

**Management Guide
FXC5710/5718/5728**

**Management Guide
FXC5710/5718/5728**

**Management Guide
FXC5710/5718/5728**

**Management Guide
FXC5710/5718/5728**

**Management Guide
FXC5710/5718/5728**

**FXC5710/5718/5728
Management Guide**

GUI ver.

**Management Guide
FXC5710/5718/5728**

**Management Guide
FXC5710/5718/5728**

**Management Guide
FXC5710/5718/5728**

**Management Guide
FXC5710/5718/5728**

**Management Guide
FXC5710/5718/5728**

**Management Guide
FXC5710/5718/5728**

**Management Guide
FXC5710/5718/5728**

Management Guide

本マニュアルについて

- 本マニュアルでは、FXC5710/FXC5718/FXC5728 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。
- 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。

製品取り扱い時のご注意

- ◆ 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

1 章 WEB 接続手順	4
1.1. 本機との接続	4
1.1.1. ネットワークへの接続方法	4
1.1.2. 動作環境	9
2 章 WEB による設定	10
2.1. WEB による設定方法	10
2.1.1. 本機へのログイン	10
2.1.2. メイン画面	11
2.1.3. メインメニューについて	13
3 章 各機能の設定	14
3.1. System Config(システムの設定)	14
3.1.1. System Homepage (システムのホームページ)	14
3.1.2. Device Info(デバイス情報)	15
3.1.3. IP Config (IP 機能設定)	16
3.1.4. Web Config(WEB 設定)	18
3.1.5. User Management (ユーザマネジメント)	21
3.1.6. Firmware Upgrade (ファームウェアアップデート)	24
3.1.7. Management Config (マネジメントの設定)	26
3.1.8. NTP	28
3.1.9. SNTP	30
3.1.10. Device Management (デバイスの管理)	32
3.2. Monitor Management (モニターの管理)	36
3.2.1. SSH Config (SSH の設定)	36
3.2.2. Telnet Config (Telnet 設定)	37
3.2.3. Port Statistics (ポートの統計情報)	38
3.2.4. DDMI Status (DDMI ステータス)	39
3.2.5. Ping	40
3.2.6. Traceroute (トレースルート)	40
3.2.7. Cable Diagnostics (ケーブル診断)	41
3.2.8. SNMP Config (SNMP 設定)	42
3.2.9. RMON Config (RMON 設定)	52
3.2.10. Camera-Detection (カメラ検出機能)	57
3.2.11. Loopback Detection (ループバック検出)	58
3.2.12. LLDP Config (LLDP 設定)	61
3.3. Switch Config(スイッチの設定)	65
3.3.1. Port Config(ポートの設定)	65
3.3.2. Port Mirror(ポートのミラーリング)	67
3.3.3. Port Isolate(ポートの隔離)	68
3.3.4. Port Channel(リンクアグリゲーション)	69
3.3.5. Jumbo Frame(ジャンボフレーム)	71
3.3.6. Port Rate(ポートレート)	72
3.3.7. Storm Control(ストームコントロール)	73
3.3.8. MAC Address Config(MAC アドレスの設定)	74
3.3.9. AM(アクセス管理機能)	77
3.3.10. AAA(認証・認可・アカウント管理機能)	78
3.3.11. DNS Config	87

3.4. VLAN Config (VLAN 設定)	88
3.4.1. VLAN Config (VLAN 設定)	88
3.4.2. GVRP Config (GVRP の設定)	88
3.4.3. QINQ	94
3.4.4. Voice VLAN (音声 VLAN)	95
3.4.5. MAC VLAN	97
3.4.6. Protocol VLAN (プロトコル VLAN)	100
3.4.7. Surveillance VLAN	101
3.5. DHCP Config	103
3.5.1. DHCP Server (DHCP サーバ)	103
3.5.2. DHCP Relay Config (DHCP リレー設定)	113
3.5.3. DHCP Snooping (DHCP スヌーピング)	115
3.6. ACL Config	121
3.6.1. Time Range Config (タイムレンジ設定)	121
3.6.2. IP ACL	123
3.6.3. MAC ACL	127
3.6.4. MAC-IP Extended ACL (拡張 MAC-IP ACL)	130
3.6.5. ACL Binding (ACL バイディング)	132
3.7. Ring Network (リング型ネットワーク)	134
3.7.1. Spanning-tree (スパニングツリー)	134
3.7.2. ERPS	142
3.8. Route Config (ルーティング設定)	147
3.8.1. Static Route (スタティックルート)	147
3.8.2. Routing Table (ルーティングテーブル)	148
3.9. Multicast Manage (マルチキャスト管理)	149
3.9.1. IGMP Snooping Config (IGMP スヌーピングの設定)	149
3.9.2. MLD Snooping Config (MLD スヌーピング設定)	154
3.10. QoS Config (QoS の設定)	159
3.10.1. Port Config (ポートの設定)	159
3.10.2. Class-Map Config (Class-Map の設定)	165
3.10.3. Policy-Map Config (ポリシーマップの設定)	174

はじめに

この度は、弊社FXC5710/FXC5718/FXC5728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、RJ-45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。

FWバージョンおよびリビジョンにより、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

本章では、WEBインターフェース(GUI)による設定方法について説明します。

本製品には、HTTPのWebエージェントが組み込まれているため、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。

1.1.1. ネットワークへの接続方法

Windows 11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」をクリックしてください。

コンピューターの設定を調整します

表示方法: カテゴリ ▾



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」をクリックしてください。

コントロールパネル ホーム

アダプターの設定の変更

共有の詳細設定の変更
メディア ストリーミング オプション

基本ネットワーク情報の表示と接続のセットアップ

アクティブなネットワークの表示

識別されていないネットワーク
パブリック ネットワーク

アクセスの種類: インターネット アクセスなし
接続: イーサネット 3

ネットワーク設定の変更

 **新しい接続またはネットワークのセットアップ**
ブロードバンド、ダイヤルアップ、または VPN 接続をセットアップします。あるいは、ルーターまたはアクセス ポイントをセットアップします。

 **問題のトラブルシューティング**
ネットワークの問題を診断して修復します。または、トラブルシューティングに関する情報を入力します。

関連項目

Windows Defender ファイアウォール
インターネット オプション

3) 「イーサネット」アイコンをダブルクリックしてください。

※下の図のように、ご利用のアダプター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。

整理 ▾

 **VPN - VPN Client**
ネットワーク ケーブルが接続されていません
VPN Client Adapter - VPN

 **Wi-Fi**
接続されていません
Intel(R) Wi-Fi 6 AX201 160MHz

 **イーサネット 3**
識別されていないネットワーク
ASIX USB to Gigabit Ethernet Fam...

 **イーサネット 4**
無効

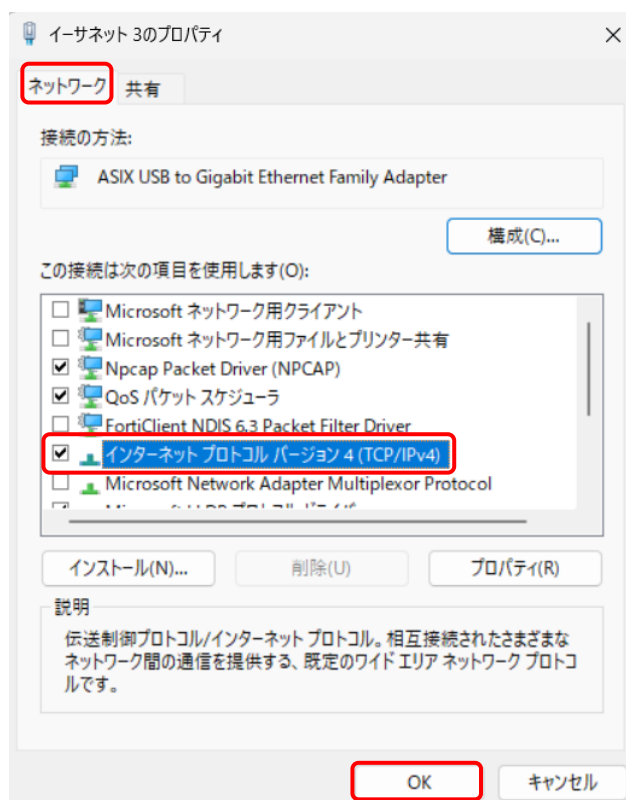
 **イーサネット 5**
無効

5 個の項目

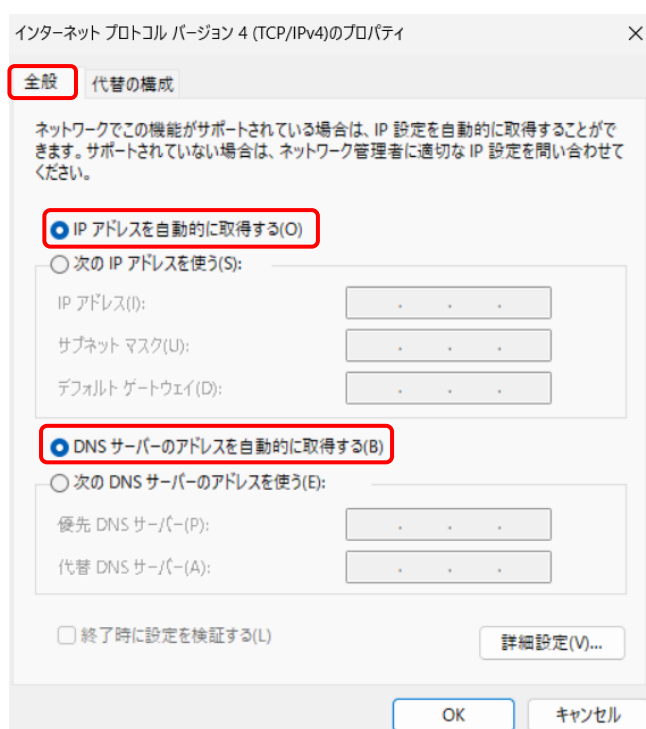
- 4) イーサネットの接続状態を確認します。
「全般」タブ → 「プロパティ」をクリックしてください。



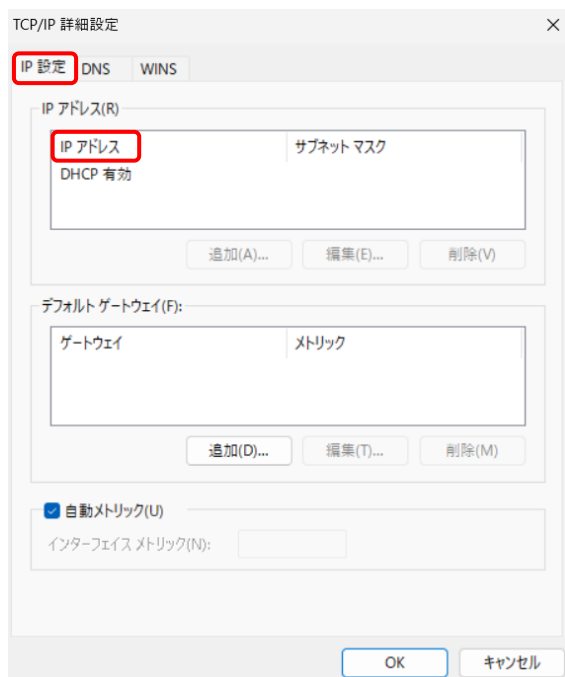
- 5) 「イーサネットのプロパティ」画面 → 「ネットワーク」タブ → 「インターネットプロトコルバージョン 4(TCP/IPv4)」を選択して、「プロパティ」をクリックしてください。



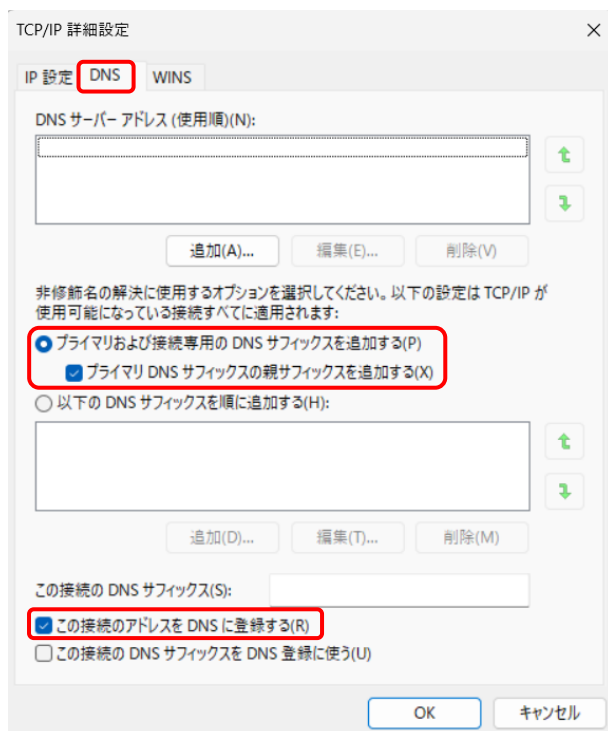
- 6) 「インターネットプロトコルバージョン 4(TCP/IPv4) のプロパティ」画面 → 「全般」タブ → 「[IP アドレスを自動的に取得する]および「DNS サーバのアドレスを自動的に取得する」に☑が入っていることを確認して、「詳細設定」をクリックしてください。



- 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てください。



- 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(P)」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(X)」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。

1.1.2. 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以降推奨
 - ・ MacOS 11 BigSir以降推奨

- 対応ブラウザ
 - ・ Microsoft Edge 84以降推奨
 - ・ Google Chrome 84以降推奨
 - ・ FireFox 78以降推奨
 - ・ Safari 13以降推奨

※最新の対応情報は、当社ホームページをご確認ください。

■ 2 章 WEB による設定 ■

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. WEB による設定方法

2.1.1. 本機へのログイン

お使いのウェブブラウザを開き、ブラウザのアドレスバーに本機のIPアドレスを入力してください。

工場出荷時のデフォルトアドレスは「192.168.1.1」です。

ブラウザの種類に応じて、標準のログインプロンプトが表示されます。

以下は、Windowsブラウザでのログイン画面を表示します。

☞ デフォルト設定のユーザ名およびパスワードは「admin」です。

ユーザ名とパスワードを入力後に<ログイン>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。



2.1.2. メイン画面

メイン画面の設定については、以下のとおりです。

本機にログインすると、RJ-45ポートおよびSFPポートのポートステータスの概要が表示されます。

メインメニュー上で、「System Config」→「System Homepage」をクリックすると、本画面に移動できます（詳細については、「[3.1.1 System Homepage \(システムのホームページ\)](#)」を参照してください）。

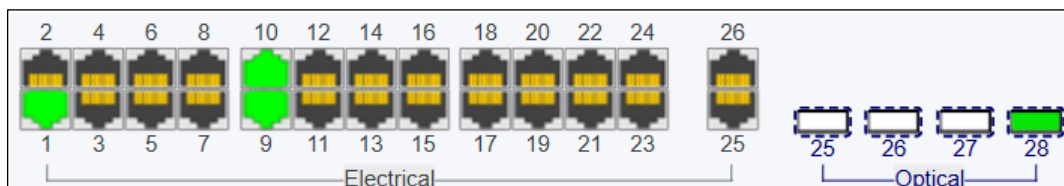
The screenshot shows the web management interface for the FXC5728 device. The main menu on the left includes System Config, Monitor Management, Switch Config, VLAN Config, DHCP Config, ACL Config, Ring Network, Route Config, Multicast, and QoS Config. The port status section at the top shows a row of 28 ports, with ports 1-24 labeled as Electrical and ports 25-28 as Optical. The 'Device Info' table shows Hostname: FXC5728, CPU MAC Address, IP Address: 192.168.11.201, Serial Num, Current System Time: Wed May 7 14:52:31 2025, Device Type: FXC5728, VLAN MAC Address, Uptime: 2W 2D 04H:37M:23S, Software Version: 1.0.0, and Firmware Compile Date: 2025-03-26 17:34:44. The 'Port Status' table shows the status of each port, including Admin Status, Config, Speed/Duplex, Actual, Flow Control, and MDI.

① メインメニュー

メインメニューの項目をクリックすると、④メインウィンドウの表示内容が切り替わります。
 (詳細については、「[2.1.3 メインメニューについて](#)」を参照してください)。

② ポートステータス

現在のポートステータスの概要を示します。 (緑:1G、橙:10/100M、黒:リンクダウン/未接続)



③ クイックアクション

このボタンでクイックアクションを行います。

Reboot	本製品を再起動します。
Save	本製品で実行中の設定を保存します。 保存せずに本製品を再起動すると、変更した設定は反映されず、以前に保存された設定に戻ります。
Logout	本製品のWeb GUI からログアウトします。

(Reboot/Save の詳細については、「[3.1.9.1 Device Reboot/Reset \(デバイスのリブート/リセット\)](#)」を参照してください)。

- ④ メインウィンドウ
メニューウィ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。
- ⑤ ステータス情報表示
各ページのメインウィンドウには、ステータス情報表示ウィンドウが表示されます。

No.	VLAN ID	VLAN Name
1	1	default
2	2	VLAN0002
3	3	VLAN0003
4	4	VLAN0004
5	5	VLAN0005
6	6	VLAN0006
7	7	VLAN0007
8	8	VLAN0008
9	9	VLAN0009
10	10	VLAN0010

Showing 10 Entries

Showing 1 to 10 of 15 entries

Search

First Previous 1 2 Next Last

表示するエントリ数を指定できます
(オプション: 全件 / 10 件 / 30 件 / 50 件 / 100 件、デフォルト: 10 件)

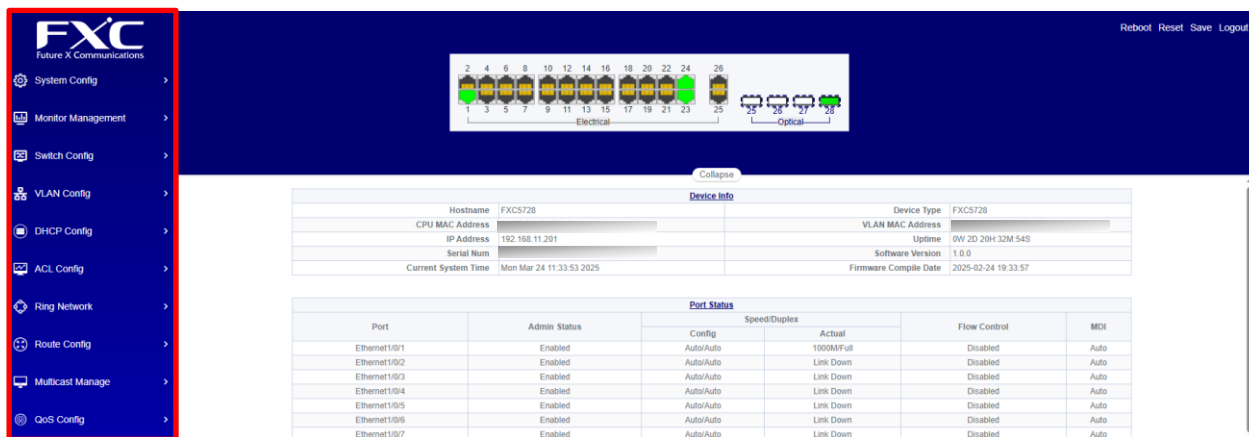
画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- 数字表記: 該当のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

2.1.3. メインメニューについて

メインメニューの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。

各メニューをクリックすると、それぞれのサブメニューが表示されます。



本機のメインメニュー画面は、以下のメニューで構成されています。

3.1 System Config(システム設定)	スイッチの基本的な設定(デバイス名、時間設定、管理者情報など)を管理します。
3.2 Monitor Management(モニター管理)	ネットワークの状態やパフォーマンスを監視するための機能(トラフィック、ポート状態など)。
3.3 Switch Config(スイッチの設定)	本機の基本設定や動作モードを管理します。
3.4 VLAN Config(VLAN設定)	仮想LANの作成や管理を行い、ネットワークを論理的に分割します。
3.5 DHCP Config(DHCP設定)	DHCPサーバやクライアントの設定を行い、IPアドレスの自動割り当てを管理します。
3.6 ACL Config(ACL設定)	アクセス制御リストを設定し、トラフィックの許可・拒否ルールを定義します。
3.7 Ring Network(リングネットワーク)	リングトポロジーのネットワーク構成や冗長性を管理します。
3.8 Route Config(ルート設定)	ルーティングテーブルの設定を行い、データパケットの経路を制御します。
3.9 Multicast Manage(マルチキャスト管理)	マルチキャスト通信の設定やグループ管理を行います。
3.10 QoS Config(QoS設定)	サービス品質(Quality of Service)を管理し、トラフィックの優先順位や帯域を調整します。

■ 3 章 各機能の設定 ■

3.1. System Config(システムの設定)

スイッチの基本的な設定(デバイス名、時間設定、管理者情報など)を管理します。
「System Config」メニューは、IP アドレス、タイムサーバ、ログ情報などのメニューで構成されています。

3.1.1. System Homepage (システムのホームページ)

本製品の基本情報(デバイス情報およびポートステータス)が表示されます。

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

Device Info	
Hostname	FXC5728
CPU MAC Address	[REDACTED]
IP Address	192.168.11.201
Serial Num	[REDACTED]
Current System Time	Mon Mar 24 11:52:54 2025
Device Type	FXC5728
VLAN MAC Address	[REDACTED]
Uptime	0W 2D 20H 51M 55S
Software Version	1.0.0
Firmware Compile Date	2025-02-24 19:33:57

Port	Admin Status	Speed/Duplex		Flow Control	MDI
		Config	Actual		
Ethernet1/0/1	Enabled	Auto/Auto	1000M/Full	Disabled	Auto
Ethernet1/0/2	Enabled	Auto/Auto	Link Down	Disabled	Auto
Ethernet1/0/3	Enabled	Auto/Auto	Link Down	Disabled	Auto

設定内容の詳細については、それぞれ下記を参照してください。

- 「Device Info」の詳細については、次項の「[3.1.2 Device Info\(デバイス情報\)](#)」にて参照して設定を行ってください。
- 「Port Status」メニューの詳細については、「[3.3.1 Port Config\(ポートの設定\)](#)」を参照して、各ポートに関する設定を行うことができます。

3.1.2. Device Info(デバイス情報)

デバイス情報の表示に加えて、デバイスのホスト名、連絡先、設置場所、および現在のシステム時刻を設定することもできます。

「System Config」→「Device Info」をクリックすると、以下の画面が表示されます。

Device Info

Hostname	FXC5728
Device Contact	Default
Device Location	Default
Device Type	FXC5728
CPU MAC Address	
VLAN MAC Address	
IP Address	
Client IP Address	
Serial Num	
Software Version	1.0.0
BootRom Version	V1.00
Firmware Compile Date	2025-02-24 19:33:57
Uptime	0W 2D 20H:53M:16S
Current System Time	11 Hour 54 Min 16 Sec 2025 Year 03 Month 24 Day

Apply

メニュー	説明
Hostname	変更するスイッチの新しいホスト名を表します (有効範囲:1 ~ 16 文字)。
Device Contact	管理者の連絡先情報を表します(0 ~ 32 文字)。
Device Location	変更するスイッチの新しいデバイスの場所(0 ~ 32 文字)
Device Type	デバイスの種類を表します。
CPU MAC Address	CPUのMACアドレスを表します。
VLAN MAC Address	VLANに関連するMACアドレスを表します。
IP Address	デバイスのIPアドレスを表します。
Client IP Address	接続されているクライアントのIPアドレスを表します。
Serial Num	デバイスのシリアル番号を表します。
Software Version	インストールされているソフトウェアのバージョンを表します。
BootRom Version	ブートローダーのバージョンを表します。
Firmware Compile Date	ファームウェアのコンパイル日時を表します。
Uptime	デバイスが稼働している時間を表します。
Current SystemTime	現在のシステム時刻を表します。 ※現在のシステム時間を手動で変更すると、スイッチを再起動時に無効になります。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定してください。

3.1.3. IP Config (IP 機能設定)

1 Ipv4 Config(IPv4 設定)

VLAN インターフェースの IP アドレスとサブネット マスクを設定できます。

「System Config」→「IP Config」→「IPv4 Config」をクリックすると、以下の画面が表示されます。

The screenshot shows the 'IPv4 Config' page. On the left is a navigation menu with 'IPv4 Config' selected. The main content area has a 'Collapse' button and the title 'IPv4 Config'. Below this is a form with the following fields:

- VLAN Interface: VLAN0001
- IP Mode: Static IP
- IP Address: 192.168.11.201 (Example: 10.10.10.1)
- Netmask: 255.255.255.0 (Example: 255.255.255.0)

There is an 'Apply' button below the form. Below the form is a table with the following data:

VLAN Interface	IP Mode	IP Address	Netmask
VLAN0001	Static IP	192.168.11.201	255.255.255.0

There are 'Delete' and 'Apply' buttons below the table. Navigation buttons 'First', 'Previous', '1', 'Next', 'Last' are also present.

メニュー	説明
VLAN Interface	VLAN インターフェースの VLAN IDを表します。
IP Mode	IPv4アドレスを取得または設定する方法を指定します。 ・Static IP: 手動で固定IPアドレスを入力して設定します。 ・Dynamic: DHCPサーバから自動的にIPアドレスを取得します。
IP Address	VLANのIP アドレスを表します(例: 10.10.10.1)。
Netmask	VLANのネットマスクを表します(例:255.255.255.0)。

- すべての項目を設定した後、<Apply>ボタンを押して変更を確定します。
- 既存の情報を削除する場合は、対象エントリに☑を入れて<Delete>ボタンをクリックしてください。

2 IPv6 Config(IPv6 設定)

VLAN インターフェースの IPv6 アドレスとサブネット マスクを設定できます。

「System Config」→「IP Config」→「IPv6 Config」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 Interface	VLANインターフェースの VLAN IDを表します。
IPv6 Address	IPv6 アドレスを表します(例:2001::1234)。
Prefix-length	プレフィックスの長さを表します(有効範囲: 3 ~ 127、デフォルト値:48)。

- すべての項目を設定した後、<Apply>ボタンを押して変更を確定してください。
- 既存の情報を削除する場合は、対象エントリに☑を入れて<Delete>ボタンをクリックしてください。

各画面で表示するエントリ数を指定できます

(オプション: 全件 / 10 件 / 30 件 / 50 件 / 100 件、デフォルト: 10 件)

画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

3.1.4. Web Config(WEB 設定)

1 Web Timeout(WEB のタイムアウト)

Web ログインのタイムアウト時間を設定できます。

「System Config」 → 「Web Timeout」 → 「Web Timeout」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
Login Timeout	Web ログイン タイムアウトを設定します (有効範囲:1 ~ 60 分、デフォルト値:10 分)。

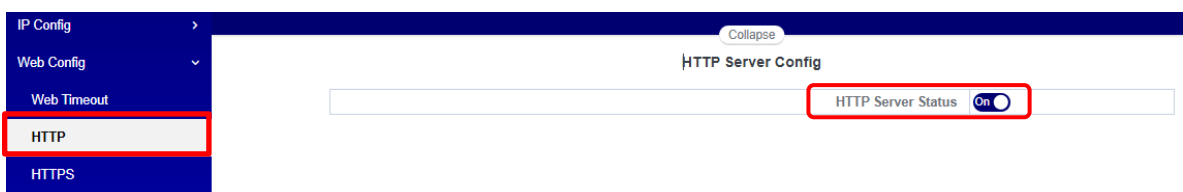
- 設定を変更した場合は、<Apply>ボタンをクリックして設定内容を確定してください。

2 HTTP

ネットワークスイッチの管理機能の一つとして提供される Webベースの管理インターフェース を実現します。HTTP (HyperText Transfer Protocol) を用いることで、管理者はスイッチにWebブラウザからアクセスし、GUIを介して設定や監視を行えます。

まず、本機の HTTP サービスを有効/無効に設定します(デフォルト:有効)。

「System Config」 → 「Web Timeout」 → 「HTTP」をクリックすると、以下の画面が表示されます。



- 設定を変更した場合は、<Apply>ボタンをクリックして設定内容を確定してください。
- 本設定を行うと、WEB 接続が一時的に切断される可能性があります。

3 HTTPS

本機の HTTPS サービスを有効/無効に設定します(デフォルト:有効)。

「System Config」→「Web Timeout」→「HTTPS」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
HTTPS Protocol Port	HTTPS通信に使用するポート番号を設定します (有効範囲: 1025-65535、デフォルト: 443)。
Encryption Type	暗号タイプを選択します(デフォルト設定: All)。 <ul style="list-style-type: none"> ・aes256-sha: HTTPSでクライアント(例えばブラウザ)とサーバ間の通信を保護するために使用される暗号を提供します。 ・ecdhe-rsa-aes256-sha: HTTPSで使用される暗号スイートで、より高度なセキュリティを提供します ・All: 利用可能なすべての暗号スイートを許可します。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定してください。
- 本設定を行うと WEB 接続が切断される可能性があります。

4 Security IP(セキュリティ IP)

ログイン時のセキュリティ IPv4 アドレス(信頼するIPアドレス)を設定できます。
ログイン方法には、Telnet/SSH/HTTP/HTTPS が含まれます。

「System Config」→「Web Timeout」→「Security IP」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
Security IP Address	指定のセキュリティIPv4アドレス(信頼するIPアドレス)を入力してください

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定してください。
- 本設定を行うと WEB 接続が切断される可能性があります。

5 ACL

IPv4 アクセス制御リストを設定できます。
Telnet/SSH/Webログインを介して、標準IP ACLプロトコルバインディングを設定します。

「System Config」→「Web Timeout」→「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
Access Control List	アクセスリストを指定します(有効範囲:1~64 文字、または番号:1~299)
Binding Method	バインディング方法は、Web/SSH/Telnet/All より選択します。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定してください。
- 本設定を行うと WEB 接続が切断される可能性があります。

3.1.5. User Management (ユーザマネジメント)

1 User Management (ユーザマネジメント)

ユーザ情報を追加または削除できます。

「System Config」→「User Management」→「User Management」をクリックすると、以下の画面が表示されます。

The screenshot shows the 'User Management' configuration page. On the left is a navigation menu with 'User Management' highlighted. The main content area includes:

- Form fields for Username (1-32 characters), Password (with an 'Encrypted Text' checkbox), and Priority (number 1-15). An 'Apply' button is below.
- A table with columns: No., Username, Password, State, Priority. One user 'admin' is listed with priority 15.
- A 'Delete' button below the table.
- 'WEB Privilege Config' section with 'Login Privilege Enable' (set to Disabled) and 'Privilege Priority' (set to 15). An 'Apply' button is below.

メニュー	説明
User Management	
Username	ユーザ名を入力します(有効範囲:1~32文字)。
Password	パスワードの設定および暗号化/暗号化なしを選択します(有効範囲:1~32文字)。 ※暗号化する場合は、 <input checked="" type="checkbox"/> を入れてください。
Priority	アクセスレベルを指定するために使用します(有効範囲:1~15)。
WEB Privilege Config	
Login Privilege Enable	ユーザの権限レベルが権限レベルのしきい値よりも低い場合、ウェブページにログインできません。設定を有効にするとログイン可能になります。 設定情報を変更することはできず、閲覧のみ可能です。 (デフォルト値:無効(ログイン不可))。
Privilege Priority	権限レベルを指定するために使用します (有効範囲: 1-15、デフォルトレベル: 15)。 このレベル以上のユーザのみがWeb経由でスイッチにログインできます。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定してください。
- <Delete>ボタンをクリックすると、そのポートの情報が削除されます。

2 Authentication Method (認証方式)

Console、VTY (Telnet/SSH)、Webインターフェースへのログイン時に、ログイン認証を設定できます。ログイン認証には、ローカル認証、Radius認証、TACACS+認証のいずれか単独、またはこれらを複数組み合わせた段階認証が利用可能です。

複数の認証方法を設定した場合、まず「認証方法1」として指定された認証が行われ、失敗した場合は次に「認証方法2」、さらに失敗した場合は「認証方法3」の順で認証が行われます。

いずれかの認証方法で認証が成功すると、それ以降の認証試行はスキップされます。

そして、いずれかの認証方法で認証に成功すれば、ユーザはログインできます。

【注記】:

Radius認証を使用する時は、AAA機能とRadiusサーバの設定が必要です。ローカル認証を設定した場合、ローカルユーザを設定していなくても、コンソール経由でスイッチにログインできます。

1. 「System Config」→「User Management」→「Authentication Method」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
Login Method	ログイン方法を選択することができます。 <ul style="list-style-type: none"> • Console: 直接接続(シリアルポート)経由でスイッチにログインします。 • Vty: 仮想端末(Telnet/SSH)経由でリモートログインします。 • Web: ブラウザ(HTTP/HTTPS)経由でGUI管理画面にログインします。
Authentication Method 1~3	認証方式を選択します。 <ul style="list-style-type: none"> • None: 認証なし。 • Local: ローカルに保存されたID/パスワードを使用します。 • Radius: Radiusサーバで認証します。 • Tacacs: TACACS+サーバで認証します。
Operation Type	操作方法を選択します。 <ul style="list-style-type: none"> • Configuration: 設定を適用します。 • Default: 設定をデフォルト設定に戻します。

2. コンソールの認証モードに「None」を選択した場合にのみ、ログイン時のパスワード認証を設定できます。

User Login Authentication Method Config

Login Method	Console	▼
Authentication Method1	None	▼
Authentication Method2	None	▼
Authentication Method3	None	▼
Operation Type	Configuration	▼

Apply

Login Method	Authentication Method1	Authentication Method2	Authentication Method3
console	None	None	None
vtv	Local	None	None
web	Local	None	None

Only when the console authentication mode is 'none', can the login authentication mode be configured.

Login Authentication	Disabled	▼
Login Authentication Password	Disabled	▼
	<input type="checkbox"/> Encrypted Text (Plain Text: 1 characters)	

Apply

メニュー	説明
Login Authentication	パスワード認証を有効/無効に設定します(デフォルト:無効)。
Login Authentication Password	認証用パスワードを設定します。 チェックを入れるとパスワード暗号化して保存します。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定してください。

3.1.6. Firmware Upgrade (ファームウェアアップデート)

1 HTTP Upgrade (HTTP アップグレード)

ファイルを選択して、HTTP 方式でファームウェアをアップグレードすることができます。

「System Config」→「Firmware Upgrade」→「HTTP Upgrade」をクリックすると、以下の画面が表示されます。

<Select File>ボタンをクリックして、アップグレード用の FWファイル(img ファイル)を選択してください。

Local Upgrade

Decompress the package and select the img file for upgrade.

2 TFTP Service (TFTP サービス)

ファイルをTFTP 方式でアップロードまたはダウンロードして、ファームウェアをアップグレードできます。

「System Config」→「Firmware Upgrade」→「TFTP Service」をクリックすると、以下の画面が表示されます。

TFTP Service

Server IP Address	<input type="text"/>	Example: 10.10.10.1
Server File Name	<input type="text"/>	1-100 characters, Example: nos.img
Operation Type	Upload	▼
Transmission Type	Binary	▼

メニュー	説明
Server IP Address	TFTPサーバのIPv4アドレスを表します(ドット区切り形式)。
Server File name	アップロードまたはダウンロードするファイル名を表します(1~100文字)。
Operation type	操作方法を選択します。 <ul style="list-style-type: none"> ・Upload: スイッチから TFTPサーバにアップグレード ファイルを転送します。 ・Download: TFTPサーバからスイッチにアップグレード ファイルを転送します。
Transmission type	ファイル転送の際に使用するデータ転送の形式を選択します。 <ul style="list-style-type: none"> ・binary: ファイルをバイナリ形式で転送します(デフォルト設定)。 ・ascii: ファイルをASCII形式で転送します。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定してください。

3 FTP Service (FTP サービス)

FTP 方式でファイルをアップロードまたはダウンロードして、ファームウェアをアップグレードします。

「System Config」→「Firmware Upgrade」→「FTP Service」をクリックすると、以下の画面が表示されます。

FTP Service

Server IP Address	<input type="text"/>	Example:10.10.10.1
Username	<input type="text"/>	1-100 characters
Password	<input type="text"/>	1-100 characters
Server File Name	<input type="text"/>	1-100 characters, Example: nos.img
Operation Type	Upload ▼	
Transmission Type	Binary ▼	

メニュー	説明
Server IP Address	FTPサーバのIPv4アドレスを表します(ドット区切り形式)。
Username	FTPサーバ間のユーザ名を設定します(有効範囲:1 ~ 100 文字)。
Password	FTPサーバ側ユーザのパスワードを設定します(有効範囲:1 ~ 100 文字)。
Server File name	アップロードまたはダウンロードするファイル名を設定します(1~100文字)。
Operation Type	操作方法を選択します。 <ul style="list-style-type: none"> ・ Upload:スイッチから FTPサーバにアップグレード ファイルをアップロードします。 ・ Download:FTPサーバからスイッチにアップグレード ファイルをダウンロードします。
Transmission Type	転送タイプを選択します。 <ul style="list-style-type: none"> ・ Binary:ファイルをバイナリ形式で転送します(デフォルト設定)。 ・ Ascii:ファイルをASCII形式で転送します。

- すべての項目を設定した後、<Apply>ボタンを押して変更を確定してください。

3.1.7. Management Config (マネジメントの設定)

1 TFTP

TFTP形式で本機の設定をインポートまたはエクスポートできます。

「System Config」→「Management Config」→「TFTP」をクリックすると、以下の画面が表示されます。

Import Configuration

Server IP Address	<input type="text"/>	Example: 10.10.10.1
Config File Name	<input type="text"/>	1-100 characters, Example: startup.cfg
Transmission Type	<input type="text" value="Binary"/>	

Export Configuration

Server IP Address	<input type="text"/>	Example: 10.10.10.1
File Type	<input type="text" value="Running Config"/>	

メニュー	説明
Import Configuration	
Server IP Address	TFTPサーバのIPv4アドレスを表します(ドット区切り形式)。
Config File Name	アップロードまたはダウンロードするファイル名を表します(1~100文字)。
Transmission type	転送方法を設定します。 <ul style="list-style-type: none"> ・Binary: ファイルをバイナリ形式で転送します(デフォルト設定)。 ・Ascii: ファイルをASCII形式で転送します。
Export Configuration	
Server IP Address	TFTPサーバのIPv4アドレスを表します(ドット区切り形式)。
File Type	ファイルタイプを選択します。 <ul style="list-style-type: none"> ・Running Config: 現在の動作中の設定ファイル(スイッチの現行設定)を表します。 ・Startup Config: 次回起動時に使用される設定ファイル(保存された初期設定)を指します。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定してください。

2 HTTP

HTTP 形式で本機の動作中の設定ファイル(Running Configuration) または、保存済みの設定ファイル(Startup Configuration)をダウンロードまたはアップロードできます。

「System Config」 → 「Management Config」 → 「HTTP」をクリックすると、以下の画面が表示されます。

HTTP Upload or Download File

Operation Type	Download ▼
File Type	Running Configuration ▼

Apply

メニュー	説明
Operation Type	操作方法を選択します。 ・Download: HTTP方式でスイッチから設定ファイルをダウンロードします。 ・Upload: HTTP方式でスイッチへ設定ファイルをアップロードします。
File Type	対象のファイルタイプを選択します。 ・Running Configuration: 現在の動作中の設定ファイル(スイッチの現行の設定)を表します。 ・Startup Configuration: 次回起動時に使用される設定ファイル(保存済みの設定)を表します。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定してください。

3.1.8. NTP

NTPは、ネットワーク上の時刻同期を行うためのプロトコルです。
本機の内部クロックを外部のNTPサーバと同期させることで、システムログやスケジュール機能の時刻が正確になります。

1 NTP Config (NTP 設定)

NTP サービスをグローバル設定で本機を操作することができます(デフォルト値:無効)。

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

NTP Global Config

NTP Global Config

NTP Server Config

Server Address	<input type="text"/>	IP address type, for example: 10.10.10.1
Version	<input type="text"/>	Version Range: 1-4 Default: 4
Key ID(optional)	<input type="text"/>	Key ID Range: 1-4294967295

Showing Entries Showing 1 to 1 of 1 entries Search

No.	Server Address	Version	Key ID
1	ntp.nict.jp	4	-

メニュー	説明
NTP Global config	NTP 機能を有効/無効に設定します。 ・Off: NTP機能を無効にします(デフォルト設定) ・On: NTP機能を有効にします。
NTP Server Config	
Server Address	指定されたNTPサーバのIPv4アドレスを表します(ドット区切り)。
Version	バージョン番号を設定します(有効範囲: 1 ~ 4、デフォルト: 4)。
Key ID(optional)	(オプション)秘密キーの値を設定します(有効範囲: 1 ~ 4294967295)。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定すると、テーブルの内容が更新されます。
- 既存のエントリの設定を削除する場合、対象の No を選択し、<Delete>ボタンを押してください。

各画面で表示するエントリ数をドラッグして設定できます
(オプション: 全件 / 10 件 / 30 件 / 50 件 / 100 件、デフォルト: 10 件)

画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

2 NTP Authentication Config (NTP 認証の設定)

本機の NTP 認証関連の設定を行うことができます。

「System Config」 → 「NTP」 → 「NTP Authentication Config」をクリックすると、以下の画面が表示されます。

NTP Authentication Config

NTP Authentication Function	Disabled
Key ID	<input type="text"/> Key ID Range:1-4294967295
MD5 For Key ID	<input type="text"/> 1-16 Characters

Apply

Showing Entries Showing 0 to 0 of 0 entries Search

No.	Key ID	MD5 For Key ID
0 results found.		

Delete **First** **Previous** **Next** **Last**

メニュー	説明
NTP Authentication Function	認証関連の設定を有効/無効に設定します。 ・Disable:NTP 認証を無効にします(デフォルト設定)。 ・Enable:NTP 認証を有効にします。
Key ID	秘密キーの値を表します(有効範囲: 1~4294967295)。
MD5 For Key ID	秘密鍵の MD5 値を表します(有効範囲:1~16)。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定すると、テーブルの内容が更新されます。
- 既存の情報を削除する場合は、対象エントリに☑を入れて<Delete>ボタンをクリックしてください。

各画面で表示するエントリ数をドラッグして設定できます
(オプション: 全件 / 10 件 / 30 件 / 50 件 / 100 件、デフォルト: 10 件)
画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

3.1.9. SNTP

1 Server Config (サーバの設定)

SNTPサーバ設定モジュールでは、指定したタイムサーバをクロックソースとして追加または削除できます。

「System Config」 → 「SNTP」 → 「Server Config」をクリックすると、以下の画面が表示されます。

SNTP Server Config

Server Address	<input type="text"/>	<small>IP address type, for example: 10.10.10.1</small>
Version	<input type="text"/>	<small>Version Range: 1-4</small>

<input type="checkbox"/>	No.	Server Address	Version	State

メニュー	説明
Server Address	指定されたタイムサーバのアドレスを入力します(ドット区切り)。
Version	バージョン番号を入力します(有効範囲 1~4、デフォルト値: 4)。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定してください。

2 Time Zone Config (タイムゾーンの設定)

SNTP はクライアントが配置されているタイムゾーンと UTC 時間差設定モジュールであり、スイッチの現在のタイムゾーンを設定して名前を付けることができます。

「System Config」 → 「SNTP」 → 「Time Zone Config」をクリックすると、以下の画面が表示されます。

Time Zone Config

Time Zone	JST	(1-16 character)
Time Difference	<input checked="" type="radio"/> After-utc <input type="radio"/> Before-utc	
Time Value	09	00 Range:0-23,0-59
Operation Type	Add	▼

Apply

メニュー	説明
Time zone	タイムゾーン名を表します(有効範囲:1~16文字)。
Time difference	タイムゾーンを選択します。 <ul style="list-style-type: none"> ・After-utc:協定世界時(UTC)より プラスの時間を設定する場合(例: UTC+9(日本標準時)) ・Before-utc:協定世界時(UTC)より マイナスの時間を設定する場合(例: UTC-5(アメリカ東部時間))
Time value	タイムゾーンの指定変更を時間単位で設定します(時間単位: 0~23)。 タイムゾーンの指定変更を分単位で設定します(分単位: 0~59)。
Operation Type	操作方法を選択します。 <ul style="list-style-type: none"> ・Add:指定された時間差をUTCに加算して現地時間を計算します。 ・Default:システムのデフォルトのタイムゾーンルールを適用します。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定してください。

3.1.10. Device Management (デバイスの管理)

1 Device Reboot/Reset (デバイスのリブート/リセット)

以下のボタンを使用して、本機のリブートおよび初期化、保存を行うことができます。

「System Config」 → 「Device Management」 → 「Device Reboot/Reset」をクリックすると、以下の画面が表示されます。

Device Management		
Reboot	Reboot	Reboot the switch.
Default	Reset	Restore factory configuration and reboot the switch.
Save	Save	Save current device configure.

- <Reboot>ボタン: 本機を再起動します。
- <Reset>ボタン: 本機の設定を初期化(工場出荷状態)して、再起動します。
- <Save>ボタン: 現在の設定内容を保存します。

2 System Utilization (システムの利用率)

現在のシステムのCPUリソース使用量とメモリリソース使用量を表示します。

「System Config」 → 「Device Management」 → 「System Utilization」をクリックすると、以下の画面が表示されます。

Show cpu usage

Last 5 second CPU usage	5%
Last 30 second CPU usage	6%
Last 1 minute CPU usage	6%
Last 5 minute CPU usage	6%
From running CPU usage	5%

Show memory usage

The memory total	128 MB
Free	64577536 Bytes
Usage	51.89%

□ Show cpu usage

短期間の負荷変動を確認でき、パフォーマンスのモニタリングに役立ちます。

- ✓ Last 5 Second CPU Usage: 直近5秒間のCPU使用率を示します。
- ✓ Last 30 Second CPU Usage: 直近30秒間のCPU使用率を示します。
- ✓ Last 1 minute CPU Usage: 直近1分間のCPU使用率を示します。
- ✓ Last 5 minute CPU Usage: 直近5分間のCPU使用率を示します。
- ✓ From running CPU Usage: 実行中のCPU使用率を示します。

□ Show Memory Usage

現在のシステムのメモリ使用量を表示します。

使用中メモリ、フリー(空き)メモリ、全体のメモリ容量を確認でき、リソース管理やパフォーマンス監視に役立ちます。

5 View Logging Flash (ログフラッシュの表示)

フラッシュメモリに保存されたログデータを表示します。
システムイベントやエラーの記録を確認でき、トラブルシューティングや監視に役立ちます。
デフォルトでは、警告度の高いログのみ保存されています。

「System Config」 → 「Device Management」 → 「View Logging Flash」をクリックすると、以下の画面が表示されます。

System Flash Log

```

Allowed max messages:655,Current messages:84
84 %Feb 24 09:01:38 2025 <critical> DEFAULT[zIMI]:System warm restart...
83 %Feb 24 00:00:00 2025 <critical> DEFAULT[tUsrRoot]:Switch is start, software version is 1.0.0
82 %Mar 21 15:00:27 2025 <critical> DEFAULT[zIMI]:System will be rebooted, reason: reload by CLI
81 %Mar 19 15:14:15 2025 <critical> MODULE_UTILS_FILESYSTEM[zIMI]:fs_write_file 1728: FS_DEV_UNLOCK Slot: 1 dev_name:flash: file_name:flash:/startup.cfg
80 %Mar 19 15:14:15 2025 <critical> MODULE_UTILS_FILESYSTEM[zIMI]:fs_write_file 1710: FS_DEV_LOCK_NO_WAIT Slot: 1 dev_name:flash: file_name:flash:/startup.cfg
79 %Feb 24 00:09:31 2025 <critical> MODULE_UTILS_FILESYSTEM[zIMI]:fs_write_file 1728: FS_DEV_UNLOCK Slot: 1 dev_name:flash: file_name:flash:/startup.cfg
78 %Feb 24 00:09:31 2025 <critical> MODULE_UTILS_FILESYSTEM[zIMI]:fs_write_file 1710: FS_DEV_LOCK_NO_WAIT Slot: 1 dev_name:flash: file_name:flash:/startup.cfg
77 %Feb 24 00:01:18 2025 <critical> DEFAULT[zIMI]:System warm restart...
76 %Feb 24 00:00:00 2025 <critical> DEFAULT[tUsrRoot]:Switch is start, software version is 1.0.0
75 %Feb 24 00:04:44 2025 <critical> DEFAULT[zIMI]:System will be rebooted, reason: reload by CLI
74 %Feb 24 00:01:18 2025 <critical> DEFAULT[zIMI]:System warm restart...
73 %Feb 24 00:00:00 2025 <critical> DEFAULT[tUsrRoot]:Switch is start, software version is 1.0.0
72 %Feb 24 00:02:49 2025 <critical> DEFAULT[zIMI]:System will be rebooted, reason: reload by CLI
71 %Feb 24 00:01:57 2025 <critical> MODULE_UTILS_FILESYSTEM[zIMI]:fs_write_file 1728: FS_DEV_UNLOCK Slot: 1 dev_name:flash: file_name:flash:/startup.cfg
70 %Feb 24 00:01:57 2025 <critical> MODULE_UTILS_FILESYSTEM[zIMI]:fs_write_file 1710: FS_DEV_LOCK_NO_WAIT Slot: 1 dev_name:flash: file_name:flash:/startup.cfg
69 %Feb 24 00:01:28 2025 <critical> MODULE_UTILS_FILESYSTEM[zIMI]:fs_write_file 1728: FS_DEV_UNLOCK Slot: 1 dev_name:flash: file_name:flash:/startup.cfg
68 %Feb 24 00:01:28 2025 <critical> MODULE_UTILS_FILESYSTEM[zIMI]:fs_write_file 1710: FS_DEV_LOCK_NO_WAIT Slot: 1 dev_name:flash: file_name:flash:/startup.cfg
67 %Feb 24 00:01:18 2025 <critical> DEFAULT[zIMI]:System warm restart...

```

3.2. Monitor Management (モニターの管理)

ネットワークの状態やパフォーマンスを監視するための機能(トラフィック、ポート状態など)。

3.2.1. SSH Config (SSH の設定)

SSH および接続タイムアウト時間を設定できます(デフォルト設定:有効)。

「Monitor Management」→「SSH Config」をクリックすると、以下の画面が表示されます。

SSH Config

Enabled

SSH Server Configuration

Timeout Time	180	(10-600s, Default:180s)
Maximum Connection Number	5	(1-16, Default:5)

メニュー	説明
SSH Config	
SSH Config	<ul style="list-style-type: none"> ・Off: SSHを無効にします。 ・On: SSHを有効にします(デフォルト設定)。
SSH Server Configuration	
Timeout Time	SSH 接続のタイムアウト時間を表します (10 ~ 600 秒、デフォルト値:180 秒)
Maximum Connection Number	SSH でログイン可能な接続数の上限を表します (有効範囲:1 ~ 16、デフォルト値:5)。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定してください。

3.2.2. Telnet Config (Telnet 設定)

Telnetおよび接続タイムアウト時間を設定できます。
デフォルト設定では、この機能は有効です。

「Monitor Management」 → 「Telnet Config」をクリックすると、以下の画面が表示されます。

Telnet Server State

Enabled

Maximum Connection

Telnet Connection Number

(1-16, Default:5)

メニュー	説明
Telnet Connection Number	Telnetで、ログイン可能な接続数の上限を設定します(有効範囲:1 ~ 16、デフォルト値:5)

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定してください。

3.2.3. Port Statistics (ポートの統計情報)

各ポートの送受信データやエラー状況を示す統計情報を表示します。

「Monitor Management」→「Port Statistics」をクリックすると、以下の画面が表示されます。

Port Statistics

<input type="checkbox"/>	PORT	Link Status	Rate(Bps) (R/T)	Rate(pps) (R/T)	unicast packets (R/T)	multicast packets (R/T)	broadcast packets (R/T)	input errors	output errors	CRC (R)	frame alignment (R)	overrun (R)	ignored (R)	abort (R)	length error (R)	undersize (R)	jabber (R)	fragments (R)	collisions (T)	late collisions (T)	pause frame (R/T)	
<input type="checkbox"/>	Ethernet1/0/1	Disconnect	0/0	0/0	0.0/0.0	0.0/0.0	0.0/0.0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0/0
<input type="checkbox"/>	Ethernet1/0/2	Connected	0/7737	0/13	0.0/139.0	0.0/411.0	0.0/1656.0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0/0
<input type="checkbox"/>	Ethernet1/0/3	Disconnect	0/0	0/0	0.0/0.0	0.0/0.0	0.0/0.0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0/0
<input type="checkbox"/>	Ethernet1/0/4	Disconnect	0/0	0/0	0.0/0.0	0.0/0.0	0.0/0.0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0/0
<input type="checkbox"/>	Ethernet1/0/5	Disconnect	0/0	0/0	0.0/0.0	0.0/0.0	0.0/0.0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0/0
<input type="checkbox"/>	Ethernet1/0/6	Disconnect	0/0	0/0	0.0/0.0	0.0/0.0	0.0/0.0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0/0
<input type="checkbox"/>	Ethernet1/0/7	Disconnect	0/0	0/0	0.0/0.0	0.0/0.0	0.0/0.0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0/0
<input type="checkbox"/>	Ethernet1/0/8	Connected	10185/6559	15/2	9637.0/7856.0	24608.0/2.0	87433.0/2.0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0/0
<input type="checkbox"/>	Ethernet1/0/9	Disconnect	0/0	0/0	0.0/0.0	0.0/0.0	0.0/0.0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0/0
<input type="checkbox"/>	Ethernet1/0/10	Disconnect	0/0	0/0	0.0/0.0	0.0/0.0	0.0/0.0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0/0
<input type="checkbox"/>	Port-Channel1	Disconnect	0/0	0/0	0.0/0.0	0.0/0.0	0.0/0.0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0/0

- 該当するポートを選択し、<Refresh>ボタンをクリックすると情報が最新のものに更新されます。
- 統計情報を削除する場合は、対象エントリに☑を入れて<Delete>ボタンをクリックしてください。
- 左上のチェックボックスに☑を入れると、すべてのポートを選択することができます。

メニュー	説明
PORT	対象のポート番号を表します。
Link Status	ポートの接続状態 (アップ/ダウン)を表します。
Rate(bps) (R/T)	送受信 (Receive/Transmit) のビットレートを表します (bps単位)。
Rate(pps) (R/T)	送受信の packets レートを表します (pps単位)。
Unicast packets(R/T)	送受信のユニキャストパケット数を表します。
multicast packets(R/T)	送受信のマルチキャストパケット数を表します。
brocast packets(R/T)	送受信のブロードキャストパケット数を表します。
Input errors	受信時のエラー数を表します。
output errors	送信時のエラー数を表します。
CRC(R)	受信時のCRC (巡回冗長検査) エラー数を表します。
frame alignment (R)	受信時のフレームアライメントエラー数を表します。
overrun (R)	受信時のオーバーランエラー数を表します
ignored (R)	受信時に無視されたパケット数を表します。
abort (R)	受信時の中断エラー数を表します。
length error (R)	受信時のパケット長エラー数を表します。
undersize (R)	受信時のアンダーサイズパケット数を表します。
jabber (R)	受信時のジャバパケット数を表します。
fragments (R)	受信時のフラグメントパケット数を表します。
collisions (T)	送信時のコリジョン数を表します。
late collisions (T)	送信時のレイトコリジョン数を表します。
pause frame (R/T)	送受信のポーズフレーム数を表します。

3.2.4. DDMI Status (DDMI ステータス)

DDMI (Digital Diagnostics Monitoring Interface) の状態を表示します。
SFPモジュールなどの光トランシーバーの動作状況 (温度、電圧、光出力など) を確認でき、障害検知やメンテナンスに役立ちます。

「Monitor Management」 → 「DDMI Status」をクリックすると、以下の画面が表示されます。

Fiber Module Table

Port	Vendor Name	Module Type	TX Power (dBm)	Send power reference value (dBm)	RX Power (dBm)	Received power reference value (dBm)	Temperature (°C)	Temperature reference value (°C)	Voltage (V)	Voltage reference value (V)	Bias (mA)	Current reference value (mA)
Ethernet1/0/25	FXC Inc.	MGB-LX	-5.18	Alarm(-11.50~-1.00) Warn(-10.50~-2.00)	-40.00(A-)	Alarm(-21.02~-2.00) Warn(-20.00~-3.00)	55	Alarm(-45~100) Warn(-40~95)	3.30	Alarm(2.80~3.80) Warn(2.97~3.60)	15.99	Alarm(0.10~80.00) Warn(0.50~70.00)
Ethernet1/0/26	FXC Inc.	MGB-SX	-7.54	Alarm(-12.00~-1.00) Warn(-11.00~-2.00)	-385.61(A-)	Alarm(-20.00~-1.00) Warn(-19.00~-0.00)	54	Alarm(-10~85) Warn(-5~80)	3.31	Alarm(2.90~3.60) Warn(3.00~3.50)	23.23	Alarm(0.50~50.00) Warn(1.00~40.00)
Ethernet1/0/27	FXC Inc.	MGB-SX	-5.99	Alarm(-11.50~-2.00) Warn(-10.50~-3.00)	-0.00(A-)	Alarm(-20.00~-2.00) Warn(-18.99~-3.00)	28	Alarm(-45~100) Warn(-40~95)	3.34	Alarm(2.80~3.80) Warn(2.97~3.60)	5.04	Alarm(0.10~25.00) Warn(0.50~20.00)
Ethernet1/0/28	FXC Inc.	MGB-LX	-6.51	Alarm(-11.50~-1.00) Warn(-10.50~-2.00)	-0.00(A-)	Alarm(-21.02~-2.00) Warn(-20.00~-3.00)	43	Alarm(-45~100) Warn(-40~95)	3.32	Alarm(2.80~3.80) Warn(2.97~3.60)	14.98	Alarm(0.10~80.00) Warn(0.50~70.00)

Refresh

項目	説明
Vendor Name	ファイバーモジュールを製造または提供したベンダを表します。
Port	モジュールが接続されているポート番号または識別子を表します。
Module Type	使用されているファイバーモジュールの種類を表します。
TX Power (dBm)	モジュールが送信する光信号の出力パワーを表します。
Send power reference value (dBm)	送信パワーの基準値を表します。
RX Power (dBm)	モジュールが受信する光信号の入力パワーを表します。
Received power reference value (dBm)	受信パワーの基準値を表します。
Temperature (°C)	モジュールの現在の動作温度を表します。
Temperature reference value (°C)	温度の基準値を表します。
Voltage (V)	現在の電圧値を表します。
Voltage Reference Value (V)	電圧の基準値を表します。
Bias (mA)	レーザーダイオードに流れるバイアス電流を表します。
Current Reference Value (mA)	バイアス電流の基準値を表します。

- 画面下の<Refresh>ボタンをクリックすると、全体の情報が最新のものに更新されます。

3.2.5. Ping

指定したホストのIPアドレスに対してPingを実行し、ネットワークの疎通性を確認します。応答時間やパケット損失率を表示し、接続性の診断やトラブルシューティングに役立ちます。

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

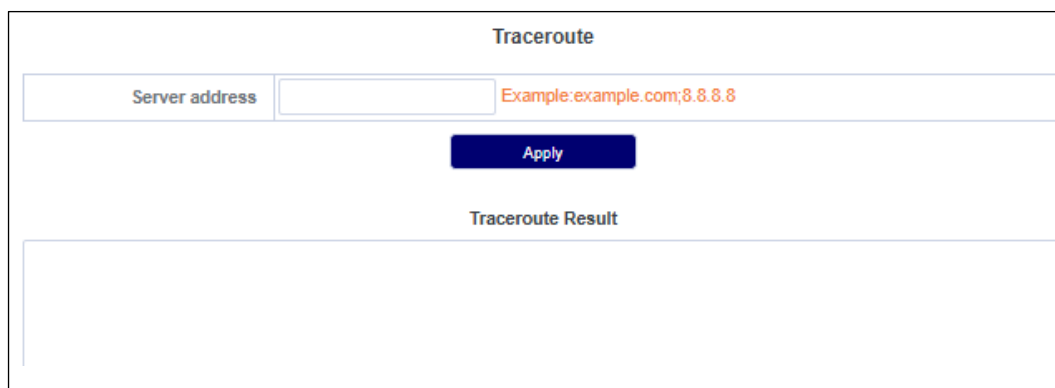


- IP アドレスを入力した後<Apply> ボタンをクリックすると、その結果が表示されます。

3.2.6. Traceroute (トレースルート)

Tracerouteを実行し、指定した宛先までのネットワーク経路を追跡します。各ホップのIPアドレスや応答時間を表示し、ルートの分析や障害箇所の特정에役立ちます。

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



- IP アドレスを入力後<Apply> ボタンをクリックすると、その結果が表示されます。

3.2.7. Cable Diagnostics (ケーブル診断)

ケーブルの状態を診断する機能を提供します。ケーブルの長さ、断線、短絡、インピーダンス異常などを検出し、物理層の問題を特定するのに役立ちます。

1. 「Monitor Management」 → 「Cable Diagnostics」をクリックすると、以下の画面が表示されます。

Cable Diagnostics

<input type="checkbox"/>	Port	Test Result	Description	Cable Length(meters)
<input type="checkbox"/>	Ethernet1/0/1	-	-	-
<input type="checkbox"/>	Ethernet1/0/2	-	-	-
<input type="checkbox"/>	Ethernet1/0/3	-	-	-
<input type="checkbox"/>	Ethernet1/0/4	-	-	-
<input type="checkbox"/>	Ethernet1/0/5	-	-	-
<input type="checkbox"/>	Ethernet1/0/6	-	-	-
<input type="checkbox"/>	Ethernet1/0/7	-	-	-
<input type="checkbox"/>	Ethernet1/0/8	-	-	-
<input type="checkbox"/>	Ethernet1/0/9	-	-	-
<input type="checkbox"/>	Ethernet1/0/10	-	-	-
<input type="checkbox"/>	Ethernet1/0/11	-	-	-

2. 該当するポートを選択して、画面下の<Start>ボタンをクリックすると診断が開始され、ケーブルのテスト結果と1対(芯線番号)ごとの長さが以下のように表示されます。

Cable Diagnostics

<input type="checkbox"/>	Port	Test Result	Description	Cable Length(meters)
<input type="checkbox"/>	Ethernet1/0/1	-	-	-
<input type="checkbox"/>	Ethernet1/0/2	-	-	-
<input type="checkbox"/>	Ethernet1/0/3	-	-	-
<input type="checkbox"/>	Ethernet1/0/4	-	-	-
<input type="checkbox"/>	Ethernet1/0/5	-	-	-
<input type="checkbox"/>	Ethernet1/0/6	-	-	-
<input type="checkbox"/>	Ethernet1/0/7	Normal	Normal(Correctly terminated pair)	(1, 2) 0 (3, 6) 0
<input type="checkbox"/>	Ethernet1/0/8	Disconnect	Please check whether the network cable is connected(Open pair,no link partner)	(1, 2) 11 (3, 6) 11 (4, 5) 12 (7, 8) 12
<input type="checkbox"/>	Ethernet1/0/9	Normal	Normal(Correctly terminated pair)	(1, 2) 11 (3, 6) 11 (4, 5) 11 (7, 8) 11

3.2.8. SNMP Config (SNMP 設定)

1 Global Config (グローバル設定)

SNMP 機能を有効/無効にできます(デフォルト設定:無効)。

1. 「Monitor Management」 → 「SNMP Config」 → 「Global Config」をクリックすると、以下の画面が表示されます。

「Agent State」メニューを有効 (Enabled) にして、RMON/Trap/Security IPの設定をそれぞれ有効/無効に選択することができます。

SNMP Management

Agent State	Enabled	▼
RMON	Disabled	▼
Trap	Disabled	▼
Security IP	Disabled	▼

Save

2 User Config (ユーザ設定)

SNMPを利用してネットワークデバイスを管理する際のユーザに関連する設定を行うことができます。

【注記】:

この機能を有効にするには、まずSNMPの「Agent Status」のメニューを有効にしてください(「3.2.8 SNMP Config」 → 「1 Global Config (グローバル設定)」を参照してください。)

「Monitor Management」 → 「SNMP Config」 → 「User Config」をクリックすると、以下の画面が表示されます。

Users

Username	<input type="text"/>	(1-32 characters)
Group Name	<input type="text"/>	(1-32 characters)
Security Level	noAuthNoPriv	▼
IPv4 Access Control List	noAuthNoPriv	(1-64 characters)
IPv6 Access Control List	authNoPriv	(1-64 characters)

Apply

User Config Status Table

Showing 10 Entries Showing 0 to 0 of 0 entries Search

<input type="checkbox"/>	Username	Group Name	Security Level	Authentication Protocol	Privacy Protocol	IPv4 Access Control List	IPv6 Access Control List
0 results found.							

Delete **First** **Previous** **Next** **Last**

メニュー	説明
Username	対象のユーザ名を設定します(有効範囲:1~32文字)。
Group Name	対象のユーザのグループ名を設定します(有効範囲:1~32文字)。
Security Level	使用するセキュリティレベルを選択します。 ・noAuthNoPriv:認証なし・暗号化なし ・authNoPriv:認証あり・暗号化なし ・authpriv:認証あり・暗号化あり
Authentication Protocol (認証あり選択時)	認証プロトコルを選択します。(ハッシュ関数:MD5/SHA)
Authentication Password (認証あり選択時)	認証パスワードを設定します。(有効範囲:8-32文字)
Privacy Protocol (暗号化あり選択時)	暗号化プロトコルを選択します。(暗号化方式:DES/AES/3DES)
Privacy Password (暗号化あり選択時)	暗号化パスワードを設定します。(有効範囲:8-32文字)
IPv4 access control list	標準 IPv4 アクセスリスト番号もしくはアクセスリスト名を入力します (有効範囲: 1 ~ 64 文字)。
IPv6 access control list	標準 IPv6 アクセスリスト番号もしくはアクセスリスト名を入力します (有効範囲: 1 ~ 64 文字)。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定してください。
- 既存の情報を削除する場合は、対象エントリに☑を入れて、<Delete>ボタンをクリックしてください。

3 Group Config (グループ設定)

SNMPv3エージェントにおいてユーザやエージェントのアクセス権限をグループ単位で管理することができます。

【注記】:

この機能を有効にするには、まずSNMPの「Agemt Status」のメニューを有効にしてください(「3.2.8 SNMP Config」→「1 Global Config (グローバル設定)」を参照してください)。

「Monitor Management」→「SNMP Config」→「Group Config」をクリックすると、以下の画面が表示されます。

Groups

Group Name	<input type="text"/>	(1-32 characters)
Security Level	noAuthNoPriv	▼
Read View	<input type="text"/>	(1-32 characters)
Write View	<input type="text"/>	(1-32 characters)
Notify View	<input type="text"/>	(1-32 characters)

Apply

Snm Group Table

Showing 10 Entries Showing 0 to 0 of 0 entries Search

<input type="checkbox"/>	Group Name	Security Level	Read View	Write View	Notify View
0 results found.					

Delete **First** **Previous** **Next** **Last**

メニュー	説明
Group Name	対象のユーザのグループ名を設定します(有効範囲:1~32 文字)。
Security level	使用するセキュリティレベルを選択します。 <ul style="list-style-type: none"> ・noAuthNoPriv:認証なし、暗号化なし ・authNoPriv:認証あり、暗号化なし ・Authpriv:認証あり、暗号化あり
Read SNMP view	読み取り可能なビューの名前を入力します(1~32 文字)。
Write SNMP view	書き込み可能なビューの名前を入力します(1~32 文字)。
Notify SNMP view	SNMPエージェントがトラップ(Trap)やインフォーム(Inform)といった通知を送信する際に、どの管理情報(MIBオブジェクト)を監視対象として含めるかを設定するビューを入力します(有効範囲:1~32 文字)。

- 各項目の設定後に<Apply>ボタンをクリックすると、設定内容が確定され、反映されます。
- 既存の情報を削除する場合は、対象エントリに☑を入れて<Delete>ボタンをクリックしてください。

各画面で表示するエントリ数をドラッグして設定できます
(オプション: 全件 / 10 件 / 30 件 / 50 件 / 100 件、デフォルト: 10 件)

画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

4 Community Config (コミュニティの設定)

SNMP コミュニティの管理が設定可能なコミュニティ管理情報を表示します。

【注記】:

この機能を有効にするには、まずSNMPの「Agemt Status」のメニューを有効にしてください(「3.2.8 SNMP Config」→「[1 Global Config \(グローバル設定\)](#)」を参照してください。)

「Monitor Management」→「SNMP Config」→「Community Config」をクリックすると、以下の画面が表示されます。

Community Managers

Community Name	<input type="text"/>	(1-255 characters)
Access Priority	<div style="border: 1px solid #ccc; padding: 2px;">Readonly ▼</div>	

Add

Community Managers Status Table

<input type="checkbox"/>	Community Name	Access Priority
--------------------------	----------------	-----------------

Delete

メニュー	説明
Community Name	コミュニティ文字列名を入力します(有効範囲:1~255文字)。
Access Priority	認証情報やアクセス権を選択します。 ・Read only:読み取り専用権限レベル ・Read-write:読み取りおよび書き込み権限レベル

- 各項目を設定した後、<Add>ボタンをクリックして設定内容を確定すると、内容が更新されます。
- 既存の情報を削除する場合は、対象エントリに☑を入れて<Delete>ボタンをクリックしてください。

5 Trap Config (トラップの設定)

SNMPエージェントが特定のイベント(例: デバイスの障害、状態変化など)が発生した際に、管理ステーションにトラップ(Trap)と呼ばれる非同期通知を送信します。

【注記】:

この機能を有効にするには、まずSNMPの「Agemt Status」のメニューを有効にしてください(「3.2.8 SNMP Config」→「[1 Global Config \(グローバル設定\)](#)」を参照してください。)

「Monitor Management」→「SNMP Config」→「Trap Config」をクリックすると、以下の画面が表示されます。

TRAP Manager Config

TRAP Receiver	<input type="text"/>	Example: 1.1.1.5
Version	V1	▼
Community Name	<input type="text"/>	▼

Add

TRAP Manager Status Table

Showing 10 Entries Showing 0 to 0 of 0 entries Search

<input type="checkbox"/>	TRAP Receiver	Community Name	Version	Security Level	Username
0 results found.					

First **Previous** **Next** **Last**

Delete

メニュー	説明
TRAP Manager Config	
TRAP Receiver	トラップ通知を受け取る管理ステーション(SNMPマネージャ)のIPアドレスを入力します。
Version	トラップ送信に使用するSNMPのバージョン(V1/V2c/V3)を選択します。
Community Name	NMPv1およびSNMPv2cで使用される認証用の文字列を選択します。
TRAP Manager Status Table	
Trap Receiver	トラップ情報の受信者のIPv4/IPv6アドレスを表示します。
Version	SNMPのバージョンを表示します。
Community Name (※ V1/V2c のみ)	コミュニティ名が表示されます。
Username (※ V3 のみ)	ユーザ名を表示します。(有効範囲: 1~24文字)
Security level (※ V3 のみ)	セキュリティレベルが表示されます。 <ul style="list-style-type: none"> ・noAuthNoPriv : 認証なし、暗号化なし ・authNoPriv: 認証あり、暗号化なし ・authpriv: 認証あり、暗号化あり

- 各項目を設定した後、<Add>ボタンをクリックして設定内容を確定すると、内容が更新されます。
- 既存の情報を削除する場合は、対象エントリに☑を入れて<Delete>ボタンをクリックしてください。

各画面で表示するエントリ数をドラッグして設定できます
(オプション: 全件 / 10 件 / 30 件 / 50 件 / 100 件、デフォルト: 10 件)
画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

6 View Config (表示の設定)

SNMP ビュー操作を追加または削除することができます。

【注記】:

この機能を有効にするには、まずSNMPの「Agemt Status」のメニューを有効にしてください(「3.2.8 SNMP Config」→「[1 Global Config \(グローバル設定\)](#)」を参照してください)。

「Monitor Management」→「SNMP Config」→「View Config」をクリックすると、以下の画面が表示されます。

Views

SNMP View	<input type="text" value=""/>	(1-32 characters)
OID	<input type="text" value=""/>	Example:1.3.6.1.2.1.1.1
Type	<input type="text" value="Include"/>	

メニュー	説明
SNMP view	操作するユーザビュー名を設定します(有効範囲:1~32文字)。
OID	OID 番号を設定します(10 進数の文字列)。 例) ・1.3.6.1.2.1.1: (システム情報全体: sysDescr, sysUpTimeなど)。 ・1.3.6.1.2.1.2: (インターフェース情報)。
Type:	アクセスタイプを選択します。 ・Include: OID を含めます(指定したOIDおよびそのサブツリーをビューに含め、アクセスを許可します)。 ・Exclude: OID を除外します(指定したOIDおよびそのサブツリーをビューから除外し、アクセスを禁止します)。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定すると、テーブルの内容が更新されます。

次に、画面下のビューテーブルにて、SNMPビューが表示されます。

View Table

Showing Entries Showing 1 to 3 of 3 entries Search

SNMP View	OID	Type
v1defaultviewname	1.0.	Include
v1defaultviewname	1.2.	Include
v1defaultviewname	1.3.	Include

SNMP EngineID Config

EngineID	<input type="text" value="18c384E5D8E1B547"/>	Example:18c30125fa
Operation Type	<input type="text" value="Config"/>	

Config
Default

メニュー	説明
EngineID	エンジン IDを表示します(16 進数、1 ~ 32 文字)。
Operation Type	操作方法を選択してます。 ・Configuration:セキュリティが重要な環境で、監視対象をシステム情報に限定し、他のデータへのアクセスを遮断します。 ・Default:小規模ネットワークで、特別な制限なくすべての基本情報を監視したい場合に使用します。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定してください。

各画面で表示するエントリ数をドラッグして設定できます
(オプション: 全件 / 10 件 / 30 件 / 50 件 / 100 件、デフォルト: 10 件)
画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

7 Security IP Config (セキュリティ IP の設定)

SNMP マネージャーの安全なIPv4/IPv6アドレスを追加または削除できます。
SNMPやネットワークデバイスの管理設定において、セキュリティを強化するために使用します。

【注記】:

この機能を有効にするには、まずSNMPの「Agemt Status」のメニューを有効にしてください(「3.2.8 SNMP Config」→「[1 Global Config \(グローバル設定\)](#)」を参照してください。)

「Monitor Management」→「SNMP Config」→「Security IP Config」をクリックすると、以下の画面が表示されます。

Manager Security IP Config

Security IP Address	<input type="text"/>	Example: 1.1.1.5
<input type="button" value="Apply"/>		
<input type="checkbox"/>	Security IP Address	
<input type="button" value="Delete"/>		

- 各項目の設定後に<Apply>ボタンをクリックすると、設定内容が確定され、反映されます。
- 既存の情報を削除する場合は、対象エントリに☑を入れて<Delete>ボタンをクリックしてください。

8 SNMP Statistics (SNMP 統計情報)

SNMPの統計情報を表示します。

送受信パケット数、エラー数、トラップ送信数などを確認でき、ネットワーク管理や監視の効率化に役立ちます。

【注記】:

この機能を有効にするには、まずSNMPの「Agent Status」のメニューを有効にしてください
(「3.2.8 SNMP Config」→「[1 Global Config \(グローバル設定\)](#)」を参照してください。)

「Monitor Management」→「SNMP Config」→「SNMP Statistics」をクリックすると、以下の画面が表示されます。

SNMP Statistics

SNMP packets input	0
Bad SNMP version errors	0
Unknown community name	0
Illegal operation for community name supplied	0
Encoding errors	0
Number of requested variables	0
Number of altered variables	0
Get-request PDUs	0
Get-next PDUs	0
Set-request PDUs	0
SNMP packets output	0
Too big errors (Max packet size 1500)	0
No such name errors	0
Bad values errors	0
General errors	0
Get-response PDUs	0
SNMP trap PDUs	0

Refresh

- 画面下の<Refresh>ボタンをクリックすると、全体の情報が最新のものに更新されます。

3.2.9. RMON Config (RMON 設定)

RMON (Remote Monitoring) の設定を行います。ネットワークトラフィックの統計情報収集、アラーム設定、イベント管理などを可能にし、詳細なモニタリングや異常検知に役立ちます。

【注記】:

この機能を有効にするには、まずSNMPの「Agent Status」および「RMON」を有効にしてください (「3.2.8 SNMP Config」→「[1 Global Config \(グローバル設定\)](#)」を参照してください)。

「Monitor Management」→「RMON Config」をクリックすると、以下の画面が表示されます。

1 RMON Statistics

RMONの機能の一部で、イーサネットなどのネットワークインターフェースにおけるトラフィックの統計データを収集します。これにより、ネットワーク管理者はリアルタイムでトラフィックの状態を把握し、問題の特定やパフォーマンスの最適化に役立てることができます。

「Monitor Management」→「RMON Config」→「RMON Statistics」をクリックすると、以下の画面が表示されます。

RMON Statistics

	Port	Drop Events	Octets	Packets	Received packets																
					Broadcast Packets	Multicast Packets	CRC Alignment Errors	Undersize Packets	Oversize Packets	Fragments Packets	Jabbers Packets	Collisions	1-64 Octets	65-127 Octets	128-255 Octets	256-511 Octets	512-1023 Octets	1024-1518 Octets			
<input type="checkbox"/>	Ethernet1/0/1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	Ethernet1/0/2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	Ethernet1/0/3	204	2885117	18881	65	372	0	0	0	0	0	0	0	29615	6071	750	666	901	24640	0	0
<input type="checkbox"/>	Ethernet1/0/4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	Ethernet1/0/5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	Ethernet1/0/6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	Ethernet1/0/7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	Ethernet1/0/8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	Ethernet1/0/9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	Ethernet1/0/10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	Ethernet1/0/11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

RMON Statistics Status

- Port: ID インデックスを表示します。
- Drop Event: リソース不足によりドロップされたパケットの総数。
- Octets: 受信したデータの総オクテット数。
- Packets: 受信したパケットの総数 (不良パケット、ブロードキャスト パケットを含む)。
- Broadcast Packets: ブロードキャスト アドレス宛ての正常な受信パケットの総数。
- Multicast Packets: マルチキャスト アドレス宛ての正常な受信パケットの総数。
- CRC Alignment Errors: 長さ (フレーミング ビットを除くが、FCS オクテットを含む) が 64 ~ 1518 オクテットの受信パケットの総数。
- Undersize Packets: 64 オクテット未満の受信パケットの総数。
- Oversize Packets: 1518 オクテットより大きい受信パケットの総数。
- Fragment: 無効な CRC で受信した、サイズが 64 オクテット未満のフレームの数。
- Jabbers Packets: 無効な CRC で受信された、サイズが 64 オクテットより大きいフレームの数。
- Collision.: Ethernet セグメントでの衝突の合計数の最良の推定値。
- 1-64 Byte: 長さが 64 オクテットの受信パケット (不良パケットを含む) の合計数。
- X~Y (65~127, 128~255, 256~511, 512~1023, 1024~1588): 長さが X オクテットと Y オクテットの間の受信パケットの合計数。

2 RMON History Config

RMONのHistoryグループ(RFC 2819のグループ2)を設定するためのメニューです。

この機能により、指定したポートのトラフィック統計を一定間隔でサンプリングし、履歴データとして保存できます。これにより、ネットワークのパフォーマンスやトラフィックのパターンを時間軸で追跡・分析することが可能になります。

「Monitor Management」→「RMON Config」→「RMON History Config」をクリックすると、以下の画面が表示されます。

RMON History Config

History ID	<input type="text" value=""/>	(1-65535)
Port	Ethernet1/0/1	
History Buckets	<input type="text" value=""/>	(1-65535, Default:50) <input type="checkbox"/> ?
History Interval	<input type="text" value=""/>	(1-3600, Default:1800) <input type="checkbox"/> ?
Owner	<input type="text" value=""/>	(1-31 characters) <input type="checkbox"/> ?

History Entry Table

<input type="checkbox"/>	History ID	Port	History Buckets	History Interval	Owner
--------------------------	------------	------	-----------------	------------------	-------

メニュー	説明
History ID	履歴エントリを一意に識別するための識別子を選択します (有効範囲:1-65535)。
Port	対象のポートを選択します。
History Buckets	履歴データとして保存するサンプル(パケット)数を設定します (有効範囲:1-65535、デフォルト値:50)。 ※ <input type="checkbox"/> を入れると、入力した値が反映されます。
History Interval	トラフィック統計を収集する時間間隔を設定します (有効範囲:1-3600、デフォルト値:1800)。 ※ <input type="checkbox"/> を入れると、入力した値が反映されます。
Owner	この履歴設定を作成または管理する所有者(管理者)の名前を設定します (有効範囲:1-31)。 ※ <input type="checkbox"/> を入れると、入力した値が反映されます。

3 RMON Event Config

RMONのEventグループ(RFC 2819のグループ9)を設定するためのメニューです。

この機能により、ネットワークの状態やトラフィックに関する特定の条件(例えば、トラフィック量が閾値を超えた場合など)を監視し、それに基づいてログの記録やトラップ(通知)の送信などのイベントを定義できます。

「Monitor Management」→「RMON Config」→「RMON Event Config」をクリックすると、以下の画面が表示されます。

RMON Event Config

Event ID	<input type="text" value=""/>	(1-65535)
Event Type	None	▼
Event Description	<input type="text" value=""/>	(1-127 characters) <input type="checkbox"/> ?
Owner	<input type="text" value=""/>	(1-31 characters) <input type="checkbox"/> ?

Add

Event Entry Table

<input type="checkbox"/>	Event ID	Event Type	Event Community	Event Description	Last Sent	Owner
0 results found.						

Delete

メニュー	説明
Event ID	イベントエントリを一意に識別するための識別子を入力します(1-65535)。
Event Type	イベントが発生したときに実行するアクションのタイプを設定します。 ・None: イベントが発生しても何もアクションを実行しません。 ・Log: イベントが発生した際に、その詳細をシステムログに記録します。 ・SNMP-Trap: イベントが発生した際に、SNMPを使用してトラップメッセージを送信します。 ・Log and Trap: 上記の「Log」と「SNMP-Trap」の両方を実行します。
Event Description	イベントの内容や目的を説明するテキストを入力します(1-127文字)。 ※☑を入れると、入力した値が反映されます。
Owner	このイベント設定を作成または管理する所有者(管理者)の名前を入力します(1-31文字)。 ※☑を入れると、入力した値が反映されます。

- 各項目を設定した後、<Add>ボタンをクリックして設定内容を確定すると、内容が更新されます。
- 既存の情報を削除する場合は、対象エントリに☑を入れて<Delete>ボタンをクリックしてください。

4 RMON Alarm Config

ネットワークの特定のパラメータ(トラフィック量、エラー率など)を監視し、異常が発生した際にアラームを生成するための設定です。サンプリング間隔や閾値を細かく調整することで、ネットワークの状態をリアルタイムで把握し、問題を早期に検知できます。

「Monitor Management」→「RMON Config」→「RMON Alarm Config」をクリックすると、以下の画面が表示されます。

RMON Alarm Config

Alarm ID	<input type="text" value=""/>	(1-65535)
Port	Ethernet1/0/1	▼
Sample Variable	Drop-Events	▼
Sample Interval	<input type="text" value=""/>	(1-2147483647s)
Sample Type	absolute	▼
Alarm Type	Rising	▼
Rising Threshold	<input type="text" value=""/>	(1-2147483647)
Rising Event	<input type="text" value=""/>	(1-65535)
Falling Threshold	<input type="text" value=""/>	(1-2147483647)
Falling Event	<input type="text" value=""/>	(1-65535)
Owner	<input type="text" value=""/>	(1-31 characters) <input type="checkbox"/> ?

Alarm Entry Table

<input type="checkbox"/>	Alarm ID	Port	Sample Variable	Sample Interval	Sample Type	Alarm Type	Rising Threshold	Rising Event	Falling Threshold	Falling Event	Owner
--------------------------	----------	------	-----------------	-----------------	-------------	------------	------------------	--------------	-------------------	---------------	-------

メニュー	説明
Alarm ID	アラームを識別するためのユニークなIDを入力します(有効範囲:1-65535)
Port	アラームが監視する対象のネットワークポートを選択します。
Sample Variable	監視対象の MIB 変数を指定します(MIB 変数の説明については、RMON 統計情報「 1 RMON Statistics 」を参照ください)。
Sample Interval	サンプリング間隔を選択します。指定した変数をどのくらいの頻度を(秒単位など)(有効範囲:1-2147483647秒)。
Sample Type	サンプリングの方法を指定します。 <ul style="list-style-type: none"> •absoul: 変数の絶対値(現在の値そのもの)を監視します。 •delta: 前回のサンプル値との差分(変化量)を監視します。ト
Alarm Type	アラームのトリガー条件を指定します。 <ul style="list-style-type: none"> •Rising: 監視値が指定した上限閾値(Rising Threshold)を超えたときにアラームを発生させます。 •Falling: 監視値が指定した下限閾値(Falling Threshold)を下回ったときにアラームを発生させます。 •Rising or Falling: 上限閾値を超えるか、下限閾値を下回るかのいずれかの場合にアラームを発生させます。
Rising Threshold	上限閾値を設定します。監視値がこの値を上回った場合に「Rising」アラームがトリガーされます(有効範囲:1-2147483647)。
Raing Event	「Rising」アラームが発生したときに実行されるイベント(有効範囲:1-65535)

Falling Threshold	下限閾値を設定します。監視値がこの値を下回った場合に「Falling」アラームがトリガーされます(有効範囲:1-2147483647)
Falling Event	「Falling」アラームが発生したときに実行されるイベントを指定します(有効範囲:1-65535)。
Ower	このアラーム設定を作成または管理するエンティティ(ユーザやシステム名など)を記録します(有効範囲:1-31)。 ※☑を入れると、入力した値が反映されます。

- 各項目を設定した後、<Add>ボタンをクリックして設定内容を確定すると、テーブルの内容が更新されます。

3.2.10. Camera-Detection (カメラ検出機能)

1 Server Config (サーバの設定)

Camera-Detection(カメラ検出)機能とは、ネットワーク上にあるIPベースのビデオ監視デバイス(カメラやNVRなど)を自動的に検出し、システムに統合する機能です。この機能により、監視システム全体を統一した設定で運用でき、管理者は効率的な制御を行うことが可能となります(デフォルト設定:有効)。

「Monitor Management」→「Camera-Detection」→「Server Config」をクリックすると、以下の画面が表示されます。

Server Config

Server Config

メニュー	説明
Server Config	サーバの設定を行います。 ・Off: 設定を無効します。 ・On: 設定を有効します(デフォルト設定)。

2 Detect Config (自動検出の設定)

本機に接続されたカメラを自動的に検出できます。
 Detect Config内で検知パケットを使用することにより、監視システムの状態を効率的に把握できます。

「Monitor Management」→「Camera-Detection」→「Detect Config」をクリックすると、以下の画面が表示されます。

Detect Config

Showing Entries Showing 0 to 0 of 0 Entries

	MAC Address	IP Address	Port	Model	Description	Location
0 results found.						

- <Send Packet>ボタンをクリックすると、検知パケットを送信して通信テストを行います。
- 既存の情報を削除する場合は、対象エントリに☑を入れて<Delete>ボタンをクリックしてください。

各画面で表示するエントリ数をドラッグして設定できます
 (オプション: 全件 / 10 件 / 30 件 / 50 件 / 100 件、デフォルト: 10 件)
 画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

3.2.11. Loopback Detection (ループバック検出)

1 Port Mode (ポートモード)

ループバックの検出は、ネットワーク内でデータがループするのを防ぎます。ポートごとのループ検出時の制御方法を設定します。ネットワークループ(データが無限に循環する状態)を検出し、自動的にポートを無効化するなどの対処を行うモードを指定できます。

「Monitor Management」→「Loopback Detection」→「Port Mode」をクリックすると、以下の画面が表示されます。

Port Mode

Port	--Please select --
Loopback-detection Mode	No ▼

Apply

Port	Loopback-detection Mode
Ethernet1/0/1	No
Ethernet1/0/2	No
Ethernet1/0/3	No
Ethernet1/0/4	No
Ethernet1/0/5	No
Ethernet1/0/6	No
Ethernet1/0/7	No

メニュー	説明
Port	対象のポート番号を選択します。 <input type="checkbox"/> Select All/Unselectに <input checked="" type="checkbox"/> を入れると、すべてのポートを選択、または解除することができます。
Loopback-detection mode	ループ検知時の動作を選択することができます。 ・Shutdown: ポートを無効にします。 ・block : ポートをブロックします。 ・No: ポートのループ検出を無効にします。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定すると、テーブルの内容が更新されます。

2 VLAN Loopback(VLAN ループバック)

VLAN単位でのループ検出機能を有効/無効に設定します。特定のVLAN内でネットワークループが発生した場合に検知し、自動的にトラフィックを制限するなどの対処を行います。

「Monitor Management」→「Loopback Detection」→「VLAN Loopback」をクリックすると、以下の画面が表示されます。

VLAN Loopback

Port	--Please select--
VLAN List	<input type="text"/> (1-4094, for example: 1,3-6)
Apply	

Port	VLAN List
Ethernet1/0/1	
Ethernet1/0/2	
Ethernet1/0/3	
Ethernet1/0/4	
Ethernet1/0/5	
Ethernet1/0/6	
Ethernet1/0/7	
Ethernet1/0/8	
Ethernet1/0/9	
Ethernet1/0/10	
Ethernet1/0/11	

メニュー	説明
Port	対象のポート番号を選択します。 <input type="checkbox"/> Select All/Unselectに <input checked="" type="checkbox"/> を入れると、すべてのポートを選択、または解除することができます。
VLAN List	ループ検出フレームを送信するVLAN IDを指定します(値の有効範囲: 1-4094)。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定すると、テーブルの内容が更新されます。

3 Interval Time(インターバルタイム)

ループ検出フレームの間隔を設定できます。

「Monitor Management」→「Loopback Detection」→「Interval Time」をクリックすると、以下の画面が表示されます。

Interval Time

Loopback-detection Interval Time	<input type="text" value="5"/>	(5-300s, Default:5s)
No Loopback-detection Interval Time	<input type="text" value="3"/>	(1-30s, Default:3s)

メニュー	説明
Loopback-detection interval time	ループからの復旧後の送信開始までのインターバルを表します (値の有効範囲:5 ~ 300 秒、デフォルト:5秒)
No Loopback-detection interval time	ループ検知フレームの送信間隔を表します。 (値の有効範囲:1 ~ 30 秒、デフォルト値:3秒)。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定してください。

4 Recovery Timeout(リカバリタイムアウト)

ループ状態が解消された後にポートを自動的に復旧させるまでの待機時間を設定することができます。

「Monitor Management」→「Loopback Detection」→「Recovery Timeout」をクリックすると、以下の画面が表示されます。

Recovery Timeout

Recovery Switch Timeout	<input type="text" value="600"/>	(0-3600s, Default:600s)
-------------------------	----------------------------------	-------------------------

メニュー	説明
Recovery switch timeout	ループによりポートが無効またはブロックされた場合、自動的にポートを復旧するまでの時間を表します(値の有効範囲:0~3600秒、デフォルト値:600秒)。 【注記】: 「0」に設定すると、自動リカバリ機能は無効になります。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定してください。

3.2.12. LLDP Config (LLDP 設定)

1 Global Config (グローバル設定)

LLDP 機能をグローバルで有効/無効に設定します。

Updateメッセージの送信間隔、メッセージのエージング時間乗数値、Updateメッセージの送信遅延時間、Trapメッセージの送信間隔を設定することができます(デフォルト設定:無効)。

「Monitor Management」→「LLDP Config」→「Global Config」をクリックすると、以下の画面が表示されます。

Global Config

This page is used to configure global properties of the LLDP function

Status	Disabled	(5-32768),Default:30
Hello Message Sending Time	30	(5-32768),Default:30
Aging Multiple	4	(2-10),Default:4
Delay Time	2	(1-8192),Default:2
Trap Interval	5	(5-3600),Default:5
Operation Type	Apply	

Apply

メニュー	説明
Status(lldp enable)	LLDPのステータスを表示します。 <ul style="list-style-type: none"> ・Enable: LLDP 機能をグローバル設定で有効にします。 ・Disable: LLDP 機能をグローバル設定で無効にします(デフォルト設定)。
Hello Message Sending Time	LLDPメッセージ(Hello)の送信間隔を表します(有効範囲:5 ~ 32768 秒、デフォルト値:30 秒)。
Aging Multiple	LLDPの情報保持時間を表します(値の有効範囲:2 ~ 10、デフォルト値 4)。
Delay Time	LLDPメッセージ送信の遅延時間を表します(値の有効範囲:1 ~ 8192 秒、デフォルト値:2)
Trap Interval	LLDPトラップ(通知)の送信間隔を表します(値の有効範囲:5 ~ 3600 秒、デフォルト値:5)。
Operation Type	LLDPの動作モードを選択します。 <ul style="list-style-type: none"> ・Apply: ユーザによる設定 ・Default: デフォルト値に戻します。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定してください。

2 Port Config(ポート設定)

LLDP ポート機能を有効/無効にできるように設定できます。

「Monitor Management」→「LLDP Config」→「Port Config」をクリックすると、以下の画面が表示されます。

Trust Config

This page is used to set port attributes for the LLDP function

Port	--Please select --				
LLDP Enable	Enabled ▼				
Trap Enable	Disabled ▼				
Agent State	both ▼				
Operation Type ?	Discard ▼				
Entry Max ?	100	(5-500,Default:100)			

Apply

Port	LLDP Enable	Trap Enable	Agent State	Operation Type	Entry Max
Ethernet1/0/1	Enabled	Disabled	Both	Discard	100
Ethernet1/0/2	Enabled	Disabled	Both	Discard	100
Ethernet1/0/3	Enabled	Disabled	Both	Discard	100
Ethernet1/0/4	Enabled	Disabled	Both	Discard	100
Ethernet1/0/5	Enabled	Disabled	Both	Discard	100
Ethernet1/0/6	Enabled	Disabled	Both	Discard	100
Ethernet1/0/7	Enabled	Disabled	Both	Discard	100
Ethernet1/0/8	Enabled	Disabled	Both	Discard	100
Ethernet1/0/9	Enabled	Disabled	Both	Discard	100

メニュー	説明
Port	対象のポート番号を選択します。
LLDP Enable	ポートごとのLLDP 機能を有効/無効に設定します。(デフォルト値: Enabled)。
Trap Enable	ポートごとのLLDPトラップ(通知)を有効/無効に設定します(デフォルト値: Disabled)。
Agent State	LLDPエージェントの動作を選択します。 (send / receive / both / disable、デフォルト値: both)
Operation Type	ネイバーの数が最大数を超えた場合のデバイスの動作を表します <ul style="list-style-type: none"> ・Discard : 新しいネイバー情報を破棄します。 ・Delete : LLDPネイバーテーブル内の情報保持時間(残り時間)が最も短いネイバー情報を削除し、新しいネイバー情報を追加します。
Entry Max	ポートが保持できる近隣デバイスの最大数を表します(値の有効範囲: 5-500、デフォルト値:100)。

- 各項目の設定後に<Apply>ボタンをクリックすると、設定内容が確定され、反映されます。

3 TLV Config(TLV の設定)

TLV(Type-Length-Value)ベースのデータを管理・編集します。
 ポートのTLV プロパティの設定手順について説明します。

「Monitor Management」→「LLDP Config」→「TLV Config」をクリックすると、以下の画面が表示されます。

TLV Config

This page is used to set the properties of TLV

Port	<input type="text" value="--Please select --"/>	
TLV Config	<input type="text" value="--Please select --"/>	
IP Address	<input type="text" value="0.0.0.0"/>	Example:10.10.10.1 (0.0.0.0 is considered as not setting management address)

Port	TLV Config
Ethernet1/0/1	
Ethernet1/0/2	
Ethernet1/0/3	
Ethernet1/0/4	
Ethernet1/0/5	
Ethernet1/0/6	
Ethernet1/0/7	

メニュー	説明
Port	対象のポート番号を選択します。 <input type="checkbox"/> Select All/Unselectに☑を入れると、すべてのポートを選択、または解除することができます。
TLV Config	ポート情報を選択します。 ・Select All/Unselect:送信する全TLVフィールドの選択/解除を切り替えます。 ・Port Description:ポートを記述する文字列を設定します。 ・System Capability:機器の役割を設定します。 ・System Description:機器の詳細を設定します。 ・System Name:機器のホスト名を設定します。
IP Address	管理アドレスTLVを設定し、デバイスの管理用IPアドレスを設定します。 例:10.10.10.1 (※0.0.0.0は管理アドレスが未設定であるとみなされます)

- 各項目の設定後に<Apply>ボタンをクリックすると、設定内容が確定され、反映されます。

4 Neighbor Info(ネイバー情報)

LLDPや類似プロトコルでネイバー情報を表示します。

「Monitor Management」→「LLDP Config」→「Neighbor Info」をクリックすると、以下の画面が表示されます。

Neighbor Info

This page is used to view information about other neighbors

Neighbor Table

Showing Entries Showing 0 to 0 of 0 entries Search

Number	Local Port	Neighbor Device Name	Neighbor Interface	Neighbor Interface Description	Neighbor MAC	Neighbor IP	System Description
0 results found.							

各画面で表示するエントリ数をドラッグして設定できます
(オプション: 全件 / 10件 / 30件 / 50件 / 100件、デフォルト: 10件)

画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

3.3. Switch Config(スイッチの設定)

本機の基本設定や動作モードを管理します。

3.3.1. Port Config(ポートの設定)

1 Port Config(ポートの設定)

ポートの基本設定を行います。

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

Port Config

This page is used to configure basic port parameters.

Ports	Ethernet1/0/1 ▼					
Description	<input type="text" value=""/> (1-200 character) <input type="checkbox"/> ?					
Admin Status	Enabled ▼					
Speed	Auto ▼ ?					
Duplex	Auto ▼					
Flow Control	Disabled ▼ ?					
MDI	auto ▼ ?					

Apply

Port	Description	Admin Status	Speed/Duplex		Flow Control	MDI
			Config	Actual		
Ethernet1/0/1		Enabled	Auto/Auto	1000M/Full	Disabled	auto
Ethernet1/0/2		Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/3		Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/4		Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/5		Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/6		Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/7		Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/8		Enabled	Auto/Auto	Link Down	Disabled	auto

メニュー	説明
Ports	対象のポート番号を選択します。
Description	ポートの役割や接続先の説明を入力します(値の有効範囲: 1 ~ 200)。※この設定を反映させるには、☑を入れてください。
Admin status	ポートの有効/無効を選択します。
Speed	Speed:ポートの動作速度を選択します。 <ul style="list-style-type: none"> ・auto: オートネゴシエーション ・10M: 10Mbps ・100M: 100Mbps ・1000M: 1000Mbps
Duplex	通信モードを選択します(Auto/ Half/Full)。
Flow Control	フローコントロールの有効/無効を選択します。
MDI	ケーブル接続方式を選択します(Mdi: auto/across/normal (デフォルト値: auto))。

2 Port Combo Mode(FXC5728 のみ)

コンボのポートでRJ45/SFPを切り替えることができます。
RJ45/SFPコンボポートの基本を設定するために使用されます。

「Switch Config」 → 「Port Config」 → 「Port Combo Mode」をクリックすると、以下の画面が表示されます。

Port Combo Mode

This page is used to configure port Combo mode.

	Ports	Ethernet1/0/25 ▼
	Port Combo Mode	copper ▼

Apply

Ports	Port Combo Mode
Ethernet1/0/25	sfp-preferred-auto
Ethernet1/0/26	sfp-preferred-auto

メニュー	説明
Ports	対象の物理ポート番号を選択します。
Port Combo Mode	対象のポートタイプを選択することができます。 <ul style="list-style-type: none"> ・copper: RJ45ポートを選択します。 ・fiber: SFPポートを選択します。 ・sfp-preferred-auto: 自動的に選択されます(※光ファイバー接続が優先されます)。

3.3.2. Port Mirror(ポートのミラーリング)

ポートのミラーリング機能を設定します。

「Switch Config」→「Port Mirror」をクリックすると、以下の画面が表示されます。

Port Mirror

This page is used to configure port mirror.

Session ID	1
Destination Port	Ethernet1/0/1
Source Port	--Please select --
CPU Source	Disabled
Access List	(1-7999)
Mirror Direction	Rx

Apply

Port Mirror Table

	Session ID	Destination Port	Source Port		Access List
			Tx	Rx	
<input type="checkbox"/>	1				
<input type="checkbox"/>	2				
<input type="checkbox"/>	3				
<input type="checkbox"/>	4				

Delete

メニュー	説明
Session	セッションIDを選択します(1~4)。
Destination port	ミラーリングされたトラフィックが送信されるポートを選択します。
Source port	トラフィックを監視(ミラーリング)する対象となるポートを設定します。
CPU Source	CPUが処理するトラフィックをミラーリングする設定します(デフォルト値:Disabled)。
Access list	ミラーリングするトラフィックをフィルタリングするためのルールを設定します(有効範囲:1~7999)。
Mirror Direction	トラフィックの監視方向を指定します。 ・Both: 送信と受信の両方のトラフィックをフィルタリングします。 ・Rx: 受信トラフィックのみをフィルタリングします(デフォルト設定)。 ・Tx: 送信トラフィックのみをフィルタリングします。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定してください。
- 既存の情報を削除する場合は、対象エントリに☑を入れて<Delete>ボタンをクリックしてください。

3.3.3. Port Isolate(ポートの隔離)

隔離ポート同士の通信を制限することができます。
この機能により、同じスイッチ内で隔離ポート間の通信を防ぎセキュリティやトラフィックの制御ができます。

「Switch Config」→「Port Isolate」をクリックすると、以下の画面が表示されます。

Port Isolation Config

This page is used to configure port isolate.

Isolate-Port Group Name	<input type="text"/>	(1-32 character)
Isolation Ports	--Please select--	
VLAN	<input type="text"/>	(1-4094, for example: 8,default not create in vlan)

Add

Port Isolation Table

<input type="checkbox"/>	VLAN	Isolate-Port Group Name	Isolation Ports
--------------------------	-------------	--------------------------------	------------------------

Delete

メニュー	説明
Isolate-Port Group Name	ポートの隔離を設定するためのグループ名を表します (値の有効範囲: 1 ~ 32 文字)
Isolation Ports	隔離対象となるポートのリストを選択します <input type="checkbox"/> Select All/Unselectに <input checked="" type="checkbox"/> を入れると、すべてのポートを選択、または解除することができます。
VLAN	該当する隔離ポートグループに関連付けられた VLAN IDを選択できます。

- 各項目の設定後に<Apply>ボタンをクリックすると、設定内容が確定され、反映されます。
- 既存の情報を削除する場合は、対象エントリにを入れて<Delete>ボタンをクリックしてください。

3.3.4. Port Channel(リンクアグリゲーション)

1 Port Channel Group(チャンネルグループ設定(LAG))

リンクアグリゲーショングループ(LAG)を設定することができます。

「Switch Config」→「Port Channel」→「Port Channel Group」をクリックすると、以下の画面が表示されます。

Port Channel

This page is used to configure port channel.

Load Balance Algorithm src-mac ▼

Apply

LAG (1-8)

Name (1-200 character)

Mode ▼

State ▼

Member Port

Apply

Port Channel Table

<input type="checkbox"/>	LAG	Name	Mode	State	Ports	Load Balance Algorithm
Delete						

メニュー	説明
Load Balance Algorithm	トラフィックをどの基準で物理リンクに割り当てるかを選択することができます。 <ul style="list-style-type: none"> ・src-mac: 送信元 MAC に応じて負荷分散を実行します。 ・dst-mac: 宛先 MAC に応じて負荷分散を実行します。 ・dst-src-mac : 宛先及び送信元 MAC に応じて負荷分散を実行します。 ・src-ip : 送信元 IP に応じて負荷分散を実行します。 ・dst-ip : 宛先 IP に応じて負荷分散を実行します。 ・dst-src-ip : 宛先及び送信元 IP に応じて負荷分散を実行します。 ・dst-src-mac-ip : 宛先および送信元 MAC とIPに応じた負荷分散を実行します。 ・ingress-port: 入力ポートに応じた負荷分散を実行します。
LAG	LAG番号を作成します(値の有効範囲: 1 ~ 8)。
Name	LAG の名前を設定します(値の有効範囲: 1 ~ 200文字)
mode	Static/LACPモードを選択します。 <ul style="list-style-type: none"> ・On : Staticでポート チャンネルに設定します。(LACP無効) ・Active : LACP を有効にし、アクティブモードに設定します。 ・Passive: LACPを有効にし、パッシブモードに設定します。
State	機能を有効/無効に設定します。 <ul style="list-style-type: none"> ・Enabled: 有効にします。 ・Disabled: 無効にします。
Member Port	対象の物理ポート番号を選択します。 <input type="checkbox"/> Select All/Unselectに <input checked="" type="checkbox"/> を入れると、すべてのポートを選択、または解除することができます。

- 各項目の設定後に<Apply>ボタンをクリックすると、設定内容が確定され、反映されます。
- 既存の情報を削除する場合は、対象エントリにを入れて<Delete>ボタンをクリックしてください

2 LACP

システムの優先度とポートの優先度を設定できます。

LACPIにおいて有効(Active)となるのは8ポートまでで、それ以上9ポート目～は予備ポート(Stanby)となります。Port Priorityで有効となるポートの優先度を設定できます。

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

LACP

This page is used to configure port channel LACP.

System Priority	<input type="text" value="32768"/>	(0-65535, default 32768)
<input type="button" value="Apply"/>		

Port	--Please select--
Port Priority	<input type="text" value=""/> (0-65535, default 32768)
Timeout	<input type="text" value="long"/>
<input type="button" value="Apply"/>	

Flags: A -- LACP_Activity, B -- LACP_timeout, C -- Aggregation, D -- Synchronization, E -- Collecting, F -- Distributing, G -- Defaulted, H -- Expired

LACP Port Setting Table

<input type="checkbox"/>	Port	Status	Port Priority	FLAG ?
<input type="button" value="Delete"/>				

メニュー	説明
System Priority	LACPを動作させるデバイス全体の優先度 (値の有効範囲:0-65535、デフォルト値:32768)
Port	LAGグループに追加するポート番号を選択します。
port priority	デバイス内の各物理ポートの優先度を選択します (値の有効範囲:0-65535、デフォルト値:32768)。
Timeout	LACPDUを送受信する間隔を設定します <ul style="list-style-type: none"> ・Long: 30秒ごとに送信します。(タイムアウトは90秒) ・short:1秒ごとに送信します。(タイムアウトは3秒)

- 各項目の設定後に<Apply>ボタンをクリックすると、設定内容が確定され、反映されます。
- 既存の情報を削除する場合は、対象エントリに☑を入れて、<Delete>ボタンをクリックしてください。

3.3.5. Jumbo Frame(ジャンボフレーム)

ジャンボ フレームを設定します。

イーサネット通信で使用される標準的なフレームサイズ(最大1500バイト)を超える大きなデータフレームを指します

「Switch Config」 → 「Jumbo Frame」をクリックすると、以下の画面が表示されます。

Jumbo Frame Config

This page is used to configure Jumbo Frame!

Jumbo Frame Size	1500	1500-9216 (Unit : Bytes)
------------------	------	--------------------------

Apply

メニュー	説明
Jumbo Frame Size(Unit: Bytes)	ジャンボフレームのサイズ(有効範囲:1500~9216、デフォルト値:1500)

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定してください。

3.3.6. Port Rate(ポートレート)

ポートレート(送受信可能なデータ量の制限)の設定を行います。

1. 「Switch Config」 → 「Port Rate」をクリックすると、以下の画面が表示されます。

Port Rate

This page is used to configure port rate.

Ports	--Please select --	
Limit Type	Ingress	▼
Status	Disabled	▼
Rate(Kbps)	No Limit	(1-1000000,16step)

Apply

Port	EgressRate(Kbps)	IngressRate(Kbps)
Ethernet1/0/1	1000000	1000000
Ethernet1/0/2	1000000	1000000
Ethernet1/0/3	1000000	1000000
Ethernet1/0/4	1000000	1000000
Ethernet1/0/5	1000000	1000000
Ethernet1/0/6	1000000	1000000
Ethernet1/0/7	1000000	1000000
Ethernet1/0/8	1000000	1000000
Ethernet1/0/9	1000000	1000000
Ethernet1/0/10	1000000	1000000

メニュー	説明
Ports	対象の物理ポート番号を選択します。 <input type="checkbox"/> Select All/Unselectに☑を入れると、すべてのポートを選択、または解除することができます。
Limit Type	ポートごとのトラフィックの入力方向を制限します。 ・Egress: 出力制限を行います。 ・Ingress: 入力制限を行います。 ・All: すべて(入出力)の制限を行います。
Status	ポートレートの有効/無効を設定します(デフォルト値:Disabled)。
Rate(Kbps)	帯域幅制御レートを設定します。 (有効範囲: 1~1,000,000 Kbps, 16Kbps単位)。

2. 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定すると、次のリスト表が更新されます。

メニュー	説明
Port	対象の物理ポート番号を表します。
Ingress Rate	各ポートの入力帯域幅しきい値(Kbps)を表示します。
Egress Rate	各ポートの出力帯域幅しきい値(Kbps)を表示します。

3.3.7. Storm Control(ストームコントロール)

ポートのストーム制御機能(特定のトラフィックが過剰になった場合の制限機能)を設定できます。

「Switch Config」→「Storm Control」をクリックすると、以下の画面が表示されます。

Storm Control

This page is used to configure storm control.

Ports	--Please select--		
Type	Broadcast		
Status	Disabled		
Rate(kbps)	No Limit	(1-1000000,16step)	

Apply

Port	Broadcast	Unknown Multicast	Unknown Unicast
Ethernet1/0/1	Disabled	Disabled	Disabled
Ethernet1/0/2	Disabled	Disabled	Disabled
Ethernet1/0/3	Disabled	Disabled	Disabled
Ethernet1/0/4	Disabled	Disabled	Disabled
Ethernet1/0/5	Disabled	Disabled	Disabled
Ethernet1/0/6	Disabled	Disabled	Disabled
Ethernet1/0/7	Disabled	Disabled	Disabled
Ethernet1/0/8	Disabled	Disabled	Disabled
Ethernet1/0/9	Disabled	Disabled	Disabled

メニュー	説明
Port	対象の物理ポート番号を選択します。 <input type="checkbox"/> Select All/Unselectに <input checked="" type="checkbox"/> を入れると、すべてのポートを選択、または解除することができます。
Type	適用するストームコントロールの種類(ブロードキャスト/マルチキャスト/ユニキャスト)を選択します。
Status	ストームコントロールの有効/無効を選択します(デフォルト設定:Disabled)。 ・Disabled: ストームコントロールを無効にします。 ・Enabled: ストームコントロール機能をオンにして、速度制限を設定します。
Rate(kbps)	ストーム制御レートを設定します (有効範囲:1~1000000 kbps ※デフォルト設定:制限なし)

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定してください。

3.3.8. MAC Address Config(MAC アドレスの設定)

1 Static MAC(スタティック MAC)

特定の機器(MACアドレス)をスイッチの特定のポート/VLANに手動マッピングする機能です。

「Switch Config」→「MAC Address Config」→「Static MAC」をクリックすると、以下の画面が表示されます。

MAC Address Config

MAC Address	00-00-00-00-00-00
VLAN ID	VLAN0001
Port	Ethernet1/0/1

Add

Static MAC List

Showing 10 Entries Showing 0 to 0 of 0 entries Search

No.	MAC Address	VLAN ID	Port
0 results found.			

First **Previous** **Next** **Last**

Delete

メニュー	説明
MAC Address	16 進数 MAC アドレスを選択します(形式:xx-xx-xx-xx-xx-xx)。
VLAN ID	対象の VLAN IDを選択します。
Port	マッピング対象のポートを選択します。

- 新規 VLAN を追加する場合は、<Add>ボタンをクリックして設定内容を確定してください。
- 既存の情報を削除する場合は、対象エントリに☒を入れて<Delete>ボタンをクリックしてください。

各画面で表示するエントリ数をドラッグして設定できます
(オプション: 全件 / 10 件 / 30 件 / 50 件 / 100 件、デフォルト: 10 件)
画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

2 Black Hole MAC(ブラックホール MAC)

特定のMACアドレスからの通信を意図的に破棄するための機能です。
これにより、そのMACアドレスに関連するデバイスやトラフィックがネットワーク内でアクセスできない状態になります。

「Switch Config」→「MAC Address Config」→「Black Hole MAC」をクリックすると、以下の画面が表示されます。

Black Hole MAC

MAC Address	<input type="text" value="00-00-00-00-00-00"/>
VLAN ID	<input type="text" value="VLAN0001"/>

Black Hole MAC List

Showing Entries Showing 0 to 0 of 0 entries

<input type="checkbox"/>	No.	MAC Address	VLAN ID
0 results found.			

メニュー	説明
MAC Address	対象のMACアドレスを選択します(16進数のMACアドレス形式: xx-xx-xx-xx-xx-xx)。このアドレスを持つパケットは破棄され、ネットワークに転送されません。
VLAN ID	対象のVLAN IDを選択します。

- 新規 VLAN を追加する場合は、<Add>ボタンをクリックして設定内容を確定してください。
- 既存の情報を削除する場合は、対象エントリに☑を入れて<Delete>ボタンをクリックしてください。

各画面で表示するエントリ数をドラッグして設定できます
(オプション: 全件 / 10 件 / 30 件 / 50 件 / 100 件、デフォルト: 10 件)
画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

3 Aging-time(エージングタイム)

スイッチが自動で学習したMACアドレスのエージング時間を設定します。
設定された時間が経過すると、そのMACアドレスはスイッチから削除されます。

「Switch Config」→「MAC Address Config」→「Aging-time」をクリックすると、以下の画面が表示されます。

Aging-time

Aging-time	300	(10-1000000)Second, default is 300, 0:No Aging
------------	-----	--

メニュー	説明
Aging-time	エージングタイムを設定します (有効範囲: 10~1000000秒、デフォルト設定: 300 (※0秒: エージングなし))。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定してください。

3.3.9. AM(アクセス管理機能)

アクセス管理(AM)機能は、指定ポートにIPアドレスまたは、MACおよびIPアドレスを設定し、許可されたIPアドレスまたは、MACおよびIPアドレスしか通信できないような機能です。

AMのポートバインディング機能により、ネットワーク管理者は正当なユーザのIPアドレス(またはMAC-IPアドレス)を指定されたポートにバインドできます。

バインディング操作後、指定のIPアドレス(またはMAC-IPアドレス)を持つユーザから送信されたパケットのみが、このポートを介して転送されるため、ネットワークセキュリティが強化されます。

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

Access Manage(AM)

Through the port binding feature of AM access management, network administrators can bind legitimate user IP (MAC-IP) addresses to specified ports. After the binding operation, only messages sent by users with specified IP (MAC-IP) addresses can be forwarded through this port, enhancing users' monitoring of network security.

Port	--Please select --	
Binding Type	IP	
IP Address		
Number ?	1	

Add

AM Configuration Table

Showing 10 Entries Showing 0 to 0 of 0 entries Search

<input type="checkbox"/>	Port	Binding Type	MAC Address	IP Address	Number
0 results found.					

Delete **First** **Previous** **Next** **Last**

メニュー	説明
Port	対象のポート番号を選択します。 <input type="checkbox"/> Select All/Unselectに <input type="checkbox"/> を入れると、すべてのポートを選択、または解除することができます。
Binding Type	バインディングタイプの設定を選択します(IPまたは MAC-IP 方式を選択)。
IP Address	IPアドレスを入力します。
Number	入力したIPからの連続アドレス数を入力します(値の有効範囲:1~32)。
MAC Address	MAC アドレスを入力します。

- 設定をする場合は、<Add>ボタンをクリックして設定内容を確定してください。
- 既存の情報を削除する場合は、対象エンTRIESにを入れて<Delete>ボタンをクリックしてください。

各画面で表示するエンTRIES数をドラッグして設定できます
(オプション: 全件 / 10 件 / 30 件 / 50 件 / 100 件、デフォルト: 10 件)
画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

3.3.10. AAA(認証・認可・アカウント機能)

1 MAC Address List (MAC アドレスリスト)

スイッチ内のMACアドレスリストを表示します。

「Switch Config」→「MAC Address Config」→「MAC Address List」をクリックすると、以下の画面が表示されます。

MAC Address List

Showing Entries Showing 1 to 10 of 29 entries

VLAN ID	MAC Address	Type	Creator	Port
1		DYNAMIC	Hardware	Ethernet1/0/1
1		DYNAMIC	Hardware	Ethernet1/0/1
1		DYNAMIC	Hardware	Ethernet1/0/1
1		DYNAMIC	Hardware	Ethernet1/0/1
1		DYNAMIC	Hardware	Ethernet1/0/1
1		DYNAMIC	Hardware	Ethernet1/0/1
1		DYNAMIC	Hardware	Ethernet1/0/1
1		DYNAMIC	Hardware	Ethernet1/0/1
1		DYNAMIC	Hardware	Ethernet1/0/1
1		DYNAMIC	Hardware	Ethernet1/0/28

First Previous 1 2 3 Next Last

メニュー	説明
VLAN ID	VLAN IDを表示します
MAC Address	16進MACアドレスを表示します(形式:xx-xx-xx-xx-xx-xx)。
Type	MACアドレスのタイプを表示します。
Creator	MACアドレスの管理者を表示します。
Port	ポート上のMACアドレスを表示します。

【注記】:

絞り込みを行う場合は、画面右上の「Search」ボックスに条件を入力してください。
絞り込み条件がない(空欄)場合は、MACアドレス情報がすべて表示されます。

各画面で表示するエントリ数をドラッグして設定できます
(オプション: 全件 / 10件 / 30件 / 50件 / 100件、デフォルト: 10件)
画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

2 Radius

Radius認証サーバは、許可されたユーザのみがネットワークリソースにアクセスできるよう制御するために使用します。

本項目では、Radius 認証サーバの設定を行うことができます。

「Switch Config」→「AAA」→「Radius」をクリックすると、以下の画面が表示されます。

Radius Global Config

The user priority for Radius authentication login is 1

Key Type	Plain Key	
Radius Global Key	<input type="text"/>	1-64Characters
System Recovery Time	<input type="text" value="5"/>	Range:1-255(Min),Default:5
Radius Retransmit Times	<input type="text" value="3"/>	Range:0-100,Default:3
Radius Server Timeout	<input type="text" value="3"/>	Range:1-1000(Sec),Default:3

Radius Global Information				
Key Type	Radius Global Key	System Recovery Time	Radius Retransmit Times	Radius Server Timeout
Plain Key		5	3	3

メニュー	説明
Key Type	RadiusサーバとNAS間の通信を保護するために使用される暗号化または認証キーの種類を選択します。 <ul style="list-style-type: none"> ・Plain Key: プレーンテキスト(平文)の共有鍵を指定します。 ・Cipher Key: 暗号化された形式の共有鍵を指定します。
Radius Global Key	Radiusで使用される共有のパスワード(共有秘密鍵)を設定します。 (値の有効範囲:1~64文字)
System Recovery Time	Radiusサーバがダウンした場合の再接続試行までの待機時間を設定します。 (値の有効範囲:1 ~ 255 分、デフォルト値:5)。
Radius Retransmit Times	Radiusサーバへのリクエストが失敗した場合の再送信回数を表します (値の有効範囲:0 ~ 100回、デフォルト値:3)。
Radius Server Timeout	Radiusサーバからの応答を待つ最大時間を表します。 (値の有効範囲:1 ~ 1000 秒、デフォルト値:3)。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定してください。

次に、Radius認証サーバの設定手順について説明します。

Radius Authentication Server Config

Authentication Server IP	<input type="text"/>	IPv4 or IPv6 address
Accounting Server Port(optional)	<input type="text"/>	Range:0-65535
Key Type	Plain Key	▼
Radius Key(optional)	<input type="text"/>	1-64Characters
Access Mode	None	▼
Primary Accounting Server	Non-primary accounting server	▼

Showing 10 Entries Showing 0 to 0 of 0 Entries Search

NO.	Server IP Address	Port Number	Primary Server	Key Type	Radius Key	Access Mode
0 results found.						

メニュー	説明
Authentication Server IP	Radius サーバの IPv4 または IPv6 アドレスを指定します。 <ul style="list-style-type: none"> IPv4 address: サーバのIPv4形式のアドレスを選択します。 IPv6 address:サーバのIPv6形式のアドレスを選択します。
Authentication Server port(optional)	Radiusサーバが認証リクエストを受け付けるポート番号を指定します (値の有効範囲:0 ~ 65535)。
Key Type	Radiusサーバとの通信を保護するための暗号化または認証キーの種類を選択します (デフォルト設定: Plain Key)。 <ul style="list-style-type: none"> Plain Key:プレーン キーを指定します Cipher Key: 暗号化するためのプレーン テキスト アプリケーションを指定します。
Radius Key	Radiusサーバとの認証に使用する共有秘密鍵を入力します (1 ~ 64 文字)。
Access Mode	Radiusサーバを使用する際のアクセスモードを選択します。 <ul style="list-style-type: none"> None: すべてのサービスは、デフォルトでRadius サーバを使用できます Telnet: Telnetでの機器ログイン認証を使用します Dot1x: LAN接続時の802.1X認証を使用します
Primary Authentication Server	複数のRadiusサーバが設定可能な場合に、最初に使用される主要な認証サーバを指定します。 <ul style="list-style-type: none"> Primary accounting server:Radius サーバをプライマリ認証サーバとして指定します。 Non-Primary accounting server:Radius サーバをバックアップ認証サーバとして指定します。

- 各項目を設定した後、<Apply>ボタンをクリックして設定を確定すると、内容が更新されます。
- 既存の情報を削除する場合は、対象エントリに☑を入れて<Delete>ボタンをクリックしてください。

各画面で表示するエントリ数をドラッグして設定できます

(オプション: 全件 / 10 件 / 30 件 / 50 件 / 100 件、デフォルト: 10 件)

画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

3 Tacacs

TACACS+機能(認証・認可・アカウントिंग)を設定します。

「Switch Config」→「AAA」→「Tacacs」をクリックすると、以下の画面が表示されます。

Tacacs Global Config

The user priority for Tacacs authentication login is 1

Key Type	Plain Key ▼	
Tacacs Global Key	<input type="text"/>	1-64 Characters
Tacacs Server Global Timeout	<input type="text" value="3"/>	Range: 1-60(Sec), Default: 3

Apply

Tacacs Global Information		
Key Type	Tacacs Global Key	Tacacs Server Global Timeout
Plain Key		3

メニュー	説明
Key Type	TACACS+サーバとの通信を保護するための共有鍵の種類を選択します(デフォルト: Plain Key)。 <ul style="list-style-type: none"> ・Plain Key: プレーンテキスト(平文)の共有鍵を指定します。 ・Cipher Key: 暗号化された形式の共有鍵を指定します。
Tacacs Global Key	TACACS+サーバとNAS(本機器)で共有するグローバルな秘密鍵(パスワード)を入力します(値の有効範囲: 1 ~ 64 文字)。
Tacacs Server Global Timeout	TACACS+サーバからの応答のタイムアウト時間を表します(値の有効範囲: 1 ~ 60 秒、デフォルト値: 3秒)。

- 各項目を設定した後、<Apply>ボタンをクリックして設定を確定すると、内容が更新されます。

次に、Tacacs+の認証サーバの設定手順について説明します。

Tacacs Authentication Server Config

Authentication Server IP	<input type="text"/>	IPv4 or IPv6 address
Authentication Server Port(optional)	<input type="text"/>	Range:0-65535
Key Type	Plain Key	
Tacacs Key(optional)	<input type="text"/>	1-64Characters
Tacacs Server Timeout(optional)	Cipher Key	Range:1-60(Sec),Default:3
Primary Accounting Server	Non-primary accounting server	

Showing 10 Entries Showing 0 to 0 of 0 entries Search

NO.	Server IP Address	port number	Primary Server	Key Type	Tacacs Key	Tacacs Server Timeout
0 results found.						

メニュー	説明
Authentication Server IP	TACACS+認証サーバのIPアドレス(IPv4またはIPv6)を入力します。
Authentication Server Port(optional)	TACACS+認証サーバのポート番号を入力します (値の有効範囲:0-65535)。
Key Type	TACACS+認証サーバとの認証に使用する暗号化キーの種類を選択します。 ・Plain Key:プレーンテキスト(平文)の共有鍵を指定します。 ・Cipher Key:暗号化された形式の共有鍵を指定します。
Tacacs Key(optional)	サーバとスイッチ間の認証に用いる共有鍵(パスワード)を設定します (値の有効範囲:1~64文字)。 【注記】: セキュリティを確保するため、サーバ側と一致させる必要があります。
Tacacs Server Timeout(optional)	TACACS+認証サーバの認証時間の間隔を入力します。 (値の有効範囲:1-60秒、デフォルト値:3)。
Primary Accounting Server	複数のアカウントサーバを設定する場合、優先的に利用する「プライマリサーバ」を指定します。障害時にはセカンダリに切り替わるよう設定可能です。 ・Primary accounting server: 最初に参照される優先サーバです。スイッチは通常、このサーバに対して認証・アカウント要求を送信します。安定運用のために最も信頼性の高いサーバを指定してください。 ・None-primary account server: プライマリサーバに障害が発生した場合にバックアップとして利用されるサーバです。セカンダリ(またはバックアップ)サーバとも呼ばれ、プライマリが利用不可のときに自動的に切り替わります。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定すると、テーブルの内容が更新されます。
- 既存の情報を削除する場合は、対象エントリに☑を入れて<Delete>ボタンをクリックしてください。

各画面で表示するエントリ数をドラッグして設定できます
(オプション: 全件 / 10 件 / 30 件 / 50 件 / 100 件、デフォルト: 10 件)
画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

4 Radius Accounting (Radius アカウンティング)

ユーザのネットワーク利用状況を記録・管理するためRadiusアカウンティングサーバを設定します。

「Switch Config」→「AAA」→「Radius Accounting」をクリックすると、以下の画面が表示されます。

Radius Accounting Server Config

Accounting Server IP	<input type="text"/>	IPv4 or IPv6 address
Accounting Server Port(optional)	<input type="text"/>	Range:0-65535
Key Type	Plain Key	
Radius Key(optional)	<input type="text"/>	1-64Characters
Primary Accounting Server	Non-primary accounting server	

Showing 10 Entries Showing 0 to 0 of 0 entries Search

NO.	Server IP Address	port number	Key Type	Radius Key	Primary Server
0 results found.					

メニュー	説明
Accounting Server IP	RadiusアカウンティングサーバのIPアドレスを指定します。 クライアントの認証・利用状況を記録するため、このサーバと通信します。 ・IPv4 address: サーバのIPv4形式のアドレスを選択します。 ・IPv6 address:サーバのIPv6形式のアドレスを選択します。
Accounting Server Port(optional)	Radiusアカウンティングサーバと通信する際に使用するポート番号を指定します。 ※省略した場合はデフォルトの1813(もしくは、1646)が利用されます。
Key Type	Radiusサーバとの認証に使用する暗号化キーの種類を選択します。 ・Plain Key:プレーンテキスト(平文)の共有鍵を指定します。 ・Cipher Key: 暗号化された形式の共有鍵を指定します。
Radius Key (optional)	サーバとスイッチ間の認証に用いる共有鍵(パスワード)を設定します(値の有効範囲:1~64文字)。 【注記】: セキュリティを確保するため、サーバ側と一致させる必要があります。
Primary Accounting Server	複数のアカウンティングサーバを設定する場合、優先的に利用する「プライマリサーバ」を指定します。障害時にはセカンダリに切り替わるよう設定可能です。 ・Primary accounting server: 最初に参照される優先サーバです。スイッチは通常、このサーバに対して認証・アカウンティング要求を送信します。安定運用のために最も信頼性の高いサーバを指定してください。 ・None-primary account server: プライマリサーバに障害が発生した場合にバックアップとして利用されるサーバです。セカンダリ(またはバックアップ)サーバとも呼ばれ、プライマリが利用不可のときに自動的に切り替わります。

- 各項目を設定した後、<Apply>ボタンをクリックして設定を確定すると、内容が更新されます。
- 既存の情報を削除する場合は、対象エントリに☑を入れて<Delete>ボタンをクリックしてください。

各画面で表示するエントリ数をドラッグして設定できます
(オプション: 全件 / 10 件 / 30 件 / 50 件 / 100 件、デフォルト: 10 件)
画面下のメニューボタンを使用して、ページを移動してください。

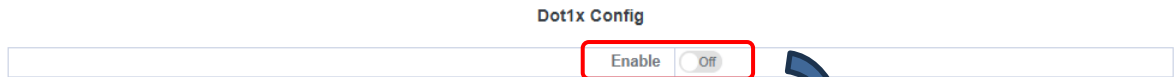
- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

5 Dot1x

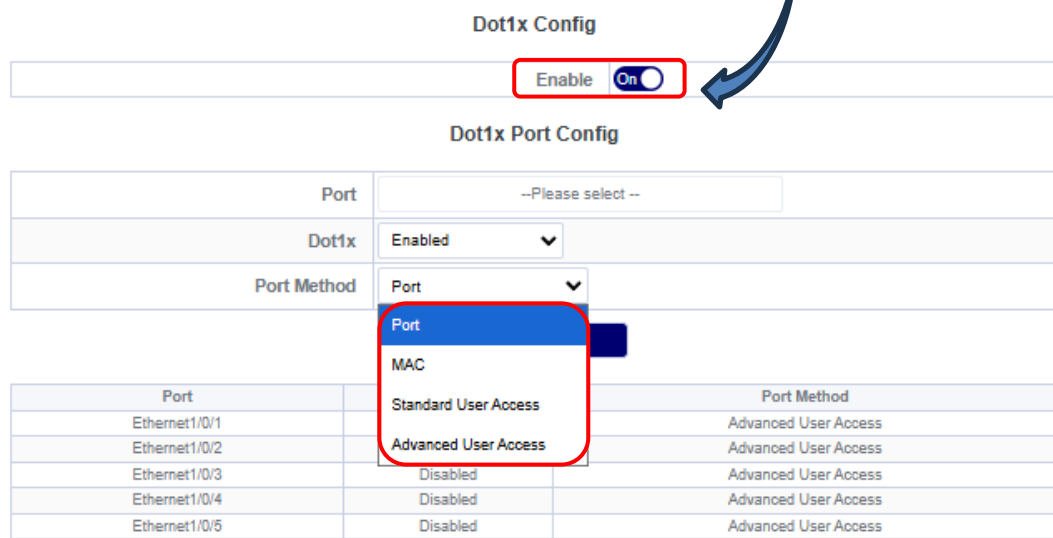
IEEE 802.1X(通称Dot1x)は、ネットワークデバイス(例: スイッチ)が接続デバイス(クライアント)を認証する仕組みです。

ネットワークに接続する前に、認証サーバ(通常はRadiusサーバ)と連携してIDとパスワードを確認し、正当なユーザのみアクセスを許可します(デフォルト設定:無効)。

1. 「Switch Config」→「AAA」→「Dot1x」をクリックすると、以下の画面が表示されます。



2. この機能を有効(Enableを「ON」)にすると、以下の画面が表示されます。



メニュー	説明
Port	対象の物理ポート番号を選択します。 □Select All/Unselectに☑を入れると、すべてのポートを選択、または解除することができます。
Dot1x	802.1Xを有効/無効に設定します。
Port Method	ポートごとの認証方式を設定します。 ※「Dot1x」メニューを有効にすると、ポートの認証方式を選択することが可能です。 ・Port:ポート単位での認証設定を管理します。 ・MAC:MACアドレスベースの認証方式を管理します ・Standard User Access:標準ユーザアクセス制御を行います。 ・Advanced User Access:高度なユーザアクセス制御を行います。

3.3.11. DNS Config

スイッチが外部ホストやサービスの名前解決を行うために、使用するDNSサーバを設定します(デフォルト設定:有効)。

適切なDNSサーバのアドレスと優先順位をここで設定することで、スイッチから外部へのアクセスが効率的に行えるようになります。

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

DNS Config

Enable

DNS Server Config

DNS Server Address	<input type="text"/>	Example:10.10.10.1 or 2001::1234
Priority	<input type="text"/>	Priority:0-255

<input type="checkbox"/>	No.	DNS Server Address	Priority
<input type="checkbox"/>	1	1.1.1.1	-
<input type="checkbox"/>	2	8.8.8.8	-

メニュー	説明
DNS Server Address	DNSサーバのIPアドレスを指定します。
Priority	複数のDNSサーバを設定した場合に、それぞれのサーバの優先順位を定義します。 値が大きいほど優先度が高く、最初にそのサーバに問い合わせが行われます。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定すると、テーブルの内容が更新されます。
- 既存の情報を削除する場合は、対象エントリに☑を入れて<Delete>ボタンをクリックしてください。

各画面で表示するエントリ数をドラッグして設定できます
(オプション: 全件 / 10 件 / 30 件 / 50 件 / 100 件、デフォルト: 10 件)
画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

3.4. VLAN Config (VLAN 設定)

VLAN(仮想LAN)の作成や管理を行い、ネットワークを論理的に分割します。

3.4.1. GVRP Config (GVRP の設定)

1 GVRP Config (GVRP の設定)

GVRP を有効/無効に設定します(デフォルト設定:無効)。

1. 「VLAN Config」→「GVRP Config」→「GVRP Config」をクリックすると、以下の画面が表示されます。

GVRP Config

Enabled Off

メニュー	説明
GVRP Config	<ul style="list-style-type: none"> ・Enable(ON):グローバル GVRP モジュール機能を有効にします ・Disable(OFF):グローバル GVRP モジュール機能を無効にします

2. GARP 機能を有効(Enabled)にすると、次の画面が表示されます。
この機能により、さまざまなタイマーの値を設定して GARP を調整することができます。

GVRP Config

Enabled On

Join Timer	200	Range:200-500 milli-second, default is 200
Leave Timer	600	Range:500-1200 milli-second, default is 600
Leaveall Timer	10000	Range:5000-60000 milli-second, default is 10000

メニュー	説明
Join timer	GVRP Joinメッセージの送信間隔を設定します(値の有効範囲:200-500ms、デフォルト値:200)。
Leave timer	GVRP Leaveメッセージを送信後、該当VLAN情報を維持する時間を設定します(値の有効範囲:500-1200ms、デフォルト値:600)。
Leaveall timer	GVRP LeaveAllメッセージの送信間隔を設定します(値の有効範囲:500-60000ms、デフォルト値:10000ms)。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定してください。

2 GVRP Port (GVRP ポート設定)

GVRP (GARP VLAN Registration Protocol)におけるポートごとにVLAN登録を動的に行うためのものです。これにより、ネットワーク全体でのVLAN管理を効率化され、手動設定の手間を軽減できます。GVRPを使用するには、対象ポートがIEEE 802.1Qトランクモードで設定されている必要があります。

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

Enable GVRP On Port

Enable the port will not be able to change the port mode!

Ports

Only display ports that enable gvrp.

Showing Entries
Showing 0 to 0 of 0 entries
Search

	Port	GVRP Status
<input type="checkbox"/>	0 results found.	

メニュー	説明
Port	対象のポートを選択します。

【注記】:

ポートを有効にするとポートモードを変更することはできなくなります。

リストには、GVRPが有効なポートのみ表示されます。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定してください。
- 既存の情報を削除する場合は、対象エントリに☑を入れて<Delete>ボタンをクリックしてください。

各画面で表示するエントリ数をドラッグして設定できます

(オプション: 全件 / 10 件 / 30 件 / 50 件 / 100 件、デフォルト: 10 件)

画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

3 Enable Dot1q Tunnel(Dot1q トンネルを有効にする)

指定したポートでDot1qトンネル機能(QINQ)を有効にします。
これにより、顧客VLANタグ(C-TAG)が付与されたフレームに、さらにサービスプロバイダVLANタグ(S-TAG)を付加して転送できるようになります。この項目は、カスタマー接続ポートを設定します。

「VLAN Config」→「QINQ」→「Enable Dot1q Tunnel」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
Port	対象のポート番号を選択します。 <input type="checkbox"/> Select All/Unselectに☑を入れると、すべてのポートを選択、または解除することができます。

- 本項目は、カスタマー接続ポートに設定します。
- 受信したフレームの C-Tag は、ペイロードとして扱われます。
- S-VLAN の設定は、VLAN Config よりアクセスポートで VLANID を割り当ててください。
- 新規ポートを追加する場合は、<Add>ボタンをクリックして設定内容を確定してください。
- 既存の情報を削除する場合は、対象エントリに☑を入れて<Delete>ボタンをクリックしてください。

各画面で表示するエントリ数をドラッグして設定できます
(オプション: 全件 / 10 件 / 30 件 / 50 件 / 100 件、デフォルト: 10 件)
画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

3.4.2. VLAN Config (VLAN 設定)

VLANの作成、編集、削除、および関連設定を行うための管理メニューです。
ネットワークを論理的に分割し、トラフィックを効率的に管理するための設定を行います。

1 VLAN ID

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

VLAN Config Management

VLAN ID	<input type="text"/>	(1-4094, for example: 1;3-6)
VLAN Name	<input type="text"/>	

Showing Entries Showing 1 to 1 of 1 entries Search

	No.	VLAN ID	VLAN Name
<input type="checkbox"/>	1	1	default

メニュー	説明
VLAN ID	VLAN のIDを設定します(値の有効範囲: 1 ~ 4094)。
VLAN Name	VLAN の名前を設定します。(デフォルトでは、「VLAN」と4桁のVLANID) (値の有効範囲: 1 ~ 64文字)。

- 新規 VLAN を追加する場合は、<Add>ボタンをクリックして設定内容を確定してください。
- 既存の情報を削除する場合は、対象エントリにを入れて<Delete>ボタンをクリックしてください。

各画面で表示するエントリ数をドラッグして設定できます
(オプション: 全件 / 10件 / 30件 / 50件 / 100件、デフォルト: 10件)
画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

2 Show VLAN (VLAN データベースの表示)

VLANリスト(VLANデータベースを表示します。

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

Show VLAN List

Showing Entries Showing 1 to 1 of 1 Entries Search

VLAN ID	VLAN Name	Type	Media	Ports
1	default	Static	ENET	Ethernet1/0/1, Ethernet1/0/2 Ethernet1/0/3, Ethernet1/0/4 Ethernet1/0/5, Ethernet1/0/6 Ethernet1/0/7, Ethernet1/0/8 Ethernet1/0/9, Ethernet1/0/10 Ethernet1/0/11, Ethernet1/0/12 Ethernet1/0/13, Ethernet1/0/14 Ethernet1/0/15, Ethernet1/0/16 Ethernet1/0/17, Ethernet1/0/18 Ethernet1/0/19, Ethernet1/0/20 Ethernet1/0/21, Ethernet1/0/22 Ethernet1/0/23, Ethernet1/0/24 Ethernet1/0/25, Ethernet1/0/26 Ethernet1/0/27, Ethernet1/0/28

[First](#) [Previous](#) [1](#) [Next](#) [Last](#)

各画面で表示するエントリ数をドラッグして設定できます
(オプション: 全件 / 10件 / 30件 / 50件 / 100件、デフォルト: 10件)

画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

3 Port Config (VLANのポート設定)

物理ポート(または論理ポート)に対してVLANの動作を設定します。

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

Port Mode Config

Ports	--Please select --	
Mode	Access	▼
Native Vlan	VLAN0001	▼
Ingress Check	Enabled	▼
Tagged VLAN	Range(1-4094)	Example 1-3;8
UnTagged VLAN	Range(1-4094)	Example 1-3;8

Apply

Port	Mode	Native Vlan	Ingress Check	Tag Vlan List	Untag Vlan List
Ethernet1/0/1	Access	VLAN0001	Enabled	-	-
Ethernet1/0/2	Access	VLAN0001	Enabled	-	-
Ethernet1/0/3	Access	VLAN0001	Enabled	-	-
Ethernet1/0/4	Access	VLAN0001	Enabled	-	-
Ethernet1/0/5	Access	VLAN0001	Enabled	-	-
Ethernet1/0/6	Access	VLAN0001	Enabled	-	-
Ethernet1/0/7	Access	VLAN0001	Enabled	-	-
Ethernet1/0/8	Access	VLAN0001	Enabled	-	-
Ethernet1/0/9	Access	VLAN0001	Enabled	-	-

メニュー	説明
Port	対象のポートを選択します。
Mode	ポートの動作モードを指定します。 <ul style="list-style-type: none"> ・Accessモード: 1つのVLANに所属するポートを指します。 ・Trunkモード: 複数のVLANをタグで識別し、中継するポートを指します。 ・Hybridモード: 複数のVLANをタグの有無で送受信できるポートを指します。
Native Vlan	タグ無しフレームが属するVLANを設定。
Ingress Check	受信フレームのVLANタグが、ポートで許可されたものかフィルタリングします <ul style="list-style-type: none"> ・Enabled: 受信フィルタを有効にします。 ・Disabled: 受信フィルタを無効にします。
Tagged VLAN	Trunk/Hybridモード時、タグ付き通信を許可するVLANのリストを設定します(有効範囲: 1-4094(例1-3;8))。
UnTagged VLAN	Hybridモード時、タグ無しで送信するVLANのリストを設定します(有効範囲: 1-4094(例1-3;8))。

- 各項目を設定した後、<Apply>ボタンをクリックして設定を確定すると、内容が更新されます。

3.4.3. QINQ

1 Dot1q Tunnel TPID(S-tag の tpid の設定)

QinQトンネリングのサービスプロバイダVLANタグ(S-TAG)として使用するTPID (Tag Protocol Identifier) の値をポートごとに指定します。この設定は、サービスプロバイダポートに設定を行います。

「VLAN Config」→「QINQ」→「Dot1q Tunnel TPID」をクリックすると、以下の画面が表示されます。

Config Dot1q Tunnel TPID

Only configure for QINQ disable port.

Ports	--Please select --
Protocol	0x8100
Protocol ID	Range:1-65535

Apply

Port	Protocol
Ethernet1/0/1	
Ethernet1/0/2	
Ethernet1/0/3	
Ethernet1/0/4	
Ethernet1/0/5	
Ethernet1/0/6	

メニュー	説明
Port	対象の物理ポート番号を選択します。 <input type="checkbox"/> Select All/Unselectに <input checked="" type="checkbox"/> を入れると、すべてのポートを選択、または解除することができます。
Protocol	Dot1qトンネリングに関連するTPIDを選択します。 <ul style="list-style-type: none"> ・0x8100:外側の TPID を 0x8100 に設定します。 ・0x88A8:外側の TPID を 0x88A8 に設定します。 ・0x9100:外側の TPID を 0x9100 に設定します。 ・0x9200:外側の TPID を 0x9200 に設定します。 ・protocol ID:カスタム TPID を設定します。
Protocol ID	[Protocol]選択時にカスタムTPIDの値を設定します。(10進数表記)

- 本項目は、サービスポートに設定をします。
- S-VLAN の設定は、トランクポートに設定を行います。

3.4.4. Voice VLAN (音声 VLAN)

1 VLAN Config (VLAN の設定)

Voice VLANは、IP電話機などの音声デバイスからのトラフィックを自動的に検出し、あらかじめ指定されたVLAN(音声専用VLAN)に割り当てる機能です。これにより、音声トラフィックをデータトラフィックから分離し、優先制御を行うことで安定した通話品質を確保できます。

1. 「VLAN Config」→「Voice VLAN」→「VLAN Config」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
Voice VLAN	音声VLANを有効/無効に設定します。

2. この機能を有効にすると、以下の画面が表示され、Voice Vlanに応じて関連情報(MAC Address、MAC Mask、Priority、Name)を設定することができます。

メニュー	説明
Voice VLAN	音声VLANのIDを選択します。
MAC Address	音声MAC アドレスを表示します(xx-xx-xx-xx-xx-xx 形式)。
MAC Mask	MAC アドレスのマスクコードの最後の 8 桁を表示します(有効な値:0xff、0xfe、0xfc、0xf8、0xf0、0xe0、0xc0、0x80、0x0)。
Priority	音声トラフィックの優先度を表示します(有効範囲:0 ~ 7)。
Name	音声機器の名前を入力します。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定してください。
- 既存の情報を削除する場合は、対象エントリに☑を入れて<Delete>ボタンをクリックしてください。

各画面で表示するエントリ数をドラッグして設定できます
 (オプション: 全件 / 10 件 / 30 件 / 50 件 / 100 件、デフォルト: 10 件)
 画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

2 Port Config (ポートの設定)

各ポートの音声VLANを有効/無効に設定します。

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

Port Config

Ports	--Please select --
Status	Enabled ▼

Port	Status
Ethernet1/0/1(A)	Enabled
Ethernet1/0/2(A)	Enabled
Ethernet1/0/3(A)	Enabled
Ethernet1/0/4(A)	Enabled
Ethernet1/0/5(A)	Enabled
Ethernet1/0/6(A)	Enabled
Ethernet1/0/7(A)	Enabled

メニュー	説明
Port	対象のポート番号を選択します。 <input type="checkbox"/> Select All/Unselectに☑を入れると、すべてのポートを選択、または解除することができます。
Status	音声VLANを有効/無効に設定します。 ・Enable: 音声VLANを有効にします。 ・Disable: 音声VLANを無効にします。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定すると、テーブルの内容が更新されます。

3.4.5. MAC VLAN

1 VLAN Config (MACVLAN 設定)

MACアドレスに基づいてVLANを割り当てるMAC VLANの設定できます。

【注記】:

この機能を有効にするには、「Surveillance VLAN」メニューを「無効」にしてください
(設定手順については、「[3.4.7 Surveillance VLAN](#)」を参照してください)。

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

VLAN Config

MAC VLAN VLAN0001 ▼

Add

Showing 10 Entries Showing 1 to 1 of 1 entries Search

	No.	MAC VLAN	VLAN Name
<input type="checkbox"/>	1	1	VLAN0001

Delete **First** **Previous** **1** **Next** **Last**

メニュー	説明
MAC VLAN	MAC VLANを追加するには、VLANを選択します。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定してください。
- 既存の情報を削除する場合は、対象エントリにを入れて<Delete>ボタンをクリックしてください。

各画面で表示するエントリ数をドラッグして設定できます
(オプション: 全件 / 10 件 / 30 件 / 50 件 / 100 件、デフォルト: 10 件)
画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- ↑: 上に移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

2 VLAN Member (VLAN メンバー)

選択したVLANに、特定のMACアドレスを持つデバイスをメンバーとして登録します。これにより、登録されたMACアドレスを持つデバイスがネットワークに接続された際、自動的に指定したVLANに所属させることができます。

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

MAC VLAN Config

MAC address	00-00-00-00-00-00
MAC Mask	FF-FF-FF-FF-FF-FF
VLAN ID	VLAN0001 ▼
Priority	Range:0-7

Add

Showing 10 ▼ Entries Showing 0 to 0 of 0 entries Search

<input type="checkbox"/>	No.	MAC address	MAC Mask	VLAN ID	Priority
0 results found.					

Delete **First** **Previous** **Next** **Last**

メニュー	説明
MAC Address	MAC アドレスを入力します(形式:XX-XX-XX-XX-XX-XX)。
MAC Mask	MAC アドレス マスクを入力します(形式:XX-XX-XX-XX-XX-XX)。
VLAN ID	VLAN の ID (値の有効範囲:1 ~ 4094)
Priority	MAC VLANエントリの優先度レベル(CoS値)を設定します(有効範囲: 0 ~ 7)。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定してください。
- 既存の情報を削除する場合は、対象エントリに☑を入れて<Delete>ボタンをクリックしてください。

各画面で表示するエントリ数をドラッグして設定できます
(オプション: 全件 / 10 件 / 30 件 / 50 件 / 100 件、デフォルト: 10 件)
画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

3 Port Config (ポート設定)

各ポートでMAC VLAN機能を有効にするか無効にするかを選択します。この設定を有効にしたポートでは、事前に「VLAN Member」で登録されたMACアドレスを持つデバイスが接続されると、自動的に指定されたVLANに割り当てられます。

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

Port Config

Ports	--Please select --
Status	Enabled ▼

Apply

Port	Status
Ethernet1/0/1(A)	Enabled
Ethernet1/0/2(A)	Enabled
Ethernet1/0/3(A)	Enabled
Ethernet1/0/4(A)	Enabled
Ethernet1/0/5(A)	Enabled
Ethernet1/0/8(A)	Enabled

メニュー	説明
Port	対象のポート番号を選択します。 <input type="checkbox"/> Select All/Unselectに☑を入れると、すべてのポートを選択、または解除することができます。
Status	ポートのMAC VLANを有効/無効に設定します。 ・Enable:MAC VLAN機能を有効にします。 ・Disable:MAC VLAN機能を無効にします。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定すると、ポートのステータスが更新されます。

3.4.6. Protocol VLAN (プロトコル VLAN)

特定のネットワークプロトコルに基づいて、受信したパケットを対応するVLANに自動的に割り当てるプロトコルVLANの設定方法を説明します。

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

Protocol VLAN Config

Mode	ethernetII
Ethernet Type	Range:1536-65535
VLAN Name	VLAN0001
Priority	Range:0-7

Add

Showing 10 Entries Showing 0 to 0 of 0 entries Search

<input type="checkbox"/>	No.	Protocol Type	VLAN Name	Priority
0 results found.				

Delete **First** **Previous** **Next** **Last**

メニュー	説明
Mode	イーサネットフレームのカプセル方式を選択します。 <ul style="list-style-type: none"> ・ethernetII : EthernetII 形式のフレームを設定します。 ・snap : SNAP形式のフレームを設定します。 ・Llc : LLC形式のフレームを設定します。
Ethernet Type	パケットのプロトコル タイプの範囲を設定します (値の有効範囲: 1536-65535)
VLAN Name	VLAN ID を設定します。
Priority	プロトコルVLANエントリの優先度レベルを設定します(有効範囲:0~7)。

- 新規 VLAN を追加する場合は、<Add>ボタンをクリックして設定内容を確定してください。
- 既存の情報を削除する場合は、対象エントリにを入れて<Delete>ボタンをクリックしてください。

各画面で表示するエントリ数をドラッグして設定できます
(オプション: 全件 / 10 件 / 30 件 / 50 件 / 100 件、デフォルト: 10 件)
画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

3.4.7. Surveillance VLAN

1 VLAN Config

監視デバイス向けに特別なVLANを設定し、自動的にカメラやレコーダーを検出してVLANを割り当てる機能を提供します。

【注記】:この機能を有効にするには、MAC VLAN/音声 VLANを設定を「無効」にしてください。
VLAN が設定されている場合は、監視 VLAN を有効にすることができません。

1. 「VLAN Config」→「Surveillance VLAN」→「VLAN Config」をクリックすると、以下の画面が表示されます。

Surveillance VLAN Config

Surveillance VLAN	None
Mode	Manual

Apply

2. 「Surveillance VLAN」に対象ポートを設定して、モードに「Manual」を選択して、<Apply>ボタンをクリックすると、下記画面が表示されます。

Surveillance VLAN Config

Surveillance VLAN	VLAN0001
Mode	Manual

Apply

Surveillance OUI Config

MAC address	MAC Mask	Priority	Name
00-00-00-00-00-00	FF-FF-FF-FF-FF-FF	Range:0-7	Up to 15 characters.

Add

Showing 10 Entries Showing 0 to 0 of 0 entries Search

No.	Name	MAC address	MAC Mask	Priority
0 results found.				

First Previous Next Last

Delete

モードを「auto」に設定したい場合は、まず「LLDP 機能」を有効にしてください(設定手順については、「3.2.12 LLDP」→「[Global Config](#)」を参照ください)。

- 新規 VLAN を追加する場合は、<Add>ボタンをクリックして設定内容を確定してください。

各画面で表示するエントリ数をドラッグして設定できます
(オプション: 全件 / 10 件 / 30 件 / 50 件 / 100 件、デフォルト: 10 件)
画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

2 Port Config

各ポートに対して、監視システム（例えばIPカメラやNVRなど）に適した設定を有効/無効に設定します（デフォルト設定：有効）。

【注記】:

この設定を行う場合は、前項の「VLAN Config」メニューにて、監視 VLAN IDを設定してください。

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

Port Config

Ports	Status
--Please select--	Enabled <input type="button" value="v"/>
<input type="button" value="Apply"/>	
Port	Status
Ethernet1/0/1(A)	Enabled
Ethernet1/0/2(A)	Enabled
Ethernet1/0/3(A)	Enabled
Ethernet1/0/4(A)	Enabled
Ethernet1/0/5(A)	Enabled
Ethernet1/0/6(A)	Enabled
Ethernet1/0/7(A)	Enabled
Ethernet1/0/8(A)	Enabled
Ethernet1/0/9(A)	Enabled
Ethernet1/0/10(A)	Enabled

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確認すると、テーブルの内容が更新されます。

3.5. DHCP Config

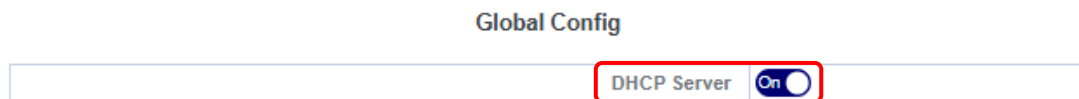
本製品がDHCPサーバまたはDHCPクライアントとして動作する際の設定を行います。IPアドレスの自動割り当てに関する管理機能です。

3.5.1. DHCP Server (DHCP サーバ)

1 Global Config (機能の有効化)

DHCPサーバとして動作させる場合の設定です。DHCPサーバは、ネットワーク上のコンピュータやその他のデバイス(クライアント)に対して、IPアドレス、サブネットマスク、デフォルトゲートウェイ、DNSサーバアドレスなどのネットワーク設定情報を自動的に割り当てる役割を持ちます。これにより、各デバイスで手動でIPアドレス等を設定する手間を省き、ネットワーク管理を効率化できます。
(デフォルト設定:無効)。

「DHCP Config」→「DHCP Server」→「Global Config」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	メニュー
DHCP server	DHCPサーバ機能の設定を有効/無効に設定します。 ・Off:DHCPサーバ機能を無効にします。 ・On:DHCPサーバ機能を有効にします。	

2 Create Address Pool(DHCP アドレスプールの作成)

DHCPサーバがクライアントにIPアドレスを割り当てる際、そのIPアドレスの範囲や関連する設定をグループ化したものを「アドレスプール」と呼びます。ここでは、そのアドレスプールに識別しやすい名前を付けて作成したり、既存のアドレスプール名を削除したりします。

「DHCP Config」→「DHCP Server」→「Create Address Pool」をクリックすると、以下の画面が表示されます。

Create Address Pool

Create Address Pool

Address Pool Name (1-32 character)

Add

DHCP Server Address Pool Table

Showing Entries Showing 0 to 0 of 0 entries Search

	Address Pool Name
0 results found.	

Delete **First** **Previous** **Next** **Last**

メニュー	説明
Address pool name	DHCPアドレスプールを設定します(有効範囲:1~32文字)。

- 新規アドレスプールを追加する場合は、<Add>ボタンをクリックして設定内容を確定してください。
- 既存の情報を削除する場合は、対象エントリに☑を入れて<Delete>ボタンをクリックしてください。

各画面で表示するエントリ数をドラッグして設定できます
(オプション: 全件 / 10 件 / 30 件 / 50 件 / 100 件、デフォルト: 10 件)
画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

3 Dynamic Pool(DHCP アドレス プールの設定)

作成した各アドレスプールに対して、クライアントに割り当てる具体的なIPアドレスの範囲、ドメイン名、クライアントタイプ(WINS設定など)、およびIPアドレスのリース期間などを設定します。
(設定手順については、「[2. Create Address Pool](#)」を参照してください。)

「DHCP Config」→「DHCP Server」→「Dynamic Pool」をクリックすると、以下の画面が表示されます。

Dynamic Pool

Address Pool Name	FXC1 ▼
Domain Name	<input type="text"/>
IP Address	<input type="text"/>
Netmask	<input type="text"/>
DHCP Client Node Type	Default ▼
Lease Time	Not Configured ▼

Dynamic Pool Config Table

Showing 10 ▼ Entries Showing 0 to 0 of 0 entries Search

<input type="checkbox"/>	Address Pool Name	Domain Name	IP Address/Netmask	DHCP Client Node Type	Lease Time
0 results found.					

メニュー	説明
Address pool Name	DHCPプールの識別名を選択します。
Domain Name	クライアントに割り当てるドメイン名を設定します。
IP Address	プールで使用するIPアドレス(ネットワークアドレス)を設定します。
Netmask	サブネットマスクを設定します(例: 255.255.255.0)。
DHCP Client Node Type	クライアントの種類を選択します。 <ul style="list-style-type: none"> ・Default: システムの標準設定に従う ・b-node: 名前解決にブロードキャストのみを使用 ・h-node: 最初にWINSサーバを使用し、失敗したらブロードキャストを試みる ・m-node: ブロードキャストを先に試し、失敗したらWINSを使用 ・p-node: WINSサーバのみで名前解決。 ・Designate: ユーザがカスタム設定を直接指定可能(詳細設定が必要な場合)
Lease Time	IPアドレスをクライアントに割り当てる期間を指定します <ul style="list-style-type: none"> ・Not Configured: デフォルト値(86400秒(1日))が適用 ・Infinite: IPアドレスのリース期限なし。 ・Specified: 具体的な時間を設定(例: 3600秒=1時間、86400秒=1日)

- 各項目を設定した後、<Add>ボタンをクリックして設定内容を確定すると、テーブルの内容が更新されます。
- 既存の情報を削除する場合は、対象エントリに☑を入れて<Delete>ボタンをクリックしてください。

各画面で表示するエントリ数をドラッグして設定できます
(オプション: 全件 / 10 件 / 30 件 / 50 件 / 100 件、デフォルト: 10 件)
画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- ↑: 上に移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

4 Manual Pool (スタティックアドレス プールの設定)

クライアントのMACアドレスに応じてパラメータを手動でバインドします。
本設定は、1プールあたり1クライアントのみ設定できます。

この機能を設定するには、まず「DHCPサーバ」の機能を有効にして、アドレスプールを追加してください
(設定手順については、「2. Create Address Pool」を参照してください)。

「DHCP Config」→「DHCP Server」→「Manual Pool」をクリックすると、以下の画面が表示されます。

Manual Pool

Address Pool Name	FXC1
IP Address	xxx.xxx.xxx.xxx
Netmask	xxx.xxx.xxx.xxx
Binding Type	Hardware Address
ARP Hardware Type	1(ethernet)
MAC Address	xx-xx-xx-xx-xx-xx

Apply

Static Pool Config Table

Showing 10 Entries Showing 0 to 0 of 0 entries Search

<input type="checkbox"/>	Address Pool Name	MAC Address	IP Address/Netmask	Binding Type	ARP Hardware Type
0 results found.					

Delete **First** **Previous** **Next** **Last**

メニュー	説明
Address Pool Name	手動割り当てに使用するIPアドレスのプールを指定します。
IP Address	DHCP サーバがクライアントに割り当てた IP アドレスを表します。
Netmask	IPアドレスに適用するサブネットマスクを指定します。
Binding Type	IPアドレスとデバイスのバインディング方法を指定します。 <ul style="list-style-type: none"> Hardware Address: MACアドレスを使用してIPアドレスをバインドします。 Client Identifier: クライアント識別子を使用してIPアドレスをバインドします。
ARP Hardware Type	ARPで使用するハードウェアタイプを指定します クライアントが使用するプロトコルタイプは rfc\ethernet\ieee802 です。 <ul style="list-style-type: none"> 1(ethernet): 10Mb Ethernet (DIX Ethernet II) を指す 6(ieee802): IEEE 802ネットワーク(例: 802.3 LAN、トークンリング、802.11 Wi-Fiなど)を指す。
MAC Address	IPアドレスを固定割り当てするデバイスのMACアドレス(例: 44-11-22-33-44-55)を指定します。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定すると、テーブルの内容が更新されます。
- 既存の情報を削除する場合は、対象エントリに☑を入れて<Delete>ボタンをクリックしてください。

各画面で表示するエントリ数をドラッグして設定できます
(オプション: 全件 / 10 件 / 30 件 / 50 件 / 100 件、デフォルト: 10 件)
画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

5 Default Gateway (DHCP クライアントのデフォルトゲートウェイの設定)

DHCP アドレス プールの配布するデフォルトゲートウェイを設定します。

この機能を設定するには、まず「DHCPサーバ」の機能を有効にして、アドレスプールを追加してください (設定手順については、「[2. Create Address Pool](#)」を参照してください)。

「DHCP Config」→「DHCP Server」→「Default Gateway」をクリックすると、以下の画面が表示されます。

Default Gateway

Address Pool Name	FXC1 ▼
Gateway0	<input type="text"/>
Gateway1	<input type="text"/>
Gateway2	<input type="text"/>
Gateway3	<input type="text"/>
Gateway4	<input type="text"/>
Gateway5	<input type="text"/>
Gateway6	<input type="text"/>
Gateway7	<input type="text"/>
Operation	Add ▼

メニュー	説明
DHCP pool name	対象のDHCPプールの名前を指定します。
Gateway0-7	DHCPクライアントに提供するデフォルトゲートウェイのIPアドレスを指定します。 ゲートウェイ0が最も高い優先度を持ちます。 数値が小さいほど、優先度が高くなります。 【注記】: 設定は必ず0から連続して開始する必要があり、途中で欠番がある場合、欠番以降の後続のパラメータを無視します (たとえば、ゲートウェイ0、ゲートウェイ1、ゲートウェイ7を設定した場合、有効になるのはゲートウェイ0とゲートウェイ1のみです)。
Operation	操作方法を選択します。 ・Add: 上記で実際に設定したゲートウェイを現在選択されているDHCPアドレスプールに追加します。 ・Delete: すべてのゲートウェイをクリアし、デフォルトの状態に戻します。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定すると、テーブルの内容が更新されます。

6 DNS Server (DNS サーバ)

DHCP アドレス プールの 配布するDNS サーバを設定します。

この機能を設定するには、まず「DHCPサーバ」の機能を有効にして、アドレスプールを追加してください (設定手順については、「[2. Create Address Pool](#)」を参照してください)。

「DHCP Config」→「DHCP Server」→「DNS Server」をクリックすると、以下の画面が表示されます。

DNS Server

Address Pool Name	FXC1 ▼
DNS Server0	<input type="text"/>
DNS Server1	<input type="text"/>
DNS Server2	<input type="text"/>
DNS Server3	<input type="text"/>
DNS Server4	<input type="text"/>
DNS Server5	<input type="text"/>
DNS Server6	<input type="text"/>
DNS Server7	<input type="text"/>
Operation	Add ▼

メニュー	説明
DHCP pool name	DNSサーバ設定を適用する対象のDHCPプールの名前を指定します。
DNS server 0-7	<p>DHCPクライアントに提供するDNSサーバのIPアドレスを指定します。DNSサーバ0が最も高い優先度を持ちます。数値が小さいほど、優先度が高くなります。</p> <p>【注記】: 設定は必ず0から連続して開始する必要があり、途中で欠番がある場合、欠番以降の後続のパラメータを無視します(たとえば、DNSサーバ0、DNSサーバ1、DNSサーバ7を設定した場合、有効になるのはDNSサーバ0とDNSサーバ1のみです)。</p>
Operation	<p>操作方法を選択します。</p> <ul style="list-style-type: none"> ・Add: 上記で有効に設定した DNS サーバを現在選択されている DHCP アドレス プールに追加します。 ・Delete: すべての DNS サーバをクリアし、デフォルトの状態に戻します。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定してください。

7 Excluded Address (除外対象のアドレス)

DHCPサーバが自動でIPアドレスを割り当てる際に、特定のIPアドレスを割り当て対象から除外します。サーバやプリンター、ルーターといった、常に同じIPアドレスである必要がある機器(固定IPアドレスが必要な機器)のために、IPアドレスを予約しておくことができ、IPアドレスの重複を防ぎます。

「DHCP Config」→「DHCP Server」→「Excluded Address」をクリックすると、以下の画面が表示されます。

Excluded Address

Starting address	<input type="text"/>
Ending address	<input type="text"/>

Exclude Address Table

Showing Entries Showing 0 to 0 of 0 entries Search

	Starting address	Ending address
<input type="checkbox"/>		

0 results found.

メニュー	説明
Starting Address	DHCPサーバがIPアドレス割り当てから除外する範囲の開始アドレスを指定します。
Ending Address	DHCPサーバがIPアドレス割り当てから除外する範囲の終了アドレスを指定します。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定してください。
- 既存の情報を削除する場合は、対象エントリにを入れて<Delete>ボタンをクリックしてください。

各画面で表示するエントリ数をドラッグして設定できます
(オプション: 全件 / 10件 / 30件 / 50件 / 100件、デフォルト: 10件)
画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

8 Packet Statistics(パケット統計情報)

DHCPサーバが送受信するパケットに関するデータの統計情報を表示します。
これにより、ネットワーク管理者はDHCPサーバの動作状況やパフォーマンスを把握し、問題のトラブルシューティングや最適化に役立てることができます。

「DHCP Config」→「DHCP Server」→「Packet Statistics」をクリックすると、以下の画面が表示されます。

Packet Statistics						
Address Pools	Database Agents	Automatic Bindings	Manual Bindings	Conflict Bindings	Expiried Bindings	Malformed Message
0	0	0	0	0	0	0

Message Received					
BOOT REQUEST	DHCP Discover	DHCP Request	DHCP Decline	DHCP Release	DHCP Inform
0	0	0	0	0	0

Message Send					
BOOT Reply	DHCP Offer	DHCP ACK	DHCP NAK	DHCP Relay	DHCP Forward
0	0	0	0	0	0

[Clear Statistics](#)

9 Client List (クライアントリスト)

DHCPサーバが現在IPアドレスを割り当てているクライアント(デバイス)の一覧情報を表示します。このリストを確認することで、ネットワーク管理者はどのデバイスがどのIPアドレスを使用しているか、またそのリース状況を把握できます。

「DHCP Config」→「DHCP Server」→「Client List」をクリックすると、以下の画面が表示されます。

IP Address	Hardware Address	Lease Expiration	Type
------------	------------------	------------------	------

メニュー	説明
IP Address	DHCPサーバがクライアントに割り当てたIPアドレスを表示します。
Hardware Address	クライアントのMACアドレスを表示します。
Lease expiration	DHCPサーバがクライアントに割り当てたIPアドレスの有効期間(リースが終了する日時)を表示します。
Type	IPアドレスの割り当て方法を表示します。 <ul style="list-style-type: none"> ・Manual: 管理者が手動で設定した固定IPアドレス ・Dynamic: DHCPサーバが自動的に割り当てた動的IPアドレス。

3.5.2. DHCP Relay Config (DHCP リレー設定)

1 DHCP Relay Config(DHCP リレー設定)

DHCPリレー機能は、あるネットワークセグメントで受信したDHCPブロードキャストメッセージを、別のネットワークセグメントに存在するDHCPサーバへ中継(リレー)するための機能です。これにより、1台のDHCPサーバで複数のネットワークセグメントのIPアドレス管理を一元的に行うことが可能になります。対象のサーバにDHCPブロードキャストメッセージをユニキャスト送信します(デフォルト設定:無効)。

1. 「DHCP Config」→「DHCP Relay Config」→「DHCP Relay Config」をクリックすると、以下の画面が表示されます。

DHCP Relay Config

DHCP Broadcast Suppress ? Off

DHCP Relay Forwarding ? Off

2. 「DHCP Relay Forwarding」を有効(On)にすると、以下の画面が表示されます。

DHCP Relay Config

DHCP Broadcast Suppress ? Off

DHCP Relay Forwarding ? On

Interface	VLAN0001
Helper-server Address	xxx.xxx.xxx.xxx

[Add](#)

DHCP Forward Protocol Table

Showing 10 Entries Showing 0 to 0 of 0 entries

	Forward Protocol	Interface	Helper-server Address
0 results found.			

[Delete](#)
[First](#)
[Previous](#)
[Next](#)
[Last](#)

メニュー	説明
DHCP Broadcast Suppress	DHCPクライアントが送信するブロードキャストメッセージを抑制するかどうかを設定します(デフォルト設定:無効)。本設定でDHCPクライアントはIPを取得できなくなります。 <ul style="list-style-type: none"> ・On: DHCP ブロードキャストを抑制します。 ・Off: DHCP ブロードキャストを抑制しません。
DHCP Relay Forwarding	DHCPリレー機能を有効化し、クライアントからのDHCPリクエストを指定された他セグメントのDHCPサーバに転送します(デフォルト設定:無効)。 <ul style="list-style-type: none"> ・On: DHCPリレー転送を有効にします。 ・Off: DHCPリレー転送を無効にします。
Interface	DHCPリレー機能を適用するVLANインターフェースを選択します。
Helper-server Address	DHCPリクエストを転送する先のDHCPサーバのIPアドレスを指定します。

- 新規エントリを追加した後、<Add>ボタンをクリックして設定内容を追加してください。
- 既存の情報を削除する場合は、対象エントリに☑を入れて<Delete>ボタンをクリックしてください。

各画面で表示するエントリ数をドラッグして設定できます
(オプション: 全件 / 10 件 / 30 件 / 50 件 / 100 件、デフォルト: 10 件)
画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

3.5.3. DHCP Snooping (DHCP スヌーピング)

1 Global Config(グローバル設定)

DHCPスヌーピング機能の有効／無効にします。

DHCPスヌーピングを有効にすると状態表示や各種設定が可能になります(デフォルト設定:無効)。

1. 「DHCP Config」→「DHCP Snooping」→「Global Config」をクリックすると、以下の画面が表示されます。

Global Config

DHCP Snooping Status Off

メニュー	説明
DHCP Snooping Status	<ul style="list-style-type: none"> ・Off: DHCPスヌーピングを無効にします。 ・On: DHCPスヌーピングを有効にします。

2. 「DHCP Snooping Status」を有効(On)に設定すると、次の画面が表示されます。DHCPスヌーピング機能の設定を行います。

Global Config

DHCP Snooping Status On

Action Num	<input type="text" value="10"/>	(1-200, default 10)
Limit Rate	<input type="text" value="100"/>	pps(0-100, default 100)

Apply

メニュー	説明
Action Num	DHCPスヌーピングが有効な場合に、特定のアクションを実行する回数を設定します。 (有効範囲: 1-200、デフォルト値:10)。
Limit Rate	インターフェースが受け取るDHCPパケットの最大数を制限します (値の有効範囲: 0-100、デフォルト値:100pps)。 ※「0」の場合は、DHCPパケットが全て破棄されます。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定してください。

2 VLAN Config (VLAN 設定)

対象のVLAN IDごとにDHCPスヌーピング機能の有効/無効を個別に設定します。
これにより、特定のVLANに対して選択的にDHCPスヌーピングを適用できます。

【注記】:

この機能を有効にするには、まずDHCPスヌーピング機能を有効にしてください。
デフォルトでは、すべてのVLAN IDでVLAN単位のDHCPスヌーピング設定は無効 (Disabled) になっています。この場合、DHCPスヌーピングの動作はグローバル設定に依存します。

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

VLAN Config

VLAN ID	--Please select --
VLAN Enable	Disabled ▼
Apply	

VLAN ID	VLAN Enable
VLAN0001	Disabled

メニュー	説明
VLAN ID	対象のVLAN-IDを選択します。 <input type="checkbox"/> Select All/Unselectに <input checked="" type="checkbox"/> を入れると、すべてのポートを選択、または解除することができます。
VLAN Enable	DHCP スヌーピング VLAN 機能を有効/無効に設定します。 ・Enable: 選択したVLAN IDでDHCPスヌーピング機能を 有効 にします。 ・Disable: 選択したVLAN IDでDHCPスヌーピング機能を 無効 にします。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定すると、テーブルの内容が更新されます。

3 Static User Binding (DHCP スタティックバインディング)

特定の機器 (MACアドレス) に対し、IPアドレス、VLAN ID、接続ポートを固定的に設定 (バインディング) します。機能を有効にするとステータスを表示および設定できます (デフォルト設定: 無効)。

1. 「DHCP Config」→ 「DHCP Snooping」→ 「Static User Binding」をクリックすると、以下の画面が表示されます。

Static User Binding

Binding Status Off

メニュー	説明
Binding status	DHCP スヌーピング バインディング機能を有効/無効に設定します。 ・Off: DHCPスヌーピングバインディング機能を無効にします。 ・On: DHCPスヌーピングバインディング機能を有効にします。

2. 「Static User Binding」メニューを「On」に設定すると、次の画面が表示されます。DHCP スヌーピングバインディングのステータスを表示および設定できます。

Static User Binding

Binding Status On

MAC Address

IP Address

VLAN ID

Port

Apply

DHCP Snooping Binding Table

Showing 10 Entries Showing 0 to 0 of 0 entries Search

<input type="checkbox"/>	MAC Address	IP Address	Port	VLAN ID	Type
0 results found.					

Delete First Previous Next Last

メニュー	説明
MAC Address	静的にバインドする MAC アドレスを入力します。
IP Address	静的にバインドするIP アドレスを入力します。
VLAN ID	VLAN ID を選択します。
Port	ポートを静的に指定します。 ポートは VLAN ID に関連付けられます。対応するVLAN の通過を許可する必要があります

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定すると、反映されます。
- 既存の情報を削除する場合は、対象エントリに☑を入れて<Delete>ボタンをクリックしてください。

各画面で表示するエントリ数をドラッグして設定できます
 (オプション: 全件 / 10 件 / 30 件 / 50 件 / 100 件、デフォルト: 10 件)
 画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

4 Helper-server Config (ヘルパーサーバの設定)

DHCPスヌーピングは、監視されたバインディング情報をヘルパーサーバに送信して保存します。本機が正しく起動しない場合は、ヘルパーサーバからバインドされたデータに戻すことができます。

「DHCP Config」→「DHCP Snooping」→「Helper-server Config」をクリックすると、以下の画面が表示されます。

Helper-server Config

Helper-server Address	<input type="text"/>
Helper-server UDP Port	9119 (1-65535, default 9119)
Local IP Address	<input type="text"/>
Server Address Type	Primary ▼

Apply

<input type="checkbox"/>	Helper-server Address	Helper-server UDP Port	Local IP Address	Server Address Type
--------------------------	-----------------------	------------------------	------------------	---------------------

Delete

メニュー	説明
Helper-server Address	ヘルパーDHCPサーバのIPアドレスを入力します。
Helper-server UDP port	DHCPスヌーピングとヘルパーDHCPサーバの通信(UDP)プロトコルを指定します(有効範囲:1~65535、デフォルト値:9119)。
Local IP Address	有効な本機の管理IPアドレスを設定します。
Server Address Type	登録するヘルパーサーバの役割をプルダウンメニューから選択します。 ・Primary: プライマリヘルパーDHCPサーバとして指定します。 ・Secondary: セカンダリヘルパーDHCPサーバとして指定します。

- 新しいサーバアドレスを追加する場合は、<Add>ボタンをクリックして設定内容を確定します。
- <Delete>ボタンをクリックすると、既存のサーバのアドレスを削除します。
 ※削除時にはパラメータの入力は不要です。

5 Port Binding(ポートバインディング設定)

ポートバインディングは、スイッチの特定のポートとデバイス(またはIPアドレス)を紐付け、許可されていないデバイスのネットワーク接続を防止するセキュリティ機能です。

この設定を有効にすると、DHCPスヌーピング機能はここで設定された紐付け情報を信頼し、紐付けられたデバイスからのアクセスを許可します。

【注記】:

この機能を有効にするには、スタティックユーザのバインディング機能を有効にしてください(設定手順については、[「3 Static User Binding \(DHCPスタティックバインディング\)」](#)を参照)

「DHCP Config」→「DHCP Snooping」→「Port Binding」をクリックすると、以下の画面が表示されます。

Port Binding

Port	--Please select--
Dot1x	Disabled ▼
User	Disabled ▼

Apply

Port	Dot1x	User
Ethernet1/0/1	Disabled	Disabled
Ethernet1/0/2	Disabled	Disabled
Ethernet1/0/3	Disabled	Disabled
Ethernet1/0/4	Disabled	Disabled
Ethernet1/0/5	Disabled	Disabled
Ethernet1/0/6	Disabled	Disabled
Ethernet1/0/7	Disabled	Disabled

メニュー	説明
Port	対象のポート番号を選択します。 <input type="checkbox"/> Select All/Unselectに☑を入れると、すべてのポートを選択、または解除することができます。
Dot1x	ポートごとにDHCP スヌーピング ポートの Dot1x バインディング ステータスを有効/無効に設定します。
User	Dot1x認証で使用するユーザカウントを有効/無効に設定します。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定すると、テーブルの内容が更新されます。

6 Trust Port (信頼ポート)

Trustポートは、DHCPスヌーピング機能において、正規のDHCPサーバが接続されるポートなどを「信頼できる」ポートとして設定する機能です。これにより、ネットワーク内での不正なDHCPサーバの動作を防ぎます。DHCPスヌーピングを有効するにすべてのポートは信頼しない(Untrust)ポートになります。

「DHCP Config」→「DHCP Snooping」→「Trust Port」をクリックすると、以下の画面が表示されます。

Trust Port

Port	--Please select --
Trust	Disabled ▼

Apply

Port	Trust	VLAN ID
Ethernet1/0/1	Disabled	-
Ethernet1/0/2	Disabled	-
Ethernet1/0/3	Disabled	-
Ethernet1/0/4	Disabled	-
Ethernet1/0/5	Disabled	-
Ethernet1/0/6	Disabled	-
Ethernet1/0/7	Disabled	-

メニュー	説明
Port	対象のポート番号を選択します。 <input type="checkbox"/> Select All/Unselectに <input checked="" type="checkbox"/> を入れると、すべてのポートを選択、または解除することができます。
Trust	ポートの信頼状態を設定します。 「Enabled」で信頼できるポート、「Disabled」で信頼できないポートに設定されます。

- 各項目を設定した後、<Apply>ボタンをクリックすると、各 DHCP スヌーピングポートの trust 属性の状態が更新されます。

3.6. ACL Config

アクセス制御リストを設定し、トラフィックの許可・拒否ルールを定義します。
アクセスリストは、1500エントリ以内で設定してください。

3.6.1. Time Range Config (タイムレンジ設定)

タイムレンジ設定では、アクセスコントロールリスト(ACL)のルールが有効になる期間を定義します。

「ACL Config」→「Time Range Config」をクリックすると、以下の画面が表示されます。

Time Range Config

In the "Absolute" type, the start time and end time must be selected. If the start time and end time are the same time, only the start time can work; In the "Absolute-period" type, a week value must be selected, including the start and end times, but cannot be the same; In the "Period" type, you must select a week value, including start and end times.

Time Range Name	<input type="text"/>	(1-64 characters)
Time Range Type	Absolute	
Start Time	2025 - 01 - 01 00 : 00 : 00	
End Time	2025 - 01 - 01 00 : 00 : 00	

Apply

Time Range Table

Showing 10 Entries Showing 0 to 0 of 0 entries Search

<input type="checkbox"/>	Time Range Name	Absolute	Periodic	Absolute-periodic
0 results found.				

Delete **First** **Previous** **Next** **Last**

メニュー	説明
Time range name	タイムレンジの名称を入力します (英数字1~64文字)
Time range type	タイムレンジのタイプを設定します。 <ul style="list-style-type: none"> ・"Absolute"タイプでは、指定した開始日時から終了日時まで、一度だけ有効になる期間を設定します。 ・"Periodic(期間)"タイプでは、毎週繰り返される曜日と時間帯を指定します。 ・"Absolute-period(絶対期間)"タイプでは、指定した絶対期間(開始日~終了日)の中で、さらに特定の曜日と時間帯を組み合わせで指定します。
Start Time	開始日および開始時刻を設定します(YYYY.MM.DD、有効範囲: 2001.1.1-2038.12.31)。
End Time	終了日および終了時間を設定します(YYYY.MM.DD、有効範囲: 2001.1.1-2038.12.31)。

- 各項目を設定した後、<Apply>ボタンをクリックして設定を確定すると、内容が更新されます。
- 既存の情報を削除する場合は、対象エントリに☑を入れて<Delete>ボタンをクリックしてください。

各画面で表示するエントリ数をドラッグして設定できます
(オプション: 全件 / 10 件 / 30 件 / 50 件 / 100 件、デフォルト: 10 件)
画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

3.6.2. IP ACL

IP ACLは、IPパケットに基づいて通信を制御するための機能です。IPアドレスやポート番号などを条件に、通信を許可したり拒否したりするルールを設定できます。

1 IP Standard ACL (標準 IP アクセスリスト)

標準IPACLは、アクセス制御リスト(ACL)の基本的な形式の一つです。この機能では、IPパケットの送信元IPアドレスのみを条件として、そのパケットを通過させるか(permit)、または遮断するか(deny)を制御します。

「ACL Config」→「IP ACL」→「IP Standard ACL」をクリックすると、以下の画面が表示されます。

IP Standard ACL

ACL Name	<input type="text"/>	(1-64 string or number 1-99)
ACL Action	Permit	▼
Source Address Type	Any IP	▼
TPID	<input type="text"/>	(0-65535, Optional configuration)
VLANID	Not Configured	▼
DSCP	Not Configured	▼

Apply

IP Standard ACL Config Status Table

Showing 10 ▼ Entries Showing 0 to 0 of 0 entries Search

<input type="checkbox"/>	ACL Name	Source IP/Mask	TPID	VLANID/Mask	DSCP	ACL Action
0 results found.						

Delete **First** **Previous** **Next** **Last**

メニュー	説明
ACL name	ACLルールの識別名または番号を入力します。 (有効範囲:1-64文字もしくは、1-99の番号)。
ACL Action	ACLルールに一致した通信に対するアクション(動作)を選択します。 ・permit:条件に一致するトラフィックを許可します。 ・deny:条件に一致するトラフィックを拒否します。
Source Address type	送信元アドレスの指定方法を選択します。 ・Any IP:全ての IP アドレスを指定します。 ・Specified IP: IPアドレス/サブネットマスク(IPアドレス範囲)を指定します。 ・Host IP:指定されたホスト IP(単一IP)を指定します。
TPID ※オプション設定	VLANタグ付きフレームのプロトコル識別子を入力します(10進数) (値の有効範囲:0-65535)。
VLANID ※オプション設定	VLAN IDを選択します(値の有効範囲:1-4094)。 ※VLANID mask:VLAN IDの範囲を指定するためのマスクを設定します(値の有効範囲:0-4095)。
DSCP ※オプション設定	QoSに関連するトラフィックの優先度を選択します (値の有効範囲:0-63)。

- 各項目を設定した後、<Apply>ボタンをクリックして設定を確定すると内容が更新されます。
- 既存の情報を削除する場合は、対象エントリに☑を入れて<Delete>ボタンをクリックしてください。

各画面で表示するエントリ数をドラッグして設定できます
(オプション: 全件 / 10 件 / 30 件 / 50 件 / 100 件、デフォルト: 10 件)
画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

2 IP Extended ACL(拡張 IP アクセスリスト)

拡張IPACLは、通信をより詳細な条件に基づいて制御するための強力な機能です。標準IPACLが主に送信元IPアドレスのみを条件とするのに対し、拡張IPACLでは様々な情報を柔軟に組み合わせて、より精密なアクセスコントロールルールを作成できます。

「ACL Config」→「IP ACL」→「IP Extended ACL」をクリックすると、以下の画面が表示されます。

IP Extended ACL

ACL Name	<input type="text" value=""/>	(1-64 string or number 100-299)
Operation Type	ICMP ▼	
ACL Action	Permit ▼	
Fragment Packet	Disabled ▼	
Source Address Type	Any IP ▼	
Destination Address Type	Any IP ▼	
IP Precedence	Not Configured ▼	
TOS	Not Configured ▼	
Time Range Name	Not Configured ▼	
ICMP Type	Not Configured ▼	
ICMP Code	Not Configured ▼	

[Apply](#)

IP Extended ACL Config Status Table

Showing Entries Showing 0 to 0 of 0 entries Search

<input type="checkbox"/>	ACL Name	Operation Type	Source IP/Mask	Destination IP/Mask	Fragment Packet	IP Precedence	TOS	Operation Type Paramer	Time Range Name	ACL Action
0 results found.										

[Delete](#) [First](#) [Previous](#) [Next](#) [Last](#)

メニュー	説明
ACL name	拡張ACLルールの識別名または番号を入力します (値の有効範囲: 1-64文字もしくは、100-199の番号)。
Operation type	制御対象のプロトコルを選択します。 ・ICMP.IGMP.TCP.UDP.EIGRP.GRE.IGRP.IPINIP.OSPF.IP, Specified_protocol(プロトコル番号指定)
ACL Action	ACLルールに一致した通信に対するアクション(動作)を選択します。 ・permit:条件に一致するトラフィックを許可します。 ・deny:条件に一致するトラフィックを拒否します。
Fragment packet	IPパケットが断片化(フラグメント)されている場合に適用するかどうかを設定します。
Source Address Type	トラフィックの送信元IPアドレスを指定する方式を選択します。 ・Any IP:全ての IP アドレスを指定します。 ・Specified IP: IPアドレス/サブネットマスク(IPアドレス範囲)を指定します。 ・Host IP:指定されたホスト IP(単一IP)を指定します。

Destination Address Type	トラフィックの宛先IPアドレスを指定する方式を選択します。 <ul style="list-style-type: none"> ・Any IP: 全ての IP アドレスを指定します。 ・Specified IP: IPアドレス/サブネットマスク(IPアドレス範囲)を指定します。 ・Host IP: 指定されたホスト IP(単一IP) を指定します。
IP Precedence/TOS	IPヘッダ内の IP Precedence/TOS フィールドに基づいて条件に指定します。
Time range name	ACLを適用する時間帯のスケジュール名を設定します (英数字で始まる必要があります(値の有効範囲: 1~64 文字))。
ICMP type	ICMP メッセージ タイプを選択します(値の有効範囲: 0-255)。
ICMP code	ICMPタイプに詳細なコードを選択します(値の有効範囲: 0-255)。

- 各項目を設定した後、<Apply>ボタンをクリックして設定を確定すると内容が更新されます。
- 既存の情報を削除する場合は、対象エントリに☑を入れて<Delete>ボタンをクリックしてください。

各画面で表示するエントリ数をドラッグして設定できます

(オプション: 全件 / 10 件 / 30 件 / 50 件 / 100 件、デフォルト: 10 件)

画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

3.6.3. MAC ACL

1 MAC Standard ACL(標準 MAC アクセスリスト)

標準MAC ACLは、レイヤー2で動作し、通信フレームのMACアドレスに基づいてアクセス制御を行います。MACアドレスを条件として、通信を許可 (permit) または拒否 (deny) する場合に有効です。

「ACL Config」→「MAC ACL」→「MAC Standard ACL」をクリックすると、以下の画面が表示されます。

MAC Standard ACL

ACL Name	<input type="text" value="(700-799)"/>
ACL Action	Permit ▼
Source Address Type	Any MAC ▼

Apply

MAC Standard ACL Config Status Table

Showing 10 ▼ Entries Showing 0 to 0 of 0 entries Search

<input type="checkbox"/>	ACL Name	Source MAC/Mask	ACL Action
0 results found.			

Delete **First** **Previous** **Next** **Last**

メニュー	説明
ACL Name	標準MAC ACLルールの識別番号を入力します。(700-799)
ACL Action	ACLルールに一致した通信に対するアクション(動作)を選択します。 ・permit: 条件に一致するトラフィックを許可します。 ・deny: 条件に一致するトラフィックを拒否します。
Source Address type	トラフィックの送信元MACアドレスを指定する方式を選択します。 ・Any MAC: 全てのMACアドレスを指定します。 ・Specified MAC: MACアドレス/サブネットマスクを指定します。 ・Host MAC: 指定されたホストMAC(単一MAC)を指定します。
Source MAC	送信元MACアドレスを入力します。

- 各項目を設定した後、<Apply>ボタンをクリックして設定を確定すると、内容が更新されます。
- 既存の情報を削除する場合は、対象エントリに☑を入れて<Delete>ボタンをクリックしてください。

各画面で表示するエントリ数をドラッグして設定できます
 (オプション: 全件 / 10件 / 30件 / 50件 / 100件、デフォルト: 10件)
 画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

2 MAC Extended ACL(拡張 MAC ACL)

拡張MAC ACLは、標準MAC ACLよりもさらに詳細なレイヤー2の情報を条件として、イーサネットフレームのフィルタリングを行います。送信元MACアドレスと宛先MACアドレスに加え、様々な情報を組み合わせ、よりきめ細やかなアクセス制御が可能です。

「ACL Config」→「MAC ACL」→「MAC Extended ACL」をクリックすると、以下の画面が表示されます。

MAC Extended ACL

ACL Name	<input type="text"/>	(1-64 string or number 1100-1199)
ACL Action	Permit	▼
Source Address Type	Any MAC	▼
Destination Address Type	Any MAC	▼
Packet Type	None	▼
Cos	Not Configured	▼
Cos Mask	Not Configured	▼
VLANID	Not Configured	▼
EtherType	<input type="text"/>	(1536-65535, Optional configure)
EtherType Mask	Not Configured	▼

[Apply](#)

MAC Extended ACL Config Status Table

Showing 10 Entries Showing 0 to 0 of 0 entries Search

<input type="checkbox"/>	ACL Name	Source MAC/Mask	Destination MAC/Mask	Packet Type	Cos/Mask	VLANID/Mask	EtherType/Mask	ACL Action
0 results found.								

[Delete](#) [First](#) [Previous](#) [Next](#) [Last](#)

メニュー	説明
ACL Name	ACLルール of 識別名または番号を入力します (値の有効範囲: 1-64文字もしくは、1100-1199の番号)。
ACL Action	ACLルールに一致した通信に対するアクション(動作)を選択します。 <ul style="list-style-type: none"> ・permit: 条件に一致するトラフィックを許可します。 ・deny: 条件に一致するトラフィックを拒否します。
Source Address type	トラフィックの送信元MACアドレスを指定する方式を選択します。 <ul style="list-style-type: none"> ・Any MAC: 全てのMACアドレスを指定します。 ・Specified MAC: MACアドレス/サブネットマスクを指定します。 ・Host MAC: 指定されたホストMAC(単一MAC)を指定します。
Destination Address type	トラフィックの宛先MACアドレスを指定する方式を選択します。 <ul style="list-style-type: none"> ・Any MAC: 全てのMACアドレスを指定します。 ・Specified MAC: MACアドレス/サブネットマスクを指定します。 ・Host MAC: 指定されたホストMAC(単一MAC)を指定します。
Packet type	フィルタリングの対象のパケットの形式を指定します。 <ul style="list-style-type: none"> ・none: 指定なし。 ・tagged-802-3: IEEE 802.3規格に基づくタグ付きパケットを指定します。 ・tagged-eth2: イーサネットII規格に基づくタグ付きパケットを指定します。

	<ul style="list-style-type: none"> ・untagged-802-3:VLANタグなし802.3規格のパケットを指定します。 ・untagged-eth2:VLANタグなしイーサネットII規格のパケットを指定します。
Cos	Cosの優先度を選択します (値の有効範囲:0-7、0:最低優先度、※7:最高優先度)。
Cos Mask	Cosマスクを選択します(値の有効範囲:0-7)。
VLANID	VLAN IDを選択します(値の有効範囲:1-4094)
VLANID mask	VLANマスクを設定します(値の有効範囲:0-4095)
EtherType	イーサネットタイプ値を指定します(値の有効範囲:1536-65535)。
EtherType Mask	イーサネットタイプ値マスクを指定します(値の有効範囲:0-65535)。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定すると、テーブルの内容が更新されます。
- 既存の情報を削除する場合は、対象エントリに☑を入れて<Delete>ボタンをクリックしてください。

各画面で表示するエントリ数をドラッグして設定できます(オプション: 全件 / 10 件 / 30 件 / 50 件 / 100 件、デフォルト: 10 件)

画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

3.6.4. MAC-IP Extended ACL(拡張 MAC-IP ACL)

拡張MAC-IP ACLは、レイヤー2のMACアドレス情報とレイヤー3のIPアドレス情報を同時に条件として使用できる、非常に柔軟性の高いアクセス制御リストです。単にMACアドレスやIPアドレスのどちらか一方を条件とするACLよりも詳細な制御が可能となり、例えば「特定のMACアドレスを持つ機器(が、特定のIPアドレスと、指定したプロトコルで通信することだけを許可する」といった、より複雑できめ細やかなフィルタリングルールを作成できます。

「ACL Config」→「MAC-IP Extended ACL」をクリックすると、以下の画面が表示されます。

MAC-IP Extended ACL

ACL Name	<input type="text"/>	(1-64 string or number 3100-3299)
Operation Type	ICMP	▼
ACL Action	Permit	▼
Source Address Type	Any MAC	▼
Destination Address Type	Any MAC	▼
Source Address Type	Any IP	▼
Destination Address Type	Any IP	▼
Parameter Options	Not Configured	▼
TPID	<input type="text"/>	(0-65535, Optional configuration)
VLANID	Not Configured	▼
Time Range Name	Not Configured	▼
ICMP Type	Not Configured	▼
ICMP Code	Not Configured	▼

[Apply](#)

MAC-IP Extended ACL Config Status Table

Showing 10 Entries Showing 0 to 0 of 0 entries Search

<input type="checkbox"/>	ACL Name	Operation Type	Source MAC/Mask	Destination MAC/Mask	Source IP/Mask	Destination IP/Mask	TPID	VLANID/Mask	DSCP	IP Precedence	TOS	Operation Type Parameter	Time Range Name	ACL Action
0 results found.														

[Delete](#) [First](#) [Previous](#) [Next](#) [Last](#)

メニュー	説明
ACL Name	拡張MAC-IP ACLの名前もしくは番号を入力します (有効範囲:1-64文字以内もしくは、3100-3199の番号)。
Operation Type	ACLルールプロトコルの種類を選択します。
ACL Action	ACLルールに一致した通信に対するアクション(動作)を選択します。 ・permit:条件に一致するトラフィックを許可します。 ・deny:条件に一致するトラフィックを拒否します。
Source Address type	トラフィックの送信元MACアドレスを指定する方式を選択します。 ・Any MAC:全てのMACアドレスを指定します。 ・Specified MAC:MACアドレス/サブネットマスクを指定します。 ・Host MAC:指定されたホストMAC(単一MAC)を指定します。
Destination Address type	トラフィックの宛先MACアドレスを指定する方式を選択します。 ・Any MAC:全てのMACアドレスを指定します。 ・Specified MAC:MACアドレス/サブネットマスクを指定します。 ・Host MAC:指定されたホストMAC(単一MAC)を指定します。

Source Address type	トラフィックの送信元IPアドレスを指定する方式を選択します。 ・Any IP:全ての IP アドレスを指定します。 ・Specified IP: IPアドレス/サブネットマスク(アドレス範囲)を指定します。 ・Host IP:指定されたホスト IP(単一IP) を指定します。
Destination Address type	トラフィックの宛先IPアドレスを指定する方式を選択します。 ・Any IP:全ての IP アドレスを指定します。 ・Specified IP: IPアドレス/サブネットマスク(アドレス範囲)を指定します。 ・Host IP:指定されたホスト IP(単一IP) を指定します。
Parameter Options	トラフィックのDSCP/IP Precedence/TOSを指定します。
TPID	VLANタグ付きフレームのプロトコル識別子(TPID)を入力します (値の有効範囲:0-65535)。
VLANID	VLAN IDを選択します(値の有効範囲:1-4094)。
Time range name	ACLを適用する時間帯のタイムレンジ名を設定します。
ICMP type	ICMP メッセージ タイプを選択します(値の有効範囲:0-255)。
ICMP code	ICMPタイプに付随する詳細なコードを設定します(値の有効範囲:0-255)。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定すると、テーブルの内容が更新されます。
- 既存の情報を削除する場合は、対象エントリに☑を入れて<Delete>ボタンをクリックしてください。

各画面で表示するエントリ数をドラッグして設定できます
(オプション: 全件 / 10 件 / 30 件 / 50 件 / 100 件、デフォルト: 10 件)
画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

3.6.5. ACL Binding (ACL バインディング)

1 Binding Port (バインディングポート)

作成したアクセスコントロールリスト(ACL)を特定のポートに適用(バインディング)します。ACLをポートにバインディングすることで、そのポートを通過する通信を制御できます。

「ACL Config」→「ACL Binding」→「Binding Port」をクリックすると、以下の画面が表示されます。

Binding Port

Port	--Please select --
ACL Type	IP
ACL Name	
Attached Direction	Ingress

Apply

Port Binding Status Table

Showing 10 Entries Showing 0 to 0 of 0 entries Search

<input type="checkbox"/>	Port	ACL Name	ACL Type	Attached Direction
0 results found.				

Delete First Previous Next Last

メニュー	説明
Port	対象のポート番号を選択します。 <input type="checkbox"/> Select All/Unselectに☑を入れると、すべてのポートを選択、または解除することができます。
ACL type	適用するACLの種類を指定します。 ・IP:IPアドレスを条件にしたACL ・MAC:MACアドレスを条件にしたACL。 ・MAC-IP:MACアドレスとIPアドレスの両方を条件に組み合わせたACL
ACL name	アクセスリスト名を選択します。
ACL Attached Direction	ACLを適用するトラフィックの方向を選択します。 ・ingress : ポートに入ってくるトラフィック(入力方向)にACLを適用します。 ・ingress /traffic-statistics: 入力方向にACLを適用し、そのトラフィックの統計情報を収集します。

- 各項目を設定した後、<Apply>ボタンをクリックして設定を確定すると、内容が更新されます。
- 既存の情報を削除する場合は、対象エントリに☑を入れて<Delete>ボタンをクリックしてください。

2 Binding Vlan (ACL VLAN バインディング)

作成したアクセスコントロールリスト(ACL)を特定のVLANに適用(バインディング)します。

「ACL Config」→「ACL Binding」→「Binding Vlan」をクリックすると、以下の画面が表示されます。

Binding Vlan

VLAN Interface	--Please select--
ACL Type	IP
ACL Name	
Attached Direction	Ingress

Apply

VLAN Binding Status Table

Showing 10 Entries Showing 0 to 0 of 0 entries Search

<input type="checkbox"/>	VLAN Interface	ACL Name	ACL Type	Attached Direction
0 results found.				

Delete First Previous Next Last

メニュー	説明
VLAN interface	対象のVLAN 番号を選択します。
ACL type	ACLの種類を指定し、どのタイプのトラフィックを制御するか選択します。 ・IP:IPアドレスやプロトコルを条件にしたACL ・MAC:MACアドレスを条件にしたACL。 ・MAC-IP:MACアドレスとIPアドレスの両方を条件に組み合わせたAC
ACL name	アクセスリスト名を選択します。
Attached Direction	ACLを適用するトラフィックの方向を選択します。 ・ingress:ポートに入ってくるトラフィック(入力方向)にACLを適用する。 ・ingress/traffic-statistics:入力方向にACLを適用し、そのトラフィックの統計情報を収集する。

- 各項目を設定した後、<Apply>ボタンをクリックして設定を確定すると、内容が更新されます。
- 既存の情報を削除する場合は、対象エントリに☑を入れて<Delete>ボタンをクリックしてください。

3.7. Ring Network (リング型ネットワーク)

リング状に接続するトポロジーのネットワーク構成や冗長性を管理します。

3.7.1. Spanning-tree (スパニングツリー)

リング型ネットワーク構成では、ケーブルの接続ミスや機器の故障によってループが発生し、通信障害を引き起こす可能性があります。スパニングツリープロトコル(STP)は、このようなループを自動的に検出し、特定のポートをブロックすることでループの発生を防ぎ、ネットワークの安定性を高める機能です。

1 Global Properties (グローバル設定)

グローバル設定でSTPやリングネットワークの設定手順について説明します(デフォルト設定:無効)。スパニングツリー環境での動作効率や安定性を調整する際に役立ちます。

1. 「Ring Network」→「Spanning-tree」→「Global Properties」をクリックすると、以下の画面が表示されます。

Global Properties

This page is used to configure the global basic parameters of the spanning tree.

Enabled Off

2. 「Global Properties」メニューを「On」に設定すると、次の画面が表示されます。本機能を有効(On)に設定すると、次の画面が表示されます。

Global Properties

This page is used to configure the global basic parameters of the spanning tree.

Enabled <input checked="" type="radio"/>		
Mode	MSTP	▼
Cost Format	dot1t	▼
Forward Time	15	Sec(4-30, default 15)
Hello Time	2	Sec(1-10, default 2)
Max Age Time	20	Sec(6-40, default 20)
Max Hop Time	20	(1-40, default 20)
Priority	32768	(0-61440, default 32768)
TC Flush	Flush	▼

Apply

メニュー	説明
Mode	スパニングツリープロトコルタイプ(MSTP/STP/RSTP)を選択します。
Cost Format	リンクのコスト(パスコスト)の計算形式(dot1t/dot1d)を指定します
Forward Time	ポートが「Blocking」状態から「Forwarding」状態に移行するまでの合計

※	時間(秒)を表します (値の有効範囲:4~30秒、デフォルト値:15)。
Hello Time ※	BPDUを送信する間隔(秒)を表します (値の有効範囲:1~10秒、デフォルト値:2)。
Max Age Time ※	BPDU情報が有効期間の最大時間(秒)を表します (値の有効範囲:6~40秒、デフォルト値:20)。
Max Hop Time ※MSTP設定	BPDUが転送される最大ホップ数を表します (値の有効範囲:1~40、デフォルト値:20)。
Priority	ブリッジ(スイッチ)のルート選出の優先度を設定します。 値が小さいほど優先度が高くなります。 (値の有効範囲:0~61440(4096単位)、デフォルト値:32768)。
TC Flush	トポロジーチェンジを検出時のアクションを選択します。 ・No Flush:転送データベースをクリアしません ・Flush:転送データベースをクリアします。 ・Limit:フラッシュの動作を制限付きで実行します。

- ※ STPが正しく機能するためには、Forward Time、Hello Time、Max Age Time の値が以下の関係を満たすように設定する必要があります。
- ・ $2 \times (\text{Forward Time} - 1\text{秒}) \geq \text{Max Age Time}$
 - ・ $\text{Max Age Time} \geq 2 \times (\text{Hello Time} + 1\text{秒})$
- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定すると、テーブルの内容が更新されます。

2 Instance Mapping (インスタンスのマッピング)

MSTP環境では、複数のVLANをグループ化し、それぞれのグループ(インスタンス)に対して個別のスパンニングツリーを構成できます。これにより、VLANごとに異なる通信経路を設定したり、特定のインスタンスのルートブリッジを制御したりすることが可能になり、ネットワークリソースの効率的な利用や負荷分散が実現できます。

「Ring Network」→「Spanning-tree」→「Instance Mapping」をクリックすると、以下の画面が表示されます。

Instance Mapping

This page is used to generate tree instance mapping vlan configuration.

Instance Mapping Config		
Instance	0	
Operation	Add	
VLAN List		(1-4094, for example: 1,3-6)
Priority		(0-61440, default 32768)

[Apply](#)

Instance Mapping Status

Showing 10 Entries Showing 1 to 1 of 1 entries Search

Instance	VLAN List	Priority
0	1-4094	32768

[First](#) [Previous](#) [1](#) [Next](#) [Last](#)

メニュー	説明
Instance	インスタンス番号を指定します (値の有効範囲: 0-64)。
Operation	インスタンスに対して実行する操作を指定します。 <ul style="list-style-type: none"> ・Add: 新規の設定情報を追加します。 ・Delete: 既存の設定情報を削除します。
VLAN List	指定したインスタンスにマッピングするVLANのリストを定義します (値の有効範囲: 1-4094)。
Priority	MSTPモード時、指定したインスタンスの優先度を指定します (有効範囲: 0-61440, デフォルト値: 32768)

※デフォルトでは、すべてのVLANがインスタンス0に所属しています。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定すると、テーブルの内容が更新されます。
- 既存の情報を削除する場合は、対象エントリにを入れて<Delete>ボタンをクリックしてください。

各画面で表示するエントリ数をドラッグして設定できます
(オプション: 全件 / 10件 / 30件 / 50件 / 100件、デフォルト: 10件)
画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- ↑: 上に移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

3 Instance Properties (インスタンスプロパティ)

MSTPリージョン内で使用するMSTPの情報(ドメイン名、リビジョンレベル、VLANとインスタンスのマッピング)を設定します。これらの設定は、リージョン内のすべてのスイッチで一致させる必要があります。

「Ring Network」→「Spanning-tree」→「Instance Properties」をクリックすると、以下の画面が表示されます。

Instance Properties

This page is used for spanning tree instance parameter configuration.

Instance Properties Configuration	
Field Name	<input type="text" value="deletion"/> (1-32 characters, and cannot special char(!%#\$&< >+"?'), not entering indicates)
Revision-level	<input type="text" value="0"/> (0-65535)

Apply

Field Name	Revision-level
	0

メニュー	説明
Field name	MSTP ドメイン名を設定します(値の有効範囲: 1-32文字)。 ※特殊文字(!%#\$&< >+"?)は使用できません 削除する場合は、空欄のままApplyを押してください。
Revision-level	MSTP リビジョンのレベルを設定します(値の有効範囲: 0-65535)

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定すると、テーブルの内容が更新されます。

各画面で表示するエントリ数をドラッグして設定できます
(オプション: 全件 / 10 件 / 30 件 / 50 件 / 100 件、デフォルト: 10 件)
画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

4 Port Config (ポート設定)

ポートごとにスパンニングツリー(STP)を設定します。特定ポートでのSTP無効化や、エッジポート設定による動作の最適化が可能です。

【注記】:

この機能を有効にするには、グローバル設定にてスパンニングツリー機能を有効にしてください(設定方法については、「[1 Global Properties](#)」の項を参照してください)。

1. 「Ring Network」 → 「Spanning-tree」 → 「Port Config」をクリックすると、以下の画面が表示されます。

Port Config

This page is used to generate tree port parameter configuration.

Port	--Please select --						
Status	Enabled ▼						
BPDU	Disabled ▼ (Aggregation port not supported)						
Edge Port	Disabled ▼						
Point-to-Point	Auto ▼						
Packet Format	Auto ▼						
Digest Snooping	Disabled ▼						
TC Flush	Default ▼ (Default to global TC FLUSH value)						

Port	Status	BPDU	Edge Port	Point-to-Point	Packet Format	Digest Snooping	TC Flush
Ethernet1/0/1	Enabled	Disabled	Disabled	Auto	Auto	Disabled	Flush
Ethernet1/0/2	Enabled	Disabled	Disabled	Auto	Auto	Disabled	Flush
Ethernet1/0/3	Enabled	Disabled	Disabled	Auto	Auto	Disabled	Flush
Ethernet1/0/4	Enabled	Disabled	Disabled	Auto	Auto	Disabled	Flush
Ethernet1/0/5	Enabled	Disabled	Disabled	Auto	Auto	Disabled	Flush
Ethernet1/0/8	Enabled	Disabled	Disabled	Auto	Auto	Disabled	Flush

メニュー	説明
Port	対象のポート番号を選択します。 <input type="checkbox"/> Select All/Unselectに <input checked="" type="checkbox"/> を入れると、すべてのポートを選択、または解除することができます。
Status	ポートごとのスパンニングツリー機能を有効化/無効化します。 ・Enable: スパンニングツリー機能を有効にします。 ・Disable: スパンニングツリー機能を無効にします。
BPDU	BPDU (Bridge Protocol Data Unit) 送受信するVLANを指定します ・Disabled: VLANベースBPDU送受信機能を無効にします ・VLAN: 1-4094: BPDUの処理を特定のVLANに紐づけて有効にします。
Edge Port	ポートをエッジポート(高速転送開始モード)として設定するかどうかを指定します ・Disabled: エッジポート機能を無効にします。 ・Enabled: エッジポート機能を有効にします。 ・BPDU Filter: エッジポートでBPDU(ブリッジプロトコルデータユニット)の送受信をフィルタリングします。 ・BPDU Guard: エッジポートでBPDUを受信した場合にポートを自動的にシャットダウンします。

Point-to-Point	ポートがポイントツーポイント接続(2台のスイッチ間など)であるかどうかを指定します ・Auto/Disabled/Enabled:
Packet Format	スパニングツリーで使用するBPDUパケットのフォーマットを指定します。 ・Auto:パケット形式を自動的に選択します。 ・Privacy:パケットにプライバシー保護機能を使用します。 ・Standard:標準的なパケット形式を使用します。
Digest Snooping	MSTP特有の機能であり、異なるMSTリージョン間でトポロジー情報交換を有効/無効にします。
TC Flush	トポロジーチェンジを検出した際に、ポートのMACアドレステーブルのアクションを選択します。 ・No Flush: MACアドレステーブルをクリアしません ・Flush: MACアドレステーブルをクリアします。 ・Limit: MACアドレステーブルのクリア動作を制限付きで実行します。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定すると、テーブルの内容が更新されます。
- <Protocol Migration Check>ボタンをクリックすると、スパニングツリープロトコル (STP) の互換性を手動で確認し、必要に応じて調整する処理を開始します。この機能は、ネットワーク内に異なる種類のスパニングツリープロトコルで動作している機器が混在している場合に、スムーズな連携を助けるために特に有効です。

5 Port Instance (ポートインスタンス)

ポートにおけるスパニングツリープロトコル (STP) の詳細な動作を設定します。
STPがネットワーク構成を決定する際に使われる「パスコスト」や「ポート優先度」をポートごとに調整したり、意図しないループやルートブリッジの変更を防ぐための「保護機能」を設定したりできます。

1. 「Ring Network」→「Spanning-tree」→「Port Instance」をクリックすると、以下の画面が表示されます。

Port Instance

This page is used to generate tree port instance parameter configuration.

Instance	0	
Port	--Please select--	
Path Cost	0	(0-200000000)(0=>Auto)
Priority	128	
Port Guard	Auto	

Apply

Instance	Port	Path Cost	Priority	Port Guard
0	Ethernet1/0/1	Auto	128	Auto
0	Ethernet1/0/2	Auto	128	Auto
0	Ethernet1/0/3	Auto	128	Auto
0	Ethernet1/0/4	Auto	128	Auto
0	Ethernet1/0/5	Auto	128	Auto
0	Ethernet1/0/6	Auto	128	Auto
0	Ethernet1/0/7	Auto	128	Auto

メニュー	説明
Instance	ツリーのインスタンス番号を選択します。
Port	対象のポート番号を選択します。 <input type="checkbox"/> Select All/Unselectに☑を入れると、すべてのポートを選択、または解除することができます。
Path Cost	パスコストを指定します(有効範囲:0-200000000)。 ※「0」を設定すると、自動にて選択されます。
Priority	ポートの優先順位を選択します。
Port Guard	ポートに適用する保護機能を選択します。 ・Auto:自動選択します。通常では保護機能を選択しません。 ・Root Guard:接続機器が意図しないルートブリッジとして選択されるのを防ぐ保護機能です。 ・Loop Guard: BPDUが受信されなくなった場合に誤って指定ポート(DP)になり、ループが発生する可能性を防ぐための保護機能です

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定すると、テーブルの内容が更新されます。

6 Status (スパンニングツリーのステータス)

現在動作しているスパンニングツリープロトコル (STP) の詳細な状態を確認できます。ネットワーク全体の構成 (トポロジー) や、各ポートがSTPにおいてどのような状態かといった情報をリアルタイムで把握できます。

1. 「Ring Network」 → 「Spanning-tree」 → 「Status」をクリックすると、以下の画面が表示されます。

Global Properties

This page is used to configure the global basic parameters of the spanning tree.

Enabled Off

2. この機能を有効(Enabled)にすると、次の画面が表示されます。

Running Status Information

Process ID 0 ▼

MSTP Bridge Config Info					
Mode	Bridge MAC	Max Age Time	Hello Time	Forward Time	Force Version
MSTP(IEEE 802.1s)		20s	2s	15s	3

Instance0	
Self Bridge ID	32788. style="background-color: #eee;">
Root ID	32788. style="background-color: #eee;">
Ext.RootPathCost	20000
Region Root ID	this switch
Int.RootPathCost	0
Root Port ID	128.28

Port	ID	Port Path Cost	Ext.RootPathCost	Int.RootPathCost	State	Role	DsgBridge	DsgPort
Ethernet1/0/1	128.001	20000	20000	0	Forward	DSGN	7	128.001
Ethernet1/0/24	128.024	20000	20000	0	Forward	DSGN	7	128.024
Ethernet1/0/28	128.028	20000	0	0	Forward	ROOT	1	128.021

3.7.2. ERPS

ERPSは、ITU-T G.8032規格に準拠したプロトコルで、リング型に接続されたネットワークにおいて、一部に障害が発生した場合でも通信経路を瞬時（通常、50ミリ秒未満）に切り替え、通信の途絶を最小限に抑えるとともに、ネットワークループの発生を防ぐための機能です。

1 ERPS Ring Config (ERPS リング設定)

ERPSリングの定義や、既存リングの基本パラメータ変更を行います。
スパンニングツリーやループ検知が有効なポートでは設定できません。

1. 「Ring Network」 → 「ERPS」 → 「ERPS Ring Config」をクリックすると、以下の画面が表示されます。

ERPS Ring Config

Create or delete ERPS ring.

Topology Change Propagation None

[Apply](#)

Ring Name	<input type="text"/>	(1-64 character)
Version	v2	
Ring-topo	major-ring	
Port1 Config	Yes	
Port0	Ethernet1/0/1	
Port1	Ethernet1/0/2	
R-APS Virtual-Channel	Without	

[Apply](#)

ERPS Config Status Table

Showing 10 Entries Showing 0 to 0 of 0 entries Search

<input type="checkbox"/>	Ring Name	Port0	Port1	Ring-topo	R-APS Virtual-Channel	Version	Instance Count
0 results found.							

[Delete](#) [First](#) [Previous](#) [Next](#) [Last](#)

メニュー	説明
Topology Change Propagation	トポロジー変更を伝播する方式を選択します。 <ul style="list-style-type: none"> ・None: :設定はありません。 ・ERPS:R-APSメッセージを使用して行われます。 ・STP:BPDUメッセージを使用して行われます。
Ring Name	ERPSリング名を設定します(値の有効範囲: 1~64文字)。 ※A (a) ~ Z (z)、_(アンダースコア)、または数字が使用可能です。 先頭に_(アンダースコア)は使用できません。
Version	ERPSのバージョンは、ITU-T G.8032規格に基づくプロトコルの実装レベルを選択します。 <ul style="list-style-type: none"> ・v1: 単一のリング構成のみをサポートする初期バージョンです。 単一のリング内で高速な障害復旧(50ミリ秒未満)を実現します。 ・v2: 複数のリングを組み合わせた構成をサポートする拡張バージョンです。

Ring- topology	ERPSリングの物理的および論理的なトポロジーを選択します。 <ul style="list-style-type: none"> ・major-ring: ERPSリングを主要なリングとして設定します。ネットワークの主経路として機能します。 ・open-ring: ERPSリングをオープンリングとして設定します。特定のノードや条件に応じて動作を調整できます。
Port1 Configure	オープンリング使用時のPort1 の設定有無を選択します。 <ul style="list-style-type: none"> ・Yes: 設定可能/No: 設定不可
Port0	接続するポート0を選択します。ポート1とペアになりリングを構成します。
Port1	接続するポート1を選択します。ポート0とペアになりリングを構成します。
R-APS Virtual-Channel	オープンリング使用時にR-APS仮想チャネルの制御メッセージ(R-APSメッセージ)を送送する専用の論理チャネルを使用するか設定します。 <ul style="list-style-type: none"> ・Without: この ERPS リングに R-APS 仮想チャネルは使用しません。 ・With: この ERPS リングに R-APS 仮想チャネルが使用します。

- 各項目の設定後に<Apply>ボタンをクリックすると、設定内容が確定され、反映されます。
- 既存の情報を削除する場合は、対象エントリに☑を入れて<Delete>ボタンをクリックしてください。

各画面で表示するエントリ数をドラッグして設定できます

(オプション: 全件 / 10 件 / 30 件 / 50 件 / 100 件、デフォルト: 10 件)

画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

2 ERPS Instance Config(ERPS インスタンスの設定)

物理的なERPSリング上で動作する、論理的な保護単位である「ERPSインスタンス」の詳細設定を行います。この機能により、1つの物理リング上で複数の独立した保護インスタンスを構成します。

「Ring Network」→「ERPS」→「ERPS Instance Config」をクリックすると、以下の画面が表示されます。

ERPS Instance Config

Ring Name	FXC	▼
Instance ID	1	▼
Control VLAN	VLAN0002	▼
Ring ID	1	▼
R-APS MEL	7	▼
Description		(1-64 characters)
Revertive Mode	Revertive	▼
Protected Instance		(0-64,use '-' and ',' splice,for example:1;3-5)
WTR Timer	5	(1-12min,default 5)
Guard Timer	50	(1-200ms,default 50)
Holdoff Timer	0	(0-10s,default 0)
Port0 Role	Common	▼
Port1 Role	Common	▼

[Apply](#)

ERPS Config Status Table

メニュー	説明
Ring Name	ERPS リング名を選択します
Instance ID	ERPS リング インスタンス ID を作成します (値の有効範囲: 1 ~ 16)。
Control Vlan	R-APS パケットの VLAN IDを選択します(値の有効範囲: 2 ~ 4094)。
Ring ID	ERPSのリング IDを選択します(値の有効範囲: 1 ~ 64)。
R-APS MEL	APS パケットのレベル値を選択します(値の有効範囲: 1 ~ 7)。
Description	ERPS インスタンス名を設定します (最大文字列は 64文字以内、かつ数字および下線を使用)。 ※最初と最後の文字に下線を使用することはできません。
Revertive Mode	リングネットワークの障害が復旧した際に、通信経路を障害発生前の状態に自動的に戻すかどうかを設定します。 ・Non-Revertive: 障害が復旧した後も、切り替わった経路のまま通信を継続します。 ・Revertive: 障害が復旧した後、WTRタイマー値の時間が経過すると、自動的に障害発生前の経路に通信が戻ります。 【注記】: ・ERPS リングが ERPSv1で動作している場合は設定できません。 ・サブリングの場合、RPL オーナーノードでのみ設定できます。
Protect Instance	ERPS リング インスタンスによって保護されている MSTP インスタンスのリストを入力します。
WTR Timer	障害が復旧してから実際に元の経路に切り戻すまでの待機時間を設定します (値の有効範囲: 1 ~ 12 分、デフォルト値: 5 分)。

Guard Timer	古い制御信号 (R-APSメッセージ) を誤って受信し、誤動作や一時的なループが発生することを防ぐためのタイマーです(値の有効範囲: 1 ~ 200ミリ秒、デフォルト: 50ミリ秒)。
Holdoff Timer	ネットワークの障害検出時に、ERPSの経路切替動作を開始するまでの遅延時間を設定します(値の有効範囲: 0 ~ 10 秒、デフォルト値: 0)。
Port0/1 Role	リング内の各ノードの役割を設定します。 <ul style="list-style-type: none"> ・Owner: リング保護リンク(RPL)のオーナーノードとして機能します ・Neighbour: RPLネイバーノード(オーナーと隣接)ノードとして機能します ・Common: 通常のリングノードとして機能します(デフォルト設定)。

- 各項目の設定後に<Apply>ボタンをクリックすると、設定内容が確定され、反映されます。

各画面で表示するエントリ数をドラッグして設定できます

(オプション: 全件 / 10 件 / 30 件 / 50 件 / 100 件、デフォルト: 10 件)

画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

3 View ERPS Statistics(ERPS 統計情報ビュー)

ERPSリングの動作状態やパフォーマンスを監視するための統計情報を表示します。
リングの健全性や障害時の挙動を把握し、トラブルシューティングや最適化に役立ちます。

「Ring Network」→「ERPS」→「View ERPS Statistics」をクリックすると、以下の画面が表示されます。

View ERPS Statistics

ERPS Instance Table

Showing Entries Showing 0 to 0 of 0 entries

Ring Name	Instance ID	Instance Port	Port Role	Port Status	Signal Status	Node Id	BPR	nrTx	nrRx	rbTx	rbRx	fsTx	fsRx	msTx	msRx	sfTx	sfRx	eventTx	eventRx	totalTx	totalRx
0 results found.																					

[First](#) [Previous](#) [Next](#) [Last](#)

メニュー	説明
Ring Name	対象の ERPS リング名を表示します。
Instance ID	対象の ERPS リングのインスタンス IDを表示します。
Intance Port	ERPS リングのメンバー ポートを表示します。
Port Role	ERPS リング ノードの役割を表示します。 ・RPL 所有者、 ・RPL ネイバー
Port Status	ポートのステータスを表示します。 ・Blocked: ポートはブロック状態 ・forwarding: ポートは転送状態
Signal Status	ERPS リング ポートの障害状態を表示します。 ・Non-failed: 障害なし ・Failed: 障害発生
Nodeid	リング内で最後に通信またはイベントに関与したノードの識別子(Node ID)を表示します。
BPR	ERPS リング ポートによって保存された受信側の最後の R-APS によって伝送されるブロックリンク情報を表示します(ブロック対象はポート 0、またはポート 1)。
nrTX	NRの送信統計情報を表示します。
nrRX	NRの受信統計情報を表示します。
rbTX	RBの送信統計情報を表示します。
rbRX	RBの受信統計情報を表示します。
fsTX	FSの送信統計情報を表示します。
fsRX	FSの受信統計情報を表示します。
msTX	MSの送信統計情報を表示します。
msRX	MSの受信統計情報を表示します。
sfTX	SFの送信統計情報を表示します。
sfRX	SFの受信統計情報を表示します。
eventTX	イベントの送信統計情報を表示します。
eventRX	イベントの受信統計情報を表示します。
totalTX	総送信統計情報(全体のデータ送信量)を表示します。
totalRX	総受信統計情報(全体のデータ受信量)を表示します。

3.8. Route Config (ルーティング設定)

ルーティングを設定します。

3.8.1. Static Route (スタティックルート)

スタティックルートを設定することで、特定の宛先ネットワークへのパケットをどの経路で転送するかを静的に指定できます(デフォルト設定:無効)。

1.「Route Config」→「Static Route」をクリックすると、以下の画面が表示されます。

Static Route

Destination IP Address	<input type="text"/>
Mask Or Prefix-length	<input type="text"/>
Nexthop Or null0	<input type="text"/>
Distance	1 <input type="text"/>

Static Routing Configuration Status Table

Showing 10 Entries Showing 1 to 1 of 1 entries Search

<input type="checkbox"/>	Destination IP Address/Mask	Nexthop Or null0	Distance	State
<input type="checkbox"/>	0.0.0.0/0	192.168.11.1	1	Connected

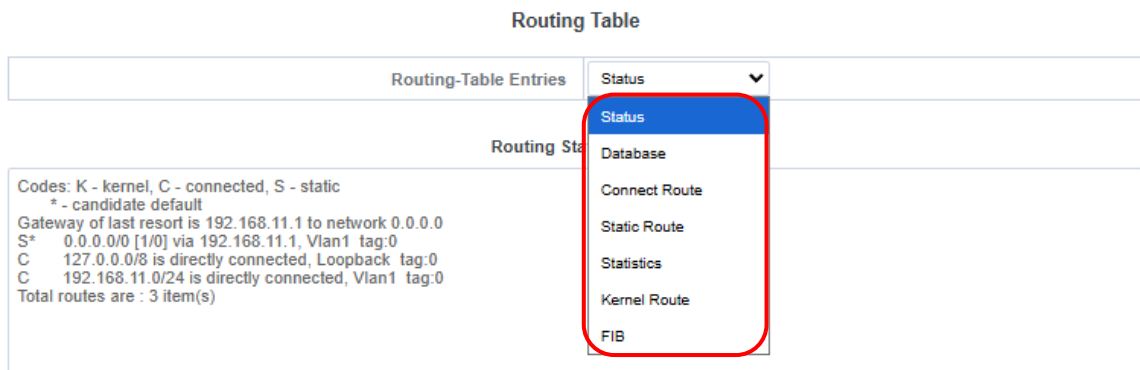
メニュー	説明
Destination IP Address	宛先IP アドレスを設定します。 デフォルトルート(ゲートウェイ)の場合は0.0.0.0 (/0)を設定します。
Mask Or Prefix-length	宛先ネットワークの範囲を設定します (サブネットマスク:255.255.255.0、プレフィックス長:/24)。
Nexthop Or null0	パケット転送先(ネクストホップ)のIPアドレスを設定します。 ・Nexthop: パケットを次に転送するルーターのIPアドレスを入力します。 ・null0: パケットを破棄するルート情報を登録します。
Distance	ルートの優先順位を決定するためのAD値を設定します。 (値の有効範囲: 1-255、デフォルト値:1)

- 各項目を設定した後、<Apply>ボタンをクリックして設定を確定すると、内容が更新されます。
- 既存の情報を削除する場合は、対象エントリにを入れて<Delete>ボタンをクリックしてください。

3.8.2. Routing Table (ルーティングテーブル)

本機器が保持しているルーティングテーブル (経路情報の一覧) の内容や状態を表示します。
 管理・表示可能なルーティングテーブルのエントリ数 (経路情報の数) には上限があります。
 経路情報が上限の512エントリを超える場合は、正しく処理されない場合がありますのでご注意ください。

「Route Config」 → 「Routing Table」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
Routing-Table Entries	<p>ルーティングテーブルのエントリを選択すると、その情報がテーブルに表示されます。</p> <ul style="list-style-type: none"> ・Status: 現在のルーティングテーブル ・Database: ルーティングプロトコルが管理するルート情報のデータベース ・Connect Route: 直接接続しているコネクトルート ・Static Route: スタティックルート ・Statistics: ルーティングテーブルの状態に関する統計情報 ・Kernel Route: オペレーティングシステムのカーネルが管理するルート情報 ・FIB: ルーティングテーブル(RIB)から実際にパケットを転送するために使われる情報

3.9. Multicast Manage (マルチキャスト管理)

マルチキャスト通信制御の設定やグループ管理を行います。

3.9.1. IGMP Snooping Config (IGMP スヌーピングの設定)

1 Basic Config (IGMP スヌーピング基本設定)

IGMPスヌーピング機能の有効/無効を設定します(デフォルト設定:無効)。IGMPスヌーピングは、マルチキャストグループへの参加状況を監視し、必要なポートのみにマルチキャストトラフィックを転送することで、ネットワーク帯域の効率的な利用をサポートする機能です。また、既存のVLANインターフェースおよび各インターフェースにおけるIGMPスヌーピングの動作状態を表示します。

1. 「Multicast Manage」→「IGMP Snooping Config」→「Basic Config」をクリックすると、以下の画面が表示されます。

2. この機能を有効にすると、VLAN IDを選択することができます。

メニュー	説明
Status	IGMPスヌーピング機能を有効/無効に設定します。
VLAN ID	対象のVLAN IDを選択します。 <input type="checkbox"/> Select All/Unselectに <input checked="" type="checkbox"/> を入れると、すべてのポートを選択、または解除することができます。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定してください。
- 既存の情報を削除する場合は、対象エントリにを入れて、<Delete>ボタンをクリックしてください。

2 Static Router Port (スタティックルーターポート)

IGMPスヌーピングが有効な環境では、マルチキャストトラフィックを配信するマルチキャストルータが接続されているポートを「スタティックルーターポート」として手動で指定できます。通常、IGMPスヌーピングはルータからのIGMPクエリを受信することでルーターポートを動的に学習しますが、この設定を行うことで、特定のポートを常にルーター接続ポートとして静的に扱うことが可能です。その結果、指定したポートには常にマルチキャストデータが転送され、安定したマルチキャスト配信を実現します。

「Multicast Manage」→「IGMP Snooping Config」→「Static Router Port」をクリックすると、以下の画面が表示されます。

Static Router Port Config

This page is used to configure static routing ports and corresponding aging time

VLAN ID	<input type="text" value="--Please select --"/>
Static Router Port	<input type="text" value="--Please select --"/>
Operation Type ?	<input type="text" value="Not Set"/>
Alive Time	<input type="text" value="255"/> (1-65535,Default:255)

VLAN Based Routing Port List

Showing Entries Showing 0 to 0 of 0 entries Search

VLAN ID	Router Port ?	Alive Time
0 results found.		

メニュー	説明
VLAN ID	対象のVLAN IDを選択します。
Static Router Port	対象のスタティックルーターポートに割り当てるポートを選択します。
Operational Type	スタティックルーターポートの操作の種類を選択します。 <ul style="list-style-type: none"> ・Not Set :スタティックルーターポートの設定は行いません。 ・Del:既存のスタティックルーターポートの設定を削除します。 ・Add:新しいスタティックルーターポートを追加します。
Alive Time	ダイナミックルーターポートの有効時間を設定します (値の有効範囲:1-65535、デフォルト値:255)。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定してください。

3 VLAN Config (VLAN の設定)

VLANごとに、IGMPスヌーピングのより詳細な動作パラメータを設定する手順について説明します。これにより、各VLANのネットワーク特性や要件に合わせて、マルチキャストトラフィックの制御できます。

「Multicast Manage」→「IGMP Snooping Config」→「VLAN Config」をクリックすると、以下の画面が表示されます。

VLAN Config

This page is used to configure IGMP SNOOPING VLAN related parameters

VLAN ID	--Please select--	
Immediate leave	Enabled ▼	
L2-general-Querier	Enabled ▼	
Group number	50	(1-65535,Default:50)
Source Table Number	40	(1-65535,Default:40)

[Apply](#)

IGMP VLAN Configuration List

Showing 10 ▼ Entries Showing 0 to 0 of 0 entries Search

VLAN ID	Immediate leave	L2-general-Querier	Group number	Source Table Number
0 results found.				

[First](#) [Previous](#) [Next](#) [Last](#)

メニュー	説明
VLAN ID	対象のVLAN IDを選択します。
Immediate leave	VLAN の IGMP 高速離脱機能(ファーストリープ)の設定を有効/無効に設定します。
L2-general-querier	IGMPクエリア機能を有効/無効に設定します。
Group number	このVLAN内で、IGMPスヌーピングが学習・管理できるマルチキャストグループの最大数を設定します。 (デフォルト値:50、値の有効範囲:1 ~ 65535)。
Source Table Number	各マルチキャストグループが保持できる送信元ソース情報のエントリ数の上限を設定します(デフォルト値:40、値の有効範囲:1 ~ 65535)。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定してください。

4 Querier Config (IGMP スヌーピング クエリア)

IGMPスヌーピング環境において、スイッチがIGMPクエリアとして動作する場合の、その動作パラメータを設定します。IGMPクエリアは、VLAN内のマルチキャストグループメンバーシップ情報を維持するために、定期的にIGMP Query (問い合わせ) メッセージを送信する役割を担います。

「Multicast Manage」→「IGMP Snooping Config」→「Querier Config」をクリックすると、以下の画面が表示されます。

Querier Config

This page is used to configure query related parameters

VLAN ID	<input type="text" value="--Please select --"/>	
Query-Interval	<input type="text" value="125"/>	(1-65535,Default:125)
Query-Mrsp-Max	<input type="text" value="10"/>	(1-25,Default:10)
Query-Robustness	<input type="text" value="2"/>	(2-10,Default:2)
Suppression-Query-Time ?	<input type="text" value="255"/>	(1-65535,Default:255)

Querier Configuration List

Showing Entries Showing 0 to 0 of 0 entries Search

VLAN ID	Query-Interval	Query-Mrsp-Max	Query-Robustness	Suppression-Query-Time ?
0 results found.				

メニュー	説明
VLAN ID	対象のVLAN IDを選択します。
Query-Interval	IGMP ジェネラル クエリ間隔を設定します (値の有効範囲: 1 ~ 65535、デフォルト値:125)。
Query-Mrsp Max	グループ クエリの最大応答待機時間を設定します (値の有効範囲: 1 ~ 25、デフォルト値:10)。
Query-Robustness	ネットワークのパケットロスに対する耐性を示す値を設定します (値の有効範囲: 2 ~ 10、デフォルト値:2)。
Suppression-Query-Time configuration	本機がクエリアとして動作を開始するまでの待機時間、自身のQuery送信を抑制する時間を設定します。 (値の有効範囲: 1 ~ 65535、デフォルト値:255) 【注記】: クエリ抑制時間が設定されていない場合: クエリ抑制時間 (秒) = (クエリ送信間隔 × 堅牢性(耐性)変数) + (最大応答時間 / 2)

- 各項目を設定した後、<Apply>ボタンをクリックして設定を確定すると、内容が更新されます。

5 Multicast Table (マルチキャストテーブル)

マルチキャストテーブル情報が表示されます。

IGMPスヌーピングを介してマルチキャストトラフィックの管理や監視を行う際に役立ちます。

【注記】:

この機能を設定には、IGMP スヌーピング機能を有効にしてください(「[1 Basic Config \(基本設定\)](#)」を参照)。

「Multicast Manage」→「IGMP Snooping Config」→「Multicast Table」をクリックすると、以下の画面が表示されます。

Multicast Table

This page is used to view the multicast table

VLAN ID Not VLAN ▼

Apply

VLAN ID	Group IP	Source IP	Member Port
Not VLAN ▼	<input type="text" value="Example:224.1.1.1"/>	<input type="text" value="Example:10.10.10.1"/>	--Please select --
Add		Del	

Multicast table

Showing 10 Entries Showing 0 to 0 of 0 entries Search

Number	Group IP	Source IP ?	Member Port	Exptime	Source MAC	Version
0 results found.						

First
Previous
Next
Last

メニュー	説明
VLAN ID	対象のVLAN IDを選択します。
Group IP	マルチキャストグループのIPアドレスを表示します。 これは、特定のマルチキャストトラフィックが送信される宛先アドレスです。
Source IP	マルチキャストデータの送信元となるIPアドレスを表示します。 どのデバイスがデータを送っているかを特定できます。
Member Port	マルチキャストグループに参加しているポート(メンバー)を示します。 ネットワーク内でどのポートがマルチキャストトラフィックを受信しているかを確認できます。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定してください。

3.9.2. MLD Snooping Config (MLD スヌーピング設定)

1 Basic Config (MLD スヌーピング基本設定)

IPv6環境におけるマルチキャストトラフィックの効率化を行うために、MLDスヌーピング機能の有効/無効を設定します(初期状態：無効)。MLDスヌーピングは、MLD (Multicast Listener Discovery) メッセージを監視し、必要なポートにのみIPv6マルチキャストトラフィックを転送することで、ネットワーク帯域を効率的に利用できるようにする機能です。

「Multicast Manage」→「MLD Snooping Config」→「Basic Config」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
Status	MLDスヌーピング機能を有効/無効に設定します。
VLAN ID	対象のVLAN IDを選択します。 <input type="checkbox"/> Select All/Unselectに <input checked="" type="checkbox"/> を入れると、すべてのポートを選択、または解除することができます。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定すると、テーブルの内容が更新されます。
- 既存の情報を削除する場合は、対象エントリにを入れて<Delete>ボタンをクリックしてください。

2 Static Router Port (スタティックルータポート)

MLDスヌーピングが有効な環境では、マルチキャストトラフィックを配信するマルチキャストルータが接続されているポートを「スタティックルータポート」として手動で指定できます。通常、MLDスヌーピングはルータからのMLDクエリを受信することでルータポートを動的に学習しますが、この設定により、特定のポートを常にルータ接続ポートとして扱うことが可能です。結果として、指定したポートには常にマルチキャストデータが転送され、安定したマルチキャスト配信を実現します。

MLDスヌーピングが有効な環境で、マルチキャストトラフィックを配信するマルチキャストルータが接続されているポートを「スタティックルータポート」として手動で指定します。MLDスヌーピングはルータからのMLDクエリを受信することでルータポートを動的に学習しますが、この設定を行うことで、特定のポートを常にルータ接続ポートとして固定的に扱うことができます。結果として、その指定ポートには常にマルチキャストデータが転送されるようになり、安定したマルチキャスト配信を行います。

「Multicast Manage」→「MLD Snooping Config」→「Static Router Port」をクリックすると、以下の画面が表示されます。

Static Router Port Config

This page is used to configure static routing ports and corresponding aging time

VLAN ID	<input type="text" value="--Please select --"/>	
Static Router Port	<input type="text" value="--Please select --"/>	
Operation Type ?	Not Set <input type="button" value="v"/>	
Alive Time	<input type="text" value="255"/>	(1-65535,Default:255)

VLAN Based Routing Port List

Showing Entries Showing 0 to 0 of 0 entries Search

VLAN ID	Router Port ?	Alive Time
0 results found.		

メニュー	説明
VLAN ID	対象のVLAN IDを選択します。
Static Router Port	対象のスタティックルータポートに割り当てるポートを選択します。
Operational Type	スタティックルータポートの操作の種類を選択します。 <ul style="list-style-type: none"> ・Not Set :スタティックルータポートの設定は行いません。 ・Del:既存のスタティックルータポートの設定を削除します。 ・Add:新しいスタティックルータポートを追加します。
Alive Time	ダイナミックルータポートの有効時間を設定します (値の有効範囲:1-65535、デフォルト値:255)。

- 各項目の設定後に<Apply>ボタンをクリックすると、設定内容が確定され、反映されます。

3 VLAN Config (VLAN の設定)

VLANごとに、MLDスヌーピングのより詳細な動作パラメータを設定する手順について説明します。各VLANのネットワーク特性や要件に合わせて、マルチキャストトラフィックの制御を行えます。

「Multicast Manage」→「MLD Snooping Config」→「VLAN Config」をクリックすると、以下の画面が表示されます。

VLAN Config

This page is used to configure MLD SNOOPING VLAN related parameters!

VLAN ID	--Please select --	
Immediate leave	Enabled	▼
L2-general-Querier	Enabled	▼
Group number	50	(1-65535,Default:50)
Source Table Number	40	(1-65535,Default:40)

Apply

MLD VLAN Config List

Showing 10 Entries Showing 0 to 0 of 0 entries Search

VLAN ID	Immediate leave	L2-general-Querier	Group number	Source Table Number
0 results found.				

First Previous Next Last

メニュー	説明
VLAN ID	対象のVLAN IDを選択します。
Immediate leave	VLAN の MLD 高速離脱機能(ファーストリーブ)の設定を有効/無効に設定します。
L2-general-querier	IGMPクエリア機能を有効/無効に設定します。
Group number	このVLAN内で、MLDスヌーピングが学習・管理できるマルチキャストグループの最大数を設定します。 (デフォルト値:50、値の有効範囲:1 ~ 65535)。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定すると、テーブルの内容が更新されます。
- 既存の情報を削除する場合は、対象エントリに☑を入れて<Delete>ボタンをクリックしてください。

4 Querier Config (クエリア情報の設定)

MLDスヌーピング環境において、スイッチがMLDクエリアとして動作する場合の、その動作パラメータを設定します。MLDクエリアは、VLAN内のマルチキャストグループメンバーシップ情報を維持するために、定期的にMLD Query (問い合わせ) メッセージを送信する役割を担います。

「Multicast Manage」→「MLD Snooping Config」→「Querier Config」をクリックすると、以下の画面が表示されます。

Querier Config

This page is used to configure query related parameters

VLAN ID	--Please select--	
Query-Interval	125	(1-65535,Default:125)
Query-Mrsp-Max	10	(1-25,Default:10)
Query-Robustness	2	(2-10,Default:2)
Suppression-Query-Time	255	(1-65535,Default:255)

[Apply](#)

Querier Config List

Showing 10 Entries Showing 0 to 0 of 0 entries Search

VLAN ID	Query-Interval	Query-Mrsp-Max	Query-Robustness	Suppression-Query-Time
0 results found.				

[First](#) [Previous](#) [Next](#) [Last](#)

メニュー	説明
VLAN ID	対象のVLAN IDを選択します。
Query-Interval	MLD ジェネラル クエリ間隔を設定します (値の有効範囲: 1 ~ 65535、デフォルト値:125)。
Query-mrsp configuration	グループ クエリの最大応答待機時間を設定します (値の有効範囲: 1 ~ 25、デフォルト値:10)。
Query-robustness configuration	ネットワークの packet loss に対する耐性を示す値を設定します (値の有効範囲: 2 ~ 10、デフォルト値:2)。
Suppression-query-time configuration	本機がクエリアとして動作を開始するまでの待機時間、自身の Query 送信を抑制する時間を設定します。 (値の有効範囲: 1 ~ 65535、デフォルト値:255)
	【注記】: クエリ抑制時間が設定されていない場合: クエリ抑制時間 (秒) = (クエリ送信間隔 × 堅牢性(耐性)変数) + (最大応答時間 / 2)

- 各項目を設定した後、<Apply>ボタンをクリックして設定を確定すると、内容が更新されます。

5 Multicast Table (マルチキャストテーブル)

マルチキャストテーブル情報を表示します。
DSCPと内部優先度のマッピング関係を設定するために使用されます。

「Multicast Manage」→「MLD Snooping Config」→「Multicast Table」をクリックすると、以下の画面が表示されます。

Multicast Table

This page is used to view the multicast table

VLAN ID Not VLAN ▼

Apply

VLAN ID	Group IP	Source IP	Member Port
Not VLAN ▼	<input style="width: 80%;" type="text"/> Example: ff01::1	<input style="width: 80%;" type="text"/> Example: 2001::1234	--Please select--
Add		Del	

Multicast table

Showing 10 Entries Showing 0 to 0 of 0 entries Search

Number	Group IP	Source IP ?	Member Port	Exptime	Version
0 results found.					
First Previous Next Last					

メニュー	説明
VLAN ID	対象のVLAN IDを選択します。
Group IP	マルチキャストグループのIPアドレスを表示します。 これは、特定のマルチキャストトラフィックが送信される宛先アドレスです。
Source IP	マルチキャストデータの送信元となるIPアドレスを表示します。 どのデバイスがデータを送っているかを特定できます。
Member Port	マルチキャストグループに参加しているポート(メンバー)を示します。 ネットワーク内でどのポートがマルチキャストトラフィックを受信しているかを確認できます。
Exptime	有効期限を表示します。
Version	バージョンを表示します。

- 各項目を設定した後、<Apply>ボタンをクリックして設定を確定すると、内容が更新されます。
- 各項目を設定した後、<Add>ボタンをクリックして設定内容を確定すると、内容が更新されます。
- 既存の情報を削除する場合は、対象エントリに☑を入れて<Delete>ボタンをクリックしてください。

3.10. QoS Config (QoS の設定)

サービス品質 (Quality of Service) を管理し、ネットワーク上を流れる様々なトラフィックの優先制御や帯域制御の設定を行います。

3.10.1. Port Config (ポートの設定)

1 Trust Config (Trust ルールの設定)

ポートごとに、受信するトラフィックのどの優先度情報を信頼してQoS処理を行うか(Trustルール)を設定します。

「QoS Config」→「Port Config」→「Trust Config」をクリックすると、以下の画面が表示されます。

Trust Config

This page is used to set port trust configuration

Port	--Please select --
Trust Class	COS ▼
Operation Type	Add ▼

Apply

Port	Trust Class
Ethernet1/0/1	COS
Ethernet1/0/2	COS
Ethernet1/0/3	COS
Ethernet1/0/4	COS
Ethernet1/0/5	COS
Ethernet1/0/6	COS

メニュー	説明
Port	対象のポート番号を選択します。 <input type="checkbox"/> Select All/Unselectに <input checked="" type="checkbox"/> を入れると、すべてのポートを選択、または解除することができます。
Trust class	どの優先度情報を基に、内部的なQoS処理を行うかを選択します。 ・COS: Cos値を基に内部優先度を決定します。 ・DSCP: DSCP値を基に内部優先度を決定します。
Operation	操作方法を選択します。 ・Add: ポートの新規ルールを追加します。 ・Del: ポートの既存ルールを削除します。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定すると、テーブルの内容が更新されます。

2 Weight Config (パケットの優先順位)

各ポートからパケットを送信する際のスケジューリング方式 (どの優先度のパケットから送信するか) と、各優先度キュー に割り当てる「重み」を設定します。

「QoS Config」 → 「Port Config」 → 「Weight Config」をクリックすると、以下の画面が表示されます。

Weight Config

This page is used to set the port scheduling mode and queue weights

Scheduling Type	sp	
Port	sp	--Please select --
Weight1	wrr	weight(0-127)
Weight2	wrr	weight(0-127)
Weight3	3	weight(0-127)
Weight4	4	weight(0-127)
Weight5	5	weight(0-127)
Weight6	8	weight(0-127)
Weight7	7	weight(0-127)
Weight8	8	weight(0-127)

Apply

メニュー	説明
Port	対象のポート番号を選択します。 <input type="checkbox"/> Select All/Unselectに <input checked="" type="checkbox"/> を入れると、すべてのポートを選択、または解除することができます。
Schedule algorithm	QoSでトラフィックの優先順位や帯域幅を管理する際に使用されます (デフォルト設定: sp)。 <ul style="list-style-type: none"> ・sp: 高優先度のトラフィックがすべて処理されるまで、低優先度のキューは待機します。 ・wrr: 各キューに「重み (Weight)」を割り当て、その重みに応じた順番と量でトラフィックを処理します。 ・wrrr :WRRの改良版で、パケットサイズの違いを考慮してより公平に帯域を分配します。
Weight1~8 ※キュー番号	キューの重み値を設定します。 (値の有効範囲:0 ~ 127)

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定すると、テーブルの内容が更新されます。

1) spモード選択時

絶対優先方式 (SP: Strict Priority)

優先度が最も高いキューの packets を、そのキューが空になるまで最優先で送信します。そのため、優先度の低いキューは、上位のキューに通信がなくなるまで待機状態になります。音声など、遅延が許されない通信を確実に最優先で処理できますが、優先度の高い通信が続くと、優先度の低い通信がいつまでも処理されない「飢餓状態」に陥る可能性があります。

このモード選択時は、「Port」のみ設定できます。

2) wrrモード選択時

重み付きラウンドロビン (WRR: Weighted Round Robin)

各キューに設定された「重み (Weight)」の比率に応じて、順番に packets を送信します。重みが大いキューほど、より多くの packets を送信する機会が与えられます。全てのキューに必ず送信機会が与えられるため、SP のような「飢餓状態」が発生しません。厳密な優先処理ではないため、最優先にしたい通信でもわずかな待ち時間が発生する場合があります。

このモード選択時は、「Port」及び、「Weight1~8」を設定できます。

3) wdrpモード選択時

重み付き不足ラウンドロビン (WDRR: Weighted Deficit Round Robin)

WRR の改良版で、packet のサイズがキューごとに異なる場合でも、より公平に帯域を分配する方式です。各キューの送信量をバイト数で管理するため、小さな packet を多く送信するキューが不利になりません。また、あるターンで割り当てられた送信権利を使い切れなかった場合、その残りを次回に持ち越して送信できます。これにより、設定した重みに応じた、より正確で公平な帯域制御を実現します。

このモード選択時は、「Port」及び、「Weight1~8」を設定できます。

3 CoS-To-IntP Map (CoS 値からキューへのマッピング設定)

ポートで受信したフレームが持つCoS値(レイヤー2の優先度)を、スイッチ内部で処理する際の内部優先度(IntP: Internal Priority)にマッピングするための設定です。

スイッチは通常、複数の優先度キューを持っており、このマッピング設定に基づいて、受信したパケットをどのキューに入れるかを決定します。この設定は、ポートのTrustルールが「COS」に設定されている場合に適用されます。

「QoS Config」→「Port Config」→「CoS-To-IntP Map」をクリックすると、以下の画面が表示されます。

CoS-To-IntP Map

This page is used to set the mapping relationship between COS and internal priority

CoS	0	1	2	3	4	5	6	7
IntP ?	0	1	2	3	4	5	6	7

Apply

メニュー	説明
CoS value	COS 値を表示します。
IntP	COS 値でマッピングするキューの番号を設定します。 (値の有効範囲: 0 ~ 7)

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定してください。

4 DSCP-To-IntP Map (DSCP 値からキューへのマッピング設定)


ポートで受信したIPパケットが持つDSCP値(レイヤー3の優先度)を、スイッチ内部で処理する際の内部優先度(IntP: Internal Priority)に対応付ける(マッピングする)ための設定です。

DSCPは0～63までの64段階で優先度を指定できるため、CoS(8段階)よりも詳細なトラフィック制御が可能です。この設定は、ポートのTrustルールが「DSCP」に設定されている場合に適用されます。

「QoS Config」→「Port Config」→「DSCP-To-IntP Map」をクリックすると、以下の画面が表示されます。

DSCP-To-IntP Map

This page is used to set the mapping relationship between DSCP and internal priority

DSCP	<input type="text" value="--Please select --"/>
IntP 	<input type="text" value="0"/>

DSCP	Internal Priority	DSCP	Internal Priority	DSCP	Internal Priority	DSCP	Internal Priority
0	0	16	2	32	4	48	6
1	0	17	2	33	4	49	6
2	0	18	2	34	4	50	6
3	0	19	2	35	4	51	6
4	0	20	2	36	4	52	6
5	0	21	2	37	4	53	6

メニュー	説明
DSCP	内部優先度にマッピングしたいDSCP値を、0～63の範囲で入力または選択します。
IntP value	DSCP値でマッピングするキューの番号を設定します (値の有効範囲: 0 ~ 7)

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定すると、テーブルの内容が更新されます。

5 Policy Config (ポリシーテーブルの設定)

事前に作成したQoSポリシーマップ(3.10.3 Policy-MAP Config)を、特定のポートに適用するための設定です。

ポリシーマップとは、通信の種類を識別しそれぞれに優先制御や帯域制限などの処理を定義したルールセットのことです。

ポートにポリシーマップを適用することで、そのポートを通過するトラフィックに対して、そのポートで定義済みのQoS処理を実行させることができます。

「QoS Config」 → 「Port Config」 → 「Policy Config」をクリックすると、以下の画面が表示されます。

Policy Config

This page is used to set policy configuration on the port

Port	--Please select --
Policy-Map Name	▼
Operation Type	Add ▼

Apply

Port	Policy-Map Name
Ethernet1/0/1	None
Ethernet1/0/2	None
Ethernet1/0/3	None
Ethernet1/0/4	None
Ethernet1/0/5	None
Ethernet1/0/6	None
Ethernet1/0/7	None

メニュー	説明
Port	対象のポート番号を選択します。 <input type="checkbox"/> Select All/Unselectに☑を入れると、すべてのポートを選択、または解除することができます。
Policy map name	ポートに適用したいポリシーマップを選択します。
Operation	操作方法を選択します。 ・Add: 選択したポリシーマップをポートに適用します。 ・Del: 選択したポリシーマップをポートから解除します。

- 各項目の設定後に<Apply>ボタンをクリックすると、設定内容が確定され、反映されます。

3.10.2. Class-Map Config (Class-Map の設定)

QoSを適用したい通信トラフィックを識別・分類するための「クラスマップ」を作成・管理します
作成したクラスマップは、ポリシーマップの設定で使用され、分類したトラフィックごとに優先制御などの具体的なQoS処理を割り当てる際に利用されます。

1 Class-Map Config (クラスマップ名の設定)

特定の基準に基づいてネットワークトラフィックを分類するクラスマップ名を設定します。

「QoS Config」→「Class-Map Config」→「Class-Map Config」をクリックすると、以下の画面が表示されます。

Class-Map Config

This page is used to set class map entries

Class-Map Name (1-64 characters)

Apply

Class-Map List

Showing 10 Entries Showing 0 to 0 of 0 entries Search

<input type="checkbox"/>	Entries	Class-Map Name
0 results found.		

Delete **First** **Previous** **Next** **Last**

メニュー	説明
Class-Map Name	クラスマップ名を設定します(有効範囲:1～64文字)。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定してください。
- 既存の情報を削除する場合は、対象エントリにを入れて<Delete>ボタンをクリックしてください。

各画面で表示するエントリ数をドラッグして設定できます
(オプション: 全件 / 10 件 / 30 件 / 50 件 / 100 件、デフォルト: 10 件)
画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

2 Class-Map Rule Config (Class-Map ルールの設定)

クラス・マップのルールや条件を指定します。

これらのルールによって、どのトラフィックがそのクラスに属するかを設定します。

「QoS Config」→「Class-Map Config」→「Class-Map Rule Config」をクリックすると、以下の画面が表示されます。

Class-Map Rule Config

This page is used to set the matching rules for class map

Class-Map Name	<input type="text"/>
Match Rule	Access Group
ACL list name	<input type="text" value="Access Group"/> (1-64 characters)
Operation Type	<ul style="list-style-type: none"> COS VLAN IP DSCP IP Precedence IPV6 DSCP IPV6 Flowlabel

Showing 10 Entries

Class-Map Name	ACL list name	COS	VLAN	IP DSCP	IP Precedence	IPV6 DSCP	IPV6 Flowlabel
0 results found.							

First Previous Next Last

メニュー	説明
Class-Map Name	分類ルールを適用させるクラスマップ名を選択します。
Match Rule	クラスマップ内でトラフィックを特定のカテゴリや条件に一致させるためのルールを選択します。 ※各ルールの詳細や設定項目は、次項以降に記載しています。 (AccessGroup/COS/VLAN/IP DSCP/IP Precedence /IPv6 dscp/IPv6 flowlabel)
Operation	Class-Mapに適用する際の操作を指定します ・Add: 新規のマッピングルールを追加します。 ・Del: 既存のマッピングルールを削除します。

- 各項目の設定後に<Apply>ボタンをクリックすると、設定内容が確定され、反映されます。

各画面で表示するエントリ数をドラッグして設定できます

(オプション: 全件 / 10 件 / 30 件 / 50 件 / 100 件、デフォルト: 10 件)

画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

1) Access Group選択時

特定の packets をアクセス制御リスト(ACL)で分類し、QoS(Quality of Service)クラスを適用します。ここで設定したACLにマッチした packets が、このクラスマップに一致するものとして扱われ、ポリシーマップで定義したQoS処理(優先制御など)の対象となります。

「Match Rule」メニューをドラッグして、「Access Group」を選択すると、以下の画面が表示されます。

Class-Map Rule Config

This page is used to set the matching rules for class map

Class-Map Name	<input type="text"/>	▼	
Match Rule	Access Group	▼	
ACL list name	<input type="text"/>	(1-64 characters)	
Operation Type	Add	▼	

Class-Map matching rule table

Showing Entries Showing 0 to 0 of 0 entries

Class-Map Name	ACL list name	COS	VLAN	IP DSCP	IP Precedence	IPv6 DSCP	IPv6 Flowlabel
0 results found.							

メニュー	説明
ACL list name	トラフィックを分類するために使用するアクセス制御リスト(ACL)の名前を指定します(有効範囲:1-64文字)。
Operation	Class-Mapに適用する際の操作を指定します <ul style="list-style-type: none"> ・Add:新規のマッチングルールを追加します。 ・Del:既存のマッチングルールを削除します。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定すると、テーブルの内容が更新されます。

2) COS選択時

COS値を基準にトラフィックを分類するというルールを設定します。

ここで設定したCOS値を持つフレームが、このクラスマップに一致するものとして扱われ、ポリシーマップで定義したQoS処理(優先制御など)の対象となります。

「Match Rule」メニューから「COS」を選択すると、以下の画面が表示されます。

Class-Map Rule Config

This page is used to set the matching rules for class map

Class-Map Name	<input type="text"/>		
Match Rule	COS <input type="text"/>		
COS 0	<input type="text"/>	(0-7)	
COS 1	<input type="text"/>	(0-7)	
COS 2	<input type="text"/>	(0-7)	
COS 3	<input type="text"/>	(0-7)	
COS 4	<input type="text"/>	(0-7)	
COS 5	<input type="text"/>	(0-7)	
COS 6	<input type="text"/>	(0-7)	
COS 7	<input type="text"/>	(0-7)	
Operation Type	Add <input type="text"/>		

Class-Map matching rule table

Showing 10 Entries Showing 0 to 0 of 0 entries

Class-Map Name	ACL list name	COS	VLAN	IP DSCP	IP Precedence	IPv6 DSCP	IPv6 Flowlabel
0 results found.							

メニュー	説明
COS 0-7 ※1	マッチさせるCOS 値を入力します。 最大 8 つまで COS値を設定可能です(値の有効範囲:0 ~ 7)。
Operation	Class-Mapに適用する際の操作を指定します <ul style="list-style-type: none"> ・Add:新規のマッチングルールを追加します。 ・Del:既存のマッチングルールを削除します。

※1) この項目名の番号はCOS値ではなく、入力フィールド番号になります。

右側の入力欄に、割り当てる COS値 を入力してください。

なお、1つのフィールドに複数の COS値 を入力することはできません。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定すると、テーブルの内容が更新されます。

3) VLAN 選択時

VLANID を基準にトラフィックを分類するというルールを設定します。
ここで設定した VLANID を持つフレームが、このクラスマップに一致するものとして扱われ、ポリシーマップで定義した QoS 処理 (優先制御など) の対象となります。

「Match Rule」メニューから「VLAN」を選択すると、以下の画面が表示されます。

Class-Map Rule Config

This page is used to set the matching rules for class map

Class-Map Name	<input type="text"/>		
Match Rule	VLAN		
VLAN 0	<input type="text"/>	(1-4094)	
VLAN 1	<input type="text"/>	(1-4094)	
VLAN 2	<input type="text"/>	(1-4094)	
VLAN 3	<input type="text"/>	(1-4094)	
VLAN 4	<input type="text"/>	(1-4094)	
VLAN 5	<input type="text"/>	(1-4094)	
VLAN 6	<input type="text"/>	(1-4094)	
VLAN 7	<input type="text"/>	(1-4094)	
Operation Type	Add		

Apply

Class-Map matching rule table

Showing 10 Entries Showing 0 to 0 of 0 entries Search

Class-Map Name	ACL list name	COS	VLAN	IP DSCP	IP Precedence	IPV6 DSCP	IPV6 Flowlabel
0 results found.							

First Previous Next Last

メニュー	説明
VLAN 0-7 ※1	マッチさせるVLANIDを入力します。 最大 8 つまで VLANIDを設定可能です(値の有効範囲: 1 ~ 4094)。
Operation	Class-Mapに適用する際の操作を指定します ・Add: 新規のマッチングルールを追加します。 ・Del: 既存のマッチングルールを削除します。

※1) 右側の入力欄に、割り当てる VLAN ID を入力してください。
なお、1 つのフィールドに複数の VLAN ID を入力することはできません。

4) IP DSCP 選択時

DSCP 値を基準にトラフィックを分類するというルールを設定します。
 ここで設定した DSCP 値を持つパケットが、このクラスマップに一致するものとして扱われ、ポリシーマップで定義した QoS 処理(優先制御など)の対象となります。

「Match Rule」メニューをドラッグして、「IP DSCP」を選択すると、以下の画面が表示されます。

Class-Map Rule Config

This page is used to set the matching rules for class map

Class-Map Name	<input type="text"/>	
Match Rule	IP DSCP	
IP DSCP 0	<input type="text"/>	(0-63)
IP DSCP 1	<input type="text"/>	(0-63)
IP DSCP 2	<input type="text"/>	(0-63)
IP DSCP 3	<input type="text"/>	(0-63)
IP DSCP 4	<input type="text"/>	(0-63)
IP DSCP 5	<input type="text"/>	(0-63)
IP DSCP 6	<input type="text"/>	(0-63)
IP DSCP 7	<input type="text"/>	(0-63)
Operation Type	Add	

Apply

Class-Map matching rule table

Showing 10 Entries Showing 0 to 0 of 0 entries Search

Class-Map Name	ACL list name	COS	VLAN	IP DSCP	IP Precedence	IPv6 DSCP	IPv6 Flowlabel
0 results found.							

First Previous Next Last

メニュー	説明
IP DSCP 0-7 ※1	マッチさせるDSCP値を入力します。 最大 8 つまで DSCP 値を設定可能です(値の有効範囲:0 ~ 63)。
Operation	Class-Mapに適用する際の操作を指定します <ul style="list-style-type: none"> ・Add:新規のマッチングルールを追加します。 ・Del:既存のマッチングルールを削除します。

※1) この項目名の番号は DSCP 値ではなく、入力フィールド番号になります。
 右側の入力欄に、割り当てる DSCP 値を入力してください。
 なお、1つのフィールドに複数のDSCP値を入力することはできません。

5) IP Precedence 選択時

IP Precedence 値を基準にトラフィックを分類するというルールを設定します。
ここで設定した IP Precedence 値を持つパケットが、このクラスマップに一致するものとして扱われ、ポリシーマップで定義した QoS 処理(優先制御など)の対象となります。

「Match Rule」メニューから「IP Precedence」を選択すると、以下の画面が表示されます。

Class-Map Rule Config

This page is used to set the matching rules for class map

Class-Map Name	<input type="text"/>	▼	
Match Rule	IP Precedence	▼	
IP Precedence 0	<input type="text"/>	(0-7)	
IP Precedence 1	<input type="text"/>	(0-7)	
IP Precedence 2	<input type="text"/>	(0-7)	
IP Precedence 3	<input type="text"/>	(0-7)	
IP Precedence 4	<input type="text"/>	(0-7)	
IP Precedence 5	<input type="text"/>	(0-7)	
IP Precedence 6	<input type="text"/>	(0-7)	
IP Precedence 7	<input type="text"/>	(0-7)	
Operation Type	Add	▼	

Class-Map matching rule table

Showing 10 Entries Showing 0 to 0 of 0 entries

Class-Map Name	ACL list name	COS	VLAN	IP DSCP	IP Precedence	IPv6 DSCP	IPv6 Flowlabel
0 results found.							

メニュー	説明
IP DSCP 0-7 ※1	マッチさせるDSCP値を入力します。 最大 8 つまで DSCP 値を設定可能です(値の有効範囲:0 ~ 63)。
Operation	Class-Mapに適用する際の操作を指定します <ul style="list-style-type: none"> ・Add:新規のマッチングルールを追加します。 ・Del:既存のマッチングルールを削除します。

※1) この項目名の番号は IP Precedence 値ではなく、入力フィールド番号になります。
右側の入力欄に、割り当てるIP Precedence値を入力してください。
なお、1つのフィールドに複数の IP Precedence値 を入力することはできません。

6) IPv6 DSCP 選択時

IPv6パケットのDSCP値を基準にトラフィックを分類するルールを設定します。

IPv6におけるDSCPは、IPv4のDSCPと同様に0～63の64段階で優先度を指定でき、IPv6ネットワーク上で詳細なQoS制御を実現します。

ここで設定したDSCP値を持つIPv6パケットが、このクラスマップに一致するものとして扱われ、ポリシーマップで定義したQoS処理（優先制御など）の対象となります。

「Match Rule」メニューから「IPv6 DSCP」を選択すると、以下の画面が表示されます。

Class-Map Rule Config

This page is used to set the matching rules for class map

Class-Map Name	<input type="text"/>	
Match Rule	IPv6 DSCP	
IPv6 DSCP 0	<input type="text"/>	(0-63)
IPv6 DSCP 1	<input type="text"/>	(0-63)
IPv6 DSCP 2	<input type="text"/>	(0-63)
IPv6 DSCP 3	<input type="text"/>	(0-63)
IPv6 DSCP 4	<input type="text"/>	(0-63)
IPv6 DSCP 5	<input type="text"/>	(0-63)
IPv6 DSCP 6	<input type="text"/>	(0-63)
IPv6 DSCP 7	<input type="text"/>	(0-63)
Operation Type	Add	

Apply

Class-Map matching rule table

Showing 10 Entries Showing 0 to 0 of 0 entries Search

Class-Map Name	ACL list name	COS	VLAN	IP DSCP	IP Precedence	IPv6 DSCP	IPv6 Flowlabel
0 results found.							

[First](#)
[Previous](#)
[Next](#)
[Last](#)

メニュー	説明
IPv6 DSCP 0-7 ※1	マッチさせるIPv6 DSCP 値を入力します。 最大 8 つまで値を設定することができます(値の有効範囲:0 ~ 63)。
Operation	Class-Mapに適用する際の操作を指定します <ul style="list-style-type: none"> ・Add:新規のマッチングルールを追加します。 ・Del:既存のマッチングルールを削除します。

※1) この項目名の番号はIPv6DSCP値ではなく、入力フィールド番号になります。
 右側の入力欄に、割り当てる IPv6DSCP 値を入力してください。
 なお、1 つのフィールドに複数の IPv6DSCP 値を入力することはできません。

7) IPv6 Flowlabel選択時

IPv6パケットのフローラベル値を基準にトラフィックを分類するルールを設定します。

フローラベルは、IPv6ヘッダ内で特定の関連する一連の通信（フロー）を識別するための情報です。これにより、特定のビデオストリーミングやWeb会議の通信全体を一つのグループとして扱うことができます。

ここで設定したフローラベル値を持つIPv6パケットが、このクラスマップに一致するものとして扱われ、ポリシーマップで定義したQoS処理の対象となります。

「Match Rule」メニューから「IPv6 Flowlabel」を選択すると、以下の画面が表示されます。

Class-Map Rule Config

This page is used to set the matching rules for class map

Class-Map Name	<input type="text"/>	
Match Rule	IPv6 Flowlabel	
IPv6 Flowlabel 0	<input type="text"/>	(0-1048575)
IPv6 Flowlabel 1	<input type="text"/>	(0-1048575)
IPv6 Flowlabel 2	<input type="text"/>	(0-1048575)
IPv6 Flowlabel 3	<input type="text"/>	(0-1048575)
IPv6 Flowlabel 4	<input type="text"/>	(0-1048575)
IPv6 Flowlabel 5	<input type="text"/>	(0-1048575)
IPv6 Flowlabel 6	<input type="text"/>	(0-1048575)
IPv6 Flowlabel 7	<input type="text"/>	(0-1048575)
Operation Type	Add	

Class-Map matching rule table

Showing 10 Entries Showing 0 to 0 of 0 entries Search

Class-Map Name	ACL list name	COS	VLAN	IP DSCP	IP Precedence	IPv6 DSCP	IPv6 Flowlabel
0 results found.							

メニュー	説明
Class-Map Name	作成されたクラスマッチングテーブルの名前を選択します。 ※ドロップダウンメニューをクリックして、選択してください。
Match Rule	クラスマップ内でトラフィックを特定のカテゴリや条件に一致させるためのルールを選択します。
IPv6 Flowlabel 0-7 ※1	1 つ以上の IPv6 フローラベル値を設定できます(値の有効範囲:0 ~ 1048575)。
Operation Type	Class-Mapに適用する際の操作を指定します <ul style="list-style-type: none"> ・Add:新規のマッチングルールを追加します。 ・Del:既存のマッチングルールを削除します。

※1) 右側の入力欄に、割り当てる IPv6 フローラベル値を入力してください。

なお、1 つのフィールドに複数の IPv6 フローラベル値を入力することはできません

3.10.3. Policy-Map Config (ポリシーマップの設定)

ポリシーマップは、トラフィックを分類する「クラスマップ」とその分類されたトラフィックに適用するQoS処理とを関連付ける一連のルールセットです。
作成したポリシーマップを最終的にポートに適用することで、QoSが機能します。

1 Policy Name Config (ポリシーマップ名の設定)

最初にこの画面でポリシーマップの名前を登録し、その後の設定で、この名前に具体的な分類ルール(クラスマップ)と処理内容(アクション)を関連付けていきます。

「QoS Config」 → 「Policy-Map Config」 → 「Class-Map Rule Config」をクリックすると、以下の画面が表示されます。

Policy Name Config

This page is used to set policy map entries

Policy-Map Name (1-64 characters)

Apply

Policy-Map List

Showing Entries Showing 0 to 0 of 0 entries Search

	Entries	Policy-Map Name
<input type="checkbox"/>		
0 results found.		
<div style="display: flex; justify-content: space-between; align-items: center;"> Delete <input type="button" value="First"/> <input type="button" value="Previous"/> <input type="button" value="Next"/> <input type="button" value="Last"/> </div>		

メニュー	説明
Policy-Map Name	ポリシーマップ名を設定します(値の有効範囲: 1~64文字)。

- 各項目の設定後に<Apply>ボタンをクリックすると、設定内容が確定され、反映されます。
- 既存の情報を削除する場合は、対象エントリに☑を入れて<Delete>ボタンをクリックしてください。

各画面で表示するエントリ数をドラッグして設定できます
(オプション: 全件 / 10 件 / 30 件 / 50 件 / 100 件、デフォルト: 10 件)
画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

2 Policy Class Config (ポリシークラスの設定)

ポリシーマップに、どのトラフィック分類ルールのクラスマップを適用するかを設定します。

「QoS Config」→「Policy-Map Config」→「Policy Class Config」をクリックすると、以下の画面が表示されます。

Policy Class Config

This page is used to set policy classification rules

Policy-Map Name	<input type="text"/>
Class-Map Name	<input type="text"/>
Inserted Before The Class-Map Name	<input type="text"/>

Policy-Map-Class List

Showing Entries Showing 0 to 0 of 0 entries Search

	Policy-Map Name	Class-Map Name
0 results found.		

メニュー	説明
Policy-Map Name	対象のポリシーマップの名前を選択します。
Class-Map Name	ポリシーマップに適用するクラスマップを選択します。
Inserted Before the Class-Map Name	選択したクラスマップを、ポリシーマップ内の他のクラスマップよりも前に評価するよう指定します。 ここで追加されたクラスマップは、指定したクラスマップよりも高い優先順位で処理されます。

- 各項目の設定後に<Apply>ボタンをクリックすると、設定内容が確定され、反映されます。
- 既存の情報を削除する場合は、対象エントリに☑を入れて<Delete>ボタンをクリックしてください。

各画面で表示するエントリ数をドラッグして設定できます
(オプション: 全件 / 10 件 / 30 件 / 50 件 / 100 件、デフォルト: 10 件)
画面下のメニューボタンを使用して、ページを移動してください。

- First: 最初のページへ移動します。
- Previous: 前のページへ移動します。
- Next: 次のページへ移動します。
- Last: 最後のページへ移動します。

3 Policy Mark Config (ポリシーマッピングの設定)

「ポリシーマップ」と「クラスマップ」で分類したトラフィックに対して、優先度情報を書き換える「リマーケティング」などのQoSアクションを設定します。

「QoS Config」 → 「Policy-Map Config」 → 「Policy Mark Config」をクリックすると、以下の画面が表示されます。

Policy Mark Config

This page is used to set policy tags

Policy-Map Name	<input type="text"/>	
Class-Map Name	<input type="text"/>	
Mark Type	COS	
COS	<input type="text"/>	(0-7)
Operation Type	<div style="border: 1px solid red; padding: 2px;"> COS IP DSCP IP Precedence Internal Priority Drop Precedence </div>	

Policy Mark List

Showing Entries Showing 0 to 0 of 0 entries Search

Policy-Map Name	Class-Map Name	COS	IP DSCP	IP Precedence	Internal Priority	Drop Precedence
0 results found.						

メニュー	説明
Policy-Map Name	対象のポリシーマップを選択します
Class-Map Name	対象の分類一致テーブルを表します。
Mark Type	トラフィックに適用するマーキングの種類を選択します。 ・Cos:ポリシー テーブルと分類マッチング テーブルで定義されたルールに従って、COS 値を再度設定します ・ip dscp:ポリシーマップとクラスマップで定義されたルールに従って、DSCP 値を再設定します。 ・ip precedence:ポリシーマップとクラスマップで定義されたルールに従って、IP precedence 値を再設定します。 ・drop-precedence:ポリシーマップとクラスマップで定義されたルールに従って、破棄の優先度を再設定します。 ・internal-priority:ポリシーマップとクラスマップで定義されたルールに従って、内部の優先度を再度設定します。
COS	再度設定する値を入力します。
Operation	操作方法を選択します。 ・Add:設定値を追加します。 ・Del:設定値を削除します。

- 各項目の設定後に<Apply>ボタンをクリックすると、設定内容が確定され、反映されます。

4 Policy Bandwidth (QoS ポリシング設定)

ネットワーク機器において、特定のトラフィック(通信の種類)に対して 帯域幅の上限を設ける制御を行う仕組みです。

「ポリシーマップ」と「クラスマップ」で分類したトラフィックに対して、帯域制限(ポリシング)を設定します。

「QoS Config」→「Policy-Map Config」→「Policy Bandwidth」をクリックすると、以下の画面が表示されます。

Policy Bandwidth

This page is used to set policy bandwidth configuration

Burst ID1	<input type="text" value="1024"/>	(1-8192)
Burst ID2	<input type="text" value="1024"/>	(1-8192)

Policy-Map Name	<input type="text"/>
Class-Map Name	<input type="text"/>
Burst ID	<input type="text" value="1"/>
Bandwidth Rate	<input type="text"/> (1-10000000)
Operation Type	<input type="text" value="Add"/>

Policy Bandwidth List

Showing Entries Showing 0 to 0 of 0 entries Search

Policy-Map Name	Class-Map Name	Burst ID	Bandwidth Rate(Kbps)
0 results found.			

メニュー	説明
Burst ID 1/2	一時的に超過を許可するデータ量(バーストサイズ)を設定します(値の有効範囲: 1-8192)。
Policy-Map Name	ポリシーマップの名前を選択します。
Class Map Name	トラフィックを分類するためのクラス名を選択します。
Burst ID	バーストIDを選択します。
Bandwidth Rate	トラフィックに適用する最大帯域幅(レート)を設定します(値の有効範囲: 1~10000000kbps)。
Operation	操作方法を選択します。 <ul style="list-style-type: none"> ・Add: 設定値を追加します。 ・Del: 設定値を削除します。

- 各項目の設定後に<Apply>ボタンをクリックすると、設定内容が確定され、反映されます。

5 Policy VLAN (ポリシーマップの VLAN への適用)

ポリシーマップを、特定のVLAN全体に適用するための設定です。

ここでポリシーマップを適用すると、そのVLANに所属する全てのポートで、ポリシーマップに定義されたQoS処理(優先制御や帯域制限など)が有効になります。VLAN単位で一括してQoSポリシーを管理できます。

「QoS Config」→「Policy-Map Config」→「Policy VLAN」をクリックすると、以下の画面が表示されます。

Policy VLAN

This page is used to set policy configurations on VLANs

Policy-Map Name	<input type="text"/>
Vlan List ?	<input type="text"/> (1-100 characters)
Operation Type	<input type="text" value="Add"/>

VLAN Policy List

Showing Entries Showing 0 to 0 of 0 entries Search

VLAN ID	Policy-Map Name
0 results found.	

メニュー	説明
Policy-map name	VLANに適用したいポリシーマップ名を選択します。
VLAN List	適用するVLAN IDを入力します (値の有効範囲: 1-100文字)。
Operation	操作方法を選択します。 <ul style="list-style-type: none"> • Add: 設定値を追加します。 • Del: 設定値を削除します。

- 各項目を設定した後、<Apply>ボタンをクリックして設定内容を確定すると、テーブルの内容が更新されます。

FXC5710/FXC5718/FXC5728 Management Guide(GUI) (FXC25-DC-2000002-R1.0)

初版 2025 年 9 月

- ◆ 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。
-

