まれています。この場合、IP アドレスが **192.168.1.10** のスイッチの <hostname.cfg> 形式のホスト名は **switchD9.cfg** になります。

スイッチが IP アドレスをホスト名にマップできない場合、自動コンフィギュレーションでは、デフォルト コンフィギュレーション ファイル **host.cfg** の TFTP 要求を送信します。

スイッチは、デフォルト コンフィギュレーション ファイルを取得すると、コンフィギュレーションにエラーがないか検証します。検証が正常に完了すると、スイッチは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 タイプにコピーしてリブートします。この場合、デフォルト コンフィギュレーション ファイル名は不揮発性メモリに保存されません。

（注） スイッチが有効なコンフィギュレーション ファイルを取得できない場合、スイッチが有効なコンフィギュレーション ファイルを取得するまで、上記のプロセスが 20 分ごとに繰り返されます。管理者は、実行コンフィギュレーションを手動で保存して、スタートアップ コンフィギュレーション ファイルを作成できます。また、管理者は、必要に応じて自動コンフィギュレーションを無効にすることもできます。

次の表に、ダウンロード可能なコンフィギュレーション ファイルと、それらが検索される順番を示します。

検索順	ファイル名	説明	最終版のファイルの検索
1	<bootfile>.cfg	ホスト固有のコンフィギュレーション ファイル。ファイル名の末尾は *.cfg ファイル拡張子[1]	あり
2	fp-net.cfg	デフォルト ネットワーク コンフィギュレーション ファイル	なし
3	<hostname>.cfg	ホスト固有のコンフィギュレーション ファイル。ホスト名に関連付けられる	あり
4	host.cfg	デフォルト コンフィギュレーション ファイル	あり

1. 「代替 TFTP サーバとファイル名」で説明されているとおり、このファイル名は DHCP を通じて得るか、手動で設定します。

オペレータは、ファイルをダウンロードする前に、いつでも自動コンフィギュレーションを終了することができます。スイッチがネットワークから切断されている場合、または必要なコンフィギュレーション ファイルが TFTP サーバ上にセットアップされていない場合に、このようにする必要があります。

コンフィギュレーション ファイルが正常にダウンロードされて、スタートアップ コンフィギュレーション ファイル タイプに保存されると、スイッチはリブートする前に重大度がアラートのメッセージをログに記録します。

DHCP 自動コンフィギュレーションの設定

[DHCP 自動コンフィギュレーション] ページを使用して、機能を有効または無効にしたり、TFTP サーバとファイル名の設定を行ったり、ステータス情報を表示することができます。

DHCP 自動コンフィギュレーションを有効にすると、DHCP クライアントから通知を受け取るまで [ブートオプションの待機中] 状態になります。DHCP クライアントは DHCP サーバから IP アドレスを受け取ると自動インストール プロセスをトリガし、その後ステータスが [DHCP/BOOTP オプションの処理および前提条件のチェック中] に変わります。

次の追加メッセージが表示されることがあります。

- ブートオプションの待機中
- DHCP/BOOTP オプションの処理および前提条件のチェック中
- ダウンロード中: tftp://<tftp address>/<filename>
- ダウンロード済みコンフィギュレーションの適用中
- タイムアウト再開の待機中
- ダウンロード済みコンフィギュレーションの保存中
- 中止されました
- 自動インストールが完了しました。
- 検証に失敗したため、自動インストール処理が中止されました。
- ダウンロード済み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への保存に失敗したため、自動インストール処理が中止されました。
- スタートアップコンフィギュレーションが手動で作成されていたため、自動インストール処理が中止されました
- 最後にダウンロードされたファイルとブートファイルが一致したため、自動インストール処理が中止されました。
- ブートファイル名を解決できなかったため、自動インストール処理が中止されました。

DHCP 自動コンフィギュレーションを設定するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで [各種管理] > [ファイル管理] > [DHCP 自動コンフィギュレーション] 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。

- **[DHCP 自動コンフィギュレーション]**：[有効] を選択すると、スイッチでこの機能が有効になります。
- **[デフォルトのネットワーク構成モード]**：[有効] を選択すると、ホスト固有のファイルがスイッチで見つからなかった場合に、スイッチは fp-net.cfg という名前のデフォルト コンフィギュレーション ファイルをダウンロードします。詳細については、**「デフォルト ネットワーク コンフィギュレーション ファイル」**を参照してください。
- **[代替 TFTP サーバ]**：バックアップとして機能する TFTP サーバの IP アドレスを指定します。代替 TFTP サーバは、オプション 66 で指定された TFTP サーバへのユニキャスト要求が 3 回失敗すると使用されます。
- **[代替コンフィギュレーションファイル]**：バックアップとして機能する代替コンフィギュレーション ファイルの名前を指定します。DHCP オプション 67 でスタートアップ コンフィギュレーション ファイルが示されていない場合、または指定されたファイルが TFTP サーバで見つからなかった場合、自動コンフィギュレーションは代替ファイル名を検索します。
- **[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]**：最後に自動コンフィギュレーション プロセスが実行されたときに使用されたコンフィギュレーション ファイルの名前。DHCP を通じて異なるファイル名が示された場合、ファイルのダウンロード処理が開始されます。
- **[現在のステータス]**：自動コンフィギュレーション プロセスのステータス。「自動インストールが完了しました。」または「処理中」と表示されます。

ステップ 3 [適用] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

HTTP 経由でのファームウェア リカバリ

スイッチには、ダウンロードが失敗した後に、スイッチ上の有効なイメージを復元することが可能なファームウェア リカバリ機能があります。イメージのダウンロード中に電源が遮断された場合、スイッチはブートできないことがあります。この場合、イメージは使用不能になりますが、ファームウェア イメージをフラッシュ メモリから RAM にロードするブート ローダ ファイルは引き続き機能します。HTTP サーバはブート ローダ ファイルに組み込まれており、これにより管理者はスイッチ ポート経由でスイッチに接続し、Web ブラウザを使用して新しいファームウェア イメージをダウンロードしてインストールすることができます。

スイッチがブートし、ブート ローダがフラッシュ メモリで有効なイメージを見つけることができなかった場合、スイッチは HTTP ファームウェア リカバリ モードになります。このモードで、ブート ローダはスイッチの内部ネットワーク ポートを次のスタティック IP アドレスに設定します。

- IP アドレス：192.168.1.254
- ネットワーク マスク：255.255.255.0
- デフォルト ゲートウェイ：192.168.1.1

HTTP サーバが起動して、ポート 80 でクライアント接続を待ち受けます。

この機能を使用して、新しいファームウェア イメージをダウンロードするには、次の手順に従います。

ステップ 1 管理用 PC をスイッチの任意のポートに直接接続します。

ステップ 2 スイッチと同じサブネットになるように、管理用 PC で IP アドレスとマスクを設定します。

（注）：デフォルト ゲートウェイの IP アドレスが 192.168.1.1 の場合は、ネットワーク経由でシステムにアクセスできます。

ステップ 3 Web ブラウザを開いて、アドレス バーにスイッチの IP アドレスを入力します（192.168.1.254）。

（注）：HTTP ファームウェア リカバリ機能は、次のブラウザをサポートしています。

- Firefox 3.0 以降
- Internet Explorer 6 以降

ファームウェア リカバリ ページが表示されます。認証は必要ありません。

Web ページに、スイッチの PIC VID（製品 ID とベンダー ID）、シリアル番号、MAC アドレスが表示されます。

ステップ 4 [参照] をクリックして、ダウンロードする有効なファームウェア イメージを選択します。

ファイルのダウンロード中は、進捗状況バーが表示されます。ダウンロードが正常に完了すると、次のメッセージが表示されます。

100% Complete
File downloaded successfully. Please wait while the file is being written to flash.

管理者が選択したファイルは RAM にダウンロードされ、次の条件を満たしているかどうか検証されます。

- ファイル CRC が良好である。
- STK ファイルがこのプラットフォーム用に構築されている。
- STK ファイルのサイズがパーティション制限値以内である（このファイル用に予約済みのサイズは 4.5 MB）。

これらの条件を満たした場合、ファイルがフラッシュ メモリに書き込まれ、システムは新しいファームウェアを使用してリブートします。

これらのいずれかのチェックに失敗すると、イメージはフラッシュ メモリに書き込まれず、リカバリ プロセスが停止します。正しいイメージ ファイルを使用すれば、リカバリ プロセスをやり直すことができます。

ブラウザ ウィンドウを更新した、または閉じたことにより、転送が中断された場合は、セッションがクリアされ、ただちにタイムアウトになります。ネットワークに到達できないために転送が中断された場合は、45 秒後にセッションがタイムアウトになります。セッションがタイムアウトになった後に、リカバリ プロセスを再度開始することができます。

スイッチのリブート

[リブート] ページを使用して、スイッチをリブートできます。スイッチをリブートするには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで [各種管理] > [リブート] の順にクリックします。

ステップ 2 次のいずれかのオプションを選択します。

- **[リブート]**：保存されている最新のコンフィギュレーションを使用してスイッチをリブートします。
- **[工場出荷時設定に戻す]**：工場出荷時のコンフィギュレーション ファイルを使用してスイッチをリブートします。カスタマイズした設定はすべて失われます。

リブートを了承またはキャンセルすることが可能な確認ウィンドウが表示されます。現在の管理セッションが終了される場合があります。

ステップ 3 リブートを了承またはキャンセルします。

ホストの Ping

スイッチから指定した IP アドレスに Ping 要求を送信するには、[Ping] ページを使用します。この機能を使用して、スイッチが特定のネットワーク ホストと通信できるかどうかチェックすることができます。

ネットワーク ホストを Ping するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで [各種管理] > [Ping] の順にクリックします。

ステップ 2 [アドレスタイプ] で [IPv4] または [IPv6] を選択します。

ステップ 3 IPv4 アドレスの場合は、次のパラメータを入力します。

- **[IP アドレス / ホスト名]**：スイッチで Ping するステーションの IP アドレスまたはホスト名を入力します。
- **[カウント]**：送信する Ping の数を指定します。
- **[間隔 (秒)]**：Ping の送信間隔を秒単位で指定します。
- **[データグラムサイズ]**：送信する Ping パケットのデータ サイズを指定します。

IPv6 アドレスの場合は、次のパラメータを入力します。

- **[Ping タイプ]**：ローカル サブネット外部のアドレスを Ping するには [グローバル] を選択します。ローカル サブネット上のアドレスを Ping するには [リンクローカル] を選択します。
- **[IPv6 アドレス / ホスト名]**：（グローバル アドレスのみ）128 ビットのグローバル アドレスを入力します。
- **[IPv6 リンクローカルアドレス]**：（リンク ローカル アドレスのみ）アドレスがスイッチと同じサブネット上にある場合は、リンク ローカル アドレスを入力します。
- **[データグラムサイズ]**：送信する Ping パケットのデータ サイズ（48 ～ 2048 バイト）を指定します。

ステップ 4 [適用] をクリックして、Ping を送信します。[Ping] ウィンドウでステータスを確認できます。

制御パケットの転送の設定

[制御パケットの転送] ページを使用して、スイッチが次のプロトコル タイプのパケットをどのように処理するかを設定できます。

- CDP：Cisco Discovery Protocol。さまざまなタイプのシスコ ネットワーク機器でサポートされています。CDP により、直接接続されているデバイスが IP アドレス、機能、ソフトウェア バージョンなどの情報を共有することができます。スイッチ自体は CDP をサポートしていませんが、デフォルトで VLAN 内の接続されているデバイスに代わって CDP パケットを転送します。
- Dot1X：IEEE 802.1X プロトコルは、Extensible Authentication Protocol（EAP; 拡張認証プロトコル）パケットが LAN 上でどのようにカプセル化されるかを定義します。Dot1X は、ユーザを認証して、スイッチ ポートで使用可能なサービスへのユーザ アクセスを許可または拒否する機能を提供します。スイッチで Dot1X 機能を設定する方法については、802.1X の説明を参照してください。
- LLDP：ネットワーク デバイスは Link Layer Discovery Protocol を使用して、各自の機能を他のデバイスにアドバタイズします。スイッチで LLDP 機能を設定する方法については、LLDP-MED の説明を参照してください。

制御パケットの転送を設定するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで [各種管理] > [制御パケットの転送] の順にクリックします。

ステップ 2 設定するプロトコル（CDP、LLDP、DOT1X）を選択します。

ステップ 3 指定したタイプのパケットを受信したときのポートのアクションを選択します。

- **[ドロップ]**：選択したタイプのすべてのパケットがドロップされます。
- **[転送]**：選択したタイプのすべてのパケットが、指定した VLAN 内で転送されます。
- **[終了]**：パケットが受け入れられ、スイッチで処理されます。このオプションは、CDP パケットでは使用できません。

ステップ 4 [適用] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

診断

診断ページを使用して、カッパー ケーブルおよび光ファイバ ケーブルの仮想ケーブル テストの実行、ポートまたは VLAN 用の診断モニタのセットアップ、CPU 利用率データの確認を行うことができます。

[各種管理] > [診断] メニューで使用可能な設定ページの詳細については、次のトピックを参照してください。

- **「カッパー ポートのテスト」**
- **「ポート ミラーリングの設定」**
- **「CPU/メモリ利用率」**

カッパー ポートのテスト

カッパー ケーブルをテストするには、[カッパーポート] ページを使用します。これらの物理層診断機能は、ケーブルの断線箇所を判断するのに使用することができます。

[カッパーポートテーブル] に、各ポートと、最新のテストによって得られた次のデータが表示されます（ポートがテストされていない場合は、デフォルトのデータが表示されます）。

- **[テスト結果]**：最新のケーブル テストの結果。表示される値は次のとおりです。
  - **[ノーマル]**：ケーブルは正常に機能しています。
  - **[オープン]**：ケーブルが接続されていないか、コネクタが故障しています。
  - **[ショート]**：ケーブルが短絡しています。
  - **[未テスト]**：テストが実行されていません。
  - **[ケーブルステータステストに失敗しました]**：テストでケーブル ステータスを判断できませんでした。ケーブルは機能している可能性があります。
- **[障害個所までの距離]**：最新のケーブル テストで検出されたケーブル障害発生箇所のポートからの距離（メートル単位）（障害が存在する場合）。
- **[最終更新]**：前回ポートをテストした日時。
- **[ケーブル長]**：ケーブル長（メートル単位）。

カッパー ポート テストを開始するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで [各種管理] > [診断] > [カッパーポート] の順にクリックします。

ステップ 2 ポートを選択して [テスト] をクリックします。

ケーブル テスト実行中にポートにアクティブ リンクが存在する場合、テスト中はリンクが停止することがあります。テストの実行には数秒かかります。完了すると、テスト結果が示されたウィンドウが表示されます。

ポート ミラーリングの設定

ポート ミラーリング機能を使用して、ポートのネットワーク トラフィックをコピーして別のポートに送信し、ネットワーク アナライザで分析することができます。

ミラーリング セッションは、宛先プローブ ポートと少なくとも 1 つの送信元ポートで構成されます。プローブされる送信元ポートのトラフィックのミラー コピーは、送信元ポートから宛先プローブ ポートに転送されます。ネットワーク アナライザは、宛先プローブ ポートに接続してネットワーク トラフィックを解析できます。

宛先プローブ ポートとして設定されているポートは、セッションが動作的にアクティブである限りミラーリング ポートとして機能します。セッションが非アクティブになると、ポートは他のコンフィギュレーション パラメータに基づいてトラフィックを転送および受信します。

（注） ポートがプローブ ポートとして設定されている場合、スイッチはトラフィックを転送または受信しません。また、Ping にも応答しません。

[ポートミラーリング] ページを表示するには、ナビゲーション ウィンドウで [各種管理] > [診断] > [ポートミラーリング] の順にクリックします。

4 つのミラーリング セッションをコンフィギュレーションで使用できます。デフォルトではこれらは無効になっています。[ポートミラーリングのセッションテーブル] には、各セッションの次のフィールドが表示されます。

- **[セッション ID]**：モニタリング セッション ID 番号。
- **[管理モード]**：ポート ミラーリング セッションが有効か無効かを示します。
- **[宛先インターフェイス]**：この機能を有効にするには、この項目を選択して、送信元ポートのトラフィックが宛先プローブ ポートにミラーリングされるポートを選択します。
- **[送信元インターフェイス]**：このミラーリング セッションに参加するように選択された送信元インターフェイスのリスト。

[ポートミラーリングのソースインターフェイステーブル] には、各セッションに割り当てられている送信元インターフェイスが表示されます。[フィルタ] を選択し、セッション ID を選択して、1 つのセッションのデータを表示できます。

ポート ミラーリングを設定するには、まずセッションに送信元インターフェイスを割り当てる必要があります。その後、宛先ポートを定義して、セッションを有効にします。

ミラーリング セッションを設定するには、次の手順に従います。

ステップ 1 [ポートミラーリングのソースインターフェイステーブル] で [追加] をクリックします。

ステップ 2 セッション ID を選択します。

ステップ 3 送信元インターフェイスと、ミラーリングするトラフィックのタイプを選択します。

ステップ 4 [タイプ] ラジオ ボタンを使用して、送信元インターフェイスでの監視対象トラフィックの方向を指定します。

- **[Rx のみ]**：着信トラフィック
- **[Tx のみ]**：発信トラフィック
- **[Tx および Rx]**：着信トラフィックと発信トラフィックの両方

ステップ 5 [適用] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

手順を繰り返して、複数の送信元インターフェイスを同じセッションに割り当てることができます。ただし、送信元インターフェイスは、一度に 1 つのアクティブ セッションでのみ使用できます。

ステップ 6 [ポートミラーリングのセッションテーブル] で、アクティブにするセッションを選択して、[編集] をクリックします。

ステップ 7 [管理モード] で、[有効] を選択します。

ステップ 8 [宛先インターフェイス] で、[有効] を選択して、データをミラーリングする宛先インターフェイスを選択します。

ステップ 9 そのセッションに適用されたコンフィギュレーションをクリアするには、[リセットセッション] を選択します。

注意 ポートが宛先プローブ ポートとして設定されると、スイッチはそのポート上のトラフィックを転送または受信しなくなり、そのポートで受信した Ping に応答しなくなります。そのポート上の以前のコンフィギュレーション パラメータはすべてクリアされ、ポート コンフィギュレーションからミラーリングを削除したときにポートを設定し直す必要があります。

ステップ 10 [適用] をクリックしてから、[閉じる] をクリックします。プローブ セッションが開始します。

（注） プローブ セッションを終了するには、[ポートミラーリングのセッションテーブル] でセッションを選択して、[編集] をクリックします。[管理モード] チェックボックスをオフにして、[適用] をクリックし、[閉じる] をクリックします。

CPU/ メモリ利用率

[CPU/ メモリ利用率] ページを使用して、CPU およびメモリの利用率を監視できます。このページを表示するには、ナビゲーション ウィンドウで [各種管理] > [診断] > [CPU/ メモリ利用率] **の順にクリックします。**

このページには、次のデータが表示されます。

- **[リフレッシュレート]**：15、30、または 60 秒ごとに最新のデータでページを更新することを指定します。または、デフォルト [リフレッシュなし] のままにしておきます。
- **[CPU 利用率レポート]**：5 秒間、1 分間、および 5 分間の利用率。
- **[メモリ利用率レポート]**：次のデータが報告されます。
  - **[割り当てメモリ]**：オペレーティング システム（OS）が使用可能なメモリ容量。
  - **[空きメモリ]**：OS が使用可能な空きメモリ容量。
  - **[合計メモリ]**：割り当てメモリ、空きメモリ、ソフトウェア イメージのコードおよびデータ セクション用に予約済みのメモリを含む合計システム メモリ。

Bonjour の有効化

Bonjour により、マルチキャスト DNS（mDNS）を使用して、スイッチとそのサービスを検出できるようになります。Bonjour は、スイッチのサービスをネットワークにアドバタイズし、サポートしているサービス タイプのクエリーに応答し、スモール ビジネス環境でのネットワーク構成をシンプルにします。

スイッチは、次のサービス タイプをアドバタイズします。

- **Cisco-specific device description**（csco-sb; シスコ製デバイスの説明）：このサービスにより、クライアントは、シスコ製のスイッチおよびスモール ビジネス ネットワークに導入されているその他の製品を検出できるようになります。
- **管理ユーザ インターフェイス**：このサービスは、スイッチで使用可能な管理インターフェイスを特定します（HTTP）。

Bonjour 対応スイッチをネットワークに接続することで、あらゆる Bonjour クライアントは事前設定を行うことなく、管理インターフェイスを検出してアクセスできるようになります。

システム管理者は、インストールされている Internet Explorer プラグインを使用してスイッチを検出できます。Web ベースのスイッチ設定ユーティリティがブラウザでタブとして表示されます。

Bonjour は、IPv4 ネットワークと IPv6 ネットワークの両方で機能します。

Bonjour を通じてスイッチを検出できるようにするには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで [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] を選択します。

ステップ 3 [適用] をクリックします。

LLDP-MED

IEEE 802.1AB 規格である Link Layer Discovery Protocol（LLDP）は、LAN に常駐しているステーションが識別情報、機能、および物理的説明をアドバタイズする方法について規定しています。情報は、Type-Length-Value（TLV）構造体を構成する LLDP データ ユニット（LLDPDU）で交換されます。アドバタイズするポートを管理者が設定する情報に応じて、さまざまな TLV が LLDPDU に含まれる場合があります。

LLDPDU を通じて得た情報は MIB に保存され、SNMP などのネットワーク管理システムによって情報にアクセスできます。このフレームワークは拡張可能で、VoIP ネットワークなどの領域での高度な利用が可能です。

（注） LLDPDU は、情報のみを通信し、スイッチを自動的に設定することはしません。

スイッチは、LLDP プロトコルの拡張機能である LLDP Media Endpoint Discovery（LLDP-MED）をサポートしています。LLDP-MED により、LAN ポリシー、デバイス ロケーション、およびデバイス特性の自動検出、および Power-over-Ethernet（PoE）エンドポイントの自動管理が可能になります。

[各種管理] > [ディスカバリ - LLDP-MED] メニューで使用可能な設定ページの詳細については、次のトピックを参照してください。

- **「グローバル LLDP-MED プロパティの設定」**
- **「ポートでの LLDP-MED の設定」**
- **「LLDP-MED ポート ステータスの詳細」**
- **「LLDP-MED ネイバー情報」**

グローバル LLDP-MED プロパティの設定

LLDP-MED の [プロパティ] ページを使用して、この機能のグローバル パラメータを指定できます。

グローバル LLDP-MED プロパティを設定するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで [各種管理] > [ディスカバリ - LLDP-MED] > [プロパティ] の順にクリックします。

ステップ 2 [アセット ID] に、スイッチのアセット ID を入力します。これはインベントリ TLV でアドバタイズされます。

ステップ 3 ロケーションのパラメータを指定して、緊急コール用にスイッチの物理的ロケーションを特定します。

- **[サブタイプ]**：次のいずれかのオプションを選択して、スイッチのロケーションがどのように TLV で特定されるかを設定します。
  - **[座標ベース]**：スイッチのロケーションは、GPS 座標（16 進数形式）を使用して特定されます。
  - **[住所]**：スイッチのロケーションは、市区町村、番地、建物名など、ロケーションの地理的説明によって特定されます。
  - **[ELIN]**：スイッチのロケーションは、スイッチの Emergency Location Identification Number（ELIN; 緊急ロケーション識別番号）によって特定されます。
- **[座標]**：スイッチの GPS 座標（16 進数形式）。
- **[ELIN アドレス]**：ELIN 番号。
- **[国]**：市区町村が存在する国。
- **[市区町村]**：番地が存在する市区町村。
- **[番地]**：建物が存在する番地。
- **[建物名]**：スイッチが存在する建物。

ステップ 4 [適用] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

ポートでの LLDP-MED の設定

LLDP for Media Endpoint Devices（LLDP-MED）プロトコルは、ネットワークの設定とポリシー、デバイス ロケーション、Power-over-Ethernet 管理、およびインベントリ管理のために LLDP 規格に対する拡張機能を提供します。

[LLDP-MED ポート設定] ページを使用して、ポートでの LLDP-MED の動作を表示および設定できます。

ポートにこれらの設定を指定するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで [各種管理] > [ディスカバリ - LLDP-MED] > [LLDP-MED ポート設定] の順にクリックします。

[LLDP-MED ポート設定テーブル] の各エントリに、ポートの LLDP-MED 設定が表示されます。

ステップ 2 設定するポートを選択して、[編集] をクリックします。

ステップ 3 選択したポートの次の項目を指定します。

- **[LLDP-MED ステータス]**：選択すると、ポートでの LLDP-MED の動作が有効になります。
- **[コンフィギュレーション通知]**：選択すると、ネットワークでトポロジが変更されたときにスイッチが通知を送信できるようになります。

ステップ 4 ポートの LLDP アドバタイズメントに含める使用可能な TLV を選択します。

- **[ネットワークポリシー]**：VLAN ID、802.1p CoS 値、および DSCP 値。この情報は、音声 VLAN 機能（**「音声とメディア」**を参照）を実装するのに使用されます。
- **[ロケーション]**：スイッチの 16 進数の GPS ロケーション座標。
- **[PSE]**：接続された Power-over-Ethernet デバイスに給電可能な Power Sourcing Equipment（PSE; 給電装置）であるとポートが自身をアドバタイズするかどうかを示します。このオプションは SG200-08P デバイスでのみ表示されます。
- **[PD]**：Power-over-Ethernet で受電可能な受電装置であるとポートが自身をアドバタイズするかどうかを示します。このオプションは SG200-08 デバイスの ポート g1 でのみ選択できます。
- **[コンポーネント]**：ハードウェアおよびソフトウェアのバージョン情報。
- **[システム機能]**：ブリッジングなどのスイッチの基本的な機能を識別します。

ステップ 5 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

（注） [ネットワークポリシーの設定] をクリックして、メディア VLAN ページを表示できます（また、ナビゲーション ウィンドウで [VLAN 管理] > [音声とメディア] > [メディア VLAN] の順にクリックして表示することもできます）。このページでは、LLDP-MED アプリケーションを VLAN に割り当てたり、関連付けられているトラフィックのプライオリティを設定することができます。

LLDP-MED ポート ステータスの詳細

[LLDP-MED ポートステータス詳細] ページには、機能が有効になっているすべてのポートの LLDP-MED 設定が表示されます。このページを表示するには、ナビゲーション ウィンドウで [各種管理] > [ディスカバリ - LLDP-MED] > [LLDP-MED ポートステータス詳細] の順にクリックします。

[ポート] リストからポートを選択します。[ネットワークポリシー] テーブルに、LLDP を通じてアドバタイズされた各サービスまたはポリシーのフィールドが表示されます。

- **[メディアポリシーアプリケーションタイプ]**：音声など、LLDP ネットワーク ポリシーに関連付けられているサービスのタイプ。
- **[VLAN ID]**：ネットワーク ポリシーに関連付けられている VLAN ID。
- **[プライオリティ]**：ネットワーク ポリシーに関連付けられている 802.1p CoS 値。
- **[DSCP]**：ネットワーク ポリシーの DSCP 値。
- **[Tagged]**：ネットワーク ポリシーはタグ付き（tagged）VLAN に対して定義されています。

次のスイッチ パラメータがインベントリ TLV でアドバタイズされます。

- **[ハードウェアリビジョン]**：スイッチのハードウェア リビジョン ID。
- **[ファームウェアリビジョン]**：スイッチのファームウェア リビジョン番号。
- **[ソフトウェアリビジョン]**：スイッチのソフトウェア リビジョン番号。
- **[シリアル番号]**：スイッチのシリアル番号。
- **[製造業者名]**：スイッチの製造元名。
- **[モデル名]**：スイッチのモデル名。
- **[アセット ID]**：スイッチの LLDP-MED アセット ID。

次のスイッチ パラメータがシステム TLV でアドバタイズされます。

- **[シャーシ ID]**：スイッチのハードウェア アドレス。
- **[シャーシ ID サブタイプ]**：ハードウェア アドレスのタイプ。
- **[システムの説明]**：事前に設定されたシステムの説明。
- **[システム名]**：ユーザ設定のホスト名（[システム設定] ページを参照）。
- **[管理アドレスサブタイプ]**：管理 IP アドレスのプロトコル バージョン。

- **[管理アドレス]**：管理ポート IP アドレス（[IPv4 インターフェイス] ページまたは [IPv6 インターフェイス] ページを参照）
- **[ポート ID サブタイプ]**：ポート ID のタイプ。
- **[ポート ID]**：ポート ID。
- **[ポートの説明]**：ポートの説明。
- **[有効になっているシステム機能]**：スイッチで有効になっている機能。
- **[サポートされているシステム機能]**：スイッチがサポート対象として現在アドバタイズしている機能。

次のスイッチ パラメータがロケーション TLV でアドバタイズされます。

- **[サブタイプ]**：サポートされているロケーション情報のタイプ（住所、ELIN、座標ベース）。
- **[座標]**：スイッチの GPS 座標（16 進数形式）（座標ベースのロケーション情報タイプを使用した場合）。
- **[ELIN アドレス]**：ELIN 番号（このロケーション情報タイプを使用した場合）。
- **[国]**：市区町村が存在する国（住所ロケーション情報タイプを使用した場合）。
- **[市区町村]**：番地が存在する市区町村（住所ロケーション情報タイプを使用した場合）。
- **[番地]**：建物が存在する番地（住所ロケーション情報タイプを使用した場合）。
- **[建物名]**：スイッチが存在する建物名（住所ロケーション情報タイプを使用した場合）。

LLDP-MED ネイバー情報

[ネイバー情報] ページには、ネットワーク内の他の LLDP-MED 対応デバイスから受信した情報が表示されます。このページを表示するには、ナビゲーション ウィンドウで [各種管理] > [ディスカバリ - LLDP-MED] > [ネイバー情報] の順にクリックします。

[ネイバー情報テーブル] に、アドバタイズメントを受信した各 LLDP ネイバー デバイスについて、次のフィールドが表示されます。

- **[ローカルポート]**：LLDP アドバタイズメントを受信した、ローカル デバイス上のポート番号
- **[リモート ID]**：ネイバー デバイス上のポートの物理アドレス。
- **[デバイスクラス]**：リモート デバイスのアドバタイズされたクラス。

エントリを選択して [詳細] をクリックし、ネイバーからの LLDP-MED アドバタイズメントから得られた追加情報を表示できます。

[ネイバー情報詳細] ページには、次の情報が表示されます。

[MED 機能] :

- **[サポートされている機能]**：アドバタイズされたデバイスの機能。
- **[有効になっている機能]**：デバイスで有効になっているアドバタイズされた機能。
- **[デバイスクラス]**：リモート デバイスのアドバタイズされたクラス。

[ネットワークポリシー] :

- **[メディアポリシーアプリケーションタイプ]**：音声など、LLDP ネットワーク ポリシーに関連付けられているサービスのタイプ。
- **[VLAN ID]**：ネットワーク ポリシーに関連付けられている VLAN ID。
- **[プライオリティ]**：ネットワーク ポリシーに関連付けられている 802.1p CoS 値。
- **[DSCP]**：ネットワーク ポリシーの DSCP 値。
- **[不明]**：802.1p 値、DSCP 値のどちらもこのネットワーク ポリシーで設定されていません。
- **[Tagged]**：ネットワーク ポリシーはタグ付き（tagged）VLAN に対して定義されています。

[コンポーネント] :

- **[ハードウェアリビジョン]**：スイッチのハードウェア リビジョン ID。
- **[ファームウェアリビジョン]**：スイッチのファームウェア リビジョン番号。
- **[ソフトウェアリビジョン]**：スイッチのソフトウェア リビジョン番号。
- **[製造業者名]**：スイッチの製造元名。
- **[モデル名]**：スイッチのモデル名。
- **[アセット ID]**：スイッチの LLDP-MED アセット ID。

[ロケーション] :

- **[サブタイプ]**：次のいずれかのオプションを選択して、スイッチのロケーションがどのように TLV で特定されるかを設定します。
  - **[座標ベース]**：スイッチのロケーションは、GPS 座標（16 進数形式）を使用して特定されます。

- **[住所]**：スイッチのロケーションは、市区町村、番地、建物名など、ロケーションの地理的説明によって特定されます。
- **[ELIN]**：スイッチのロケーションは、スイッチの Emergency Location Identification Number（ELIN; 緊急ロケーション識別番号）によって特定されます。

▪ **[ロケーション情報]**：[サブタイプ] フィールドで指定された形式でのスイッチのロケーション情報。

[拡張 PoE]：

▪ **[PoE デバイスタイプ]**：PoE 機能がアドバタイズされた場合、このフィールドにはデバイスが Powered Device（PD; 受電装置）であるか Power Sourcing Equipment（PSE; 給電装置）であるかが示されます。

[拡張 PoE PD]：

このデバイスが PoE によって給電される場合、次のプロパティをアドバタイズできます。

▪ **[PoE 電力値]**：デバイスが要求した電力（ワット単位）。

▪ **[PoE 電源]**：受電装置の受電方法を示します。

- **[プライマリ]**：電源が直接デバイスに接続されています。
- **[バックアップ]**：デバイスは、PoE 給電装置から受電します。

▪ **[PoE 電力プライオリティ]**：[高]、[低]、[重要] のいずれかにより、すべての受電装置の合計要求電力よりも PoE 供給電力が少ない場合に、ポートにどのようなプライオリティが付けられているかを示します。

DHCP クライアント ベンダー オプションの設定

スイッチで DHCP クライアント機能を設定して、DHCP 要求にベンダー情報を含めることができます（DHCP オプション 60）。DHCP サーバは、ベンダー情報を使用して、識別されたハードウェア タイプや機能に基づいてクライアントを区別します。

DHCP ベンダー オプション文字列を設定するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで [各種管理] > [DHCP オプション] の順にクリックします。

このページには、ベンダー オプションと文字列に加え、DHCP サーバから時間帯情報を取得するときにスイッチが使用する形式が表示され、そのような情報が受信されたかどうかが示されます。DHCP から時間帯を取得するようにスイッチを設定する方法については、**「時間設定」**を参照してください。

ステップ 2 [ベンダーオプション] で [有効] を選択します。

ステップ 3 [ベンダーオプション文字列] テキスト ボックスに値を入力します。

ステップ 4 [適用] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

4

ポートの管理

この章では、スイッチのポートの設定方法、ポートを組み合わせてリンク アグリゲーション グループを作成する方法、およびポートの電源機能を設定する方法について説明します。

次のトピックが含まれています。

- 「ポート設定の指定」
- 「リンク アグリゲーション」
- 「PoE の設定」
- 「Green Ethernet」

ポート設定の指定

[ポート設定] ページでは、管理者設定として、ポートを有効または無効にしたり、ポート速度とデュプレックス モードの自動ネゴシエーションを設定することができます。また、このページを使用してポートのフロー制御を設定することもできます。

ポート情報を設定するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで [ポート管理] > [ポート設定] の順にクリックします。

ステップ 2 設定す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 選択したポートの次の項目を指定します。

- **[管理ステータス]**: ポートを有効にするには [アップ]、無効にするには [ダウン] を選択します。
- **[自動ネゴシエーション]**: スイッチが、接続されているデバイスと、ポート速度およびデュプレックス モードを自動ネゴシエートできるようにするには [有効] を選択します。[自動ネゴシエーション] を有効にすると、[管理ポート速度] および [管理デュプレックスモード] フィールドは編集不可になります。

- **[管理ポート速度]**：[自動ネゴシエーション] を無効にした場合は、ポートの対応速度として 10 Mbit/s または 100 Mbit/s を選択します。
- **[管理デュプレックスモード]**：[自動ネゴシエーション] を無効にした場合、ポートを半二重モードにするには [半二重]、全二重モードにするには [全二重] を選択します。
- **[管理アドバタイズメント]**：[自動ネゴシエーション] を有効にした場合は、ポートがネゴシエートする最大ポート速度とデュプレックス設定を選択します。[最大機能] を選択すると、ポートはハードウェアがサポートしている最大ポート速度とデュプレックス設定で自動ネゴシエートします。
- **[フロー制御]**：選択すると、IEEE 802.3x フロー制御が有効になります。フロー制御により、スイッチイングされるフレームの量にポートが追従できない場合にデータが失われるのを防止できます。有効にすると、ポート上のパケットよって使用されるメモリの量が事前に設定されたしきい値を超えた場合に、スイッチは PAUSE フレームを送信して、ポートのトラフィックを停止することができます。一時停止されたポートは、PAUSE フレームに指定されている時間にわたってパケットを転送しません。PAUSE フレームに指定されている時間が経過するか、使用率が指定された下限しきい値に戻ると、スイッチはポートを有効にして、再度フレームを伝送できるようにします。
- **[LAG のメンバ]**：ポートが LAG（Link Aggregation Group）のメンバであるかどうかを示します。LAG の設定方法については、**「リンク アグリゲーション」**を参照してください。
- **[MTU]**：最大伝送ユニットのサイズをバイト単位で指定します。MTU のデフォルト値は 1518 で、指定可能な範囲は 1518 ～ 9216 バイトです。

ステップ 4 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

リンク アグリゲーション

リンク アグリゲーションにより、1 つまたは複数の全二重イーサネット リンクを集約して、LAG（Link Aggregation Group）を形成することができます。スイッチは LAG を 1 つの物理ポートとして扱い、優れたフォールト トレランスおよび負荷分散機能を提供します。

LAG インターフェイスは、スタティックまたはダイナミックにすることができます。

- **スタティック LAG**：ポートは管理者が直接 LAG に割り当てます。設定が変更されるまでポートは LAG メンバのままになります。
- **ダイナミック LAG**：ダイナミック LAG は、1 つまたは複数の候補ポートとともに設定します。LAG は、候補ポートに接続するリモートデバイスと Link Aggregation Control Protocol Data Unit（LACPDU）を交換することによって形成されます。形成されると、LAG のポート数制限およびその他の要因によって LAG には適格なポートのサブセットのみが含まれることがあります。LAG のアクティブ メンバ ポートとして選択されていない候補ポートは、スタンバイ ポートです。スタンバイ ポートは、同じ LAG 内のアクティブ ポートで障害が発生した場合にアクティブ メンバとして選択されることがあります。

次のトピックでは、[ポート管理] > [リンクアグリゲーション] メニューで使用可能な設定ページに関する追加情報を提供しています。

- **「LAG の設定」**
- **「LAG 情報の設定」**
- **「LACP 情報の設定」**

LAG の設定

スイッチは最大 4 つの LAG をサポートしていて、LAG あたり 8 つのポートを割り当てることができます。[LAG 管理] ページを使用して、ポートを LAG と LACP に割り当てることができます。

このページを表示するには、ナビゲーション ウィンドウで [ポート管理] > [リンクアグリゲーション] > [LAG 管理] の順にクリックします。

4 つのダイナミック LAG がデフォルトで設定されていて、ch1 ～ ch4 の名前が付けられています。これらにポート メンバは割り当てられていません。また、これらは無効になっています。

LAG のトラフィックを中断することなく、LAG にポートを追加したり、LAG からポートを削除できます。

LAG には、VLAN のメンバシップを割り当てることができます。ただし、個々のポートは、LAG メンバになったときに個々の VLAN メンバシップを失います。LAG からポートを削除すると、ポートは、スタートアップ コンフィギュレーションに指定されている、以前に属していた VLAN に再度参加します。

LAG を設定するには、次の手順に従います。

ステップ 1 設定する LAG を選択して、[編集] をクリックします。

ステップ 2 選択した LAG で、次の項目を指定します。

- **[LAG 名]**：LAG を識別するための 15 文字以内の英数字を入力します。
- **[タイプ]**：LAG にポートを手動で割り当てる場合は [スタティック] を選択します。ポートが LACPDU を交換して LAG をダイナミックに形成できるようにするには、[ダイナミック] を選択します。
- **[ポートリスト]/[LAG メンバ]**：スタティック LAG にポートを追加するか、スタティック LAG からポートを削除するには、各ポートを選択し、左矢印または右矢印をクリックして、[ポートリスト] または [LAG メンバ] リストへ移動します。

ステップ 3 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

LAG 情報の設定

[LAG 設定] ページを使用して、管理者設定として、LAG を有効または無効にしたり、ロード バランシング設定を行うことができます。

LAG を設定するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで [ポート管理] > [リンクアグリゲーション] > [LAG 設定] の順にクリックします。

[LAG 設定テーブル] に、使用可能な各 LAG が表示されます。

ステップ 2 設定する LAG を選択して、[編集] をクリックします。

ステップ 3 選択した LAG で、次の項目を指定します。

- **[管理ステータス]**：[アップ] または [ダウン] を選択すると、管理者設定として、LAG が有効または無効になります。LAG を無効にすると、そのメンバ ポートはスタンドアロンの物理ポートとして動作します。

- **[ロードバランシングアルゴリズム]**：スイッチが LAG のメンバ ポート間で送信パケットをロード バランシングできるようにするには、いずれかのオプションを選択します。スイッチは、特定のパケットの伝送用にチャネル内のいずれかのリンクを選択します。スイッチは、オプションに表示されている順序で、ロード バランシングの各条件にプライオリティを付けます。次のオプションがあります。
  - **[送信元/宛先 MAC、VLAN、イーサタイプ、着信ポート]**：送信元 MAC アドレスと宛先 MAC アドレス、VLAN メンバシップ、イーサタイプ フィールド、およびパケットを受信したポート。
  - **[送信元/宛先 IP および TCP/UDP ポートフィールド]**：送信元 IP アドレスと宛先 IP アドレス、および IP パケット内の TCP または UDP ポート番号。

  IP パケット オプションを選択した場合、ポートで受信した非 IP パケットは、送信元 MAC アドレスと宛先 MAC アドレスを使用してロード バランシングされます。
- **[MTU]**：最大伝送ユニットのサイズをバイト単位で指定します。MTU のデフォルト値は 1518 で、指定可能な範囲は 1518 ～ 9216 バイトです。

ステップ 4 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

LACP 情報の設定

スイッチは Link Aggregation Control Protocol（LACP）を使用して、ダイナミック LAG の形成を自動化します。LACP 対応ポートは、プロトコル データ ユニット（LACPDU）を送信して、ネットワーク上で互いを検出して、LAG をネゴシエートします。

プロトコルの動作を表示および設定するには、[LACP] ページを使用します。

個々のポートの LACP 設定を指定するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで [ポート管理] > [リンクアグリゲーション] > [LACP] の順にクリックします。

[LACP インターフェイステーブル] に、スイッチ上の各ポートのローカル（アクター）およびリモート（パートナー）LACP 設定が表示されます。LACP アクター設定には、スイッチの [システムプライオリティ] と LACP メッセージ内のポートを一意に識別する [管理キー] があります。これらの値は設定できません。

LACP 情報を編集するには、次の手順に従います。

ステップ 1 設定するポートを選択して、[編集] をクリックします。

ステップ 2 選択したポートの次の設定を指定します。

- **[モード]**：このチェックボックスをオンにすると、ポートで LACP が有効になります。
- **[アクタータイムアウト]**：タイムアウトが経過すると、アクターからの情報が無効になります。
  - **[ショート]**：ショート LACP タイムアウトは、LACP パケットを伝送する短い周期的タイマーの 3 倍です。ショート LACP タイムアウトのデフォルト値は 3 秒です。
  - **[ロング]**：ロング LACP タイムアウトは、LACP パケットを伝送する長い周期的タイマーの 3 倍です。ロング LACP タイムアウトのデフォルト値は 90 秒です。
- **[パートナータイムアウト]**：タイムアウトが経過すると、パートナーからの情報が無効になります。
  - **[ショート]**：ショート LACP タイムアウトは、LACP パケットを伝送する短い周期的タイマーの 3 倍です。ショート LACP タイムアウトのデフォルト値は 3 秒です。
  - **[ロング]**：ロング LACP タイムアウトは、LACP パケットを伝送する長い周期的タイマーの 3 倍です。ロング LACP タイムアウトのデフォルト値は 90 秒です。

ステップ 3 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

PoE の設定

SG200-08P で、ポート 1 ～ 4 は、Power-over-Ethernet（PoE）Power Sourcing Equipment（PSE; 給電装置）として動作できます。PSE は、接続されている PoE Powered Device（PD; 受電装置）に給電できます。

SG200-08P スイッチの [ポート管理] > [PoE] メニューで表示可能な設定ページについては、次のトピックを参照してください。

- **「PoE プロパティの設定」**
- **「PoE ポート設定の指定」**

（注） これらの設定ページは、PSE 機能をサポートしていないスイッチでは表示されません。

PoE プロパティの設定

[プロパティ] ページを使用して、特定の条件を満たしたときにスイッチがトラップ メッセージを生成するかどうかを設定したり、現在の電力設定を表示できます。

PoE プロパティを設定するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで [ポート管理] > [PoE] > [プロパティ] の順にクリックします。

ステップ 2 次のパラメータを設定します。

- **[電力トラップしきい値]**：使用可能な合計システム電力の割合を指定します。PoE ポート上の要求電力がしきい値を超えた場合、ログにトラップが生成されます。
- **[電力管理モード]**：スイッチが複数のポートに供給する電力のプライオリティをどのように付けるかを選択します。
  - **[ポートプライオリティによる静的管理]**：プライオリティを使用して静的に電力を管理します。このアルゴリズムでは、ポートの設定されている電力制限とプライオリティに基づいて電力を事前に割り当てます。
  - **[ポートプライオリティによる動的管理]**：プライオリティを使用して動的に電力を管理します。このアルゴリズムでは、消費電力が、設定済みの制限およびプライオリティの範囲内である限りデバイスに電力を供給します。電力は事前に割り当てられません。

  スイッチが複数のポートに電力を供給する場合、どちらのモードでも、プライオリティの高いポートが優先されます。複数のポートのプライオリティが等しい場合、ポート番号が小さいポートが優先されます。
- **[リセットモード]**：[有効] を選択すると、スイッチはすべての PoE ポート ステート マシンを初期化できるようになります。

ステップ 3 [適用] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

（注） このページには、スイッチの PoE 電力に関する次のデータが表示されます。

- **[電力]**：現在の電力の状態を示します。[オン] の場合、スイッチは接続されているデバイスに PoE 経由で電力を供給しています。[オフ] の場合、スイッチは接続されているデバイスに PoE 経由で電力を供給していません。
- **[最大有効電力]**：スイッチがすべての PoE 対応ポートに供給することができる合計電力（ワット単位）です。

- **[しきい値電力]**：カットオフ電力値で、この値を超えた場合には追加の PD に電力が供給されなくなります。このしきい値は、[電力トラップしきい値] 設定を基に計算されます。
- **[割り当て電力]**：スイッチが実際に PoE ポートに供給している合計電力（ワット単位）です。

PoE ポート設定の指定

[ポート設定] ページを使用して、PSE として機能しているポートの設定を表示および指定できます。

ポートの PoE 設定を指定するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで [ポート管理] > [PoE] > [ポート設定] の順にクリックします。

[PoE 設定テーブル] に、PoE 動作で有効なポート、それらのプライオリティ、電力割り当て（ミリワット単位）、および各ポートのその他の設定が表示されます。

ステップ 2 設定するポートを選択して、[編集] をクリックします。

ステップ 3 次の設定を行います。

- **[PoE]**：[有効] ボックスをオンにすると、ポートが PSE として設定されます。
- **[電力プライオリティレベル]**：[重要]、[高]、または [低] を選択して、接続されているデバイスへの電力供給に関するポートのプライオリティ レベルを設定します。

  スイッチは、電力を要求するすべての接続済みデバイスに電力を供給できないこともあります。ポートのプライオリティにより、すべての有効なポート用の十分な電力容量を確保できない場合に電力を供給するポートが決まります。プライオリティ レベルが同じポートでは、ポート番号が小さいポートの方が、プライオリティが高くなります。特定の数のデバイスにピーク電力を供給しているシステムの場合、新しいシステムをプライオリティが高いポートに接続すると、プライオリティが低いポートに接続されているデバイスの電力が遮断され、新しいデバイスに電力が供給されます。
- **[電力制限タイプ]**：次のいずれかの方法を選択して、接続されているデバイスにスイッチが供給する電力を制限します。
  - **[Dot3AF]**：ポートで供給可能な最大電力は、検出された IEEE 802.3af クラスによって制限されます。
  - **[ユーザ定義]**：ポートで供給可能な最大電力は、ユーザが指定します。このオプションを選択した場合は、[電力割り当て] フィールドに値を指定します。

- **[LLDP-MED]**：ポートで供給可能な最大電力は、ポートに接続されたデバイスから受信した LLDP-MED TLV の値によって制限されます。デバイスによって指定される値は、3 ～ 16.2 ワットの範囲でなければなりません。値が範囲外の場合は、デフォルト値である 16.2 ワットが使用されます。

  注：[電力制限タイプ] で [LLDP-MED] を選択した場合、リモート デバイスからのプライオリティ設定は使用されません。スイッチは、ポートに設定された [電力プライオリティレベル] を使用します。

- **[Dot3AF および LLDP-MED]**：ポートで供給可能な最大電力は、ポートに接続されたデバイスから受信した LLDP-MED TLV の値によって制限されます。デバイスによって指定される値は、3 ～ 16.2 ワットの範囲でなければなりません。値が範囲外の場合は、最大電力が IEEE 802.3AF クラスによって制限されます。

- **[ユーザ定義および LLDP-MED]**：ポートで供給可能な最大電力は、ポートに接続されたデバイスから受信した LLDP-MED TLV の値によって制限されます。デバイスによって指定される値は、3 ～ 16.2 ワットの範囲でなければなりません。値が範囲外の場合は、最大電力が [電力割り当て] フィールドに指定した値によって制限されます。

- **[電力割り当て]**：[電力制限タイプ] に [ユーザ定義] オプションを設定した場合は、ポートに割り当てる電力を 3000 ～ 16200 ミリワットで入力します。
- **[検出タイプ]**：ポートに接続されている PoE 受電装置を検出するための方法を次の中から選択します。
  - **[レガシーのみ]**：受電デバイスのみが検出されます。
  - **[802.3af 4 ポイントのみ]**：抵抗デバイスのみが最初のアルゴリズムで検出されます。
  - **[802.3af 4 ポイントおよびレガシー]**：受電デバイスと抵抗デバイスの両方が 2 番目のアルゴリズムで検出されます。
  - **[802.3af 2 ポイントのみ]**：抵抗デバイスのみが最初のアルゴリズムで検出されます。
  - **[802.3af 2 ポイントおよびレガシー]**：受電デバイスと抵抗デバイスの両方が最初のアルゴリズムで検出されます。
- **[リセットモード]**：[有効] を選択すると、スイッチはポートの PoE ステート マシンを初期化できるようになります。

次の統計情報も表示されます。

- **[電力消費]**：ポートの実際の電力消費量。
- **[過負荷カウンタ]**：過電力発生総数。

- **[不足カウンタ]**：ポートでの電力不足発生総数。
- **[拒否カウンタ]**：受電装置に給電されなかった回数。
- **[不在カウンタ]**：受電装置が検出されなくなったために、受電装置への給電が停止された回数。
- **[無効な署名カウンタ]**：無効な署名が受信された回数。署名は、受電装置が PSE に自身を識別させるための手段です。署名は、受電装置の検出、分類、またはメンテナンス中に生成されます。

ステップ 4 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

Green Ethernet

それぞれのギガビット イーサネット カッパー ポートでは、スイッチがエネルギー検出モードと呼ばれる Green Ethernet 省電力機能を提供します。エネルギー検出モードは、カッパー リンク パートナーからの信号が存在しない場合にポート PHY を低電力モードに切り替えて、チップ電力を削減します （PHY とは、OSI モデルの物理層の短縮形です）。

エネルギー検出が有効になっている場合、ライン上のエネルギーが失われると、スイッチは自動的に低電力モードになります。エネルギーが検出されると、スイッチは通常動作に戻ります。ポート PHY が低電力モードになっている場合、PHY は一定時間後にウェイクアップし、リンク パルスを送信して、リンク パートナーからのエネルギーを監視します。ポートがウェイクアップ モードになっているときにエネルギーを検出した場合、スイッチはポートを通常動作に戻します。ウェイクアップ期間が経過すると、ポートは低電力モードに戻ります。

ショート リーチ自動モードを有効にすると、リンクが稼動したときにケーブル テストが実行されます。ケーブル長が 10 m 未満の場合、PHY は低電力モードになることがあり、短いケーブルをサポートするのに必要な電力しか使用されなくなります。リンクが停止すると、低電力モードが無効になります。

また、スイッチは、管理者設定としてポートが強制的に低電力モードになるショート リーチ強制もサポートします。

有効になっている場合、Green Ethernet 機能はポートの自動ネゴシエーションが有効になっているかどうかを問わず機能します。

Green Ethernet プロパティの設定

Green Ethernet 機能をグローバルに有効にするには、Green Ethernet の [プロパティ] ページを使用します。グローバル設定は、すべてのポートに適用されます。

（注） 個々のポートでこれらの機能を設定することでグローバル設定を上書きすることができます（**「Green Ethernet ポート設定の指定」**を参照）。その後、グローバル設定を変更すると、個々のポートのあらゆる設定が上書きされます。

Green Ethernet のグローバル プロパティを設定するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで [ポート管理] > **[Green Ethernet]** > **[プロパティ]** の順にクリックします。

デフォルトでは、エネルギー検出モードとショート リーチ自動モードがグローバルかつすべてのポートで有効になっています。

ステップ 2 設定を行います。

- **[エネルギー検出]**：[有効] を選択すると、スイッチのエネルギー検出モードが有効になります。ライン上のエネルギーが失われたときにスイッチは自動的に低電力モードになり、エネルギーが検出されたときに通常動作に戻ります。
- **[ショートリーチ自動]**：[有効] を選択すると、リンクが Green Ethernet ポートで稼動したときにケーブル テストが実行されます。短いケーブルが検出された場合、ポートは低電力モードになります。リンクが停止すると、低電力モードが無効になります。
- **[ショートリーチ強制]**：[有効] を選択すると、管理者設定として、すべてのポートがデフォルトで低電力モードになります。この設定は個々のポートで別の設定に上書きできます（**「Green Ethernet ポート設定の指定」**を参照）。

ステップ 3 [適用] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

Green Ethernet ポート設定の指定

個々のポートの Green Ethernet 設定を表示および指定するには、Green Ethernet の [ポート設定] ページを使用します。

（注） その後、グローバル設定を変更すると、Green Ethernet ポート設定が上書きされます（「Green Ethernet プロパティの設定」を参照）。

Green Ethernet ポート設定を指定するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで [ポート管理] > **[Green Ethernet]** > **[ポート設定]** の順にクリックします。

[Green Ethernet 設定テーブル] ページには、各ポートの次の情報が表示されます。

[エネルギー検出] フィールド

- **[管理]**：ポートでエネルギー検出が有効になっているかどうかを示します。
- **[動作]**：現在ポートでエネルギー検出モードが動作している（有効になっている）かどうかを示します。
- **[理由]**：動作ステータスが有効または無効になっている理由を示します。エネルギー検出動作ステータスが有効になっている場合、次の理由が表示されます。
  - **[エネルギー未検出]**：リンク上でエネルギーが検出されませんでした。

  エネルギー検出動作ステータスが無効になっている場合、次の理由が表示されます。
  - **[ファイバ]**：管理ステータスはアクティブになっている可能性がありますが、ポートはファイバ モードで動作しています（Green Ethernet 機能は、カッパー ポートにのみ適用されます）。
  - **[リンクアップ]**：リンク上にアクティビティが存在します。
  - **[管理ダウン]**：管理者の設定により、エネルギー検出モードが無効になっています。

[ショートリーチ] フィールド

- **[自動]**：管理者の設定により、ポートでショート リーチ モードが有効になっているかどうかを示します。
- **[強制]**：ポートでショート リーチ強制モードが有効になっているかどうかを示します。
- **[動作]**：ポートでショート リーチ モードが動作している（有効になっている）かどうかを示します。

- **[理由]**：ショート リーチ動作ステータスがアクティブまたは非アクティブである理由を示します。ショート リーチ動作ステータスが有効になっている場合、次の理由が表示されます。
  - **[短いケーブル]**：ポートにショート リーチ ケーブルが接続されていることが検出されました。
  - **[強制]**：管理者の設定により、ポートがショート リーチ モードになっています。

  ショート リーチ動作ステータスが無効になっている場合、次の理由が表示されます。
  - **[長いケーブル]**：ケーブル長が 10 m を超えています。
  - **[リンクダウン]**：リンクが停止しています。
  - **[ファイバ]**：ポートは、ファイバ モードで動作していて、Green Ethernet 動作に適格ではありません。
  - **[管理ダウン]**：管理者の設定により、ショート リーチが無効になっています。
  - **[非 GIG 速度]**：ポートは、1G の速度で動作していないため、Green Ethernet 動作に適格ではありません。
  - **[ケーブル長不明]**：ケーブル長を判断できませんでした。

ステップ 2 設定するポートを選択して、[編集] をクリックします。

ステップ 3 次の設定を行います。

- **[エネルギー検出]**：選択すると、管理者設定として、ポートでエネルギー検出が有効になります。
- **[ショートリーチ自動]**：選択すると、ポートでショート リーチ モードが有効になります。
- **[ショートリーチ強制]**：選択すると、ポートでショート リーチ強制モードが有効になります。

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に変更を保存します。

5

VLAN 管理

この章では、仮想 LAN を設定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。

- 「VLAN の作成」
- 「VLAN インターフェイスの設定」
- 「VLAN メンバシップの設定」
- 「ポート VLAN メンバシップの設定」
- 「デフォルト VLAN の設定」
- 「メディア VLAN」
- 「音声とメディア」

レイヤ 2 スイッチの Virtual LAN（VLAN; 仮想 LAN）は、ブリッジ処理とルーティング両方のいくつかの利点を実現します。ブリッジと同様に、VLAN スイッチは、レイヤ 2 ヘッダーに基づいてトラフィックを転送するため、処理が高速です。ルータと同様に、ネットワークを論理セグメントに区切ることで、管理がしやすくなり、セキュリティやマルチキャストトラフィックの管理が向上します。

VLAN は、エンド ステーションとそれらを接続するスイッチ ポートの組み合わせです。論理的な分割を行うのは、部門やプロジェクトのメンバシップを区別するため、などのさまざまな理由が考えられます。唯一の要件は、エンド ステーションと、接続されるポートの両方が、同じ VLAN に属していることです。

ネットワーク内の各 VLAN は、VLAN で送信されるパケットのレイヤ 2 ヘッダーで VLAN タグとも呼ばれる IEEE 802.1Q タグで表される VLAN ID に関連付けられています。エンド ステーションがタグそのもの、またはタグの VLAN 部分を含めなかった場合、パケットを受信する最初のスイッチ ポートはそのパケットを拒否するか、デフォルトの VLAN ID に一致するタグを挿入します。ポートは、複数の VLAN に対してトラフィックを処理できますが、Port VLAN ID（PVID; ポート VLAN ID）のみをサポートします。

スイッチでは、デフォルト VLAN として VLAN ID 1 が事前に設定されています。すべてのポートは、この VLAN のメンバであり、PVID として VLAN ID (1) を使用します。

VLAN の作成

[VLAN の作成] ページでは、ネットワーク上の VLAN を定義および設定できます。このページを表示するには、ナビゲーション ウィンドウで [VLAN 管理] > [VLAN の作成] の順にクリックします。

[VLAN テーブル] には、VLAN ID、名前（存在する場合）、および事前定義された VLAN（VLAN ID 1）および追加した VLAN が表示されます。デフォルト VLAN として 1 つのポートを設定する必要があります。その他すべてのポートのタイプは、スタティックです。スイッチでは、デフォルト VLAN として VLAN ID 1 が事前に設定されています。すべてのポートは、この VLAN のメンバであり、PVID として VLAN ID (1) を使用します。

追加の VLAN を作成する場合、それらのうちの 1 つをデフォルト VLAN として設定できます（**「デフォルト VLAN の設定」**を参照）。設定されたデフォルト VLAN は削除できません。スタティック VLAN は削除できます。ただし、VLAN ID 1 は、スタティック VLAN として設定された場合でも削除できません。

最大 16 の VLAN を作成でき、最大 4094 の VLAN ID を割り当てることができます。新しい VLAN または VLAN の範囲を作成するには、次の手順に従います。

ステップ 1 [追加] をクリックします。

ステップ 2 [VLAN] を選択して、[VLAN ID] を入力します。

または、[範囲] を選択して、範囲の最初と最後の VLAN ID を指定することで、VLAN の範囲を作成します。

ステップ 3 単一の VLAN を作成する場合は、参照しやすいように任意で VLAN 名を入力できます。

ステップ 4 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

VLAN インターフェイスの設定

[インターフェイス設定] ページを使用して、ポート VLAN のタギング機能を表示および設定できます。このページを表示するには、ナビゲーション ウィンドウで [VLAN 管理] > [インターフェイス設定] の順にクリックします。

[インターフェイス設定テーブル] には、各ポートの VLAN 設定が表示されます。Link Aggregation Group（LAG）の VLAN 設定を表示するには、[インターフェイスタイプ] リストから [LAG] を選択します。

VLAN インターフェイスを設定するには、次の手順に従います。

ステップ 1 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 2 選択したポートまたは LAG の次の設定を指定します。

- **[インターフェイス VLAN モード]**：（VLAN メンバシップおよびタギングに関して）ポート タイプを選択します。ポート VLAN ID（PVID）は、そのインターフェイスがメンバとして属するデフォルト VLAN を示します。スイッチ上の有効な VLAN ID に対しては、一般ポートの PVID を設定します。アクセス VLAN ID に対してはアクセス ポートの PVID を設定します。設定されているネイティブ VLAN ID に対してはトランク ポートの PVID を設定します。
  - **[一般]**：ポートは、1 つまたは複数のタグ付きまたはタグなし VALN のメンバになることができます。このモードにより、IEEE 802.1Q 規格の「VLAN タギング」で指定された機能がすべて有効になります。[一般] を選択した場合、PVID には、ポートがタグなしメンバである VLAN ID と同じ値を設定します。
  - **[アクセス]**：ポートはタグなしフレームのみを受け入れることができます。アクセス ポートは、1 つの VLAN のみのメンバになることができ、そのポートの VLAN ID（PVID）として VLAN ID を使用します。アクセス ポートは、通常、ホストの接続に使用されます。このホストはポートに物理的に接続されているので VLAN のメンバになります。[アクセス] を選択した場合、アクセス ポートは、アクセス VLAN と呼ばれる 1 つだけの VLAN のメンバになることができます。アクセス VLAN はアクセス ポートの PVID に設定します。
  - **[トランク]**：ポートは、ネイティブ VLAN という 1 つだけのタグなし VLAN に割り当てることができます。また、任意の数（または 0 個の）タグ付き VLAN のメンバに割り当てることができます。トランク ポートは、スイッチから他のネットワーク デバイス（アップストリーム ルータやエッジ スイッチなど）への、複数の VLAN のトラフィックを伝送します。

- **[PVID]**：（一般ポートのみ）ポート VLAN ID（PVID）は、インターフェイスがメンバとして属するデフォルト VLAN を示します。PVID には、ポートがタグなしメンバである VLAN ID と同じ値を設定します（アクセス ポートの場合、PVID はアクセス VLAN ID に自動的に設定されます。トランク ポートの場合、PVID は設定済みのネイティブ VLAN ID に設定されるか、指定がない場合はデフォルトの VLAN ID に設定されます）。
- **[ネイティブ VLAN]**：（トランク ポートのみ）ネイティブ VLAN は、トランク ポートの 1 つのタグなし VLAN のメンバシップを識別します。次のいずれかを選択します。
  - **[なし]**：ポートにはタグなし VLAN メンバシップがありません。ポートの PVID は、デフォルトの VLAN ID に設定されます。
  - **[デフォルト]**：ネイティブ VLAN がデフォルト VLAN になります。また、ポートの PVID もデフォルトの VLAN ID に設定されます。
  - **[ユーザ定義]**：ユーザが指定した VLAN ID がトランク ポートのタグなし VLAN メンバシップとして使用されます。また、ポートの PVID も指定された VLAN ID に設定されます。
- **[アクセス VLAN]**：（アクセス ポートのみ）アクセス ポートは、アクセス VLAN ID のみに設定されたメンバになることができます。
- **[フレームタイプ]**：ポートで受け入れられるフレーム タイプを指定します。
  - **[Untagged のみ通過]**：タグなし（untagged）フレームのみがポートで受け入れられます。タグ付きフレームは廃棄されます。
  - **[Tagged のみ通過]**：タグ付き（tagged）フレームのみがポートで受け入れられます。タグなしフレームは廃棄されます。
  - **[すべて通過]**：タグ付きとタグなしの両方のフレームがポートで受け入れられます。

  アクセス ポートは、タグなしフレームのみを通過させることができます。トランク ポートは、最大 1 つのタグなし VLAN のメンバと、1 つまたは複数のタグ付き VLAN のメンバになることができます。トランク ポートがタグなしとタグ付き両方の VLAN のメンバである場合、すべてのフレーム タイプを通過させます。トランク ポートがタグ付き VLAN のみのメンバの場合、タグ付きフレームのみを通過させます。
- **[入力フィルタリング]**：選択すると、ポートでの入力フィルタリングが有効になります。入力フィルタリングが有効な場合、スイッチは、自身がメンバである VLAN からのフレームだけを受け入れます。他の VLAN から受信したフレームは廃棄します。アクセス モードまたはトランク モードのすべてのポートでは、常に入力フィルタリングが有効です。入力フィルタリングの無効化および有効化は、一般モードに設定されたポートでだけ可能です。

- **[VLAN プライオリティ]**：ポートのデフォルトの 802.1p プライオリティ値。値は、ポートで設定された QoS 信頼モードとパケットのタイプに基づいて、着信パケットに適用されます。ポートの信頼モードの設定に関する情報と手順については、**「QoS プロパティ」**を参照してください。

ステップ 3 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

インターフェイス VLAN モードの変更

ポートのインターフェイス VLAN モードが変更されると、スイッチは、影響のある VLAN メンバシップの設定を次のように自動的に処理します。

アクセス ポートからトランク ポートへの変更

VLAN 設定は変更されません。アクセス ポートの VLAN は、トランク ポートのネイティブ VLAN になります。ポートは、トランク ポートの制約に従う必要があります。

トランク ポートからアクセス ポートへの変更

元のトランク ポートに、タグなし VLAN メンバがある場合、そのポートは、タグなし VLAN 以外のすべての VLAN から削除されます。PVID は、タグなし VLAN ID に設定されます。

元のトランク ポートに、タグなし VLAN メンバがない場合、そのポートはすべての VLAN から削除され、デフォルト VLAN のメンバになります。その PVID は、デフォルト VLAN ID に設定され、ポートはタグなし、またはプライオリティ タグ付きのパケットのみ通過するように設定されます。ポートはデフォルト VLAN に対してはタグなしです。

アクセス ポートから一般ポートへの変更

VLAN 設定は、ポートですべてのフレームが通過できるようになること以外、変更されません。一般ポートとして、このポートは任意の VLAN のタグ付きまたはタグなしのメンバになることができます。

一般ポートからアクセス ポートへの変更

一般ポートにポートの PVID を提供するタグなし VLAN メンバシップがない場合、ポートがアクセス ポートに変更されるとすべての一般ポートの VLAN から削除され、デフォルト VLAN のタグなしメンバになります。アクセス ポート PVID は、デフォルト VLAN に設定されます。

アクセス ポートは、タグなしまたはプライオリティ タグ付きのパケットのみを通過させます。

トランク ポートから一般ポートへの変更

VLAN 設定は変更されません。一般ポートとして、このポートは任意の VLAN のタグ付きまたはタグなしのメンバになることができます。

一般ポートからトランク ポートへの変更

VLAN 設定は変更されません。一般ポートの PVID は、トランク ポートのネイティブ VLAN を設定するために使用されます。ポートは、トランク ポートの制約に従う必要があります。

たとえば、一般ポートは、VLAN 1、10、および 20 のタグなしメンバで、ポートの PVID は 1 であるとします。

ポートがトランク ポートに変更された場合、VLAN 1 がネイティブ VLAN になります。トランク ポートは VLAN 10 および 20 のメンバのままですが、タギングが有効になります。

VLAN の削除

VLAN を削除する場合、次のアクションが発生します。

- 削除される VLAN がトランク ポートのネイティブ VLAN の場合、トランク ポートのネイティブ VLAN と PVID はデフォルト VLAN に変更されます。
- アクセス ポートが削除される VLAN のメンバである場合、アクセス ポートは、デフォルト VLAN のメンバになり、その PVID はデフォルト VLAN に変更されます。
- 一般ポートが PVID として VLAN ID を使用するように設定されていた場合、一般ポートの PVID はデフォルト VLAN ID に変更されます。その他の VLAN メンバシップは変更されません。

VLAN メンバシップの設定

次のページを使用して、VLAN メンバシップを表示および設定できます。

- [VLAN へのポート] ページでは、VLAN を選択し、そのメンバシップ ポートを設定できます。**「VLAN へのポートの設定」**を参照してください。
- [ポート VLAN メンバシップ] ページでは、ポートを選択して、そのポートを 1 つまたは複数の VLAN のメンバとして設定できます。**「ポート VLAN メンバシップの設定」**を参照してください。

デフォルトでは、すべてのポートは、VLAN 1 のメンバです。任意のポートの VLAN メンバシップを変更できます。VLAN メンバシップは、タグ付きまたはタグなしとして設定できます。

- スイッチがタグなしフレームを VLAN から受信した場合、スイッチは、VLAN のタグ付きメンバとして設定された出力ポートにフレームを転送する前に、VLAN タグを挿入します。
- スイッチがタグなしフレームを VLAN から受信した場合、スイッチは、VLAN のタグなしメンバとして設定された出力ポートに、そのままフレームを転送します。

- スイッチがタグ付きフレームを VLAN から受信した場合、スイッチは、VLAN のタグなしメンバとして設定された出力ポートにフレームを転送する前に、VLAN タグを削除します。
- スイッチがタグ付きフレームを VLAN から受信した場合、スイッチは、VLAN のタグ付きメンバとして設定された出力ポートに、フレームをそのまま転送します。

VLAN へのポートの設定

[VLAN へのポート] ページを使用して、ポートを VLAN に割り当てるには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで、[VLAN 管理] > [VLAN へのポート] の順にクリックします。

このページには、選択した VLAN ID とポートまたは LAG に対して、その VLAN に関連するポートごとのインターフェイス ポート モードの管理上の設定（アクセス、トランク、および一般）、メンバシップ、タグ付きオプション、および PVID が表示されます （この設定の手順については、**「VLAN インターフェイスの設定」**を参照）。

ステップ 2 設定する VLAN ID を選択し、[インターフェイスタイプ] リストを使用してポートまたは LAG のいずれかを表示します。

ステップ 3 インターフェイスごとに、次のパラメータを設定します。

- **[メンバ]**：ポートを VLAN のメンバにする場合は、このボックスをオンにします。ポートを VLAN のメンバにしない場合は、このボックスをオフにします。デフォルトでは、ポートは VLAN のメンバではありません。
- **[Tagged]**：ポートに出力する VLAN のパケットすべてをタグ付きにする場合は、[Tagged] を選択します。そうでない場合は、[Untagged] を選択します。トランクポートは、デフォルトではタグ付きです。このオプションは、ポートが VLAN のメンバである場合のみ関係があります。
- **[Untagged]**：VLAN からポートに出力されるパケットをタグなしにする場合、[Untagged] を選択します。そうでない場合は、[Tagged] を選択します。アクセスポートは、常にタグなしです。一般ポートは、デフォルトではタグなしです。このオプションは、ポートが VLAN のメンバである場合のみ関係があります。
- **[PVID]**：ポートが、選択した VLAN ID をそのポートの VLAN ID（PVID）として使用する場合、このボックスをオンにします。そうでない場合は、このボックスをオフにします。アクセス ポートまたはトランク ポートに対して PVID が選択された場合、ポートは VLAN のタグなしメンバである必要があります。ポートから受信したタグなしパケットは、対応する VLAN に割り当てられます。

ステップ 4 [適用] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

ポート VLAN メンバシップの設定

ポートの VLAN 設定を指定するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで、[VLAN 管理] > [ポート VLAN メンバシップ] の順にクリックします。

デフォルトでは、このページには各ポートの VLAN 情報が表示されます。LAG ポートの VLAN 情報の表示に、フィルタ設定を使用できます。このページには、インターフェイス VLAN モード（トランクまたはアクセス）、PVID、VLAN メンバシップが表示されます。ポートが複数の VLAN のメンバである場合、ポートを選択して [詳細] をクリックすると単一のポートの情報が表示されます。

ステップ 2 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 3 VLAN メンバシップを割り当てる、または削除するには、次の説明のように矢印ボタンを使用します。

- VLAN メンバシップを追加するには：[使用可能] リストで VLAN を選択して、必要に応じて [タギング] プロパティを変更します（下記参照）。その後、右矢印ボタンをクリックして、[選択済み] リストに移動します。
- VLAN メンバシップを削除するには：[選択済み] リストで VLAN を選択してから、左矢印ボタンをクリックして、[使用可能] リストに移動します。

タギングおよび PVID プロパティ

インターフェイス VLAN モード（トランク、アクセス、または一般）によって、VLAN を [使用可能] リストで選択するときに、VLAN をそのインターフェイスの [選択済み] リストに移動する前に、インターフェイスの次のプロパティを指定できる場合があります。

- **[メンバシップ]**：インターフェイスを、選択した VLAN のタグ付きまたはタグなしのメンバとして設定できます。
  - **[Tagged]**：選択した場合、ポートは選択した VLAN のタグ付きメンバになります。スイッチがこのインターフェイス経由でこの VLAN について受信したパケットを転送する場合、VLAN ID をパケットに追加します。
  - **[Untagged]**：選択した場合、ポートは、選択した VLAN のタグなしメンバになります。スイッチがこの VLAN のパケットをこのインターフェイス経由で転送する場合、VLAN ID をパケットに追加しません。

  インターフェイス VLAN モードが [一般] の場合、任意の VLAN に対してどちらのオプションも選択できます。インターフェイス VLAN モードが [アクセス] の場合は、1 つの VLAN のみ選択でき、インターフェイスに対して [Untagged] オプションを選択する必要があります。インターフェイス VLAN モードが [トランク] の場合、インターフェイスは 1 つの VLAN のタグなしメンバとして指定でき、その他の VLAN のタグ付きメンバとして指定できます。

- **[PVID]**：このオプションを選択した場合、ポートは選択した VLAN ID をそのポートの VLAN ID（PVID）として使用します。ポートは、転送前に、ポートで受信したすべてのタグなしフレームに PVID を割り当てます。次の設定ルールが適用されます。
  - インターフェイス VLAN モードが [一般] の場合、PVID を指定するために、インターフェイスがタグ付きまたはタグなしのメンバである任意の VLAN を選択できます。
  - インターフェイス VLAN モードが [トランク] の場合、PVID は、ポートがタグ付きメンバである VLAN ID に設定されます。
  - インターフェイス VLAN タイプが [アクセス] の場合、PVID は、アクセス VLAN ID に設定され、このフィールドは変更できません。

[Untagged]、[Tagged]、および [PVID] オプションを選択し、VLAN を [選択済み] リストに移動した場合、「U」、「T」、「P」が VID に追加されます。

ステップ 4 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

デフォルト VLAN の設定

デフォルトでは、スイッチは自動的に VLAN 1 をすべてのポートと LAG のデフォルト VLAN として作成します。ポートに VLAN メンバシップがない場合、スイッチはデフォルト VLAN のメンバとしてポートを自動的に設定します。

[デフォルト VLAN 設定] ページを使用してデフォルト VLAN を変更できます。

デフォルト VLAN の VID が変更された場合、次のようになります。

- 元のデフォルト VLAN のメンバであったポートが、その VLAN のメンバとして削除され、新しいデフォルト VLAN のメンバとして設定されます。
- 元のデフォルト VLAN のメンバであったポートの Port VLAN Identifier（PVID; ポート VLAN ID）は、新しいデフォルト VLAN の VID に変更されます。
- 管理 VLAN が元のデフォルト VLAN と同じだった場合、管理 VLAN は新しいデフォルト VLAN に更新されます。
- 元のデフォルト VLAN のタイプは、デフォルトからスタティックに変更され、削除することもできます。ただし、VLAN 1 は例外です。デフォルトとして指定されていない場合でも、VLAN 1 は削除できません。

デフォルト VLAN を選択するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで、[VLAN 管理] > [デフォルト VLAN 設定] をクリックします。

ステップ 2 VLAN をリストから選択します。

ステップ 3 [適用] をクリックします。

音声とメディア

Voice-over-Internet-Protocol（VoIP）によって、コンピュータ データ ネットワークを音声電話に使用できます。最近のネットワークでは VoIP など遅延に影響されやすいアプリケーションの導入が増え、高品質なパフォーマンスを保証するために、適切な QoS 設定が必要とされます。音声とメディアの機能は、音声パケットをデータ パケットより高いプライオリティにできるように、音声パケットのシンプルな分類メカニズムを提供します。

音声とメディアの機能では、イーサネット スイッチで VoIP ストリームを識別し、それらに通常のトラフィックより高い Class-of-Service（CoS）を与えます。スイッチは、次の 2 種類の音声とメディアをサポートします。

- **プロトコル ベース**：Session Initiation Protocol（SIP）と H.323 コントロール トラフィックを使用する VoIP セッションを識別し、それらのパケットに音声 VLAN 上で最も高いプライオリティを割り当てます。
- **OUI ベース**：この機能が有効なポートは、設定済みの音声 VLAN のメンバに自動的になります。スイッチは、クライアント パケットで MAC アドレスの最初の 3 バイトにある組織固有識別子（OUI）の値を検出し、それらを VoIP VLAN で分類して、自動 VoIP が有効なポート上でプライオリティを付けます。

[VLAN 管理] > [音声とメディア] メニューで利用可能な設定ページについて詳しくは、次のトピックで説明します。

- **「テレフォニー OUI の表示と追加」**
- **「OUI ベースの音声とメディアの設定」**
- **「SIP/H323 ベースの音声とメディアの設定」**

テレフォニー OUI の表示と追加

[テレフォニー OUI] ページには、さまざまな音声 VLAN に関連付けられた組織固有識別子（OUI）が表示されます。

このページを表示するには、ナビゲーション ウィンドウで、[VLAN 管理] > [音声とメディア] > [テレフォニー OUI] の順にクリックします。

[テレフォニー OUI テーブル] は、一般的に使用されるテレフォニー デバイスの識別子で事前に設定されています。管理者は OUI を追加または削除できます。音声とメディアが有効な場合、ポートは、受信パケットの送信元 IP アドレスと宛先 IP アドレスのいずれかまたは両方の MAC アドレスでの OUI 数値を使用して、音声トラフィックを音声 VLAN に自動的に割り当てます。VLAN と IEEE 802.1p プライオリティの関連付け、および音声とメディアのポートの有効化について詳しくは、**「OUI ベースの音声とメディアの設定」**を参照してください。

新しい OUI の説明を追加するには、次の手順に従います。

ステップ 1 [追加] をクリックします。

ステップ 2 次の値を指定します。

- **[テレフォニー OUI]**：テレフォニー アプリケーションの 3 オクテットの識別子を入力します。
- **[説明]**：ベンダー名やテレフォニー製品など、サービスの説明を入力します。

ステップ 3 [適用]、[閉じる] の順にクリックします。

OUI ベースの音声とメディアの設定

[テレフォニー OUI ベース自動 VoIP] ページを使用して、次のことができます。

- MAC アドレスの OUI 数値を使用して識別される音声とメディアのトラフィックに対する IEEE 802.1p プライオリティ レベルの設定。
- OUI ベースの VoIP パケット用の VLAN の指定。スイッチでまだ作成されていない VLAN ID を割り当てることは可能ですが、機能が動作するためには、続けて VLAN を作成する必要があります（**「VLAN の作成」**を参照）。
- ポートでのこの機能の有効化。ポートでこの機能が有効な場合、ポートは設定された音声 VLAN のメンバに自動的になります（つまり、管理者が手動で、ポートを VLAN のメンバとして追加する必要はありません）。

[ポート VLAN メンバシップ] ページには、ポートが音声 VLAN のメンバであることが表示されます。

OUI ベースの音声とメディアを設定するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで、[VLAN 管理] > [音声とメディア] > [テレフォニー OUI ベース] の順にクリックします。

ステップ 2 [VLAN] を有効にして、[VLAN ID] と [プライオリティ] フィールドを編集できるようにします。

ステップ 3 [VLAN ID] フィールドで、音声トラフィックを伝送する VLAN 指定します。この VLAN は、すでにスイッチ上で設定されている必要があります（**「VLAN の作成」**を参照）。

ステップ 4 [プライオリティ] フィールドで、VoIP トラフィックに対して IEEE 802.1p Class-of-Service（CoS）プライオリティ レベルを指定します。

ステップ 5 [適用] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

ステップ 6 [テレフォニー OUI ベースのインターフェイス設定テーブル] で、設定するインターフェイスを選択してから、[編集] をクリックします。

ステップ 7 [自動 VoIP モード] で [有効] を選択します。ポートは、音声 VLAN のメンバとして自動的に追加されます。

ステップ 8 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

SIP/H323 ベースの音声とメディアの設定

[SIP/H323 ベース自動 VoIP] ページを使用して、スイッチが Session Initiation Protocol（SIP）や H.323 などのプロトコルで、VoIP トラフィックを認識できるように設定できます。トラフィックは、ポートで設定された VoIP トラフィックのトラフィック クラスに基づいて自動的にプライオリティが付けられます。

SIP/H323 ベースの音声とメディアを設定するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで、[VLAN 管理] > [音声とメディア] > [SIP/H323 ベース] 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] リストを使用して、ポートまたは LAG を [プロトコルベースのインターフェイス設定テーブル] に表示します。

ステップ 3 設定するポートまたは LAG 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 [自動 VoIP モード] で [有効] を選択します。

ステップ 5 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

メディア VLAN

メディア VLAN 機能によって、スイッチ ポートは、割り当てられたプライオリティ値で、音声、ビデオ、およびシグナリング トラフィックを伝送できます。さまざまなプライオリティをトラフィックに割り当てることで、ポートに入るメディア トラフィックとデータ トラフィックを分けることができます。メディア VLAN 機能によって、ポート上でデータ トラフィックが多い場合でも、IP 電話やビデオ デバイスの音声またはビデオの品質が低下することなく確保されます。

VLAN が提供する固有のトラフィック分離により、VLAN 間のトラフィックが管理制御され、ネットワークに接続されたクライアントは音声コンポーネントの直接攻撃を開始できなくなります。スイッチは、メディア デバイスからのパケットで IP-DSCP または 802.1p 値を使用し、このトラフィックを高いプライオリティ キューに割り当てます。

スイッチはメディア VLAN を使用して LLDP-MED アプリケーションをサポートします（プロトコルについては、**「LLDP-MED」**を参照）。各メディア VLAN は、特定のタイプのメディア トラフィックの LLDP-MED アプリケーションに対応します。LLDP-MED アプリケーションには、音声、音声シグナリング、ゲスト音声、ゲスト音声シグナリング、ソフトフォン音声、ビデオ会議、ストリーミング ビデオ、ビデオ シグナリングがあります。各メディア VLAN は次のパラメータと関連付けられています。

- オプションの VLAN タギングのある VLAN
- IEEE 802.1p プライオリティ値
- DSCP 値

ポートが、ネットワーク ポリシーが有効な LLDP-MED である場合、スイッチは、LLDP-MED ネットワーク ポリシー TLV でそのメディア VLAN をポートにアドバタイズします。LLDP Media Endpoint が検出された場合、スイッチは対応するポートでメディア VLAN をインストールします。[各種管理] > [ディスカバリ - LLDP-MED] のページで、LLDP-MED とネットワーキング ポリシーを有効にできます。

メディア VLAN はグローバルに有効化および無効化されます。各アプリケーションとそのメディア VLAN は、ポートごとに設定されます。たとえば、ゲスト音声はインターフェイス g1 のメディア VLAN 1 に設定できますが、インターフェイス g2 のメディア VLAN 10 にも設定できます。

[メディア VLAN インターフェイス設定テーブル] には、有効にできる各メディア トラフィック タイプに加え、選択したポートのステータスと設定が表示されます。

メディア VLAN アプリケーションを設定するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで [VLAN 管理] > [音声とメディア] > [メディア VLAN] の順にクリックします。

ステップ 2 [管理モード] で [有効] を選択して、この機能をスイッチでグローバルに有効にします。次に、[適用] をクリックします。

ステップ 3 [インターフェイス] リストから設定するインターフェイスを選択します。

注意 LAG のメンバであるポートは、メディア VLAN アプリケーションに対して有効にできません（**「LAG の設定」**を参照）。

ステップ 4 [編集] をクリックします。

ステップ 5 [アプリケーション] リストで、設定するメディア トラフィック タイプを選択します。

- [音声]
- [音声シグナリング]
- [ゲスト音声]
- [ゲスト音声シグナリング]
- [ソフトフォン音声]
- [ビデオ会議]
- [ストリーミングビデオ]
- [ビデオシグナリング]

ステップ 6 [アプリケーションステータス] で [有効] を選択して、選択したアプリケーションのプライオリティ割り当てを有効にします。この機能を無効にするには、チェックボックスをオフにします。

ステップ 7 [アプリケーションステータス] を有効にした場合、次の機能を有効または無効にします。

- **[Untagged]**：メディア デバイス（LLDP-MED Endpoint）がタグなしパケットを送信する場合は、[有効] を選択します。スイッチからのネットワーク ポリシー TLV も、この設定に対応する必要があり、メディア デバイスは、タグなしフレームを使用することを認識している必要があります。この機能を無効にするには、チェックボックスをオフにします。

- **[VLAN]** および **[VLAN ID]**：[有効] を選択して VLAN を指定し、リストから VLAN ID を指定します。この機能を無効にするには、チェックボックスをオフにします。
- **[プライオリティ]** および **[プライオリティ値]**：[有効] を選択して、選択したアプリケーションのパケットにプライオリティを付けます。その後メディア VLAN トラフィックの IEEE 802.1p CoS プライオリティ タギング値を入力します。プライオリティ タグの範囲は 0 ～ 7 です。
- **[DSCP]** および **[DSCP 値]**：[有効] を選択して、選択したアプリケーションの DSCP を指定します。その後、ポートの DSCP 値を入力します。範囲は 0 ～ 63 です。

ステップ 8 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

ステップ 9 LLDP-MED がインターフェイス上で有効なことを確認します。手順については、**「LLDP-MED」**を参照してください。

自動 VoIP セッション

[自動 VoIP セッション] ページには、各 Voice over IP セッションの送信元、宛先、およびプロトコルに関する情報が表示されます。

6

スパニング ツリー

この章では、スイッチの Spanning Tree Protocol（STP; スパニング ツリー プロトコル）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。

- 「スパニング ツリーの概要」
- 「STP のステータスとグローバル情報の設定」
- 「STP インターフェイスの設定」
- 「RSTP インターフェイス設定」

スパニング ツリーの概要

STP は、複数のブリッジのあるネットワークで効率的な通信を可能にします。これらのネットワーク上にあるデバイスは、同じエンドポイントへの複数の（つまり、冗長な）パスを学習できます。パスの冗長性は、特定のリンクがダウンした場合にトラフィック フローを維持するために望ましい一方で、トラフィック ループを引き起こし、ネットワーク パフォーマンスに影響を与え、フォワーディング アルゴリズムを混乱させる可能性があります。

STP が有効な各ブリッジは、Bridge Protocol Data Unit（BPDU）と他のブリッジを交換します。BPDU は、ブリッジ ポートの MAC アドレスと、各ポートに関連づけられたプライオリティおよびコストを識別します。STP は、この情報を使用して、ネットワーク上の任意の 2 台のステーション間に 1 本のアクティブ パスを提供するトポロジを構築します。これらのステーション間の冗長パスは、アクティブ パスが利用できなくなった場合のみ使用できるように、スタンバイ状態で配置されます。

BPDU の交換により、ネットワークのルート ブリッジとルート ポートの選択も容易になります。ルート ブリッジは、その他のブリッジがそれぞれ、各パスでポートのコストを合計し、最も低いものを選択することによって、最小のコスト パスを計算するために使用する参照ポイントを提供します。ブリッジを最小のコスト パスに接続するポートは、ブリッジのルート ポートと呼ばれます。

ルート ブリッジが選択され、各ルート ポートが確立されると、各ネットワーク セグメントは、どのブリッジがルート ポートへの最小のコスト パスを提供するかを決定できます。このパスを提供するポートは、ネットワーク セグメントの指定ポートと呼ばれます。スパニング ツリーは、そのネットワーク セグメントのその他のポートを無効にし、それらを代替またはバックアップ ポートに指定します。

サポートされるスパニング ツリーのバージョンには、Common Spanning Tree（CST）Rapid STP（RSTP; 高速 STP）があります。

- CST（IEEE 802.1D）は、オリジナルのプロトコル バージョンであり、エンド ステーション間で生成されるパスが 1 本のみになるため、ループが解消されます。
- RSTP（IEEE 802.1w）は、拡張プロトコルであり、ネットワークは最適な STP トポロジをより迅速に実現できます。

STP のステータスとグローバル情報の設定

[STP ステータス & グローバル設定] ページを使用して、STP を有効にできます。STP 動作モードを選択して、ブリッジのプライオリティを設定してください。STP トポロジに関するステータス情報を表示することもできます。このページを表示するには、ナビゲーション ウィンドウで [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。

このページでは、グローバル情報とブリッジを設定でき、指定ルートに関する情報を表示できます。

グローバル情報とブリッジの設定

STP のグローバル情報とブリッジを設定するには、次の手順に従います。

ステップ 1 次のグローバル情報を指定します。

- **[スパニングツリー状態]**：選択すると、スイッチで STP 動作が有効になります。個々のポートでも STP 動作を有効にする必要があります（**「STP インターフェイスの設定」**を参照）。
- **[STP 動作モード]**：従来の STP または高速 STP モードを選択します。
  - **[従来の STP]**：元の IEEE 802.1D スパニング ツリー プロトコルに従って動作します。
  - **[高速 STP]**：デフォルト値であり、トポロジ変更後のスパニング ツリーの収束時間が従来の STP よりも短縮されます。

- **[BPDU 処理]**：Bridge Protocol Data Unit（BPDU）は、STP トポロジを計算するためにスイッチ間で交換されるメッセージです。スパニング ツリーがインターフェイス上で無効な場合の BPDU パケットの処理方法を選択します。
  - **[フィルタリング]**：STP に対して有効ではないインターフェイス上で受信した BPDU を廃棄するためのポートを有効にします。
  - **[フラッディング]**：スパニング ツリーではないポートで受信した BPDU を、スパニング ツリーではない他のすべてのポートにフラッディングすることを許可します。

ステップ 2 次のブリッジ設定を指定します。

- **[プライオリティ]**：ブリッジのプライオリティ値。スイッチまたはブリッジが STP を実行中の場合、それぞれにプライオリティが割り当てられます。BPDU を交換した後、ブリッジ ID が最も小さいスイッチがルート ブリッジになります。ブリッジ プライオリティは、4096 の倍数である必要があります。4096 の倍数以外のプライオリティを指定した場合、プライオリティはその数より小さい直近の 4096 の倍数に自動的に設定されます。たとえば、プライオリティを 0 ～ 4095 の間の任意の値に指定すると、0 に設定されます。デフォルトのプライオリティは 32768 です。値の範囲は 0 ～ 61440 です。

このページのセクションには、次の情報が表示されます。

- **[ハロータイム]**：ブリッジが設定メッセージを送信する間隔。
- **[最大経過時間]**：トポロジの変更を実装するまでにブリッジが待機する秒数。
- **[最大ホップ]**：BDPU が廃棄され、ポート情報が期限切れになるまでのホップ数。最大ホップ数は、20 に設定されており、変更できません。
- **[転送遅延]**：ブリッジがリスニング ステートとラーニング ステートを維持する秒数。この時間を過ぎると、パケットが転送されます。
- **[保留時間]**：コンフィギュレーション BPDU がブリッジ ポートを通過する間の最短間隔（秒数）。

ページの [指定ルート] セクションには次の情報が表示されます。

- **[ブリッジ ID]**：ブリッジ ID。ブリッジ プライオリティとブリッジの基本 MAC アドレスを連結したものです。
- **[ルートブリッジ ID]**：ルート ブリッジのブリッジ ID。すべてのブリッジの中でブリッジ ID が最も小さいブリッジが、ルート ブリッジになります。
- **[ルートポート]**：このブリッジからルート ブリッジまでのコスト パスが最も小さいポートのポート番号。この値は、ブリッジがルートでない場合に重要です。デフォルトは 0 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 状態の変更が発生した回数の合計。
- **[最後のトポロジ変更からの経過時間]**：最後のトポロジ変更からの時間。

ステップ 3 [適用] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

STP インターフェイスの設定

[STPインターフェイス設定] ページでは、STP プロパティを、個々のポートまたは LAG に割り当てます。これらの設定は、従来の STP と高速 STP の両方に適用可能です。

ポートまたは LAG を設定するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで、[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。

[STPインターフェイス設定テーブル] には、各ポートと LAG の設定情報が表示されます。デフォルトでは、すべてのポートが STP 動作で有効です。

(注)：ポートと LAG のリストは複数ページにわたる場合があります。[ページ] リストを使用すると、次のエントリ セットを表示できます。

ステップ 2 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 3 パラメータを入力します。

- **[STP]**：選択すると、ポートまたは LAG での STP 動作が有効になります。
- **[自動エッジ]**：[有効] を選択することで、ポートがエッジ ポートかどうかをスイッチが自動的に判別できます。ブリッジに接続されていないポートがエッジ ポートです。自動検出によって、ポートがフォワーディング状態に移行するのを速めます。ポートは、フォワーディング状態にある間、トラフィックを転送したり、MAC アドレスを学習したりできます。
- **[エッジポート]**：[有効] を選択すると、ポートをエッジ ポートとして手動で設定できます。
- **[BPDU 処理]**：Bridge Protocol Data Unit（BPDU）は、STP トポロジを計算するためにスイッチ間で交換されるメッセージです。スパニング ツリーがインターフェイス上で無効な場合の BPDU パケットの処理方法を選択します。

- **[フィルタリング]**：STP に対して有効ではないインターフェイス上で受信した BPDU を廃棄するためのポートを有効にします。
- **[フラッディング]**：スパニング ツリーではないポートで受信した BPDU を、スパニング ツリーではない他のすべてのポートにフラッディングすることを許可します。

- **[パスコスト]**：ポート パス コストを指定します。ルート ブリッジまでのポートのパス コストは、そのパスにおける全ポートのコストの合計です。パス コストは、パスを再ルーティングする場合にトラフィックを転送するために使用されます。[デフォルトを使用] を選択すると、パス コストはポート速度に設定されます。または、[ユーザ定義] を選択すると、0 ～ 200,000,000 の間の値を設定できます。値 0 は、パス コストをポート速度に従って設定することを意味します。

ステップ 4 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

新しい設定が、ポートと LAG に関する次の情報と一緒に [STP インターフェイス設定テーブル] に表示されます。

- **[エッジ動作ステータス]**：ポートが現在エッジ ポート（または PortFast ポート）として動作しているかどうかを示します。次の条件のいずれかに該当するためにポートがフォワーディング状態にある場合、[有効] と示されます。
  - ポートがエッジ ポートとして設定されており、そのため自動的にフォワーディング状態にある。
  - ポートが自動エッジ ポートとして設定されており、BPDU を受信していないため、フォワーディング状態に移行されている。
- **[ポート状態]**：ポートの現在の STP 状態。有効な場合は、ポート状態により、トラフィック上で行われるフォワーディング動作が決まります。ポート状態には次のものがあります。
  - **[無効]**：ポートで STP は現在無効になっています。ポートはスパニング ツリーに参加していませんが、動作状態にあり、MAC アドレスを学習し、トラフィックを転送します。
  - **[廃棄]**：ポートは現在ブロックされており、トラフィックの転送や MAC アドレスの学習に使用できません。
  - **[ラーニング]**：ポートは現在ラーニング 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]**：ポートは現在フォワーディング状態になっています。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]**：LAN へのルート パス コストが最も低いブリッジのブリッジ ID。ID は、ブリッジ プライオリティとブリッジの基本 MAC アドレスが連結したものです。
- **[指定ポート ID]**：LAN へのルート パス コストが最も低い代表ブリッジのポート ID。この ID は、ポート プライオリティとポートのインターフェイス番号が連結したものです。
- **[指定コスト]**：代表ブリッジからルート ブリッジへのルート パス コスト。指定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。
- **[速度]**：ポート速度。
- **[LAG]**：ポートがメンバーである LAG（存在する場合）。

RSTP インターフェイス設定

Rapid Spanning Tree Protocol（RSTP; 高速スパニング ツリー プロトコル）は、ブリッジ型 LAN のループのないスパニング ツリーが構成されるまでの収束時間を短縮します。[RSTP インターフェイス設定] ページを表示するには、ナビゲーション ウィンドウで [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。

スパニング ツリー モードとして RSTP が選択された場合に、高速スパニング ツリー トポロジが自動的に形成されます。[STP ステータス & グローバル設定] ページで、RSTP モードを有効にすることができます。

デフォルトでは、[RSTP インターフェイス設定テーブル] には各ポートの情報が表示されます。インターフェイス タイプのリストを使用して、このテーブルにポートまたは LAG を表示できます。[RSTP インターフェイス設定テーブル] には、各ポートに関する次の情報が表示されます。

- **[ポイントツーポイント動作ステータス]**：全二重で動作する場合、物理ポートに LAN へのポイントツーポイント接続があります。
- **[ポートロール]**：STP パスに提供する、STP アルゴリズムによって割り当てられたポートのロール。設定可能なフィールド値は次のとおりです。
  - **[ルート]**：スイッチのすべてのポートの中でルート ブリッジへのルート パス コストが最も低くなります。
  - **[指定]**：LAN からルート ブリッジへのルート パス コストが最も低くなります。スイッチは、LAN の代表ブリッジです。

- **[代替]**：ルート インターフェイスからルート 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。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状に接続されている場合、または共有セグメントに接続された 2 つ以上の接続が LAN に存在する場合にだけ割り当てられます。
- **[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]**：ポートに対して RSTP の管理モードが有効か無効かを示します。
- **[エッジポート動作ステータス]**：ポートまたは LAG に対して有効な場合、ポートは自動的にフォワーディング状態になります。この設定の変更の手順については、**「STP インターフェイスの設定」**を参照してください。
- **[ポートステータス]**：ポートの動作状態。

ポートを選択して、[プロトコル移行のアクティブ化] をクリックすることで、スイッチからポートに RSTP BPDU を送信させることができます。これは、LAN にある既存のブリッジがすべて削除されたかどうかをテストするために使用できます。

7

MAC アドレス テーブル

この章では、スイッチのフィルタリング データベースへの Media Access Control（MAC; 媒体アクセス制御）アドレスのスタティックな設定とダイナミックな学習について説明します。スイッチは、フィルタリング データベースを検索し、パケットがどのポートに転送されるかを決定します。このマニュアルでは、フィルタリング データベースをブリッジング テーブルとも呼びます。検索は、VLAN とパケットの宛先 MAC アドレスに基づいています。検索で一致するエントリが見つからなかった場合、スイッチは入力ポート以外の VLAN にパケットをフラッディングします。

具体的な内容は、次のとおりです。

- 「スタティック MAC アドレスの設定」
- 「ダイナミック アドレスのエージング タイムの設定」
- 「ダイナミック MAC アドレス」

スタティック MAC アドレスの設定

[スタティックアドレス] ページには、スイッチのブリッジング テーブルに手動で設定される MAC アドレスのリストが表示されます。スタティック MAC アドレスは、VLAN とポートにも関連付けられます。

スタティック MAC アドレス エントリを追加するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで、[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]**：スタティック MAC アドレスを持つデバイスがある VLAN を選択します。
- **[インターフェイス]**：スタティック MAC アドレスを持つデバイスにアクセスできるポートまたは LAG を指定します。
- **[MAC アドレス]**：スタティック MAC アドレスを入力します。
- **[ステータス]**：このスタティック MAC アドレスのステータスを選択します。
  - **[固定]**：このステータスを選択すると、スタティック MAC アドレスは期限切れになりません。ただし、スイッチがリブートされた場合、実行コンフィギュレーション ファイル タイプがスタートアップ コンフィギュレーション ファイル タイプにコピーされない限り、エントリがリストアされないことに注意してください。**「コンフィギュレーション ファイルのコピーと保存」**を参照してください。
  - **[セキュア]**：このステータスが選択されると、MAC アドレスがセキュリティ保護され、ポート セキュリティ機能とともに使用されます。MAC アドレスがポートでセキュリティ保護されている場合、その MAC アドレスからのパケットは、セキュリティ保護されているポートからのみ入力できます。そうでない場合、パケットは破棄されます。ポート セキュリティがそのポートで無効な場合、MAC アドレスは、スタティック MAC アドレスのリストから削除されます。ポート セキュリティがポートで有効な場合、ポートは最大 256 のスタティックおよびダイナミック MAC アドレスをサポートできます （詳細については、**「ポート セキュリティの有効化」**を参照）。
  - **[タイムアウト時に削除]**：このステータスを選択すると、スタティック MAC アドレスは固定的ですが、アクティブでないために期限切れになる場合があります。このため、ダイナミックに学習された MAC アドレスと同じように扱われます。エージング期間の設定については、[ダイナミックアドレス設定]ページを参照してください。

ステップ 4 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

（注） スタティック MAC アドレスを削除するには、テーブルで選択して、[削除] をクリックします。

ダイナミック アドレスのエージング タイムの設定

[ダイナミックアドレス設定] ページでは、エージング タイムを設定できます。この期間が経過すると、リフレッシュされていないダイナミック MAC アドレス テーブルでアドレスが削除されます。エージング期間は、ダイナミックに学習されたアドレスと、[タイムアウト時に削除] に設定されたスタティック アドレスに適用されます。デフォルトのエージング タイムは、300 秒です。

エージング タイムを設定するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで、[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 10 ～ 1,000,000 秒の範囲でエージング タイムを指定します。

ステップ 3 [適用] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

ダイナミック MAC アドレス

VLAN と着信パケットの宛先 MAC アドレスに一致するブリッジング テーブルでエントリが見つからない場合、スイッチは MAC アドレス、VLAN、パケットの入力ポートを学習し、エントリを [ダイナミックアドレステーブル] に追加します。

ブリッジング テーブルがオーバーフローしないようにし、新しいアドレスのための余地を空けておくために、設定されたエージング期間ダイナミック MAC アドレスからのトラフィックがない場合、そのアドレスはブリッジング テーブルから削除されます（**「ダイナミック アドレスのエージング タイムの設定」**を参照）。

[ダイナミックアドレス] ページを表示するには、ナビゲーション ウィンドウで [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。

（注） [ダイナミックアドレステーブル] に含まれているエントリ数が最大数の場合は、このページが表示されるまでに最大 45 秒かかることがあります。

デフォルトでは、[ダイナミックアドレステーブル] に、ダイナミックに学習されたすべての MAC アドレスが表示されます。フィルタ基準を入力し、[実行] をクリックして表示をフィルタリングできます。特定の VLAN のテーブル エントリを表示するには、[VLAN ID] フィルタを使用します。特定の MAC アドレスのエントリを表示するには、[MACアドレス] フィルタを使用します。特定のポートまたは LAG のエントリを表示するには、[インターフェイス] フィルタを使用します。すべてのエントリを表示するには、[フィルタのクリア] をクリックします。

[ダイナミックアドレステーブル] には、学習されたエントリごとに次のフィールドが表示されます。

- **[VLAN ID]**：MAC アドレスが学習された VLAN。フレームは、この VLAN に関連付けられている場合のみ、インターフェイスに転送されます。
- **[MAC アドレス]**：ダイナミックに学習された MAC アドレス。
- **[インターフェイス]**：MAC アドレスがダイナミックに学習されたポート。この MAC アドレスと VLAN を宛先として指定するフレームは、このポートに転送されます。

すべてのダイナミック MAC アドレス エントリをテーブルからクリアするには、[テーブルのクリア] をクリックします。

8

マルチキャスト

この章では、パケットを 1 つの送信元から複数の宛先に転送するマルチキャスト プロトコルを設定する方法について説明します。

この章で説明する項目は次のとおりです。

- 「マルチキャスト プロパティ」
- 「MAC グループ アドレスの設定」
- 「IGMP スヌーピングの設定」
- 「MLD スヌーピングの設定」
- 「IGMP マルチキャスト ルータ インターフェイスの設定」
- 「MLD マルチキャスト ルータ インターフェイスの設定」

マルチキャスト プロトコルはパケットを 1 つの送信元から複数の宛先に送信します。これによって帯域利用率が向上し、ホストとルータの処理負荷が削減されるので、ビデオ / 音声会議、ホワイトボード ツール、株式ティッカーなどのアプリケーションでの利用に役立ちます。

スイッチは、マルチキャスト宛先 MAC アドレスで届くパケットの転送を決定するために、マルチキャスト転送テーブルを保持します。マルチキャストが指定されたポートのみに制限された場合、受信者がないネットワークの部分へのトラフィックは抑制されます。パケットがスイッチに入ると、宛先 MAC アドレスは VLAN ID と組み合わされ、マルチキャスト転送テーブルで検索が実行されます。該当するものがない場合、スイッチの設定によって、パケットは VLAN のすべてのポートにフラッディングされるか、破棄されます。該当するものが見つかった場合、パケットはそのマルチキャスト グループのメンバであるポートのみに転送されます。

マルチキャスト エントリは、マルチキャスト メンバシップを管理するレイヤ 3 プロトコルのスヌーピング（待ち受け）によって学習できます。

- IPv4 マルチキャスト グループ アドレスは、Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）で学習できます。
- IPv6 マルチキャスト グループ アドレスは、Multicast Listener Discovery（MLD; マルチキャスト リスナー検出）プロトコルで学習できます。

特定の VLAN の IGMP および MLD マルチキャスト ルータとのインターフェイスは、スタティックまたはダイナミックのいずれかで設定できます。マルチキャスト ルータは、マルチキャスト グループのメンバシップを管理するために IGMP と MLD を使用します。スイッチが IGMP/MLD スヌーピングを VLAN で適切にサポートするには、マルチキャスト ルータも必要です。

マルチキャスト プロパティ

マルチキャストの [プロパティ] ページを使用して、VLAN 内でのマルチキャスト パケットの転送方法を指定できます。

VLAN を作成すると、デフォルトのマルチキャスト転送オプションが割り当てられます。スイッチに現在設定されているすべての VLAN を、選択した転送モードを設定するために、グローバル マルチキャスト モード設定を使用できます。グローバル設定により、その後作成された VLAN のデフォルト設定が作成されるわけではありません。すべての既存の VLAN が、指定したモードで設定されるだけです。また、スイッチがマルチキャスト パケットを転送する方法を、個別にまたは VLAN ごとに設定することもできます。

すべての VLAN でのマルチキャスト転送モードの設定

現在のすべての VLAN を特定のマルチキャスト転送モードで設定するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで、[マルチキャスト] > [プロパティ] の順にクリックします。

ステップ 2 [グローバルマルチキャストモード] ですべての VLAN に適用する設定を選択します。VLAN が別のモードで設定されている場合、次のモードにリセットされます。

- **[未登録の転送]**：パケットがマルチキャスト宛先アドレスのある VLAN から受信され、VLAN にそのアドレスのマルチキャスト パケットを受信するように登録されたポートがない場合、パケットは VLAN のすべてのポートにフラッディングされます。

パケットを受け入れるかドロップするかの対応はホストが行います。マルチキャスト パケットが受信され、それを受信するように登録されたポートが存在する場合、パケットは登録されたポートにのみ送信されます。

- **[すべて転送]**：VLAN から受信されたすべてのマルチキャスト パケットは、マルチキャスト アドレスへのポートの登録に関係なく、VLAN のすべてのポートにフラッディングされます。
- **[未登録のフィルタ]**：パケットがマルチキャスト宛先アドレスの VLAN から受信され、VLAN にそのアドレスのマルチキャスト パケットを受信するように登録されたポートがない場合、パケットはドロップされます。

ステップ 3 [適用] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

個々の VLAN でのマルチキャスト プロパティの設定

グローバル マルチキャスト モード設定とは異なる転送モードを VLAN に設定するには、次の手順に従います。

ステップ 1 [VLAN ID] メニューから VLAN を選択して、[編集] をクリックします。

ステップ 2 **「すべての VLAN でのマルチキャスト転送モードの設定」**の説明に従って、[マルチキャスト モード] を選択します。

ステップ 3 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

MAC グループ アドレスの設定

[MAC グループアドレス] ページでは、スイッチのマルチキャスト グループ MAC アドレスと VLAN の関連付けを表示および設定できます。スタティックな関連付けの設定や、IGMP または MLD スヌーピングでのダイナミックな学習が可能です。[MAC グループアドレステーブル] のエントリと一致するマルチキャスト グループ アドレスに対してパケットが受信された場合、そのパケットは VLAN のメンバのポートにのみ送信されます。

スイッチは、最大 32 のスタティックおよびダイナミック MAC グループ アドレス テーブルのエントリをサポートします。設定可能な時間、MAC グループ アドレスに対して受信されたパケットがない場合、ダイナミック エントリは期限切れになります（IGMP グループ メンバシップ間隔の設定については、[IGMP スヌーピング] ページを参照）。

MAC グループ アドレス テーブルの表示

[MAC グループアドレステーブル] を表示するには、ナビゲーション ウィンドウで、[マルチキャスト] > [MAC グループアドレス] の順にクリックします。

デフォルトでは、すべてのエントリがこのテーブルに表示されます。[VLAN ID] および [MAC グループアドレス] フィルタを使用すると、指定した値に一致するエントリのみを表示できます。次のフィールドが表示されます。

- **[タイプ]**：エントリがスタティックに設定されたかダイナミックに学習されたかを示します。
- **[VLAN ID]**：マルチキャスト パケットが、指定したマルチキャスト MAC アドレスに一致する場合に、マルチキャスト パケットが転送される VLAN ID。
- **[MAC グループアドレス]**：着信パケットの宛先 MAC アドレスと比較される、16 進数形式でのマルチキャスト グループ MAC アドレス。

スタティックな MAC グループ アドレス テーブル エントリの追加

スタティックなマルチキャスト MAC アドレスを追加し、VLAN と関連付けるには、次の手順に従います。

ステップ 1 [MAC グループアドレス] ページで、[追加] をクリックします。

ステップ 2 パラメータを入力します。

- **[VLAN ID]**：リストから VLAN を選択します。
- **[アドレスタイプ]**：[IPv4] を選択して 32 ビットの IPv4 表記（xxx.xxx.xxx.xxx）でアドレスを指定するか、[MAC] を選択して 6 バイトの 16 進数形式（xx.xx.xx.xx.xx.xx）でアドレスを指定します。
- **[MAC グループアドレス]**：選択した形式でアドレスを入力します。IPv4 アドレスについては、下位 23 ビットはイーサネット MAC アドレスにマッピングされます。

ステップ 3 [適用] をクリックしてから、[閉じる] をクリックします。エントリは、[MAC グループアドレステーブル] に表示されます。

MAC アドレス グループ ポート メンバシップの設定

デフォルトでは、マルチキャスト MAC アドレスに向かうパケットは、すべてのポートでフラッディングされます。ポートは、IGMP パケットの交換によってダイナミックに特定の MAC アドレス グループのメンバになる可能性があります。または、ポートをメンバとしてスタティックに設定することもできます。

マルチキャスト グループ アドレスのポート メンバの詳細の表示と設定を行うには、次の手順に従います。

ステップ 1 [MAC グループアドレス] ページでエントリを選択して、[詳細] をクリックします。

このページでは、各ポートのマルチキャスト グループ アドレスのメンバが特定されます。

ステップ 2 [スタティック] をクリックして、ポートをマルチキャスト MAC アドレスのスタティック メンバとして設定します。または、[なし] をクリックして、MAC マルチキャスト アドレスのスタティック メンバとしてのポートを削除します。

ステップ 3 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

IGMP スヌーピングの設定

Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）は、レイヤ 3 のインターネット プロトコルであり、これにより、IPv4 ネットワークでマルチキャスト グループへのメンバシップを管理できます（**「MLD スヌーピングの設定」**で説明されているように、IPv6 マルチキャスト トラフィックは、MLD プロトコルで管理されます）。IGMP 通信は IGMP ルータと IGMP が有効なホスト（クライアント）の間で発生します。スイッチは、IGMP パケットの開始や IGMP パケットへの応答を行いませんが、スイッチで接続されたルータとクライアントの間の IGMP 通信を待ち受けし、また、不要なネットワーク トラフィックを減らす転送の決定を行うように設定できます。この待ち受け動作は、IGMP スヌーピングと呼ばれます。これは、高帯域マルチキャスト ネットワーク トラフィックでは特に利点があります。

通常、スイッチがブロードキャストまたはマルチキャスト パケットを受信した場合、スイッチは、残りのネットワーク セグメントのそれぞれにコピーを転送します。この方法は、接続されたすべてのノードで処理されるブロードキャスト パケットでは有効です。ただし、マルチキャスト パケットでは、この方法は、ネットワーク帯域幅の利用効率の低下につながる可能性があります。特に、パケットが少数のノードのみを対象にしている場合、パケットは、パケット受信に関係するノードがないネットワーク セグメントにフラッディングされます。

IGMP スヌーピングによって、スイッチは、IGMP クライアントからのメンバシップ レポートと、ルータからのクエリーを傍受できます。傍受された通信が、VLAN 内の特定のマルチキャスト宛先アドレスのリンクに IGMP クライアントが存在しないことを示す場合、スイッチはそのネットワーク セグメントにマルチキャスト パケットのコピーを送信しません。

IGMP スヌーピングは VLAN ごとに有効または無効にできます。VLAN で有効な場合、IGMP スヌーピングは、その VLAN のメンバであるすべてのインターフェイスで実行されます。

IGMP は、IP マルチキャスト アドレスに基づいていますが、スイッチは実際のマルチキャスト転送を、対応する MAC アドレスに基づいて実行します。

IGMP スヌーピングを設定するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで、[マルチキャスト] > [IGMP スヌーピング] の順にクリックします。

ステップ 2 [IGMP スヌーピングステータス] で [有効] を選択します。

ステップ 3 [IGMP スヌーピングテーブル] で [追加] をクリックします。

ステップ 4 [VLAN ID] では、IGMP スヌーピングをサポートする VLAN を選択します。

ステップ 5 次の設定を行います。

- **[IGMP 高速離脱モード]**：[有効] を選択すると、スイッチは、マルチキャスト グループの IGMP 離脱メッセージを受信した場合、ポート（または LAG）をマルチキャスト転送テーブルからただちに削除することができます。有効な場合、スイッチは、最初にインターフェイスに通常のクエリーを送信することなく、ポートを削除します。各ポートに 1 つのホストしか接続されていない VLAN でのみ高速離脱モードを有効にしてください。これによって、同一ポートに接続され、そのグループへのマルチキャスト トラフィックの受信対象であり続ける他のホストの誤ったドロップを防ぐことができます。
- **[IGMP グループメンバシップ間隔]**：特定のインターフェイスで特定のグループからの IGMP メンバシップ レポートをスイッチが待機する秒数を指定します。この秒数が経過すると、スイッチはそのインターフェイスをマルチキャスト転送データベース エントリから削除します。[デフォルト] を選択して 260 秒を指定するか、または [ユーザ定義] を選択して、2 ～ 3600 秒の範囲で値を入力します。
- **[IGMP 最大応答時間]**：インターフェイスでクエリーを送信した後、そのインターフェイスで特定のグループのレポートを受信しなかったために、スイッチが応答を待機する秒数を指定します。この値は、[IGMP グループメンバシップ間隔] の値未満である必要があります。[デフォルト] を選択して 10 秒を指定するか、または [ユーザ定義] を選択して、1 ～ 25 秒の範囲で値を入力します。

- **[IGMP MRouter 期限]**：ダイナミック マルチキャスト ルータ インターフェイスで受信されるクエリーをスイッチが待機する秒数を指定します。この秒数が経過すると、そのインターフェイスが VLAN から削除されます。値 0 は、無限のタイムアウト、つまり期限切れなしを示します。[デフォルト] を選択して 0 秒を指定するか、または [ユーザ定義] を選択して、0 ～ 3600 秒の範囲で値を入力します。

ステップ 6 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

新しい VLAN エントリが [IGMP スヌーピングテーブル] に表示されます。

ステップ 7 IGMP Mrouter インターフェイスがこの VLAN（またはすべての VLAN）に対して設定されていることを確認します。**「IGMP マルチキャスト ルータ インターフェイスの設定」**を参照してください。

MLD スヌーピングの設定

MLD は、直接接続されたリンクのマルチキャスト リスナー（IPv6 マルチキャスト パケットを受信するノード）の存在を検出し、どのマルチキャスト パケットが近隣ノードの対象であるかを検出するために、IPv6 マルチキャスト ルータで使用されるプロトコルです。MLD は IGMP から派生したものであり、IPv4 マルチキャスト トラフィックに対して同様の機能を実行します（**「IGMP スヌーピングの設定」**を参照）。

MLD スヌーピングが有効な場合、スイッチは、VLAN のすべてのポートにパケットをフラッディングする代わりに、データを受信するポートのリストに IPv6 マルチキャスト パケットを選択的に転送します。このリストは、IPv6 マルチキャスト コントロール パケットをスヌーピングすることで構築されます。

（注） スイッチは、MLD バージョン 1 およびバージョン 2 のパケットの MLD スヌーピングをサポートします。スイッチは、MLD スヌーピングと IGMP スヌーピングを同時に実行するように設定できます。

MLD スヌーピングは、VLAN ごとに別々に有効または無効にできます。MLD は、IPv6 アドレスに基づいていますが、スイッチは実際のマルチキャスト転送を、対応する MAC アドレスに基づいて実行します。

MLD スヌーピングを有効にし、設定するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで、[マルチキャスト] > [MLD スヌーピング] の順にクリックします。

[MLD スヌーピングテーブル] に、この機能が有効な各 VLAN が表示されます。

ステップ 2 [MLD スヌーピングステータス] で [有効] を選択します。

ステップ 3 [MLD スヌーピングテーブル] で [追加] をクリックします。

ステップ 4 [VLAN ID] では、MLD スヌーピングをサポートする VLAN を選択します。

ステップ 5 パラメータを入力します。

- **[MLD 高速離脱モード]**：[有効] を選択すると、スイッチは、マルチキャスト グループの MLD 離脱メッセージを受信した場合、ポート（または LAG）をマルチキャスト転送テーブルからただちに削除することができます。有効な場合、スイッチは、最初にインターフェイスに MAC ベースの通常のクエリーを送信することなく、ポートを削除します。各ポートに 1 つのホストしか接続されていない VLAN でのみ高速離脱モードを有効にしてください。これによって、同一ポートに接続され、そのグループへのマルチキャスト トラフィックの受信対象であり続ける他のホストの誤ったドロップを防ぐことができます。
- **[MLD グループメンバシップ間隔]**：特定のインターフェイスで特定のグループからの MLD メンバシップ レポートをスイッチが待機する秒数を指定します。この秒数が経過すると、スイッチはそのインターフェイスをマルチキャスト転送データベース エントリから削除します。[デフォルト] を選択して 260 秒を指定するか、または [ユーザ定義] を選択して、2 ～ 3600 秒の範囲で値を入力します。
- **[MLD 最大応答時間]**：インターフェイスでクエリーを送信した後、そのインターフェイスで特定のグループのレポートを受信しなかったために、スイッチが応答を待機する秒数を指定します。この値は、[MLD グループメンバシップ間隔] の値未満である必要があります。[デフォルト] を選択して 10 秒を指定するか、または [ユーザ定義] を選択して、1 ～ 65 秒の範囲で値を入力します。
- **[MLD MRouter 期限]**：インターフェイスで受信されるクエリーをスイッチが待機する秒数を指定します。この秒数が経過すると、MLD マルチキャスト ルータが接続されているインターフェイスのリストからそのインターフェイスが削除されます。値 0 は、無限のタイムアウト、つまり期限切れなしを示します。[デフォルト] を選択して 0 秒を指定するか、または [ユーザ定義] を選択して、0 ～ 3600 秒の範囲で値を入力します。

ステップ 6 [適用] をクリックしてから、[閉じる] をクリックします。

新しい VLAN エントリが [MLD スヌーピングテーブル] に表示されます。

ステップ 7 MLD マルチキャスト ルータ インターフェイスがこの VLAN に設定されていることを確認します。**「MLD マルチキャスト ルータ インターフェイスの設定」**を参照してください。

IGMP マルチキャスト ルータ インターフェイスの設定

IGMP ルータは、VLAN で IGMP クライアントを管理するために存在する必要があります。IGMP スヌーピングをサポートする各 VLAN に対して、スイッチは、IGMP ルータのある 1 つまたは複数のインターフェイスでスタティックに設定されるか、またはそれをダイナミックに学習する必要があります。IGMP ルータのあるインターフェイスは、IGMP マルチキャスト ルータ インターフェイスと呼ばれます。IGMP スヌーピングが有効な VLAN には 1 つまたは複数の IGMP マルチキャスト ルータ インターフェイスが必要です。IGMP マルチキャスト ルータは 1 つまたは複数の VLAN をサポートできます。

スイッチ ポートまたは LAG を IGMP Mrouter インターフェイスとして有効にし、関連する設定を行うには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで、[マルチキャスト] > [IGMP Mrouter] の順にクリックします。

デフォルトでは、[IGMP Mrouter テーブル] に各スイッチ ポートが表示されます。LAG を表示するには、[インターフェイスタイプ] リストから [LAG] を選択します。

ステップ 2 設定するポートまたは LAG を選択して、[編集] をクリックします。

ステップ 3 [モード] で [有効] を選択します。

ステップ 4 このインターフェイスを使用する VLAN を IGMP Mrouter インターフェイスとして指定するには、次のように VLAN を [選択済み] リストに移動します。

- VLAN を選択するには：[使用可能] リストで VLAN を選択してから、右矢印ボタンをクリックして、[選択済み] リストに移動します。
- VLAN を削除するには：[選択済み] リストで VLAN を選択してから、左矢印ボタンをクリックして、[使用可能] リストに移動します。

ステップ 5 [適用] をクリックしてから、[閉じる] をクリックします。

[IGMP Mrouter テーブル] では、[モード] 列が [有効] になり、選択した VLAN が表示されます。

MLD マルチキャスト ルータ インターフェイスの設定

MLD マルチキャスト ルータは、VLAN で MLD クライアントを管理するために存在する必要があります。MLD スヌーピングをサポートする各 VLAN に対して、スイッチは、MLD マルチキャスト ルータのある 1 つまたは複数のインターフェイスでスタティックに設定されるか、またはそれをダイナミックに学習する必要があります。MLD ルータのあるインターフェイスは、MLD マルチキャスト ルータ インターフェイスと呼ばれます。MLD スヌーピングが有効な VLAN には 1 つまたは複数の MLD マルチキャスト ルータ インターフェイスが必要です。MLD マルチキャスト ルータは 1 つまたは複数の VLAN をサポートできます。

スイッチ ポートまたは LAG を MLD Mrouter インターフェイスとして有効にするには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで、[マルチキャスト] > [MLD Mrouter] の順にクリックします。

デフォルトでは、[MLD Mrouter テーブル] に各スイッチ ポートが表示されます。LAG を表示するには、[インターフェイスタイプ] リストから [LAG] を選択します。

ステップ 2 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 3 [モード] で [有効] を選択します。

ステップ 4 VLAN ID を [使用可能] リストと [選択済み] リストの間で移動します。[選択済み] リストの VLAN は、このポートまたは LAG を MLD Mrouter インターフェイスとして使用します。

- VLAN を選択するには：[使用可能] リストで VLAN を選択してから、右矢印ボタンをクリックして、[選択済み] リストに移動します。
- VLAN を削除するには：[選択済み] リストで VLAN を選択してから、左矢印ボタンをクリックして、[使用可能] リストに移動します。

ステップ 5 [適用] をクリックしてから、[閉じる] をクリックします。

[MLD Mrouter テーブル] では、[モード] 列が [有効] になり、選択した VLAN が表示されます。

9

IP コンフィギュレーション

この章では、Address Resolution Protocol（ARP; アドレス解決プロトコル）と Domain Name System（DNS; ドメイン ネーム システム）クライアント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。

- 「ARP テーブル」
- 「ドメイン ネーム システム」

ARP テーブル

スイッチは、Address Resolution Protocol（ARP）テーブルを保持します。このテーブルの各エントリには、最近スイッチと通信したデバイスの IP アドレスと MAC アドレスが含まれています。

[ARP] ページを使用して、管理 VLAN で学習された ARP エントリを表示できます。このページを表示するには、ナビゲーション ウィンドウで、[IP コンギフュレーション] > [ARP] の順にクリックします。

[ARP のクリア] をクリックすると、管理ポートの IP アドレスと MAC アドレス以外のすべてのエントリをテーブルから削除できます。

ドメイン ネーム システム

スイッチは、IPv4 DNS クライアント機能をサポートします。スイッチは、DNS クライアントとして有効な場合、ホスト名検索サービスをスイッチの他のアプリケーション（Ping、RADIUS、Syslog、Auto Configuration、TFTP など）に提供します。スイッチには、ホスト名を IP アドレスに変換する DNS サーバを設定できます。また、スイッチには、DNS サーバをバイパスする、ホスト名と IP アドレスのスタティックなマッピングを設定することもできます。

[IP コンギフュレーション] > [ドメインネームシステム] メニューで利用可能な設定ページについて詳しくは、次のトピックを参照してください。

- 「DNS サーバの設定」
- 「ホスト名マッピング」

DNS サーバの設定

ホスト名を IP アドレスに変換するために、クライアントは 1 つまたは複数の DNS サーバにアクセスします。管理インターフェイスも DHCP クライアントとして設定されている場合、DNS サーバをダイナミックに学習できます（「管理インターフェイス」を参照）。[DNS サーバ] ページを使用して、DNS サーバをスタティックに設定することもできます。

デフォルトでは DNS クライアントの機能は有効です。

グローバル DNS の設定

DNS サーバ モード設定およびグローバル設定を行うには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで、[IP コンギフュレーション] > [ドメインネームシステム] > [DNS サーバ] の順にクリックします。

ステップ 2 DNS クライアント機能がまだ有効でない場合は、[有効] を選択してこの機能をスイッチで実行できるようにします。

ステップ 3 次の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全にするために使用するドメイン名を指定します。たとえば、finance.yahoo.com は完全修飾ドメイン名です。非修飾ホスト名 finance のみが指定された場合、デフォルトのドメイン名 yahoo.com がピリオドに続いて追加されます。エントリには、非修飾ホスト名とドメイン名の間のピリオドを含まないでください。入力できる文字数は 1 ～ 255 です（英数字）。

- **[ドメインリトライ]**：DNS クエリーを再送信する回数を指定します。範囲は 0 ～ 100 で、デフォルト値は 2 回です。
- **[ドメインタイムアウト]**：スイッチが DNS クエリーへの応答を待機する秒数を指定します。範囲は 0 ～ 3600 秒で、デフォルトは 3 秒です。

(注)：デフォルトのドメイン名が DHCP 応答メッセージで学習されている場合、その名前が [デフォルトドメイン名リスト] に表示されます。

ステップ 4 [適用] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

DNS サーバの追加

[DNS サーバテーブル] には設定されたサーバが表示されます。

DNS サーバを追加するには、次の手順に従います。

ステップ 1 [追加] をクリックします。

ステップ 2 DNS サーバの IPv4 または IPv6 アドレスを指定します。

ステップ 3 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存され、サーバが [DNS サーバテーブル] に表示されます。

ホスト名マッピング

[ホストマッピング] ページを使用して、ホスト名と IP アドレスの関連付けを表示および設定します。ホスト名と IP アドレスをスタティックに関連付けることができます。また、DNS 検索サービスを使用するアプリケーションで動的に学習されたホスト名を表示することもできます。

スタティック DNS マッピングの設定

[ホストマッピングテーブル] には、スイッチの IP アドレスにスタティックに割り当てられたホスト名が表示されます。スタティックなホスト名マッピングを設定するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで、[IP コンギフュレーション] > [ドメインネームシステム] > [ホストマッピング] 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 [ホスト名] フィールドに 1 ～ 255 文字の英数字でホスト名を入力します。ホスト名はアルファベットで始まる必要があります。

ステップ 4 [IP アドレス] フィールドに、ホスト名と関連付けられる IPv4 または IPv6 アドレスを入力します。

ステップ 5 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

ダイナミック DNS エントリの表示と削除

[DNS ダイナミックエントリテーブル] には、DNS 検索サービスを使用するアプリケーションで学習されたホスト名が表示されます。たとえば、ホスト名を ping した場合、DNS 検索サービスが呼び出され、関連付けられた IP アドレスが学習されてテーブルに追加されます。

[DNS ダイナミックエントリテーブル] には、次のフィールドが表示されます。

- **[ホスト名]**：IP アドレス（または、正式なホスト名）に割り当てられたホスト名。
- **[合計]**：ホスト名がこの割り当てに予約されている時間（分）。
- **[経過]**：ホスト名が割り当てられてから経過した時間（分）。
- **[タイプ]**：ホスト名を次のいずれかとして示します。
  - **[IP アドレス]**：割り当てられたホスト名は、IP アドレスと関連付けられます。
  - **[正規]**：割り当てられたホスト名は、正式表記の（公式な）ホスト名のエイリアスまたはニックネームです。たとえば、www.google.com は、公式なホスト名 www.l.google.com に関連付けられたホスト名のエイリアスです。
- **[アドレス]**：[タイプ] が [IP] の場合、このフィールドには、ホスト名と関連付けられた IPv4 または IPv6 アドレスが表示されます。[タイプ] が [正規] の場合、このフィールドには、エイリアスが関連付けられた正式なホスト名が表示されます。正式な DNS アドレスには、関連付けられたホスト名のエイリアスが複数ある場合があります。

ダイナミック エントリを削除するには、そのエントリを選択し、[削除] をクリックします。テーブルからすべてのダイナミック エントリを削除するには、[すべてのダイナミックエントリの削除] をクリックします。

10

セキュリティ

この章では、ポート、ユーザ、およびサーバに対するセキュリティ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。

- 「RADIUS」
- 「パスワード強度」
- 「管理アクセス プロファイル ルール」
- 「認証方式」
- 「ストーム制御」
- 「ポート セキュリティ」
- 「802.1X」

RADIUS

スイッチは、Remote Authorization Dial-In User Service（RADIUS）クライアント機能をサポートします。RADIUS は、アクセス前にユーザを認証するため、広範囲にアクセス可能なネットワークの管理者によって選択されるプロトコルです。安全な方法でユーザを認証するために、RADIUS クライアントと RADIUS サーバは、同じ共有パスワードまたはシークレットで設定されます。このシークレットは、すべての RADIUS パケットに存在する 1 方向の暗号化認証を生成するために使用されます。シークレットが知られていなければ、悪意のあるユーザによってパケットをスプーフィングされる可能性が大幅に低くなります。

スイッチ上の RADIUS クライアントは、スイッチ管理アクセス認証と IEEE 802.1X（dot1X）ポート アクセス コントロールで使用されます（「管理アクセス プロファイル ルール」および「802.1X」を参照）。

[RADIUS] ページを使用して、グローバル RADIUS を設定し、RADIUS サーバを追加できます。

グローバル RADIUS の設定

グローバル設定を行うには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで、[セキュリティ] > [RADIUS] 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。

- **[リトライ回数]**：RADIUS クライアントが要求を RADIUS サーバに再送信する最大回数。範囲は 1 ～ 10 です。デフォルトは 3 です。
- **[応答タイムアウト]**：スイッチが、別の要求を送信する前に、RADIUS サーバがサーバ要求に応答するのを待機する秒数。範囲は 1 ～ 30 です。デフォルトは 3 です。
- **[デッドタイム]**：スイッチが、RADIUS サーバを利用不可能と判別してから、その RADIUS サーバがバイパスされる時間。利用不可能なスイッチをバイパスすることで、スイッチの応答時間が向上します。範囲は 0 ～ 2000 です。デフォルトは 0 です。
- **[RADIUS 属性 4(NAS-IP アドレス)]**：選択すると、スイッチは Access Request RADIUS サーバ パケットに Network Access Server（NAS; ネットワーク アクセス サーバ）属性を含むことができます。このオプションが無効な場合、RADIUS クライアントはスイッチ管理ポート アドレスを NAS-IP アドレスとして使用します。
- **[NAS-IP アドレス]**：Access Request パケットに含める IP アドレス。このフィールドは、RADIUS 属性 4 が有効な場合のみ、編集可能です。アドレスは、RADIUS サーバのスコープ内の NAS で一意である必要があります。

ステップ 3 [適用] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

RADIUS サーバの追加

複数の RADIUS サーバを設定でき、それらがアクセスされる順序を決定するプライオリティ レベルを設定できます。

注意 すべての管理ユーザは、読み取りおよび書き込み権限付きで作成されます。設定したすべての RADIUS サーバのユーザには同じ特権レベルがあることを確認してください。そうでない場合は、スイッチへのアクセスが認められません。

RADIUS サーバを [RADIUS テーブル] に追加するには、次の手順に従います。

ステップ 1 [追加] をクリックします

ステップ 2 パラメータを入力します。

- **[RADIUS サーバ]**：サーバの IP アドレスまたはホスト名。
- **[プライオリティ]**：プライオリティ数値が低いほど、サーバの実際のプライオリティは高くなります。たとえば、プライオリティ値 1 のサーバには、プライオリティ値 2 で設定されたサーバより高いプライオリティがあります。すべてのサーバが、同一またはデフォルトのプライオリティ値で設定されている場合、スイッチは、早いものから順に RADIUS サーバを処理します。範囲は 1 ～ 65535 です。デフォルトは 8 です。
- **[キーストリング]**：スイッチと RADIUS サーバの間のすべての RADIUS 通信の認証と暗号化に使用される共有シークレット テキスト文字列。このシークレットは、RADIUS サーバ側で設定されているシークレットと一致していなければなりません。シークレット キーは、エントリを削除し、対象のシークレット キーでエントリを再作成することで、編集できます。これは、32 ～ 176 文字の ASCII 英数文字である必要があります。
- **[認証ポート]**：RADIUS 認証要求および応答で使用されるポート番号。デフォルトポートである 1812 は、RADIUS 認証サーバ用の既知の IANA ポート番号です。範囲は 1025 ～ 65535 です。デフォルトは 1812 です。
- **[メッセージオーセンティケータ]**：このフィールドは、デフォルトで選択されます。有効な場合、メッセージ オーセンティケータ属性が、サーバへの RADIUS 要求メッセージに含まれます。この属性は、スプーフィングと不正改ざんから RADIUS メッセージを保護します。共有シークレットは、キーとして使用されます。RADIUS Message Authenticator 属性がパケットに存在する場合、サーバによって検証されます。検証に失敗した場合、サーバは要求パケットをドロップします。

ステップ 3 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

パスワード強度

[パスワード強度] ページを使用して、セキュアな管理ユーザ パスワードの属性を設定できます。

パスワード強度を設定するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで、[セキュリティ] > [パスワード強度] の順にクリックします。

ステップ 2 次のパラメータを入力します。

- **[パスワードの長さ (最短)]**：管理ユーザ パスワードに必要な最小文字数。0 を指定して、パスワードの長さを 1 ～ 7 文字に設定するか、または、8 ～ 64 文字の値で特定のパスワード長を設定します。
- **[パスワードエージングタイム]**：チェックボックスをオンにして、パスワードの期限切れ後の期間を 1 ～ 365 日の間で入力します。パスワードの有効期限が切れた場合、ユーザは、続行する前に新しいパスワードを入力する必要があります。

ステップ 3 [強度チェック] フィールドで [有効] を選択して、実行するチェックのタイプを設定します。

- **[パスワードの除外キーワードチェック]**：[有効] を選択すると、ユーザがパスワードを作成または変更するときに、事前設定されたキーワードがパスワードで使用されているかどうかを、スイッチがチェックできるようになります。事前定義されたキーワードは、cisco と ocsic です。
- **[パスワードのユーザ名チェック]**：[有効] を選択すると、ユーザがパスワードを作成または変更するときに、パスワードにユーザ名を含めないようにできます。
- **[文字は 3 回まで繰り返し可能]**：[有効] を選択すると、パスワードで使用されている文字が、4 回以上連続して繰り返されているかどうか、スイッチがチェックできるようになります。
- **[文字クラスの最小数]**：チェックボックスをオンにして、パスワード文字列に含まなければならない文字クラスの最小数を入力します。文字クラスには、大文字、小文字、数字、および標準キーボードで利用可能な特殊文字の 4 つがあります。

ステップ 4 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

管理アクセス プロファイル ルール

[管理アクセスプロファイルルール] ページを使用して、管理目的でデバイスにアクセスするためのプロファイルとルールを定義できます。

特定のユーザ名、入力ポートまたは LAG、および送信元 IP アドレスへのアクセスを制限できます。

このページを表示するには、ナビゲーション ウィンドウで、[セキュリティ] > [管理アクセスプロファイルルール] の順にクリックします。

[アクセスプロファイルテーブル] には、現在設定されているプロファイル（存在する場合）のプロファイル名が表示されます。[プロファイルルールテーブル] には、プロファイルに対する既存のルールが表示されます。デフォルトでは、スイッチで設定されるアクセス プロファイルやルールはありません。1 つのプロファイルのみ作成および有効化でき、そのプロファイルに、作成するすべてのルールが割り当てられます。

アクセス プロファイルとルールの設定

アクセス プロファイルを作成し、ルールを割り当てるには、次の手順に従います。

ステップ 1 [アクセスプロファイルテーブル] で、[追加] をクリックします。

ステップ 2 アクセス プロファイル名を指定し、[有効] を選択します。

ステップ 3 [適用] をクリックしてから、[閉じる] をクリックします。

新しいプロファイルが [アクセスプロファイルテーブル] に表示されます。ここで、ルールをプロファイルに追加できます。

ステップ 4 [プロファイルルールテーブル] で、[追加] をクリックします。

ステップ 5 次のパラメータのいくつかを指定し、アクセスを制限または許可します。

- **[ルールプライオリティ]**：ルールは、着信管理要求に対して、プライオリティの昇順で検証されます。ルールが一致する場合、指定されたアクションが実行され、それ以降のルールは無視されます。たとえば、プライオリティ 1 の送信元 IP 10.10.10.10 を [許可] に設定し、プライオリティ 2 の送信元 IP 10.10.10.10 を [拒否] に設定した場合、プロファイルがアクティブであれば、この IP アドレスに対してアクセスが許可され、2 番目のルールは無視されます。範囲は 1 ～ 16 です。1 は最も高いプライオリティを示します。

- **[管理方式]**：スイッチ設定へのアクセスに使用する方式。デフォルトでは、すべてのユーザが Web ベースのスイッチ設定ユーティリティを使用できるように、HTTP アクセスが許可されます。指定したユーザのみを許可するには、たとえば、すべてのユーザに対して HTTP アクセスが拒否されるルールを作成してから、特定のユーザが許可される別のルールを作成します。特定のユーザを許可するルールには、すべてのユーザを拒否するルールより高い [ルールプライオリティ] が必要です。

  （注）：HTTP は唯一の管理アクセス方式であるため、[HTTP] オプションと [すべて] オプションは同じです。

- **[アクション]**：ルールの基準が一致した場合に実行されるアクションを選択します。
  - **[許可]**：指定したインターフェイス、ユーザ、または IP アドレスは、拒否ルールで明示的に禁止されているスイッチへのアクセスを許可されます。
  - **[拒否]**：指定したインターフェイス、ユーザ、または IP アドレスは、スイッチへのアクセスを拒否されます。
- **[インターフェイスに適用]**：[すべて] を選択して、このルールをすべてのインターフェイス（ポートおよび LAG）に適用します。または、[ユーザ定義] を選択して、ルールを適用するポートまたは LAG を選択します。
- **[ユーザに適用]**：このルールをすべてのシステム ユーザに適用する場合は [すべて] を選択します。または、[ユーザ定義] を選択して、ルールを適用するユーザを [ユーザ名] から選択します。
- **[送信元 IP アドレスに適用]**：[すべて] を選択して、あらゆる送信元 IP アドレスにルールを適用します。または、[ユーザ定義] を選択して、このルールを適用する送信元 IPv4 アドレスおよびマスクを指定します。

ステップ 6 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

新しいルールが [プロファイルルールテーブル] に表示されます。ルールを選択して、[編集] をクリックして編集したり、[削除] をクリックしてアクセス プロファイルからルールを削除したりできます。

（注） ユーザ **cisco** は、管理アクセスを拒否されません。

注意 現在 Web 管理セッションがアクティブなイントラネットまたはドメインへのアクセスを拒否するプロファイルがアクティブになった場合、セッションは、ログアウトまたはタイムアウトされるまでアクティブなままになります。それ以降のセッションは、プロファイルによってブロックされます。Internet Explorer 8 を使用するアクティブなセッションは、スイッチ管理 IP アドレスが Internet Explorer の [ローカル イントラネット サイト] リストに追加されていない場合、ただちに終了します。手順については、**「Web ベースのスイッチ設定ユーティリティの開始」**を参照してください。

アクセス プロファイルおよびルールの修正と削除

アクセス プロファイルを削除する、またはルールを修正する前に、プロファイルを無効にする必要があります。

アクセス プロファイルを無効にするには、次の手順に従います。

ステップ 1 [アクセスプロファイルテーブル] でプロファイルを選択して、[編集] をクリックします。

ステップ 2 [有効] チェックボックスをオフにします。

ステップ 3 [適用] をクリックしてから、[閉じる] をクリックします。

変更が完了したら、アクセス プロファイルを再び有効にします。

アクセス プロファイルを（無効にした後）削除するには、次の手順に従います。

ステップ 1 [アクセスプロファイルテーブル] で、プロファイルを選択します。

ステップ 2 [削除] をクリックします。

（アクセス プロファイルを無効にした後）プロファイル ルールを削除するには、次の手順に従います。

ステップ 1 [プロファイルルールテーブル] でルールを選択します。

ステップ 2 [削除] をクリックします。

（アクセス プロファイルを無効にした後）プロファイル ルールを修正するには、次の手順に従います。

ステップ 1 [プロファイルルールテーブル] でルールを選択して、[編集] をクリックします。

ステップ 2 新しい設定を入力します。

ステップ 3 [適用] をクリックしてから、[閉じる] をクリックします。

(すべての変更が完了した後) アクセス プロファイルを有効にするには、次の手順に従います。

ステップ 1 [アクセスプロファイルテーブル] でプロファイルを選択して、[編集] をクリックします。

ステップ 2 [有効] チェックボックスをオンにします。

ステップ 3 [適用] をクリックしてから、[閉じる] をクリックします。

認証方式

[認証方式] ページを使用して、ユーザがスイッチ ポートへのアクセスをどのように許可されるかを指定できます。

認証方式を選択するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで、[セキュリティ] > [認証方式] の順にクリックします。

ステップ 2 [HTTP] リストで認証方法を選択します。

- **[ローカル]**：サプリカントからのユーザ ID とパスワードの組み合わせは、スイッチでローカルに保存されたユーザ データベースと比較されます。
- **[なし]**：ユーザ認証方式は使用されません。
- **[RADIUS]**：スイッチが認証要求を RADIUS サーバに渡し、RADIUS サーバが RADIUS の Access-Accept または Access-Reject フレームで応答します。
- **[RADIUS、なし]**：スイッチが認証要求を RADIUS サーバに渡します。サーバにアクセスできない場合、認証は使用されません。
- **[RADIUS、ローカル]**：スイッチが認証要求を RADIUS サーバに渡します。サーバにアクセスできない場合、ローカル ユーザ データベースが使用されます。

ステップ 3 [適用] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

ストーム制御

トラフィック ストームは、過剰な数のブロードキャスト、マルチキャスト、または不明なユニキャスト メッセージが、単一ポートによってネットワーク全体で同時に送信された結果、発生します。転送されたメッセージ応答がネットワークのリソースに過負荷を与え、ネットワークをタイムアウトさせる可能性があります。

スイッチは、ポートあたりの着信ブロードキャスト / マルチキャスト / 不明なユニキャストのパケット レートを測定し、レートが定義された値を超過した場合はパケットを破棄します。ストーム制御は、インターフェイスごとに有効または無効にできます。

[ストーム制御] ページを使用して、スイッチのインターフェイスでストーム制御を有効にし、設定できます。このページを表示するには、ナビゲーション ウィンドウで、[セキュリティ] > [ストーム制御] の順にクリックします。

ストーム制御は、デフォルトではすべてのパケット タイプに対してすべてのポートで無効です。ポートのストーム制御設定を編集するには、次の手順に従います。

ステップ 1 設定するポートを選択して、[編集] をクリックします。

ステップ 2 ブロードキャスト、マルチキャスト、およびユニキャストの各トラフィックに対して、選択したポートに次のパラメータを指定します。

- **[モード]**：[有効] を選択すると、そのトラフィック タイプに対してストーム制御保護が有効になります。
- **[レートしきい値タイプ]**：トラフィックがしきい値を超えたかどうかを、スイッチがどのように判別するかを選択します。
  - **[パーセント]**：リンクで容量の割合を超えた場合、トラフィックはドロップされます。
  - **[pps]**：1 秒あたりのパケット。リンクで 1 秒あたりのパケットのしきい値を超過した場合、トラフィックはドロップされます。
- **[レートしきい値]**：パケットが転送される最大レートを指定します。[レートしきい値タイプ] が [パーセント] の場合は、全体のポート容量の割合を入力します（0% ～ 100%）。[レートしきい値タイプ] が [pps] の場合は、1 秒あたりのパケットのレートを入力します（0 ～ 14880000）。10Mpbs、100Mbps、および 1000Mbps で動作するポートの最大スループットは、それぞれ、1 秒あたり 14880、148800、1488000 パケットです。

(注)：ストーム制御をアクティブにするのに必要な入力トラフィックの実際のレートは、着信パケットのサイズと、ハードコーディングされた平均パケット サイズ（512 バイト）に基づきます。ハードウェアでは kbps での絶対レートに対する pps 値が必要とされるため、1 秒あたりのパケット レートが計算されます。たとえば、設定された制限が 10 パーセントの場合、これは約 25000 pps（100 M ポートに対して）に変換されます。

ステップ 3 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

ポート セキュリティ

ポート単位でポートのセキュリティを有効にできます。ポートがセキュリティ保護されている（ロックされている）場合、スイッチは、送信元 MAC アドレスがポートでセキュリティ保護されているパケットのみを転送します。他のすべてのパケットは破棄されます。スイッチは、送信元 MAC アドレスが別のポートでセキュリティ保護されているポートからのパケットも破棄します。

セキュアな MAC アドレスは、静的に設定したり、動的に学習したりできます。セキュリティ保護されているポートでのセキュアな MAC アドレスの最大数は、256 です。スタティック セキュア MAC アドレスは、[スタティックアドレス] ページを使用して設定します。スタティック セキュア MAC アドレスおよびダイナミック セキュア MAC アドレスの両方にエージング制限があります（**「ダイナミック アドレスのエージング タイムの設定」**を参照）。

[ポートセキュリティ] ページを表示するには、ナビゲーション ウィンドウで、[セキュリティ] > [ポートセキュリティ] の順にクリックします。

[ポートセキュリティテーブル] には、各ポートの現在のセキュリティ設定が表示されます。LAG のデータのみを表示するには、[インターフェイスタイプ] リストから LAG を選択します。デフォルトでは、ポートのセキュリティは、グローバルおよび各インターフェイスで無効です。

ポート セキュリティの有効化

ポート セキュリティを設定するには、次の手順に従います。

ステップ 1 [ポートセキュリティ] ページで、[管理モード] で [有効] を選択して、[適用] をクリックします。

ステップ 2 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 3 次の設定を行います。

- **[インターフェイスステータス]**：[ロック] を選択すると、インターフェイスでポート セキュリティが有効になります。インターフェイスがロック解除状態からロック状態に移行した場合、そのポートのスイッチで動的に学習されたすべてのアドレスは、MAC アドレス リストから削除されます。
- **[スタティック MAC アドレスの最大数]**：ポートまたは LAG でのスタティック セキュア MAC アドレスの最大数を指定します。スタティック セキュア MAC アドレスは、[スタティックアドレス] ページで設定されます。セキュアなアドレスの合計数は、256 を超えることはできません。
- **[ダイナミック MAC アドレスの最大数]**：ポートまたは LAG から学習可能な、ダイナミック セキュア MAC アドレスの最大数を指定します。セキュアなアドレスの合計数は、256 を超えることはできません。

  ポート セキュリティがポートで有効で、スタティックおよびダイナミックな制限が新しい値に設定された場合、次のルールが適用されます。

  - 新しい値が、前の値より大きい場合は、ダイナミック アドレスまたはスタティック アドレスのどちらに対してもアクションは実行されません。
  - 新しい値が、前の値より小さい場合は、次のアクションが実行されます。

    ダイナミック アドレス：スイッチは、ポートで学習されたすべてのアドレスのフラッシュを開始します。

    スタティック アドレス：アドレスがセキュア、永続的、またはタイムアウトでの削除のいずれで設定されたかにかかわらず、スイッチは、スタティック アドレスを保持します（スタティック制限まで）。その後、MAC アドレス テーブルから残りのスタティック アドレスを削除します。

- **[違反時アクション]**：ロックされたポートで許可されていない着信パケットをスイッチが処理する方法を選択します。
  - **[廃棄]**：パケットはドロップされます。
  - **[転送]**：パケットは転送されますが、送信元 MAC アドレスは転送データベースに追加されません。
  - **[シャットダウン]**：パケットは廃棄され、ポートはシャットダウンされます。
- **[ダイナミックアドレスをスタティックに変換]**：[有効] を選択すると、すべてのダイナミック セキュア MAC アドレスがスタティック セキュア MAC アドレスに変換されます。
- **[ポートのリセット]**：選択すると、ポート セキュリティ機能によってポートがシャットダウンされた場合に、ポートがリセットされます。

ステップ 4 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

セキュア MAC アドレスの表示と設定

セキュア MAC アドレスの現在のリストと、関連付けられたポートおよび VLAN を表示するには、[ポートセキュリティ] ページで [セキュアアドレステーブル] をクリックします。

インターフェイスごとに、ポートのステータスがロックかロック解除かにかかわらず、[セキュアアドレステーブル] には、スタティックにセキュリティ保護された設定済みの各 MAC アドレスが表示されます。このテーブルには、ロックされたポートに対してダイナミックに学習された MAC アドレスも表示されます。ポートがロックからロック解除に変更された場合、またはリンクがダウンした場合、ポートのダイナミック エントリは、クリアされます。

[スタティックアドレステーブル] をクリックして、スタティック アドレスを設定するページを表示できます。**「スタティック MAC アドレスの設定」**を参照してください。エントリの [ステータス] フィールドは [セキュア] に設定するようにしてください。

[ポートセキュリティテーブル] をクリックして、[ポートセキュリティ] ページを再表示できます。

802.1X

Local Area Network（LAN; ローカルエリア ネットワーク）は、未承認デバイスが LAN インフラストラクチャに物理的に接続されることを許可する環境、または未承認ユーザがすでに接続された機器を経由して LAN にアクセスしようとすることを許可する環境で導入されている場合があります。そのような環境では、LAN で提供されるサービスへのアクセスを、それらのサービスの使用を許可されているユーザやデバイスに制限することが望ましい場合があります。

ポート ベースのアクセス制御では、接続されたポートで提供されるサービスにホストがアクセスできるかどうかをネットワークがコントロールすることができます。IEEE 802.1x プロトコルをベースにした、ポートベースのネットワーク アクセス制御を使用するようにスイッチを設定できます。

802.1x プロトコルでは、次の 3 種類のエンティティを定義します。

- サプリカント：リンクのリモート エンドでポートへのアクセスを要求するエンティティ。サプリカントは、ネットワーク上の別のノード、つまりオーセンティケータが、サーバからの認証を要求するために使用するネットワークに資格情報を提供します。
- オーセンティケータ：リンクのリモート エンドでサプリカントの認証を容易にするエンティティ。オーセンティケータは、認証が成功した場合、サプリカントにポートアクセスを許可します。
- 認証サーバ：オーセンティケータに代わって認証を実行するサーバ（RADIUS サーバなど）。サプリカントが認証中のポート経由で提供されるサービスへのアクセスを承認されているかどうかを示します。

認証プロセスでは、802.1X は、サプリカントとオーセンティケータ間の Extensible Authentication Protocol Over LAN（EAPOL）メッセージをサポートします。

スイッチ ポートは、オーセンティケータ、サプリカントのどちらにも設定できますが、両方には設定できません。

802.1X プロパティ値の設定

802.1X の [プロパティ] ページを使用して、グローバルな 802.1X 管理モードをスイッチで設定できます。

802.1X セキュリティをグローバルに有効にするには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで、[セキュリティ] > [802.1X] > [プロパティ] の順にクリックします。

ステップ 2 [ポートベース認証の状態] で [有効] を選択し、802.1X ポートベースの認証をスイッチでグローバルに許可します。

ステップ 3 [認証方式] リストから認証方式を選択します。

- **[なし]**：ユーザ認証方式は使用されません。
- **[ローカル]**：スイッチは、EAP-MD5 をベースにしたリモート サプリカントのローカル認証を実行します。サプリカント識別情報は、スイッチに設定された管理ユーザのいずれかである必要があります（**「ユーザ アカウントの管理」**を参照）。
- **[RADIUS]**：スイッチは、1 つまたは複数の外部 RADIUS サーバに依存して認証を実行します。サプリカントの ID と認証を、直接サーバに設定する必要があります（詳しくは、**「RADIUS」**を参照）。
- **[RADIUS、なし]**：スイッチは、1 つまたは複数の外部 RADIUS サーバに依存して認証を実行します （前述の [RADIUS] の説明を参照）。スイッチがどのサーバにもアクセスできない場合、どの認証も使用されません。
- **[RADIUS、ローカル]**：スイッチは、1 つまたは複数の外部 RADIUS サーバに依存して認証を実行します（前述の [RADIUS] の説明を参照）。スイッチがどのサーバにもアクセスできない場合、ローカルで認証を実行します（前述の [ローカル] の説明を参照）。

ステップ 4 [適用] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

（注） 個々のポートの役割を選択する手順については、**「ポート PAE 機能の変更」**を参照してください。また、個々のポートで認証を設定する手順については、**「ポート認証の設定」**を参照してください。

ポート PAE 機能の変更

[ポート PAE 機能] ページを使用して、各ポートの 802.1X 役割を表示したり、その役割をオーセンティケータまたはサプリカントとして設定したりできます。

オーセンティケータまたはサプリカントとしてポートの役割を変更するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで、[セキュリティ] > [802.1X] > [プロパティ] の順にクリックします。

ステップ 2 設定するポートを選択して、[編集] をクリックします。

ステップ 3 ポートの役割を選択します。

- **[オーセンティケータ]**：ローカル ポートへのアクセスを許可する前に、ポートがリモート サプリカントの認証を必要とする場合、このオプションを選択します。
- **[サプリカント]**：リモート ポートにアクセスする前に、ポートがリモート オーセンティケータから権限を求める必要がある場合、このオプションを選択します。

ステップ 4 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

ポート認証の設定

[ポート認証] ページを使用して、オーセンティケータとして動作するポートでのポート アクセス コントロールを設定できます。ポートをオーセンティケータとして有効にするには、**「ポート PAE 機能の変更」**を参照してください。

ポートのオーセンティケータ設定を編集するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで、[セキュリティ] > [802.1X] > [ポート認証] の順にクリックします。

[ポート認証テーブル] に、各ポートの現在の設定が表示されます。

ステップ 2 設定するポートを選択して、[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。

- **[ローカルデータベースユーザ名]**：右矢印および左矢印を使用して、設定された管理ユーザを [使用可能] または [選択済み] リストに移動します。[選択済み] リストのユーザのみがポートにアクセスでき、認証の対象になります。このリストは、認証がローカルの場合のみ適用され、RADIUS サーバが認証に使用される場合は適用されません。
- **[現在のポート制御]**：ポートの現在の認証ステータス（「許可」または「無許可」）。
- **[管理ポート制御]**：ポート認証モードを選択します。表示される値は次のとおりです。
  - **[強制無許可]**：ポートに接続されているサプリカントによるポート アクセスを常に拒否するには、このオプションを選択します。選択した場合、ポート制御ステータスは「無許可」になります。
  - **[自動]**：ポート制御が認証プロセスの結果に基づく場合は、このオプションを選択します。サプリカントが認証された場合、ポート制御ステータスは「許可」になり、サプリカントはポートへのアクセスを許可されます。サプリカントが認証されない場合、ポート制御ステータスが「無許可」になり、サプリカントはアクセスを拒否されます。
  - **[強制許可]**：リモート サプリカントの認証が必要ない場合に常にポート アクセスを許可するには、このオプションを選択します。選択した場合、ポート制御ステータスは「許可」になります。
- **[定期再認証]**：ポートがそのサプリカントを定期的に再認証する場合は、このオプションを選択します。認証された状態が維持される場合でも、ポートは、スケジュールされた間隔で再認証します。
- **[再認証期間]**：再認証試行の間隔。範囲は 300 ～ 4294967295 秒です。デフォルトは 3600 秒です。
- **[即時再認証]**：選択した場合、ただちにポートの再認証が強制的に実行されます。
- **[認証状態]**：現在のポート認証状態。示される状態には、初期化、接続解除、接続中、認証中、認証済み、打ち切り中、ホールド済み、強制認証、および強制非認証があります。
- **[バックエンド状態]**：バックエンドの認証ステート マシンの現在の状態。示される値には、要求、応答、成功、失敗、タイムアウト、アイドル、および初期化があります。

- **[待機期間]**：認証失敗情報交換後にスイッチが待機する時間。待機期間中、スイッチは認証要求の受け入れも開始も行いません。特定のクライアントと認証サーバに関する信頼できないリンクや特定の動作の問題など、一般的ではない事情に対応する場合にのみ、このコマンドのデフォルト値を変更してください。より迅速な応答時間をユーザに提供するには、デフォルト（60 秒）より小さい値を入力します。範囲は 0 ～ 65535 秒です。
- **[EAP の再送信]**：EAP 要求が再送信されるまでの時間。範囲は 1 ～ 65535 秒で、デフォルトは 30 秒です。
- **[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時間。特定のクライアントと認証サーバに関する信頼できないリンクや特定の動作の問題など、一般的ではない事情に対応する場合にのみ、このコマンドのデフォルト値（30 秒）を変更してください。より迅速な応答時間をユーザに提供するには、デフォルトより小さい値を入力します。範囲は、1 ～ 65535 秒です。
- **[サーバタイムアウト]**：スイッチが要求を認証サーバに再送信するまでの時間。範囲は 1 ～ 65535 秒で、デフォルトは 30 秒です。
- **[最大 EAP 要求]**：応答を受信しない場合、認証プロセスを再び開始する前に、スイッチが EAP 要求を送信できる、事前設定された最大回数。
- **[終了原因]**：終了の理由。

ステップ 4 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

サプリカント ポート認証の設定

[サプリカントポート認証] ページを使用して、サプリカント役割で設定されたポートでポート アクセス コントロールを設定できます。ポートをサプリカントとして有効にするには、**「ポート PAE 機能の変更」**を参照してください。

サプリカント ポート認証を設定するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで、[セキュリティ] > [802.1X] > [サプリカントポート認証] の順にクリックします。

ステップ 2 設定するポートを選択して、[編集] をクリックします。

[現在のポート制御] フィールドに、ポートの現在の認証モードが表示されます。

ステップ 3 次の設定を行います。

- **[管理ポート制御]**：ポート認証モードを選択します。表示される値は次のとおりです。
  - **[強制無許可]**：インターフェイスを未承認状態に移行することにより、選択されたインターフェイスからのシステム アクセスを拒否します。
  - **[自動]**：サプリカント、オーセンティケータ、および認証サーバの間の認証交換の結果に基づいたインターフェイスのモードをスイッチが検出します。
  - **[強制許可]**：認証サーバでの認証を必要とせずに、ポートは承認済み状態になります。インターフェイスは、クライアントのポート ベースの認証なしに通常のトラフィックを送受信します。
- **[ユーザ名]**：サプリカントとして自身を特定するためにポートによって使用されるユーザを選択します。ユーザは、スイッチで設定されたスイッチ管理ユーザのいずれかである必要があります。ユーザに設定されたパスワードは、認証プロセスで使用されます。サプリカントとして、スイッチは EAP-MD5 認証方式をサポートします（ユーザの設定については、**「ユーザ アカウントの管理」**を参照）。

ステップ 4 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

認証済みホストの表示

認証済みユーザが存在するポートを [認証済みホスト] ページで表示するには、ナビゲーション ウィンドウで、[セキュリティ] > [802.1X] > [認証済みホスト] の順にクリックします。

[認証済みホスト] に、各ホストの次の情報が表示されます。

- **[ポート]**：認証に使用されるポート。
- **[ユーザ名]**：ホストのユーザ名。
- **[サプリカント MAC アドレス]**：サプリカント デバイス MAC アドレス。
- **[セッション時間]**：サプリカントがログインしてからの時間（秒数）。
- **[セッションタイムアウト]**：指定のセッションが有効な時間。ポート認証で RADIUS サーバによって時間（秒数）が返されます。

11

Quality of Service

この章では、Quality of Service（QoS）の概要と、[Quality of Service] メニューで利用可能な QoS 機能について説明します。

- 「QoS プロパティ」
- 「キューの定義」
- 「CoS/802.1p プライオリティのキューへのマッピング」
- 「IP Precedence のキューへのマッピング」
- 「DSCP 値のキューへのマッピング」
- 「レート制限プロファイルの定義」
- 「レート制限プロファイルのインターフェイスへの適用」
- 「トラフィック シェーピング」

一般的なスイッチでは、各物理ポートは、接続されたネットワークでパケットを送信するための 1 つまたは複数のキューで構成されます。ポートあたりの複数キューは、ユーザが定義した基準に基づき、一部のパケットをそれ以外のパケットより優先するように設定されることがあります。パケットがポートで通信のためにキューイングされる場合、処理されるレートは、どのようにキューが構成されているか、また、場合によってはポートの他のキューに存在するトラフィック量によって変わります。遅延が必要な場合は、スケジューラがキューの通信を承認するまで、パケットがキューで保持されます。キューがいっぱいになると、通信するパケットを保持する場所がなくなり、スイッチによってパケットがドロップされる場合があります。

QoS とは、厳密なタイミング要件のあるパケットを、遅延をより許容できるパケットから区別することで、一貫した予測可能なデータ提供を実現する方法です。厳密なタイミング要件のあるパケットは、QoS 対応ネットワークで特別に扱われます。

QoS 動作が有効なネットワークでは、ネットワークのすべての要素が QoS 対応である必要があります。QoS 対応ではないノードが 1 つでも存在すると、ネットワーク パスの欠損が生じ、全体のパケット フローのパフォーマンスが低下します。

スイッチは、ポートまたは LAG ごとに 4 つの出力キューをサポートします。キュー 1 のプライオリティは最も低く、キュー 4 のプライオリティは最も高くなります。

[Quality of Service] メニューのページでは、キューのプロパティを定義し、それらを特定の特性があるトラフィックや特定のインターフェイスで到達するトラフィックと関連付けることができます。ポートが処理できる以上のトラフィックを受信するかどうかを決定する基準を定義するレート制限プロファイルを作成することもできます。その後、レート制限プロファイルをポートに割り当てることができます。

QoS プロパティ

イーサネット フレームや IP パケット ヘッダーでエンコードされたプライオリティ情報に基づいて、出力キューにトラフィックを割り当てるようにスイッチ ポートを設定できます。または、トラフィックでは、到達するポートで設定されたデフォルトのプライオリティ値が使用される場合もあります。ポートが、エンコードされたプライオリティ値（802.1p、IP precedence、DSCP 値など）を使用するように設定された場合、そのポートは信頼できるポートと見なされます。キュー割り当て決定を行うために、フレームまたはパケットでエンコードされた値ではなく、自身のプライオリティ値を使用するように設定されたポートは、信頼できないと見なされます。

ポートが信頼できるポートとして設定されているものの、フレームまたはパケットにプライオリティ情報がない場合、デフォルト ポートのプライオリティがパケットに割り当てられます。デフォルト ポートのプライオリティは 0 です。

[VLAN 管理] > [インターフェイス設定] ページを使用して、[VLAN プライオリティ] の値を変更できます。

[QoS プロパティ] ページを使用して、信頼できるポートまたは信頼できないポートとしてポートを定義し、どのプライオリティ値を信頼するか設定できます。

ポートまたは LAG で信頼モードを設定するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで、[Quality of Service] > [QoS プロパティ] 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] リストを使用して、ポートまたは LAG を [信頼モードの設定テーブル] に表示します。

ステップ 3 設定す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 4 パケットの出力キューの決定に使用されるプライオリティ値のタイプを設定するには、次の信頼モードのいずれかを選択します。

- **[非信頼]**：ポートは自身のデフォルト 802.1p プライオリティ（0）を割り当てます。

- **[dot1p を信頼]**：ポートは、VLAN タグ付きイーサネット フレームで 802.1p プライオリティ値を使用します。タグなしフレームでは、ポートのデフォルト プライオリティが割り当てられます。
- **[IP precedence を信頼]**：ポートは、IP パケット ヘッダーの IP Precedence 値を使用します。値がない場合は、ポートのデフォルト プライオリティが割り当てられます。非 IP VLAN タグ付きおよびタグなしのフレームには、ポートのデフォルト プライオリティが割り当てられます。
- **[IP-DSCP を信頼]**：ポートは、VLAN タグ付きとタグなしの両方の IP パケットで、IP パケット ヘッダーの DSCP マーキングを使用します。非 IP VLAN タグ付きおよびタグなしのフレームには、ポートのデフォルト プライオリティが割り当てられます。
- **[すべて信頼]**：IP パケットに対して、ポートはプライオリティを決定するために DSCP マーキングを使用します。非 IP フレームに対しては、ポートは、フレームが VLAN タグ付きの場合は 802.1p プライオリティを使用し、フレームが VLAN タグ付きではない場合はポートのデフォルト プライオリティを使用します。

ステップ 5 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

キューの定義

[キュー] ページを使用して、出力ポートにアクセスできるキューをトラフィック スケジューラが判別する方法を設定できます。キューは、Strict Priority（SP; 完全優先）モードまたは、Weighted Round-Robin（WRR; 重み付けラウンドロビン）モードで設定できます。デフォルトでは、すべてのキューは SP モードのキューです。

パケットは、次の原則に従って送信されます。

- プライオリティが最も高いキューのパケットが最初に送信されます。
- キューが SP モードの場合、パケットがなくなるまで、またはプライオリティがより高いキューに送信パケットがある状態になるまで、送信できます。
- キューが WRR モードの場合は、設定可能なウェイト値に比例したパケット数を送信できます。ウェイトは、各ポートの全体の帯域幅の割合として表されます。

1 つのポートに SP キューと WRR キューの組み合わせを設定することができます。

キュー設定の推奨事項

より高い値が付けられたキューには、より高いプライオリティ、ウェイト、および最小帯域幅を設定することを推奨します。

キュー 1 ～ 4 での SP モードと WRR モードに推奨されるシナリオは次のとおりです。

- **4 つのキューすべてが SP モード**（Q4 > Q3 > Q2 > Q1）：Q4 は、Q4 で処理するパケットが存在する限り、帯域幅が割り当てられます。その後、Q3 が処理され、続いて、Q2、Q1 が順に処理されます。
- **4 つのキューすべてが WRR モード**（Q4:Q3:Q2:Q1 = A:B:C:D）：このモードでは、各キューは、設定されたウェイトに従って、その最小帯域幅が割り当てられます。
- **1 つのキューが SP モード、3 つのキューが WRR モード**（Q4 > Q3/Q2/Q1; Q3:Q2:Q1 = A:B:C）：このシナリオでは、Q4 を SP モードで設定し、Q3、Q2、および Q1 を WRR モードで設定することを推奨します。
- **2 つのキューが SP モード、残り 2 つのキューが WRR モード**（q4 > q3 > q2/q1; q2:q1 = A:B）：このシナリオでは、Q4 と Q3 を SP モードで設定し、Q2 と Q1 を WRR モードで設定することを推奨します。

これらのシナリオでは、出力ポートの別のキューに向かうトラフィックがある入力ポートがより多く存在する場合に、システムが Head of Line（HOL; 行頭）ブロッキング状態になる可能性があることを、考慮に入れています。より番号が大きいキューはより小さい最小帯域幅とウェイトで設定されているにもかかわらず、HOL では、番号が大きいキューほど、より多くの帯域幅を取得する結果になる場合があります。より番号が大きいキューは、SP モードでより大きいウェイトで設定することを常に推奨します。これによって、HOL 状態になっても、対象の出力の分離がキューの間で行われます。

キューの設定

QoS プロパティを設定するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで、[Quality of Service] > [キュー] の順にクリックします。

ステップ 2 設定するポートまたは LAG を選択します。

ステップ 3 選択したインターフェイスでキューごとに、次のモードのいずれかを選択します。

- **[完全優先]**：選択すると、スケジューラは、キューのプライオリティ レベルに厳密に基づいて、トラフィックを転送します。プライオリティが最も高いトラフィックがあるキューは、そのようなトラフィックがすべて転送されるまで、出力ポートにアクセスできます。低遅延サービスを、よりプライオリティが高いトラフィック クラスに提供するために、SP モードを使用できます。

- **[WRR]**：選択すると、その他の WRR キューと相対的な帯域幅の割合に基づいて、スケジューラが他の WRR キューとともに順番にキューを処理します。SP モードのキューは、プライオリティがより高いトラフィックがある間、処理され続けます。

ステップ 4 キューに WRR モードを選択した場合、[WRR 帯域幅のパーセント] フィールドに帯域幅の割合を入力します。すべてのキューの帯域幅の割合の合計は、100% を超えてはなりません。

ステップ 5 [適用] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

これらのキュー プロパティを、スイッチ上の他のインターフェイスすべてに適用するには、[設定をすべてのインターフェイスにコピー] をクリックします。

CoS/802.1p プライオリティのキューへのマッピング

インターフェイスで到達するパケットのプライオリティは、イーサネット フレーム ヘッダーにある IEEE 802.1p プライオリティ値で特定される場合があります。802.1p は、8 つのプライオリティ レベル（0 ～ 7）を指定します。[CoS/802.1p 値のキューへのマッピング] ページを使用して、これらのプライオリティ レベルを 4 つの CoS キューにマッピングし、パケットを適切なアウトバウンド キューに方向付けることができます。キュー 1 のプライオリティは最も低く、キュー 4 のプライオリティは最も高くなります。

（注） CoS/802.1p のプライオリティ レベルとキューのマッピングは、インターフェイスごとに設定されます。着信インターフェイスでこれらのマッピング値を設定します。

802.1p プライオリティ値をキューにマッピングするには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで、[Quality of Service] > [CoS/802.1p 値のキューへのマッピング] の順にクリックします。

ステップ 2 設定するポートまたは LAG を選択します。

ステップ 3 各 802.1p サービス クラスに対して、[出力キュー] リストからのキューを選択します。キュー 1 のプライオリティは最も低く、キュー 4 のプライオリティは最も高くなります。

ステップ 4 [適用] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

ステップ 5 これらのマッピングを、スイッチ上の他のインターフェイスすべてに適用するには、[設定をすべてのインターフェイスにコピー] をクリックします。

（注） [デフォルトの復元] をクリックした場合、次のマッピングがすべてのインターフェイスに適用されます。

802.1p プライオリティ	出力キュー
0	1
1	1
2	2
3	3
4	3
5	4
6	4
7	4

IP Precedence のキューへのマッピング

インターフェイスで到達するパケットのプライオリティは、IP パケット ヘッダーの Type of Service（ToS）フィールドで特定される場合があります。8 つの precedence レベルが定義されます（0 ～ 7）。[IP precedence のキューへのマッピング] ページを使用して、これらの値を 4 つの CoS キューにマッピングし、パケットを適切なアウトバウンド キューに方向付けることができます。キュー 1 のプライオリティは最も低く、キュー 4 のプライオリティは最も高くなります。

（注） IP Precedence とキューのマッピングはインターフェイスごとに設定されます。着信インターフェイスでこれらのマッピング値を設定します。

IP Precedence 値をキューにマッピングするには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで、[Quality of Service] > [IP precedence のキューへのマッピング] の順にクリックします。

ステップ 2 設定するポートまたは LAG を選択します。

ステップ 3 各 IP Precedence 値に対して、[出力キュー] リストからキューを選択します。キュー 1 のプライオリティは最も低く、キュー 4 のプライオリティは最も高くなります。

ステップ 4 [適用] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

これらのマッピングを、スイッチ上の他のインターフェイスすべてに適用するには、[設定をすべてのインターフェイスにコピー] をクリックします。

（注） [デフォルトの復元] をクリックした場合、次のマッピングがすべてのインターフェイスに適用されます。

IP Precedence	出力キュー
0	1
1	1
2	2
3	3
4	3
5	4
6	3
7	3

DSCP 値のキューへのマッピング

インターフェイスで到達するパケットのプライオリティは、IP パケット ヘッダーの Differentiated Service Code Point（DSCP）値で特定される場合があります。IP DSCP フィールドには、64 の値（0 ～ 63）のいずれかが含まれます。[DSCP 値のキューへのマッピング] ページを使用して、これらの値を 4 つの出力キューにマッピングできます。キュー 1 のプライオリティは最も低く、キュー 4 のプライオリティは最も高くなります。

DSCP マッピング設定は、すべてのポートにグローバルに適用されます。

DSCP 値をキューにマッピングするには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで、[Quality of Service] > [DSCP 値のキューへのマッピング] の順にクリックします。

ステップ 2 各入力 DSCP 値に対して、[出力キュー] リストからキューを選択します。キュー 1 のプライオリティは最も低く、キュー 4 のプライオリティは最も高くなります。

ステップ 3 [適用] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

（注） [デフォルトの復元] をクリックした場合、次のマッピングがすべてのインターフェイスに適用されます。

DSCP 値	出力キュー
00 ～ 07	1
08 ～ 15	1
16 ～ 23	2
24 ～ 31	3
32 ～ 39	3
40 ～ 47	4
48 ～ 55	3
56 ～ 63	3

レート制限プロファイルの定義

レート制限機能によって、ポートに対して最大着信トラフィック レートを設定できます。データ レートが設定された値を超えると、スイッチは、ポートからそれ以降のすべてのトラフィックをドロップします。レート制限はポートごとに適用されます。

レート制限を適用するには、まずこのページを使用して 1 つまたは複数のレート制限プロファイルを作成します。プロファイルは、どのような場合にレート制限を超えたと判断するかの基準を指定します。その後、レート制限プロファイルをインターフェイスに割り当てます（**「レート制限プロファイルのインターフェイスへの適用」**を参照）。

[レート制限プロファイルテーブル] にエントリを追加するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで、[Quality of Service] > [レート制限プロファイル] 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 パラメータを入力します。

- **[プロファイル ID]**：プロファイルを識別する 1 ～ 64 の任意の数を指定します。
- **[CIR]**：データが送信された時点のレートである、認定情報レートを指定します。レートは、最小時間間隔で平均されます。範囲は 64 ～ 1048576 Kbps です。
- **[CBS]**：ポート上のバースト トラフィック用の保証された帯域幅である、認定バースト サイズを指定します。範囲は 4 ～ 16384 KB です。

ステップ 4 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

レート制限プロファイルのインターフェイスへの適用

1 つまたは複数のレート制限プロファイルを作成した場合、このページを使用してインターフェイスに割り当てることができます。プロファイル作成の手順については、**「レート制限プロファイルの定義」**を参照してください。

レート制限プロファイルをインターフェイスに適用するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで、[Quality of Service] > [インターフェイスレート制限] 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] リストを使用して、[インターフェイスレート制限テーブル] にポートまたは LAG を表示します。

ステップ 3 設定す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 4 プロファイルを追加または削除します。

- このインターフェイスにプロファイルを割り当てるには、[使用可能] リストでプロファイル ID を選択してから、右矢印ボタンをクリックして、[選択済み] リストに移動します。ポートに割り当てることができるのは 1 つのプロファイルのみであるため、すべてのプロファイルが [使用可能] リストから消えます。
- プロファイルを削除するには、[選択済み] リストでプロファイル ID を選択してから、左矢印ボタンをクリックして、[使用可能] リストに移動します。すべてのプロファイルが [選択済み] リストに表示されます。

ステップ 5 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

トラフィック シェーピング

[トラフィックシェーピング] ページを使用して、パケット出力レートを平滑化できます。各ポートと LAG に対して、帯域幅の割合で表される、最大の出力レートを設定できます。トラフィック レートがこの制限に達した場合、過剰なパケットはキューに保持された後、一定時間間隔でその後送信されるようにスケジューリングされます。

トラフィック シェーピングをポートまたは LAG で設定するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで、[Quality of Service] > [トラフィックシェーピング] 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] リストを使用して、ポートまたは LAG を [トラフィックシェーピング設定テーブル] に表示します。

ステップ 3 設定す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 4 選択したポートまたは LAG に対して、全体の帯域幅の割合として、出力レート制限を入力します。[適用] をクリックします。

ステップ 5 必要に応じて前のステップを繰り返して、他のポートと LAG に帯域利用率を割り当てます。

ステップ 6 完了したら、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるように要求されることがあります。 VCCI-A

接続ケーブル、電源コード、ACアダプタなどの部品は、必ず添付品または指定品をご使用ください。添付品・指定品以外の部品をご使用になると故障や動作不良、火災の原因になります。また、電気用品安全法により、当該法の認定（PSEとコードに表記）ではなくUL認定（ULまたはCSAマークがコードに表記）の電源ケーブルは弊社が指定する製品以外の電気機器には使用できないためご注意ください。

Cisco および Cisco ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の国における商標です。Cisco の商標の一覧は、www.cisco.com/go/trademarks でご確認いただけます。掲載されている第三者の商標はそれぞれの権利者の財産です。「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。（1005R）

Copyright © 2011 Cisco Systems, Inc. All rights reserved.

78-19568-01