Future X Communications

FXCX5512PE Management Guide

2024 年 6 月 Ver.1.3

FXC株式会社

本マニュアルについて

■ 本マニュアルでは、FXCX5512PE の各種設定およびシステムの管理手順について説明します。

製品取り扱い時のご注意

この度は、お買い上げいただきましてありがとうございます。製品を安全にお使いいただくため、必ず最初にお読みください。

・下記事項は、安全のために必ずお守りください。

● 安全のための注意事項を守る

注意事項をよくお読みください。製品全般の注意事項が記載されています。

● 故障したら使わない

すぐに販売店まで修理をご依頼ください。

● 万一異常が起きたら

・煙が出たら

・異常な音、においがしたら

・内部に水・異物が入ったら

・製品を高所から落としたり、破損したとき

①電源を切る（電源コードを抜く）

②接続ケーブルを抜く

③販売店に修理を依頼する

- 下記の注意事項を守らないと、火災・感電などにより死亡や大けがの原因となります。

● 電源ケーブルや接続ケーブルを傷つけない

- 電源ケーブルを傷つけると火災や感電の原因となります。
- 重いものをのせたり、引っ張ったりしない。
- 加工したり、傷つけたりしない。
- 熱器具の近くに配線したり、加熱したりしない。
- 電源ケーブルを抜くときは、必ずプラグを持って抜く。

● 内部に水や異物を入れない

- 火災や感電の原因となります。
- 万一、水や異物が入ったときは、すぐに電源を切り（電源ケーブルを抜き）、販売店に点検・修理をご依頼ください。

● 内部をむやみに開けない

本体及び付属の機器（ケーブル含む）をむやみに開けたり改造したりすると、火災や感電の原因となります。

● 落雷が発生したらさわらない

感電の原因となります。また、落雷の恐れがあるときは、電源ケーブルや接続ケーブルを事前に抜いてください。本機が破壊される原因となります。

● 屋外（またはそれに準ずる場所）には設置しない

火災や故障の原因となります。
ほこりの多い場所、直射日光の当たる場所、温度変化や振動の激しい場所、腐食性ガス・油煙の発生する場所、高温多湿などの環境ではご使用できません。

● 油煙、湯気、湿気、ほこりの多い場所には設置しない

本書に記載されている使用条件以外の環境でのご使用は、火災や感電の原因となります。

- 下記の注意事項を守らないとけがをしたり周辺の物品に損害を与える原因となります。

● ぬれた手で電源プラグやコネクタに触らない

感電の原因となります。

● 指定された電源コードや接続ケーブルを使う

マニュアルに記載されている電源ケーブルや接続ケーブルを使わないと、火災や感電の原因となります。

● 指定の電圧で使う

マニュアルに記されている電圧の範囲で使わないと、火災や感電の原因となります。

● コンセントや配線器具の定格を超えるような接続はしない

発熱による火災の原因となります。

● 通風孔をふさがない

- 通風孔をふさいでしまうと、内部に熱がこもり、火災や故障の原因となります。また、風通しをよくするために次の事項をお守りください。
- 毛足の長いジュウタンなどの上に直接設置しない。
- 布などでくるまない。

● 移動させるときは、電源ケーブルや接続ケーブルを抜く

接続したまま移動させると、電源ケーブルが傷つき、火災や感電の原因となります。

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要求されることがあります｡ VCCI-A

目次

はじめに 3
1 章 WEB 接続手順 4
1.1 本機との接続 4
1.1.1 動作環境 4
1.1.2 ネットワークへの接続方法 5
2 章 WEB による機能設定 9
2.1 本機の画面について 9
2.2 モニター 11
2.2.1 ダッシュボード 12
2.2.2 リアルタイムメーター 13
2.2.3 統計情報 14
2.2.4 MAC アドレステーブル 18
2.2.5 RMON 21
2.2.6 SFP モジュール情報 26
2.3 設定 28
2.3.1 システム設定 28
2.3.2 SNMP 39
2.3.3 ポートの設定 50
2.3.4 電源 63
2.3.5 VLAN 設定 70
2.3.6 STP(スパニングツリー) 80
2.3.7 リンクアグリゲーション 92
2.3.8 L3 プロトコル 97
2.3.9 LBD 121
2.3.10 QoS 122
2.3.11 アクセス制御 132
2.3.12 ファームウェア 144
2.4 解析 147
2.4.1 ログ 147
2.4.2 診断ツール 152
2.5 ユーザとグループ 156
2.6 セキュリティ 157
2.6.1 802.1X 157
2.6.2 アクセス 160
2.6.3 ポートセキュリティ 162
2.6.4 DoS 164
2.6.5 DAI 165
3 章 CLI による設定方法 174
3.1 CLI による設定方法 174
3.1.1 接続手順 174
3.1.2 ユーザのアクセスレベルの設定方法 177
3.1.3 CLI の使用方法 178
3.1.4 各コマンドモード 181

3.2 各コマンドによる設定 182
3.2.1 System 182
3.2.2 EEE/PoE 210
3.2.3 SSH 213
3.2.4 PD Lifeguard 214
3.2.5 Link Aggregation 219
3.2.6 mirror 222
3.2.7 STP 224
3.2.8 LLDP 249
3.2.9 IGMP 254
3.2.10 MLD 266
3.2.11 jumbo-frame 274
3.2.12 SNMP 275
3.2.13 DNS 285
3.2.14 IP 286
3.2.15 DHCP Server 291
3.2.16 IPv6 293
3.2.17 VLAN 298
3.2.18 Voice-VLAN 304
3.2.19 GVRP 307
3.2.20 PNAC(ポートベースネットワークアクセス制御) 309
3.2.21 Log 322
3.2.22 ACL 325
3.2.23 QoS 341
3.2.24 Bandwidth control 348
3.2.25 arp inspection 349

はじめに

この度は、弊社FXCX5212PEをお買い上げ頂き誠にありがとうございます。

お使いになる前に、本書をよくお読みください。
また、お読みになった後は、後日お役に立つこともありますので必ず保管してください。
本書は、本製品を正しくご利用頂く上で必要な機能説明および操作方法について記述しています。

本機は主な設定は、イーサネットポート経由でPCからWEBブラウザにておこないますが、基本的な設定については、
付属のコンソールケーブルを用いてコンソールポート経由でログインして設定することも可能です。

旧バージョンおよびリビジョンでは、本マネジメントガイドに示されているコマンドやGUI表示が異なる場合があります。

■ 1 章 WEB 接続手順 ■

1.1 本機との接続

本製品にはHTTPのWebエージェントが組み込まれているので、Webブラウザを使用して、本機を設定し、統計値を確認してネットワークアクティビティをモニタリングすることができます。
Webエージェントには、標準のWebブラウザを使用して、ネットワーク上の任意のPCからアクセスすることができます。

本章では、WEBインタフェースによる設定方法について説明します。
コマンドラインインタフェース(CLI)による接続方法については、「3.1 CLIによる設定方法」をご参照ください。

1.1.1 動作環境

本製品の動作環境は、下記のとおりです。

❑本製品の対応 OS:
・Windows 10/11(32 ビット/64 ビット)
・MacOS

❑対応ブラウザー
・Microsoft Edge
・Google Chrome
・Firefox
・Safari

※最新の対応情報は、当社ホームページをご確認ください。

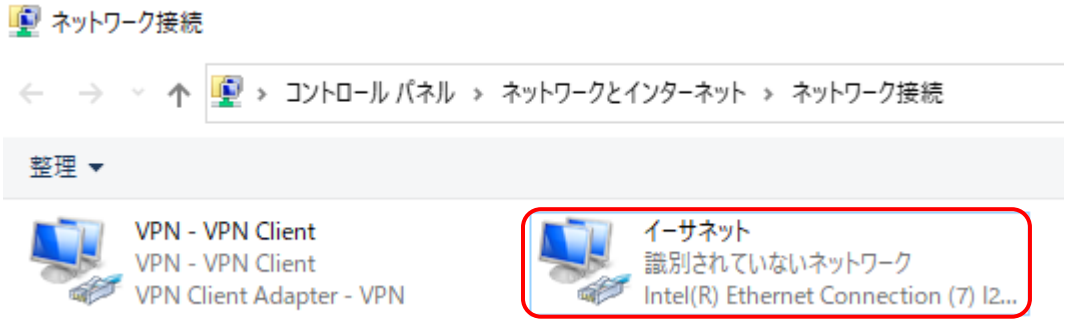
1.1.2 ネットワークへの接続方法

Windows 10のIPアドレスを固定にて設定する方法について説明します。
下記の手順に従って、お使いのPCのIPアドレスを設定してください。

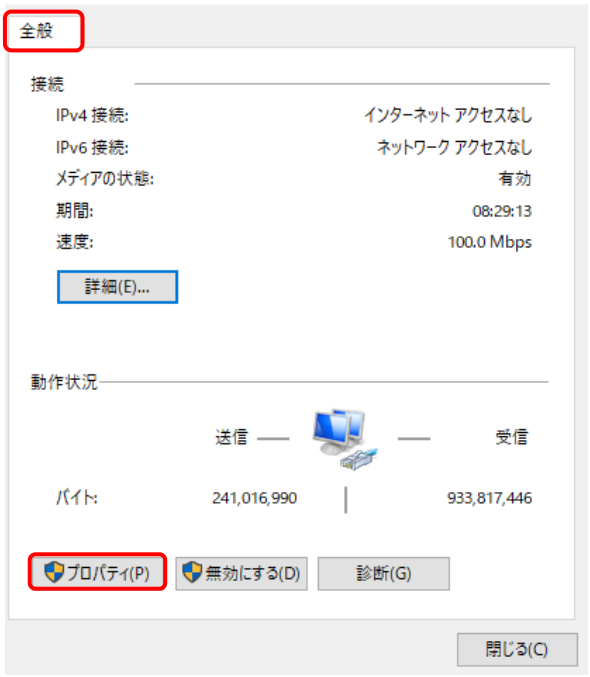
1) TCP/IP の設定
「コントロールパネル」画面 →「ネットワークの状態とタスクの表示」をクリック します。

2)「ネットワークと共有センター」画面→「アダプターの設定の変更」をクリックします。

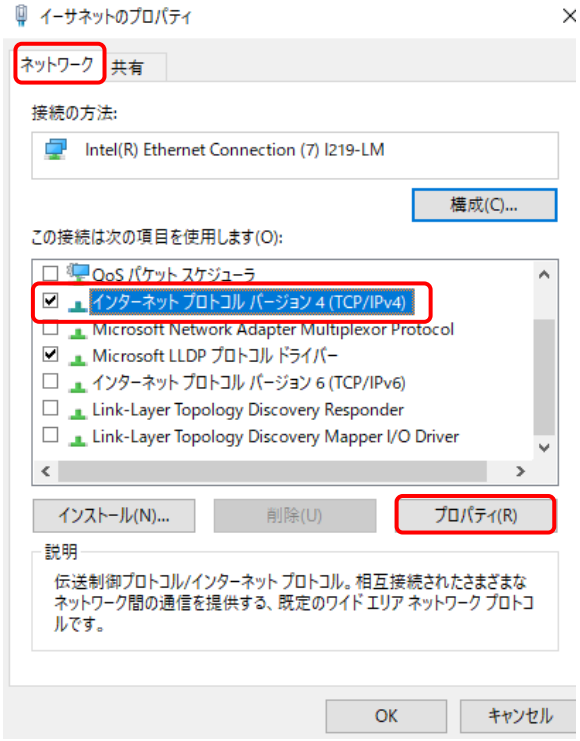
3) イーサネットアイコンをダブルクリックします。
※下の図のように、ご利用のアダプタ名がついたアイコンがすでに存在する場合は、インターネットがご利用可能な状態になっています。



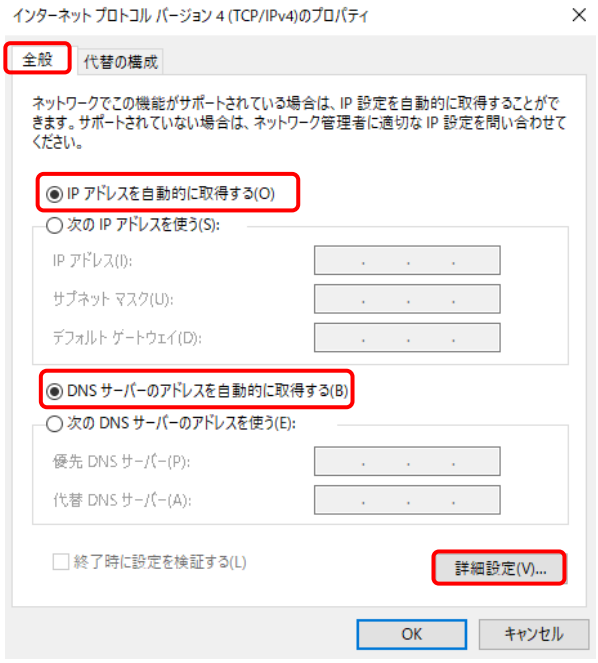
4) イーサネットの接続状態を確認します。
「全般」タブ→「プロパティ」をクリックしてください。



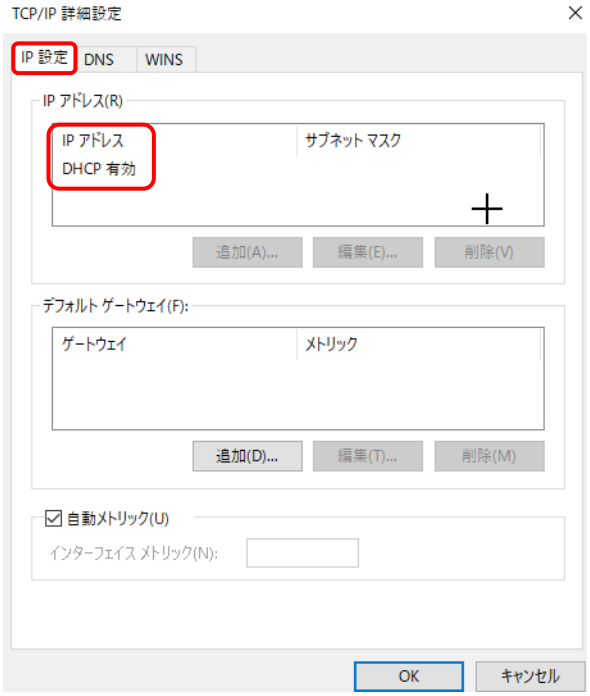
5) 「イーサネットのプロパティ」画面→「ネットワーク」タブ→「インターネットプロトコルバージョン 4(TCP/IPv4)」を選択して、「プロパティ」をクリックしてください。



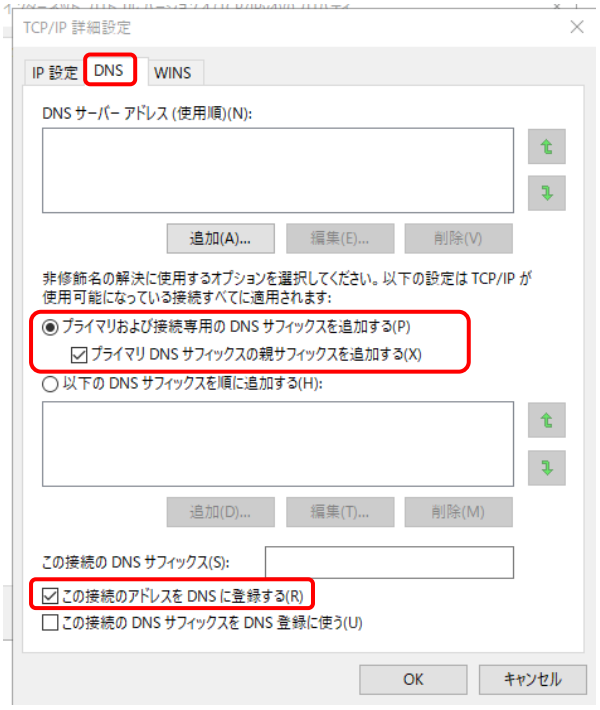
6) 「インターネットプロトコルバージョン 4(TCP/IPv4) のプロパティ」画面→「全般」タブ→[IP アドレスを自動的に取得する]および「DNS サーバのアドレスを自動的に取得す る」に☑が入っていることを確認して、「詳細設定」をクリックします。



7)「TCP/IP 詳細設定」画面→「IP 設定」タブ→「IP アドレス」欄に“DHCP 有効”と表示 されていることを確認して、<OK>ボタンをクリックします。



8)「DNS」タブ→「プライマリおよび接続専用の DNS サフィックスを追加する」と「プライマリ DNS サフィックスの親サフィックスを追加する」にチェックを入れます。
※「この接続のアドレスを DNS に登録する」に☑を入れてください。



以上で、設定は完了です。

■ 2 章 WEB による機能設定 ■

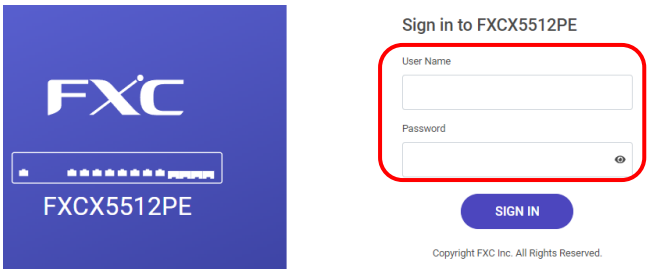
ここでは、WEBによる本体の設定方法について説明します。

ネットワークへの接続方法については、前項の「1.1.2 ネットワークへの接続方法」を参照してください。

2.1 本機の画面について

1. 本機へのログイン

ユーザ名とパスワードを入力後に<**SIGN IN**>ボタンをクリックすると、本機のメイン画面が表示されます。
☞ デフォルト設定のユーザ名およびパスワードは「admin」です。



2. メイン画面の構成

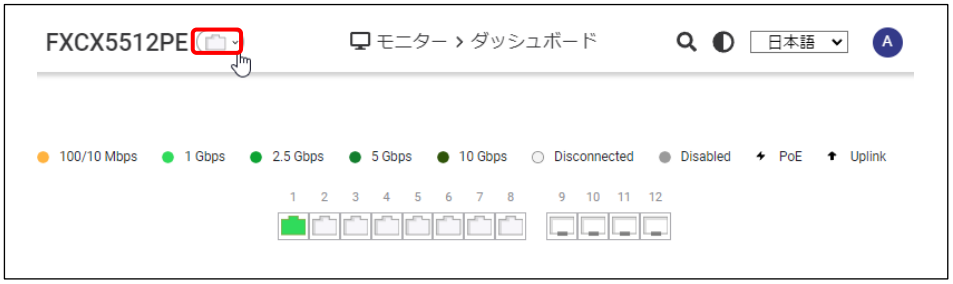
メイン画面の設定については、以下のとおりです。

① メニューウィンドウ

本メニューは、上記の5つのメニュー（「モニター」、「設定」、「解析する」、「ユーザとグループ」、「セキュリティ」、）により設定されています。

② ポート選択メニュー

ポートの各機能の設定時に、この画面より設定することができます。



③ 言語の切り替え

プルダウンメニューにより、「日本語」や「英語」等の言語に切り替えることができます。

④ メインウィンドウ

メニューウインドウで選択したメニューに応じて、各機能の設定を行ったり、ステータス情報が表示されます。

3. 基本メニューについて

基本的な機能について説明すると共に、Webブラウザを使用して個々の機能について説明します。

このセクションは、以下のメニューで構成されています。

2.1 モニター	より効率的な方法で機器をモニタリングできるようになり、各特定の機能項目を使用して、PoE 使用率、使用統計、接続先の機器情報などを含む機器のステータスを迅速に把握できるようになります。
2.2 設定	本機の主な機能（スパニングツリー、リンクアグリゲーション、ミラーリング、ループ検知、VLAN）の設定方法について説明します。
2.3 解析する	ネットワークや装置に負荷をかけずにログ情報や診断ツールを介してモニタリングしたり、解析することができます。
2.4 ユーザとグループ	手動で設定したユーザごとに、ユーザ名とパスワードに基づいて本機への管理アクセスを制御します。
2.5 セキュリティ	ポートベースのセキュリティ機能とその設定手順について説明します。

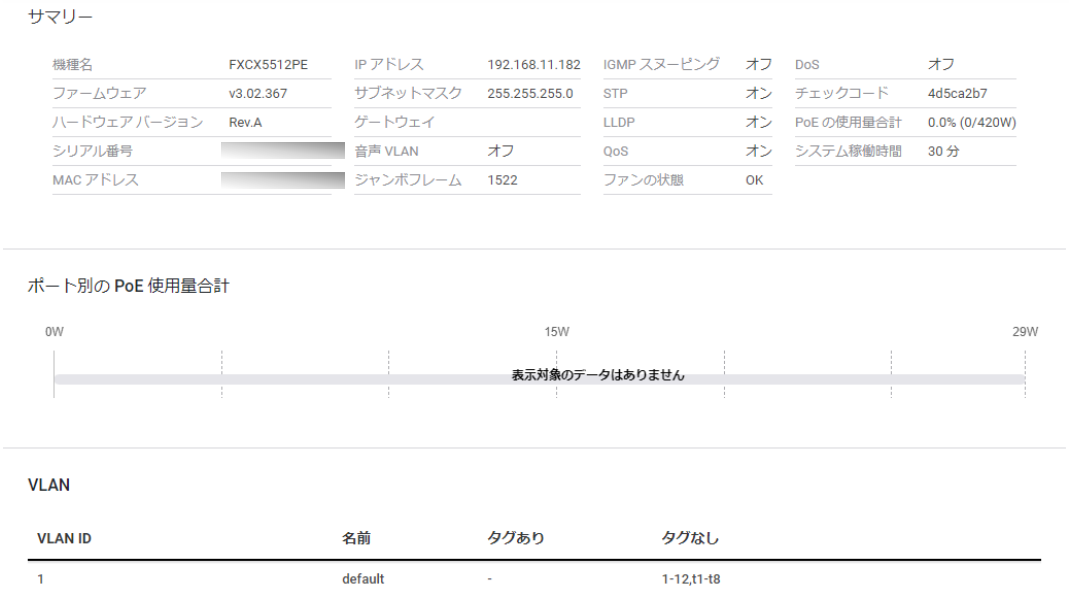
2.2 モニター

このセクションでは、より効率的な方法で本機をモニタリングできるようになり、各特定の機能項目を使用して、PoE使用量の合計、各種システム情報、ポートに関する統計情報など機器のステータスを迅速に把握することができます。

2.2.1 ダッシュボード

各種システム情報やステータス情報を、図表やグラフなどで表示します。
運用管理やトラブルシューティングなど、情報収集を効率よく行いたいときに便利です。

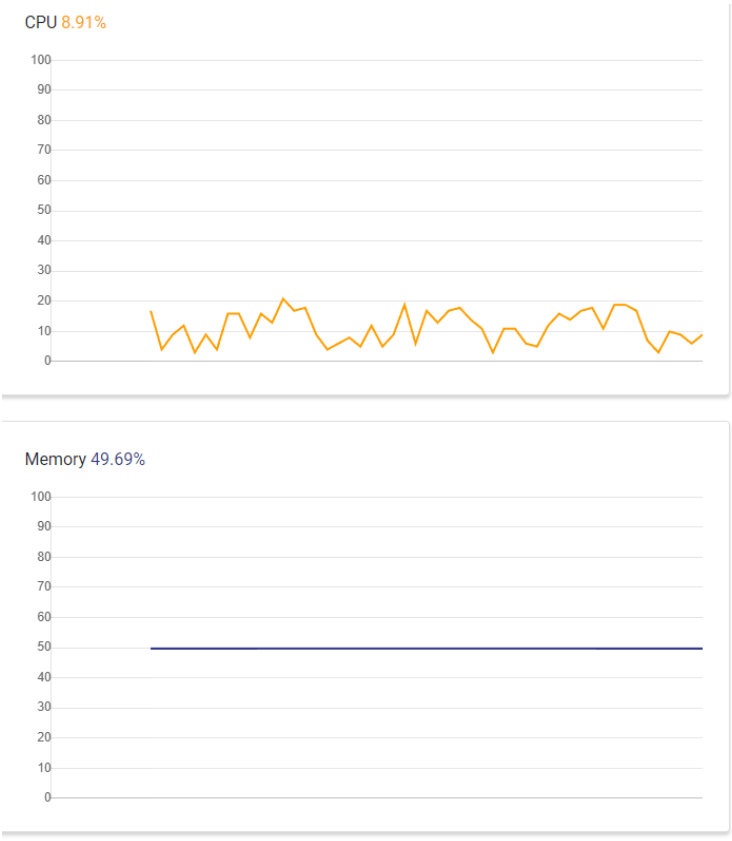
「モニター」→「ダッシュボード」をクリックすると、以下の画面が表示されます。



2.2.2 リアルタイムメーター

現在使用している計算処理を実行するCPUや受信したデータを一時的に格納したり、CPUで計算した結果を保存しておくメモリがグラフで表示されます。

「モニター」→「リアルタイムメーター」をクリックすると、以下の画面が表示されます。



2.2.3 統計情報

ポートに関する統計情報を収集します。それらの情報を使用して、一般的なネットワークエラーや全体的なトラフィックレートをモニタリングすることができます。

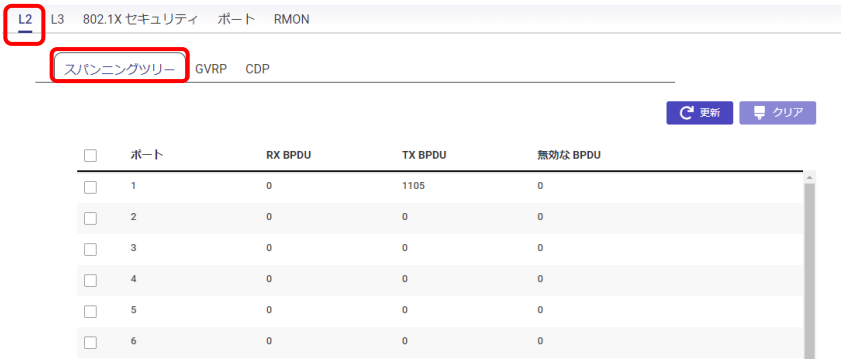
「モニター」→「統計情報」をクリックしてください。

1. L2

1) スパニングツリー

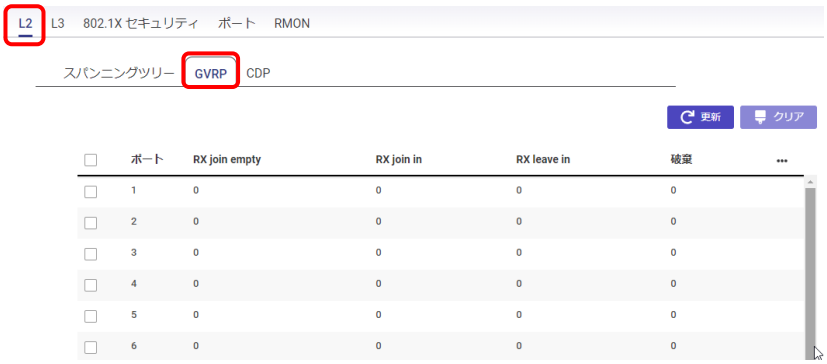
L2ネットワークでのループを防止をするための機能です。スパニングツリーを介してループを防止し、ネットワークを冗長化することにより、耐障害性が向上します。

「モニター」→「統計情報」→「L2」→「スパニングツリー」をクリックすると、以下の画面が表示されます。



2) GVRP

GVRP(Generic VLAN Registration Protocol)を使用してVLAN情報を相互に交換することができます。
「モニター」→「統計情報」→「L2」→「GVRP」をクリックすると、以下の画面が表示されます。



3) CDP

ネットワーク 管理アプリケーションは CDP を使用することにより、ネイバーのデバイ スを検出することができます。この機能によって、アプリケーションからネイバーデバイスに SNMP クエリーを送信可能になります。

「モニター」→「統計情報」→「L2」→「CDP」をクリックすると、以下の画面が表示されます。

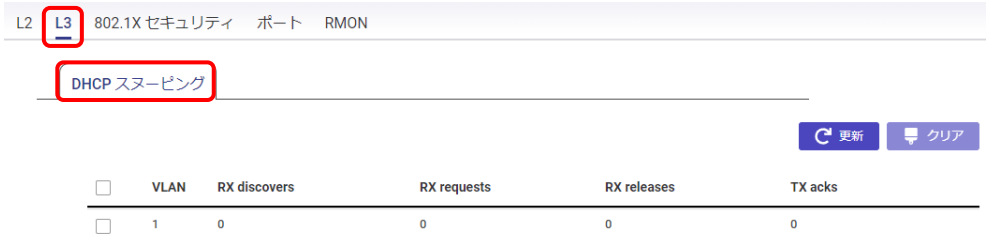
❑最新の情報を表示したい場合は、<更新>ボタンをクリックしてください。

2. L3

1) DHCP スヌーピング

DHCPメッセージのやりとりをモニタリングして、DHCPクライアントの情報に基づいてIPパケットのフィルタリングを行います。

「モニター」→「統計情報」→「L3」→「DHCPスヌーピング」をクリックすると、以下の画面が表示されます。

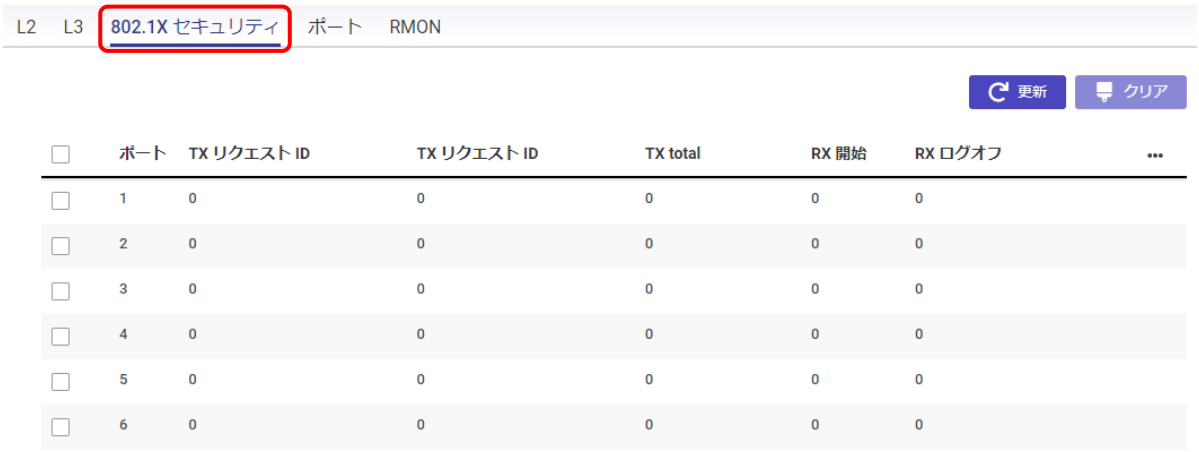


❑最新の情報を表示したい場合は、<更新>ボタンをクリックしてください。

2) 802.1X セキュリティ

ネットワークに接続するコンピュータなどの端末を認証する方法を定めた標準規格の一つであり、不正にネットワークに参加することを防ぐことができます。

「モニター」→「統計情報」→「802.1X セキュリティ」をクリックすると、以下の画面が表示されます。



❑最新の情報を表示したい場合は、<更新>ボタンをクリックしてください。

3) ポート

各ポートの情報をモニタリングすることができます。

「モニター」→「統計情報」→「ポート」をクリックすると、以下の画面が表示されます。

❑画面右側の設定（•••）をクリックすると、以下のようにメニューが表示されるため、表示したい項目を選択してください。

❑最新の情報を表示したい場合は、<更新>ボタンをクリックしてください。

3. RMON

リモートでLANの通信状況をモニタリングすることができます。

指定したイベントに対する詳細情報については、次項の「2.1.4 RMON」の項を参照してください。

「モニター」→「統計情報」→「RMON」をクリックすると、以下の画面が表示されます。

❑<更新>ボタンをクリックして最新の情報を表示するか、ポートの設定をクリアしたい場合は<クリア>ボタンをクリックしてください。

2.2.4 MAC アドレステーブル

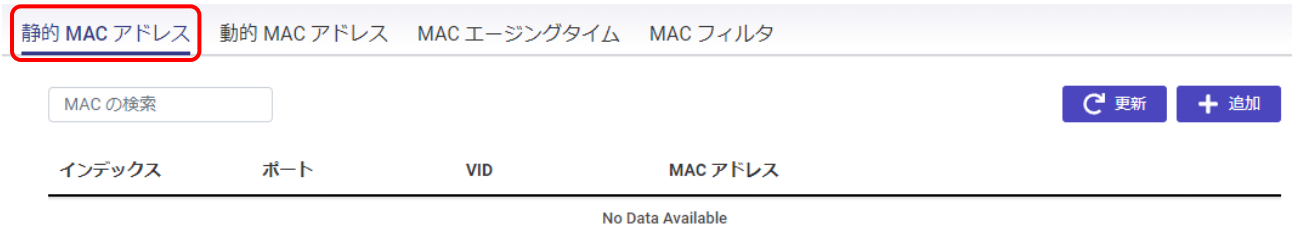
MACアドレス テーブルには、受信ポートと送信ポート間のトラフィックを転送するために使用するアドレス情報が含まれています。アドレス テーブル内のすべての MACアドレスは、1 つ以上のポートに関連付けられています。
ポートがトラフィックを受信すると、イーサネット スイッチング テーブル上で宛先の MACアドレスを検索します。MACアドレスが見つからない場合、トラフィックは VLAN に関連付けられている他のすべてのポートにフラッディングされます。

本機はトラフィックをモニタリングすることによって学習したすべての MACアドレスは、動的アドレスに格納されます

1. 静的 MAC アドレス

静的アドレスを使用する場合は、MACアドレスを手動で入力して、特定のポートと VLAN を設定することができます。

「モニター」→「MACアドレステーブル」→「静的MACアドレス」をクリックすると、以下の画面が表示されます。



メニュー	説明
インデックス	スタティックMACアドレス テーブルのインデックスを表示します。
ポート	前のフィールドに入力した MACアドレスが自動的に転送されるポートを選択します。
VID	IGMPスヌーピングのクエリアが管理上有効になっており、VLAN データベースに VLAN が存在する VLAN ID を入力してください。
MACアドレス	スイッチが転送またはフィルタリング情報を持つユニキャスト MACアドレスを入力してください。

1.設定を追加したい場合は、<追加>ボタンをクリックすると、次の画面が表示されるため、設定を追加してください。

2.設定内容を適用する場合は、<適用>ボタン、キャンセルする場合は、<キャンセル>ボタンをクリックしてください。

2. 動的 MAC アドレス

通信状況に応じて、MACアドレスは自動的に登録されます。

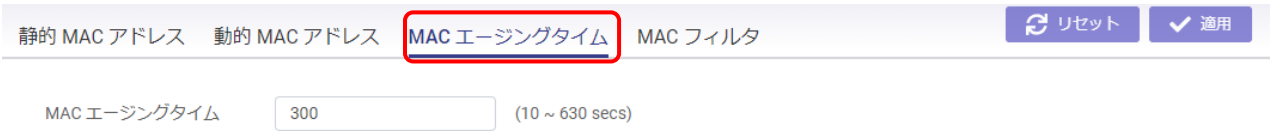
「モニター」→「MACアドレステーブル」→「動的MACアドレス」をクリックすると、以下の画面が表示されます。

❑最新の情報を表示したい場合は、<更新>ボタンをクリックしてください。

3. MAC エージングタイム

MACアドレステーブルに保存されたエントリが自動的に削除されるまでの時間を表示します。

「モニター」→「MACアドレステーブル」→「MACエージングタイム」をクリックすると、以下の画面が表示されます。



❑それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<リセット>ボタンをクリックして変更を破棄してください。

4. MAC フィルタ

特定の MAC アドレスを登録し、他の端末に接続できないようにする機能です。

「モニター」→「MAC アドレステーブル」→「MAC フィルター」をクリックすると、以下の画面が表示されます。

1.MAC フィルターに追加したい場合は、VID および MAC アドレスを追加してください。

2.設定内容を適用する場合は、<適用>ボタン、キャンセルする場合は、<キャンセル>ボタンをクリックしてください。

2.2.5 RMON

RMONを使用すると、リモート側の機器で情報を収集したり、指定したイベントに対して個別にアクションを実行できます。
本製品は、RMON 対応機器であり、さまざまなタスクを個別に実行して、ネットワーク管理トラフィックを大幅に削減することができます。また、診断を継続的に実行し、ネットワークパフォーマンスに関する情報をログに記録することが可能です。イベントのトリガーとなる場合は、障害は自動的にネットワーク管理者に通知され、イベントの履歴情報が提供されます。
本製品は、管理エージェントに接続できない場合には、指定されたタスクを引き続き実行し、次回、接続時にデータを管理ステーションに配信します。

1. 統計情報リスト

「モニター」→「RMON」→「統計情報」をクリックすると、以下の画面が表示されます。

1.エントリを追加したい場合は、メニュー右上の<追加>ボタンをクリックすると、次の画面が表示されます。

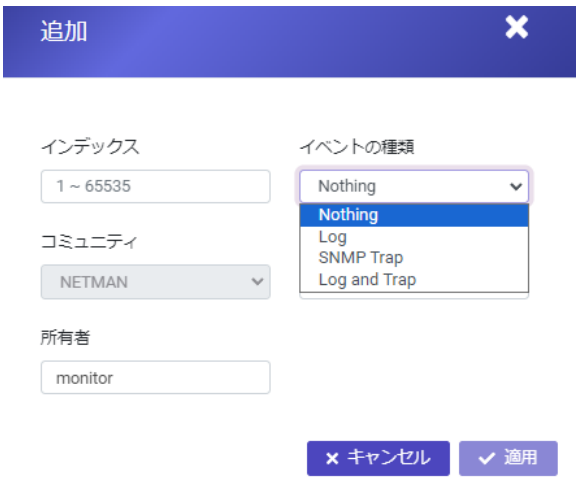
2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容を一括してクリアにすることができます。

2. イベントリスト

RMON アラームの発生した際にログエントリまたは SNMP 通知を生成できます。

「モニター」→「RMON」→「イベントリスト」をクリックすると、以下の画面が表示されます。

1.エントリを追加したい場合は、メニュー右上の<追加>ボタンをクリックすると、次の画面が表示されます。



2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容を一括してクリアにすることができます。

3. イベントログテーブル

RMON イベントテーブルのエントリが表示されます。

「モニター」→「RMON」→「イベントログテーブル」をクリックすると、以下の画面が表示されます。

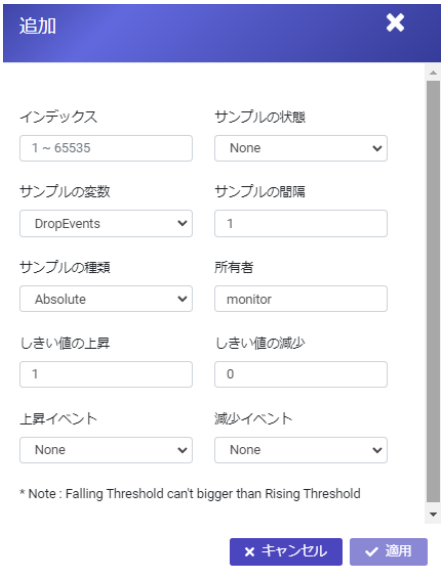
❑最新の情報を表示したい場合は、<更新>ボタンをクリックしてください。

4. アラームリスト

RMONのアラームに関する情報(サンプルの変数、閾値、種類)が表示されます。

「モニター」→「RMON」→「アラームリスト」をクリックすると、以下の画面が表示されます。

1.エントリを追加したい場合は、メニュー右上の<追加>ボタンをクリックすると、次の画面が表示されます。



2.設定内容を適用する場合は、<適用>ボタン、キャンセルする場合は、<キャンセル>ボタンをクリックしてください。

5. 履歴リスト

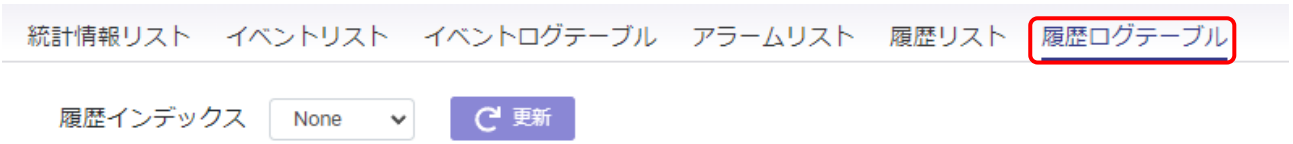
「モニター」→「RMON」→「履歴リスト」をクリックすると、以下の画面が表示されます。

1.エントリを追加したい場合は、メニュー右上の<追加>ボタンをクリックすると、次の画面が表示されます。

2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容を一括してクリアにすることができます。

6. 履歴ログテーブル

「モニター」→「RMON」→「履歴ログテーブル」をクリックすると、以下の画面が表示されます。



❑最新の情報を表示したい場合は、<更新>ボタンをクリックしてください。

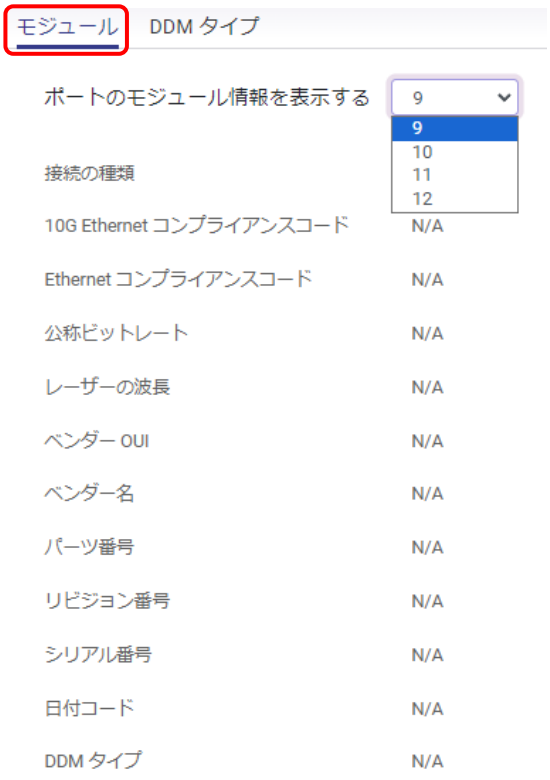
2.2.6 SFP モジュール情報

SFPモジュール(Port 9～12)の各情報を表示します。

1. モジュール

モジュールポート(Port 9 ～12)の接続の種類、その他の情報を表示します。

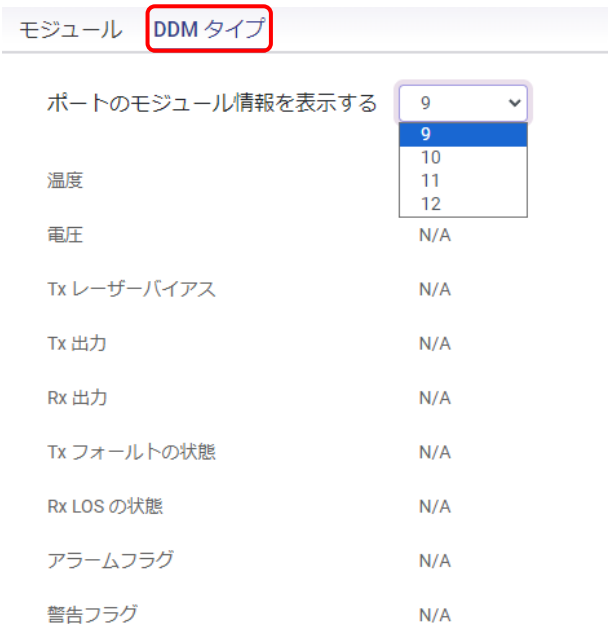
「モニター」→「SFPモジュール情報」→「モジュール」をクリックすると、以下の画面が表示されます。
表示したいポートを選択してください。



2. DDM タイプ

モジュールポート(Port 9 ～12)のパラメータの情報(光出力パワー、光入力パワー、温度、レーザー バイアス電流、および電圧)を表示します。

「モニター」→「SFPモジュール情報」→「DDMタイプ」をクリックすると、以下の画面が表示されます。
表示したいポートを選択してください。



2.3 設定

2.3.1 システム設定

本章では、システム情報、IP 設定、ARP 設定、システム時刻、近隣探索テーブルなど、本機の一般的なシステム情報の概要が表示されます。

この情報は、同じローカルエリアネットワーク内の他の機器の中から特定の機器を識別する際に役立ちます。

本メニューでは、以下の機能を設定することができます。

1. システム情報

本製品の基本情報が表示されます。

「設定」→「システム設定」→「システム情報」をクリックすると、以下の画面が表示されます。

メニュー	説明
システム名	本機のシステム名を設定/表示します。
システムの場所	本機の設置場所を設定/表示します。
システム連絡先	本機の連絡先を設定/表示します。

❑それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<リセット>ボタンをクリックして変更を破棄してください。

2. IP アドレスの設定

「IPアドレスの設定」タブでは、IP アドレスを管理 VLAN に割り当てることができます。

1) IPv4 管理

IP アドレスは、手動で設定するか、DHCP（ダイナミックホストコンフィグレーションプロトコル)を介して自動的に設定することができます。

「設定」→「システム設定」→「IPアドレスの設定」→「IPv4管理」をクリックすると、以下の画面が表示されます。

メニュー	説明
VLAN	本機の管理 VLAN を設定/表示します（デフォルト設定:1）。
アドレス	本機の IPv6 アドレスを表示します。
サブネットマスク	本機の管理 VLAN を設定/表示します。
DNS サーバ 1	DNSサーバ1(ドメイン名とIPアドレスを紐付けし変換する)を表します。
DNS サーバ 2	DNSサーバ2(ドメイン名とIPアドレスを紐付けし変換する)を表します。
設定	本機の IP アドレスの設定(Static/DHCP)を選択します。

❑それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<リセット>ボタンをクリックして変更を破棄してください。

2) IPv6 管理

IPv6アドレスの設定方法（手動、または自動設定）を選択することができます。

「設定」→「システム設定」→「IPアドレスの設定」→「IPv6管理」をクリックすると、以下の画面が表示されます。

メニュー	説明
DHCPv6	DHCPv6のタイプ(Static/Stateless DHCPv6/Stateful DHCPv6)を選択してください(デフォルト設定: static)
ゲートウェイ	本機のゲートウェイのアドレスを表示します。

1.エントリを追加したい場合は、メニュー右上の<追加>ボタンをクリックすると、次の画面が表示されます。

2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容を一括してクリアにすることができます。

3) IPv4 ネットワーク

IPv4 ネットワークの情報が表示されます。

「設定」→「システム設定」→「IPアドレスの設定」→「IPv4ネットワーク」をクリックすると、以下の画面が表示されます。

メニュー	説明
VLAN ID	IPv4 ネットワークの VLAN ID を選択します。
アドレス	追加したネットワークの IP アドレスが表示されます。
サブネットマスク	追加したネットワークのサブネットマスクが表示されます。

1.エントリを追加したい場合は、メニュー右上の追加>ボタンをクリックすると、下記の画面が表示されます。

2.設定内容を適用する場合は、<適用>ボタン、キャンセルする場合は、<キャンセル>ボタンをクリックしてください。

4) IPv6 ネットワーク

IPv6 ネットワークの情報が表示されます。

「設定」→「システム設定」→「IPアドレスの設定」→「IPv6ネットワーク」をクリックすると、以下の画面が表示されます。

1.VLAN ID を追加したい場合は、メニュー右上の<追加>ボタンをクリックすると、次の画面が表示されます。

メニュー	説明
VLAN ID	IPv6 ネットワークの VLAN ID を選択します。
アドレス	IP アドレスを入力してください。
プレフィックスの長さ	追加されたネットワークのプレフィックス長を入力してください。
アドレスタイプ	IPv6アドレスは、3つのタイプ（ユニキャストアドレス、マルチキャストアドレス、エニーキャストアドレス）に分類されます。

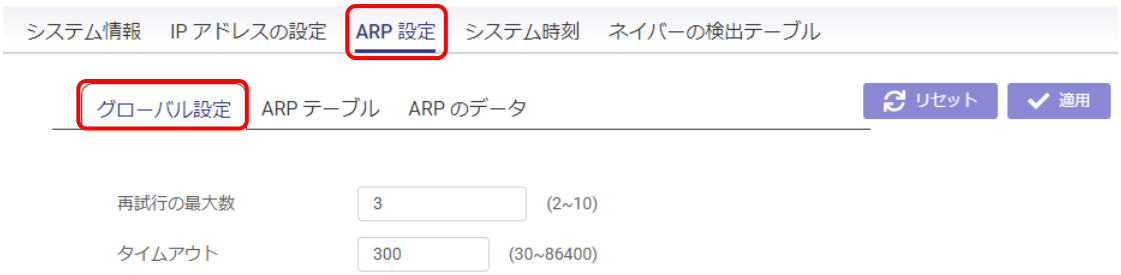
2.設定内容を適用する場合は、<適用>ボタン、キャンセルする場合は、<キャンセル>ボタンをクリックしてください。

3. ARP 設定

統計情報のリストには、ARP統計情報（それぞれの特定のタイプとその合計）が表示されます。

1) グローバル設定

「設定」→「システム設定」→「ARP設定」→「グローバル設定」をクリックすると、以下の画面が表示されます。



メニュー項目	説明
最大再試行回数	ARP リトライの最大回数を設定/表示します。
タイムアウト	ARP タイムアウトの値を設定/表示します。

❑それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<リセット>ボタンをクリックして変更内容を破棄してください。

2) ARP テーブル

ARP（Address Resolution Protocol）によって割り出したIPアドレスとMACアドレス（EthernetやWi-Fiなどの物理アドレス）の対応表です。

「設定」→「システム設定」→「ARP設定」をクリックすると、以下の画面が表示されます。

メニュー	説明
アドレス	検出した機器の IP アドレスを表示します。
MACアドレス	関連する IP アドレスの MACアドレスを表示します。
インタフェース	検出した IP アドレスのインタフェースを表示します。
マッピング	検出した IP アドレスのマッピング方法を表示します。

1.エントリを追加したい場合は、メニュー右上の追加>ボタンをクリックすると、下記の画面が表示され

2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容を一括してクリアにすることができます。

3) ARP のデータ

リストには、それぞれの特定のタイプのシステムの ARP 統計情報が表示されます。

「設定」→「システム設定」→「ARP設定」をクリックすると、以下の画面のとおりARPデータの情報が表示されます。

2) システム時刻

「システム時刻」タブでは、日付と時刻の設定を表示および調整します。
本機は、SNTP(Simple Network Time Protocol)に対応しているため、SNTPサーバによって正確なネットワーク機器 クロック時刻に同期することができます。
本機は 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。

「設定」→「システム設定」→「システム時刻」をクリックすると、以下の画面が表示されます。

メニュー	説明
現在の時刻	現在のシステム時刻を表示します。
SNTP	SNTPサーバとのシステム時刻同期を有効/無効を選択します。
タイムゾーン	GMT 差を設定するか、国別にタイムゾーン設定を設定します。
サマータイム	「無効」、「繰り返し」、または「繰り返しなし」から選択します。
サマータイムオフセット	サマータイム オフセットの時刻を入力してください。
繰り返しの開始	リストから開始する日、週、月、および時間を選択します。
繰り返しの終了	リストから終了する日、週、月、および時間を選択します。
SNTP/NTPサーバアドレス	SNTP/NTPサーバの IP アドレスまたはホスト名を入力してください。
サーバポート	SNTP/NTPサーバの サーバポートを入力してください。

❑SNTPを介して、日付/時刻を設定するには、以下の手順に従ってください。

1. 「SNTP」 フィールドを 「オンにする」 を選択します。

2. 「タイム ゾーン オフセット」 リストで、本機が配置されている「国別で設定」または「時間で設定」を選択します。
3. 次に、サマータイムの 「オフに設定」、「繰り返す」のいずれかを選択します。
サマータイムは春の終わりから初秋にかけての期間で、各国に応じて、時計を 1 時間進めたり遅らせたりして調整します。
4. 「SNTP/NTP サーバ アドレス」 フィールドに、SNTP/NTP サーバの IP アドレスまたはホスト名を入力してください。
5. 最後に、SNTP 要求が送信される SNTP サーバのポート番号を入力してください（有効な範囲：1 ～ 65535、デフォルト：123）。
6. <適用>ボタンをクリックして、システムの設定を確定してください。

❑SNTPを介さずに、日付/時刻を手動で設定するには、以下の手順に従ってください。

1. 「SNTP」フィールドを「オフにする」を選択します。
2. 「手動での時刻」フィールドで、ドロップダウン ボックスを使用して、設定する日付と時刻を手動で選択します。
3. 「タイム ゾーン オフセット」 リストで、本機が配置されている「国別で設定」または「時間で設定」を選択します。
4. 次に、サマータイムの 「オフに設定」、「繰り返す」のいずれかを選択します。
サマータイムは春の終わりから初秋にかけての期間で、各国に応じて、時計を 1 時間進めたり遅らせたりして調整します。
5. <適用>ボタンをクリックして、システムの設定を確定してください。

3) ネイバーの検出テーブル

このリストは、本機が NDP (ネイバー探索プロトコル) を使用してネイバーホストのレイヤー2 MACアドレスを決定する IPv6ネイバーが表示されます。

「設定」→「システム設定」→「ネイバーの検出ケーブル」をクリックすると、以下の画面が表示されます。

1.エントリを追加したい場合は、メニュー右上の<追加>ボタンをクリックすると、次の画面が表示されます。

2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容を一括してクリアにすることができます。

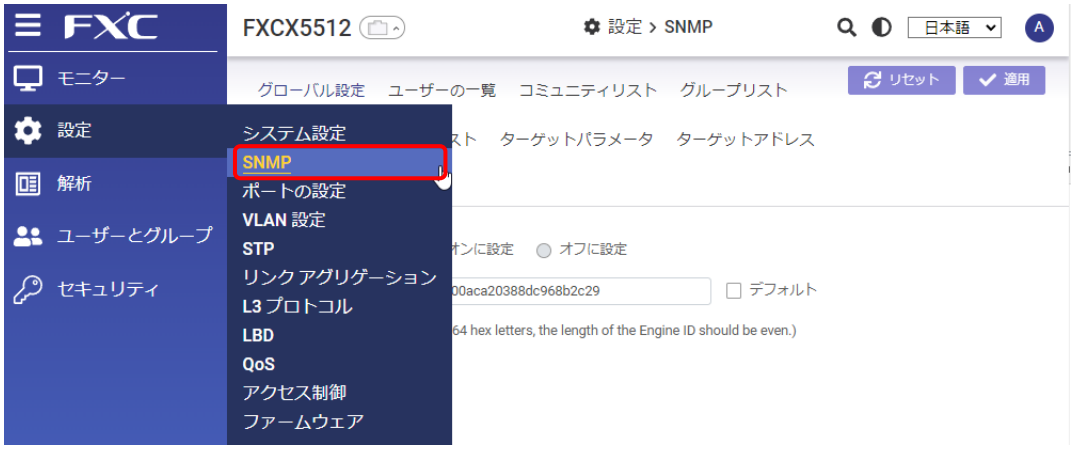
2.3.2 SNMP

SNMP(Simple Network Management Protocol) は、ネットワーク機器の管理とモニタリング専用に設計されたアプリケーション層プロトコルです。SNMPは、ネットワーク管理用の一般的なプロトコルです。インターネット プロトコル (IP) ネットワーク上の サーバ、プリンター、ハブ、スイッチ、ルータなどのネットワーク機器から情報を収集し、設定するために使用されます。
また、ネットワーク管理システム (NMS)とネットワーク機器の間で管理情報を交換するために使用されます。マネージャステーションは、SNMPv1、v2c、および v3 を介してネットワーク経由で本機を管理およびモニタリングできます。
SNMP 管理ネットワークは、エージェントとマネージャの 2 つのコンポーネントで設定されます。
エージェントは、管理対象の機器からのローカル管理情報を SNMP と互換性のある形式に変換します。SNMP を使用すると、管理情報ベース (MIB) にアクセスするために、マネージャとエージェントを相互に通信できます。SNMP は、利用可能な情報が MIB によって定義される拡張可能な設計を使用します。
MIB は、サブシステムの管理データの構造を記述します。オブジェクト識別子 (OID) を含む階層的な名前空間を使用します。各 OID は、SNMP を介して読み取りまたは設定できる変数を識別します。
マネージャは、ネットワーク管理者がネットワーク管理機能を実行するためのコンソールです。
SNMP では、いくつかのバージョン（v1、v2c、および v3）がサポートされています。

また、SNMPは、SNMP 対応機器間の通信方法を定義し、SNMP メッセージ タイプを指定する標準です。バージョン 1 は、シンプルで最も基本的なバージョンです。古いハードウェアのサポートが必要になる場合があります。SNMPv2c は、RFC 1901「Introduction to Community-Based SNMPv2」、RFC 1905「Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)」、および RFC 1906「Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)」。SNMPv2c は、コミュニティ名に基づく GetBulk 要求と認証を導入することにより、プロトコル操作を更新します。バージョン 2c では、「Informs」のサポートなど、プロトコルにいくつかの拡張機能が追加されています。このため、v2c が最も広く使用されているバージョンになりました。残念ながら、v1 と v2c の主な弱点はセキュリティです。
SNMPv3 では、ユーザベースのセキュリティ モデル (USM) 認証が暗号化と共に実装され、安全な SNMP 環境を設定できます。SNMPv3 プロトコルは、SNMPv1 および SNMPv2c とは異なる用語も使用します。SNMPv1 および SNMPv2c プロトコルでは、エージェントおよびマネージャという用語を用います。SNMPv3 プロトコルでは、エージェントとマネージャはエンティティに名前が変更されます。SNMPv3 プロトコルを使用して、ユーザを設定、メッセージ認証に使用するプロトコルと、2 つの SNMP エンティティ間で送信されるデータを暗号化するかどうかを決定します。
SNMPv3 プロトコルは、HMAC-MD5-96 (MD5) と HMAC-SHA-96 (SHA) の 2 つの認証プロトコルをサポートしています。MD5 と SHA はどちらもアルゴリズムを使用してメッセージ ダイジェストを生成します。各認証プロトコルは、メッセージ ダイジェストをチェックしてユーザを認証します。さらに、どちらのプロトコルもキーを使用して認証を実行します。両方のプロトコルのキーは、エンジン ID とユーザ パスワードを使用してローカルで生成され、セキュリティをさらに強化します。
SNMPv1 および SNMPv2c では、ユーザ認証は“コミュニティ ストリング”を用いて実行されます。
コミュニティ ストリングは、マネージャからエージェントへアクセスする際にパスワードのように使う文字列として使用されます。

ユーザは、リモート SNMP マネージャがアクセスできる MIB オブジェクトを指定するコミュニティ ストリングにビューを割り当てることができます。
本機の SNMPv1 および SNMPv2c 管理アクセスに使用される本機のデフォルト コミュニティ ストリングには、許可された管理ステーションが MIB オブジェクトを取得できるようにする「パブリック」と、許可された管理ステーションが MIB オブジェクトを取得および変更できるようにする「プライベート」があります。

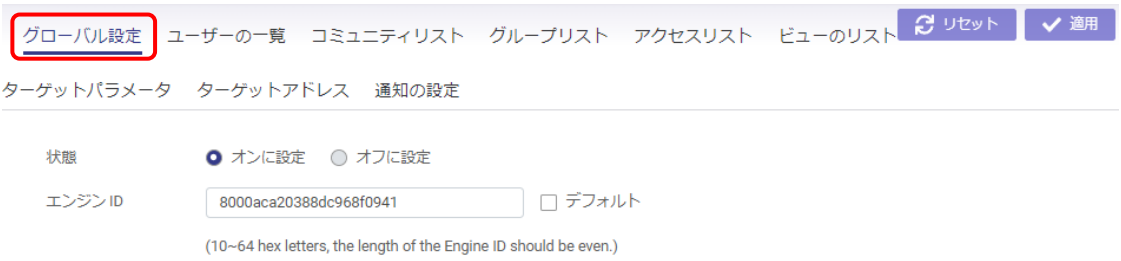
「設定」→「SNMP」をクリックすると、以下の画面が表示されます。



1. グローバル設定

SNMPは、ネットワーク機器の管理とモニタリング専用に設計された アプリケーション層プロトコルです。
SNMP エージェントは、本機の管理に使用される変数のリストを維持します。
変数はMIBで定義され、SNMP エージェントによって制御される情報を表示します。

「設定」→「SNMP」→「グローバル設定」をクリックすると、以下の画面が表示されます。



❑それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<リセット>ボタンをクリックして変更内容を破棄してください。

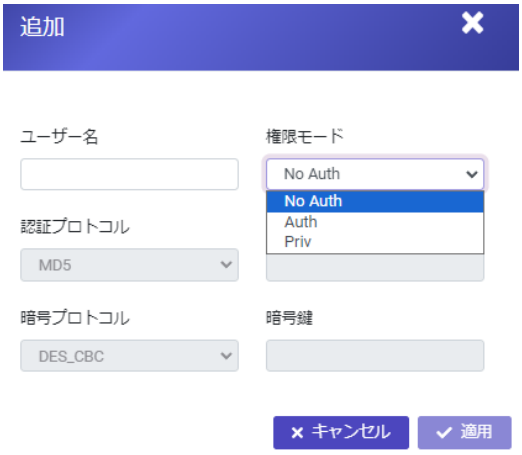
2. ユーザーの一覧

ユーザの特権情報、認証/暗号化プロトコルが表示されます。

「設定」→「SNMP」→「ユーザーの一覧」をクリックすると、以下の画面が表示されます。

メニュー	説明
ユーザ名	SNMP ユーザ名を表示します。
特権モード	ユーザの対応する特権モードを表示します。
認証プロトコル	ユーザが使用する対応する認証プロトコルを表示します。
暗号化プロトコル	ユーザが使用する対応する暗号化プロトコルを表示します。

1.<追加>ボタンをクリックして、ユーザを追加してください。



2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容を一括してクリアにすることができます。

3. コミュニティリスト

「設定」→「SNMP」→「コミュニティリスト」をクリックすると、以下の画面が表示されます。

メニュー	説明
コミュニティ名	SNMPで管理対象の機器のグループを表す名前を表示します。
セキュリティ名	コミュニティに対応するセキュリティメソッド/名前を表示します。
トランスポートタグ	コミュニティに対応するトランスポートタグを表示します。

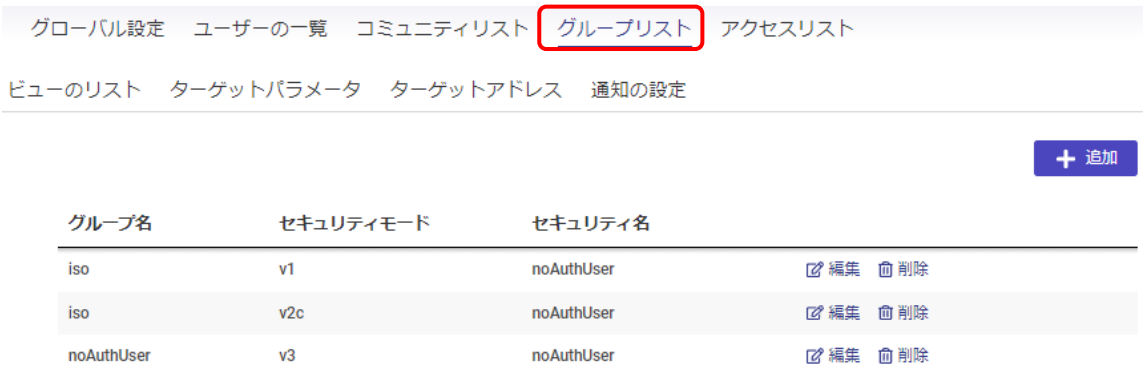
1.エントリを追加/編集したい場合は、画面右上の<追加>ボタンをクリックするか、メニューの横にある<編集>ボタンをクリックすると、次の画面が表示されます。

2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容を一括してクリアにすることができます。

4. グループリスト

各 SNMP グループは、グループ名とセキュリティモードの組み合わせによって一意に識別されます。

「設定」→「SNMP」→「グループリスト」をクリックすると、以下の画面が表示されます。



メニュー	説明
グループ名	SNMP グループ名を表示します。
セキュリティモード	グループに対応するセキュリティ モードを表示します。
セキュリティ名	グループに対応するセキュリティ メソッド/名前を表示します。

1.エントリを追加/編集したい場合は、画面右上の<追加>ボタンをクリックするか、メニューの横にある<編集>ボタンをクリックすると、次の画面が表示されます。

2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容を一括してクリアにすることができます。

5. アクセスリスト

SNMPのセキュリティモードごとに、SNMPビュー（読み取り用ビュー、書き込み用ビュー、および通知用ビュー）を設定できます。SNMPv3の場合は、認証および暗号化の要否を設定できます

「設定」→「SNMP」→「アクセスリスト」をクリックすると、以下の画面が表示されます。

メニュー	説明
グループ名	SNMP グループ名を表示します。
セキュリティモード	グループに対応するセキュリティ モードを表示します。
特権モード	グループに対応する特権モードを表示します。
読み取りビュー	読み取りビューの許可モードを表示します。
書き込みビュー	書き込みビューの許可モードを表示します。
通知ビュー	通知ビューの許可モードを表示します。

1.エントリを追加/編集したい場合は、画面右上の<追加>ボタンをクリックするか、メニューの横にある<編集>ボタンをクリックすると、次の画面が表示されます。

2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容をクリアにします。

6. ビューのリスト

ビュー名ごとに、サブツリー OID/マスク、ビューの種類を選択することができます。

「設定」→「SNMP」→「ビューのリスト」をクリックすると、以下の画面が表示されます。

メニュー	説明
ビュー名	SNMP ビュー名を表示します。
サブツリー OID	対応するサブツリー OID を表示します。
サブツリー マスク	対応するサブツリー マスクを表示します。
ビューの種類	含まれる/除外される対応するビュー タイプを表示します。

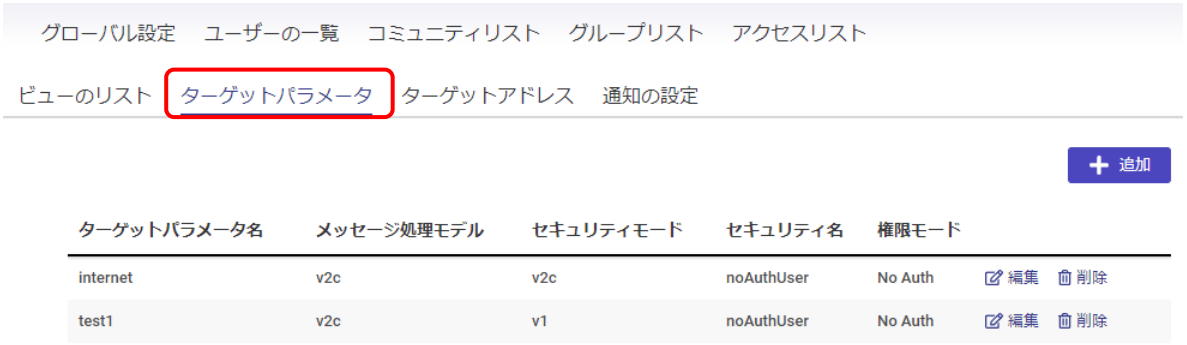
1.エントリを追加/編集したい場合は、画面右上の<追加>ボタンをクリックするか、メニューの横にある<編集>ボタンをクリックすると、次の画面が表示されます。

【注記】:一部の OID を除外したい場合は、ペアレントノードに含まれるルールを設定する必要があります。

2.設定内容を適用する場合は、<適用>ボタン、キャンセルする場合は、<キャンセル>ボタンをクリックしてください。

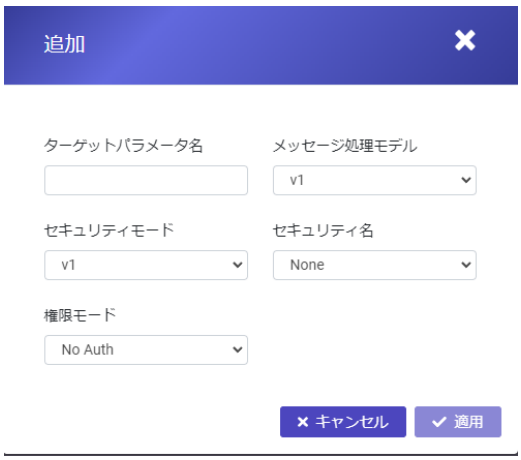
7. 宛先パラメータ

特定の宛先に通知を送信するときに使用するセキュリティパラメータの情報を設定します。
デフォルトでは、SNMP エンジン ID は企業番号と個々の機器情報で設定されます。



メニュー	説明
宛先パラメータ名	対象パラメータ名を表示します。
メッセージ処理モデル	対応するメッセージ処理モデル(v1、v2c、または v3)を表示します。
セキュリティモード	対応するセキュリティ モード (v1、v2c、または v3) を表示します。
セキュリティ名	対応するセキュリティ名を表示します。
特権モード	対応する特権モードを表示します。

1.エントリを追加/編集したい場合は、画面右上の<追加>ボタンをクリックするか、メニューの横にある<編集>ボタンをクリックすると、次の画面が表示されます。

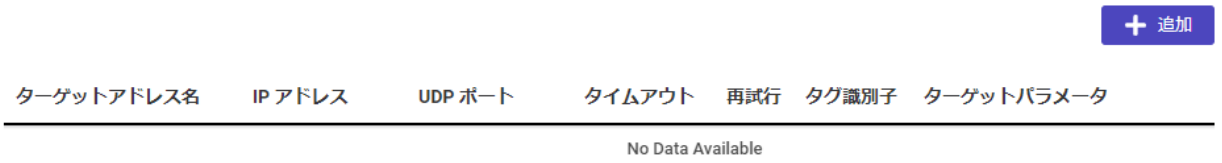


2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容を一括してクリアにすることができます。

8. 宛先アドレス

宛先ホストの IP アドレスの情報を表示します。

「設定」→「SNMP」→「宛先アドレス」をクリックすると、以下の画面が表示されます。



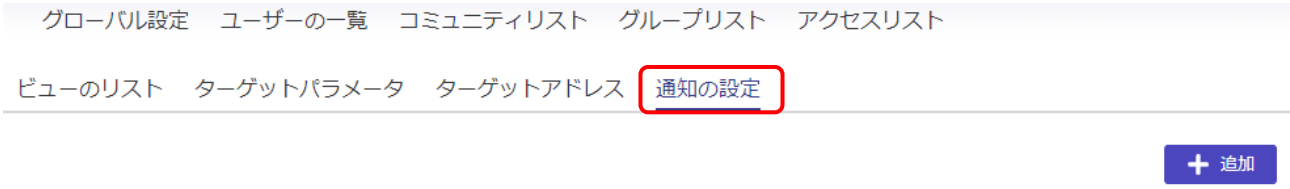
メニュー	説明
宛先アドレス名	宛先アドレス名を表示します。
IPアドレス	対応する IP アドレスを表示します。
UDP ポート	対応する UDP ポートを表示します。
タイムアウト	対応するタイムアウト値を表示します。
リトライ	対応する再試行回数を表示します。
タグ識別子	対応するタグ識別子を表示します。
宛先パラメータ	対応する宛先パラメータを表示します。

1.エントリを追加したい場合は、メニュー右上の<追加>ボタンをクリックすると、次の画面が表示されます。

2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容をクリアにします。

9. 通知の設定

「設定」→「SNMP」→「通知の設定」をクリックすると、以下の画面が表示されます。



メニュー	説明
名前	対応する通知名を表示します。
タグ識別子	対応するタグ識別子を表示します。
種類	対応する通知タイプ (Trap、またはInformation) を表示します。

1.エントリを追加したい場合は、メニュー右上の<追加>ボタンをクリックすると、次の画面が表示されます。

2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容を一括してクリアにすることができます。

1) 通知の設定

「設定」→「SNMP」→「通知の設定」をクリックすると、以下の画面が表示されます。

メニュー	説明
通知名	対応する通知名を表示します。
タグ識別子	対応するタグ識別子を表示します。 タグは、通知を受信する宛先アドレスのセットを定義するために使用されます。
通知タイプ	対応する通知タイプ (Trap、またはInformation) を表示します

1.エントリを追加したい場合は、メニュー右上の<追加>ボタンをクリックすると、次の画面が表示されます。

2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容を一括してクリアにすることができます。

2.3.3 ポートの設定

本機の各ポートの設定情報(ポートミラーリング、ジャンボフレーム、LLDP、CDP、マルチキャストフィルタリング)を表示および設定します。

1. ポート

「ポート設定」メニューでは、本機のポートの設定を変更して、速度とフロー制御を最適なバランスに設定することができます。

「設定」→「ポートの設定」→「ポート」をクリックすると、以下の画面が表示されます。

メニュー	説明
ポート	ポート番号を表示します。
リンク ステータス	リンクのアップ/ダウンを表します。
モード	このポートのイーサネット接続の速度とデュプレックス モードを選択します。 Auto (オートネゴシエーション) を選択すると、1 つのポートがピア ポートと自動的にネゴシエートし、両端がサポートする接続速度とデュプレックス モードを取得できます。 ・オートネゴシエーションがオンになっている場合、本機のポートはピアと自動的にネゴシエーションを行い、接続速度とデュプレックス モードを決定します。ピア ポートがオートネゴシエーションをサポートしていないか、この機能をオフにしている場合、本機はケーブル上の信号を検出し、半二重モードを使用して接続速度を決定します。 ・オートネゴシエーションがオフになっている場合、ポートは接続時に事前設定された速度とデュプレックス モードを使用するため、接続するにはピア ポートの設定が同じであることを確認してください。
フロー制御	ポートにトラフィックが集中すると、ポートの帯域幅が減少し、バッファ メモリがオーバーフローして、パケットの破棄やフレームの損失が発生します。 フロー制御は、受信ポートの帯域幅に合わせて信号の送信を調整するために使用されます。 本機は、全二重モードで IEEE 802.3x フロー制御を使用し、半二重モードでバックプレッシャ フロー制御を使用します。 ・IEEE 802.3x フロー制御は、全二重モードで使用され、一時停止信号を送信ポートに送信します。これにより、受信ポートのメモリ バッファがいっぱいになると、信号の送信が一時的に停止します。 ・バック プレッシャーフロー制御は、通常半二重モードで使用され、送信ポートに「衝突」信号を送信し (パケット衝突の状態を模倣)、送信ポートが信号の送信を一時的に停止後再送信します。

1.<更新>ボタンをクリックして最新の情報を表示するか、ポートの設定を変更したい場合は<編集>ボタンをクリックすると、以下の画面が表示されます。

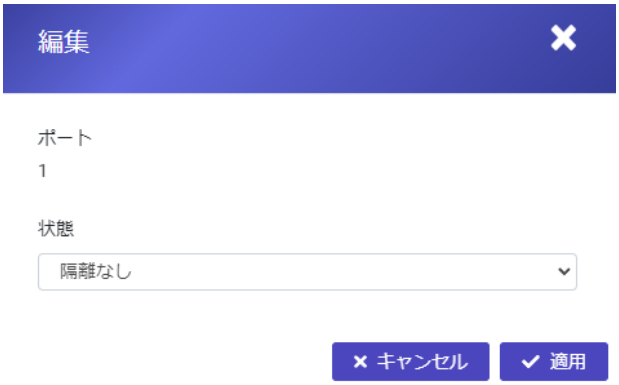
2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容をクリアにします。

2. ポートの隔離

ポートの隔離機能は、同じブロードキャストドメイン内のポート間の L2 分離を行うことができます。この機能を有効にすると、分離ポートは非分離ポートにトラフィックを転送できますが、他の分離ポートには転送できません。
分離されていないポートは、分離の有無に関係なく、任意のポートにトラフィックを送信できます。
デフォルト設定では、分離されていません。

「設定」→「ポートの設定」→「ポートの隔離」をクリックすると、以下の画面が表示されます。

1.ポートの設定を変更したい場合は、該当ポートを選択し、<編集>ボタンをクリックすると、下記の画面が表示されます。



2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容をクリアにします。

3. ポートミラーリング

ミラー設定は、特定のポートからモニタリング ポートに着信および発信パケットのコピーを転送することにより、ネットワーク トラフィックをミラーリングします。モニタリングポートにコピーされるパケットは、元のパケットと同じ形式になります。
ポート ミラーリングは、ネットワークのモニタリングに役立ち、診断ツールとして使用できます。ポート ミラーリングを使用して、コンプライアンスのモニタリング、侵入の検出、トラフィック パターンのモニタリングと予測、その他の相関イベントなどの目的でトラフィックを分析するアプリケーションにトラフィックを送信します。通常、本機は接続先の機器のポートにのみパケットを送信するため、本機のトラフィック分析にはポート ミラーリングが必要です。アナライザーは、元のポートのクライアントに影響を与えることなく、データをキャプチャして評価します。ポート ミラーリングは、アクティブなときに大量のCPU リソースの消費を要する可能性があるため注意が必要です。

「設定」→「ポートの設定」→「ポートミラーリング」をクリックすると、以下の画面が表示されます。

メニュー	説明
セッションID	ミラーセッションを識別する番号。本機は、最大 4 つのミラーセッションのみをサポートします。
宛先ポート	このポートにミラーリングされた送信元ポートから、トラフィック用のポートを選択します。
出力/入力	トラフィックがミラーリングされる送信元ポートを設定します。 ・TX ポート: このポートから送信されたフレームのみが宛先ポートにミラーリングされます。 ・RX ポート: このポートで受信したフレームのみが宛先ポートにミラーリングされます。 ・Both: このポートで送受信されるフレームは、出力と入力にそれぞれポート番号が記載されます。
出力と入力	入力トラフィックの転送を有効/無効を選択します。
セッションの状態	ポート ミラーリングを有効/無効を選択します。

1.設定内容を編集したい場合は、該当のセッション ID の<編集>ボタンをクリックすると、以下の画面が表示されます。

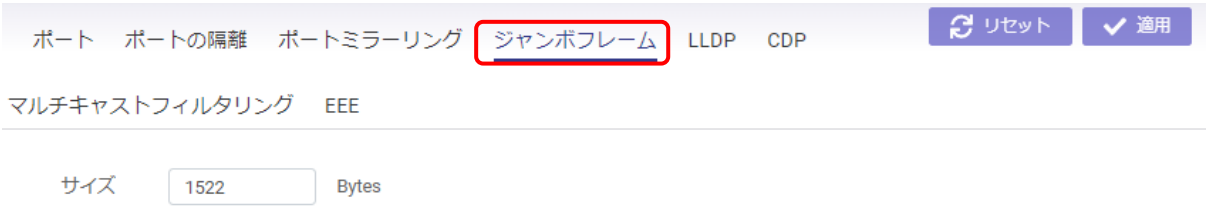
2.設定をクリアしたい場合は<リセット>ボタンをクリックするか、<適用>ボタンをクリックして、システム設定を確定してください。

4. ジャンボフレーム

イーサネット標準の最大フレームサイズ、1,518 byteを超えるフレームサイズのことを“ジャンボフレーム”と呼びます。ジャンボフレームを有効にすると、一度に転送するデータサイズが大きくなり、その回数も少なくなるため、データ転送速度（スループット）を向上することができます。
ジャンボフレームにより、高速、かつ大量のデータ転送に伴う負荷を軽減し、スループットが向上します。

本機は、最大 10,240 byteのジャンボ フレーム サイズをサポートします。ジャンボ フレームは、エンドツー エンドの伝送パスに応じて各機器の入力ポートと出力ポートで動作するように設定する必要があります。

「設定」→「ポートの設定」→「ジャンボフレーム」をクリックすると、以下の画面が表示されます。



メニュー	説明
ジャンボフレーム	ジャンボフレームのサイズを入力してください(有効範囲：1522 ～ 10,240 byte)。

❑ジャンボフレームのサイズの設定後、<適用>ボタンをクリックして変更内容を確定するか、<リセット>ボタンをクリックして変更内容を一括してクリアにすることができます。

1) ローカル デバイス

LLDP 機器は、システム名、システム ID、システムの説明、およびシステム機能のアドバタイズだけでなく、シャーシとポート ID のアドバタイズも同様にサポートします。
ここでは、本機のローカル側のLLDP の詳細情報を表示します。

「設定」→「ポートの設定」→「LLDP」→「ローカルデバイス」をクリックすると、以下の画面が表示されます。

メニュー	説明
シャーシ IDの サブタイプ	シャーシ IDのサブタイプを表示します。
シャーシ ID	LLDP フレームの送信先の機器のシャーシ ID を表示します。
システム名	管理上割り当てられた機器名を表示します。
システムの説明	機器について説明します。
サポートされる機能	機器の機能について説明します。
有効機能	機器の機能について説明します。
ポート ID サブタイプ	ポート ID タイプを表示します。

❑最新の情報を表示したい場合は、<更新>ボタンをクリックしてください。

2) リモートデバイス

LLDP 機器は、システム名、システム ID、システムの説明、およびシステム機能のアドバタイズだけでなく、シャーシとポート ID のアドバタイズも同様にサポートします。
ここでは、リモート側のLLDPの詳細情報を表示できます。

「設定」→「ポートの設定」→「LLDP」→「リモートデバイス」をクリックすると、以下の画面が表示されます。

❑画面右側の設定(•••)をクリックすると、以下のようにメニューが表示されるため、表示したい項目を選択してください。

❑最新の情報を表示したい場合は、<更新>ボタンをクリックしてください。

5. LLDP

LLDP (Link Layer Discovery Protocol)を介したルートブリッジやルータなどのイーサネットネットワーク機器は、ネットワーク上で隣接する機器(ネイバー)との間で関連の情報を送受信し、ネイバー情報について学習したデータを保存できます。

LLDP は、“LLDPDU”(LLDP データ ユニット)と呼ばれるパケットとして情報を送信します。1 つの 802.3 イーサネットフレーム内で LLDPDUは 1 つのみ送信されます。
基本的な LLDPDU は、一連の TLV(Type-Length-Value) 要素で設定され、それぞれの機器に関する情報が含まれています。1 つの LLDPDU には複数の TLV が含まれます。
TLV は、複雑なデータを通信する短い情報要素であり、各 TLV は、1 タイプの情報をアドバタイズします。

「設定」→「ポートの設定」→「LLDP」をクリックすると、以下の画面が表示されます。

❑各項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<リセット>ボタンをクリックして変更内容を一括してクリアにすることができます。

メニュー	説明
状態	「オンに設定」または「オフに設定」を選択して、本機の LLDP を有効にします。
転送間隔	LLDP アドバタイズメントの更新が送信される間隔を入力してください(デフォルト値:30、有効範囲: 5 ～ 32768)。
ホールドタイムの乗数	LLDP パケットが破棄される前に保持される時間を入力し、Advertised Interval の倍数で測定します(デフォルト値:4、有効範囲:2 ～ 10)。
再初期化の遅延	LLDP を再初期化するまでの遅延時間を入力してください(デフォルト値:2、有効範囲: 1 ～ 10)。
転送遅延	連続する LLDP フレーム送信の間に経過する時間を入力してください(デフォルト値: 2 秒、有効範囲:1 ～ 8181 秒)。

1) グローバル設定

LLDP 機能をグローバルで有効/無効にします。
転送間隔、ホールドタイムの乗数、再初期化の遅延、転送遅延の値を設定することができます。

「設定」→「ポートの設定」→「LLDP」→「グローバル設定」をクリックすると、以下の画面が表示されます。

❑各項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<リセット>ボタンをクリックして変更内容を一括してクリアにすることができます。

6. CDP

1) グローバル設定

「設定」→「ポートの設定」→「CDP」→「グローバル設定」をクリックすると、以下の画面が表示されます。

❑各項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<リセット>ボタンをクリックして変更内容を一括してクリアにすることができます。

2) ポート

CDPのポート情報が表示されます。

「設定」→「ポートの設定」→「CDP」→「ポート」をクリックすると、以下の画面が表示されます。

1.最新の情報を表示したい場合は、<更新>ボタンをクリックしてください。

2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容をクリアにします。

3) ローカルデバイス

CDPのローカルデバイスのポート情報を表示します。

「設定」→「ポートの設定」→「CDP」→「ローカルデバイス」をクリックすると、以下の画面が表示されます。

❑最新の情報を表示したい場合は、<更新>ボタンをクリックしてください。

4) リモート側の機器

CDP のリモートデバイスのポート情報を表示します。

❑最新の情報を表示したい場合は、<更新>ボタンをクリックしてください。

7. マルチキャストフィルタリング

マルチキャストフィルタリングの「有効」または「無効」を設定します。
「設定」→「ポートの設定」→「マルチキャストフィルタリング」をクリックすると、以下の画面が表示されます。

❑それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<リセット>ボタンをクリックして変更を破棄してください。

8. EEE

IEEE802.3azで標準化されたイーサネット用の省電力技術であり、無通信時に装置の一部の通電を停止して消費電力を低減します。
イーサネットリンクがデータ伝送中にのみ使用する電力を利用することができます。
LPI(ローワー パワー アイドル) は、イーサネットを使用する推奨時間帯に省電力を実現する方法です。

「設定」→「ポートの設定」→「EEE」をクリックすると、以下の画面が表示されます。

1.ポートの設定を変更したい場合は、該当ポートを選択し、<編集>ボタンをクリックすると、下記の画面が表示されるためそれぞれ設定を行ってください。

2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容を一括してクリアにすることができます。

2.3.4 電源

1. PoE

PoE 管理画面には、現在の電力使用量をモニタリングするためのシステム PoE 情報が含まれており、スイッチがすべての PoE ポートに供給可能な電力の合計量を割り当てます。

「設定」→「電源」をクリックすると、以下の画面が表示されます。

メニュー	説明
パワーバジェット	スイッチがすべてのポートに供給可能な電力量を入力してください。
消費電力	現在すべての PoE ポートに供給されている電力の合計量 (ワット単位) を表示します。

2) パワーバジェット

「設定」→「電源」→「パワーバジェット」をクリックすると、以下の画面が表示されます。

❑それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<リセット>ボタンをクリックして変更を破棄してください。

2. PoE ポート設定

ポートごとにPoE情報を表示します。

「設定」→「電源」→「PoE ポート設定」をクリックすると、以下の画面が表示されます。

❑画面右側の設定(•••)をクリックすると、以下のようにメニューが表示されるため、表示したい項目を選択してください。

メニュー	説明
ポート	PoEのパラメータが設定されている特定のポートを表示します。PoE パラメータは、選択したポートに接続されている受電装置に割り当てられます。
状態	トランクグループのアクティブな参加メンバーを表示します。有効化: デバイス検出プロトコルを有効にし、PoE モジュールを使用してデバイスに電力を供給します。 Device Discovery プロトコルにより、デバイスは、デバイス インタフェースに接続された受電デバイスを検出し、それらの分類を学習できます。 無効: デバイス検出プロトコルを無効にし、PoE モジュールを使用してデバイスに電力を供給する電源を停止します。
優先度	電力供給が少ない場合は、ポートの優先度を選択します。フィールドのデフォルトは低です。たとえば、電源装置が 99% の使用率で動作していて、ポート 1 の優先度が高く、ポート 6 の優先度が低い場合、ポート 1 は優先的に電力を受け取り、ポート 6 は電力が拒否される可能性があります。 ・低: PoE 優先レベルを低に設定します。 ・中: PoE 優先レベルを中に設定します。 ・高: PoE 優先レベルを高に設定します。 ・重要: PoE 優先レベルをクリティカルに設定します。
パワーリミットの種類	受電装置の分類を表示します。このクラスは、受電デバイスに提供可能な最大電力を設定します。
ユーザパワーリミット (W)	このオプションを選択して、「ユーザ電力制限」フィールドで設定された値に電力制限を設定します。ポートが供給可能な最大電力量を設定します。 【注記】: ユーザ電力制限は、クラス値がユーザにより設定されている場合にのみ実装できます。
状態	ポートの PoE ステータスを表示します。可能なフィールド値は次のとおりです。 電力の供給: デバイスはポート経由で電力を供給可能です。 ・disabled: デバイスはポート経由で電力を供給できません。 ・Test Fail: 受電装置のテストに失敗しました。たとえば、ポートを有効にできず、受電装置に電力を供給するために使用できません。 ・Testing: 受電装置はテスト中です。たとえば、受電デバイスは、電源から電力を受け取っていることを確認するためにテストされます。 ・searching: デバイスは現在、受電デバイスを検索しています。検索は、デフォルトの PoE 動作ステータスです。 ・障害: ポートが強制的にオンになっているときに、デバイスが受電装置の障害を検出しました。たとえば、電源電圧が範囲外である、ショートが発生している、PoE デバイスとの通信エラーが発生している、または不明なエラーが発生しています。
Mode-A/Mode-B クラス	フィールド値は次のとおりです。 ・クラス 0: 給電装置の最大電力レベルは 15.4 ワット ・クラス 1: 給電装置の最大電力レベルは 4.0 ワット ・クラス 2: 給電装置の最大電力レベルは 7.0 ワット ・クラス 3: 給電装置の最大電力レベルは 15.4 ワット ・クラス 4: 給電装置の最大電力レベルは 30 ワット ・クラス 5:給電装置の最大電力レベルは 45 ワット ・クラス 6:給電装置の最大電力レベルは 60 ワット

Mode-A/Mode-B 電力(W)	Mode-A/Mode-B電力(W)を表示します。
出力電力合計(W)	出力電力の合計を表示します。

❑それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容を一括してクリアにすることができます。

1. 3. PoE キープアライブ

この機能は信頼性の高い高品質のビデオストリーミングを長距離間で提供し、カメラ等に問題が生じた場合にリアルタイムでモニタリングしてリカバリすることができます。

【注記】:ファームウェアのアップグレード中に電源を切らないように注意してください。

1) グローバル設定

PoEキープアライブ機能をグローバルで有効にします。
この機能を有効にするには、「オンに設定」を選択してください。

「設定」→「電源」→「PoEキープアライブ」をクリックすると、以下の画面が表示されます。

❑それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<リセット>ボタンをクリックして変更を破棄してください。

2) 詳細設定

PoEキープアライブ機能をポート単位で詳細設定を行うことができます。

「設定」→「電源」→「PoEキープアライブ」→「詳細設定」をクリックすると、以下の画面が表示されます。

❑画面右側の設定（ ••• ）をクリックすると、以下のようにメニューが表示されるため、表示したい項目を選択してください。

メニュー	説明
ポート	ポート番号を表示します。
状態	有効/無効を表示します。
モード	対応するモードを表示します。 ・Force Ping: Ping メソッドを使用します。 ・自動:LLDP & Ping (デフォルト)
指定されたIPアドレス	Pingで指定したIPを表示します。
ping 間隔	Ping 間隔を表示します(デフォルトでは 10 秒)。
Ping の最大数	Ping の最大回数を表示します (デフォルト:30 回)。 ※30 回以上 pingに失敗すると、対応するポートが再起動されます。
アクションタイプ	対応するアクション タイプを表示します 。 Syslog を使用して再起動して、syslog を送信するか、単に syslog を送信します
電源復旧間隔	本機の電源を切断した後、PoE 電源を PD デバイスに再度供給するまでの間隔を表示します(秒単位)。
再起動の最大数	syslog 通知から「再起動の最大数」を受け取った後、ユーザが PD デバイスのステータスを手動で確認できる再起動の最大回数を表示します。
再起動のカウント	読み取り専用の値を表示し、「再起動の最大数」機能に使用されます。

	ユーザは、この項目で再起動回数の値をモニタリングするか、ドロップダウンリストの「更新」機能を使用して再起動回数を 0 に更新できます。
PoE起動時間	機器を起動してから、デバイスを検出するまでの時間を表示します。
LLDP保持期間	対応する LLDP 満了の保持時間を表示します。

1.各ポートの設定を変更したいポート場合は、該当ポートを選択し、<編集>ボタンをクリックすると、下記の画面が表示されます。

2.それぞれの項目を設定後、それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容をクリアにします。

3) 供給ポートの状態

ポートの状態を表示します。

「設定」→「電源」→「PoEキープアライブ」→「供給ポートの状態」をクリックすると、以下の画面が表示されます。

メニュー	説明
ポート	ポート番号を表示します。
状態	有効/無効を表示します。
モード	対応するモードを表示します。 ・Force Ping： Ping メソッドを使用します。 ・Auto：LLDP & Ping (デフォルト設定)
ポーリング方法	対応するポーリング方法を表示します
MACアドレス	対応するMACアドレスを表示
管理 IPアドレス	管理 IP を表示します。
実行したアクション	対応するアクションを表示します。

❑最新の情報を表示したい場合は、<更新>ボタンをクリックしてください。

2.3.5 VLAN 設定

仮想 LAN (VLAN) は、レイヤー2 スイッチ上で論理イーサネットセグメントを形成するポートのグループであり、マルチキャストトラフィックのより優れた管理およびセキュリティを提供します。VLAN は、物理レイアウトではなく論理スキームに従って設定されたネットワーク トポロジです。VLAN を使用すると、物理的な場所ではなく、論理的な機能によってユーザをグループ化できます。相互に頻繁に通信するすべてのポートは、ネットワーク上の物理的な配置に関係なく、同じ VLAN に割り当てられます。
VLAN を使用すると、ネットワークをさまざまなブロードキャストドメインに論理的にセグメント化できるため、関連する機能を持つポートを個別の論理 LAN セグメントにグループ化できます。これにより、ブロードキャスト パケットは VLAN 内のポート間にのみ転送されるようになり、すべてのポートに送信されるのを回避できます。また、VLAN は、特定のブロードキャストドメインへのトラフィックを制限することにより、セキュリティも向上させます。

1. 802.1Q

ネットワーク内の各VLANには識別番号としてVLAN IDがあり、イーサネットフレームの識別タグ（IEEE802.1Qタグ）に記述されています。これにより、1つの物理的な通信ポートで複数の異なるVLANを通信させることが可能です。フレームの中にタグが付くため、タグVLANとも呼ばれています。802.1Q VLANを設定する際は、物理ポートをVLAN IDが登録されたグループに所属させます。ポートが登録されたものと同じVLAN IDを持つフレームを受信すると、同じVLAN IDを持つポートにのみ転送されます。異なるVLAN IDを持つポートには転送されず、破棄されます。

【注記】デフォルトでは、すべてのポートがVLAN 1（VLAN ID＝1）に割り当てられています

「設定」→「VLAN 設定」→「802.1Q」をクリックすると、以下の画面が表示されます。

メニュー	説明
VID	ネットワーク ポリシーが設定されている VLAN ID を表示します。VLAN ID の範囲は 1 ～ 4094 です。
名前	VLAN 名を入力してください。最大 32 文字の英数字を使用できます。
タグありポート	このポートから送信されるフレームには、VLAN ID がタグ付けされます。
タグなしポート	このポートから送信されるフレームはタグなしです
禁止	設定が禁止対象のポートを選択します。
GVRPアドバタイズ	GVRP(Generic VLAN Registration Protocol)を使用して、VLAN対応デバイスはVLAN情報を相互に交換することができます。

1.各項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<リセット>ボタンをクリックして変更内容を一括してクリアにすることができます。
VLANを追加して設定したい場合は、<追加>ボタンをクリックすると次の画面が表示されるため、VIDの値(有効範囲：1～4094）および名前を設定してください。

2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容を一括してクリアにすることができます。

2. VLAN テーブル

このテーブルは、VLAN ID とそのポート メンバーを示しています。

「設定」→「VLAN 設定」→「VLAN テーブル」をクリックすると、以下の画面が表示されます。

メニュー	説明
VID	本機の VLAN ID を表示します (有効範囲は 1 ～ 4094)。
名前	VLAN 名を表示します。
状態	VLAN の状態を表示します。
プロトコル	この VID に関連付けられているプロトコルを表示します。
ポートの状態	メンバー ポートのステータス (タグ付きまたはタグなし) を表示します。

❑最新の情報を表示したい場合は、<更新>ボタンをクリックしてください。

3. PVID と入力フィルター

タグなしパケットがスイッチ ポートに入ると、PVID (Port VLAN ID) がタグなしパケットに付加され、PVID の VID 部分で指定された VLAN にフレームが転送されます。特定のポートで受信されたパケットには、そのポートの PVID が割り当てられ、パケットの宛先アドレスに対応するポートに転送されます。パケットを受信したポートの PVID が、パケットを送信するポートの PVID と異なる場合、スイッチはパケットをドロップします。スイッチ内では、異なる PVID は異なる VLAN を意味するため、PVID に基づく VLAN 識別では、本機の外部に拡張する VLAN を作成できません。VLAN が設定されていない場合、すべてのポートは PVID が「1」(デフォルト VLAN) に割り当てられます。

【注記】:PVID 機能を有効にするには、次の要件を満たす必要があります。
・すべてのポートには設定済みの PVID が必要です。
・他の値が指定されていない場合は、デフォルトの VID が使用されます。
・デフォルトの PVID を変更する場合は、まず対象ポートがメンバーの VLAN を設定てください。

「設定」→「VLAN 設定」→「PVID と入力フィルタ」をクリックすると、以下の画面が表示されます。

メニュー	説明
ポート	PVID タグが割り当てられている VLAN ID を表示します。PVID を設定して、選択したポートで受信したタグなしまたはタグ付きフレームを割り当てます。
PVID	PVID 値を入力してください(有効範囲:1 ～ 4094)。
受け入れる種類	リストから「タグ付き・タグなし・すべて」を選択します。 タグ付あり: ポートは、受信したタグなしフレームをすべて破棄します。 ポートはタグ付きフレームのみを受信します。 タグなし: ポートは、タグなしフレームのみを受信します。 すべて: ポートは、タグ付きフレームとタグなしフレームの両方を受信します。
優先度タグ入力フィルタリング	ポートがタグ付きフレームを処理する方法を指定します。リストから「オンに設定」または「オフに設定」を選択します。 オンに設定: VID がポートの PVID と一致しない場合、タグ付きフレームは破棄されます。 オフに設定: すべてのフレームは、IEEE 802.1Q VLAN に従って転送されます。

1.ポートの設定を変更したい場合は、該当ポートを選択し、<編集>ボタンをクリックすると、下記の画面が表示されます。

2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容をクリアにします。

4. GVRP

GVRP (GARP VLAN Registration Protocol または Generic VLAN Registration Protocol) は、スイッチが持っているVLAN情報を別のスイッチと交換するためのプロトコルです。
GARPおよび 802.1 Q に基づいており、大規模なネットワーク内での VLAN の設定を簡単に制御できるようになります。
GVRP がアクティブ化されると、GARP パケット データ ユニット (GPDU) が送受信されるため、ユーザは 1 つのスイッチ上で VLAN を設定し、その情報をネットワーク全体に伝達できます。

1) グローバル設定

隣接する VLAN 対応デバイスとGVRPを使用して VLAN 情報をグローバルで相互に交換できるようになります。

「設定」→「VLAN 設定」→「GVRP」→「グローバル設定」をクリックすると、以下の画面が表示されます。

❑各項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<リセット>ボタンをクリックして変更内容を一括してクリアにすることができます。

2) ポートの設定

GVRP 設定が有効になると、各スイッチ ポートをさらに編集して、関連する設定を行うことができます。

「設定」→「VLAN 設定」→「GVRP」→「ポートの設定」をクリックすると、以下の画面が表示されます。

1.ポートの設定を変更したい場合は、該当ポートを選択し、<編集>ボタンをクリックすると、下記の画面が表示されます。

【注記】:
タイマー値は 10 の倍数であり、Leave-all-time > Leave-time > 2 * Join-timeに設定してください。

2.それぞれ設定後、変更内容を確定する場合は、<適用>ボタン、キャンセルする場合は、<キャンセル>ボタンをクリックしてください。

5. 音声 VLAN

特定の VLAN 上の IP 電話からの IP 音声トラフィックを伝送するようにポートを設定することにより、VoIP(Voice over IP)サービスを強化します。Voice VLAN は VoIP に QoS を提供し、IP トラフィックが不規則または不均一に受信された場合でも通話の品質の低下を防ぎます。

1) グローバル設定

音声VLANをグローバルで有効/無効にすることができます。

「設定」→「VLAN設定」→「音声VLAN」→「グローバル設定」をクリックすると、以下の画面が表示されます。

メニュー	説明
音声 VLAN の状態	本機の音声 VLAN に「Disable」、「Auto」、または「OUI」の3つからいずれかを選択します。
音声 VLAN ID	ネットワークの音声 VLAN ID を設定します。本機でサポート可能な音声 VLAN は 1つのみです。
VLAN 優先度タグ	優先度キューイングの機能は拡張され、サーバを越えて LAN ブリッジおよび交換機を含むようになります。
DSCP	DiffServを利用してIPパケットの優先度制御（QoS）を行う際に、パケットの優先度を表す値のこと。6ビットで表され、64段階の優先度を指定することができます。
802.1p CoS状態	この機能を有効にすると、発信音声トラフィックが選択した CoS 値でマークされます。
CoS優先度	音声 VLAN 上のトラフィックのサービスのプライオリティを設定します。音声 VLAN 機能がポートでアクティブになっている場合、受信した VoIP パケットのプライオリティは新しいプライオリティで上書きされます(有効範囲: 0 ～ 7、デフォルト: 5)。
エージングタイム	ポートが動的VLAN メンバーである場合、音声 VLAN からポートを削除するためにエージングタイムが使用されます。最後の音声デバイスがトラフィックの送信を停止し、この音声デバイスの MACアドレスが期限切れになると、音声 VLAN のエージングのタイマーが開始されます。音声 VLAN のエージングのタイマーが満了すると、ポートは音声 VLAN から削除されます。

	エージングタイム中に音声トラフィックが再開すると、エージングのタイマーがリセットされて停止します(エージングタイムの有効範囲:30～1440分、デフォルト値:1440 分)。

❑設定内容を適用する場合は、<適用>ボタン、キャンセルする場合は、<キャンセル>ボタンをクリックしてください。

2) OUI 設定

送信元 MACアドレスをチェックして、受信したパケットが音声パケットかどうかを判断します。
VoIP トラフィックには、送信元 MACアドレスに設定済みの組織固有識別子 (OUI) プレフィックスがあります。特定の製造元の MACアドレスと説明を手動で OUI テーブルに追加することができます。リストされた OUI を持つ特定の IP Phone から音声 VLAN ポートで受信されたすべてのトラフィックは、音声 VLAN で転送されます。

「設定」→「VLAN設定」→「音声VLAN」→「OUI 設定」をクリックすると、以下の画面が表示されます。

メニュー	説明
インデックス	VoIP シーケンス ID を表示します。
OUIアドレス	VoIP 機器を識別するために IEEE によってベンダーに割り当てられた一意の ID。
説明	VoIP 機器ベンダーの ID を表示します。

1.エントリをポートの設定を追加/変更したい場合は、画面上の<追加>ボタン、または該当のインデックスを選択し、<編集>ボタンをクリックすると、下記の画面が表示されるためそれぞれ設定を行ってください。

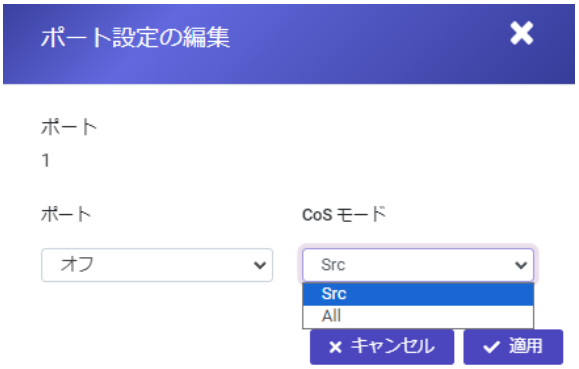
2.設定内容を適用する場合は、<適用>ボタン、キャンセルする場合は、<キャンセル>ボタンをクリックしてください。

3) ポート設定

特定の VLAN 上の IP 電話からの IP 音声トラフィックを伝送するようにポートを設定することにより、VoIP サービスをさらに強化します。Voice VLAN は VoIP に QoS を提供し、IP トラフィックが不均一に受信されても音声の品質が低下しないように保護します。
VoIP対応機器が特定のポートに接続されている場合は、ポートに音声 VLAN を設定し、CoS モードを割り当てるために使用します。

「設定」→「VLAN設定」→「音声VLAN」→「ポート設定」をクリックすると、以下の画面が表示されます。

1.ポートの設定を変更したい場合は、該当ポートを選択し、<編集>ボタンをクリックすると、下記の画面が表示されるためそれぞれ設定を行ってください。



2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容をクリアにします。

2.3.6 STP(スパニングツリー)

スパニングツリープロトコル(Spanning Tree Protocol: STP)は、IEEE802.1Dで定義されるデータリンク層のプロトコルです。複数のスイッチが円環状に構成されているレイヤー2ネットワーク間で生じたデータトラフィックの永続的な流れ(ループ状態)を防止します。
STPでは、STA(スパニングツリーアルゴリズム)を使用し、計算によって選出されたポートをブロッキング状態にします。このポートではフレームの送受信が行われず、ループを防ぐことができます。
フォワーディングポート(フレームの送受信を行っているポート)や機器に障害が発生してリンクがダウンしたときはSTPの再計算を行い、自動的に迂回路を用いて通信できるようにすることが可能です。

サポートしているSTPのバージョンは、下記のとおりです。
- MSTP(Multiple Spanning Tree Protocol)
- RSTP(Rapid Spanning Tree Protocol)

【注記】:一度にアクティブ可能なスパニングツリーは 1 つのみです。

1. グローバル設定

STP機能をグローバルで設定します。

1) STP 設定

スパニングツリーの強制バージョン（MSTP/RSTP）の切り替えやそれぞれの詳細設定を行うことができます。
一度にグローバルで有効にできるスパニングツリーの強制バージョンは 1つのみです（デフォルト設定：MSTP）。

「設定」→「STP」→「グローバル設定」→「STP」をクリックすると、以下の画面が表示されます。

メニュー	説明
STP状態	本機のスパニングツリーを有効/無効を選択します。
強制バージョン	本機の強制バージョンの設定を選択します。 RSTP (高速スパニングツリープロトコル): IEEE 802.1wポート転送状態への移行を高速化します。 MSTP (マルチプルスパニングツリープロトコル): IEEE 802.1s複数のVLANをインスタンスという単位で処理可能です。
構成名	設定名を指定します。
構成リビジョン	リビジョンを指定します。
優先度	ブリッジにプライオリティを割り当てます。スイッチが STP を実行している場合、それぞれに優先度が割り当てられます。BPDU の交換後、この値が最も小さいスイッチがルートブリッジになります。
転送遅延	スイッチ転送遅延時間を設定します。これは、ルートブリッジの状態が変更するまでの待機時間 (秒単位) を表します(リスニング状態からラーニング状態)。
最大時間	ブリッジ スイッチの最大エージングタイムを設定します。これは、設定メッセージを送信するまでのブリッジの待機時間を表します(デフォルト値: 20秒)。
Tx保留カウント	送信ホールド数を設定して、hello 時間ごとに送信できる BPDU の数が最小 1 から最大 Tx-Hold-Count 値までの範囲の本機の最大送信レートを制限します。
Hello時間	本機のHello時間を設定します。これは、パケットを転送するまでの、ブリッジがリスニングおよびラーニング状態にとどまる時間を表します。

❑各項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<リセット>ボタンをクリックして変更内容を一括してクリアにすることができます。

2) ルートブリッジ情報

ルートブリッジは、ループ構成となっているネットワークをツリー状にして管理するための中心となるスイッチです。スパニングツリーネットワークを構成するスイッチの中で、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IDには優先度(2byte)とMACアドレス(6byte)の部分が含まれています。802.1Dのデフォルトのブリッジは「32768」です。
STPデバイスは、定期的にBPDU(ブリッジプロトコルデータユニット)を送信しています。隣接するデバイスから送信されてきたBPDUに含まれるブリッジIDを自身のブリッジIDと比較し、ルートブリッジを決定します。
あらかじめ設定した時間(”BPDU保持時間”や”Max Age”と呼びます)が経過してもBPDUが受信できない場合は、スイッチまたはリンクに障害が発生したとみなします。

「設定」→「STP」→「グローバル設定」→「ルートブリッジ情報」をクリックすると、以下の画面が表示されます。

メニュー	説明
ブリッジアドレス	ブリッジの MACアドレスを表示します。
ルートアドレス	ルートブリッジの MACアドレスを表示します。
優先度	ブリッジのプライオリティを表示します。スイッチが STP を実行している場合、それぞれに優先度が割り当てられます。BPDU の交換後、この値が最も小さいスイッチがルートブリッジになります。
コスト	ルートブリッジのコストを表示します。
ポート	ルートブリッジのポートを表示します。
転送遅延	本機の転送遅延時間を表示します。これは、ルートブリッジの状態が変更するまでの待機時間(秒単位) を表します(リスニング状態からラーニング状態)。
最大時間	ブリッジ スイッチの最大エージングタイムを設定します。これは、設定メッセージを送信するまでのブリッジの待機時間を表します(デフォルト値: 20秒)。
Hello時間	本機のHello時間を表示します。これは、BPDUがポートに送られる間隔を表します(デフォルト値: 2秒)。

2. RSTP ポート設定

「設定」→「STP」→「RSTP ポート設定」をクリックすると、以下の画面が表示されます。

【注記】:処理モードが「MSTP」に設定されている場合、RSTP モードに変更するには、
「グローバル設定」→「強制バージョン」にて変更を行ってください。

メニュー	説明
ポート	ポートまたはトランクポートの識別子。
優先度	スパニングツリー アルゴリズムでこのポートに使用されるプライオリティを設定します。本機すべてのポートのパスコストが同じ場合、優先度が最も高い (つまり、値が最も小さい) ポートが、スパニングツリーのアクティブリンクとして設定されます。これにより、スパニングツリーがループを検出した場合に、プライオリティの高いポートがブロックされる可能性が低くなります。複数のポートに最高のプライオリティが割り当てられている場合、識別子が最も小さいポートが有効になります(有効範囲:0 ～ 240(16単位)、デフォルト値:128)。
パスコスト	ネットワーク通信において、ノード間の通信にかかるコストを表す値です。このコストは、データの伝送速度や伝送距離、通信路の混雑状況などの要素によって決まります。
割り当てられたルートブリッジ	ルートブリッジを表示します。これは、ブリッジの優先度とブリッジのベースMACアドレスを使用して設定されます。
外部ルートコスト	外部ルートコストを表示します
指定ブリッジ	指定ポートのブリッジのブリッジ識別子です。これは、ブリッジの優先度とブリッジのベース MACアドレスを使用して設定されます。
エッジ ポート設定/オペレーション	エッジ ポートの状態を表示します。
P2P MAC Conf/オペレーション	P2P MAC Conf/Oper を表示します。
ポートのロール	有効な各ブリッジ ポートには、各スパニングツリー内でポートの役割が割り当てられます。ポートの役割は、「Root」、「Designated」、「Discarding」、「Disabled」の4つです。 それぞれ、ルートポート、指定ポート、代替ポート、バックアップポート、無効ポートになります。
ポート状態	現在のポートのSTP 状態を表示します。有効にすると、ポートの状態によって、トラフィックの転送方法が異なります。ポート状態は次のとおりです。

	・Discarding: 送信元 MAC アドレスの学習をせず、フレームを転送しません。 ・Learning: ポートは学習モードです。ポートはトラフィックを転送できません。ただし、新しい MAC アドレスを学習することはできます。 ・Forwarding: ポートは転送モードです。ポートは、この状態でトラフィックを転送し、新しい MAC アドレスを学習できます。

3. CIST ポート設定

CIST(Common Instance Spanning Tree)プロトコルは、IEEE 802.1w、IEEE 802.1s、および IEEE 802.1D 規格に準拠しているブリッジ間で実行されるスパニングツリー アルゴリズムによって形成されます。CISTは、ネットワーク全体の接続を表し、STP/RSTP のスパニングツリーに相当します。MSTI(マルチ スパニングツリーインスタンス)リージョン内のCIST は、リージョン外の CST と同じです。MSTI はリージョン内のトポロジを制御しますが、すべてのリージョンは CIST を使用して結合されます。CIST は、リージョン間でループのないトポロジを作成する役割を果たします。CSTインスタンスにより、
異なるリージョンが相互に通信できるようになります。CST は、MSTI でカバーされていない VLAN のリージョン内のトラフィックにも使用されます。MSTP 対応ネットワークでは、MST リージョンとシングル スパニングツリー対応の機器間で動作する CIST は 1つのみです。ネットワークには、複数のMSTリージョンと、RSTP を実行する他のネットワーク セグメントが含まれる場合があります。複数のリージョンと他の STP ブリッジは、単一の CST を使用して相互接続されます。
スパニングツリー モードが STP または RSTP に設定されている場合は、「CIST ポート設定」メニュー上で、インタフェースの STA 属性を設定および表示します。同じメディア タイプのポートに異なる優先度またはパスコストを使用して、優先パスまたはエッジ ポートを示し、接続先の機器が高速転送をサポートできるかどうかを示すか、リンク タイプを使用してポイントツーポイント接続または共有メディアを示すことができます。

「設定」→「STP」→「CIST ポート設定」をクリックすると、以下の画面が表示されます。

❑画面右側の設 •••)をクリックすると、以下のようにメニューが表示されるため、表示したい項目を選択してください。

メニュー	説明
ポート	ポートまたはトランクポートの識別子。
優先度	スパニングツリー アルゴリズムでポートに使用されるプライオリティを設定します。本機すべてのポートのパスコストが同じ場合、優先度が最も高い (つまり、値が最も小さい) ポートが、スパニングツリーのアクティブリンクとして設定されます。これにより、スパニングツリーがループを検出した場合に、プライオリティの高いポートがブロックされる可能性が低くなります。複数のポートに最高のプライオリティが割り当てられている場合、識別子が最も小さいポートが有効になります（有効範囲:0 ～ 240(16秒単位)、デフォルト: 128）。
パスコスト	ネットワーク通信において、ノード間の通信にかかるコストを表す値です。このコストは、データの伝送速度や伝送距離、通信路の混雑状況などの要素によって決まります。
割り当てられたルートブリッジ	内部パスコスト設定では、スパニングツリー トラフィックをインタフェース経由でスパニングツリー リージョン内の隣接するブリッジに送信する際の相対的なコストを指定できます。
外部ルートコスト (Conf/Oper)	外部パスコストの設定は、インタフェースを介してスパニングツリー トラフィックを送信し、隣接するスパニングツリー リージョンに到達するコストを計算するために使用されます。スパニングツリー アルゴリズムは、ツリーの各ポイントとルートブリッジ間の合計パスコストを最小化します。
地域のルートブリッジ	CST リージョナル ルートのブリッジ ID です。これは、ブリッジの優先度とブリッジのベース MACアドレスを使用して設定されます。
Edgeポート設定/オペレーション	エッジ ポートの状態を表示します。
P2P MAC設定/オペレーション	指定ポートのブリッジのブリッジ識別子です。これは、ブリッジの優先度とブリッジのベース MACアドレスを使用して設定されます。
ポートのロール	有効な各 MST ブリッジ ポートには、各スパニングツリー内でポートの役割が割り当てられます。ポートの役割は、ルート ポート、指定ポート、代替ポート、バックアップ ポート、マスター ポート、または無効のいずれかの値になります。
ポート状態	現在のポートのSTP 状態を表示します。有効にすると、ポートの状態によって、トラフィックの転送方法が異なります。 ポート状態は次のとおりです。 ・Disabled: STP が無効になっています。ポートは、MAC アドレスを学習しながらトラフィックを転送します。 ・Blocking: ポートはブロックされており、トラフィックの転送や MAC アドレスの学習には使用できません。 ・Listening: ポートはリスニングモードです。この状態では、ポートは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せん。 ・Learning: ポートは学習モードです。ポートはトラフィックを転送できません。ただし、新しい MAC アドレスを学習することはできます。 ・Forwarding: ポートは転送モードです。ポートは、この状態でトラフィックを転送し、新しい MAC アドレスを学習できます。

1.ポートの設定を変更したい場合は、該当ポートを選択し、<編集>ボタンをクリックすると、下記の画面が表示されるためそれぞれ設定を行ってください。

2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容を一括してクリアにすることができます。

4. MST インスタンスの設定

本機の現在の MSTI 設定情報が表示されます
MSTPはvlanごとにグループ分けすることができ、このグループをインスタンスと呼び、インスタンス単位でルートブリッジや代替ポート等を変更することができます。

MSTI ID のポート設定を設定することができます。ループが発生した場合、MSTP 機能はポートのプライオリティに応じて、フォワード状態にするインタフェースを選択します。まず、転送用に選択したいポートのプライオリティ値を高く設定します。プライオリティ値が同じ場合、MSTP 機能は最小の MACアドレスをフォワード状態に実装し、他のインタフェースはブロックされます。プライオリティ値が低いほど、パケット転送の優先度が高くなるため注意してください。

「設定」→「STP」→「MSTインスタンスの設定」をクリックすると、以下の画面が表示されます。

メニュー	説明
MST ID	作成された MST グループの ID を表示します。スイッチには最大 15 グループまで設定できます。
ポート	ポートまたはトランクポート ID を表示します。
優先度	MST のブリッジの優先度を選択します。スイッチまたはブリッジが STP を実行している場合、それぞれに優先度が割り当てられます。 BPDU の交換後、この値が最も小さいスイッチがルートブリッジになります。ブリッジの優先度は「4096」の倍数です。 「4096」の倍数ではないプライオリティを指定すると、プライオリティは「4096」の倍数である次に低いプライオリティに自動的に設定されます（有効範囲: 0 ～ 4095、優先度:0）。 デフォルトの場合、優先度は「32768」です。
内部パスコスト設定	内部パスコスト設定では、スパニングツリー トラフィックをインタフェース経由でスパニングツリー リージョン内の隣接するブリッジに送信する際の相対的なコストを指定できます。
内部パスコスト オペレーション	このブリッジからルートブリッジまでのパスの運用コストを表示します。
リージョナル ルートブリッジ	これは、CST リージョナル ルートのブリッジ ID です。これは、ブリッジの優先度とブリッジのベース MACアドレスを使用して設定されます。
内部ルートコスト	選択した MSTインスタンスの指定ルートへのパスコストを表示します。
指定ブリッジ	指定ポートのブリッジのブリッジ識別子を表示します。これは、ブリッジの優先度とブリッジのベース MACアドレスを使用して設定されます。
内部ポート コスト	このパラメータは、STPインスタンス内でインタフェースが選択されたときに、指定のポートにパケットを転送するための相対的なコストを表すために設定されます（値の有効範囲:1 ～ 200000000）。 このパラメータを選択すると、ループが発生した場合の最速ルートが設定されます。内部コストが低いほど、送信が速くなります。 このパラメータに" 0"を選択すると、インタフェースの最速の最適ルートが自動的に設定されます。
ポートの役割	有効な各 MST ブリッジ ポートには、各スパニングツリーのポートの役割が割り当てられます。 ポートの役割は、ルート、指定、代替、バックアップ、マスター、または無効のいずれかの値です。
ポート状態	現在のポートのSTP 状態を表示します。有効にすると、ポートの状態によって、トラフィックの転送方法が異なります。ポート状態は次のとおりです。 ・Disabled: STP が無効になっています。ポートは、MAC アドレスを学習しながらトラフィックを転送します。 ・Blocking: ポートはブロックされており、トラフィックの転送や MAC アドレスの学習には使用できません。 ・Listening: ポートはリスニング モードです。この状態では、ポートは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せん。 ・Learning: ポートは学習モードです。ポートはトラフィックを転送できません。ただし、新しい MAC アドレスを学習することはできます。 ・Forwarding: ポートは転送モードです。ポートは、この状態でトラフィックを転送し、新しい MAC アドレスを学習できます。

1.MST ID を新たに追加したい場合は、メニュー右上の<追加>ボタンをクリックすると、下記の画面が表示されるので、それぞれ設定を行ってください。

2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容を一括してクリアにすることができます。

5. MST ポート設定

MSTは、複数のVLANをインスタンスというグループにまとめて、そのインスタンスごとにスパニングツリーを動作させます。MSTPを使用することで、スイッチのCPU負荷を減少させ、またRSTP（Rapid Spanning Tree Protocol）も有効になり、高速なコンバージェンスが実現できます。

【注記】:MSTインスタンスがあらかじめ設定されていない場合は、MSTポートの情報は表示されません。

「設定」→「STP」→「MSTポート設定」をクリックすると、以下の画面が表示されます。

メニュー	説明
MST ID	作成された MST グループの ID を表示します。スイッチには最大 15 グループまで設定できます。
ポート	ポートまたはトランクポート ID を表示します。
優先度	MST のブリッジの優先度を選択します。スイッチまたはブリッジが STP を実行している場合、それぞれに優先度が割り当てられます。 BPDU の交換後、この値が最も小さいスイッチがルートブリッジになります。 ブリッジの優先度は「4096」の倍数です。 「4096」の倍数ではないプライオリティを指定すると、プライオリティは「4096」の倍数である次に低いプライオリティに自動的に設定されます。 たとえば、プライオリティを任意の値に設定すると、有効範囲「0 ～ 4095」、優先度は「0」に設定されます。 デフォルトの優先度は「32768」、有効な範囲：「0 ～ 61440」です。
内部パスコストの構成/オペレーション	内部パスコスト設定では、スパニングツリー トラフィックをインタフェース経由でスパニングツリー リージョン内の隣接するブリッジに送信する際の相対的なコストを指定できます。
地域のルートブリッジ	これは、CST リージョナル ルートのブリッジ ID です。 これは、ブリッジの優先度とブリッジのベース MACアドレスを使用して設定されます。
内部ルートコスト	選択した MSTインスタンスの指定ルートへのパスコストを表示します。

❑編集したい MST ID を選択し、<編集>ボタン をクリックして設定を変更してください。
それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容を一括してクリアにすることができます。

2.3.7 リンクアグリゲーション

LAG(Link Aggregation) は、複数のリンクを束ねて仮想的に1本のリンクとする技術です。
ポートを集約すると、帯域幅が倍増し、ポートの柔軟性が向上します。リンクアグリゲーションは、サーバなどの帯域幅を集中的に使用するネットワーク機器をネットワークのバックボーンにリンクするために最もよく使用されます。
参加ポートは、ポート トランクグループのメンバーとなります。トランクグループの 1 つのポートの設定がトランクグループのすべてのポートに適用され、トランクグループのすべてのポートが同じように動作するように設定する必要があるため、ます。したがって、トランクグループ内の任意のポートのいずれかから1つのみ設定する必要があります。特定のデータ通信パケットは、トランクグループ内の同じポートを介して常に送信されます。これにより、データ通信パケットの個々のフレームの配信が正しい順序で受信されることが保証されます。LAG のトラフィック負荷は、集計演算に従ってポート間でバランスが取られます。1 つまたは複数のポートの接続が切断された場合、これらのポートのトラフィックは通常のポートで送信され、信頼性の高い接続を実現させることができます。

ポートを集約する場合、ポートと LAG は次の条件を満たす必要があります。
- LAG 内のすべてのポートは、同じメディア/フォーマット タイプである。
- ポートに VLAN が設定されていない。
- ポートが別のLAGに割り当てられていない。
- ポートにオートネゴシエーション モードが設定されていない。
- ポートは全二重モードである。
- LAG 内のすべてのポートは、同じイングレスのフィルタリングとタグ付きモードである。
- LAG のすべてのポートは、同じフロー制御モードである。
- LAG 内のすべてのポートの優先度は同じである。
- LAG 内のすべてのポートは、同じトランシーバ タイプである。
- ポートが事前に設定された LAG の一部でない場合にのみ、ポートを LACP ポートとして設定可能。

LACP(Link Aggregation Control Protocol) は、LAG の設定とメンテナンスを自動化する際に有用なダイナミックプロトコルです。LACP の主な目的は、必要に応じて新しいリンクを追加し、リンク障害からのリカバリをサポートしながら、個々のリンクを集約バンドルに自動的に設定することです。LACP は、すべてのリンクが許可されたグループに接続されているかどうかを確認するためにモニタリングできます。LACP はPC ネットワーキングの標準です。したがって、LACP を使用するには、最初に本機のトランクポートで有効にして、規格に準拠している両方の対象機器に対して有効にする必要があります。

「設定」→「リンクアグリゲーション」をクリックすると、以下の画面が表示されます。

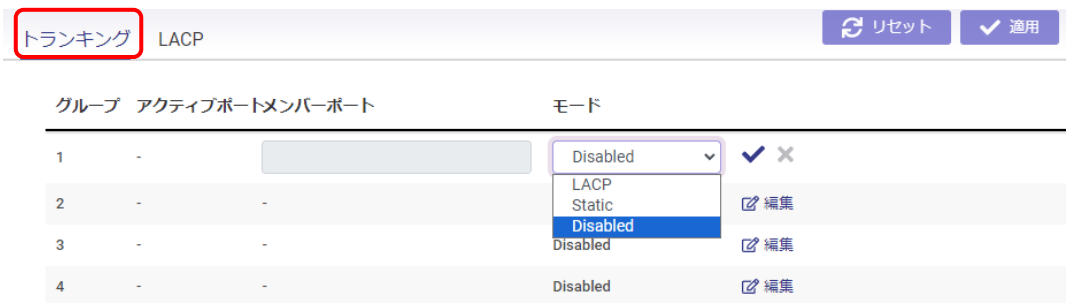
1. トランキング

ポート トランキングを使用すると、単一の高速リンクとして機能する1 つの論理リンクに物理リンクを割り当てることができ、帯域幅が大幅に増加します。ポート トランキングを使用して複数の接続をバンドルし、結合された帯域幅を 1 つの大きな「パイプ」のように使用します。

「設定」→「リンクアグリゲーション」→「トランキング」をクリックすると、以下の画面が表示されます。

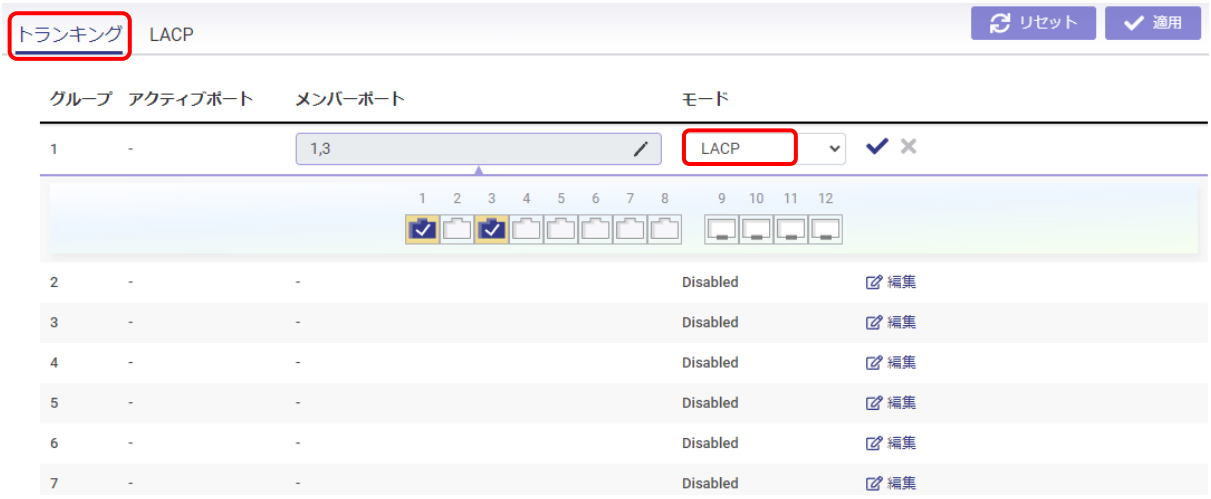
メニュー項目	説明
グループ	特定のトランクグループの番号を表示します。最大 8 つのポートで設定される各グループで、最大 8 つのリンクアグリゲーション グループを利用できます。
アクティブポート	トランクグループのアクティブな参加メンバーを表示します。
メンバー ポート	トランクグループに追加するポートを選択します。グループごとに最大 8 つのポートを割り当てることができます。 静的: リンクアグリゲーションは、指定のトランクグループに対して手動で設定されます。 LACP: リンクアグリゲーションは、指定のトランクグループに対して自動的に設定されます。
モード	LACP は、LACP 準拠のスイッチに接続されている場合、ポート トランキング グループ内のリンクの自動検出を可能にします。この自動検出を有効にするには、両方の機器が同じモードに設定してください。モードが異なる場合は機能しません。LACP をサポートしていないスイッチに接続する場合は、手動により設定してください。

1.トランキングポートを設定したい場合、グループごとに<編集>ボタンをクリックすると、モードを「LACP」、「Static」、「Disabled」のいずれかを選択してください。



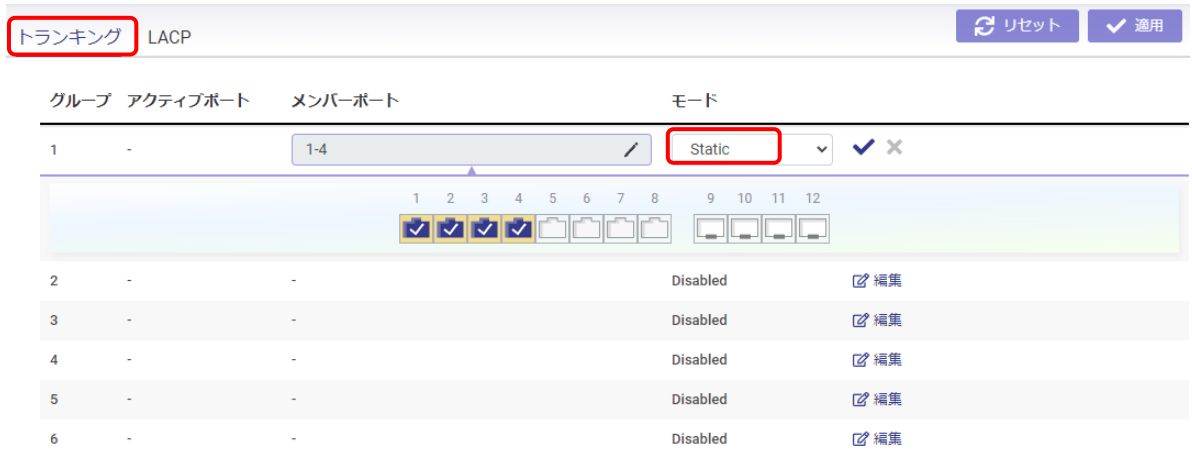
■トランキングの LACP モードを設定する場合：

グループごとに<編集>ボタンをクリックした後、モードを“LACP”に設定して をクリックすると、ポート画面が下に表示されるため、メンバーポートを選択してください。



■トランキングのスタティックモードを設定する場合

1. グループごとに<編集>ボタンをクリックした後、モードを“Static”に設定して をクリックすると、ポート画面が下に表示されるため、メンバーポートを選択してください。



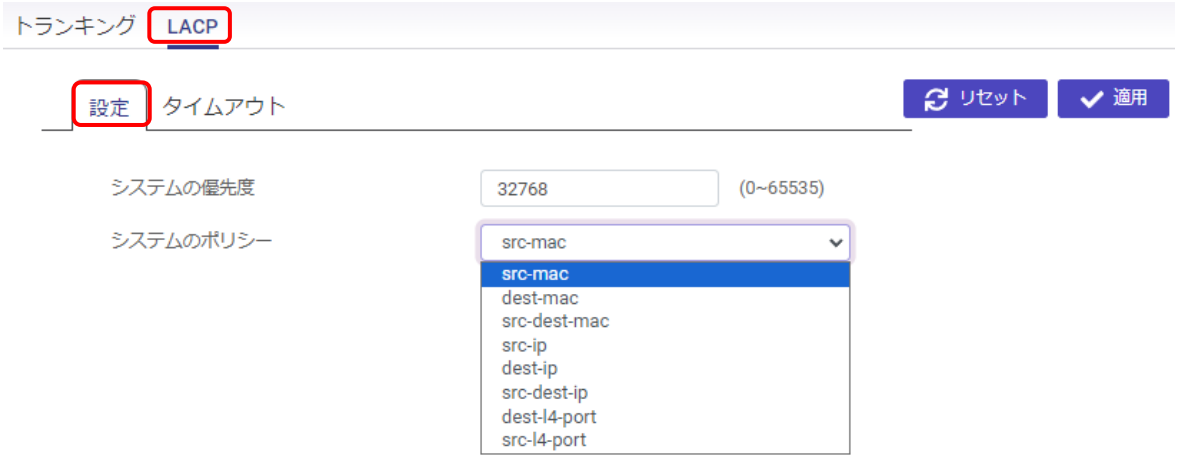
2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容を一括してクリアにすることができます。

2. LACP

1) 設定

LACP(Link Aggregation Control Protocol) で実行するシステム優先度を割り当てます。LACP は、別のリンクがダウンした場合にバックアップリンクになります。最も低いシステム プライオリティは、リンクがダウンした場合にどのポートをアクティブに実行するかを決定できます。2 つ以上のポートの LACP ポートのプライオリティが同じ場合、物理ポート番号が最も小さいポートがバックアップ ポートとして選択されます。許可された最大数のポート メンバーを持つ LAG がすでに存在し、その後、既存のメンバーよりも高い優先度を使用して別のポートで LACP が有効な場合、新しく設定されたポートは、優先度の低い既存のポート メンバーを置き換えます。数字が小さいほど優先度が高いことを表します(有効範囲:は 0 ～ 65535、デフォルト値:32768)。

「設定」→「LACP」→「設定」をクリックすると、以下の画面が表示されます。



メニュー	説明
システムの優先度	システムに LACPのプライオリティ値を入力してください(デフォルト:32768、有効範囲:1 ～ 65535)。
システムのポリシー	ドロップダウン リストからシステムのポリシーを選択します。

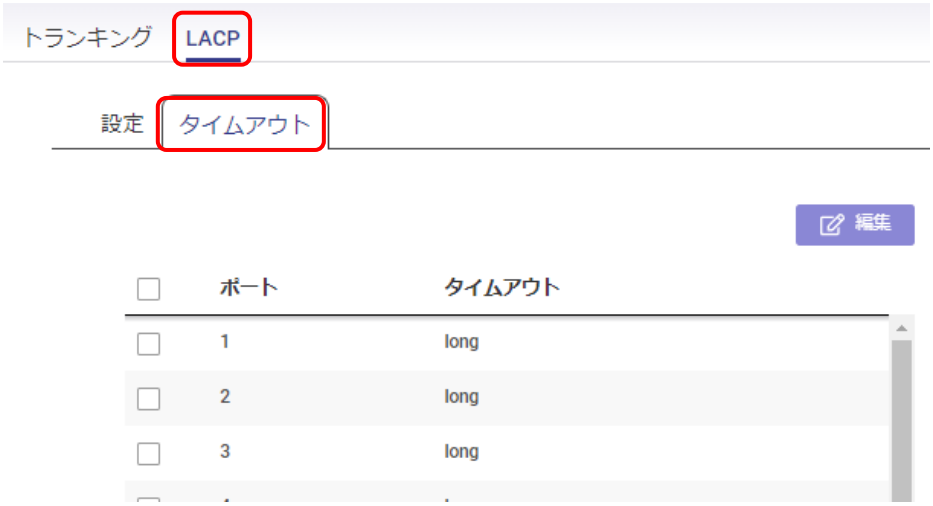
❑それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<リセット>ボタンをクリックして変更内容を破棄してください。

2) タイムアウト

LACPタイムアウトは、対向装置から受信したLACPパケットを無効と見なすまでの時間を示し、LACPの長さは長・短2種類があります。
LACPを使用すると、2つのメンバー間でリンクアグリゲーションに関する情報を交換され、タイムアウト値は、定期的に測定されます。

まず、トランクグループのポートが動作しているかどうかを確認してください。
一定の時間が満了すると、トランクから削除されます。
LACP タイムアウトのデフォルト値は、「Long Timeout」です。

「設定」→「リンクアグリゲーション」→「LACP」→「タイムアウト」をクリックすると、以下の画面が表示されます。



メニュー	説明
タイムアウト	管理 LACP タイムアウト(「Long」と「Short」のいずれか)を選択します。 ・Long Timeout: LACP PDU は 30 秒ごとに送信されます(LACP タイムアウト値:90 秒)。 ・Short Timeout: LACP PDU は毎秒ごとに送信されます(LACP タイムアウト値:3 秒)。

1.設定を変更したいポートを選択し、<編集>ボタンをクリックしてタイムアウト値を変更してください。

2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容を一括してクリアにすることができます。

2.3.8 L3 プロトコル

1. IGMP スヌーピング

IGMPスヌーピング(Internet Group Management Protocol Snooping)は、レイヤー2スイッチでのマルチキャストのフラッディングを制御して、受信側のホストにより接続されていないポートの不要な帯域消費を防ぐための機能です。

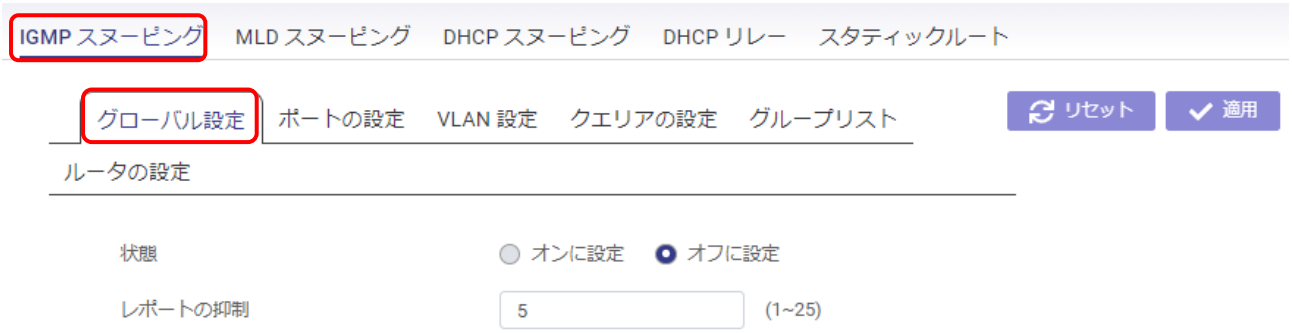
マルチキャストは、ビデオ会議やストリーミング オーディオなどのリアルタイム アプリケーションをサポートするために使用されます。マルチキャスト サーバは、各クライアントと個別の接続を確立する必要はありません。サービスをネットワークにブロードキャストするだけで、マルチキャストを受信したいホストはローカル マルチキャストスイッチに登録します。
マルチキャストグループは、マルチキャストアプリケーションからマルチキャストパケットを受信するエンド ノードのグループです。マルチキャストグループに参加した後、ホスト ノードはメンバーであり続けるために定期的にレポートを発行し続ける必要があります。そのマルチキャストグループに属するマルチキャストパケットは、ポートから転送されます。
IGMPスヌーピングをサポートするスイッチは、IP マルチキャストスイッチと IP マルチキャストホスト間で転送される IGMP クエリ、レポート、およびLeaveパケットをスヌーピングして、IP マルチキャストグループ メンバーシップを決定できます。IGMPスヌーピングは、ネットワークを通過する IGMP パケットをチェックし、それに応じてマルチキャストを設定します。スイッチは、IGMP クエリおよびレポート メッセージに基づいて、マルチキャストトラフィックを要求するポートだけにトラフィックを転送します。これにより、スイッチはマルチキャストグループのパケットを、検証済みのホスト ノードを持つポートに転送できます。スイッチは、IGMP 指定ポートへのトラフィックのフラッディングを制限することもできます。これにより、ホスト ノードが配置されている本機の ポートのみにマルチキャストパケットを制限することで、ネットワーク パフォーマンスが向上します。IGMPスヌーピングは、本機を通過する全体的なマルチキャストトラフィックを大幅に削減します

IGMPv1	RFC 1112 で定義されています。明示的な参加メッセージが本機に送信されますが、タイムアウトを使用して、ホストがいつグループを脱退するかが決定されます。
IGMPv2	RFC 2236 で定義されています。参加メッセージに明示的なLeaveメッセージを追加して、グループが LAN 上に関心のあるリスナーを持っていない場合に、本機がより簡単に判断できるようにします。
IGMPv3	RFC 3376 で定義されています。マルチキャストグループのコンテンツの単一ソースのサポート。

1) グローバル設定

IGMPスヌーピング機能をグローバルで有効/無効にします。

「設定」→「L3 プロトコル」→「IGMPスヌーピング」→「グローバル設定」をクリックすると、以下の画面が表示されます。



メニュー	説明
状態	本機で IGMPスヌーピングを有効/無効にするために選択します。本機は、受信するすべての IGMP パケットをスヌーピングして、有効な場合にグループ アドレス宛てのパケットを受信するセグメントを決定します（デフォルト設定：オフ）。
レポートの抑制	IGMPスヌーピングのレポート抑制を有効/無効を選択します。 レポートの抑制機能は、メンバーがマルチキャスト対応のルータに送信するメンバーシップのレポートの量を制限します（値の有効範囲:1-25）。

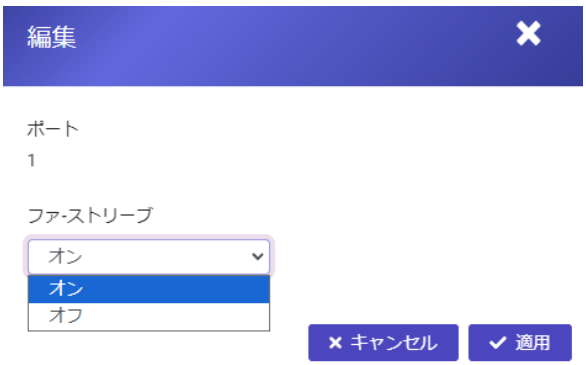
❑<適用>ボタンをクリックして、システムの設定を更新します。

2) ポート設定

ポートごとに Fast Leave オプションを確認または設定します。

「設定」→「L3 プロトコル」→「IGMPスヌーピング」→「ポート設定」をクリックすると、以下の画面が表示されます。

1.設定したいポートを選択し、<編集>ボタンをクリックしてブリッジ設定を変更してください。



2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容を一括してクリアにすることができます。

3) VLAN 設定

システム上の VLAN の IGMPスヌーピング設定を設定します。
本機は、IGMP パケットを送信する VLAN で IGMPスヌーピングを実行します。IGMPスヌーピングを実行する VLAN を指定できます。IGMPスヌーピングを有効/無効をドロップダウン ボックスから選択します。次に、VLAN ID の Fast Leave を有効/無効を選択します。

Fast Leave が使用されていない場合、マルチキャストクエリアは、IGMPv2/v3 グループのLeave メッセージが受信時にグループスペシフィッククエリメッセージを送信します。指定のタイムアウト期間内にホストがクエリに応答しない場合にのみ、クエリアはそのグループのトラフィックの転送を停止します。
本機は、Fast Leave が有効な場合、1 つのホストのポートにのみ接続されていると想定されているため、Fast Leaveは、1台のIGMP 対応機器にのみ接続されている場合にのみ有効にする必要があります。
Fast Leaveは、IGMPスヌーピングが有効な場合、IGMPv2 または IGMPv3 スヌーピングでのみサポートされます。マルチキャストクエリアが接続されていることを学習した場合、Fast Leaveはポートに適用されません。
Fast Leave は、多くの IGMP ホストの追加およびLeave要求が頻繁に発生するネットワークの帯域幅の使用を改善できます。

「設定」→「L3 プロトコル」→「IGMPスヌーピング」→「VLAN 設定」をクリックすると、以下の画面が表示されます。

メニュー	説明
VLAN ID	VLAN ID を表示します。
IGMPスヌーピングの状態	指定の VLAN ID の IGMPスヌーピング機能を有効/無効にします。
バージョン	使用する IGMP バージョンを選択します。インタフェースが受信した IGMP パケットのバージョンが指定のバージョンよりも高い場合、このパケットはドロップされます。

1.設定したいポートを選択し、<編集>ボタンをクリックしてブリッジ設定を変更してください。

2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容を一括してクリアにすることができます。

4) クエリアの設定

IGMPスヌーピングでは、中央の機器がネットワーク上のすべてのエンド デバイスに定期的にクエリを実行して、マルチキャストメンバーシップを通知する必要があり、この中央の機器が IGMP クエリアです。スヌーピングは、設定されたクエリアのクエリ間隔と同じ間隔で定期的なクエリを送信します。IGMPクエリは、現在のマルチキャストグループのメンバーシップ情報を最新の状態に保ちます。
更新されたメンバーシップ情報を受信しない場合、指定の VLAN へのマルチキャストの転送は停止されます。

「設定」→「L3 プロトコル」→「IGMPスヌーピング」→「クエリアの設定」をクリックすると、以下の画面が表示されます。

メニュー	説明
VLAN ID	VLAN ID を表示します。
クエリア状態	指定した VLAN ID の IGMP クエリア状態を有効/無効を選択します。 クエリアは、マルチキャストトラフィックを受信するかどうかを定期的にホストに問い合わせることができます。 クエリア機能が有効な場合、ホストがマルチキャストトラフィックを受信するかどうかをチェックします。選出されたクエリアは、LAN にグループ メンバーを問い合わせる役割を担い、アップストリームのマルチキャスト機器にサービス要求を伝達して、マルチキャストサービスを引き続き受信できるようにします。 この機能は、IGMPv1 および v2 スヌーピングでのみサポートされています。
クエリアのバージョン	このポートから送信される IGMP パケットのバージョンを入力してください。 ポートが受信した IGMP パケットのバージョンが指定のバージョンよりも高い場合、このパケットはドロップされます。
クエリアの種類	クエリアのタイプを表示します。
間隔	ジェネラルクエリの送信間隔を秒単位で入力してください(デフォルト値:125 秒)。
最大応答間隔	スヌーピングクエリアによって送信されるクエリで使用される最大応答時間を表示します(デフォルト値:10 秒)。
起動時の クエリカウンタ	起動時のクエリカウンタの数を入力してください。
起動クエリ間隔	実行中のクエリ間隔を指定します。

❑最新の情報を表示したい場合は、<更新>ボタンをクリックしてください。

5) グループリスト

グループ リストには、IGMPスヌーピング リストの VLAN ID、グループ IP アドレス、メンバー ポートが表示されます。

「設定」→「L3 プロトコル」→「IGMPスヌーピング」→「グループリスト」をクリックすると、以下の画面が表示されます。

❑最新の情報を表示したい場合は、<更新>ボタンをクリックしてください。

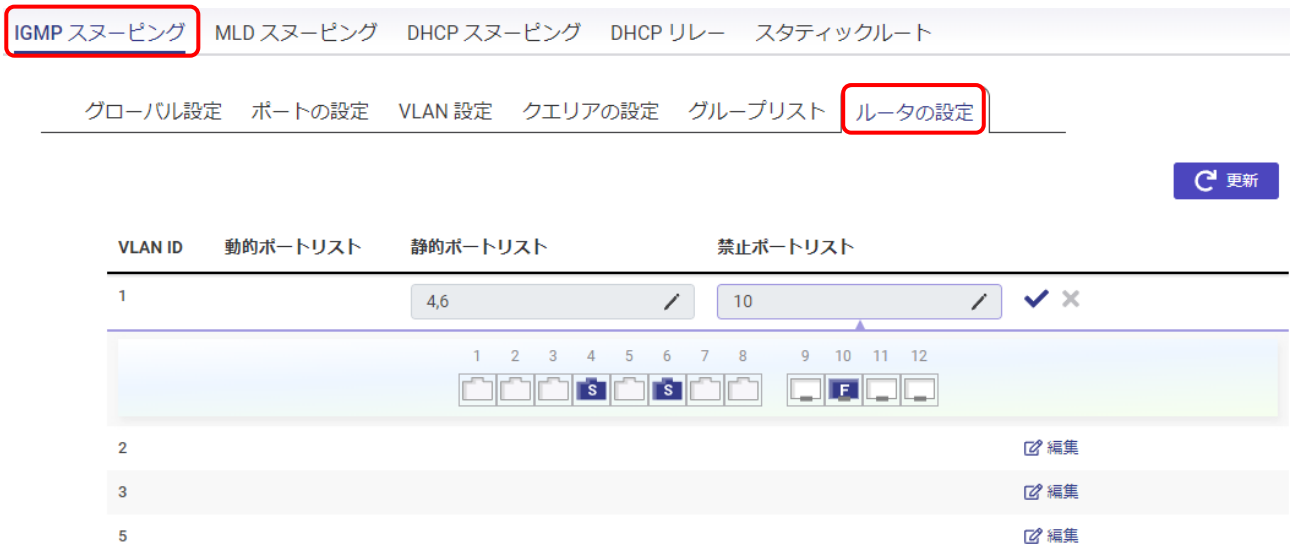
6) ルータの設定

ポートがアクティブで VLAN のメンバーである場合、ルータの設定には、学習したマルチキャストルータの接続されたポートが表示されます。設定する VLAN ID を選択し、設定したい VLAN ID の静的ポートと禁止ポートを入力してください。スヌーピングされたすべての IGMP パケットは、ポートから到達可能なマルチキャストルータに転送されます。

「設定」→「L3 プロトコル」→「IGMPスヌーピング」→「ルータの設定」をクリックすると、以下の画面が表示されます。

アイテム	説明
VLAN ID	VLAN ID を表示します。
動的ポート リスト	動的に設定されたルータのポートを表示します。
静的ポート リスト	マルチキャスト対応のルータに接続されているポートの範囲を指定します。すべてのパケットがマルチキャスト対応のルータに確実に到達可能にします。 画面上では、“S”で表示ます。
禁止ポートリスト	マルチキャスト対応のルータから切り離されているポートの範囲を指定します。 禁止されたルータのポートがルーティング パケットを伝搬しないようにします。 画面上では、“F”で表示されます。

1.ポートの設定を変更したい場合は、ポートを選択して<編集>ボタンをクリックすると、次の画面が表示されます。



2.静的ポートストおび禁止ポートリストにそれぞれ該当ポートを選択して、<更新ボタン>をクリックしてください。

2. MLD スヌーピング

マルチキャストリスナー検出 (MLD) スヌーピングは、直接接続されたポートでマルチキャストリスナーを検出するために IPv6 トラフィック レベルで動作し、IPv4 の IGMPスヌーピングと同様の機能を実行します。MLD スヌーピングを使用すると、本機は MLD パケットを検査し、コンテンツに基づいて転送を決定できます。MLD スヌーピングは、スイッチ ポートを自動的に設定することで IPv6 マルチキャストトラフィックを制限し、マルチキャストトラフィックが受信を希望するポートにのみ転送されるようにします。これにより、指定の VLAN での IPv6 マルチキャストパケットのフラッディングが減少します。IGMP と MLD スヌーピングの両方を同時にアクティブにすることができます。

1) グローバル設定

MLDスヌーピング機能をグローバルで有効/無効にします。

「設定」→「L3 プロトコル」→「MLDスヌーピング」→「グローバル設定」をクリックすると、以下の画面が表示されます。

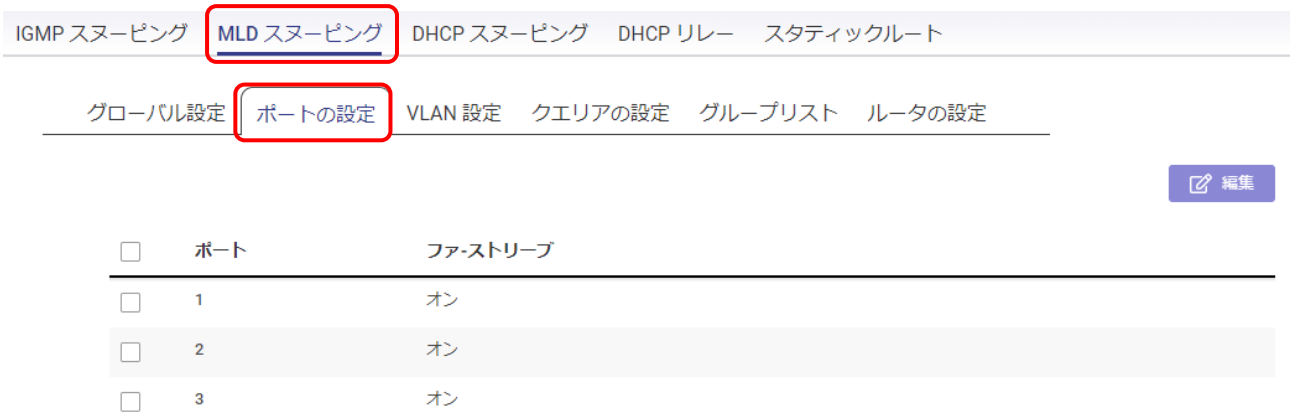
メニュー	説明
状態	スイッチで MLD スヌーピングを有効/無効にします。受信するすべての MLD パケットをスヌーピングして、有効な場合にグループ アドレス宛てのパケットを受信するセグメントを決定します。
レポートの抑制	スヌーピングのレポート抑制を有効/無効を選択します。 レポートの抑制機能は、メンバーがマルチキャスト対応のルータに送信するメンバーシップのレポートの量を制限します（値の有効範囲:1-25）。

❑設定内容を適用する場合は<適用>ボタン、一括してクリアする場合は<リセット>ボタンをクリックしてください。

2) ポートの設定

ポートごとに Fast Leave オプションを確認または設定します。

「設定」→「L3 プロトコル」→「MLDスヌーピング」→「ポートの設定」をクリックすると、以下の画面が表示されます。



1.ポートの設定を変更したい場合は、該当ポートを選択し、<編集>ボタンをクリックすると、下記の画面が表示されます。

2.設定内容を適用する場合は、<適用>ボタン、キャンセルする場合は、<キャンセル>ボタンをクリックしてください。

3) VLAN 設定

Fast Leave 機能が使用されていない場合、MLD グループ Leave メッセージを受信すると、マルチキャストクエリアは GS-query メッセージを送信します。指定のタイムアウト期間内にホストがクエリに応答しない場合にのみ、クエリアはそのグループのトラフィックの転送を停止します。
Fast Leave が有効な場合、スイッチは 1 つのホストのみがポートに接続されていると想定します。したがって、Fast Leaveは、ポートが 1 つの MLD 対応機器にのみ接続されている場合にのみ、ポートを有効にする必要があります。

「設定」→「L3 プロトコル」→「MLDスヌーピング」→「VLAN設定」をクリックすると、以下の画面が表示されます。

1.ポートの設定を変更したい場合は、該当ポートを選択し、<編集>ボタンをクリックすると、下記の画面が表示されます。

2.設定内容を適用する場合は、<適用>ボタン、キャンセルする場合は、<キャンセル>ボタンをクリックしてください。

4) クエリアの設定

MLDクエリアの種類および送信間隔を設定することができます。
MLDクエリアはVLAN内にマルチキャストルータが存在せず，マルチキャストパケットの送信ホストと受信ホストだけが存在する場合、本装置はMLDクエリアのメッセ―ジを代理で受信ホストに対して送信します。

「設定」→「L3 プロトコル」→「MLDスヌーピング」→「クエリアの設定」をクリックすると、以下の画面が表示されます。

1.ポートの設定を変更したい場合は、該当ポートを選択し、<編集>ボタンをクリックすると、下記の画面が表示されます。

2.設定内容を適用する場合は、<適用>ボタン、キャンセルする場合は、<キャンセル>ボタンをクリックしてください。

5) グループリスト

グループ リストには、MLDスヌーピング リストの VLAN ID、グループ IP アドレス、メンバー ポートが表示されます。

「設定」→「L3 プロトコル」→「MLDスヌーピング」→「グループリスト」をクリックすると、以下の画面が表示されます。

❑最新の情報を表示したい場合は、<更新>ボタンをクリックしてください。

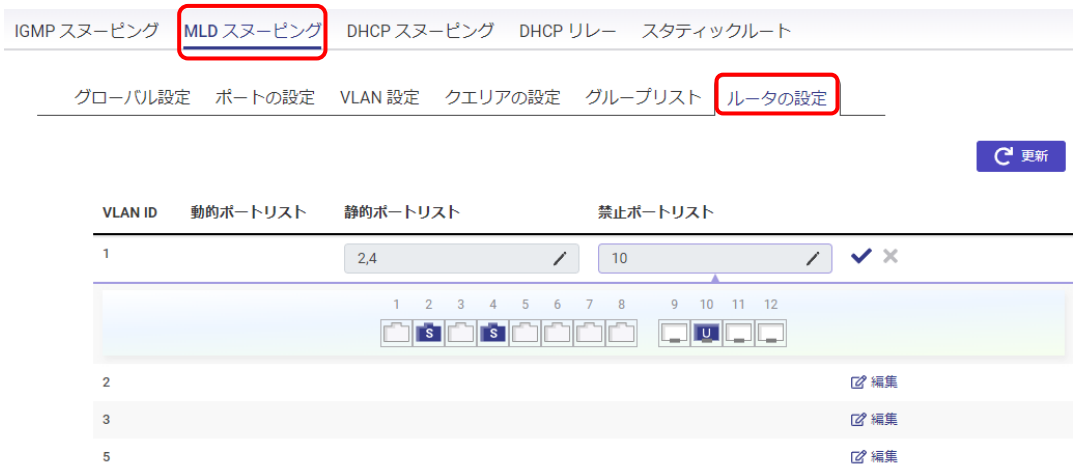
6) ルータの設定

ポートがアクティブで VLAN のメンバーである場合、ルータの設定には、学習したマルチキャストルータの接続されたポートが表示されます。設定する VLAN ID を選択し、設定したい VLAN ID の静的ポートと禁止ポートを入力してください。スヌーピングされたすべてのMLDパケットは、ポートから到達可能なマルチキャストルータに転送されます。

「設定」→「L3 プロトコル」→「MLDスヌーピング」→「ルータの設定」をクリックすると、以下の画面が表示されます。

❑最新の情報を表示したい場合は、<更新>ボタンをクリックしてください。

1.VID ID の設定を変更したい場合は、該当の VID ID を選択して<編集>ボタンをクリックすると、次の画面が表示されます。



2.静的ポートストおび禁止ポートリストにそれぞれ該当ポートを選択して、<更新ボタン>をクリックしてください。

3. DHCP スヌーピング

1) グローバル設定

DHCPスヌーピング機能をグローバルで有効/無効にします。

「設定」→「L3 プロトコル」→「DHCPスヌーピング」→「グローバル設定」をクリックすると、以下の画面が表示されます。

❑設定内容を適用する場合は<適用>ボタン、一括してクリアする場合は<リセット>ボタンをクリックしてください。

2) VLAN 設定

VLAN IDごとに、DHCPスヌーピングの状態を有効/無効にします。

「設定」→「L3 プロトコル」→「DHCPスヌーピング」→「VLAN設定」をクリックすると、以下の画面が表示されます。

1.VLAN ID の設定を変更したい場合は、該当の VLAN ID を選択し、<編集>ボタンをクリックすると、下記の画面が表示されます。

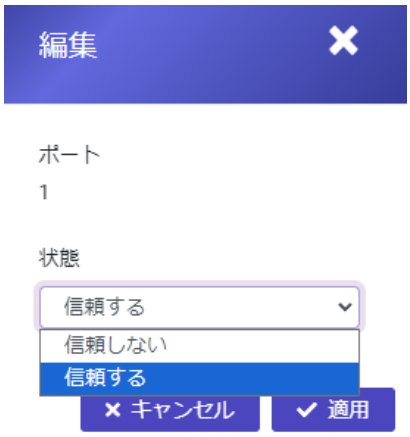
2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容をクリアにします。

3) 信頼するポートの設定

ポートごとに信頼性の有無をそれぞれ設定できます。

「設定」→「L3 プロトコル」→「DHCPスヌーピング」→「信頼するポートの設定」をクリックすると、以下の画面が表示されます。

1.設定したいポートを選択し、<編集>ボタンをクリックしてブリッジ設定を変更してください。



2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容をクリアにします。

4) バインディング

DHCPスヌーピングのバインディングリストが表示されます。

「設定」→「L3 プロトコル」→「DHCPスヌーピング」→「バインディングリスト」をクリックすると、以下の画面が表示されます。

❑最新の情報を表示したい場合は、<更新>ボタンをクリックしてください。

5) IP ソースガード

DHCPスヌーピングのIPソースガードを表示します。
送信元IPアドレス、MACアドレス、着信ポート番号のバインディングをトラッキングすることにより、IPのなりますしを防止します。

「設定」→「L3 プロトコル」→「DHCPスヌーピング」→「IPソースガード」をクリックすると、以下の画面が表示されます。

1.エントリを追加したい場合は、メニュー右上の<追加>ボタンをクリックすると、下記の画面が表示されるので、それぞれ設定を行ってください。

2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容をクリアにします。

6) IPSG ポート

IPSG を有効にすると、DHCP スヌーピングにより許可されたDHCP パケットを除き、インタフェース上で受信したすべての IP トラフィックをブロックします。

「設定」→「L3 プロトコル」→「DHCPスヌーピング」→「IPSGポート」をクリックすると、以下の画面が表示されます。

1.ポートの設定を変更したい場合は、ポートを選択して<編集>ボタンをクリックすると、次の画面が表示されます。

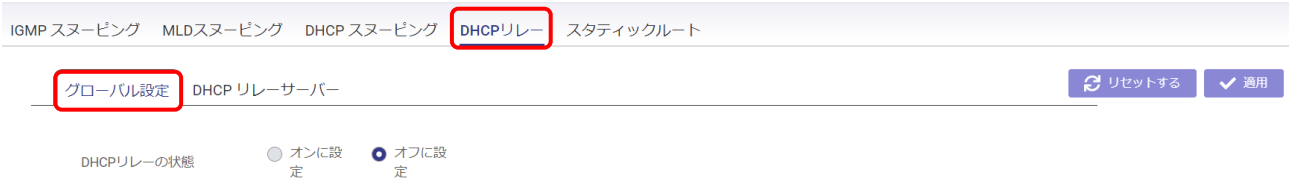
2.設定を変更後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容をクリアにします。

4. DHCP リレー

1) グローバル設定

DHCPリレーをグローバルで有効/無効にします。

「設定」→「L3 プロトコル」→「DHCP リレー」→「グローバル設定」をクリックすると、以下の画面が表示されます。



❑設定を変更後、<適用>ボタンをクリックして変更内容を確定するか、<リセット>ボタンをクリックして変更内容を一括してクリアにすることができます。

2) DHCP リレーサーバ

リレーする DHCPサーバの IP アドレスを指定します。

「設定」→「L3 プロトコル」→「DHCP リレー」→「DHCPリレーサーバ」をクリックすると、以下の画面が表示されます。

1.アドレスを追加したい場合は、メニュー右上の追加>ボタンをクリックすると、下記の画面が表示されるので、それぞれ設定を行ってください。

2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容を一括してクリアにすることができます。

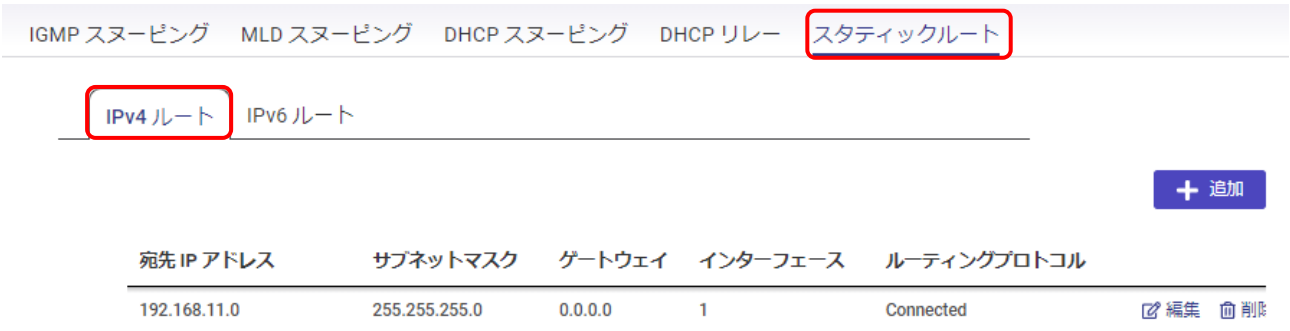
5. スタティック ルート

スタティック ルートは、ネットワーク管理者がルートをルーティング テーブルに設定し、ネットワーク機器が特定の IPv4 または IPv6 ルート/ゲートウェイ経由で宛先ネットワークにパケットを送信するために使用されます。

1) IPv4 ルート

IPv4 ルートを設定します。宛先IPv4アドレスを登録することによって、データの送信先を振り分けることができる機能です

「設定」→「L3 プロトコル」→「スタティックルート」→「IPv4 ルート」をクリックすると、以下の画面が表示されます。



1.エントリを追加/編集したい場合は、画面右上の<追加>ボタンをクリックするか、アドレスを選択して<編集>ボタンをクリックすると、次の画面が表示されます（例:<追加>ボタンをクリックした場合）。

2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容を一括してクリアにすることができます。

2) IPv6 ルート

IPv6 ルートを設定します。宛先IPv6アドレスを登録することによって、データの送信先を振り分けることができる機能です

「設定」→「L3 プロトコル」→「スタティックルート」→「IPv4 ルート」をクリックすると、以下の画面が表示されます。

1.アドレスを追加したい場合は、メニュー右上の<追加>ボタンをクリックすると、下記の画面が表示されるので、それぞれ設定を行ってください。

2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容を一括してクリアにすることができます。

2.3.9 LBD

ループによるシステム パフォーマンスへの影響を軽減するために、LBD メカニズムを有効にして、スイッチがループバック検出パケットを定期的にブロードキャストできるようにすることで、独自の LBD パケットを受信したときにループを検出することができます。

1. グローバル設定

LBD機能をグローバルで有効/無効にします。

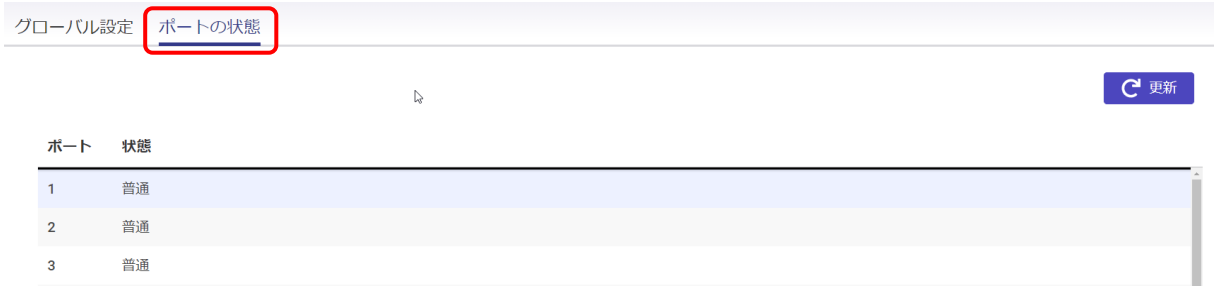
「設定」→「LBD」→「グローバル設定」をクリックすると、以下の画面が表示されます。

❑設定を変更後、<適用>ボタンをクリックして変更内容を確定するか、<リセット>ボタンをクリックして変更内容を一括してクリアにすることができます。

2. ポートの状態

ポートごとに状態を表示します。

「設定」→「LBD」→「ポートの状態」をクリックすると、以下の画面が表示されます。



❑最新の情報を表示したい場合は、<更新>ボタンをクリックしてください。

2.3.10 QoS

パケットに QoS 情報を適用するには、タグ付きイーサネット フレームの VLAN タグ内の 802.1p サービス クラス (CoS) 優先度フィールドと、差別化サービス (DiffServ) コード ポイント (DSCP) の 2 つのオプションがあります。本機の各ポートは、パケット フィールド (802.1p、DSCP、または DSCP+802.1p) のいずれかを信頼するように設定できます。本機のポートに入るパケットも、QoS 情報を伝送しない場合があります。その場合、スイッチは次のノードに送信する前に、そのような情報をパケットに入れます。したがって、ネットワーク内のノード間で QoS 情報が保存され、ノードは各パケットにどのラベルを付けるかを認識します。マッピング テーブルを使用するには、信頼できるフィールドがパケットに存在する必要があります。ポートが untrusted として設定されている場合、<適用>ボタンをクリックして、システムの設定を確定してください。

1. グローバル設定

QoS 機能をグローバルで有効/無効にします。

「設定」→「QoS」→「グローバル設定」をクリックすると、以下の画面が表示されます。

メニュー	説明
状態	本機の QoS を有効/無効を選択します。
スケジューリング方法	Strict Priority または WRR を選択して、トラフィックのスケジューリング方法を指定します。 ・Strict Priority: キューの優先度に厳密に基づいてトラフィックのスケジューリングを指定します。 ・WRR: Weighted Round-Robin (WRR) アルゴリズムを使用して、優先度の高いサービス クラスでパケットを処理します。キューに WRR 重みを割り当てます。
信頼モード	スイッチに入るパケットを分類するために使用するパケット フィールドを選択します。 ・DSCP: DSCP (Differentiated Services Code Point) タグ値に基づいてトラフィックを分類します。 ・802.1p: 802.1p に基づいてトラフィックを分類します。IEEE 802.1p で指定されている 8 つのプライオリティ タグは、1 ～ 8 です。

❑各項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<リセット>ボタンをクリックして変更内容を一括してクリアにすることができます。

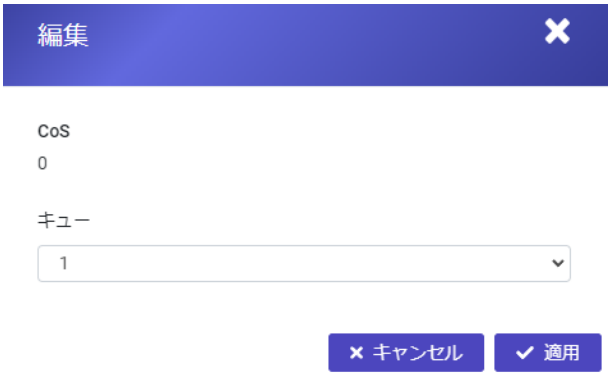
2. CoS レベル

サービスクラス (CoS) マッピング機能を使用して、対応する CoS 値にマッピングする内部トラフィック クラスを指定します。CoS を使用すると、輻輳によってトラフィックがバッファリングされたときに、どのデータ パケットの優先度を高くするかを指定できます。

「設定」→「QoS」→「CoSマッピング」をクリックすると、以下の画面が表示されます。

メニュー	説明
CoS	CoS プライオリティ タグの値を表示します（0 :最低、7:最高）。
キュー	「CoS プライオリティ タグ」ボックスをオンにして、提供されたフィールドで各 CoS 値のキュー値を選択します。8 つのトラフィック プライオリティ キューがサポートされており、フィールド値は 1 ～ 8 です（1:最低のプライオリティ、8:最高のプライオリティ）。

1.CoS のキューの設定を変更したい場合、該当の CoS を選択して<編集>ボタンをクリックすると、次の画面が表示されます。



2.設定内容を適用する場合は、<適用>ボタン、キャンセルする場合は、<キャンセル>ボタンをクリックしてください。

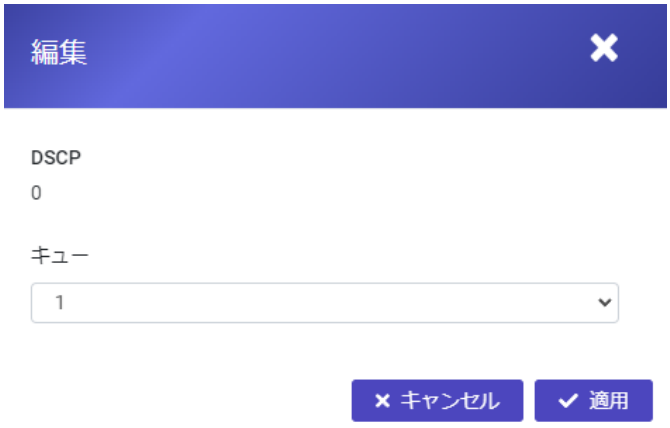
3. DSCP について

DSCP(Differentiated Services Code Point)のマッピング機能を使用して、対応する DSCP 値にマッピングする内部トラフィック クラスを指定します。DSCP マッピングは、優先度付けのために IP パケットのビットを再割り当てすることにより、設定可能な優先レベルの数を増やします。

「設定」→「QoS」→「DSCPマッピング」をクリックすると、以下の画面が表示されます。

メニュー	説明
DSCP	パケットの DSCP 値を表示します。0 が最低で 10 が最高です。
列	「CoS プライオリティ タグ」ボックスをオンにして、表示されたフィールドで各 DSCP のキュー値を選択します。8 つのトラフィック プライオリティ キューがサポートされており、フィールド値は 1 ～ 8 です(「1」:最低のプライオリティ～「8」:最高のプライオリティ)。

1.CoS のキューの設定を変更したい場合、該当の CoS を選択して<編集>ボタンをクリックすると、次の画面が表示されます



2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容を一括してクリアにすることができます。

4. ポート CoS

本機の QoS ポートを設定できます。設定するポートを選択し、ドロップダウン ボックスから CoS 値を選択します。次に、信頼設定を有効/無効にして、すべての CoS パケットが入力時にマークされるようにします。

「設定」→「QoS」→「ポートCoS」をクリックすると、以下の画面が表示されます。

メニュー	説明
ポート	CoS パラメータが設定されているポートを表示します。
CoS 値	CoS プライオリティのタグの値を選択します（0 :最低、7:最高）。
信頼	受信時にすべての CoS パケット マーキングを信頼する場合は、「オン」 を選択します。入力時の CoS パケット マーキングを信頼しない場合は、「オフ」 を選択します。

1.CoS のキューの設定を変更したい場合、該当の CoS を選択して<編集>ボタンをクリックすると、次の画面が表示されます

2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容を一括してクリアにすることができます。

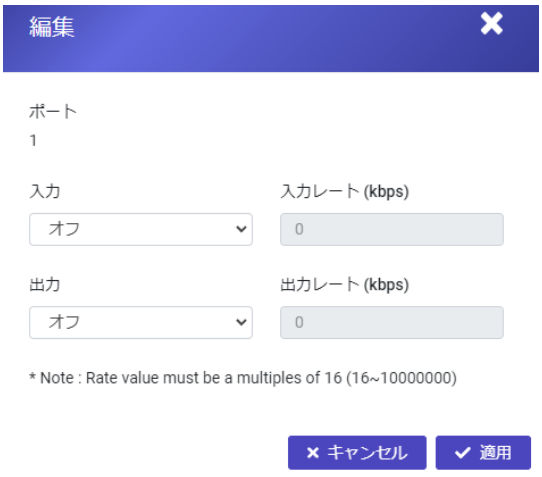
5. 帯域幅制御

帯域幅制御機能を使用すると、指定したポートの入力レート制限と出力レートの帯域幅を設定できます。

「設定」→「QoS」→「帯域幅制御」をクリックすると、以下の画面が表示されます。

メニュー	説明
ポート	帯域幅設定が表示されているポートを表示します。
入力	インタフェースでの入力の有効化/無効化を選択します。
入力レート(kbps)	イングレス レートをキロビット/秒で入力してください。ギガビット イーサネット ポートの最大速度は 1000000 キロビット/秒です。
出力	インタフェースでの出力の有効化/無効化を選択します。
出力レート(kbps)	エグレス レートをキロビット/秒で入力してください。ギガビット イーサネット ポートの最大速度は 1000000 キロビット/秒です。

1.ポートの設定を変更したい場合、該当のポートを選択して<編集>ボタンをクリックすると、次の画面が表示されます



2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容を一括してクリアにすることができます。

6. ストーム 制御

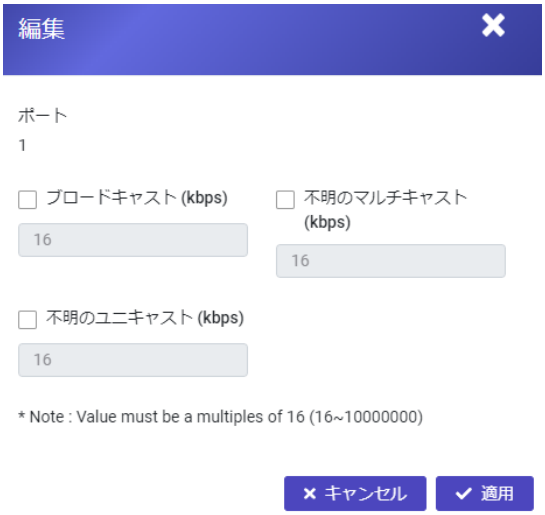
ストーム コントロールは、スイッチが受け入れて転送するブロードキャスト、不明のマルチキャスト、および不明のユニキャスト フレームの量を制限します。ストーム コントロールは、パケット タイプとパケットの送信レートを設定することで、ポートごとに有効にできます。スイッチは、受信ブロードキャスト、不明のマルチキャスト、および不明のユニキャスト フレーム レートをポートごとに個別に測定し、レートがユーザにより設定されたレートを超えるとフレームを破棄します。

【注記】:値は 16 の倍数 (16~10000000)で設定してください。

「設定」→「QoS」→「ストーム制御」をクリックすると、以下の画面が表示されます。

メニュー	説明
ポート	ストーム コントロール情報が表示されるポートを表示します。
ブロードキャスト	ブロードキャスト レートをキロビット/秒で入力してください。ギガビット イーサネット ポートの最大速度は 1000000 キロビット/秒です。 インタフェースのブロードキャスト トラフィックの入力レートが設定されたしきい値を超えて増加すると、トラフィックはドロップされます。
不明のマルチキャスト	不明のマルチキャストレートをキロビット/秒で入力してください。ギガビット イーサネット ポートの最大速度は 1000000 キロビット/秒です。 インタフェースのブロードキャスト トラフィックの入力レートが設定されたしきい値を超えて増加すると、トラフィックはドロップされます。
不明なユニキャスト	不明のユニキャスト レートをキロビット/秒で入力してください。ギガビット イーサネット ポートの最大速度は 1000000 キロビット/秒です。インタフェースのブロードキャスト トラフィックの入力レートが設定されたしきい値を超えて増加すると、トラフィックはドロップされます。

1.ポートの設定を変更したい場合、該当のポートを選択して<編集>ボタンをクリックすると、次の画面が表示されます。



2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容を一括してクリアにすることができます。

7. アドバンストモード

詳細モードでは、ユーザは一致基準をさらにカスタマイズして、着信トラフィックに QoS を適用できます。スイッチは、次のノードに送信する前に、そのような情報をパケットに入れます。

「設定」→「QoS」→「アドバンスモード」をクリックすると、以下の画面が表示されます。

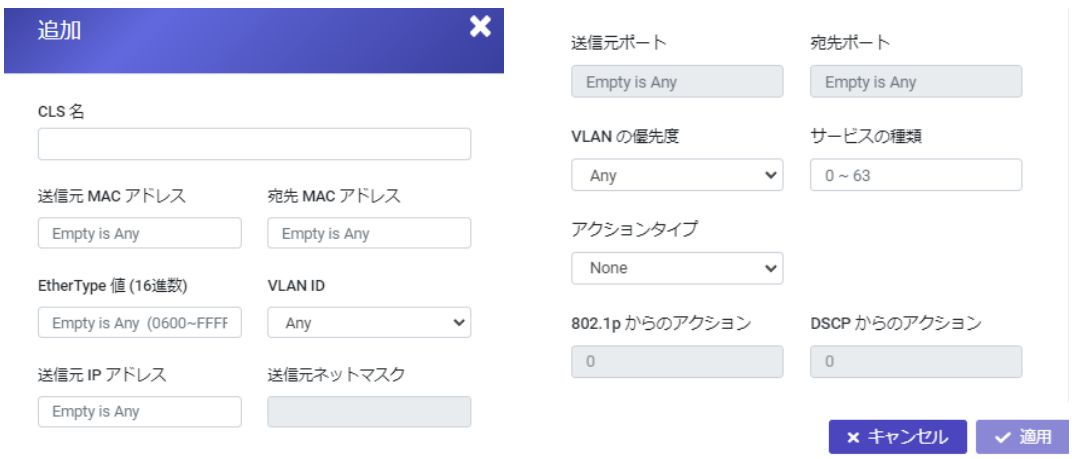
1) クラスマッピング

このメニュー上で、QoS のクラスマッピングを[illegible]および設定可能です。
「設定」→「QoS」→「クラスマッピング」をクリックすると、以下の画面が表示されます。

❑画面右側の設定（ ••• ）をクリックすると、以下のようにメニューが表示されるため、表示したい項目を選択してください。

メニュー	説明
CLS名	QoS マッピングのクラスのポリシー名を入力してください。
状態	クラスマッピング ポリシーのステータスを表示します。
送信元 MACアドレス	送信元 MACアドレスを入力してください。
送信元 IP アドレス	送信元IP アドレスを入力してください。
送信元 IP アドレス マスク	送信元IP アドレスのマスクを入力してください。
送信元 ポート	送信元ポートを入力してください。
宛先 MACアドレス	宛先 MACアドレスを入力してください。
宛先 IP アドレス	宛先 IP アドレスを入力してください。
宛先 IP アドレス マスク	宛先 IP アドレスのマスクを入力してください。
宛先ポート	宛先ポートを入力してください。
EtherType値(16進数)	フレームが運んでいるデータの種類を表す2バイト（16ビット）の値を入力してください。
VLAN ID	ドロップダウンリストから、VLAN ID を選択します。
VLANの優先度	ドロップダウンリストから、VLAN 優先度を選択します。
プロトコル	リストまたは ID からプロトコルを選択します。
DSCP	「サービスの種類」に DSCP を入力してください(有効範囲: 0 ～ 63 です。
ICMP	リストから選択したICMPのタイプが表示されます。(Echo Reply, Destination Unreachable, Source Quench, Echo Request, Router Advertisement, Router Solicitation, Time Exceeded, Timestamp, Timestamp Reply, Traceroute)
ICMPコード	0～255のICMPコードが出力されます。
アクションタイプ	「802.1p 設定」または「DSCP 設定」のいずれかを、対応するフィールドで指定の値とともに選択して、QoS クラスマッピングを適用します。

1.エントリを追加したい場合は、メニュー右上の追加>ボタンをクリックすると、下記の画面が表示されるので、それぞれ設定を行ってください。

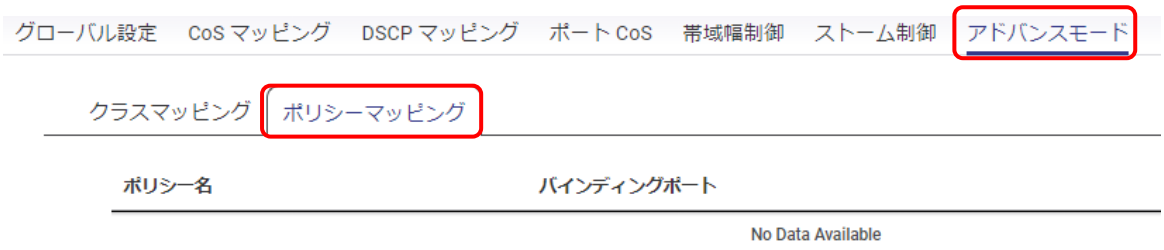


2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容を一括してクリアにすることができます。

2) ポリシーマッピング

外部ボリュームのマッピングに必要な情報をまとめた設定一覧のことです。
マッピングポリシーを事前に設定しておくことで、マッピング時の設定が容易になります。

「設定」→「QoS」→「アドバンスモード」→「ポリシーマッピング」をクリックすると、以下の画面が表示されます。



メニュー	説明
ポリシー名	クラスマッピングで設定されたクラスマッピング ポリシーを表示します。
ポートのバインド	本機のポート番号を入力して、QoS のマッピング ポリシーをバインドします。

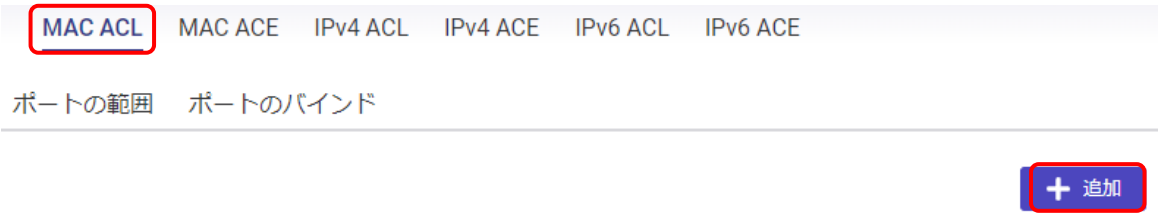
2.3.11 アクセス制御

ACL(アクセス制御リスト)は、分類ルールを設定したり基準を確立することにより、許可されていないユーザをブロックし、許可されたユーザのみ特定の領域またはリソースにアクセスできるようにすることで、ネットワークにセキュリティを提供できます。ACL は、スイッチ ポートでパケットを転送するかブロックするかを制御することで、ネットワークへのアクセスに基本的なセキュリティを提供できます。
ACLは、送信元アドレス、宛先アドレス、送信元ポート番号、宛先ポート番号など、パケットのヘッダの内容に従ってデータ パケットを分類できるフィルタです。パケット分類子は、より効率的な処理のためにフローを識別します。各フィルタは、一致する必要のある条件を設定します。ACLは、IP フレームのパケットのフィルタリングを提供します (プロトコルに基づいて、TCP/UDP ポート番号またはフレームタイプ) またはレイヤー2のフレーム (ユニキャスト、ブロードキャスト、またはマルチキャストの宛先 MACアドレスに基づくか、VLAN ID または VLAN タグの優先度に基づく)。ACL を使用すると、不要なネットワーク トラフィックをブロックしてパフォーマンスを向上させたり、特定のネットワーク リソースまたはプロトコルへのアクセスを制限してセキュリティ制御を実装したりできます。ポリシーを使用して、クライアント ポート、サーバ ポート、ネットワーク ポート、またはゲスト ポートのサービスを区別できます。また、特定のポートの送信元 MAC と送信元 IP アドレスに一致する受信フレームのみを許可することで、ネットワーク トラフィックを厳密に制御するためにも使用できます。ACL は、トラフィックの分類を決定するルールである ACE(アクセス制御エントリ) で設定されます。
ACEは単一のルールとみなされ、ACLに登録します。ACLは最大256個作成することができ、各ポートにバインドします。ACL は、トラフィック フロー制御の提供、ルーティング アップデートの内容の制限、転送またはブロックされるトラフィックのタイプの決定に使用されます。
この基準は、MACアドレスまたは IP アドレスベースで指定できます。

1. MAC ACL

現在設定されている MAC ベースの ACL プロファイルが表示されます。

「設定」→「アクセス制御」→「MAC ACL」をクリックすると、以下の画面が表示されます。



メニュー	説明
インデックス	プロファイル識別子を表示します。
名前	MAC ベースの ACL 名を入力してください。 最大 32 文字の英数字を使用できます。

1.エントリを追加したい場合は、メニュー右上の追加>ボタンをクリックすると、下記の画面が表示されます。

2.項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容をクリアにします。

2. MAC ACE

現在設定されている MAC ベースの ACEプロファイルを表示します。

「設定」→「アクセス制御」→「MAC ACE」をクリックすると、以下の画面が表示されます。

❑画面右側の設 •••)をクリックすると、以下のようにメニューが表示されるため、表示したい項目を選択してください。

メニュー	説明
ACL 名	リストから ACL を選択します。
シーケンス	選択したインタフェースに割り当てられた他の ACL に対して指定された ACL の順序を示すシーケンス番号を入力してください(有効な範囲:1 ～ 2147483647)。 ※1 から順に処理されます。
アクション	パケットが基準に一致した場合に実行するアクションを選択します。 ・Permit: ACE 基準を満たすパケットを転送します。 ・Deny: ACE 基準を満たすパケットをドロップします。
宛先 MACアドレス	宛先 MACアドレスを入力してください。
宛先 MACアドレスマスク	宛先 MACアドレスの MACアドレスマスクを入力してください。 ”00:00:00:00:00:00” のマスクは、ビットが正確に一致する必要があることを意味します。 ・”ff:ff:ff:ff:ff:ff” は、ビットが無関係であることを意味します。 ・”0”と”f” の任意の組み合わせを使用できます。
送信元MAC 値	送信元 MACアドレスを入力してください。
送信元 アドレスマスク	送信元 MACアドレスの MACアドレス マスクを入力してください。 00:00:00:00:00:00 のマスクは、ビットが正確に一致する必要があることを意味します。 ・ff:ff:ff:ff:ff:ff は、ビットが無関係であることを意味します。 ・“0” と”f” の任意の組み合わせを使用できます。
VLAN ID	MAC ACE に MACアドレスが付加されている VLAN ID を入力してください(有効範囲:1 ～ 4094)。
802.1p 値	802.1p 値を入力してください(有効範囲:0 ～ 7)。

EtherType	このオプションを選択すると、各フレームのヘッダのイーサネット タイプの値を調べるようにスイッチに指示します。このオプションは、Ethernet II フォーマットのパケットをフィルタリングするためにのみ使用できます。イーサネット プロトコル タイプの詳細なリストは、RFC 1060 にあります。 一般的なタイプには、0800 (IP)、0806 (ARP)、8137 (IPX) などがあります。

1.<追加>ボタンをクリックして、新しい MAC ACE ルールを追加してください。

2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容をクリアにします。

3. IPv4 ACL

現在設定されている IPv4ベースの ACL プロファイルを表示します。

「設定」→「アクセス制御」→「IPv4 ACL」をクリックすると、以下の画面が表示されます。

メニュー	説明
インデックス	ACL の現在の数を表示します。
名前	IPv4 ベースの ACL 名を入力してください。 最大 32 文字の英数字を使用できます。

1.エントリを追加したい場合は、<追加>ボタンをクリックすると次の画面が表示されるため、設定を追加してください。

2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容をクリアにします。

4. IPv4 ACE

このメニュー上で、ルールを表示し、IPv4 ベースの ACE に追加してください。

「設定」→「アクセス制御」→「IPv4 ACE」をクリックすると、以下の画面が表示されます。

❑画面右側の設定(•••)をクリックすると、以下のようにメニューが表示されるため、表示したい項目を選択してください。

メニュー	説明
ACL 名	ルールを作成するリストから ACL を選択します。
シーケンス	選択したインタフェースに割り当てられた他の ACL に対して指定された ACL の順序を示すシーケンス番号を入力してください(有効な範囲:1 ～ 2147483647)。 ※1 から順に処理されます。
アクション	パケットが基準に一致した場合に実行するアクションを選択します。 ・Permit: ACL 基準を満たすパケットを転送します。 ・Deny: ACL 基準を満たすパケットをドロップします。
プロトコル	ドロップダウンメニューで「任意」、「プロトコル ID」、または「リストから選択」を選択します。 ・任意: 任意のプロトコルを使用するには、「任意」をオンにします。 ・プロトコル ID: パケットが一致する ACE のプロトコルを入力してください。 ・リストから選択: 指定されたフィールドのリストからプロトコルを選択します。 ・ICMP:インターネット制御メッセージ プロトコル (ICMP)。ICMP は、ゲートウェイまたは宛先ホストがソース ホストと通信できるようにします。 ・IPinIP : IP in IP は、IP パケットをカプセル化して、2 つのルータ間にトンネルを設定ます。これにより、IP トンネル内の IP が、複数の個別のインタフェースではなく、単一のインタフェースとして表示されるようになります。 ・TCP:伝送制御プロトコル (TCP)。2 つのホストが通信し、データ ストリームを交換できるようにします。TCP は、パケットの配信を保証し、パケットが送信された順序で送受信されることを保証します。 ・EGP: 外部ゲートウェイ プロトコル (EGP)。自律システム ネットワーク内の 2 つの隣接するゲートウェイ ホスト間でルーティング情報を交換できるようにします。 ・IGP:内部ゲートウェイ プロトコル (IGP)。自律ネットワーク内のゲートウェイ間のルーティング情報交換を有効にします。 ・UDP:ユーザ データグラム プロトコル (UDP)。UDP は、パケットを送信する通信プロトコルですが、配信を保証するものではありません。

	・HMP:ホスト マッピング プロトコル (HMP) は、さまざまなネットワーク ホストからネットワーク情報を収集します。HMP は、単一ネットワーク内のホストだけでなく、インターネット上に広がるホストもモニタリングします。 ・RDP:信頼できるデータ プロトコル (RDP)。パケットベースのアプリケーションに信頼性の高いデータ転送サービスを提供します。 ・IPv6:パケットを IPv6 プロトコルに一致させます。 ・IPv6 Rout: IPv6 のルーティングヘッダ ・IPv6 Frag: IPv6 のフラグメントヘッダ ・RVSP:パケットを ReSerVation Protocol (RSVP) に一致させます。 ・IPv6 ICMP: Internet Control Message Protocol (ICMP) により、ゲートウェイまたは宛先ホストがソース ホストと通信可能になります。 ・OSPF: Open Shortest Path First (OSPF) プロトコルは、ネットワーク ルーティングレイヤー2 (2) トンネリング プロトコル用のリンクステート階層型内部ゲートウェイ プロトコル (IGP) です。これは、ISP が仮想プライベート ネットワーク (VPN) を操作できるようにする PPP プロトコルの拡張機能です。 ・PIM:パケットを Protocol Independent Multicast (PIM) に一致させます。 ・L2TP:パケットをインターネット プロトコル (L2IP) に一致させます。
宛先IPアドレス	宛先 IP アドレスを入力してください。
宛先ネットマスク	宛先 IP アドレスのマスクを入力してください。
宛先ポート範囲	宛先ポート範囲を入力してください。
送信元IP アドレスの値	送信元IP アドレスを入力してください。
送信元ネットマスク	送信元IP アドレスのマスクを入力してください。
送信元ポート範囲	送信元ポート範囲を入力してください。
フラグセット	6 つのTCP制御フラグをそれぞれ処理するかどうかをドロップダウン メニューから選択します。 ・URG (緊急フラグ)、ACK (応答確認フラグ)、PSH (転送強制フラグ)、RST (リセットフラグ)、SYN (同期フラグ)、および FIN (転送終了フラグ) ・Don't Care: ACE：TCP 制御フラグを処理しません。 ・設定: TCP 制御フラグが設定されているパケットは条件に一致します。 ・Unset: TCP 制御フラグが設定されていないパケットが条件に一致します。

❑エントリ を追加するには、「追加」をクリックして、新しい AC の名前を入力してください。
それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容を一括してクリアにすることができます。

5. IPv6 ACL

現在定義されている IPv6 ベースの ACL プロファイルを表示します。

「設定」→「アクセス制御」→「IPv6 ACL」をクリックすると、以下の画面が表示されます。

メニュー	説明
インデックス	ACL の現在の数を表示します。
名前	IPv6 ベースの ACL 名を入力してください。最大 32 文字の英数字を使用できます。

1.新しい ACL を追加するには、「追加」をクリックして、新しい ACL の名前を入力してください。

2.名前を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容を一括してクリアにすることができます。

6. IPv6 ACE

このメニュー上でルールを表示し、IPv6 ベースの ACE に追加してください。

「設定」→「アクセス制御」→「IPv6 ACE」をクリックすると、以下の画面が表示されます。

❑画面右側の設定（•••）をクリックすると、以下のようにメニューが表示されるため、表示したい項目を選択してください。

メニュー	説明
ACL 名	リストから ACL を選択します。
シーケンス	選択したインタフェースに割り当てられた他の ACL に対して指定された ACL の順序を示すシーケンス番号を入力してください（有効な範囲は 1 ～ 2147483647）。 ※1 から順番に処理されます。
アクション	パケットが基準に一致した場合に実行するアクションを選択します。 ・Permit: ACE 基準を満たすパケットを転送します。 ・Deny: ACE 基準を満たすパケットをドロップします。
MACタイプ	ドロップダウン メニューから「Any」、「Protocol ID」、または「Select from List」を選択します。 ・プロトコル ID: パケットが一致する ACE のプロトコルを入力してください。 ・リストから選択: 提供されたフィールドのリストからプロトコルを選択します。
送信元MACアドレス	送信元MACアドレスを入力してください。
送信元 アドレスマスク	送信元 MACアドレスの MACアドレス マスクを入力してください。00:00:00:00:00:00 のマスクは、ビットが正確に一致する必要があることを意味します。 ・ff:ff:ff:ff:ff:ff は、ビットが無関係であることを意味します。 ・“0” と”f” の任意の組み合わせを使用できます。
IPアドレス	IP アドレスを入力してください。
送信元IPアドレス	送信元IP アドレスを入力してください。
宛先IPv6のプレフィックスの長さ	宛先 IP アドレスのプレフィックス長を入力してください(有効範囲:0 ～ 128)。
宛先ポート範囲	リストから任意または範囲を選択します。パケットに一致する宛先ポートを入力してください(有効範囲:0 ～ 65535)。
送信元IPv6	送信元IPv6アドレスを入力してください。
送信元IPv6のプレフィックスの長さ	新しい送信元 IPv6アドレスのプレフィックス長を入力してください(有効範囲:0 ～ 128)。
送信元ポート範囲	リストから任意または範囲を選択します。パケットに一致する送信元ポートを入力してください(有効範囲:0 ～ 65535)。
フラグセット	6 つの TCP 制御フラグをそれぞれ処理するかどうかを選択します。ドロップダウン メニューから URG (緊急)、ACK (承認)、PSH (プッシュ)、RST (リセット)、SYN (同期)、および FIN (フィン)。 ・Don't Care: ACE は TCP 制御フラグを処理しません。 ・設定: TCP 制御フラグが設定されているパケットは条件に一致します。 ・Unset: TCP 制御フラグが設定されていないパケットが条件に一致します。
DSCP	照合する DSCP を選択した場合は、DSCPの値 を入力してください(有効範囲:0 ～ 63 です。
ICMP	ドロップダウンメニューから「任意」、「プロトコル ID」、または「リストから選択」を選択します。 ・プロトコル ID:パケットが一致する ACE のプロトコルを入力してください(有効範囲:0 ～ 255)。 ・リストから選択:指定されたフィールドのリストから ICMP を選択します。
ICMP コード	ドロップダウン メニューから「任意」または「ユーザ定義」を選択します。 User Defined を選択した場合は、ICMP コードの値を入力してください(有

	効範囲:0 ～ 255)。

❑<追加>ボタンをクリックして、新しい IPv6 ACE ルールを追加してください。

7. ポート範囲

指定したポート範囲を設定します。

「設定」→「アクセス制御」→「ポート範囲」をクリックすると、以下の画面が表示されます。

1.ポート範囲を追加したい場合は、<追加>ボタンをクリックして設定内容を記入してください。

2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容を一括してクリアにすることができます。

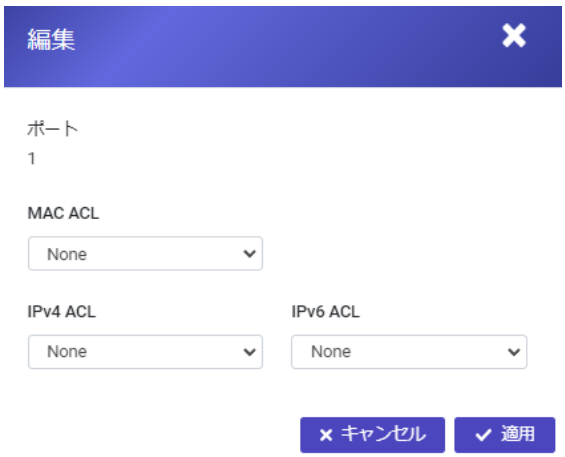
8. ポートのバインド

ACL がインタフェースにバインドされると、ACL に定義されているすべてのルールがそのインタフェースに適用されます。ACL がポートまたは LAG に割り当てられると、ACL に一致しない入力または出力インタフェースからのフローは、一致しないパケットをドロップするデフォルトのルールに一致します。
ACL をインタフェースにバインドするには、インタフェースを選択し、バインドする ACL を選択するのみです。

「設定」→「アクセス制御」→「ポートのバインド」をクリックすると、以下の画面が表示されます。

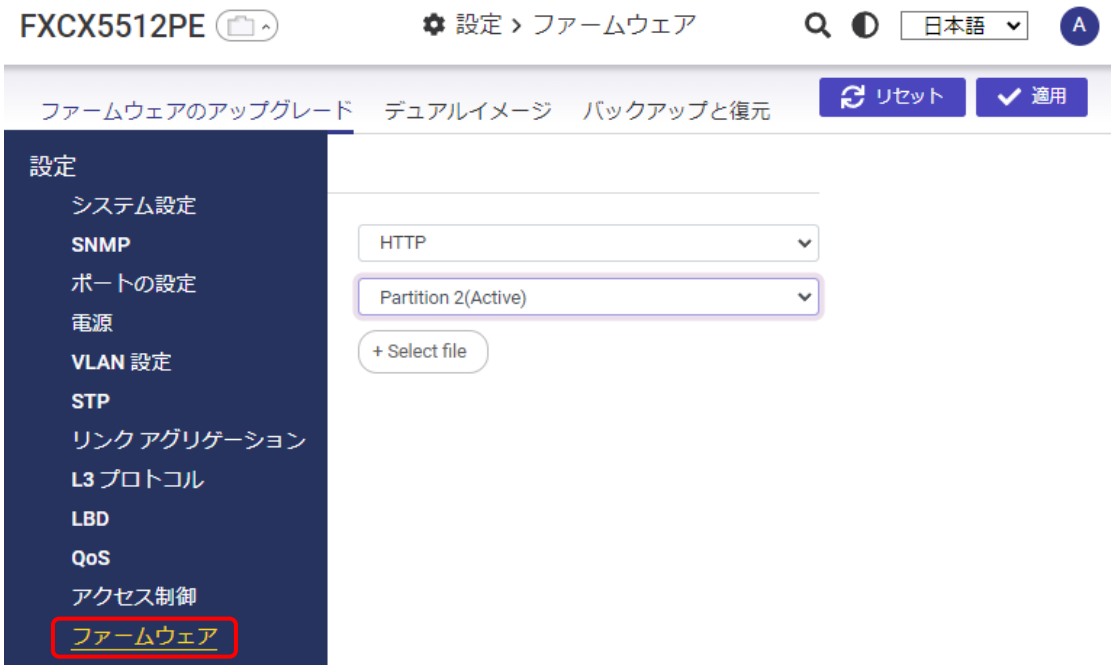
メニュー	説明
ポート	ACL がバインドされるポートを選択します。
MAC ACL	ポートに適用する MAC ACL ルールを選択します。
IPv4 ACL	ポートに適用する IPv4 ACL ルールを選択します。
IPv6 ACL	ポートに適用する IPv6 ACL ルールを選択します。

1.設定内容を編集したい場合は、該当ポートを選択し、<編集>ボタンをクリックして設定項目を入力してください。



2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容を一括してクリアにすることができます。

2.3.12 ファームウェア



1. ファームウェアのアップグレード

「設定」→「ファームウェアのアップグレード」をクリックすると、以下の画面が表示されます。

この手順に従って、ファームウェアをアップグレードしてください。

1. アップグレート方法(HTTP または TFTP のいずれか)を選択します。

2. パーティション（Active または Backup のいずれか）を選択します。

3. アップグレードの方法に応じて、以下の手順に従ってください。

1) HTTP の場合:

<+Select file>ボタンをクリックしてファイルを参照して、新しいファームウェアを選択すると、
次の画面が表示されます。

2) TFTP の場合:

TFTPサーバとファイル名をそれぞれ入力して、<適用>ボタンをクリックすることにより、ファームウェアのアップグレードを完了します。

【警告】:
設定情報の損失を防ぐために、アップグレードする前に設定をバックアップしてください。

【注記】:
アップグレード プロセスが完了するまでに数分かかる場合があります。ファームウェアをアップグレードした後、ブラウザのキャッシュをクリアすることをお勧めします。

2. デュアルイメージ

スイッチのイメージの 2 つのバージョンをFLASHメモリに保持します。1 つのイメージがアクティブイメージ、2 番目のイメージがバックアップイメージです。デュアルイメージ画面では、次回のリセット後にどのパーティションをアクティブに設定するかを選択できます。
スイッチは、まずアクティブイメージを起動して動作し、アクティブなイメージが破損している場合、バックアップイメージが自動的に起動されます。

メニュー	説明
有効	アクティブにしたいパーティションを選択します。
Flashパーティション	パーティションの番号を表示します。
状態	本機の現在のパーティションの状態を表示します。
イメージ名	イメージの名前/バージョン番号を表示します。
イメージサイズ(バイト)	イメージファイルのサイズを表示します。
作成時刻	イメージが作成された時間を表示します。

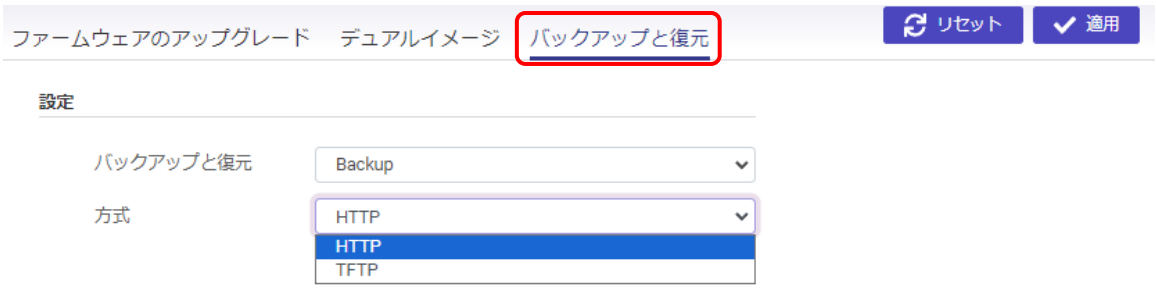
❑各項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<リセット>ボタンをクリックして変更内容を一括してクリアにすることができます。

3. バックアップと復元

この機能は、現在の設定をTFTPサーバ上のフォルダに保存するため、またはローカルドライブまたは

TFTPサーバからのconfigファイルを使用して、元の設定に戻すために使用します。

「設定」→「ファームウェア」→「バックアップと復元」をクリックすると、以下の画面が表示されます。



❑<適用>ボタンをクリックして、config の設定を TFTP サーバ上のフォルダにダウンロードするか、以前に保存した config ファイルをシステムにアップロードします。

2.4 解析

ネットワークや装置の負荷をかけずにログ情報や診断ツールを介してモニタリングしたり、解析することができます。

「設定」→「解析」をクリックすると、以下の画面が表示されます。

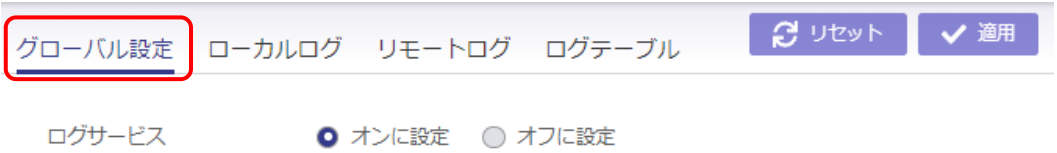
2.4.1 ログ

Syslog プロトコルを使用すると、プラットフォームで発生するイベント、障害、またはエラー、および設定の変更やその他の発生に応答して、IP ネットワークを介して syslog サーバにイベント通知メッセージを送信できます。その後、イベント メッセージを収集し、ユーザがネットワーク操作をモニタリングして誤動作を診断するための強力なサポートを提供します。
Syslog 対応機器は、syslog メッセージを生成し、それを Syslog サーバに送信できます。
Syslog は RFC 3164 で定義されています。RFC は、Syslog メッセージのパケット形式、内容、およびシステム ログ関連の情報を定義しています。各 Syslog メッセージには、ファシリティと重大度レベルがあります。Syslog 機能は、Syslog サーバ内のファイルを識別します。
詳細については、Syslog プログラムのドキュメントを参照してください。

1. グローバル設定

ログ設定をグローバルで「有効」または「無効」を選択できます。

「設定」→「解析」→「ログ」→「グローバル設定」をクリックすると、以下の画面が表示されます。

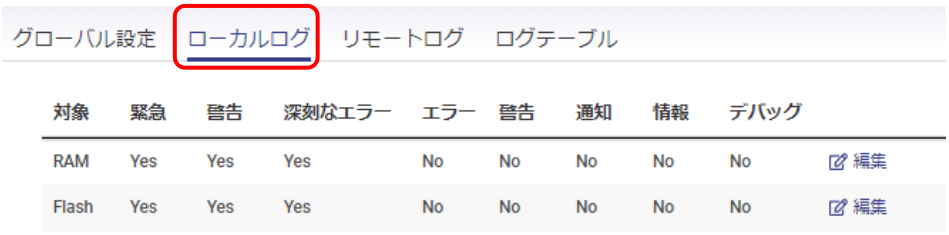


❑それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<リセット>ボタンをクリックして変更を破棄してください。

2. ローカルログ

ローカルデバイスのRAM ログおよびフラッシュログの重大度のレベルを設定できます。

「設定」→「解析」→「ログ」→「ローカルログ」をクリックすると、以下の画面が表示されます。



次の表に、Syslog の重要度レベルを表します。

コード	重大度	説明	概要
0	EMERG	システムは利用不可の状態	通常、複数のアプリ/ サーバ/サイトに影響を与える「パニック」状態。このレベルは、オンコールのすべての技術スタッフに通知されます。
1	ALERT	直ちに対処する必要あり	直ちに修正する必要があります。担当者に直ちに通知してください。たとえば、プライマリ ISP の接続不良の可能性があります。
2	CRITICAL	危機的状況	直ちに修正する必要がありますが、セカンダリシステムの障害を示しています。たとえば、バックアップ ISPの 接続不良の可能性があります。
3	ERROR	エラー状態	開発者または管理者に中継する必要のある緊急ではない障害。各項目は、指定された時間内に解決する必要があります。
4	WARNING	警告条件	重大なエラーではなく、アクションを実行しないとエラーが発生することを示す警告メッセージ (例: ファイルシステムが 85% フル)。各項目は、指定された時間内に解決する必要があります。
5	NOTICE	特筆すべき事項	異常ではあるがエラー状態ではないイベント: 潜在的な問題を特定するために、開発者または管理者へメールで通知される場合があります。 直ちに対応する必要はありません。
6	INFO	情報メッセージ	通常の運用メッセージ: レポート、スループットの測定などのために収集される可能性があります。 特に対応する必要はありません。
7	DEBUG	デバッグメッセージ	デバッグ用の情報を含むメッセージ。

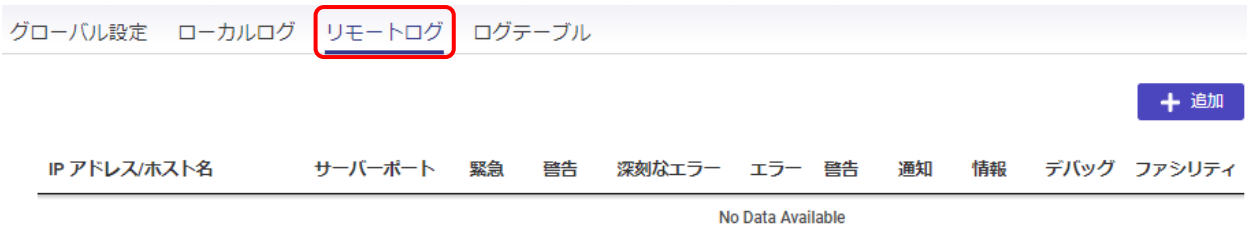
1.<編集>ボタン をクリックして、RAM またはフラッシュ 宛先の変更をそれぞれ適用します。

2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容を一括してクリアにすることができます。

3. リモートログ

本機の内部ログの容量は固定されています。
最新のエントリのスペースを確保するために、古い順からエントリが削除されるため、すべてのログの記録を永続的に保存する必要がある場合は、syslogサーバを本機からログの内容を受信するように設定することにより、すべてのログ情報を syslogサーバに送信します。
Syslog の重大度レベルについては、前項の「2.ローカルログ」を参照して下さい。

「解析する」→「ログ」→「リモートログ」をクリックすると、以下の画面が表示されます。



1.<追加>ボタンをクリックして、syslog ログ用のリモート サーバを追加してください。

2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容を一括してクリアにすることができます。

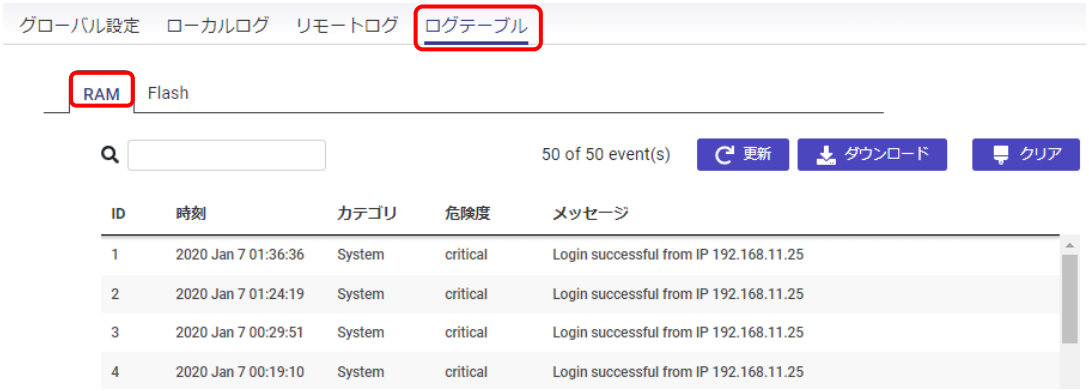
4. ログテーブル

本機の内部ログの最新の記録が表示されます。ログエントリは新しい順に一覧表示されます (最新のログが一覧の一番上に表示されます)。
ヘッダをクリックすると、そのカテゴリでコンテンツをソートすることができます。

「解析する」→「ログ」→「ログテーブル」をクリックすると、以下の画面が表示されます。

1) RAM

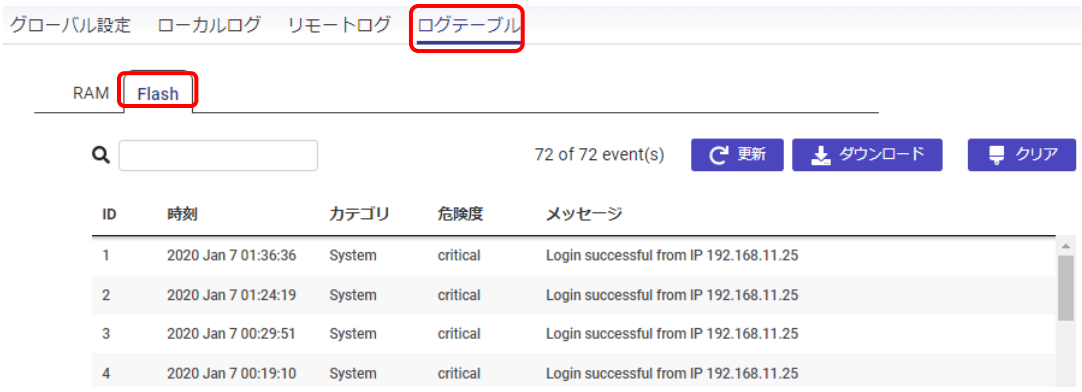
システムの RAM ログに保存されている情報は、本機を再起動したり、電源を切ると失われます。



1. ダウンロード>ボタンをクリックすると、現在のバッファリングされたログが .txt ファイルにエクスポートされます。
2. <クリア>ボタンをクリックすると、システムのメモリにバッファリングされたログがクリアされます。
3. <更新>ボタンをクリックすると、最新情報が表示されます。

2) Flash

フラッシュ:システムのフラッシュに保存された情報は、本機を再起動したり、電源を切っても維持されます。



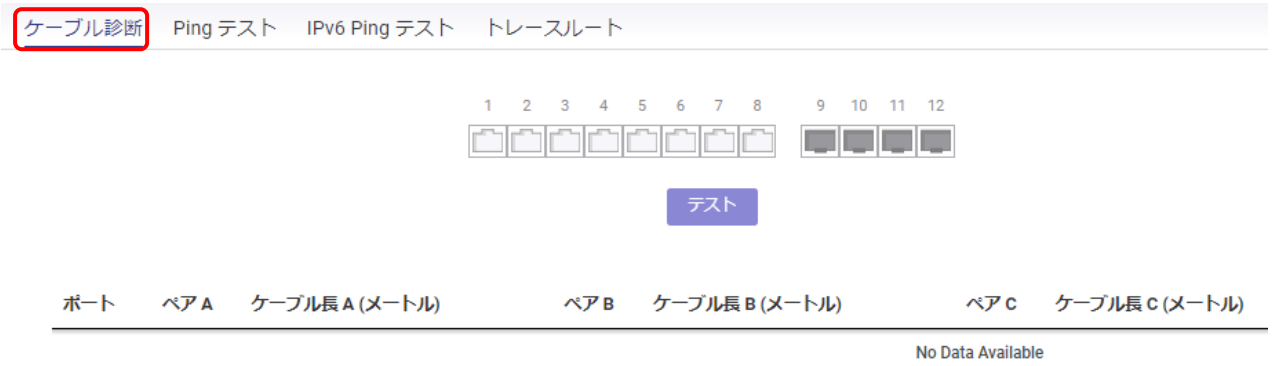
1. ダウンロード>ボタンをクリックすると、現在のバッファリングされたログが .txt ファイルにエクスポートされます。
2. <クリア>ボタンをクリックすると、システムのメモリにバッファリングされたログがクリアされます。
3. <更新>ボタンをクリックすると、最新情報が表示されます。

2.4.2 診断ツール

1. ケーブル診断

ケーブル診断は、ケーブルに接続の問題があるかどうかを検出するのに役立ち、ケーブルでエラーが発生した場所に関する情報を提供します。このテストでは、TDR(Time Domain Reflectometry)テクノロジを使用して、ポートに接続されたイーサネットケーブルの品質をテストします。TDR は、ケーブルを介して信号を送信し、反射された信号を読み取ることによって、ケーブル障害を検出します。信号のすべてまたは一部は、ケーブルの欠陥によって、または問題が存在する場合はケーブルの端によって反射されます。
ケーブル長のテストを除いて、ポートがダウン状態のときにケーブルがテストされます。

「解析」→「診断ツール」→「ケーブル診断」をクリックすると、以下の画面が表示されます。

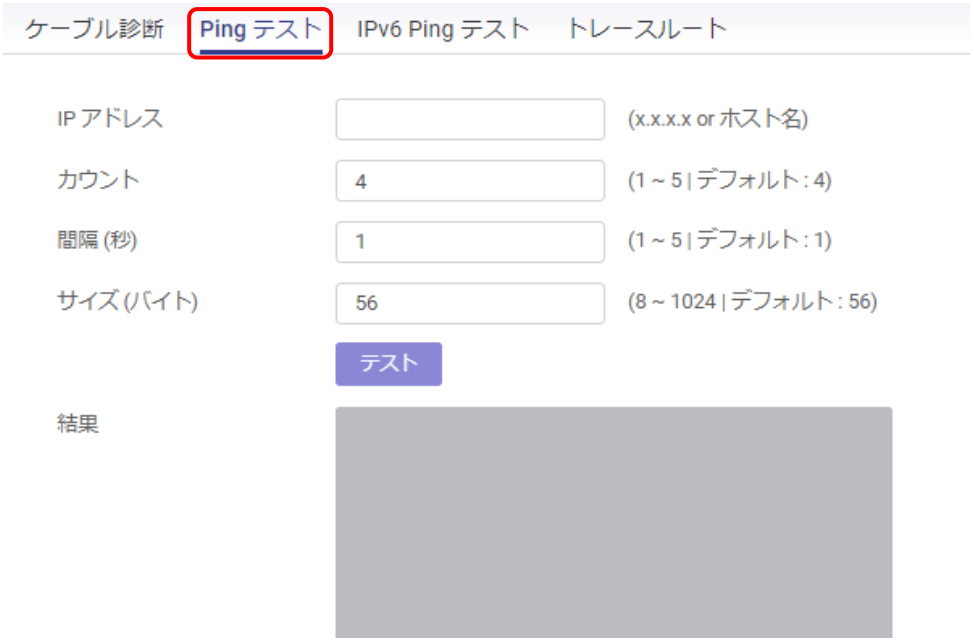


【注記】:
テストの正確性を検証するには、テストエラーまたはユーザエラーが発生した場合に備えて、複数のテストを実行することをお勧めします。
<テスト>ボタンをクリックして、選択したポートのケーブルテストを実行してください。

2. Ping テスト

Ping(Packet Internet Groper) テストでは、リモート ホストへの接続を確認できます。
ping テストは、インターネット制御メッセージ プロトコル (ICMP) 要求パケットをテスト対象ホストに送信することによって動作し、ICMP 応答を待ちます。その過程で、送信から受信までの時間を測定し、パケット損失を記録します。指定した IPv4 アドレスに ping 要求を送信します。テストする前に、特定のネットワーク ホストと通信可能な状態かどうか確認してください。

「解析」→「診断ツール」→「Ping テスト」をクリックすると、以下の画面が表示されます。



❑適切なボックスにデータを入力することで、テスト パラメータを変更できます。テストの正確性を検証するには、テストエラーまたはユーザエラーが発生した場合に備えて、複数のテストを実行することをお勧めします。

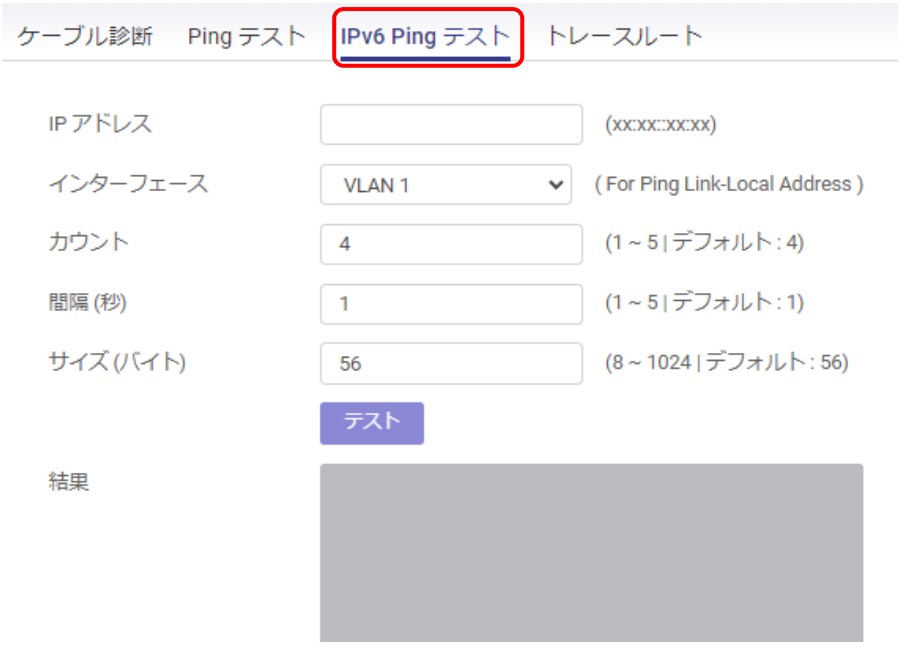
メニュー	説明
IPアドレス	スイッチが ping を送信するステーションのIPv6アドレス、またはホスト名を入力してください。
インタフェース	対象のインタフェースを選択します。
カウント	送信する ping の数を入力してください(有効範囲:1 ～ 5、デフォルト:4)。
間隔	ping の送信間隔を秒数で入力してください(有効範囲:1 ～ 5、デフォルト:1)。
サイズ(バイト)	送信する ping パケットのサイズを入力してください(有効範囲:8 ～ 1024、デフォルト:56)。

【注記】:
テストの正確性を検証するために、テストエラーまたはユーザエラーが発生した場合に備えて、複数のテストを実行することをお勧めします。

3. IPv6 Ping テスト

指定した IPv6 アドレスに ping 要求を送信します。テストする前に、特定のネットワーク ホストと通信可能な状態かどうか確認してください。

「解析」→「診断ツール」→「IPv6 Ping テスト」をクリックすると、以下の画面が表示されます。



メニュー	説明
IPアドレス	ping を送信するステーションの IPv6アドレスを入力してください。
インタフェース	対象のインタフェースを選択します。
カウント	送信する ping の数を入力してください(有効範囲:1 ～ 5、デフォルト:4)。
間隔	ping の送信間隔を秒数で入力してください(有効範囲:1 ～ 5、デフォルト:1)。
サイズ(バイト)	送信する ping パケットのサイズを入力してください(有効範囲:8 ～ 1024、デフォルト:56)。

メニューに適切な値を入力することにより、テストのパラメータを変更できます。

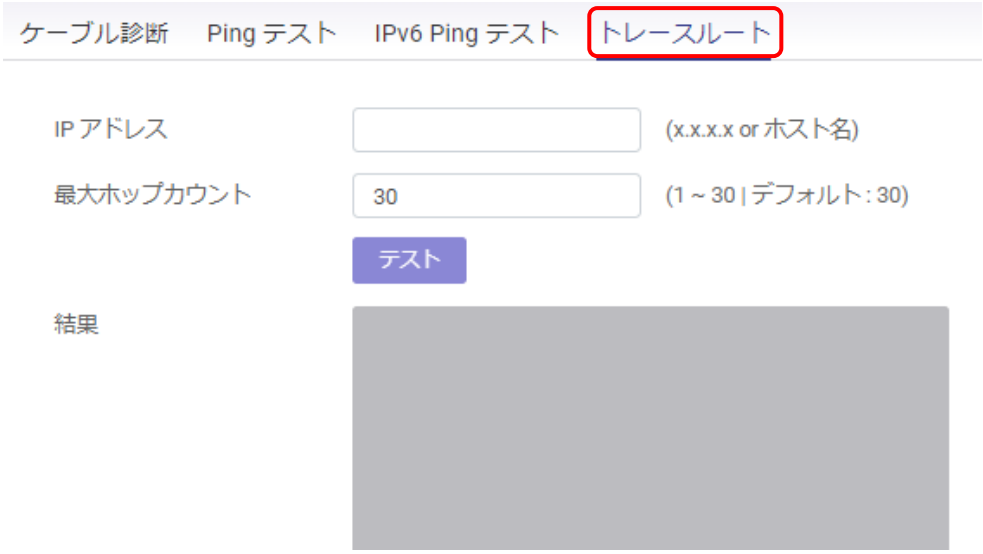
【注記】:
テストの正確性を検証するには、テストエラーまたはユーザエラーが発生した場合に備えて、複数のテストを実行することをお勧めします。

❑<テスト>ボタンをクリックして、ping テストを実行してください。

4. トレースルート

トレースルート機能は、パケットが宛先に移動する際にたどるルートを検出するために使用されます。宛先に到達するか、宛先に到達できずに破棄されるまで、通過するすべてのルータを一覧表示します。テストでは、ルート内の連続する各ホストから送受信されるパケットのトリップ時間によって、ルータからルータへの各ホップにかかる時間がわかります。

「解析」→「診断ツール」→「トレースルート」をクリックすると、以下の画面が表示されます。



メニュー	説明
IPアドレス	ping を送信するステーションの IP アドレスを入力してください。
最大ホップカウント	最大ホップ数を入力してください(有効範囲 : 1 ～ 30、デフォルト: 30)。
結果	トレースルートの結果を表示します。

❑<テスト>ボタンをクリックして、トレースルートを開始してください。

2.5 ユーザとグループ

手動で設定したユーザ名とパスワードに基づいて本機への管理アクセスを制御します。
「ユーザ」アカウントは、本機を設定する権限のない設定のみ表示します。
「管理者」アカウントは、本機のすべての機能を設定できます。

「ユーザとグループ」をクリックすると、以下の画面が表示されます。

メニュー	説明
ユーザ名	ユーザ名を表示します。最大 18 文字の英数字を使用できます。
権限の種類	リストから「Admin」または「User」のいずれかを選択します。
パスワード	本機にアクセスするための新しいパスワードを入力してください。
パスワードの確認入力	本機へのアクセスに使用する新しいパスワードを繰り返します。

1.<追加>ボタンをクリックしてアカウントを追加するか、<編集>ボタンをクリックして既存のアカウントを編集します。

【重要】:
ユーザ アカウントの権限を決定する際、管理者ユーザには本機への完全なアクセス権があることに注意してください。

2.それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<キャンセル>ボタンをクリックして変更内容を一括してクリアにすることができます。

2.6 セキュリティ

ここでは、ポートベースのセキュリティ機能とその設定手順について説明します。

本メニューは、以下のメニューで構成されています。

2.6.1 802.1X

サプリカントがスイッチ ポートに接続されると、ポートは接続された 802.1X サプリカントに 802.1X 認証要求を発行します。サプリカントは指定されたユーザ名とパスワードで応答し、認証要求は設定済みの RADIUS サーバに渡されます。認証 サーバのユーザ データベースは、個々のユーザに基づいて特定の VLAN メンバーシップを定義できる拡張認証プロトコル (EAP) をサポートします。認証後、認証されたサプリカントに接続されたポートは、指定された VLAN のメンバーになります。サプリカントが正常に認証されると、トラフィックは自動的に VLAN に割り当てられます。本機がサポートする EAP 認証方式は、「EAP-MD5、EAP-PEAP、および EAP-CHAPv2」です。

1. グローバル設定

セキュリティ機能をグローバルで有効にします。

「セキュリティ」→「802.1X」→「グローバル設定」をクリックすると、以下の画面が表示されます。

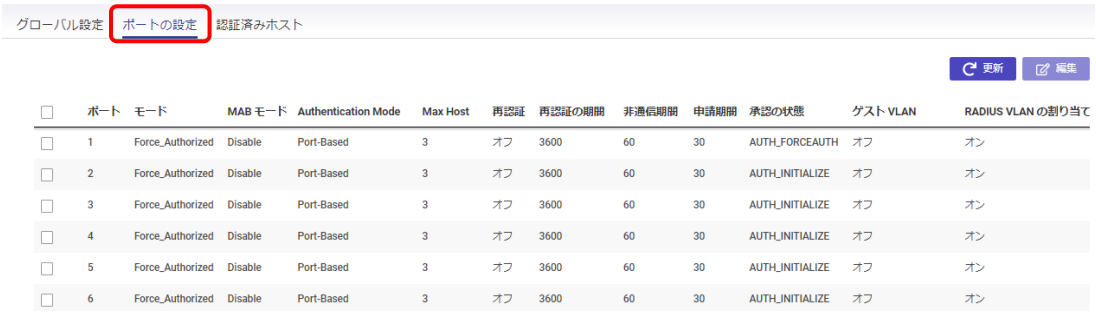
メニュー	説明
状態	本機の認証が有効/無効を選択します。
ゲスト VLAN	本機のゲスト VLAN を有効/無効を選択します。デフォルトは無効です。
ゲスト VLAN ID	現在定義されている VLAN のリストからゲスト VLAN ID を選択します。

❑それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<リセット>ボタンをクリックして変更内容を破棄してください。

2. ポート設定

IEEE 802.1X ポートベースの認証は、RADIUS サーバによるネットワーク アクセス制御のセキュリティ標準を提供し、認証が完了するまでネットワーク ポートを切断したままにします。802.1X ポートベースの認証では、サプリカントはユーザ名、パスワード、デジタル証明書などの必要な資格情報をオーセンティケータに提供し、オーセンティケータはその資格情報を認証 サーバに転送して、ゲスト VLAN に対する検証を行います。認証 サーバがクレデンシャルが有効であると判断した場合、サプリカントはネットワークの保護側にあるリソースにアクセスできます。
ここでは、802.1X に関連するポート設定を設定できます。まず、ドロップダウン ボックスから使用するモードを選択します。次に、ポートの再認証を有効/無効を選択します。再認証期間、休止期間、およびサプリカント期間の経過時間を入力してください。この後、本機が EAP 要求を再送信する最大回数を入力してください。最後に、VLAN ID を有効/無効を選択します。

「セキュリティ」→「802.1X」→「ポートの設定」をクリックすると、以下の画面が表示されます。



メニュー	説明
ポート	802.1X 情報が表示されるポートを表示します。
モード	リストから「Auto」、「Force_UnAuthorized」、または「Force_Authorized」モードを選択します。
MABモード	「MAB/Hybrid/Disable」を表示します。
Authentication Mode	認証モード(ポートベース/MACベース)を選択します。
Max Host	最大ホスト数を表示します。
再認証	ポートの再認証を有効/無効を選択します。
再認証期間	選択したポートが再認証される期間を入力してください(デフォルト値:3600 秒)。
非通信期間	認証交換に失敗した後、静止状態を維持する機器の数を入力してください(デフォルト値:60 秒)。
申請期間	EAP 要求がサプリカントに再送信されるまでの時間を入力してください(デフォルト値:30 秒)。
最大再試行	認証セッションがタイムアウトする前に、本機がクライアントに EAP 要求を再送信する最大回数を入力してください(デフォルト値:2 回)。
ゲスト VLAN	ゲストVLAN ID が有効/無効を選択します。
RADIUS VLAN の割り当て	RADIUS VLANの割り当てを有効/無効にします。

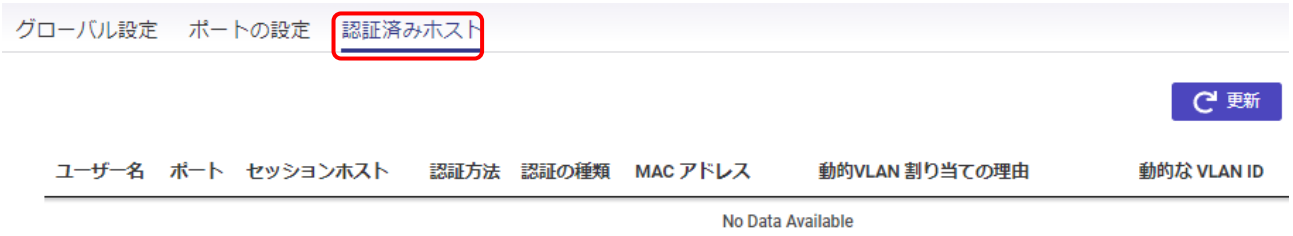
1. ポートの設定を変更したい場合、ポートを選択して<編集>ボタンをクリックすると、次の画面が表示されます。

2. 設定内容を適用する場合は、<適用>ボタン、キャンセルする場合は、<キャンセル>ボタンをクリックしてください。

3. 認証済みホスト

認証済みユーザ名、ポート、セッション時間、認証済みメソッド、および MACアドレスが表示されます。

「セキュリティ」→「802.1X」→「認証済みホスト」をクリックすると、以下の画面が表示されます。



❑最新の情報を表示したい場合は、<更新>ボタンをクリックしてください。

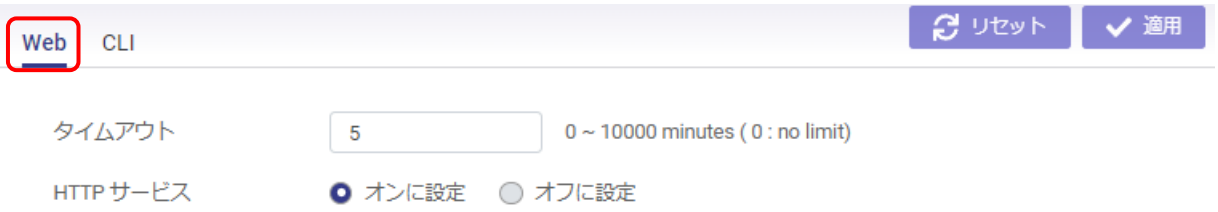
2.6.2 アクセス

1. WEB

本機は、ネットワーク上のセキュリティ違反を防止するために、HTTP(Hypertext Transfer Protocol)を介してWEBブラウザインタフェースを提供します。
HTTP リクエストのセッション タイムアウトの長さを選択することで、本機の HTTPの設定を管理します。

HTTP サービスを有効/無効を選択して、HTTPタイムアウトセッションに入ります。

「セキュリティ」→「アクセス」→「Web」をクリックすると、以下の画面が表示されます。



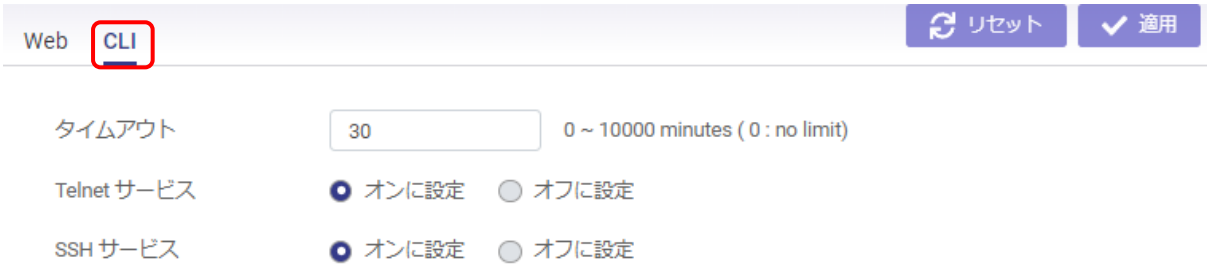
メニュー	説明
タイムアウト	HTTP がタイムアウトするまでの時間を入力してください(デフォルト値:5 分、有効範囲:0 ～ 10000分)。※値を“0”にするとタイムアウトは無効になります。
HTTP サービス	本機の HTTP サービスが有効/無効を選択します(デフォルトでは、有効)。

❑それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<リセット>ボタンをクリックして変更内容を破棄してください。

2. CLI

本機の Telnet プロトコル設定を設定および管理できます。Telnet プロトコルは標準のインターネットプロトコルであり、仮想端末接続を使用してコマンド ライン インタフェース (CLI) 通信を提供することにより、端末とアプリケーションがインターネット経由でリモート ホストとインタフェースできるようにします。このプロトコルは、クライアントをコマンド インタープリターにリンクできるようにするための基本的なルールを提供します。本機の Telnet サービスは、デフォルトで有効になっています。安全な通信を行うには、Telnet 経由で SSH を使用することをお勧めします。
本機のSSH(Secure Shell)を設定するには、まずSSH サービスを有効/無効を選択します。使用するサービスを決定する際、SSH は Telnet サービスよりも安全です。
まず、SSH に実装するセッション タイムアウトを入力してください。安全なデータ通信ネットワーク サービスのための暗号化ネットワーク プロトコルです。SSH は、ネットワーク コマンド ライン インタフェースにアクセスする方法です。トラフィックは暗号化されているため、インターネットなどのセキュリティで保護されていないネットワーク内のセキュリティで保護された接続が作成されるため、盗聴は困難です。攻撃者がトラフィックを閲覧できたとしても、データを解読するための正しい暗号化キーがなければ、データを理解することはできません。

「セキュリティ」→「アクセス」→「CLI」をクリックすると、以下の画面が表示されます。



メニュー	説明
タイムアウト	Telnet サービスがタイムアウトになるまでの時間を入力してください(デフォルト値:5分、有効範囲:0 ～ 10000分)。※値を“0”にするとタイムアウトは無効になります。
Telnet サービス	Telnet サービスが有効/無効を選択します(デフォルト設定:有効)。
SSH サービス	SSH サービスが有効/無効を選択します(デフォルト設定:無効)。

❑それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<リセット>ボタンをクリックして変更内容を破棄してください。

2.6.3 ポートセキュリティ

特定のポートへのアクセスを特定の MACアドレスを持つユーザに制限することで、ネットワーク セキュリティを強化できます。ポート セキュリティは、自動学習処理を停止する前に、許可されていない機器が本機に接続されるのを防ぎます。

「セキュリティ」→「ポートセキュリティ」をクリックすると、以下の画面が表示されます。

メニュー	説明
ポート	ポート セキュリティが定義されているポートを表示します。
状態	選択したポートのポート セキュリティ機能について、「有効」または「無効」を選択します。
最大 MACアドレス	ポートで学習できる MACアドレスの最大数を入力してください(有効範囲：1 ～ 256)。

1.ポートの設定を変更したい場合は、該当ポートを選択し、<編集>ボタンをクリックすると、下記の画面が表示されます。

2.設定内容を適用する場合は、<適用>ボタン、キャンセルする場合は、<キャンセル>ボタンをクリックしてください。

1. RADIUS サーバ

RADIUSサーバとRADIUSクライアントの間の通信に用いられ、ネットワーク上で利用者の認証や権限の付与したり、利用状況の記録などを行うことができます。

RADIUS(Remote Authentication Dial in User Service)は、利便性を高めるためにネットワークサービスを使用するユーザに対して、一元化された認証、承認、アカウンティング (AAA) 管理を提供するネットワーク プロトコルです。本機のポートに接続されたクライアントは、LAN上のサービスにアクセスする前に、認証 サーバにる認証が必要です。RADIUS サーバを使用して、クライアントと サーバ間でEAPOL(Extensible Authentication Protocol over LAN)パケットをリレーすることにより、ネットワークにアクセスするユーザの認証を行います。
この サーバは、ネットワークの使用を許可する前に、ユーザ名とパスワードを認証することができます。

「セキュリティ」→「RADIUSサーバ」をクリックすると、以下の画面が表示されます。

メニュー	説明
インデックス	RADIUS サーバが表示されているインデックスを表示します。
サーバ IPアドレス	RADIUS サーバの IP アドレスを入力してください。
許可されたポート	許可されたポート番号を入力してください(デフォルトのポート:1812)。
アカウンティング ポート	本機を識別するために使用する名前を入力してください。
キーストロング	機器と RADIUS サーバ間のすべての RADIUS 通信の暗号化に使用されるキー文字列を入力してください。
タイムアウトの返信	次の サーバに切り替える前に、機器が RADIUS サーバからの応答の待機時間を入力してください(デフォルト値:3)。
再試行	障害が発生する前に RADIUS サーバに送信される送信要求の数を入力してください(デフォルト値:3)。

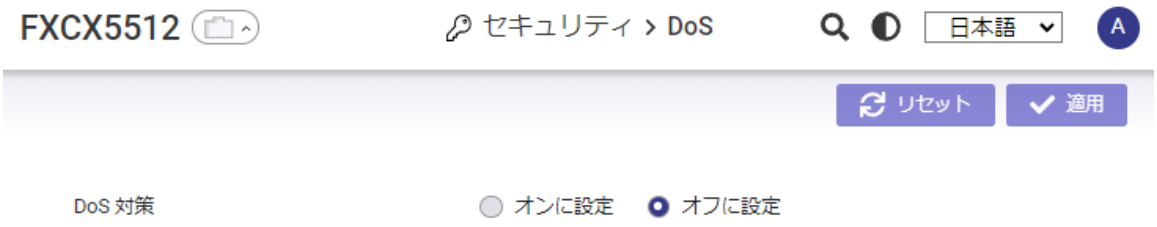
1.エントリを追加したい場合は、<追加>ボタンをクリックすると次の画面が表示されます。

2.設定内容を適用する場合は、<適用>ボタン、キャンセルする場合は、<キャンセル>ボタンをクリックしてください。

2.6.4 DoS

DoS（Denial of Service: サービス妨害）は、特定の種類の DoS攻撃を分類してブロックするために使用されます。
この機能により、さまざまなタイプの DoS 攻撃の防止を有効/無効にできます。

「セキュリティ」→「DoS」をクリックすると、以下の画面が表示されます。



❑それぞれの項目を設定後、<適用>ボタンをクリックして変更内容を確定するか、<リセット>ボタンをクリックして変更内容を破棄してください。

2.6.5 DAI

ここでは、DAI(Dynamic ARP Inspection)の設定を行います。
この機能は、ARPスプーフィング攻撃からの保護を強化し、ネットワーク内のデバイス間の通信を安全に保つことができます。

1. ARP ACL

ACLはアクセスレベル制御を指します。これは、ユーザやシステムがアクセスできるデータや機能を制御するセキュリティ機能です。
アクセスレベルは、ユーザの役割や権限に基づいて設定され、重要な情報やシステムリソースへの不正アクセスを防止します。

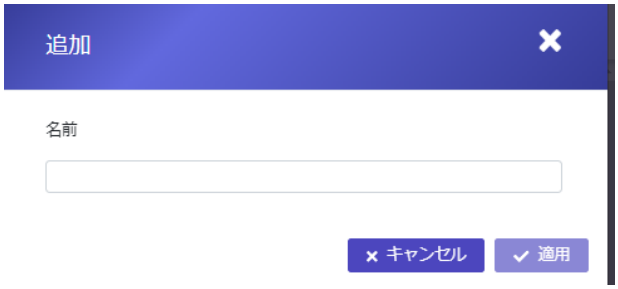
「セキュリティ」→「DAI」→「ARP ACL」をクリックすると、以下の画面が表示されます。

1) ARP アクセスリスト

ARPアクセスリストは、ネットワークセキュリティを強化するための有効な手段であり、特定のIPアドレスとMACアドレスの組み合わせを許可または拒否することで、ARPスプーフィング攻撃やその他のARP関連の脅威を防ぐことができます。
正確なARP ACLの設定と管理により、ネットワークのセキュリティレベルを向上させることができます。

「セキュリティ」→「DAI」→「ARP ACL」→「アクセスエントリー」をクリックすると、以下の画面が表示されます。

<＋追加>ボタンをクリックすると、次の画面が表示されます。



❑名前を入力後、<適用>ボタンをクリックして設定した名前を確定するか、<キャンセル>ボタンをクリックしてキャンセルしてください。

2) アクセスエントリー

アクセスエントリーは、特定のリソースに対するアクセスを許可または禁止するために設定される具体的なルールやエントリーを指します。これにより、セキュリティポリシーが適切に適用され、リソースが保護されます。

「セキュリティ」→「DAI」→「ARP ACL」→「アクセスエントリー」をクリックすると、以下の画面が表示されます。

❑画面右側の設定（ ••• ）をクリックすると、以下のようにメニューが表示されるため、表示したい項目を選択してください。

メニュー項目	説明
ARR ACL 名	ACL名を表示します。
シーケンス	選択したインタフェースに割り当てられた他の ACL に対して指定された ACL の順序を示すシーケンス番号を表示します(有効な範囲:1 ～ 16)。 ※1 から順に処理されます。
アクション	パケットが基準に一致した場合に実行するアクションを表示します。 ・Permit: ACE基準を満たすパケットを転送します。 ・Deny: ACE基準を満たすパケットをドロップします。
MACタイプ	MACアドレスのタイプを表示します。
送信元MACアドレス	送信元 MACアドレスを表示します。
送信元 アドレスマスク	送信元 MACアドレスの MACアドレス マスクを表示します。 ・00:00:00:00:00:00 のマスクは、ビットが正確に一致する必要があることを意味します。 ・ff:ff:ff:ff:ff:ff は、ビットが無関係であることを意味します。 ・“0” と”f” の任意の組み合わせを使用できます。
送信元MACアドレスマスク	送信元 MACアドレスの MACアドレスマスクを表示します。 ・”00:00:00:00:00:00” のマスクは、ビットが正確に一致する必要があることを意味します。 ・”ff:ff:ff:ff:ff:ff” は、ビットが無関係であることを意味します。

	・”0”と”f” の任意の組み合わせを使用できます。
IPタイプ	IPタイプを表示します。
送信元 IP アドレス	送信元IP アドレスを表示します。
送信元 IPネットマスク	送信元 IPネットマスクを表示します。

2. ARP インスペクション

ネットワークセキュリティを強化するための重要な機能です。
ARPスプーフィングやポイズニング攻撃を防止することで、ネットワークの安全性と信頼性を向上させます。

1) 検証

「セキュリティ」→「DAI」→「 ARPインスペクション」→「検証」をクリックすると、以下の画面が表示されます。

検証対象とするアドレスを選択し、それぞれ設定(「オンに設定」/「オフに設定」)してください。

2) VLAN ログテーブル

「セキュリティ」→「DAI」→「ARPインスペクション」→「VLANログテーブル」をクリックすると、以下の画面が表示されます。

メニュー	説明
ACLログ	ネットワークトラフィックに対するアクセス制御の結果を記録し、セキュリティ監視やトラブルシューティングに役立ちます。
DHCPログ	ネットワークデバイスにIPアドレスやその他の設定を自動的に割り当てる過程を記録し、IPアドレス管理やネットワークのトラブルシューティングに使用されます。

3) フィルターテーブル

「セキュリティ」→「DAI」→「 ARPインスペクション」→「フィルターテーブル」をクリックすると、以下の画面が表示されます。

メニュー	説明
VID	VLAN ID を表示します (有効範囲は 1 ～ 4094)。
ARPアクセスリスト名	ARPアクセスリスト名を表示します。 ネットワークのセキュリティポリシーの適用や監視、不正アクセスの検出などに役立ちます。
static ACLの使用	static ACLの使用状況を表示します。 ネットワークの運用やトラブルシューティング、リソースの管理などに役立ちます。

4) VLAN 設定

VLAN設定のDAI状態をオフにする場合は、VIDを選択して設定してください。

「セキュリティ」→「DAI」→「 ARPインスペクション」→「VLAN設定」をクリックすると、以下の画面が表示されます。

3. ポート設定

各ポートのTrustの状態(trust/untrusted)を設定します。
この設定により、ネットワーク上でのARPスプーフィング攻撃などのセキュリティリスクを軽減し、ネットワークのセキュリティを強化することができます。

「セキュリティ」→「DAI」→「ポート設定」をクリックすると、以下の画面が表示されます。

<編集>ボタンをクリックすると、以下の画面が表示されます。

❑Trust の状態を変更したいポートを☑して選択後、Trust の状態(trust/untrusted)を選択して、設定内容を適用する場合は、<適用>ボタン、キャンセルする場合は、<キャンセル>ボタンをクリックしてください。

4. 統計情報とログ

これらの統計情報を定期的に監視することで、ネットワーク上でのARP関連の問題や攻撃の試みを把握し、迅速に対処することができます。また、適切なトラブルシューティングやセキュリティポリシーの調整に役立ちます。

「セキュリティ」→「DAI」→「統計情報とログ」→「統計情報」をクリックすると、以下の画面が表示されます。

1) 統計情報

「セキュリティ」→「DAI」→「統計情報とログ」→「統計情報」をクリックすると、以下の画面が表示されます。

❑画面右側の設定(•••)をクリックすると、以下のようにメニューが表示されるため、表示したい項目を選択してください。

メニュー	説明
VID	VLAN ID を表示します (有効範囲は 1 ～ 4094)。
送信済み	送信されたパケット数を表示します。
破棄	破棄されたパケット数を表示します。
DHCP破棄	DHCPスヌーピングによって破棄されたパケット数を表示します。
ACL破棄	ACLに一致して、破棄されたパケット数を表示します。
DHCP許可	DHCPスヌーピングによって許可されたパケット数を示します。
ACL許可	ACLに一致して、許可されたパケット数を示します。
送信元MACアドレスエラー	不正な送信元MACアドレスエラーの数を示します。
宛先MACアドレスエラー	不正な宛先MACアドレスエラーの数を示します。
IPアドレス検証エラー	不正なIPアドレス検証エラーの数を示します。

❑最新の情報を表示したい場合は<更新>ボタン、すべての情報をクリアしたい場合は<クリア>ボタンをクリックしてください。

2) ログ

統計情報のログを定期的に監視することで、ネットワーク上でのARP関連の問題や攻撃の状況を把握し、迅速に対処することができます。また、適切なトラブルシューティングやセキュリティポリシーの調整に役立ちます。

「セキュリティ」→「DAI」→「統計情報とログ」→「ログ」をクリックすると、以下の画面が表示されます。

❑更新ボタン：最新の情報を表示したい場合は、<更新>ボタンをクリックしてください。

❑ログバッファボタン：ログバッファの容量を設定することができます（デフォルト設定：「100」）。

❑クリアボタン：ログ情報をクリアにしたい場合は、<クリア>ボタンをクリックしてください。

■ 3 章　CLI による設定方法 ■

3.1 CLI による設定方法

3.1.1 接続手順

1. コンソール接続

コンソールポートへの接続は以下の手順で行います。

接続方法:

本体前面の右側にあるコンソールポートに同梱のコンソールケーブルの片方を接続し、もう片方を PC などのCOM ポートに接続します。
その後PCのCOMポートをターミナルエミュレータで開きます(COMポート番号はPCで確認してください)。

ターミナルエミュレータは、以下のとおりに設定してください。

ボーレート	115200 Baud
データ	8 Bit
パリティ	なし
ストップビット	1 Bit
フロー制御	なし

（1）コンソールプロンプトでユーザ名とパスワードを入力してください。
初期設定のユーザ名は"admin"、パスワードも同じく"admin”となっています。

（2）ユーザ名とパスワードを入力後は、必要に応じたコマンドを入力し、本機の設定および統計情報の閲覧を行います。

（3）終了時には"exit"コマンドを使用しセッションを終了します。
コンソールポートからシステムに接続すると以下のログイン画面を表示します。

2. ネットワークの接続方法

1) Telnet 接続方法

Telnetを利用するとネットワーク経由での管理が可能となります。
Telnetを行うには管理端末側と本機側のどちらにもIPアドレスを事前に設定する必要があります。
また、異なるサブネットからアクセスする場合にはデフォルトゲートウェイもあわせて設定する必要があります。

【注意】: Telnet接続は、同時に最大4セッションまで可能です。

2) IP アドレス手動設定の場合

本機の IP アドレスを設定した後、以下の手順で Telnet セッションを開始することができます。

（1）リモートホストから Telnet コマンドと本機の IP アドレスを入力してください。

（2）ログインすると”FXCX5512PE”と表示されます。

（3）ユーザ名とパスワードを入力後は、以下の手順にしたがってください。

```
------------------------------------------------------------
FXCX5512PE login: admin
Password:

FXCX5512PE#configure terminal
FXCX5512PE(config)# interface vlan 1
FXCX5512PE(config-if)# ip address 192.168.1.1 255.255.255.0
  （※ IP アドレス・サブネットマスクは自由に設定してください。）
FXCX5512PE(config-if)# exit
FXCX5512PE(config)# ip route 192.168.1.0 255.255.255.0
 192.168.1.254
  （※必要に応じてデフォルトゲートウェイを設定してください。）
FXCX5512PE(config)#
------------------------------------------------------------
```

（4）終了時には"quit"又は"exit"コマンドを使用しセッションを終了します。

（5）Telnetを有効化するには、以下の手順にしたがってください。

```
------------------------------------------------------------
FXCX5512PE(config)#
FXCX5512PE(config)# ip telnet server
FXCX5512PE(config)#
------------------------------------------------------------
```

Telnetを有効化であることを確認するには、以下の手順にしたがってください。

```
------------------------------------------------------------
FXCX5512PE# show telnet server
  telnet service enabled
FXCX5512PE#
------------------------------------------------------------
```

IPアドレスの設定が完了後、システム情報を表示する場合は、“show system information”と入力すると、以下の情報が表示されます。

```
------------------------------------------------------------
Firmware Version                   : 3.02.367
 Switch Name                        : FXCX5512PE
 System Contact                     : Default Contact
 System Location                    : Default Location
 Logging Option                     : Console Logging
 Login Authentication Mode          : Local
 Config Save Status                 : Successful
 Remote Save Status                 : Not Initiated
 Config Restore Status              : Successful
 Traffic Separation Control         : none
 Serial Nums                        : 20B0L9F11D88
 Loader Version                     : 03.02.02
 MAC Address                        : 88:dc:96:8f:09:41
 System Uptime                      : 8 days, 3 hours, 59 mins
 Hardware Version                   : Rev.A
------------------------------------------------------------
```

3.1.2 ユーザのアクセスレベルの設定方法

デフォルト設定では、それぞれのアクセスレベルは以下のとおりです。

1. 管理者向けレベル（レベル 15) :
すべての機能にアクセス可能であり、すべての機器を管理可能です。

2. 標準ユーザ向けレベル (レベル 1～14):
本機のステータスと設定内容の表示、一部のメンテナンスコマンドを実行することができます。

【注記】:
・ この設定は、レベル 15 の管理者向けアカウントを持ったユーザのみ設定可能です。
初期設定時のユーザ名およびパスワードは"admin"/”admin”です。
・ システムメンテナンス（ソフトウェアのアップロード、工場出荷時設定など）を行う場合は、
「レベル 15(管理者向けアカウント)」が必要となります。

ユーザの権限レベル設定は、以下のコマンドを使用します。

```
------------------------------------------------------------
(config)# username <※1 ユーザ名>password <※1 パスワード>
confirm-password <パスワード再入力>
[privilege <※2 権限番号>]
  （※1:ユーザ名およびパスワードは18文字までの英数字が設定可能）
   （※2:権限番号（任意）:1～15までの数値が設定可能）
------------------------------------------------------------
```

【注記】:レベル 1～14は一般ユーザ、15は管理ユーザ。省略されている場合は一般ユーザに設定されます。

以上で、アクセスレベルの設定は完了です。

アクセスレベルの設定が完了後、基本コマンドモードに移動して"logout"または”exit”コマンドにより一旦ログアウトした後、設定したユーザ名とパスワードを使ってログインしてください(この場合、ユーザ名:guest、パスワード:guest)。

3.1.3 CLI の使用方法

1. ファンクションキー

ここでは、コンソール画面用のファンクションキーについて説明します。

ファンクションキー	概要
Tab	コマンドの最初の一部の文字を入力すると、コマンド名が正しく表示されます。例えば、"his"と入力した後に、"Tab"キーを押すと、コマンド名は“history”と表示されます。
↑	1つ前に入力したコマンドを表示します。
↓	1つ後に入力したコマンドを表示します。
←/→	カーソルを左右に移動します。
Backspace	カーソルの前の文字を削除します。
spaceキー	showコマンドなどで”-More-“と表示された際にそれ以降の情報を表示します。
?	コマンドリストを表示します。

2. コマンド上でのヘルプの表示

コマンド上で"help"コマンドを入力することで、簡単なヘルプ情報が表示されます。
また、"?”と入力するとキーワードやパラメータのコマンド文法が表示されます。

コマンドの表示
コマンド上で"?”と入力すると、現在のコマンドクラスの第一階層にあるすべてのキーワードが表示されます。また特定のコマンドのキーワードを表示することもできます。
例えば"show ?"、"account ? “と入力すると、"show"、"account"コマンド内で使用できるコマンド一覧が表示されます。

1) help コマンド

コマンド上で"help"コマンドを入力することで、簡単なヘルプ情報が表示されます。

"help"コマンドを入力すると、以下の画面が表示されます。

例:

```
------------------------------------------------------------
FXCX5512PE# help

EXEC commands :
  boot system { image1 | image2 }
  clear counters [ <interface-type> <interface-id> ]
  clear interfaces [ <interface-type> <interface-id> ] counters
  clear screen
  configure terminal
  copy startup-config {tftp://ip-address/filename}
  copy {tftp://ip-address/filename} startup-config
  dot1x re-authenticate [interface <interface-type><interface-
 id>]
  end
  exit
  firmware upgrade { tftp://ip-address/filename} {flash:normal |
 flash:fallback} image <1-2>
  free
  help [ command ]
  ip dhcp client fast-access
  listuser
  lock
  logout
  mpstat
  ping [ ip ] { ip_address | hostname } [{ repeat | count }
 packet_count(1-10)] [size packet_size(8-1
024)] [timeout time_out(1-100)]
  ping ipv6 <prefix%interface> [repeat <count>] [size <value(8-
 1024)>] [source {vlan <vlan-id> | <sou
rce_prefix>}] [timeout <value (1-100)>]
  reboot
  reboot-flick
  renew dhcp
  reset UBIRecoveryCount
  restore-default-without-IP
  restore-defaults
  save
  show UBIRecoveryCount
  show access-lists [{ip | mac | ipv6 | range} [<access-list-
 name (31)> ]]
  show activepartition
  show cdp
--More—
------------------------------------------------------------
```

2) ? コマンド

コマンド上で"?"と入力するとキーワードやパラメータのコマンド文法が表示されます。
"?" コマンドを入力すると、以下の画面が表示されます。

```
================================================================
 ==
FXCX5512PE# ?

boot                        Set active image after next to reload
clear                       Clears the specified parameters
configure                   Configures the terminal
copy                        Copies the configuration or system
 logs
dot1x                       PNAC related configuration
end                         Exit to the privileged Exec (#) mode
exit                        Exit from the privileged Exec (#) mode
firmware                    Upgrades firmware
free                        Show the usage of physical memory and
 Swap in the system.
help                        Displays help for the command
ip                          IP related protocol configuration
listuser                    List the user,mode and groups
lock                        Lock the console
logout                      Terminate the session
mpstat                      Show the status of the system.
ping                        Sends echo messages
reboot                      Restarts the switch
reboot-flick                Restarts the switch but not reset PoE
renew                       Performs renew operation
reset                       Reset the configuration / statistics /
 general information
restore-default-without-IP  Restore configure to default without
IP
restore-defaults            Restore configure to default
save                        Save the Startup Configuration.
show                        Displays the configuration /
 statistics /
                            general information
traceroute                  Traces route to the Destination IP
web-proxy                   web-proxy test
================================================================
 ==
```

3.1.4 各コマンドモード

次の表の形式は、各種 CLI コマンドモードを示しています。

コマンドモード	アクセス方法	プロンプト表示
Privileged EXEC	これはセッションに入るための初期モードです。	FXCX5512PE#
Global Configuration	グローバル コンフィグレーション モードに入るには、EXEC コマンドを使用します。	FXCX5512PE (config)#
Interface Configuration	インタフェースコンフィグレーションモードに入るには、グローバルコンフィグレーションモード(<interfacetype><interfaceid>コマンド)を使用します。	FXCX5512PE (config-if)#
Interface Range Mode	インタフェースのレンジに入るには、グローバルコンフィグレーションモード (interface range({ <interfacetype><slot/port-port>} {vlan <vlan-id(1-4093)>- <vlan- id(2-4094)>}コマンド)を使用します。	FXCX5512PE (config-if-range)#
SNTP Configuration	SNTPコンフィグレーションモードに入るには、config-sntpコマンドを使用します。	FXCX5512PE (config-sntp)#
Config-VLAN	config-vlanモードに入るには、グローバルコンフィグレーションモード (vlan vlan-idコマンド)を使用します。	FXCX5512PE (config-vlan)#
Line Configuration	lineコンフィギュレーションモードに入るには、line configコマンドを使用します。	FXCX5512PE (config-line)#
IPv4 ACL Extended Access List Configuration	IPv4 ACL 拡張アクセスリスト設定に入るには、ip access-list extended <name>コマンドを使用します。	FXCX5512PE (config-ext-nacl)#
IPv6 ACL Extended Access List Configuration	IPv6 ACL 拡張アクセス リスト コンフィギュレーションモードに入るには、ipv6 access-list extend <name>コマンドを使用します。	FXCX5512PE (config-ipv6-acl)#
MAC ACL Extended Access List Configuration	MAC ACL 拡張アクセス リスト コンフィギュレーションモードに入るには、mac access-list extend <name>コマンドを使用します。	FXCX5512PE (config-ext-macl)#
Policy Map Configuration Mode	ポリシーマップ コンフィギュレーションモードに入るには、class-policy <name>コマンドを使用します。	FXCX5512PE (config-qc-ply)#
MSTP Configuration Mode	MSTP コンフィギュレーションモードに入るには、spaning-tree mst Configurationコマンドを使用します。	FXCX5512PE (config-mst)#
ARP ACL Configuration Mode	ARP ACLコンフィグレーションモードに入るには、arp inspectionコマンド を使用します。	config-arp-acl)#

3.2 各コマンドによる設定

3.2.1 System

1. boot system

■説明：システムのブートイメージパーティッションを設定します。

■構文：boot system { image1 | image2 }

■設定モード：特権EXECモード

2. clear counters

■説明：
特定のインタフェース タイプ (シリアル、イーサネットなど) のみをクリアするためにオプションの引数 type とnumber が指定されていない限り、インタフェースから現在のインタフェースのカウンタをすべてクリアします。

■構文：clear counters [<interface-type> <interface-id>]

■パラメータの説明：
・ <interface-type> - 指定されたタイプのインタフェースのIPインタフェースを表示します。
インタフェースは次のとおりです。
  - gigabitethernet -1 秒あたり最大 1 ギガビットのデータ転送をサポートする LAN 標準アーキテクチャのバージョン。
  - port-channel – 複数のポートが集約されたアグリゲータを表す論理インタフェース。
・ <interface-id> - 指定されたインタフェース識別子のIPインタフェース設定を設定します。これは、特定のインタフェースを表す一意の値です。この値は、スロット番号とポート番号をスラッシュで区切って組み合わせたものです（例: 0/1 は、スロット番号が「0」、ポート番号が「1」であることを表します）。

■設定モード:特権EXECモード

3. clear interfaces - counters

■説明:
特定のインタフェース タイプ (シリアル、イーサネットなど) のみをクリアするためにオプションの引数 type とnumber が指定されていない限り、インタフェースから現在のインタフェース カウンタをすべてクリアします。

■構文:clear interfaces [<interface-type> <interface-id>] counters

■パラメータの説明:

・ <interface-type> - 指定されたタイプのインタフェースを設定します。
インタフェースは次のとおりです。
  - gigabitethernet – 1 秒あたり最大 1 ギガビットのデータ転送がサポート可能な LAN 標準アーキテクチャのバージョン。
  - port-channel – 複数のポートが集約されたアグリゲータを表す論理インタフェース。
・ <interface-id> - 指定されたインタフェース識別子のIPインタフェースを表示します。これは、特定のインタフェースを表す一意の値です。この値は、スロット番号とポート番号をスラッシュで区切って組み合わせたものです。
・ 例) 0/1:スロット番号が「0」、ポート番号が「1」であることを表します。

■設定モード:特権EXECモード

4. clear screen

■説明:画面からすべての内容をクリアします。

■構文:clear screen

■設定モード:すべてのモード

5. cli exec-timeout

■説明:
回線切断時のデフォルトの EXEC タイムアウト(分単位) を設定します。
【注記】:このコマンドは、コンソール接続時のみ使用可能です。

■構文:
・ cli exec-timeout <integer(1-10000>
・ no cli exec-timeout

■パラメータの説明:<minutes(0-10000)> - EXECタイムアウトの値(分単位)

■設定モード:グローバルコンフィグレーションモード

6. clock set

■説明:このコマンドはシステムクロックを管理します。

■構文
・ clock set hh:mm:ss <day (1-31)> {january|february|march|april|may|
june|july|august|september|october|november|december} <year (2000 - 2035)>

■パラメータの説明:
・ hh:mm:ss - 現在の時刻を設定します。
・ <day (1-31)> -現在の日付を設定します(有効範囲:1 ～ 31)。
・ january - 月を 1 月に設定します。
・ february - 月を 2 月に設定します。
・ march - 月を 3 月に設定します。
・ april - 月を 4 月に設定します。
・ may - 月を 5 月に設定します。
・ june - 月を 6 月に設定します。
・ july - 月を 7 月に設定します。
・ august - 月を 8 月に設定します。
・ september - 月を 9 月に設定します。
・ october - 月を 10 月に設定します。
・ november - 月を 11 月に設定します。
・ december - 月を 12 月に設定します。
・ <year (2000 - 2035)> - 年を設定します(有効範囲:2000年～2035年)

■設定モード:グローバルコンフィグレーションモード

7. clock set time

■説明:プライマリクロックの時間を設定します。

■構文:clock set time <time-nanoseconds>

■設定モード:グローバルコンフィグレーションモード

8. clock time source

■説明:
プライマリクロックのタイム ソースを設定します。
このコマンドの no 形式を使用すると、プライマリクロックのタイム ソースがデフォルトのタイム ソースにリセットされます。

■構文
・ clock time source { ntp | internal-oscillator }
・ no clock time source [{ ntp | internal-oscillator }]

■パラメータの説明:
・ ntp - システムのプライマリタイム ソースは ntp です。
・ internal-oscillator - システムの主な時間源は内部発振器です。

■設定モード:グローバルコンフィグレーションモード

9. clock utc-offset

■説明:
UTC を基準にしてシステムのタイムゾーンを設定します。
no 形式のコマンドは、システムのタイムゾーンを GMT にリセットします。

■構文:
・ clock utc-offset <offset>
  Eg: +05:30
・ no clock utc-offset

■パラメータの説明:
・ +/- - クライアントのタイムゾーンを UTC 以降または UTC より前に設定します。プラスは順方向のタイム ゾーンを示し、マイナスは逆方向のタイム ゾーンを表します。
・ <offset> -UTC オフセット値を時間単位で設定します。現在の UTCオフセット値(+HH:MM /-HH:MM)(+00:00 to +14:00)/ (-00:00 to -12:00).
  Eg: +05:30

■設定モード:グローバルコンフィグレーションモード

10. configure terminal

■説明:
グローバル コンフィグレーション モードに入り、グローバルコンフィグレーションモードをサポートするすべてのコマンドを実行可能になります。

■構文:configure terminal

■設定モード:特権EXECモード

11. copy startup-config

■説明
送信元のリモートサイト /flash から宛先リモート サイト /flash にファイルをコピーします。
コピー処理の全体には数分かかりますが、それぞれプロトコル、ネットワークに応じて異なります。

■構文:
・ copy startup-config {flash: filename | tftp://ip-address/filename}

■パラメータの説明:
・ tftp://ip-address/filename - TFTPサーバの初期設定をバックアップするための TFTP の詳細を設定します。
・ ip-address - サーバの IP アドレスまたはホスト名。
・ filename - 初期設定を保存するファイルの名前。ファイル名とディレクトリ名は大文字と小文字が区別されます。

■設定モード: 特権EXECモード

12. copy - startup-config

■説明: コンフィグレーションログまたはシステムログをリモート サイトからフラッシュにコピーします。

■構文:
・ copy { tftp://ip-address/filename startup-config | flash: filename startup-config }

■パラメータの説明:
・ tftp://ip-address/filename startup-config -ファイルのコピー元のアドレスと設定のコピー元のファイル名を設定します。このオプションは、TFTPサーバの詳細を設定します。ファイル名とディレクトリ名は大文字と小文字が区別されます。

■設定モード:特権EXECモード

13. description

■説明: インタフェースに説明書きを設定します。

■構文:
・ description <description of this interface>
・ no description

■設定モード:インタフェースコンフィグレーションモード

14. exit

■説明:現在のモードを終了し、現在のモードの前に使用されていたモードに戻ります。

■構文:exit

■設定モード:すべてのモード

15. end

■説明:コンフィグレーションモードを終了します。

■構文:end

■設定モード:すべてのモード

16. extended speed

■説明: ポートの拡張速度を有効にします。

■構文: extended speed

■設定モード:インタフェースコンフィグレーションモード

17. firmware upgrade

■説明
TFTP を使用してリモートの場所からファームウェアのアップグレードを実行してください。

■構文
・ firmware upgrade { tftp://ip-address/filename} {flash:normal | flash:fallback} image <1-2>

■設定モード:特権EXECモード

18. flowcontrol

■説明:インタフェースの送信または受信フロー制御値を設定するために使用されます。

■構文:flowcontrol { on | off }

■パラメータの説明:

・ on - インタフェースがフロー制御パケットをリモート側の機器に送信します (デバイスがサポートしている場合)。
・ off - インタフェースまたはリモート側の機器にフロー制御パケットをそれぞれ送信しないようにします。

■設定モード:インタフェースコンフィグレーションモード

19. free

■説明:
システムのメモリ使用量に関する詳細なレポートを取得します。free コマンドは、空きメモリと使用済みメモリだけでなく、物理メモリとスワップ メモリの合計量に関する情報を提供します。

■構文:free

■設定モード:特権EXECモード

20. help

■説明:指定されたコマンドの簡単な説明を表示します。

■構文:help [command]

■設定モード:すべてのモード

21. interface

■説明:VLAN などのインタフェースを設定できます。

■構文:
・ interface {vlan < vlan-id > | port-channel <integer (1-8)> |<interface-type> <interface-id>}
・ no interface vlan < vlan-id >

■パラメータの説明:

・ port-channel<port-channel-id (1-8)> - ホストがルータを設定するために使用するポートを設定します(有効範囲:1 ～ 8)。本機のリンクアグリゲーション機能が有効な場合にのみ、ポート チャネル ID を設定たり、ポート チャネル関連の設定を実行したりできます。
・ <interface-type> - 指定されたタイプのインタフェースを設定します。
インタフェースは次のとおりです。
  - gigabitethernet -1 秒あたり最大 1 ギガビットのデータ転送がサポート可能な LAN 標準アーキテクチャのバージョン。
  - port-channel – 複数のポートが集約されたアグリゲータを表す論理インタフェース。

■設定モード:グローバルコンフィグレーションモード

22. interface range

■説明:設定する物理インタフェースの範囲を選択します。

■構文:interface range { <interface-type> <slot/port-port> }

■パラメータの説明:
・ <interface-type> - 指定されたタイプのインタフェースのIPインタフェースを表示します。
インタフェースは次のとおりです。
  - gigabitethernet -1 秒あたり最大 1 ギガビットのデータ転送をサポートする LAN 標準アーキテクチャのバージョン。
  - port-channel – 複数のポートが集約されたアグリゲータを表す論理インタフェース。
・ <slot/port-port> - 指定したインタフェース識別子の範囲を選択します。これは、特定のインタフェースを表す一意の値です。この値は、スロット番号とポート番号をスラッシュで区切って組み合わせたものです。

■設定モード:グローバルコンフィグレーションモード

23. ip http port

■説明:このコマンドは HTTP ポートを設定します。

■構文:ip http port <port-number(1-65535)>

■パラメータの説明:
・ <port-number(1-65535)> -HTTPポートを表します。

■設定モード:グローバルコンフィグレーションモード

24. http session-idle-timeout

■説明:回線切断時の HTTPセッションのタイムアウト(分単位)を設定します。

■構文:ip http session-idle-timeout <minutes(0-10000)>

■パラメータの説明:
・ <minutes(0-10000)> -HTTPセッションタイムアウト値 (分単位)

■設定モード:グローバルコンフィグレーションモード

25. ip telnet service

■説明：システムで Telnet サービスを有効にします。

■構文：このコマンドの no 形式を使用すると、Telnet サービスが無効になります。
・ ip telnet service
・ no ip telnet service

■設定モード： グローバルコンフィグレーションモード

26. listuser

■説明：デフォルトのユーザと新しく作成されたユーザをすべて、有効なモードとともにリストします。

■構文：listuser

■設定モード：特権EXECモード

27. line cli

■説明：
設定する特定の回線を識別し、lineコンフィグレーション モードに入り、lineコンフィグレーション モードをサポートするすべてのコマンドを実行できるようにします。
【注記】:このコマンドは、コンソール接続時のみ使用可能です。

■構文：line cli

■設定モード：グローバルコンフィグレーションモード

28. lock

■説明
このコマンドは CLI コンソールをロックします。これにより、ユーザ/システム管理者はコンソールをロックして、権限のないユーザが CLI コマンドのシェルにアクセスできないようにすることができます。
ログイン用のパスワードを入力してコンソールのロックを解除し、CLI コマンドのシェルにアクセスします。

■構文：lock

■設定モード：特権EXECモード

29. logging synchronous

■説明:
特定の回線を識別し、lineコンフィグレーションモードに入り、ユーザがlineコンフィグレーション モードをサポートするすべてのコマンドを実行できるようにします。
【注記】:このコマンドは、コンソール接続時のみ使用可能です。

■構文:
・ logging [severity {alerts | critical | debugging | emergencies | errors | informational | notification | warnings}] [facility {local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7}] [buffered [<value(1-200)>]]

■設定モード:ラインコンフィグレーションモード

30. logout

■説明
コンソールセッションの場合、特権 EXEC/ユーザ EXEC モードを終了して、ISS ログイン プロンプトに戻ります。
Telnetセッションの場合、セッションを終了します。

■構文:logout

■設定モード:特権EXECモード

31. mpstat

■説明:
プロセッサー関連の統計情報を報告するために使用されます。システムの CPU 使用率の統計情報を正確に表示します。CPU 使用率とパフォーマンスに関する情報が表示されます。

■構文:mpstat

■設定モード:特権EXECモード

32. mtu

■説明:インタフェースの最大伝送単位(MTU)を設定します。

■構文:
・ mtu <frame-size(1522-10240)>

■パラメータの説明:
・ <frame-size(1522-10240)>:有効範囲は、1522 ～ 10240 です。

■設定モード:インタフェースコンフィグレーションモード
※PORTインタフェースモードで使用可能です。

33. negotiation

■説明:
インタフェースでの自動ネゴシエーションを有効にします。
コマンドの no 形式は、インタフェースでの自動ネゴシエーションを無効にします。
自動ネゴシエーションが有効なポートは、ポートのプロパティ(速度、duplexなど)について相手側とネゴシエートします。
通常のポートは、管理者が設定したポートのプロパティ値を使用します。

■構文:
・ negotiation
・ no negotiation

■設定モード:インタフェースコンフィグレーションモード

34. no shutdown switch-instance-shared-port

■説明:
スイッチのSISP(switch-instance-shared-port)を開始します。SISP が開始されると、適切な SISP 設定を通じてインタフェースを複数のスイッチのインスタンスにマッピングできます。

■構文:no shutdown switch-instance-shared-port

■設定モード:グローバルコンフィグレーションモード

35. no user-defined system name

■説明:システム情報をデフォルト値に設定します。

■構文:no user-defined system name

■設定モード:グローバルコンフィグレーションモード

36. ping

■説明
このコマンドはエコー メッセージを送信します。Packet Internet Groper (Ping) モジュールは、ICMP エコー要求および ICMP エコー応答メッセージに基づいて構築されます。ネットワーク管理者は、リモート側の機器上でこの ping を使用して、その存在を確認します。Ping では、ICMP エコー メッセージを繰り返し送信し、メッセージの送信と受信の間の時間を測定します。出力には、各パケットの送信にかかった時間、送信されたパケット数、受信されたパケット数、およびパケット損失の割合が表示されます。

■構文:
・ ping [ip] {IpAddress | hostname } [{repeat|count} <packet_count(1-10)>] [<size packet_size (8-1024)>] [<timeout time_out (1-100)>]

■パラメータの説明:
・ ip - ping を送信するノードの IP アドレスを設定します。
・ ipAddress - ping されるノードの送信元 IP アドレスを設定します。
・ hostname - ホストの名前を設定します。
・ repeat - ping メッセージの数を設定します。
・ count - 指定されたノード アドレスに ping を実行する回数を設定します。
・ size packet_size (8-1024) - PING PDU のデータ部分のサイズを設定します（値の有効範囲:8 ～ 1024）。
・ timeout time_out (1-100) - ping 応答を待っているエンティティがタイムアウトになるまでの時間を秒単位で設定します（値の有効範囲:1 ～ 100）。

■設定モード:特権EXECモード

37. port-security

■説明:特定のインタフェース ポートの学習アドレスの数を設定します。

■構文:
・ port-security <limit-size(1-256)>
・ no port-security

■パラメータの説明:
・ < limit-size(1-256)>-有効範囲は、1 ～ 256 です。

■設定モード:インタフェースコンフィグレーションモード
※PORTインタフェースモードで使用可能です。

38. port speed – duplex

■説明:通信速度とduplexモードを設定します。

■構文:
・ speed { 10 | 100 | 1000 | 10000 } duplex { full | half }
・ no speed
・ no duplex

■パラメータの説明:
・ 10 – ポートは 10Mbps で動作します(※本機器では未サポート)
・ 100 - ポートは 100Mbps で動作します。
・ 1000 - ポートは 1000Mbps で動作します。
・ 10000 - ポートは 10000Mbps で動作します。
・ full - ポートは全二重モードです。つまり、データは双方向に同時に通信します。
・ Half - ポートは半二重モードです。つまり、データは両方向に通信できますが、一度に一方向のみ通信できます(※本機器では未サポート)。

■設定モード:インタフェースコンフィグレーションモード

39. power inline

■説明:
イーサネットケーブルを介してエンドポイントまたは受電装置に電力を供給するために、指定ポート上の PoEを有効/無効にします。

■構文:power inline { enable | disable }

■設定モード:インタフェースコンフィグレーションモード

40. power inline limit

■説明:
イーサネットケーブルを介してエンドポイントまたは受電装置に電力を供給するために、指定ポート上の PoEを制限します。

■構文:power inline limit { auto | <value> }

■パラメータの説明:
・ auto - 十分な電力が利用可能な場合、デバイスを検出後に自動的に電力を PoE ポートに割り当てます。
・ <value> - 最大ワット数機能により、ポートに割り当てられる電力が制限されます。

■設定モード:インタフェースコンフィグレーションモード

41. reboot

■説明:このコマンドはスイッチを再起動します

■構文:reboot

■設定モード:特権EXECモード

42. reboot-flick

■説明:このコマンドは本機を再起動しますが、PoE はリセットしません。

■構文:reboot-flick

■設定モード:特権EXECモード

43. reset UBIRecoveryCount

■説明:UBIのリカバリ回数をリセットします。

■構文:reset UBIRecoveryCount

■設定モード:特権EXECモード

44. restore-defaults

■説明:このコマンドはデフォルト設定に戻します。

■構文:restore-defaults

■設定モード:特権EXECモード

45. restore-defaults-without-IP

■説明:IP設定以外をデフォルト設定に戻します。

■構文:restore-defaults-without-IP

■設定モード:特権EXECモード

46. save

■説明
動作中のrunning-configをNVRAMのstartup-configファイルに保存します。
ここで、running-configはルータの現在の設定であり、startupコンフィグレーションはスイッチの起動時にロードされるコンフィグレーションです。

■構文:save

■設定モード:特権EXECモード

47. set cli pagination

■説明:改ページ機能(1ページごとに「–More–」表示)を使用するかどうかを設定します。

■構文:set cli pagination {on | off}

■設定モード:グローバルコンフィグレーションモード

48. set ip http

■説明:スイッチのHTTPを有効/無効にします。

■構文:set ip http {enable | disable}

■パラメータの説明:
・ enable - 本機のHTTPを有効にします。
・ disable - 本機のHTTPを無効にします。

■設定モード:グローバルコンフィグレーションモード

49. set ip-management-vlan

■説明:IP管理のVLANを設定します。

■構文:
・ set ip-management-vlan <integer(1-4094)>

■パラメータの説明:
・ <integer(1-4094)> – Vlan id.

■設定モード:グローバルコンフィグレーションモード

50. set sntp client

■説明:SNTP クライアント モジュールを有効/無効にします。

■構文:set sntp client {enabled | disabled}

■パラメータの説明:
・ enabled - SNTP クライアント モジュールを有効にし、時刻同期の要求をホストに送信します。
・ disabled - SNTP クライアント モジュールを無効にし、時刻同期の要求はホストに送信しません。

■設定モード:SNTPコンフィグレーションモード

51. set sntp client clock-summer-time

■説明:
このコマンドは DST (サマータイム) を有効にします。DST は、日の出と日の入りの両方が遅くなるように時計を早めに設定するシステムです。多くの国が DST を採用していますが、その開始と終了に関しては、ほとんどの国が独自の規則と規制を設けています。DST の日付は年によって変更される場合があります。

このコマンドの no 形式を使用すると、サマータイムが無効になります。

■構文:
・ set sntp client clock-summer-time <start week-day-month,hh:mm><end week-day-month,hh:mm>
・ Eg: set sntp client clock-summer-time First-Sun-Mar,05:10 Second-Sun-Nov,06:10
・ no sntp client clock summer-time

■パラメータの説明:
・ week-day-month －リストを以下に示します。
・ week:First, Second, Third, Last (※Forthは、入力不可)
・ day:Sun, Mon, Tue, Wed, Thu, Fri, Sat
・ month:Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec
・ hh:mm - 時間と分単位の時間

■設定モード:SNTPコンフィグレーションモード

52. set sntp client port

■説明:
クライアント接続を待機している サーバ上のポートを指す SNTP クライアントのリスニング ポートを設定します(値の有効範囲:1 ～ 65535)。
このコマンドの no 形式を使用すると、SNTP クライアントのリスニング ポートが削除され、デフォルト値が設定されます。

■構文:
・ set sntp client port <integer(1-65535)>
・ no sntp client port

■設定モード:SNTPコンフィグレーションモード

53. set sntp client time-zone

■説明:
UTC を基準にしてシステムのタイムゾーンを設定します。
no 形式のコマンドは、システムのタイムゾーンを GMT にリセットします。

■構文:
・ set sntp client time-zone <UTC-offset value as (+HH:MM /- HH:MM)(+00:00 to +14:00)/ (-00:00 to -12:00)>
Eg: +05:30
・ no sntp client time-zone

■パラメータの説明:

・ +/- - クライアントのタイムゾーンを UTCの前後に設定します。＋は順方向のタイム ゾーン、ーは逆方向のタイム ゾーンを表します。
・ UTC-offset value as - UTC オフセット値を時間単位で設定します。
  - +00:00 to +14:00
  - -00:00 to -12:00

■設定モード: SNTPコンフィグレーションモード

54. set sntp unicast-server

■説明:
SNTPユニキャストサーバを設定します。
このコマンドの no 形式を使用すると、SNTPユニキャストサーバ属性が削除され、デフォルト値に戻ります。

■構文:
・ set sntp unicast-server {ipv4 <ucast_addr> | domain-name <string(64)>} [port <integer(1-65535)>]
・ no sntp unicast-server {ipv4 <ucast_addr> | domain-name <string(64)>}

■パラメータの説明:

・ ipv4 <ucast_addr> -SNTPユニキャストサーバのIPv4アドレスを設定します。
・ domain-name <string(64)> -ユニキャストサーバのドメイン名を設定します。この値は、最大サイズが 64 の文字列です。
・ port <integer(1-65535)> - 選択した サーバのポート識別子番号を選択します(値の有効範囲:1 ～ 65535)。

■設定モード:SNTPコンフィグレーションモード

55. set switch-name

■説明:このコマンドはスイッチの名前を設定します。

■構文:set switch-name <20文字まで>

■設定モード:グローバルコンフィグレーションモード

56. set system description

■説明:このコマンドはシステムの説明を設定します。

■構文:set system description <255文字まで>

■設定モード:グローバルコンフィグレーションモード

57. show activepartition

■説明:アクティブなイメージ パーティションを表示します。

■構文:show activepartition

■設定モード:特権EXECモード

58. show cli

■説明:EXEC タイムアウトなどの TTY 回線情報を表示します。

■構文:show cli

■設定モード:特権EXECモード

59. show clock

■説明:システムの日時を表示します。

■構文:show clock

■設定モード:特権EXECモード

60. show clock properties

■説明:プライマリ システムのクロック情報を表示します。

■構文:show clock properties

■設定モード:特権EXECモード

61. show device temperature

■説明:機器の現在の温度を表示します。

■構文:show device temperature

■設定モード:特権EXECモード

62. show flow-control

■説明:フロー制御情報を表示します。

■構文:
・ show flow-control [interface <interface-type> <interface-id>]

■パラメータの説明:

・ <interface-type> - 指定されたタイプのインタフェースのIPインタフェースを表示します。
インタフェースは次のとおりです。
  - gigabitethernet -1 秒あたり最大 1 ギガビットのデータ転送がサポート可能な LAN 標準アーキテクチャのバージョン。
・ <interface-id> - 指定されたインタフェース識別子のIPインタフェースを表示します。これは、特定のインタフェースを表す一意の値です。この値は、スロット番号とポート番号をスラッシュで区切って組み合わせたものです(例: 0/1 は、スロット番号が「0」、ポート番号が「1」であることを表します)。

■設定モード:特権EXECモード

63. show history

■説明:最近実行されたコマンドのリストを表示します。

■構文:show history

■設定モード:特権EXECモード

64. show http server status

■説明:http サーバのステータスとHTTP ポートを表示します。

■構文:show http server status

■設定モード:特権EXECモード

65. show ip interface

■説明:IP インタフェースのステータスと設定を表示します。

■構文:

・ show ip interface [vrf <vrf-name>] [{[vlan <vlan-id> [switch <switch-name>]] | [<interface-type> <interface-id>] | [loopback<loopback-id]}]

■パラメータの説明:

・ <vrf -name– VRF>-インスタンスの名前。
・ <vlan-id>- 作成されたVLANを表す一意の値です(値の有効範囲:1 ～ 4094)。
・ <interface-type> - 指定されたタイプのインタフェースのIPインタフェースを表示します。
インタフェースは次のとおりです。
  - gigabitethernet -1 秒あたり最大 1 ギガビットのデータ転送がサポート可能な LAN 標準アーキテクチャのバージョン。
・ <interface-id> - 指定されたインタフェース識別子のIPインタフェースを表示します。これは、特定のインタフェースを表す一意の値です。この値は、スロット番号とポート番号をスラッシュで区切って組み合わせたものです(例: 0/1 は、スロット番号が「0」、ポート番号が「1」であることを表します)。
・ <loopback-id>」ループバックIDを表示します(値の有効範囲:0～100)。

■設定モード:特権EXECモード

66. show interfaces

■説明:インタフェースのステータスと設定を表示します。

■構文:

・ show interfaces [{ [<interface-type> <interface-id>][{ description | storm-control | flowcontrol | capabilities | status | port-security-state | rate-limit }]| {vlan <vlan-id> }

■パラメータの説明:

・ <interface-type> - 指定されたタイプのインタフェースのステータスと設定を表示します。
インタフェースは次のとおりです。
  - gigabitethernet -1 秒あたり最大 1 ギガビットのデータ転送がサポート可能な LAN 標準アーキテクチャのバージョン。
  - port-channel – 複数のポートが集約されたアグリゲータを表す論理インタフェース。
・ <interface-id> - 指定したインタフェース識別子のインタフェースのステータスと設定を表示します。これは、特定のインタフェースを表す一意の値です。この値は、スロット番号とポート番号をスラッシュで区切って組み合わせたものです。
例) 0/1:スロット番号が「0」、ポート番号が「1」であることを表します。
・ description - インタフェースの説明を表示します。
・ storm-control - 指定したインタフェースのブロードキャスト、マルチキャスト、およびユニキャストのストーム抑制レベルを表示します。
・ flowcontrol - 指定したインタフェースのフロー制御関連の統計情報を表示します。
・ capabilities - 指定したインタフェースのインタフェース タイプ、インタフェース速度、デュプレックス動作、およびフロー制御ステータスを表示します。
・ status - 指定したインタフェースのステータス、デュプレックスの詳細、速度、およびネゴシエーション モードを表示します。
・ port-security-state - ポート セキュリティ オプションの状態を表示します。
・ vlan <vlan-id> - VLANを表す一意の値です(値の有効範囲:1 ～ 4094)。

■設定モード:特権EXECモード

67. show interface cable-diag

■説明:
ケーブルの診断に使用されます。ケーブルに障害が発生した場合、エラーの種類とエラーが発生した位置を特定できます。

■構文:
・ show interface cable-diag Gigabitethernet <interface-id>

■パラメータの説明:
・ <interface-id> - 指定したインタフェースの識別子に関する情報を表示します。これは、特定のインタフェースを表す一意の値です。この値は、スロット番号とポート番号をスラッシュで区切って組み合わせたものです（例: 0/1 は、スロット番号が“0”、ポート番号が“1” であることを表します）。

■設定モード: 特権EXECモード

68. show interfaces - counters

■説明: 各ポートのインタフェース統計情報を表示します。

■構文: show interfaces {counters | { <interface-type> <interface-id>} counters }

■パラメータの説明:
・ counter - 使用可能なすべてのインタフェースのインタフェース統計情報を表示します。
<interface-type> - 指定されたタイプのインタフェースの IP インタフェースを表示します。
インタフェースは次のとおりです。
  - gigabitethernet -1 秒あたり最大 1 ギガビットのデータ転送がサポート可能な LAN 標準アーキテクチャのバージョン。
  - port-channel – 複数のポートが集約されたアグリゲータを表す論理インタフェース。
・ <interface-id> - 指定されたインタフェース識別子のIPインタフェースを表示します。これは、特定のインタフェースを表す一意の値です。この値は、スロット番号とポート番号をスラッシュで区切って組み合わせたものです。
例) 0/1:スロット番号が「0」、ポート番号が「1」 であることを表します。

■設定モード: 特権EXECモード

69. show interface mtu

■説明:最大伝送単位 (MTU) を表示します。

■構文:
・ show interface mtu [{ vlan <vlan-id> | port-channel <port- channel-id (1-8)> | <interface-type> <interface-id> }]

■パラメータの説明:

・ <interface-type> - 指定されたタイプのインタフェースのIPインタフェースを表示します。
インタフェースは次のとおりです。
  - gigabitethernet – 1 秒あたり最大 1 ギガビットのデータ転送がサポート可能な LAN 標準アーキテクチャのバージョン。
  - port-channel – 複数のポートが集約されたアグリゲータを表す論理インタフェース。
・ <interface-id> - 指定されたインタフェース識別子のIPインタフェースを表示します。これは、特定のインタフェースを表す一意の値です。この値は、スロット番号とポート番号をスラッシュで区切って組み合わせたものです。
・ 例) 0/1:スロット番号が「0」、ポート番号が「1」であることを表します。

■設定モード:特権EXECモード

70. show interface port-security

■説明:最大学習アドレス数とロックモードを表示します。

■構文:
show interface port-security<interface-type> <interface-id>

■パラメータの説明:
・ <interface-type> - 指定されたタイプのインタフェースのIPインタフェースを表示します。
インタフェースは次のとおりです。
  - gigabitethernet -1 秒あたり最大 1 ギガビットのデータ転送がサポート可能な LAN 標準アーキテクチャのバージョン。
  - port-channel – 複数のポートが集約されたアグリゲータを表す論理インタフェース。
・ <interface-id> - 指定したインタフェースの識別子に関する情報を表示します。これは、特定のインタフェースを表す一意の値です。この値は、スロット番号とポート番号をスラッシュで区切って組み合わせたものです(例: 0/1 は、スロット番号が“0”、ポート番号が“1” であることを表します)。

■設定モード:特権EXECモード

71. show interface sfp-info

■説明:SFP モジュールの情報を表示します。

■構文:show interface sfp-info <interface-type> <interface-id>

■パラメータの説明:

・<interface-type> - 指定されたタイプのインタフェースのIPインタフェースを表示します。
インタフェースは次のとおりです。
- gigabitethernet -1 秒あたり最大 1 ギガビットのデータ転送がサポート可能な LAN 標準アーキテクチャのバージョン。
- port-channel – 複数のポートが集約されたアグリゲータを表す論理インタフェース。

・<interface-id> - 指定されたインタフェース識別子のIPインタフェースを表示します。これは、特定のインタフェースを表す一意の値です。この値は、スロット番号とポート番号をスラッシュで区切って組み合わせたものです。
例) 0/1:スロット番号が「0」、ポート番号が「1」であることを表します。

■設定モード:特権EXECモード

72. show privilege

■説明: 現在の特権レベルを表示します。

■構文:show privilege

■設定モード:特権EXECモード

73. show sntp clock

■説明:このコマンドは現在時刻を表示します。

■構文:show sntp clock

■設定モード:ユーザ / 特権EXECモード

74. show sntp status

■説明:このコマンドは SNTP ステータスを表示します。

■構文:show sntp status

■設定モード:ユーザ / 特権EXECモード

75. show system information

■説明:このコマンドはシステム情報を表示します。

■構文:show system information

■設定モード:特権EXECモード

76. show system utilization

■説明:このコマンドはシステム使用率を表示します。

■構文:show system utiliaztion

■設定モード:特権EXECモード

77. show telnet server

■説明:Telnet サーバのステータスを表示します。

■構文:show telnet server

■設定モード:特権EXECモード

78. show UBIRecoveryCount

■説明:UBI リカバリ回数を表示します。

■構文:show UBIRecoveryCount

■設定モード:特権EXECモード

79. show users

■説明:現在のユーザに関する情報を表示します。

■構文:show users

■設定モード:特権EXECモード

80. shutdown

■説明:インタフェースの AdminStatus を down/up に設定します。

■構文:
・ shutdown
・ no shutdown

■設定モード:インタフェースコンフィグレーションモード

81. snmp trap link-status

■説明:
インタフェースでのトラップ生成を有効/無効にします。
インタフェースが linkUp または linkDown トラップを生成します。
・ linkUp トラップは、通信リンクが利用可能であり、トラフィック フローの準備ができていることを示します。
・ linkDown トラップは、通信リンクに障害が発生し、トラフィック フローの準備ができていないことを示します。

■構文
・ snmp trap link-status
・ no snmp trap link-status
・

■設定モード:インタフェースコンフィグレーションモード

82. sntp

■説明:
このコマンドは NTPコンフィグレーションモードに移行し、ユーザは SNTP コンフィグレーションモードをサポートするすべてのコマンドを実行可能になります。

■構文:sntp

■設定モード:グローバルコンフィグレーションモード

83. system contact

■説明:このコマンドは連絡先情報を設定します。

■構文:system contact <contact info>

■設定モード:グローバルコンフィグレーションモード

84. system location

■説明:このコマンドは場所の名前を設定します。

■構文:system location <location name>

■設定モード:グローバルコンフィグレーションモード

85. system mtu

■説明:すべてのインタフェースの最大伝送単位 (MTU) を設定します。

■構文:
・ system mtu <frame-size(1522-10240)>
・ no system mtu <frame-size(1522-10240)>

■パラメータの説明:
・ <frame-size(1522-10240)>-有効範囲は、1522 ～ 10240 です。

■設定モード:グローバルコンフィグレーションモードsystem name

■説明:このコマンドはシステム名を設定します。

■構文:system name <system-name>

■設定モード:グローバルコンフィグレーションモード

86. traceroute

■説明:宛先までのルートをトレースします。

■構文:traceroute {<ip-address>| hostname | ipv6 <prefix>} [max- ttl <value (2-255)>]

■パラメータの説明:
・ <ip-address> - ルートをトレースする必要のある宛先 IP アドレスを設定します。
・ <hostname> - ルートをトレースする必要のある宛先 IP ホスト名を設定します。
・ ipv6 <ipv6-address> - ルートをトレースする必要のある宛先 IPv6 アドレスを設定します。
・ [max-ttl <short (2-255)>] - トレースルートに使用される IP パケットに埋められる TTL フィールドの最大値を設定します。

■設定モード:特権EXECモード

87. username

■説明
このコマンドはユーザを作成し、そのユーザの有効なパスワードを特権レベルで設定します。
コマンドの no 形式を使用すると、ユーザは削除され、そのユーザのパスワードが無効になります。

■構文:
・ username <user-name> [password <passwd>] [privilege <1-15>]
・ no username < user-name >

■パラメータの説明:
・ <user-name> - 作成するログインユーザ名を指定します。
・ <passwd> - ユーザがシステムにログインするために入力するパスワードを指定します。
・ privilege <1-15> - CLI コマンドにアクセスするための制限をユーザに適用します(値の有効範囲:1 ～ 15)。
・ たとえば、特権レベル 4 が設定されたユーザ ID は、特権 ID が 4 以下のコマンドにのみアクセスできます。

■設定モード:グローバルコンフィグレーションモード

3.2.2 EEE/PoE

1. eee

■説明:
指定したポートで EEE(Energy Efficient Ethernet)を有効にします。
コマンドの no 形式を使用すると、指定したポートのEEEは無効になります。

■構文:
・ eee
・ no eee

■設定モード:インタフェースコンフィグレーションモード

2. power inline

■説明:
イーサネットケーブルを介してエンドポイントまたは受電装置に電力を供給するために、指定ポート上の PoEを有効/無効にします。

■構文:power inline { enable | disable }

■設定モード:インタフェースコンフィグレーションモード

3. power inline limit

■説明:
イーサネットケーブルを介してエンドポイントまたは受電装置に電力を供給するために、指定ポート上の PoE を制限します。

■構文:power inline limit { auto | <value> }

■パラメータの説明:
・ auto - 十分な電力が利用可能な場合、デバイスを検出後に自動的に電力を PoE ポートに割り当てます。
・ <value> - 最大ワット数機能により、ポートに割り当てられる電力が制限されます。

■設定モード:インタフェースコンフィグレーションモード

4. power inline priority

■説明:
指定したポート上の PoEの優先度を設定します。

■構文:
・ power inline priority { critical | high | medium | low }

■パラメータの説明:
・ PoEポートの優先度をcritical（クリティカル）に設定します。
・ high - PoEポートの優先度をmedium（高）に設定します。
・ medium - PoEポートの優先度をmedium（中）に設定します
・ low - PoE(Power Over Ethernet) ポートの優先度を低く設定します。

■設定モード:インタフェースコンフィグレーションモード

5. set poe global power threshold

■説明:
スイッチの PoEモジュールのグローバルの電力バジェットを変更します。

■構文:set poe global power threshold <value>

■設定モード:グローバルコンフィグレーションモード

6. show eee

■説明:各ポートの EEE(Energy Efficient Ethernet)情報を表示します。

■構文:show eee

■設定モード:特権EXECモード

7. show power detail

■説明:
PoE グローバル管理状態、PSE 動作ステータス、最大供給電力などの PoE電源ステータス情報を表示します。

■構文:show power detail

■設定モード:特権EXECモード

8. show power inline

■説明:
各 PSE の PoE電源装置のステータス情報を表示します。

■構文:
・ show power inline [{<interface-type> <interface-id>}]

■パラメータの説明:
・ <interface-type> - 指定されたタイプのインタフェースに関する情報を表示します。
インタフェースは次のとおりです。
  - gigabitethernet -1 秒あたり最大 1 ギガビットのデータ転送をサポートする LAN 標準アーキテクチャのバージョン。
・ <interface-id> - 指定したインタフェースの識別子に関する情報を表示します。これは、特定のインタフェースを表す一意の値です。この値は、スロット番号とポート番号をスラッシュで区切って組み合わせたものです。
例: 0/1 は、スロット番号が“0”、ポート番号が“1” であることを表します。

■設定モード:特権EXECモード

3.2.3 SSH

1. ip ssh server

■説明:
このコマンドは ssh システムを有効にします
コマンドの no 形式は ssh システムを無効にします。

■構文:
・ ip ssh server
・ no ip ssh server

■設定モード:グローバルコンフィグレーションモード

2. show ssh-configurations

■説明:SSHシステムの状態、使用するポート、暗号アルゴリズム、ハッシュアルゴリズムの情報を表示します

■構文:show ssh-configurations

■設定モード:特権EXECモード

3.2.4 PD Lifeguard

1. set pdlg

■説明:スイッチの PD Lifeguard モジュールを有効/無効にします。

■構文:
・ set pdlg {enable | disable}

■設定モード:グローバルコンフィグレーションモード

2. set pdlg port - integer

■説明:指定したポート上の PD Lifeguard モジュールを有効/無効にします。

■構文:
・ set pdlg port <integer(1-48)> {enable | disable}

■設定モード:グローバルコンフィグレーションモード

3. set pdlg port - lldp-exp-pending

■説明:LLDPを保持する時間を指定します。

■構文:
・ set pdlg port - lldp-exp-pending <value (30-600)>

■デフォルト設定: 300

■設定モード:グローバルコンフィグレーションモード

4. set pdlg port - mode

■説明:指定ポートのPD Lifeguard モードを選択します。

■構文:
・ set pdlg port <integer(1-48)> mode { auto | force-ping }

■パラメータの説明:
・ auto - PD 到達可能性は、LLDP パケット (優先) または ping IP テストによって判断されます。
・ force-ping - PD 到達可能性は ping IP テストによって判断されます。

■設定モード:グローバルコンフィグレーションモード

5. set pdlg port - ping ip

■説明:指定ポートに PD Lifeguard のping IP アドレスを設定します。

■構文:

・ set pdlg port <integer(1-48)> ping ip <ucast_addr>

■設定モード:グローバルコンフィグレーションモード

6. set pdlg port - ping interval

■説明:指定したポートのPing 間隔を設定します。

■構文:
・ set pdlg port <integer(1-48)> ping interval <integer(1-3600)>

■設定モード:グローバルコンフィグレーションモード

7. set pdlg port - ping max-try

■説明:指定したポートのPing の最大回数を設定します。

■構文:
・ set pdlg port <integer(1-48)> ping max-try <integer(1-255)>

■設定モード:グローバルコンフィグレーションモード

8. set pdlg port - pd-boot-time

■説明:機器を起動してから、デバイスを検出するまでの時間を設定します。

■構文:
・ set pdlg port <integer(1-48)> pd-boot-time <integer(50-1200)>

■パラメータの説明:
・ pd-boot-time <integer(50-1200)>: 再起動の最大再試行値は 50 ～ 1200 に設定できます。

■設定モード:グローバルコンフィグレーションモード

9. set pdlg port - reboot interval

■説明:指定したポートのLLDP満了の保持時間を設定します。

■構文:
・ set pdlg port <integer(1-48)> reboot interval <integer(1-600)>

■設定モード:グローバルコンフィグレーションモード

10. set pdlg port - reboot max-try

■説明:指定したポートでPD再起動の最大回数を設定します。

■構文:set pdlg port <integer(1-48)> reboot max-try <integer(0-20)>

■設定モード:グローバルコンフィグレーションモード

11. set pdlg port - reboot refresh

■説明:指定したポートの再起動試行回数をリセットします。

■構文:
・ set pdlg port <integer(1-48)> reboot refresh

■設定モード:グローバルコンフィグレーションモード

12. set pdlg port - reboot

■説明:指定したポートで PD Lifeguard の再起動を許可するか拒否するかを設定します。

■構文:
・ set pdlg port <integer(1-48)> reboot {allow | deny}

■パラメータの説明:
・ allow – 再起動 (再起動 + システム ログ) を許可します。
・ deny - 再起動を拒否します(システム ログのみ)。

■設定モード:グローバルコンフィグレーションモード

13. set pdlg reboot port

■説明:指定のPoE ポートを再起動します。

■構文:
・ set pdlg reboot port <integer(1-48)>

■設定モード:グローバルコンフィグレーションモード

14. show pdlg detail

■説明:PD Lifeguard のステータスの詳細を表示します。

■構文:show pdlg detail

■設定モード:特権EXECモード

15. show pdlg port

■説明：PD Lifeguard のポートごとのステータスを表示します。

■構文：show pdlg port <integer(1-48)>

■設定モード：特権EXECモード

3.2.5 Link Aggregation

1. channel-group

■説明:
スイッチ内にすでに作成されている指定ポート チャネルのメンバーとしてポートを追加してください。
このコマンドの no 形式を使用すると、すべてのポート チャネルからポートの集約は削除されます。

■構文:
・ channel-group <channel-group-number(1-8)> mode { on | active | passive }
・ no channel-group

■パラメータの説明:
・ <channel-group-number(1-8)> - 指定ポートのチャネルのメンバーとしてポートを追加してください。
作成された特定のポートチャネルを表す一意の値です(有効範囲は 1 ～ 8)。
・ active - 無条件で LACP ネゴシエーションを開始します。
・ passive - LACP パケットがピアから受信された場合にのみ LACP ネゴシエーションを開始します。
・ on - LACPを使わず、インタフェースを手動でチャネル化します。

■設定モード:インタフェースコンフィグレーションモード
※このコマンドは、PORTインタフェースモードで使用可能です。

2. lacp system-priority

■説明:
アクターのシステム ID に関連付けられた LACP 優先度を設定します。
LACPのプライオリティ値が最も小さいスイッチが、LA 内のスタンバイリンクとアクティブリンクを決定します。

■構文:
・ lacp system-priority <short(0-65535)>
・ no lacp system-priority

■設定モード:グローバルコンフィグレーションモード

3. lacp timeout

■説明:
集約リンクのタイムアウトを回避するためにポートで LACPDU を受信する LACP タイムアウト期間を設定します。
コマンドの no 形式は、LACP タイムアウト期間をデフォルト値に設定します。

■構文:
・ lacp timeout {long | short }
・ no lacp timeout

■パラメータの説明:
・ long - LACP タイムアウト期間を 90 秒に設定します。LACP PDU は 30 秒ごとに送信されます。
・ short - LACP タイムアウト期間を 3 秒に設定します。LACP PDU は毎秒送信されます。

■設定モード:インタフェースコンフィグレーションモード

4. no shutdown port-channel

■説明:
スイッチのLA機能を開始して有効にし、必要なメモリをLAモジュールに割り当てます。LA機能は、本機のLAが有効な場合にのみ、使用可能になります。

LA機能により、個々のポイントツーポイントリンクをポートチャネルグループに集約できるため、既存のインタフェーステクノロジーを使用して機器間の通信チャネルの容量と可用性が向上します。

■構文:no shutdown port-channel

■設定モード:グローバルコンフィグレーションモード

5. port-channel load-balance

■説明:すべてのポートチャネルのロードバランシングポリシーを設定します。

■構文:
・ port-channel load-balance {src-mac | dest-mac | arc-dest-mac | src-ip | dest-ip | src-dest-ip | dest-l4-port | src-l4-port}

■パラメータの説明:

・ src-mac - 送信元 MACアドレスに基づいて負荷を分散します。パケット内の送信元 MACアドレスのビットは、トラフィックが送受信されるポートを選択するために使用されます。異なるホストからのパケットはチャネル内の異なるポートを使用しますが、同じホストからのパケットは同じポートを使用します。
・ dest-mac - 宛先MACアドレスに基づいて負荷を分散します。ホストのMACアドレス。パケット内の宛先 MACアドレスのビットは、トラフィックが送受信されるポートを選択するために使用されます。同じ宛先へのパケットは同じポートで送信されますが、異なる宛先へのパケットはチャネル内の異なるポートで送信されます。
・ src-dest-mac - 送信元と宛先の MACアドレスに基づいて負荷を分散します。パケット内の送信元 MACアドレスと宛先 MACアドレスのビットは、トラフィックが送受信されるポートを選択するために使用されます。
・ src-ip - 送信元 IP アドレスに基づいて負荷を分散します。パケット内の送信元 IP アドレスのビットは、トラフィックが送受信されるポートを選択するために使用されます。
・ dest-ip - 宛先 IP アドレスに基づいて負荷を分散します。パケット内の宛先 IP アドレスのビットは、トラフィックが送受信されるポートを選択するために使用されます。
・ src-dest-ip - 送信元と宛先の IP アドレスに基づいて負荷を分散します。パケット内の送信元 IP アドレスと宛先 IP アドレスのビットは、トラフィックが送受信されるポートを選択するために使用されます。
・ dest-l4-port - 宛先レイヤー4 ポートに基づいて負荷を分散します。パケット内の宛先レイヤー 4 ポートのビットは、トラフィックが送受信されるポートを選択するために使用されます。
・ src-l4-port - 送信元レイヤー 4 ポートに基づいて負荷を分散します。パケット内の送信元レイヤー 4 ポートのビットは、トラフィックが送受信されるポートを選択するために使用されます。

■設定モード:グローバルコンフィグレーションモード

6. show etherchannel

■説明:
すべてのポート チャネル グループの EtherChannel 情報を表示します。この情報には、ポート チャネル モジュールの admin および oper ステータス、および各グループのプロトコル操作モードのステータスが含まれます。

■構文:
・ show etherchannel [<channel-group-number>{ detail | load- balance | port | port-channel | summary | protocol}]

■パラメータの説明:
・ <channel-group-number (1-8)> – ここで指定したポートチャネルグループのEtherChannel情報を表示します。
・ detail – EtherChannelの詳細情報を表示します。
・ load-balance – 各ポートチャネルグループに適用されるロードバランシングポリシーを表示します。
・ port – 各グループのプロトコル動作モードについて、ステータスとポートの詳細を表示します。
・ port-channel – ポートチャネルモジュールの詳細を表示します。
・ summary – ポートチャネルモジュールの簡易情報を表示します。
・ protocol – 各ポートチャネルグループのプロトコル動作モードの状態を表示します。

■設定モード: 特権EXECモード

3.2.6 mirror

1. monitor session - destination

■説明:
ミラーリングセッションの宛先ポートを設定します。
このコマンドの no 形式を使用すると、ミラーリングセッションの宛先ポート設定は削除されます。

■構文:
・ monitor session <session-id (1-3)> destination { interface<interface-type> <interface-id>} [allow-ingress]
・ no monitor session <session-id (1-3)> destination{ interface<interface-type> <interface-id> }[allow-ingress]

■パラメータの説明:
・ session-id - ミラーリングセッションのインデックスを指定します(値の有効範囲:1 ～ 3)。
・ interface - ミラーリングセッションの宛先ポートを指定します。
・ <interface-type> - 指定されたタイプのインタフェースのIPインタフェースを表示します。
インタフェースは次のとおりです。
  - gigabitethernet -1 秒あたり最大 1 ギガビットのデータ転送をサポートする LAN 標準アーキテクチャのバージョン。
  - port-channel – 複数のポートが集約されたアグリゲータを表す論理インタフェース。
・ <interface-id> – インタフェース識別子。これはスロット番号とポート番号の組み合わせです。
・ allow-ingress- 宛先ポートへのパケットの進入を許可します。

■設定モード:グローバルコンフィグレーションモード

2. monitor session - source

■説明:
ミラーリングセッションの送信元ポート/リモート VLAN を設定します。
コマンドの no 形式を使用すると、ミラーリングセッションの送信元ポート/リモート VLAN 設定は削除されます。

■構文:
・ monitor session <session-id (1-3)> { source { interface<interface-type> <interface-id> [{ rx | tx | both }]}
・ no monitor session <session-id (1-3)> { source{interface<interface-type> <interface-id> [{rx|tx|both}]}

■パラメータの説明:
・ session-id - セッションを識別するために使用されるセッション番号を設定します。
・ interface - トラフィックをミラーリングする送信元 インタフェースを設定します。提供する詳細は次のとおりです。
・ <interface-type> - インタフェースのタイプを設定します。
インタフェースは次のとおりです。
  - gigabitethernet -1 秒あたり最大 1 ギガビットのデータ転送をサポートする LAN 標準アーキテクチャのバージョン。
・ <interface-id> - インタフェース識別子を設定します。これは、特定のインタフェースを表す一意の値です。この値は、スロット番号とポート番号をスラッシュで区切って組み合わせたものです。
・ rx - 受信したトラフィックをミラーリングします
・ tx - 送信トラフィックをミラーリングします
・ both - モニタリングするトラフィックの方向を指定します。トラフィックの方向が指定されていない場合、送信トラフィックと受信トラフィックの両方がミラーリングされます。

■設定モード:グローバルコンフィグレーションモード

3. no monitor session

■説明:ミラーリング設定を削除するために使用されます。

■構文:
・ no monitor session { <session-id (1-3)>}

■パラメータの説明:
・ <session-id (1-3)> - ミラーリングセッションのインデックスを指定します。

■設定モード:グローバルコンフィグレーションモード

4. show monitor

■説明:システム内のミラーリング情報を表示します。

■構文:
・ show monitor { <session <session-id (1-3)> | all } [detail]

■パラメータの説明:
・ <session-id (1-3)> - ミラーリングセッションの指定されたインデックスのミラーリング情報を表示します。
・ all - すべてのセッションのミラーリング情報を表示します。
・ detail - セッションに関する詳細情報を表示します。

■設定モード:特権EXECモード

3.2.7 STP

1. clear spanning-tree counters

■説明:すべてのブリッジおよびポート単位のスパニングツリーの統計情報を削除します。

・RSTP の場合、情報には次の数が含まれます。
　・フォワーディング状態への遷移
　・送受信されたRSTP BPDU数
　・送受信されたConfig BPDU数
　・TCN BPDU 受信/送信数
　・送信された無効な BPDU カウント
　・ポートプロトコル移行数

・MSTP の場合、情報には次の数が含まれます。
　・ポートのフォワード遷移
　・ポートが受信した BPDU数
　・ポートが送信した BPDU数
　・ポートが受診した無効な BPDU
　・ポートプロトコルの遷移回数
　・MSTI ごとに送受信されるBPDU数

統計情報は、本機のスパニングツリー機能が動作している場合にのみ削除できます。
機能が無効な場合は、スパニングツリーのモードを有効にする必要があります。

■構文:
・clear spanning-tree [mst <instance-id>] counters[interface<interface-type> <interface-id>]

■パラメータの説明:
・mst <instance-id>] - スイッチ内ですでに作成されている MSTインスタンスに固有の統計カウンターをクリアします（値の有効範囲は 1 ～ 64）。このオプションは、スパニングツリー モードが"mst"に設定されている場合にのみ適用されます。
・interface - 指定されたポートのすべてのポートのレベルのスパニングツリーの統計情報をクリアします。
・<interface-type> - 指定されたタイプのインタフェースのIPインタフェースを表示します。
　インタフェースは次のとおりです。
　　➢ gigabitethernet -1 秒あたり最大 1 ギガビットのデータ転送をサポートする LAN 標準アーキテクチャのバージョン。
　　➢ port-channel – 複数のポートが集約されたアグリゲータを表す論理インタフェース。
・<interface-id> - 指定されたインタフェース識別子のすべてのポート単位のスパニングツリーの統計情報をクリアします。これは、特定のインタフェースを表す一意の値です。この値は、スロット番号とポート番号をスラッシュで区切って組み合わせたものです（例: 0/1 は、スロット番号が「0」、ポート番号が「1」であることを表します）。インタフェース タイプのポートチャネルの場合、ポートチャネル ID のみが提供されます（例: 1 はポートチャネル ID を表します）。

■設定モード:グローバルコンフィグレーションモード

2. instance

■説明:
MSTインスタンスを設定、それをVLAN にマッピングします。
このコマンドの no 形式を使用すると、インスタンスが削除され、MSTインスタンスから特定の VLAN のマッピングが解除されます。

■構文:
・ instance <instance-id(1-4 | 4094)> vlan <vlan-range>
・ no instance <instance-id (1-4 | 4094)> [vlan <vlan-range>]

■設定モード:MSTコンフィグレーションモード

3. lbd

■説明:ループバック検出を有効/無効にします。

■構文:lbd { enable | disable }

■設定モード:グローバルコンフィグレーションモード

4. mac-address-table aging-time

■説明:
動的に学習されたMACアドレステーブルのエントリをエージングアウトするためのタイムアウト期間 (秒単位) を設定します。
設定したエージタイムが経過すると、動的に学習されたエントリは削除されます。
トラフィックが頻繁に伝送されない場合、エージングタイムの値を高くすると、動的エントリをより長時間記録する際に有用です。これにより、フラッディングの可能性が軽減されます。

このコマンドの no 形式は、MACアドレス テーブル内のエントリのエージングタイムをデフォルト値にリセットします。

■構文:
・ mac-address-table aging-time <10-630 seconds>
・ no mac-address-table aging-time

■設定モード:グローバルコンフィグレーションモード

5. mac-address-table static unicast

■説明:
転送データベースに静的ユニキャスト MACアドレスを設定します。
このコマンドの no 形式を使用すると、設定済みの静的ユニキャスト MACアドレスが転送データベースから削除されます。

■構文:
・ mac-address-table static unicast <aa:aa:aa:aa:aa:aa> vlan <vlan-id> interface <interface-type> <interface-id>
・ no mac-address-table static unicast <aa:aa:aa:aa:aa:aa> vlan<vlan-id >

■パラメータの説明:
・ <aa:aa:aa:aa:aa:aa> - 静的ユニキャスト宛先 MACアドレスを設定します。指定された MACアドレスを持つ受信パケットが処理されます。
・ vlan <vlan-id> - 指定された VLAN の静的ユニキャスト宛先 MACアドレスを設定します(値の有効範囲:1 ～ 4094)。
・ <vlan –id> - VLANを表す一意の値です(値の有効範囲:1 ～ 4094)。
・ interface - メンバー ポートのインタフェース タイプと ID を設定します。
・ <interface-type> - 指定されたタイプのインタフェースのメンバー ポートを設定します。
インタフェースは次のとおりです。
  - gigabitethernet -1 秒あたり最大 1 ギガビットのデータ転送をサポートする LAN 標準アーキテクチャのバージョン。
・ <interface-id> - 指定されたインタフェース識別子のメンバー ポートを設定します。これは、特定のインタフェースを表す一意の値です。この値は、スロット番号とポート番号をスラッシュで区切って組み合わせたものです(例: 0/1-2、0/3など)。

■設定モード:グローバルコンフィグレーションモード

6. name

■説明:MSTリージョンの名前を設定します。

名前は一意であり、特定のMSTリージョンを識別するために使用されます。各MSTリージョンには複数のスパニングツリーインスタンスが含まれており、ISTと呼ばれるスパニングツリーの特別なインスタンスを実行して、他の STPインスタンスの STP トポロジ情報を配布します。

このコマンドの no 形式を使用すると、名前がデフォルト値にリセットされます。

■構文:
・ name <string(32文字)>
・ no name

■設定モード:MSTコンフィグレーションモード

7. revision

■説明:
MST 領域のリビジョン番号を設定します(値の有効範囲:0 ～ 65535)。
このコマンドの no 形式を使用すると、リビジョン番号がデフォルト値にリセットされます。

■構文:
・ revision <value(0-65535)>
・ no revision

■設定モード:MSTコンフィグレーションモード

8. spanning-tree

■説明:
選択したスパニングツリー モードのスパニングツリーの動作を有効にします。

スパニングツリー動作はパスの冗長性を提供し、ステーション間の複数のアクティブ パスによってネットワーク内に発生する不正なループを防ぎます。このようなループを論理的に切断し、ループするトラフィックがネットワークのパフォーマンスを低下させるのを防ぎます

このコマンドの no 形式を使用するとブリッジのスパニングツリー動作が無効になります。
スパニングツリー モードが変更されると、本機のスパニングツリー動作が自動的に有効になります。

✏スパニングツリー機能が有効な場合にのみ、スパニングツリー動作を有効にできます。
機能が無効な場合は、スパニングツリーのモードを”mst”に設定してください。

■構文:
・ spanning-tree
・ no spanning-tree

■設定モード:グローバルコンフィグレーションモード

9. spanning-tree auto-edge

■説明:
インタフェースのEdge port パラメータの自動検出を有効にします。

このコマンドの no 形式を使用すると、インタフェースのEdge port パラメータの自動検出が無効になります。スパニングツリーのモードを変更しても、Edge port パラメータの自動検出は無効になります。

自動検出を有効にすると、Edge port パラメータが自動的に検出され、設定されます。ポートで BPDU が受信されない場合、ポートはEdge port として設定されます。

BPDU を受信した場合、ポートはnon-edgeポートとして設定されます。

✏ エッジポートパラメータの自動検出は、スパニングツリー機能が有効な場合にのみ有効にできます。
機能が無効な場合は、スパニングツリーのモードを”mst”に設定してください。

■構文:
・ spanning-tree auto-edge
・ no spanning-tree auto-edge

■設定モード:インタフェースコンフィグレーションモード
※PORT/PORT-CHANNEL インタフェース モードで使用できます。

10. spanning-tree forward-time

■説明:
このコマンドはスパニングツリーの転送タイマーを設定し、コマンドの no 形式は転送タイマーをデフォルト値に設定します。
フォワード タイマーは、ポートがスパニングツリーの状態をリスニング状態からラーニング状態、およびラーニング状態からフォワーディング状態に遷移する際の待機時間です。タイマー値の有効範囲は 4 ～ 30 秒です。

✏ スパニングツリー転送タイマーに設定する値は、次の条件を満たす必要があります。
2* (forward-time - 1) >= max-age, and max-age >= 2 * (hello-time +1)

■構文:
・ spanning-tree forward-time <seconds(4-30)>
・ no spanning-tree forward-time

■設定モード:グローバルコンフィグレーションモード

11. spanning-tree hello-time

■説明:
スパニングツリーの Hello時間を設定します。
このコマンドの no 形式を使用すると、Hello時間がデフォルト値にリセットされます。

Hello時間は、BPDU 間の間隔 (秒単位) を表します。この値は 1 秒、または 2 秒です。
この値は、アクティブなすべての MSTI に適用されます。

■構文:
・ spanning-tree hello-time<value(1-2)>
・ no spanning-tree hello-time

■設定モード:グローバルコンフィグレーションモード

12. spanning-tree max-age

■説明:
max-age タイマーは、任意のポート上のネットワークから学習したスパニングツリープロトコル情報が破棄されるまでの時間 (秒単位) を示します。タイマー値の有効範囲は 6 ～ 40 秒です。

コマンドの no 形式は、max-age タイマーをデフォルト値に設定します。

✏ スパニングツリー転送タイマーに設定する値は、次の条件を満たす必要があります。
2* (forward-time - 1) >= max-age、および max-age >= 2 * (hello-time +1)

■構文:
・ spanning-tree max-age <seconds(6-40)>
・ no spanning-tree max-age

■設定モード:グローバルコンフィグレーションモード

13. spanning-tree mode

■説明:
スパニングツリーのプロトコルを次のように設定します。
・ 実行すると、スパニングツリー動作が有効になり、スパニングツリー機能が開始される。
・ 現在選択されているスパニングツリー タイプが有効になり、既存のスパニングツリー タイプは無効になる。

■構文:
・ spanning-tree mode {mst|rst}

■パラメータの説明:
・ mst - 不正なループを防止するために MSTP を実行するようにスイッチを設定します。MSTP は、VLAN ごとにスパニングツリーを設定するか、スパニングツリーごとに複数の VLAN を設定します。ベース ブリッジ モードがトランスペアレントブリッジとして設定されている場合、モードを mst として設定することはできません。
・ rst - 不正なループを防止するために RSTP を実行するようにスイッチを設定します。

■設定モード:グローバルコンフィグレーションモード

14. spanning-tree transmit hold-count

■説明:
スイッチの送信ホールドカウント値を設定します。送信ホールドカウント値は、スイッチの最大送信レートを制限し、フラッディングを回避するために使用されるカウンタです。この値は、特定の Hello時間間隔で送信できるパケットの最大数を指定します(値の有効範囲:1 ～ 10)。

このコマンドの no 形式を使用すると、送信ホールドカウントがデフォルト値に設定されます。スパニングツリーのモードを変更しても送信ホールドカウントはデフォルト値に変更されます。

✏ 送信ホールドカウント値は、スパニングツリー機能が有効な場合にのみ有効にできます。
機能が無効な場合は、スパニングツリーのモードを”mst”に設定してください。

■構文:
・ spanning-tree transmit hold-count <value (1-10)>
・ no spanning-tree transmit hold-count

■パラメータの説明:
・ hold-count - この値は、特定の Hello時間間隔内に送信できるパケットの最大数を指定します(値の有効範囲: 1 ～ 10)。

■設定モード:グローバルコンフィグレーションモード

15. spanning-tree mst forward-time

■説明:
このコマンドはスパニングツリーの転送タイマーを設定し、コマンドの no 形式は転送タイマーをデフォルト値に設定します。
フォワードタイマーは、ポートがスパニングツリーの状態をディスカーディング状態からラーニング状態、およびラーニング状態からフォワーディング状態に遷移する際の待機時間です。タイマー値の有効範囲は 4 ～ 30 秒です。

✏ スパニングツリー転送タイマーに設定する値は、次の条件を満たす必要があります。
2* (forward-time - 1) >= max-age, and max-age >= 2 * (hello-time +1)

✏ STP 転送タイマーは、スパニングツリー機能が有効な場合にのみ有効にできます。
機能が無効な場合は、スパニングツリー機能を有効にしてください。

■構文:
・ spanning-tree mst forward-time <seconds(4-30)>
・ no spanning-tree mst forward-time

■設定モード:グローバルコンフィグレーションモード

16. spanning-tree mst max-age

■説明:
スパニングツリーの max-age タイマーを設定します。max-age タイマーは、任意のポート上のネットワークから学習したスパニングツリープロトコル情報が破棄されるまでの時間(秒単位)を示します。タイマー値の有効範囲は 6 ～ 40 秒です。
コマンドの no 形式は、max-age タイマーをデフォルト値に設定します。

✏ スパニングツリー転送タイマーに設定する値は、次の条件を満たす必要があります。
2* (forward-time - 1) >= max-age, and max-age >= 2 * (hello-time +1)

✏STP 転送タイマーは、スパニングツリー機能が有効な場合にのみ有効にできます。
機能が無効な場合は、スパニングツリー機能を有効にしてください。

■構文:
・ spanning-tree mst max-age <seconds(6-40)>
・ no spanning-tree mst max-age

■設定モード:グローバルコンフィグレーションモード

17. spanning-tree mst hello-time

■説明:
スパニングツリーの Hello時間を設定します。

このコマンドの no 形式を使用すると、Hello時間がデフォルト値にリセットされます。

Hello時間は、BPDU 間の間隔 (秒単位) を表します。
この値は 1 秒または 2 秒です (この値は、アクティブなすべての MSTI に適用されます)。

✏本コマンドは、本機のスパニングツリー機能が動作している場合にのみ正常に実行できます。
スパニングツリーのモードを"mst"に設定する必要があります。

■構文:
・ spanning-tree mst hello-time<value(1-2)>
・ no spanning-tree mst hello-time

■設定モード:グローバルコンフィグレーションモード / ポートインタフェースモード

18. spanning-tree mst max-instance

■説明:
作成できるアクティブな MSTI の最大数を設定します(値の有効範囲:1 ～ 64)。

このコマンドの no 形式を使用すると、MSTインスタンスの最大値がデフォルト値にリセットされます。

✏本コマンドはスイッチ内でスパニングツリー機能が起動し有効な場合のみ正常に実行できます。
スパニングツリーのモードを”mst” に設定する必要があります。

■構文:
・ spanning-tree mst max-instance <short(1-64)>
・ no spanning-tree mst max-instance

■設定モード:グローバルコンフィグレーションモード

19. spanning-tree mst root

■説明:
インタフェース上で BPDU (Bridge Protocol Data Unit) の送受信を有効にします。

spanning-tree priorityは、既存のコマンドの標準で実装されています。既存のコマンドと同様に動作します。
コマンドの no 形式は、インタフェースでの BPDU の送受信を無効にします。

✏このコマンドは次の場合にのみ実行されます。
- インスタンスが作成されている場合
- スパニングツリーのモードは”mst”に設定されている場合

■構文:
・ spanning-tree mst {instance-id <instance-id(1-64)>} root{primary | secondary}
・ no spanning-tree mst {instance-id <instance-id(1-64)>} root

■パラメータの説明:
・ instance-id <instance-id(1-64)> - スイッチ内にすでに作成されている MSTインスタンスの ID を設定します(値の有効範囲:1 ～ 64)。このオプションは、スパニングツリー モードが”mst”に設定されている場合にのみ適用されます。
・ primary - スイッチをスパニングツリーインスタンスのルートブリッジにできるように、スイッチに十分高い優先度 (低い値) を設定します。優先度の値は “24576” に設定されます。
・ secondary - スイッチをセカンダリブリッジとして設定します。プライマリブリッジに障害が発生した場合、セカンダリとして設定したスイッチをプライマリブリッジとします。優先度の値は “28672”に設定されます。

■設定モード:グローバルコンフィグレーションモード

20. spanning-tree mst configuration

■説明
このコマンドは MSTP コンフィグレーション モードに入ります。
インスタンス固有のMSTリージョン設定を行うことができます。

✏本コマンドはスイッチ内でスパニングツリー機能が起動し有効な場合のみ正常に実行できます。
スパニングツリーのモードを”mst”に設定してください。

■構文：spanning-tree mst configuration

■設定モード：グローバルコンフィグレーションモード

21. spanning-tree mst- Properties of an interface for MSTP

■説明：
ポート内の指定された MSTI のポート関連のスパニングツリー情報を設定します。
このコマンドの no 形式を使用すると、ポートのスパニングツリー情報がデフォルト値にリセットされます。

✏本コマンドは、スパニングツリー機能が動作している場合にのみ正常に実行できます。
スパニングツリーのモードを”mst”に設定してください。

■構文：
- spanning-tree mst <instance-id(1-64)> { cost <value(1- 200000000)>| port-priority <value(0-240)> | disable }
- no spanning-tree mst <instance-id(1-64)>{cost|port-priority | disable}

■パラメータの説明：
- <instance-id(1-64)> - スイッチ内にすでに作成されている MSTインスタンスの ID を設定します（値の有効範囲：1 ～ 64）。
- cost<value(1-200000000)> - この特定のポートを含むパスのパスコストに寄与するポートのパスコスト値を設定します。パスのパスコストは、ルートに到達する最短パスの計算中に使用されます。パスコストは、ルート ポートと指定ポートの間の距離を表します（値の有効範囲：1 ～ 200000000）。動的パスコスト計算機能または LAGG 速度機能が有効な場合でも、設定されたパスコストが使用されます。
- port-priority<value(0-240)> - ポートに割り当てられる優先度の値を設定します。この値は、ポートの役割を選択時に使用されます（値の有効範囲：0 ～ 240）。値は16の倍数（0, 16, 32, 48, …）で設定する必要があります。
- すべてのインタフェースのプライオリティ値が同じである場合、MSTP は番号が最も小さいインタフェースをフォワード状態にして、他のすべてのインタフェースをブロックします。
- disable - ポート上のスパニングツリー操作を無効にします。ポートは、ネットワーク内の不正なループを防止するためのスパニングツリーの実行には参加しません。

■設定モード：インタフェースコンフィグレーションモード
※このコマンドは、PORT/PORT-CHANNEL インタフェース モードで使用できます。

22. spanning-tree priority

■説明:
スイッチに割り当てられる優先度の値を設定します。
このコマンドの no 形式を使用すると、優先度がデフォルト値にリセットされます。スパニングツリーのモードを変更しても、プライオリティ値はデフォルト値に変更されます。

RSTP では、この値はルートの選出中に使用されます。MSTP では、この値は CIST ルート、CIST 地域ルート、および IST ルートの選択中に使用されます。

✏スイッチ内でスパニングツリー機能が有効な場合のみ、スイッチ内でプライオリティ値を設定できます。
機能が無効な場合は、スパニングツリーのモードを”mst”に設定してください。

■構文:
・ spanning-tree [mst <instance-id>] priority <value(0-61440)>
・ no spanning-tree [mst <instance-id(1-64)>] priority

■パラメータの説明:
・ mst <instance-id> - スイッチ内にすでに作成されている MSTインスタンスの ID を設定します(値の有効範囲:1 ～ 64)。値 4094 は、PBB-TE をサポートする機器でのみ使用できます。この特別な値は、ESP によって使用される VID を識別する PTETID を表します。このオプションは、スパニングツリー モードが”mst”に設定されている場合にのみ適用されます。
・ priority <value(0-61440)> - スイッチと MSTIのプライオリティ値を、それぞれ RSTP と MSTP で設定します(この値の有効範囲:0 ～ 61440)。値は4096の倍数（0, 4096, 8192, 12288, …）で設定する必要があります。

■設定モード:グローバルコンフィグレーションモード

23. spanning-tree - Properties of an interface

■説明:
すべての種類の STP のポート関連のスパニングツリー情報を設定します。これは、RSTP/MSTP モードの任意のポートに適用できます。このコマンドは、自動ポート作成機能が無効になっている場合に STP にポートを設定ます。

このコマンドの no 形式を使用すると、ポート関連のスパニングツリー情報がデフォルト値にリセットされます。スパニングツリーのモードを変更しても、ポート関連のスパニングツリー情報はデフォルト値に変更されます。このコマンドは、自動ポート作成機能が無効になっている場合、STPポートも削除します。

✏ STP モジュールでは、ポートが任意のコンテキストにマッピングされるたびに、インタフェースで STP を有効にするかどうかに関係なく、対応するポートが作成されます。これは STP スケーリングの問題につながりますが、この問題は、STP モジュール自体でポート エントリの作成を STP モジュールで制御することで解決されます。

■構文:
・ spanning-tree [{cost value(0-200000000)>|disable|link-type{point-to-point|shared}|
・ no spanning-tree [{cost disable|link-type|}]

■パラメータの説明:
・ cost <value(0-200000000)> - パスコスト値を設定します。値の範囲は1～200000000です。"0"はオートを示します。ルートブリッジまでのコスト値の合計をルートパスコストといい、ルートパスコストが最も小さいインタフェースがルートポートになります。ルートポートにならなかったインタフェースは、接続スイッチとの間でルートパスコストが小さい方を指定ポートとします。ルートポートにも指定ポートにもならなかったポートはブロッキングポートになります。
・ disable - ポート上のスパニングツリー操作を無効にします。ポートは、ネットワーク内の不正なループを防止するためのスパニングツリー動作の実行には参加しません。
・ link-type - ポートに接続されている LAN セグメントのリンク ステータスを設定します。利用可能なオプションは次のとおりです。
  - point-to-point – ポートはポイントツーポイントリンクに接続されているかのように扱われます。
  - shared - ポートは共有メディア接続を使用しているかのように扱われます。

■設定モード:インタフェースコンフィグレーションモード
※このコマンドは、PORT/PORT-CHANNEL インタフェース モードで使用できます。

24. show dot1d mac-address-table

■説明:
VLANベースのブリッジ モードがトランスペアレントブリッジである場合に、FDB テーブルに作成されたすべての動的ユニキャストおよびマルチキャストMACアドレスのエントリを表示します。

これらのエントリには、ユニキャスト/マルチキャストMACアドレス、メンバー ポート、エントリのタイプ (学習済みなど) が含まれます。

■構文:
・ show dot1d mac-address-table [address <aa:aa:aa:aa:aa:aa> [{interface <interface-type> <interface-id> | switch<context_name>}]

■パラメータの説明:
・ address <aa:aa:aa:aa:aa:aa> - 指定されたユニキャスト/マルチキャストMACアドレスの MACアドレス テーブルに作成されたすべての動的ユニキャストおよびマルチキャストMAC エントリを表示します。
・ <interface-type> - 指定されたタイプのインタフェースのステータスと設定を表示します。
インタフェースは次のとおりです。
  - gigabitethernet -1 秒あたり最大 1 ギガビットのデータ転送をサポートする LAN 標準アーキテクチャのバージョン。
・ port-channel – 複数のポートが集約されたアグリゲータを表す論理インタフェース。
・ switch <context_name> - 指定されたコンテキストの VLAN エントリ関連情報または既存の VLAN の総数を表示します。この値は、本機のコンテキストの一意の名前を表します。この値は、最大サイズが 32の文字列です。このパラメータは、マルチインスタンス機能に固有です。

■設定モード:特権EXECモード

25. show dot1d mac-address-table static multicast

■説明:
VLANベースのブリッジ モードがトランスペアレントブリッジの場合に、FDB テーブルに作成されたすべてのスタティック マルチキャストMACアドレスのエントリを表示します。

これらのエントリには、マルチキャストMACアドレス、メンバー ポート、受信側ポート、エントリのステータス (静的など)、および表示されるエントリの総数が含まれます。

■構文:
・ show dot1d mac-address-table static multicast [address<aa:aa:aa:aa:aa:aa>] [interface <interface-type> <interface-id>]

■パラメータの説明:

・ address <aa:aa:aa:aa:aa:aa> - 指定のユニキャスト/マルチキャストMACアドレスの MACアドレス テーブルに作成されたすべての静的ユニキャストおよびマルチキャストMAC エントリを表示します。
・ <interface-type> - 指定のタイプのインタフェースのステータスと設定を表示します。
インタフェースは次のとおりです。
  - gigabitethernet -1 秒あたり最大 1 ギガビットのデータ転送をサポートする LAN 標準アーキテクチャのバージョン。
  - port-channel – 複数のポートが集約されたアグリゲータを表す論理インタフェース。
・ switch <context_name> - 指定のコンテキストの VLAN エントリ関連情報または既存の VLAN の総数を表示します。この値は、本機のコンテキストの一意の名前を表します。この値は、最大サイズが 32の文字列です。このパラメータは、マルチインスタンス機能に固有です。

■設定モード:特権EXECモード

26. show dot1d mac-address-table static unicast

■説明:
VLANベースのブリッジ モードがトランスペアレントブリッジである場合に、FDB テーブルに作成されたすべてのスタティック ユニキャスト MACアドレスのエントリを表示します。

これらのエントリには、ユニキャストMACアドレス、メンバー ポート、レシーバ ポート、エントリのステータス(“static”など)、および表示されるエントリの総数が含まれます。

■構文:
・ show dot1d mac-address-table static unicast [address<aa:aa:aa:aa:aa:aa>] [interface <interface-type> <interface-id>]

■パラメータの説明:
・ address <aa:aa:aa:aa:aa:aa> - 指定のユニキャスト/マルチキャストMACアドレスの MACアドレス テーブルに作成されたすべての静的ユニキャストおよびマルチキャストMAC エントリを表示します。
・ <interface-type> - 指定のタイプのインタフェースのステータスと設定を表示します。
インタフェースは次のとおりです。
  - gigabitethernet -1 秒あたり最大 1 ギガビットのデータ転送をサポートする LAN 標準アーキテクチャのバージョン。
  - port-channel – 複数のポートが集約されたアグリゲータを表す論理インタフェース。
・ switch <context_name> - 指定のコンテキストの VLAN エントリ関連情報または既存の VLAN の総数を表示します。この値は、本機のコンテキストの一意の名前を表します。この値は、最大サイズが 32の文字列です。このパラメータは、マルチインスタンス機能に固有です。

■設定モード:特権EXECモード

27. show lbd port state

■説明:各ポートのループバック検出情報を表示します。

■構文:show lbd port state

■設定モード:特権EXECモード

28. show lbd state

■説明:ループバック検出情報を表示します。

■構文:show lbd state

■設定モード:特権EXECモード

29. show mac-address-table aging-time

■説明:
MACアドレス テーブルに設定されたエージングタイムを表示します。
この時間は、動的に学習されたMACアドレステーブルのエントリが削除されるまでの時間(秒単位)を示します。

■構文:show mac-address-table aging-time [switch <context_name>]

■パラメータの説明:
・ switch <context_name> - 指定のコンテキストの MACアドレス テーブルのエージングタイムを表示します。この値は、本機のコンテキストの一意の名前を表します。この値は、最大サイズが 32 の文字列です。
・ このパラメータはマルチインスタンス機能に固有です。

■設定モード:特権EXECモード

30. show mac-address-table

■説明:
MACアドレス テーブルに作成されたすべての静的/動的ユニキャストおよびマルチキャストMAC エントリを表示します。これらのエントリには、VLAN ID、ユニキャスト/マルチキャストMACアドレス、ピアのバックボーンのエッジ ブリッジのユニキャスト バックボーン MACアドレス、メンバー ポート、エントリのタイプ (静的、学習済みなど)、および表示されるエントリの総数が含まれます。

■構文:
・ show mac-address-table [vlan <string(9)>] [address <mac_addr>][{interface <interface-type> <ifnum> | switch <string(32)>}]

■パラメータの説明:
・ vlan <vlan-range> - 指定の VLAN のみの MACアドレス テーブルに作成されたすべての静的/動的ユニキャストおよびマルチキャストMAC エントリを表示します。この値は、エントリを表示する必要がある VLAN ID の範囲を示します。この値は、最大サイズが 9 の文字列です。
  たとえば、「4000 ～ 4010」の VLAN ID のエントリを表示するには、値を「4000 - 4010」に指定します。
・ address <aa:aa:aa:aa:aa:aa> - 指定のユニキャスト/マルチキャストMACアドレスの MACアドレス テーブルに作成されたすべての静的/動的ユニキャストおよびマルチキャストMAC エントリを表示します。
・ <interface-type> - 指定のインタフェースのすべての動的マルチキャストMACアドレスのエントリを表示します。
  インタフェースは次のとおりです。
  - gigabitethernet -1 秒あたり最大 1 ギガビットのデータ転送をサポートする LAN 標準アーキテクチャのバージョン。
・ switch <context_name> - 指定のコンテキストのすべての VLAN に適用される VLANのグローバル情報を表示します。この値は、スイッチのコンテキストの一意の名前を表します。この値は、最大サイズが 32の文字列です。このパラメータは、マルチインスタンス機能に固有です。

■設定モード:特権EXECモード

31. show mac-address-table count

■説明:
FDB テーブルに作成された静的/動的ユニキャストおよびマルチキャストMACアドレスのエントリの総数を表示します。この数は、すべてのアクティブな VLAN、ポートの詳細が設定されている VLAN (アクティブではない)、および MACアドレス テーブルのエントリが作成されている VLAN について表示されます。

■構文:
・ show mac-address-table count [vlan <vlan_id>] [switch<string(32)>]

■パラメータの説明:
・ vlan <vlan-id> - 指定の VLAN ID に対して作成された静的/動的ユニキャストおよびマルチキャストMACアドレスのエントリの総数を表示します(値の有効範囲:1～4094)。
・ switch <context_name> - 指定のコンテキストのすべての VLAN に適用される VLAN グローバル情報を表示します。この値は、本機のコンテキストの一意の名前を表します。この値は、最大サイズが 32の文字列です。このパラメータは、マルチインスタンス機能に固有です。

■設定モード:特権EXECモード

32. show mac-address-table dynamic unicast

■説明:
MACアドレス テーブルから動的に学習されたすべてのユニキャスト エントリを表示します。

これらのエントリには、ユニキャスト MACアドレスのエントリが学習される VLAN ID、ユニキャスト MACアドレス、エントリが学習されるポート、ピアのバックボーンのエッジのユニキャスト バックボーン MACアドレスが含まれます。また、MACアドレステーブルのエントリの合計を表示します。

■構文:
・ show mac-address-table dynamic unicast [vlan <string(9)>] [address <ucast_mac>] [{interface <interface-type> <interface-id> | switch <string(32)>}]

■パラメータの説明:
・ vlan <vlan-range> - 指定の VLAN のみの MACアドレス テーブルに作成されたすべての動的ユニキャストおよびマルチキャストMAC エントリを表示します。この値は、エントリを表示する必要がある VLAN ID の範囲を示します。この値は、最大サイズが 9 の文字列です。
  たとえば、「4000 ～ 4010」の VLAN ID のエントリを表示するには、値は「4000 - 4010」という形式で指定します。
・ address <aa:aa:aa:aa:aa:aa> - 指定のユニキャスト/マルチキャストMACアドレスの MACアドレス テーブルに作成されたすべての動的ユニキャストおよびマルチキャストMAC エントリを表示します。
・ <interface-type> - 指定のインタフェースのすべての動的マルチキャストMACアドレスのエントリを表示します。
  インタフェースは次のとおりです。
  - gigabitethernet -1 秒あたり最大 1 ギガビットのデータ転送をサポートする LAN 標準アーキテクチャのバージョン。
・ switch <context_name> - 指定のコンテキストのすべての VLAN に適用される VLAN グローバル情報を表示します。この値は、本機のコンテキストの一意の名前を表します。この値は、最大サイズが 32 の文字列です。
・ このパラメータはマルチインスタンス機能に固有です。

■設定モード:特権EXECモード

33. show mac-address-table static multicast/unicast

■説明:
FDB テーブルに作成された静的マルチキャスト/ユニキャスト MACアドレスのエントリを表示します。

これらのエントリには、マルチキャスト/ユニキャスト MACアドレスのエントリが割り当てられている VLAN ID、マルチキャスト/ユニキャスト MACアドレス、メンバー ポート、受信ポート、禁止ポート、エントリのステータス (永続的、静的など)、および表示されるエントリの総数が含まれます。

■構文:
- show mac-address-table static multicast [vlan <vlan-range>] [address <aa:aa:aa:aa:aa:aa>] [{interface <interface-type><interface-id> | switch<context_name>}]
- show mac-address-table static unicast [vlan <vlan-range>] [address <aa:aa:aa:aa:aa:aa>] [{interface <interface-type><interface-id> | switch <context_name>}]

■パラメータの説明:
- vlan <vlan-range> - 指定の VLAN のみの MACアドレス テーブルに作成されたすべての静的/動的ユニキャストおよびマルチキャストMAC エントリを表示します。この値は、エントリを表示する必要がある VLAN ID の範囲を示します。この値は、最大サイズが 9 の文字列です。
- たとえば、「4000 ～ 4010」の VLAN ID のエントリを表示するには、値を「4000 - 4010」に指定します。
- address <aa:aa:aa:aa:aa:aa> - 指定のユニキャスト/マルチキャストMACアドレスの MACアドレス テーブルに作成されたすべての静的/動的ユニキャストおよびマルチキャストMAC エントリを表示します。
- <interface-type> - 指定のインタフェースのすべての静的マルチキャストMACアドレスのエントリを表示します。インタフェースは次のとおりです。
  - gigabitethernet -1 秒あたり最大 1 ギガビットのデータ転送をサポートする LAN 標準アーキテクチャのバージョン。
- switch <context_name> - 指定のコンテキストのすべての VLAN に適用される VLAN グローバル情報を表示します。この値は、本機のコンテキストの一意の名前を表します。この値は、最大サイズが 32 の文字列です。このパラメータはマルチインスタンス機能に固有です。

■設定モード:特権EXECモード

34. show spanning-tree - Summary, Blockedports, Pathcost

■説明:
有効な現在の STP について、利用可能なスパニングツリー関連の情報を表示します。

情報には、ルートとブリッジの優先度、アドレスとタイマーの詳細、動的パスコスト計算機能のステータス、スパニングツリー機能のステータス、使用されている STP 互換バージョン、設定されたスパニングツリーが含まれます。

モード、ブリッジおよびポート単位のスパニングツリーの統計情報、および有効なポートの詳細。ポートの詳細には、ポート ID、ポートの役割、ポートの状態、ポートのコスト、ポートの優先度、リンクタイプが含まれます。

✏本コマンドは、スイッチ内でスパニングツリー機能が動作している場合にのみ正常に実行できます。
機能が無効な場合は、スパニングツリーのモードを"mst"に設定してください。

■構文:
・ show spanning-tree [{ summary | blockedports | pathcost method }] [switch <context_name>]

■パラメータの説明:
・ summary - 現在使用されている STP、適用されているパスコスト方式、およびポート ID、ポートの役割、ポートの状態などのポートの詳細を表示します。
・ blockedports - ブロックされた状態のポートのリストとブロックされたポートの総数を表示します。
・ pathcost method - スイッチに設定されているポートのパスコスト方式を表示します。
・ switch <context_name> - 指定のコンテキストのスイッチ内の STP 関連の情報を表示します。この値は、本機のコンテキストの一意の名前を表します。この値は、最大サイズが 32 の文字列です。このパラメータはマルチインスタンス機能に固有です。

■設定モード:特権EXECモード

35. show spanning-tree detail

■説明:
スイッチおよび有効なすべてのポートの詳細なスパニングツリー関連の情報を表示します。

この情報には、スパニングツリー動作のステータス、現在選択されているスパニングツリーのモード、現在のスパニングツリー互換バージョン、ブリッジとルートの優先度、ブリッジとルートのMACアドレス、ポート パスコスト、ポートの優先度、ポート タイマー、ブリッジとポート単位のスパニングツリーの統計情報、転送保留カウント値、リンクタイプ、ループガードの状態、BPDU送信、BPDU受信、制限付きロール、制限付きTCN、ポートファストの状態 が含まれています。

✏本コマンドは、スイッチ内でスパニングツリー機能が動作している場合にのみ正常に実行できます。
機能が無効な場合は、スパニングツリーのモードを”mst”に設定してください。

■構文:show spanning-tree detail [switch <context_name>]

■パラメータの説明:
・ switch <context_name> - 指定のコンテキストの詳細なスパニングツリー関連の情報を表示します。この値は、本機のコンテキストの一意の名前を表します。この値は、最大サイズが 32 の文字列です。このパラメータはマルチインスタンス機能に固有です。

■設定モード:特権EXECモード

36. show spanning-tree active

■説明:
スイッチで有効な現在の STP について、スイッチで利用可能なスパニングツリー関連の情報を表示します。

この情報には、ルートとブリッジの優先度、アドレスとタイマーの詳細、動的パスコスト計算機能のステータス、スパニングツリー機能のステータス、使用される STP 互換バージョン、設定されたスパニングツリー モード、ブリッジおよびポート単位のスパニングツリーの統計情報、およびポートの詳細が含まれます。スイッチで有効になります。
ポートの詳細には、ポート ID、ポートの役割、ポートの状態、ポートのコスト、ポートの優先度、リンク タイプが含まれます。

✏本コマンドは、スイッチ内でスパニングツリー機能が動作している場合にのみ正常に実行できます。
機能が無効な場合は、スパニングツリーのモードを”mst”に設定してください。

■構文:show spanning-tree active [detail] [switch <context_name>]

■パラメータの説明:
・ detail - スイッチおよびポートにおけるスパニングツリー関連の詳細情報を表示します。
・ switch <context_name> - 指定のコンテキストについて、スイッチで利用可能なスパニングツリー関連の情報を表示します。この値は、本機のコンテキストの一意の名前を表します。この値は、最大サイズが 32 の文字列です。このパラメータはマルチインスタンス機能に固有です。

■設定モード:特権EXECモード

37. show spanning-tree interface

■説明:
指定したインタフェースのポート関連のスパニングツリー情報を表示します。

この情報には、ポート ID、ポートの役割、ポートの状態、ポートのコスト、ポートの優先度、リンク タイプが含まれます。

✏本コマンドは、スイッチ内でスパニングツリー機能が動作している場合にのみ正常に実行できます。
機能が無効な場合は、スパニングツリーのモードを”mst”に設定してください。

■構文:
・ show spanning-tree interface <interface-type> <interface-id>[{ cost | priority | portfast | rootcost | restricted-role | restricted-tcn| state | stats | detail }]

■パラメータの説明:
・ <interface-type> - 指定されたタイプのインタフェースのポート関連のスパニングツリー情報を表示します。
インタフェースは次のとおりです。
  - gigabitethernet -1 秒あたり最大 1 ギガビットのデータ転送をサポートする LAN 標準アーキテクチャのバージョン。
  - port-channel – 複数のポートが集約されたアグリゲータを表す論理インタフェース。
・ <interface-id> - 指定したインタフェース識別子に関する情報を表示します。これは、特定のインタフェースを表す一意の値です。この値は、スロット番号とポート番号をスラッシュで区切って組み合わせたものです。
・ 例) 0/1:スロット番号が「0」、ポート番号が「1」であることを表します。
・ インタフェース タイプ ポート チャネルの場合、ポート チャネル ID のみが提供されます（例: 1 はポートチャネル ID を表します。）
・ cost - ポートまたはそのポートに割り当てられたインスタンスのコストを表示します。
・ priority - ポートまたはそのポートに割り当てられたインスタンスの優先度を表示します。
・ rootcost - ポートまたはそのポートに割り当てられたインスタンスのルートコストを表示します。ルートコストは、ルートブリッジに到達するまでのパスコストを定義します。
・ restricted-role - ポートの制限された役割機能のステータスを表示します。
※ただし、このモードは本機器では搭載していません。
・ limited-tcn - ポートの制限された TCN 機能のステータスを表示します。
※ただし、このモードは本機器では搭載していません。
・ state - ポートの状態を表示します。
・ stats - ポート単位のスパニングツリーの統計情報を表示します。
・ detail -ポートのスパニングツリー関連の詳細情報を表示します

■設定モード:特権EXECモード

38. show spanning-tree root

■説明:
スパニングツリーのルート情報を表示します。情報には、ルート ID、ルート パスコスト、最大エージングタイム、転送遅延時間、およびRSTPのルート ポート、MSTP のインスタンス ID が含まれます。

✏本コマンドは、スイッチ内でスパニングツリー機能が動作している場合にのみ正常に実行できます。
機能が無効な場合は、スパニングツリーのモードを”mst”に設定してください。

■構文:
・ show spanning-tree root [{ address | cost | forward-time | id | max- age | port | priority | detail }] [switch <context_name>]

■パラメータの説明:
・ address - ルートブリッジの MACアドレスを表示します。
・ cost - ルートパスコストを表示します。
・ forward-time - ルートブリッジの転送遅延時間を表示します。
・ id - ルートブリッジのIDを表示します。
・ max-age - ルートブリッジの最大エージングタイムを表示します。
・ port - ルートポートのIDを表示します。
・ priority - ルートブリッジの優先度を表示します。
・ detail - ルート優先度、ルート ブリッジのMACアドレス、ルートコスト、ルート ポート、転送遅延時間、および最大経過時間を表示します。
・ switch <context_name> - 指定されたコンテキストのスパニングツリー ルート情報を表示します。この値は、本機のコンテキストの一意の名前を表します。この値は、最大サイズが 32 の文字列です。このパラメータはマルチインスタンス機能に固有です。

■設定モード: 特権EXECモード

39. show spanning-tree bridge

■説明:
スパニングツリー のブリッジを表示します。
情報には、RSTP のブリッジ ID、Hello時間、最大エージングタイム、転送遅延時間、有効なプロトコル、MSTP のインスタンス ID が含まれます。

✏本コマンドは、スイッチ内でスパニングツリー機能が動作している場合にのみ正常に実行できます。
機能が無効な場合は、スパニングツリーのモードを”mst”に設定してください。

■構文:
・ show spanning-tree bridge [{ address | forward-time | hello-time | id | max-age | protocol | priority | detail }]
[switch<context_name>]

■パラメータの説明:
・ address - ブリッジの MACアドレスを表示します。
・ forward-time - ブリッジの転送遅延時間を表示します。
・ hello-time - ブリッジの Hello時間を表示します。
・ id - ブリッジの ID を表示します。
・ max-age - ブリッジの最大エージングタイムを表示します。
・ プロトコル - ブリッジで現在有効なプロトコルを表示します。
・ priority - ブリッジの優先度を表示します。
・ detail- ブリッジの優先度、アドレス、最大経過時間、および転送遅延時間を表示します。
・ switch - 指定されたコンテキストのスパニングツリー ブリッジ情報を表示します。この値は、本機のコンテキストの一意の名前を表します。この値は、最大サイズが 32 の文字列です。このパラメータはマルチインスタンス機能に固有です。

■設定モード: 特権EXECモード

40. show spanning-tree mst - CIST or specified mst Instance

■説明:
スイッチ内のすべての MSTI のマルチスパニングツリー情報を表示します。

この情報には、MSTI ID、インスタンスにマッピングされた VLAN ID、ブリッジ アドレスと優先度、ルート アドレスと優先度、IST ルート アドレス、優先度とパスコスト、転送遅延、最大経過時間、最大ホップ カウント、インタフェースで有効なインタフェースのポート詳細が含まれます。ポートの詳細には、インタフェース ID、ポートの役割、ポートの状態、ポートのコスト、ポートの優先度、およびポートのリンク タイプが含まれます。

✏本コマンドは、スイッチ内でスパニングツリー機能が動作している場合にのみ正常に実行できます。
スパニングツリーのモードを"mst"に設定する必要があります。

■構文:show spanning-tree mst [<instance-id(1-4094)>] [detail] [switch <context_name>]

■パラメータの説明:
・ <instance-id(1-4094)> - 指定した MSTI のマルチスパニングツリー情報を表示します(値の有効範囲:1～4094)。
・ detail - MSTI の詳細なマルチスパニングツリー情報を表示します。
・ switch<context_name> - 指定されたコンテキストのマルチスパニングツリーブリッジ情報を表示します。この値は、本機のコンテキストの一意の名前を表します。この値は、最大サイズが 32 の文字列です。
・ このパラメータはマルチインスタンス機能に固有です。

■設定モード:特権EXECモード

41. show spanning-tree mst configuration

■説明:
マルチスパニングツリーンスタンス関連の情報を表示します。この情報には、MST リージョン名、MST リージョン リビジョン、および対応する MSTI にマッピングされた MSTI ID と VLAN ID を含むリストが含まれます。

✏ 本コマンドは、スイッチ内でスパニングツリー機能が動作している場合にのみ正常に実行できます。
スパニングツリーのモードを”mst”に設定してください。

■構文:
・ show spanning-tree mst configuration [switch <context_name>]

■パラメータの説明:
・ switch <context_name> - 指定されたコンテキストのマルチ スパニングツリーインスタンス関連の情報を表示します。この値は、本機のコンテキストの一意の名前を表します。この値は、最大サイズが 32 の文字列です。このパラメータはマルチインスタンス機能に固有です。

■設定モード:特権EXECモード

42. show spanning-tree mst - Port Specific Configuration

■説明:
指定したポートのマルチ スパニングツリー ポート固有の情報を表示します。
この情報には、インタフェース ID、エッジ ポート ステータス、ポートリンク タイプ、ポート Hello時間、ポート上で送受信される BPDU、およびインスタンス関連の詳細が含まれます。インスタンスの詳細には、MSTI ID、MSTI ロール、MSTI ステータス、MSTI コスト、および MSTI 優先度が含まれます。

✏本コマンドは、スイッチ内でスパニングツリー機能が動作している場合にのみ正常に実行できます。
スパニングツリーのモードを”mst”に設定してください。

■構文:
・ show spanning-tree mst [<instance-id(1-4094)>] interface<interface-type> <interface-id> [{ stats | hello-time | detail }]

■パラメータの説明:
・ <instance-id(1-4094)> - 指定された MSTI のマルチスパニングツリーポート固有の情報を表示します(値の有効範囲:1-4094)。
・ <interface-type> - 指定されたタイプのインタフェースのポート関連のスパニングツリー情報を表示します。
インタフェースは次のとおりです。
  - gigabitethernet -1 秒あたり最大 1 ギガビットのデータ転送をサポートする LAN 標準アーキテクチャのバージョン。
  - port-channel – 複数のポートが集約されたアグリゲータを表す論理インタフェース。
・ <interface-id> - 指定したインタフェース識別子に関する情報を表示します。これは、特定のインタフェースを表す一意の値です。この値は、スロット番号とポート番号をスラッシュで区切って組み合わせたものです。
・ 例）0/1 : スロット番号が「0」、ポート番号が「1」であることを表します。インタフェース タイプ ポート チャネルの場合、ポート チャネル ID のみが提供されます(例: 1 はポートチャネル ID を表します)。
・ stats - 指定されたインタフェースに割り当てられた MSTI に対して送受信された BPDU の数を表示します。
・ hello-time - 指定されたインタフェースに割り当てられた MSTI の Hello時間を表示します。
・ detail - 指定したインタフェースの詳細なマルチスパニングツリー ポート固有の情報を表示します。

■設定モード:特権EXECモード

3.2.8 LLDP

1. lldp transmit-interval

■説明:
サーバによるLLDPフレームのLLDPモジュールへの送信間隔を設定します（値の有効範囲:5 ～ 32768 秒）。
コマンドの no 形式は、送信間隔をデフォルト値に設定します。

■構文:
・ lldp transmit-interval <seconds(5-32768)>
・ no lldp transmit-interval

■設定モード:グローバルコンフィグレーションモード

2. lldp holdtime-multiplier

■説明:
サーバがLLDPを保持する時間であるholdtime-multiplier値を設定します(値の有効範囲:2 ～ 10 秒)。

コマンドの no 形式を使用すると、乗数がデフォルト値に設定されます。

✏TLV:Type(データの種類)/Length(データ長)/Value(データの値)が並ぶデータの構造。
TTL:Time To Live（情報の保持時間）

TTL = LLDP 送信間隔 * LLDP 保持乗数
・ ==========
（たとえば、LLDP 送信間隔の値が “30”、LLDP 保持乗数の値が “4” の場合、値 “120” は
LLDP ヘッダーの TTL フィールドに設定されます）

■構文:
・ lldp holdtime-multiplier <value(2-10)>
・ no lldp holdtime-multiplier

■設定モード:グローバルコンフィグレーションモード

3. lldp reinitialization-delay

■説明:
LLDP送信を再初期化する前にLLDPポートが待機する最小時間である再初期化遅延時間を設定します(値の有効範囲:1 ～ 10 秒)。

コマンドの no 形式は、再初期化遅延時間をデフォルト値に設定します。

■構文:
・ lldp reinitialization-delay <seconds(1-10)>
・ no lldp reinitialization-delay

■設定モード:グローバルコンフィグレーションモード

4. lldp tx-delay

■説明:
LLDPフレームの送信遅延間隔を設定します(有効範囲:1 ～ 8181 秒)。
コマンドの no 形式は、送信遅延をデフォルト値に設定します。

✏TxDelay は (0.25 * LLDPDU（LLDP data unit）送信間隔) 以下の値を設定してください。

■構文:
・ lldp tx-delay <seconds(1-8181)>
・ no lldp tx-delay

■設定モード:グローバルコンフィグレーションモード

5. set lldp version

■説明:システムで lldp バージョンを使用可能になります。

■構文:set lldp version {v1 | v2}

■パラメータの説明:
・ v1 - ポート上で LLDP 2005 バージョン 1 を有効にします
・ v2 - ポート上で LLDP 2009 バージョン 2 を有効にします

■設定モード:グローバルコンフィグレーションモード

6. set lldp

■説明:
サーバから LLDP モジュールに LLDP フレームを送受信します。

■構文:set lldp {enable | disable}

■パラメータの説明:
・ enable - LLDP モジュールと サーバの間で LLDP パケットを送受信します。
・ disable - LLDP モジュールと サーバの間で LLDP パケットを送受信しません。

■設定モード:グローバルコンフィグレーションモード

7. show lldp

■説明:インタフェース上で初期化する LLDP グローバル設定の詳細を表示します。

■構文:show lldp

■設定モード:特権EXECモード

8. show lldp interface

■説明:
LLDP が有効なインタフェースに関する情報を表示します。

■構文:
・ show lldp interface [<interface-type> <interface-id>] [mac-address <mac_addr>]

■パラメータの説明:
・ <interface-type> - 指定されたタイプのインタフェースに関する情報を表示します。
インタフェースは次のとおりです。
  - gigabitethernet -1 秒あたり最大 1 ギガビットのデータ転送をサポートする LAN 標準アーキテクチャのバージョン。
・ <interface-id> - 指定したインタフェース識別子に関する情報を表示します。これは、特定のインタフェースを表す一意の値です。この値は、スロット番号とポート番号をスラッシュで区切って組み合わせたものです。
例) 0/1:スロット番号が「0」、ポート番号が「1」であることを表します。
・ インタフェース タイプ ポート チャネルの場合、ポート チャネル ID のみが提供されます(例: “1” はポートチャネル ID を表します)。
・ mac-address <mac_addr> - LLDP エージェントの指定された宛先 MACアドレスのネイバーに関する情報を表示します。

■設定モード: 特権EXECモード

9. show lldp neighbors

■説明:
すべてのインタフェース上のネイバーに関する情報を表示します。

■構文:
・ show lldp neighbors [chassis-id <string(255)> port-id<string(255)>] [<interface-type> <interface-id> [mac-address<mac_addr>]][detail]

■パラメータの説明:
・ chassis-id <string(255)> - シャーシ識別子の文字列を設定します。この値は、最大サイズが 255 の文字列値です。
・ port-id <string(255)> - 関連する集約ポートを表すポート番号を設定します。この値は、最大サイズが 255 の文字列値です。
・ <interface-type> - 指定されたタイプのインタフェースのネイバーに関する情報を表示します。
インタフェースは次のとおりです。
  - gigabitethernet -1 秒あたり最大 1 ギガビットのデータ転送をサポートする LAN 標準アーキテクチャのバージョン。
・ <interface-id> - 指定されたインタフェース識別子のネイバーに関する情報を表示します。これは、特定のインタフェースを表す一意の値です。この値は、スロット番号とポート番号をスラッシュで区切って組み合わせたものです。
例) 0/1:スロット番号が「0」、ポート番号が「1」であることを表します。
・ インタフェース タイプ ポートチャネルの場合、ポートチャネル ID のみが提供されます(例: 1 はポートチャネル ID を表します)。
・ mac-address <mac_addr> - LLDP エージェントの指定された宛先 MACアドレスのネイバーに関する情報を表示します。
・ detail - 受信したすべての TLV から取得した情報を表示します。

■設定モード: 特権EXECモード

10. show lldp local

■説明:
特定のすべてのインタフェースの送信 LLDP アドバタイズメントを設定するために使用される現在のスイッチ情報を表示します。

■構文:
・ show lldp local {[<interface-type> <interface-id> [mac-address<mac_addr>]] | [mgmt-addr]}

■パラメータの説明:
・ <interface-type> - 指定されたタイプのインタフェースの現在のスイッチ情報を表示します。
インタフェースは次のとおりです。
  - gigabitethernet -1 秒あたり最大 1 ギガビットのデータ転送をサポートする LAN 標準アーキテクチャのバージョン。
・ <interface-id> - 指定されたインタフェース識別子の現在のスイッチ情報を表示します。これは、特定のインタフェースを表す一意の値です。この値は、スロット番号とポート番号をスラッシュで区切って組み合わせたものです。
・ 例) 0/1:スロット番号が「0」、ポート番号が「1」であることを表します。
・ インタフェース タイプ ポートチャネルの場合、ポートチャネル ID のみが提供されます。例: 1 はポートチャネル ID を表します。
・ mac-address <mac_addr> - LLDP エージェントの指定された宛先 MACアドレスのネイバーに関する情報を表示します。
・ mgmt-addr - システムおよび Tx 対応ポートに設定されているすべての管理アドレス。

■設定モード: 特権EXECモード

11. show lldp peers

■説明:
すべてのインタフェースで学習されたネイバーに関する情報を表示します。

■構文:
・ show lldp peers [chassis-id <string(255)> port-id <string(255)>]<interface-type> <interface-id>[[mac-address <mac_addr>] [detail]]
・

■パラメータの説明:
・ <interface-type> - 指定されたタイプのインタフェースの現在のスイッチ情報を表示します。
インタフェースは次のとおりです。
  - gigabitethernet -1 秒あたり最大 1 ギガビットのデータ転送をサポートする LAN 標準アーキテクチャのバージョン。
・ <interface-id> - 指定されたインタフェース識別子の現在のスイッチ情報を表示します。これは、特定のインタフェースを表す一意の値です。この値は、スロット番号とポート番号をスラッシュで区切って組み合わせたものです。
・ 例) 0/1:スロット番号が「0」、ポート番号が「1」であることを表します。
・ インタフェース タイプ ポートチャネルの場合、ポートチャネル ID のみが提供されます(例: 1 はポートチャネル ID を表します)。
・ mac-address <mac_addr> - LLDP エージェントの指定された宛先 MACアドレスのネイバーに関する情報を表示します。
・ detail - 受信したTLVから取得した情報の詳細を表示します。

■設定モード:特権EXECモード

3.2.9 IGMP

1. ip igmp querier-timeout

■説明:
マルチキャストルータ(Querier)が存在しなくなったと判断するまでの時間を示します(値の範囲:「60～600秒」)。

■構文:
・ ip igmp querier-timeout <(60 - 600) seconds>

■設定モード:グローバルコンフィグレーションモード

2. ip igmp snooping

■説明:
スイッチ/特定の VLAN の IGMPスヌーピングを有効にします。スイッチまたはインタフェースでIGMPスヌーピングが有効な場合、IGMP Joinメッセージの送信元IPアドレスをスヌーピングすることで、レシーバにマルチキャストパケットが届くようにします。IGMPスヌーピングがグローバルで有効な場合、既存のすべてのVLANインタフェースで有効になります。

コマンドの no 形式は、スイッチ/特定の VLAN で IGMPスヌーピングを無効にします。IGMPスヌーピングがグローバルで無効にすると、既存のすべての VLAN インタフェースは無効になります。

■構文:
・ グローバルコンフィグレーションモード
  - ip igmp snooping [vlan < vlan–id >]
  - no ip igmp snooping [vlan < vlan–id >]

・ Config-VLANモード
  - ip igmp snooping
  - no ip igmp snooping

■パラメータの説明:
・ <vlan –id> -VLANを表す一意の値です(値の有効範囲:1 ～ 4094)。

■設定モード:グローバルコンフィグレーションモード / Config-VLANモード

3. ip igmp snooping blocked-router

■説明
ルータポートをブロック・ルータポートに設定します。
コマンドの no 形式は、ブロックされているルータポートを通常のルータポートに戻します。

✏ 動作中のルータポートにこの設定をしないでください

■構文:
・ ip igmp snooping blocked-router <interface-type> <interface-id>

■パラメータの説明:
・ <interface-type> - 指定されたタイプのインタフェースのIPインタフェースを表示します。
インタフェースは次のとおりです。
  - gigabitethernet -1 秒あたり最大 1 ギガビットのデータ転送をサポートする LAN 標準アーキテクチャのバージョン。
  - port-channel – 複数のポートが集約されたアグリゲータを表す論理インタフェース。
・ <interface-id> - インタフェースのリストまたは特定のインタフェース識別子のマルチキャストルータのポートのリストを設定します。この値は、スロット番号とポート番号をスラッシュで区切って組み合わせたものです。インタフェースタイプ ポート チャネルのポート チャネル ID が提供されます。インタフェースのリストを設定する際には、スペースを使用せずにカンマを区切り文字として使用します（例: 0/1, 0/3）。

■設定モード: Config-VLANモード

4. ip igmp snooping fast-leave

■説明
特定の VLAN に対してfast leave処理とIGMPスヌーピングを有効にします。IGMPスヌーピングがグローバルで無効になっている場合、特定の VLAN に対してのみ IGMPスヌーピングを有効にします。
fast leave機能が有効な場合leaveメッセージを受信すると、マルチキャストグループ エントリから削除されます。

コマンドの no 形式は、特定の VLAN のfast leave処理を無効にします。

✏ VLAN で IGMPスヌーピングが無効になっているときに VLAN で行われたfast leave設定は、VLAN で IGMPスヌーピングが有効な場合にのみ適用されます。

■構文:
・ ip igmp snooping fast-leave
・ no ip igmp snooping fast-leave

■設定モード: Config-VLANモード

5. ip igmp snooping group-query-interval

■説明:
スイッチがLeaveメッセージを受信したとき、グループ内に他にレシーバが存在するかどうかを確認するため、グループスペシフィックククエリを送信します。このコマンドで設定される時間の間、応答を受信しない場合はグループのメンバーシップから削除されます（値の範囲：2～5）。

コマンドの no 形式は、グループ固有のクエリ間隔時間をデフォルト値に設定します。

■構文:
・ ip igmp snooping group-query-interval <2-5) seconds>
・ no ip igmp snooping group-query-interval

■設定モード：グローバルコンフィグレーションモード

6. ip igmp snooping max-response-code

■説明:
ホストに送信されるジェネラルクエリに挿入される最大応答コードを設定します。
応答コードの単位は10分の1秒です(値の有効範囲:0 ～ 255)。

コマンドの no 形式は、クエリ応答コードをデフォルト値に設定します。

■構文:
・ ip igmp snooping max-response-code <(0 - 255)>
・ no ip igmp snooping max-response-code

■設定モード：Config-VLANモード

7. ip igmp snooping mrouter

■説明:
IGMPスヌーピングがグローバルで有効な場合、IGMPスヌーピングを有効にし、マルチキャストルータのポートを設定します。

スイッチが受信したIGMPメッセージはルータが接続されているポートにのみ転送され、ホストのポートには転送されません。したがって、ホストからネットワーク全体へIGMPクエリメッセージがフラッディングされるのを防ぎます。

このコマンドの no 形式は、VLAN に対して手動で設定されたマルチキャストルータのポートを削除します。

■構文:
・ ip igmp snooping vlan <integer (1-4094)> mrouter <interface-type><iinterface-id>
・ no ip igmp snooping vlan <integer (1-4094)> mrouter <iinterface-type><interface-id>

■パラメータの説明:
・ <interface-type> - 指定されたタイプのインタフェースのIPインタフェースを表示します。
  インタフェースは次のとおりです。
  - gigabitethernet -1 秒あたり最大 1 ギガビットのデータ転送をサポートする LAN 標準アーキテクチャのバージョン。

- port-channel – 複数のポートが集約されたアグリゲータを表す論理インタフェース。

■設定モード:Config-VLANモード

8. ip igmp snooping mrouter-port -time-out

■説明:マルチキャストルータポートのタイムアウト間隔を設定します。

■構文:
- ip igmp snooping mrouter-port <interface-type> <interface-id>time-out <short(60-600)>
- no ip igmp snooping mrouter-port <interface-type> <interface-id>time-out

■パラメータの説明:
- <interface-type> - 指定されたタイプのインタフェースを設定します。
  - インタフェースは次のとおりです。
  - gigabitethernet - 1 秒あたり最大 1 ギガビットのデータ転送をサポートする LAN 標準アーキテクチャのバージョン。
- <interface-id> - インタフェースのリストまたは特定のインタフェース識別子のマルチキャストルータのポートのリストを設定します。この値は、スロット番号とポート番号をスラッシュで区切って組み合わせたものです。インタフェースタイプ ポート チャネルのポート チャネル ID が提供されます。インタフェースのリストを設定する際には、スペースを使用せずにカンマを区切り文字として使用します(例: 0/1, 0/3)。
- <short(60-600)> - タイムアウト値を表します。

■設定モード:Config-VLANモード

9. ip igmp snooping mrouter-port -version

■説明:マルチキャストルータポートのIGMPバージョンを設定します。

■構文:
- ip igmp snooping mrouter-port <interface-type> <interface-id> version {v1 | v2 | v3}
- no ip igmp snooping mrouter-port <interface-type> <interface-id> version

■パラメータの説明:
- <interface-type> - 指定されたタイプのインタフェースを設定します。
  インタフェースは次のとおりです。
  - gigabitethernet - 1 秒あたり最大 1 ギガビットのデータ転送をサポートする LAN 標準アーキテクチャのバージョン。
- <interface-id> - インタフェースのリストまたは特定のインタフェース識別子のマルチキャストルータのポートのリストを設定します。この値は、スロット番号とポート番号をスラッシュで区切って組み合わせたものです。インタフェースタイプ ポート チャネルのポート チャネル ID が提供されます。インタフェースのリストを設定する際には、スペースを使用せずにカンマを区切り文字として使用します(例: 0/1, 0/3)。
  - v1 - IGMP スヌーピング バージョン 1
  - v2 - IGMP スヌーピング バージョン 2
  - v3 - IGMP スヌーピング バージョン 3

■設定モード:Config-VLANモード

10. ip igmp snooping querier

■説明
IGMPスヌーピングを特定の VLAN のクエリアとして設定します。クエリアとして設定されている場合、スイッチは IGMP クエリメッセージを送信します。ネットワーク内にルータ（クエリア）が存在する場合、本機器からのクエリメッセージは制御されます。

このコマンドの no形式を設定すると、特定のVLANのクエリアではなくなります。

■構文:
・ ip igmp snooping querier
・ no ip igmp snooping querier

■設定モード：Config-VLANモード

11. ip igmp snooping query-interval

■説明
VLAN 上でクエリアに設定されている場合に、IGMPスヌーピングによってジェネラルクエリが送信される期間を設定します。(値の有効範囲:60 ～ 600 秒)。

このコマンドの no 形式は、IGMP クエリア間隔をデフォルト値に設定します。

✏この設定を適用するには、スイッチをクエリアに設定する必要があります。

■構文:
・ ip igmp snooping query-interval <(60 - 600) seconds>
・ no ip igmp snooping query-interval

■設定モード：Config-VLANモード

12. ip igmp snooping report-suppression interval

■説明:
IGMPスヌーピングレポート抑制時間間隔を設定します。同じマルチキャストグループのIGMPv2のレポートメッセージが、ルータポートに転送されない時間間隔です。

このコマンドの no 形式は、IGMPスヌーピングレポート抑制間隔時間をデフォルト値に設定します。

✏ ip igmp snooping report-suppression-interval は、プロキシとプロキシレポートが無効になっている場合に使用できます。

■構文:
・ ip igmp snooping report-suppression-interval <(0 – 25) seconds>
・ no ip igmp snooping report-suppression-interval

■設定モード：グローバルコンフィグレーションモード

13. ip igmp snooping static-group

■説明:
IGMPスヌーピングにスタティック マルチキャストフォワード のエントリを追加します。

■構文:
・ ip igmp snooping static-group <mcast_addr> ports<interface-type><interface-id>
・ no ip igmp snooping static group <mcast-addr>

■パラメータの説明:
・ <mcast_addr> - マルチキャストIPアドレス。
・ <interface-type> - 指定されたタイプのインタフェースのIPインタフェースを表示します。
インタフェースは次のとおりです。
  - gigabitethernet - 1 秒あたり最大 1 ギガビットのデータ転送をサポートする LAN 標準アーキテクチャのバージョン。
  - port-channel - 複数のポートが集約されたアグリゲータを表す論理インタフェース。
・ <interface-id> - インタフェースのリストまたは特定のインタフェース識別子のマルチキャストルータのポートのリストを設定します。この値は、スロット番号とポート番号をスラッシュで区切って組み合わせたものです。インタフェースタイプ ポート チャネルのポート チャネル ID が提供されます。インタフェースのリストを設定する際には、スペースを使用せずにカンマを区切り文字として使用します(例: 0/1, 0/3)。

■設定モード: Config-VLANモード

14. ip igmp snooping startup-query-count

■説明
スイッチがクエリアに設定されている場合に、スイッチの実行中に送信されるジェネラルクエリのメッセージの最大数を設定します（値の有効範囲:2 ～ 5）。起動クエリ メッセージは、スイッチの存在とその ID を通知するために送信されます（値の有効範囲:2 ～ 5）。

コマンドの no 形式は、スイッチがクエリアに設定されている場合に、スイッチの実行中に送信されるジェネラルクエリのメッセージ数をデフォルト値に設定します。

✏起動クエリ数設定を有効にするには、スイッチをクエリアに設定する必要があります。

■構文:
・ ip igmp snooping startup-query-count <2 - 5>
・ no ip igmp snooping startup-query-count

■設定モード: Config-VLANモード

15. ip igmp snooping startup-query-interval

■説明:
クエリア選択プロセスの実行中に、IGMPスヌーピングによって送信されるジェネラルクエリのメッセージ間の時間間隔を設定します。この値の範囲は 15 ～ 150 秒、query-interval * 0.25以下の値に設定してください。

コマンドの no 形式は、IGMP 起動クエリ間隔をデフォルト値に設定します。

✏ このコマンドを実行するには、スイッチをクエリアとして設定する必要があります。
実行中のクエリ間隔は、query-interval * 0.25 以下の値に設定してください。

■構文:
・ ip igmp snooping startup-query-interval <(15 - 150) seconds>
・ no ip igmp snooping startup-query-interval

■設定モード:Config-VLANモード

16. ip igmp snooping version

■説明
特定の VLAN の IGMPスヌーピングの動作時のバージョンを設定します。
バージョンを手動で設定することにより、条件に応じた固有のコマンドを実行できます。

■構文:ip igmp snooping version { v1 |v2 | v3}

■パラメータの説明:
・ v1 - IGMPスヌーピングのバージョン1を設定します。
・ v2 - IGMPスヌーピングのバージョン 2 を設定します。
・ v3 - IGMPスヌーピングのバージョン 3 を設定します。

■設定モード:Config-VLANモード

17. ip igmp snooping vlan - immediate leave

■説明:
特定の VLAN に対してfast leave処理と IGMPスヌーピングを有効にします。IGMPスヌーピングがグローバルで無効になっている場合、特定の VLAN に対してのみ IGMPスヌーピングを有効にします。fast leave機能が有効な場合、leaveメッセージを受信すると、マルチキャストグループ エントリから削除されます（VLAN ID の範囲:1 ～ 4094）。

コマンドの no 形式は、特定の VLAN のfast leave処理を無効にします。

VLAN のIGMPスヌーピングが無効になっているときに VLAN で実行されたfast leaveの設定は、VLANのIGMPスヌーピングが有効な場合にのみ適用されます。

■構文:
・ ip igmp snooping vlan <vlanid(1-4094)> immediate-leave
・ no ip igmp snooping vlan <vlanid(1-4094)> immediate-leave

■設定モード:グローバルコンフィグレーションモード

18. no ip igmp snooping other-querier-present-interval

■説明:他のクエリアが存在すると判断するまでの時間をデフォルト値に設定します。

■構文:no ip igmp snooping other-querier-present-interval

■設定モード:Config-VLANモード

19. snooping multicast-forwarding-mode

■説明:
スヌーピング マルチキャスト転送モード (IP ベースまたは MAC ベース) を指定します。

■構文:snooping multicast-forwarding-mode {ip | mac}

■パラメータの説明:
・ ip - マルチキャスト転送モードを IP アドレスベースとして設定します。
・ mac - マルチキャスト転送モードを MACアドレスベースとして設定します。

■設定モード:グローバルコンフィグレーションモード

20. show ip igmp snooping

■説明
指定したスイッチまたは指定したVLANのIGMPスヌーピング情報を表示します。スイッチとVLANは、指定されていない場合はすべての情報を表示します。

■構文:
・ show ip igmp snooping [Vlan <vlan-id >] [switch<switch_name>]

■パラメータの説明:
・ < vlan-id (1-4094)> - VLANを表す一意の値です(値の有効範囲:1 ～ 4094)。
・ switch <switch_name> - 指定されたコンテキストを表示します。この値は、本機のコンテキストの一意の名前を表します。この値は、最大サイズが 32の文字列です。このパラメータは、マルチインスタンス機能に固有です。

■設定モード:特権EXECモード

21. show ip igmp snooping blocked-router

■説明:指定したスイッチまたは指定したVLANのブロック・ルータポートを表示します。

■構文:
・ show ip igmp snooping blocked-router [Vlan <vlan-id >] [switch<switch_name>]

■パラメータの説明:

・ < vlan-id (1-4094)> - VLANを表す一意の値です(値の有効範囲:1 ～ 4094)。
・ switch <switch_name> - 指定されたコンテキストのブロックされたルータのポートを表示します。この値は、本機のコンテキストの一意の名前を表します。この値は、最大サイズが 32の文字列です。このパラメータは、マルチインスタンス機能に固有です。

■設定モード:特権EXECモード

22. show ip igmp snooping forwarding-database

■説明:マルチキャストのFDB(Forwarding Database)を表示します。」

■構文:
・ show ip igmp snooping forwarding-database [Vlan <vlan-id>]

■パラメータの説明:
・ < vlan-id (1-4094)> - VLANを表す一意の値です(値の有効範囲:1 ～ 4094)。
・ group <address> - VLAN ID のグループアドレスを表示します。

■設定モード:特権EXECモード

23. show ip igmp snooping globals

■説明: 指定したスイッチのIGMPスヌーピング情報を表示します。

■構文:show ip igmp snooping globals [switch <switch_name>]

■パラメータの説明:
・ switch <switch_name> - 指定されたコンテキストを表示します。この値は、本機のコンテキストの一意の名前を表します。この値は、最大サイズが 32の文字列です。このパラメータは、マルチインスタンス機能に固有です。

■設定モード:特権EXECモード

24. show ip igmp snooping groups

■説明
指定したスイッチまたは指定したVLANのIGMPグループ情報とグループアドレスを表示します。スイッチとVLANは、指定されていない場合はすべての情報を表示します。

■構文:
・ show ip igmp snooping groups [Vlan <vlan-id > [Group<Address>]] [switch <switch_name>]

■パラメータの説明:
・ < vlan-id (1-4094)> - VLAN ID は一意の値です。特定の VLAN を表します(値の有効範囲:1 ～ 4094)。
・ Group <Address> - VLAN ID のグループ アドレスを表示します。
・ switch <switch_name> - 指定されたコンテキストを表示します。この値は、本機のコンテキストの一意の名前を表します。この値は、最大サイズが 32の文字列です。このパラメータは、マルチインスタンス機能に固有です。

■設定モード: 特権EXECモード

25. show ip igmp snooping mrouter

■説明:
指定したスイッチまたは指定したVLANのルータポートの情報を表示します。スイッチとVLANは、指定されていない場合はすべての情報を表示します。インタフェースの詳細と、対応するポート番号、およびそのタイプ (静的/動的) が表示されます。

■構文:show ip igmp snooping mrouter [Vlan <vlan-id >] [detail] [switch<switch_name>]

■パラメータの説明:
・ < vlan-id (1-4094)> - VLANを表す一意の値です(値の有効範囲:1 ～ 4094)。
・ detail - 詳細情報を表示します。
・ switch <switch_name> - 指定されたコンテキストのルータのポートを表示します。この値は、本機のコンテキストの一意の名前を表します。この値は、最大サイズが 32の文字列です。このパラメータは、マルチインスタンス機能に固有です。

■設定モード:特権EXECモード

26. show ip igmp snooping multicast-vlan

■説明:
スイッチ内のマルチキャストVLAN 統計情報を表示し、マルチキャストVLAN にマッピングされたさまざまなプロファイルを表示します。

■構文:show ip igmp snooping multicast-vlan [switch <switch_name>]

■パラメータの説明:
・ switch <switch_name> - 指定のコンテキストを表示します。この値は、本機のコンテキストの一意の名前を表します。この値は、最大サイズが 32の文字列です。このパラメータは、マルチインスタンス機能に固有です。

■設定モード:特権EXECモード

27. show ip igmp snooping port-cfg

■説明
すべての内部 VLAN、指定した内部VLAN、またはIGMP スヌーピングポートの設定情報を表示します。

■構文:
・ show ip igmp snooping port-cfg [{interface <interface-type><interface-id> [vlan-id(1-4094)] | switch<switch_name>}]

■パラメータの説明:
・ interface - インタフェースのタイプと識別子。
・ <interface-type> - 指定されたタイプのインタフェースのIPインタフェースを表示します。
インタフェースは次のとおりです。
  - gigabitethernet -1 秒あたり最大 1 ギガビットのデータ転送をサポートする LAN 標準アーキテクチャのバージョン。
  - port-channel – 複数のポートが集約されたアグリゲータを表す論理インタフェース。
・ <interface-id> - 指定されたインタフェース識別子のIPインタフェースを表示します。これは、特定のインタフェースを表す一意の値です。この値は、スロット番号とポート番号をスラッシュで区切って組み合わせたものです。
・ 例) 0/1:スロット番号が「0」、ポート番号が「1」であることを表します。
・ vlan-id(1-4094) - VLANを表す一意のIDです。
・ <switch_name> - 指定されたコンテキストを表示します。この値は、本機のコンテキストの一意の名前を表します。この値は、最大サイズが 32の文字列です。このパラメータは、マルチインスタンス機能に固有です。

■設定モード:特権EXECモード

28. show ip igmp snooping statistics

■説明
指定したスイッチ、または指定したVLANのブロック・ルータポートを表示します。

■構文:
・ show ip igmp snooping statistics [Vlan <vlan-id >] [switch<switch_name>]

■パラメータの説明:
・ < vlan-id (1-4094)> - VLANを表す一意の値です(値の有効範囲:1 ～ 4094)。
・ switch <switch_name> - 指定のコンテキストを表示します。この値は、本機のコンテキストの一意の名前を表します。この値は、最大サイズが 32の文字列です。このパラメータは、マルチインスタンス機能に固有です。

■設定モード:特権EXECモード

29. shutdown snooping

■説明:
本機のスヌーピングをシャットダウンします。ユーザが IGMPスヌーピング モジュールを実行する必要がない場合は、シャットダウンできます。シャットダウンすると、スヌーピング モジュールによって取得されたすべてのリソースがシステムに解放されます。

コマンドの no 形式を使用すると、本機のスヌーピングが開始され、有効になります。

■構文:
・ shutdown snooping
・ no shutdown snooping

■設定モード:グローバルコンフィグレーションモード

3.2.10 MLD

1. ipv6 mld snooping

■説明:スイッチまたは指定したVLAN での MLD スヌーピングを有効にします。

このコマンドのno形式を使用すると、スイッチまたは特定のVLANでのMLDスヌーピングが無効になります。

✏ MLDスヌーピング が VLAN に対して有効にできるのは、MLDスヌーピング が開始されている場合のみです。
スイッチと VLAN がアクティブになります。

■構文:
・ ipv6 mld snooping
・ no ipv6 mld snooping

■設定モード:グローバルコンフィグレーションモード/ Config-VLANモード

2. ipv6 mld snooping report-suppression-interval

■説明:
同じマルチキャストグループのMLDv1のレポートメッセージが、ルータポートに転送されない時間間隔です。

このタイマーは、プロキシとプロキシ レポートの両方が無効な場合に使用されます。そのグループのレポート メッセージが転送される開始されます。この時間内に同じグループの別のレポートを受信した場合、そのレポートは転送されません。

このコマンドの no 形式は、MLD スヌーピングレポート抑制間隔をデフォルト値に設定します。

■構文:
・ ipv6 mld snooping report-suppression-interval <(0-25) seconds>
・ no ipv6 mld snooping report-suppression-interval

■設定モード:グローバルコンフィグレーションモード

3. ipv6 mld snooping group-query-interval

■説明:グループスペシフィックククエリをポートに送信するまでの時間間隔を設定します(値の有効範囲:2 ～ 5)。

このコマンドの no 形式は、MLDスヌーピングの クエリ間隔をデフォルト値に設定します。

■構文:
・ ipv6 mld snooping group-query-interval <(2 - 5) seconds>
・ no ipv6 mld snooping group-query-interval

■設定モード:グローバルコンフィグレーションモード

4. ipv6 mld snooping version

■説明:特定の VLAN の MLDスヌーピングの動作時のバージョンを指定します。

■構文:ipv6 mld snooping version {v1 | v2}

■パラメータの説明:

・ v1 - バージョンを MLDv1 として設定します。MLDスヌーピングのレポートには、グループ アドレスを使用してのみ アクセスできます。leaveリクエストのオプションが提供されます。
・ v2 - バージョンを MLDv2 として設定します。MLDスヌーピングのレポートには、送信元およびグループ アドレスを 使用してアクセスします(※ただし、サポート対象外となります)。

■設定モード:Config-VLANモード

5. ipv6 mld snooping fast-leave

■説明:
VLAN のfast leave処理を有効にします。fast-leaveが有効な場合は、スイッチはグループスペシフィックククエリを送信せず、マルチキャストテーブルのエントリから即座に削除します。
fast-leaveが無効になっている場合、Leaveメッセージを受信したルータは、マルチキャストテーブルのエントリから削除する前にグループスペシフィックククエリを送信し、グループに他のレシーバがいるかどうかを確認します。

コマンドの no 形式は、指定したVLAN のfast leave処理を無効にします。

■構文:
・ ipv6 mld snooping fast-leave
・ no ipv6 mld snooping fast-leave

■設定モード:Config-VLANモード

6. IPv6 mld snooping querier

■説明:
MLDスヌーピングを特定の VLAN のクエリアとして設定します。スイッチは、一定の時間間隔でジェネラルクエリの送信を開始します。ルータのポートが動作的にダウンし、スイッチにルータのポートがない場合、スイッチはクエリア機能を継続します。

このコマンドの no 形式は、no形式を設定すると、指定したVLANのクエリアではなくなります。

✏本設定は、本機のVLAN機能が有効な場合のみ実行可能です。

■構文:
・ ipv6 mld snooping querier
・ no ipv6 mld snooping querier

■設定モード: Config-VLANモード

7. ipv6 mld snooping query-interval

■説明:
マルチキャストグループが有効かどうかを確認するグループスペシフィックククエリの送信間隔を設定します（値の有効範囲:60 ～ 600）。
このコマンドの no 形式は、MLDスヌーピングクエリ間隔をデフォルト値に設定します。

■構文:
・ ipv6 mld snooping query-interval <(60 - 600) seconds>
・ no ipv6 mld snooping query-interval

■設定モード: Config-VLANモード

8. ipv6 mld snooping mrouter

■説明:
マルチキャストルータを接続するポートを手動で設定します。

このコマンドの no 形式を使用すると、手動で設定したルータポートは削除されます。
デフォルトでは、静的なルータポートは設定されておらず、ルータポートは動的に登録されます。

物理インタフェースの設定は、VLANインタフェースのメンバーポートとして設定されている場合にのみ可能です。

■構文:
・ ipv6 mld snooping mrouter <interface-type> <interface-id>
・ no ipv6 mld snooping mrouter <interface-type> <interface-id>

■パラメータの説明:
・ <interface-type> - 指定されたタイプのインタフェースのIPインタフェースを表示します。
  インタフェースは次のとおりです。
  - gigabitethernet -1 秒あたり最大 1 ギガビットのデータ転送をサポートする LAN 標準アーキテクチャのバージョン。
  - port-channel – 複数のポートが集約されたアグリゲータを表す論理インタフェース。
・ <interface-id> - インタフェースのリストまたは特定のインタフェース識別子のマルチキャストルータのポートのリストを設定します。この値は、スロット番号とポート番号をスラッシュで区切って組み合わせたものです。インタフェースタイプ ポート チャネルのポート チャネル ID が提供されます。インタフェースのリストを設定する際には、スペースを使用せずにカンマを区切り文字として使用します(例: 0/1, 0/3 または1、3)。

■設定モード: Config-VLANモード

9. ipv6 mld snooping blocked-router

■説明:ルータポートをブロック・ルータポートとして設定します。

コマンドの no 形式は、ブロック・ルータポートを通常のルータポートに戻します。

✏ 動作中のルータポートにこの設定をしないでください。

■構文:
・ ipv6 mld snooping blocked-router <interface-type> <interface-id>
・ no ipv6 mld snooping blocked-router <interface-type> <interface-id>

■パラメータの説明:
・ <interface-type> - 指定されたタイプのインタフェースのIPインタフェースを表示します。
インタフェースは次のとおりです。
  - gigabitethernet -1 秒あたり最大 1 ギガビットのデータ転送をサポートする LAN 標準アーキテクチャのバージョン。
  - port-channel – 複数のポートが集約されたアグリゲータを表す論理インタフェース。
・ <interface-id> - インタフェースのリストまたは特定のインタフェース識別子のマルチキャストルータのポートのリストを設定します。この値は、スロット番号とポート番号をスラッシュで区切って組み合わせたものです。インタフェースタイプ ポート チャネルのポート チャネル ID が提供されます。インタフェースのリストを設定する際には、スペースを使用せずにカンマを区切り文字として使用します(例: 0/1, 0/3 または 1、3)。

■設定モード:Config-VLANモード

10. multicast-filtering

■説明:スイッチのマルチキャストフィルタリングを有効/無効にします。

■構文:multicast-filtering {enable | disable}

■パラメータの説明:
・ enable - マルチキャストフィルタリングを有効にします。
・ disable - マルチキャストフィルタリングを無効にします。

■設定モード:グローバルコンフィグレーションモード

11. show ipv6 mld snooping mrouter

■説明:
MLDスヌーピングが設定されているVLANを指定してルータポートを表示します。VLANの指定をしない場合は、すべてのVLANについての情報が表示されます。

■構文:
・ show ipv6 mld snooping mrouter [Vlan <vlan-id >] [detail] [switch <switch_name>]

■パラメータの説明:
・ < vlan-id (1-4094)> - VLANを表す一意の値です(値の有効範囲:1 ～ 4094)。
・ detail - ルータのポートに関する詳細情報を表示します。
・ switch <switch_name> - 指定されたコンテキストのルータのポートを表示します。この値は、本機のコンテキストの一意の名前を表します。この値は、最大サイズが 32の文字列です。このパラメータは、マルチインスタンス機能に固有です。

■設定モード:特権EXECモード

12. show ipv6 mld snooping globals

■説明:スイッチ全体でのMLDスヌーピング情報を表示します。

■構文:show ipv6 mld snooping globals [switch <switch_name>]

■パラメータの説明:
・ switch <switch_name> - 指定されたコンテキストのルータのポートを表示します。この値は、本機のコンテキストの一意の名前を表します。この値は、最大サイズが 32の文字列です。このパラメータは、マルチインスタンス機能に固有です。

■設定モード:特権EXECモード

13. show ipv6 mld snooping

■説明:
指定したVLANのMLDスヌーピングの情報を表示します。VLANを指定しない場合は、すべてのVLANの情報を表示します。

■構文:
・ show ipv6 mld snooping [Vlan <vlan-id >] [switch<switch_name>]

■パラメータの説明:
・ < vlan-id (1-4094)> - VLANを表す一意の値です(この値の有効範囲は 1 ～ 4094。
・ switch <switch_name> - 指定されたコンテキストのルータのポートを表示します。この値は、本機のコンテキストの一意の名前を表します。この値は、最大サイズが 32の文字列です。このパラメータは、マルチインスタンス機能に固有です。

■設定モード:特権EXECモード

14. show ipv6 mld snooping forwarding-database

■説明:マルチキャストのFDB(Forwarding Database)を表示します。

■構文:
・ show ipv6 mld snooping forwarding-database [Vlan <vlan-id >] [switch <switch_name>]

■パラメータの説明:
・ < vlan-id (1-4094)> - VLAN を表す一意の値です(値の有効範囲:1 ～ 4094)。
・ switch <switch_name> - 指定されたコンテキストを表示します。この値は、本機のコンテキストの一意の名前を表します。この値は、最大サイズが 32の文字列です。このパラメータは、マルチインスタンス機能に固有です。

■設定モード:特権EXECモード

15. show ipv6 mld snooping groups

■説明:
指定したVLANのマルチキャストグループの情報を表示します。VLANを指定しない場合は、すべてのVLANの情報を表示します。

■構文:
・ show ipv6 mld snooping groups [Vlan <vlan-id > [Group<Address>]] [switch <string (32)>]

■パラメータの説明:
・ < vlan-id (1-4094)> - VLAN を表す一意の値です(値の有効範囲:1 ～ 4094)。
・ Group <Address> - VLAN ID のグループ アドレスを表示します。
・ switch <switch_name> - 指定されたコンテキストを表示します。この値は、本機のコンテキストの一意の名前を表します。この値は、最大サイズが 32の文字列です。このパラメータは、マルチインスタンス機能に固有です。

■設定モード:特権EXECモード

16. show ipv6 mld snooping statistics

■説明:
指定したVLANのMLDスヌーピングの統計情報を表示します。VLANを指定しない場合は、すべてのVLANの情報を表示します。

■構文:
・ show ipv6 mld snooping statistics [vlan <vlan-id >] [switch<string (32)>]

■パラメータの説明:

・ < vlan-id (1-4094)> - VLAN を表す一意の値です(値の有効範囲:1 ～ 4094)。
・ switch <switch_name> - 指定されたコンテキストを表示します。この値は、本機のコンテキストの一意の名前を表します。この値は、最大サイズが 32の文字列です。このパラメータは、マルチインスタンス機能に固有です。

■設定モード:特権EXECモード

17. show multicast-filtering status

■説明:マルチキャストフィルタリングのステータスを表示します。

■構文:show multicast-filtering status

■設定モード:特権EXECモード

3.2.11 jumbo-frame

1. jumbo-frame

■説明:
イーサネット標準の最大フレームサイズ（1518byte）を超えるサイズのフレームをジャンボフレームと呼びます。
インタフェースで送受信できる1フレームあたりの最大サイズを設定します。値の範囲は1522～10240、単位はbyte です。ただし、ファストイーサネットの場合、値は1522以下の値のみ有効です。

■構文:jumbo-frame <frame-size(1522-10240)>

■パラメータの説明:
・ <frame-size(1522-10240)> - 有効なジャンボフレームのサイズを表します。

■設定モード:グローバルコンフィグレーションモード

2. show jumbo-frame

■説明:スイッチで送受信されるジャンボフレームのサイズを表示します。

■構文:show jumbo-frame

■設定モード:特権EXECモード

3.2.12 SNMP

1. disable snmpagent

■説明:このコマンドは SNMP エージェントを無効にします。

■構文:disable snmpagent

■設定モード:グローバルコンフィグレーションモード

2. enable snmpagent

■説明:
SNMPエージェントを有効にします。
SNMPエージェントは、SNMPマネージャからの要求を受けて応答を返したり、何らかの状態変化が発生した際にSNMPマネージャに通知(トラップ)したりします。

■構文:enable snmpagent

■設定モード:グローバルコンフィグレーションモード

3. show mib name

■説明:対応する mib オブジェクト識別子の名前を表示します。

■構文:show mib name <Object OID>

■パラメータの説明
・ OID:例 1.3.6.1.6.1

■設定モード:特権EXECモード

4. show snmp

■説明:SNMP 通信のステータス情報を表示します。

■構文:show snmp

■設定モード:特権EXECモード

5. show snmp community

■説明:SNMP コミュニティの詳細を表示します。

■構文:show snmp community

■設定モード:特権EXECモード

6. show snmp group

■説明:設定されたSNMPグループを表示します。

■構文:show snmp group

■設定モード:特権EXECモード

7. show snmp group access

■説明:設定されたSNMPグループアクセスの詳細を表示します。

■構文:show snmp group access

■設定モード:特権EXECモード

8. show snmp inform statistics

■説明:通知メッセージの統計情報を表示します。

■構文:show snmp inform statistics

■設定モード:特権EXECモード

9. show snmp engineid

■説明:このコマンドはエンジン識別子を表示します。

■構文:show snmp engineid

■設定モード:特権EXECモード

10. show snmp notif

■説明:SNMP通知タイプを表示します。

■構文:show snmp notif

■設定モード:特権EXECモード

11. show snmp-server proxy-udp-port

■説明:このコマンドはプロキシの udp ポートを表示します。

■構文:show snmp-server proxy-udp-port

■設定モード:特権EXECモード

12. show snmp-server traps

■説明:現在有効なトラップのセットを表示します。

■構文:show snmp-server traps

■設定モード:特権EXECモード

13. show snmp targetaddr

■説明:SNMP 宛先アドレスを表示します。

■構文:show snmp targetaddr

■設定モード:特権EXECモード

14. show snmp targetparam

■説明:SNMP 宛先アドレスのパラメータを表示します。

■構文:show snmp targetparam

■設定モード:特権EXECモード

15. show snmp user

■説明:SNMP ユーザを表示します。

■構文:show snmp user

■設定モード:特権EXECモード

16. show snmp tcp

■説明:tcp 経由で snmp の設定を表示します。

■構文:show snmp tcp

■設定モード:特権EXECモード

17. show snmp viewtree

■説明:SNMP ツリービューを表示します。

■構文:show snmp viewtree

■設定モード:特権EXECモード

18. snmp access

■説明:
SNMP グループ アクセスの詳細を設定します。
グループに応じて SNMP アクセスを設定するには、snmp group コマンドを使用してグループを設定してください。

このコマンドの no 形式を使用すると、SNMP グループのアクセス詳細は削除されます。

■構文:
- snmp access <GroupName> {v1 | v2c | v3 {auth | noauth | priv}} [read <ReadView | none>] [write <WriteView | none> [notify <NotifyView | none>] [{volatile | nonvolatile}] [context<string(32)>]
- no snmp access <GroupName> {v1 | v2c | v3 {auth | noauth | priv}}

■パラメータの説明:
- <GroupName> - アクセスを提供するグループの名前を設定します。
- v1 | v2c | v3 - SNMP バージョンを設定します。
  - v1 – SNMP バージョンをバージョン 1 に設定します。
  - v2c – SNMP バージョンをバージョン 2c に設定します。
  - v3 – SNMP バージョンをバージョン 3 に設定します。これは、priv キーワードを使用したパケット暗号化を許可するため、最も安全なモデルです。
- auth - メッセージ ダイジェスト (MD5) またはセキュア ハッシュ アルゴリズム (SHA) パケット認証を有効にします。
- noauth - 認証なしを設定します。
- priv - 認証とプライバシーの両方を設定します。
- read<ReadView> - 読み取りが許可されるSNMPのMIBビューのコンテキストを指定します。<none>を指定すると、ビューを指定しません。
- write<WriteView> - 書き込みが許可されるSNMPのMIBビューのコンテキストを指定します。<none>を指定すると、ビューを指定しません。
- notify<NotifyView> -通知が許可されるSNMPのMIBビューのコンテキストを指定します。<none>を指定すると、ビューを指定しません。
  - volatile| nonvolatile - グループ エントリに必要なストレージ タイプを設定します。
  - volatile – ストレージ タイプを一時的に設定します。システムの再起動時に config の設定を消去します。
- nonvolatile – ストレージの種類を永続的に設定します。設定を保存し、システムを再起動すると保存した設定が表示されます。
- context<string(32)> - SNMP コンテキストの名前を設定します。文字列の最大長は 32 です。

■設定モード:グローバルコンフィグレーションモード

19. snmp agent port

■説明:
SNMPエージェントが使用するUDPポートを設定します（デフォルトの値は161、値の有効範囲:1 ～ 65535）。

■構文:snmp agent port <port>

■設定モード:グローバルコンフィグレーションモード

20. snmp community

■説明:
SNMP マネージャとスイッチ間のインタフェースを提供する SNMP エージェントを有効にします。エージェントは、マネージャから受信した SNMP パケットを処理し、適切な応答パケットをフレーム化してマネージャに送信します。

■構文:
- snmp community name <CommunityName> security<SecurityName> [context <name>] [{volatile | nonvolatile}] [transporttag <TransportTagIdentifier | none>]
- no snmp community name < CommunityName >

■パラメータの説明:
- name<CommunityName> - コミュニティ文字列を格納するコミュニティ名を設定ます。
- security<SecurityName> - 対応する SNMP コミュニティ名のセキュリティ モデルを格納します。
- context - SNMP コンテキストの名前を設定します。
- volatile | nonvolatile - エントリに必要なストレージ タイプを設定します。
- volatile – ストレージ タイプを一時的に設定します。システムの再起動時にconfigの設定を消去します。
- nonvolatile – ストレージの種類を永続的に設定します。設定をシステムに保存します。保存された設定は、システムを再起動すると表示されます。
- <TransportTagIdentifier> - コマンド レスポンダー アプリケーションが管理リクエストに応答可能なトランスポート エンドポイントのセットを指定します。

■設定モード:グローバルコンフィグレーションモード

21. snmp engineid

■説明:
SNMPv3エージェントを識別するためのエンジンID を設定します。
コマンドの no 形式は、エンジンID をデフォルト値にリセットします。

■構文:
- snmp engineid <EngineIdentifier>
- no snmp engineid

■設定モード:グローバルコンフィグレーションモード

22. snmp group

■説明:
SNMP グループの詳細を設定します。
このコマンドの no 形式を使用すると、SNMP グループの詳細は削除されます。

■構文:
・ snmp group <GroupName> user <UserName> security-model {v1 | v2c | v3 } [{volatile | nonvolatile}]
・ no snmp group <GroupName> user <UserName> security-model {v1 | v2c | v3 }

■パラメータの説明:
・ <GroupName> - SNMP グループの名前を設定ます。
・ user<UserName> - 設定されたグループのユーザを設定します。
・ security-model - SNMP のセキュリティ モデルを設定します。
  - v1 - SNMP バージョンをバージョン 1 に設定します。
  - v2c - SNMP バージョンをバージョン 2c に設定します。
  - v3 - SNMP バージョンをバージョン 3 に設定します。
・ volatile| nonvolatile - グループ エントリに必要なストレージ タイプを設定します。
・ volatile – ストレージ タイプを一時的に設定します。システムの再起動時にconfigの設定を消去します。
・ nonvolatile – ストレージの種類を永続的に設定します。設定をシステムに保存します。保存された設定は、システムを再起動すると表示されます。

■設定モード: グローバルコンフィグレーションモード

23. snmp notify

■説明:
SNMP 通知の詳細を設定します。
このコマンドの no 形式を使用すると、SNMP 通知の詳細は削除されます。

■構文:
・ snmp notify <NotifyName> tag <TagName> type {Trap | Inform} [{volatile | nonvolatile}]
・ no snmp notify <NotifyName>

■パラメータの説明:
・ <NotifyName> - エントリに関連付けられた一意の識別子を設定します。
・ tag<TagName> - 宛先アドレステーブル内のエントリを選択する通知タグを設定します。
・ type - 通知タイプを設定します。
  リストには次のものが含まれます。
  - Trap - SNMP マネージャにトラップを送信するようになります。
  - Inform - SNMP マネージャに通知のリクエストを送信します
・ volatile - ストレージ タイプを一時的に設定します。システムの再起動時にconfigの設定を消去します。
・ nonvolatile - ストレージ タイプを永続的に設定します。設定をシステムに保存します。保存された設定は、システムを再起動すると表示できます。

■設定モード: グローバルコンフィグレーションモード

24. snmp-server enable traps snmp authentication

■説明:
SNMP認証失敗を通知するSNMPトラップを有効にします。

コマンドの no 形式を使用すると、認証失敗トラップの生成が無効になります。

■構文:
・ snmp-server enable traps snmp authentication
・ no snmp-server enable traps snmp authentication

■設定モード:グローバルコンフィグレーションモード

25. snmp targetaddr

■説明:
SNMP 宛先アドレスを設定します。
コマンドの no 形式は、設定された SNMP 宛先アドレスを削除します。

■構文:
・ snmp targetaddr <TargetAddressName> param <ParamName>{<IPAddress> | <IPv6Address>} [timeout <Seconds(1-1500)] [retries <RetryCount(1-3)] [taglist <TagIdentifier(1-20)>] [{volatile | nonvolatile}] [port <integer (1-65535)>]
・ no snmp targetaddr <TargetAddressName>

■パラメータの説明:
・ <TargetAddressName> - 宛先の一意の識別子を設定します。
・ param<ParamName> -宛先パラメータの名前を設定します。
・ IP Address - SNMPトラップの通知先になるホストのIPアドレスを設定します。
・ IPv6Address -SNMPトラップの通知先になるホストのIPv6アドレスを設定します(※本機器では未サポート)。
・ timeout<Seconds(1-1500)> - SNMP エージェントが通知要求メッセージを再送信する前に SNMP からの応答を待つ時間を設定します（値の有効範囲:1 ～ 1500 秒）。
・ retries<RetryCount(1-3)> - エージェントが通知要求メッセージを再送信できる最大回数を設定します（値の有効範囲は 1 ～ 3）。
・ タグリスト<タグ識別子 | none> - SNMP の宛先アドレスを選択するタグ識別子を設定します。
・ volatile - ストレージタイプを一時的に設定します。システムの再起動時にconfigの設定を消去します。
・ nonvolatile - ストレージタイプを永続的に設定します。設定をシステムに保存します。保存された設定は、システムを再起動すると表示できます。
・ port <integer (1-65535)> - 生成された SNMP 通知が宛先アドレスに送信されるポート番号を設定します(値の有効範囲:1 ～ 65535)。

■設定モード:グローバルコンフィグレーションモード

26. snmp targetparams

■説明:
SNMP 宛先パラメータを設定します。
コマンドの no 形式は、SNMP 宛先パラメータを削除します。

■構文:
・ snmp targetparams <ParamName> user <UserName> security- model {v1 | v2c | v3 {auth | noauth | priv}} message-processing{v1 | v2c | v3} [{volatile | nonvolatile}]

・ no snmp targetparams <ParamName>

■パラメータの説明:
・ <ParamName> - パラメータの一意の識別子を設定します。
・ user <UserName> - 宛先パラメータを実行するユーザを設定します。
・ security-model - セキュリティ モデルを設定します
  - v1 – SNMP バージョンをバージョン 1 に設定します。
  - v2c – SNMP バージョンをバージョン 2c に設定します。
  - v3 – SNMP バージョンをバージョン 3 に設定します。priv キーワードを使用したパケット暗号化が可能なため、最も安全なモデルです。
  - auth - メッセージ ダイジェスト (MD5) またはセキュア ハッシュ アルゴリズム (SHA) パケット認証を有効にします。
  - noauth - 認証なしを設定します
  - priv - 認証とプライバシーの両方を指定します
・ message-processing - メッセージ処理モデルを設定します
  - v1 – SNMP バージョンをバージョン 1 に設定します。
  - v2c – SNMP バージョンをバージョン 2c に設定します。
  - v3 – SNMP バージョンをバージョン 3 に設定します。これは、priv キーワードを使用したパケット暗号化を許可するため、最も安全なモデルです。
・ volatile - ストレージ タイプを一時的に設定します。システムの再起動時にconfigの設定を消去します。
・ nonvolatile - ストレージ タイプを永続的に設定します。設定をシステムに保存します。保存された設定は、システムを再起動すると表示できます。

■設定モード: グローバルコンフィグレーションモード

27. snmp trap link-status

■説明:
インタフェースでのトラップ生成を有効/無効にします。
インタフェースのリンクアップ／リンクダウンを検出した場合、Link-up／Link-downのSNMPトラップを生成します。

■構文:
・ snmp trap link-status
・ no snmp trap link-status

■設定モード:インタフェースコンフィグレーションモード

28. snmp user

■説明:
SNMP ユーザの詳細を設定します。

このコマンドの no 形式を使用すると、SNMP ユーザの詳細は削除されます。

■構文:
・ snmp user <UserName> [auth {md5 | sha} <passwd> [priv {{{DES| AES_CFB128} <passwd> } | None}]] [{volatile | nonvolatile}]
・ no snmp user <UserName>

■パラメータの説明:
・ <UserName> - セキュリティユーザ名を設定します。
・ auth - 認証アルゴリズムを設定します。オプションは次のとおりです。
  - md5 - メッセージ ダイジェスト 5 ベースの認証を設定します。
  - sha - セキュリティ ハッシュ アルゴリズム ベースの認証を設定します。
・ <Passwd> - 設定された認証アルゴリズムに使用される認証パスワードを設定します。
・ priv - DES 暗号化と、暗号化キーに使用されるパスワードを設定します。オプションは次のとおりです。
  - DES – データ暗号化標準アルゴリズム関連の設定を設定します。
  - AES_CFB128 – 暗号化用の Advanced Encryption Standard (AES) アルゴリズムを設定します。
  - <Passwd> - 設定された認証アルゴリズムに使用される認証パスワードを設定します。
  - None - 暗号化設定を設定しません。
・ volatile - ストレージタイプを一時的に設定します。システムの再起動時にconfigの設定を消去します。
・ nonvolatile - ストレージタイプを永続的に設定します。設定をシステムに保存します。保存された設定は、システムを再起動すると表示できます。

■設定モード:グローバルコンフィグレーションモード

29. snmp view

■説明:
このコマンドは SNMP ビューを設定します。

このコマンドの no 形式を使用すると、SNMP ビューは削除されます。

■構文:
・ snmp view <ViewName> <OIDTree> [mask <OIDMask>] {included| excluded} [{volatile | nonvolatile}]
・ no snmp view <ViewName> <OIDTree>

■パラメータの説明:
・ <ViewName> - ビューの詳細を設定するビューの名前を指定します（最大20文字の文字列」）。
・ <OIDTree> - 特定のビューのサブツリー値を指定します。
・ mask <OIDMask> - 特定のビューのマスク値を指定します。
・ included - サブツリーへのアクセスを許可します
・ excluded - サブツリーへのアクセスを拒否します
・ volatile - ストレージタイプを一時的に設定します。システムの再起動時にconfigの設定を消去します。
・ nonvolatile - ストレージタイプを永続的に設定し、設定内容をシステムに保存します。保存された設定は、システムを再起動すると表示できます。

■設定モード: グローバルコンフィグレーションモード

3.2.13 DNS

1. ip name-server

■説明:
ドメインネームサーバのIPアドレスを設定します。

コマンドの no 形式は、ドメイン ネーム サーバに設定した IP アドレスを削除します。

■構文:
・ ip name-server ipv4 <ucast_addr>
・ no ip name-server ipv4 <ucast_addr>
・

■パラメータの説明:
・ <ucast_addr> - ドメイン ネーム サーバの IP アドレスを IPv4 アドレス形式で設定します。

■設定モード:グローバルコンフィグレーションモード

2. show ip dns name-server

■説明:DNS ネーム サーバの情報を表示します。

■構文:show ip dns name-server

■設定モード:特権EXECモード

3.2.14 IP

1. arp

■説明:ARPテーブルに静的にエントリを追加します。

■構文:
・ arp <ucast_addr> <ucast_mac> { Vlan <vlan_vfi_id> }
・ no arp {<ucast_addr>}

■パラメータの説明:
・ <ucast_addr> - ARP エントリの IP アドレスを設定します。
・ <ucast_mac> - 上記の IP アドレスに対応する MACアドレスを設定します。
・ <vlan_vfi_id> - VLANを表す一意の値です(値の有効範囲:1 ～ 4094)。

■設定モード:グローバルコンフィグレーションモード

2. arp timeout

■説明:
ARPキャッシュのタイムアウト値を設定します(値の範囲:30～86400)。スタティックのARPエントリは、この値の影響を受けません。

このコマンドの no 形式を使用すると、ARP キャッシュ タイムアウトがデフォルト値に設定されます。

■構文:
・ arp timeout <integer (30-86400)>
・ no arp timeout

■設定モード:グローバルコンフィグレーションモード

3. ip address

■説明:インタフェースの IP アドレスを設定します。

■構文:
・ ip address <ucast_addr> <ip_mask>
・ no ip address <ucast_addr>

■パラメータの説明:
・ ucast_addr - インタフェースの IP アドレスを設定します。インタフェースが属するネットワークにDHCPサーバを含む場合、DHCPのアドレスプールに含まれる範囲のIPアドレスを設定しないでください。
・ ip_mask - 設定された IP アドレスのサブネットマスクを設定します。設定されたサブネットマスクは、スイッチが配置されているネットワークの同じサブネット内にある必要があります。

■設定モード:インタフェースコンフィグレーションモード
※VLAN インタフェース モードに適用されます。

4. ip address dhcp

■説明:動的にIPアドレスを設定します。

■構文:
・ ip address dhcp
・ no ip address

■パラメータの説明:
・ dhcp – DHCP プロトコルを使用して IP を取得します。

■設定モード:インタフェースコンフィグレーションモード
※このコマンドは、VLAN インタフェース モードに適用されます。

5. ip arp max-retries

■説明:
ARP リクエストの最大再試行回数を設定します(値の有効範囲 2 ～ 10)。

このコマンドの no 形式では、ARPリクエストの最大再試行回数がデフォルト値に設定されます。

■構文:
・ ip arp max-retries <short (2-10)>
・ no ip arp max-retries

■パラメータの説明:
・ <short (2-10)> - ARP リクエストの最大再試行回数を設定します(値の有効範囲: 2 ～ 10)。

■設定モード:グローバルコンフィグレーションモード

6. ip dhcp snooping(グローバルコンフィグレーション)

■説明:
本機のレイヤー 2 DHCP スヌーピングをグローバルで有効にするか、特定の VLAN 内でスヌーピングを有効にします。DHCP スヌーピング モジュールは、スヌーピングがグローバルで有効な場合にプロトコル動作を開始します。

■構文:
・ ip dhcp snooping [vlan < vlan-id (1-4094)>]
・ no ip dhcp snooping [vlan < vlan-id (1-4094)>]

■設定モード:グローバルコンフィグレーションモード

7. ip dhcp snooping（Config-VLAN モード）

■構文:
・ ip dhcp snooping
・ no ip dhcp snooping

■設定モード:Config-VLANモード

8. ip dhcp snooping verify mac-address

■説明:Untrustポートに受信したDHCPパケットのmacアドレス検証を有効にします

■構文:
・ ip dhcp snooping verify mac-address
・ no ip dhcp snooping verify mac-address

■設定モード:グローバルコンフィグレーションモード

9. ip dhcp snooping trust

■説明:ポートをtrustedポートとして設定します。
■構文:
・ ip dhcp snooping trust
・ no ip dhcp snooping trust

■設定モード:インタフェースコンフィグレーションモード
※このコマンドは、PORT/PORT-CHANNEL インタフェース モードで適用されます。

10. ip route

■説明:
このコマンドはスタティック ルートを追加してください。ルートは、宛先に到達可能なIP アドレスまたはインタフェースを定義します。
このコマンドの no 形式を使用すると、スタティック ルートは削除されます。

■構文:
・ ip route <ip_addr> <ip_mask> <ucast_addr> [<short (1-254)>]
・ no ip route <ip_addr> <ip_mask>

■パラメータの説明:
・ <ip_addr>- 宛先ネットワークアドレスを設定します。
・ <ip_mask>-宛先ネットワークアドレスに対するサブネットマスクを設定します。
・ <ucast_addr> - そのネットワークに到達するために使用できるネクストホップの IP アドレスまたは IP エイリアスを定義します。

■設定モード:グローバルコンフィグレーションモード

11. show ip arp

■説明:ARPテーブルを表示します。

■構文:
・ show ip arp [{ Vlan <vlan_vfi_id> | <ucast_addr> | <ucast_mac>| summary | information | statistics }]

■パラメータの説明:
・ Vlan <vlan_vfi_id> - VLANを表す一意の値です(値の有効範囲:1 ～ 4094)。
・ <ucast_addr> - ARP エントリの IP アドレスを表示します。
・ <ucast_mac> - ARP エントリの MACアドレスを表示します。
・ summary - ARPテーブルの概要を表示します。
・ information - 最大再試行数とARP キャッシュ タイムアウトに関する ARP 設定情報を表示します。
・ statistics – ARP パケット統計情報を表示します。
・
・ ■設定モード:特権EXECモード

12. show ip dhcp snooping

■説明:
DHCP スヌーピング機能が有効なすべての VLAN の DHCP スヌーピング設定と統計情報を表示します。

■構文:
・ show ip dhcp snooping [vlan <vlan-id (1-4094)>] [switch<context name>]

■設定モード:特権EXECモード

13. show ip dhcp snooping globals

■説明:
DHCP スヌーピングのグローバル設定を表示します。レイヤー2のDHCP スヌーピングと MAC 検証のグローバル ステータスが表示されます。

■構文:show ip dhcp snooping globals [switch <string (32)>]

■設定モード:特権EXECモード

14. show ip route

■説明:IP ルーティング テーブルを表示します。

■構文:
・ show ip route [{ <ip_addr> [<ip_mask>] | connected | static | summary | details}]

■パラメータの説明:
・ <ip-address> - 指定された宛先 IP アドレスの IP ルーティング テーブルを表示します。
・ <mask> - 指定されたプレフィックス マスク アドレスの IP ルーティング テーブルを表示します。
・ Connected- 直接接続されているネットワーク ルートを表示します。
・ static - テーブルに登録されているスタティックルートを表示します。
・ summary - すべてのルートの概要を表示します。
・ details - すべてのルートの詳細を表示します。

■設定モード:特権EXECモード

15. show ip source binding dhcp-snooping

■説明:DHCPスヌーピングバインディングテーブルを表示します。

■構文:
・ show ip source binding dhcp-snooping [interface <interface- type> <interface-id>] [vlan <vlan-id (1-4094)>] [switch<switch_name>]

■パラメータの説明:
・ <interface-type> - DHCPスヌーピングバインディングテーブルを表示します。
インタフェースは次のとおりです。
  - gigabitethernet -1 秒あたり最大 1 ギガビットのデータ転送をサポートする LAN 標準アーキテクチャのバージョン。

■設定モード:特権EXECモード

3.2.15 DHCP Server

1. ip dhcp client fast-access

■説明:
Discoveryパケットのタイムアウト時間を短くし、待機時間を短くするDHCPクライアント高速接続モードを有効にします。

■構文:ip dhcp client fast-access

■設定モード:特権EXECモード

2. ip dhcp server

■説明:
ネットワーク上のDHCPサーバのIPアドレスを設定します。

コマンドの no 形式は、DHCPサーバのIPアドレスの設定を削除します。

■構文:
・ ip dhcp server <ip address>
・ no ip dhcp server <ip address>

■設定モード:グローバルコンフィグレーションモード

3. service dhcp-relay

■説明:
スイッチの DHCP リレー エージェントを有効にします。DHCP リレー エージェントは、異なるサブネットにある DHCP クライアントと DHCPサーバの間で DHCP メッセージを中継します。

コマンドの no 形式は、DHCP リレー エージェントを無効にします。

■構文:
・ service dhcp-relay
・ no service dhcp-relay

■設定モード:グローバルコンフィグレーションモード

4. show dhcp server

■説明: DHCPサーバの IP アドレスを表示します。

■構文:show dhcp server

■設定モード:特権EXECモード

5. show dhcp-relay

■説明:DHCP リレー エージェントの設定を表示します。

■構文:show dhcp-relay

■設定モード:特権EXECモード

3.2.16 IPv6

1. clear ipv6 neighbors

■説明:IPv6 ネイバー テーブル内のすべてのエントリを削除します。

■構文:clear ipv6 neighbors

■設定モード:グローバルコンフィグレーションモード

2. clear ipv6 route

■説明:IPv6 ルート テーブルのすべてのエントリを削除します。

■構文:clear ipv6 route

■設定モード:グローバルコンフィグレーションモード

3. clear ipv6 traffic

■説明:IPv6 トラフィック テーブル内のすべてのエントリを削除します。

■構文:clear ipv6 traffic

■設定モード:グローバルコンフィグレーションモード

4. ipv6 address dhcp

■説明:
インタフェース上で DHCPv6 クライアント機能を有効にし、クライアントからの設定情報を要求します。
コマンドの no 形式は、インタフェース上の DHCPv6 クライアント機能を無効にします。

■構文:
・ ipv6 address dhcp [stateful | stateless]
・ no ipv6 address dhcp

■パラメータ
・ stateful - ステートフルDHCPv6を設定します。
・ stateless - ステートレスDHCPv6を設定します。

■設定モード:インタフェースコンフィグレーションモード
※VLANインタフェースモードに適用されます。

5. ipv6 address - link local

■説明:
インタフェース上に IPv6リンクローカル アドレスを設定します。リンクローカル アドレスは、ローカル ネットワークのセグメント(リンク)またはポイントツーポイント接続内の通信のみを目的とした IP アドレスです。

■構文:ipv6 address <prefix> link-local

■パラメータの説明:
・ <prefix> - インタフェースの IPv6 プレフィックスを設定します。

設定モード:インタフェースコンフィグレーションモード

6. ipv6 address - prefix and prefix length

■説明:
インタフェース上に IPv6 アドレスを設定します。

コマンドの no 形式は、インタフェース上の IPv6 アドレスを無効にします。

■構文:
・ ipv6 address { <prefix> "/" <prefix Len>} [{unicast| link-local }]
・ no ipv6 address <prefix> <prefix Len> [unicast]

■パラメータの説明:
・ <prefix> - インタフェースの IPv6 プレフィックスを設定します。
・ <prefix Len> - IPv6 アドレスのサブネットプレフィックスのビット数を設定します。この値は、ネットワーク内のすべてのホストで共通です(値の有効範囲:0 ～ 128)。
・ unicast - プレフィックスのアドレス タイプをユニキャストとして設定します。
・ link-local - プレフィックスのアドレス タイプをリンク ローカルとして設定します。

■設定モード:インタフェースコンフィグレーションモード
※VLAN インタフェース モードに適用されます。

7. ipv6 enable

■説明:
明示的な IPv6 アドレスが設定されていないインタフェースでの IPv6 処理を有効にします。

コマンドの no 形式は、インタフェースでの IPv6 処理を無効にします。

■構文:
・ ipv6 enable
・ no ipv6 enable

■設定モード:インタフェースコンフィグレーションモード
※VLANインタフェースモードに適用されます。

8. ipv6 neighbor

■説明:
IPv6 ネイバー キャッシュ テーブルに静的エントリを設定します。

このコマンドの no 形式を使用すると、IPv6 ネイバー キャッシュ テーブルからスタティック エントリは削除されます。

■構文:
・ pv6 neighbor <prefix> {vlan <vlan-id> <MAC ADDRESS (xx:xx:xx:xx:xx:xx)>}
・ no ipv6 neighbor <prefix> {vlan <vlan-id> <MAC ADDRESS xx:xx:xx:xx:xx:xx>}

■設定モード:グローバルコンフィグレーションモード

9. ipv6 route

■説明:
ルートは、宛先に到達可能なIPv6 アドレスまたはインタフェースを定義します。

このコマンドの no 形式を使用すると、スタティック ルートは削除されます。

■構文:
・ ipv6 route <prefix> <prefix len> ([<NextHop>])
・ no ipv6 route <prefix> <prefix len>

■設定モード:グローバルコンフィグレーションモード

10. ipv6 unicast-routing

■説明:
ユニキャストルーティングを有効にします。
IPv6 ユニキャスト アドレスは、単一ノード上の単一インタフェースの識別子です。ユニキャスト アドレスに送信されたパケットは、そのアドレスによって識別されるインタフェースに配信されます。

このコマンドの no 形式を使用すると、ユニキャストルーティングが無効になります。

■構文:
・ ipv6 unicast-routing
・ no ipv6 unicast-routing

■設定モード:グローバルコンフィグレーションモード

11. ping ipv6

■説明:IPv6 エコー メッセージと合計パケット数を宛先に送信します。

■構文:
・ ping ipv6 <prefix%interface> [repeat <count>] [size <value>] [source {vlan <vlan-id> <source_prefix>}] [timeout <value (1- 100)>]

■パラメータの説明:
・ <prefix%interface> - IPv6 宛先プレフィックスを設定します。
・ repeat<count> - ping メッセージの送信数を設定します。範囲は 0 ～ 10 の間で変化します。
・ size<value> - メッセージ内の Ping パケットのデータ部分のサイズを設定します。
・ source - ping メッセージの送信元 インタフェースを設定します。
・ vlan <vlan-id> - VLAN を表す一意の値です(値の有効範囲:1 ～ 4094)。
・ <source_prefix> - ping メッセージの送信元プレフィックスを設定します。
・ timeout <値 (1-100)> - ping応答が確認できずタイムアウトするまでの時間を設定します(値の有効範囲: 1 ～ 100)。

■設定モード:特権EXECモード

12. show ipv6 interface

■説明:IPv6 インタフェースを表示します。

■構文:show ipv6 interface [{vlan <vlan-id> [prefix]}]

■パラメータの説明:
・ < vlan-id (1-4094)> - VLANを表す一意の値です(値の有効範囲:1 ～ 4094)。

■設定モード:特権EXECモード

13. show ipv6 neighbors

■説明:IPv6ネイバーテーブルを表示します。

■構文:show ipv6 neighbors

■設定モード:特権EXECモード

14. show ipv6 route

■説明:IPv6 ルーティングテーブルを表示します。

■構文:show ipv6 route

■設定モード:特権EXECモード

15. show ipv6 route summary

■説明:IPv6 ルートの概要を表示します。

■構文:show ipv6 route summary

■設定モード:特権EXECモード

3.2.17 VLAN

1. gvrp advertisement

■説明:指定したVLANの情報を別のスイッチと交換させる機能(GVRP)を有効/無効に設定します。

■構文:gvrp advertisement {enable | disable}

■設定モード:Config-VLANモード

2. ports

■説明:
必要なメンバー ポート、タグなしポート、禁止ポート、あるいはその両方を含む VLAN エントリを静的に設定し、VLAN をアクティブにします。VLAN は、vlan active コマンドを使用してアクティブにすることもできます。

■構文:
- ports <interface-type> <interface-id> [<interface-type> <interface-id>…] [untagged <interface-type> <interface-id>[…] (all) [[forbidden <interface-type> <interface-id> [<interface-type> <interface-id> …]]]
- ports add [forbidden] <interface-type> <interface-id> [untagged <interface-type> <interface-id> (all)]
- no ports <interface-type> <interface-id> [<interface-type> <interface-id>…] [untagged <interface-type> <interface-id>[…] (all) [[forbidden <interface-type> <interface-id> [<interface-type> <interface-id> …]]]
- no ports add [forbidden] <interface-type> <interface-id> [untagged <interface-type> <interface-id> (all)]

■パラメータの説明:
- add - VLANにポートを追加します。
- <interface-type> <interface-id> - VLAN のメンバーとして設定するポートを設定します。
- port-channel<channel-number> - ポート チャネル インタフェースのリストまたは特定のポート チャネル識別子を設定します。インタフェースのリストを設定する際には、スペースを使用せずにカンマを区切り文字として使用します(例: 1、3)。
- all- VLAN に設定されているすべてのメンバー ポートを削除し、メンバー ポートを “none” に設定します。
- このオプションは、コマンドの no 形式でのみ使用できます。
- untagged<interface-type> <interface-id> - VLAN が出力パケットをタグなしパケットとして送信するために使用するポートを設定します。

■設定モード:Config-VLANモード

3. ports name

■説明:このコマンドは VLAN 名を設定します。

■構文:ports name [<vlan-name>]

■設定モード:Config-VLANモード

4. switchport pvid

■説明:
指定されたポートに PVID を設定します。PVID は、ポートで受信されたタグなしフレーム、優先タグ付きフレーム、または C-VLAN フレームに割り当てられる VLAN ID を表します。

PVID は、タグなしフレームを受信したときに割り当てられるVLAN IDです(値の有効範囲:1 ～ 4094)。

■構文:
・ switchport pvid <vlan-id/vfi_id>
・ no switchport pvid

■パラメータの説明:
・ pvid<vlan-id(1-4094)> - 指定された VLAN ID の PVID を設定します。
・ これは、VLANを表す一意の値です(値の有効範囲:1 ～ 4094)。

■設定モード:インタフェースコンフィグレーションモード
物理インタフェースまたはポートチャネルにて適用されます。

5. switchport acceptable-frame-type

■説明:
ポートが受信できるフレームのタイプを指定します。

コマンドの no 形式を使用すると、ポートが受信可能なフレームのタイプをデフォルトにリセットします。

この設定は、GVRPやSTPのBPDUなど、VLANに依らないフレームの転送には影響しません。

■構文:
・ switchport acceptable-frame-type {all | tagged | untaggedAndPrioritytagged }

■パラメータの説明:
・ all- すべてのフレームを受信します。
・ tagged- タグのついているフレームのみを受信可能とします。
・ untaggedAndPrioritytagged -タグなしフレームおよびPriorityタグのみを受信します。

■設定モード:インタフェースコンフィグレーションモード
物理インタフェースまたはポートチャネルにて設定できます。

6. switchport ingress-filter

■説明:
ポートの入力フィルタリング機能を有効にします。

コマンドの no 形式は、ポートの入力フィルタリング機能を無効にします。

■構文:
・ switchport ingress-filter
・ no switchport ingress-filter

■設定モード:インタフェースコンフィグレーションモード/物理インタフェース、またはポートチャネル
※物理インタフェース、またはポートチャネルにて設定できます。

7. show forward-all

■説明:
VLAN forward all テーブル内のすべてのエントリを表示します。
これらのエントリには、スイッチ内のすべてのアクティブな VLAN の詳細が含まれます。

■構文:show forward-all [switch <context_name>]

■設定モード:特権EXECモード

8. show vlan

■説明:VLANデータベースを表示します。

■構文:show vlan [brief | id <vlan-range> | summary] [switch<context_name>]

■パラメータの説明:
・ brief - VLANデータベースを表示します。
・ id <vlan-range> -情報を表示したいVLAN IDのVLANデータベースエントリを表示します。この値は、最大サイズが 9 の文字列です。たとえば、4000 ～ 4010 の VLAN ID の情報を表示するには、値は、「4000-4010」の形式で指定します。
・ summary - スイッチ内に存在する VLAN の総数のみを表示します。
・ switch <context_name> - 指定されたコンテキストの VLAN エントリ関連情報または既存の VLAN の総数を表示します。この値は、本機のコンテキストの一意の名前を表します。この値は、最大サイズが 32の文字列です。このパラメータは、マルチインスタンス機能に固有です。

■設定モード:特権EXECモード

9. show vlan device capabilities

■説明:
スイッチ/すべてのコンテキストでサポートされているVLAN機能の一覧を表示します。

■構文:show vlan device capabilities

■設定モード:特権EXECモード

10. show vlan device info

■説明:
スイッチ/すべてのコンテキストで作成されたすべての VLAN に適用される VLAN グローバル情報を表示します。

■構文:show vlan device info

■設定モード:特権EXECモード

11. show vlan port config

■説明:ポートに設定されているVLAN関連情報を表示します。

■構文:
・ show vlan port config [{port < interface-type > <interface-id> | switch<string(32)>}]

■パラメータの説明:
・ <interface-type> - 指定したインタフェースの VLAN 関連のポート固有の情報を表示します。
インタフェースは次のとおりです。
  - gigabitethernet -1 秒あたり最大 1 ギガビットのデータ転送をサポートする LAN 標準アーキテクチャのバージョン。
・ switch <context_name> - 指定されたコンテキストのすべての VLAN に適用される VLAN グローバル情報を表示します。この値は、本機のコンテキストの一意の名前を表します。この値は、最大サイズが 32の文字列です。このパラメータは、マルチインスタンス機能に固有です。

■設定モード:特権EXECモード

12. show vlan static

■説明:指定した値または範囲のVLANのステータス情報を表示します。

■構文:show vlan static [id <vlan-range>]

■パラメータの説明:
・ vlan <vlan-range> - 表示したいVLANの値または範囲を指定します。この値は、最大サイズが 9 の文字列です。たとえば、4000 ～ 4010 の VLAN ID の詳細を表示するには、値は、「4000-4010」の形式で指定します。

■設定モード:特権EXECモード

13. show vlan statistics

■説明:ユニキャストおよびブロードキャストVLANの統計情報を表示します。

■構文:show vlan statistics [vlan <vlan-range>] [switch <string(32)>]

■パラメータの説明:
・ vlan <vlan-range> - 表示したいVLAN IDの値または範囲を指定します。この値は、最大サイズが 9 の文字列です。たとえば、4000 ～ 4010 の VLAN ID の詳細を表示するには、値は、「4000-4010」の形式で指定します。
・ switch <context_name> - 指定されたコンテキストのすべての VLAN に適用される VLAN グローバル情報を表示します。この値は、本機のコンテキストの一意の名前を表します。この値は、最大サイズが 32の文字列です。このパラメータは、マルチインスタンス機能に固有です。

■設定モード:特権EXECモード

14. vlan

■説明:
VLAN ID を設定、VLAN 固有の設定が行われる config-VLAN モードに入ります。VLAN がすでに作成されている場合、指定された VLAN ID の Config-VLAN モードに直接入ります。

■構文:
・ vlan <vlan-id>
・ no vlan <vlan-id>

■パラメータの説明:
・ <vlan –id> -VLANを表す一意の値です(値の有効範囲:1 ～ 4094)。

■設定モード:グローバルコンフィグレーションモード

15. vlan restricted

■説明:ポート上の制限された VLAN 登録を有効/無効にします。

■構文:vlan restricted {enable | disable}

■パラメータの説明:
・ enable - 制限付き VLAN 登録を有効にします。
・ disable - 制限付きVLAN登録を無効にします。

■設定モード:インタフェースコンフィグレーションモード

16. voice vlan state

■説明:スイッチの音声 VLAN を有効/無効にします。

■構文:

・ voice vlan state [{oui-enabled | disabled | auto}]

■パラメータの説明:

・ oui-enable－OUI で音声 VLAN を有効にします。
・ disabled－音声 VLAN を無効にします。
・ auto－LLDP-MED で音声 VLAN を有効にします。

■設定モード:グローバルコンフィグレーションモード

3.2.18 Voice-VLAN

1. show voice vlan

■説明:音声 VLAN の状態を表示します。

■構文:show voice vlan [oui-table]

■パラメータの説明:
・ [oui-table] –OUIテーブルを指定します。

■設定モード:特権EXECモード

2. voice vlan aging-time

■説明:音声 VLAN エージングのタイムアウト間隔を分単位で指定します。

■構文:voice vlan aging-time <integer(30-65535)>

■パラメータの説明:
・ <integer(30-65535)> –タイムアウト (分単位)を表します。

■設定モード:グローバルコンフィグレーションモード

3. voice vlan cos

■説明:OUI 音声 VLAN サービス クラス (CoS) を設定します。

■構文:voice vlan cos <integer(0-7)> [remark]

■パラメータの説明:
・ <integer(0-7)> – cosのレベルを選択します。
・ [remark] – L2 ユーザ優先度がCoS値で再マークされることを指定します。

■設定モード:グローバルコンフィグレーションモード

4. voice vlan cos mode

■説明:インタフェース上の OUIの 音声 VLAN CoS モードを指定します。

■構文:voice vlan cos mode {src | all }

■パラメータの説明:
・ src –QoS 属性は、送信元 MACアドレスに OUIを含むパケットに適用されます。
・ all - QoS 属性は、音声 VLAN に分類されたパケットに適用されます。

■設定モード:インタフェースコンフィグレーションモード

5. voice vlan dscp

■説明:LLDP-MEDのDSCP を指定します。

■構文:voice vlan dscp <integer(0-63)>

■パラメータの説明:
・ <integer(0-63)> – dscpを表します。

■設定モード:グローバルコンフィグレーションモード

6. voice vlan enable

■説明:インタフェース上で OUI 音声 VLAN の有効化/無効化を指定します。

■構文:
・ voice vlan enable
・ no voice vlan enable
・

■設定モード:インタフェースコンフィグレーションモード

7. voice vlan id

■説明:音声VLAN識別子を静的に設定します。

■構文:voice vlan id <integer(1-4094)>

■パラメータの説明:
・ <integer(1-4094)> – VLAN IDを表します。

■設定モード:グローバルコンフィグレーションモード

8. voice vlan oui-table

■説明:音声 VLAN OUI テーブルを指定します。

■構文:
・ voice vlan oui-table {add <aa:aa:aa> [text] | remove <aa:aa:aa> }

■パラメータの説明:
・ add <aa:aa:aa> – 音声機器の MACアドレス プレフィックスを OUI テーブルに追加してください。
・ [text] - 音声機器のプレフィックスの説明。
・ remove <aa:aa:aa> - OUI テーブルから音声機器の MACアドレス プレフィックスを削除します。

■設定モード:グローバルコンフィグレーションモード

9. voice vlan vpt

■説明:LLDP-MED VLAN 優先タグを指定します。

■構文:voice vlan vpt <integer(0-7)>

■パラメータの説明:
・ <integer(0-7)> – vptを表します。

■設定モード:グローバルコンフィグレーションモード

3.2.19 GVRP

1. set gvrp

■説明:スイッチの GVRP を有効/無効にします。

■構文:set gvrp {enable | disable}

■パラメータの説明:
・ enable - GVRP を有効にします。
・ disable - GVRP を無効にします。

■設定モード:グローバルコンフィグレーションモード

2. set port gvrp

■説明:ポート上の GVRP を有効/無効にします。

■構文:set port gvrp <interface-type> <interface-id> { enable | disable }

■パラメータの説明:
・ <interface-type> - 指定されたタイプのインタフェースを設定します。
インタフェースは次のとおりです。
  - gigabitethernet - 1 秒あたり最大 1 ギガビットのデータ転送をサポートする LAN 標準アーキテクチャのバージョン。
  - port-channel – 複数のポートが集約されたアグリゲータを表す論理インタフェース。
・ <interface-id> – 指定されたインタフェース識別子のIPインタフェースを表示します。これは、特定のインタフェースを表す一意の値です。この値は、スロット番号とポート番号をスラッシュで区切って組み合わせたものです。
例) 0/1:スロット番号が「0」、ポート番号が「1」であることを表します。
・ enable - インタフェース上で GVRP を有効にします。
・ disable - インタフェース上でGVRPを無効にします。

■設定モード:グローバルコンフィグレーションモード

3. set garp timer

■説明:ポートに GARP タイマーを設定します。

■構文:set garp timer {join | leave | leaveall} <integer>

■パラメータの説明:
・ join - GARP PDU を送信する機会間の間隔 (ミリ秒単位)。
・ leave - GARP状態から離脱するまでにLeave状態で待機する時間待機する時間 (ミリ秒単位)。
・ leave all - すべてのデバイスがGARP状態から離脱するまでに待機する時間(ミリ秒単位)。
・ <integer> - 時間を表す値 (ミリ秒単位)。
【注記】:Joinタイマー、Leaveタイマー、Leaveallタイマーの値は、下記のとおりです。
10の倍数、かつLeaveall-time > Leave-time > 2*Join-time

■設定モード:インタフェースコンフィグレーションモード

4. show garp timer

■説明:インタフェース上の GARP タイマー情報を表示します。

■構文:
・ show garp timer [{ port <interface-type> <interface-id> | switch<context_name>}]

■パラメータの説明:

・ <interface-type> - 指定されたタイプのインタフェースを設定します。
インタフェースは次のとおりです。
  - gigabitethernet - 1 秒あたり最大 1 ギガビットのデータ転送をサポートする LAN 標準アーキテクチャのバージョン。
  - port-channel – 複数のポートが集約されたアグリゲータを表す論理インタフェース。
・ <interface-id> – 指定されたインタフェース識別子のIPインタフェースを表示します。これは、特定のインタフェースを表す一意の値です。この値は、スロット番号とポート番号をスラッシュで区切って組み合わせたものです(例: 0/1 は、スロット番号が「0」、ポート番号が「1」であることを表します)。
・ switch<context_name> - コンテキスト名を表します。

■設定モード:特権EXECモード

5. show gvrp statistics

■説明:インタフェースの GVRP 統計情報を表示します。

■構文:show gvrp statistics port <interface-type> <interface-id>

■パラメータの説明:
・ <interface-type> - 指定されたタイプのインタフェースを設定します。
インタフェースは次のとおりです。
  - gigabitethernet - 1 秒あたり最大 1 ギガビットのデータ転送をサポートする LAN 標準アーキテクチャのバージョン。
  - port-channel - 複数のポートが集約されたアグリゲータを表す論理インタフェース。
・ <interface-id> – 指定されたインタフェース識別子のIPインタフェースを表示します。これは、特定のインタフェースを表す一意の値です。この値は、スロット番号とポート番号をスラッシュで区切って組み合わせたものです(例: 0/1 は、スロット番号が「0」、ポート番号が「1」であることを表します)。

■設定モード:特権EXECモード

3.2.20 PNAC(ポートベースネットワークアクセス制御)

1. dot1x clear statistics

■説明:本機すべてのポートの dot1x カウンタをクリアします。

■構文:dot1x clear statistics {interface<interface-id><interface-type> | all}

■パラメータの説明:

・ <interface-type> - 指定されたタイプのインタフェースを設定します。
インタフェースは次のとおりです。
  - gigabitethernet – 1 秒あたり最大 1 ギガビットのデータ転送がサポート可能な LAN 標準アーキテクチャのバージョン。
  - port-channel – 複数のポートが集約されたアグリゲータを表す論理インタフェース。
・ <interface-id> - 指定されたインタフェース識別子のIPインタフェースを表示します。これは、特定のインタフェースを表す一意の値です。この値は、スロット番号とポート番号をスラッシュで区切って組み合わせたものです。
・ 例) 0/1:スロット番号が「0」、ポート番号が「1」であることを表します。

■設定モード:グローバルコンフィグレーションモード

2. dot1x default

■説明:
このポートのデフォルト値としてdot1xを設定します。このポートの以前の設定情報はデフォルト値にリセットされます。
これらの詳細は表示されませんが、ポートの基本設定が表示されます。

■構文:dot1x default

■設定モード:インタフェースコンフィグレーションモード

3. dot1x guest-vlan

■説明:dot1x ゲスト VLAN ID を設定します。

■構文:
・ dot1x guest-vlan <short (1-4094)>
・ no dot1x guest-vlan

■パラメータの説明:
・ <vlan –id>-これは、VLANを表す一意の値です(値の有効範囲:1 ～ 4094)。

■設定モード:グローバルコンフィグレーションモード

4. dot1x max-req

■説明:
認証プロセスを再開する前に、オーセンティケータによるクライアントに対する EAP (Extensible Authentication Protocol) の最大再試行回数を設定します（カウント値の有効範囲:1 ～ 10）。

■構文:
・ dot1x max-req <count(1-10)>
・ no dot1x max-req

■設定モード:インタフェースコンフィグレーションモード

5. dot1x max-start

■説明:
オーセンティケータに対する EAPOLの再試行の最大数を設定します。値の有効範囲は 1 ～ 65535 です。

■構文:
・ dot1x max-start <count(1-65535)>
・ no dot1x max-start

■設定モード:インタフェースコンフィグレーションモード

6. dot1x radius-vlan-assignment

■説明:ポートの RADIUS VLANの割り当て機能を有効にします。

■構文:
・ dot1x radius-vlan-assignment enable
・ no dot1x radius-vlan-assignment

■設定モード:インタフェースコンフィグレーションモード

7. dot1x reauthentication

■説明:
オーセンティケータからクライアントへの定期的な再認証を有効にします。同じサプリカントが保護されたリソースにアクセスしているかどうかを確認するために、定期的に再認証を要求します。
定期的な再認証試行の間隔は手動で設定できます。

■構文:
・ dot1x reauthentication
・ no dot1x reauthentication

■設定モード:インタフェースコンフィグレーションモード

8. dot1x re-authenticate

■説明:
すべての dot1x 対応ポートまたは指定のdot1x 対応ポートの再認証を開始します。
これにより、ステートマシンが初期化され、新たな認証のための環境がセットアップされます。

定期的な再認証が有効になっていない場合、再認証は手動で設定されます。再認証は、設定された待機時間(再認証期間)を待たずに、認証 サーバによってサプリカントに ID を提供するように要求されます。インタフェースが指定されていない場合は、すべての dot1x ポートで再認証が開始されます。

■構文:dot1x re-authenticate [interface <interface-type><interface-id>]

■パラメータの説明:
・ <interface type> - 指定されたタイプのインタフェースを設定します。
・ <interface id> - 指定されたインタフェース識別子を設定します。これは、特定のインタフェースを表す一意の値です。この値は、スロット番号とポート番号をスラッシュで区切って組み合わせたものです。
・ 例) 0/1:スロット番号が「0」、ポート番号が「1」であることを表します。

■設定モード:特権EXECモード

9. dot1x system-auth-control

■説明:dot1x は認証方式であり、dot1x を有効にします。

■構文:
・ dot1x system-auth-control
・ no dot1x system-auth-control

■設定モード:グローバルコンフィグレーションモード

10. dot1x timeout

■説明:
dot1x タイマーを設定します。タイマー モジュールは、タイマーの管理、タイマー用のメモリプールの作成、タイマー リストの作成、タイマーの開始と停止を行います。タイマーが期限切れになった場合、その処理を行います。

■構文:
- dot1x timeout {quiet-period <short(0-65535)> | {reauth-period | server-timeout | supp-timeout | tx-period | start-period | held- period | auth-period} <short(1-65535)>}
- no dot1x timeout {quiet-period | reauth-period | server-timeout | supp-timeout | tx-period | start-period | held-period | auth-period}

■パラメータの説明:
- quiet-period <value (0-65535)> - dot1x認証が失敗した後、該当のインタフェースで非認証状態を保持する時間を設定します。
- reauth-period- dot1x認証が成功した後、サプリカントが再認証を行うまでの時間を設定します。
- server-timeout- サーバタイムアウトの秒数を設定します。スイッチは認証 サーバへのパケットの再送信を待ちます。supp-timeout- サプリカントへ送信するEAP要求に対して、スイッチがサプリカントからの応答を待つ時間を指定します。
- start-period- サプリカントがオーセンティケータへの連続したEAPOL-Startフレームの送信間隔を設定します。
- hold-period - サプリカントが試行に失敗した場合、再度クレデンシャルを送信するまでに待機する時間を設定します。
- auth-period <value(1-65535)> - オーセンティケータがタイムアウトになるまでサプリカントが待機する秒数を設定します。

■設定モード:インタフェースコンフィグレーションモード

11. dot1x port-control

■説明:
オーセンティケータ ポート制御パラメータを設定します。dot1x はポートベースの認証を実行して、ネットワークのセキュリティを強化します。ポートに採用されているさまざまなモードにより、各アクセス レベルが提供されます。802.1x プロトコルは、レイヤー 2のスタティック アクセス ポートとレイヤー 3のルーテッド ポートの両方でサポートされています。

■構文:
・ dot1x port-control {auto | force-authorized | force-unauthorized}
・ no dot1x port-control

■パラメータの説明:
・ auto- このポートで 802.1x 認証プロセスを設定します。ポートが無許可状態になり、EAPOL フレームのみがポート経由で送受信可能になります。認証プロセスは、ポートのリンク状態がダウンからアップに移行したとき、または EAPOL 開始フレームを受信したときに開始されます。スイッチはクライアントの ID を要求し、クライアントと認証 サーバの間で認証メッセージの中継を開始します。スイッチは、ネットワークにアクセスしようとしている各クライアントをクライアントの MACアドレスによって一意に識別できます。
・ force-authorized- このポートを通過するすべてのトラフィックを許可するようにポートを設定します。802.1X 認証を無効にし、認証交換を必要とせずにポートを許可された状態に移行させます。このポートは、クライアントの 802.1X ベースの認証を行わずに、通常のトラフィックを送受信します。
・ force-unauthorized- このポートを通過するすべてのトラフィックをブロックするようにポートを設定します。ポートを未承認状態のままにし、クライアントによる認証の試みをすべて無視します。スイッチは、インタフェースを介してクライアントに認証サービスを提供できません。

■設定モード:インタフェースコンフィグレーションモード

12. dot1x mab

■説明:
MAC認証バイパス(MAB)は、802.1X のサプリカント機能を持たない機器(プリンタやIP Phone)のネットワークアクセスを可能にする認証機能のことです。プリンターなどが接続するポートではMABを有効にします。

■構文:dot1x mab {mab_mode | hybrid_mode | disable}

■パラメータの説明:
・ mab_mode - MAC 認証バイパスのみを使用。
・ hybrid_mode - ユーザ名/パスワードおよび MAC認証バイパスを使用。
・ disable - ユーザ名/パスワードによる認証を行う。

■設定モード:インタフェースコンフィグレーションモード

13. dot1x guest-vlan enable

■説明:ゲスト VLAN 機能を有効/無効にします。

■構文:
・ dot1x guest-vlan enable
・ no dot1x guest-vlan enable

■設定モード:インタフェースコンフィグレーションモード

14. port-isolation

■説明:指定したポートにポートアイソレーション機能を設定します。

■構文:port-isolation {enable | disable}

■パラメータの説明:

・ enabled - このingressインタフェースでポートの分離ルールを有効にします。
・ disabled - このingressインタフェースのポートの分離ルールを無効にします。

■設定モード:インタフェースコンフィグレーションモード

15. radius-server host

■説明:
パラメータ (ホスト、タイムアウト、キー、再送信) を使用して RADIUS クライアントを設定します。

■構文:
・ radius-server host <ipv4-address> [acct-port <integer(1-65535)>] [auth-port <integer(1-65535)>] [key <secret-key-string>] [retransmit <1-254>] [timeout <1-120>] [primary]
・ no radius-server host {ipv4-address | host-name} [primary]

■パラメータの説明:
・ ipv4-address - RADIUS サーバ ホストの IPv4 アドレスを設定します。
・ acct-port <integer(1-65535)> - この RADIUS 上の特定の UDP 宛先ポートをアカウンティング要求のみに使用するように設定します。認証ポートの値の有効範囲は 1 ～ 65535 です。
・ auth-port <integer(1-65535)> - この RADIUS サーバ上の特定の UDP (ユーザ データグラム プロトコル) 宛先ポートを認証要求のみに使用するように設定します。認証ポートの値の有効範囲は 1 ～ 65535 です。
・ key <secret-key-string> - オーセンティケータと RADIUS サーバ間のすべての RADIUS 通信の認証キーと暗号化キーを指定する サーバごとの暗号化キーを設定します。秘密鍵文字列の最大長の値は 46 です。
・ retransmit <1-254> - クライアントが サーバへの接続を試行する最大回数を設定します。再送信試行回数の値の有効範囲は 1 ～ 254 です。
・ timeout <1-120> - クライアントがリクエストを再送信する前に サーバからの応答を待つ時間を秒単位で設定します。タイムアウトの値の有効範囲は 1 ～ 120 秒です。
・ primary - RADIUS サーバをプライマリ サーバとして設定します。プライマリ サーバとして設定できる サーバは 1 つだけです。このオプションを指定してコマンドを実行すると、既存のプライマリ サーバが置き換えられます。

■設定モード:グローバルコンフィグレーションモード

16. rmon alarm

■説明:
監視対象MIBオブジェクトにRMONアラームを設定します。
アラームグループは、プローブ内の変数からサンプルを定期的に取得し、設定された閾値と比較します。

■構文:
・ rmon alarm <alarm-number(1-65535)> <stats-number(1-65535)>{etherStatsDropEvents | etherStatsOctets | etherStatsPkts | etherStatsBroadcastPkts | etherStatsMulticastPkts | etherStatsCRCAlignErrors | etherStatsUndersizePkts | etherStatsOversizePkts | etherStatsFragments | etherStatsJabbers | etherStatsCollisions | etherStatsPkts64Octets | etherStatsPkts65to127Octets | etherStatsPkts128to255Octets | etherStatsPkts256to511Octets | etherStatsPkts512to1023Octets | etherStatsPkts1024to1518Octets } <sample-interval-number(1-2147483647)> <rising-event-number(1-65535)>{ absolute | delta } rising-threshold <rising-threshold-number(0-2147483647)> [<integer (1- 65535)>] falling-threshold <falling-threshold-number(0-2147483647)> [<integer(1-65535)>] [owner <string (32)>]

・ no rmon alarm <number (1-65535)>

■パラメータの説明:
・ <alarm-number>/<number (1-65535)> - RMONアラームのインデックス番号を設定します。(値の有効範囲:1 ～ 65535)。
・ <stats-number(1-65535)> - 統計情報リストのインデックス番号を入力します。
・ <sample-interval-time (1-2147483647)> - サンプリング間隔を設定します。
・ absolute - サンプリング間隔の終了時に、選択した変数の値をしきい値と比較します。
・ delta - 最新のサンプル値と前回取得時の値の差を閾値と比較します。
・ rising-threshold <value (0-2147483647)> - 上限しきい値を設定します。起動アラームが Rising アラームまたは RisingOrFalling アラームとして設定されており、設定されたしきい値に達すると、アラームが発生します。現在のサンプリング値が設定された上限しきい値以上で、最後のサンプリング間隔の値がこの設定されたしきい値より小さい場合、単一のイベントが生成されます(値の有効範囲:0 ～ 2147483647)。
・ <rising-event-number (1-65535)> - 上限しきい値に到達すると、イベントのインデックスを上げます。このインデックスの特定の値によって識別されるイベント エントリは、イベント インデックス オブジェクトの同じ値によって識別されるものと同じです(値の有効範囲:1 ～ 65535)。
・ <falling-value-number(1-65535)> - 下限しきい値を設定します。起動アラームが Falling アラームまたは RisingOrFalling アラームとして設定されており、設定されたしきい値に達すると、アラームが発生します。現在のサンプリング値が設定された下限しきい値以下で、最後のサンプリング間隔の値がこのしきい値より大きい場合、単一のイベントが生成されます(値の有効範囲:0 ～ 2147483647)。
・ <falling-event-number (1-65535)> - 下限しきい値に達したときにイベントのインデックスを上げます。このインデックスの特定の値によって識別されるイベント エントリは、イベント インデックス オブジェクトの同じ値によって識別されるものと同じです (値の有効範囲:1 ～ 65535)。
・ owner<ownername (32)> - このエントリを設定するエンティティを設定します。

■設定モード:グローバルコンフィグレーションモード

17. rmon collection history

■説明:
指定された時間間隔におけるバケット内のインタフェース/VLAN 統計の履歴収集を有効にします。
コマンドの no 形式は、インタフェース/VLAN での履歴収集を無効にします。

■構文:
・ rmon collection history <index (1-65535)> [buckets <bucket- number (1-65535)>] [interval <seconds (1-3600)>] [owner<ownername (32)>]

・ no rmon collection history <index (1-65535)>

■パラメータの説明:
・ <index (1-65535)> - 履歴制御テーブル内のエントリを識別します。このような各エントリは、機器上のインタフェースに対して特定の間隔でのサンプルのセットを定義します(値の有効範囲:1 ～ 65535)。
・ buckets<bucket-number (1-65535)> - RMON 統計収集履歴グループに必要なバケットの数を設定します。
・ これは、この履歴制御エントリに関連付けられたメディア固有のテーブルの一部にデータが保存される離散時間間隔の要求された数です。ポーリング サイクルは、インタフェース統計の詳細が保存されるバケット間隔です(値の有効範囲:1 ～ 65535)。
・ Interval<second(1-3600)> - 各バケットのデータがサンプリングされる時間間隔を設定します(値の有効範囲:1 ～ 3600)。
・ owner<ownername (32)> - 統計の RMON グループの所有者の名前を設定します。

■設定モード:インタフェースコンフィグレーションモード / Config VLANモード

18. rmon collection stats

■説明:
インタフェース/VLAN での RMON 統計収集を有効にします。

コマンドの no 形式を使用すると、インタフェース/VLAN での RMON 統計情報の収集が無効になります。

■構文:
・ rmon collection stats <index (1-65535)> [owner <ownername(127)>]
・ no rmon collection stats <index (1-65535)>

■パラメータの説明:
・ <index (1-65535)> - 統計テーブルのエントリを識別します。(値の有効範囲:1 ～ 65535)。
・ owner <ownername (127)> - 統計の RMON グループの所有者の名前を設定します。

■設定モード:インタフェースコンフィグレーションモード / Config VLANモード

19. rmon event

■説明:
RMONイベントテーブルにエントリを設定ます。イベントが追加されると、RMONイベント番号に関連付けられます。

■構文:
・ rmon event <number (1-65535)> [description <event-description (127)>] [log] [owner <ownername (127)>] [trap <community (127)>]
・ no rmon event <number (1-65535)>

■パラメータの説明:
・ <number (1-65535)> - イベント テーブルに追加するイベントの数を設定します(値の有効範囲:1 ～ 65535)。
・ description<event-description (127)> - イベントの説明を提供します。この値は、最大長が 127 の文字列です。
・ log - イベントごとにログ テーブルにエントリを設定ます。
・ owner<ownername (127)> - このエントリが設定されているエンティティを表示します。この値は、最大値が 127 の文字列です。
・ trap<community (127)> - トラップを生成します。指定されたトラップには SNMP コミュニティ文字列が渡されます。この値は、最大値が 127 の文字列です。

■設定モード:グローバルコンフィグレーションモード

20. security-suite

■説明:DoSプロテクションを有効/無効にします。

■構文:
・ security-suite
・ no security-suite

■設定モード:グローバルコンフィグレーションモード

21. security-suite enable

■説明:インタフェース上でDoSプロテクションを有効/無効にします。

■構文:
・ security-suite enable
・ no security-suite enable

■設定モード:インタフェースコンフィグレーションモード

22. set rmon

■説明:RMON 機能を有効/無効にします。

■構文:set rmon {enable | disable}

■パラメータの説明:
・ enable - システムの RMON 機能を有効にします。
・ 有効にすると、RMON はローカルとリモートの両方のネットワークのモニタリングを開始し、ネットワーク障害診断を提供します。
・ disable - システムの RMON 機能を無効にします。
・ 無効にすると、RMON のネットワークモニタリングが中止されます。

■設定モード:グローバルコンフィグレーションモード

23. show dot1x

■説明:
dot1x 情報を表示します。設定された情報は、この show コマンドを実行することで表示できます。設定を変更したい場合、ポートが指定どおりに設定されてるかを確認する際に、show コマンドが使用されます。

■構文:
・ show dot1x [{ interface <interface-type> <interface-id> | statistics interface <interface-type> <interface-id> | supplicant-statistics interface <interface-type> <interface-id>|local-database | mac- info [address <aa:aa:aa:aa:aa:aa>] | mac-statistics [address<aa:aa:aa:aa:aa:aa>] | all }]

■パラメータの説明:
・ interface <interface-type> <interface-id> - スイッチまたは指定されたインタフェースの dot1x パラメータを表示します。
・ statistics interface <interface-type> <interface-id> - スイッチまたは指定されたインタフェースの dot1x オーセンティケータ ポート統計パラメータを表示します。
・ supplicant-statisticsinterface<interface-type> <interface-id> - スイッチまたは指定されたインタフェースの dot1x サプリカント統計パラメータを表示します。
・ local-database- ユーザ名とパスワードを含む dot1x 認証 サーバ データベースを表示します。
・ mac-info [address <aa:aa:aa:aa:aa:aa>] - すべての MACセッションまたは指定された MACアドレスの dot1x情報を表示します。
・ mac-statistics [address <aa:aa:aa:aa:aa:aa>] - すべての MACセッションまたは指定された MACアドレスの dot1x MAC 統計情報を表示します。
・ all - すべてのインタフェースの dot1x ステータスを表示します。

■設定モード:特権EXECモード

24. show dot1x authenticated host

■説明:dot1x 認証されたホストのステータスを表示します。

■構文:show dot1x authenticated host

■設定モード:特権EXECモード

25. show dot1x dynamic-vlan

■説明:dot1xのダイナミックVLANの割り当て情報を表示します

■構文:show dot1x dynamic-vlan

■設定モード:特権EXECモード

26. show dot1x guest-vlan

■説明:dot1x ゲスト VLAN 情報を表示します。

■構文:show dot1x guest-vlan

■設定モード:特権EXECモード

27. show port-isolation status

■説明:ポートアイソレーションテーブルを表示します。

■構文:show port-isolation status

■設定モード:特権EXECモード

28. show radius server

■説明:RADIUSサーバステータスやIPアドレスなど、RADIUSサーバのホスト情報を表示します。

■構文:show radius server <ucast_addr>

■パラメータの説明:
・ <ucast_addr>- RADIUSサーバのIPv4ユニキャストアドレスを設定します。

■設定モード:特権EXECモード

29. show radius statistics

■説明:
サーバとクライアント間のデータ転送に関する RADIUS サーバの開始時からの統計情報を表示します。

■構文:show radius statistics

■設定モード:特権EXECモード

30. show rmon

■説明:
インタフェースに設定されている RMON 統計、アラーム、イベント、および履歴を表示します。

■構文:
・ show rmon [statistics [<stats-index (1-65535)>]] [alarms] [events] [history [history-index (1-65535)] [overview]]

■パラメータの説明:
・ statistics - 特定のイーサネット インタフェースの統計情報を表示します。この機器上の各モニタリング対象インタフェースのプローブは統計情報を測定します。
・ alarms - 最後のサンプリング期間中の統計の値を表示します。この値は、現在のサンプリング期間が完了するまで利用可能です。
・ events - 関連する条件が機器内で発生するたびにイベントを生成します。条件はアラームである場合があります。サンプリングされた統計変数の値が定義されたしきい値を超えると、アラームが生成されます。アラームモジュールはイベントモジュールを呼び出します。
・ history - 設定された RMON の履歴を表示します。
・ overview - rmon 履歴エントリの概要のみを表示します。

■設定モード:特権EXECモード

31. show security-suite

■説明:DoS情報を表示します。

■構文:show security-suite

■設定モード:特権EXECモード

32. shutdown dot1x

■説明:
dot1x機能を無効にします。dot1x機能を無効にすると、サプリカント・オーセンティケータ・認証サーバの情報が削除されます。

■構文:
・ shutdown dot1x
・ no shutdown dot1x

■設定モード:グローバルコンフィグレーションモード

3.2.21 Log

1. clear logs

■説明:syslog バッファをクリアします。

■構文:clear logs

■設定モード:グローバルコンフィグレーションモード

2. logging

■説明:
syslog サーバを有効にし、syslog 関連のパラメータを設定します。
ロギングのプロセスは、Syslogサーバに送信するログのファシリティやシビリティをコントロールします。

■構文:
・ logging { [facility {local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7}] | [severity { alerts | critical | debugging | emergencies | errors | informational | notification| warnings }]}logging {buffered [<short (1-200)>]}

■パラメータの説明:
・ facility - メッセージに示されるファシリティ。
・ 次の値のいずれかを指定できます: local0、local1、local2、local3、local4、local5、local6、local7
・ severity - メッセージの重大度レベル。指定された値以上の重大度レベルを持つメッセージは非同期的に出力されます。オプションは次のとおりです。
  - 0. Emergency:システムが使用できない状態。
  - 1. Alerts:即時対応が必要な状態。
  - 2. Critical:危険な状態。
  - 3. Errors:一般的なエラー状態。
  - 4. Warnings:警告状態。
  - 5. Notification:正常だが重大な状態。
  - 6.Information:情報通知メッセージ。
  - 7. Debugging:デバッグメッセージ。

・ buffered - 内部バッファから表示される Syslog メッセージを制限します。このサイズの範囲は 1 ～ 200 エントリです。

■設定モード:グローバルコンフィグレーションモード

3. logging-file

■説明:ファイル テーブルに flash_log というエントリを追加してください。

■構文:logging-file <short(0-191)> flash_log

■パラメータの説明:
・ <short(0-191)> - syslog メッセージの優先度を設定します。
  - 128: Emergency
  - 129: Alert
  - 130: Critical
  - 131: Error
  - 132: Warning
  - 133: Notice
  - 134: Information
  - 135: Debug

■設定モード:グローバルコンフィグレーションモード

4. logging-server

■説明:
エントリを記録するログテーブルを設定します。
コマンドの no 形式は、サーバ テーブルからエントリを削除します。

■構文:
・ logging-server {facility {local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7}} {severity {emergencies | alerts | critical | errors | warnings | notification | informational| debugging}} {ipv4<ucast_addr> |ipv6 <ip6_addr> | <string>} [port <integer(0- 65535)>]

・ no logging-server {facility {local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7}} {severity {emergencies | alerts | critical | errors | warnings | notification | informational| debugging}} {ipv4 <ucast_addr> |ipv6 <ip6_addr>| <string>

■パラメータの説明:
・ facility - メッセージに示されるファシリティ。次の値のいずれかを指定できます:
・ local0、local1、local2、local3、local4、local5、local6、local7。
・ severity - メッセージの重大度レベル。指定された値以上の重大度レベルを持つメッセージは非同期的に出力されます。オプションは次のとおりです。
  - 0. Emergency:システムが使用できない状態。
  - 1. Alerts:即時対応が必要な状態。
  - 2. Critical:危険な状態。
  - 3. Errors:一般的なエラー状態。
  - 4. Warnings:警告状態。
  - 5. Notification:正常だが重大な状態。
  - 6.Information:情報通知メッセージ。
  - 7. Debugging:デバッグメッセージ。
・ ipv4 <ucast_addr> - サーバ アドレス タイプをインターネット プロトコル バージョン 4 に設定します。
・ ipv6 <ip6_addr> - サーバ アドレス タイプをインターネット プロトコル バージョン 6 に設定します。
・ <string> - エントリをログに記録する サーバのホスト名を設定します。

・ port<integer(0-65535)> - syslog メッセージの送信に使用するポート番号を設定します(値の有効範囲: 0 ～ 65535)。

■設定モード: グローバルコンフィグレーションモード

5. show logging

■説明: すべてのログ状態と設定情報を表示します。

■構文:show logging

■設定モード: 特権EXECモード

6. show logging-file

■説明:
syslog ファイル テーブルに設定されている 3 つのファイルすべての優先度とファイル名を表示します。

■構文:show logging-file

■設定モード: 特権EXECモード

7. show logging-server

■説明: syslogログ用のサーバ テーブルに関する情報を表示します。

■構文:show logging-server

■設定モード: 特権EXECモード

8. syslog filename-one

■説明:
syslog メッセージをローカルに保存するためのファイルを設定します。
ファイル名の最大サイズは 32 です。

■構文:syslog filename-one <string(32)>

■設定モード: グローバルコンフィグレーションモード

3.2.22 ACL

1. deny- ip/ospf/pim/protocol type

■説明:
deny ステートメントで定義された条件が一致する場合、特定のプロトコル パケットのトラフィックを拒否します。

■構文:
・ deny { ip | ospf | pim | <protocol-type (1-255)> | IPinIP | egp | igp| hmp | rdp | ipv6 | ipv6route | ipv6frag | rsvp | ipv6icmp | l2tp}{ any | host <src-ip-address> | <src-ip-address> <mask> } { any | host <dest-ip-address> | <dest-ip-address> <mask> } ace-priority<integer (1-2147483647)> [dscp <value (0-63)>]

■パラメータの説明:
・ ip| ospf|pim|<protocol-type (1-255)>| IPinIP | egp | igp | hmp| rdp | ipv6 | ipv6route | ipv6frag | rsvp | ipv6icmp | l2tp - パケットのプロトコルのタイプ。プロトコル番号を指定することもできます。
・ any| host <src-ip-address>|<src-ip-address> <mask> - 送信元IPアドレスに関するパラメータは、次のとおりです。
  - any
  - ドット付き 10 進数のアドレス
  - パケットの送信元となるネットワークまたはホストの IP アドレス、および宛先アドレスで使用するネットワーク マスク
・ any|host <dest-ip-address>|<dest-ip-address> <mask> - 宛先IPアドレスに関するパラメータは、次のとおりです。
  - any
  - ドット付き 10 進数のアドレス
  - パケットの宛先となるネットワークまたはホストの IP アドレス、および宛先アドレスで使用するネットワーク マスク
・ ace-priority <integer (1-2147483647)> - フィルタの優先度は、パケットが複数のフィルタリングルールに一致する場合に、どのフィルタリングルールを適用するかを決定します。
・ dscp <short (0-63)> - DSCP値を設定します。

■設定モード:
・ IPv4 のACL拡張アクセスリストコンフィグレーションモード

2. deny icmp

■説明:ICMPパケットと関連パラメータに基づいて、拒否するパケットを指定します

■構文:

・ deny icmp {any |host <src-ip-address>|<src-ip-address> <mask>}{any | host <dest-ip-address> | <dest-ip-address> <mask> } [type <message-type (0-255)>] [code <message-code (0-255)>]ace-priority <integer (1-2147483647)> [dscp <integer (0-63)>]

■パラメータの説明:

・ icmp – ICMP(インターネット制御メッセージ プロトコル)を表します。
・ any| host <src-ip-address>|<src-ip-address> <src-mask> - 送信元IPアドレスに関するパラメータは、次のとおりです。
  - any
  - ドット付き 10 進数のアドレス
  - パケットの送信元となるネットワークまたはホストの IP アドレス、および宛先アドレスで使用するネットワーク マスク
・ any|host <dest-ip-address>|<dest-ip-address> <dest-mask> - 宛先IPアドレスに関するパラメータは、次のとおりです。
  - any
  - ドット付き 10 進数のアドレス
  - パケットの宛先となるネットワークまたはホストの IP アドレス、および宛先アドレスで使用するネットワーク マスク
・ type <short (0-255)> - メッセージのタイプを表します。
・ code <short (0-255)> - メッセージのコードを表します。
・ ace-priority <integer (1-2147483647)> - フィルターの優先度は、パケットが複数のフィルタリングルールに一致する場合に、どのフィルタリングルールを適用するかを決定します。
・ dscp <short (0-63)> - 差別化サービスコードポイントは、サービス品質制御を提供します。

■設定モード:IPv4 ACL拡張アクセスリストコンフィグレーションモード

3. deny icmpv6

■説明:
関連するパラメータに基づいて転送される ICMPv6パケットを指定します。

■構文:
・ deny icmpv6 {any | host <src-ipv6-addr><src-prefix-len (0-128)>} {any | host <dst-ipv6-addr> <dst- prefix-len (0-128)>} ace-priority <integer (1-2147483647)> [type<short (0-255)>] [code <short (0-255)>] [dscp <value (0-63)>]

■パラメータの説明:
・ icmpv6 - インターネット制御メッセージ プロトコル。
・ any | host <ip6_addr> <integer(0-128)> - ホストの送信元アドレス / 任意のホスト
・ any | host <ip6_addr> <integer(0-128)> - ホストの宛先アドレス / 任意のホスト。
・ ace-priority <integer (1-2147483647)> - フィルターの優先度は、パケットが複数のフィルタリングルールに一致する場合に、どのフィルタリングルールを適用するかを決定します。
・ type <short (0-255)> - メッセージタイプ
・ code <short (0-255)> - メッセージコード
・ dscp <short (0-63)> - 差別化サービスコードポイントは、サービス品質制御を提供します。

■設定モード: IPv6 ACL拡張アクセスリストコンフィグレーションモード

4. deny ipv6

■説明:
プロトコルおよび関連パラメータに基づいて転送される IPv6 パケットを指定します。

■構文:
・ deny ipv6 {any | host <ip6_addr> <src-prefix-len (0-128)> }{ any | host <ip6_addr><dst-prefix-len (0-128)> } ace-priority<integer (1-2147483647)> [dscp <short(0-63)>]

■パラメータの説明:
・ ipv6 – IPv6 プロトコル。
・ any | host <ip6_addr> <integer(0-128)> - ホスト/任意のホストの送信元アドレス。
・ any | host <ip6_addr> <integer(0-128)> - ホスト/任意のホストの宛先アドレス。
・ ace-priority <integer (1-2147483647)> - フィルターの優先度は、パケットが複数のフィルタリングルールに一致する場合に、どのフィルタリングルールを適用するかを決定します。
・ dscp <short (0-63)> - 差別化サービスコードポイントは、サービス品質制御を提供します。

■設定モード: IPv6 ACL拡張アクセスリストコンフィグレーションモード

5. deny mac

■説明:
MACアドレスと関連パラメータに基づいて、拒否するパケットを指定します。

■構文:
・ deny { any | host <src-mac-address>{any | host <src-mac-address> <mask>}
・ {any | host <dest-mac-address> <mask>} { any | host <dest-mac- address>{any | host <src-mac-address> <mask>}
・ {any | host <dest-mac-address> <mask>} } {ace-priority <integer (1-2147483647)>} [ethertype<integer (1-65535)>] [vlan <vlan-id (1-4094)>] [vlan- priority <priority (0-7)>]

■パラメータの説明:
・ any | host <src-mac-address > - パケットと照合する送信元 MACアドレス
・ any | host <dest-mac-address > - パケットと照合する宛先 MACアドレス
・ <mask> - パケットの送信元/宛先MACアドレスと照合するMACアドレスの範囲を定義します。照合に使用するビットを1、任意にするビットを0とします。
・ ace-priority <integer (1-2147483647)> - フィルターの優先度は、パケットが複数のフィルタリングルールに一致する場合に、どのフィルタリングルールを適用するかを決定します。
・ ethertype <integer (1-65535)> - フィルタリングする非 IP プロトコル タイプを指定します。
・ vlan <integer (1-4094)> - 受信パケットと照合する VLAN 値。
・ vlan-priority <short (0-7)> - 受信パケットと照合する VLAN 優先度の値。

■設定モード:MAC ACL拡張アクセスリストコンフィグレーションモード

6. deny tcp（IPv6）

■説明:
関連するパラメータに基づいて拒否される IPv6 TCP パケットを指定します。

■構文:
・ deny tcp {any | host <src-ipv6-addr> <src-prefix-len (0-128)} [eq <port-number (1-65535)>] {any | host <dst-ipv6-addr><dst-prefix-len (0-128)>} [eq <port-number (1-65535)>]ace-priority <integer (1-2147483647)> [{ack | non_ack}] [{rst | non_rst}] [{psh | non_psh}] [{urg | non_urg}] [{syn | non_syn}] [{fin | non_fin}] [dscp <value (0-63)>]

■パラメータの説明:
・ tcp - TCPを指定します。
・ any | host <ip6_addr> <integer(0-128)> - ホスト/任意のホストの宛先アドレス。
・ any hosteq <short (1-65535)> - ポート番号。
・ ace-priority <integer (1-2147483647)> - フィルターの優先度は、パケットが複数のフィルタリングルールに一致する場合に、どのフィルタリングルールを適用するかを決定します。
・ ack | non_ack - パケットに対してチェックされる TCP ACK ビット。
・ rst | non_rst - パケットに対してチェックされる TCP RST ビット。
・ psh | non_psh - パケットに対してチェックされる TCP PSH ビット。
・ urg | non_urg - パケットに対してチェックされる TCP URG ビット。
・ syn | non_syn - パケットに対してチェックされる TCP SYN ビット。
・ fin | non_fin- パケットに対してチェックされる TCP FIN ビット。
・ dscp <short (0-63)> - 差別化サービスコードポイントは、サービス品質制御を提供します。

■設定モード:
IPv6 ACL拡張アクセスリストコンフィグレーションモード

7. deny tcp

■説明:関連するパラメータに基づいて拒否するTCP パケットを指定します。

■構文:
・ deny tcp {any | host <src-ip-address> | <src-ip-address> <src- mask> } [eq <port-number (1-65535)>] { any | host <dest-ip-address> | <dest-ip-address> <dest-mask> } [eq <port-number (1-65535)>] ace-priority <integer (1-2147483647)> [{ack | non_ack}] [{rst | non_rst}] [{psh | non_psh}] [{urg | non_urg}] [{syn | non_syn}] [{fin | non_fin}] [dscp <value (0-63)>]

■パラメータの説明:
・ tcp -TCPを指定します。
・ any| host <src-ip-address>|<src-ip-address> <src-mask> - 送信元IPアドレスに関するパラメータは、次のとおりです。
  - any
  - ドット付き 10 進数のアドレス
  - パケットの送信元となるネットワークまたはホストの IP アドレス、および宛先アドレスで使用するネットワーク マスク
・ eq <short (1-65535)> - ポート番号。
・ any|host <dest-ip-address>|<dest-ip-address> <dest-mask> - 宛先IPアドレスに関するパラメータは、次のとおりです。
  - any
  - ドット付き 10 進数のアドレス
  - パケットの宛先となるネットワークまたはホストの IP アドレス、および宛先アドレスで使用するネットワーク マスク
・ ace-priority <integer (1-2147483647)> - フィルターの優先度は、パケットが複数のフィルタリングルールに一致する場合に、どのフィルタリングルールを適用するかを決定します。
・ ack | non_ack - パケットに対してチェックされる TCP ACK ビット。
・ rst | non_rst - パケットに対してチェックされる TCP RST ビット。
・ psh | non_psh - に対してチェックされる TCP PSH ビット
・ urg | non_urg - パケットに対してチェックされる TCP URG ビット。
・ syn | non_syn - パケットに対してチェックされる TCP SYN ビット。
・ fin | non_fin - パケットに対してチェックされる TCP FIN ビット。
・ dscp <short (0-63)> - 差別化サービスコードポイントは、サービス品質制御を提供します。

■設定モード:
・ IPv4 ACL拡張アクセスリストコンフィグレーションモード

8. deny udp（IPv6）

■説明：関連するパラメータに基づいて拒否される IPv6 UDP パケットを指定します。

■構文:
・ deny udp {any | host <src-ipv6-addr> <src-prefix-len (0-128)>} [eq <port-number (1-65535)>] {any | host <dst-ipv6-addr><short(0-128)>} [eq <port-number (1-65535)>]ace-priority <integer (1-2147483647)> [dscp <value (0-63)>]

■パラメータの説明:
・ udp - UDPパケットを指定します。
・ any | host <ip6_addr> <integer(0-128)> - ホストの送信元アドレス / 任意のホスト
・ eq <short (1-65535)> - ポート番号。
・ any | host <ip6_addr> <integer(0-128)> - ホスト/任意のホストの宛先アドレス。
・ ace-priority <integer (1-2147483647)> - フィルターの優先度は、パケットが複数のフィルタリングルールに一致する場合に、どのフィルタリングルールを適用するかを決定します。
・ dscp <short (0-63)> - 差別化サービスコードポイントは、サービス品質制御を提供します。

■設定モード：IPv6 ACL拡張アクセスリストコンフィグレーションモード

9. deny udp

■説明：関連付けられたパラメータに基づいて拒否される UDP パケットを指定します。

■構文:
・ deny udp { any | host <src-ip-address> | <src-ip-address> <src- mask>} [eq <port-number (1-65535)>] { any | host <dest-ip-address> | <dest-ip-address> <dest-mask> } [eq <port-number (1-65535)>] ace-priority <integer (1-2147483647)> [dscp <value (0-63)>]

■パラメータの説明:
・ udp - ユーザデータグラムプロトコルを表します。
・ any| host <src-ip-address>|<src-ip-address> <src-mask> - 送信元IPアドレスに関するパラメータは以下の通りです。
  - any
  - ドット付き 10 進数のアドレス
  - パケットの送信元となるネットワークまたはホストの IP アドレス、および宛先アドレスで使用するネットワーク マスク
・ eq <short (1-65535)> - ポート番号。
・ any|host <dest-ip-address>|<dest-ip-address> <dest-mask> - 宛先 Pアドレスに関するパラメータは以下の通りです。
  - any
  - ドット付き 10 進数のアドレス
  - パケットの宛先となるネットワークまたはホストの IP アドレス、および宛先アドレスで使用するネットワーク マスク
・ ace-priority <integer (1-2147483647)> - フィルターの優先度は、パケットが複数のフィルタリングルールに一致する場合に、どのフィルタリングルールを適用するかを決定します。
・ dscp <short (0-63)> - 差別化サービスコードポイントは、サービス品質制御を提供します。

10. ip access-group

■説明:
インタフェース上のパケットのアクセス制御を有効にします。

このコマンドの no 形式を使用すると、すべてのアクセス グループまたは指定されたアクセス グループがインタフェースから削除されます。

■構文:
・ ip access-group <string (31)> in
・ no ip access-group [<string(31)>] in

■パラメータの説明:name<string(31)> - IP アクセス制御リスト名を表します。

■設定モード:インタフェースコンフィグレーションモード

11. ip access-list extend

■説明:
IPv4 を設定、IP アクセスリスト コンフィグレーション モードに入ります。

このコマンドの no 形式を使用すると、IP アクセスリストは削除されます。

■構文:
・ ip access-list extended <string(31)>
・ no ip access-list extended <string(31)>

■パラメータの説明:
・ <string(31)> – 拡張アクセスリスト名を設定します。

■設定モード:グローバルコンフィグレーションモード

12. ipv6 access-group

■説明:
インタフェース上のパケットの ipv6 アクセス制御を有効にします。

このコマンドの no 形式を使用すると、すべてのアクセス グループまたは指定されたアクセス グループがインタフェースから削除されます。

■構文:Ipv6 access-group <string (31)> in

13. ipv6 access-list extend

■説明:
ipv6 ACL を設定、ipv6 アクセスリスト コンフィグレーション モードに入ります。
このコマンドの no 形式は、ipv6 アクセスリストを削除します。

■構文:
・ ipv6 access-list extended <string(31)>

・ no ipv6 access-list extended <string(31)>

■パラメータの説明:
・ <string(31)> –拡張アクセスリスト名を設定します。

■設定モード:グローバルコンフィグレーションモード

14. mac access-group

■説明:
MAC アクセス制御リストをレイヤー 2 インタフェースに適用します。

このコマンドの no 形式を使用すると、インタフェースから MAC ACL を削除できます。

■構文:
・ mac access-group <string (31)> in
・ no mac access-group [<string(31)>] in

■パラメータの説明:
・ <string(31)> - MAC アクセス制御リスト名を表します。

■設定モード:インタフェースコンフィグレーションモード

15. mac access-list extend

■説明:
mac ACL を設定、mac アクセスリスト コンフィグレーション モードに入ります。

このコマンドの no 形式を使用すると、MAC アクセスリストは削除されます。

■構文:
・ mac access-list extended <string(31)>
・ no mac access-list extended <string(31)>

■パラメータの説明: <string(31)> –アクセスリスト名を設定します。

■設定モード:グローバルコンフィグレーションモード

16. no ace-priority（IPv4 ACE）

■説明：このコマンドは ACL エントリを削除します。

■構文:
・ no ace-priority <integer (1-2147483647)>

■パラメータの説明:
・ ace-priority <integer (1-2147483647)> - フィルターの優先度は、パケットが複数のフィルタリングルールに一致する場合に、どのフィルタリングルールを適用するかを決定します。

・ no ace-priority <integer (1-2147483647)>

■パラメータの説明:
・ ace-priority <integer (1-2147483647)> - フィルターの優先度は、パケットが複数のフィルタリングルールに一致する場合に、どのフィルタリングルールを適用するかを決定します。

■設定モード：IPv4 ACL拡張アクセスリストコンフィグレーションモード

17. no ace-priority（IPv6 ACE）

■説明：このコマンドは ace エントリを削除します。

■構文:no ace-priority <integer (1-2147483647)>

■パラメータの説明:
・ ace-priority <integer (1-2147483647)> - フィルターの優先度は、パケットが複数のフィルタリングルールに一致する場合に、どのフィルタリングルールを適用するかを決定します。

■設定モード：IPv6 ACL拡張アクセスリストコンフィグレーションモード

18. no ace-priority（MAC ACE）

■説明：このコマンドは ace エントリを削除します。

■構文:no ace-priority <integer (1-2147483647)>

■パラメータの説明:
・ ace-priority <integer (1-2147483647)> - フィルターの優先度は、パケットが複数のフィルタリングルールに一致する場合に、どのフィルタリングルールを適用するかを決定します。

■設定モード：MAC ACL拡張アクセスリストコンフィグレーションモード

19. permit udp

■説明:
関連するパラメータに基づいて転送される UDP パケットを指定します。

■構文:
・ permit udp { any | host <src-ip-address> | <src-ip-address> <src- mask>} [eq <port-number (1-65535)>] { any | host <dest-ip- address> | <dest-ip-address> <dest-mask> } [eq <port-number (1- 65535)>] ace-priority <integer (1-2147483647)> [dscp <value (0-63)>]

■パラメータの説明:
・ udp - UDPプロトコルを指定します。
・ any| host <src-ip-address>|<src-ip-address> <src-mask> - 送信元IPアドレスに関するパラメータは、次のとおりです。
  - any
  - ドット付き 10 進数のアドレス
  - パケットの送信元となるネットワークまたはホストの IP アドレス、および宛先アドレスで使用するネットワーク マスク
・ eq <short (1-65535)> - ポート番号。
・ any|host <dest-ip-address>|<dest-ip-address> <dest-mask> - 宛先IPアドレスに関するパラメータは、次のとおりです。
  - any
  - ドット付き 10 進数のアドレス
  - パケットの宛先となるネットワークまたはホストの IP アドレス、および宛先アドレスで使用するネットワーク マスク
・ ace-priority <integer (1-2147483647)> - フィルターの優先度は、パケットが複数のフィルタリングルールに一致する場合に、どのフィルタリングルールを適用するかを決定します。
・ dscp <short (0-63)> - 差別化サービスコードポイントは、サービス品質制御を提供します。

■設定モード: IPv4 ACL 拡張アクセス リスト コンフィグレーション モード

20. permit icmp

■説明:
IP アドレスと関連パラメータに基づいて転送される ICMP パケットを指定します。

■構文:
・ permit icmp {any |host <src-ip-address>|<src-ip-address><mask>} {any | host <dest-ip-address> | <dest-ip-address> <ma sk> } [type <message-type (0-255)>] [code <message-code (0- 255)>] ace-priority <integer (1-2147483647)> [dscp <integer (0-63)>]

■パラメータの説明:
・ icmp - インターネット制御メッセージ プロトコルを表します。
・ any| host <src-ip-address>|<src-ip-address> <src-mask> - 送信元IPアドレスに関するパラメータは、次のとおりです。
  - any
  - ドット付き 10 進数のアドレス
  - パケットの送信元となるネットワークまたはホストの IP アドレス、および宛先アドレスで使用するネットワーク マスク
・ any|host <dest-ip-address>|<dest-ip-address> <dest-mask> - 宛先IPアドレスに関するパラメータは、次のとおりです。
  - any
  - ドット付き 10 進数のアドレス
  - パケットの宛先となるネットワークまたはホストの IP アドレス、および宛先アドレスで使用するネットワーク マスク
・ type <short (0-255)> - メッセージのタイプを表します。
・ code <short (0-255)> - メッセージのコードを表します。
・ ace-priority <integer (1-2147483647)> - フィルターの優先度は、パケットが複数のフィルタリングルールに一致する場合に、どのフィルタリングルールを適用するかを決定します。
・ dscp <short (0-63)> - 差別化サービスコードポイントは、サービス品質制御を提供します。

■設定モード: IPv4 ACL拡張アクセスリストコンフィグレーションモード

21. permit icmpv6

■説明:
関連するパラメータに基づいて転送される IPv6 ICMPV6 パケットを指定します。

■構文:
・ permit icmpv6 {any | host <src-ipv6-addr><src-prefix-len (0-128)>} {any | host <dst-ipv6-addr><dst-prefix-len (0-128)} ace-priority <integer (1-2147483647)> [type <short(0-255)>] [code <short(0-255)>][dscp <value (0-63)>]

■パラメータの説明:
・ icmpv6 - インターネット制御メッセージ プロトコル。
・ any | host <ip6_addr> <integer(0-128)> - ホストの送信元アドレス / 任意のホスト
・ any | host <ip6_addr> <integer(0-128)> - ホスト/任意のホストの宛先アドレス。
・ ace-priority <integer (1-2147483647)> - フィルターの優先度は、パケットが複数のフィルタリングルールに一致する場合に、どのフィルタリングルールを適用するかを決定します。
・ type <short (0-255)> - メッセージタイプ
・ code <short (0-255)> - メッセージコード
・ dscp <short (0-63)> - 差別化サービスコードポイントは、サービス品質制御を提供します。

■設定モード: IPv6 ACL拡張アクセスリストコンフィグレーションモード

22. permit- ip/ospf/pim/protocol type

■説明:
permit ステートメントで定義された条件が一致する場合に、特定のプロトコル パケットのトラフィックを許可します。

■構文:
・ permit { ip | ospf | pim | <protocol-type (1-255)> | IPinIP | egp | igp | hmp | rdp | ipv6 | ipv6:route | ipv6:frag | rsvp | ipv6:icmp | l2tp} { any | host <src-ip-address> | <src-ip-address> <mask> }{ any | host <dest-ip-address> | <dest-ip-address> <mask> } ace- priority <integer (1-2147483647)> [dscp <value (0-63)>]

■パラメータの説明:
・ any| host <src-ip-address>|<src-ip-address> <mask> - 送信元IPアドレスに関するパラメータは、次のとおりです。
  - any
  - ドット付き 10 進数のアドレス
  - パケットの送信元となるネットワークまたはホストの IP アドレス、および宛先アドレスで使用するネットワーク マスク
・ any|host <dest-ip-address>|<dest-ip-address> <mask> -送信元IPアドレスに関するパラメータは、次のとおりです。
  - any
  - ドット付き 10 進数のアドレス
  - パケットの送信元となるネットワークまたはホストの IP アドレス、および宛先アドレスで使用するネットワーク マスク
・ ace-priority <integer (1-2147483647)> - フィルターの優先度は、パケットが複数のフィルタリングルールに一致する場合に、どのフィルタリングルールを適用するかを決定します。
・ dscp <short (0-63)> - 差別化サービスコードポイントは、サービス品質制御を提供します。

■設定モード: IPv4 ACL拡張アクセスリストコンフィグレーションモード

23. permit ipv6

■説明:
プロトコルおよび関連パラメータに基づいて転送される IPv6 パケットを指定します。

■構文:
・ permit ipv6 {any | host <src-ipv6-addr> <src-prefix-len (0- 128)> } { any | host <dst-ipv6-addr> <dst-prefix-len (0-128)> } ace-priority <integer (1-2147483647)> [dscp <short(0-63)>]

■パラメータの説明:
・ ipv6 – IPv6を指定します。
・ any | host <ip6_addr> <integer(0-128)> - ホスト/任意のホストの送信元アドレス。
・ any | host <ip6_addr> <integer(0-128)> - IPv6を指定します。
・ ace-priority <integer (1-2147483647)> - フィルターの優先度は、パケットが複数のフィルタリングルールに一致する場合に、どのフィルタリングルールを適用するかを決定します。
・ dscp <short (0-63)> - 差別化サービスコードポイントは、サービス品質制御を提供します。

■設定モード: IPv6 ACL拡張アクセスリストコンフィグレーションモード

24. permit tcp(IPv6)

■説明:
関連するパラメータに基づいて転送される IPv6 TCP パケットを指定します。

■構文:
・ permit tcp {any | host <src-ipv6-addr> <src-prefix-len (0-128)} [eq <port-number (1-65535)>] {any | host <dst-ipv6-addr> <dst- prefix-len (0-128)>} [eq <port-number (1-65535)>] ace-priority<integer (1-2147483647)> [{ack | non_ack}] [{rst | non_rst}] [{psh | non_psh}] [{urg | non_urg}] [{syn | non_syn}] [{fin | non_fin}] [dscp <value (0-63)>]

■パラメータの説明:
・ tcp - TCPを指定します。
・ any | host <ip6_addr> <integer(0-128)> - ホスト/任意のホストの宛先アドレス。
・ any hosteq <short (1-65535)> - ポート番号。
・ ace-priority <integer (1-2147483647)> - フィルターの優先度は、パケットが複数のフィルタリングルールに一致する場合に、どのフィルタリングルールを適用するかを決定します。
・ ack | non_ack - パケットに対してチェックされる TCP ACK ビット。
・ rst | non_rst - パケットに対してチェックされる TCP RST ビット。
・ psh | non_psh - パケットに対してチェックされる TCP PSH ビット。
・ urg | non_urg - パケットに対してチェックされる TCP URG ビット。
・ syn | non_syn - パケットに対してチェックされる TCP SYN ビット。
・ fin | non_fin- パケットに対してチェックされる TCP FIN ビット。
・ dscp <short (0-63)> - 差別化サービスコードポイントは、サービス品質制御を提供します。

■設定モード: IPv6 ACL拡張アクセスリストコンフィグレーションモード

25. permit tcp(IPv4)

■説明:
関連するパラメータに基づいて転送される TCP パケットを指定します。

■構文:
・ permit tcp {any | host <src-ip-address> | <src-ip-address> <src- mask> } [eq <port-number (1-65535)>] { any | host <dest-ip- address> | <dest-ip-address> <dest-mask> } [eq <port-number (1- 65535)>] ace-priority <integer (1-2147483647)> [{ack | non_ack}] [{rst | non_rst}] [{psh | non_psh}] [{urg | non_urg}] [{syn | non_syn}] [{fin | non_fin}] [dscp <value (0-63)>]

■パラメータの説明:
・ tcp - TCPを指定します。
・ any| host <src-ip-address>|<src-ip-address> <src-mask> - 送信元IPアドレスに関するパラメータは、次のとおりです。
  - any
  - ドット付き 10 進数のアドレス
  - パケットの送信元となるネットワークまたはホストの IP アドレス、および宛先アドレスで使用するネットワーク マスク
・ eq <short (1-65535)> - ポート番号。
・ any|host <dest-ip-address>|<dest-ip-address> <dest-mask> - 宛先IPアドレスに関するパラメータは、次のとおりです。
  - any
  - ドット付き 10 進数のアドレス
  - パケットの宛先となるネットワークまたはホストの IP アドレス、および宛先アドレスで使用するネットワーク マスク
・ ace-priority <integer (1-2147483647)> - フィルターの優先度は、パケットが複数のフィルタリングルールに一致する場合に、どのフィルタリングルールを適用するかを決定します。
・ ack | non_ack - パケットに対してチェックされる TCP ACK ビット。
・ rst | non_rst - パケットに対してチェックされる TCP RST ビット。
・ psh | non_psh - に対してチェックされる TCP PSH ビット
・ urg | non_urg - パケットに対してチェックされる TCP URG ビット。
・ syn | non_syn - パケットに対してチェックされる TCP SYN ビット。
・ fin | non_fin - パケットに対してチェックされる TCP FIN ビット。
・ dscp <short (0-63)> - 差別化サービスコードポイントは、サービス品質制御を提供します。

■設定モード: IPv4 ACL拡張アクセスリストコンフィグレーションモード

26. permit udp（IPv6）

■説明:関連するパラメータに基づいて転送される IPv6 UDP パケットを指定します。

■構文:

・ permit udp {any | host <src-ipv6-addr> <src-prefix-len (0-128)>} [eq <port-number (1-65535)>] {any | host <dst-ipv6-addr><dst-prefix-len (0-128)>} [eq <port-number (1-65535)>]ace-priority <integer (1-2147483647)> [dscp <value (0-63)]

■パラメータの説明:

・ udp - ユーザデータグラムプロトコルを表します。
・ any | host <src-ipv6-address> <src-prefix-len(0-128)> - ホスト/任意のホストの送信元アドレス。
・ eq <short (1-65535)> - ポート番号
・ any | host <ip6_addr> <integer(0-128)> - ホスト/任意のホストの宛先アドレス。
・ ace-priority <integer (1-2147483647)> - フィルターの優先度は、パケットが複数のフィルタリングルールに一致する場合に、どのフィルタリングルールを適用するかを決定します。
・ dscp <short (0-63)> - 差別化サービスコードポイントは、サービス品質制御を提供します。

■設定モード:IPv6 ACL拡張アクセスリストコンフィグレーションモード

27. permit mac

■説明:

MACアドレスと関連パラメータに基づいて転送されるパケットを指定します。条件が一致する場合に非 IP トラフィックの転送を許可します。

■構文:

・ permit { any | host <src-mac-address> <mask> } { any | host <dest-mac- address> } {ace-priority <integer (1-2147483647)>} [ethertype<integer (1-65535)>] [vlan <vlan-id (1-4094)>] [vlan- priority <value (0-7)>]

■パラメータの説明:

・ any | host <src-mac-address > - パケットと照合する送信元 MACアドレス
・ any | host <dest-mac-address > - パケットと照合する宛先 MACアドレス
・ <mask> - パケットの送信元/宛先MACアドレスと照合するMACアドレスの範囲を定義します。照合に使用するビットをf、任意にするビットを0とします。
・ ace-priority <integer (1-2147483647)> - フィルターの優先度は、パケットが複数のフィルタリングルールに一致する場合に、どのフィルタリングルールを適用するかを決定します。
・ ethertype <integer (1-65535)> - フィルタリングする非 IP プロトコル タイプを指定します。
・ vlan <integer (1-4094)> - 受信パケットと照合する VLAN 値。
・ vlan-priority <short (0-7)> - 受信パケットと照合する VLAN 優先度の値。

■設定モード:MAC ACL拡張アクセスリストコンフィグレーションモード

28. show access-lists

■説明:アクセスリストの設定を表示します。

■構文:show access-lists [{ip | mac | ipv6 } [<string(31)>]]

■パラメータの説明:
・ ip - IP アクセスリストを表します。
・ mac – MAC アクセスリストを表します。
・ ipv6 – IPv6 アクセスリストを表します。
・ <string(31)> - アクセスリストの名前を表します。

■設定モード:特権EXECモード

3.2.23 QoS

1. class-policy

■説明:
このコマンドは QoS ポリシーを設定ます。
コマンドの no 形式は、QoSポリシーを削除します。

■構文:
・ class-policy <name (23)>
・ no class-policy <name (23)>

■パラメータの説明:
・ <name (23)> – QoS ポリシーの名前を表します。

■設定モード: グローバルコンフィグレーションモード

2. match policy – icmp

■説明:
関連するパラメータに基づいて転送される ICMP パケットを指定します。

■構文:
・ match policy { any | host <src-mac-address>} { any | host <dest- mac-address>} [ethertype <integer (1-65535)>] [vlan <vlan-id (1-4094)>] [vlan-priority <value (0-7)>] icmp {any | host <src-ip- address>| <src-ip-address> <src-mask> } { any | host <dest-ip- address> | <dest-ip-address> <dest-mask> } [type <message-type (0-255)>] [code <message-code (0-255)>] [dscp <dscp-value (0- 63)>]

■パラメータの説明:
・ any | host <src-mac-address> - パケットと照合する送信元 MACアドレス
・ any | host <dest-mac-address> - パケットと照合する宛先 MACアドレス
・ ethertype <integer (1-65535)> - フィルタリングする非 IP プロトコル タイプを指定します。
・ vlan <vlan-id (1-4094)> - 受信パケットと照合する VLAN 値。
・ vlan-priority <value (0-7)> - 受信パケットと照合する VLAN 優先度の値。
・ any | host <src-ip-address>| <src-ip-address> <src-mask> - 送信元IPアドレスに関するパラメータは、次のとおりです。
  - any
  - ドット付き 10 進数のアドレス
  - パケットの送信元となるネットワークまたはホストの IP アドレス、および宛先アドレスで使用するネットワーク マスク
・ any | host <dest-ip-address> | <dest-ip-address> <dest-mask>- 宛先IPアドレスに関するパラメータは、次のとおりです。
  - any
  - ドット付き 10 進数のアドレス
  - パケットの宛先となるネットワークまたはホストの IP アドレス、および宛先アドレスで使用するネットワーク マスク
・ type <message-type (0-255)> - メッセージタイプ
・ code <message-code (0-255)> - メッセージコード
・ dscp <dscp-value (0-63)> - 差別化サービスコードポイントは、サービス品質制御を提供します。
・ dscp <value (0-63)> -DSCP値を設定します

■設定モード: ポリシーマップコンフィグレーションモード

3. match policy - ip/ospf/pim/protocol type

■説明:
関連付けられたパラメータに基づいて転送される ip/ospf/pim/protocol タイプのパケットを指定します。

■構文:
・ match policy { any | host <src-mac-address> } { any | host <dest- mac-address>} [ethertype <integer (1-65535)>] [vlan <vlan-id (1-4094)>] [vlan-priority <value (0-7)>] { ip | ospf | pim |<protocol-type (1-255)>} {any | host <src-ip-address>| <src-ip- address> <src-mask> } { any | host <dest-ip-address> | <dest-ip-address> <dest-mask> } [dscp <dscp-value (0-63)>] [action { vpt<tos-value(0-7)> | dscp <value (0-63)>}]

■パラメータの説明:
・ any | host <src-mac-address> - パケットと照合する送信元 MACアドレス
・ any | host <dest-mac-address> - パケットと照合する宛先 MACアドレス
・ ethertype <integer (1-65535)> - フィルタリングする非 IP プロトコル タイプを指定します。
・ vlan <vlan-id (1-4094)> - 受信パケットと照合する VLAN 値。
・ vlan-priority <value (0-7)> - 受信パケットと照合する VLAN 優先度の値。
・ any | host <src-ip-address>| <src-ip-address> <src-mask> - 送信元IPアドレスに関するパラメータは、次のとおりです。
  - any
  - ドット付き 10 進数のアドレス
  - パケットの送信元となるネットワークまたはホストの IP アドレス、および宛先アドレスで使用するネットワーク マスク
・ any | host <dest-ip-address> | <dest-ip-address> <dest-mask>- 宛先IPアドレスに関するパラメータは、次のとおりです。
  - any
  - ドット付き 10 進数のアドレス
  - パケットの宛先となるネットワークまたはホストの IP アドレス、および宛先アドレスで使用するネットワーク マスク
・ type <message-type (0-255)> - メッセージタイプを設定します。
・ code <message-code (0-255)> - メッセージコードを設定します。
・ dscp <dscp-value (0-63)> - DSCP値を設定します。
・ vpt <tos-value(0-7)> - ToS値を設定します。
・ dscp <value (0-63)> - DSCP値に設定します。

■設定モード: ポリシーマップコンフィグレーションモード

4. match policy – tcp/udp

■説明:
関連するパラメータに基づいて転送される TCP/UDP パケットを指定します。

■構文:
・ match policy { any | host <src-mac-address> } { any | host <dest- mac-address>} [ethertype <integer (1-65535)>] [vlan <vlan-id (1-4094)>] [vlan-priority <value (0-7)>] { tcp | udp } {any | host<src-ip-address>| <src-ip-address> <src-mask> } [eq <port- number (1-65535)>] { any | host <dest-ip-address> | <dest-ip- address> <dest-mask> } [eq <port-number (1-65535)>] [dscp<dscp-value (0-63)>] [action { tos <tos-value(0-7)> | dscp <value (0-63)>}]

■パラメータの説明:
・ any | host <src-mac-address> - パケットと照合する送信元 MACアドレス
・ any | host <dest-mac-address> - パケットと照合する宛先 MACアドレス
・ ethertype <integer (1-65535)> - フィルタリングする非 IP プロトコル タイプを指定します。
・ vlan <vlan-id (1-4094)> - 受信パケットと照合する VLAN 値。
・ vlan-priority <value (0-7)> - 受信パケットと照合する VLAN 優先度の値。
・ tcp - TCPを指定します。
・ udp - ユーザ データグラム プロトコル。
・ any | host <src-ip-address>| <src-ip-address> <src-mask> - 送信元IPアドレスに関するパラメータは、次のとおりです。
  - any
  - ドット付き 10 進数のアドレス
  - パケットの送信元となるネットワークまたはホストの IP アドレス、および宛先アドレスで使用するネットワーク マスク
・ eq <port-number (1-65535)> - ポート番号。
・ any|host <dest-ip-address>|<dest-ip-address> <dest-mask> - 宛先IPアドレスに関するパラメータは、次のとおりです。
  - any
  - ドット付き 10 進数のアドレス
  - パケットの宛先となるネットワークまたはホストの IP アドレス、および宛先アドレスで使用するネットワーク マスク
・ dscp <dscp-value (0-63)> - DSCP値を設定します。
・ tos <tos-value(0-7)> - ToS値に設定します。
・ dscp <value (0-63)> - DSCP値に設定します。

■設定モード: ポリシーマップコンフィグレーションモード

5. no match policy

■説明: すべてのポリシー設定をクリアします。

■構文:no match policy

■設定モード: ポリシーマップコンフィグレーションモード

6. priority-map

■説明:
受信優先度マッピングのタイプをキューに設定します。
コマンドの no 形式はデフォルト値を設定します。

■構文:
・ priority-map in-priority-type { vlanPri | ipDscp } <integer(0-63)> [<integer(0-63)>] [<integer(0-63)>] [<integer(0-63)>] [<integer(0-63)>] [<integer(0-63)>] [<integer(0-63)>] [<integer(0-63)>] to <integer(1-8)>
・ no priority-map in-priority-type { vlanPri | ipDscp } <integer(0-63)> [<integer(0-63)>] [<integer(0-63)>] [<integer(0-63)>] [<integer(0-63)>] [<integer(0-63)>] [<integer(0-63)>] [<integer(0-63)>]

■パラメータの説明:
・ vlanPri－VLAN の優先度を表します。
・ ipDscp－DSCPを表します
・ <integer(0-63)>－優先度の値。vlanPri の場合は (0 ～ 7)、ipDscp の場合は (0 ～ 63)。
・ integer(1-8)－キューIDを表します。

■設定モード:グローバルコンフィグレーションモード

7. qos

■説明:QoS サブシステムを有効/無効にします。

■構文:qos {enable | disable}

■パラメータの説明:
・ enable - QoS サブシステムを有効にします
・ disable - QoS サブシステムを無効にします

■設定モード:グローバルコンフィグレーションモード

8. qos interface

■説明:ポートのデフォルトの入力ユーザの優先度を設定します。

■構文:qos interface <iftype> <ifnum> def-user-priority <integer(0-7)>

■パラメータの説明:
・ iftype - インタフェースのタイプ。
・ ifnum - インタフェース番号。
・ def-user-priority - ポートのデフォルトの入力ユーザの優先度。

■設定モード:グローバルコンフィグレーションモード

9. qos trust(QoS モード)

■説明: QoSモードを設定します。

■構文:qos trust {cos | dscp | cos-dscp}

■パラメータの説明:
・ cos – trust cosを表します。
・ dscp – trust dscpを表します。
・ cos-dscp – trust cosを表します。cosが設定されていない場合は、trust dscpを指定します。

■設定モード:グローバルコンフィグレーションモード

10. qos trust(QoS trust)

■説明:ポート上の QoS trustを有効/無効にします。

■構文:qos trust {enable | disable}

■パラメータの説明:
・ enable – ポート上の QoS 信頼を有効にします。
・ disable - ポート上の QoS 信頼を無効にします。

■設定モード:インタフェースコンフィグレーションモード

11. scheduler

■説明:
スケジューラを作成し、スケジューラ パラメータを設定します。

■構文:
・ scheduler sched-algo {strict-priority | {wrr [weight <integer(0- 128)> <integer(0-128)> <integer(0-128)> <integer(0-128)><integer(0-128)> <integer(0-128)> <integer(0-128)> <integer(0- 128)>]}}

■パラメータの説明:
・ strict-priority – strictPriorityを表します
・ wrr –weightedRoundRobinを表します。
・ weight <integer(0-128)> <integer(0-128)> <integer(0-128)><integer(0-128)> <integer(0-128)> <integer(0-128)><integer(0-128)> <integer(0-128)> – キュー 1 ～8 までの wrr の重みを表します。

■設定モード:グローバルコンフィグレーションモード

12. service-policy

■説明:
インタフェース上で qos ポリシーを有効にします。
このコマンドの no 形式を使用すると、インタフェースから qos ポリシーは削除されます。

■構文:
・ service-policy <class-policy-name (31)> in
・ no service-policy <class-policy-name (31)>

■パラメータの説明:
・ <class-policy-name (31)> –QoS ポリシー名を表します。

■設定モード:インタフェースコンフィグレーションモード

13. show class-policy

■説明:QoS ポリシーを表示します。

■構文:show class-policy [{<name(23)> | interface <iftype> <ifnum>}]

■パラメータの説明:
・ <string(31)> – QoS ポリシー名を表します。
・ iftype - インタフェースのタイプを表します。
・ ifnum - インタフェース番号を表します。

■設定モード:特権EXECモード

14. show priority-map in-priority-type { vlanPri | ipDscp }

■説明:キューへの優先度のマッピングを表示します。

■パラメータの説明:
・ vlanPri – VLAN の優先度を表します。
・ ipDscp – DSCPを表します。

■設定モード:特権EXECモード

15. show qos def-user-priority [interface <iftype> <ifnum>]

■説明:ポートに設定されているデフォルトの入力ユーザの優先度を表示します。

■構文:show qos def-user-priority [interface <iftype> <ifnum>]

■パラメータの説明:
・ iftype - インタフェースのタイプを表します。
・ ifnum - インタフェース番号を表します。

■設定モード:特権EXECモード

16. show qos global info

■説明:QoS 関連のグローバル設定を表示します。

■構文:show qos global info

■設定モード:特権EXECモード

17. show scheduler

■説明:設定されたスケジューラを表示します。

■構文:show scheduler

■設定モード:特権EXECモード

18. Storm-control

■説明:

ブロードキャスト、unknownマルチキャスト、および DLF パケットのストーム制御レートを設定します。

コマンドの no 形式は、ブロードキャスト、unknownマルチキャスト、および DLF パケットのストーム制御レートをデフォルト値に設定します。

■構文:
・ storm-control { broadcast | unknown-multicast | dlf } level <rate-value(16-10000000)>
・ no storm-control { broadcast | unknown-multicast | dlf } level

■パラメータの説明:
・ broadcast - パケットをブロードキャストします。
・ unknown-multicast –unknownマルチキャストパケットを表します。
・ dlf - unknownなユニキャスト パケットを表します。
・ <rate-value(16-10000000)> - ストームコントロールのレートとして設定する値(単位:kbps)を表します。
・ 値は16の倍数である必要があります。

■設定モード:インタフェースコンフィグレーションモード

3.2.24 Bandwidth control

1. rate-limit

■説明:
インタフェースのレート制限を有効にします。

コマンドの no 形式を使用すると、レート制限が無効になります。

■構文:
・ rate-limit { output | input } [<integer(16-1000000)>]
・ no rate-limit { output | input }

■パラメータの説明:
・ output – egress制限を表します。
・ input – ingress制限を表します。
・ <integer(16-10000000)> -回線速度 (kbps)を表します。

■設定モード:インタフェースコンフィグレーション

3.2.25 arp inspection

1. ip arp inspection trust

1) ip arp inspection trust

■説明:
DHCP snoopingの有効時に、インタフェースをtrustポート(ダイナミックARP検査を実施しない)として設定します。

■構文:
・ ip arp inspection trust
・ no ip arp inspection trust

■パラメータの説明: なし

■デフォルト値: このオプションは、無効です。

■設定モード: インタフェースコンフィギュレーションモード

2) ip arp inspection filter vlan

■説明:
VLAN の ARP インスペクションをチェックする場合、ARP アクセスリストを指定します。

■構文:
・ ip arp inspection filter arp-acl-name vlan <vlan-id(1-4094)> [static]
・ no ip arp inspection filter arp-acl-name vlan <vlan-id(1-4094)> [static]

■パラメータの説明:
・ arp-acl-name - アクセス制御リスト名を指定します。
・ vlan <vlan-id(1-4094)> - 指定した VLAN ID の範囲を選択します。
・ ・static - 静的ARPエントリに一致しないパケットを破棄します。

■デフォルト値: なし

■設定モード: グローバルコンフィギュレーションモード

2. ip arp inspection validate

■説明: ARPインスペクションをチェックする際に、追加のチェックを指定します。

■構文:
・ ip arp inspection validate { src-mac | dst-mac | ip }
・ no ip arp inspection validate { src-mac | dst-mac | ip }

■パラメータの説明:
・ src-mac - ARP 要求および応答パケット、ARP ペイロードの送信元 MAC アドレスに対するイーサネットの ヘッダの送信元 MAC アドレスの一貫性をチェックします。
・ dst-mac - ARP 応答パケットと、ARP ペイロードの宛先 MAC アドレスに対するイーサネットのヘッダの宛先 MAC アドレスの一貫性をチェックします。
・ ip - ARP ペイロード内の IP アドレスの有効性をチェックします。ARP 要求および応答の両方の送信側の IP と、ARP 応答の宛先 IP が検証され、IP アドレス(0.0.0.0、255.255.255.255)、およびすべての IP マルチキャストアドレス宛てのパケットは破棄されます。送信側の IP アドレスの場合はすべてのARP 要求および応答がチェックされ、宛先 IP アドレスの場合は ARP 応答のみチェックされます。

■デフォルト値: なし

■設定モード: グローバルコンフィギュレーションモード

1) ARP ACL

(1)arp access-list

■説明: ARPのACLを設定、ARP アクセスリストコンフィギュレーションモードに入ります。

■構文:
・ arp access-list <string(31)>
・ no arp access-list <string(31)>

■パラメータの説明:
・ <string(31)> - アクセスリスト名を設定します。

■デフォルト値: なし

■設定モード: グローバルコンフィギュレーションモード

(2)permit arp

■説明:
送信側のMAC アドレスで定義された条件に一致した場合、特定のプロトコル パケットのトラフィックを許可します。

■構文:
・ permit ip {any | host SENDER-IP | SENDER-IP SENDER-IP-MASK} mac {any | host SENDERMAC|SENDER-MAC SENDER-MAC-MASK} ace-priority <integer (1-2147483647>

■パラメータの説明:
・ ip –送信元IPアドレスを指定します。
・ any | host < SENDER-IP > | <SENDER-IP> <SENDER-IP-MASK> - 送信側のIPアドレスは、次のいずれかになります。
  - ‘any’
  - ドット付き 10 進表記のアドレス
  - パケットの送信元ホストのネットワークの IP アドレスと、その IP アドレスで使用するネットワークマスク。
・ any | host < SENDER-MAC > | < SENDER-MAC > < SENDER-MAC -MASK> - 送信側のIPアドレスは、次のいずれかになります。
  - ‘any’
  - パケットの照合対象となる送信側の MAC アドレス。
・ ace-priority <integer (1-2147483647> - フィルタリングの優先順位は、パケットが複数のフィルタリングルールに一致する場合に、どのフィルタリングルールを適用するかを決定します。

■デフォルト値: なし

■設定モード: ARP ACLアクセスリストコンフィギュレーションモード

(3)deny arp

■説明:
ARP アドレスと関連パラメータに基づいて、denyパケットを指定します。

■構文:
・ deny ip {any | host SENDER-IP | SENDER-IP SENDER-IP-MASK} mac {any | hostSENDER-MAC| SENDER-MAC SENDER-MAC-MASK} ace-priority <integer (1-2147483647>

■パラメータの説明:
・ ip –送信元IPアドレスを指定します。
・ any | host < SENDER-IP > | <SENDER-IP> <SENDER-IP-MASK> - 送信側のIPアドレスは、次のいずれかになります。
  - ‘any’
  - ドット付き 10 進表記のアドレス
  - パケットの送信元ホストのネットワークの IP アドレスと、その IP アドレスで使用するネットワークマスク。
・ any | host < SENDER-MAC > | < SENDER-MAC > < SENDER-MAC -MASK> -送信側のIPアドレスは、次のいずれかになります。
  - ‘any’
  - パケットの照合対象となる送信側の MAC アドレス。
  - ace-priority <integer (1-2147483647> - フィルタリングの優先順位は、パケットが複数のフィルタリングルールに一致する場合に、どのフィルタリングルールを適用するかを決定します。
・

■デフォルト値: なし

■設定モード: ARP ACLアクセスリストコンフィギュレーションモード

(4)show arp access-lists

■説明: ARP アクセスリストの設定を表示します。

■構文: show arp access-lists [<string(31)>]

■パラメータの説明:
・ <string(31)> - アクセスリストの名前。

■デフォルト値: なし

■設定モード: 特権EXECモード

■設定例:

```
FXCX5512PE# show arp access-lists

 ARP ACCESS LISTS
 
ARP ACL Group : fxcarp01

 Status                 : Active

Sequence                : 2
ARP Access List 16

 IP address Type              : IPV4
 Sender IP address            : 192.168.2.0
 Sender IP address mask       : 255.255.255.0
 Sender MAC                   : 00:00:00:00:00:00
 Sender MAC mask              : 00:00:00:00:00:00
 Filter Action                : Permit
```

(5)no ace-priority

■説明: ace エントリを削除します。

■構文:
・ no ace-priority <integer (1-2147483647)>

■パラメータの説明:
・ ace-priority <integer (1-2147483647)> - フィルタリングの優先順位は、パケットが複数のフィルタリングルールに一致する場合に、どのフィルタリングルールを適用するかを決定します。

■デフォルト値 : なし

■設定モード: ARP ACL アクセスリストコンフィギュレーションモード

2) Log

(1) ip arp inspection vlan logging

■説明: ログ情報に記録されるパケットのタイプを制御します。

■構文:

・ ip arp inspection vlan <vlan-id(1-4094)> logging {acl-match {permit | deny | all | none} |dhcp-bindings {permit | deny | all | none}}

■パラメータの説明:

・ vlan <vlan-id(1-4094)> - 指定した VLAN ID の範囲を選択します。
・ acl-match - ACL に基づいて、破棄または許可されるパケットのログ情報の基準を指定します。
  - permit – 設定された ACL によって許可された場合のログ情報
  - deny - 設定された ACL によって拒否された場合のログ情報
  - all - 設定された ACL によって許可または拒否された場合のログ情報.
  - none - ACL に一致したパケットをログに記録しないことを指定します。
・ dhcp-bindings - DHCPスヌーピングバインディングテーブル上のマッチングルールに基づいて、破棄または許可されたパケットのログ情報基準を指定します。
  - permit - DHCP スヌーピングバインディングテーブルで許可された場合はログ情報を記録します。
  - deny - DHCP スヌーピングバインディングテーブルによって拒否された場合のログ情報を記録します。
  - all - DHCP スヌーピングバインディングテーブルによって許可または拒否された場合のログ情報を記録します。
  - none - すべてのパケットのログ情報は記録されません。

■デフォルト値: 拒否、または破棄されたパケットはすべてログに記録されます。

■設定モード: グローバルコンフィグレーションモード

(2) clear ip arp inspection log

■説明: ARPインスペクションのログバッファをクリアします。

■構文: clear ip arp inspection log

■パラメータの説明: なし

■デフォルト値: なし

■設定モード: 特権EXECモード

(3) ip arp inspection log-buffer

■説明:ARPインスペクションのログバッファのパラメータを設定します。

■構文: ip arp inspection log-buffer <integer (1-1024)>

■パラメータの説明:
・ log-buffer <integer (1-1024)> -バッファエントリ番号を指定します。

■デフォルト値: 32

■設定モード: コンフィギュレーションモード

(4) show ip arp inspection log

■説明: ARPインスペクションのログバッファを表示します

■構文 show ip arp inspection log

■パラメータの説明: なし

■デフォルト値: なし

■設定モード: 特権EXECモード

■設定例:

```
FXCX5512PE# show ip arp inspection log
Total log buffer size: 32

Port  VLAN  Sender IP       Sender MAC          Occurrence
----- ----  --------------  ------------------  ----------------
 -------

Total Entries: 0

FXCX5512PE#
```

3) ARP inspection statistics

(1) clear ip arp inspection statistics

■説明: ダイナミックARP インスペクションの統計情報をクリアします。

■構文: clear ip arp inspection statistics { all | vlan <vlan-range>}

■パラメータの説明:
・ all - すべての VLAN からダイナミックARP インスペクションの統計情報をクリアします。
・ vlan <vlan-range> - VLAN または VLAN の範囲を指定します。

■デフォルト値: なし

■設定モード: 特権EXECモード

(2)show ip arp inspection statistics

■説明: ダイナミックARP インスペクションの統計情報を表示します。

■構文: show ip arp inspection statistics

■パラメータの説明: なし

■デフォルト値: なし

■設定モード: 特権EXECモード

■設定例:

```
FXCX5512PE# show ip arp inspection statistics

VLAN  Forwarded  Dropped  DHCP Drops    ACL Drops
----- ---------  -------  ----------    ---------

VLAN  DHCP Permits  ACL Permits  Source MAC Failures
----- ------------  -----------  -------------------

VLAN  Dest MAC Failures  IP Validation Failures
----- -----------------  ----------------------
```

FXCX5512/FXCX5512PE Management Guide
（FXC23-DC-2000009-R1.3）

初版	2023 年 12 月
第 2 版	2024 年 2 月
第 3 版	2024 年 5 月
第 4 版	2024 年 6 月

- 本ユーザマニュアルは、FXC 株式会社が制作したもので、全ての権利を弊社が所有します。弊社に無断で本書の一部、または全部を複製 / 転載することを禁じます。
- 改良のため製品の仕様を予告なく変更することがありますが、ご了承ください。
- 予告なく本書の一部または全体を修正、変更することがありますが、ご了承ください。
- ユーザマニュアルの内容に関しましては、万全を期しておりますが、万一ご不明な点がございましたら、弊社サポートセンターまでご相談ください。