





# 安全にお使いいただくために

ご自身の安全を確保し、システムを破損から守るために、以下に記述する安全のための指針をよくお読みください。

安 <u>全</u> 上	のご注意 必ずお守りください	
本製品を安全にお使いいただくために、以下の項目をよ	くお読みになり必ずお守りください。	
▲ 危険 この表示を無視し、間違った使い方をすると	、死亡または重傷を負うおそれがあります。	
▲警告 この表示を無視し、間違った使い方をすると	、火災や感電などにより人身事故になるおそれがあります。	
▲注意 この表示を無視し、間違った使い方をすると	、傷害または物損損害が発生するおそれがあります。	
記号の意味 ○してはいけない「禁止」内容です。 ● 必ず実行していただく「指示」の内容です。		
	危険	
<ul> <li>◇ 分解・改造をしない</li> <li>☆ 止 火災、やけど、けが、感電などの原因となります。</li> <li>◇ ぬれた手でさわらない</li> </ul>	☆ 止     は煙、湯気、湿気、埃の多い場所、高温になる場所や     熱のこもりやすい場所(火のそば、暖房器具のそば、     こたつや布団の中、直射日光の当たる場所、炎天下の車内、     風呂場など)、振動の激しい場所では、使用、保管、放置しない     仏災、 やけど、けざ、感雲、か障の原用となります     ない     ない     ない     ない     ない     ちょう     ない     ない     ちょう     ない     なの     ない     ない     ない     ない     ない     ない     ない     なの     ない     ない     ない     ない     なの     なの     なの     なの     なの     ない     なの     ない     なの     ない     ない     なの     ない     なの     なの	
☆ 止 感電の原因となります。	○ 内部に金属物や燃えやすいものを入れない	
	☆ 止 火災、感電、故障の原因となります。	
水などの液体(飲料水、汗、海水、ペットの尿など) でぬれた状態で触ったり、電源を入れたりしない 火災、やけど、けが、感電、故障の原因となります。	● 砂や土、泥をかけたり、直に置いたりしない。 また、砂などが付着した手で触れない 火災、やけど、けが、感電、故障の原因となります。     ●	
各種端子やスロットに水などの液体(飲料水、汗、海2 ペットの尿など)をいれない。万が一、入ってしまった場合 直ちに電源プラグをコンセントから抜く 火災、やけど、けが、感電、故障の原因となります。	K、 素 止 火災、やけど、けが、感電、故障の原因となります。	
	444 11	
	<b>」</b> 警告	
	ガソリンスタンドなど引火性ガスが発生する可能性のある場所や 粉じんが発生する場所に立ち入る場合は、必ず事前に本製品の電源を切る 引火性ガスなどが発生する場所で使用すると、爆発や火災の原因となります。	
発煙、焦げ臭い匂いの発生などの異常状態のまま 使用しない 感電、火災の原因になります。 使用たいな、 「類を共いて、「「「」」」で、「類を共いて、「「」」」」で、	★ カメラのレンズに直射日光などを長時間あてない 素子の退色、焼付きや、レンズの集光作用により、 火災、やけど、けがまたは故障の原因となります。	
	無線製品は病院内で使用する場合は、 各医療機関の指示に従って使用する 電子機器や医療電気機器に悪影響を及ぼすおそれがあります。	
<u>奈</u> 止火災、感電、または故障の原因となります。 <u>へ</u> たこ足配線禁止                 たこ足配線などで定格を超えると火災、感電、または故障の	本製品の周辺に放熱を妨げるようなもの (フィルムやシールでの装飾を含む)を置かない 火災、または故障の原因となります。	
<ul> <li>◎ ()</li> <li>◎ ()</li> <li>○ ()</li></ul>	耳を本体から離してご使用ください 大きな音を長時間連続して聞くと、難聴などの耳の障害の原因となります。	
ア、火、 松竜、まには (20) (20) (20) (20) (20) (20) (20) (20)	無線製品をご使用の場合、医用電気機器などを 装着している場合は、医用電気機器メーカーもしくは、 販売業者に、電波による影響について確認の上使用する 医常常を構想に再影響を取ぼすたるわざもします。	
ケーブル/コード類や端子を破損させない     無理なねじり、引っ張り、加工、重いものの下敷きなどは、     ケーブル/コードや端子の破損の原因となり、火災、感電、     または故障の原因となります。	この「「「「」」」の「「」」の「「」」の「「」」の「」」の「「」」の「」」の「」	
本製品付属のACアダプタもしくは電源ケーブルを 指定のコンセントに正しく接続して使用する 火災、感電、または故障の原因となります。	ディスプレイ部やカメラのレンズを破損した際は、 割れたガラスや露出した端末内部に注意する 破損部や露出部に触れると、やけど、けが、感電の原因となります。	
<ul> <li>各光源をのぞかない</li> <li>※ 止</li> <li>光ファイバケーブルの断面、コネクタおよび本製品のコネクタギ</li> <li>LED をのぞきますと強力な光源により目を損傷するおそれがありま</li> </ul>	<ul> <li>ペットなどが本機に噛みつかないように注意する</li> <li>火災、やけど、けがなどの原因となります。</li> </ul>	
各種端子やスロットに導電性異物(金属片、鉛筆の芯など)を 接触させたり、ほこりが内部に入ったりしないようにする 火災、やけど、けが、感電または故障の原因となります。	スレイントに AC アダプタや電源ケーブルを 抜き差しするときは、金属類を接触させない 火災、やけど、感電または故障の原因となります。     マンズン・マンズン・マンズン・マンズン・マンズン・マンズン・マンズン・マ	
使用中に布団で覆ったり、包んだりしない     紫 止 火災、やけどまたは故障の原因となります。	ACアタフタや電源ケーブルに 海外旅行用の変圧器等を使用しない 発火、発熱、感電または故障の原因となります。     ■	



#### 電波障害自主規制について

本製品は、情報処理装置等電波障害自主規制協議会(VCCI)の基準に基づくクラス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。

### ご使用上の注意

けがや感電、火災および装置の破損のリスクを減らすために、以下の注意事項を遵守してください。

- マニュアルなどに記載されている以外の方法でのご使用はやめてください。
- 食べ物や飲み物が本製品にかからないようにしてください。また、水気のある場所での運用は避けてください。
- 本製品の開口部に物をさしこまないでください。火事や感電を引き起こすことがあります。
- 付属の AC アダプタもしくは電源ケーブルのみを使用してください。
- 感電を防止するために、本製品と周辺機器の電源ケーブルは、正しく接地された電気コンセントに接続してください。
- やむなく延長コードや電源分岐回路を使用する場合においても、延長コードと電源分岐回路の定格を守ってください。延長コードまたは電源分岐回路に差し込まれているすべての製品の合計定格アンペア数が、その延長コードまたは、電源分岐回路の定格アンペア限界の8割を超えないことを確認してください。
- 一時的に急激に起こる電力の変動から本製品を保護するためには、サージサプレッサ、回線調整装置、または無停電電源装置(UPS)を使用してください。
- ケーブルと電源コードは慎重に取り付けてください。踏みつけられたり躓いたりしない位置に、ケーブルと電源コードを配線し、コンセントに 差し込んでください。また、ケーブル上に物を置いたりしないようにしてください。
- 電源ケーブルや電源プラグを改造しないでください。
- システムに対応しているホットプラグ可能な電源装置に電源を接続したり、切り離したりする際には、以下の注意を守ってください。
  - 電源装置を取り付ける場合は、電源装置を取り付けてから、電源ケーブルを電源装置に接続してください。
  - 電源装置を取り外す場合は、事前に電源ケーブルを抜いておいてください。
  - システムに複数の電源がある場合、システムから電源を切り離すには、すべての電源ケーブルを電源装置から抜いておいてください。
- 抜け防止機構のあるコンセントをご使用の場合、そのコンセントの取り扱い説明書に従ってください。
- 本製品は動作中に高温になる場合があります。本製品の移動や取り外しの際には、ご注意ください。
- 本製品は動作中に高温になる場合がありますが、手で触れることができる温度であれば故障ではありません。ただし長時間触れたまま使用しないでください。低温やけどの原因になります。
- 市販のオプション品や他社製品を使用する場合、当社では動作保証は致しませんので、予めご了承ください。
- 製品に貼られている製品ラベルや認証ラベルをはがさないでください。はがしてしまうとサポートを受けられなくなります。

## 静電気障害を防止するために

静電気は、本製品内部の精密なコンポーネントを損傷する恐れがあります。静電気による損傷を防ぐため、本製品に触れる前に、身体から静電気を 逃がしてください。

さらに、静電気放出(ESD)による損傷を防ぐため、以下の手順を実行することをお勧めします。

- 1. 機器を箱から取り出すときは、機器をシステム等に取り付ける準備が完了するまで、本製品を静電気防止包装から取り出さないでください。静 電気防止包装から取り出す直前に、必ず身体の静電気を逃がしてください。
- 2. 静電気に敏感な部品を運ぶ場合、最初に必ず静電気対策を行ってください。
- 3. 静電気に敏感な機器の取り扱いは、静電気のない場所で行います。可能であれば、静電気防止床パッド、作業台パッド、および帯電防止接地ス トラップを使用してください。

### 電源の異常

万一停電などの電源異常が発生した場合は、必ず本スイッチの電源プラグを抜いてください。電源が再度供給できる状態になってから電源プラグを 再度接続します。

### ラック搭載型製品に関する一般的な注意事項

ラックの安定性および安全性に関する以下の注意事項を遵守してください。また、システムおよびラックに付随する、ラック設置マニュアル中の注 意事項や手順についてもよくお読みください。

● システムとは、ラックに搭載されるコンポーネントを指しています。コンポーネントはシステムや各種周辺デバイスや付属するハードウェアも 含みます。



前面および側面のスタビライザを装着せずに、システムをラックに搭載すると、ラックが倒れ、人身事故を引き起こす場合があります。ラックにシステムを搭載する前には、必ずスタビライザを装着してください。



接地用伝導体を壊したり、接地用伝導体を適切に取り付けないで装置を操作しないでください。適切な接地ができるかわからない場合、電気保安協会または電気工事士にお問い合わせください。

警告

システムのシャーシは、ラックキャビネットのフレームにしっかり接地される必要があります。接地ケーブルを接続してから、システムに 電源を接続してください。電源および安全用接地配線が完了したら、資格を持つ電気検査技師が検査する必要があります。安全用接地ケー ブルを配線しなかったり、接続されていない場合、エネルギーハザードが起こります。

- ラックにシステム/コンポーネントを搭載した後は、一度にスライド・アセンブリに乗せて引き出すコンポーネントは1つのみとしてください。
   2つ以上のコンポーネントが引き出されると、ラックがバランスを失い、倒れて重大な事故につながる恐れがあります。
- ラックに装置を搭載する前に、スタビライザがしっかりとラックに固定されているか、床面まで到達しているか、ラック全体の重量がすべて床 にかかるようになっているかをよく確認してください。ラックに搭載する前に、シングルラックには前面および側面のスタビライザを、複数結 合型のラックには前面用スタビライザを装着してください。
- ラックへの装置の搭載は、常に下から上へ、また最も重いものから行ってください。
- ラックからコンポーネントを引き出す際には、ラックが水平で、安定しているかどうか確認してから行ってください。
- コンポーネントレール解除ラッチを押して、ラックから、またはラックへコンポーネントをスライドさせる際は、指をスライドレールに挟まな いよう、気をつけて行ってください。
- ラックに電源を供給する AC 電源分岐回路に過剰な負荷をかけないでください。ラックの合計負荷が、分岐回路の定格の 80 パーセントを超えな いようにしてください。
- ラック内部のコンポーネントに適切な空気流があることを確認してください。
- ラック内の他のシステムを保守する際には、システムやコンポーネントを踏みつけたり、その上に立ったりしないでください。

注意 資格を持つ電気工事士が、DC 電源への接続と接地を行う必要があります。すべての電気配線が、お住まいの地域、および国の電気基準と 規制に準拠していることを確認してください。

## バッテリの取り扱いについて



不適切なバッテリの使用により、爆発などの危険性が生じることがあります。バッテリの交換は、必ず同じものか、製造者が推奨する同等の仕様のものをご使用ください。バッテリの廃棄については、製造者の指示に従って行ってください。

このたびは、弊社製品をお買い上げいただきありがとうございます。 本書は、製品を正しくお使いいただくための取扱説明書です。 必要な場合には、いつでもご覧いただけますよう大切に保管してください。 また、必ず本書、設置マニュアル、および弊社 WEB に掲載された製品保証規程をよくお読みいただき、内容をご理解いただいた上で、記載事項に従っ てご使用ください。

製品保証規定は以下を参照ください。 https://www.dlink-jp.com/support/product-assurance-provision

- 本書の記載内容に逸脱した使用の結果発生した、いかなる障害や損害において、弊社は一切の責任を負いません。あらかじめご了承ください。
- 弊社製品の日本国外でご使用の際のトラブルはサポート対象外になります。

なお、本製品の最新情報やファームウェアなどを弊社ホームページにてご提供させていただく場合がありますので、ご使用の前にご確認ください。 製品保証、保守サービス、テクニカルサポートご利用について、詳しくは弊社ホームページのサポート情報をご確認ください。 https://www.dlink-jp.com/support

目	次	

Lμ

<b>目次</b>	
安全にお使いいただくために	2
ご使用上の注意	4
静電気障害を防止するために	4
電源の異常	4
ラック搭載型製品に関する一般的な注意事項	5
バッテリの取り扱いについて	5
はじめに	16
本マニュアルの対象者	
表記規則について	
製品名 / 品番一覧	
<u>第1章 本製品のご使用にあたって</u>	19
DGS-3630 シリーズについて	
ポート	
前面パネル	21
アラームポート(RJ-45)	23
LED 表示	24
背面パネル	26
側面パネル	27
第2章 スイッチの設置	28
バッケージの内容	
ネットワーク接続前の準備	
コム足の取り付げ (19 インナフックに設直しない場合 )	
19 1 ノナフックへの取り付け	
SFF/SFF+ 小一下、のてノュールの取り下り	30
電源派の例面アプランジン役者にいた。このでは、「「「「」」のでは、「」。	33
DPS-500A	
DPS-700	
DPS-800	
電源の投入	
電源の異常	35
第3章 スイッチの接続	36
エンドノードと接続する	36
ニットッ トビスポップ いいちょう パン・ション イン・シート シート・シート	
バックボーンまたはサーバと接続する	
第4章 スイッチ管理について	38
 Web GUI による管理	
SNMP による管理	
CLI による管理	
端末をコンソールポートに接続する	
端末を Mini-USB コンソールポートに接続する	
ユーザアカウント / バスワードの設定	
IP パトレスの割り当(	
<u>第5章 Webベースのスイッチ管理</u>	42
Web ヘースの管理について	
Web マネージャへのロクイン	
Web マネージャの画面構成	
Web マネージャのメイ ノ画面について Web マネージャのメニュー構成	
第6章 System (スイッチの主な設定)	49
Device Information (デバノフ 信報)	
Device information (アハイ 人)同報/ System Information Settings (システル 桂紀設定 )	
System Information Settings(ノヘナム旧牧政化) Perinheral Settings(信音設定)	
Port Configuration (ポート設定)	
Port Settings (スイッチのポート設定)	
Port Status (ポートステータス)	
Port GBIC	
i	

гБ

# 目次

Port Auto Negotiation(オートネゴシエーション)	56
Error Disable Settings(エラーによるポートの無効)	
Jumbo Frame(ジャンボフレームの有効化)	57
Interface Description(インタフェース概要)	57
Loopback Test(ループバックテスト)	
PoE (PoE の管理)(DGS-3630-28PC/52PC)	
PoE System (PoE システム設定)	
PoE Status (PoE ステータス)	60
PoE Configuration(PoE ポート設定)	60
PD Alive(PD アライブ設定)	61
PoE Statistics (PoE 統計)	61
PoE Measurement (PoE 測定)	
PoE LLDP Classification (PoE LLDP 分類表示)	
System Log (システムログ構成)	
System Log Settings(システムログ設定)	
System Log Discriminator Settings(システムログディスクリミネーター設定)	
System Log Server Settings(システムログサーバの設定)	
System Log (Syslog ログ)	
System Attack Log (システムアタックログ)	67
Time and SNTP(時刻設定)	68
Clock Settings(時間設定)	
Time Zone Settings (タイムゾーン設定)	2A
SNTP Settings(STP 設定)	
Shring Schrings (Shring) Time Dange (タイトレンジ設定)	
Thine Range (アイムレンノ設定)	
FIF (FIF 設定)	
FIF GIODAI SEULINGS(FIF クローバル放走)	
PTP Port Global Settings (PTP ホートクローハル設定)	
PTP Boundary Port Settings (PTP 現界ホート設定)	
PTP P2P Transparent Port Settings (PTP P2P 透過ホート設定)	
PIP Clock Information (PIP クロック情報の表示)	
PTP Port Information (PTP ホート情報)	
PTP Foreign Master Records Port Information (PTP 外部マスタレコードのホート情報)	76
USB Console Settings(USB コンソール設定)	77
SRM(Switch Resource Management 設定)	
SRM Prefer Current Settings(SRM 最適化設定)	77
SRM Prefer Current Settings(SRM 最適化設定) SRM Prefer Mode(SRM 設定モード) 5.7 音 Management (フィッチの答理)	77 
SRM Prefer Current Settings (SRM 最適化設定) SRM Prefer Mode (SRM 設定モード) <u>37章 Management (スイッチの管理)</u>	
SRM Prefer Current Settings(SRM 最適化設定) SRM Prefer Mode(SRM 設定モード) <u>3 7 章 Management(スイッチの管理)</u> Command Logging(コマンドログ設定)	
SRM Prefer Current Settings(SRM 最適化設定) SRM Prefer Mode(SRM 設定モード) <u> 57章 Management(スイッチの管理)</u> Command Logging (コマンドログ設定) User Accounts Settings(ユーザアカウント設定)	
SRM Prefer Current Settings(SRM 最適化設定) SRM Prefer Mode(SRM 設定モード) <u> 57章 Management(スイッチの管理)</u> Command Logging (コマンドログ設定) User Accounts Settings(ユーザアカウント設定) CLI Alias Settings(CLI エイリアス設定)	
SRM Prefer Current Settings (SRM 最適化設定) SRM Prefer Mode (SRM 設定モード) <u> 57章 Management (スイッチの管理)</u> Command Logging (コマンドログ設定) User Accounts Settings (ユーザアカウント設定) CLI Alias Settings (CLI エイリアス設定) Password Encryption (パスワード暗号化)	
SRM Prefer Current Settings (SRM 最適化設定) SRM Prefer Mode (SRM 設定モード) <u>57章 Management (スイッチの管理)</u> Command Logging (コマンドログ設定) User Accounts Settings (ユーザアカウント設定) CLI Alias Settings (CLI エイリアス設定) Password Encryption (パスワード暗号化) Password Recovery (パスワードリカバリ)	
SRM Prefer Current Settings (SRM 最適化設定) SRM Prefer Mode (SRM 設定モード) <u>57章 Management (スイッチの管理)</u> Command Logging (コマンドログ設定) User Accounts Settings (ユーザアカウント設定) CLI Alias Settings (CLI エイリアス設定) Password Encryption (パスワード暗号化) Password Recovery (パスワードリカバリ) Login Method (ログイン方法)	
SRM Prefer Current Settings (SRM 最適化設定)         SRM Prefer Mode (SRM 設定モード)         7 章 Management (スイッチの管理)         Command Logging (コマンドログ設定)         User Accounts Settings (ユーザアカウント設定)         CLI Alias Settings (CLI エイリアス設定)         Password Encryption (パスワード暗号化)         Password Recovery (パスワードリカバリ)         Login Method (ログイン方法)         SNMP (SNMP 設定)	
SRM Prefer Current Settings (SRM 最適化設定) SRM Prefer Mode (SRM 設定モード) <u>57章 Management (スイッチの管理)</u> Command Logging (コマンドログ設定) User Accounts Settings (ユーザアカウント設定) User Accounts Settings (ユーザアカウント設定) CLI Alias Settings (CLI エイリアス設定) Password Encryption (パスワード暗号化) Password Recovery (パスワード暗号化) Login Method (ログイン方法) SNMP (SNMP 設定) トラップ	
SRM Prefer Current Settings (SRM 最適化設定) SRM Prefer Mode (SRM 設定モード) <u>SRM Prefer Mode (SRM 設定モード)</u> <u>SRM Prefer Mode (SRM 設定モード)</u> <u>SRM Prefer Mode (スイッチの管理)</u> Command Logging (コマンドログ設定) User Accounts Settings (ユーザアカウント設定) User Accounts Settings (ユーザアカウント設定) CLI Alias Settings (CLI エイリアス設定) Password Encryption (パスワード暗号化) Password Recovery (パスワード暗号化) Login Method (ログイン方法) SNMP (SNMP 設定) トラップ MIB	
SRM Prefer Current Settings (SRM 最適化設定) SRM Prefer Mode (SRM 設定モード) <u>SRM Prefer Mode (SRM 設定モード)</u> Command Logging (コマンドログ設定) User Accounts Settings (ユーザアカウント設定) User Accounts Settings (ユーザアカウント設定) CLI Alias Settings (CLI エイリアス設定) Password Encryption (パスワード暗号化) Password Recovery (パスワード暗号化) Login Method (ログイン方法) SNMP (SNMP 設定) トラップ	
SRM Prefer Current Settings (SRM 最適化設定) SRM Prefer Mode (SRM 設定モード) <u>SRM Prefer Mode (SRM 設定モード)</u> Command Logging (コマンドログ設定) User Accounts Settings (ユーザアカウント設定) CLI Alias Settings (CLI エイリアス設定) Password Encryption (パスワード暗号化) Password Recovery (パスワード暗号化) Login Method (ログイン方法) SNMP (SNMP 設定) トラップ	
SRM Prefer Current Settings (SRM 最適化設定) SRM Prefer Mode (SRM 設定モード) <u>SRM Prefer Mode (SRM 設定モード)</u> Command Logging (コマンドログ設定) User Accounts Settings (ユーザアカウント設定) CLI Alias Settings (CLI エイリアス設定) Password Encryption (パスワード暗号化) Password Recovery (パスワード暗号化) Login Method (ログイン方法) SNMP (SNMP 設定) トラップ MIB SNMP Global Settings (SNMP グローバル設定) SNMP Linkchange Trap Settings (SNMP リンクチェンジトラップ設定) SNMP View Table Settings (SNMP ビューテーブル)	
SRM Prefer Current Settings (SRM 最適化設定)         SRM Prefer Mode (SRM 設定モード)         SRM Prefer Mode (SRM 設定モード)         Command Logging (コマンドログ設定)         User Accounts Settings (ユーザアカウント設定)         CLI Alias Settings (CLI エイリアス設定)         Password Encryption (パスワード暗号化)         Password Recovery (パスワードリカバリ)         Login Method (ログイン方法)         SNMP (SNMP 設定)         トラップ         MIB         SNMP Global Settings (SNMP グローバル設定)         SNMP Linkchange Trap Settings (SNMP ビューテーブル)         SNMP View Table Settings (SNMP コミュニティテーブル設定)	
SRM Prefer Current Settings (SRM 最適化設定) SRM Prefer Mode (SRM 設定モード)	
SRM Prefer Current Settings (SRM 最適化設定)         SRM Prefer Mode (SRM 設定モード)         SRM Prefer Mode (SRM 設定モード)         ST 章 Management (スイッチの管理)         Command Logging (コマンドログ設定)         User Accounts Settings (ユーザアカウント設定)         CLI Alias Settings (CLI エイリアス設定)         Password Encryption (パスワード暗号化)         Password Recovery (パスワードリカバリ)         Login Method (ログイン方法)         SNMP (SNMP 設定)         トラップ         MIB         SNMP Global Settings (SNMP グローバル設定)         SNMP Linkchange Trap Settings (SNMP リンクチェンジトラップ設定)         SNMP View Table Settings (SNMP ゴューテーブル)         SNMP Group Table Settings (SNMP ゴループテーブル)         SNMP Group Table Settings (SNMP ブループテーブル)         SNMP Fingine ID Local Settings (SNMP エンジン ID ローカル設定)	
SRM Prefer Current Settings (SRM 最適化設定)	
SRM Prefer Current Settings (SRM 最適化設定)         SRM Prefer Mode (SRM 設定モード)         SRM Prefer Mode (SRM 設定モード)         ST 章 Management (スイッチの管理)         Command Logging (コマンドログ設定)         User Accounts Settings (ユーザアカウント設定)         CLI Alias Settings (CLI エイリアス設定)         Password Encryption (パスワード暗号化)         Password Recovery (パスワード時号化)         Password Recovery (パスワードリカバリ)         Login Method (ログイン方法)         SNMP (SNMP 設定)         トラップ         MIB         SNMP Global Settings (SNMP グローバル設定)         SNMP Linkchange Trap Settings (SNMP リンクチェンジトラップ設定)         SNMP View Table Settings (SNMP ジューテーブル)         SNMP Community Table Settings (SNMP コミュニティテーブル設定)         SNMP Group Table Settings (SNMP エンジン ID ローカル設定)         SNMP Lot Settings (SNMP エンジン ID ローカル設定)         SNMP Host Table Settings (SNMP エンジン ID ローカル設定)	
SRM Prefer Current Settings (SRM 最適化設定)	
SRM Prefer Current Settings (SRM 最適化設定)	
SRM Prefer Current Settings (SRM 最適化設定)         SRM Prefer Mode (SRM 設定モード)         G 7 章 Management (スイッチの管理)         Command Logging (コマンドログ設定)         User Accounts Settings (ユーザアカウント設定)         CLI Alias Settings (CLI エイリアス設定)         Password Encryption (パスワード暗号化)         Password Recovery (パスワード明白バリ)         Login Method (ログイン方法)         SNMP (SNMP 設定)         トラッブ         MIB         SNMP Global Settings (SNMP グローバル設定)         SNMP Global Settings (SNMP グローバル設定)         SNMP Community Table Settings (SNMP ビューテーブル)         SNMP Community Table Settings (SNMP ジューテーブル)         SNMP Group Table Settings (SNMP エンジン ID ローカル設定)         SNMP Ispine ID Local Settings (SNMP エンジン ID ローカル設定)         SNMP Host Table Settings (SNMP エンジン ID ローカル設定)         SNMP Host Table Settings (SNMP エンジン ID ローカル設定)         SNMP Context Mapping Table Settings (SNMP コンテキストマッピングテーブル設定) (El/MI モードのみ)         RMON (RMON 設定)         RMON (RMON 設定)	
SRM Prefer Current Settings (SRM 最適化設定)         SRM Prefer Mode (SRM 設定モード)         第7章 Management (スイッチの管理)         Command Logging (コマンドログ設定)         User Accounts Settings (ユーザアカウント設定)         CLI Alias Settings (CLI エイリアス設定)         Password Encryption (パスワード暗号化)         Password Recovery (パスワード暗号化)         Password Recovery (パスワード暗号化)         Password Recovery (パスワード暗号化)         Password Recovery (パスワードロカバリ)         Login Method (ログイン方法)         SNMP (SNMP 設定)         トラッブ         MIB         SNMP Global Settings (SNMP グローバル設定)         SNMP Global Settings (SNMP グローバル設定)         SNMP Global Settings (SNMP グローバル設定)         SNMP Group Table Settings (SNMP ビューテーブル)         SNMP Community Table Settings (SNMP ジューテーブル)         SNMP Group Table Settings (SNMP ガループテーブル)         SNMP Local Settings (SNMP ガループテーブル設定)         SNMP User Table Settings (SNMP ガループテーブル設定)         SNMP Local Settings (SNMP ガーデデーブル設定)         SNMP Kont Table Settings (SNMP オーゲテーブル設定)         SNMP Context Mapping Table Settings (SNMP コンテキストマッピングテーブル設定)         SNMP Context Mapping Table Settings (SNMP コンテキストマッピングテーブル設定)         RMON (RMON 設定)         RMON (RMON 設定)         RMON Statiet Context Context (MON グロー/バル設定)	
SRM Prefer Current Settings (SRM 最適化設定)         SRM Prefer Mode (SRM 設定モード)         第7章 Management (スイッチの管理)         Command Logging (コマンドログ設定)         User Accounts Settings (ユーザアカウント設定)         CLI Alias Settings (CLI エイリアス設定)         Password Encryption (パスワード暗号化)         Password Recovery (パスワード時号化)         Password Recovery (パスワード時号化)         Password Recovery (パスワードリカバリ)         Login Method (ログイン方法)         SNMP (SNMP 設定)         トラップ         MIB         SNMP Global Settings (SNMP グローバル設定)         SNMP Global Settings (SNMP グローバル設定)         SNMP Global Settings (SNMP ビューテーブル)         SNMP Global Settings (SNMP ビューテーブル)         SNMP Group Table Settings (SNMP ジループテーブル)         SNMP Group Table Settings (SNMP ブループテーブル)         SNMP Group Table Settings (SNMP エンジン ID ローカル設定)         SNMP Iser Table Settings (SNMP エンジン ID ローカル設定)         SNMP Host Table Settings (SNMP エンジン ID ローカル設定)         SNMP Host Table Settings (SNMP ホトテーブル設定)         SNMP Context Mapping Table Settings (SNMP コンテキストマッピングテーブル設定)         RMON Global Settings (RMON グローバル設定)         RMON Global Settings (RMON グローバル設定)         RMON Global Settings (RMON グローバル設定)         RMON Statistics Settings (RMON グローバル設定)         RMON Statistics Settings (RMON グローバル設定) <td></td>	
SRM Prefer Current Settings (SRM 最適化設定)         SRM Prefer Mode (SRM 設定モード)         第7章 Management (スイッチの管理)         Command Logging (コマンドログ設定)         User Accounts Settings (ユーザアカウント設定)         CLI Alias Settings (CLI エイリアス設定)         Password Encryption (パスワード暗号化)         Password Recovery (パスワード暗号化)         Password Recovery (パスワード暗号化)         Password Recovery (パスワード暗号化)         Password Recovery (パスワードリカパリ)         Login Method (ログイン方法)         SNMP (ShMP 設定)         トラッブ         MIB.         SNMP Global Settings (SNMP グローバル設定)         SNMP Global Settings (SNMP グローバル設定)         SNMP Global Settings (SNMP グローバル設定)         SNMP Compunity Table Settings (SNMP ジューテーブル)         SNMP Compunity Table Settings (SNMP ジューテーブル)         SNMP Compunity Table Settings (SNMP ブシジン ID ローカル設定)         SNMP Link Table Settings (SNMP エーザテーブル設定)         SNMP Host Table Settings (SNMP エーザテーブル設定)         SNMP Kont Table Settings (SNMP エーザテーブル設定)         SNMP Kont Table Settings (SNMP コンテキストマッピングテーブル設定)         SNMP Kont Table Settings (SNMP コンテキストマッピングデーブル設定)         RMON Global Settings (RMON 校コーバル設定)         RMON Global Settings (RMON 校コーバル設定)         RMON History Settings (RMON 校コーバル設定)	
SRM Prefer Current Settings (SRM 最適化設定)         SRM Prefer Mode (SRM 設定モード)         第7章 Management (スイッチの管理)         Command Logging (コマンドログ設定)         User Accounts Settings (ユーザアカウント設定)         CLI Alias Settings (CLI エイリアス設定)         Password Encryption (パスワード暗号化)         Password Recovery (パスワードロカバリ)         Login Method (ログイン方法)         SNMP (SNMP 設定)         NMP (SNMP 設定)         SNMP Global Settings (SNMP グローバル設定)         SNMP Inikchange Trap Settings (SNMP リンクチェンジトラップ設定)         SNMP View Table Settings (SNMP ビューテーブル)         SNMP Community Table Settings (SNMP グリーブテーブル)         SNMP Group Table Settings (SNMP グループテーブル)         SNMP Local Settings (SNMP グルンジン ID ローカル設定)         SNMP Local Settings (SNMP エンジン ID ローカル設定)         SNMP Local Settings (SNMP エンジン ID ローカル設定)         SNMP Local Settings (SNMP エンジン ID ローカル設定)         SNMP Context Mapping Table Settings (SNMP コンテキストマッビングテーブル設定)         SNMP Context Mapping Table Settings (SNMP コンテキストマッビングテーブル設定)         SNMP Context Mapping Table Settings (SNMP コンテキストマッビングテーブル設定)         RMON Global Settings (RMON グローバル設定) <td></td>	
SRM Prefer Current Settings(SRM 漫遊七設定) SRM Prefer Mode(SRM 設定モード) 57章 Management(スイッチの管理) Command Logging(コマンドログ設定) User Accounts Settings(ユーザアカウント設定) CLI Alias Settings(ユーザアカウント設定) Password Encryption(パスワード暗号化) Password Encryption(パスワード暗号化) Password Recovery(パスワード暗号化) Login Method(ログイン方法) SNMP (SNMP 設定) トラッブ MIB SNMP Global Settings(SNMP グローバル設定) SNMP Linkchange Trap Settings(SNMP リンクチェンジトラップ設定) SNMP View Table Settings(SNMP グューテーブル) SNMP Community Table Settings(SNMP ゴューテーブル) SNMP Community Table Settings(SNMP エュニティテーブル設定) SNMP Linkchange Trap Settings(SNMP エューテーブル) SNMP Local Settings(SNMP エューテーブル) SNMP Local Settings(SNMP エューデーブル) SNMP Community Table Settings(SNMP エュニティテーブル設定) SNMP Host Table Settings(SNMP エンジンID ローカル設定) SNMP Host Table Settings(SNMP エンジンID ローカル設定) SNMP Context Mapping Table Settings(SNMP コンテキストマッピングテーブル設定)(EI/MI モードのみ) RMON (RMON 設定) RMON Katistics Settings(RMON ボコーバル設定) RMON Alarm Settings(RMON ドフーム設定) RMON Alarm Settings(RMON イベント設定)	77         78         79         80         80         80         80         82         82         83         83         83         83         83         83         83         83         83         83         83         85         85         86         87         87         88         89         90         90         91         92         93         93         93         94         95         96

гE

cŀ

եը

.1		
DH	CP(DHCP 設定)	99
	Service DHCP(DHCP サービス)	99
	DHCP Class Settings (DHCP クラス設定)	99
	DHCP Server (DHCP $\psi - i \chi$ )	100
	DHCPv6 Server (DHCPv6 サーバ設定)	106
	DHCP Relay (DHCP $UV-$ )	110
	DHCPv6 Relay (DHCPv6 リレー)	117
DH	CP Auto Configuration (DHCP 目動コンフィク設定)	122
DH	CP Auto Image Settings(DHCP 目動イメージ設定)	123
DN	S (トダインネームンステム)	124
	DNS Global Settings (DNS クローハル設定)	124
	DNS Name Server Settings (DNS ネームサーハ設定)	125
NT	_DNS Host Settings (DNS 小人下名設定)	125
IN I	P (ネットワークメイムノロトコル) NTD Global Sattings (NTD グローバル設定)	120
	NTP Global Settings (NTP クローハル設定)	120
	NTP Server Settings (NTP ジーハ設定)	127
	NTP Access Group Settings (NTP アクセスグループ設定)	127
	NTP Key Settings (NTP 建設定)	120
	NTP Interface Settings (NTP インタフェース設定)	129
	NTP Associations (NTP アソシエーション)	130
	NTP Status (NTP ステータス)	130
IP S	Source Interface (IP ソースインタフェース)	131
File	- System (ファイルシステム設定)	132
Sta	cking (スタッキング設定)	134
	- Physical Stacking(物理スタッキング)	138
	Stacking Bandwidth (スタッキング帯域)	139
Vir	tual Stacking (SIM)(仮想スタック設定(SIM))	140
	シングル IP マネジメント(SIM)の概要	140
	バージョン 1.61 へのアップグレード	141
	Single IP Settings(シングル IP 設定)	142
	Topology (トポロジ)	143
	Firmware Upgrade(ファームウェア更新)	147
	Configuration File Backup/ Restore(コンフィグレーションファイルの更新)	147
	Upload Log File (ログファイルのアップロード)	147
D-L	ink Discovery Protocol(D-Link ディスカバリプロトコル)	148
SM	TP Settings(SMTP 設定)	149
Rel	boot Schedule Settings(再起動スケジュール設定)	150
NL	3 FDB Settings(NLB FDB 設定)	151
SD	Card Management (SD カート官理)	152
	SD Card Backup Settings(SD カートへのハックアッフ設定)	152
	SD Card Execute Settings(SD カート美行設定)	152
<u>第8</u> 重	看 L2 Features(L2 機能の設定)	<u>154</u>
EDI		155
FD	D (FUD	155
	Static FDB(スタナイック FDB の設定)	155
	MAC Address Table Settings (MAC アドレステーブル)	150
	MAC Address Table (MAC ) ドレスフ (アル)	158
VL		159
• 27	IEEE 802.1p プライオリティについて	159
	VLAN とは	159
	IEEE 802.10 VLAN	159
VL/	AN (VLAN 設定)	163
	VLAN Configuration Wizard (VLAN 設定ウィザード)	163
	802.1Q VLAN (802.1Q VLAN)	165
	VLAN Interface (VLAN インタフェース)	166
	802.1v Protocol VLAN(802.1v プロトコル VLAN)	172
	GVRP(GVRP の設定)	173
	Asymmetric VLAN (Asymmetric VLAN 設定)	175
	MAC VLAN (MAC VLAN 設定)	176
	LL2VLAN Interface Description (L2VLAN インタフェース概要)	176
	Subnet VLAN (サブネット VLAN)	177
	Super VLAN(Super VLAN 設定)(EI/MI モートのみ)	177

<u>q</u>l

đ

rfi<sup>r</sup>

g	L <sub>E</sub>
Auto Surveillance VLAN (自動サーベイランス VLAN)	
Voice VLAN(音声 VLAN)	
Private VLAN (プライベート VLAN 設定)	
VLAN Tunnel (VLAN トンネル)	
Dot1g Tunnel(Dot1g トンネル)	
VLAN Mapping (VLAN マッピング)	186
VI AN Mapping Profile (VI AN マッピングプロファイル)	187
STP (スパニングツリー設定)	191
802.10-2005 MSTP	191
802 1D-2004 Rapid STP	191
ポートの壮能凄な	102
ホートの状態をす	103
STP Port Settings (STP ポートの設定)	10/
MST Configuration Identification (MST の設定)	105
MST Configuration dentification (MST の設定)	106
MSTD Dart Information (MSTD ポート桂恕)	106
MSTFF011111011111111111111111111111111111	107
ERF5((3.0032))(イークネット・ワンクフロアクフョン設定)	107
ERPS Prolilie (ERPS ノロノ パイル)	
Loopback Detection (ルーノバック検知設定)	
Link Aggregation (リンクアクリケーション)	
ホートトフノックルーフについ(	
MLAG (マルチジャージリンクアクリケーション)	
MLAG Settings (MLAG 設定)	
MLAG Group (MLAG $\mathcal{P}\mathcal{W}-\mathcal{T}$ )	
Flex Links (フレックスリンクス)	
L2 Protocol Tunnel (レイヤ 2 プロトコルトンネル)	
L2 Multicast Control (L2 マルチキャストコントロール)	
IGMP Snooping (IGMP Snooping の設定)	
MLD Snooping (MLD スヌーピング)	
Multicast VLAN (マルチキャスト VLAN)	
PIM Snooping (PIM スヌーピング)	
Multicast Filtering Mode(マルチキャストフィルタリングモード)	
LLDP	232
LLDP Global Settings(LLDP グローバル設定)	
LLDP Port Settings(LLDP ポート設定)	
LLDP Management Address List(LLDP 管理アドレスリスト)	
LLDP Basic TLVs Settings(LLDP ベーシック TLV 設定)	234
LLDP Dot1 TLVs Settings(LLDP Dot1 TLV 設定)	
LLDP Dot3 TLVs Settings(LLDP Dot3 TLV 設定)	
LLDP-MED Port Settings(LLDP-MED ポート設定)	236
LLDP-DCBX Port Settings(LLDP-DCBX ポート設定)	
LLDP Statistics Information(LLDP 統計情報)	
LLDP Local Port Information(LLDP ローカルポート情報)	
LLDP Neighbor Port Information(LLDP ネイバポート情報)	
第0 音  2 Fasturas (  イヤ2 機能の記字)	242
<u> </u>	242
ARP(ARP 設定)	
ARP Elevation (ARP エレベーション)	
ARP Aging Time(ARP エージングタイム設定)	
Static ARP(スタティック ARP 設定)	
ARP Force Aging IP Address(ARP 強制エージアウト設定)	
Proxy ARP (プロキシ ARP)	
ARP Table (ARP テーブルの参照)	
Gratuitous ARP(Gratuitous ARP 設定)	
IPv6 Neighbor (IPv6 ネイバ設定)	
Interface (インタフェース設定)	
IPv4 Interface (IPv4 インタフェース)	
IPv6 Interface(IPv6 インタフェース)	
Loopback Interface (ループバックインタフェース設定)	253
Null Interface (Null インタフェース)	255
	254
IP Forward Protocol (IP 転送プロトコル)	
IP Helner Address (IP ヘルパーアドレス)	255
IPv4 Static/Default Route (IPv4 スタティック / デフォルトルート設定	)
IPv4 Static Boute BED (IPv4 スタティックルート RED)	,

ĻЩ

IDuc Static/Dofault Pouto (IDuc フタニノック / デフェルトルート恐中)	250
IPv6 Static Route RED (IPv6 スタティックルート RED)	
IPv6 Route Table (IPv6 ルートテーブル)	
Route Preference (ルート優先度設定)	
ECMP Settings(ECMP 設定)(EI/MI モードのみ)	
IPv6 General Prefix (IPv6 汎用プリフィクス)	
IP Tunnel Settings(IP トンネル設定)	
URPF Settings(URPF 設定)	
VRF(Virtual Routing and Forwarding)(EI/MI モードのみ)	
VRF Settings (VRF 設定)	
VRF Interface Settings(VRF インタフェース設定)	
RIP (Routing Information Protocol)	
RIP Settings(RIP 設定)	
RIP Distribute List (RIP ディストリビュートリスト)	
RIP Interface Settings (RIP インタフェース設定)	
RIP Database (RIP テータベース)	
KIPng (KIPng 設定)	
KIPng Settings (KIPng 設定)	
RIPhg Interface Settings (RIPhg イノダノエース改正)	
NiFing Database (NiFing ) ータパース)	
OSPFv2 (OSPFv2 設定)	273
OSPEv3	
IP Multicast Routing Protocol (IP マルチキャストルーティングプロトコル)	
IGMP(IGMP 設定)(EI/MI モードのみ)	
MLD(MLD 設定) (EI/MI モードのみ)	
IGMP Proxy(IGMP プロキシ)(EI/MI モードのみ)	
MLD Proxy(MLD プロキシ)(EI/MI モードのみ)	
DVMRP(EI/MI モードのみ)	
PIM(PIM 設定)(EI/MI モードのみ)	
IPMC(IP マルチキャスト設定)	
IPv6MC(IPv6 マルチキャスト設定)	
BGP (Border Gateway Protocol) (EI/MI モードのみ)	
BGP Global Settings(BGP グローバル設定)	
BGP Aggregate Address Settings (BGP アクリゲートアドレス設定)	
BGP Network Settings (BGP ネットワーク設定)	
BGP Route Redistribution Settings(BGP ルート冉万配設定)BGP Route Redistribution Settings(BGP ルート復生記会)	
DGP Route Preference Settings (DGP ルート復元改正)	
BGP Dampening Settings (DGP ダンノニング設定) BGP Dampening Dampened Paths Table (BGP ダンプニングダンプドパステーブル)	348
BGP Dampening Dampened Fatisfics Table (BGP ダンプニングフラップ統計テーブル)	349
BGP Reflector Settings (BGP リフレクタ設定)	350
BGP Confederation Settings (BGP コンフェデレーション設定)	
BGP AS Path Access List Settings(BGP AS パスアクセスリストリスト設定)	
BGP Community List Settings (BGP コミュニティリスト設定)	
BGP Extended Community List Settings(BGP 拡張コミュニティリスト設定)	
BGP Clear Settings(BGP クリア設定)	354
BGP Summary Table(BGP サマリテーブル)	
BGP Routing Table(BGP ルーティングテーブル)	
BGP Labels Table(BGP ラベルテーブル)	357
BGP Neighbor(BGP ネイバ設定)	357
BFD (Bidirectional Forwarding Detection)	
BFD Settings(BFD 設定)	
BFD Neighbor Table (BFD ネイバテーフル)	
ISIS (Intermediate System to Intermediate System) (MI $\pm -FOH$ )	
ISIS Deuter Settings (ISIS クローハル設定)	
isis nouter Settings (ISIS /Vーダ設正)	
isis interface settings (ISIS 1 ノブノエー人政化/ ISIS Padictributa Sattings (ISIS 再副分設空)	
ISIS Redistribute ISIS Settings (ISIS 再配分 ISIS 設定)	
ISIS Route Table (ISIS ルートテーブル)	377
ISIS Database (ISIS データベース)	
ISIS Topology (ISIS トポロジ)	
ISIS Hostname(ISIS ホスト名)	
ISIS Neighbors(ISIS ネイバ)	
IP Route Filter(IP ルートフィルタ)	

цI

ct

IP Prefix List (IP プレフィックスリスト設定) (EI/MI モードのみ)	
Route Map (ルートマップ設定)	
Policy Route(ポリシールート設定)	
VRRP(VRRP 設定)	
VRRPv3 Settings(VRRPv3 設定)	
<u>第 10 章 QoS(QoS 機能の設定)</u>	389
OoS の長所	
QoS について	
Basic Settings(基本設定)	
Port Default CoS(ポートデフォルト CoS 設定)	
Port Scheduler Method(ポートスケジューラーメソッド設定)	
Queue Settings (QoS 設定)	
Cos to Queue Mapping(Cos キューマッヒンク設定)	
Port Kate Limiting(ホートレート制限設定)	
Queue Rate Limiting(キューレード制限設定) Oueue Statistics Table(キュー統計テーブル)	
Advanced Settings (アドバンス設定)	
DSCP Mutation Map (DSCP 変更マップ設定)	
Port Trust State and Mutation Binding(ポートトラスト設定)	
DSCP CoS Mapping(DSCP CoS マップ設定)	
CoS Color Mapping(CoS カラーマップ設定)	
DSCP Color Mapping(DSCP カラーマップ設定)	
Class Map (クラスマップ設定)	
Aggregate Policer(アクリケートホリサー設定) Delie: Man (ポリシーフップ認定)	
POIIcy Map(ホリシーマッフ設定) Policy Binding(ポリシーバインディング設定)	
	405
Network OoS Class Map (ネットワーク OoS クラスマップ)	
Network QoS Policy Map(ネットワーク QoS ポリシーマップ)	
Network QoS Policy Binding(ネットワーク QoS ポリシーバインディング)	
PFC Port Settings(PFC ポート設定)	
WRED (WRED 設定)	
WRED Profile (WRED プロファイル設定)	
WRED Queue (WRED ギュー設定)	
WRED Drop Counter (WRED ドロッフガワフタ設定)	
iSCSI (アイスカジー)iSCSI Settings (アイスカジー設定)	
iSCSI Sessions(アイスカジーセッション)	
	<i>A</i> 1 <i>A</i>
	<u>+1+</u>
ACL Configuration Wizard (ACL 設定ウィザード)	
: ALL CONTIGURATION WIZARD(ALL 設定ワイサートの開始)	
バッットダイン選択 (ACL 設定ワイッート)	
パレート設定 (ACI 設定ウィザード)	
ACL Access List (ACL アクセスリスト)	
Standard IP ACL(通常 IP ACL)	
Extended IP ACL(拡張 IP ACL)	
Standard IPv6 ACL(通常 IPv6 ACL)	
Extended IPv6 ACL(拡張 IPv6 ACL)	
Extended MAC ACL(拡張 MAC ACL)	
Extended Expert ACL(孤張詳細 ACL)	
ACLINIERIACE ACCESS Group (ACL イノダノエースパクセスクルーフ)	
ACL VLAN ACCESS Wap(ACL VLAN ノンセスキッフ) Match Access-List(合致するアクセスリスト設定)	
ACL VLAN Filter (ACL VLAN フィルタ設定)	449
CPU ACL(CPU ACL 設定)	

٦<u>e</u>

rБ

cŀ

## 目次

	Ļ
第 12 章 Security(セキュリティ機能の設定)	452
Port Security(ポートセキュリティ)	
Port Security Global Settings(ポートセキュリティグローバル設定)	
Port Security Port Settings (ポートセキュリティポート設定)	
Port Security Address Entries(ポートセキュリティアドレスエントリ設定)	
802.1X(802.1X 設定)	
802.1X Global Settings(802.1X グローバル設定)	
802.1X Port Settings(802.1X ポート設定)	
Authentication Session Information(オーセンティケーションセッションの状態)	
Authenticator Statistics(オーセンティケータ統計情報)	
Authenticator Session Statistics(オーセンティケータセッション統計情報)	
Authenticator Diagnostics(オーセンティケータ診断)	
AAA(AAA 設定)	
AAA Global Settings (AAA グローバル設定)	
Application Authentication Settings(アプリケーションの認証設定)	
Application Accounting Settings(アプリケーションアカウント設定)	
Authentication Settings(認証設定)	
Accounting Settings(アカウンティング設定)	
RADIUS(RADIUS 設定)	
RADIUS Global Settings(RADIUS グローバル設定)	
RADIUS Server Settings (RADIUS サーバの設定)	
RADIUS Group Server Settings(RADIUS グループサーバの設定)	
RADIUS Statistic (RADIUS 統計情報)	
TACACS+(TACACS+ 設定)	
TACACS+ Global Settings(TACACS+ サーバグローバル設定)	
TACACS+ Server Settings (TACACS+ サーバの設定)	
TACACS+ Group Server Settings(TACACS+ グループサーバの設定)	
TACACS+ Statistic (TACACS+ 統計情報)	
IMPB(IP-MAC-Port Binding / IP-MAC- ボートバインディング)	
IPv4	
DHCP Server Screening (DHCP サーバスクリーニンク設定)	
DHCP Server Screening Global Settings (DHCP サーバスクリーニンググローバル設定)	
DHCP Server Screening Port Settings(DHCP サーバスクリーニンクホート設定)	
ARP Spoofing Prevention (ARP スフーノインク防止設定)	
BPDU Attack Protection (BPDU パダック防止設定)	
NetBIOS Filtering (NetBIOS フィルタリンク設定)	
MAC AULINERLICATION (MAC 認証)	
Web-based Access Control (Web 認証)	
Web Authentication(Web 認証改進) WAC Part Cattings(Web 認証文化)	
WAC Poil Settings (Web 誌証小一下改定/	
WAC Customize Page(WAC ガスダマイスペーン設定)	
Japanese web-based Access Control (JWAC 設定)	500
JWAC Global Settings (JWAC ジローハル設定)	501
JWAC Fuctomize Dage Language (IWAC カフタマイブ画面言語設定)	502
JWAC Customizer age Language (JWAC カスタマイズ)	502
Network Access Authentication (ネットワークアクセス認証)	504
Network Access Addition (ホットワーフナフラビス認証)	504
Guest VEAN (アスト VEAN 設定)	504
Network Access Authentication Port Settings (ネットワークアクセス認証プロ ノバル設定)	505
Network Access Authentication Sessions Information (ネットワークアクセス認証が、1000)	506
Safeguard Engine (オーフガードエンジン)	507
Safeguard Engine (ビークガードエンジン設定)	508
CPU Protect Counters (CPU プロテクトカウンタ)	508
CPU Protect Sub-Interface (CPU プロテクトサブインタフェース)	509
CPU Protect Type (CPU プロテクトタイプ)	509
Trusted Host $( h = \lambda h + \lambda h)$	
Traffic Segmentation (トラフィックセグメンテーション)	
Storm Control Settings (ストームコントロール設定)	
DoS Attack Prevention Settings (DoS 攻撃防止設定)	
Zone Defense Settings(ゾーンディフェンス設定)	
SSH (Secure Shell)	514
SSH Global Settings(SSH グローバル設定)	
Host Key (Host Key 設定)	
SSH Server Connection(SSH サーバ接続)	
	r

ц.

đ

ch

ц	
SSH User Settings (SSH コーザ設定)	516
SSH Client Settings(SSH クライアント設定)	517
SSI (Secure Socket Laver)	518
SSE Global Settings (SSI グローバル設定)	519
Crypto PKI Trustpoint(暗号 PKI トラストポイント)	
SSL Service Policy (SSLサービスポリシー)	
SFTP Server Settings (SFTP サーバ設定)	
SFTP Client Settings (SFTP クライアント設定)	
Network Protocol Port Protect Settings(ネットワークプロトコルポートプロテクト設定)	
<u>第13章 OAM (Operations, Administration, Maintenance:連用・管理・保守)</u>	523
CFM(Connectivity Fault Management : 接続性障害管理)	
CFM Settings (CFM 設定)	
CFM Port Settings(CFM ポート設定)	
CFM Loopback Test (CFM ループバックテスト)	534
CFM Linktrace Settings(CFM リンクトレース設定)	
CFM Packet Counter (CFM パケットカウンタ)	
CFM Counter CCM(CFM カウンタ CCM)	
CFM MIP CCM Table(CFM MIPCCM テーブル)	537
CFM MEP Fault Table(CFM MEP 障害テーブル)	
Cable Diagnostics(ケーブル診断機能)	537
Ethernet OAM(イーサネット OAM)	538
Ethernet OAM Settings(イーサネット OAM 設定)	538
Ethernet OAM Configuration Settings(イーサネット OAM コンフィグレーション設定)	539
Ethernet OAM Event Log Table(イーサネット OAM イベントログテーブル)	
Ethernet OAM Statistics Table(イーサネット OAM 統計情報テーブル)	
Ethernet OAM DULD Settings(イーサネット OAM DULD 設定)	541
DDM(DDM 設定)	
DDM Settings(DDM 設定)	
DDM Temperature Threshold Settings(DDM 温度しきい値設定)	
DDM Voltage Threshold Settings(DDM 電圧しきい値設定)	
DDM Bias Current Threshold Settings(DDM ハイアス電流しきい値設定)	
DDM TX Power Threshold Settings(DDM 送信電力しきい値設定)	
DDM RX Power Threshold Settings(DDM 受信電力しざい値設定)	
DDM Status Table(DDM ステーダステーブル)	
<u>第 14 章 MPLS(MI モードのみ)</u>	546
MDISIDPInformation Sattings(MDISIDP 情報設定)	547
MPLS LSP Trigger Information (MPLS LSP 目前版定)	549
MPLS Forwarding Settings (MPLS フォワーディング設定)	550
MPISIDP Neighbor Password Settings(MPISIDP ネイバパスワード設定)	551
MPLS LDP Neighbor Targeted Settings (MPLS LDP ネイバターゲット設定)	
MPLS LDP Neighbor Information (MPLS LDP ネイバ情報)	
MPLS Global Settings (MPLS グローバル設定)	
MPLS LDP Interface Settings(MPLS LDP インタフェース設定)	
MPLS LDP Session Information (MPLS LDP セッション情報)	
MPLS LDP Statistic (MPLS LDP スタティスティック)	
MPLS LDP Binding Table(MPLS LDP バインディングテーブル)	
MPLS LDP Discovery Information (MPLS LDP ディスカバリ情報)	
MPLS QoS Settings(MPLS QoS 設定)	
Ping MPLS	
Traceroute MPLS IPv4 (トレースルート MPLS IPv4)	
第 15 音 MPI S I 2VPN (MI モードのみ)	567
VYWS Settings(VYWS 設定)	
LZVC INTERFACE DESCRIPTION(LZVC インダノエース概要)	
VFLS Settings (VFLS 政府)	

lը

第 16 章 Monitoring(スイッチのモニタリング)	570
VLAN Counter (VLAN カウンタ)	
Utilization(利用分析)	
Port Utilization(ポート使用率)	
History Utilization(使用履歷)	
Statistics (統計情報)	
Port (ポート統計情報)	
CPU Port (CPU $\cancel{r} - \cancel{r}$ )	
Interface Counters(インタフェースカウンタ)	
Interface History Counters(インタフェースカウント履歴)	
Counters (カウンタ)	
Mirror Settings(ミラー設定)	
sFlow (sFlow 設定)	
sFlow Agent Information (sFlow エージェント情報)	
sFlow Receiver Settings(sFlow レシーハ設定)	
sFlow Sampler Settings (sFlow サンフラ設定)	
SFIOW Poller Settings (SFIOW ホーフ設定)	
Device Environment (機奋項項唯認)	
External Alarm Settings (外部) ワーム設定)	
第 17 章 Green(省電力機能)	584
Power Saving (省雷力)	585
EEE(Energy Efficient Ethernet/ 省電力イーサネット)	
× 10 辛 Onen-Flaux	F 0 7
<u>お18 卓 OpenFlow</u>	
OpenFlow Settings(OpenFlow 設定)	
育 19 章 Save and Tools(Save メニュー /Tools メニュー)	590
Save (Save メニュー)	
Save Configuration (コンフィグレーションの保存)	
Tools (Tools $\neq = = -$ )	
Firmware Upgrade & Backup(ファームウェアアップグレード&バックアップ)	
Configuration Restore & Backup (コンフィグレーションリストア&バックアップ)	
Certificate & Key Restore & Backup (証明書 / 鍵リストア&ハックアップ)	
Log Backup (ロクノアイルのハックパッフ)	
Ping	
Face Route (FV - XV - F)	
Reset (リゼット) Behaat System (シスニノ再規動)	
Rebool System (クステム冉起動) DI MS Sattings (DI MS 設定)	
	615
付録 A パスワードリカバリ手順	615
付録 B システムログエントリ	616
付録 C トラップログエントリ	
付録 D OpenFlow オフジェクト	
Flow Table $(7 \Box - \tau - 7 \mu)$	
Group Table $(\mathcal{I}\mathcal{V} - \mathcal{I}\mathcal{T} - \mathcal{I}\mathcal{V})$	
L2 Interface Group Entry Type	
L2 Rewrite Group Entry Type	
L2 Unicast Group Entry Type	
LS Officast Group Entry Type	
Meter Table (メーターテーブル)	665
付録 E RADIUS 属性割り当て	
付録 F IETF RADIUS 属性サポート	
付録 G 機能設定例	
対象機器について	
Traffic Segmentation(トラフィックセグメンテーション)	
VLAN	
Link Aggregation (リンクアグリゲーション)	
Access List (アクセスリスト)	
Loopback Detection(LBD)(ループ検知)	675

d

```
はじめに
```

# はじめに

DGS-3630 シリーズユーザマニュアルは、本スイッチのインストールおよび操作方法を例題と共に記述しています。

- 第1章 本製品のご使用にあたって
  - 本スイッチの概要とその機能について説明します。また、前面、背面、側面の各パネルと LED 表示について説明します。
- 第2章 スイッチの設置
  - システムの基本的な設置方法について説明します。また、本スイッチの電源接続の方法についても紹介します。
- 第3章 スイッチの接続
  - スイッチをご使用のネットワークに接続する方法を説明します。
- 第4章 スイッチ管理について
  - パスワード設定、SNMP 設定、および各種デバイスからの本スイッチへの接続など基本的なスイッチの管理について説明します。
- 第5章 Web ベースのスイッチ管理
  - Web ベースの管理機能への接続方法および使用方法について説明します。
- 第6章 System(スイッチの主な設定)
  - デバイス情報、ポート設定、ユーザアカウント、システムログ設定、時刻設定などの基本機能の設定について説明します。
- 第7章 Management (スイッチの管理)
  - シングル IP マネジメント設定、SNMP 設定、Telnet 設定、Web 設定などの管理機能について説明します。
- 第8章 L2 Features(L2機能の設定)
  - VLAN、トランキング、スパニングツリー、LLDP などのレイヤ 2 機能について説明します。
- 第9章 L3 Features (レイヤ3機能の設定)
  - ARP 設定、インタフェース設定、ルート再配布設定、スタティック / ダイナミックルート設定、ルート優先度設定、RIP、OSPF、VRRP、IP マルチキャ ストルーティングプロトコル、BGP、BFD、ISIS、VRRP などのレイヤ 3 機能について説明します。
- 第10章 QoS (QoS 機能の設定)
  - QoS 機能について説明します。帯域制御、QoS スケジューリング、802.1p デフォルトプライオリティ、802.1p ユーザプライオリティなどの 機能を含みます。
- 第11章 ACL (ACL 機能の設定)
  - ACL アクセスリスト、ACL VLAN アクセスマップ、CPU ACL などの ACL(アクセスコントロールリスト)機能について説明します。
- 第 12 章 Security(セキュリティ機能の設定)
  - 802.1X、トラストホスト、アクセス認証コントロール、ポートセキュリティ、トラフィックセグメンテーション、SSL、SSH、IP-MAC-ポート バインディング、IP マルチキャスト範囲の制限、Web ベースアクセスコントロール、MAC ベースアクセスコントロールおよびセーフガー ドエンジンなどのセキュリティ機能について説明します。
- 第 13 章 OAM (Operations, Administration, Maintenance:運用・管理・保守)
  - CFM (接続性障害管理)、イーサネット OAM、DDM、ケーブル診断機能機能について説明します。
- 第14章 MPLS (MIモードのみ)
  - MPLS LDP、MPLS LSP、MPLS フォワーディング、MPLS QoS、Ping MPLS、トレースルート MPLS などについて説明します。
- 第15章 MPLS L2VPN (MIモードのみ)
  - VPWS 設定、L2VC インタフェース、VPLS 設定、VPLS MAC アドレステーブルなどについて説明します。
- 第16章 Monitoring (スイッチのモニタリング)
  - CPU 使用率、パケット統計情報、エラー、パケットサイズ、ミラーリング、sFlow、外部アラーム設定などのモニタ機能について説明します。
- 第 17 章 Green(省電力機能)
  - Power Saving(省電力)、EEE(Energy Efficient Ethernet/ 省電力イーサネット)について説明します。
- 第18章 OpenFlow
  - OpenFlow の設定について説明します。
- 第 19 章 Save and Tools (Save メニュー /Tools メニュー)
  - コンフィグレーションの保存、ファームウェアアップグレード&バックアップ、コンフィグレーションリストア&バックアップ、ログファ イルのバックアップ、Ping、トレースルート、リセット、システム再起動、DLMS 設定について説明します。

### ● 付録

- 付録 A パスワードリカバリ手順
- パスワードのリセット、リカバリについて説明します。
- 付録 B システムログエントリ
   スイッチのシステムログに表示される可能性のあるログイベントについて説明します。
- ・ 付録 C トラップログエントリ
  - トラップログエントリついて説明します。
- 付録 D OpenFlow オブジェクト
  - OpenFlow オブジェクトについて説明します。
- ・ 付録 E RADIUS 属性割り当て
  - スイッチの RADIUS 属性割り当てについて説明します。
- 付録 F IETF RADIUS 属性サポート
  - 現在スイッチによりサポートされる IETF RADIUS 属性一覧です。
- 付録 G 機能設定例
  - スイッチの機能設定例です。

# 本マニュアルの対象者

本マニュアルは、本製品の設置および管理についての情報を記載しています。また、ネットワーク管理の概念や用語に十分な知識を持っているネッ トワーク管理者を対象としています。

## 表記規則について

本項では、本マニュアル中での表記方法について説明します。



注意 注意では、特長や技術についての詳細情報を記述します。

警告では、設定の組み合わせ、イベントや手順によりネットワークの接続状態やセキュリティなどに悪影響を及ぼす恐れのある事項につい 警告 て説明します。

表1に、本マニュアル中での字体、・記号についての表記規則を表します。

#### 表1 字体・記号の表記規則

字体・記号	解説	例
٢J	メニュータイトル、ページ名、ボタン名。	「Submit」ボタンをクリックして設定を確定してください。
青字	参照先。	" ご使用になる前に "(13 ページ)をご参照ください。
courier フォント	CLI 出力文字、ファイル名。	(switch-prompt)#
<b>courier</b> 太字	コマンド、ユーザによるコマンドライン入力。	show network
<i>courier</i> 斜体	コマンドパラメータ(可変または固定)。	value
< >	可変パラメータ。<>にあたる箇所に値または文字を入力します。	<value></value>
[]	任意の固定パラメータ。	[value]
[<>]	任意の可変パラメータ。	[ <value>]</value>
{}	{}内の選択肢から1つ選択して入力するパラメータ。	{choice1   choice2}
(垂直線)	相互排他的なパラメータ。	choice1 choice2
[{ }]	任意のパラメータで、指定する場合はどちらかを選択します。	[{choice1   choice2}]

# 製品名 / 品番一覧

製品名	HW バージョン	区分	品番
	A1	SI 版	DGS-3630-28SCSI/A1
	A1	EI 版	DGS-3630-28SCEI/A1
DCC 2620 200C	A1	MI版	DGS-3630-28SCMI/A1
DGS-3630-28SC	A2	SI 版	DGS-3630-28SCSI/A2
	A2	EI 版	DGS-3630-28SCEI/A2
	A2	MI版	DGS-3630-28SCMI/A2
	A1	SI 版	DGS-3630-28TCSI/A1
	A1	EI 版	DGS-3630-28TCEI/A1
DGS-3630-28TC	A1	MI 版	DGS-3630-28TCMI/A1
	A2	SI 版	DGS-3630-28TCSI/A2
	A2	EI 版	DGS-3630-28TCEI/A2
	A2	MI版	DGS-3630-28TCMI/A2
	A1	SI 版	DGS-3630-52TCSI/A1
	A1	EI 版	DGS-3630-52TCEI/A1
DGS-3630-52TC	A1	MI 版	DGS-3630-52TCMI/A1
DG3-3030-321C	A2	SI 版	DGS-3630-52TCSI/A2
	A2	EI 版	DGS-3630-52TCEI/A2
	A2	MI版	DGS-3630-52TCMI/A2
	A2	SI 版	DGS-3630-28PCSI/A2
DGS-3630-28PC	A2	EI 版	DGS-3630-28PCEI/A2
	A2	MI版	DGS-3630-28PCMI/A2
	A2	SI 版	DGS-3630-52PCSI/A2
DGS-3630-52PC	A2	EI 版	DGS-3630-52PCEI/A2
	A2	MI版	DGS-3630-52PCMI/A2

# 第1章 本製品のご使用にあたって

- DGS-3630 シリーズについて
- ポート
- 前面パネル
- 背面パネル
- 側面パネル

## DGS-3630 シリーズについて

D-Link Green 機能を実装した DGS-3630 シリーズは、SMB からエンタープライズ向けの中規模ネットワークにおいて柔軟性、冗長性、セキュリティ を実現し、安定したパフォーマンスでネットワーク通信を提供することが可能な高性能な次世代ギガビットレイヤ3スイッチです。 本シリーズは、DGS-3630-28TC、DGS-3630-52TC に加え、PoE/PoE+ に対応した DGS-3630-28PC、DGS-3630-52PC、SFP 多ポートに対応した DGS-3630-28SC の5 製品で構成されています。全ての製品には 10GE SFP+ スロットが4つ搭載されており、物理スタック /10G アップリンクとして利用 が可能です。また高密度 SFP ポートスイッチの利点を活かし、FTTB ネットワークのコアを形成します。ITU-T G.8032 準拠の E-RPS プロトコルに対 応したリング構成による冗長化や、IEEE802.3ah、Q-in-Q などメトロイーサネット機能にも対応し、柔軟なネットワーク構築が可能です。また、ルー プ検知 / 遮断機能、ケーブル診断機能、デジタル診断モニタ(DDM)などの障害切り分けを容易にするサポート機能等が充実しています。

#### ニーズに合わせたイメージを選択

本スイッチは、ユーザのニーズに合わせて MPLS バージョン (MI)、エンハンスドバージョン (EI) とスタンダードバージョン (SI) に分かれており、必要な機能に応じて機器のバージョンを選択することが可能です。MI バージョン、EI バージョンは SI バージョンの全ての機能を搭載し、様々な機能を追加した高機能版となっております。主に EI バージョンは「OSPF」「BGP」やL3 マルチキャスト対応機能などを有し、MI バージョンは「IS-IS」や「MPLS L2/L3 VPN」などの VPN サービスを提供します。

#### IPv6 テクノロジー

本シリーズは、IPv6 Ready Logo Phase-2 を取得しています(DGS-3630-28PC/52PC は除く)。また、OSFPv3(EI/MI)、BGP4(EI/MI)、PIM SMv6(EI/ MI)など IPv6 環境でのルーティングやマルチキャスト制御にも対応しています。

#### 安定の可用性と多様な管理機能

「Switch Resource Management」(SRM)の実装により、「IP モード」「LAN モード」「L2 VPN モード」が選択可能になり、スイッチの使用モードに よって L2/L3 テーブルサイズを変更され、各機能の最適化を行うことができます。更に DGS-3630 シリーズはネットワークマネージメントシステム や Web GUI、CLI を使用することでリモートからの管理や、SNMP などにより帯域外の多数の機器をコンソールポートを通して集権的に管理をする ことが可能です。パネルには「mini-USB」「RJ45」二つのコンソールポート、USB ポート、MGMT ポートが装備され、広いニーズに対応した多彩な 管理を実現することが可能です。

#### 10G テクノロジー

本シリーズは、高速なバックボーンネットワークに対応するため、10G に対応した SFP+ スロットを各4 スロット搭載しています。10G SFP+ スロットでの最大9 台までの物理スタックに対応し、帯域を最大80G まで選択することが可能です。

本マニュアルでは、DGS-3630シリーズの設置、管理、および設定の方法について記述しています。

# ポート

#### DGS-3630 シリーズは以下のポートを搭載しています。

製品名	DGS-3630-28SC	DGS-3630-28TC	DGS-3630-28PC	DGS-3630-52TC	DGS-3630-52PC
10/100/1000BASE-Tポート (RJ-45) (PoE 給電)	4 (SFP 4 スロットとのコンボ)	24	24 (24)	48	48 (48)
SFPスロット	24	4	4	4	4
	24	(1000BASE-T 4 ポートとのコンボ)	(1000BASE-T4ポートとのコンボ)	(1000BASE-T4ポートとのコンボ)	(1000BASE-T4ポートとのコンボ)
10ギガSFP+スロット			4		
コンソールポート (RJ-45)			1		
コンソールポート (Mini USB)			1		
管理ポート(MGMT)(RJ-45)			1		
アラームポート (ALARM) (RJ-45)			1		
USB ポート (USB2.0)			1		

### DGS-3630 シリーズスイッチ対応オプションモジュール

種別	製品名
	DEM-431XT
	DEM-432XT
SFP+(10Giga) <sup>* 1</sup>	DEM-433XT
SFF+(TUGIGA)	DEM-434XT
	DEM-436XT-BXU
	DEM-436XT-BXD
Copper SFP+(10Giga) <sup>** 1</sup>	DEM-410T
	DEM-330T
VDM 対応 1 芯 SFP(1Giga)	DEM-330R
	DEM-331T
	DEM-331R
	DEM-310GT
	DEM-311GT
2芯SFP(1Giga)	DEM-312GT2
	DEM-314GT
	DEM-315GT
Copper SFP(1Giga)	DGS-712
100PV SED * 2	DEM-220T
	DEM-220R
100FX SFP ** 2	DEM-210

※1 SFP+ スロットでのみ使用可能です。

※2 SFP スロットもしくは SFP コンボスロットでのみ使用可能です。

## 前面パネル

28TC/28SC の前面パネルには、10BASE-T/100BASE-TX/1000BASE-T ポート、SFP(コンボ)スロット、10 ギガ SFP +スロット、コンソールポート(RJ-45/ Mini-USB)、RJ-45 管理ポート、アラームおよび USB ポートが配置されています。また、電源、コンソール、RPS(冗長電源システム)、USB、ファン、 管理、およびオプションモジュール用の SFP ポートを含む各ポートの Link/Act/Speed の状態を表示する LED を搭載しています。「LED 表示」の項で 詳細の動作について説明します。

52TC の前面パネルには、10BASE-T/100BASE-TX/1000BASE-T ポート、SFP コンボスロット、10 ギガ SFP +スロットが配置されています。また、電 源、コンソール、RPS (冗長電源システム)、ファンおよびオプションモジュール用の SFP ポートを含む各ポートの Link/Act/Speed の状態を表示す る LED を搭載しています。「LED 表示」の項で詳細の動作について説明します。

#### DGS-3630-28TC

- 10BASE-T/100BASE-TX/1000BASE-T ポート x 24
- SFP コンボスロットx4
- SFP+スロットx4
- RJ-45 アラームポート x 1
- RJ-45 コンソールポート x 1
- Mini-USB コンソールポート x 1
- RJ-45 管理ポート x 1
- USB ポート x 1
- LED: Power、Console、RPS、USB、Fan Err、MGMT、Link/Act/Speed(各ポート/スロット)
- スタックモジュール番号 LED



図 3-1 DGS-3630-28TC の前面パネル

#### DGS-3630-28SC

- SFP スロット x 24
- 10BASE-T/100BASE-TX/1000BASE-Tコンボポート x4
- SFP+スロットx4
- RJ-45 アラームポート x 1
- RJ-45 コンソールポート x 1
- Mini-USB コンソールポート x 1
- RJ-45 管理ポート x 1
- USB ポート x 1
- LED: Power、Console、RPS、USB、Fan Err、MGMT、Link/Act/Speed(各ポート/スロット)
- スタックモジュール番号 LED



図 3-2 DGS-3630-28SC の前面パネル

#### DGS-3630-28PC

- 10BASE-T/100BASE-TX/1000BASE-Tポート (PoE 給電) x 24
- SFP コンボスロット x 4
- SFP+スロットx4
- RJ-45 アラームポート x 1
- RJ-45 コンソールポート x 1
- Mini-USB コンソールポート x 1
- RJ-45 管理ポート x 1
- USB ポート x 1
- LED: Power、Console、RPS、USB、Fan Err、MGMT、Link/Act/Speed(各ポート/スロット)
- Mode ボタン & LED:PoE、Link/Act
- スタックモジュール番号 LED



図 3-3 DGS-3630-28PC の前面パネル

### DGS-3630-52TC

- 10BASE-T/100BASE-TX/1000BASE-T ポート x 48
- SFP コンボスロット x 4
- SFP+スロットx4
- Power、Console、RPS、Fan Err、Link/Act/Speed (各ポート / スロット)
- スタックモジュール番号 LED

注意 RJ-45 アラームポート、RJ-45/Mini-USB コンソールポート、管理ポート、USB ポートは背面に配置されています。



図 3-4 DGS-3630-52TC の前面パネル

#### DGS-3630-52PC

- 10BASE-T/100BASE-TX/1000BASE-Tポート (PoE 給電) x 48
- SFP コンボスロット x 4
- SFP+スロットx4
- Power、Console、RPS、Fan Err、Link/Act/Speed(各ポート/スロット)
- Mode ボタン & LED: PoE、Link/Act
- スタックモジュール番号 LED

注意 RJ-45 アラームポート、RJ-45/Mini-USB コンソールポート、管理ポート、USB ポートは背面に配置されています。



図 3-5 DGS-3630-52PC の前面パネル

## アラームポート(RJ-45)

外部からの機器をアラームイベントのトリガとして、またはスイッチによって発動されたアラームイベントの受信機として、スイッチのアラームポート(RJ-45)に接続することが可能です。外部機器との接続は RJ45 コネクタのアラームポートを使用します。他の RJ45 接続と同様、4 ペアの銅線が使用され、2 ペアが温度センサなどの入力接続に、もう 2 ペアがスピーカや LED 用の出力接続に使用されます。



図 3-6 アラームコネクタ

#### アラームコネクタポート

コンタクト	アラームコネクタポート		
1	Normal open2(42VAC 50Hz、60VDC、1Amax)		
2	Common2 (42VAC 50Hz、60VDC、1Amax)		
3	Normal open1(42VAC 50Hz、60VDC、1Amax)		
4	Common1 (42VAC 50Hz、60VDC、1Amax)		
5	Din2-(最大入力電圧:3VDC)		
6	Din2+(最大入力電圧:3VDC)		
7	Din1-(最大入力電圧:3VDC)		
8	Din1+(最大入力電圧:3VDC)		

アラーム入力は「pin-pairs」(ピンのペア)で行われ、ペア1(Din1+/Din1-)そしてペア2(Din2+/Din2-)はスイッチの CPU へのアラームシグナ ル送信に使用されます。「Din+」と「Din-」間の回路に短絡が生じるとアラームシグナルは CPU へ送信されます。アラーム出力も「pin-pairs」(ピ ンのペア)で行われ、ペア1(Common1/Normal open1)そしてペア2(Common2/Normal open2)はスイッチの CPU にコントロールされて、アラー ムシグナルを外部機器へ送信します。「Common」と「Normal」間の回路がオープンになると「42VAC/50Hz、60VDC、1A」が送信されます。CPU はイベント発生時にこの回路を短絡することができます。

### LED 表示

LED はスイッチとネットワークの状態を表示します。Power、Console、MGMT など、および各ポートについて LED をサポートします。以下に、スイッ チ上の LED の配置と、各 LED の状態が表す意味を示します。

#### DGS-3630-28TC



🗵 3-7 DGS-3630-28TC の前面パネル LED 配置図

#### DGS-3630-28SC



24F

図 3-8 DGS-3630-28SC の前面パネル LED 配置図

### DGS-3630-28PC



図 3-9 DGS-3630-28PC の前面パネル LED 配置図

#### DGS-3630-52TC



1000M 😑 Link 😤 Act





図 3-10 DGS-3630-52TC の背面パネル LED 配置図(上:前面/下:背面)

#### DGS-3630-52PC







以下の表に LED の状態が意味するスイッチの状態を示します。

LED	色	状態	状態説明	
Mode ボタン& LED(DGS	-3630	)-28PC/52P	このみ)(PoE モード、Link/Act モードへの切り替え)	
PoE	緑	点灯	ポート LED は各ポートの PoE の状態について表示します。	
Link/Act	緑	点灯	ポート LED は各ポートの Link/Act/Speed の状態について表示します。	
システム LED				
Power		点灯	スイッチに電源が供給され正常に動作しています。	
	_	消灯	スイッチに電源が供給されていません。	
MGMT	緑	点灯	管理ポートでリンクが確立されています。	
		点滅	ポートで通信が発生しています。	
	_	消灯	リンクが確立されていない、もしくはインタフェースが管理者によりシャットダウンされています。	
Console	緑	点灯	RJ-45 コンソールポートのリンクが確立しています。	
	橙	点灯	Mini-USB コンソールポートのリンクが確立しています。	
	_	消灯	リンクが確立していません。	
Fan Err	赤	点灯	ファンに不具合が発生しています。	
	_	消灯	ファンは通常通り動作しています。	
RPS	緑	点灯	リダンダント電源ユニットが動作しています。	
	_	消灯	リダンダント電源ユニットは動作していません。	
USB	4 <b>7</b>	点灯	USB メモリが挿入されています。	
	称	点滅	読み / 書きが実行されています。	
	赤	点灯	USB メモリの不具合を検出しました。	
	_	消灯	USB メモリが挿入されていません。	
スタック ID LED		点灯(1-9)	スイッチスタックにおけるスイッチのボックス番号が表示されます。	
		点灯(H)	スイッチがスイッチスタックのプライマリマスタである場合、大文字の「H」の文字が表示されます。	
	緑	点灯(h)	スイッチがスイッチスタックのバックアップマスタの場合は、小文字の「h」が表示されます。	
		点灯(E)	システムによるセルフテストエラーです。	
		点灯(G)	セーフガードエンジンが「exhausted」モードに入っています。	
10/100/1000 ポート LED				
Link/Act/Speed	4 <b>-</b>	点灯	1000Mbps でリンクが確立しています。	
	緑	点滅	1000Mbps でデータを送受信しています。	
	T2.ŕ	点灯	10/100Mbps でリンクが確立しています。	
	位	点滅	10/100Mbps でデータを送受信しています。	
	_	消灯	リンクが確立していません。	
PoE	緑	点灯	接続中の PoE 受電機器に給電中です。	
(DGS-3630-28PC/52PC)	橙	点灯	PoE ポートにエラーが発生しました。	
	_	消灯	給電をしていません。(受電機器が未検出または未接続)	
SFP ポート LED				
Link/ACT	緑	点灯	1000Mbps でリンクが確立しています。	
		点滅	1000Mbps でデータを送受信しています。	
	126	点灯	100Mbps でリンクが確立しています。	
	橙	点滅	100Mbps でデータを送受信しています。	
	_	消灯	リンクが確立していません。	
SFP+ポート LED				
Link/ACT	緑	点灯	10Gbps でリンクが確立しています。	
		点滅	10Gbps でデータを送受信しています。	
		点灯	1000Mbps でリンクが確立しています。	
	橙	点滅	1000Mbps でデータを送受信しています。	
	_	消灯	リンクが確立していません。	

## 背面パネル

## DGS-3630-28TC、28SC、28PC

switck end C	Berger Code retainer	Redundant Power Supply
図 3-12 DGS-3630-28TC、28SC 背面パネル図		
ACLINE Solder Solder Solder	Redundant Power Supply	SWITCH GADE

DGS-3630-28TC、28SC、28PCの背面パネルには、セキュリティスロット、接地コネクタ、電源抜け防止クリップ挿入口(28PC は除く)、AC 電源コネクタ、 オプションの外部リダンダント電源用のコネクタが配備されています。オプションのリダンダント電源ユニット用のアウトレットがあります。内蔵 電源ユニットに異常が発生した場合に外部リダンダント電源ユニット(オプション)が自動的にスイッチに電源を供給します。AC 電源コネクタは標 準の電源ケーブルを接続する三極インレットです。ここに付属の電源ケーブルを接続します。スイッチは自動的に 50/60Hz、100 ~ 240VAC 内の電 圧に調整されます。

#### DGS-3630-52TC、52PC



図 3-15 DGS-3630-52PC 背面パネル図

DGS-3630-52TC、52PC の背面パネルには、セキュリティスロット、接地コネクタ、USB ポート、ステータス LED (USB/MGMT)、MGMT ポート、コンソー ルポート (RJ-45)、コンソールポート (Mini-USB)、ALARM ポート、電源抜け防止クリップ挿入口 (52PC は除く)、AC 電源コネクタ、オプションの 外部リダンダント電源用のコネクタが配備されています。オプションのリダンダント電源ユニット用のアウトレットがあります。内蔵電源ユニット に異常が発生した場合に外部リダンダント電源ユニット (オプション)が自動的にスイッチに電源を供給します。AC 電源コネクタは標準の電源ケー ブルを接続する三極インレットです。ここに付属の電源ケーブルを接続します。スイッチは自動的に 50/60Hz、100 ~ 240VAC 内の電圧に調整され ます。

図 3-13 DGS-3630-28PC 背面パネル図

# 側面パネル

システムのファンと通気口がスイッチにあり内部の熱を放出します。これらをふさがないようにご注意ください。スイッチの適切な通気のためには、 少なくとも4インチ(10 cm)以上のスペースを確保してください。最適な熱放出、空気の循環をしないとシステム障害や部品の激しい損傷を引き 起こす場合がありますのでご注意ください。

### DGS-3630-28TC、28SC



図 3-16 側面パネル図 (DGS-3630-28TC / DGS-3630-28SC)

### DGS-3630-52TC



図 3-17 側面パネル図 (DGS-3630-52TC)

### DGS-3630-28PC、52PC



図 3-18 側面パネル図 (DGS-3630-28PC/DGS-3630-52PC)

# 第2章 スイッチの設置

- パッケージの内容
- ネットワーク接続前の準備
- ゴム足の取り付け(19インチラックに設置しない場合)
- 19インチラックへの取り付け
- SFP/SFP+ポートへのモジュールの取り付け
- 電源抜け防止クリップの装着
- リダンダント電源システムの設置
- 電源の投入

## パッケージの内容

ご購入いただいたスイッチの梱包箱を開け、同梱物を注意して取り出してください。以下のものが同梱されています。

- ・本体 x 1
- AC 電源ケーブル(100V 専用) x 1
- ・ USB/Mini-USB ケーブル x 1
- RJ-45/RS232C コンソールケーブル x 1
- ・19インチラックマウントキット
- マニュアル x 1
- ・ ゴム足 x 4
- CD-ROM x 1
- 電源抜け防止クリップ(DGS-3630-28PC/52PC は除く) x 1
- シリアルラベル x 1
- PLシート x 1

万一、不足しているもの損傷を受けているものがありましたら、ご購入頂いた販売代理店までご連絡ください。

## ネットワーク接続前の準備

スイッチの設置場所が性能に大きな影響を与えます。以下のガイドラインに従って本製品を設置してください。

- スイッチは、しっかりとした水平面で耐荷重性のある場所に設置してください。また、スイッチの上に重いものを置かないでください。
- ・ 本スイッチから 1.82m 以内の電源コンセントを使用してください。
- ・ 電源ケーブルが AC/DC 電源ポートにしっかり差し込まれているか確認してください。
- 本スイッチの周辺で熱の放出と充分な換気ができることを確認してください。換気のためには少なくとも製品の前後10cm以上の空間を保つようにしてください。
- スイッチは動作環境範囲内の温度と湿度を保つことができる、なるべく涼しくて乾燥した場所に設置してください。
- ・ スイッチは強い電磁場が発生するような場所(モータの周囲など)や、振動、ほこり、および直射日光を避けて設置してください。
- スイッチを水平面に設置する際は、スイッチ底面に同梱のゴム足を取り付けてください。ゴム製の足はスイッチのクッションの役割を果たし、筐体自体や他の機器に傷がつくのを防止します。

## ゴム足の取り付け(19インチラックに設置しない場合)

机や棚の上に設置する場合は、まずスイッチに同梱されていたゴム製足をスイッチの裏面の四隅に取り付けます。スイッチの周囲に十分な通気を確 保するようにしてください。



図 2-1 ゴム足の取り付け

## 19 インチラックへの取り付け



前面、側面にスタビライザを取り付けないで製品を設置すると、ラックが転倒し、場合によっては人身事故を引き起こすことがあります。 そのため、ラック内に製品を取り付ける前に必ずスタビライザを取り付けてください。ラックにシステム/コンポーネントを取り付けた後は、一度にスライド・アセンブリに乗せて引き出すコンポーネントは1つだけとしてください。2つ以上のコンポーネントが引き出される と、ラックがバランスを失い、倒れて重大な事故につながる恐れがあります。

注意 スイッチをラックに固定するネジは付属品には含まれません。別途ご用意ください。

- 1. 電源ケーブルおよびケーブル類が本体、拡張モジュールに接続していないことを確認します。
- 2. 付属のネジで、スイッチの両側側面にブラケットを取り付けます。



図 2-2 スイッチへのブラケットの取り付け図

3. 完全にブラケットが固定されていることを確認し、本スイッチを以下の通り標準の19インチラックに固定します。



図 2-3 スイッチのラックへの設置図

## SFP/SFP+ ポートへのモジュールの取り付け

スイッチは SFP と SFP+ ポートを搭載しており、通常の RJ-45 接続をサポートしないスイッチとネットワークを構成することが可能です。 以下に、スイッチに SFP ポートモジュールを挿入した例を図に示します。

注意 コンボポートの SFP ポートモジュール挿入時は 1000BASE-T ポートとしての使用はできません。SFP ポートが優先されます。



図 2-4 DGS-3630 シリーズ前面パネルの SFP ポートへのモジュールの挿入

## 電源抜け防止クリップの装着

アクシデントにより AC 電源コードが抜けてしまうことを防止するために、スイッチに電源抜け防止クリップを装着します。 以下の手順に従って電源抜け防止クリップを装着します。

注意 DGS-3630-28PC/52PC は未サポートです。

1. スイッチの背面の電源プラグの下にある穴に、付属の電源抜け防止クリップのタイラップ(挿し込み先のあるバンド)を下記の図のように差し 込みます。



2. AC 電源コードをスイッチの電源プラグに挿し込みます。



3. 以下の図のように挿し込んだタイラップにリテイナー(固定具)をスライドさせ装着します。



図 2-7 リテイナー(固定具)のスライド

4. 以下の図のようにリテイナーを電源コードに巻き付け、リテイナーのロック部分に挿し込みます。



図 2-8 リテイナーの巻き付け、固定

5. 4. リテイナーを電源コードにしっかりと巻き付けた後、電源コードが抜けないか確かめます。



図 2-9 電源抜け防止クリップの固定確認

## リダンダント電源システムの設置

DGS-3630 シリーズは外付けのリダンダント電源システム (RPS)、DPS-500A (DGS-3630-28SC/28TC/52TC)、DPS-700 (DGS-3630-28PC/52PC) をサポー トしています。DPS-500A、DPS-700 は緊急時に必要な電力を供給するリダンダント電源ユニットです。DPS-500A は DPS-800 に取り付けることが できます。DPS-700 は PoE スイッチに対応しているため、スイッチの PoE 給電可能電力を倍にすることができます。

本スイッチヘリダンダント電源ユニットを接続する手順は以下の通りです。



当古 リダンダント電源ユニットの接続を行う前に、スイッチの AC 電源ケーブルを抜いておいてください。また、はじめに必ず電源ケーブルと コネクタの仕様書および設定手順をご確認ください。

警告 使用する「RPS」を DC 電源ケーブルに接続する前に AC 電源へ接続しないでください。RPS にダメージを与える場合があります。

RPS を設置する場合、スイッチの背後に少なくとも 15cm(6インチ)の空間を設けてください。ケーブルが損傷する場合があります。

### **DPS-500A**

DPS-500AはDGS-3630-28SC/28TC/52TCに対応しています。DPS-500Aのマスタスイッチへの接続は、14ピンのDC電源ケーブルを使用して行います。 標準の三極の AC 電源ケーブルでリダンダント電源装置とメイン電源を接続します。



図 2-10 DGS-3630-28TC/SC と DPS-500A RPS の接続

- 1. 14 ピン DC 電源ケーブルの一端をスイッチのソケットに挿入し、もう一端をリダンダント電源装置に挿入します。
- 標準の AC 電源ケーブルでリダンダント電源装置とメインの AC 電源を接続します。DPS-500A 前面の緑の LED 点灯により、正しく接続が行わ 2. れたことが確認できます。
- 3. スイッチを再び AC 電源に接続します。RPS LED が点灯してリダンダント電源が動作していることを確認できます。
- 本手順の実行による設定変更は必要ありません。 4



本製品に対し DPS-500A 以外のリダンダント電源ユニットに使用しないでください。

注意 さらに詳細な情報については DPS-500A のマニュアルをご参照ください。

### **DPS-700**

DPS-700 は DGS-3630-28PC/52PC に対応しています。DPS-700 は 22 ピンの DC 電源ケーブルを使用したスイッチに接続します。電源にはリダンダント電源同梱の AC 電源ケーブルをご使用ください。



図 2-11 DPS-700 をラックに取り付ける

- 1. 22 ピン DC 電源ケーブルの一端をスイッチのソケットに挿入し、もう一端をリダンダント電源装置に挿入します。
- 2. 標準の AC 電源ケーブルでリダンダント電源装置とメインの AC 電源を接続します。リダンダント電源装置の前面にある緑の LED 点灯により、 正しく接続が行われたことが確認できます。
- 3. スイッチを再び AC 電源に接続します。スイッチの LED が点灯し、リダンダント電源が動作していることを確認できます。 本手順の実行による設定変更は必要ありません。



## DGS-3630-28PC背面

図 2-12 DPS-700 に取り付ける

注意 DGS-3630-28PC/52PC と DPS-700 の接続には 22 ピンの DC 電源ケーブル以外使用しないでください。

### DPS-800

DPS-800 は標準サイズのラックマウント(1U サイズ)シャーシです。2 台までの DPS-500A を収容できます。



図 2-13 DPS-500A を DPS-800 に取り付ける

リダンダント電源システムは標準19インチラックにも取り付けることができます。以下の図を参照してください。



図 2-14 DPS-800 をラックに取り付ける

## 電源の投入

- 1. 電源ケーブルを本スイッチの電源コネクタに接続します。電源ケーブルのプラグを電源コンセントに接続します。
- 2. 本スイッチに電源が供給されると、Power LED が点灯します。システムのリセット中、LED は点滅します。

#### 電源の異常

万一停電などの電源異常が発生する / した場合は、必ず本スイッチの電源プラグを抜いてください。電源が再度供給できる状態になってから電源プラグを再度接続します。

# 第3章 スイッチの接続

- エンドノードと接続する
- ハブまたはスイッチと接続する
- バックボーンまたはサーバと接続する

注意 すべてのポートは Auto MDI/MDI-X 接続をサポートしています。

# エンドノードと接続する

「エンドノード」とは本スイッチと接続するネットワーク機器の一般的な呼称です。パソコン、ノート PC、アクセスポイント、プリントサーバ、 VoIP 電話機などが該当します。各エンドノードは「100/1000/10000Mbps」RJ-45 ネットワークポートを有している必要があります。通常エンドノー ドはスタンダードなツイストペア UTP/STP ネットワークケーブルを使ってスイッチと接続されます。接続が成功すると、対応ポートの LED がポー トでのネットワーク動作に従い点灯 / 点滅します。



図 3-1 エンドノードと接続した図

エンドノードと正しくリンクが確立すると本スイッチの各ポートの Link/Act LED は緑または橙に点灯します。データの送受信中は点滅します。

# ハブまたはスイッチと接続する

使用するケーブルによって以下のように接続します。

- ・ カテゴリ 3 以上の UTP/STP ケーブル: 10BASE-T ハブまたはスイッチと接続する。
- ・ カテゴリ 5 以上の UTP/STP ケーブル: 100BASE-TX ハブまたはスイッチと接続する。
- ・エンハンスドカテゴリ 5e 以上の UTP ケーブル: 1000BASE-T スイッチと接続する。
- ・ 光ファイバケーブル: SFP/SFP+ ポート経由で光ファイバをサポートするスイッチにアップリンクする。



図 3-2 ストレート、クロスケーブルでハブまたはスイッチと接続する図
# バックボーンまたはサーバと接続する

SFP ポートと 1000BASE-T ポートは、ネットワークバックボーンやサーバとのアップリンク接続に適しています。RJ-45 ポートは、全二重モード時に おいて 10/100/1000Mbps の速度を提供し、SFP ポートは、全二重モード時において 100Mbps または 1000Mbps の速度を提供します。

ギガビットイーサネットポートとの接続はポートのタイプによって光ファイバケーブルまたはエンハンスドカテゴリ5ケーブルを使用します。正しくリンクが確立すると Link LED が点灯します。



図 3-3 サーバ、PC、スイッチスタックとのアップリンク接続図

# 第4章 スイッチ管理について

- Web GUI による管理
- SNMP による管理
- CLIによる管理

### Web GUI による管理

Microsoft<sup>®</sup> Internet Explorer などの Web ブラウザによって、本製品の設定をグラフィカルに表示し、管理することができます。 Web GUI の詳細については「第5章 Web ベースのスイッチ管理」を参照してください。

# SNMP による管理

SNMP(Simple Network Management Protocol)は、OSI 参照モデルの第7層(アプリケーション層)のプロトコルです。ネットワークに接続された通信機器の管理や監視を行います。

SNMPの詳細については「SNMP(SNMP設定)」を参照してください。

# CLI による管理

スイッチのモニタリングと設定のために、RJ-45 コンソールポートと MIni-USB コンソールポートを搭載しています。コンソールポートを使用するためには、以下をご用意ください。

- ・ ターミナルソフトを操作する、シリアルポート搭載の端末またはコンピュータ
- RJ-45/RS-232C 変換ケーブル

#### 端末をコンソールポートに接続する

#### ケーブルの接続

- 1. RJ-45/RS-232C 変換ケーブルの RS-232C コネクタを、シリアルポート搭載の端末またはコンピュータに接続します。
- 2. RJ-45/RS-232C 変換ケーブルの RJ-45 コネクタを、本製品のコンソールポートに接続します。

#### ターミナルソフトの設定

- 1. VT100のエミュレーションが可能なターミナルソフトを起動します。
- 2. 適切なシリアルポート (COM 1 など) を選択します。
- ターミナルソフトの設定をスイッチのシリアルポートの設定に合わせます。 スイッチのシリアルポートの設定は以下の通りです。
  - スピード:「115200」
  - ・ データ:「8bit」
  - パリティ:「なし (none)」
  - ・ ストップビット :「1bit」

#### ログインとログアウト

- 1. 本製品と管理 PC をケーブルで接続後、本製品の電源をいれます。
- 2. 管理 PC とスイッチが正しく接続されると、画面に「Press any key to login...」というメッセージが表示されます。 キーボード上のいずれかのキーを押します。
- 3. 設定済みのユーザ名とパスワードがある場合は、設定したユーザ名とパスワードを入力し「Enter」を押します。 初めてログインする場合は、なにも入力せず「Enter」を2回押します。

注意パスワードの大文字と小文字は区別されます。

4. コマンドを入力し、必要な設定を行います。

コマンドの多くは管理者レベルのアクセス権が必要です。 管理者レベルのアカウント作成については「ユーザアカウント / パスワードの設定」を参照してください。 CLIの詳細及びコマンドリストについては、CLI マニュアルを参照してください。

5. ログアウトする場合は、logout コマンド使用するか、ターミナルソフトを終了します。

### 端末を Mini-USB コンソールポートに接続する

Mini-USB コンソールポートの接続には次の条件があります。

- ・ ターミナルをエミュレートできる USB 2.0 ポートのあるターミナル、またはコンピュータ
- ・5ピンミニBオスコネクタ/USB Type Aオスコネクタのコンソールケーブル(付属)。コンソールポートとの物理的な接続に使用されます。
- ターミナルエミュレーションソフトウェアで使用される仮想 COM ポートをエミュレートするソフトウェア

#### Mini-USB コンソールポートとコンピュータの接続

- 1. コンピュータの仮想 COM ポートをエミュレートするソフトウェアをインストールします。
- 2. 付属のコンソールケーブルの USB Type A オスコネクタのコンピュータへの接続し、5 ピンミニ B オスコネクタのスイッチのコンソールポート への物理的な接続を行います。



図 4-4 Mini-USB コンソールポートの接続

3. コンピュータの「デバイスマネージャ」でシリアルポート番号を確認します。 仮想 COM ポートの名称は「Prolific USB-to-Serial Comm Port」です。



⊠ 4-5 Device Manager

- 4. ターミナルエミュレーションソフトを次のように設定します。
  - ・ シリアルポート(COM1 または 2)を選択
  - ・「115200」ビット / 秒にデータ速度を設定
- ・「データビット」は「8」、「ストップビット」は「1」、「パリティ」は「なし」に設定
- ・「フロー制御」は「なし」に設定

コンソールに接続すると、コンソール画面が表示されます。画面上でコマンドを入力し、管理機能を実行します。

## ユーザアカウント / パスワードの設定

管理者レベルのユーザアカウントとパスワードを設定する方法について説明します。



工場出荷時のユーザアカウントおよびパスワードは「admin」、権限レベルは「15」です。 はじめてログインした際は、本スイッチに対する不正アクセスを防ぐために、ユーザ名に対して必ず新しいパスワードを設定してください。 このパスワードは忘れないように記録しておいてください。

Switch> enable
Switch# configure terminal
Switch(config)# username Administrator password 12345
Switch(config)# username Administrator privilege 15
Switch(config)# line console
Switch(config-line)# login local
Switch(config-line)#

- 1. 「enable」コマンドを入力し、Privileged EXEC モードにアクセスします。
- 2. 「configure terminal」コマンドを入力し、Global Configuration モードにアクセスします。
- 3. 「username Administrator password 12345」コマンドを入力し、ユーザ名「Administrator」、パスワード「12345」を指定します。
- 4. 「username Administrator privilege 15」コマンドを入力し、ユーザアカウントに権限レベル 15 を指定します。 権限レベルは 1 から 15 まで指定できます。「15」が最大、「1」が最小の権限レベルです。
- 5. 「line console」コマンドを入力し、LINE Configuration モードにアクセスします。
- 6. 管理インタフェースにアクセス可能なユーザアカウントが作成されました。コマンドは「login local」です。
- 注意 パスワードの大文字と小文字は区別されます。 ユーザ名とパスワードは 15 文字以内の半角英数字で指定してください。
- 注意 CLIの設定コマンドは実行中の設定ファイルの編集でありスイッチが再起動した場合、設定は保存されません。設定内容変更の安全な保存 については「copy running-config startup-config」コマンドを使用して実行中の設定ファイルをスタート時の設定ファイルとし てコピーする必要があります。

# IP アドレスの割り当て

- CLIを使用してスイッチの IP アドレスを設定する方法について説明します。
- IP アドレスの初期値: 10.90.90.90/8

Switch> enable Switch# configure terminal Switch(config) # interface vlan 1 Switch(config-if)# ip address xxx.xxx.xxx yyy.yyy.yyy Switch(config-if)#

- 1. 「enable」コマンドを入力し、Privileged EXEC モードにアクセスします。
- 2. 「configure terminal」コマンドを入力し、Global Configuration モードになります。
- 「interface vlan 1」コマンドを入力し、デフォルト VLAN の VLAN Configuration モードに入り「VLAN 1」を指定します。 3.
- 「ip address xxx.xxx.xxx.xxx yyy.yyy.yyy」を入力し、IP アドレスを変更します。 4 xxx.xxx.xxx : IPアドレス yyy.yyy.yyy.yyy : IP アドレスに対応するサブネットマスク

## 管理ポートへの接続

スイッチの前面パネルには Out-of-Band (OOB) 管理ポート (MGMT ポート) があります。 ポートは、標準的なイーサネットケーブルを使用してノート PC に簡単に接続可能な RJ-45 ポートです。管理ポートを使ってスイッチに接続するた めに、Web ブラウザもしくは Telnet クライアントを使用することができます。

管理ポートを使用するためには、イーサネットケーブルを使用してスイッチ管理に使用するコンピュータのイーサネットインタフェースにポートを 接続します。IP アドレスの初期値は 192.168.0.1 で、サブネットマスクは 255.255.255.0 です。スイッチ管理に使用するコンピュータが、192.168.0.x サブネットで重複しない IP アドレスを持っていることを確認してください。

コンソールポート、またはWebベースのスイッチ管理インタフェースを通じてIP設定または管理ポートのステータスを変更することができます。

管理ポートの設定を変更するためには、以下のコマンドを使用します。

```
Switch#configure terminal
Switch(config)#interface mgmt 0
Switch(config-if) #ip default-gateway 192.168.0.254
Switch(config-if)#
```

IP 設定のステータスを参照するためには、以下のコマンドを使用します。

```
Switch#show ip interface mgmt 0
mgmt ipif 0 is enabled, Link status is up
IP address is 192.168.0.1/24
Gateway is 0.0.0.0
Switch#
```

注意 管理ポートの MAC アドレスは、「System MAC」を使用するため、「VLAN1」と重複します。

【注意】 VLAN インタフェースを経由して「Mgmt 0」の IP アドレス宛に通信を行うことはできません。

# 第5章 Web ベースのスイッチ管理

- Web ベースの管理について
- Web マネージャへのログイン
- Web マネージャの画面構成
- Web マネージャのメニュー構成

### Web ベースの管理について

本スイッチのすべてのソフトウェア機能は、実装されている Web ベース (HTML) インタフェース経由で管理、設定およびモニタできます。標準的な ブラウザを使用してネットワーク上のリモートステーションから本スイッチを管理できます。ブラウザが普遍的なアクセスツールの役割をし、HTTP プロトコルを使用してスイッチと直接通信することが可能です。

Web ベースの管理モジュールとコンソールプログラム(および Telnet)は、異なるインタフェースを経由して同じスイッチ内部のソフトウェアに アクセスし、その設定を行います。つまり、Web ベースでスイッチ管理を実行して行う設定は、コンソール接続によっても行うことができます。

# Web マネージャへのログイン

スイッチの管理を行うには、はじめにコンピュータでブラウザを起動し、本スイッチに定義した IP アドレスを入力します。ブラウザのアドレスバー に以下のように URL を入力します。例: http://10.90.90.90 (10.90.90.00 はスイッチの IP アドレス。)



注意

工場出荷時設定では IP アドレス「10.90.90.90」、サブネットマスク「255.0.0.0」が設定されています。端末側の IP インタフェースを本スイッチにあわせるか、本スイッチを端末側の IP インタフェースにあわせてください。

以下のユーザ認証画面が表示されます。



図 5-2 パスワード入力用画面

「ユーザー名」欄と「パスワード」欄を空白のまま「OK」をクリックし、Web ベースユーザインタフェースに接続します。Web ブラウザによって 使用可能な機能を以下で説明します。

CLIでユーザ名、パスワードを既に設定している場合は、設定したパラメータを入力します。



# Web マネージャの画面構成

Web マネージャによるスイッチの設定または管理画面にアクセス、およびパフォーマンス状況やシステム状態をグラフィック表示で参照できます。

## Web マネージャのメイン画面について

Web マネージャのメイン画面は3つのエリアで構成されています。



図 5-3 Web マネージャのメインページ

エリア	機能
エリア①	本エリアではスイッチの前面パネルの状態がほぼリアルタイムにグラフィカル表示されます。スイッチのポート、拡張モジュー
	ルが表示されます。また、指定モードでのボートの動作も表示されます。ボートモニタなどの管理機能はここからアクセスする
	事も可能です。「D-Link」ロゴをクリックすると D-Link Web サイト(英語)へ移動します。
エリア②	「Save」メニュー / 「Tools」メニューにアクセスするツールバーです。
エリア③	設定項目のメニューツリーを表示します。表示するフォルダ、またはウインドウを選択します。フォルダを開きハイパーリンク
	のウィンドウをクリック、サブフォルダには上位フォルダに関連するカテゴリの詳細情報や設定項目が表示されます。
エリア④	選択したスイッチ情報の表示と設定を行うことができます。

注意「ASCII」文字のみサポートします。

注意 Web UI を表示する最適の解像度は「1280 x 1024」ピクセルです。

# Web マネージャのメニュー構成

Webマネージャで本スイッチに接続し、ログイン画面でユーザ名とパスワードを入力して本スイッチの管理モードにアクセスします。 Webマネージャで設定可能な機能を次に説明します。

メインメニュー	サブメニュー	説明
System	Device Information(デバイス情報)	スイッチの主な設定情報を表示します。
	System Information Settings (システム情報設定)	スイッチの基本情報を表示します。
	Peripheral Settings (周辺機器設定)	システムの警告温度や環境トラップの設定を行います。
	Port Configuration (ポート設定)	スイッチポートの詳細設定などを行います。
	Interface Description (インタフェース概要)	スイッチの各ポートの概要、管理ステータスなどについて表示します。
	Loopback Test $(\mu - \mathcal{T} / \mathcal{T} / \mathcal{T} / \mathcal{T})$	物理ポートインタフェースのループバック設定とループバックテストを行います。
	PoE (PoE の管理) (DGS-3630-28PC/52PC)	DGS-3630-28PC/52PCのPoE 機能について設定を行います。
	Svstem Log(システムログ構成)	スイッチのフラッシュメモリにスイッチログを保存する方法を選択します。
	Time and SNTP(時刻設定)	スイッチに時刻を設定します。
	Time Range(タイムレンジ設定)	スイッチのタイムレンジを設定します。アクセスプロファイル機能を実行する期間を 決定します
	PTP(PTP 設定)	PTP(Precision Time Protocol : 高精度時刻同期方式)システムは、イーサネットネット ワークを通して時刻を同期します。
	USB Console Settings (USB コンソール設定)	USB コンソールの設定、表示を行います。
	SRM (Switch Resource Management 設定)	「Switch Resource Management」(SRM)により大規模なリソースを最適化します。
Management	Command Logging(コマンドログ設定)	コマンドログ設定を有効にします。コマンドログ出力機能は、コマンドラインインタフェー スを通じてスイッチへの設定が成功したコマンドをログに出力するために使用されます。
	User Accounts Settings (ユーザアカウント設定)	スイッチはユーザ権限の制御を行うことができます。ユーザパスワードとアクセス権 限を含むユーザアカウントを設定します。
	CLI Alias Settings(CLI エイリアス設定)	CLI エイリアスの設定を行います。
	Password Encryption (パスワード暗号化)	パスワードを暗号化し設定ファイルに保存します。
	Password Recovery (パスワードリカバリ)	パスワードリカバリを行います。例えば管理者がパスワードを忘れた場合に有効です。
	Login Method(ログイン方法)	各管理インタフェースでのログイン方法について設定します。
	SNMP(SNMP 設定)	SNMP 設定を有効にします。本スイッチシリーズは、SNMP v1、v2c、および v3 をサポートしています。
	RMON (RMON 設定)	SNMP 機能に対するリモートモニタリング (RMON) ステータスを有効にします。
	Telnet/Web(Telnet/Web 設定)	スイッチに Telnet/Web 設定を有効にします。
	Session Timeout	各セッション(Web やコンソールなど)のタイムアウトの設定をします。
	(セッションタイムアウト)	
	DHCP(DHCP 設定)	スイッチの DHCP について設定します。
	DHCP Auto Configuration (DHCP 自動コンフィグ設定)	DHCP 自動コンフィグ機能の設定を行います。
	DHCP Auto Image Settings (DHCP 自動イメージ設定)	DHCP 自動イメージ設定を行います。スタートアップ時に、外部サーバからイメージファ イルを取得する機能です。
	DNS(ドメインネームシステム)	DNS(Domain Name System)は、ドメイン名と IP アドレスの関連付けをコンピュー タ間の通信で行います。
	NTP(ネットワークタイムプロトコル)	スイッチの時刻を同期するための NTP プロトコルの設定を行います。
	IP Source Interface (IP ソースインタフェース)	IP ソースインタフェースの設定を行います。
	File System(ファイルシステム設定)	フラッシュファイルシステムにより、Firmware、Config 情報、および Syslog 情報はフ ラッシュ内のファイルに保存されます。
	Stacking (スタッキング設定)	物理スタッキングの設定を行います。
	Virtual Stacking(SIM) (仮想スタック設定(SIM))	仮想(SIM)スタッキングの設定を行います。
	D-Link Discovery Protocol (D-Link ディスカバリプロトコル)	D-Link ディスカバリプロトコル(DDP)の設定を行います。
	SMTP Settings(SMTP 設定)	Simple Mail Transfer Protocol (SMTP) の設定を行います。
	Reboot Schedule Settings (再起動スケジュール設定)	スイッチの再起動スケジュール設定を行います。
	NLB FDB Settings(NLB FDB 設定)	ネットワークロードバランシング (NLB) の設定を行います。
	SD Card Management(SD カード管理)	USB ドライバストレージなどのリムーバブル機器の設定を行います。

PDB (FOR Static)         FDB (Forwarding DataStel) - 4/2 - ディングデータベースの設定を行います。           VIAN Truncel (MAN E)2:         0010 276 - 27 - 27 AAN 0555 EFON ENT.           VIAN Truncel (MAN E)2:         0010 276 - 27 - 27 AAN 0555 EFON ENT.           STP (2.75 - 27 )1 - 355 (S SDD2)         C/5 - 27 - 27 - 27 - 27 - 27 - 27 - 27 - 2	メインメニュー	サブメニュー	説明
WAN (MAN BZE)         80710 2 をすっく 2 MAN 600 法を行います。           WAN (MAN BZE)         80710 2 をすっく 2 MAN 600 法を行います。           STP (スパニングソリー型E)         82710 2 MAN 5 MAN 5 2 MAN 5 M	L2 Features	FDB (FDB 設定)	FDB(Forwarding DataBase)フォワーディングデータベースの設定を行います。
VLAN Turnel (WAN トンネル)         90210 VLAN トンネルの認定を行います。           STP (スパニングツリー設定)         スパニングリレフロト Dit OF MB 建築作います。 5つのバージョンの5 Fig.           STP (スパニングツリー設定)         スパニングリレフロト Dit OF MB 建築作います。 5つのバージョンの5 Fig.           FR95 (GB83)         Ethernet flog Potection Subcriting (FR95)の要求。 #江を行います。           Loopback Detection (レーンパンクが自由クション2020)         BP 514イ・サネットリングのボートランキング機能の設定を行います。           Loopback Detection (レーンパンクが建築使用)         Din Aggregation (L ーンパンク 建築加速度)           NMAG         MAG (Multi-Chassis Unit Aggregation Goup) の設定を行います。           Liver To Loup A U ンクア (L イヤス ス) Loup A U ンクス         Z レックス U ンクス Z 地クス U ン Z 地クス U ンクス Z 地クス U ンク Z 地クス U ンクス Z 地クス U ンク Z 地クス U ン Z 地クス U ン Z 地クス U ン Z 地 U A U N U N W U U Z マ ル T キャ X レ U ン U U X N U U X U U X U U X U U X U U X U U X U U X U U X U U X U U X V U X E U X U X U X U X U X U X U X U X U		VLAN(VLAN 設定)	802.1Q スタティック VLAN の設定を行います。
STP (スパニングツリー部定)         スパニングツリープにトロル (STP) 認定者(Styles), 5 つの(ビーンのの) StP) をyポート LS(Vます。           CPS (58922)         Chemral Rig Potection Switching (LPS) のかぶ, 5 ながらります。 LS(Vます。           (イージネットリングプロテクション鍵定)         LD(Var) (Styles)           (レーブパック機能の)         LD(Var) (Styles)           (レーブパック機能の)         LD(Var) (Styles)           (レーブパック機能の)         LD(Var) (Styles)           (レーブパック機能の)         LD(Var) (Styles)           (LA) (Styles)         LD(Var) (Styles)           <		VLAN Tunnel(VLAN トンネル)	802.1Q VLAN トンネルの設定を行います。
FRIST (CR30)         Fheme Ring Protection Switching (FRIS) の表示、型を客行います。 (アージネットリッグプロテクション設定)         Energ Kid ージネットリッグで加入スイッデンの実践構成(1) (LG003)です。 (レージパック税30 (LG0) 機能の設定を行います。 (リンクアグリゾーション)           Unk Aggregation (LUxAggregation (LUンクアグリグーション/ボートトランキング撮影)の設定を行います。 (リンクアグリゾーション)         Unk Aggregation (LUンクアグリグーション/ボートトランキング撮影)の設定を行います。 (リンクアグリゾーション)           MLAG         MLAG (Multi Chassis Link Aggregation Group) の設定を行います。 (リンクアグリゾーション)         Environment (LUイヤ2 プロトコルトンネル)         Distact Filter (LUTY2 (LUTY2 ) (LUイヤ2 プロトコルトンネル)           12 Protocol Turnel (LUイヤ2 プロトコルトンネル)         E2 Protocol Turnel (LUイヤ2 プロトコルトンネル)         E2 Protocol Turnel (LUイヤ2 プロトコルトンネル)         Distact Filter (LUTY2 ) (LUTY2 + AL>12 N - LUTN)           13 Peatures         APP (Addess Feak (LUT2))         Multicast Control (LU マインジス+AL>12 N - LUTN)         Multicast Control (LU マインジス+AL>12 N - LUTN)           13 Peatures         APP (Addess Feak (LUT2))         E2 Protocol Turnel (LU マインジス+AL>12 N - LUTN)         E2 Protocol Turnel (LU マインジス+AL>12 N - LUTN)           13 Peatures         APP (Addess Feak (LUT2))         E2 Protocol Turnel (LU マインジス+AL>12 N - LUTN)         E2 Protocol Turnel (LUTN)         E2 Protocol Turnel (LU マインジス+AL>12 N - LUTN)           13 Peatures         APP (Addess Feak (LUT2))         PA - Aly Z - SAW Feat (LUTR2))         E2 Protocol Turnel (LU Y 2) Z - Z - Z - Z - Z - Z - Z - Z - Z - Z		STP(スパニングツリー設定)	スパニングツリープロトコル(STP)設定を行います。3 つのバージョンの STP (8802.1D-1998 STP、802.1D-2004 Rapid STP、および 802.1Q-2005 MSTP)をサポート しています。
Loopback Detection         ルーブパック検知 (LBD) 機能の設定を行います。           (ルーブパック検知認知)         Link Aggregation (Dンクアグリゲーション/ボートトランキング機能)の設定を行います。           Link Aggregation (Dンクアグリゲーション/ボートトランキング機能)の設定を行います。         MLAG           MLAG         MLAG (Multi-Chassis Link Aggregation Group) の設定を行います。           Li2 Protocol Tunnel (レイヤップロトコルトンネル)         D2 Protocol Tunnel (レイヤップロトコルトンネル)           L2 Protocol Tunnel (L-イヤップロトコルトンネル)         D2 Protocol Tunnel (L-イヤップロトコルトンネル)           L2 Protocol Tunnel (L-イヤップロトコルトンネル)         D2 Protocol Tunnel (L-イヤップロトンネル)           L2 Protocol Tunnel (L-イヤップロトンネル)         Protocol Tunnel (L-イヤップロトンネル)           L2 Pro		ERPS (G.8032) (イーサネットリングプロテクション設定)	Ethernet Ring Protection Switching (ERPS) の表示、設定を行います。 ERPS はイーサネットリング保護スイッチングの業界標準 (ITU-T G.8032) です。
Link Aggregation         Link Aggregation (リンクアグリゲーション/ボートトランキング機能)の設定を行います。           MLAC         MLAG (Multi-Chassis Link Aggregation Croup)の設定を行います。           Filex Links (フレックスリンクス)         フレックスリンクス機能の数定を行います。           L2 Protocol Turnel         L2 Protocol Turnel           L2 Protocol Turnel         L2 Protocol Turnel           L2 Protocol Turnel         L2 Protocol Turnel           L2 Protocol Turnel         L2 Protocol Turnel (レイヤ2 プロトコルトンネル)の設定を行います。           L3 Features         APP (Address Resolution Protocol) & In PT-LXを制能力をTU-LX 変速ム・P           Filex Links (Croutious APP 安定)         Prof Artiggz を行います。           Control (L0 P の意力を受けた)         APP (Address Resolution Protocol) & In PT-LX abs TU-LX 変速ム・P           Filex Links (Croutious APP 安定         Prof Artiggz を行います。           IDP Holper (IDP ヘルレイー)         Prof X-1(安定を行います。           Prof Neighbor (IPV 4-1/ Ggz を行います。         Prof Artiggz を行います。           IDP Holper (IDP ヘルレイー)         PreSiz/TL-JMOG2を行います。           IDP Holper (IDP ヘルレイー)         PreSiz/TL-JMOG2を行います。           IDP Holper (IDP ヘルレイー)         PreSiz/TL-JMOG2を行います。           IDP Holper (IDP ヘルレートラーブル)         Prof Artiggz を行います。           IDP Holper (IDP ヘルレートラーブル)         Prof Artiggz を行います。           IDP A Static Route BTD         IDP A スタティックルート FDD (BidDectinal Forwarding Devection) の設定を行います。		Loopback Detection (ループバック検知設定)	ループバック検知(LBD)機能の設定を行います。
MAG         MAG (Multi Chassi Link Aggregation Group) の設定を行います。           Hex Links (フレックスリンクス)         フレックスリンクス構成の設定を行います。           LD Protocol Tunnel (レイヤ2 プロトコルトンネル)         LD Protocol Tunnel (レイヤ2 プロトコルトンネル)           LD Multicast Control (L2 マルチキャストコントロール)         GMP (Internet Group Management Protocol Suppling 機能を始めとした L2 Multicast Control (L2 マルチキャストコントロール)           IDP         Unkl ager Discovery Protocol TunDP (DADEを行います。)           IIDP         Unkl ager Discovery Protocol TunDP (DADEを行います。)           Gratuitous ARP (Gratuitous ARP 2002)         NP FLスと MAC 7F L/L2を対応させます。           Gratuitous ARP (Gratuitous ARP 2002)         PO 6 ネイン (認定) Prof Neighbor (PV6 ネイン(認定)           UPP Heiger (UDP へル/(ー))         PEは安子 L2 Tab TunDo認定を行います。)           PA 5 Static Default Route         # スイッ 5 (L2 PT L2 Advast Discovery Du- F + レンズ Discovery Du- F + Discovery D		Link Aggregation (リンクアグリゲーション)	Link Aggregation (リンクアグリゲーション / ポートトランキング機能) の設定を行います。
Flex Links (フレックスリンクス)         フレックスリンクス細胞の設定を行います。           L2 Protocol Tunnel         L2 Protocol Tunnel         L/ イヤ2 プロトコルトンネル)           L2 Protocol Tunnel         L/ Protocol Tunnel         L/ イヤ2 プロトコルトンネル)           L3 Features         Multicast Control         LGMP (Internet Group Management Protocol) Snooping 機能を始めとした12           L1 DP         Multicast Control         LD (MP (Internet Group Management Protocol) AL (PT FL/スを観躍的な アドレスに変換し、P           L3 Features         ANP (ARP 設定)         Multicast Control         LD (LD P) の設定を行います。           L3 Features         ANP (ARP 設定)         Pri K / Xz MC / FL/ Xz & Ath / Xz MC / L/ Xz / Xz MC / L/ Xz & Ath / Xz / Xz / Yz / Xz / Xz / Xz / Xz / Xz		MLAG	MLAG(Multi-Chassis Link Aggregation Group)の設定を行います。
L2 Protocol Tunnel         L3 Pr		Flex Links(フレックスリンクス)	フレックスリンクス機能の設定を行います。
L2 Multicast Control (L2 ペルチキャストコントロール)         IGMP (Internet Group Management Protocol) Snooping 鍵能を始めとした L2 (L2 ペルチキャストコントロール)           L1DP         LinkLayer Discovery Protocol (L1DP) の設定を行います。           L3 Features         APP (Address Resolution Protocol) は、 P アドレスを物理的な アドレスに変換し、 P アドレスタメ MAC アドレスタガ応させます。           Gratultous ARP (Gratultous ARP 設定)         Park LAyex Discovery Protocol (L1DP) の設定を行います。           Interface (インタフェース設定)         IPP インクフェース設定を行います。           Interface (インタフェース設定)         IP インクフェース設定を行います。           Interface (インタフェース設定)         IP インクフェース設定を行います。           Interface (インタフェース設定)         IP インクフェース設定を行います。           IDP Helper (UDP ヘルパー)         IP 超拡プロトコルの設定を行います。           Interface (インタフェース設定)         IP インクフェース設定を行います。           IDP Helper (UDP ヘルパー)         IP 超拡プロトコルの設定を行います。           IDP Advまれたの設定を行います。         IP インタウェース設定を行います。           IDP Adva アイデンタクルート BFD)         IP インタフェース設定を行います。           IP Adva Static Default Route         IP Adva SF イックルート BFD)           IP Adva Static Route BFD         IP IN スティックガーン BFD (Bidirectional Forwarding Detection) の設定を行います。           IP Adva SF イックガルート BFD)         IP Adva SF イックガルート BFD           IP Adva SF イックガルート BFD         IP Adva SF イックガルート BFD (Bidirectional Forwarding Detection) の設定を行います。           IP Adva SF イックガルート BFD)         IP Adva SF イックガルート BFD           IP Adva SF イッ		L2 Protocol Tunnel (レイヤ 2 プロトコルトンネル)	L2 Protocol Tunnel(レイヤ 2 プロトコルトンネル)の設定を行います。
LDP         Link Layer Discovery Protocol (LDP) の設定を行います。           L3 Features         ARP (ARP 設定)         ARP (Address Resolution Protocol) (は、P) アドレスを物感りなアドレスに変換し、P) アドレスと MAC アドレスを対応させます。           Gratultous ARP (Gratultous ARP 設定)         Gratultous ARP として知られている ARP 通知は、TAP と SPA が等しい場合、それを送信 したれた人に物かざあら SHA と SPA を含むパケット (通常 ARP リクエスト)です           IPv6 Neighbor (IPv6 ネイバ設定)         Pv6 ネイバ設定を行います。           Interface (インタフェース設定)         P インタフェース設定を行います。           IDP Helper (UDP へルパペ)         P 粘気ブロトコルの設定を行います。           IDP A Static Default Route         レスイッチに PAY アドレンシグのためにスタティックルーティング機能をサポートして (IPv4 スタティック/ドフォルトルート設定)           IPv4 Static Default Route         レスイッチ(レスを指定します。)           IPv4 Static Route BFD         IPv4 インタティックルート BFD           IPv4 Static Route BFD         IPv4 スタティックルート P FD           IPv4 Static Route BFD         IPv4 スタティックルート BFD           IPv6 Static Route BFD         IPv6 アビスのスタティックエント US Pr0 Mielを構成することできます。           IPv6 Static Route BFD         IPv6 アビスのスタティックエント VIG IPv6 Right Row FU スズ ペンチャラルート マクライングデーブルは入力ます。           IPv6 Static Route BFD         IPv6 アレスのスタティックエント VIG IPv6 Right Row FU スズ ペンチャラルー マクジテーブルは入力します。           IPv6 Static Route BFD         IPv6 スタティックルート BFD (Bidirectional Forwarding Detection) の設定を行います。           IPv6 Route Table (IPv6 ルートテーブル)         IPv6 TeuzaStatic ま、小さい商用 Ty マスの設定を行います。           IPv6 Route Table (IPv6 ルートテーブル)         IPv6 Route Table		L2 Multicast Control (L2 マルチキャストコントロール)	IGMP(Internet Group Management Protocol)Snooping 機能を始めとした L2 Multicast Control(L2 マルチキャストコントロール)の設定を行います。
IS Features         ARP (Address Resolution Protocol) は、ウアドレスを物理的なアドレス定変換し、IP アドレスを加えてどスすがさせます。           Gratuitous ARP 設定)         Gratuitous ARP 設定)           Gratuitous ARP (Gratuitous ARP 設定)         FVレスを対応させます。           Interface (インタフェース設定)         IP インタフェース設定を行います。           Interface (インタフェース設定)         IP インタフェース設定を行います。           UDP Helper (UDP へ)レバー)         P 転送プロトコルの設定を行います。           IDP Helper (UDP へ)レバー)         P 転送プロトコルの設定を行います。           IPv4 Static/Default Route         本スイッチは IPv4 アドレンングのためにスタティックルーティング機能をサポートして (IPv4 スタティック/レート BFD)           IPv4 Static/Default Route         Pv4 スクティックルート BFD (Bidirectional Forwarding Detection) の設定を行います。           IPv4 Static/Default Route         Pv4 スクティックルート BFD (Bidirectional Forwarding Detection) の設定を行います。           IPv4 Static/Default Route         Pv4 スクティックルート BFD (Bidirectional Forwarding Detection) の設定を行います。           IPv6 Static/Default Route         Pv6 アレラングラーブルになスクティックエント U IPv6 形式のアドレスで本スイッチのルーティーグ (IPv6 スタティック/ルート BFD)           IPv6 Static/Default Route         Pv6 アングラーブルを設定します。           IPv6 Static/Default Route         Pv6 アングラーブルレートレートーデーブル)           IPv6 Static/Default Route         Pv6 アングラーブーンを表定します。           IPv6 Static/Default Route         Pv6 アングラーブルを設定します。           IPv6 Static/Default Route         Pv6 アングラーブルを表示して、FI/Sシンジグアルコリンスを設定します。           IPv6 Static/Default Route         Pv6 アングラーブル		LLDP	Link Layer Discovery Protocol(LLDP)の設定を行います。
Gratuitous ARP 設定)         Gratuitous ARP 設定)         Gratuitous ARP 設定)         Gratuitous ARP 設定)         FA ために したホストに有効である SHA と SPA を含むパケット (通常 ARP リクユスト)です           INFeface (インタフェース設定)         PF やるイパ設定を行います。         PF やるスパ気定を行います。         PF のたろパ気定を行います。           IDP Helper (UDP へ)レパー)         P 転送 つトコルの設定を行います。         PF もとスイブロパケット の転送を有効にします。また UDP プロードキャストパケットを転送するターゲットア ドレスを指定します。           IPv4 Static/Default Route         キスペッチは IPv4 アビシングのためにスタティックルートモントリを作成することできます。           IPv4 Static/Default Route         キスペッテレート BFD (Bidirectional Forwarding Detection)の設定を行います。           IPv4 Static Route BFD         PV4 スタティックパート FF D)           IPv4 Static/Default Route         PV エティングデーブルはスイッテに関するすべての外部経路情報を保存します。ここ ではスイッデにおかちずての外部経路情報を感見とます。           IPv6 Static/Default Route         Pv6 アビンスのスタティックパントリは IPv6 形式のアドレスで本スイッチのルーティ           IPv6 Static/Default Route         Pv6 アビンスのスタティックパントリは IPv6 形式のアドレスで本スイッチのルーティ           IPv6 Static/Default Route         Pv6 スタティックパート BFD)           IPv6 Static/Default Route         Pv6 スタティックパート BFD           IPv6 Static/Default Route         Pv6 スタティックパート BFD           IPv6 Static/Default Route         Pv6 スタティックパート APV アンシンドレス           IPv6 Static/Default Route         Pv6 スタティックパート APV アンプレード           IPv6 Static/Default Route         Pv6 スタティックパート           IPv6 Static/Default Route         Pv6 スタティックパート           IPv6 Static	L3 Features	ARP(ARP 設定)	ARP(Address Resolution Protocol)は、IP アドレスを物理的なアドレスに変換し、IP アドレスと MAC アドレスを対応させます。
IPv6 NetGabor (IPv6 ネイ/設定)         IPv6 ネイ/設定を行います。           Interface (インタフェース設定)         IP インタフェース設定を行います。           UDP Helper (UDP へルパー)         P 転送プロトコルの設定を行います。また UDP プロードキャストパケットを転送するターゲットア ドレスを指定します。また UDP プロードキャストパケットを転送するターゲットア ドレスを指定します。           IPv4 Static/Default Route         キスイッチは IPv4 アドレシングのためにスタティックルーティング機能をサポートして (IPv4 スタティック/アフォルトルート設定)           IPv4 Static/Default Route         キスイッチは IPv4 アドレシングのためにスタティックルートエントリを作成することできます。           IPv4 Static/Default Route         IPv4 Fu2 スタティックルートエントリント           IPv4 Route Table (IPv4 ルートテーブル)         IPv1 アングテーブルはスイッチに関するすべての外部経路情報を保存します。ここ ではスイッチにおけるすべての外部経路情報を保存します。ここ ではスイッチャングテーブルはスクッチィックルート           IPv6 Static/Default Route         IPv6 アレクレート Mor アレスのスタティックルーントンドレスで本スイッチのルーティ (IPv6 スタティック/アラォルトルート設定)           IPv6 Static/Default Route         IPv6 アイングラーブルを表示します。           IPv6 Static/Default Route         IPv6 アレクレート           IPv6 ASタティック/ デフォルレートレード         IPv6 アレクレート           IPv6 Static Route BFD         IPv6 スタティックルート BFD           IPv6 Asper マックルート BFD         IPv6 スタティックルート BFD           IPv6 Asper マックルート BFD         IPv6 スタティックルート BFD           IPv6 Koute Table (IPv6 ルートテージブル)         IPv6 ルーティングラーブルを表示します。           IPv6 Koute Table (IPv6 ルートテージ)         IPv6 Not アイングラーン IPvを引きます。           IPv6 Koute BFD         IPv6 スターン         IPv6 スターン           IPv6 Koute BFD         IPv6 スターン         <		Gratuitous ARP(Gratuitous ARP 設定)	Gratuitous ARP として知られている ARP 通知は、TAP と SPA が等しい場合、それを送信 したホストに有効である SHA と SPA を含むパケット (通常 ARP リクエスト)です
Interface         (インタフェース設定)         PT インタフェース設定を行います。           UDP Helper         (UDP へルバー)         PT 電送プロトコルの設定を行います。         PT キャストック・シャア ドレスを指定します。           IPv4 Static/Default Route         本スイッサイドレタアドレンングのためにスタティックルーテェンク爆能をサポートして           (IPv4 Static/Default Route         ホスイッサイドレタアドレンングのためにスタティックルーテェンク爆能をサポートして           (IPv4 Static Route BFD         IPv4 Static Route BFD         IPv4 Static Route BFD           IPv4 Route Table         IPv4 スタティックルート BFD         IPv4 Ag ティックルート BFD           IPv4 Route Table         IPv4 Nute Table (IPv4 ルートテープルレ         PP レーティングテーブルはスイッチに関するすべての外部経路情報を保存します。ここではスイッチに応するすべての外部経路情報を保存します。ここではスイッチにあけるすべての外部経路情報を保存します。ここではスイッチにしかうタティックルート BFD           IPv6 Static Route BFD         IPv6 スタティックルート BFD         IPv6 Ag ティックルート BFD           IPv6 Static Route BFD         IPv6 スタティックルート BFD         IPv6 スタティックルート BFD           IPv6 Static Route BFD         IPv6 Ag ティックルート BFD (Bidirectional Forwarding Detection) の設定を行います。           IPv6 Static Route BFD         IPv6 Au ーティングテーブルを表示します。           IPv6 Static Route BFD         IPv6 Au ーティングテーンリート BFD (Bidirectional Forwarding Detection) の設定を行います。		IPv6 Neighbor(IPv6 ネイバ設定)	IPv6 ネイバ設定を行います。
UDP Helper         IUDP (UDP へ)レパー)         P 転送プロトコルの設定を行います。また UDP プロードキャストパケットを転送するターゲットア の転送を有効にします。また UDP プロードキャストパケットを転送するターゲットア ドレスを指定します。           IPv4 Static /Default Route         本スイッチは IPv4 アレシングのためにスタティックルーティング機能をサポートして (IPv4 スタティック/レートBED)         IPv4 Static /Default Route BED (IPv4 Static Route BED           IPv4 Static Route BED         IPv4 スタティックルート BFD)         IPv4 スタティックルート BFD)           IPv4 Static Route BED         IPv4 スタティックルート BFD)         IPv4 スタティックルート PFD)           IPv4 Static Route BED         IPv4 スタティックルート BFD)         IPv6 スタティックルート PFD)           IPv4 Static Route BED         IPv4 スタティックルート DFD)         IPv6 スタティックルート DFD)           IPv6 Static Route BED         IPv6 スタティックルート BFD)         IPv6 アドレスのスタティックエントリは IPv6 Pitz(スワティングアーブ)レートスマグラーブルに入力します。           IPv6 Static Route BFD         IPv6 スタティックルート BFD (Bidirectional Forwarding Detection) の設定を行います。           (IPv6 Static Route BFD         IPv6 スタティックルート BFD (Bidirectional Forwarding Detection) の設定を行います。           (IPv6 General Prefix         IPv6 パート優先度を設定)         IPv6 アンプレートロード/バランシングアルロリズムを設定します。           (IPv6 General Prefix         IVLN インタフェース IPv6 汎用プリフィクスの設定を行います。         IPv6 General Prefix           (IPv6 SUPF Static Route Broute Static Route Broute Static Route Broute Static Route Broute Static Route Static Route Broute Static Route Broute Static Static Route Broute Static Route Static Rou		Interface(インタフェース設定)	IP インタフェース設定を行います。
IPv4 Static/Default Route         本スイッチは IPv4 アドレラングのためにスタティックルーティング機能をサポートして (IPv4 スタティック/アフォルトルート設定)           IPv4 Static Route BFD         IPv4 には最大 S12 個のスタティックルート エントリを作成することできます。           IPv4 Route Table (IPv4 ルートテーブル)         IPv1 ティングテーブルはスイッチに関するすべての外部経路情報を保存します。ここ ではスイッチにおけるすべての外部経路情報を保存します。ここ ではスイッチにおけるすべての外部経路情報を保存します。ここ ではスイッチルトルート設定)           IPv6 Static/Default Route         IPv6 アレスのスタティックエントリは IPv6 形式のアドレスで本スイッチのルーティ (IPv6 スタティック/デフォルトルート設定)         IPv6 アレスのスタティックエントリは IPv6 形式のアドレスで本スイッチのルーティ (IPv6 スタティック/デフォルトルート設定)           IPv6 Static Route BFD         IPv6 スタティックルート BFD (Bidirectional Forwarding Detection)の設定を行います。           IPv6 Route Table (IPv6 ルートテーブル)         IPv6 ルートティングテーブルを表示します。           Route Preference (ルート優先度設定)         ルート優先度を設定します。小さい優先度値を持つルートほど高いブライオリティを持ちます。           IPv6 Static Route BFD         IPv6 Static Route BED           IPv6 Route Table (IPv6 がートテーブル)         IPv6 レーティングテーブルを表示します。           Route Preference (ルート優先度設定)         ルート優先度を設定します。小さい優先度値を持つルートほど高いブライオリティを持ちます。           IPv6 General Prefix (IPv6 3規用 プリフィクス)         IP Not パンタフェース IPv6 3規用 プリフィクスの設定を行います。           IP Routing Information Protocol)         RIP Routing Information Protocol)         Ruma Routing and Forwarding I (URPF) の設定を行います。           (IPVA F Rigz)         IP Not スレーティングプロトコルです。         RPPG (Ruting Information Protocol)         RIP Routing Information Protocol)           RIP Routing Information Protocol         RIP Routing Information Protocol)         RIP		UDP Helper(UDP ヘルパー)	IP 転送プロトコルの設定を行います。本機能は指定の UDP サービスタイプのパケット の転送を有効にします。また UDP ブロードキャストパケットを転送するターゲットア ドレスを指定します。
IPv4 Static Route BFD (IPv4 スタティックルート BFD)IPv4 スタティックルート BFD (Bidirectional Forwarding Detection)の設定を行います。IPv4 Route Table (IPv4 ルートテーブル)IP ルーティングテーブルはスイッチに関するすべての外部経路情報を保存します。ここ ではスイッチにおけるすべての外部経路情報を参照します。IPv6 Static/Default Route (IPv6 スタティック/デフォルトルート設定)IPv6 アドレスのスタティックエントリは IPv6 形式のアドレスで本スイッチのルーティ ングテーブルに入力します。IPv6 Static/Default Route (IPv6 スタティック/レート BFD)IPv6 スタティックルート BFD)IPv6 Static Route BFD (IPv6 Route Table (IPv6 ルートテーブル)IPv6 スタティックルート BFD)IPv6 Route Table (IPv6 ルートテーブル)IPv6 ルーティングテーブルを表示します。Route Table (IPv6 ルートテーブル)IPv6 ルーティングテーブルを表示します。Route Table (IPv6 ルートテーブル)IPv6 ルーティングテーブルを表示します。IPv6 General Prefix (IPv6 気用 プリフィクス)VAN インタフェース IPv6 汎用プリフィクスの設定を行います。IPv1 General Prefix (IPv6 気用 プリフィクス)IP トンネルを設定します。IPv1 General Prefix (IPv6 Stitings (IP トンネル設定)IP トンネルを設定します。IPv6 Fourier Stitings (IP トンネル設定)IP トンネルを設定します。IPv7 Fixings (IRPF 設定)IP いたるまをPath Forwarding」(URPF)の設定を行います。(IPv6 Routing Information Protocol)RIP (Routing Information Protocol) によ距離ベクトル型のルーティングプロトコルです。RIPng (Routing Information Protocol)RIP (Routing Information Protocol) によ距離でクトルーティングプロトコルです。RIP (Routing Information Protocol)IP Multicast Routing ProtocolIP マルチキャストルーティングプロトコル)IP Multicast Routing ProtocolIP Routing Information ProtocolIP Multicast Routing ProtocolIP Routing Information Protocol (IP マルチキャストルーティングプロトコル)の設定を行います。RD General ProtocolIP Multicast Routing ProtocolRPF (Soting Super)RP (Routing Information Protocol) (IP マルチャストルーティングプロトコルです。 <tr< td=""><td></td><td>IPv4 Static/Default Route (IPv4 スタティック/デフォルトルート設定)</td><td>本スイッチは IPv4 アドレシングのためにスタティックルーティング機能をサポートして います。IPv4 には最大 512 個のスタティックルートエントリを作成することできます。</td></tr<>		IPv4 Static/Default Route (IPv4 スタティック/デフォルトルート設定)	本スイッチは IPv4 アドレシングのためにスタティックルーティング機能をサポートして います。IPv4 には最大 512 個のスタティックルートエントリを作成することできます。
IPv4 Route Table (IPv4 ルートテーブル)IP ルーティングテーブルはスイッチに関するすべての外部経路情報を保存します。ここではスイッチにおけるすべての外部経路情報を参照します。IPv6 Static/Default RouteIPv6 アレスのスタティックエントリは IPv6 形式のアドレスで本スイッチのルーティ(IPv6 スタティック/デフォルトルート設定)ングテーブルに入力します。IPv6 Static Route BFDIPv6 スタティックルート BFD (Bidirectional Forwarding Detection) の設定を行います。IPv6 Route Table (IPv6 ルートテーブル)IPv6 ルーティングテーブルを表示します。Route Preference (ルート優先度設定)ルート優先度を設定します。小さい優先度値を持つルートほど高いプライオリティを持ちます。ECMP Settings (IECMP 設定) (EI/MI モードのみ)ECMP OSPF 状態と ECMP ルートロードバランシングアルゴリズムを設定します。IPv6 原enal PrefixVLN インタフェース IPv6 汎用プリフィクスの設定を行います。IPv6 原用プリフィクス)IP トンネルを設定します。IP Tunnel Settings (IP トンネル設定)IP トンネルを設定します。IP Kintual Routing and Forwarding)IVitual Routing and Forwarding] (URPF) の設定を行います。IRP (Routing Information Protocol)RIP (Routing Information Protocol) は、距離ベクトル型のルーティングプロトコルです。RIPng (RIPng 設定)IP Routing Information Protocol (kt 距離ベクトル型のルーティングプロトコルです。IP Multicast Routing ProtocolIP Multicast Routing Protocol (IP マルチキャストルーティングプロトコルです。IP Multicast Routing ProtocolIP Multicast Routing Protocol (IP マルチキャストルーティングプロトコル)BGP (Border Gateway Protocol)BGP (Border Gateway Protocol)IE(I/MI モードのみ)BGP (Border Gateway Protocol)BFD (Bidirectional Forwarding Detection)Bidirectional Forwarding DetectionBFD (Bidirectional Forwarding Detection)Bidirectional Forwarding DetectionBFD (Bidirectional Forwarding Detection)Bidirectional Forwarding Detection		IPv4 Static Route BFD (IPv4 スタティックルート BFD)	IPv4 スタティックルート BFD(Bidirectional Forwarding Detection)の設定を行います。
IPv6 Static/Default Route (IPv6 スタティック/デフォルトルート設定)IPv6 アドレスのスタティックエントリは IPv6 形式のアドレスで本スイッチのルーティ ングデーブルに入力します。IPv6 スタティック/デフォルトルート設定)ングデーブルに入力します。IPv6 スタティックルート BFDIPv6 スタティックルート BFDIPv6 スタティックルート BFDIPv6 スタティックルート BFDIPv6 Route Table (IPv6 ルートテーブル)IPv6 ルーティングデーブルを表示します。Route Preference (ノルート優先度設定)ルート優先度を設定します。小さい優先度値を持つルートほど高いプライオリティを持ちます。ECMP Settings (ECMP 設定)IPv6 ルーティングテーブルを表示します。IPv6 General PrefixVLAN インタフェース IPv6 汎用プリフィクスの設定を行います。IPv6 General PrefixVLAN インタフェース IPv6 汎用プリフィクスの設定を行います。IPv6 Static Souting of IP トンネル設定)IP トンネルを設定します。IP Tunnel Settings (IP トンネル設定)IP トンネルを設定します。VRF (Virtual Routing and Forwarding) (E/MI モードのみ)IVitual Routing and Forwarding.) (VRF) の設定を行います。RIP (Routing Information Protocol)RIP (Routing Information Protocol I 体のペースのネットワーク用です。OSPF (OSPF 設定) (EI/MI モードのみ)OSPF を設定します。IP Multicast Routing Protocol (IP マルチキャストルーティングプロトコル)IP Multicast Routing Protocol (IP マルチキャストルーティングプロトコル)BGP (Border Gateway Protocol)BGP (Border Gateway Protocol) をサポートしています。これは AS (自律システム) 内のネットワーク男達性を指定する IP ネットワークまたはプレフィックスのテーブル を保持するレイヤ 3 ユニキャストルーティングプロトコルです。BFD (Bidirectional Forwarding Detection)Bidirectional Forwarding Detection (BFD) の設定を行います。BFD (Bidirectional Forwarding Detection)Bidirectional Forwarding Detection (BFD) の設定を行います。		IPv4 Route Table(IPv4 ルートテーブル)	IP ルーティングテーブルはスイッチに関するすべての外部経路情報を保存します。ここではスイッチにおけるすべての外部経路情報を参照します。
IPv6 Static Route BFD (IPv6 スタティックルート BFD)IPv6 スタティックルート BFD (Bidirectional Forwarding Detection)の設定を行います。 (IPv6 Route Table (IPv6 ルートテーブル)IPv6 Route Table (IPv6 ルートテーブル)IPv6 ルーティングテーブルを表示します。 ルート優先度を設定します。小さい優先度値を持つルートほど高いプライオリティを持ちます。 ECMP Settings (ECMP 設定) ルート優先度を設定します。小さい優先度値を持つルートほど高いプライオリティを持ちます。ECMP Settings (ECMP 設定) (EI/MI モードのみ)ECMP OSPF 状態と ECMP ルートロードパランシングアルゴリズムを設定します。IPv6 General Prefix (IPv6 汎用プリフィクス)VLAN インタフェース IPv6 汎用プリフィクスの設定を行います。IP Tunnel Settings (IP トンネル設定)IP トンネルを設定します。URPF Settings (URPF 設定)IP トンネルを設定します。VRF (Virtual Routing and Forwarding) (E/MI モードのみ)FUritual Routing and Forwarding) (IPv6 ペースのネットワーク用です。RIP (Routing Information Protocol)RIP (Routing Information Protocol) kt, 距離ベクトル型のルーティングプロトコルです。 あり、IPv6 ベースのネットワーク用です。OSPF (OSPF 設定) (EI/MI モードのみ)OSPF を設定します。IP Multicast Routing Protocol (IP マルチキャストルーティングプロトコル)IP Multicast Routing Protocol)BGP (Border Gateway Protocol)BGP (Border Gateway Protocol) をサポートしています。これは AS (自律システム) 内のネットワーク知道性を指定する IP ネットワークまたはプレフィックスのテーブル を保持するレイヤ 3 ユニキャストルーティングプロトコルです。BFD (Bidirectional Forwarding Detection)Bidirectional Forwarding Detection (BFD) の設定を行います。		IPv6 Static/Default Route (IPv6 スタティック / デフォルトルート設定)	IPv6 アドレスのスタティックエントリは IPv6 形式のアドレスで本スイッチのルーティ ングテーブルに入力します。
IPv6 Route Table (IPv6 ルートテーブル)IPv6 ルーティングテーブルを表示します。Route Preference (ルート優先度設定)ルート優先度を設定します。小さい優先度値を持つルートほど高いプライオリティを持ちます。ECMP Settings (ECMP 設定) (EI/MI モードのみ)ECMP OSPF 状態と ECMP ルートロードパランシングアルゴリズムを設定します。IPv6 General PrefixVLAN インタフェース IPv6 汎用プリフィクスの設定を行います。(IPv6 汎用プリフィクス)IP Tunnel Settings (IP トンネル設定)IP Tunnel Settings (URPF 設定)IP トンネルを設定します。VRF (Virtual Routing and Forwarding)FUnicast Reverse Path Forwarding」(URPF) の設定を表示を行います。(EI/MI モードのみ)RIP (Routing Information Protocol)RIP (Routing Information Protocol)RIP (Routing Information Protocol) は、距離ベクトル型のルーティングプロトコルです。RIPng (RIPng 設定)OSPF を設定します。IP Multicast Routing ProtocolIP Multicast Routing ProtocolIP Multicast Routing ProtocolIP Multicast Routing ProtocolIP Multicast Routing ProtocolBCP (Border Gateway Protocol)BCP (Border Gateway Protocol)BCP (Border Gateway Protocol)BCD (Bidirectional Forwarding Detection)Bidirectional Forwarding DetectionBFD (Bidirectional Forwarding Detection)Bidirectional Forwarding Detection		IPv6 Static Route BFD (IPv6 スタティックルート BFD)	IPv6 スタティックルート BFD(Bidirectional Forwarding Detection)の設定を行います。
Route Preference (ルート優先度設定)ルート優先度を設定します。小さい優先度値を持つルートほど高いプライオリティを持ちます。ECMP Settings (ECMP 設定) (EI/MI モードのみ)ECMP OSPF 状態と ECMP ルートロードバランシングアルゴリズムを設定します。IPv6 General Prefix (IPv6 汎用プリフィクス)VLAN インタフェース IPv6 汎用プリフィクスの設定を行います。IP Tunnel Settings (IP トンネル設定)IP トンネルを設定します。URPF Settings (URPF 設定)FUnicast Reverse Path Forwarding」 (URPF) の設定と表示を行います。VRF (Virtual Routing and Forwarding) (EI/MI モードのみ)FV (Routing Information Protocol) は、距離ベクトル型のルーティングプロトコルです。RIP (Routing Information Protocol)RIP (Routing Information Protocol) は、距離ベクトル型のルーティングプロトコルです。RIPng (RIPng 設定)RIPng (Routing Information Protocol) は、距離ベクトル型のルーティングプロトコルです。OSPF (OSPF 設定) (EI/MI モードのみ)OSPF を設定します。IP Multicast Routing Protocol (IP マルチキャストルーティングプロトコル)PMulticast Routing Protocol (IP マルチキャストルーティングプロトコル)BGP (Border Gateway Protocol) (EI/MI モードのみ)BGP (Border Gateway Protocol) (BGP (Border Gateway Protocol)BGP (Border Gateway Protocol) (IP マルチキャストルーティングプロトコル)BFD (Bidirectional Forwarding Detection)Bidirectional Forwarding DetectionBidirectional Forwarding Detection		IPv6 Route Table(IPv6 ルートテーブル)	IPv6 ルーティングテーブルを表示します。
ECMP Settings (ECMP 設定) (EI/MI モードのみ)ECMP OSPF 状態と ECMP ルートロードバランシングアルゴリズムを設定します。IPv6 General Prefix (IPv6 汎用プリフィクス)VLAN インタフェース IPv6 汎用プリフィクスの設定を行います。IP Tunnel Settings (IP トンネル設定)IP トンネルを設定します。URPF Settings (URPF 設定)FUnicast Reverse Path Forwarding」 (URPF) の設定と表示を行います。VRF (Virtual Routing and Forwarding) (EI/MI モードのみ)FVirtual Routing and Forwarding」 (VRF) の設定を行います。RIP (Routing Information Protocol)RIP (Routing Information Protocol) は、距離ベクトル型のルーティングプロトコルです。RIPng (RIPng 設定)RIPng (Routing Information Protocol) は、距離ベクトル型のルーティングプロトコルです。OSPF (OSPF 設定) (EI/MI モードのみ)RIPng (Routing Information Protocol) Rest Reverse Apt Forwarding I (PR マルチキャストルーティングプロトコル)OSPF (OSPF 設定) (EI/MI モードのみ)OSPF を設定します。IP Multicast Routing Protocol (IP マルチキャストルーティングプロトコル)PM Multicast Routing Protocol)BGP (Border Gateway Protocol) (EI/MI モードのみ)BGP (Border Gateway Protocol) をサポートしています。これは AS (自律システム) 内のネットワーク到達性を指定する IP ネットワークまたはプレフィックスのテーブル を保持するレイヤ3 ユニキャストルーティングプロトコルです。BFD (Bidirectional Forwarding Detection)Bidirectional Forwarding Detection (BFD) の設定を行います。		Route Preference( ルート優先度設定)	ルート優先度を設定します。小さい優先度値を持つルートほど高いプライオリティを持ちます。
IPv6 General Prefix (IPv6 汎用プリフィクス)VLAN インタフェース IPv6 汎用プリフィクスの設定を行います。IP Tunnel Settings (IP トンネル設定)IP トンネルを設定します。URPF Settings (URPF 設定)「Unicast Reverse Path Forwarding」 (URPF) の設定と表示を行います。VRF (Virtual Routing and Forwarding) (EI/MI モードのみ)「Virtual Routing and Forwarding」 (VRF) の設定を行います。RIP (Routing Information Protocol)RIP (Routing Information Protocol) は、距離ベクトル型のルーティングプロトコルです。RIPng (RIPng 設定)RIPng (Routing Information Protocol) は、距離ベクトル型のルーティングプロトコルです。OSPF (OSPF 設定) (EI/MI モードのみ)RIPng (Routing Information Protocol next generation) をサポートしています。RIPng は、 ルートを計算するのに使用するルーティング情報を交換するルーティングプロトコルで あり、IPv6 ベースのネットワーク用です。OSPF (OSPF 設定) (EI/MI モードのみ)OSPF を設定します。IP Multicast Routing Protocol (IP マルチキャストルーティングプロトコル)IP Multicast Routing Protocol のネットワーク到達性を指定する IP ネットワークまたはプレフィックスのテーブル を保持するレイヤ3ユニキャストルーティングプロトコルです。BGP (Border Gateway Protocol) (EI/MI モードのみ)BGP (Border Gateway Protocol) をサポートしています。これは AS (自律システム) 内のネットワーク到達性を指定する IP ネットワークまたはプレフィックスのテーブル を保持するレイヤ3ユニキャストルーティングプロトコルです。BFD (Bidirectional Forwarding Detection)Bidirectional Forwarding Detection		ECMP Settings (ECMP 設定)(EI/MI モードのみ)	ECMP OSPF 状態と ECMP ルートロードバランシングアルゴリズムを設定します。
IP Tunnel Settings (IP トンネル設定)IP トンネルを設定します。URPF Settings (URPF 設定)「Unicast Reverse Path Forwarding」(URPF)の設定と表示を行います。VRF (Virtual Routing and Forwarding) (EI/MI モードのみ)「Virtual Routing and Forwarding」(VRF)の設定を行います。RIP (Routing Information Protocol)RIP (Routing Information Protocol) は、距離ベクトル型のルーティングプロトコルです。RIPng (RIPng 設定)RIPng (Routing Information Protocol next generation)をサポートしています。RIPng は、 ルートを計算するのに使用するルーティング情報を交換するルーティングプロトコルで あり、IPv6 ベースのネットワーク用です。OSPF (OSPF 設定) (EI/MI モードのみ)OSPF を設定します。IP Multicast Routing Protocol (IP マルチキャストルーティングプロトコル)IP Multicast Routing Protocol (IP マルチキャストルーティングプロトコル)の設定を行います。BGP (Border Gateway Protocol) (EI/MI モードのみ)BGP (Border Gateway Protocol)BGP (Border Gateway Protocol)BFD (Bidirectional Forwarding Detection)Bidirectional Forwarding DetectionBidirectional Forwarding Detection (BFD) の設定を行います。		IPv6 General Prefix (IPv6 汎用プリフィクス)	VLAN インタフェース IPv6 汎用プリフィクスの設定を行います。
URPF Settings (URPF 設定)「Unicast Reverse Path Forwarding」(URPF) の設定と表示を行います。VRF (Virtual Routing and Forwarding) (EI/MI モードのみ)Nitrual Routing and Forwarding」(VRF) の設定を行います。RIP (Routing Information Protocol)RIP (Routing Information Protocol) は、距離ベクトル型のルーティングプロトコルです。RIPng (RIPng 設定)RIPng (Routing Information Protocol next generation)をサポートしています。RIPng は、 ルートを計算するのに使用するルーティング情報を交換するルーティングプロトコルで あり、IPv6 ベースのネットワーク用です。OSPF (OSPF 設定) (EI/MI モードのみ)OSPF を設定します。IP Multicast Routing Protocol (IP マルチキャストルーティングプロトコル)IP Multicast Routing Protocol (IP マルチキャストルーティングプロトコル)の設定を行います。BGP (Border Gateway Protocol) (EI/MI モードのみ)BGP (Border Gateway Protocol)BGP (Border Gateway Protocol) をサポートしています。これは AS (自律システム) 内のネットワーク到達性を指定する IP ネットワークまたはプレフィックスのテーブル を保持するレイヤ 3 ユニキャストルーティングプロトコルです。BFD (Bidirectional Forwarding Detection)Bidirectional Forwarding DetectionBidirectional Forwarding Detection		IP Tunnel Settings(IP トンネル設定)	IP トンネルを設定します。
VRF (Virtual Routing and Forwarding) (EI/MI モードのみ)「Virtual Routing and Forwarding」(VRF) の設定を行います。RIP (Routing Information Protocol)RIP (Routing Information Protocol) は、距離ベクトル型のルーティングプロトコルです。RIPng (RIPng 設定)RIPng (Routing Information Protocol next generation)をサポートしています。RIPng は、 ルートを計算するのに使用するルーティング情報を交換するルーティングプロトコルで あり、IPv6 ベースのネットワーク用です。OSPF (OSPF 設定) (EI/MI モードのみ)OSPF を設定します。IP Multicast Routing Protocol (IP マルチキャストルーティングプロトコル)IP Multicast Routing Protocol (IP マルチキャストルーティングプロトコル)の設定を行います。BGP (Border Gateway Protocol) (EI/MI モードのみ)BGP (Border Gateway Protocol) をサポートしています。これは AS (自律システム) 内のネットワーク到達性を指定する IP ネットワークまたはプレフィックスのテーブル を保持するレイヤ 3 ユニキャストルーティングプロトコルです。BFD (Bidirectional Forwarding Detection)Bidirectional Forwarding Detection (BFD) の設定を行います。		URPF Settings(URPF 設定)	「Unicast Reverse Path Forwarding」(URPF)の設定と表示を行います。
RIP (Routing Information Protocol)RIP (Routing Information Protocol) は、距離ベクトル型のルーティングプロトコルです。RIPng (RIPng 設定)RIPng (Routing Information Protocol next generation)をサポートしています。RIPng は、 ルートを計算するのに使用するルーティング情報を交換するルーティングプロトコルで あり、IPv6 ベースのネットワーク用です。OSPF (OSPF 設定) (EI/MI モードのみ)OSPF を設定します。IP Multicast Routing Protocol (IP マルチキャストルーティングプロトコル)IP Multicast Routing Protocol (IP マルチキャストルーティングプロトコル)の設定を行います。BGP (Border Gateway Protocol) (EI/MI モードのみ)BGP (Border Gateway Protocol) をサポートしています。これは AS (自律システム) 内のネットワーク到達性を指定する IP ネットワークまたはプレフィックスのテーブル を保持するレイヤ 3 ユニキャストルーティングプロトコルです。BFD (Bidirectional Forwarding Detection)Bidirectional Forwarding Detection		VRF(Virtual Routing and Forwarding) (EI/MI モードのみ)	「Virtual Routing and Forwarding」(VRF) の設定を行います。
RIPng (RIPng 設定)RIPng (Routing Information Protocol next generation)をサポートしています。RIPng は、 ルートを計算するのに使用するルーティング情報を交換するルーティングプロトコルで あり、IPv6 ベースのネットワーク用です。OSPF (OSPF 設定) (EI/MI モードのみ)OSPF を設定します。IP Multicast Routing Protocol (IP マルチキャストルーティングプロトコル)IP Multicast Routing Protocol (IP マルチキャストルーティングプロトコル)の設定を行います。BGP (Border Gateway Protocol) (EI/MI モードのみ)BGP (Border Gateway Protocol) をサポートしています。これは AS (自律システム) 内のネットワーク到達性を指定する IP ネットワークまたはプレフィックスのテーブル を保持するレイヤ 3 ユニキャストルーティングプロトコルです。BFD (Bidirectional Forwarding Detection)Bidirectional Forwarding Detection)		RIP (Routing Information Protocol)	RIP(Routing Information Protocol)は、距離ベクトル型のルーティングプロトコルです。
OSPF (OSPF 設定)(EI/MI モードのみ)OSPF を設定します。IP Multicast Routing Protocol (IP マルチキャストルーティングプロトコル)の設定を行います。IP Multicast Routing Protocol (IP マルチキャストルーティングプロトコル)の設定を行います。BGP (Border Gateway Protocol) (EI/MI モードのみ)BGP (Border Gateway Protocol) をサポートしています。これは AS (自律システム) 内のネットワーク到達性を指定する IP ネットワークまたはプレフィックスのテーブル を保持するレイヤ 3 ユニキャストルーティングプロトコルです。BFD (Bidirectional Forwarding Detection)Bidirectional Forwarding Detection)		RIPng(RIPng 設定)	RIPng (Routing Information Protocol next generation)をサポートしています。RIPng は、 ルートを計算するのに使用するルーティング情報を交換するルーティングプロトコルで あり、IPv6 ベースのネットワーク用です。
IP Multicast Routing Protocol (IP マルチキャストルーティングプロトコル)の設定を行います。BGP (Border Gateway Protocol) (EI/MI モードのみ)BGP (Border Gateway Protocol) をサポートしています。これは AS (自律システム) 内のネットワーク到達性を指定する IP ネットワークまたはプレフィックスのテーブル を保持するレイヤ 3 ユニキャストルーティングプロトコルです。BFD (Bidirectional Forwarding Detection)Bidirectional Forwarding Detection)		OSPF(OSPF 設定)(EI/MI モードのみ)	OSPF を設定します。
BGP (Border Gateway Protocol)BGP (Border Gateway Protocol)をサポートしています。これは AS (自律システム)(EI/MI モードのみ)内のネットワーク到達性を指定する IP ネットワークまたはプレフィックスのテーブル を保持するレイヤ 3 ユニキャストルーティングプロトコルです。BFD (Bidirectional Forwarding Detection)Bidirectional Forwarding Detection (BFD)の設定を行います。		IP Multicast Routing Protocol (IP マルチキャストルーティングプロトコル)	IP Multicast Routing Protocol (IP マルチキャストルーティングプロトコル) の設定を行います。
BFD(Bidirectional Forwarding Detection) Bidirectional Forwarding Detection (BFD) の設定を行います。		BGP(Border Gateway Protocol) (EI/MI モードのみ)	BGP(Border Gateway Protocol)をサポートしています。これは AS(自律システム) 内のネットワーク到達性を指定する IP ネットワークまたはプレフィックスのテーブル を保持するレイヤ 3 フェキャストルーティングプロトコルです
		BFD (Bidirectional Forwarding Detection)	Bidirectional Forwarding Detection (BFD) の設定を行います。

メインメニュー	サブメニュー	説明
L3 Features	ISIS(Intermediate System to Intermediate System)(MI モードのみ)	Intermediate System to Intermediate System (ISIS) の設定を行います。
	IP Route Filter(IP ルートフィルタ)	IP プレフィックスリスト、ルートマップの作成、またはルートマップへのシーケンスの 追加、およびシーケンスの削除を行います。
	Policy Route(ポリシールート設定)	ポリシーベースルーティングの設定、表示を行います。
	VRRP Settings(VRRP 設定)	VRRP (Virtual Routing Redundancy Protocol)は、LAN 上の VRRP ルータの 1 つに仮想ルー タとしての役割を動的に割り当てる機能です。
	VRRPv3 Settings(VRRPv3 設定)	VRRPv3 設定を行います。
QoS	Basic Settings(基本設定)	QoS の Basic Settings(基本設定)を行います。
	Advanced Settings(アドバンス設定)	QoS の Advanced Settings(アドバンス設定)を行います。
	QoS PFC	ネットワーク「Quality of Service」(QoS) プライオリティベースフローコントロール (PFC) クラスマップの設定を行います。
	WRED(WRED 設定)	WRED(WRED 設定)の設定を行います。
	iSCSI(アイスカジー)	iSCSIの設定を行います。
ACL	ACL Configuration Wizard (ACL 設定ウィザード)	ACL 設定ウィザードは、アクセスプロファイルと ACL ルールの新規作成を行います。
	ACL Access List(ACL アクセスリスト)	ACL アクセスリストの設定を行います。
	ACL Interface Access Group (ACL インタフェースアクセスグループ)	ACL インタフェースアクセスグループの設定を行います。
	ACL VLAN Access Map (ACL VLAN アクセスマップ)	ACL VLAN アクセスマップの設定を行います。
	ACL VLAN Filter(ACL VLAN フィルタ設定)	ACL VLAN フィルタの設定を行います。
	CPU ACL	CPU インタフェースフィルタリング機能の設定を行います。
Security	Port Security(ポートセキュリティ)	ポートセキュリティは、ポートのロックを行う前にスイッチが(ソース MAC アドレスを) 認識していない不正なコンピュータが、ロックしたポートに接続してネットワークへの アクセスを行わないようにするための機能です。
	802.1X(802.1X 認証設定)	IEEE 802.1X 標準規格は、クライアント・サーバベースのアクセスコントロールモデル の使用により、特定の LAN 上の様々な有線 / 無線デバイスへのアクセスを行う場合に ユーザ認証を行うセキュリティ方式です。
	AAA(AAA 設定)	AAA(Authentication、Authorization、Accounting)の設定を行います。
	RADIUS (RADIUS 設定)	RADIUS の設定を行います。
	TACACS+(TACACS+ 設定)	TACACS+ の設定を行います。
	IMPB(IP-MAC-Port Binding/IP-MAC- ポー トバインディング)	IP-MAC バインディングにより、スイッチにアクセスするユーザ数を制限します。
	DHCP Server Screening (DHCP サーバスクリーニング設定)	DHCP サーバスクリーニングは不正な DHCP サーバへのアクセスを拒否する機能です。
	ARP Spoofing Prevention (ARP スプーフィング防止設定)	ARP スプーフィング防止機能は、設定したゲートウェイ IP アドレスとマッチしなかった IP アドレスの ARP パケットをバイパスします。
	BPDU Attack Protection (BPDU アタック防止設定)	スイッチのポートに BPDU 防止機能を設定します。
	NetBIOS Filtering (NetBIOS フィルタリング設定)	NetBIOS フィルタリングの設定を行います。
	MAC Authentication(MAC 認証)	MAC 認証機能は、MAC アドレスにてネットワークの認証を設定する方法です。
	Web-based Access Control (Web 認証)	Web ベース認証はスイッチを経由でインターネットにアクセスする場合、ユーザを認 証する機能です。
	Japanese Web-based Access Control (JWAC)	JWAC(Japanese Web-based Access Control)の有効化および設定をします。
	Network Access Authentication (ネットワークアクセス認証)	Network Access Authentication(ネットワークアクセス認証)の設定を行います。
	Safeguard Engine (セーフガードエンジン)	セーフガードエンジンは、攻撃中にスイッチの稼働を最小化して、スイッチ全体の操 作性を保ち、限られたリソース内で必要不可欠なパケットの送受信を可能にします。
	Trusted Host(トラストホスト)	トラストホストの設定を行います。
	Traffic Segmentation Settings (トラフィックセグメンテーション)	トラフィックセグメンテーション機能はポート間のトラフィックの流れを制限を行い ます。
	Storm Control Settings(ストームコント ロール設定)	ストームコントロールの設定を行います。
	DoS Attack Prevention Settings (DoS 攻撃防止設定)	各 DoS 攻撃に対して防御設定を行います。

メインメニュー	サブメニュー	説明
Security	Zone Defense Settings(ゾーンディフェ ンス設定)	「ゾーンディフェンス(Zone Defense)」機能の設定と表示を行います。
	SSH (Secure Shell)	SSH(Secure Shell)は、安全性の低いネットワーク上で、安全なリモートログインと 安全なネットワークサービスを実現するためのプログラムです。
	SSL (Secure Socket Layer)	Secure Sockets Layer(SSL)とは、認証、デジタル署名および暗号化を使用して、ホストとクライアント間に安全な通信パスを提供するセキュリティ機能です。
	SFTP Server Settings(SFTP サーバ設定)	本項目では「Secure File Transfer Protocol」(SFTP) サーバの設定、表示を行います。
	SFTP Client Settings (SFTP クライアント設定)	本項目では「Secure File Transfer Protocol」(SFTP) クライアントの設定、表示を行います。
	Network Protocol Port Protect Settings	ネットワークプロトコルポート保護設定を行います。
OAM	CFM(Connectivity Fault Management : 接 続性障害管理)	CFM 機能を設定します。
	Cable Diagnostics(ケーブル診断機能)	スイッチの特定のポートに接続する UTP ケーブルの詳細について表示します。
	Ethernet OAM(イーサネット OAM)	ポートにイーサネット OAM モード、イベント、ログを設定します。
	DDM(DDM 設定)	Digital Diagnostic Monitoring(DDM)機能を実行します。スイッチに挿入した SFP モジュールの DDM 状態の参照、各種設定(アラーム設定、警告設定、温度しきい値設定、 電圧しきい値設定、バイアス電流しきい値設定、Tx(送信)電力しきい値設定、および Rx(受信)電力しきい値設定)を行うことができます。
MPLS (MIモードのみ)	MPLS LDP Information Settings (MPLS LDP 情報設定)	「Multiprotocol Label Switching」 (MPLS) の「Label Distribution Protocol」 (LDP) 情報の 設定を行います。
	MPLS LSP Trigger Information (MPLS LSP トリガ情報)	「Multiprotocol Label Switching」(MPLS)の「Label-Switched Label-Switched Path」(LSP) トリガ情報の設定を行います
	MPLS Forwarding Settings (MPLS フォワーディング設定)	MPLS フォワーディングの設定を行います。
	MPLS LDP Neighbor Password Settings (MPLS LDP ネイバパスワード設定)	MPLS LDP ネイバパスワードの設定を行います。
	MPLS LDP Neighbor Targeted Settings (MPLS LDP ネイバターゲット設定)	MPLS LDP ネイバターゲットの設定を行います。
	MPLS LDP Neighbor Information (MPLS LDP ネイバ情報)	MPLS LDP Neighbor Information(MPLS LDP ネイバ情報)の表示をします。
	MPLS Global Settings (MPLS グローバル設定)	MPLS Global Settings(MPLS グローバル設定)の設定を行います。
	MPLS LDP Interface Settings (MPLS LDP インタフェース設定)	MPLS LDP Interface Settings(MPLS LDP インタフェース設定)の設定をします。
	MPLS LDP Session Information (MPLS LDP セッション情報)	MPLS LDP Session Information(MPLS LDP セッション情報)の検出、表示をします。
	MPLS LDP Statistic (MPLS LDP スタティスティック)	MPLS LDP Statistic(MPLS LDP スタティスティック)の表示をします。
	MPLS LDP Binding Table (MPLS LDP バインディングテーブル)	MPLS LDP Binding Table(MPLS LDP バインディングテーブル)の表示をします。
	MPLS LDP Discovery Information (MPLS LDP ディスカバリ情報)	MPLS LDP Discovery Information(MPLS LDP ディスカバリ情報)の表示をします。
	MPLS QoS Settings(MPLS QoS 設定)	MPLS QoS Settings(MPLS QoS 設定)の設定、表示をします。
	Ping MPLS	指定 FEC の LSP の接続状態を確認します。
	Traceroute MPLS IPv4 (トレースルート MPLS IPv4)	指定 FEC の LSP パストレースのような「hop-by-hop fault localization」を指定します。
MPLS L2VPN	VPWS Settings(VPWS 設定)	「Virtual Private Wire Service」(VPWS) を設定を行います。
(MIモードのみ)	L2VC Interface Description (L2VC インタフェース概要)	L2VC Interface Description(L2VC インタフェース概要)を設定を行います。
	VPLS Settings(VPLS 設定)	「Virtual Private LAN Service」(VPLS) を設定を行います。
	VPLS MAC Address Table (VPLS MAC アドレステーブル)	「VPLS MAC Address Table」(VPLS MAC アドレステーブル)を表示を行います。

メインメニュー	サブメニュー	説明
Monitoring	VLAN Counter(VLAN カウンタ)	VLAN カウンタの設定を行います。L2 VLAN インタフェースにおけるトラフィック統計 のコントロールエントリを指定します。
	 Utilization(利用分析)	スイッチの Utilization(利用分析)を表示します。
	Statistics(統計情報)	スイッチの Statistics(統計情報)を表示します。
	Mirror Settings(ミラー設定)	ミラーリング機能の設定を行います。本スイッチは対象ポートで送受信するフレーム をコピーし、フレームの出力先を他のポートに変更する機能(ポートミラーリング) があります。
	sFlow(sFlow 設定)	sFlow は(RFC3176)、スイッチやルータを経由するネットワークトラフィックをモニ タする機能です。sFlow によるモニタリングは「sFlow エージェント」(スイッチやルー タ内に内蔵)と「セントラル sFlow コレクタ」によって構成されています。
	Device Environment(機器環境確認)	Device Environment(機器環境確認)ではスイッチの内部の温度状態を表示します。
	External Alarm Settings (外部アラーム設定)	外部アラーム設定はアラーム起動時のアラームメッセージについて設定します。
Green	Power Saving(省電力)	スイッチの省電力機能を設定、表示します。
	EEE (Energy Efficient Ethernet/省電力イーサネット)	「Energy Efficient Ethernet」(EEE/ 省電力イーサネット ) は「IEEE 802.3az」によって定義 されており、パケットの送受信がリンクに発生していない場合の電力消費を抑える目 的で設計されています。
OpenFlow	OpenFlow Settings(OpenFlow 設定)	OpenFlow の設定を行います。
Save	Save Configuration (コンフィグレーションの保存)	「Save Configuration」ではスイッチのコンフィグレーションを保存します。
Tools	Firmware Upgrade & Backup (ファームウェアアップグレード&バックアップ)	様々なプロトコルを使用してファームウェアアップグレード/バックアップを実行します。
	Configuration Restore & Backup (コンフィグレーションリストア&バックアップ)	様々なプロトコルを使用してコンフィグレーションリストア/バックアップを実行します。
	Certificate & Key Restore & Backup (証明書 / 鍵リストア&バックアップ)	様々なプロトコルを使用して証明書と鍵のリストア/バックアップを実行します。
	Log Backup (ログファイルのバックアップ)	様々なプロトコルを使用してログファイルのバックアップを実行します。
	Ping	「Ping」は指定した IP アドレスに ICMP Echo パケットを送信するプログラムです。
	Trace Route(トレースルート)	パケットの経路をスイッチに到着する前に遡ってトレースすることができます。
	Reset (リセット)	スイッチの設定内容を工場出荷時状態に戻します。
	Reboot System(システム再起動)	スイッチの再起動を行います。
	DLMS Settings(DLMS 設定)	「D-Link License Management System」(DLMS) の設定、表示を行います。

# 第6章 System (スイッチの主な設定)

以下は、System サブメニューの説明です。

必要に応じて、設定/変更/修正を行ってください。

サブメニュー	説明
Device Information(デバイス情報)	スイッチの主な設定情報を表示します。
System Information Settings(システム情報設定)	スイッチの基本情報を表示します。
Peripheral Settings(環境設定)	システムの警告温度や環境トラップの設定を行います。
Port Configuration(ポート設定)	スイッチポートの詳細設定などを行います。
Interface Description (インタフェース概要)	スイッチの各ポートの概要、管理ステータスなどについて表示します。
Loopback Test(ループバックテスト)	物理ポートインタフェースのループバック設定とループバックテストを行います。
PoE (PoE の管理) (DGS-3630-28PC/52PC)	PoE 機能の設定、表示を行います。(DGS-3630-28PC/52PC のみ)
System Log (システムログ構成)	スイッチのフラッシュメモリにスイッチログを保存する方法を選択します。
Time and SNTP(時刻設定)	スイッチに時刻を設定します。
Time Range (タイムレンジ設定)	スイッチのタイムレンジを設定します。アクセスプロファイル機能を実行する期間を決定します。
PTP(PTP 設定)	PTP(Precision Time Protocol : 高精度時刻同期方式)システムは、イーサネットネットワークを通し て時刻を同期します。
USB Console Settings (USB コンソール設定)	USB コンソールの設定、表示を行います。
SRM(Switch Resource Management 設定)	「Switch Resource Management」(SRM)により大規模なリソースを最適化します。

# Device Information (デバイス情報)

本画面は、ログインを行うと自動的に表示される画面で、スイッチの主な設定情報を確認できます。本画面に戻るためには「DGS-3630 シリーズ」フォ ルダをクリックします。本画面には、スイッチの「MAC Address」(工場による設定のため変更不可)、「Boot PROM Version」と「Firmware Version」、 「Hardware Version」などが表示されます。これらの情報は、PROM やファームウェアの更新状況の把握や他のネットワークデバイスのアドレステー ブルにスイッチの MAC アドレスを登録する際の確認などに便利です



図 6-1 Device Information 画面

#### 画面に表示される項目:

項目	説明	
	Device Information	
Device Type	工場にて定義した機種名と型式を表示します。	
System Name	ユーザが定義したシステム名を表示します。	
System Location	システムが現在動作している場所を表示します。(半角英数字 160 文字以内)	
System Contact	担当者名を表示します。(半角英数字 31 文字以内)	
Boot PROM Version	デバイスのブートバージョンを表示します。	
Firmware Version	デバイスのファームウェアバージョンを表示します。	
Hardware Version	デバイスのハードウェアバージョンを表示します。	
Serial Number	デバイスのシリアル番号を表示します。	
MAC Address	デバイスに割り当てられた MAC アドレスを表示します。	
IP Address	デバイスに割り当てられた IP アドレスを表示します。	
Mask	デバイスに割り当てられたサブネットマスクを表示します。	
Gateway	デバイスに割り当てられたデフォルトゲートウェイを表示します。	
System Time	最後のデバイスリセットからの経過時間を表示します。	
Utilization		
CPU	CPU の使用率を表示します。	
Flash	Flashの使用率を表示します。	
Memory	Memory の使用率を表示します。	

# System Information Settings (システム情報設定)

ここでは、スイッチの詳細情報を表示します。本画面の「System Information Settings」で「System Name」、「System Location」、「System Contact」 などを入力し、スイッチの定義を行う際にも利用できます。また「Mangement Interface」で管理インタフェースの設定を行います。

System > System Information Settings の順にメニューをクリックして、以下の画面を表示します。

System Information S	ettings	
System Information Setting	5	
System Name	Switch	
System Location	255 chars	
System Contact	255 chars	Apply
Interface Name State IPv4 Address	mgmt_ipif Enabled I92 - 168 - 0 - 1	
Subnet Mask	255 · 255 · 255 · 0	
Gateway	0 . 0 . 0 . 0	
Description	64 chars	· · · · · · · · · · · · · · · · · · ·
Link Status	Link Down	Apply

図 6-2 System Information Settings 画面

画面に表示される項目:

項目	説明		
	System Information Settings		
System Name	ユーザが定義するシステム名を設定します。		
System Location	システムが現在動作している場所を定義します。(半角英数字 160 文字以内)		
System Contact	スイッチの管理者情報を入力します。		
	Mangement Interface		
State	管理インタフェースの有効/無効を指定します。		
IPv4 Address	管理インタフェースの IPv4 アドレスを指定します。		
Subnet Mask	管理インタフェースのサブネットマスクを指定します。		
Gateway	管理インタフェースのゲートウェイ IPv4 アドレスを指定します。		
Description	管理インタフェースについての概要を指定します。(半角英数字 64 文字以内)		

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

# Peripheral Settings (環境設定)

システムの警告温度や環境トラップの設定を行います。

#### System > Peripheral Settings の順にクリックし、以下の画面を表示します。

Peripheral Settings			
Environment Trap Settings			
Fan Trap	Enabled	Disabled	
Power Trap	CEnabled	Disabled	
Temperature Trap	CEnabled	Disabled	Apply
Environment Temperature Threshol     Unit	d Settings		
Thermal	1		
High Threshold (-100-200)		C Default	
Low Threshold (-100-200)		Default	Apply

図 6-3 Peripheral Settings 画面

#### 画面に表示される項目:

項目	説明	
	Environment Trap Settings	
Fan Trap	プルダウンメニューを使用して、ファン警告設定のトラップを有効 / 無効に設定します。	
Power Trap	プルダウンメニューを使用して、電源警告設定のトラップを有効 / 無効に設定します。	
Temperature Trap	プルダウンメニューを使用して、温度警告設定のトラップを有効 / 無効に設定します。	
Environment Temperture Threshold Settings		
Unit	本設定を適用するユニットを選択します。	
Thermal	温度センサIDを選択します。	
High Threshold	高温警告しきい値を指定します。-100℃から200℃の間で指定できます。「Default」をチェックすると初期値に戻ります。	
Low Threshold	低温警告しきい値を指定します。-100℃から200℃の間で指定できます。「Default」をチェックすると初期値に戻ります。	
シーシー シー・シー・シー・シー・シー・シー・シー・シー・シー・シー・シー・シー・シー・シ		

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

# Port Configuration (ポート設定)

各ポートの設定を行います。

### Port Settings (スイッチのポート設定)

スイッチポートの詳細を設定します。「State」、「Speed/Duplex」、「Flow Control」、「Address Learning」、「Media Type」、および「MDIX」を含むさ まざまなポート設定をスイッチに行うことができます。

注意 「10M」と「100M」は管理ポート(Mgmt 0)でのみ有効です。

ポートの設定や情報の表示を行うには、System > Port Configuration > Port Settings の順にメニューを選択し、以下の画面を表示します。

Init		From Port		To Port	M	edia Type	e							
	<b>~</b>	eth1/0/1	~	eth1/0/1	✓ A	Auto	~							Apply
nit	I	From Port		To Port	S	state		Flow Control	I	Link St	atus Log	Descrip	otion	
1 [	~	eth1/0/1	~	eth1/0/1	✓ E	Enabled	~	Off [	~	Enab	led 🗸	64 cha	rs	✓
ledia Type		Auto Dowr	ngrade	MDIX	D	)uplex		Speed		Capab	ility Advertised	d		
RJ45	~	Disabled		Auto	V /	Auto	~	Auto		10N	1 🗌 100M 🗖	1000M	10G	Apply
nit 1 Settings Port	Link	Status	Medium	State	MDIX	Flow	Control	Duplex	Spee	be	Auto Down	orade	Link Status Lon	Descriptio
nit 1 Settings Port	Link	status	Medium	State	MDIX	Flow Send	Control Receive	- Duplex	Spee	d	Auto Down	grade	Link Status Log	Descriptio
nit 1 Settings Port eth1/0/1	Link	<b>Status</b> Up	Medium -	State Enabled	MDIX Auto-MDIX	Flow Send	Control Receive Off	Duplex Auto-duplex	Spee Auto-sp	d	Auto Down	grade d	Link Status Log On	Descriptio
nit 1 Settings Port eth1/0/1 eth1/0/2	Link	s Status Up Down	Medium -	State Enabled Enabled	MDIX Auto-MDIX Auto-MDIX	Flow Send C Off	Control Receive Off Off	Duplex Auto-duplex Auto-duplex	Spee Auto-sp Auto-sp	ed beed beed	Auto Down Disable Disable	grade d d	Link Status Log On On	Descriptio
Port eth1/0/1 eth1/0/2 eth1/0/3	Link	C Status Up Down Up	Medium - -	State Enabled Enabled Enabled	MDIX Auto-MDIX Auto-MDIX Auto-MDIX	Flow Send C Off C Off	Control Receive Off Off Off	Duplex Auto-duplex Auto-duplex Auto-duplex	Spee Auto-sp Auto-sp Auto-sp	ed beed beed beed	Auto Down Disable Disable Disable	grade d d d	Link Status Log On On On	Descriptio
Port eth1/0/1 eth1/0/2 eth1/0/3 eth1/0/4		Up Oown Up Oown	Medium - - -	State Enabled Enabled Enabled Enabled	MDIX Auto-MDIX Auto-MDIX Auto-MDIX Auto-MDIX	Flow Send C Off C Off C Off C Off	Control Receive Off Off Off Off	Duplex Auto-duplex Auto-duplex Auto-duplex Auto-duplex	Spee Auto-sp Auto-sp Auto-sp Auto-sp	ed beed beed beed beed	Auto Downy Disable Disable Disable Disable	grade d d d d	Link Status Log On On On On	Descriptic
nit 1 Settings Port eth1/0/1 eth1/0/2 eth1/0/3 eth1/0/4 eth1/0/5		C Status Up Down Up Down Down	Medium - - - -	State Enabled Enabled Enabled Enabled	MDIX Auto-MDIX Auto-MDIX Auto-MDIX Auto-MDIX Auto-MDIX	Flow Send Off Off Off Off Off	Control Receive Off Off Off Off Off Off	Duplex Auto-duplex Auto-duplex Auto-duplex Auto-duplex Auto-duplex	Spee Auto-sp Auto-sp Auto-sp Auto-sp Auto-sp	ed beed beed beed beed beed beed	Auto Down Disable Disable Disable Disable Disable	grade d d d d d d	Link Status Log On On On On On	Descriptio

図 6-4 Port Settings 画面

画面に表示される項目:

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を設定します。
Media Type	ポートメディアタイプを「Auto」「RJ45」「SFP」から選択します。SFP オプションは SFP+ を使用する 10G 接続も含まれます。
State	物理ポートの有効 / 無効を指定します。 ・ Enabled - 選択した物理ポートが有効です。 ・ Disabled - 選択した物理ポートが無効です。
Flow Control	「On」(フロー制御あり)または「Off」(フロー制御なし)を選択します。Full-Duplex のポートでは 802.3x フローコントロール による制御を行います。「Auto」は自動的にいずれかを使用します。物理スタックのスイッチはサポートしていません。
Link Status Log	リンクステータスのログ機能を有効/無効にします。
Description	当該のポートについて 64 文字以内に概要を指定します。
Auto Downgrade	リンクが有効なスピードを確立できなかった場合、アドバタイズスピードの自動的なダウングレードを有効 / 無効にします。
MDIX	<ul> <li>Auto - 最適なケーブル接続を自動的に設定します。</li> <li>Normal - ケーブル接続に Normal を選択します。</li> <li>Cross - ケーブル接続に Cross を選択します。</li> </ul>
	「Normal」を選択すると、MDI モードにあるボートはストレートケーブルを通して PC のネットワークボード、またはクロスケー ブルで別のスイッチのポート (MDI モード) に接続することができます。「Cross」を選択すると、MDIX モードにあるポートは ストレートケーブルで別のスイッチのポート (MDI モード) に接続することができます。
Duplex	Duplex モードの選択を行います。「Auto」「Full」から選択します。半二重モードはサポートされていません。

項目	説明
Speed	「Speed」欄でポートの速度を選択します。ここでは指定したポートを指定した速度のみで接続するように手動で設定します。 「Auto」を指定すると、接続相手の状況に合わせて、最適な通信を行うよう自動的に判別します。
	オプションには「Auto」「10M」「100M」「1000M」「1000M Master」「1000M Slave」「10G」「10G Master」および「10G Slave」 があります。「Auto」以外のオプションのポート設定は固定となります。
	マスタ設定 (1000M Master) によりポートはデュプレックス、さらに 2 つの接続している物理レイヤ間のマスタおよびスレーブ を決定します。この関係は 2 つの物理レイヤ間のタイミングコントロールを確立するために必要です。タイミング制御は、ロー カルソースによってマスタの物理層に設定されます。 スレーブ設定 (1000M Slave) はループタイミングを使用します。マスタから受信したデータストリームによりタイミングを合わ せます。一方の接続に「1000M Master」を設定すると、他方の接続は「1000M Slave」とする必要があります。その他の設定は両ポー
	トのリンクタウンを引き起こします。 Auto - カッパーポートの設定を行います。オートネゴシエーションが開始されリンクパートナーと速度、フローコントロール の調整を行います。光ファイバポートではオートネゴシエーションが開始されリンクパートナーとクロック、フローコントロー ルの調整を行います。
	<ul> <li>10M - ポート速度を 10Mbps に固定します。10Mbps カッパー接続でのみ有効です。</li> <li>100M - ポート速度を 100Mbps に固定します。100Mbps カッパー接続でのみ有効です。</li> <li>1000M - ポート速度を 1Gbps に固定します。1Gbps 光ファイバ接続でのみ有効です。</li> <li>1000M Master - ポート速度を 1Gbps に固定しマスタとして指定し、送受信のタイミングについての動作を制御します。 1Gbps カッパー接続でのみ有効です。</li> <li>1000M Slave - ポート速度を 1Gbps に固定しスレーブとして指定し、送受信のタイミングについての動作を制御します。 1Gbps カッパー接続でのみ有効です。</li> <li>10G - ポート速度を 10Gbps に固定します。10Gbps 光ファイバ接続でのみ有効です。</li> <li>10G Master - ポート速度を 10Gbps に固定しマスタとして指定し、送受信のタイミングについての動作を制御します。 10Gbps 光ファイバ接続でのみ有効です。</li> <li>10G Slave - ポート速度を 10Gbps に固定しスレーブとして指定し、送受信のタイミングについての動作を制御します。 10Gbps 光ファイバ接続でのみ有効です。</li> </ul>
Capability Advertised	上記「Speed」が「Auto」に設定されている場合、オートネゴシエーションの間、本機能は有効になります。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。 「Refresh」ボタンをクリックして、本画面を更新します。

注意 ハードウェア制限により接続先の相手が「10M/Half」でネゴシエートする場合や、「10Mbps Shared HUB」である場合はリンクアップしません。

注意 ハードウェア制限により 10G での auto-negotiation 情報は表示できません。

注意 10G ポートでの auto-downgrade はサポートされません。

# Port Status(ポートステータス)

ポートの状態、設定について表示します。

#### System > Port Configuration > Port Status の順にメニューをクリックし、以下の画面を表示します。

ort Status	_	_	_	_	_	_	_	_
ort Status								
Unit	1 •							
Unit 1 Settings								
Dort	Status	MAC Address	MAN	Flow Cont	rol Operator	Duploy	Smod	Tuno
PUIL	status	MAC AUDIESS	VLAN	Send	Receive	Duplex	speeu	type
eth1/0/1	Connected	00-01-02-03-04-01	1	Off	Off	Auto-Full	Auto-1000M	1000BASE-T
eth1/0/2	Not-Connected	00-01-02-03-04-02	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/3	Not-Connected	00-01-02-03-04-03	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/4	Not-Connected	00-01-02-03-04-04	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/5	Not-Connected	00-01-02-03-04-05	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/6	Not-Connected	00-01-02-03-04-06	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/7	Not-Connected	00-01-02-03-04-07	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/8	Not-Connected	00-01-02-03-04-08	1	Off	Off	Auto	Auto	1000BASE-T
eth 1/0/9	Not-Connected	00-01-02-03-04-09	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/10	Not-Connected	00-01-02-03-04-0A	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/11	Not-Connected	00-01-02-03-04-0B	1	Off	Off	Auto	Auto	1000BASE-T

図 6-5 Port Status 画面

画面に表示される項目:

項目	説明
Unit	表示するユニットを選択します。

# Port GBIC

スイッチの各物理ポートの GBIC 情報について表示します。

System > Port Configuration > Port GBIC の順にメニューをクリックし、以下の画面を表示します。

Port GBIC	
Port GBIC -	
Unit	
Unit 1 Setti	
eth1/0/1	
Interface Ty	1000BASE-T
eth1/0/2	
Interface Ty	1000BASE-T
eth1/0/3	
Interface Ty	1000BASE-T
eth1/0/4	
Interface Ty	1000BASE-T
eth1/0/5	
Interface Ty	1000BASE-T
eth1/0/6	
Interface Ty	1000BASE-T
eth1/0/7	
Interface Ty	1000BASE-T

図 6-6 Port GBIC 画面

画面に表示される項目:

項目	説明
Unit	表示するユニットを選択します。

# Port Auto Negotiation (オートネゴシエーション)

以下の画面ではオートネゴシエーションの詳しい情報を表示します。

System > Port Configuration > Port Auto Negotiation Information の順にメニューをクリックし、以下の画面を表示します。

and moge	otiation							
	1 🗸							
a: AN: Au	o Negotiation; R	S: Remote Signaling;	CS: Config Status;	CB: Capability Bit	s;CAB: Capbility A	dvertised Bits;		
CRB: (	apbility Receive	d Bits: RFA: Remote I	Fault Advertised: R	FR: Remote Fault	Received			
					110001100			
it 1 Setting	5				10001100			
it 1 Setting Port	s AN	RS	CS	СВ	САВ	CRB	RFA	RFR
it 1 Setting Port eth1/0/1	s AN Enabled	RS Not Detected	CS Complete	CB 10M_Half,	CAB 10M_Half,	CRB 10M_Half,	RFA Disabled	RFR
nit 1 Setting Port eth1/0/1 eth1/0/2	s AN Enabled Enabled	RS Not Detected Not Detected	CS Complete Configuring	CB 10M_Half, 10M_Half,	CAB 10M_Half, 10M_Half,	CRB 10M_Haif,	RFA Disabled Disabled	RFR NoError NoError

図 6-7 Port Auto Negotiation Information 画面

### Error Disable Settings (エラーによるポートの無効)

以下の画面では、パケットストームの発生やループバックの検出などの理由で、スイッチが切断したポートに関する情報を表示します。 この画面を参照するためには、System > Port Configuration > Port Error Disabled の順にメニューをクリックし、以下の画面を表示します。

ror Disable Trap Settings				
sserted	Disabled 🗸			
Cleared	Disabled 🗸			
lotification Rate (0-1000)				Apply
or Disable Recovery Setti	igs			
rrDisable Cause All	State	Disabled V Interv	al (5-86400)	sec Apply
	ErrDisable Cause		State	Interval (sec)
	Port Security		Disabled	300
	Storm Control		Disabled	300
	BPDU Attack Protection		Disabled	300
	Dynamic ARP Inspection		Disabled	300
	DHCP Snooping		Disabled	300
	Loopback Detect		Disabled	300
	L2PT Guard		Disabled	300
	D-LINK Unidirectional Link Dete	ectio	Disabled	300
terfaces that will be recov	ared at the next timeout:			

図 6-8 Port Error Disabled 画面

画面には以下の項目があります。

#### Error Disable Trap Settings(エラー無効トラップ設定)

項目	説明
Asserted	エラー無効状態になったとき、通知送信の有効 / 無効を指定します。
Cleared	エラー無効状態から回復したとき、通知送信の有効 / 無効を指定します。
Notification Rate	1 分あたりのトラップ数を入力します。指定したしきい値超えたパケットは破棄されます。0 から 1000 までの間で指定できます。

「Apply」ボタンをクリックすると設定が更新されます。

#### Error Disable Recovery Settings(エラー無効リカバリ設定)

項目	説明
ErrDisable Cause	エラー無効の原因を次から選択します。 「All」「Port Security」「Storm Control」「BPDU Attack Protection」「Dynamic ARP Inspection」「DHCP Snooping」「Loopback
State	指定した原因によるエラー無効ポートの自動リカバリ機能を有効/無効にします。
Interval	ポートリカバリ実行の間隔時間を 5 から 86400(秒)で指定します。
<b>F i i i i i i i i i i</b>	

「Apply」ボタンをクリックすると設定が更新されます。

### Jumbo Frame(ジャンボフレームの有効化)

ジャンボフレームにより、同じデータを少ないフレームで転送することができます。有効にすると、最大 12288 バイトを持つジャンボフレーム (1518 バイトの標準イーサネットフレームより大きいサイズのフレーム)の送信が可能になります。

ここでは、スイッチでジャンボフレームを扱うことを可能にします。これによりオーバヘッド、処理時間、割り込みを確実に減らすことができます。

#### System > Port Configuration > Jumbo Frame の順にクリックし、以下の画面を表示します。

Jumbo Frame	
Jumbo Frame	
Unit From Port	To Port Maximum Receive Frame Size (64-12288)
1 V eth1/0/1 V	eth1/0/1 🔽 1536 bytes Apply
Unit 1 Settings	
Port	Maximum Receive Frame Size (bytes)
eth1/0/1	1536
eth1/0/2	1536
eth1/0/3	1536
eth1/0/4	1536
eth1/0/5	1536
eth1/0/6	1536
eth1/0/7	1536
eth1/0/8	1536

図 6-9 Jumbo Frame Settings 画面

画面に表示される項目:

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を設定します。
Maximum Receive	スイッチのジャンボフレーム機能の最大値を 64 から 12288(バイト)で指定します。
Frame Size	初期値:1536 バイト

「Apply」ボタンをクリックすると設定が更新されます。

# Interface Description(インタフェース概要)

スイッチの各ポートの概要、管理ステータスなどについて表示します。

#### System > Interface Description の順にクリックし、以下の画面を表示します。

Interface Description			
Interface Description			
Total Entries: 30			
Interface	Status	Administrative	Description
eth1/0/1	up	enabled	
eth1/0/2	down	enabled	
eth1/0/3	up	enabled	
eth1/0/4	down	enabled	
eth1/0/5	down	enabled	
eth1/0/6	down	enabled	
eth1/0/7	down	enabled	
eth1/0/8	down	enabled	
eth1/0/9	down	enabled	
eth1/0/10	down	enabled	
			1/3 < 1 2 3 > > Go

図 6-10 Interface Description 画面

ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

# Loopback Test (ループバックテスト)

物理ポートインタフェースのループバック設定とループバックテストを行います。

System > Loopback Test の順にメニューをクリックし、以下の画面を表示します。

oopback Test		_	_	_	_	_	_	_	_
oopback Test									
Unit From	Port To Port	Loopback Mod	le						
1 🗸 eth	1/0/1 🔽 eth1/0/1 🔽	None		•					Apply
Unit 1 Settings									
0-4		64 6	Bytes	512	Bytes	1024	Bytes	1536	Bytes
Port	Loopback Mode	тх	RX	тх	RX	тх	RX	ТХ	RX
eth1/0/1	None	0	0	0	0	0	0	0	0
eth1/0/2	None	0	0	0	0	0	0	0	0
eth1/0/3	None	0	0	0	0	0	0	0	0
eth1/0/4	None	0	0	0	0	0	0	0	0
eth1/0/5	None	0	0	0	0	0	0	0	0
eth1/0/6	None	0	0	0	0	0	0	0	0
eth1/0/7	None	0	0	0	0	0	0	0	0

図 6-11 Loopback Test 画面

画面に表示される項目:

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を設定します。
Loopback Mode	<ul> <li>ループバックモードを指定します。</li> <li>None - ループバックモードを有効にしません。</li> <li>Internal MAC - インターナルループバックモードを MAC レイヤで指定します。</li> <li>Internal PHY Default - インターナルループバックモードを PHY レイヤで指定し初期メディアのテストをします。</li> <li>Internal PHY Copper - インターナルループバックモードを PHY レイヤで指定しカッパーメディアのテストをします。</li> <li>Internal PHY Fiber - インターナルループバックモードを PHY レイヤで指定し光ファイバメディアのテストをします。</li> <li>External MAC - エクスターナルループバックモードを MAC レイヤで指定します。</li> <li>External PHY Default - エクスターナルループバックモードを PHY レイヤで指定し初期メディアのテストをします。</li> <li>External PHY Default - エクスターナルループバックモードを PHY レイヤで指定し初期メディアのテストをします。</li> <li>External PHY Copper - エクスターナルループバックモードを PHY レイヤで指定しカッパーメディアのテストをします。</li> <li>External PHY Fiber - エクスターナルループバックモードを PHY レイヤで指定しカッパーメディアのテストをします。</li> </ul>

「Apply」ボタンをクリックすると設定が更新されます。

# PoE (PoE の管理) (DGS-3630-28PC/52PC)

DGS-3630-28PC/52PC は IEEE の 802.3af と IEEE802.3at 規格の PoE 機能をサポートしています。ポート 1-24/48 は 30W まで PoE、エンハンスドカテ ゴリ5以上のUTPイーサネットケーブル経由で PoE受電機器に約 48VDC 電力を供給できます。本スイッチは PSE pinout Alternative A に準拠しており、 電力はピン1、2、3、および6を通じて供給されます。 本スイッチでは次の PoE 機能を使用することができます。

本スイッチでは次の PoE 機能を使用することができます。

- ・ Auto-discovery 機能は PD( 受電機器 ) に自動的に電力を供給します。
- Auto-disable 機能は、「消費電力がシステム電源のリミットを超えている場合」と「各ポートの消費電力リミットを超えている場合」において 動作します。
- ・ Active circuit 防止機能は電力の不足が生じた場合、自動的にポートを無効にする機能です。他のポートは有効性は変わりません。

#### 802.3af/at 準拠の受電機器の最大受信電力一覧:

クラス	受電機器の最大受信電力
0	12.95W
1	3.84W
2	6.49W
3	12.95W
4	25.5W

#### PSE を使用したの最大電力一覧:

クラス	PSE の最大供給電力
0	16.2W
1	4.2W
2	7.4W
3	16.2W
ユーザ定義	31.6W
2 3 ユーザ定義	7.4W 16.2W 31.6W

## PoE System (PoE システム設定)

デバイスの PoE 情報を参照および変更します。

System > PoE > PoE System の順にクリックし、以下の画面を表示します。

PoE System	m					
PoE System						
Unit	Usage Three	shold (1-99)	Policy Preempt	Trap State		
1 💌	99	%	Disabled 💌	Disabled 💌		Apply
						Show Detail
Unit	Delivered (W)	Power Bud	lget (W)	Usage Threshold (%)	Policy Preempt	Trap State
1	0	193		99	Disabled	Disabled

図 6-12 PoE System 画面

#### 画面に表示される項目:

項目	説明
Unit	ユニット番号を設定します。全てのユニットを選択する場合は「All」にチェックします。
Usage Threshold	ログの記録や通常の通知送信を実行するしきい値を指定します。1 から 99(%)で指定できます。
Policy Preempt	電力供給不足となった新規接続のデバイスの優先値を高く指定し、既存の低優先度の電力供給デバイス(PD)接続の解除 機能を有効 / 無効に指定します。
Trap State	PoE の通知送信について有効 / 無効を指定します。

「Apply」ボタンをクリックすると設定が更新されます。

#### 「Show Detail」ボタンをクリックすると以下の画面が表示されます。

- PoE System Parameters ----

Unit	Max Ports	Device ID	SW Version
1	24	E111	13

図 6-13 PoE System (Show Detail) 画面

## PoE Status (PoE ステータス)

各ポートの PoE ステータスの表示と概要の設定を行います。

**System > PoE > PoE Status** の順にクリックし、以下の画面を表示します。

oE Status	_	_	_			_
oE Status						
Unit From Port	To Port	Desc	ription			
1 💌 eth1/0/1	<ul> <li>eth1/0/1</li> </ul>	<ul> <li>32 ch</li> </ul>	hars			Apply
Unit d Continues						
Unit 1 Settings						
Port	State	Class	Max (W)	Used (W)	Description	
Port eth1/0/1	State Searching	Class N/A	Max (W) 0.0	Used (W) 0.0	Description	Delete Descripti
Onit 1 Settings           Port           eth 1/0/1           eth 1/0/2	State Searching Searching	Class N/A N/A	Max (W) 0.0 0.0	Used (W) 0.0 0.0	Description	Delete Descripti Delete Descripti

図 6-14 PoE Status 画面

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を設定します。
Description	PoE インタフェースに接続中の PD の概要について入力します。32 文字以内で指定できます。
Delete Description L d	ジャンをクリックオスとふ力」と概要が削除されます

「Delete Description」ホタンをクリックすると人力した概要か削除されます。 「Apply」ボタンをクリックすると設定が更新されます。

### PoE Configuration (PoE ポート設定)

PoE 機能の有効化、現在の電力消費の表示、PoE トラップの有効化などシステムの PoE 情報の操作を行います。

**System > PoE > PoE Configuration**の順にクリックし、以下の画面を表示します。

E Configuration	_				_
E Configuration					
Init From Port	To Port eth1/0/1 ▼	Priority Legacy Support Low  Disabled	Mode Max Wattage (100 Auto	0-30000) Time Rang	pe
nit 1 Settings					Apply
Init 1 Settings Port	Admin	Priority	Legacy Support	Time Range	Apply
Init 1 Settings Port eth1/0/1	Admin Auto	Priority Low	Legacy Support Disabled	Time Range	Apply Delete Time Rang
Init 1 Settings Port eth 1/0/1 eth 1/0/2	Admin Auto Auto	Priority Low Low	Legacy Support Disabled Disabled	Time Range	Apply Delete Time Range Delete Time Range

図 6-15 PoE Configuration 画面

#### 画面に表示される項目:

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を設定します。
Priority	プルダウンメニューを使ってポートの優先度(Critical、High、Low)を指定します。 ポート優先度はシステムがどのポートに優先的に電力供給を行うかを設定します。優先度には 3 段階あり「Critical」「High」 「Low」で設定できます。
Legacy Support	レガシー PD へのサポートの有効 / 無効を指定します。
Mode	PoE ポートの電力管理モードを選択します。「Auto」か「Never」から指定できます。
Max Wattage	上記「Mode」で「Auto」を選択した場合、本オプションが表示されます。
	チェックボックスにチェックを入れ、自動検出 PD へ供給する最大電力数(W)を指定します。
	数値を指定しない場合は PD のクラスは供給可能な最大の電力で指定されます。「1000mW」から「30000mW」までで指定 可能です。
Time Range	上記「Mode」で「Auto」を選択した場合、本オプションが表示されます。 ポートの PoE 機能を有効にする時間設定を行います。タイムレンジの名前を指定します。ポートは設定したタイムレンジの 時間内のみ給電を行います。

「Delete Description」ボタンをクリックすると入力した概要が削除されます。 「Apply」ボタンをクリックすると設定が更新されます。



IEEE802.3at PD への給電に失敗する場合は、対象の PD デバイスが IEEE802.3at に準拠しているのかを確認するか、対象のポートを 30W に 手動設定してください。

### PD Alive (PD アライブ設定)

PoE PD アライブの表示、設定を行います。「PD アライブ」機能は Ping メカニズムを使用して、応答のない PD や停止した PD への給電を自動で OFF/ON することにより、復旧を図ります。自動で行うため、ネットワーク者の負荷を軽減することが可能となる機能です。

System > PoE > PD Alive の順にクリックし、以下の画面を表示します。

PD Alive	_	_	_	_	_	_	_		_
PD Alive Configu	ration								
Unit	From Port	To Port	PD Alive State	PD IP Add	iress				
1 🗸	eth1/0/1 🔽	eth1/0/1 🔽	Disabled V		· · ·				
Poll Interval (10-3	300)	Retry Count (0	-5)	Waiting Ti	me (30-300)	Action			
30	sec	2		90	sec	Both [	~		Apply
Unit 1 Settings									
Port	PD Ali	ve State	PD IP Add	ress	Poll Interval		Retry Count	Waiting Time	Action
eth1/0/1	Dis	abled	0.0.0.0	)	30		2	90	Both
eth1/0/2	Dis	abled	0.0.0.0	)	30		2	90	Both
eth1/0/3	Dis	abled	0.0.0.0	)	30		2	90	Both

図 6-16 PD Alive 画面

画面に表示される項目:

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を設定します。
PD Alive State	PoE アライブ機能を有効 / 無効にします。
PD IP Address	PD の IPv4 アドレスを指定します。
Poll Interval	ポールインターバル(10-300 秒)を指定します。指定の PD の状況を確認する Ping 送信の間隔になります。
Retry Count	リトライカウント(再試行回数 /0-5)を指定します。指定の PD からの回答がなかった際に Ping を再送信する回数を指定し
	ます。
Waiting Time	待機時間(30-300 秒)を指定します。指定の PD が再起動から回復するまでスイッチが待つ時間を指定します。
Action	実行する動作を指定します。
	・ Reset - PoE ポートをリセットします。
	・ Notify - 管理者に通知するログとトラップを送信します。
	• Both - 管理者に通知するログとトラップを送信し、PoE ポートをリセットします。

「Apply」ボタンをクリックすると設定が更新されます。

## PoE Statistics (PoE 統計)

PoE の統計情報を表示します。

**System > PoE > PoE Statistics** の順にクリックし、以下の画面を表示します。

PoE Statistics		_	_			_
PoE Statistics Table Unit 1 Unit 1 Settings						Clear All
Port	MPS Absent	Overload	Short	Power Denied	Invalid Signature	
eth1/0/1	0	0	0	0	44	Clear
eth1/0/2	0	0	0	0	46	Clear
eth1/0/3	0	0	0	0	46	Clear
eth1/0/4	0	0	0	0	46	Clear
eth1/0/5	0	0	0	0	133	Clear

図 6-17 PoE Statistics 画面

画面に表示される項目:

項目	説明
Unit	本設定を適用するユニットを選択します。

「Clear All」ボタンをクリックすると全ポートの PoE 統計情報がクリアされます。 「Clear」ボタンをクリックすると対象ポートの PoE 統計情報がクリアされます。

## PoE Measurement (PoE 測定)

PoE の測定情報を表示します。

#### **System > PoE > PoE Measurement** の順にクリックし、以下の画面を表示します。

PoE Measurement				
PoE Measurement Table				
Unit 1				
Unit 1 Settings				
Port	Voltage (V)	Current (mA)	Temperature (C)	Power (W)
eth1/0/1	N/A	N/A	N/A	N/A
eth1/0/2	N/A	N/A	N/A	N/A
eth1/0/3	N/A	N/A	N/A	N/A
eth1/0/4	N/A	N/A	N/A	N/A
eth1/0/5	N/A	N/A	N/A	N/A
eth1/0/6	N/A	N/A	N/A	N/A

図 6-18 PoE Measurement 画面

#### 画面に表示される項目:

項目	説明
Unit	本設定を適用するユニットを選択します。

# PoE LLDP Classification (PoE LLDP 分類表示)

PoE の LLDP 分類情報を表示します。

**System > PoE > PoE LLDP Classification**の順にクリックし、以下の画面を表示します。

PoE LLDP Classification
PoE LLDP Classification Table
Unit 1
Dort eth/10/4
PSF TX information
None
Information from PD
None
Port eth1/0/2
PSE TX information
None
Information from PD
None
Port eth1/0/3
PSE TX information
None
Information from PD
None
Port eth1/0/4
PSE TX Information
None
Information from PD
None

図 6-19 PoE LLDP Classification 画面

画面に表示される項目:

項目	説明
Unit	本設定を適用するユニットを選択します。

# System Log (システムログ構成)

システムログの設定を行います。

## System Log Settings(システムログ設定)

システムログ機能を有効または無効にし、スイッチのフラッシュメモリにスイッチログを保存する方法を選択します。

System > System Log > System Log Settings の順にメニューをクリックし、以下の画面を表示します。

System Log Settings		
Log State		
Log State	Enabled	Apply
Source Interface Settings		
Source Interface State	Enabled	
Туре	VLAN VLAN Interface ID (1-4094)	Apply
Buffer Log Settings		
Buffer Log State	Enabled	
Severity	4(Warnings)	
Discriminator Name	15 chars	
Write Delay (0-65535)	300 sec 🗌 Infinite	Apply
Console Log Settings		
Console Log State	Disabled	
Severity	4(Warnings)	
Discriminator Name	15 chars	Apply
SMTP Log Settings		
SMTP Log State	Disabled	
Severity	4(Warnings)	
Discriminator Name	15 chars	Apply
Monitor Log Settings		
Monitor Log State	Disabled	
Severity	4(Warnings)	
Discriminator Name	15 chars	Apply

図 6-20 System Log Settings 画面

System Log Settings 画面には次の項目があります。

#### Log State(グローバルステート)

項目	説明
Log State	グローバルにシスログを有効/無効に指定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし設定内容を適用してください。

#### Source Interface Settings(ソースインタフェース設定)

項目	説明
Source Interface	ソースインタフェースをグローバルに有効/無効に指定します。
State	
Туре	インタフェースの種類を選択します。
Interface ID	インタフェース ID を指定します。ループバックインタフェースの場合、「1」から「8」、
	管理インタフェース(Mgmt)の場合、常に「0」、VLAN インタフェースの場合、「1」から「4094」になります。

設定を変更する際は、必ず「Apply」ボタンをクリックし設定内容を適用してください。

### Buffer Log Settings(バッファログ設定)

項目	説明
Buffer Log State	「Enable」「Disabled」「Default」から選択します。
	「Default」を選択するとバッファログのグローバルステートは初期設定のまま動作します。
Severity	ログされる情報のレベルをプルダウンメニューから選択します。「0:Emergencies」(緊急)、「1:Alerts」(警告)、「2:Critical」(重 大)、「3:Errors」(エラー)、「4:Warnings」(警告)、「5:Notifications」(通知)、「6:Informational」(情報)、「7:Debugging」(デ バッグ)から選択します。
Discriminator	ディスクリミネーターの名前を入力します。15 字以内に指定できます。
Name	
Write Delay	フラッシュにロギングバッファを定期的に書き込む間隔を指定します。0 から 65535(秒)の間で指定できます。 初期値は 300 秒です。「Infinite」にチェックを入れると本機能は無効になります。

設定を変更する際は、必ず「Apply」ボタンをクリックし設定内容を適用してください。

#### Console Log Settings(コンソールログ設定)

項目	説明
Console Log	コンソールログのグローバルステートを有効 / 無効にします。
State	
Severity	ログされる情報のレベルをプルダウンメニューから選択します。「1:Emergencies」(緊急)、「2:Alerts」(警告)、「3:Critical」(重
	大)、「4:Errors」(エラー)、「4:Warnings」(警告)、「5:Notifications」(通知)、「6:Informational」(情報)、「7:Debugging」(デ
	バッグ)から選択します。
Discriminator	ディスクリミネーターの名前を入力します。15 字以内に指定できます。
Name	

設定を変更する際は、必ず「Apply」ボタンをクリックし設定内容を適用してください。

#### SMTP Log Settings(SMTP ログ設定)

項目	説明
SMTP Log	SMTP ログのグローバルステートを有効 / 無効にします。
State	
Severity	ログされる情報のレベルをプルダウンメニューから選択します。「1:Emergencies」(緊急)、「2:Alerts」(警告)、「3:Critical」(重 大)、「4:Errors」(エラー)、「4:Warnings」(警告)、「5:Notifications」(通知)、「6:Informational」(情報)、「7:Debugging」(デ バッグ)から選択します。
Discriminator Name	ディスクリミネーターの名前を入力します。15 字以内に指定できます。

設定を変更する際は、必ず「Apply」ボタンをクリックし設定内容を適用してください。

#### Monitor Log Settings(SMTP ログ設定)

項目	説明
Monitor Log State	モニタログのグローバルステートを有効/無効にします。
Severity	ログされる情報のレベルをプルダウンメニューから選択します。「1:Emergencies」(緊急)、「2:Alerts」(警告)、「3:Critical」(重 大)、「4:Errors」(エラー)、「4:Warnings」(警告)、「5:Notifications」(通知)、「6:Informational」(情報)、「7:Debugging」(デ バッグ)から選択します。
Discriminator Name	ディスクリミネーターの名前を入力します。15 字以内に指定できます。

設定を変更する際は、必ず「Apply」ボタンをクリックし設定内容を適用してください。

# System Log Discriminator Settings(システムログディスクリミネーター設定)

システムログディスクリミネーターの設定、設定内容の表示を行います。

System > System Log > System Log Discriminator Settings の順にクリックし、以下の画面を表示します。

iscriminator Name	15 chars				
ction	Drops 🗸				
	SYS	STACKING	PORT	VPLS	
	STP	LAC	VOICE_VL	LLDP	
	PORTSEC	WAC	DHCP	DHCPV6	
	STORM_CT	SSH	CLI	WEB	
	SNMP	OSPF	BGP	VRRP	
	CFM	ALARM	ERPS	DDM	
	AAA	DoS	DEVICE	DAI	
	MPLS	LDP	L2VPN	SURVEILL	
	RADIUS	DOT1X	POE	LBD	
	BPDU_PRO	MAC	SAFEGUAR	DULD	
	RIPNG	CFG	FIRMWARE	REBOOT_S	
	OAM	SRM	IPV6	AUTO_SAV	
	SDMGMT	IPSG	DNSRESOV	OSPFv3	
	ZONEDEFE	IPV6SG	MLAG	OPENFLOW	
everity	Drops 🗸				
	0(Emergencies)	1(Alerts)	2(Critical)		
	3(Errors)	4(Warnings)	5(Notifications)		Apply
	6(Informational)	7(Debugging)			7,664
otal Entries: 0					

図 6-21 System Log Discriminator Settings 画面

#### 画面に表示される項目:

項目	説明
Discriminator	ディスクリミネーターの名前を入力します。15 字以内に指定できます。
Facility	機能が実行する動作内容と選択した動作に関連する機能の種類を選択します。「Drops」「Includes」から選択します。
Severity	ログされる情報のレベルをプルダウンメニューから選択します。「1:Emergencies」(緊急)、「2:Alerts」(警告)、「3: Critical」(重大)、「4:Errors」(エラー)、「4:Warnings」(警告)、「5:Notifications」(通知)、「6:Informational」(情報)、 「7:Debugging」(デバッグ)から選択します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。 「Delete」ボタンをクリックすると指定のエントリが削除されます。

# System Log Server Settings(システムログサーバの設定)

システムログはイベントの記録と管理、エラーと情報のメッセージをレポートします。イベントメッセージは、すべてのエラーレポートに Syslog プロトコルの推奨する固有のフォーマットを使用します。例えば、Syslog とローカルデバイスのレポートメッセージはその重要度や、メッセージを 生成するアプリケーションを識別するためのメッセージ識別名を含みます。メッセージは緊急度かその関連する事項に基づいてフィルタされます。 各メッセージの重要度によって、イベントメッセージの送信先となるイベントを記録するデバイスを決めることができます。

本スイッチは指定した4台までの Syslog サーバに Syslog メッセージを送信できます。

#### System > System Log > System Log Server Settings の順にクリックし、以下の画面を表示します。

System Log Server Settir	ngs		_		_	_
Log Server						
Host IPv4 Address	· · · · · ·	01	lost IPv6 Address	2013::1		
UDP Port (514,1024-65535)	514	Severity		4(Warnings)		
Facility	23 🗸	Discriminator Name		15 chars		
VRF Name	12 chars					Apply
Total Entries: 1						
Server IP	VRF Name	Severity	Facility	Discriminator Name	UDP Port	
192.168.70.1		Warnings	23	Discrimina	514	Delete

図 6-22 System Log Server Settings 画面

#### 画面に表示される項目:

項目	説明			
Host IPv4 Address	ログを記録するサーバの IPv4 アドレスを設定します。			
Host IPv6 Address	ログを記録するサーバの IPv6 アドレスを設定します。			
UDP Port				
	値は「514」、ま	たは「1024」から「65	535」で指定します。	
Severity	ログされる情報の		メニューから選択します。「1:Emergencie	es」(緊急)、「2:Alerts」(警告)、「3:
	Critical」(重大)、	$\lceil 4: \text{Errors} \mid ( \pm \neg - ) \rceil$	、「4:Warnings」(警告)、「5:Notification	ns」(诵知)、「6:Informational」(情報)、
	[7: Debugging	(デバッグ)から選択	、 ・ ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	
Facility	プルダウンメニュ	ューを使用して「0」か	、	
	Facility 値	Facility 名	Facility 概要	
	0	kern	カーネルメッセージ	
	1	user	ユーザレベルメッセージ	
	2	mail	メールシステム	
	3	daemon	システム daemon	
	4	auth1	セキュリティ / 権限メッセージ 1	
	5	syslog	Syslog により内部生成されたメッセージ	
	6	lpr	ラインプリンタサブシステム	
	7	news	ネットワークニュースサブシステム	
	8	uucp	UUCP サブシステム	
	9	clock1	クロック daemon 1	
	10	auth2	セキュリティ / 権限メッセージ2	
	11	ftp	FTP daemon	
	12	ntp	NTP サブシステム	
	13	logaudit	<u>ログ検査</u>	
	14	logalert	<u>ログ警告</u>	
	15	clock2	クロック daemon 2	
	16	local0	ローカル使用 0(local0)	
	17	local1	ローカル使用 1(local1)	
	18	local2	ローカル使用 2(local2)	
	19	local3	ローカル使用 3(local3)	
	20	local4	ローカル使用 4(local4)	
	21	local5	ローカル使用 5(local5)	
	22	local6	ローカル使用 6(local6)	
	23	local7	ローカル使用 7(local7)	
Discriminator	ディスクリミネ-	-ターの名前を入力しき	ます。15 字以内に指定できます。	
VRF Name	VRF インスタンス	へ名を指定します。12	字以内に指定できます。	

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。 「Delete」ボタンをクリックすると指定のエントリが削除されます。

## System Log(Syslog ログ)

スイッチの管理エージェントでまとめたローカルなヒストリログの表示および削除を行います。

System > System Log > System Log の順にメニューをクリックし、以下の画面を表示します。

m Log			Clear Log
al Entries: 5			
Index	Time	Level	Log Description
5	2015-12-28 11:13:05	CRIT(2)	Stacking topology is
4	2015-12-28 11:13:05	CRIT(2)	Unit 1, System start
3	2015-12-28 11:13:05	CRIT(2)	Unit 1, System warm
2	2015-12-28 11:01:01	CRIT(2)	System started up
1	2015-12-28 11:01:01	CRIT(2)	System warm start

図 6-23 System Log 画面

スイッチは自身のログにイベント情報を記録できます。「Go」ボタンをクリックすると、「System Log」画面の次のページへ移動します。 「Clear Log」ボタンをクリックして、表示画面内のすべてのエントリをクリアします。

## System Attack Log(システムアタックログ)

攻撃を受けたシステムログの閲覧/消去を行います。

System > System Log > System Attack Log の順にクリックし、以下の画面を表示します。

System Attack Log		
System Attack Log		
Unit 1 🔽		Clear Attack Log
Unit 1 Settings		
Total Entries: 0		
Index Time	Level	Log Description

図 6-24 System Attack Log 画面

画面に表示される項目:

項目	説明		
Unit	本設定を適用するユニットを選択します。		

「Clear Attack Log」ボタンをクリックして、表示画面内のすべてのエントリをクリアします。

# Time and SNTP(時刻設定)

#### System > Time and SNTP

SNTP (Simple Network Time Protocol) は、コンピュータのクロックにスイッチを同期させるために使用されます。

### Clock Settings(時間設定)

スイッチに時刻を設定します。

System > Time and SNTP > Clock Settings の順にクリックし、以下の画面を表示します。

Time Settings		() Safeguard
Set Current Time Date (DD / MM / YYYY) Time (HH: MM: SS)	31/07/2011 13:45:26	
		Apply

図 6-25 Time Settings 画面

画面に表示される項目:

項目	説明			
Date (DD/MM/YYYY)	システムクロックの更新を行うために現在の年月日を入力します。項目のフォーマットは日 / 月 / 年です。			
Time (HH:MM:SS)	現在のシステム時刻を時 : 分 : 秒(24 時間制)で設定します。例えば午後 9 時であれば 21:00:00 と指定します。			
「Apply」ボタンをクリックし、設定を適用します。				

### Time Zone Settings(タイムゾーン設定)

以下の画面では、SNTP 用のタイムゾーンとサマータイム(Daylight Saving Time)の設定を行います。

#### System > Time and SNTP > Time Zone Settings の順にメニューをクリックし、以下の設定画面を表示します。

mmer Time State	Disabled 🗸
lime Zone	+ • 0 • 0 •
Recurring Setting	
From: Week of the Month	Last
From: Day of the Week	Sun 🗸
From: Month	Jan 🗸
From: Time (HH:MM)	
To: Week of the Month	Last
To: Day of the Week	Sun 🗸
To: Month	Jan 🗸
To: Time (HH:MM)	
Offset	60
Date Setting	
From: Date of the Month	01 🗸
From: Month	Jan 🗸
From: Year	
From: Time (HH:MM)	
To: Date of the Month	01 🗸
To: Month	Jan 🗸
To: Year	
To: Time (HH:MM)	
Offset	60

図 6-26 Time Zone Settings 画面

表示される項目:

項目	説明	
Summer Time State	デバイスに設定するサマータイムの種類を設定します。	
	・ Disabled - サマータイムを無効にします。(初期値)	
	• Recurring Setting - サマータイムを周期的に有効にします。このオプションでは開始と終了のタイミ	
	ングを指定月の指定週で設定する必要があります。	
	Date Setting - サマータイムを日付指定で有効にします。このオプションでは開始と終了の日付を設	
	定する必要があります。	
Time Zone	UTC からのタイムゾーンを選択します。	
	Recurring Setting	
Recurring Setting モードを使用すると、サ	マータイムの設定を指定した期間で自動的に調整できるようになります。例えば、サマータイムを4月	
	1曜日よぐと指走りることかぐさより。	
From: Week Of The Month	月の弟何週から DSI か始まるかを設定します。	
	<ul> <li>FIRSE - 月の取初の週に設定しより。</li> <li>Second 日の2番日の週に記字します</li> </ul>	
	<ul> <li>Second - 月の2番日の週に設定します。</li> <li>Third 日の2番日の週に設定します。</li> </ul>	
	<ul> <li>Initid - 月の3番目の週に設定します。</li> <li>Fourth - 日の4番目の週に設定します。</li> </ul>	
From: Day Of Wook		
FIOITI. Day OF Week	リマータイムが開始する唯口を以下がつ相定します。 Sup Mon Tue Web Thurs Fri Sat	
From: Month	サマータイトが開始する日を以下から指定します	
	Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov. Dec	
From: Time (HH·MM)	サマータイムが開始する時間を指定します。	
To: Week Of The Month	日の筆何调でサマータイムが終わるかを設定します。	
	・ First - 月の最初の调に設定します。	
	<ul> <li>Second - 月の2番目の调に設定します。</li> </ul>	
	<ul> <li>Third - 月の3番目の週に設定します。</li> </ul>	
	<ul> <li>Fourth - 月の4番目の週に設定します。</li> </ul>	
To: Day Of Week	サマータイムが終了する曜日を指定します。	
To: Month	サマータイムが終了する月を指定します。	
To: Time (HH:MM)	サマータイムが終了する時間を指定します。	
Offset	サマータイムに追加する時間を以下から指定します。	
	ГЗОЈ Г6ОЈ Г9ОЈ Г12ОЈ	
	初期値:60(分)	
	Date Setting	
From: Date of the Month	サマータイムが始まる月日を指定します。	
From: Month	サマータイムが開始する月を指定します。(毎年)	
From: Day	サマータイムが開始する日を指定します。(毎年)	
From: Time (HH:MM)	サマータイムが開始する時間を指定します。(毎年)	
To: Date of the Month	サマータイムが修了する月日を指定します。	
To: Month	サマータイムが終了する月を指定します。(毎年)	
To: Day	サマータイムが終了する日を指定します。(毎年)	
To: Time (HH:MM)	サマータイムが終了する時間を指定します。(毎年)	
Offset	サマータイムに追加する時間を以下から指定します。	
	ГЗОJ Г60J Г90J Г120J	
	初期値:60(分)	

# SNTP Settings(SNTP 設定)

SNTP(Simple Network Time Protocol )はインターネット経由でコンピュータのクロックに同期するプロトコルです。標準時と周波数標準サービス へのアクセス、サーバとクライアントの SNTP サブネットの体系付け、および各関連機器のシステムクロックの調整を行う包括的なメカニズムを提 供します。

System > Time and SNTP > SNTP Settings の順にクリックし、以下の画面を表示します。

SNTP Settings		_		
SNTP Global Settings Current Time Source SNTP State Poll Interval (30-99999)	System Clock Disabled 220 720	Sec		Apply
SNTP Server Setting IPv4 Address VRF Name	12 chars	] (	) IPv6 Address	2013::1
Total Entries: 1				
SNTP server	Stratum	Version	Last Receive	
192.168.70.1		-		Delete

図 6-27 SNTP Settings 画面

画面に表示される項目:

項目	説明		
	SNTP Global Settings		
Current Time Source	現在の日付と時刻の提供元を表示します。		
SNTP State	SNTP を「Enabled」(有効)または「Disabled」(無効)にします。初期値は「Disabled」です。		
Poll Interval	同期する間隔(秒)を指定します。		
	「30」から「99999」(秒)で指定します。 初期値は「720 秒」です。		
SNTP Server Settings			
IPv4 Address	SNTP 情報の取得元であるサーバの IP アドレスを設定します。		
IPv6 Address	SNTP 情報の取得元であるサーバの IPv6 アドレスを設定します。		
VRF Name	VRF インスタンス名を指定します。12 字以内に指定できます。		

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

「Add」をクリックして SNTP サーバを追加します。

「Delete」をクリックして指定のエントリを削除します。

# Time Range (タイムレンジ設定)

スイッチのタイムレンジを設定します。

System > Time Range の順にメニューをクリックし、以下の画面を表示します。

lime Range	_	_	_	_	_	_
Time Range						
Danga Nama	22 shore	Daily				
Range Name	32 chars			2.4		
From: Week	Sun	~	To: Week	Sun	End Weekday	
From: Time (HH:MM)	00 🔽 00	~	To: Time (HH:MM)	00 🗸 0	0 🗸	Apply
Range Name	32 chars					Find
Total Entries: 1						
Range Name	Start Weekday	Start Time	End Weekday	End Time		
Weekdays	Mon	00:00	Fri	23:59	Delete Periodic	Delete
					1/1 < < 1	> > Go

図 6-28 Time Range 画面

画面に表示される項目:

項目	説明
Range Name	タイムレンジを識別するために使用する名前を半角英数字 32 文字以内で入力します。
From Week /	タイムレンジに使用する「始まり」と「終わり」の曜日を指定します。
To Week	「Daily」にチェックを入れると「毎日」がタイムレンジとして指定されます。
	「End Week Day」にチェックを入れると「始まり」に指定された日から週の最後(日曜日)までがタイムレンジになります。
From Time / To Time	タイムレンジに使用する「始まり」と「終わり」の時間を指定します。ドロップダウンメニューから時間と分を指定します。

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。 設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。 関連情報を入力して「Find」ボタンをクリックすると指定のエントリを検索できます。

#### エントリの削除

削除するエントリ横の「Delete」ボタンをクリックすると該当エントリは削除されます。 削除するエントリ横の「Delete Periodic」ボタンをクリックすると定期エントリは削除されます。

# PTP (PTP 設定)

#### System > PTP

PTP(Precision Time Protocol:高精度時刻同期方式)システムは、イーサネットネットワークを通して1マイクロ秒未満の精度で配信されるクロックに同期することができます。

PTP は、システムにおいて正確なクロックの同期を可能にする技術です。PTP はイーサネットおよび UDP を含むマルチキャストメッセージ送信をサ ポートするローカルエリアネットワークで通信するシステムに適切です。PTP により、様々な固有の精度、解像度、および安定性のクロックを含む 異種システムはグランドマスタクロックへ同期が可能となります。

同期は2つの処理に分けられます。ベストマスタクロック(BMC: Best Master Clock)アルゴリズムは、すべてのローカルポートの PTP 状態(マス タ/スレーブ)を決定します。同期アルゴリズムはマスタとスレーブクロック間のクロックオフセットを計算します。イベントメッセージの伝搬時 間を計算するために、2つのメカニズム(Delay Request-response Mechanism および Peer Delay Mechanism)があります。

PTP システムには、3 つ PTP デバイスタイプ(境界クロック、エンドツーエンド透過クロック、およびピアツーピア透過クロック)があります。境界クロックのみベストマスタクロックの選択に参加できます。

スタックモードが有効で、トランクグループのメンバポートが複数のスタックユニットに存在する場合、PTP 機能は、

- ・同じスタックユニットのメンバポートへの PTP メッセージの送受信時に通常通り動作します。
- ・違うスタックユニットのメンバポートへの PTP メッセージの送受信時は正常に動作しません。

注意 PTP 機能は、単体利用の場合のみサポートしている機能です。スタック構成時にはご使用になれませんのでご注意ください。

#### PTP Global Settings (PTP グローバル設定)

PTP 機能をグローバルに設定します。

System > PTP > PTP (	Global Settings	の順にメニューをク	フリックし、	以下の画面を表示します。
----------------------	-----------------	-----------	--------	--------------

PTP Global Settings		
PTP Global Settings		
PTP State	Disabled	
PTP Mode	E2E Transparent 🔽	
PTP Transport Protocol	UDP 🔽	Apply
PTP Clock Domain Settings		
PTP Clock Domain Number (0-127)	0	
PTP Clock Domain Name	32 chars	Apply
PTP Boundary Clock Settings		
Priority 1 (0-255)		
Priority 2 (0-255)		Apply

図 6-29 PTP Global Settings 画面
画面に表示される項目:

説明
PTP Global Settings
プルダウンメニューを使用して、PTP 状態を「Enabled」( 有効 )/「Disabled」( 無効 ) にします。
スイッチの PTP タイプを選択します。スイッチには、3 つ PTP デバイスタイプ、「Boundary」(境界)、「P2P Transparent」(ピ
アツービア透過)、およびTE2E Transparent」(エンドツーエンド透過)があります。初期値は「E2E Transparent」です。
通信パスに使用する送信プロトコルを「Ethernet」「UDP」から選択します。初期値は UDP です。
PTP Clock Domain Settings
本設定を適用するユニットを選択します。
ローカルクロックのドメイン属性を入力します。すべての PTP メッセージ、データセット、ステートマシン、およびそ
の他すべての PTP エンティティがいつも特定のドメイン番号に関連付けられます。範囲は 0-127 です。初期値は 0 です。
指定したドメイン番号に対してドメイン名を入力します。
PTP Boundary Clock Settings
PTP 境界クロックの「Priority 1」を指定します。「Priority 1」の属性は「Best Master Clock(BMC)」アルゴリズムの実
行に使用されます。低い値ほど優先値は高くなります。「0」が最優先になります。0 から 255 の間で指定します。
PTP 境界クロックの「Priority 2」を指定します。「Priority 2」の属性は「Best Master Clock(BMC)」アルゴリズムの実
行に使用されます。「Priority 1」を基準にした BMC アルゴリズムの失敗にともない、「Priority 2」の属性が採用されます。
低い値ほど優先値は高くなります。「0」が最優先になります。0から255の間で指定します。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

## PTP Port Global Settings(PTP ポートグローバル設定)

PTP の状態をポートごとに設定します。

System > PTP > PTP Port Global Settings の順にメニューをクリックし、以下の画面を表示します。

PTP Port Globa	PTP Port Global Settings				
PTP Port Global Se	ttings				
From Port	To Port	State			
eth1/0/1 🔽	eth1/0/1 🔽	Disabled 🔽		Apply	
	Port		State		
eth1/0/1			Disabled		
eth1/0/2			Disabled		
	eth1/0/3		Disabled		

図 6-30 PTP Port Global Settings 画面

画面に表示される項目:

項目	説明
From Port / To Port	この設定に使用するポート範囲を選択します。
State	プルダウンメニューを使用して、指定ポートの PTP 状態を「Enabled」( 有効 )/「Disabled」( 無効 ) にします。

「Apply」ボタンをクリックして行った変更を適用します。

## PTP Boundary Port Settings(PTP 境界ポート設定)

PTP 境界クロックの属性を設定します。PTP デバイスが境界タイプである場合に、本設定は機能します。

**System > PTP > PTP Boundary Port Settings** の順にメニューをクリックし、以下の画面を表示します。

PTP Boundary Port	Settings	_		_	_	_	_
PTP Boundary Port Setting	gs						
From Port	To Port	Announce	Interval (1-16)	Announce Recei	pt Timeout (2-10)		
eth1/0/1 🔽	eth1/0/1 🔽	2	sec	3	]		
Delay Mechanism	Delay Request Interval (0-5)	Pdelay Re	quest Interval (1-32)	Synchronization	Interval (1-2)		
E2E 🔽	0	1	sec	1	sec 🗌 Half Second	Apply	
Note: DM: Delay Mechanism; AI: Announce Interval; CART: The Coefficient of Announce Receipt Timeout; SI: Synchronization Interval; EDRI: The Exponent of Delay Request Interval; PDRI: Pdelay Request Interval The Announce Interval value and Pdelay Request Interval value are represented as the logarithm to the base 2. The Delay Request Interval value is an exponent of 2.							
Port	DM	AI	CART	SI	EDRI	PDRI	
eth1/0/1	F2F	2	3	1 00	0	1	

図 6-31 PTP Boundary Port Settings 画面

画面に表示される項目:

項目	説明
From Port / To Port	この設定に使用するポート範囲を選択します。
Announce Interval (1-16)	ラジオボタンをクリックし、連続するアナウンスメッセージ間の平均時間を入力します。アナウンス間隔とし
	て参照されます。IEEE 1588 プロトコルに従い、アナウンス間隔の値は底を 2 とする測定時間 (秒) の対数とし
	て表示されます。入力値は1、2、4、8、または16とします。無効な数字が入力されると、それより大きくて最
	も近い値に自動的に調整されます。初期値は2(秒)です。
Announce Receipt Timeout (2-10)	ラジオボタンをクリックして、ANNOUNCE_RECEIPT_TIMEOUT_EXPIRES イベントの発生前にアナウンスメッ
	セージを受信せずに通過すべきアナウンス間隔を入力します。アナウンス間隔値の乗数は、アナウンス受信の
	タイムアウトの間隔に一致します。範囲は 2-10 です。
Delay Mechanism	プルダウンメニューを使用して、イベントメッセージの伝搬遅延時間を測定するメカニズムを指定します。
	・ E2E - ポートは Delay Request-response Mechanism を使用します。(初期値)
	・ P2P - Peer Delay Mechanism を使用します。
Delay Request Interval (0-5)	スレーブがマスタ上の指定ポートに送信する連続する遅延要求メッセージの許容される間隔の平均を入力しま
	す。この間隔の平均は、マスタによって決定されて、通知されます。
Pdelay Request Interval (1-32)	連続する Pdelay_Request メッセージの許容される間隔の平均を入力します。
Synchronization Interval (1-2)	同期間隔を入力します。同期成功メッセージの平均時間間隔となります。IEEE 1588 プロトコル標準において、
	本値は、同期間隔の2を底とする対数とされています。1-2秒の間で指定します。「Half Second」オプション
	にチェックを入れると、0.5 秒に設定されます。

「Apply」ボタンをクリックして行った変更を適用します。

### PTP P2P Transparent Port Settings (PTP P2P 透過ポート設定)

P2P 透過クロックの Pdelay Request Interval を設定します。

System > PTP (Precise Time Protocol) > PTP P2P Transparent Port Settings の順にメニューをクリックし、以下の画面を表示します。

PTP P2P Transparent Port S	ettings	
PTP P2P Transparent Port Settings		
From Port To Port eth1/0/1  eth1/0/1	P2P Transparent Pdelay Request Interval (1-32)  1 Apply	
Port	P2P Transparent Pdelay Request Interval	
eth1/0/1	1	
eth1/0/2	1	
eth1/0/3	1	
eth1/0/4	1	
eth1/0/5	1	
eth1/0/6	1	

図 6-32 PTP Peer to Peer Transparent Port Settings 画面

画面に表示される項目:

項目	説明	
From Port / To Port	この設定に使用するポート範囲を選択します。	
P2P Transparent Pdelay Request	連続する Pdelay_Request メッセージの許容される間隔の平均を入力します。	
Interval (1-32)		
「Apply」ボタンをクリックして行った変更を適用します。		

### PTP Clock Information (PTP クロック情報の表示)

PTP クロックのアクティブな属性を表示します。 PTP の状態が「PTP Global Settings」画面で無効にされると、PTP クロック ID は「00000000000000000」と表示されます。 表示するユニットを指定します。

System > PTP > PTP Clock Information の順にメニューをクリックし、以下の画面を表示します。

PTP Clock Information			
PTP Clock Information			
DTD Baundamy Clask Information			
P IP Boundary Clock Information			
PTP State	Disabled		
PTP Clock Mode	End-to-End Transparent Clock		
PTP Transport Protocol	UDP		
PTP Clock Domain Number	0		
PTP Clock Domain Name			
PTP Clock Identity	0000000000000		
PTP Clock Class	-		
PTP Steps Removed			
PTP Last Offset	-		
PTP Mean Path Delay	-		
PTP Enabled Ports			
PTP Clock Parent Information			
PTP Parent Port Identity	-		
PTP Parent Port Number			
PTP Grandmaster Identity	-		
PTP Grandmaster Clock Class			
PTP Grandmaster Clock Accuracy			
PTP Grandmaster Priority 1			
PTP Grandmaster Priority 2	-		

図 6-33 PTP Clock Information 画面

### PTP Port Information (PTP ポート情報)

スイッチにおいて特別である PTP ポートのアクティブな属性を表示します。表示するユニットを指定します。

System > PTP > PTP Port Information の順にメニューをクリックし、以下の画面を表示します。

TP Port Informa	tion	_	-	_	_	_	_	_	_	_
TP Port Information										
Note: DM: Delay Me	chanism; AI: Announ	e Interval;	ART:	Announce	Receipt Tin	neout; <b>SI</b> : Syr	chronization	Interval; <b>DR</b>	I <b>M</b> : Delay_Req	uest Interval-Master;
DRIS: Delay_I	Request Interval-Slav	e; <b>PDRI</b> : P	delay	Request In	terval; PMP	D: Peer Mear	n Path Delay			
Port	Role	DM	AI	ART	SI	DRIM	DRIS	PDRI	PMPD	State
eth1/0/1	Disabled	E2E	2	0	1.00	1	0	1	0	Disabled
eth1/0/2	Disabled	E2E	2	0	1.00	1	0	1	0	Disabled
eth1/0/3	Disabled	E2E	2	0	1.00	1	0	1	0	Disabled
eth1/0/4	Disabled	E2E	2	0	1.00	1	0	1	0	Disabled
eth1/0/5	Disabled	E2E	2	0	1.00	1	0	1	0	Disabled
eth1/0/6	Disabled	E2E	2	0	1.00	1	0	1	0	Disabled
eth1/0/7	Disabled	E2E	2	0	1.00	1	0	1	0	Disabled
eth1/0/8	Disabled	E2E	2	0	1.00	1	0	1	0	Disabled
eth1/0/9	Disabled	E2E	2	0	1.00	1	0	1	0	Disabled

図 6-34 PTP Port Information 画面

### PTP Foreign Master Records Port Information (PTP 外部マスタレコードのポート情報)

境界クロックの特定ポートにおける現在の外部マスタレコードを表示します。表示するユニットを指定します。

**System > PTP > PTP Foreign Master Records Port Information**の順にメニューをクリックし、以下の画面を表示します:

PTP Foreign	PTP Foreign Master Records Port Information				
PTP Foreign Ma	PTP Foreign Master Records Port Information				
Note: FM Port FM Port FM Ann	Note:       FM Port Identity: The identity of the Foreign Master Port;         FM Port Number:       The port number of the Foreign Master Port;         FM Announce Messages:       The number of Foreign Master announce messages.				
Port	Port FM Port Identity FM Port Number FM Announce Messages				

図 6-35 PTP Foreign Master Records Port Information 画面

## USB Console Settings (USB コンソール設定)

USB コンソールの設定、表示を行います。

System > USB Console Settings の順にメニューをクリックし、以下の画面を表示します:

USB Console Settings			
USB Console Settings			
USB Console State	<ul> <li>Enabled          <ul> <li>Disabled</li> </ul> </li> </ul>		
USB Inactivity Timeout (1-240)	min	Active	Apply

図 6-36 USB Console Settings 画面

画面に表示される項目:

項目	説明
USB Console State	USB コンソールを有効 / 無効にします。
USB Inactivity Timeout	USB タイムアウトについて設定します。1-240(秒)の範囲で指定可能です。USB コンソールが無動作の状態 が指定の秒数を過ぎるとタイムアウトします。「Active」を選択するとタイムアウトすることはありません。
E	

「Apply」ボタンをクリックして行った変更を適用します。

注意 アクティブなコンソール接続が RJ-45、mini-USB の両方で構築されている場合、mini-USB コンソールの方により高い優先値があります。

### SRM(Switch Resource Management 設定)

#### System > SRM

「Switch Resource Management」(SRM)機能はアプリケーションによって必要な大規模なリソースを最適化します。これにより、より多くのエントリに必要なテーブルの提供や、不使用の機能によるリソースの消費などを抑えることなどにより、フレキシブルなリソース設定が提供されます。

#### SRM Prefer Current Settings(SRM 最適化設定)

SRM の設定、表示を行います。本画面は、スイッチにおける頻繁に使用する機能リソースの最適化を行う SRM モードの指定を行います。

#### System > SRM > SRM Prefer Current Settings の順にメニューをクリックし、以下の画面を表示します。

RM Prefer Current Se	ettings	
RM Prefer Current Settings		
SRM Prefer Mode	● LAN ○ IP ○ L2VPN	Apply
Total Entries: 1		
Unit	Current Mode	Configured Mode
4	IP	IP

図 6-37 SRM Prefer Current Settings 画面

画面に表示される項目:

項目	説明
SRM Prefer Mode	SRM モードの選択を行います。
	・ LAN - スイッチを「LAN スイッチ」モードとして指定します。
	・ IP - スイッチを「IP ルート」モードとして指定します。
	・ L2VPN - スイッチを「L2VPN」モードとして指定します。

「Apply」ボタンをクリックして行った変更を適用します。



【注意】 スイッチが物理スタックされている場合、スタック内すべてのスイッチが同じ SRM モードで設定されている必要があります。

### SRM Prefer Mode(SRM 設定モード)

SRM の設定モードの表示を行います。テーブル内の各機能の最大エントリ値を示す値などが表示されます。

System > SRM > SRM Prefer Mode の順にメニューをクリックし、以下の画面を表示します。

SRM Prefer Mode		
SRM Prefer Mode		
SRM Prefer Mode	● LAN ○ IP ○ L2VPN	Find
SRM Prefer Mode Detail		
L2 Forwarding Table Size		68K
Max number of mac table entries		69632
L3 Host Table /Multicast Size		16K
Max number of ipv4 host entries		16384
Max number of ipv6 host entries		8192
Max number of ipv4 multicast groups	entries	8192
Max number of ipv6 multicast groups	entries	4096
MPLS Table Size		4К
Max number of MPLS entries		2944
Max number of L2VPN entries		1024
Max number of L3VPN entries		127
Ingress VLAN Translate Table Size		4K
Max number of mac based VLAN en	tries	3072
Max number of VLAN translate entrie	35	3072
Max number of I2 tunnel entries		1024
Egress VLAN Translate Table Size		4К
Max number of egress VLAN transla	te entries	3072

図 6-38 SRM Prefer Mode 画面

#### 画面に表示される項目:

項目	説明
SRM Prefer Mode	表示する SRM モードの選択を行います。「LAN」「IP」「L2VPN」から指定します。
 「Find」をクリックして各 SRM モー	ドの設定内容を表示します。

# 第7章 Management (スイッチの管理)

以下は、Management サブメニューの説明です。必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明
Command Logging(コマンドログ設定)	コマンドログ設定を有効にします。コマンドログ出力機能は、コマンドラインインタフェース を通じてスイッチへの設定が成功したコマンドをログに出力するために使用されます。
User Accounts Settings(ユーザアカウント設定)	スイッチはユーザ権限の制御を行うことができます。ユーザパスワードとアクセス権限を含む ユーザアカウントを設定します。
CLI Alias Settings(CLI エイリアス設定)	CLI エイリアスの設定を行います。CLI エイリアスコマンドは指定の CLI コマンドと連携するカ スタムの文字列になります。
Password Encryption(パスワード暗号化)	パスワードを暗号化し設定ファイルに保存します。
Password Recovery (パスワードリカバリ)	パスワードリカバリを行います。例えば管理者がパスワードを忘れた場合に有効です。
Login Method (ログイン方法)	各管理インタフェースでのログイン方法について設定します。
SNMP(SNMP 設定)	SNMP 設定を有効にします。本スイッチシリーズは、SNMP v1、v2c、および v3 をサポートしています。
RMON (RMON 設定)	SNMP 機能に対するリモートモニタリング (RMON) ステータスを有効にします。
Telnet/Web(Telnet/Web 設定)	スイッチに Telnet/Web 設定を有効にします。
Session Timeout(セッションタイムアウト)	各セッション(Web やコンソールなど)のタイムアウトの設定をします。
DHCP(DHCP 設定)	スイッチの DHCP について設定します。
DHCP Auto Configuration(DHCP 自動コンフィグ 設定)	DHCP 自動コンフィグ機能の設定を行います。
DHCP Auto Image Settings(DHCP 自動イメージ 設定)	DHCP 自動イメージ設定を行います。スタートアップ時に、外部サーバからイメージファイル を取得する機能です。
DNS(ドメインネームシステム)	DNS(Domain Name System)は、ドメイン名と IP アドレスの関連付けをコンピュータ間の通 信で行います。
NTP(ネットワークタイムプロトコル)	スイッチの時刻を同期するための NTP プロトコルの設定を行います。
IP Source Interface (IP ソースインタフェース)	IP ソースインタフェースの設定を行います。
File System (ファイルシステム設定)	フラッシュファイルシステムにより、Firmware、Config 情報、および Syslog 情報はフラッシュ 内のファイルに保存されます。
Stacking(スタッキング設定)	物理スタッキングの設定を行います。
Virtual Stacking (SIM)(仮想スタック設定(SIM))	仮想(SIM)スタッキングの設定を行います。
D-Link Discovery Protocol(D-Link ディスカバリ プロトコル)	D-Link ディスカバリプロトコル(DDP)の設定を行います。
SMTP Settings(SMTP 設定)	Simple Mail Transfer Protocol (SMTP) の設定を行います。
Reboot Schedule Settings(再起動スケジュール 設定)	スイッチの再起動スケジュール設定を行います。
NLB FDB Settings (NLB FDB 設定)	ネットワークロードバランシング (NLB) の設定を行います。
SD Card Management (SD カード管理)	USB ドライバストレージなどのリムーバブル機器の設定を行います。

## Command Logging (コマンドログ設定)

コマンドログ設定を有効または無効にします。コマンドログ出力機能は、コマンドラインインタフェースを通じてスイッチへの設定が成功したコマンドをログに出力するために使用されます。システムログには、コマンド及びコマンドを入力したユーザ情報が含まれます。スイッチの設定または 操作で変更を引き起こさないコマンド(例:show)はログに出力されません。「save」コマンドは設定ファイルを変更するため、ログに出力されます。

Management > Command Logging の順にメニューをクリックし、以下の画面を表示します。

Command Logging Settings	O Safeguard
Command Logging Settings Command Logging State O Enabled O Disabled	
図 7-1 Command Logging Settings 画面	

画面に表示される項目:

項目	説明
Command Logging State	ラジオボタンを使用して機能を「Enabled」(有効)/「Disabled」(無効)にします。
設定を変更する場合は、必ず	「Apply」ボタンをクリックし、設定内容を適用してください。

注意 スイッチの再起動中またはダウンロードしたコンフィグレーションの処理実行中は、すべてのコンフィグレーションコマンドがログに出 力されるというわけではありません。または、ユーザが AAA 認証を使用してログインした際、ユーザが権限を取り替えるために「enable admin」コマンドを使用した場合には、ユーザ名を変更するべきではありません。

### User Accounts Settings (ユーザアカウント設定)

スイッチはユーザ権限の制御を行うことができます。ユーザパスワードとアクセス権限を含むユーザアカウントを設定します。以下の手順でユーザ アカウント情報を設定します。

注意 初期値ではユーザアカウントは設定されていません。

Web UI にはいくつかの設定方法が用意されています。いくつかの設定オプションはアカウントの権限レベルにより設定が可能になります。高い権限レベルを有するユーザアカウントはより多くの機能設定へのアクセスを行うことができます。

Management > User Account Settings の順にクリックし、次の画面を表示します。

User Accounts Settings			_
User Management Settings	Session Table		
User Name 32 chars Password Type None	Privilege (1-15) Password		Apply
Total Entries: 1			
User Name	Privilege	Password	
admin	15	*****	Delete
		1/1 < 1	> > Go

図 7-2 User Accounts Settings - User Management Settings 画面

両面にまう	=+++;	2 西口・
回回に衣り	いごうしつ	う泊日・

項目	説明
User Name	ユーザ名を定義します。(半角英数字 32 文字以内)
Privilege	アカウントの権限レベルを指定します。1 から 15 までで設定可能です。
Password Type	アカウントで使用する暗号化の方法を「None」「Plain Text」「Encrypted-SHA1」「Encrypted-MD5」から選択します。
Password	アカウントで使用するパスワードを入力します。

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

#### エントリの削除

削除するエントリ横の「Delete」ボタンをクリックすると該当エントリは削除されます。

### Session Table

「Session Table」タブをクリックするとユーザアカウントの現在の状況が表示されます。

User Accounts Se	ettings				
User Management	Settings Ses	sion Table			
Total Entries: 2					
Туре	User Name	Privilege	Login Time	IP Address	
console	Anonymous	1	5M10S		
* web	Anonymous	15	4M57S	10.90.90.14	Edit
			1/1	< 1 > > Go	

図 7-3 User Accounts Settings - Session Table 画面

#### User Level

```
「Session Table」タブで「Edit」をクリックするとユーザレベル設定が表示されます。
```

User Level			
User Level			
Action	Enabled Obisabled		
Level	15 💌		
Password	35 chars	Apply	Back

図 7-4 User Accounts Settings - User Level 画面

画面に表示される項目:

項目	説明
Action	ユーザレベル設定を「Enabled」(有効)/「Disabled」(無効)に指定します。
Level	ユーザレベル(1-15)を指定します。
Password	パスワード(35 字以内)を指定します。

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。 「Back」ボタンをクリックし、前画面に戻ります。

## CLI Alias Settings (CLI エイリアス設定)

CLIエイリアスの設定を行います。

CLI エイリアスコマンドは指定の CLI コマンドと連携するカスタムの文字列になります。CLI で長文コマンドの繰り返し使用の際に有効です。

Management > CLI Alias Settings の順にクリックし、次の画面を表示します。

CLI Alias Settings			
CLI Alias Settings			
Mode ca-trustpoint 🔽	Alias Command 16 chars	Original Command 128 chars	Apply
Mode ca-trustpoint			Find
Mode	Alias Command	Original Command	
	h	help	Delete
Exec mode	lo	logout	Delete
	р	ping	Delete
	S	show	Delete
			1/1  < < 1 > >  Go

図 7-5 CLI Alias Settings 画面

画面に表示される項目:

項目	説明	
Mode	オリジナルコマンドのコマンドモードを指定します。	
Alias Command	エイリアスコマンドを入力します。16 文字まで入力可能です。	
Original Command	オリジナルコマンドを入力します。128 文字まで入力可能です。	
設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。		

設定を変更する場合は、必ず「Apply」ホタンをクリックし、設定内谷を適用してくたさし 「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

「FINU」小ダノをクリックして、八川した旧報に奉して付走のエノドリを快出します。

削除するエントリ横の「Delete」ボタンをクリックすると該当エントリは削除されます。

## Password Encryption (パスワード暗号化)

パスワードを暗号化して設定ファイルに保存します。

Management > Password Encryption の順にクリックし、次の画面を表示します。

Password Encryption		
Password Encryption Settings		
Password Encryption State	O Enabled   Disabled	
Password Type	Encrypted-SHA1	Apply

図 7-6 Password Encryption 画面

画面に表示される項目:

項目	説明	
Password	パスワードの暗号化のコンフィグファイル保存ついての「Enabled」(有効)/「Disabled」(無効)を設定します。	
Encryption State		
Password Type	パスワード暗号化を有効すると、次のオプションが選択可能です。	
	• Encrypted-SHA1 - 「SHA-1」を使用してパスワード暗号化が可能です。	
	・ Encrypted-MD5 - 「MD-5」を使用してパスワード暗号化が可能です。	

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

## Password Recovery (パスワードリカバリ)

本画面ではパスワードリカバリの設定を行います。例えば管理者がユーザアカウント更新時にパスワードを忘れた場合などに行います。

Management > Password Recovery の順にクリックし、次の画面を表示します。

Password Recovery			
Password Recovery Settings			
Password Recovery State	Enabled	O Disabled	Apply
Running Configuration	Enabled		
NV-RAM Configuration	Enabled		

図 7-7 Password Recovery 画面

画面に表示される項目	:
------------	---

項目	説明
Password Recovery	パスワードリカバリを「Enabled」(有効)/「Disabled」(無効)に指定します。有効にすると CLI でのリセットコンフィグレー
State	ションモードへのアクセスが可能になります。リセットコンフィグモードからユーザアカウントのアップデートが可能で、パ
	スワード機能は管理者権限レベルにアップデートされ、AAA 機能がローカル認証において無効にすることが可能です。実行
	中のコンフィグレーションはスタート時のコンフィグとして保存されます。再起動が必要です。

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

## Login Method (ログイン方法)

各管理インタフェースでのログイン方法について表示、設定します。

Management > Login Method の順にクリックし、次の画面を表示します。

Login Method			
Enable Password			
Level 15 Password	Level 15 Password Type Plain Text Password 32 chars Apply		
Login Method			
Application	Login Method		
Console	No Login	Edit	
Telnet	Login	Edit	
SSH	Login	Edit	
Login Password       Application     Console     Password Type     Plain Text     Password     32 chars     Apply			
Application	Password		
SSH	*****	Delete	

図 7-8 Login Method 画面

画面に表示される項目:

項目	説明		
	Enable Password		
Level	ユーザの権限レベルを指定します。1から15の間で指定可能です。		
Password Type	暗号化の方法を「Plain Text」「Encrypted」「Encrypted-MD5」から選択します。		
Password	選択したアプリケーションで使用するパスワードを入力します。 指定のアプリケーションのログイン方法が「Login」に設定されている時のパスワードになります。入力するパスワードのルー ルは、暗号化の方法によって異なります。 ・「Plain Text」選択時:32文字以内(大文字と小文字を区別、スペースを含める) ・「Encrypted」選択時:35 バイト(大文字と小文字を区別) ・「Encrypted-MD5」選択時:31 バイト(大文字と小文字を区別)		
Login Method			
Login Method	「Edit」ボタンをクリックしてパラメータの設定を行います。指定のアプリケーションへのログイン方法を選択します。「No Login」「Login」「Login Local」から選択可能です。「No Login」では指定のアプリケーションへのアクセスに対してユーザ名 入力などの必要がありません。「Login」では指定のアプリケーションへのアクセスにパスワードを入力する必要があります。 「Login Local」はユーザ名とパスワードの入力が必要になります。		
	Login Password		
Application	設定するアプリケーションを選択します。「Console」「Telnet」「SSH」から選択できます。		
Password Type	暗号化の方法を「Plain Text」「Encrypted」「Encrypted-MD5」から選択します。		
Password	選択したアプリケーションで使用するパスワードを入力します。 指定のアプリケーションのログイン方法が「Login」に設定されている時のパスワードになります。入力するパスワードのルー ルは、暗号化の方法によって異なります。 ・「Plain Text」選択時:32文字以内(大文字と小文字を区別、スペースを含める) ・「Encrypted」選択時:35バイト(大文字と小文字を区別) ・「Encrypted-MD5」選択時:31バイト(大文字と小文字を区別)		
「Apply」ボタンをク	7リックし、設定内容を適用してください。		

「Edit」ボタンをクリックすると、設定内容を編集できます。

#### エントリの削除

削除するエントリ横の「Delete」ボタンをクリックすると該当エントリは削除されます。

### SNMP (SNMP 設定)

SNMP(Simple Network Management Protocol)は、OSI 参照モデルの第7層(アプリケーション層)のプロトコルです。ネットワークに接続され た通信機器の管理や監視を行います。

SNMP によって、ネットワーク管理ステーションはゲートウェイやルータなどのネットワークデバイスの設定状態の確認・変更をすることができま す。適切な動作のためにシステム機能を設定、パフォーマンスを監視し、スイッチやスイッチグループおよびネットワークの潜在的な問題を検出し ます。

SNMP をサポートするデバイスは、SNMP エージェントと呼ばれるソフトウェアを実装しています。

定義された変数(管理対象オブジェクト)が SNMP エージェントに保持され、デバイスの管理に使用されます。これらの管理オブジェクトは MIB (Management Information Base)内に定義され、SNMP エージェントにより管理される情報表示の基準を管理ステーションに伝えます。 SNMP は、MIB の仕様フォーマット、およびネットワーク経由で情報にアクセスするために使用するプロトコルの両方を定義しています。

#### ■ SNMP のバージョンについて

SNMP には、「SNMPv1」「SNMPv2c」「SNMPv3」の3つのバージョンがあります。 これらの3つのバージョンでは、ネットワーク管理ステーションとネットワークデバイス間に適用されるセキュリティのレベルが異なります。

注意 本製品がサポートしている SNMP のバージョンは SNMPv1、SNMPv2c、SNMPv3 です。

#### SNMPv1とSNMPv2c

SNMPv1 と SNMPv2c では、SNMP のコミュニティ名を使用して認証を行います。 リモートユーザの SNMP アプリケーションとスイッチの SNMP は同じコミュニティ名を使用する必要があります。認証が行われていない SNMP パ ケットを受信した場合、そのパケットは破棄されます。

SNMPv1と SNMP v2c を使用する場合、初期値のコミュニティ名は以下のとおりです。

- public:管理ステーションは、MIBオブジェクトの読み取りができます。
- ・ private: 管理ステーションは、MIB オブジェクトの読み取りと書き込みができます。

#### SNMPv3

SNMPv3 では、2 つのパートで構成される、より高度な認証を行います。 最初のパートは SNMP マネージャとして動作することのできるユーザとその属性を掲載したリストを保持しています。次のパートではリスト上の ユーザの SNMP マネージャとしての権限を記載しています。

ユーザのグループをリストにまとめ、権限を設定できます。また、リスト上の SNMP マネージャのグループに対して、SNMP バージョン情報を登録 可能です。「SNMPv1 を使用して読み取り専用の情報とトラップの受信のみを可能にするグループ」や、「SNMPv3 を使用して高いセキュリティレベ ルを与え、読み書き可能にするグループ」など、グループごとに異なる設定を登録することができます。

個別のユーザや SNMP マネージャグループに SNMPv3 を使用すると、特定の SNMP 管理機能を許可または制限できるようになります。 管理機能の可否は各 MIB に関連付けられる OID (Object Identifier) を使用して定義します。 SNMPv3 では SNMP メッセージを暗号化することにより、 さらに強固なセキュリティを実現できます。

#### トラップ

トラップは、スイッチ上で発生したイベントをネットワーク管理者に警告するためのメッセージです。

イベントには、再起動(誤ってスイッチの電源を切ってしまった)などの重大なものから、ポートの状態変化を知らせる軽微なものまで幅広い種類 があります。スイッチはトラップを生成し、事前に設定された IP アドレスに送信します。トラップの例には、認証の失敗、トポロジの変化などがあ ります。

#### MIB

MIB (Management Information Base)には、管理情報およびカウンタ情報が格納されています。

本製品は標準 MIB-II モジュールを使用し、MIB オブジェクトの値を SNMP ベースのネットワーク管理ソフトウェアにより取得します。本製品は、標 準 MIB-II に加えて、拡張 MIB としてベンダ固有の MIB もサポートしています。MIB OID の指定によってもベンダ固有の MIB を取得することができます。 MIB の値には「読み取り専用」「読み書き可能」があります。

### SNMP Global Settings(SNMP グローバル設定)

SNMP グローバルステート設定を有効または無効にします。

Management > SNMP > SNMP Global Settings の順にメニューをクリックし、以下の画面を表示します。

SNMP Global Settings	
SNMP Global Settings	
SNMP Global State	O Enabled
SNMP Response Broadcast Request	O Enabled
SNMP UDP Port (1-65535)	161
Trap Source Interface	vian1
Trap Settings	
Trap Global State	O Enabled
SNMP Authentication Trap	
Port Link Up	
Port Link Down	
Coldstart	
Warmstart	Apply

図 7-9 SNMP Global Settings 画面

### 以下の項目が表示されます。

#### SNMP Global Settings(SNMP グローバル設定)

項目	説明
SNMP Global State	SNMP 機能の「Enabled」(有効)/「Disabled」(無効)を選択します。
SNMP Response Broadcast	SNMP GetRequest パケットのブロードキャストに対応するサーバを「Enabled」(有効)/「Disabled」(無効)に指
Request	定します。
SNMP UDP Port	SNMP UDP ポート番号を指定します。
Trap Source Interface	SNMP トラップパケットを送信する送信元アドレスとしての IP アドレスのインタフェースを入力します。

#### Trap Settings(トラップ設定)

項目	説明
Trap Global State	SNMP トラップを「Enabled」(有効)/「Disabled」(無効)にします。
SNMP Authentication Trap	SNMP 認証失敗の通知送信の設定を行います。認証失敗トラップは、機器が正しく認証されていない SNMP メッ セージを受信した時に実行されます。認証方法は使用している SNMP のバージョンによります。SNMPv1 または
	SNMPv2c の場合、不正なコミュニティ文字列によってパケットが構成されている時に認証に失敗します。
Port Link Up	ポートリンクアップ通知送信の設定を行います。リンクアップトラップは機器がリンクアップを認識すると実行します。
Port Link Down	ポートリンクダウン通知送信の設定を行います。リンクダウントラップは機器がリンクダウンを認識すると実行します。
Coldstart	コールドスタートを「Enabled」(有効)/「Disabled」(無効)にします。
Warmstart	ウォームスタートを「Enabled」(有効)/「Disabled」(無効)にします。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

### SNMP Linkchange Trap Settings (SNMP リンクチェンジトラップ設定)

SNMP リンクチェンジトラップを設定します。

Management > SNMP > SNMP Linkchange Trap Settings の順にメニューをクリックし、以下の画面を表示します。

SNMP Li	nkchange Trap Sett	ings	_		
SNMP Link	kchange Trap Settings				
Unit	From Port	To Port	Trap Sending	Trap State	
1	✓ eth1/0/1 ✓	eth1/0/1 🗸	Disabled 🗸	Disabled 🔽	Apply
	Port		Trap Sending		Trap State
	eth1/0/1		Enabled		Enabled
	eth1/0/2		Enabled		Enabled
	eth1/0/3		Enabled		Enabled

図 7-10 SNMP Linkchange Trap Settings 画面

#### 画面に表示される項目:

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	ポートの始点 / 終点を設定します。
Trap Sending	SNMP 通知トラップ送信の「Enabled」(有効)/「Disabled」(無効)を指定します。
Trap State	SNMP リンクチェンジトラップの「Enabled」(有効)/「Disabled」(無効)を設定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

### SNMP View Table Settings (SNMP ビューテーブル)

コミュニティ名に対しビュー(アクセスできる MIB オブジェクトの集合)を割り当て、リモート SNMP マネージャがどの MIB オブジェクトにアク セスするかを定義するために使用します。

Management > SNMP > SNMP View Table Settings の順にメニューをクリックし、以下の画面を表示します。

SNMP View Table Settings				
SNMP View Settings				
View Name * 32 chars				
Subtree OID * N.N.NN				
View Type Included				
* Mandatory Field			Add	
Total Entries: 8				
View Name	Subtree OID	View Type		
restricted	1.3.6.1.2.1.1	Included	Delete	
restricted	1.3.6.1.2.1.11	Included	Delete	
restricted	1.3.6.1.6.3.10.2.1	Included	Delete	

図 7-11 SNMP View Table Settings 画面

### エントリの削除

「SNMP View Table Settings」画面のエントリを削除するためには、エントリの行の「Delete」ボタンをクリックします。

エントリの新規作成

新しいエントリを作成するためには、上記テーブルに情報を入力し、「Add」ボタンをクリックします。

SNMP ユーザ(「SNMP User Table」で設定)と本画面で登録するビューは、「SNMP Group Table」によって作成する SNMP グループによって関連付けます。

画面に表示される項目	:	

項目	説明
View Name	32 文字までの半角英数字を入力します。新しい SNMP ビューを登録し、識別する際に使用します。
Subtree OID	ビューの OID (Object Identifier) サブツリーを入力します。OID は、オブジェクトツリー (MIB ツリー) が SNMP マネージャによっ
	てアクセス可能な範囲かどうかを識別します。
View Type	「Subtree OID」で指定した OID が、SNMP マネージャがアクセス可能な範囲であるかを指定します。
	<ul> <li>Included - アクセス可能になります。</li> </ul>
	・ Excluded - アクセス不可になります。

### SNMP Community Table Settings (SNMP コミュニティテーブル設定)

定義済みの SNMP コミュニティテーブルの参照、および、SNMP マネージャとエージェントの関係を定義する SNMP コミュニティ名を登録します。 コミュニティ名は、スイッチのエージェントへのアクセスを行う際のパスワードの役割をします。以下の特性はコミュニティ名と関係します。

- ・コミュニティ名を使用して、スイッチの SNMP エージェントにアクセスを行う SNMP マネージャの IP アドレスが掲載されるアクセスリスト。
- ・ MIB オブジェクトのすべてのサブセットを定義する MIB ビューは SNMP コミュニティにアクセス可能である。
- ・ SNMP コミュニティにアクセス可能な MIB オブジェクトが Read/Write または Read-only レベルである。

#### エントリの設定

「SNMP Community Table」画面でコミュニティエントリを設定します。

Management > SNMP > SNMP Community Table Settings の順にクリックし、以下の画面を表示します。

SNMP Community	Table Setting	S			
SNMP Community Settin	gs				
Кеу Туре	Plain Text	~			
Community Name	32 chars				
View Name	32 chars				
Access Right	Read Only	~			
IP Access-List Name	32 chars				
					Add
Total Entries: 2					
Community Na	ame	View Name	Access Right	IP Access-List Name	
public		CommunityView	ro		Delete
privata		CommunityView	DV/		Dalata

図 7-12 SNMP Community Table Settings 画面

#### 画面に表示される項目:

項目	説明
Кеу Туре	SNMP コミュニティのキーの種類を選択します。「Plain Text」「Encrypted」から選択可能です。
Community Name	32 文字までの半角英数字を入力し、SNMP コミュニティメンバを識別します。本コミュニティ名は、リモートの SNMP マネー ジャが、スイッチの SNMP エージェント内の MIB オブジェクトにアクセスする際にパスワードのように使用します。
View Name	32 文字までの半角英数字を入力します。本値は、リモート SNMP マネージャがアクセスすることのできる MIB グループの定 義に使用します。View Name は SNMP View Table に存在する必要があります。
Access Right	<ul> <li>Read Only - 指定した Community Name を使用する SNMP コミュニティメンバは、スイッチの MIB の内容の読み取りのみ 可能となります。</li> <li>Read Write - 指定した Community Name を使用する SNMP コミュニティメンバは、スイッチの MIB の内容の読み取り、お よび書き込みが可能です。</li> </ul>
IP Access-List Name	SNMP エージェントにアクセスするために文字列を使用するユーザを管理するアクセスリストの名前を入力します。

#### エントリの作成

新しいエントリを作成するためには、上記テーブルに情報を入力し、「Add」ボタンをクリックします。

エントリの削除

削除するエントリ横の「Delete」ボタンをクリックし、エントリを削除します。

### SNMP Group Table Settings (SNMP グループテーブル)

SNMP グループを登録します。本グループは、SNMP ユーザ(「SNMP User Table」で設定)と「SNMP View Table」で設定するビューを関連付けるものです。

Management > SNMP > SNMP Group Table Settings の順にメニューをクリックし、以下の画面を表示します。

NMP Group	Table Sett	ings						_
SNMP Group Sett	tings							
Group Name * User-based Secu Security Level IP Access-List Na * Mandatory Field	urity Model ame	32 chars SNMP NoAuth 32 chars	NoPriv	Read Vi Write Vi Notify Vi	ew Name 3 ew Name 3 ew Name 3	2 chars 2 chars 12 chars	] ] ]	Add
Total Entries: 5								
Group Name	Read View	v Name	Write View Name	Notify View Name	Security Model	Security Level	IP Access-List Name	
public	Commun	iityV		CommunityV	v1			Delete
public	Commun	iityV		CommunityV	v2c			Delete
initial	restrict	ted		restricted	V3	NoAuthNoPriv		Delete
private	Commun	iityV	CommunityV	CommunityV	v1			Delete
private	Commun	ityV	CommunityV	CommunityV	v2c			Delete

図 7-13 SNMP Group Table Settings 画面

#### 「SNMP Group Table」画面のエントリの削除

エントリの行の「Delete」ボタンをクリックします。

#### 「SNMP Group Table」画面への新規エントリの追加

上記画面に情報を入力し、「Add」ボタンをクリックします。

画面に表示される項目:

項目	説明
Group Name	32 文字までの半角英数字を入力します。SNMP ユーザのグループの識別に使用します。
User-based	・ SNMPv1 - SNMP バージョン 1 が使用されます。
Security Model	・ SNMPv2c - SNMP バージョン 2c が使用されます。SNMP バージョン 2 は集中型、分散型どちらのネットワーク管理にも対応
	します。SNMP バージョン 1 と比較して SMI(Structure of Management Information)およびセキュリティ機能において強
	化されています。
	・ SNMPv3 - SNMP バージョン 3 が使用されます。ネットワーク上で認証とパケットの暗号化を併用することにより、デバイス
	への安全なアクセスを提供します。
Security Level	セキュリティレベル設定は SNMP バージョン 3 にのみ適用されます。
	・ NoAuthNoPriv - スイッチとリモート SNMP マネージャ間のパケットは認証も暗号化もされません。
	・ AuthNoPriv - スイッチとリモート SNMP マネージャ間のパケットは認証あり、暗号化なしになります。
	・ AuthPriv - スイッチとリモート SNMP マネージャ間のパケットは認証あり、暗号化ありになります。
IP Access-List Name	アクセスするための IP アクセスコントロールリストの名前を入力します。
Read View Name	SNMP メッセージを要求する SNMP グループ名を入力します。
Write View Name	SNMP エージェントに書き込み権限を与える SNMP グループ名を入力します。
Notify View Name	SNMP エージェントによるトラップメッセージを送信する SNMP グループ名を入力します。

### SNMP Engine ID Local Settings(SNMP エンジン ID ローカル設定)

エンジン ID は、SNMP バージョン 3 で使用される場合に定義される固有の識別名です。識別名は半角英数字の文字列で表記され、スイッチ上の SNMP エンジン(エージェント)を識別するために使用します。

Management > SNMP > SNMP Engine ID Local Settings の順にメニューをクリックし、以下の画面でスイッチの SNMP エンジン ID を表示します。

SNMP Engine ID Local Settings	
SNMP Engine ID Local Settings	
Engine ID 800000ab03f07d683630	Default Apply
Engine ID length is 24, the accepted character is from 0 to F.	
図 7-14 SNMP Engine ID Settings 画面	

画面に表示される項目:

項目	説明
Engine ID	スイッチの SNMP エンジンの識別子を指定します。24 文字内で指定可能です。
	、「Apply」ボタンをクリックします。

「Default」をクリックするとエンジン ID は初期値に戻ります。

### SNMP User Table Settings (SNMP ユーザテーブル設定)

SNMP ユーザを登録します。また、スイッチに現在設定されているすべての SNMP ユーザを表示します。

Management > SNMP > SNMP User Table Settings の順にメニューをクリックし、以下の画面を表示します。

SNMP User Table Set	ungs			_		
SNMP User Settings						
User Name *	32 chars					
Group Name *	32 chars					
SNMP Version	v3	~				
SNMP V3 Encryption	None [	<b>~</b>				
Auth-Protocol by Password	MD5 [	Password	d (8-16 chars)			
Priv-Protocol by Password	None [	✓ Password	1 (8-16 chars)			
Auth-Protocol by Key	MD5	✓ Key (32 c)	chars)			
Priv-Protocol by Key	None [	✓ Key (32 c)	chars)			
IP Address-List Name	32 chars					
* Mandatory Field						Add
Total Entries: 1						
User Name Group Na	me Security Model	Authentication Protocol	Privacy Protocol	Engine ID	IP Address-List Name	
initial initial	V3	None	None	800000ab03		Delete

図 7-15 SNMP User Table Settings 画面

#### エントリの削除

エントリの行の「Delete」ボタンをクリックします。

#### エントリの新規登録

新規エントリを追加するためには、上記画面に情報を入力し、「Add」ボタンをクリックします。

画面にえ	長示され	る項目	:

項目	説明			
User Name	32 文字までの半角英数字。SNMP ユーザを識別します。			
Group Name	作成した SNMP グループが SNMP メッセージを要求するために使用される名前です。			
SNMP Version	・ v1 - SNMP バージョン 1 が使用されています。			
	・ v2 - SNMP バージョン 2 が使用されています。			
	・ v3 - SNMP バージョン 3 が使用されています。			
SNMP V3	SNMP v3 に対して暗号化を有効にします。本項目は「SNMP Version」で「v3」を選択した場合に有効になります。			
Encryption	・ None - ユーザ認証は使用しません。			
	・ Key - HMAC-MD5 アルゴリズムまたは HMAC-SHA アルゴリズムレベルのユーザ認証を行います。			
	・ Password - HMAC-SHA アルゴリズムレベルのパスワードか HMAC-MD5-96 パスワードによる認証を行います。			

項目	説明
Auth-Protocol	本項目は「SNMP Version」で「V3」を選択し、「SNMP V3 Encryption」で「Password」または「Key」を選択した場合に有効に
by Password	なります。本項目を選択後、「Password」/「Key」にパスワードを入力します。
Auth-Protocol by	・ MD5 - HMAC-MD5-96 認証レベルが使用されます。(Password:半角英数字 8-16 文字 /Key:半角英数字 32 文字)
Key	・ SHA - HMAC-SHA 認証プロトコルが使用されます。(Password:半角英数字 8-20 文字 /Key:半角英数字 40 文字)
Кеу	Auth-Protocol 鍵を入力します。(MD5:32 文字、SHA:40 文字)
Priv-Protocol by	本項目は「SNMP Version」で「V3」を選択し、「SNMP V3 Encryption」で「Password」または「Key」を選択した場合に有効に
Password	なります。
Priv-Protocol by	・ None - 認証プロトコルは使用されていません。
Кеу	・ DES56 - CBC-DES (DES-56) 標準に基づく DES 56 ビット暗号化方式が使用されています。本項目を選択後、「Password」/「Key」
	にパスワード(半角英数字 8-16 文字)、または Key(半角英数字 32 文字)を入力します。
	・ AES - AES 暗号が使用されます。本項目を選択後、「Password」/「Key」にパスワード(半角英数字 8-16 文字)、または Key(半
	角英数字 32 文字)を入力します。
Кеу	Priv-Protocol 鍵を入力します。(DES56/AES:32 文字)
IP Access-List	アクセスするための IP アクセスコントロールリストの名前を入力します。
Name	

### SNMP Host Table Settings(SNMP ホストテーブル設定)

SNMP トラップの送信先を設定します。

### Management > SNMP > SNMP Host Table Settings の順にメニューをクリックし、以下の画面を表示します。

SNMP Host Table Settings		_		
SNMP Host Settings				
Host IPv4 Address     Host IPv6 Address	2013::1			
VRF Name	12 chars			
User-based Security Model	SNMPv1			
Security Level	NoAuthNoPriv 🗸			
UDP Port (1-65535)	162			
Community String / SNMPv3 User Name	32 chars			Add
Total Entries: 1				
Host IP Address VRF Nam	SNMP Version	UDP Port	Community String / SNMPv3 User Name	
192.168.70.1	V1	162	private	Delete

図 7-16 SNMP Host Table Settings 画面

画面に表示される項目:	
-------------	--

項目	説明
Host IPv4 Address	スイッチの SNMP ホストとなるリモート管理ステーション(トラップの送信先)の IPv4 アドレスを入力します。
Host IPv6 Address	スイッチの SNMP ホストとなるリモート管理ステーション(トラップの送信先)の IPv6 アドレスを入力します。
VRF Name	VRF インスタンス名を 12 文字以内で入力します。
User-based Security Model	<ul> <li>SNMPV1: SNMP バージョン 1 が使用されます。</li> <li>SNMPV2c: SNMP バージョン 2c が使用されます。</li> <li>SNMPV3: SNMP バージョン 3 が使用されます。</li> </ul>
Security Level	<ul> <li>NoAuthNoPriv: NoAuth-NoPriv セキュリティレベルの SNMP バージョン 3 が使用されます。</li> <li>AuthNoPriv: V3-Auth-NoPriv セキュリティレベルの SNMP バージョン 3 が使用されます。</li> <li>AuthPriv: V3-Auth-Priv セキュリティレベルの SNMP バージョン 3 が使用されます。</li> </ul>
UDP Port	UDP ポート番号を入力します。UDP ポート番号の初期トラップは 162 です。UDP ポート範囲は 0 から 65535 です。いくつかのポート番号は他のプロトコルと衝突する可能性があります。
Community String/ SNMPv3 User Name	コミュニティ名または SNMP V3 ユーザ名を入力します。

### エントリの削除

「SNMP Host Table」画面内のエントリを削除するためには、エントリの行の「Delete」ボタンをクリックします。

### エントリの新規登録

スイッチの SNMP ホストテーブルに新しいエントリを追加するためには、上記画面に情報を入力し、「Add」ボタンをクリックします。

### SNMP Context Mapping Table Settings(SNMP コンテキストマッピングテーブル設定)(EI/MI モードのみ)

SNMP コンテキストマッピングテーブルの表示、設定を行います。

Management > SNMP > SNMP Context Mapping Table Settings の順にメニューをクリックし、以下の画面を表示します。

NMP Context Mapping Tab	le Settings			
SNMP Context Mapping Settings				
Context Name	32 chars			
Instance ID (1-65535)				
Instance Name	12 chars			
VRF Name	12 chars			
				Add
Total Entries: 1				
Context Name	Instance ID	Instance Name	VRF Name	
Context1	0			Delete

図 7-17 SNMP Context Mapping Table Settings 画面

#### 画面に表示される項目:

項目	説明
Context Name	SNMP View-based Access Control Model(VACM)コンテキスト名を 32 字以内で入力します。コンテキスト 名は文字で開始する必要がありますが、終わりは文字、数字どちらでも構いません。それ以外は文字、数字、 ハイフンが使用可能です。
Instance ID	OSPF インスタンス ID を入力します。(1-65535)
Instance Name	ISIS ルーティングエリアタグを 12 文字以内で入力します。
VRF Name	VRF インスタンス名を 12 文字以内で入力します。

#### エントリの削除

エントリを削除するためには、エントリの行の「Delete」ボタンをクリックします。

#### エントリの新規登録

新しいエントリを追加するためには、上記画面に情報を入力し、「Add」ボタンをクリックします。

### RMON (RMON 設定)

スイッチの SNMP 機能に対するリモートモニタリング (RMON) ステータスを有効または無効にします。

### RMON Global Settings (RMON グローバル設定)

Management > RMON > RMON Global Settings の順にメニューをクリックし、以下の「RMON Global Settings」画面を表示します。

RMON Global Settings	_		
RMON Global Settings			
RMON Rising Alarm Trap	Enabled	Disabled	
RMON Falling Alarm Trap	Enabled	Disabled	Apply

図 7-18 RMON Global Settings 画面

#### 画面に表示される項目:

項目	説明	
RMON Rising Alarm Trap	「RMON Rising Alarm Trap」を有効にします。	
RMON Falling Alarm Trap	「RMON Falling Alarm Trap」を有効にします。	
g定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。		

### RMON Statistics Settings (RMON 統計情報)

RMON 統計情報を表示、設定します。

**Management > RMON > RMON Statistics Settings** の順にメニューをクリックし、以下の「RMON Statistics Settings」画面を表示します。

RMON Statistics	Settings		
RMON Statistics Set	tings		
Unit * Port *		Index (1-65535) *	Owner
1 💌 eth1/0	/1 💌		127 chars Add
Index	Dort	Oumor	
2	eth1/0/1	RMON	Delete Show Detail

図 7-19 RMON Statistics Settings 画面

#### 画面に表示される項目:

項目	説明
Unit	設定するユニットを選択します。
Port	RMON 情報を取得するポートを指定します。
Index (1 - 65535)	RMON イーサネット統計情報エントリの番号を指定します。
Owner	オーナーの文字列を入力します。127 文字まで入力可能です。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

#### 統計情報の登録を行う場合

1. 設定項目を入力します。

2. 「Add」をクリックします。

#### 統計情報の削除を行う場合

「Delete」をクリックします。

#### 指定ポートの統計情報を表示する場合

「Show Detail」をクリックします。以下の画面が表示されます。

RMO	RMON Statistics Table																	
RMON	Statistic	s Table —																
	Data	Des	Dee	Deserves	Bullinest	lle deseites	0			CDC		Deere		05 407	420.055	250 544	512-	1024-
Inde	Data	Rec.	Rec.	Boradcast	MUITICAST	Undersize	Oversize	Fragments	Jabbers	CRC	Collisions	Urop	04 Octote	05-12/	128-255	256-511 Octote	1023	1518
	Source	Octets	PRIS	PRIS	PRIS	PRIS	PRIS			EIIU		Event	OCIEIS	Ociers	Ociers	Octers	Octets	Octets
2	eth1/0/1	4840998	27108	1130	1756	0	0	0	0	0	0	2881	16448	2494	399	7051	716	0
																	E	Back

図 7-20 RMON Statistics Settings - Show Detail 画面

「Back」をクリックすると前ページへ移動します。

### RMON History Settings (RMON ヒストリ設定)

ポートから RMON MIB のヒストリ(履歴)情報を取得するための設定を行います。

Management > RMON > RMON History Settings の順にメニューをクリックし、以下の「RMON Global Settings」画面を表示します。

RMON Histo	ory Settings	9 <b>0</b>			_		
Unit *		Port = eth1/0/1	Index (1-65535) *	Bucket Number (1- 50	-65535) Inte	erval (1-3600) 00 sec	Owner 127 chars Add
Index	Port	Buckets Requested	Buckets Granted	Interval	Owner		
1	eth1/0/1	50	50	1800		Delete	Show Detail
						1/1 < <	1 > > Go

図 7-21 RMON History Settings 画面

#### 画面に表示される項目:

項目	説明
Unit	設定するユニットを選択します。
Port	RMON 情報を取得するポートを指定します。
Index (1 - 65535)	ヒストリ制御エントリ番号を指定します。
Bucket Number (1 - 65535)	デバイスが保存するバケット数を指定します。初期値は 50 です。
Interval (1 - 3600)	ポートからサンプリングする間隔(秒)を設定します。 • 初期値:1800(秒) • 入力可能範囲:1-3600(秒)
Owner	オーナーの文字列を入力します。127 文字まで入力可能です。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

#### 履歴情報の登録を行う場合

1. 設定項目を入力します。

2. 「Add」をクリックします。

#### 履歴情報の削除を行う場合

「Delete」をクリックします。

#### 指定ポートの履歴情報を表示する場合

「Show Detail」をクリックします。以下の画面が表示されます。

NON	Statistics	Table																
ndex	Data Source	Rec. Octets	Rec. PKTs	Boradcast PKTs	Multicast PKTs	Undersize PKTs	Oversize PKTs	Fragments	Jabbers	CRC Error	Collisions	Drop Event	64 Octets	65-127 Octets	128-255 Octets	256-511 Octets	512- 1023 Octets	1024- 1518 Octet
2	eth1/0/1	4840998	27108	1130	1756	0	0	0	0	0	0	2881	16448	2494	399	7051	716	0

図 7-22 RMON History Settings - Show Detail 画面

「Back」をクリックすると前ページへ移動します。

### RMON Alarm Settings (RMON アラーム設定)

ネットワークアラームを設定します。ネットワークの問題またはイベントが検出されると、ネットワークアラームが発生します。

**Management > RMON > RMON Alarm Settings** の順にメニューをクリックし、以下の「RMON Alarm Settings」画面を表示します。

RMON Alarm Settings					
RMON Alarm Settings					
Index (1-65535) * Variable * Rising Threshold (0-2147483647) * Rising Event Number (1-65535) Owner	N.N.NN	Interval (1-2147 Type Falling Threshol Falling Event Nu	483647) * Absol d (0-2147483647) * imber (1-65535)	ute 🔽	
Total Entries: 1 Index Interval (sec) Variable	Type Last Value Risi	ng Threshold Falling Threshold	Rising Event No. Falling Eve	nt No. Startup Alarm Ow	Add
1 30 1.3.6.1.2.1.2.2.	1.12.0 Absolute U	20 10		1/1 K < 1	>>> Go

#### 図 7-23 RMON Alarm Settings 画面

画面に表示される項目:

項目	説明
Index (1-65535)	特定のアラームを指定します。
Interval	アラームの間隔(秒)を定義します。1 から 2147483648(秒)の間で指定可能です。
Variable	選択した MIB 変数の値を指定します。
Туре	選択した変数に対するサンプリング方式としきい値と比較する値を定義します。 ・「Delta」-現在の値から最後にサンプリングされた値を引きます。値の差がしきい値と比較されます。 ・「Absolute」-サンプリング間隔の終わりで値を直接しきい値と比較します。
Rising Threshold	上昇しきい値を設定します。0から2147483647(秒)の間で指定可能です。
Falling Threshold	下降しきい値を設定します。0から2147483647(秒)の間で指定可能です。
Rising Event Number (1~65535)	上昇しきい値を超えたときに始動するイベントを設定します。 設定可能な項目は、ユーザ定義の RMON イベントです。1 から 65535(秒)の間で指定可能です。
Falling Event Number (1 ~ 65535)	下降しきい値を超えたときに始動するイベントを設定します。 設定可能な項目は、ユーザ定義の RMON イベントです。1 から 65535(秒)の間で指定可能です。
Owner	オーナーの文字列を入力します。127 文字まで入力可能です。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

#### エントリの登録を行う場合

1. 設定項目を入力します。

2. 「Add」をクリックします。

#### エントリの削除を行う場合

「Delete」をクリックします。

### RMON Event Settings (RMON イベント設定)

RMON イベント統計情報の定義、編集、および参照を行います。

**Management > RMON > RMON Event Settings** の順にメニューをクリックし、以下の「RMON Event Settings」画面を表示します。

	RMON Ev	ent Settings			_		
ſ	RMON Even	nt Settings					
	Index (1-65	5535) *					
	Description	1	1-127 0	hars			
	Туре		None				
	Community	ý	1-127 (	hars			
	Owner		1-127 (	hars			
							Add
	Total Entri	ies: 1					
	Index	Description	Community	Event Trigger	Owner	Last Trigger Time	
	1	event	commuity	Log and Trap	owner	0d:0h:0m:0s	Delete View Logs
							111 [< < 1 > >] Go
1							

#### 図 7-24 RMON Event Settings 画面

画面に表示される項目:

項目	説明
Index (1~65535)	イベントを指定します。
Description	ユーザ定義のイベントの記述を指定します。
Туре	イベントタイプを指定します。 選択肢:「None」「Log」「Trap」「Log and Trap」 ・ None - イベントが発生しなかったことを示します。 ・ Log - イベントがログエントリであることを示します。 ・ Trap - イベントがトラップであることを示します。 ・ Log and Trap - イベントがログエントリとトラップの両方であることを示します。
Community	イベントが所属するコミュニティを指定します。127 文字まで入力可能です。
Owner	オーナーの文字列を入力します。127 文字まで入力可能です。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

#### エントリの登録を行う場合

1. 設定項目を入力します。

2. 「Add」をクリックします。

#### エントリの削除を行う場合

「Delete」をクリックします。

#### 指定エントリのログ情報を表示する場合

「View Logs」をクリックします。以下の画面が表示されます。

Event Logs Table		
Event Logs Table Event Index: 1		
Total Entries: 0		
Log Index	Log Time	Log Description
	ad s	Back

図 7-25 Event Logs Table 画面

「Back」をクリックすると前ページへ移動します。

## Telnet/Web(Telnet/Web 設定)

スイッチに Telnet/Web 設定をします。

Management > Telnet/Web Settings の順にメニューをクリックし、以下の画面を表示します。

Telnet/Web		_	_	_	
Telnet Settings					
Telnet State Port (1-65535)	Enabled Disabled 23				Apply
Source Interface Source Interface State Type	C Enabled  Disabled VLAN	Interface ID (1-4094)			Apply
Web Settings					
Web State Port (1-65535)	Enabled O Disabled				Apply

図 7-26 Telnet/Web Settings 画面

以下の項目が使用されます。

#### **Telnet Settings**

項目	説明
Telnet State	Telnet 設定は初期値で「Enabled」(有効)です。Telnet 経由のシステム設定を許可しない場合は、「Disabled」(無効)を
	選択しより。
Port	スイッチの Telnet マネジメントに使用される TCP ポート番号(1-65535)。Telnet プロトコルに通常使用される TCP ポー
(1-65535)	トは 23 です。

「Apply」ボタンをクリックし、設定内容を適用してください。

#### Source Interface

項目	説明
Source Interface State	Source インタフェースの「Enabled」(有効)/「Disabled」(無効)を指定します。
Туре	Source インタフェースの種類を指定します。「Loopback」「Mgmt」「VLAN」から指定します。
Interface ID	インタフェース ID を指定します。 「Loopback」選択時は 1-8、「Mgmt」選択時は 0 のみ、「VLAN」選択時は 1-4094 が選択可能です。

「Apply」ボタンをクリックし、設定内容を適用してください。

#### Web Settings

項目	説明
Web State	Web ベースマネジメントは初期値で「Enabled」(有効)です。「Disabled」を選択しステータスを無効にすると、設定はす
	ぐに適用され、Web インタフェースを使用したシステムの設定はできなくなります。
Port (1-65535)	スイッチのWebベースマネジメントに使用されるTCPポート番号。Webプロトコルに通常使用されるTCPポートは80です。

「Apply」ボタンをクリックし、設定内容を適用してください。

## Session Timeout (セッションタイムアウト)

各セッション(Web やコンソールなど)のタイムアウトの設定をします。外向き(outgoing)セッションのタイムアウト値は、他スイッチの Telnet インタフェースに向けた、CLI 経由の「Console/Telnet/SSH」接続において使用されます。

Management > Session Timeout の順にメニューをクリックし、以下の画面を表示します。

Session Timeout			
Session Timeout			
Web Session Timeout (60-36000)	180 sec	☑ Default	
Console Session Timeout (0-1439)	3 min	✓ Default	
Outgoing Console Session Timeout (0-1439)	0 min	✓ Default	
Telnet Session Timeout (0-1439)	3 min	✓ Default	
Outgoing Telnet Session Timeout (0-1439)	0 min	✓ Default	
SSH Session Timeout (0-1439)	3 min	✓ Default	
Outgoing SSH Session Timeout (0-1439)	0 min	☑ Default	Apply

図 7-27 Session Timeout 画面

画面に表示される項目:

項目	説明
Web Session Timeout	Web セッションのタイムアウト時間(秒)を設定します。 「Default」にチェックを入れると初期値に戻ります。60から 36000(秒)で設定可能です。 初期値:180(秒)
Console Session Timeout	コンソールセッションのタイムアウト時間(分)を設定します。「Default」にチェックを入れると初期値に戻ります。0 から 1439(分)で設定可能です。0 に指定するとタイムアウトしません。 初期値:3(分)
Outgoing Console Session Timeout	外向き(Outgoing)コンソールセッションのタイムアウト時間(分)を設定します。「Default」にチェックを入れると 初期値に戻ります。0から1439(分)で設定可能です。0に指定するとタイムアウトしません。 初期値:0(分)
Telnet Session Timeout	Telnet セッションのタイムアウト時間(分)を設定します。「Default」にチェックを入れると初期値に戻ります。0から1439(分)で設定可能です。0に指定するとタイムアウトしません。 初期値:3(分)
Outgoing Telnet Session Timeout	外向き(Outgoing) Telnet セッションのタイムアウト時間(分)を設定します。「Default」にチェックを入れると初期 値に戻ります。0から1439(分)で設定可能です。0に指定するとタイムアウトしません。 初期値:0(分)
SSH Session Timeout	SSH セッションのタイムアウト時間(分)を設定します。「Default」にチェックを入れると初期値に戻ります。0から 1439(分)で設定可能です。0に指定するとタイムアウトしません。 初期値:3(分)
Outgoing SSH Session Timeout	外向き(Outgoing) SSH セッションのタイムアウト時間(分)を設定します。「Default」にチェックを入れると初期値 に戻ります。0から1439(分)で設定可能です。0に指定するとタイムアウトしません。 初期値:0(分)

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

## DHCP(DHCP 設定)

スイッチの DHCP について設定します。

### Service DHCP(DHCP サービス)

スイッチの DHCP リレーサービスについて設定します。

Management > DHCP > Service DHCP の順にメニューをクリックし、以下の画面を表示します。

Service DHCP		
Service DHCP		
Service DHCP State	Disabled     O Enabled	Apply
Service IPv6 DHCP		
Service IPv6 DHCP State	Disabled      Enabled	Apply

図 7-28 Service DHCP 画面

#### 画面に表示される項目:

項目	説明
Service DHCP State	DHCP リレーサービスを「Enabled」(有効)/「Disabled」(無効)に設定します。
Service IPv6 DHCP State	IPv6 DHCP リレーサービスを「Enabled」(有効)/「Disabled」(無効)に設定します。
設定を変更する際は、必ず「A	vpply」ボタンをクリックし、設定内容を適用してください。

### DHCP Class Settings (DHCP クラス設定)

スイッチの DHCP クラスとその合致する方式についての DHCP オプションについて表示、設定します。

Management > DHCP > DHCP Class Settings の順にメニューをクリックし、以下の画面を表示します。

DHCP Class Settings		
DHCP Class Settings		
Class Name	32 chars	Apply
Total Entries: 1		
	Class Name	
	DHCPClass	Edit Delete
		1/1  < < 1 > >) Go

図 7-29 DHCP Class Settings 画面

#### 画面に表示される項目:

項目	説明
Class Name	DHCP クラス名を 32 文字までで指定します。
設定を変更する	」際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

#### エントリの削除を行う場合

「Delete」をクリックします。

#### 指定エントリの編集を行う場合

「Edit」をクリックします。以下の画面が表示されます。

DHCP Class Option Se	ttings			
DHCP Class Option Settings				
Class Name Option (1-254) Hex Bitmask	class			Apply
Total Entries: 0				
Optio	n	Hex	Bitmask	

図 7-30 DHCP Class Option Settings (Edit) 画面

以下の項目が使用されます。

項目	説明
Option	DHCP オプション番号を指定します。1-254 までで指定可能です。
Hex	指定した DHCP オプションの 16 進数方式を入力します。「*」にチェックを入れると残りのオプションのビットはマッチされません。
Bitmask	16進数ビットマスクを入力します。マスクされたビット方式はマッチします。指定されない場合、16進数のすべてのビットはチェックされます。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。 「Back」をクリックすると前ページへ移動します。

#### エントリの削除を行う場合

「Delete」をクリックします。

#### DHCP Server (DHCP $\forall -1\vec{i}$ )

#### Management > DHCP > DHCP Server

DHCP (Dynamic Host Configuration Protocol) によってスイッチは、IP アドレス、サブネットマスク、デフォルトゲートウェイ、および他の IP パラメー タをこの情報を要求するデバイスに発行することができます。DHCP が有効なデバイスが起動すると、ローカルなネットワークに割り当てられます。 このデバイスは DHCP クライアントであり、有効にすると、IP パラメータが設定される前にネットワークにクエリメッセージを送信します。DHCP サー バがこのリクエストを受信すると、DHCP クライアントがローカル設定に利用する上記 IP 情報を含む応答をクライアントに返します。

ローカルに割り当てられたネットワークを利用するために、DHCP に関連する多くのパラメータを設定できます。これにより、割り当てた IP アドレスのリースタイム、DHCP プール内で許可されている IP アドレス範囲、ネットワークに同一のエントリを作成しないようにアドレスプール内の各 IP アドレスを排除する機能など自動IP 設定を希望するクライアントの IP 設定をコントロールおよび制限します。また、DNS サーバまたはデフォルトルートの IP アドレスなどネットワークの別のデバイスに重要なデバイスの IP アドレスを割り当てることができます。

さらに、スタティック IP アドレスを必要とするネットワークメンテナンスに重要なデバイスの IP アドレスを同一に保つために、DHCP プール内の IP アドレスを指定した MAC アドレスに割り当てることができます。

注意 DHCP サーバ機能の設定変更を行った際は、設定変更後に必ず DHCP サーバサービスの再起動を行ってください。

#### DHCP Server Global Settings (DHCP サーバグローバル設定)

DHCP サーバグローバルパラメータを設定します。

**Management > DHCP > DHCP Server > DHCP Server Global Settings**の順にメニューをクリックし、以下の画面を表示します。

DHCP Server Global Settings		
DHCP Use Class State		
DHCP Use Class State	○ Enabled	Apply
DHCP Server Settings		
DHCP Ping Packet (0-10)	2	
DHCP Ping Timeout (100-10000)	500 ms	Apply

図 7-31 DHCP Server Global Settings 画面

画面に表示される項目:

項目	説明
DHCP Use Class State	スイッチを DHCP サーバとしてグローバルに「Enabled」(有効)/「Disabled」(無効)にします。
Ping Packets (0-10)	割り当て済みの IP アドレスを含むネットワークにスイッチが送信する ping パケットの数(0-10)を指定します。ping リクエストが戻らない場合、その IP アドレスは、ローカルネットワークに対して固有であると見なされて、要求側ク ライアントに割り当てられます。0 は ping テストを行わないことを意味します。初期値は 2 パケットです。
Ping Timeout (10-10000)	ping パケットがタイムアウトになる前に DHCP サーバが待つ時間を選択します。初期値は 500 です。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

### DHCP Server Pool Settings(DHCP サーバプール設定)

DHCP サーバプールの追加および削除を行います。

#### Management > DHCP > DHCP Server > DHCP Server Pool Settings の順にメニューをクリックし、以下の画面を表示します。

HCP Server Pool		
ool Name	32 chars	Apply
otal Entries: 1		
	Dool Namo	
	Poor Name	
	pool	Edit Class Edit Option Configure Delete

図 7-32 DHCP Server Pool Settings 画面

画面に表示される項目:

項目	説明
Pool Name	DHCP サーバプール名を 32 字以内で入力します。
E	

「Apply」ボタンをクリックし、設定内容を適用してください。

はじめに「Pool Name」欄に名前 (半角英数字 12 文字以内) を入力して、「Add」をクリックすることによって、プールを作成します。一度作成されると、 対応する「Edit Class」「Edit Option」「Configure」ボタンをクリックして、プールの設定を編集することができます。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

#### エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

#### エントリの編集(Edit Class)

「Edit Class」ボタンをクリックすると、以下の画面が表示されます。

pool		
Please Select		
		Apply
Start Address	End Address	
		Delete by Name Delete by Address
	pool Please Select	pool Please Select

図 7-33 DHCP Server Pool Settings (Edit Class) 画面

#### 画面に表示される項目:

項目	説明
Pool Name	パラメータを調整する DHCP プール名を表示します。
Class Name	対応する DHCP クラス名を指定します。
Start Address	DHCP クラスの開始 IPv4 アドレスを指定します。
End Address	DHCP クラスの終了 IPv4 アドレスを指定します。

「Apply」ボタンをクリックし、設定内容を適用してください。 「Delete by Name」をクリックすると DHCP クラスを名前で削除します。 「Delete by Address」をクリックすると DHCP クラスをアドレスで削除します。 「Back」をボタンをクリックすると前のページに戻ります。

### エントリの編集(Edit Option)

「Edit Option」ボタンをクリックすると、以下の画面が表示されます。

HCP Server Pool	Option Settings			
DHCP Server Pool Optio	n Settings			
Pool Name Option (1-254) Type	pool ASCII			Apply
Option		Туре	Value	
200		ip	192.168.90.250	Delete
				Back

図 7-34 DHCP Server Pool Settings (Edit Option) 画面

#### 画面に表示される項目:

項目	説明
Pool Name	パラメータを調整する DHCP プール名を表示します。
Option	DHCP オプション番号(1-254)を指定します。
Туре	<ul> <li>DHCP オプションタイプを「ASCII」「Hex」「IP」から選択し、入力します。</li> <li>ASCII -「ASCII」文字列で入力します。最大 255 文字まで入力可能です。</li> <li>HEX - 16 進数文字列で入力します。最大 254 文字まで入力可能です。</li> <li>IP - IPv4 アドレスを入力します。8個のアドレスを入力することが可能です。</li> <li>「Hex」を選択した場合に、長さ 0 の hex 文字列を指定する場合は、「None」オプションにチェックを入れます。</li> </ul>

「Apply」ボタンをクリックし、設定内容を適用してください。 「Delete」をクリックすると指定のエントリを削除します。 「Back」をボタンをクリックすると前のページに戻ります。

#### エントリの編集(Configure)

「Configure」ボタンをクリックすると、以下の画面が表示されます。

Pool Name	Pool												
RF Name	12 chars												
oot File	64 chars												
omain Name	64 chars												
letwork (IP/Mask)	0 - 0 - 0 - 0		0 . 0	- 0	- 0								
lext Server	0 · 0 · 0 · 0												
efault Router	1 1 1		2	1		14	10			<u></u>	<u></u>	10	
	1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1			8		1.1				2	2	- C	
NS Server	- 1 - 1 - 1			2	74	24	13			12	81	12	
	1						•				$\sim$		
letbios Name Server			1	γ.		-			E			- 1	
	14 (A 4)				14 - C		÷.	- e				- 6	
Netbios Node Type	Please Select	7							Ļ			•	
												-	 

図 7-35 DHCP Server Pool Settings (Configure) 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Pool Name	パラメータを調整する DHCP プール名を表示します。
VRF Name	VRF インスタンス名を 12 文字以内で入力します。
Boot File	ブートイメージのファイル名(64 字以内)を指定します。
Domain Name	クライアントのドメイン名(64 字以内)を入力します。
Network (IP/Mask)	プールのネットワークアドレスと対応するネットマスクを入力します。
Next Server	ネクストサーバの IP アドレスを指定します。本サーバに格納されているブートイメージファイルが DHCP クライアントに 検索されます。TFTP サーバである必要があります。ネクストサーバの IP アドレスはひとつのみ指定できます。
Default Router	デフォルトルータの IP アドレス。DHCP クライアントにデフォルトルータの IP アドレスを入力します。ここでは最大8つの IP アドレスを指定できます。本ルータの IP アドレスはクライアントのサブネットと同じサブネットである必要があります。ルータは推奨される順に表示されます。デフォルトルータが既に設定済みの場合、あとで設定されたデフォルトルータがデフォルトインタフェースリストに追加されます。
DNS Server	DNS サーバの IP アドレス。DHCP クライアントが使用可能である DNS サーバの IP アドレスを入力します。ここでは最大 8 つの IP アドレスを指定できます。DNS サーバは推奨される順に表示されます。DNS サーバが既に設定済みの場合、あと で設定された DNS サーバが DNS サーバリストに追加されます。
NetBIOS Name Server	WINS サーバの IP アドレス。WINS(Windows Internet Naming Service) は、マイクロソフト DHCP クライアントが通常グルー プ分けされているネットワーク内の IP アドレスにホスト名を関連付けるために使用する名前解決サービスです。最大 8 つ の IP アドレスを指定できます。
NetBIOS Node Type	マイクロソフト DHCP クライアントの NetBIOS のノードタイプを設定します。プルダウンメニューを使用して、4 つのノー ドタイプ (Broadcast、Peer to Peer、Mixed および Hybrid)から選択します。「Broadcast」システムはブロードキャストを 使用します。「Peer to Peer」 (p-node)システムは、「point-to-point name queries」のみをネームサーバ (WINS) に使用 します。「Mixed」 (h-nod)システムは、まずブロードキャストを先に抽出し、その後ネームサーバを抽出します。「Hybrid」 はまずネームサーバを先に抽出し、その後ブロードキャストを抽出します。「Hybrid」が推奨されます。
Lease	<ul> <li>初期値では、DHCP サーバに割り当てられる各 IP アドレスのリース期間(アドレスが有効であることの時間)は1日です。</li> <li>Days - リースする日(0-365)</li> <li>Hours - リースする時間(時)</li> <li>Minutes - リースする時間(分)</li> <li>Infinite - リース期間が無制限</li> </ul>

「Apply」ボタンをクリックし、設定内容を適用してください。 「Back」をボタンをクリックすると前のページに戻ります。

### DHCP Server Exclude Address (DHCP サーバ除外アドレス設定)

DHCP サーバがクライアントに割り当てない IP アドレスを指定します。除外する複数のグループを定義するために本コマンドを繰り返して使用します。DHCP サーバは、DHCP プールサブネットにあるすべての IP アドレスを DHCP クライアントに割り当てることができるものとします。

Management > DHCP > DHCP Server > DHCP Server Exclude Address の順にメニューをクリックし、以下の画面を表示します。

ICP Server Exclude Address			
'RF Name	12 chars		
egin Address			
nd Address			Apply
otal Entries: 1			
VRF Name	Begin Address	End Address	
	192,168,70,2	192.168.70.100	Delete

図 7-36 DHCP Server Exclude Address 画面

項目	説明
VRF Name	VRF インスタンス名を 12 文字以内で入力します。
Begin Address	除外する開始 IP アドレスを指定します。
End Address	除外する終了 IP アドレスを指定します。

IP アドレスまたは IP アドレス範囲を設定するために、範囲の「Begin Address」(開始アドレス)と「End Address」(終了アドレス)を入力し、「Add」 ボタンをクリックします。設定したアドレス範囲は以下の画面下半分に表示されます。

#### エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

### DHCP Server Manual Binding(DHCP サーバマニュアルバインディング)

アドレスバインディングはクライアントの IP アドレスと MAC アドレスの間のマッピングです。クライアントの IP アドレスを管理者が手動で割り当てるか、または DHCP サーバがプールから自動的に割り当てることができます。プールネットワークのアドレスからクライアントに IP アドレスを割り当てると、ダイナミックバインディングエントリが作成されます。

Management > DHCP > DHCP Server > DHCP Server Manual Binding の順にメニューをクリックし、以下の画面を表示します。

DHCP Server Manual E	Binding	_			_
DHCP Server Manual Binding	1				
Pool Name Host Hardware Address Client Identifier	32 chars	AD Mask	• • •		Apply
Pool Name	Host	Mask	Hardware Address	Client Identifier	
pool 1	92.168.70.220	255.55.55.0	00-11-22-33-44-55		Delete

図 7-37 DHCP Server Manual Binding 画面

#### 画面に表示される項目:

ってフォー

「Apply」ボタンをクリックし、設定内容を適用してください。 「Back」をボタンをクリックすると前のページに戻ります。

「Delete」をクリックすると指定のエントリを削除します。

#### DHCP Server Dynamic Binding (DHCP サーバダイナミックバインディング)

DHCP サーバダイナミックバインディングテーブルの表示と削除を行います。

Management > DHCP > DHCP Server > DHCP Server Dynamic Binding の順にメニューをクリックし、以下の画面を表示します。

DHCP Server Dynam	nic Binding					
DHCP Server Dynamic Bir	nding					
VRF Name	12 chars		IP Address	· · · ·		Find
Pool Name	32 chars	All	VRF Name	12 chars		
IP Address	1 1 1					Clear
Total Entries: 0						
VRF Name	IP Address		Client-ID/Hard	ware Address	Lease Expiration	Туре

図 7-38 DHCP Server Dynamic Binding 画面

画面に表示される項目:
-------------

項目	説明				
VRF Name	VRF インスタンス名を 12 文字以内で入力します。				
IP Address	本スイッチの DHCP サーバ機能によってこのデバイスに割り当てられた IP アドレスを表示します。				
Pool Name	ダイナミックにバインドされている DHCP エントリのプール名を表示します。				
「Clear」ボタンをクリ					

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

### DHCP Server IP Conflict(DHCP サーバ IP コンフリクト)

DHCP サーバデータベースの DHCP コンフリクトエントリを表示、クリアします。

#### Management > DHCP > DHCP Server > DHCP Conflict IP の順にメニューをクリックし、以下の画面を表示します。

DHCP Server IP Co	onflict			
DHCP Server IP Conflic	t			
VRF Name	12 chars	IP Address	· · · ·	Find
Pool Name	32 chars	All VRF Name	12 chars	
IP Address				Clear
Total Entries: 0				
IP Addres	s	Detection Method	Detection Time	VRF Name

図 7-39 DHCP Conflict IP 画面

#### 画面に表示される項目:

項目	説明			
VRF Name	VRF インスタンス名を 12 文字以内で入力します。			
IP Address	クリア / 登録されたコンフリクトエントリの IPv4 アドレスを入力します。			
Pool Name	DHCP エントリのプール名を表示します。			

「Clear」ボタンをクリックして、本欄に入力したすべてのエントリをクリアします。 「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

#### DHCP Server Statistic (DHCP サーバ統計)

DHCP サーバの統計情報を表示します。

Management > DHCP > DHCP Server > DHCP Statistic の順にメニューをクリックし、以下の画面を表示します。

DHCP Server Statistic			
			Clear
		DHCP Server Statistic	
Address Pools	1		
Automatic bindings	0		
Manual binding	1		
Malformed messages	0		
Renew messages	0		
Message Received			
BOOTREQUEST	0		
DHCPDISCOVER	0		
DHCPREQUEST	0		
DHCPDECLINE	0		
DHCPRELEASE	0		
DHCPINFORM	0		
Message Sent			
BOOTREPLY	0		
DHCPOFFER	0		
DHCPACK	0		
DHCPNAK	0		

図 7-40 DHCP Server Statistic 画面

「Clear」ボタンをクリックして、エントリをクリアします。

### DHCPv6 Server (DHCPv6 サーバ設定)

#### Management > DHCP > DHCPv6 Server

### DHCPv6 Server Pool Settings(DHCP サーバプール設定)

DHCPv6 プールの作成および設定を行います。

Management > DHCP > DHCPv6 Server > DHCPv6 Server Pool Settings の順にメニューをクリックし、以下の画面を表示します。

DHCPv6 Server Poo	ol Settings	
DHCPv6 Server Pool		
Pool Name	12 chars	Apply
Total Entries: 1		
	Pool Name	
	Pool	Configure Delete
		1/1 < 1 > 3 60

図 7-41 DHCPv6 Server Pool Settings 画面

#### 画面に表示される項目:

項目	説明
Pool Name	DHCPv6 サーバプール名を入力します。
 「Apply」ボタンをクリック」	て、入力した情報に基づいて新しいエントリを追加します

「Apply」ボタンをクリックして、人力した情報に基ついて新しいエントリを追加します。 「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。

「Configure」ボタンをクリックして、該当エントリの編集を行います。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

#### エントリの編集(Configure)

「Configure」ボタンをクリックすると、以下の画面が表示されます。

CPV6 Server Pool Configure					
ool Name	Pool				
Address Prefix	2001:0DB8::0/64				
Prefix Delegation Pool	12 chars				
/alid Lifetime (60-4294967295)	sec				
Preferred Lifetime (60-4294967295)	sec				Apply
INS Server	2013::1				
NS Server	2013::1				
				Back	Apply
omain Name					
omain Name atic Bindings					1
oomain Name atic Bindings Static Bindings Address	2001:0DB8::0	O Static Bindings Prefix	2001:0DB8::0/64		
oomain Name atic Bindings Static Bindings Address Slient DUID	2001:0DB8::0 28 chars	O Static Bindings Prefix	2001:0DB8::0/64		

図 7-42 DHCPv6 Server Pool Settings (Configure) 画面

画面に表示される項目:

項目						
DHCPv6 Server Pool Configure						
Address Prefix	DHCPv6 サーバプール IPv6 ネットワークアドレスとプレフィクス長を入力します。(例;2015::0/64)					
Prefix Delegation Pool	DHCPv6 サーバプールプレフィクス委任名を 12 字以内で入力します。					
Valid Lifetime (60-4294967295)	指定プールに基づいた IPv6 アドレスが有効な状態を維持する時間 ( 秒 ) を入力します。初期値は「2592000」 (30 日)です。					
Preferred Lifetime (60-4294967295)	指定プールに基づいた IPv6 アドレスが preferred-lifetime 状態を維持する時間 ( 秒 ) を入力します。初期値 は「604800」(7 日)です。					
DNS Server	このプールに対する DNS サーバの IPv6 アドレスを入力します。					
Domain Name ドメイン名は、DNS と共にホスト名を解決する場合に DHCPv6 クライアントに使用されます。						
	Static Bindings					
Static Bindings Address	指定クライアントにアサインするスタティックバインディング IPv6 アドレスを入力します。					
Static Bindings Prefix	スタティックバインディング IPv6 ネットワークアドレスとプレフィクスを入力します。					
Client DUID	デバイスの DUID を 28 字以内で入力します。					
IAID	「Identity Association Identifier」(IAID/IA 識別子)を入力します。IAID クライアントに割り当てられる一時的ではないアドレス(IANA)の集合体を固有に識別します。					
Valid Lifetime (60-4294967295)	指定プールに基づいた IPv6 アドレスが有効な状態を維持する時間 ( 秒 ) を入力します。 初期値 : 「2592000」(30 日)					
Preferred Lifetime (60-4294967295)	指定プールに基づいた IPv6 アドレスが preferred-lifetime 状態を維持する時間 ( 秒 ) を入力します。 初期値 :「604800」(7 日)					

「Apply」をクリックし、設定内容を適用します。 「Back」をクリックすると前のページに戻ります。

### DHCPv6 Server Local Pool Settings(DHCPv6 サーバローカルプール設定)

DHCPv6 サーバローカルプールの表示および設定を行います。

#### Management > DHCP > DHCPv6 Server > DHCPv6 Server Local Pool Settings の順にメニューをクリックし、以下の画面を表示します。

DHCPV6 Server Loca	i Pool Settings		_	_	
DHCPv6 Server Local Pool					
Pool Name IPv6 Address/Prefix Length	11	2 chars			
Assigned Length					Apply
Pool Name	1	2 chars			Find
Total Entries: 1					
Pool Name	Prefix	Assigned Length	Free	In Use	
Pool	2016::/64	64	1	0	User Detail Delete
					1/1 K < 1 > > Go
User		Prefix			Interface

図 7-43 DHCPv6 Server Local Pool Settings 画面

#### 画面に表示される項目:

項目	説明
Pool Name	DHCPv6 サーバプール名を入力します。
IPv6 Address / Prefix Length	IPv6 プレフィクスアドレスとプレフィクス長を入力します。
Assigned Length	プール内のユーザに委任されるプレフィクス長を入力します。アサイン長の値はプレフィクス長の値より長い必要が あります。

「Apply」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「User Detail」をクリックするとユーザについての詳細が表示されます。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

### DHCPv6 Server Exclude Address(DHCPv6 サーバエクスクルードアドレス)

DHCPv6 サービスを希望するクライアントに割り当てない IPv6 アドレスの範囲を設定します。DHCPv6 サーバ、スイッチの IPv6 アドレスも含め、 全アドレスをクライアントへアサインすることが可能です。本画面では IPv6 アドレス / アドレス範囲をアサインメントから除外します。除外された アドレスはアドレスアサインメントにのみプールされます。

Management > DHCP > DHCPv6 Server > DHCPv6 Server Exclude Address の順にメニューをクリックし、以下の画面を表示します。

HCPv6 Server Exclude Ad	Iress		
ICT TO SETTER EXClude Au			
ow IPv6 Address	2013::1		
High IPv6 Address	2013::1		Apply
otal Entries: 1			
Range	Low IPv6 Address	High IPv6 Address	

図 7-44 DHCPv6 Server Excluded Address Settings 画面

画面に表示される項目:

項目	説明
Low IPv6 Address	除外する IPv6 アドレス(単体)、または除外 IPv6 アドレス範囲の開始 IPv6 アドレスを指定します。
High IPv6 Address	除外 IPv6 アドレス範囲の終了 IPv6 アドレスを指定します。

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

### DHCPv6 Server Binding(DHCPv6 サーババインディング)

DHCPv6 バインディング情報を参照、クリアします。

Management > DHCP > DHCPv6 Server > DHCPv6 Server Binding の順にメニューをクリックし、以下の画面を表示します。

DHCPv6 Server Binding						
DHCPv6 Server Binding	I					
IPv6 Address	2013::1	All		Find	Clear	
Total Entries: 0						
Client DUID		IPv6 Address	Preferred Lifetime	Valid L	ifetime	

図 7-45 DHCPv6 Server Binding 画面

画面に表示される項目:

項目	説明
IPv6 Address	表示、クリアするバインディングエントリの IPv6 アドレスを入力します。「AII」を選択するとバインディン グテーブルの全ての DHCPv6 クライアントプリフィクスバインディングが対象になります。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。 「Clear」ボタンをクリックして、本欄に入力したすべてのエントリをクリアします。
## DHCPv6 Server Interface Settings(DHCPv6 サーバインタフェース設定)

インタフェースごとに DHCPv6 サーバ状態を表示および設定します。

Management > DHCP > DHCPv6 Server > DHCPv6 Server Interface Settings の順にメニューをクリックし、以下の画面を表示します。

DHCPv6 Server Interfac	ce Settings		_		
DHCPv6 Server Interface Sett	ings				
Interface VLAN (1-4094) Rapid Commit	Disabled 🔽	Pool Name Preference	12 chars	Allow Hint	Apply
Interface Name	vlan1				Find
Total Entries: 1					
Interface Name	Pool Name	Rapid Commit	Preference	Hint From Client	
vlan1	Pool	Disabled	0	Allowed	Delete
				1/1 <	< 1 > > Go

図 7-46 DHCPv6 Server Interface Settings 画面

画面に表示される項目	:
------------	---

項目	説明
Interface VLAN	インタフェース VLAN を指定します。1-4094 の間で指定可能です。
Pool Name	DHCPv6 サーバプール名を入力します。
Rapid Commit	2 メッセージ交換の「Enabled」(有効)/「Disabled」(無効)を指定します。初期値は無効です。
Preference	希望値を指定します。「Allow Hint」を選択するとヒントが表示されます。
Interface Name	インタフェース名を入力します。

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

## DHCPv6 Server Operational Information (DHCPv6 サーバ操作情報)

DHCPv6 サーバ状態を表示します。

Management > DHCP > DHCPv6 Server > DHCPv6 Server Operational Information の順にメニューをクリックし、以下の画面を表示します。

DHCPv6 Server Operational Information	
DHCPv6 Server Operational Information	
Total Entries: 0	

図 7-47 DHCPv6 Server Operational Information 画面

# DHCP Relay (DHCP リレー)

### Management > DHCP > DHCP Relay

注意 DHCP Relay 機能を有効にした VLAN では、Unicast Relay が初期設定で有効のため、Option 82 付きの DHCP Request が破棄されます。 回避するには、Unicast Relay 機能を無効にするか、"ip dhcp relay information trust-all" を設定してください。

#### DHCP Relay Global Settings (DHCP リレーグローバル設定)

DHCP リレーグローバル設定の有効化および設定を行うことができます。

## Management > DHCP > DHCP Relay > DHCP Relay Global Settings の順にメニューをクリックし、以下の画面を表示します。

DHCP Relay Global Settings		
DHCP Relay Unicast State		
DHCP Relay Unicast State	Enabled Obisabled	Apply

図 7-48 DHCP Relay Global Settings 画面

画面に表示される項目:

項目	説明			
DHCP Relay Unicast State	DHCP リレーユニキャストをグローバルに「Enabled」(有効)/「Disabled」(無効)に指定します。			
 Apply」をクリック」 設定内容を適用				

「Apply」をクリックし、設定内容を適用します。

## DHCP Relay Pool Settings (DHCP リレープール設定)

DHCP リレーエージェントの DHCP リレープールの表示、設定を行います。

Management > DHCP > DHCP Relay > DHCP Relay Pool Settings の順にメニューをクリックし、以下の画面を表示します。

DHCP Relay Pool Settings	_	_	_	_
DHCP Relay Pool Settings				
Pool Name 32 chars				Apply
Total Entries: 1				
Pool Name	Source	Destination	Class	
DHCPpool	Edit	Edit	Edit	Delete
		ľ	l/1  < < 1	> >] Go
DHCPpool	Edit	Edit	Edit	Delete     >     Output     Go

図 7-49 DHCP Relay Pool Settings 画面

画面に表示される項目:

項目	説明	
Pool Name	32 文字以内でプール名を指定します。	
「Apply」をクリックし、設定内容を適用します。		

「Delete」をクリックすると指定のエントリを削除します。

「Edit」をクリックして、指定エントリの編集を行います。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

# 各プールエントリの編集を行う(Edit)

各エントリの「Source」「Destination」「Class」下にある「Edit」をクリックして、それぞれの内容を編集します。

#### ■ 「Source」の編集を行う場合

「Source」下の「Edit」をクリックします。以下の画面が表示されます。

DHCP Relay Poo	I Source Settings		_	_		
DHCP Relay Pool Sou	Irce Settings					
Pool Name Source IP Address	pool	Subnet Mask				Apply
Total Entries: 0						
	Source IP Addre	<b>S</b> S			Subnet Mask	
						Back

図 7-50 DHCP Relay Pool Source Settings 画面

#### 画面に表示される項目:

項目	説明
Source IP Address	クライアントパケットのソースサブネットを入力します。
Subnet Mask	ソースサブネットのネットマスクを入力します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。 エントリの削除を行う際は「Delete」をクリックします。 「Back」をクリックすると前の画面へ戻ります。

## ■「Destination」の編集を行う場合

「Destination」下の「Edit」をクリックします。以下の画面が表示されます。

DHCP Relay Pool Destina	tion Settings		
Pool Name VRF State VRF Name Relay Destination	Pool True I2 chars Global Global		Apply
Total Entries: 0			
	Destination Address	VRF State	VRF Name
			Back

図 7-51 DHCP Relay Pool Destination Settings 画面

#### 以下の項目が使用されます。

項目	説明
VRF State	VRF の状態を指定します。「True」「False」から指定可能です。
VRF Name	VRF インスタンス名を 12 字以内で入力します。 「Global」オプションを使用するとグローバルアドレスから IP アドレスを指定します。
Relay Destination	宛先 DHCP サーバの IP アドレスを入力します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

エントリの削除を行う際は「Delete」をクリックします。

「Back」をクリックすると前の画面へ戻ります。

# ■ 「Class」の編集を行う場合

「Class」下の「Edit」をクリックします。以下の画面が表示されます。

HCP Relay Pool Class	Settings	
Pool Name Class Name Total Entries: 1	DHCPpool Please Select	Apply
	Name	
Class		

図 7-52 DHCP Relay Pool Class Settings 画面

画面に表示される項目:

画面に衣示さ1	
項目	説明
Class Name	DHCP クラスの名前です。
シーンをあませる	

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。 エントリの削除を行う際は「Delete」をクリックします。「Back」をクリックすると前の画面へ戻ります。

#### クラス名の横の「Edit」をクリックすると以下の画面が表示されます。

	lass Eult Setungs			
DHCP Relay Pool Class E	alt Settings			
Pool Name	Pool			
Class Name	Class			
VRF State	True	<		
VRF Name	12 chars	Global		
Relay Target	2 2 D			Apply
Total Entries: 1				
Targ	et Address	VRF State	VRF Name	
192.	168.70.254	True		Delete
				Back

図 7-53 DHCP Relay Pool Class Settings 画面

画面に表示される項目:

項目	説明
VRF State	VRF の状態を指定します。「True」「False」から指定可能です。
VRF Name	VRF インスタンス名を 12 字以内で入力します。 「Global」オプションを使用するとグローバルアドレスから IP アドレスを指定します。
Relay Target	DHCP クラスで設定したオプションの方式とマッチするパケットをリレーする DHCP リレーターゲットを入力します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

エントリの削除を行う際は「Delete」をクリックします。

「Back」をクリックすると前の画面へ戻ります。

## DHCP Relay Information Settings(DHCP リレーインフォメーション設定)

Management > DHCP > DHCP Relay > DHCP Relay Information Settings の順にメニューをクリックし、以下の画面を表示します。

DHCP Relay Informat	tion Settings					
DHCP Relay Information G	lobal					
Information Trust All	Disabled		formation Check	lisabled 🔽		
Information Policy	Replace		formation Option	isabled 🔽		
Information Option VPN	Disabled	~				Apply
DHCP Relay Information						
Total Entries: 1						
Interface	Trusted	Check Relay	Policy	Option Insert	VPN Option	
vlan1	Disabled	Not Configured	Not Configured	Not Configured	Not Configured	Edit
					1/1 < < 1	> >  Go

図 7-54 DHCP Relay Information Settings 画面

画面に表示される項目:

項目	説明
Information Trust All	すべてのインタフェースで DHCP リレーエージェントによる IP DHCP リレーインフォメーションへの信頼を「Enabled」
	(有効)/「Disabled」(無効)に設定します。
Information Check	DHCP リレーエージェントによる、受信した DHCP リレーパケットにあるリレーエージェントインフォメーションの破棄、 または有効化を「Enabled」(有効)/「Disabled」(無効)に設定します。
Information Policy	<ul> <li>「Replace」、「Drop」または「Keep」を選択します。初期値は「Replace」です。</li> <li>Replace - DHCP クライアントから受信したパケット内の既存のリレー情報をスイッチの DHCP リレー情報に置き換えます。</li> <li>Drop - DHCP クライアントから受信したパケット内に既にリレー情報があった場合はそのパケットを削除します。</li> <li>Keep - DHCP クライアントから受信したパケット内の既存のリレー情報を保持します。</li> </ul>
Information Option	DHCP リクエストパケットのリレーの間にリレーエージェント情報(Option82)を挿入を「Enabled」(有効)/「Disabled」 (無効)に設定します。
Information Option VPN	VPN 機能の情報オプションを「Enabled」(有効)/「Disabled」(無効)にします。DHCP リクエストパケットのリレー におけるインタフェースの VPN 関連サブオプションの挿入を「Enabled」(有効)/「Disabled」(無効)に指定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

「Edit」をクリックして対応するインタフェースの編集を行うことができます。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

## DHCP Relay Information Option Format Settings (DHCP リレーインフォメーションオプションフォーマット設定)

DHCP 情報フォーマットの表示、設定を行います。

#### Management > DHCP > DHCP Relay > DHCP Relay Information Option Format Settings の順にメニューをクリックし、以下の画面を表示します。

DHCP Relay Inform	ation Option Format \$	Settings	
DHCP Relay Information	Option Format Global		
Information Format Remo	te ID Default [	<b>~</b>	
Information Format Circui	t ID Default [	✓	Apply
DHCP Relay Information	Option Format Type		
Linit From I	Port To Port	Format Type	Value
1 v eth1/	0/1 v eth1/0/1		32 chars
Unit 1 Settings			
Port	Format	Remote ID Value	Circuit ID Value
eth1/0/1			
eth1/0/2			
eth1/0/3			
eth1/0/4			
eth1/0/5			
eth1/0/6			

図 7-55 DHCP Relay Information Option Format Settings 画面

## 以下の項目が使用されます。

#### DHCP Relay Information Option Format Global

項目	説明
Information Format Remote ID	「DHCP information remote ID」のサブオプションを選択します。
	・ Default - リモート ID はシステムの MAC アドレスを使用します。
	・ User Define - リモート ID はユーザ定義の文字列を使用します。32 文字以内。
	・ Vendor2 - リモート ID はベンダ 2 を使用します。
	• Expert UDF - Expert UDF サーキット ID を使用します。スタンドアロンのユニットフォーマット選択します。
Information Format Circuit ID	「DHCP information circuit ID」のサブオプションを選択します。
	・ Default - 初期値のサーキット ID を使用します。
	・ User Define - ユーザ定義のサーキット ID を使用します。32 文字以内。
	・ Vendor1 - サーキット ID はベンダ 1 を使用します。
	・ Expert UDF - Expert UDF リモート ID を使用します。スタンドアロンのユニットフォーマット選択します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

## DHCP Relay Information Option Format Type

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	ポートの始点 / 終点を設定します。
Format	Expert UDF フォーマットを指定します。
Туре	リレー情報オプションの種類を選択します。「Remote ID」「Circuit ID」を選択できます。
Value	ベンダ定義の文字列を入力します。32 字まで指定可能です。
設定を変更する際は、必ず	「Apply」ボタンをクリックし、設定内容を適用してください。

DHCP Relay Information Profile Settings(DHCP リレー情報プロファイル設定)

DHCP リレー情報プロファイル設定を行います。

xample	AABBCCDDEEFF		Apply
vemale			
elimiter Number	2		
alimitar Numbar			
	Trone V		

図 7-56 DHCP Relay Information Profile Settings 画面

Management > DHCP > DHCP Relay > DHCP Relay Information Profile Settings の順にメニューをクリックし、以下の画面を表示します。

画面に表示される項目:	
項目	説明
	DHCP Relay Information Option MAC Format
Case	オプション 82 のネットワークアクセス認証に使用する MAC アドレスの形式を「Uppercase」(大文字)または「Lowercase」 (小文字)から選択します。(例 ;aa-bb-cc-dd-ee-ff(Lowercase)/AA-BB-CC-DD-EE-FF(Uppercase))
Delimiter	<ul> <li>MAC アドレスを入力する際の区切り「Hyphen」(ハイフン)、「Colon」(コロン)または「Dot」(ドット)を選択します。</li> <li>区切り文字を持たない場合には「None」を選択します。各項目の例は次の通りです。</li> <li>Hyphen - 「AA-BB-CC-DD-EE-FF」</li> <li>Colon - 「AA:BB:CC:DD:EE:FF」</li> <li>Dot - 「AA.BB.CC.DD.EE.FF」</li> <li>None - 「AABBCCDDEEFF」</li> </ul>
Delimiter Number	<ul> <li>MAC アドレスにおける区切り数を選択します。「1」「2」「5」から指定します。各項目の例は次の通りです。</li> <li>1 - 「AABBCC.DDEEFF」</li> <li>2 - 「AABB.CCDD.EEFF」</li> <li>5 - 「AA.BB.CC.DD.EE.FF」</li> </ul>
	DHCP Relay Information Profile Settings
Profile Name	オプション 82 のプロファイル名を入力します。
Format String	「Edit」をクリックし、ユーザ定義のオプション 82 フォーマット文字列を指定します。251 文字まで指定できます。ルールは次の通りです。
	<ul> <li>本パラメータは、16進数、ASCII 文字列、または16進数とASCII 文字列の組み合わせで指定することができます。 ASCII 文字列はダブルコーテーション("")で括られた "Ethernet" のような形になります。ダブルコーテーションに括られない文字は16進数として認識されます。</li> <li>フォーマットされたキー文字列はパケットに格納される前に変換される必要があります。フォーマットされたキー文字</li> </ul>
	<ul> <li>マダイ マイドインマーステクリネイン アドレス相当について、したいのないののないののないののないののないののないののないののないで、</li> <li>マタリは、「"%" + "5"+"1-32"+"keyword"+":":」のように ASCII 文字列、または 16 進数のどちらも含むことができます。</li> <li>「%」後の文字列はフォーマットされたキー文字列を意味します。</li> <li>「\$」または「0」はフィルインディケータです。文字長オプションに対してフォーマットキー文字列の対応方法を設定します。「\$」はスペースを埋め(0x20)、「0」は(0)を埋めます。「0」が初期値です。(オプション)</li> <li>「1-32」は文字長オプションです。どれくらいの文字やバイトがキー文字列に変換されるのかを指定します。もし変換済みキー文字列の実際の文字長が本オプションに指定された文字長よりも短い場合、フィルインディケータにより埋められます。そうでない場合、文字長オプションとフィルインディケータは無視され、実際の文字長がそのまま採用されます。</li> <li>(オプション)</li> <li>「keyword」はシステムの実際の値を基に変換されます。次の「Keyword」がサポートされています。:</li> <li>「devtype」は機器のモデル名です。「show version」コマンドのモジュール名項目から生成されます。ASCII 文字列のみ有効です。</li> <li>「sysname」はスイッチのシステム名を意味します。最大文字長は 128 です。ASCII 文字列のみ有効です。</li> <li>「portmac」はポートの MAC アドレスを意味します。ASCII 文字列、または 16 進数値で表示されます。ASCII 文字列フォーマットの場合、MAC アドレスを意味します。ASCII 文字列で表示されます。(例、「ip dhcp relay information option mac-format case」など)。16 進数フォーマットの場合、MAC アドレスのフォーマッ</li> </ul>
	<ul> <li>トは特定のコマンドでカスタムされます。(例,「ip dhcp relay information option mac-format case」など)。16 進数フォーマットの場合、MAC アドレスは16 進数として格納されます。</li> <li>「unit」はユニット ID を意味します。ASCII 文字列、または16 進数値で表示されます。スタンドアロンのデ バイスの場合、ユニット ID は「ip dhcp relay information option format remote-id」、そして「ip dhcp relay information option format circuit-id」コマンドで設定されます。</li> <li>「module」はモジュール ID 番号を意味します。ASCII 文字列、または16 進数値で表示されます。</li> <li>「port」はローカルポート番号を意味します。ASCII 文字列、または16 進数値で表示されます。</li> <li>「port」はローカルポート番号を意味します。ASCII 文字列、または16 進数値で表示されます。</li> <li>「svlan」はアウタ VLAN ID を意味します。ASCII 文字列、または16 進数値で表示されます。</li> <li>「cvlan」はインナ VLAN ID を意味します。ASCII 文字列、または16 進数値で表示されます。</li> <li>「cvlan」はインナ VLAN ID を意味します。ASCII 文字列がコマンドの最後のパラメータの場合(:) は無視されます。「%」と「:」の間のスペース(0x20) は無視され、他のスペースはパケットに格納されます。</li> <li>ASCII 文字列は「0-9」「a-z」「A-Z」「!」「@」「#」「\$」「^」「」「」「」「」」「+」「」」「-」「=」「\」「[」「]」「{」 「!」「」「」」「!」「」」「」」「」」「」」「&gt;」「&gt;」「+」「」」「-」「=」「\」「[」「]」「{」 「!」「:」「!」「'」「'」「」」「」「」」「&gt;」「」とスペース、フォーマットキー文字列のいかなる組み合わせも可能 です。「\」はエスケープキャラクターになります。「」以後の特別なキャラクターはキャラクターそのものになります。 例えば「%」は「%」を意味します。フォーマットキー文字列の開始インディケータではありません。フォーマットキー 文字列内のスペースもまたパケットに格納されます。</li> <li>16 進数値は「0-9」「A+」「a-f」」とスペースとフォーマットキー文字列からなります。フォーマットキー文字列は16</li> <li>進数を比ずーー」「のみサポート」」「ます、フォーマットキー文字列がのスペースしたサーマー」「</li> </ul>

# 第7章 Management (スイッチの管理)

「Apply」をクリックし、設定内容を適用します。 「Delete」をクリックすると指定のエントリを削除します。 「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。 「Edit」をクリックして、指定エントリの編集を行います。 設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

## DHCP Relay Port Settings(DHCP リレーポート設定)

DHCP リレーポートの設定、表示を行います。

#### Management > DHCP > DHCP Relay > DHCP Relay Port Setings の順にメニューをクリックし、以下の画面を表示します。

DHCP Relay Port Settings	
DHCP Relay Port Settings	
Unit From Port To Port 1	State       Disabled     Apply
Onit 1 Settings Port	State
eth1/0/1	Enabled
eth1/0/2	Enabled
eth1/0/3	Enabled
eth1/0/4	Enabled
eth1/0/5	Enabled
eth1/0/6	Enabled
eth1/0/7	Enabled
eth1/0/8	Enabled

図 7-57 DHCP Relay Port Settings 画面

#### 画面に表示される項目:

項目	説明
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。
State	指定のポートの DHCP リレーを「Enabled」(有効)/「Disabled」(無効)に設定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

## DHCP Local Relay VLAN(DHCP ローカルリレー VLAN)

VLAN、またはグループ VLAN のリレー設定を行います。

#### Management > DHCP > DHCP Relay > DHCP Local Relay VLAN の順にメニューをクリックし、以下の画面を表示します。

DHCP Local Relay VLAN					
DHCP Local Relay VLAN Setting	gs				
DHCP Local Relay VID List DHCP Local Relay VID List	1,3-5	All VLANs	State	Disabled	Apply

図 7-58 DHCP Local Relay VLAN 画面

#### 画面に表示される項目:

項目	説明
DHCP Local Relay VID List	DHCP ローカルリレーを適用する VLAN ID を入力します。「All VLANs」にチェックを入れるとすべての VLAN を選択します。
State	指定の VLAN の DHCP ローカルリレーを「Enabled」(有効)/「Disabled」(無効)に設定します。
シーシー シー・シー・シー・シー・シー・シー・シー・シー・シー・シー・シー・シー・シー・シ	

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。



DHCP リレーポートが無効の場合、ポートは受信 DHCP パケットのリレー / ローカルリレーを行いません。

# DHCPv6 Relay (DHCPv6 リレー)

# DHCPv6 Relay Global Settings (DHCPv6 リレーグローバル設定)

スイッチの DHCPv6 リレー機能を設定します。

Management > DHCP > DHCPv6 Relay > DHCPv6 Relay Global Settings の順にメニューをクリックし、以下の画面を表示します。

DHCPv6 Relay Global Settings		_		
DHCPv6 Relay Remote ID Settings				
IPv6 DHCP Relay Remote ID Format	Default	✓ Star	Idalone Unit Format	
IPv6 DHCP Relay Remote ID UDF	ASCII	✔ 128	chars	
IPv6 DHCP Relay Remote ID Policy	Keep	~		
IPv6 DHCP Relay Remote ID Option	Disabled	~		Apply
DHCPv6 Relay Interface ID Settings				
IPv6 DHCP Relay Interface ID Format	Default	✓ Star	Idalone Unit Format	
IPv6 DHCP Relay Interface ID Policy	Keep	~		
IPv6 DHCP Relay Interface ID Option	Enabled	~		Apply
DHCPv6 Relay Information Option MAC Form	at			
Case	Uppercase	~		
Delimiter	None	~		
Delimiter Number	2	~		
Example	AABBCCDDEEFF			Apply

図 7-59 DHCPv6 Relay Global Settings 画面

#### 以下の項目を使用して設定、表示を行います。

項目	説明
	DHCPv6 Relay Remote ID Settings
IPv6 DHCP Relay Remote ID Format	リモート ID のサブタイプを指定します。 「Default」「CID With User Define」「User Define」「Expert UDF」から選択します。
Standalone Unit Format	「Expert UDF」を選択すると、ここでスタンドアロンユニットのフォーマットを選択します。「0」「1」が選択可能です。
IPv6 DHCP Relay Remote ID UDF	リモート ID のユーザ定義項目 (UDF) の入力形式 を選択します。「ASCII」「Hex」から選択します。 ・ ASCII - 「ASCII」文字列で入力します。最大 128 文字まで入力可能です。 ・ HEX - 16 進数文字列で入力します。最大 256 文字まで入力可能です。
IPv6 DHCP Relay Remote ID Policy	<ul> <li>DHCPv6 リレーエージェントのオプション 37 フォワーディングポリシーを選択します。</li> <li>「Drop」「Keep」から選択します。</li> <li>・ Drop - DHCP クライアントから受信したパケット内に既にオプション 37 リレー情報があった場合はそのパケットを削除します。</li> <li>・ Keep - DHCP クライアントから受信したパケット内の既存のオプション 37 リレー情報を保持します。</li> </ul>
IPv6 DHCP Relay Remote ID Option	DHCP IPv6 リクエストパケットのリレーの間にリレーエージェント情報 (Option37) の挿入を 「Enabled」(有 効)/「Disabled」(無効)に設定します。
	DHCPv6 Relay Interface ID Settings
IPv6 DHCP Relay Interface ID Format	インタフェース ID のフォーマットを指定します。 「Default」「CID」「User Define」「Vendor1」「Expert UDF」から選択します。
Standalone Unit Format	「Expert UDF」を選択すると、ここでスタンドアロンユニットのフォーマットを選択します。「0」「1」が選択可能です。
IPv6 DHCP Relay Interface ID Policy	<ul> <li>DHCPv6 リレーエージェントのオプション 18 フォワーディングポリシーを「Drop」「Keep」から選択します。</li> <li>Drop - DHCP クライアントから受信したパケット内に既にオプション 18 リレー情報があった場合はそのパケットを削除します。</li> <li>Keep - DHCP クライアントから受信したパケット内の既存のオプション 18 リレー情報を保持します。</li> </ul>
IPv6 DHCP Relay Interface ID Option	DHCP IPv6 リクエストパケットのリレーの間にリレーエージェント情報 (Option18) を挿入を 「Enabled」(有 効)/「Disabled」(無効)に設定します。
	DHCPv6 Relay Information Option MAC Format
Case	オプション 82 のネットワークアクセス認証に使用する MAC アドレスの形式を「Uppercase」(大文字)ま たは「Lowercase」(小文字)から選択します。(例 ;aa-bb-cc-dd-ee-ff(Lowercase)/AA-BB-CC-DD-EE-FF (Uppercase))

項目	説明
Delimiter	<ul> <li>MAC アドレスを入力する際の区切り「Hyphen」(ハイフン)、「Colon」(コロン)または「Dot」(ドット)</li> <li>を選択します。区切り文字を持たない場合には「None」を選択します。各項目の例は次の通りです。</li> <li>Hyphen - 「AA-BB-CC-DD-EE-FF」</li> <li>Colon - 「AA.BB:CC:DD:EE:FF」</li> <li>Dot - 「AA.BB.CC.DD.EE.FF」</li> <li>None - 「AABBCCDDEEFF」</li> </ul>
Delimiter Number	<ul> <li>MAC アドレスにおける区切り数を選択します。「1」「2」「5」から指定します。各項目の例は次の通りです。</li> <li>1 - 「AABBCC.DDEEFF」</li> <li>2 - 「AABB.CCDD.EEFF」</li> <li>5 - 「AA.BB.CC.DD.EE.FF」</li> </ul>

「Apply」ボタンをクリックし、設定を適用します。

# DHCPv6 Relay Interface Settings(DHCPv6 リレーインタフェース設定)

DHCPv6 リレーインタフェース設定の表示と設定を行います。

## Management > DHCP > DHCPv6 Relay > DHCPv6 Relay Interface Settings の順にメニューをクリックし、以下の画面を表示します。

HCPv6 Relay Interface Settings —			
nterface VLAN (1-4094)			
Destination IPv6 Address	2012::100		
Output Interface VLAN (1-4094)			Apply
nterface VLAN (1-4094)			Find
otal Entries: 1			
Interface	Destination IPv6 Address	Output Interface	
vlan1	2015::10	vlan1	Delete
		1/1 < < 1	> >  G

図 7-60 DHCPv6 Relay Interface Settings 画面

#### 画面に表示される項目:

項目	説明
Interface VLAN	DHCPv6 リレーの VLAN を 1 から 4094 の間で指定します。
Destination IPv6 Address	DHCPv6 リレーの宛先アドレスを入力します。
Output Interface VLAN	リレー宛先の送信インタフェースを入力します。

「Apply」ボタンをクリックし、設定を適用します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

「Delete」をクリックすると指定のエントリを削除します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

## DHCPv6 Relay Remote ID Profile Settings(DHCPv6 リレーリモート ID プロファイル設定)

DHCPv6 リレーリモート ID プロファイル設定の表示と設定を行います。DHCPv6 リレーオプション 82 のプロファイルの作成に使用されます。

## Management > DHCP > DHCPv6 Relay > DHCPv6 Relay Remote ID Profile Settings の順にメニューをクリックし、以下の画面を表示します。

HCPV6 Relay Remote	ID Profile Settings			_
HCPv6 Relay Remote ID Pro	file Settings			
Profile Name	32 chars		Apply	Find
Total Entries: 1				
Profile N	ame	Format String		
Profil	e .		Edit	Delete
			1/1 📧 < 1	G



項目	説明
Profile Name	オプション 82 のプロファイル名を入力します。
Format String	「Edit」をクリックし、ユーザ定義のオプション 82 フォーマット文字列を指定します。251 文字まで指定できます。ルー ルは次の通りです。
	<ul> <li>本パラメータは、16 進数、ASCII 文字列、または 16 進数と ASCII 文字列の組み合わせで指定することができます。</li> <li>ASCII 文字列はダブルコーテーション("")で括られた "Ethernet"のような形になります。ダブルコーテーションに括られない文字は 16 進数として認識されます。</li> </ul>
	<ul> <li>フォーマットされたキー文字列はパケットに格納される前に変換される必要があります。フォーマットされたキー文字列は、「"%" +"\$"+"1-32"+"keyword"+":":」のように ASCII 文字列、または 16 進数のどちらも含むことができます。</li> <li>「%」後の文字列はフォーマットされたキー文字列を意味します。</li> </ul>
	<ul> <li>「\$」または「0」はフィルインディケータです。文字長オプションに対してフォーマットキー文字列の対応方法を設定します。「\$」はスペースを埋め(0x20)、「0」は(0)を埋めます。「0」が初期値です。(オプション)</li> <li>「1-32」は文字長オプションです。どれくらいの文字やバイトがキー文字列に変換されるのかを指定します。もし変</li> </ul>
	換済みキー文字列の実際の文字長が本オプションに指定された文字長よりも短い場合、フィルインディケータによ り埋められます。そうでない場合、文字長オプションとフィルインディケータは無視され、実際の文字長がそのま ま採用されます。(オプション)
	・「keyword」はシステムの実際の値を基に変換されます。次の「Keyword」がサポートされています。:
	- 「devtype」は機器のモデル名です。「show version」コマンドのモジュール名項目から生成されます。ASCII 文字 列のみ有効です。
	- 「sysname」はスイッチのシステム名を意味します。最大文字長は 128 です。ASCII 文字列のみ有効です。 - 「ifdescr」は「ifDescr」(IF-MIB) から生成されます。ASCII 文字列のみ有効です。
	- 「portmac」はポートの MAC アドレスを意味します。ASCII 文字列、または 16 進数値で表示されます。ASCII 文 字列フォーマットの場合、MAC アドレスのフォーマットは特定のコマンドでカスタムされます。(例,「ip dhcp relay information option mac-format case」など)。16 進数フォーマットの場合、MAC アドレスは 16 進数とし て格納されます。
	- 「sysmac」はシステムの MAC アドレスを意味します。ASCII 文字列で表示されます。MAC アドレスのフォーマットは特定のコマンドでカスタムされます。(例 ,「ip dhcp relay information option mac-format case」など)。16 進数フォーマットの場合、MAC アドレスは 16 進数として格納されます。
	- 「unit」はユニット ID を意味します。ASCII 文字列、または 16 進数値で表示されます。スタンドアロンのデ バイスの場合、ユニット ID は「ip dhcp relay information option format remote-id」、そして「ip dhcp relay information option format circuit-id」コマンドで設定されます。
	- 「module」はモジュール ID 番号を意味します。ASCII 文字列、または 16 進数値で表示されます。 - 「port」はローカルポート番号を意味します。ASCII 文字列、または 16 進数値で表示されます。 - 「svlan」はアウタ VLAN ID を音味します。ASCII 文字列。または 16 進数値で表示されます。
	- 「cvlan」はインナ VLAN ID を意味します。ASCII 文字列、または 16 進数値で表示されます。
	・「:」はフォーマット文字列の終わりを意味します。フォーマット文字列がコマンドの最後のパラメータの場合 (:)
	は無視されます。「%」と「:」の間のスペース (0x20) は無視され、他のスペースはパケットに格納されます。
	● ASCII 文字例は「0-9」「a-z」「A-Z」「!」「@」「#」「\$」「%」「^」」&」「*」「(」「)」「_」「+」「 」「-」「=」「\」「[」「]」「]」「]」「 □ たいていていていていていたろ組み合わせも可能
	です。「」はエスケープキャラクターになります。「」以後の特別なキャラクターはキャラクターそのものになります。
	例えば「\%」は「%」を意味します。フォーマットキー文字列の開始インディケータではありません。フォーマットキー
	<ul> <li>又字列内の人へ一人もまたバケットに格納されます。</li> <li>16 進数値は「0-9」「A-F」「a-F」とスペースとフォーマットキー文字列からたります。フォーマットキー文字列は 16</li> </ul>
	進数をサポートするキーワードのみサポートします。フォーマットキー文字列外のスペースは無視されます。

以下の項目を使用して設定、表示を行います。

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

# DHCPv6 Relay Interface ID Profile Settings(DHCPv6 リレーインタフェース ID プロファイル設定)

DHCPv6 リレーインタフェース ID プロファイル設定の表示と設定を行います。DHCPv6 リレーオプション 82 のプロファイルを作成に使用されます。

Management > DHCP > DHCPv6 Relay > DHCPv6 Relay Interface ID Profile Settings の順にメニューをクリックし、以下の画面を表示します。

DHCPv6 Relay Remote	ID Profile Settings			_
DHCPv6 Relay Remote ID Pro	ofile Settings			
Profile Name	32 chars	]	Apply	Find
Total Entries: 1				
Profile	lame	Format String		
Profi	le		Edit	Delete
			1/1  < < 1	Go

図 7-62 DHCPv6 Relay Interface ID Profile Settings 画面

一回に表示される項目:
-------------

項目	説明
Profile Name	オプション 82 のプロファイル名を入力します。
Format String	「Edit」をクリックし、ユーザ定義のオプション 82 フォーマット文字列を指定します。251 文字まで指定できます。ルー ルは次の通りです。
	<ul> <li>本パラメータは、16 進数、ASCII 文字列、または 16 進数と ASCII 文字列の組み合わせで指定することができます。</li> <li>ASCII 文字列はダブルコーテーション("") で括られた "Ethernet" のような形になります。ダブルコーテーションに括られない文字は 16 進数として認識されます。</li> </ul>
	<ul> <li>フォーマットされたキー文字列はパケットに格納される前に変換される必要があります。フォーマットされたキー文字列は、「"%" +"\$"+"1-32"+"keyword"+":":」のように ASCII 文字列、または 16 進数のどちらも含むことができます。</li> <li>「%」後の文字列はフォーマットされたキー文字列を意味します。</li> </ul>
	<ul> <li>・「\$」または「0」はフィルインディケータです。文字長オプションに対してフォーマットキー文字列の対応方法を設定します。「\$」はスペースを埋め(0x20)、「0」は(0)を埋めます。「0」が初期値です。(オプション)</li> <li>「1,22」は京島長式プレーンです。じたくこいの京島やボスーがた。京島町に変換されるのわちが良します。すし変更になられていた。</li> </ul>
	<ul> <li>・ 「1-32」は文字長オフションです。とれくらいの文字やハイトがキー文字列に変換されるのかを指定します。もし変換済みキー文字列の実際の文字長が本オプションに指定された文字長よりも短い場合、フィルインディケータにより埋められます。そうでない場合、文字長オプションとフィルインディケータは無視され、実際の文字長がそのまたが思われます。(オプンニン)</li> </ul>
	ま採用されます。(オフンヨフ) ・「keyword」はシステムの実際の値を其に変換されます。次の「Keyword」がサポートされています。
	- 「devtype」は機器のモデル名です。「show version」コマンドのモジュール名項目から生成されます。ASCII 文字 列のみ有効です。
	- 「sysname」はスイッチのシステム名を意味します。最大文字長は 128 です。ASCII 文字列のみ有効です。 - 「ifdescr」は「ifDescr」(IF-MIB) から生成されます。ASCII 文字列のみ有効です。
	- 「portmac」はポートの MAC アドレスを意味します。ASCII 文字列、または 16 進数値で表示されます。ASCII 文 字列フォーマットの場合、MAC アドレスのフォーマットは特定のコマンドでカスタムされます。(例,「ip dhcp relay information option mac-format case」など)。16 進数フォーマットの場合、MAC アドレスは 16 進数とし て格納されます。
	- 「sysmac」はシステムの MAC アドレスを意味します。ASCII 文字列で表示されます。MAC アドレスのフォーマットは特定のコマンドでカスタムされます。(例,「ip dhcp relay information option mac-format case」など)。16 進数フォーマットの場合、MAC アドレスは 16 進数として格納されます。
	- 「unit」はユニット ID を意味します。ASCII 文字列、または 16 進数値で表示されます。スタンドアロンのデ バイスの場合、ユニット ID は「ip dhcp relay information option format remote-id」、そして「ip dhcp relay information option format circuit-id」コマンドで設定されます。
	<ul> <li>「module」はモジュール ID 番号を意味します。ASCII 文字列、または 16 進数値で表示されます。</li> <li>「port」はローカルポート番号を意味します。ASCII 文字列、または 16 進数値で表示されます。</li> <li>「svlan」はアウタ VLAN ID を意味します。ASCII 文字列、または 16 進数値で表示されます。</li> </ul>
	<ul> <li>「cvlan」はインナ VLAN ID を意味します。ASCII 文字列、または 16 進数値で表示されます。</li> <li>「:」はフォーマット文字列の終わりを意味します。フォーマット文字列がコマンドの最後のパラメータの場合(:) け無視されます「%」と「:」の問のスペース(0x20)け無視され、他のスペースはパケットに終続されます。</li> </ul>
	・ ASCII 文字列は「0-9」「a-z」「A-Z」「!」「@」「#」「\$」「%」「^」「&」「*」「(」「)」「_」「+」「 」「-」「=」「\」「[」「]」「}」「;」「'」「'」「'」「'」「,」「,」「<」「>」「'」とスペース、フォーマットキー文字列のいかなる組み合わせも可能
	です。「\」はエスケープキャラクターになります。「\」以後の特別なキャラクターはキャラクターそのものになります。 例えば「\%」は「%」を意味します。フォーマットキー文字列の開始インディケータではありません。フォーマットキー 文字列中のスペースたまたパケットに教練されます。
	<ul> <li>         × エッリンワイ、「へもまた」の ットに 伯柄 されます。     </li> <li>         16 進数値は「0-9」「A-F」「a-f」とスペースとフォーマットキー文字列からなります。フォーマットキー文字列は 16         進数をサポートするキーワードのみサポートします。フォーマットキー文字列外のスペースは無視されます。     </li> </ul>

「Apply」をクリックし、設定内容を適用します。 「Delete」をクリックすると指定のエントリを削除します。 「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。 設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

# DHCPv6 Relay Format Type Settings(DHCPv6 リレーフォーマットタイプ設定)

DHCPv6 リレーフォーマットタイプ設定の表示と設定を行います。各ポートの「expert UDF」文字列のの DHCPv6 オプション 37 とオプション 18 を 設定します。

## Management > DHCP > DHCPv6 Relay > DHCPv6 Relay Format Type Settings の順にメニューをクリックし、以下の画面を表示します。

DHCPv6 Relay Format Type Settings						
DHCPv6 Relay Form	at Type Settings					
Unit	From Port eth1/0/1	To Port eth1/0/1	Type Remote ID 💌	Format Type Expert UDF 32 chars	Apply	
Unit 1 Settings						
	Port		Remote ID Forma	It Type Expert UDF	Interface ID Format Type Expert UDF	
	eth1/0/1					
	eth1/0/2					
	eth1/0/3					
	eth1/0/4					
	eth1/0/5					
	eth1/0/6					
	eth1/0/7					
	eth1/0/8					

図 7-63 DHCPv6 Relay Format Type Settings 画面

画面に表示される項目:

項目	説明
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。
Туре	以下のタイプから指定します。
	Remote ID -「Expert UDF」フォーマットタイプ文字列を DHCPv6 オプション 37 で指定します。
	Interface ID-「Expert UDF」フォーマットタイプ文字列を DHCPv6 オプション 18 で指定します。
Format Type Expert UDF	指定ポートで使用する「expert UDF」文字列のフォーマットを設定します。

「Apply」ボタンをクリックし、設定を適用します。

# DHCPv6 Relay Port Settings(DHCPv6 リレーポート設定)

DHCPv6 リレーポート設定を行います。

Management > DHCP > DHCPv6 Relay > DHCPv6 Relay Port Settings の順にメニューをクリックし、以下の画面を表示します。

DHCPv6 Relay Port Settings	
DHCPv6 Relay Port Settings	
Unit         From Port         To Port           1         V         eth1/0/1         eth1/0/1	State Enabled Apply
Unit 1 Settings	
Port	State
eth1/0/1	Enabled
eth1/0/2	Enabled
eth1/0/3	Enabled
eth1/0/4	Enabled
eth1/0/5	Enabled
eth1/0/6	Enabled
eth1/0/7	Enabled
eth1/0/8	Enabled

図 7-64 DHCPv6 Relay Port Settings 画面

## 画面に表示される項目:

項目	説明
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。
State	指定ポートの DHCPv6 リレーポート機能を「Enabled」(有効)/「Disabled」(無効)に指定します。

# DHCPv6 Local Relay VLAN(DHCPv6 ローカルリレー VLAN 設定)

DHCPv6 ローカルリレー VLAN 設定を行います。DHCPv6 ローカルリレーが有効の場合、クライアントからのリクエストパケットにオプション 37 と 18 を追加します。オプション 37 のチェックステートが有効の場合、クライアントからのリクエストパケットをチェックし、オプション 37DHCPv6 リレー機能が含まれる場合、パケットを破棄します。無効の場合、ローカルリレー機能は、オプション 37 が有効であろうとなかろうと、常にオプショ ン 37 をリクエストパケットに追加します。DHCPv6 ローカルリレー機能はサーバからのパケットを直接クライアントに転送します。

Management > DHCP > DHCPv6 Relay > DHCPv6 Local Relay VLAN の順にメニューをクリックし、以下の画面を表示します。

DHCPv6 Local Relay VLA	N		
DHCPv6 Local Relay VLAN Settin	gs		
DHCPv6 Local Relay VID List DHCPv6 Local Relay VID List	1,3-5 All VLANs	State Disabled	Apply

図 7-65 DHCPv6 Local Relay VLAN 画面

画面に表示される項目:

項目	説明		
DHCPv6 Local Relay VID List	DHCPv6 ローカルリレー VLAN ID を入力します。 一つ以上の VLAN ID が入力可能です。 「ALL VLANs」オプションを指定すると、すべての VLAN が対象になります。		
State	指定 VLAN の DHCPv6 ローカルリレー機能を「Enabled」(有効)/「Disabled」(無効)に指定します。		

「Apply」ボタンをクリックし、設定を適用します。

注意 「DHCPv6 リレーポート」が無効の場合、ポートは受信した DHCPv6 パケットをリレー / ローカルにリレーしません。

# **DHCP Auto Configuration**(DHCP 自動コンフィグ設定)

DHCP 自動コンフィグ機能の設定を行います。

Management > DHCP > DHCP Auto Configuration の順にメニューをクリックし、以下の画面を表示します。

DHCP Auto Configuration				
DHCP Auto Configuration				
Auto Configuration State	Enabled	Disabled		Apply
Note: If autoconfig State enabled, it won't take effect until reboot.				
図 7-66 DHCP Auto Co	nfiguration 画面			

画面に表示される項目:

項目	説明
Auto Configuration State	自動設定機能の「Enabled」(有効)/「Disabled」(無効)を設定します。

# DHCP Auto Image Settings (DHCP 自動イメージ設定)

ここでは DHCP 自動イメージ設定を行います。スイッチのスタートアップ時に、DHCP サーバからの「DHCP OFFER」メッセージにその IP アドレス が含まれる外部 TFTP サーバから、イメージファイルを取得する機能を提供します。システムはこのイメージファイルを起動イメージとして使用し ます。システム起動時に自動イメージ機能が有効の場合、スイッチは自動的に DHCP クライアントになります。

DHCP クライアントは DHCP サーバからのネットワーク設定を取得しアクティブになり、DHCP サーバは TFTP サーバ IP アドレスとメッセージ付き イメージファイル名を含みます。スイッチはこの情報を受け、指定 TFTP サーバからの TFTP ダウンロード機能を実行します。このステージではシス テムはコンソールにダウンロード設定を表示します。このレイアウトは「download firmware」コマンドを使用した場合と、同様になります。ファー ムウェアのダウンロードが完了すると、スイッチはただちに再起動します。

自動コンフィグ機能 (auto-configuration) と自動イメージ (auto-image) 機能のどちらも有効な場合、システムはイメージファイルを先にダウンロードし、次にコンフィグをダウンロードし再起動します。

スイッチはダウンロードされたファームウェアを必ずチェックします。現在のバージョンと同じ場合は、スイッチは自動イメージプロセスを終了します。ですが、自動コンフィグの場合は実行します。

本機能は自動コンフィグ機能と似ています。イメージファイル、コンフィグファイル両方とも同じ TFTP サーバに格納されており、DHCP オプショ ンの項目は自動イメージ機能のみのために使用されておらず、自動コンフィグにも適用されています。TFTP サーバ IP アドレスは「DHCP siaddr」項 目オプション 66、またはオプション 150 に存在します。オプション 66 とオプション 150、そして「siaddr」項目が DHCP 回答メッセージに同時に 存在する場合、オプション 150 が先に解決されます。システムが TFTP サーバとの接続に失敗した場合、システムはオプション 66 を解決し、まだ TFTP サーバとの接続を確立できない場合「siaddr」は最後のチョイスになります。

スイッチがオプション 66 を TFTP サーバ名取得に使用する場合、オプション 6 を先に解決し DNS サーバの IP アドレスを取得します。スイッチが DNS サーバとの接続に失敗、またはオプション 6 が回答メッセージに含まれていない場合、スイッチはシステムで手動で設定された DNS サーバへの接続を試みます。

オプション 67 は、DHCP ヘッダの「file」項目が DHCP オプションに使用されている時に、ブートファイルの識別に使用されます。これは DHCP 自 動コンフィグモード中のみで使用され、DHCP 自動イメージモードでは使用されません。さらなる情報については、「RFC 2132」を参照してください。 イメージファイル名を指定する場合、DHCP オプション 125 (RFC 3925) が必ず使用されます。スイッチは「enterprise-number1」項目をチェックす る必要があります。もしこの値が D-Link ベンダ ID (171) と違う場合、スイッチはプロセスを停止します。このオプションが一つ以上の項目を含んで いる場合、最初の「enterprise-number1」エントリのみ使用されます。

Management > DHCP > DHCP Auto Image Settings の順にメニューをクリックし、以下の画面を表示します。

DHCP Auto Image Settings				
DHCP Auto Image Settings				
DHCP Auto Image State	Disabled			
DHCP Auto Image Timeout (1-65535)	50 sec	Apply		

図 7-67 DHCP Auto Image Settings 画面

#### 画面に表示される項目:

項目	説明
DHCP Auto Image State	DHCP 自動イメージ機能を「Enabled」(有効)/「Disabled」(無効)にします。
DHCP Auto Image Timeout	DHCP 自動イメージ機能のタイムアウト時間を指定します。1 から 65535(秒)で指定可能です。

# DNS(ドメインネームシステム)

DNS(Domain Name System)は、ドメイン名と IP アドレスの関連付けをコンピュータ間の通信で行います。DNS サーバは「name-to-address」翻 訳を実行し、ドメイン名とアドレスの変換を行うためにいくつかのネームサーバと連絡を取る必要があります。ドメインネームサービスを行うデバ イスのアドレスは、DHCP または BOOTP サーバから得る場合と、初期設定時に手動で OS に設定する場合があります。

# DNS Global Settings(DNS グローバル設定)

本項目ではグローバルに DNS を設定します。

## Management > DHCP > DNS Global Settings の順にメニューをクリックし、以下の画面を表示します。

DNS Global Settings			
DNS Global Settings			
IP DNS Lookup Static State	Enabled 🗸		
IP DNS Lookup Cache State	Enabled 🗸		
IP Domain Lookup	Disabled 🗸		
IP Name Server Timeout (1-60)	3 sec		
IP DNS Server	Disabled 🗸		Apply
IP Domain Lookup Source Interface			
Source Interface State	Disabled 🔽		
Interface Type	VLAN 🔽	Interface ID (1-4094)	Apply

図 7-68 DNS Global Settings 画面

画面に表示される項目:

項目	説明				
DNS Global Settings					
IP DNS Lookup Static State	IP DNS ルックアップスタティックを「Enabled」(有効)/「Disabled」(無効)に指定します。				
IP DNS Lookup Cache State	IP DNS ルックアップキャッシュを「Enabled」(有効)/「Disabled」(無効)に指定します。				
IP Domain Lookup	IP ドメインルックアップを「Enabled」(有効)/「Disabled」(無効)に指定します。				
IP Name Server Timeout	指定ネームサーバからの回答を待つタイムアウトを1から60(秒)で指定します。				
IP DNS Server DNS サーバを「Enabled」(有効)/「Disabled」(無効)します。					
	IP Domain Lookup Source Interface				
Source Interface State	ソースインタフェースを指定します。				
Interface Type	インタフェース種類を「Loopback」「Mgmt」「VLAN」から指定します。				
Interface ID	インタフェース ID を指定します。ループバックインタフェースの場合、「1」から「8」、 管理インタフェース (Mgmt) の場合、常に「0」、VLAN インタフェースの場合、「1」から「4094」になります。				

# DNS Name Server Settings(DNS ネームサーバ設定)

スイッチに DNS のネームサーバを作成します。

Management > DNS > DNS Name Server Settings の順にメニューをクリックし、以下の画面を表示します。

NS Name Server Settings				
VRF Name	12 chars			
Name Server IPv4	14 - 14 ( - 4)			
Name Server IPv6	2233::1			Apply
/RF Name	12 chars			Find
otal Entries: 1				
VRF Name	Na	me Server		
	19	2 168 70 1	Delete	

図 7-69 DNS Name Server Settings 画面

画面に表示される項目:

項目	説明
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Name Server IPv4	選択して DNS サーバの IPv4 アドレスを入力します。
Name Server IPv6	選択して DNS サーバの IPv6 アドレスを入力します。
「Apply」ボタンをク	クリックし、設定を適用します。
「Find」をクリック	して、入力した情報に基づく特定のエントリを検出します。

「Delete」ボタンをクリックして、指定エントリを削除します。

# DNS Host Settings (DNS ホスト名設定)

ホスト名のスタティックマッピングの設定とホストテーブルの IP アドレスを設定します。

Management > DNS > DNS Host Settings の順にメニューをクリックし、以下の画面を表示します。

tatic Host Settings				
VRF Name	12 chars			
IP Address	200 chara			- Arch
VPE Name	12 chare			Find
Static Total Entrice: 1				Clear Al
static rotal chules. I				
Dynamic Total Entries: 0				
Dynamic Total Entries: 0 VRF Name	Host Name	IPv4/IPv6 Address	Aging Time	

図 7-70 DNS Host Settings 画面

画面に表示される項目:	
項目	説明
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Host Name	ホスト名を入力します。
IP Address	ホストの IPv4 アドレスを入力します。
IPv6 Address	ホストの IPv6 アドレスを入力します。

「Apply」ボタンをクリックし、設定を適用します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Clear All」をクリックすると入力したエントリを全てクリアします。

「Delete」ボタンをクリックして、指定エントリを削除します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

# NTP(ネットワークタイムプロトコル)

スイッチが持つ時計の時刻を同期するための通信プロトコルの設定を行います。

# NTP Global Settings (NTP グローバル設定)

NTP のグローバル設定を行います。

# Management > NTP > NTP Global Settings の順にメニューをクリックし、以下の画面を表示します。

NTP Global Settings	_		
NTP State			
NTP State	O Enabled	Disabled	Apply
NTP Authentication State			
NTP Authentication State	Enabled	O Disabled	Apply
NTP Update Calendar			
NTP Update Calendar	O Enabled	Disabled	Apply
NTP Settings			
NTP Master Stratum (1-15)		✓ Default	
NTP May Associations (1-64)	32		Apply
図 7-71 NTP Global Settings	画面		

画面に表示される項目:

# NTP Server Settings(NTP サーバ設定)

NTP サーバの設定を行います。

Management > NTP > NTP Server Settings の順にメニューをクリックし、以下の画面を表示します。

TP Server Settings							
<ul> <li>IP Address</li> <li>Version (1-4)</li> <li>Min Poll (3-16)</li> <li>Profer</li> </ul>	4 6 Falso		O IPv6 Address Key ID (1-255) Max Poll (4-17)	2233: 10	1		Analy
Total Entries: 1							
NTP Serv	ver	Version	Key ID	Prefer	Min Poll	Max Poll	
192.168.70	.100	4	1	False	6	10	Edit Delete

図 7-72 NTP Server Settings 画面

画面に表示される項目	:
------------	---

項目	説明
IP Address	NTP サーバの IPv4 アドレスを指定します。
IPv6 Address	NTP サーバの IPv6 アドレスを指定します。
Version	NTP サーバのバージョンを指定します。1 から 4 で指定します。
Key ID	認証鍵 ID を指定します。1 から 255 で指定します。
Min Poll	NTP メッセージ送信の最小ポーリング間隔を指定します。3 から 16(秒)で指定します。
Max Poll	NTP メッセージ送信の最大ポーリング間隔を指定します。4 から 17(秒)で指定します。
Prefer	対象のサーバが好ましいか否かをリストに振り分けます。True または False から指定します。

「Apply」ボタンをクリックし、設定を適用します。

「Delete」で指定エントリを削除します。

「Edit」をクリックして、指定エントリの編集を行います。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

# NTP Peer Settings (NTP ピア設定)

NTP のピア設定を行います。

Management > NTP > NTP Peer Settings の順にメニューをクリックし、以下の画面を表示します。

NTP Peer Settings		_		_			
NTP Peer Settings							
IP Address			O IPv6 Address	2233:	:1		
Version (1-4)	4		Key ID (1-255)				
Min Poll (3-16)	6		Max Poll (4-17)	10			
Prefer	False	~					Apply
Total Entries: 1							
NTP Peer		Version	Key ID	Prefer	Min Poll	Max Poll	
192.168.70.10	)1	4	1	False	6	10	Edit Delete
						1/1	< < 1 > >  Go

図 7-73 NTP Peer Settings 画面

画面に表示される項目:	
-------------	--

項目	説明
IP Address	NTP ピアの IPv4 アドレスを指定します。
IPv6 Address	NTP ピアの IPv6 アドレスを指定します。
Version	NTP ピアのバージョンを指定します。1 から 4 で指定します。
Key ID	認証鍵 ID を指定します。1 から 255 で指定します。
Min Poll	最小ポーリング間隔を指定します。3 から 16(秒)で指定します。
Max Poll	最大ポーリング間隔を指定します。4 から 17(秒)で指定します。
Prefer	対象のピアが好ましいか否かをリストに振り分けます。True または False から指定します。

「Apply」ボタンをクリックし、設定を適用します。「Delete」で指定エントリを削除します。

# NTP Access Group Settings(NTP アクセスグループ設定)

NTP のアクセスグループ設定を行います。

Management > NTP > NTP Access Group Settings の順にメニューをクリックし、以下の画面を表示します。

NTP Access Group Settings		
NTP Access Group Settings		
Default		
O IP Address	Netmask · · ·	
O IPv6 Address 2233::1	IPv6 Mask	
Ignore No Serve No Trust Version No	Peer No Query No Modify	Apply
Total Entries: 2		
NTP Access Group	Flag	
default	Version	Delete
192.168.70.21 255.255.255.0	Nomodify	Delete
	1/1 < 1	> >  Go

図 7-74 NTP Access Group Settings 画面

画面に表示される項目:	
-------------	--

項目	説明
Default	チェックを入れるとデフォルトのエントリ(0.0.0.0/0.0.0.0)が最小の優先値でリストに含まれます。
IP Address	ホスト / ネットワークの IPv4 アドレスを指定します。
Netmask	ホスト / ネットワークの IPv4 ネットワークマスクを指定します。
IPv6 Address	ホスト / ネットワークの IPv6 アドレスを指定します。
IPv6 Mask	ホスト / ネットワークの IPv6 ネットワークマスクを指定します。
Ignore	全ての NTP 関連パケットを無視します。
No Serve	全ての NTP 関連パケットを拒否します。(NTP コントロールクエリは除く)
No Trust	全ての暗号認証されていない NTP 関連パケットを拒否します。
Version	全ての NTP バージョンと合致しない NTP 関連パケットを拒否します。
No Peer	全ての認証されていないピアの NTP 関連パケットを拒否します。
No Query	全ての NTP コントロールクエリを拒否します。
No Modify	全てのサーバ状態を変更しようとする NTP コントロールクエリを拒否します。

「Apply」ボタンをクリックし、設定を適用します。「Delete」で指定エントリを削除します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

# NTP Key Settings (NTP 鍵設定)

NTP の鍵設定を行います。

Management > NTP > NTP Key Settings の順にメニューをクリックし、以下の画面を表示します。

NTP Key Settings				
NTP Control Key				
NTP Control Key (1-255)		None None		Apply
NTP Request Key				
NTP Request Key (1-255)		None None		Apply
NTP Key Settings				
Key ID (1-255)				
MD5	32 chars			Apply
Total Entries: 1				
Trusted Key	Key ID	Кеу Туре	Value	
	1	MD5	MD5MD5MD5MD5	Delete
			1/1 < < 1	1 > >  Go

図 7-75 NTP Key Settings 画面

## 画面に表示される項目:

項目	説明						
	NTP Control Key						
NTP Control Key	NTP コントロールキー(制御鍵)を1から255で指定します。「None」を選択するとNTP コントロールキーは使用しません。						
NTP Request Key							
NTP Request Key	NTP リクエストキー(要求鍵)を 1 から 255 で指定します。「None」を選択すると NTP リクエストキーは使用しません。						
	NTP Key Settings						
Key ID	NTP キーを 1 から 255 で指定します。						
MD5	MD5 NTP キーを指定します。32 文字まで指定可能です。						
Trusted Key	ピア NTP システムのキーが認証に合致するための設定を行います。						

「Apply」ボタンをクリックし、設定を適用します。「Delete」で指定エントリを削除します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

# NTP Interface Settings(NTP インタフェース設定)

NTP のインタフェース設定を行います。

Management > NTP > NTP Interface Settings の順にメニューをクリックし、以下の画面を表示します。

NTP Interface Settings		
NTP Interface Settings		
Total Entries: 1		
Interface Name	NTP State	
vlan1	Enabled	Edit
	1/1	< < 1 > > Go

図 7-76 NTP Interface Settings 画面

画面に表示される項目:

項目	説明
NTP State	「Edit」をクリックして該当インタフェース上の NTP 機能の「Enabled」(有効)/「Disabled」(無効)を指定します。
 「Apply」ボタンをクリック	1設定を適用します。「Delete」で指定エントリを削除します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

# NTP Associations (NTP アソシエーション)

NTP アソシエーションを表示します。

```
Management > NTP > NTP Assosiations の順にメニューをクリックし、以下の画面を表示します。
```

al Entries: 2								
Remote	Local	Stratum	Poll	Reach	Delay	Offset	Dispersion	
+192.168.70.100	0.0.00	16	64	0	0.00000	0.000000	4.00000	Show Detail
=192.168.70.123	0.0.0.0	16	64	0	0.00000	0.000000	4.00000	Show Detail
						1/1 <	< 1 >	>

図 7-77 NTP Assosiations 画面

指定エントリ横の「Show Detail」ボタンをクリックし、該当 NTP アソシエーションの詳細を表示します。

Detail						
Remote	192.168.70.100	Local	0.0.0.0			
Our mode	client	Peer mode	unspec			
Stratum	16	Precision	-7			
Leap	11	RefID	[INIT]			
RootDistance	0.00000	RootDispersion	0.00000			
PPoll	10	HPoll	6			
KeyID	1	Version	4			
Association	8355	Reach	000			
Jnreach	0	Flash	0x1400			
Timer	4294967093s	Flags	Config			
Reference Time	00000000.00000000 Thu, Feb 7	Originate Timestamp	00000000.00000000 Thu, Feb 7			
Receive Timestamp	00000000.00000000 Thu, Feb 7	Transmit Timestamp	00000000.00000000 Thu, Feb 7			
Filter Delay	0.00000 , 0.00000 , 0.00000 ,	Filter Offset	0.000000, 0.000000, 0.000000,			
ilter Order	7, 6, 5, 4, 3, 2, 1, 0	Offset	0.000000			
Delay	0.00000	Error Bound	4.00000			
Filter Error	0.08838					

図 7-78 NTP Assosiations - Detail 画面

# NTP Status (NTP ステータス)

NTP ステータスを表示します。

```
Management > NTP > NTP Status の順にメニューをクリックし、以下の画面を表示します。
```

NTP Status	
NTP Status	
	NTP Status
Leap Indicator	Unsynchronized
Stratum	16
Precision	-8
Root Distance	0.00000 s
Root Dispersion	0.00000 s
Reference ID	[STEP]
Reference Time	00000000.00000000 Thu, Feb 7 2036 6:28:16.00000
System Flags	Monitor NTP Kernel Stats
Jitter	0.003906 s
Stability	0.000 ppm
Auth Delay	0.000000 s

図 7-79 NTP Status 画面

# IP Source Interface (IP ソースインタフェース)

IP ソースインタフェースを設定します。

Management > IP Source Interface の順にメニューをクリックし、以下の画面を表示します。

IP Source Interface				
IP TFTP Source Interface				
Source Interface State Interface Type	Disabled VLAN	Interface ID (1-4094)		Apply
IP FTP Source Interface				
Source Interface State Interface Type	Disabled VLAN	Interface ID (1-4094)	0	Apply
IP RCP Source Interface				
Source Interface State Interface Type	Disabled VLAN V	Interface ID (1-4094)	0	Apply
IP SSH Source Interface				
Source Interface State Interface Type	Disabled VLAN V	Interface ID (1-4094)	0	Apply

図 7-80 IP Source Interface 画面

### 画面に表示される項目:

項目	説明			
	IP TFTP Source Interface			
Source Interface State	IP TFTP ソースインタフェースを指定します。			
Interface Type	インタフェース種類を「Loopback」「Mgmt」「VLAN」から指定します。			
Interface ID	インタフェース ID を指定します。ループバックインタフェースの場合、「1」から「8」、			
	管理インタフェース(Mgmt)の場合、常に「0」、VLAN インタフェースの場合、「1」から「4094」になります。			
	IP FTP Source Interface			
Source Interface State	IP FTP ソースインタフェースを指定します。			
Interface Type	インタフェース種類を「Loopback」「Mgmt」「VLAN」から指定します。			
Interface ID	インタフェース ID を指定します。ループバックインタフェースの場合、「1」から「8」、			
	管理インタフェース(Mgmt)の場合、常に「0」、VLAN インタフェースの場合、「1」から「4094」になります。			
	IP RCP Source Interface			
Source Interface State	IP RCP ソースインタフェースを指定します。			
Interface Type	インタフェース種類を「Loopback」「Mgmt」「VLAN」から指定します。			
Interface ID	インタフェース ID を指定します。ループバックインタフェースの場合、「1」から「8」、			
	管理インタフェース(Mgmt)の場合、常に「0」、VLAN インタフェースの場合、「1」から「4094」になります。			
	IP SSH Source Interface			
Source Interface State	IP SSH ソースインタフェースを指定します。			
Interface Type	インタフェース種類を「Loopback」「Mgmt」「VLAN」から指定します。			
Interface ID	インタフェース ID を指定します。ループバックインタフェースの場合、「1」から「8」、			
	管理インタフェース(Mgmt)の場合、常に「0」、VLAN インタフェースの場合、「1」から「4094」になります。			

「Apply」ボタンをクリックし、設定を適用します。



注意 NTP Server の機能において、経路に従って送信元の IP が決定されるため、構成によりクライアントは同期に失敗する場合が有ります。 また、Loopbask Interface は未サポートです。

# File System (ファイルシステム設定)

## フラッシュファイルシステムを使用する理由

古いスイッチシステムでは、ファームウェア、コンフィグレーション、およびログ情報は固定アドレスとサイズを持つフラッシュに保存されます。 最大のコンフィグレーションファイルは 2M バイトであり、現在のコンフィグレーションが 40K バイトにすぎなくても、フラッシュストレージスペー スの 2M バイトを消費します。また、コンフィグレーションファイル番号とファームウェア番号は固定されています。コンフィグレーションファイ ルまたはファームウェアサイズが元々設計されたサイズを超えている場合、互換性の問題が発生します。

## 使用するシステムにおけるフラッシュファイルシステム

フラッシュファイルシステムは、フラッシュメモリにおける柔軟なファイル操作を提供します。すべてのファームウェア、コンフィグレーション情報、 および Syslog ログ情報はフラッシュ内のファイルに保存されます。これは、すべてのファイルが取得したフラッシュスペースが固定されておらず、 実ファイルサイズであることを意味します。フラッシュスペースが十分であれば、より多くのコンフィグレーションファイルまたはファームウェア ファイルをダウンロードできます。また、フラッシュファイル情報の表示やファイル名の変更、および削除するコマンドを使用することができます。 その上、必要に応じて、起動用のランタイムイメージや動作するコンフィグレーションファイルを設定できます。

ファイルシステムに不具合がある場合、Z-モデムを使用して直接システムにバックアップファイルをダウンロードすることができます。

Management > File System の順にメニューをクリックし、以下の画面を表示します。



図 7-81 File System 画面

#### 画面に表示される項目:

項目	説明
Unit	設定を行うユニットを指定します。
Path	パスの文字列を入力します。

「Path」に現在のパスを入力し、「Go」ボタンをクリックすると入力したパスに遷移します。 「Copy」をクリックすると指定のファイルをスイッチへコピーします。 「<u>C:</u>」リンクをクリックすると、「C:」ドライブに遷移します。

「<u>C:</u>」リンクをクリックすると、以下の画面が表示されます。

it th		1 c:/	~				[	Go
Pre	vious	Create	Directory	Сору				
Index	Info	Attr	Size (byte)	Update Time	Name			80 <i>8</i>
	Chi Ibilat	-rw	15400620	Dec 28 2015 10:58:09	R1.00.015.had	Boot Up	Rename	Delete
1	RUN(*)							
1 2	RUN(*)	-rw	15396400	Dec 21 2015 09:39:30	R1.00.014.had	Boot Up	Rename	Delete
1 2 3	RUN(*) RUN CFG(*)	-rw -rw	15396400 46371	Dec 21 2015 09:39:30 Dec 28 2015 11:11:12	R1.00.014.had config.cfg	Boot Up Boot Up	Rename Rename	Delete Delete

図 7-82 File System (Drive) 画面

画面に表示される項目:

項目	説明
Go	入力したパスへ進みます。
Previous	前のページに戻ります。
Create Directory	スイッチのファイルシステムに新しいディレクトリを作成します。
Сору	指定ファイルをスイッチにコピーします。
Boot Up	起動用のブートアップイメージとして指定したランタイムイメージを設定します。
Rename	指定ファイルを変更します。
Delete	ファイルシステムから指定ファイルを削除します。

## ファイルのコピー

「Copy」ボタンをクリックすると、以下の画面が表示されます。

File System						
Unit Path	1 C:	~				Go
Copy File Source Destination	Unit Unit	1 V 1 V	startup-config 🔽	C:/config.cfg C:/config.cfg	Replace	Cancel

図 7-83 Flash File System Settings 画面 - Copy

このスイッチのファイルシステムにファイルをコピーする場合、送信元と送信先のパスを入力します。

項目	説明
Source	コピー元ファイルのあるスイッチのユニットIDとコピーされるファイルのタイプを選択します。「startup-config」「Source
	File」から選択します。「Source File」選択時にはファイルパスを指定欄に入力します。
Destination	宛先スイッチのユニット ID とコピーファイルのタイプを選択します。「startup-config」「running-config」「Destination
	File」から選択します。「Destination File」選択時にはファイルパスを指定欄に入力します。「Replace」にチェックする
	と現在実行中のコンフィグファイルを指定のコンフィグファイルと差し替えます。

「Apply」ボタンをクリックして、コピーを開始します。「Cancel」ボタンをクリックすると処理は破棄されます。

注意 ブートコンフィグファイルが破損しているとスイッチは自動的に初期設定に戻ります。

注意 ブートイメージファイルが破損しているとスイッチは自動的にバックアップイメージファイルを使用します。

# Stacking (スタッキング設定)

本スイッチは、スイッチのスタックをサポートしています。9個のスイッチをコンソールポート、MGMT ポート経由の IP アドレス、または Telnet、 GUI インタフェース (Web)、SNMP を使用した RJ-45/SFP/SFP+ の複数 IP アドレスで1つに結合し、管理することができます。SFP+ ポートを使用し たスイッチのスタックにより、ネットワークのアップグレードをリーズナブルでコストパフォーマンスの高い方法で実現します。これによりお使い のネットワークの信頼性、サービス性、そして可用性が向上します。

- Duplex Chain Duplex Chain トポロジはチェーン・リンク形式でスイッチをスタックします。この方法を使用すると、一方向のデータ転送だけが可能となります。そして、1 カ所中断が発生すると、データ転送は明らかに影響を受けます。
- Duplex Ring Duplex Ring は、データが双方向に転送できるようにリングまたは円の形式でスイッチをスタックします。このトポロジは、リング に1カ所中断が発生しても、データはスタック内のスイッチ間のスタックケーブル経由で転送されるため高い冗長性を実現できます。

本シリーズのスイッチは光ファイバケーブルを使用した SFP +モジュール、または SFP +ダイレクトアタッチケーブルを使用して、物理的にスタックすることが可能です。最後の4ポートのみ物理スタックに使用できます。

注意 スタッキングが有効にしている時、最後の SFP+ ポート 2/4 つは他のデバイスやスイッチなどへのアップリンクとして使用できません。ス タッキングはこれらのポートを使用してのみ可能です。

物理スタックでは「2 ポート」または「4 ポート」スタッキングコンフィグレーションを設定し、有効にする必要があります。「2 ポート」スタッキング設定時にはスイッチ間のフルデュプレックススピードで、最大 40Gbps が使用可能です。「4 ポート」スタッキング設定時にはスイッチ間のフル デュプレックススピードで、最大 80Gbps が使用可能です。

以下は、光ファイバケーブルを使用した SFP +モジュール、または SFP +ダイレクトアタッチケーブルを使用して「2 ポート」スタッキング設定、 「Duplex Chain」構成での物理スタック図です。



図 7-84 Duplex Chain でスタックされているスイッチ画面 (SFP +)

光ファイバケーブルを使用した SFP +モジュール、または SFP +ダイレクトアタッチケーブルを使用して「2 ポート」スタッキング設定、「Duplex Ring」構成での物理スタック図です。



図 7-85 Duplex Ring でスタックされているスイッチ画面 (SFP +)

「Stacking Input/Output logical port 1」(SIO1)と「SIO2」は、それぞれ論理スタッキングポートのペアです。4 ポートスタッキングを行う 場合、1 つの論理スタッキングポートのペア(例:スイッチ A の SIO2 × 2)が、接続先スイッチの同じ SIO(例:スイッチ B の SIO1 × 2) に接続するようにしてください。それぞれ異なるスイッチや異なる SIO ポートに接続された場合、安定したスタッキング接続を保証できま せん。SIO1/SIO2 に対応する物理ポートについては、「Stacking Bandwidth(スタッキング帯域)」を参照してください。

以下の図は、4ポートスタッキングにおける適切な接続例です。





以下の図では、異なる SIO に接続されているため、安定したスタッキング接続を保証できません。



# スタック内のスイッチ役割

各トポロジにおいて、各スイッチはスイッチスタックにおける役割を果たします。各スイッチには役割を設定でき、スイッチスタック機能により自動的に決定することもできます。スイッチをスタックする場合に、3 つの役割があります。

#### ● プライマリマスタ

プライマリマスタは、スタックのリーダです。スタックの通常操作、モニタ操作、およびトポロジの実行をメンテナンスします。本スイッチは、 スイッチスタック内にあるスイッチにスタックユニット番号の割り当て、コンフィグレーションの同期、コマンドの送信を行います。プライマ リマスタには、スタックを物理的に構成する前、またはすべての優先度が同じである場合には最も数字の低い MAC アドレスを持つスイッチに 決定します。また、スタックが自動的に決定される前に、最も高い優先度(低い番号ほど優先度は高くなります。)を本スイッチに割り当てるこ とで手動で設定することができます。プライマリマスタは、スイッチの前面パネルの一番右にある LED によって Box ID と「H」が表示されます。

● バックアップマスタ

バックアップマスタは、プライマリマスタに対するバックアップであり、プライマリマスタが故障、またはスタックから取り外される場合に、 プライマリマスタの機能を引き継ぎます。また、スタック内で隣接するスイッチの状態をモニタし、プライマリマスタによって割り当てられた コマンドを実行して、プライマリマスタの動作状態をモニタします。バックアップマスタは、スタックを物理的に構成する前、またはすべての 優先度が同じである場合には2番目に数字の低い MAC アドレスに決定します。また、スタックが自動的に決定される前に、2番目に高い優先度(低 い番号ほど優先度は高くなります。)を本スイッチに割り当てることで手動で設定することができます。バックアップマスタは、物理的にスイッ チの前面パネルの一番右にある7個のセグメント LED によって Box ID と「h」が表示されます。

• スレーブ

スレーブスイッチは、残りのスイッチスタックを構成します。プライマリマスタまたはバックアップマスタスイッチではありません。プライマリ マスタおよびバックアップマスタが故障、またはスタックから取り外される場合に、それらの機能を引き継ぎます。スレーブスイッチは、マスタ に要求された操作を実行して、スタックとスタックトポロジにある近接スイッチの状態をモニタします。さらに、バックアップマスタがプライマ リマスタになるとバックアップマスタのコマンドに従います。スレーブスイッチは、バックアップマスタがプライマリマスタに移行する場合、バッ クアップマスタが故障、またはスイッチから取り外される場合に、セルフチェックを行い、自身がバックアップマスタになるかどうかを決定します。 プライマリマスタとバックアップマスタの両方が故障、またはスイッチから取り外される場合、プライマリマスタになるかどうか決定します。こ れらの役割は、はじめに優先度によって決定され、さらに優先度が同じである場合は、最も低い MAC アドレスによって決定されます。

スイッチが希望したトポロジで構成されると、スタックは機能する状態に到達するまでに3つの過程を経由します。

• 初期化状態

これは、スタックの最初の状態で、ランタイムコードが設定および初期化され、システムは各スイッチが適切に機能していることを検証するために周辺機器の診断を行います。

#### ・ マスタ選出状態

コードがロードされ、初期化されると、スタックはマスタ選出状態になり、使用されるトポロジのタイプを検出し、プライマリマスタ、バッ クアップマスタの順に選出します。

#### • 同期状態

プライマリマスタとバックアップマスタが確立すると、プライマリマスタがスイッチにスタックユニット番号を割り当て、すべてのスイッチに構成を同期させ、プライマリマスタの構成に基づき、残りのスイッチにコマンドを送信します。

これらの手順が終了すると、スイッチスタックは正常な操作モードに入ります。

#### スタックスイッチのスワップ

スイッチのスタック機能は、動作中のスタック内またはスタック外のスイッチの「ホットスワップ」をサポートしています。いくつかの簡単な条件 により、電源オフやスタック内のスイッチ間のデータ転送に大きな影響を与えずに、スタックからのスイッチの取り外しやスタックへの追加を行う ことができます。

スイッチが動作中のスタックに「ホットインサート」される場合、設定された優先度や MAC アドレスなど新たに追加されたコンフィグレーション によって、新しいスイッチはプライマリマスタ、バックアップマスタまたはスレーブとなる可能性があります。しかし、共に以前の選出過程を経て、 その結果、プライマリマスタとバックアップマスタを持った2つのスタックが追加されると、新しいプライマリマスタが、優先度または MAC アド レスに基づいて、既存のプライマリマスタから選出されます。このプライマリマスタは、ホットインサートされた新しいスイッチすべてにプライマ リマスタの全役割を引き継ぎます。この過程は、検出処理が完了するまで1.5 秒ごとにスイッチスタックを通して循環するディスカバリパケットを 使用して行われます。

「ホットリムーブ」の動作は、スタックが既に動作している場合にスタックからデバイスを取り外すことを意味します。ホットリムーブは、指定した間にデバイスからハートビートパケットを受信しない場合、またはスタックポートの中の1つのリンクがダウンした場合に、スタックによって検出されます。デバイスが一度取り外されると、残りのスイッチは、スタックトポロジデータベースを更新し、変更を反映します。スタックから3つの役割(プライマリマスタ、バックアップマスタ、またはスレーブ)のどれか1つが取り外される場合には、異なる過程がそれぞれの特定デバイス取り外しに発生します。

スレーブデバイスが取り外される場合、プライマリマスタは unit leave メッセージの使用を通じ、このデバイスのホットリムーブを他のスイッチに 通知します。スタック内のスイッチは、取り外されたユニットの ARP などのダイナミックに学習されたデータベースをクリアします。

バックアップマスタがホットリムーブされると、新しくバックアップマスタが前述の選出過程を経由して選ばれます。スタック内のスイッチは、取り外されたユニットの ARP などのダイナミックに学習されたデータベースをクリアします。その後、データベース同期がスタックによって完了した際に、バックアップマスタはプライマリマスタのバックアップを開始します。

プライマリマスタが取り外されると、バックアップマスタはプライマリマスタの役割を引き受けて、新しいバックアップマスタが選出過程を経て選 ばれます。スタック内のスイッチは、取り外されたユニットの ARP などのダイナミックに学習されたデータベースをクリアします。新しいプライマ リマスタは、スタックとネットワーク内の矛盾を避けるために、前のプライマスタの MAC と IP アドレスを引き継ぎます。

プライマリマスタとバックアップマスタの両方が取り外される場合、選出過程では、直ちに処理を行い、新しいプライマリマスタとバックアップマスタを決定します。スタック内のスイッチは、取り外されたユニットの ARP などのダイナミックに学習されたデータベースをクリアします。スタティックなスイッチ構成は、スタックに存在するスイッチに関するデータベースに残りますが、それらの機能には影響されません。



スタックが検出過程にある時、Box IDの矛盾があると、そのデバイスは特別なスタンドアロントポロジモードに入ります。ユーザはデバイス情報の取得、Box IDの設定、保存、および再起動だけ行うことができます。すべてのスタックポートが無効とされ、エラーメッセージがスタック内の各デバイスのローカルコンソールポートに生成されます。ユーザは、Box IDを再設定し、スタックを再起動する必要があります。

# Physical Stacking(物理スタッキング)

物理スタッキングの設定を行います。

Management > Stacking > Physical Stacking の順にメニューをクリックし、以下の画面を表示します。

			_					_
hysical Stat	cking							
Stacking Mo	de	Enabled	O Disable	be				Apply
Stack Preen	npt	Enabled	O Disable	ed				Apply
Trap State		O Enabled	Disable	ed				
tack ID								
Current Unit	ID 1	V	New Box	CID	Auto	Priority (1-63)		Apply
						Street and all strengths in the		
Topology:		Duplex_Chain			My Box ID:	1		
Master ID: Rev Count:		1			BK Master ID:	95.9		
Box Count.								
Box ID	User Set	Module Name	Exist	Priority	MAC	PROM Version	Runtime Version	H/W Version
1	Auto	DGS-3630-28TC	Exist	32	F0-7D-68-36-30-00	1.00.006	1.00.015	A1
	1. 17	NOT_EXIST	No	-	-	-	÷	-
2		NOT EVICT	No	-			-	-
2 3	1.1	NOT_EXIST	140					
2 3 4		NOT_EXIST	No		-		-	-
2 3 4 5	•	NOT_EXIST NOT_EXIST	No	•	•	•	•	-
2 3 4 5 6	•	NOT_EXIST NOT_EXIST NOT_EXIST NOT_EXIST	No No No	•	•	•	•	•
2 3 4 5 6 7	- - -	NOT_EXIST NOT_EXIST NOT_EXIST NOT_EXIST	No No No No	•	- - - -	+ + + +	- - -	• • •

図 7-86 Physical Stacking 画面

## 画面に表示される項目:

項目	説明			
	Physical Stacking			
Stacking Mode	初期値では「Disabled」(無効)になっています。			
Stack Preempt	「Enabled」(有効)/「Disabled」(無効)にします。新しいデバイスが現在のスタックトポロジに追加した際にマスタロール が変更されないことを保証するために使用されます。「Disabled」(無効)を選択すると、スタックが安定した後にマスタの 優先度は0になります。			
Trap State				
	Stack ID			
Current Unit ID	スタックにおけるスイッチの現在のユニット番号を選択します。			
New Box ID	「Current Unit ID」で選択したスタック内のスイッチに新しくボックス番号 (1-9) を指定します。「Auto」はスイッチスタック 内のスイッチに自動的にボックス番号を割り当てます。			
Priority (1-63)	スイッチの優先度番号を表示します。低い値ほど高いプライオリティを示します。スタック内で最も低い優先度番号を持つ ボックス (スイッチ)が、プライマリマスタです。プライマリマスタスイッチは、スイッチスタックにおけるアプリケーショ ンを設定するために使用されます。			

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

## Stacking Bandwidth (スタッキング帯域)

本項目ではスタッキング帯域の設定、表示を行います。物理スタッキングは有効化と、2 ポート /4 ポートでのスタッキング設定を行う必要があります。 「2 ポート」スタッキング設定時にはスイッチ間のフルデュプレックススピードで、最大 40Gbps が使用可能です。

- ・ DGS-3630-28TC/28SC/28PC は物理ポート 27(SIO1)と 28(SIO2)を「2 ポート」スタッキングに使用します。
- ・ DGS-3630-52TC/52PC は物理ポート 51 (SIO1) と 52 (SIO2) を「2 ポート」スタッキングに使用します。

「4 ポート」スタッキング設定時にはスイッチ間のフルデュプレックススピードで、最大 80Gbps が使用可能です。

- ・ DGS-3630-28TC/28SC/28PC は物理ポート 25(SIO1)、26(SIO2)、27(SIO1)、28(SIO2)を「4 ポート」スタッキングに使用します。
- ・ DGS-3630-52TC/52PC 物理ポート 49(SIO1)、50(SIO2)、51(SIO1)、52(SIO2)を「4 ポート」スタッキングに使用します。

「Stacking Input/Output logical port 1」(SIO1)と「SIO2」は、それぞれ論理スタッキングポートのペアです。4 ポートスタッキングを行う場合、1 つの論理スタッキングポートのペア(例:スイッチAのSIO2×2)が、接続先スイッチの同じSIO(例:スイッチBのSIO1×2)に接続するようにしてください。それぞれ異なるスイッチや異なるSIOポートに接続された場合、安定したスタッキング接続を保証できません。

注意 スタッキング帯域のボックス ID、プライオリティの設定はスイッチをスタックする前に設定する必要があります。

#### Management > Stacking > Stacking Bandwidth の順にメニューをクリックし、以下の画面を表示します。

Stacking Bandwid	th		
Stacking Bandwidth	2-Port		Apply
Box ID	User Set Bandwidth	SIO1 Active Bandwidth	SIO2 Active Bandwidth
1	2-port	Down	Down
2	-	-	-
3	-	- · · · ·	· ·
4	-		
5			
6	•	-	*
7		-	
8	•		
9			•

図 7-87 Stacking Bandwidth 画面

画面に表示される項目:

項目	説明	
Stack Bandwidth	スタッキング帯域を「2-Port」「4-Port」から指定します。	

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

# Virtual Stacking (SIM) (仮想スタック設定 (SIM))

仮想(SIM)スタッキングの設定を行います。

# シングル IP マネジメント(SIM)の概要

D-Link シングル IP マネジメントとは、スタックポートまたはモジュールを使用する代わりにイーサネット経由でスイッチをスタックする方法です。 シングル IP マネジメント機能を利用する利点を以下に示します。

- 1. ネットワークを拡大し、増大する帯域幅に対する要求に対処しながら、小規模のワークグループや、ワイヤリングクローゼット(ユーザ接続エ リア)を簡単に管理できるようになります。
- 2. ネットワークに必要な IP アドレス数を減らします。
- 3. スタック接続のために特別なケーブル配線を必要とせず、他のスタック技術ではトポロジ上の問題になる距離的制限を取り除きます。

D-Link シングル IP マネジメント(以下 SIM と呼びます)機能を搭載するスイッチには、以下の基本的なルールがあります。

- SIM はスイッチのオプション機能であり、CLI または Web インタフェース経由で簡単に「Enabled」(有効) /「Disabled」(無効) にできます。また、 SIM グループはご使用のネットワーク内でスイッチの操作に影響を与えることはありません。
- SIMには3つのクラスのスイッチがあります。Commander Switch (CS) はグループのマスタスイッチ、Member Switch (MS) はCS によって SIM グルー プのメンバとして認識されるスイッチ、Candidate Switch (CaS) は SIM グループに物理的にリンクはしているが、 SIM グループのメンバとして 認識されていないスイッチです。
- ・1つの SIM グループには、Commander Switch(CS)を1つだけ持つことができます。
- 特定の SIM グループ内のすべてのスイッチは、同じ IP サブネット(ブロードキャストドメイン)内にある必要があります。ルータを越えた位置 にあるメンバの設定はできません。
- ・ 1 つの SIM グループには、Commander Switch (番号:0)を含めずに、最大 32 台のスイッチ(番号:1-32)が所属できます。
- 同じIPサブネット(ブロードキャストドメイン)内のSIMグループ数に制限はありませんが、各スイッチは、1つのSIMグループにしか所属することができません。
- ・ マルチプル VLAN が設定されていると、SIM グループはスイッチ上のデフォルト VLAN だけを使用します。
- ・ SIM は SIM をサポートしていないデバイスを経由することができます。そのため CS から 1 ホップ以上はなれたスイッチを管理することができます。

SIM グループは1つのエンティティとして管理されるスイッチのグループです。SIM スイッチは3つの異なる役割を持っています。

- 1. Commander Switch (CS) グループの管理用デバイスとして手動で設定されるスイッチで、以下の特長を持っています。
  - IP アドレスを1つ持つ。
  - 他のシングル IP グループの CS や MS ではない。
  - マネジメント VLAN 経由で MS に接続する。
- 2. Member Switch (MS) シングル IP グループに所属するスイッチで、CS からアクセスが可能です。MS は以下の特徴を持ちます。
  - 他のシングル IP グループの CS や MS ではない。
  - CS マネジメント VLAN 経由で CS に接続する。
- 3. Candidate Switch (CaS) SIM グループに参加する準備が整っているが、まだ MS ではないスイッチです。CaS を SIM グループ内の MS として、 本スイッチの機能を使用して手動で登録することが可能です。CaS として登録されたスイッチは、SIM グループには所属せず、以下の特長を持っ ています。
  - 他のシングル IP グループの CS や MS ではない。
  - CS マネジメント VLAN 経由で CS に接続する。

上記の役割には、以下のルールを適用します。

- 各デバイスは、まず CS の状態から始まります。
- ・ CS は、はじめに CaS に、その後 MS となり、SIM グループの MS へと遷移します。つまり CS から MS へ直接遷移することはできません。
- ユーザは、CSからCaSへ手動で遷移させることができます。
- 以下のような場合に MS から CaS に遷移します。
  - CS を介して CaS として設定される時。
  - CS から MS への Report パケットがタイムアウトになった時。
- ユーザが手動で CaS から CS に遷移するように設定できます。
- ・ CS を介して CaS は MS に遷移するように設定されます。

SIM グループの CS として運用するスイッチを1台登録した後、スイッチを手動によりグループに追加して MS とします。CS はその後 MS へのアク セスのためにインバンドエントリポイントとして動作します。CS の IP アドレスがグループのすべての MS への経路になり、CS の管理パスワードや 認証によって、SIM グループのすべての MS へのアクセスを制御します。

SIM 機能を有効にすると、CS 内のアプリケーションはパケットを処理する代わりに、リダイレクト(宛先変更)します。アプリケーションは管理者 からのパケットを復号化し、データの一部を変更し、MS へ送信します。処理後、CS は MS から Response パケットを受け取り、これを符号化して 管理者に返送します。

CS が MS に遷移すると、自動的に CS が所属する最初の SNMP コミュニティ (リード権 / ライト権、リード権だけを含む)のメンバになります。しかし、 自身の IP アドレスを持つ MS は、グループ内の他のスイッチ(CS を含む)が所属していない SNMP コミュニティに加入することができます。

# バージョン 1.61 へのアップグレード

SIM 管理機能強化の目的で、本スイッチは本リリースにおいて、バージョン 1.61 にアップグレードしています。本バージョンでは以下の改善点が加わりました。

1. CS は、再起動または Web での異常検出によって、SIM グループから抜けたメンバスイッチを自動的に再検出する機能が搭載しました。この 機能は、以前設定された SIM メンバが再起動の後に発行する Discovery パケットと Maintain パケットを使用することにより実現されます。一 度 MS の MAC アドレスとパスワードが CS のデータベースに記録され、MS が再起動を行うと、CS はこの MS の情報をデータベースに保存し、 MS が再検出された場合、これを SIM ツリーに自動的に戻します。これらのスイッチを再検出するために設定を行う必要はありません。

ー度保存を行った MS の再検出ができないという場合もあります。例えば、スイッチの電源がオンになっていない場合、他のグループのメンバとなっている場合、または CS スイッチとして設定された場合は再検出処理をすることができません。

- トポロジマップには、ポートトランクグループのメンバの接続に関する新機能が加わりました。これはポートトランクグループを構成するイー サネット接続の速度と接続数を表示する機能です。
- 3. 本バージョンでは、以下のファームウェア、コンフィグレーションファイル、およびログファイルのアップロードやダウンロードを複数スイッ チに対して行う機能が追加されました。
  - ファームウェア: TFTP サーバから複数の MS に対するファームウェアダウンロードがサポートされました。
  - コンフィグレーションファイル:TFTP サーバを使用した複数のコンフィグレーションのダウンロード / アップロード (コンフィグレーションの復元やバックアップ用) が可能になりました。
  - ログ:複数のログファイルを TFTP サーバにアップロード可能になりました。
- 4. 詳細に構成を確認しやすいようにトポロジ画面を拡大、縮小することができます。

# Single IP Settings(シングル IP 設定)

スイッチは工場出荷時設定で Candidate Switch(CaS)として設定され、SIM は無効になっています。

Web インタフェースを使用してスイッチの SIM を有効にするためには Management > Virtual Stacking (SIM) > Single IP Settings の順にメニューを クリックし、以下の画面を表示します。

Single IP Settings		
SIM State Configure		
SIM State	Disabled	Apply
SIM Role Configure		
Role State	Candidate 🔽	
Group Name	64 chars	Apply
SIM Settings		
Trap State	Disabled 🔽	
Interval (30-90)	30 sec	
Hold Time (100-255)	100 sec	
Management VLAN (1-4094)	1	Apply

図 7-88 Single IP Settings 画面(CaS 無効状態)

以下の項目が使用できます。

SIM State ConfigureSIM Stateプルダウンメニューから「Enabled」(有効) または「Disabled」(無効) を選択します。「Disabled」を選択すると、スイッ チのすべてのSIM 機能が無効になります。初期値は「Disabled」です。Role StateプルダウンメニューからスイッチのSIM での役割を選択します。以下の2つから選択できます。 ・ Candidate - Candidate Switch (CaS) は SIM グループメンバではありませんが、Commander スイッチに接続しています。 本スイッチのSIM 機能の初期設定です。 ・ Commander - Commander Switch (CS) ユーザは CS に他のスイッチを参加させて SIM グループを作成します。cont ブションを選択すると、本スイッチは SIM 機能対象のスイッチとして設定されます。Group NameSIM グループ名を入力します。Trap StateSIM グループ名を入力します。Interval (30-90)CAny手が Discovery パケットを送信する Discovery プロトコル送信間隔(秒)を設定します。CS スイッチに情報が送られ でくると、接続する他のスイッチ (MS、CaS) の情報が CS に組み込まれます。値は 30-90 (初) の間から指定します。初期値は 100 (秒) です。Hold Time (100-255)他のスイッチが 「Discovery Interval」の間隔で送信してきた情報をスイッチが保持する時間(秒)を指定します。値は 100 です。Management VLANジングル IP マネージメントメッセージ VLAN ID を指定します。	項目	説明				
SIM Stateプルダウンメニューから「Enabled」(有効) または「Disabled」(無効) を選択します。「Disabled」を選択すると、スイッ チのすべての SIM 機能が無効になります。初期値は「Disabled」です。Role Stateプルダウンメニューからスイッチの SIM での役割を選択します。以下の 2 つから選択できます。 ・ Candidate - Candidate Switch (CaS) は SIM グループメンバではありませんが、Commander スイッチに接続しています。 本スイッチの SIM 機能の初期設定です。 ・ Commander - Commander Switch (CS)。ユーザは CS に他のスイッチを参加させて SIM グループを作成します。このオ プションを選択すると、本スイッチは SIM 機能対象のスイッチとして設定されます。Group NameSIM グループ名を入力します。Trap StateSIM トラップを「Enabled」(有効) / Disabled」(無効) にします。 スイッチが Discovery パケットを送信する Discovery プロトコル送信間隔(秒) を設定します。CS スイッチに情報が送られ なると、接続する他のスイッチ (MS、CaS) の情報が CS に組み込まれます。値は 30-90 (秒) の間から指定します。初期 値は 30 (秒) です。Hold Time (100-255)他のスイッチが Discovery Interval」の間隔で送信してきた情報をスイッチが保持する時間(秒) を指定します。値は 100- 255 (秒) の間から指定します。初期値は 100 (秒) です。Management VLANシングル IP マネージメント メッセージ VLAN ID を指定します。		SIM State Configure				
SIM Role ConfigureRole Stateプルダウンメニューからスイッチの SIM での役割を選択します。以下の 2 つから選択できます。 ・ Candidate - Candidate Switch (CaS) は SIM グループメンバではありませんが、Commander スイッチに接続しています。 本スイッチの SIM 機能の初期設定です。 ・ Commander - Commander Switch (CS) ューザは CS に他のスイッチを参加させて SIM グループを作成します。 c のオ プジョンを選択すると、本スイッチは SIM 機能対象のスイッチとして設定されます。 プジョンを選択すると、本スイッチは SIM 機能対象のスイッチとして設定されます。 Top StateGroup NameSIM グループ名を入力します。Trap StateSIM トラップを「Enabled」(有効) / 「Disabled」(無効) にします。Interval (30-90)スイッチが Discovery パケットを送信する Discovery プロトコル送信間隔(秒)を設定します。CS スイッチに情報が送られ てくると、接続する他のスイッチ (MS、CaS) の情報が CS に組み込まれます。値は 30-90 (秒) の間から指定します。初期 値は 30 (秒) です。Hold Time (100-255)他のスイッチが 「Discovery Interval」の間隔で送信してきた情報をスイッチが保持する時間(秒)を指定します。値は 100- 255 (秒) の間から指定します。初期値は 100 (秒) です。Management VLANシングル IP マネージメントメッセージ VLAN ID を指定します。	SIM State	プルダウンメニューから「Enabled」(有効)または「Disabled」(無効)を選択します。「Disabled」を選択すると、スイッチのすべての SIM 機能が無効になります。初期値は「Disabled」です。				
Role Stateプルダウンメニューからスイッチの SIM での役割を選択します。以下の 2 つから選択できます。 、 Candidate - Candidate Switch (CaS) は SIM グループメンバではありませんが、Commander スイッチに接続しています。 本スイッチの SIM 機能の初期設定です。 、 Commander - Commander Switch (CS)。ユーザは CS に他のスイッチを参加させて SIM グループを作成します。このオ プションを選択すると、本スイッチは SIM 機能対象のスイッチとして設定されます。Group NameSIM グループ名を入力します。Trap StateSIM トラップを「Enabled」(有効) / 「Disabled」(無効) にします。Interval (30-90)スイッチが Discovery パケットを送信する Discovery プロトコル送信間隔(秒) を設定します。CS スイッチに情報が送られ てくると、接続する他のスイッチ (MS, CaS) の情報が CS に組み込まれます。値は 30-90 (秒) の間から指定します。初期 値は 30 (秒) です。Hold Time (100-255)他のスイッチが 「Discovery Interval」の間隔で送信してきた情報をスイッチが保持する時間(秒) を指定します。値は 100- (秒) の間から指定します。初期値は 100 (秒) です。Management VLANシングル IP マネージメント メッセージ VLAN ID を指定します。		SIM Role Configure				
Group NameSIM グループ名を入力します。Group NameSIM グループ名を入力します。Trap StateSIM トラップを「Enabled」(有効) / 「Disabled」(無効) にします。Interval (30-90)スイッチが Discovery パケットを送信する Discovery プロトコル送信間隔(秒)を設定します。CS スイッチに情報が送られ てくると、接続する他のスイッチ(MS、CaS)の情報が CS に組み込まれます。値は 30-90 (秒) の間から指定します。初期 値は 30 (秒) です。Hold Time (100-255)他のスイッチが「Discovery Interval」の間隔で送信してきた情報をスイッチが保持する時間(秒)を指定します。値は 100- 255 (秒) の間から指定します。初期値は 100 (秒) です。Management VLANシングル IP マネージメントメッセージ VLAN ID を指定します。	Role State	<ul> <li>プルダウンメニューからスイッチの SIM での役割を選択します。以下の 2 つから選択できます。</li> <li>Candidate - Candidate Switch (CaS) は SIM グループメンバではありませんが、Commander スイッチに接続しています。</li> <li>本スイッチの SIM 機能の初期設定です。</li> <li>Commander - Commander Switch (CS)。ユーザは CS に他のスイッチを参加させて SIM グループを作成します。このオプションを選択すると、本スイッチは SIM 機能対象のスイッチとして設定されます。</li> </ul>				
SIM SettingsTrap StateSIM トラップを「Enabled」(有効) / 「Disabled」(無効) にします。Intervalスイッチが Discovery パケットを送信する Discovery プロトコル送信間隔(秒)を設定します。CS スイッチに情報が送られ てくると、接続する他のスイッチ (MS、CaS) の情報が CS に組み込まれます。値は 30-90 (秒) の間から指定します。初期 値は 30 (秒) です。Hold Time他のスイッチが「Discovery Interval」の間隔で送信してきた情報をスイッチが保持する時間(秒)を指定します。値は 100- 255 (秒) の間から指定します。初期値は 100 (秒) です。Management VLANシングル IP マネージメントメッセージ VLAN ID を指定します。	Group Name	SIM グループ名を入力します。				
Trap StateSIM トラップを「Enabled」(有効) / 「Disabled」(無効) にします。Intervalスイッチが Discovery パケットを送信する Discovery プロトコル送信間隔(秒)を設定します。CS スイッチに情報が送られ てくると、接続する他のスイッチ (MS、CaS) の情報が CS に組み込まれます。値は 30-90(秒) の間から指定します。初期 値は 30(秒) です。Hold Time他のスイッチが「Discovery Interval」の間隔で送信してきた情報をスイッチが保持する時間(秒)を指定します。値は 100- 255(秒) の間から指定します。初期値は 100(秒) です。Management VLANシングル IP マネージメントメッセージ VLAN ID を指定します。		SIM Settings				
Interval (30-90)         スイッチが Discovery パケットを送信する Discovery プロトコル送信間隔(秒)を設定します。CS スイッチに情報が送られ てくると、接続する他のスイッチ(MS、CaS)の情報が CS に組み込まれます。値は 30-90(秒)の間から指定します。初期 値は 30(秒)です。           Hold Time (100-255)         他のスイッチが「Discovery Interval」の間隔で送信してきた情報をスイッチが保持する時間(秒)を指定します。値は 100- 255(秒)の間から指定します。初期値は 100(秒)です。           Management VLAN         シングル IP マネージメントメッセージ VLAN ID を指定します。	Trap State	SIM トラップを「Enabled」(有効)/「Disabled」(無効)にします。				
Hold Time         他のスイッチが「Discovery Interval」の間隔で送信してきた情報をスイッチが保持する時間(秒)を指定します。値は 100- (100-255)           255(秒)の間から指定します。初期値は 100(秒)です。           Management VLAN           シングル IP マネージメントメッセージ VLAN ID を指定します。	Interval (30-90)	スイッチが Discovery パケットを送信する Discovery プロトコル送信間隔(秒)を設定します。CS スイッチに情報が送られ てくると、接続する他のスイッチ(MS、CaS)の情報が CS に組み込まれます。値は 30-90(秒)の間から指定します。初期 値は 30(秒)です。				
Management VLAN シングル IP マネージメントメッセージ VLAN ID を指定します。	Hold Time (100-255)	他のスイッチが「Discovery Interval」の間隔で送信してきた情報をスイッチが保持する時間(秒)を指定します。値は 100- 255(秒)の間から指定します。初期値は 100(秒)です。				
	Management VLAN	シングル IP マネージメントメッセージ VLAN ID を指定します。				

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

スイッチを CS として登録すると、「Single IP Management」フォルダには 4 つのリンクが追加され、Web を使用した SIM 設定が続けられるように なります。追加されるリンクは「Topology」、「Firmware Upgrade」、「Configuration Backup/Restore」、「Upload Log File」です。

# Topology(トポロジ)

SIM グループ内のスイッチの設定および管理を行います。本画面は表示のためには、ご使用のコンピュータに Java スクリプトが必要です。

```
Management > Virtual Stacking (SIM) > Topology の順にメニューをクリックします。以下の画面が表示されます。
```

Cluster 1	Device Name	Local Port	Speed	Remote Port	MAC Address	Model Name
	Switch	-	-	-	00-0F-36-30-AE-01	DGS-3630-28TC
Switch	Switch	194	Gigabit-Full	65	00-01-02-03-04-00	DGS-3630-52TC
Switch	Switch	1	Gigabit-Full	196	00-01-12-33-40-00	DGS-3630-52TC
Switch						

図 7-89 トポロジ画面

# メニューバー

トポロジ画面には、デバイスの設定のために以下のようなメニューバーが配置されています。

File	Group	Device	View	Help
図 7-90	トポロジメ	ニューバー		

メニューバーには以下の5つのメニューが存在します。

## ■「File」メニュー

- Print Topology トポロジマップを印刷します。
- Preference ポーリング間隔 (interval) など表示プロパティを設定します。

Preference	
Interval (10-300)	20
<ul> <li>Show All</li> </ul>	Show Member Only
	OK Cancel

⊠ 7-91 Preference

以下の項目が使用できます。

項目	説明				
Interval	SIM トポロジ表示の更新間隔(10-300)を指定します。				
Show All	トポロジにおいて全ての有効な SIM デバイスを表示します。				
Show Member Only	トポロジにおいて SIM メンバデバイスのみを表示します。				

設定を変更する際は、「OK」ボタンをクリックし、設定内容を適用してください。

「Cancel」ボタンをクリックし、変更した設定内容を破棄します。

## ■「Group」メニュー

Add to Group – グループに CaS を追加します。このオプションを選択すると、以下のパスワード入力画面が表示され、CaS を SIM グループに追加するための認証を行います。パスワードを入力して「Apply」ボタンをクリックするか、「Cancel」ボタンをクリックして画面を閉じます。

Input Passwor	đ		
Password			
	Apply	Cancel	

図 7-92 Input password ダイアログボックス

- Remove from Group MS をグループから削除します。
- ■「Device」メニュー
- Configure 指定したデバイスの Web マネージャを開きます。

# ■「View」メニュー

- Refresh ビューを最新の状態に更新します。
- ・ Topology トポロジビューを表示します。

Jom Out	Zoom In	Save	Back	
				~
				<b>S</b>
				Switch
				Switch
				Sultan
				SWICCH
				Switch

図 7-93 View >Topology 画面

「Zoom In」をクリックすると表示アイテムが拡大します。 「Zoom Out」をクリックすると表示アイテムが縮小します。 「Save」をクリックすると表示が保存されます。 「Back」をクリックすると前画面に戻ります。

本画面は、SIM グループ内のデバイスが他のグループやデバイスとどのように接続しているかを表示します。

本画面で表示されるアイコンは以下の通りです。

アイコン	説明	7	アイコン	説明
	グループ	ĺ	<b>?</b> }	他のグループの Member スイッチ
۲	レイヤ 2 Commander スイッチ	(	$\langle \rangle$	レイヤ 2 Candidate スイッチ
<b>(</b>	レイヤ 3 Commander スイッチ	(	<b>&gt;</b>	レイヤ 3 Candidate スイッチ
2	他のグループの Commander スイッチ		-	不明なデバイス
	レイヤ 2 Member スイッチ			SIM 非対応のデバイス
	レイヤ 3 Member スイッチ			
# ツールヒント

トポロジビュー画面では、マウスはデバイス情報の確認と設定のために重要な役割を果たします。トポロジ画面の特定のデバイス上にマウスポイン タを指定すると、ツリービューと同様にデバイス情報(ツールヒント)を表示します。以下にその例を示します。



図 7-94 ツールヒントを利用したデバイス情報の表示

図 7-95

2つのデバイスの間のライン上でマウスポインタを静止させると、以下の図のようにデバイス間の接続速度を表示します。



図 7-96 ツールヒントを利用したポート速度の表示①



図 7-97 ツールヒントを利用したポート速度の表示②

# 右クリックメニュー

デバイスのアイコン上で右クリックすると、SIM グループ内でのスイッチの役割や、関連付けられているアイコンの種類に応じた様々な機能を実行できます。

グループ	Commanderスイッチ	Memberスイッチ	Candidateスイッチ
Switch	Switch	Remove from Group Configure Swit <sup>Property</sup>	Add to Group Property Switch

図 7-98 各アイコン上での右クリック

画面には以下の情報が表示されます。

項目	説明
Property	ポップアップ画面が開き、デバイスの情報を表示します。
Configure	Web 管理機能を起動して、スイッチの設定を可能にします。
(Member スイッチのみ)	
Add to group	CaS をグループに追加します。このオプションを選択すると、以下のパスワード入力画面が表示され、CaS スイッチ
(Candidate スイッチのみ)	を SIM グループに追加するための認証を行います。
Remove from Group	メンバをグループから削除します。
(Member スイッチのみ)	

# ■ 各アイコンの「Property」

Name	Switch	Name:	Switch	
Model:	Group	Model:	DGS-3630-28TC	
MAC:	00-0F-36-30-AE-01	MAC:	00-0F-36-30-AE-01	
ocal Port	-	Local Port		
Remote Port	-	Remote Port		
Port Speed:	-	Port Speed.		
	グループ		Commanderスイッチ	
roperty	グループ	Property	Commanderスイッチ	_
roperty Name.	グループ Switch	Property Name:	Commanderスイッチ Switch	
roperty Name. Model:	グループ Switch DGS-3630-52TC	Property Name: Model:	Commanderスイッチ Switch DGS-3630-52TC	_
roperty Name. Model: MAC:	グループ Switch DGS-3630-52TC 00-01-02-03-04-00	Property Name: Model: MAC:	Commanderスイッチ Switch DGS-3630-52TC 00-01-12-33-40-00	-
roperty Name. Model: MAC: Local Port:	グループ Switch DGS-3630-52TC 00-01-02-03-04-00 194	Property Name: Model: MAC: Local Port:	Commanderスイッチ Switch DG8-3630-52TC 00-01-12-33-40-00 1	_
roperty Name. Model: MAC: Local Port: Remote Port:	グループ Switch DGS-3630-52TC 00-01-02-03-04-00 194 65	Property Name: Model: MAC: Local Port: Remote Port:	Commanderスイッチ Switch DG8-3630-52TC 00-01-12-33-40-00 1 196	_

図 7-99 各アイコンの Property

画面には以下の情報が表示されます。

項目	説明
Name	SIM グループ内のスイッチのデバイス名を表示します。デバイス名がない場合は、「default」が与えられ、識別のために MAC ア
	ドレスの終わり6桁が付加されます。
Module	スイッチのモジュール名を表示します。
MAC Address	スイッチの MAC アドレスを表示します。
Local Port	MS または CaS が接続している CS の物理ポートの番号を表示します。CS の場合は何も表示されません。
Remote Port	CS が接続している MS または CaS の物理ポートの番号を表示します。CS の場合は何も表示されません。
Port Speed	CS と MS/CaS 間の接続スピードを表示します。

■「Help」メニュー

・ About – 現在の SIM バージョンなどの SIM 情報を表示します。

Message	from webpag	e		×
	Single IP Mar Copyright(C) Release Date	nagement 2017 D-Link : 2017/6/15	Corporation	
			OK	-

# Firmware Upgrade(ファームウェア更新)

CS から MS へのファームウェアの更新を行います。

Management > Virtual Stacking (SIM) > Firmware Upgrade の順にメニューをクリックし、以下の画面を表示します。

rmware Upgrade		_	 	
IFTP Server IP	Path\Filename			Download
Total Entries: 0				

図 7-101 Firmware Upgrade 画面

MS は、「Port」(MS に接続する CS 上のポート)、「MAC Address」、「Model Name」、「Version」の情報と共にリスト表示されます。ダウンロード対象のスイッチは、「Port」欄の下のチェックボックスで選択します。ファームウェアを格納する「TFTP Server IP」を入力して、ファームウェアの「Path、 Filename」を指定します。「Download」ボタンをクリックすると、ファイル転送が開始されます。

### Configuration File Backup/ Restore (コンフィグレーションファイルの更新)

CSからMSに対してTFTPサーバを使用してコンフィグレーションファイルのバックアップまたはリストアを行います。

Management > Virtual Stacking (SIM) > Configuration File Backup/Restore の順にメニューをクリックし、以下の画面を表示します。

Configuration File Backu	p/Restore				
Configuration File Backup/Resto	re				
TFTP Server IP	Path\Filename				
				Res	tore Backup
Total Entries: 0					
Member ID	MAC Address	Platform	Hold Time	Firmware Version	Device Name

図 7-102 Configuration File Backup/Restore 画面

MS は「Port」(MS に接続する CS 上のポート)、「MAC Address」、「Model Name」、「Version」の情報と共にリスト表示されます。コンフィグレーショ ンファイルのアップデート対象のスイッチは、「Port」欄の下のラジオボタンで選択します。ファームウェアを格納する「TFTP Server IP」を入力して、 ファームウェアの「Path\Filename」を指定します。「Restore」ボタンをクリックすると、TFTP サーバからファイル転送が開始されます。「Backup」 ボタンをクリックすると、TFTP サーバにファイルがバックアップされます。

# Upload Log File(ログファイルのアップロード)

CS は、MS から指定したサーバに送信したログファイルを依頼することができます。

Management > Virtual Stacking (SIM) > Upload Log File の順にメニューをクリックし、以下の画面を表示します。

pload Log File					
FTP Server IP	Path\Filename	_			Unload
ntal Entries: 0					opious
Mambas ID	MAC Address	Diatform	Lield Time	Firmunase Version	Deutice Name

図 7-103 Upload Log File 画面

ログを格納する「TFTP Server IP」と MS のログファイルの「Path\Filename」を入力します。「Upload」 ボタンをクリックすると TFTP サーバにログファ イルを送信します。

# D-Link Discovery Protocol (D-Link ディスカバリプロトコル)

D-Link ディスカバリプロトコル(DDP)の表示、設定を行います。

Management > D-Link Discovery Protocol の順にメニューをクリックし、以下の画面を表示します。

D-Link Discovery Protocol			
D-Link Discovery Protocol DDP Global Settings D-Link Discovery Protocol State Report Timer	<ul> <li>Enabled</li> <li>Disabled</li> <li>30</li> <li>sec</li> </ul>		Apply
DDP Port Settings Unit 1 From Port	eth1/0/1 To Port eth1	/0/1 V State Disabled V	Apply
onit i settings	Port	State	
	eth1/0/1	Enabled	
	eth1/0/2	Enabled	

図 7-104 D-Link Discovery Protocol 画面

#### 画面に表示される項目:

項目	説明
	D-Link Discovery Protocol
D-Link Discovery Protocol	DDP をグローバルに有効にします。
State	
Report Timer	DDP レポートメッセージの送信間隔(秒)を以下から指定します。
	「30」「60」「90」「120」「Never」
	DDP Port Settings
Unit	設定するユニットを選択します。
From Port / To Port	ポートの始点 / 終点を設定します。
State	DDP ポートを「Enabled」(有効)/「Disabled」(無効)にします。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

# SMTP Settings (SMTP 設定)

Simple Mail Transfer Protocol (SMTP) の表示、設定を行います。

Management > SMTP Settings の順にメニューをクリックし、以下の画面を表示します。

ITP Global Settings		
	IDv4	
SMTP IPv4 Server Address	0.0.0	
SMTP IPv4 Server Port (1-65535)	25	
VRF Name	12 chars	
Self Mail Address	254 chars	
Send Interval (0-65535)	30 min	Apply
SMTP Mail Receiver Address		
Add A Mail Receiver	254 chars	Add
Send a Test Mail to All		
Subject	128 chars	
Content	512 chars	Apply
		~
Total Entries: 0		Delete All
Index	Mail Receiver Address	
1		Delete
2		Delete
3		Delete
4		Delete
5		Delete
6		Delete
7		Delete
8		Delete

図 7-105 SMTP Settings 画面

設定には以下の項目を使用します。

	C			
SMTP Global Settings				
SMTP IP	SMTP サーバ IP アドレスタイプを「IPv4」「IPv6」から指定します。			
SMTP IPv4 Server Address	SMTP サーバ IPv4 アドレスを指定します。			
SMTP IPv6 Server Address	SMTP サーバ IPv6 アドレスを指定します。			
SMTP IPv4 Server Port	SMTPIPv4 サーバポート番号を指定します。1 から 65535 まで指定可能です。 初期値:25			
SMTP IPv6 Server Port	SMTPIPv6 サーバポート番号を指定します。1 から 65535 まで指定可能です。 初期値:25			
VRF Name	VRF インスタンス名を 12 字以内で入力します。			
Self Mail Address	スイッチの E メールアドレスを指定します。254 字以内に指定します。			
Send Interval	送信間隔を指定します。0 から 65535 まで指定可能です。 初期値:30(分)			
	SMTP Mail Receiver Address			
Add A Mail Receiver	受信する E メールアドレスを指定します。254 字以内に指定します。			
	Send a Test Mail to All			
Subject	E メールの件名を指定します。128 字以内に指定します。			
Content	E メールの内容を指定します。512 字以内に指定します。			

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

「Delete」をクリックすると指定のエントリを削除します。

「Delete All」をクリックするとすべてのエントリを削除します。

# Reboot Schedule Settings(再起動スケジュール設定)

本項目ではスイッチの再起動スケジュール設定を行います。再起動スケジュールは 30 日以内に設定する必要があります。再起動スケジュールが実 行され、再起動が開始されると、スイッチが再起動スケジュールを使用して再起動をした旨のログメッセージが生成されます。再起動、またはシャッ トダウン後に、再起動スケジュールは自動的に削除されます。スイッチが再起動スケジュールが実行される前に、手動で再起動やシャットダウンさ れた場合は、指定の再起動スケジュールはキャンセルされます。

Management > Reboot Schedule Settings の順にメニューをクリックし、以下の画面を表示します。

Reboot Schedule Settings		
Time Interval (1-43200)     Time (HH:MM)     Date (DD / MM / YYYY)	min 18:00 27/12/2013	
Save Before Reboot		Apply Delete

図 7-106 Reboot Schedule Settings 画面

画面に表示される項目:

項目	説明
Time Interval	再起動スケジュールの間隔を選択します。再起動は指定の間隔(分)を過ぎると実行されます。
	1から43200(30日)の同じ指定可能です。
Time	再起動を実行する時間を指定します。24 時間のフォーマットを使用します。(例;21:30) 日付が指定されていない場合、次の 24 時間以内の指定時間に再起動が実行されます。
Date	再起動を実行する日付を指定します。「DD/MM/YYYY」のフォーマットを使用します。( 例;23/12/2015) 30 日以内の再起動スケジュールが指定可能です。
Save Before Reboot	再起動実行前に行われた設定変更について保存します。
	Apply」ボタンをクリックし、設定内容を適用してください。

# NLB FDB Settings(NLB FDB 設定)

本スイッチはネットワークロードバランシング (NLB) をサポートしています。これは、複数のサーバは同じ IP アドレスと MAC アドレスを共有する Microsoft サーバロードバランシングアプリケーションの MAC フォワーディングコントロールです。クライアントからのこのリクエストは、全ての サーバに転送されますが、その中の 1 つのみにより行われます。サーバは 2 つのモード「ユニキャストモード」と「マルチキャストモード」で動作 可能です。

- ・ ユニキャストモード:クライアントはユニキャスト MAC アドレスをサーバへの宛先 MAC として使用します。
- ・ マルチキャストモード:クライアントはマルチキャスト MAC アドレスをサーバへの宛先 MAC として使用します。

宛先となる MAC は共有 MAC になります。しかしサーバは応答パケットの送信元 MAC アドレスとして (共有 MAC よりむしろ) 自身の MAC アドレ スを使用します。つまり NLB ユニキャストアドレスは通常パケットの送信元 MAC アドレスではありません。

受信パケットがユニキャスト MAC アドレスと照合する宛先 MAC アドレスを含んでいると、VLAN 設定に関わらず、指定のポートへ転送されます。

管理者は MAC アドレステーブルのスタティックアドレスを NLB アドレスとして設定はできません。しかし、MAC アドレスが NLB MAC アドレスエ ントリとして生成されている場合、同じ MAC アドレスは L2 MAC アドレステーブルにおいて学習されます。この場合、NLB はより高い優先値を持ち、 自動的に学習された FDB には影響はありません。

Management > NLB FDB Settings の順にメニューをクリックし、以下の画面を表示します。

NLB FDB Settings		_			
NLB FDB Settings					
NLB Type VID (1-4094)	MAC Address	Unit	From Port eth1/0/1	To Port eth1/0/1	Apply
Total Entries: 1					Delete All
MAC Address	VID		Interface		
00-11-22-33-44-55	-		eth1/0/20		Delete
				1/1 < <	1 > > Go

図 7-107 NLB FDB Settings 画面

#### 画面に表示される項目:

項目	説明
NLB Type	NLB タイプを「Unicast」「Multicast」から指定します。
VID	「Multicast」を選択した場合、設定する VLAN ID を入力します。
MAC Address	作成される NLB マルチキャスト FDB エントリの MAC アドレスを入力します。
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

「Delete All」をクリックするとすべてのエントリを削除します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

注意

物理スタックしているスイッチにおいて、L3の NLB を行っているサーバを筐体またぎの LAG(リンクアグリゲーショングループ)では接続できません。物理スタックとの併用は、しないでください。

# SD Card Management (SD カード管理)

USB ドライバストレージなどのリムーバブル機器の設定を行います。

# SD Card Backup Settings(SD カードへのバックアップ設定)

USB ストレージのバックアップの表示、設定を行います。SD 管理バックアップスケジュールエントリの作成、編集を行います。

### Management > SD Card Management > SD Card Backup Settings の順にメニューをクリックし、以下の画面を表示します。

Card Backup Settings						
ackup Entry Name	32 chars				Apply	Find
tal Entries: 1						
Backup Entry Name	Time Range	Type	File Name	State		

図 7-108 SD Card Backup Settings 画面

以下の項目が表示されます。

項目	説明
Backup Entry Name	SD カード管理バックアップスケジュール名(32 字以内)を指定します。
Time Range	Edit をクリック後、スケジュール範囲の指定を行います。
Туре	Edit をクリック後、設定するコンフィグレーション/ログのどちらか選択します。 ・ Configuration - バックアップの対象をコンフィグレーションに指定します。 ・ Log - バックアップの対象をシステムログに指定します。
File Name	Edit をクリック後、宛先ファイル名とパスを指定します。
State	Edit をクリック後、バックアップスケジュールの有効・無効を設定します。

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Edit」をクリックして、指定エントリの編集を行います。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

# SD Card Execute Settings (SD カード実行設定)

USB ストレージからスイッチのファイルシステムへの設定を手動で実行するために使用します。

Management > SD Card Management > SD Card SD Card Execute Settings の順にメニューをクリックし、以下の画面を表示します。

ocuto Configuration							
ecute comgutation							
ile URL	d:/config-vlan-1		Increment	Disabled	~		Apply
Card Execute Settings							
xecute Entry Name	32 chars					Apply	Find
otal Entries: 1							
Execute Entry Name	Time Range	Mode	File Name		State		
Execute		Reset			Disabled	Edit	Delete
					1/1	< 1	> >

図 7-109 SD Card Execute Settings 画面

画面に表示される項目:

項目	説明			
	Execute Configuration			
File URL	設定ファイルの URL を指定します。現在のディレクトリが SD カードファイルシステムのそれでない場合、 フルパスを入力する必要があります。			
Increment	本オプションが有効に設定されると、実行前に現在の設定がリセットされません。			
SD Card Execute Settings				
Execute Entry Name	実行エントリ名を 32 字以内で指定します。			
Time Range	Edit をクリック後、スケジュール範囲を設定します。			
Mode	Edit をクリック後、モードを次から選択します。 ・「Increase」- 設定の実行前に、現在の設定がクリアされません。 ・「Reset」- 設定の実行前に現在の設定がクリアされます。			
File URL	Edit をクリック後、設定ファイル名とパスを指定します。			
State	Edit をクリック後、スケジュール実行の「Enabled」(有効)/「Disabled」(無効)を設定します。			

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Edit」をクリックして、指定エントリの編集を行います。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

# 第8章 L2 Features (L2 機能の設定)

L2 Features メニューを使用し、本スイッチにレイヤ2機能を設定することができます。

以下は L2 Features サブメニュー	の説明です。	必要に応じて、	設定/変更/	修正を行ってくださ	5い。

サブメニュー	説明
FDB(FDB 設定)	FDB(Forwarding DataBase)フォワーディングデータベースの設定を行います。
VLAN(VLAN 設定)	802.1Q スタティック VLAN の設定を行います。
VLAN Tunnel (VLAN トンネル)	802.1Q VLAN トンネルの設定を行います。
STP(スパニングツリー設定)	スパニングツリープロトコル(STP)設定を行います。3 つのバージョンの STP(802.1D- 1998 STP、802.1D-2004 Rapid STP、および 802.1Q-2005 MSTP)をサポートしています。
ERPS (G.8032) (イーサネットリングプロテクション設定)	「Ethernet Ring Protection Switching」(ERPS) の表示、設定を行います。 ERPS はイーサネットリング保護スイッチングの業界標準 (ITU-T G.8032) です。
Loopback Detection(ループバック検知設定)	ループバック検知(LBD)機能の設定を行います。
Link Aggregation(リンクアグリゲーション)	Link Aggregation(リンクアグリゲーション / ポートトランキング機能)の設定を行います。
MLAG(マルチシャーシリンクアグリゲーション)	複数のスイッチでリンクアグリゲーションを設定し、帯域の増加を行います。
Flex Links(フレックスリンクス)	フレックスリンクス機能の設定を行います。
L2 Protocol Tunnel(レイヤ 2 プロトコルトンネル)	L2 Protocol Tunnel(レイヤ 2 プロトコルトンネル)の設定を行います。
L2 Multicast Control (L2 マルチキャストコントロール)	IGMP(Internet Group Management Protocol)Snooping 機能始めとした L2 Multicast Control(L2 マルチキャストコントロール)の設定を行います。
LLDP	Link Layer Discovery Protocol(LLDP)の設定を行います。

# FDB (FDB 設定)

FDB(Forwarding DataBase)フォワーディングデータベースの設定を行います。

# Static FDB(スタティック FDB の設定)

Unicast Static FDB(ユニキャストスタティック FDB の設定)

スイッチにスタティックなユニキャストフォワーディングを設定します。

#### L2 Features > FDB > Static FDB > Unicast Static FDB の順にメニュークリックし、以下の画面を表示します。

Unicast Static FDB			
Unicast Static FDB			
Port V 1V eth1/	0/1 VID (1-4094)	MAC Address 00-84-57-00-00-00	Apply
Total Entries: 1			Delete All
VID	MAC Address	Port	
1	00-12-34-56-79-81	eth1/0/19	Delete
		1/1 < <	1 > >  Go

図 8-1 Unicast Static FDB 画面

以下の項目を使用して設定を行います	0
-------------------	---

項目	説明
Port/Drop	上記 MAC アドレスのあるポート番号を指定します。また、本オプションはユニキャストのスタティックな FDB から MAC ア
	ドレスを破棄します。
	• Port - 上記 MAC アドレスのあるポート番号を指定します。「ユニット ID: ポート番号」(例 1:5)または「ポート番号」(例 5)
	という形式とします。ポート番号だけを入力する場合、ユニット番号の初期値は1となります。
	・ drop - ユニキャストのスタティックな FDB から MAC アドレスを破棄します。
Unit	設定を行うユニットを指定します。
Port Number	「Port」を選択した場合、ポート番号を入力します。
VID	ラジオボタンをクリックし、関連するユニキャスト MAC アドレスが存在する VLAN ID を入力します。
MAC Address	パケットがスタティックに送信される宛先の MAC アドレス。ユニキャスト MAC アドレスを指定します。

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。「Delete All」をクリックするとすべてのエントリを削除します。 設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

#### Multicast Static FDB(マルチキャストスタティック FDB の設定)

スイッチにスタティックなマルチキャストフォワーディングを設定します。

L2 Features > FDB > Static FDB > Multicast Static FDB の順にメニュークリックし、以下の画面を表示します。

Multicast Static FDB				
Multicast Static FDB				
Unit From Port	To Port	VID (1-4094)	MAC Address	
1 v eth1/0/1 v	eth1/0/1 🔽		01-00-00-00-02	Apply
Total Entries: 1				Delete All
VID	MAC Address	Egi	ress Ports	
1	01-00-00-00-02	e	eth1/0/18	Delete
			1/1  < <	1 > >  Go

#### 図 8-2 Multicast Static FDB 画面

以下の項目を使用して設定を行います。

項目	説明
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。
VID	指定の Multicast MAC アドレスが属する VLAN の VLAN ID。
MAC Address	マルチキャストパケットの送信先 MAC アドレス。マルチキャスト MAC アドレスを指定します。宛先 MAC アドレスの形 式は「01-xx-xx-xxxxxx」です。

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。「Delete All」をクリックするとすべてのエントリを削除します。 設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

# MAC Address Table Settings(MAC アドレステーブル設定)

スイッチの MAC アドレスフォワーディングテーブルを参照します。スイッチが MAC アドレス、VLAN、およびポート番号間の関連性を学習するとテーブルに記載します。それらのエントリは、スイッチ経由でパケットを送信するのに使用されます。

L2 Features > FDB > MAC Address Table Settings の順にメニューをクリックし、以下の画面を表示します。

### Global Settings(グローバル設定タブ)

MAC Address Table Sett	ings		
Global Settings	MAC Address Port Learning Settings	MAC Address VLAN Learning Settings	
Aging Time (0, 10-1000000)	300 sec		
Aging Destination Hit	OEnabled		Apply

図 8-3 MAC Address Table Settings 画面(Global Settings)

以下の項目を使用して設定を行います。

項目	説明				
Aging Time (10-1000000)	MAC アドレステーブルのエージングタイムを入力します。 設定した時間中にアクセスのない端末について、学習した MAC アドレスを MAC アドレステーブルから削除します。 ・ 入力可能範囲:0, 10 ~ 1000000(秒) ・ 初期値:300(秒) 0に設定した場合、学習した MAC アドレスは削除されません。				
Aging Destination Hit	エージングタイム内に宛先アドレスにより受信します。				
記点を変更する際は、シギー					

設定を変更する際は、必ず「Apply」ボタンをクリックし設定内容を適用してください。

#### MAC Address Port Learning Settings(MAC アドレスポートラーニング設定タブ)

MAC Address Table Setting	js		
Global Settings	MAC Address Port Learning Settings	MAC Address VLAN Learning Settings	
Unit From Port       I     Eth1/0/1       Unit 1 Settings	To Port Status eth1/0/1 V Enabled V		Apply
	Port	Status	
	eth1/0/1	Enabled	
	eth1/0/2	Enabled	
	eth1/0/3	Enabled	
	eth1/0/4	Enabled	
	eth1/0/5	Enabled	

図 8-4 MAC Address Table Settings (MAC Address Port Learning Settings) 画面

#### 以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定するユニットを指定します。
From Port / To Port	ポートの始点 / 終点を設定します。
Status	MAC アドレスラーニングを「Enabled」(有効)/「Disabled」(無効)にします。
記点を変更する際に、	

設定を変更する際は、必ず「Apply」ボタンをクリックし設定内容を適用してください。

# MAC Address VLAN Learning Settings(MAC アドレス VLAN ラーニング設定タブ)

MAC Address Table Setting	js		
Global Settings	MAC Address Port Learning Settings	MAC Address VLAN Learning Settings	
MAC Address VLAN Learning Settin	ngs		
VID List 3 or 2-5	Status Enabled V		Apply
Find MAC Address VLAN Learning			
VID (1-4094)			
			Find Show All
Total Entries: 1			
VID		Status	
1		Enabled	
		1/	1  < < 1 > >  Go

図 8-5 MAC Address Table Settings (MAC Address VLAN Learning Settings) 画面

#### 以下の項目を使用して、設定および表示を行います。

項目	説明
VID List	参照するフォワーディングテーブルの VLAN リストを入力します。
MAC Address	参照するフォワーディングテーブルの MAC アドレスを入力します。
Status	MAC アドレスラーニングを「Enabled」(有効)/「Disabled」(無効)にします。
	空内家を通用します

「Apply」をクリックし、設定内容を適用します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Show All」をクリックして、すべてのエントリを表示します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

# MAC Address Table (MAC アドレステーブル)

スイッチの MAC アドレスフォワーディングテーブルを参照します。スイッチが MAC アドレス、VLAN、およびポート番号間の関連性を学習するとテーブルに記載します。それらのエントリは、スイッチ経由でパケットを送信するのに使用されます。

#### L2 Features > FDB > MAC Address Table の順にメニューをクリックし、以下の画面を表示します。

C Address Table					
ort	1 V eth1/0/1 V		Clear Dynamic by Port	Find	
ID (1-4094)			Clear Dynamic by VLAN	Find	
IAC Address	00-84-57-00-00-00		Clear Dynamic by MAC	Find	
otal Entries: 11			Clear All	Show All	
VID	MAC Address	Туре	Port		
1	00-12-34-56-79-81	Static	eth1/0/19		
1	00-23-7D-BC-08-44	Dynamic	eth1/0/5		
1	00-23-7D-BC-2E-18	Dynamic	eth1/0/1		
1	00-FF-47-77-70-B8	Dynamic	eth1/0/5		
1	10-BF-48-D6-E2-E2	Dynamic	eth1/0/5	eth1/0/5	
1	24-24-0E-E5-96-DE	Dynamic	eth1/0/5		
1	40-B8-37-B1-06-9A	Dynamic	eth1/0/5		
1	5C-33-8E-43-B3-68	Dynamic	eth1/0/5		
1	CC-B2-55-8B-27-79	Dynamic	eth1/0/5		
1	F0-7D-68-34-00-10	Static	CPU		

#### 図 8-6 MAC Address Table 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Port	以下の MAC アドレスと関連付けられるポートを選択します。
VID	参照するフォワーディングテーブルの VLAN ID を入力します。
MAC Address	参照するフォワーディングテーブルの MAC アドレスを入力します。

# 第8章 L2 Features (L2機能の設定)

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

#### エントリの検索

「Find」ボタンをクリックして、指定したポート、VLAN または MAC アドレスをキーとして検索します。

#### ダイナミックエントリの削除

「Clear Dynamic Entries (by Port/by VLAN/by MAC)」ボタンをクリックして、アドレステーブルのダイナミックエントリを削除します。

#### エントリの表示

「Show All」ボタンをクリックして、アドレステーブルのすべてのエントリを表示します。

#### 全エントリの削除

「Clear All」ボタンをクリックして、アドレステーブルのすべてのエントリを表示します。

#### MAC Notification (MAC 通知)

スイッチの MAC 通知をグローバルに設定します。また、スイッチの各ポートに MAC 通知を設定します。

注意 本機能をご使用になる場合、NMS 側で、MAC Notification トラップを受信できる環境が必要になります。E-mail や Syslog における通知に は対応しておりません。

L2 Features > FDB > MAC Notification の順にメニューをクリックし、以下の画面を表示します。

MAC Notification				
MAC Notification Settings	MAC Notification History			
MAC Notification Global Settings MAC Address Notification Interval (1-2147483647) History Size (0-500) MAC Notification Trap State Trap Type	Enabled Obisable 1 Enabled Obisable Without VID	ed sec ed		Apply
Unit From Port	To Port eth1/0/1	Added Trap Remove Disabled V Disable	d Trap	Apply
Unit 1 Settings Port	Add	ed Trap	Removed Trap	
eth1/0/1	Dis	abled	Disabled	
eth1/0/2	Dis	abled	Disabled	

図 8-7 MAC Notification 画面

以下の項目を使用して設定を行います。

項目	説明			
MAC Address Notification	スイッチ上の MAC 通知をグローバルに「Enabled」(有効)/「Disabled」(無効)にします。			
Interval (1-2147483647 sec)	通知を行う間隔(秒)。初期値:1(秒)			
History Size (0-500)	通知用に使用するヒストリログの最大エントリ数(最大 500 エントリ)。初期値 : 1			
MAC Notification Trap State	MAC 通知トラップを「Enabled」(有効)/「Disabled」(無効)に設定します。			
Тгар Туре	トラップタイプを選択します。			
	・ Without VID - トラップ情報に VLAN ID を含みません。			
	・ With VID - トラップ情報に VLAN ID を含みます。			
Unit	設定するユニットを選択します。			
From Port /To Port	プルダウンメニューから、MAC 通知設定を有効または無効にするポートを指定します。			
Added Trap	選択したポートの追加トラップを「Enabled」(有効)/「Disabled」(無効)に設定します。			
Removed Trap	選択したポートの削除トラップを「Enabled」(有効)/「Disabled」(無効)に設定します。			

設定を変更する際は、必ず「Apply」ボタンをクリックし設定内容を適用してください。

#### MAC Notification History タブ

MAC Notification			
MAC Notification Setti	ngs MAC Notification History	]	
Total Entries: 0			
History Index		MAC Changed Message	

図 8-8 MAC Notification History 画面 MAC 通知メッセージの履歴が表示されます。

# VLAN について

### IEEE 802.1p プライオリティについて

IEEE 802.1p 標準規格で定義されるプライオリティタグ機能では、多くの異なる種類のデータが同時に送受信されるようなネットワークにおいてトラフィックを制御することができます。本機能は、混雑したネットワーク上でのタイムクリティカルなデータの伝送時に発生する問題を解決するため に開発されました。例えばビデオ会議のような、タイムクリティカルなデータに依存するタイプのアプリケーションの品質は、わずかな伝送遅延に も多大な影響を受けてしまいます。

IEEE 802.1p 標準規格に準拠するネットワークデバイスは、データパケットのプライオリティレベル(優先度)を認識することができます。また、これらのデバイスでは、パケットに対してプライオリティレベルやタグを割り当てたり、パケットからタグを取り外したりすることも可能です。この プライオリティタグ(優先タグ)により、パケットの緊急度および送信キューが決定します。

プライオリティタグは0から7までの値で設定され、0が最も低い優先度、7が最も高い優先度を表します。一般的にプライオリティ値「7」は、伝送遅 延に影響を受けやすい音声・映像に関連するデータや、データ転送速度が保証されているような特別なユーザに対して使用されます。

本スイッチでは、プライオリティタグ付きのパケットをどのように扱うかを細かく調整することができます。キューを利用してプライオリティタグ 付きのデータを管理することにより、ご使用のネットワークのニーズに合わせてデータの優先度を設定できます。複数の異なるタグ付きパケットを 同じキューにグループ化することで効果を発揮するケースもありますが、通常は、優先度の最も高いキュー(キュー7)をプライオリティレベル7 のパケットに割り当てることをお勧めします。プライオリティレベルが設定されていないパケットは、キュー0に割り当てられ、最も低い送信優先 度となります。

本スイッチは、優先制御方式として Strict モードと WRR (重み付けラウンドロビン) モードをサポートしています。WRR モードではキューからパケットが送信される比率が決定します。キュー 0 とキュー 7 の送信比率が 4:1 の場合、キュー 0 から 1 つのパケットが送信される毎に、キュー 7 から 4 つのパケットが送信されます。

プライオリティキューはスイッチ上のすべてのポートに対して設定されるため、スイッチに接続されるすべてのデバイスがこの設定による影響を受けることに注意してください。ご利用のネットワーク上のスイッチがプライオリティタグ割り当て機能をサポートしている場合、プライオリティ キューイング機能は特に効果を発揮します。

# VLAN とは

VLAN(Virtual Local Area Network:仮想LAN)とは、物理的なレイアウトではなく、論理的なスキームに従って構成されるネットワークトポロジです。 VLAN を使用することで、LAN セグメントの集まりを自律的なユーザグループへと結合し、1つのLAN のように見せることができます。また、ネットワークを異なるブロードキャストドメインに論理的に分割し、パケットが特定 VLAN 内のポート間にのみ送信されるように設定することが可能です。一般的に、VLAN とサブネットは1対1で対応付けられますが、必ずしもそうである必要はありません。

VLAN では、ネットワーク帯域の消費を抑えることでパフォーマンスを改善し、トラフィックを特定のドメイン内に制限することでセキュリティを 強化します。

VLAN は、物理的位置ではなく論理的にエンドノードを束ねた集合体です。頻繁に通信を行うエンドノード同士に対しては、ネットワーク上の物理 的位置に関わらず、同じ VLAN を割り当てます。ブロードキャストパケットは送信元と同じ VLAN メンバに対してのみ送信されるため、VLAN は論 理的にはブロードキャストドメインと同等と言えます。

#### 本スイッチシリーズにおける VLAN について

エンドノードの識別方法やVLANメンバシップ割り当て方法に関わらず、VLAN間にルーティング機能を持つネットワークデバイスが存在しない限り、 パケットが VLAN をまたいで送信されることはありません。

本スイッチは、IEEE 802.1Q VLAN とポートベース VLAN をサポートします。タグなし機能では、パケットヘッダから 802.1Q タグを取り外すことにより、 タグを認識しないデバイスとの互換性を保ちます。

スイッチの初期状態では、すべてのポートに「default」と名付けられた 802.1Q VLAN が割り当てられています。 「default」VLAN の VID は 1 です。ポートベース VLAN のメンバポートは重複して設定することが可能です。

#### IEEE 802.1Q VLAN

#### 用語の説明

- ・ タグ付け パケットのヘッダに 802.1Q VLAN 情報を挿入すること。
- ・ タグなし パケットのヘッダから 802.1Q VLAN 情報を削除すること。
- ・ イングレスポート(Ingress Port)- スイッチ上のパケットを受信するポート。VLAN の照合が行われます。
- ・ イーグレスポート (Egress Port) スイッチ上のパケットを送信するポート。タグ付けの決定が行われます。

本スイッチには、IEEE 802.1Q(タグ付き)VLAN が実装されています。802.1Q VLAN で行われるタグ付けによってネットワーク全体で 802.1Q VLAN が有効になります(ネットワーク上のすべてのスイッチが IEEE 802.1Q 準拠である場合)。

# 第8章 L2 Features (L2機能の設定)

VLAN によりネットワークを分割することで、ブロードキャストドメインの範囲を小さくすることができます。パケットは、(IEEE 802.1Qをサポートするスイッチを経由して)受信 VLAN と同じ VLAN メンバのステーションのみに送信されます。このパケットには、送信元の不明なブロードキャスト、マルチキャスト、ユニキャストパケットも含まれます。

このほか、VLAN はネットワークにおけるセキュリティ機能を提供します。IEEE 802.1Q VLAN では、VLAN メンバであるステーションにのみパケットが送信されます。

各ポートに対して、タグ付けまたはタグなしに設定することが可能です。IEEE 802.1Q VLAN のタグなし機能により、パケットヘッダ中の VLAN タグ を認識しない旧式のスイッチと連携することができます。タグ付け機能では、802.1Q 準拠の複数のスイッチを1つの物理接続により結びつけ、す べてのポート上でスパニングツリーを有効にして正常に動作させることができます。

IEEE 802.1Q 標準では、受信ポートが所属する VLAN へのタグなしパケットの送信を禁じています。

IEEE 802.1Q 標準規格の主な特徴は以下の通りです。

- ・フィルタリングによりパケットを VLAN に割り当てます。
- 全体で1つのスパニングツリーが構成されていると仮定します。
- ・1レベルのタグ付けにより明示的なタグ付けスキームを使用します。
- ・ 802.1Q VLAN のパケット転送
- パケットの転送は以下の3種類のルールに基づいて決定されます。
   イングレスルール VLAN に所属する受信フレームの分類に関するルール。
   ポート間のフォワーディングルール 転送するかしないかを決定します。
   イーグレスルール パケットが送信される時にタグ付きかタグなしかを決定します。



図 8-1 IEEE 802.1Q パケットフォワーディング

#### 02.1Q VLAN タグ

次の図は 802.1Q VLAN のタグについて表しています。ソース MAC アドレスの後に 4 オクテットのフィールドが挿入されており、EtherType フィー ルドに設定された0x8100 という値により、パケットに IEEE 802.1Q/802.1p タグが含まれていることが示されています。 タグはその後に続く 2 オクテッ トに含まれており、ユーザプライオリティの 3 ビット、CFI(Canonical Format Identifier: イーサネットバックボーンを介して転送できるようにトーク ンリングパケットをカプセル化するために使用される)の1 ビット、および VID(VLAN ID)の 12 ビットによって構成されています。ユーザプライオ リティの 3 ビットは 802.1p によって使用されます。VID は VLAN を識別するためのもので、802.1Q 規格によって使用されます。VID は長さが 12 ビッ トであるため、4094 個の一意の VLAN を構成することができます。

タグはパケットヘッダに埋め込まれ、パケット全体は4オクテット分長くなります。元々のパケットに含まれていた情報はすべて保持されます。



IEEE 802.1Q タグ

EtherType と VLAN ID は、ソース MAC アドレスと元の Length/EtherType または Logical Link Control の間に挿入されます。パケットは元のものよりも少し長くなるため、CRC は再計算されます。



図 8-3 IEEE 802.1Q タグの挿入

#### ポート VLAN ID

802.1Q VID 情報が含まれるタグ付きパケットは、802.1Q に対応したネットワークデバイスから他のデバイスまで、VLAN 情報を完全に保持したまま 転送されます。従って、すべてのネットワークデバイスが 802.1Q に準拠している場合、ネットワーク全体をまるごと 802.1Q VLAN によって結ぶこ とができます。

しかしながら、すべてのネットワークデバイスが 802.1Q に準拠しているわけではありません。これらの 802.1Q 非準拠のデバイスを tag-unaware (タ グ認識不可)、 802.1Q 準拠のデバイスを tag-aware (タグ認識可能) と呼ぶことにします。

802.1Q VLAN が採用される以前は、ポートベースや MAC ベースの VLAN が主流でした。これら VLAN のパケット送信は、ポート VLAN ID (PVID) を元に行われます。あるポートでタグなしパケットを受信した場合、パケットにはその受信ポートの PVID が割り当てられ、パケットの宛先アドレスに対応するポート(スイッチのフォワーディングテーブルで検出)へと送信されます。パケットを受信したポートの PVID が送信先ポートの PVID と異なる場合、パケットは破棄されます。

スイッチ内では、PVID が異なるということは VLAN が異なることを意味します(2 つの VLAN は外部ルータを経由しないと通信ができません)。そのため、PVID をベースにした VLAN の識別の場合、スイッチ(またはスイッチスタック)の外部へ VLAN を拡張することができません。

スイッチの各物理ポートには PVID が割り当てられています。802.1Q ポートにも PVID が割り当てられており、スイッチ内で使用されます。スイッ チ上で VLAN が定義されていない場合、すべてのポートは PVID 1 のデフォルト VLAN が割り当てられます。タグなしのパケットは、パケットの受信 ポートの PVID が割り当てられます。フォワーディングはこの PVID を元に決定されます。タグ付きのパケットにも PVID が割り当てられますが、フォ ワーディング処理はタグ中に含まれる VID に従います。

tag-aware(タグ認識可能)スイッチは、スイッチ内の PVID とネットワークの VID を対応付けるテーブルを保持している必要があります。スイッチ は送信されるパケットの VID と、パケット送信を行うポートの VID を比較します。これらの VID が一致しない場合、パケットは廃棄されます。タグ なしパケットには PVID、タグ付きパケットには VID が存在するため、タグを認識するネットワークデバイスも認識しないデバイスも、同じネットワー ク内に共存が可能になります。

PVID は 1 ポートあたり 1 つしか持つことはできませんが、VID はスイッチの VLAN テーブルのメモリ上限まで持つことができます。

ネットワーク上にはタグを認識しないデバイスが存在するため、送信するパケットにタグを付けるかどうかの判断を、タグを認識できるデバイスの 各ポートで行わなければなりません。送信するポートがタグを認識しないデバイスと接続していれば、タグなしのパケットを送信し、逆にタグを認 識するデバイスと接続していれば、タグ付きのパケットを送信します。

#### タグ付きとタグなし

802.1Qに対応するスイッチのすべてのポートは、タグ付きかタグなしに設定できます。

タグ付きのポートは、送受信するすべてのパケットのヘッダに VID、プライオリティ、その他の VLAN 情報を埋め込みます。パケットが既にタグ 付けされている場合、パケットは変更されず VLAN 情報は完全に保たれます。これにより、ネットワーク上の他の 802.1Q 対応デバイスは、タグの VLAN 情報を使用してパケットの転送処理を決定することができます。

タグなしとして設定されているポートは、送受信するすべてのパケットから802.1Qタグを削除します。パケットに802.1Q VLAN タグがない場合、ポートはパケットを変更しません。従って、タグなしのポートで受信、転送されたすべてのパケットは802.1Q VLAN 情報を持っていません。PVID はスイッチの内部のみで使用されます。タグの削除は、802.1Q 対応のデバイスから非対応のデバイスにパケットを送信する場合に使用されます。

#### イングレスフィルタリング

スイッチ上のポートの内、スイッチへのパケットの入り口となり、VLANを照合するポートをイングレスポートと呼びます。イングレスフィルタリ ングがポート上で有効に設定されていれば、スイッチはパケットヘッダ内の VLAN 情報を参照し、パケットの送信を行うかどうかを決定します。

パケットに VLAN 情報のタグが付加されている場合、イングレスポートはまず、自分自身がその VLAN のメンバであるかどうかを確認します。メン バでない場合、そのパケットは廃棄されます。イングレスポートが 802.1Q VLAN のメンバであれば、スイッチは送信先ポートが 802.1Q VLAN のメ ンバであるかどうかを確認します。802.1Q VLAN メンバでない場合は、そのパケットは廃棄されます。送信先ポートが 802.1Q VLAN のメンバであれば、 そのパケットは送信され、送信先ポートはそのパケットを接続するネットワークセグメントに転送します。

パケットに VLAN 情報のタグが付加されていない場合は、イングレスポートはそのパケットに VID として自分の PVID を付加します。するとスイッ チは、送信先ポートはイングレスポートと同じ VLAN のメンバであるか(同じ VID を持っているか)を確認します。同じ VLAN メンバでない場合、 パケットは廃棄されます。同じ VLAN メンバである場合、パケットは送信され、送信先ポートはそのパケットを接続するネットワークセグメントに 転送します。

本プロセスは、イングレスフィルタリングと呼ばれ、イングレスポートとの VLAN とは異なるパケットを受信時に廃棄することにより、スイッチ内 での帯域を有効利用するために使用されます。これにより、送信先ポートに届いてから廃棄されるパケットを事前に処理することができます。

#### デフォルト VLAN

スイッチには、初期設定で「default」という名前で VID が 1 の VLAN が設定されています。本製品の初期設定ではスイッチ上のすべてのポートが 「default」に割り当てられています。新しい VLAN がポートベースモードで設定される時、そのポートは自動的に「default」 VLAN から削除されます。

パケットは VLAN 間を通過できません。ある VLAN のメンバが他の VLAN と接続を行うためには、そのリンクは外部ルータを経由する必要があります。

注意

スイッチ上に VLAN が設定されていない場合、各パケットは任意の送信先ポートへと転送されます。宛先アドレスが不明なパケットやブロードキャストパケット、マルチキャストパケットはすべてのポートに送信されます。

VLAN の設定例を以下に示します。

VLAN 名	VID	ポート番号
System (default)	1	5、6、7
Engineering	2	9、10
Sales	5	1、2、3、4

#### ポートベース VLAN

ポートベース VLAN は、スイッチポート単位で送受信するトラフィックを制限します。そのため、スイッチのポートに1台のコンピュータが直接接 続されていようと、部門全体が接続されていようと、そのポートに接続されたすべてのデバイスは、そのポートが所属している VLAN のメンバにな ります。

ポートベース VLAN では、NIC はパケットヘッダ内の 802.1Q タグを識別できる必要はありません。NIC は通常のイーサネットパケットを送受信しま す。パケットの送信先が同じセグメント上にある場合、通常のイーサネットプロトコルを使用して通信が行われます。パケットの送信先が別のスイッ チポートである場合、スイッチによってパケットが破棄されるか転送を行うかは VLAN の照会によって決定されます。

#### VLAN セグメンテーション

VLAN 2 に所属するポート1から送信されるパケットを例に説明します。宛先が別のポートである場合(通常のフォワーディングテーブル検索により判定)、スイッチはそのポート(ポート10)が VLAN 2 に所属しているか(つまり VLAN 2 パケットを受け取れるか)どうかを確認します。ポート 10が VLAN 2 のメンバでない場合は、スイッチはそのパケットを廃棄します。メンバである場合、パケットは送信されます。ポート1が VLAN 2 にのみ送信を行うという点が重要です。このように VLAN の仕組みに基づいて選択的にフォワーディング処理が行われることで、ネットワークの分割を実現します。

# VLAN (VLAN 設定)

# VLAN Configuration Wizard (VLAN 設定ウィザード)

VLAN の作成と設定を行います。

L2 Features > VLAN > VLAN Configuration Wizard の順にメニューをクリックして、以下の画面を表示します。

VLAN Configuration Wizard	
VLAN Configuration Wizard	
Create VLAN	
VID (1-4094)	
O Configure VLAN	
VID (1-4094)	
	Next

図 8-4 VLAN Configuration Wizard 画面

画面に表示される項目:

項目	内容
Create VLAN	新しく VLAN を作成する場合に選択します。VID を 2-4094 の間で入力します。
	VID 1 は default VLAN に設定されているため、本項目では入力できません。
Configure VLAN	作成済みの VLAN を設定する場合に選択します。設定するの VID を入力します。

「Next」をクリックし、以下の画面で設定を行います。

/ID	2
/LAN Name	VLAN0002
Port	Select All 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 9 20 21 22 23 24 25 26 27 2
Tagged	
Untagged	
Not Member	
Native VLAN (PVID)	
VLAN Mode	нннннннннннннннннннн
Access, n-nybrid, 1-11drik,	
lote: The selected member p access Mode: The port will be 'runk Mode: The port is either lybrid Mode: The port can be lot1q-Tunnel Mode: The port	ont(s) will be mandatory configured to Hybird mode. an untagged member of VLAN. a tagged port or an untagged member port of it's native VLAN and can be a tagged member of other VLANs configured. an untagged or a tagged member of all VLANs configured. behaves as an UNI port of a service VLAN.
lote: The selected member p access Mode: The port will be frunk Mode: The port is either lybrid Mode: The port can be Dot1q-Tunnel Mode: The port Private VLAN Mode: The port	ont(s) will be mandatory configured to Hybird mode. an untagged member of VLAN. a tagged port or an untagged member port of it's native VLAN and can be a tagged member of other VLANs configured. an untagged or a tagged member of all VLANs configured. behaves as an UNI port of a service VLAN. behaves as a Private VLAN port.

画面に表示される項目	:	
------------	---	--

項目	内容
VID	選択した VID が表示されます。
VLAN Name	VLAN名を入力します。
Port	各ポートを以下の通り VLAN のメンバとして定義します。
	• Tagged - ポートを 802.1Q タグ付きとして定義します。タグ付きとするポートのボックスをチェックします。
	・ Not Member - 各ポートが VLAN メンバでないことを定義します。
	・ Native VLAN (PVID) - ポートをネイティブ VLAN として定義します。
	「AII」ボタンをクリックすると、すべてのポートが選択されます。
VLAN Mode	各ポートの VLAN モードが表示されます。
	アルファベットの表示は以下のモードを表します。
	・ A:Access モード ポートは VLAN のタグなしメンバになります。
	・ H:Hybrid モード ポートは設定されているすべての VLAN のタグなしまたはタグ付きメンバにすることができます。
	<ul> <li>T: Trunk モード ポートはネイティブ VLAN のタグ付きポートまたはタグなしメンバポートのいずれかであり、設定されている他の VLAN のタグ付きメンバにすることができます。</li> </ul>
	・ D:Dot1q トンネルモード ポートはサービス VLAN の UNI(User Network Interface ) ポートとして動作します。
	・ P:Private VLAN (Host/Promiscuous/Trunk Promiscuous/Trunk Secondary) モード ポートはプライベート VLAN ポートとして動作します。
View Allowd VLAN	許可された VLAN の一覧が別ウィンドウで表示されます。

「Apply」をクリックし、設定を適用します。

# 802.1Q VLAN (802.1Q VLAN)

802.1Q VLAN を設定します。

L2 Features > VLAN > 802.1Q VLAN の順にメニューをクリックして、以下の画面を表示します。

#### VLAN リストの表示

「VLAN List」タブでは、既に設定されている VLAN の VLAN ID と VLAN 名が表示されます。

02.1Q VLAN						
VID List	3 or 2-5				Apply	Delete
nd VLAN						
VID (1-4094)					Find	Show All
Total Entries	:1					
VID	VLAN Name	Tagged Member Ports	Untagged Member Ports	VLAN Type		
	default		1/0/1-1/0/22		Edit	Delete
1	ordram					-

図 8-6 802.1Q VLAN Settings 画面

#### 画面に表示される項目:

項目	内容		
	802.1Q VLAN		
VID List	ist VID の範囲を指定します。		
	Find VLAN		
VID(1-4094)	表示する VLAN ID を指定します。		

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Show All」をクリックして、すべてのエントリを表示します。

「Edit」をクリックして、指定エントリの編集を行います。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

# VLAN Interface (VLAN インタフェース)

VLAN インタフェースの設定を行います。

**L2 Features > VLAN > VLAN Interface** の順にメニューをクリックします。 本画面には、「VLAN Interface Settigns」タブと「Port Summary」タブがあります。

# VLAN Interface(VLAN インタフェース設定)

「VLAN Interface Settings」タブでは、各ポートの VLAN インタフェース設定の確認、および編集を実行できます。

N Inter	face erface Settings	Port Sum	mary		
Port	VLAN Mode	Ingress Checking	Acceptable Frame Type		-
1/0/1	Hybrid	Enabled	Admit-All	Show Detail	Edit
1/0/2	Hybrid	Enabled	Admit-All	Show Detail	Edit
/0/3	Hybrid	Enabled	Admit-All	Show Detail	Edit
/0/4	Hybrid	Enabled	Admit-All	Show Detail	Edit

図 8-7 VLAN Interface Settings タブ 画面

#### エントリの編集

「Edit」ボタンをクリックして、指定エントリの編集をします。

#### VLAN 詳細情報の表示

「Show Detail」ボタンをクリックして、指定インタフェースの VLAN について詳細情報について表示します。

#### ■ Show Deteil (VLAN 詳細情報の表示)

「Show Detail」をクリックすると、以下の画面で各ポートの VLAN インタフェース設定を確認できます。

LAN Interface Informati	on
VLAN Interface Information	
Port	eth1/0/1
VLAN Mode	Hybrid
Native VLAN	1
Hybrid Untagged VLAN	1
Hybrid Tagged VLAN	
Dynamic Tagged VLAN	
VLAN Precedence	MAC-VLAN
Ingress Checking	Enabled
Acceptable Frame Type	Admit-All
	Back

図 8-8 VLAN Interface Information 画面

#### ■ Edit (VLAN インタフェース設定の編集)

「Edit」をクリックすると、各ポートの VLAN インタフェース設定を編集できます。

画面に表示される項目は、「VLAN Mode」で設定した VLAN モードによって異なります。 選択できる VLAN モードは以下です。

#### ● VLAN モード「Access」を選択した場合:

Configure VLAN Interface			
Configure VLAN Interface			
Port	eth1/0/1	Clone	
VLAN Mode	Access 🗸	From Port	To Port
Acceptable Frame	Untagged Only	eth1/0/1 🗸	eth1/0/1 🔽
Ingress Checking	Enabled O Disabled		
VID (1-4094)	1		
			Back Apply

図 8-9 Configure VLAN Interface - Access 画面

#### 画面に表示される項目:

項目	内容
Port	選択したポートが表示されます。
VLAN Mode	VLAN モードを「Access」にします。
Acceptable Frame	許可するフレームの種類を「Tagged Only」「Untagged Only」「Admit All」から選択します。
Ingress Checking	イングレスチェック機能を「Enabled」(有効)/「Disabled」(無効)に指定します。
VID	設定する「VLAN ID」を指定します。1 から 4094 で指定可能です。
Clone	クローンを有効にします。
From Port / To Port	設定するポートの始点 / 終点を設定します。
Et la la la la la la	

「Apply」をクリックし、設定を適用します。 「Back」をクリックすると前の画面に戻ります。

#### ● VLAN モード「Hybrid」を選択した場合:

Configure VLAN Interface			
Configure VLAN Interface			
Port	eth1/0/1	Clone	
VLAN Mode	Hybrid 🗸	From Port	To Port
Acceptable Frame	Admit All	eth1/0/1 🔽	eth1/0/1 🔽
Ingress Checking	Enabled      Disabled		
VLAN Precedence	Mac-based VLAN		
Native VLAN	✓ Native VLAN		
VID (1-4094)	1		
Action	Add		
Add Mode	● Untagged ◯ Tagged		
Allowed VLAN Range			
Current Hybrid Untagged VLAN Range	1		
Current Hybrid Tagged VLAN Range			
			Back Apply

図 8-10 Configure VLAN Interface - Hybrid 画面

# 第8章 L2 Features (L2機能の設定)

### 画面に表示される項目:

項目	内容
Port	選択したポートが表示されます。
VLAN Mode	VLAN モードを「Hybrid」にします。
Acceptable Frame	許可するフレームの種類を「Tagged Only」「Untagged Only」「Admit All」から選択します。
Ingress Checking	イングレスチェック機能を「Enabled」(有効)/「Disabled」(無効)に指定します。
VLAN Precedence	優先 VLAN を以下から選択します。
	「Mac-based VLAN」「Subnet-based VLAN」
Native VLAN	Native VLAN を有効にします。
VID	Native VLAN を有効にした場合は、設定する「VLAN ID」を指定します。1 から 4094 で指定可能です。
Action	実行する動作を「Add」「Remove」「Tagged」「Untagged」から選択します。
Add Mode	「Add Mode」のパラメータに「Untagged」または「Tagged」を追加します。
Allowed VLAN Range	許可した VLAN 範囲情報を指定します。
Clone	クローンを有効にします。
From Port / To Port	設定するポートの始点 / 終点を設定します。
 「Apply」をクリックし。	設定を適用します。

「Apply」をクリックし、設定を適用します。 「Back」をクリックすると前の画面に戻ります。

### ● VLAN モード「Trunk」を選択した場合:

Configure VLAN Interface			
Configure VLAN Interface			
Port	eth1/0/1	Clone	
VLAN Mode	Trunk	From Port	To Port
Acceptable Frame	Admit All	eth1/0/1 🔽	eth1/0/1 🔽
Ingress Checking	Enabled O Disabled		
Native VLAN	Native VLAN Outlagged C Tagged		
VID (1-4094)	1		
Action	None		
Allowed VLAN Range			
Current Allowed VLAN Range			
			Back Apply

図 8-11 Configure VLAN Interface - Trunk 画面

#### 画面に表示される項目:

項目	内容
Port	選択したポートが表示されます。
VLAN Mode	VLAN モードを「Trunk」にします。
Acceptable Frame	許可するフレームの種類を「Tagged Only」「Untagged Only」「Admit All」から選択します。
Ingress Checking	イングレスチェック機能を「Enabled」(有効)/「Disabled」(無効)に指定します。
Native VLAN	Native VLAN を有効にします。「Untagged」または「Tagged」フレームを選択します。
VID	Native VLAN を有効にした場合は、設定する「VLAN ID」を指定します。1 から 4094 で指定可能です。
Action	実行する動作を「All」「Add」「Remove」「Except」「Replace」から選択します。
Allowed VLAN Range	許可した VLAN 範囲情報を指定します。
Clone	クローンを有効にします。
From Port / To Port	設定するポートの始点 / 終点を設定します。

「Apply」をクリックし、設定を適用します。

### ● VLAN モード「Dot1q-Tunnel」を選択した場合:

Configure VLAN Interface		_	
Configure VLAN Interface			
Port	eth1/0/1	Clone	
VLAN Mode	Dot1q-Tunnel	From Port	To Port
Acceptable Frame	Admit All	eth1/0/1 🔽	eth1/0/1 🔽
Ingress Checking	Enabled      Disabled		
VLAN Precedence	Mac-based VLAN 🔽		
VID (1-4094)	1		
Action	Add 🗸		
Add Mode	Untagged   Tagged		
Allowed VLAN Range			
Current Hybrid Untagged VLAN Range	1		
			Back Apply

図 8-12 Configure VLAN Interface - Dot1q-Tunnel 画面

#### 画面に表示される項目:

項目	内容
Port	選択したポートが表示されます。
VLAN Mode	VLAN モードを「Dot1q-Tunnel」にします。
Acceptable Frame	許可するフレームの種類を「Tagged Only」「Untagged Only」「Admit All」から選択します。
Ingress Checking	イングレスチェック機能を「Enabled」(有効)/「Disabled」(無効)に指定します。
VLAN Precedence	優先 VLAN を以下から選択します。
	「Mac-based VLAN」「Subnet-based VLAN」
VID	Native VLAN を有効にした場合は、設定する「VLAN ID」を指定します。1 から 4094 で指定可能です。
Action	実行する動作を「Add」「Remove」から選択します。
Add Mode	「Add Mode」のパラメータに「Untagged」を追加します。
Allowed VLAN Range	許可した VLAN 範囲情報を指定します。
Clone	クローンを有効にします。
From Port / To Port	設定するポートの始点 / 終点を設定します。

「Apply」をクリックし、設定を適用します。 「Back」をクリックすると前の画面に戻ります。

#### ● VLAN モード「Promiscuous」を選択した場合:

Configure VLAN Interface				_
Configure VLAN Interface				
Port	eth1/0/1	Clone		
VLAN Mode	Promiscuous 🗸	From Port	To Port	
Acceptable Frame	Tagged Only	eth1/0/1 🔽	eth1/0/1 🔽	
Ingress Checking	$\odot$ Enabled $\bigcirc$ Disabled			
			Back	Apply

図 8-13 Configure VLAN Interface - Promiscuous 画面

#### 画面に表示される項目:

項目	内容
Port	選択したポートが表示されます。
VLAN Mode	VLAN モードを「Promiscuous」にします。
Acceptable Frame	許可するフレームの種類を「Tagged Only」「Untagged Only」「Admit All」から選択します。
Ingress Checking	イングレスチェック機能を「Enabled」(有効)/「Disabled」(無効)に指定します。
Clone	クローンを有効にします。
From Port / To Port	設定するポートの始点 / 終点を設定します。

「Apply」をクリックし、設定を適用します。

# ● VLAN モード「Host」を選択した場合:

I	Configure VLAN Interface			
	Configure VLAN Interface			
	Port	eth1/0/1	Clone	
	VLAN Mode	Host 🗸	From Port	To Port
	Acceptable Frame	Admit All	eth1/0/1 🔽	eth1/0/1 🔽
	Ingress Checking	Enabled O Disabled		
				Back Apply

図 8-14 Configure VLAN Interface - Host 画面

#### 画面に表示される項目:

項目	内容
Port	選択したポートが表示されます。
VLAN Mode	VLAN モードを「Host」にします。
Acceptable Frame	許可するフレームの種類を「Tagged Only」「Untagged Only」「Admit All」から選択します。
Ingress Checking	イングレスチェック機能を「Enabled」(有効)/「Disabled」(無効)に指定します。
Clone	クローンを有効にします。
From Port / To Port	設定するポートの始点 / 終点を設定します。

「Apply」をクリックし、設定を適用します。

「Back」をクリックすると前の画面に戻ります。

#### ● VLAN モード「Trunk Promiscuous」を選択した場合:

Configure VLAN Interface			
Configure VLAN Interface			
Port	eth1/0/1	Clone	
VLAN Mode	Trunk Promiscuous 🔽	From Port	To Port
Acceptable Frame	Admit All	eth1/0/1 🔽	eth1/0/1 🔽
Ingress Checking	Enabled      Disabled		
Native VLAN	<ul> <li>Native VLAN</li> <li>Untagged  Tagged</li> </ul>		
VID (1-4094)	1		
Action	None 🔽		
Allowed VLAN Range	1		
Current Allowed VLAN Range			
			Back Apply

🗵 8-15	Configure	VLAN Interface	- Trunk	Promiscuous	画面
--------	-----------	----------------	---------	-------------	----

#### 画面に表示される項目:

項目	内容
Port	選択したポートが表示されます。
VLAN Mode	VLAN モードを「Trunk Promiscuous」にします。
Acceptable Frame	許可するフレームの種類を「Tagged Only」「Untagged Only」「Admit All」から選択します。
Ingress Checking	イングレスチェック機能を「Enabled」(有効)/「Disabled」(無効)に指定します。
Native VLAN	Native VLAN を有効にします。「Untagged」または「Tagged」フレームを選択します。
VID	Native VLAN を有効にした場合、設定する「VLAN ID」を指定します。1 から 4094 で指定可能です。
Action	実行する動作を「All」「Add」「Remove」「Except」「Replace」から選択します。
Allowed VLAN Range	許可した VLAN 範囲情報を指定します。
Current Allowed VLAN	現在の許可された VLAN の範囲が表示されます。
Range	
Clone	クローンを有効にします。
From Port / To Port	設定するポートの始点 / 終点を設定します。

「Apply」をクリックし、設定を適用します。

● VLAN モード「Trunk Secondary」を選択した場合:

Configure VLAN Interface			
Port VLAN Mode Acceptable Frame Ingress Checking Native VLAN VID (1-4094)	eth1/0/1 Trunk Secondary Admit All Enabled  Native VLAN Untagged Tagged 1	Clone From Port eth1/0/1	To Port eth1/0/1
Action Allowed VLAN Range Current Allowed VLAN Range	None		Back Apply

図 8-16 Configure VLAN Interface - Trunk Secondary 画面

#### 画面に表示される項目:

項目	内容	
Port	選択したポートが表示されます。	
VLAN Mode	VLAN モードを「Trunk Secondary」にします。	
Acceptable Frame	許可するフレームの種類を「Tagged Only」「Untagged Only」「Admit All」から選択します。	
Ingress Checking	イングレスチェック機能を「Enabled」(有効)/「Disabled」(無効)に指定します。	
Native VLAN	Native VLAN を有効にします。「Untagged」または「Tagged」フレームを選択します。	
VID	Native VLAN を有効にした場合、設定する「VLAN ID」を指定します。1 から 4094 で指定可能です。	
Action	実行する動作を「All」「Add」「Remove」「Except」「Replace」から選択します。	
Allowed VLAN Range	許可した VLAN 範囲情報を指定します。	
Clone	クローンを有効にします。	
From Port / To Port	設定するポートの始点 / 終点を設定します。	

「Back」をクリックすると前の画面に戻ります。

# Port Summary (ポートサマリー)

「Port Summary」タブでは、各ポートの VLAN インタフェース設定を確認できます。

# VLAN Interface

face Settings	Port Sumn	nary		
VLAN Mode	Native VLAN	Untagged VLAN	Tagged VLAN	Dynamic Tagged VLAN
Hybrid	1	1		
Hybrid	1	1		
Hybrid	1	1		
Hybrid	1	1		
Hybrid	1	1		
Hybrid	1	1		
Hybrid	1	1		
Hybrid	1	1		
Hybrid	1	1		
	face Settings           VLAN Mode           Hybrid           Hybrid	VLAN ModeNative VLANHybrid1Hybrid1Hybrid1Hybrid1Hybrid1Hybrid1Hybrid1Hybrid1Hybrid1Hybrid1Hybrid1Hybrid1Hybrid1Hybrid1Hybrid1Hybrid1Hybrid1Hybrid1Hybrid1	Face SettingsPort SummaryVLAN ModeNative VLANUntagged VLANHybrid11Hybrid11Hybrid11Hybrid11Hybrid11Hybrid11Hybrid11Hybrid11Hybrid11Hybrid11Hybrid11Hybrid11Hybrid11Hybrid11Hybrid11	Face SettingsPort SummaryVLAN ModeNative VLANUntagged VLANTagged VLANHybrid11Hybrid11Hybrid11Hybrid11Hybrid11Hybrid11Hybrid11Hybrid11Hybrid11Hybrid11Hybrid11Hybrid11Hybrid11Hybrid11Hybrid11

図 8-17 VLAN Interface - Port Summary 画面

# 802.1v Protocol VLAN (802.1v プロトコル VLAN)

802.1v Protocol VLAN フォルダには「Protocol VLAN Profile」および「Protocol VLAN Profile Interface」の2つの画面があります。

### Protocol VLAN Profile(プロトコル VLAN プロファイル設定)

本テーブルで、プロトコル VLAN グループを作成し、そのグループにプロトコルを追加します。802.1v プロトコル VLAN グループ設定は、各プロト コルのためにマルチプル VLAN をサポートし、同じ物理ポートに異なるプロトコルを持つタグなしポートの設定が可能です。例えば、同じ物理ポー トに 802.1Q と 802.1v タグなしポートを設定できます。

L2 Features > VLAN > 802.1v Protocol VLAN > Protocol VLAN Profile の順にメニューをクリックし、以下の画面を表示します。

Protocol VLAN Profile			
Add Protocol VLAN Profile Profile ID (1-16) Total Entries: 1	Frame Type Ethernet2  Ether Type (0x0-0)	xFFFF) 0x	Apply
Profile ID	Frame Type	Ether Type	
1	Ethernet2	0xFFFF(User define)	Delete

図 8-18 Protocol VLAN Profile 画面

#### 画面に表示される項目:

項目	説明
Profile ID	802.1v プロトコル VLAN プロファイル ID 番号を 1-16 の範囲から指定します。
Frame Type	フレームタイプを選択します。本機能は、関連するプロトコルのタイプを検出するためにパケットヘッダのタイプオクテット を検証することで、パケットをプロトコルで定義された VLAN にマップします。「Ethernet 2」「LLC」「SNAP」から選択します。
Ether Type	グループに対してイーサネットタイプを指定します。プロトコル値は、指定されたフレームタイプのプロトコルを識別す るために使用されます。入力形式は 0x0 から 0xffff です。オクテット文字列は、フレームタイプによって、以下に示す値 の 1 つを持っています。 ・ Ethernet 2 - 16 ビット (2 オクテット)の 16 進数です。例えば、IPv4 は 0800、IPv6 は 86dd、ARP は 0806 などです。 ・ IEEE802.3 SNAP - 16 ビット (2 オクテット)の 16 進数です。 ・ IEEE802.3 LLC - 2 オクテットの IEEE 802.2 Link Service Access Point(LSAP) ペアです。はじめのオクテットは、 Destination Service Access Point (DSAP) のための値であり、2 番目のオクテットは送信元のための値です。

「Apply」をクリックし、設定内容を適用します。 「Delete」をクリックすると指定のエントリを削除します。

# Protocol VLAN Profile Interface(プロトコル VLAN プロファイルインタフェース)

プロトコル VLAN ポートの設定を行います。テーブルの下半分は定義済みのすべての設定を表示します。

L2 Features > VLAN > 802.1v Protocol VLAN > Protocol VLAN Profile Interface の順にメニューをクリックし、以下の画面を表示します。

otocol VLAN Profile Int	erface			
dd New Protocol VLAN Interfac	e			
Port 1 v eth1/0/1	V Profile ID 1 VI	D (1-4094)	Priority 0	<ul> <li>Apply</li> </ul>
Jnit 1 Settings				
Port	Profile ID	VID	Priority	
eth1/0/18	1	1	0	Delete

図 8-19 Protocol VLAN Profile Interface 画面

両エにまことやて西口	•	
囲間に表示される項目		
	•	

項目	説明
Port	設定するスタッキングユニット ID とポート番号を指定します。
Profile ID	対応するボタンをチェックし、プルダウンメニューから定義済みの Profile ID を選択します。
VID (1-4094)	対応するボタンをチェックし、VID を入力します。これは、VLAN 名と共に、ユーザが作成する VLAN を識別するために使用する ID です。
Priority	スイッチに設定済みの 802.1p デフォルトプライオリティ(パケットが送られる CoS キューを決定するために使用)の設定を書 き換える場合に使用します。本項目を選択すると、スイッチが受信したパケット内の本プライオリティに一致するパケットは、 既に指定した CoS キューに送られます。本画面で設定した基準に一致するパケットが、指定された CoS キューに送られる前に、 パケットの 802.1p デフォルトプライオリティを、「Priority(0-7)」に指定した値に書き換える場合に対応するボックスをクリッ クします。指定しない場合は、パケットは送出される前に、入力用の 802.1p ユーザプライオリティを元の値に書き換えられます。

「Apply」をクリックし、設定内容を適用します。 「Delete」をクリックすると指定のエントリを削除します。

# GVRP (GVRP の設定)

### GVRP Global (GVRP グローバル設定)

GVRP(GARP VLAN Registration Protocol)が有効なスイッチ同士で VLAN 構成情報を共有するかどうかを指定することができます。さらに、Ingress を「Enabled」(有効)にすることで、VID がポートの PVID と一致しない入力パケットをフィルタしてトラフィックを制限します。 設定内容は、設定画面下部のテーブルで参照することができます。

#### L2 Features > VLAN > GVRP > GVRP Global の順にクリックし、以下の画面を表示します。

GVRP Global	
GVRP Global	
Global GVRP State	CEnabled  ODisabled
Dynamic VLAN Creation	Enabled     Obisabled
NNI BPDU Address	Dot1d 🔽
	Apply

図 8-20 GVRP Global 画面

画面に表示される項目:	
項目	説明
Global GVRP State	GVRP 状態をグローバルに有効 / 無効にします。
	• Enabled - デバイスで GVRP を有効に設定します。
	・ Disabled - デバイスで GVRP を無効に設定します。(初期値)
Dynamic VLAN	ダイナミック VLAN クリエーション機能を「Enabled」(有効)/「Disabled」(無効)に指定します。
Creation	
NNI BPDU Address	カスタマネットワークにおける GVRP の BPDU プロトコルアドレスを決定します。802.1d GVRP アドレス、802.1ad サービ
	スプロバイダの GVRP アドレスまたはユーザ定義のマルチキャストを使用します。「Dot1d」「Dot1ad」から指定します。

「Apply」ボタンをクリックし、デバイスに GVRP 設定を適用します。

#### GVRP Port (GVRP ポート設定)

GVRP ポートパラメータを設定します。

#### L2 Features > VLAN > GVRP Settings > GVRP Port の順にクリックし、以下の画面を表示します。

VRP Port				
Unit From Port	To Port	GVRP Status Join Time (10-10000)	Leave Time (10-10000)	Leave All Time (10-10000)
1 v eth1/0/1 v Note:	eth1/0/1 🗸	Disabled 20 centised	conds 60 centisecon	nds 1000 centiseconds Apply
The Leave Time should be	no less than 3 * Join Time.			
Leave All Time should be g	reater than Leave Time.			
Jnit 1 Settings Port	GVRP Status	Join Time	Leave Time	Leave All Time
Joit 1 Settings Port eth1/0/1	GVRP Status Disabled	Join Time 20	Leave Time	Leave All Time 1000
Jnit 1 Settings Port eth1/0/1 eth1/0/2	GVRP Status Disabled Disabled	Join Time           20           20           20	Leave Time           60           60	Leave All Time 1000 1000
Jnit 1 Settings Port eth1/0/1 eth1/0/2 eth1/0/3	GVRP Status Disabled Disabled Disabled	Join Time           20           20           20           20           20	Leave Time 60 60 60 60	Leave All Time 1000 1000 1000
Unit 1 Settings Port eth1/0/1 eth1/0/2 eth1/0/3 eth1/0/4	GVRP Status Disabled Disabled Disabled Disabled Disabled	Join Time           20           20           20           20           20           20           20           20           20           20           20	Leave Time           60           60           60           60           60           60           60           60	Leave All Time 1000 1000 1000 1000 1000
Jnit 1 Settings Port eth1/0/1 eth1/0/2 eth1/0/3 eth1/0/4 eth1/0/5	GVRP Status Disabled Disabled Disabled Disabled Disabled Disabled Disabled	Join Time           20           20           20           20           20           20           20           20           20           20           20           20           20           20           20	Leave Time           60           60           60           60           60           60           60           60           60           60           60	Leave All Time 1000 1000 1000 1000 1000 1000

図 8-21 GVRP Port 画面

画面に表示される項目:

項目	説明
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。
GVRP Status	GVRP が各ポートで有効かどうかを設定します。有効にするとポートが自動的に VLAN のメンバになります。 ・ Enabled - 選択したポートで GVRP を有効にします。 ・ Disabled - 選択したポートで GVRP を無効にします。(初期値)
Join Time (10-10000)	センチ秒で開始時間を設定します。初期値は 20 です。
Leave Time (10-10000)	センチ秒で終了時間を設定します。初期値は 60 です。
Leave All Time (10-10000)	センチ秒で全終了時間を設定します。初期値は 1000 です。

「Apply」ボタンをクリックし、デバイスに GVRP 設定を適用します。

# GVRP Advertise VLAN(GVRP Advertise VLAN 設定)

GVRP advertised VLAN の設定、表示を行います。

L2 Features > VLAN > GVRP > GVRP Advertise VLAN の順にクリックし、以下の画面を表示します。

GVRP Ad	vertise VLAN				
GVRP Adve	ertise VLAN				
Unit	From Port	To Port	Action	Advertise VID List	
1	eth1/0/1	eth1/0/1	Add 💌	1,3 or 2-5	Apply
Unit 1 Sett	tings				
	Port			Advertise VLAN	
	eth1/0	/1			
	eth1/0	/2			
	eth1/0	/3			
	eth1/0	/4			
	eth1/0	/5			

図 8-22 GVRP Advertise VLAN 画面

画面に表示される項目:

項目	説明
Unit	設定するユニットを指定します。
From Port / To Port	ポートの始点 / 終点を設定します。
Action	アドバタイズ VLAN によるポートマッピングの動作を選択します。「AII」「Add」「Remove」「Replace」から選択 可能です。「AII」を選択するとすべてのアドバタイズ VLAN が使用されます。
Advertise VID List	アドバタイズ VLAN ID を入力します。

「Apply」ボタンをクリックし、設定を適用します。

### GVRP Forbidden VLAN(GVRP Forbidden VLAN 設定)

GVRP Forbidden VLAN の設定、表示を行います。

#### L2 Features > VLAN > GVRP > GVRP Forbidden VLAN の順にクリックし、以下の画面を表示します。

GVRP Forbidden VLAN	
GVRP Forbidden VLAN	
Unit From Port To Port A          Unit       From Port       To Port       A         1       eth1/0/1       eth1/0/1       A         Unit 1 Settings       A	ction     Forbidden VID List       Add     2 or 3-5
Port	Forbidden VLAN
eth1/0/1	
eth1/0/2	

図 8-23 GVRP Forbidden VLAN 画面

画面に表示される項目:

項目	説明
Unit	設定するユニットを指定します。
From Port / To Port	ポートの始点 / 終点を設定します。
Action	禁止 VLAN によるポートマッピングの動作を選択します。「All」「Add」「Remove」「Replace」から選択可能です。「All」 を選択するとすべての禁止 VLAN が使用されます。
Forbidden VID List	禁止 VLAN ID を入力します。

「Apply」ボタンをクリックし、設定を適用します。

### GVRP Statistics Table (GVRP 統計テーブル)

GVRP の統計情報を表示します。

### L2 Features > VLAN > GVRP > GVRP Statistics Table の順にクリックし、以下の画面を表示します。

GVRP Statistic	s Tabl	e	_		_	_	_
GVRP Statistics T	able						
Unit 1	~	Port e	eth1/0/1 🔽		5	Find Show All	Clear Clear All
Unit 1 Settings							
Port		JoinEmpty	JoinIn	LeaveEmpty	Leaveln	LeaveAll	Empty
oth 1 /0/1	RX	0	0	0	0	0	0
eth1/0/1	ΤX	0	0	0	0	0	0
oth1/0/2	RX	0	0	0	0	0	0

図 8-24 GVRP Statistics Table 画面

#### 画面に表示される項目:

項目	説明
Unit	統計情報を表示するユニットを指定します。
Port	統計情報を表示するポートを指定します。

#### エントリの検索

「Find」ボタンをクリックして、エントリを検索します。

#### エントリの削除

「Clear」ボタンをクリックして、表示されたエントリを削除します。

#### 全エントリの表示

「Show All」ボタンをクリックして、すべてのエントリを表示します。

#### 全表示エントリの削除

「Clear All」ボタンをクリックして、すべての表示エントリを削除します。

### Asymmetric VLAN (Asymmetric VLAN 設定)

共有 VLAN 学習 (SVL: Shared VLAN Learning) は Asymmetric VLAN のための第一の必要条件となる例です。通常の環境下では、VLAN 環境で通信する 1 組の装置は、同じ VLAN を使用して送受信します。しかし、Asymmetric VLAN が必要とされる場合、B に送信するために A に使用される VLAN と A に送信するために使用される VLAN の 2 つの異なる VLAN を使用することが便利です。このタイプの設定が必要とされる例は、クライアントが 異なる IP サブネットにある場合、または機密に関連する必要性があり、クライアント間のトラフィックを分ける場合です。

L2 Features > VLAN > Asymmetric VLAN の順にメニューをクリックし、以下の画面を表示します。

Asymmetric VLAN Settings	() Safeguard
Asymmetric VLAN State O Enabled  O Disabled	
	Apply

図 8-25 Asymmetric VLAN Settings 画面

「Asymmetric VLAN State」を「Enabled」(有効)または「Disabled」(無効)に設定し、「Apply」ボタンをクリックして、変更を有効にします。

# MAC VLAN (MAC VLAN 設定)

新しく MAC ベース VLAN エントリを作成し、設定済みのエントリを検索 / 編集 / 削除します。

エントリがポートに作成されると、ポートは自動的に指定した VLAN のタグなしメンバポートになります。スタティック MAC ベース VLAN のエントリがユーザに作成されると、このユーザからのトラフィックはこのポートで動作する認証機能に関わらず指定 VLAN の下で送信されます。

#### L2 Features > VLAN > MAC VLAN の順にメニューをクリックし、以下の画面を表示します。

MAC VLAN					
MAC VLAN					
MAC Address 00-84-	57-00-00-00 V	ID (1-4094)	Priority 0	~	Apply
Total Entries: 1					
MAC Ad	dress	VID	Priority	Status	
00-11-22-3	3-44-55	1	0	Active	Delete
				1/1 < < 1	> >  Go

図 8-26 MAC VLAN 画面

画面に表示される項目:

項目	説明
MAC Address	ユニキャスト MAC アドレスを入力します。
VID	VLAN ID を入力します。
Priority	プルダウンメニューを使用してタグなしパケットに割り当てる優先度(0-7)を選択します。
VID Priority	VLAN ID を入力します。 プルダウンメニューを使用してタグなしパケットに割り当てる優先度(0-7)を選択します。

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

# LL2VLAN Interface Description (L2VLAN インタフェース概要)

L2 VLAN インタフェースの概要について表示、設定を行います。

#### L2 Features > VLAN > L2VLAN Interface Description をクリックします。次の画面が表示されます。

eate L2VLAN Interface Des	cription					
2VLAN Interface	Description 64 chars		]			Apply
nd L2VLAN Interface Descr	iption					
nd L2VLAN Interface Desci 2VLAN Interface	iption					
nd L2VLAN Interface Descr 2VLAN Interface	iption				Find	Show All
ad L2VLAN Interface Descr 2VLAN Interface	iption				Find	Show All
od L2VLAN Interface Descr 2VLAN Interface otal Entries: 1 Interface	iption	Status	Administrative	Description	Find	Show All

図 8-27 L2VLAN Interface Description 画面

画面に表示される項目:

項目	説明
L2VLAN Interface	L2 VLAN インタフェースの ID を指定します。
Description	L2 VLAN インタフェースの概要を入力します。

「Apply」をクリックし、設定内容を適用します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Show All」をクリックして、すべてのエントリを表示します。

「Delete Description」をクリックすると指定の L2 VLAN の概要を削除します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

# Subnet VLAN(サブネット VLAN)

サブネット VLAN エントリは IP サブネットベースの VLAN クラシフィケーションルールです。ポートにタグなしまたはプライオリティタグを持つ IP パケットを受信すると、送信元 IP アドレスがサブネット VLAN エントリへの照合のために使用されます。エントリのサブネットに送信元 IP があると、 パケットはこのサブネットのために定義された VLAN に分類されます。

サブネット VLAN のパラメータを設定します。

L2 Features > VLAN > Subnet VLAN の順にメニューをクリックし、以下の画面を表示します。

Subnet VLAN				
Subnet VLAN				
OIPv4 Network Prefix/Prefix Length VID (1-4094)	20.0.1.0/8	OIPv6 Network Prefix/Prefix Length Priority	8FFE::/64	Apply
Total Entries: 1				
Subnet		VID	Priority	
10.0.0/8		1	0	Delete
			1/1 < < 1 >	Go

図 8-28 Subnet VLAN 画面

#### 画面に表示される項目:

項目	説明
IPv4 Network Prefix / Prefix Length	使用する IPv4 アドレスとプレフィクス長を入力します。
IPv6 Network Prefix / Prefix Length	使用する IPv6 アドレスとプレフィクス長を入力します。
VID	VID 値のリストを入力します。
Priority	優先値を指定します。0-7 の範囲で指定できます。値が高い方が優先度が高くなります。

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

# Super VLAN(Super VLAN 設定)(EI/MI モードのみ)

Super VLAN は、同じ IP サブネットにある複数のサブ VLAN を集約するために使用されます。サブ VLAN は L2 の独立したブロードキャストドメイン です。Super VLAN はホストがサブ VLAN にある物理メンバポートを持つことができません。一度、IP インタフェースが Super VLAN に割り当てられ ると、プロキシ ARP はサブ VLAN 間の通信のためにインタフェースで自動的に有効にされます。IP インタフェースが Super VLAN に割り当てられると、 他の VLAN に割り当てられることはできなくなります。Super VLAN は他の Super VLAN のサブ VLAN となることはできません。



Private VLAN と Super VLAN は相互排他機能です。Private VLAN は Super VLAN として設定できません。 L3 ルートプロトコル、マルチキャストプロトコルは Super VLAN インタフェースで動作できません。

L2 Features > VLAN > Super VLAN の順にメニューをクリックして以下の画面を表示します。

Super VLAN		_			_
Add Super VLAN					
Super VID List	3 or 2-5				Apply
Add Sub VLAN					
Super VID (1-4094)		Sub VID List	3 or 2-5		Apply
Find Super VLAN					
Super VID (1-4094)				Find	Show All
Total Entries: 1					
SuperVLAN ID	SubVLAN ID		SubVLAN Status		
2	3	Delete	Inactive	IP Range List	Delete
				1/1 < < 1	> >  Go

図 8-29 Super VLAN Settings 画面

画面に表示される項目:

項目	説明		
	Add Super VLAN		
Super VID List	作成する Super VLAN の VLAN を入力します。		
	Add Sub VLAN		
Super VID	サブ VLAN に関連する Super VLAN の VLAN ID(1 - 4094)を入力します。		
Sub VID List	Super VLAN のサブ VLAN を入力します。		
	Find Super VLAN		
Super VID	表示する Super VLAN の VLAN ID(1 - 4094)を入力します。		

-「Delete」をクリックすると指定のエントリを削除します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Show All」をクリックして、すべてのエントリを表示します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「IP Range List」をクリックするとサブ VLAN に IP 範囲を指定することができます。

# ■ サブ VLAN の IP 範囲を設定

「IP Range List」リンクをクリックすると、以下の画面が表示されます。

Sub VLAN	
Sub VLAN	
Sub VLAN	3
Action	Add
<ul> <li>Start IP Address</li> </ul>	
End IP Address	
<ul> <li>Start IPv6 Address</li> </ul>	2013::1
End IPv6 Address	2013::1 Back Apply
Total Entries: 1	
NO.	SubVLAN IP Address Range
1	192.168.70.20-192.168.70.24

図 8-30 Sub VLAN Settings - IP Range List 画面

画面に表示される項目:

説明
サブ VLAN の指定 IP アドレスを追加(Add)または削除(Remove)します。
開始IPアドレスを入力します。
終了IPアドレスを入力します。
開始 IPv6 アドレスを入力します。
終了 IPv6 アドレスを入力します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。 「Back」をボタンをクリックして前のページに戻ります。

# Auto Surveillance VLAN (自動サーベイランス VLAN)

自動サーベイランス VLAN は、IP サーベイランスサービスを強化するための機能です。音声 VLAN と同様、D-Link IP カメラからのビデオトラフィックに対して自動的に VLAN をアサインします。優先度が高いこと、また個別の VLAN を使用することで、サーベイトラフィックの品質とセキュリティを保証します。

Auto Surveillance Properties (自動サーベイランスプロパティ)

L2 Features > VLAN > Auto Surveillance VLAN > Auto Surveillance Properties の順にクリックし、次の画面を表示します。

Auto Surveillance Propert	ies	
Global Settings		
Surveillance VLAN	Enabled Disabled	
Surveillance VLAN ID (2-4094)		
Surveillance VLAN CoS	5 🗸	
Aging Time (1-65535)	720 min	
		Apply
Port Settings		
Unit From Port	To Port State	
1 V eth1/0/1 V	eth1/0/1 V Disabled V	Apply
Unit 1 Settings		
	Port	State
	eth1/0/1	Disabled

図 8-31 Auto Surveillance Properties 画面

#### 画面に表示される項目:

項目	説明			
Grobal Settings				
Surveillance VLAN	サーベイランス VLAN を「Enabled」(有効)/「Disabled」(無効)に設定します。			
Surveillance VLAN ID	サーベイランス VLAN の VLAN ID を指定します。2 から 4094 で指定できます。			
Surveillance VLAN CoS	サーベイランス VLAN の優先値を指定します。0 から 7 で指定できます。			
Aging Time	エージングタイム (1-65535 分) を設定します。初期値は 720 (分) です。 エージングタイムは、ポートがオートサーベイランス VLAN メンバである場合にサーベイランス VLAN からポート を削除するために使用されます。最後のサーベイランスデバイスが、トラフィックの送信を止めて、このサーベ イランスデバイスの MAC アドレスがエージングタイムに到達すると、サーベイランス VLAN エージングタイマが 開始されます。ポートはサーベイランス VLAN のエージングタイム経過後にサーベイランス VLAN から削除され ます。サーベイランストラフィックがエージングタイム内に再開すると、エージングタイマはキャンセルされます。			
	Port Settings			
Unit	設定するユニットを選択します。			
From Port / To Port	設定するポート範囲を指定します。			
State	指定したポートでサーベイランス VLAN を「Enabled」(有効)/「Disabled」(無効)にします。 サーベイランス VLAN が有効な場合、ポートはアンタグのサーベイランス VLAN メンバとして自動的に学習され、 受信したアンタグのサーベイランスパケットはサーベイランス VLAN に転送されます。受信したパケットの送信 元 MAC アドレスが OUI(Organizationally Unique Identifier)アドレスに一致している場合、そのパケットはサー ベイランスパケットとして認識されます。			

「Apply」ボタンをクリックし、設定を適用します。

# MAC Settings and Surveillance Device(MAC 設定 & サーベイランスデバイス設定)

ユーザ定義のサーベイランストラフィックの OUI を設定します。

L2 Features > VLAN > Auto Surveillance VLAN > MAC Settings and Surveillance Device の順にメニューをクリックして以下の画面を表示します。

MAC Settin	ngs and Surveillan	ce Device				
User-defin	ed MAC Settings	Auto Surveillance VLAN Summ	nary			
To add more d	device(s) for Auto Surveilla	ance VLAN by user-defined confi	guration as below.			
Component Ty	ype Video Mana	agement Server 🔽	Description	32 chars		
MAC Address	00-01-02-03-	00-00	Mask			Apply
Total Entries:	: 4					
ID	Component Type	Descri	ption	MAC Address	Mask	
1	D-Link Device	IP Survei	llance	28-10-7B-00-00-00	FF-FF-FF-E0-00-00	Delete
2	D-Link Device	IP Survei	llance	28-10-7B-20-00-00	FF-FF-FF-F0-00-00	Delete
	O Link Davies	ID Oursel	10000	DD 05 54 00 00 00		0.11
3	D-LINK Device	IP Survei	lance	B0-C5-54-00-00-00	FF-FF-FF-80-00-00	Delete

図 8-32 User -defined MAC Settings タブ画面

#### 画面に表示される項目:

項目	説明
Component Type	プルダウンメニューを使用して、サーベイランス VLAN が自動検出可能なサーベイランスコンポーネントを選択します。 選択可能項目は次の通りです。: [Video Management Server」 [VMS Client/Remote Viewer」 [Video Encoder」 [Network
	Storage」「Other IP Surveillance Device」
Description	ユーザ定義 OUI に関する説明を入力します。(最大 32 文字)
MAC Address	ユーザ定義の OUI MAC アドレスを入力します。
Mask	ユーザ定義 OUI MAC アドレスマスクを入力します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

#### エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

### 自動サーベイランス VLAN サマリの表示

「Auto Surveillance VLAN Summary」タブをクリックして、以下の画面を表示します。

MAC Settings and Surveillance Device					
User-defined MAC Settings Auto Surveillance VLAN Summary					
Unit 1	]				
Total Entries: 0					
Port	Component Type	Description	MAC Address	Start Time	

図 8-33 Auto Surveillance VLAN Summary タブ画面

#### 画面に表示される項目:

項目	説明
Unit	表示するユニットを選択します。
## Voice VLAN (音声 VLAN)

## Voice VLAN Global(音声 VLAN グローバル設定)

音声 VLAN は、IP 電話からの音声トラフィックを送信するのに使用される VLAN です。不規則にデータを送信すると IP 電話の音の品質を低下させる ため、音声トラフィックの QoS (Quality of Service)が音声パケットの伝送優先度を通常のトラフィックより確実に高くなるように設定する必要が あります。

スイッチは、送信元 MAC アドレスをチェックすることで受信パケットが音声パケットであるかどうか判断します。パケットの送信元 MAC アドレス がシステムによって定義される OUI (Organizationally Unique Identifier: 組織で一意な識別子) アドレスを受諾すると、パケットは音声パケットとし て判断されて、音声 VLAN に送信されます。

音声 VLAN をグロバールに有効 / 無効にします。

L2 Features > VLAN > Voice VLAN > Voice VLAN Global の順にメニューをクリックし、以下の画面を表示します。

Voice VLAN Global		
Voice VLAN Global Voice VLAN State	OEnabled  OEnabled	
VOICE VLAIN ID (2-4054)		Apply
Voice VLAN CoS Aging Time (1-65535)	5 V 720 min	Apply

図 8-34 Voice VLAN Global Settings 画面

画面に表示される項目:

項目	説明
Voice VLAN State	プルダウンメニューを使用して、本機能を「Enabled」(有効)/「Disabled」(無効)にします。
Voice VID (2-4094)	選択をして音声 VLAN の VLAN ID を入力します。
Voice VLAN CoS	プルダウンメニューを使用して音声 VLAN の優先度を設定します。音声 VLAN 優先度はデータトラフィック中の音声トラ
	フィックの QoS を判別する上で使用されます。範囲は 0-7 の間で設定できます。初期値は 5 です。
Aging Time (1-65535)	ポートが自動 VLAN の一部の場合、音声 VLAN からポートを削除するまでの時間を設定します。最新の音声機器がトラフィックを送信したくたり、 辛吉機器の MAC アドレスが期間切ねにたる トー辛吉 VLAN タイプは開始されます。ポート
	は音声 VLAN タイマの時間切れのあと、音声 VLAN から削除されます。初期値は 720 分です。

#### 音声 VLAN の有効化

「Voice VLAN State」を「Enabled」にして音声 VLAN を有効にする VLAN を「Voice VLAN Name」または「Voice VID」で指定後、「Apply」ボタンをクリッ クします。

#### 音声 VLAN のパラメータ設定

音声 VLAN の有効後、「Priority」、「Aging Time」または「Log State」を設定後、「Apply」ボタンをクリックします。

## Voice VLAN Port(音声 VLAN のポート設定)

ポートの音声 VLAN 情報を表示します。

#### L2 Features > VLAN > Voice VLAN > Voice VLAN Port の順にメニューをクリックし、以下の画面を表示します。

Voice VLAN Port				
Voice VLAN Port				
Unit From Port	To Port eth1/0/1	State Disabled 🔽	Mode Auto Untagged	Apply
Port	State		Mode	
eth1/0/1	Disabled		Auto/Unta	ig
eth1/0/2	Disabled		Auto/Unta	ag
eth1/0/3	Disabled		Auto/Unta	ag
eth1/0/4	Disabled		Auto/Unta	g

図 8-35 Voice VLAN Port 画面

画面に表示される項目:

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	設定するポート範囲を選択します。
State	指定ポートの音声 VLAN 機能を「Enabled」(有効)/「Disabled」(無効)に設定します。 音声 VLAN が有効になると、受信した音声パケットは音声 VLAN として送信されます。受信した音声 VLAN パケットの送 信元 MAC アドレスが OUI アドレスに一致すると、音声 VLAN と認識されます。
Mode	モードを選択します。 • Auto Untagged - タグなしの音声 VLAN が自動的に学習されます。 • Auto Tagged - タグ付きの音声 VLAN タメンバシップが自動的に学習されます。 • Manual - 音声 VLAN メンバシップを手動で設定します。
	指定ポートで自動学習が有効化されている場合、音声 VLAN メンバは自動的に学習され、エージアウトします。 「Auto Tagged」モードにおいて、デバイスの OUI により音声デバイスがキャプチャされた場合、タグ付きメンバとして 音声 VLAN に自動的に参加します。音声デバイスにより送信されたタグ付きパケットの優先度は変更されます。タグなし パケットは Port VLAN ID (PVID) で転送されます。
	「Auto Untagged」モートにおいて、デバイスのOULにより音声デバイスかキャプチャされた場合、ダクなしメンバとし て音声 VLAN に自動的に参加します。音声デバイスにより送信されたタグ付きパケットお優先度は変更されます。タグな しパケットは音声 VLAN で転送されます。 スイッチが LLDP-MED パケットを受信した場合、VLAN ID、Tagged フラグ、優先度フラグがチェックされます。スイッ
	チは Tagged フラグ、優先度フラグに従います。

「Apply」ボタンをクリックして行った変更を適用します。

## Voice VLAN OUI (音声 VLAN OUI 設定)

ユーザ定義の音声トラフィックの OUI を設定します。

OUI は音声トラフィックを識別するために使用されます。多くの定義済み OUI があり、必要に応じて、さらにユーザ定義の OUI を設定できます。 ユーザ定義 OUI は定義済みの OUI と同じとすることはできません。

L2 Features > VLAN > Voice VLAN > Voice VLAN OUI の順にメニューをクリックし、以下の画面を表示します。

/oice VLAN OUI			_
Voice VLAN OUI			
OUI Address	Mask	Description	Annly
Total Entries: 7			
OUI Address	Mask	Description	
00-01-E3-00-00-00	FF-FF-FF-00-00-00	Siemens	Delete
00-03-6B-00-00-00	FF-FF-FF-00-00-00	Cisco	Delete
00-09-6E-00-00-00	FF-FF-FF-00-00-00	Avaya	Delete
00-0F-E2-00-00-00	FF-FF-FF-00-00-00	Huawei&3COM	Delete
00-60-B9-00-00-00	FF-FF-FF-00-00-00	NEC&Philips	Delete
00-D0-1E-00-00-00	FF-FF-FF-00-00-00	Pingtel	Delete

図 8-36 Voice VLAN OUI 画面

画面に表示される項目:

項目	説明
OUI Address	ユーザ定義の OUI MAC アドレスを入力します。
Mask	ユーザ定義 OUI MAC アドレスマスクを入力します。
Description	ユーザ定義 OUI に関する説明文を入力します。

「Apply」ボタンをクリックして行った変更を適用します。

## エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

## Voice VLAN Device(音声 VLAN デバイス)

ポートに接続する音声デバイスを表示します。開始時刻はデバイスがこのポートで検出される時間です。また、アクティベート時間はデバイスが一 番最近トラフィックを送信した時間です。

L2 Features > VLAN > Voice VLAN > Voice VLAN Device の順にメニューをクリックし、以下の画面を表示します。

Voice VLAN Device			O Safeguard
Unit 1			
Total Entries: 0			
Port	Voice Device	Start Time	Last Active Time

図 8-37 Voice VLAN Device 画面

画面に表示される項目:

項目	説明
Unit	表示するユニットを選択します。

#### Voice VLAN LLDP-MED Device(音声 VLAN LLDP-MED 音声デバイス)

スイッチに接続する音声 VLAN LLDP-MED 音声デバイスを表示します。

L2 Features > VLAN > Voice VLAN > Voice VLAN LLDP-MED Device の順にメニューをクリックして以下の画面を表示します。

N	/oice \	/LAN	LLDP-MED Device	_	_	_	_		
Г	Voice VI	LAN LLC	DP-MED Device Table						
	Total E	ntries: 0	)						
	Index	Port	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	Create Time	Remain Time (sec)	

図 8-38 Voice VLAN LLDP-MED Voice Device 画面

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

# Private VLAN (プライベート VLAN 設定)

プライベート VLAN のパラメータを設定します。

L2 Features > VLAN > Private VLAN の順にメニューをクリックし、以下の画面を表示します。

	LAN									
ID List		State		Туре						
or 2-5		Disabled		Community 🗸						Apply
rivate Vl	LAN Assoc	iation								
ID List		Action		Secondary VID List						
or 2-5		Add	~	3 or 2-5						Apply
1 🔽	eth1/0/1	~	eth1/0/1	▼ Trunk				Remove Associa	ation	Apply
rivate Vl	LAN Mappi	ng								
	From Port		To Port		Primary VID	Action	Se	condary VID List		
Init	ath 1/0/1	~	eth1/0/1	Trunk		Add	✓ 3 (	or 2-5	Remove I	Mapping
1 🔽	eurivovi									

図 8-39 Private VLAN 画面

画面に表示される項目:

項目	説明
	Private VLAN
VID List	VLAN ID のリストを指定します。
State	プライベート VLAN の「Enabled」(有効)/「Disabled」(無効)を指定します。
Туре	プライベート VLAN のタイプを指定します。「Community」「Isolated」「Primary」から指定します。
	Private VLAN Association
VID List	VLAN ID のリストを指定します。
Action	プライベート VLAN の動作を指定します。「Add」「Remove」「Disabled」から指定します。
Secondary VID List	セカンダリ VLAN ID のリストを入力します。
	Private VLAN Host Association
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。「Trunk」オプションをチェックすると本設定にトランクポートを指定します。
Primary VID	プライマリ VLAN ID を入力します。
Secondary VID	セカンダリVLAN IDを入力します。「Remove Association」にチェックを入れると本コンフィグレーションは有効になりません。
	Private VLAN Mapping
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。「Trunk」オプションをチェックすると本設定にトランクポートを指定します。
Primary VID	プライマリ VLAN ID を入力します。
Action	「Add」- 入力した情報に基づきエントリを追加します。
	「Remove」- 入力した情報を削除します。
Secondary VID	セカンダリ VLAN ID を入力します。「Remove Mapping」にチェックを入れると本コンフィグレーションは有効になりません。
$\lceil A n n   v   t + f + f + v + f  $	記字由のた海田」ます

「Apply」をクリックし、設定内容を適用します。

# VLAN Tunnel (VLAN トンネル)

## L2 Features > VLAN Tunnel

VLAN トンネルの設定を行います。

# Dot1q Tunnel (Dot1q トンネル)

本項目では「802.1Q VLAN」トンネルの設定、表示を行います。802.1Q トンネルポートはサービス VLAN においての「User Network Interface」(UNI) ポートとして動作します。サービス VLAN のタグ付きメンバであるトランクポートは、サービス VLAN の「Network Node Interface」(NNI) ポートと して動作します。

プロバイダブリッジネットワークに接続するポートの、802.1Q トンネリングイーサネットタイプのみを設定すると、サービス VLAN のタグ付きフレームを送受信します。トンネルイーサネットタイプが設定されると、指定の値は選択ポートの送信フレームの出力 VLAN タグ「Tag Protocol ID」(TPID) に指定されます。指定 TPID は当該ポートの受信フレームのサービス VLAN タグの識別に使用されます。

L2 Features > VLAN Tunnel > Dot1q Tunnel の順にメニューをクリックし、以下の画面を表示します。

Dorig lunnel Settings	
TPID Settings Dot1q Tunnel Po Inner TPID (0x1-0xfff) 0x 8100	Apply
Unit         From Port         To Port           1         eth1/0/1         eth1/0/1	Outer TPID (0x1-0xfff) Ox 3100 Apply
Unit 1 Settings	
Unit 1 Settings Port	Outer TPID
Unit 1 Settings Port eth1/0/1	Outer TPID 0x8100
Unit 1 Settings Port eth1/0/1 eth1/0/2	Outer TPID 0x8100 0x8100
Unit 1 Settings  Port  eth1/0/1  eth1/0/2  eth1/0/3	Outer TPID           0x8100           0x8100           0x8100           0x8100
Unit 1 Settings Port eth1/0/1 eth1/0/2 eth1/0/3 eth1/0/4	Outer TPID           0x8100           0x8100           0x8100           0x8100           0x8100           0x8100

図 8-40 Dot1g Tunnel (TPID Settings) 画面

#### 画面に表示される項目:

項目	説明
Inner TPID	インナーTPID値を指定します。16進数方式です。「0x1」から「0xFFFF」の間で指定します。インナーTPIDはイングレスパケッ
	トが「C タグ付き」であるかを指定します。このインナー TPID は各システムで設定されます。
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。
Outer TPID	アウター TPID 値を指定します。16 進数方式です。「0x1」から「0xFFFF」の間で指定します。

「Apply」ボタンをクリックして行った変更を適用します。

#### Dot1q Tunnel Port Settings タブをクリックすると以下の画面が表示されます。

Dot1q Tun	nel	_	_			
TP	ID Settings	Dot1q	Funnel Port Setting	js		
Unit	From Port eth1/0/1	To Port eth1/0/1	Trust Inner Priori	ty Miss Drop Disabled	Insert Dot1q Tag (1-4094)	Apply
Unit	From Port eth1/0/1	To Port eth1/0/1	VLAN Mapping F (1-1000)	Profile Action		Apply
Unit 1 Setting	js					
Port	Trust Inn	er Priority	Miss Drop	Insert Dot1q Tag	VLAN M	apping Profiles
eth1/0/1	Disa	abled	Disabled			
eth1/0/2	Disa	abled	Disabled			

図 8-41 Dot1q Tunnel (Dot1q Tunnel Port Settings) 画面

以下の項目を使用して設定します。

項目	説明
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。
Trust Inner Priority	「802.1Q Inner Trust Priority」を「Enabled」(有効)/「Disabled」(無効)に指定します。802.1Q トンネルポートでトラス トプライオリティオプションが有効な場合、受信パケットの VLAN タグの優先値はサービス VLAN タグにコピーされます。
Miss Drop	「Miss Drop」を「Enabled」(有効)/「Disabled」(無効)に指定します。受信ポートで VLAN マッピング Miss Drop オプショ ンが有効な場合、受信パケット VLAN は VLAN マッピングエントリやポートのルールとマッチしなくなり、パケットは破 棄されます。
Insert Dot1q Tag	802.1Q トンネルポートに受信したタグなしパケットに挿入される 802.1Q VLAN ID を 1 から 4094 の間で指定します。
VLAN Mapping Profile	VLAN マッピングプロファイル ID(1-1000)を指定します。値が低い方が優先度が高くなります。
Action	「Add」- 入力した情報に基づきエントリを追加します。 「Remove」- 入力した情報を削除します。

「Apply」ボタンをクリックして行った変更を適用します。

# VLAN Mapping (VLAN マッピング)

本項目では VLAN マッピングの設定、表示を行います。インタフェースにプロファイルが適用されると、スイッチはプロファイルルールに従い受信 パケットを照合します。パケットがルールに合致したことを確認すると、ルールに設定された操作が実行されます。この操作は「送信 VID」の追加 や削除、新しい送信タグの優先値設定、またはパケットの新しい入力 VID の設定などがあります。

この照合はプロファイル内にあるルールのシーケンス番号に依存しており、最初の操作が合致すると照合は停止します。シーケンス番号が設定され ていない場合、自動的に付与されます。シーケンス番号は、10から始まり10単位で設定されます。複数のタイプのプロファイルが一つのインタフェー スに設定可能です。

L2 Features > VLAN Tunnel > VLAN Mapping の順にメニューをクリックし、以下の画面を表示します。

1 v ID (1-4094) Init 1 v	eth1/0/1  Inner VID (1-4094) Port eth1/0/1	eth1/0/1 v Priority 0 v	3 or 2-5 Egress Priority Copy		Translate 💌	Apply Find
otal Entries: 1						
Port	Original V	LAN	Translated VLAN	Priority	Status	

図 8-42 VLAN Mapping 画面

画面に表示される項目:

項目	説明		
Unit	設定を行うユニットを指定します。		
From Port / To Port			
Port	検索するポートを指定します。		
Original VID List	オリジナルの VID リスト(1-4094)を指定します。		
Original Inner VID	オリジナルのインナー VID(1-4094)を指定します。		
Action	実行する動作を指定します。「Translate」「Dot1q-tunnel」から指定します。 ・「Translate」- マッチしたパケットの出力 VID と交換する VID を指定します。 ・「Dot1q-tunnel」- マッチしたパケットに出力 VID を追加します。		
VID	VLAN ID(1-4094)を指定します。		
Inner VID	インナー VLAN ID(1-4094)を指定します。		
Priority	優先値を指定します。0-7 の範囲で指定できます。値が高い方が優先度が高くなります。		
Egress Priority	<ul> <li>VLAN トンネルインタフェースのイーグレス C タグ (C-tag) 優先値を指定します。次の項目から選択します。</li> <li>Copy - サービス VLAN 優先値のコピーを使用します。</li> <li>0 to 7 - イーグレス C-tag 優先値を 0-7 の範囲で指定します。</li> </ul>		

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

## VLAN Mapping Profile (VLAN マッピングプロファイル)

本項目では VLAN マッピングプロファイルの設定、表示を行います。

L2 Features > VLAN Tunnel > VLAN Mapping Profile の順にメニューをクリックし、以下の画面を表示します。

/LAN Mapping	Profile			
VLAN Mapping Pro	ofile			
Profile ID (1-1000)		Type Ethernet	~	Add Profile
Profile ID (1-1000)				Find
Total Entries: 1				
	Profile ID	Туре		
1		Ethernet		Add Rule Delete
			1	/1 << 1 >>
Profile 1 Rules				
Rule ID	Match	Action	802.1P Priority	New Inner VID
2	inner-vid: 1 ether-t	dot1q-tunnel outer-v	0	1 Delete
			1/	M  < < 1 > >  G

図 8-43 VLAN Mapping Profile 画面

画面に表示される項目:

項目	説明
Profile ID	VLAN マッピングプロファイルの ID を入力します。1-1000 の範囲で指定できます。値が低い方が優先度が高くなります。
Туре	プロファイルタイプを「Ethernet」「IP」「IPv6」「Ethernet-IP」から指定します。
	・ Ethernet - L2 項目にマッチするプロファイルを指定します。
	・ IP - L3 IP 項目にマッチするプロファイルを指定します。
	・ IPv6 - IPv6 宛先 / 送信元アドレスにマッチするプロファイルを指定します。
	・ Ethernet-IP - L2/L3 IP 項目にマッチするプロファイルを指定します。

「Add Profile」をクリックし、新しい VLAN マッピングプロファイルを追加します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Add Rule」をクリックし、新しいルールを追加します。

「Delete」をクリックすると指定のエントリを削除します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

### Add VLAN Mapping Rule(Ethernet)(VLAN マッピングルールの追加 /Ethernet)

「VLAN Mapping Profile」の Type で「Ethernet」を選択、Add Rule をクリックし、新しいルールを追加します。

Add VLAN Mapping R	ule		
VLAN Mapping Rule			
Profile ID	1		
Туре	Ethernet		
Rule ID (1-10000)	2		
Src-MAC Address	00-84-57-00-00-00		
Dst-MAC Address	00-84-57-00-00-00		
Priority	None 🗸		
Inner VID (1-4094)			
Ethernet Type (0x0-0xffff)	<b>0</b> ×0800		
Action	Dot1q-Tunnel 🗸	(1-4094)	
802.1P Priority	None 🗸		
New Inner VID (1-4094)			Back Apply

図 8-44 Add VLAN Mapping Rule (Ethernet) 画面

# 第8章 L2 Features (L2機能の設定)

## 以下の項目を使用して設定します。

項目	説明
Rule ID	VLAN マッピングルール ID を入力します。指定されていない場合、ルール ID は 10 から始まり新しいルールごとに 10 ず
	つ増えていきます。1 から 10000 の間で指定可能です。
Src-MAC Address	送信元 MAC アドレスを指定します。
Dst-MAC Address	宛先 MAC アドレスを指定します。
Priority	802.1p 優先値を指定します。0-7 の範囲で指定できます。値が高い方が優先度が高くなります。
Inner VID	インナー VLAN ID(1-4094)を指定します。
Ethernet Type	イーサネットタイプを指定します。「0x0」から「0xFFFF」の間で指定可能です。
Action	実行する動作を指定します。「Translate」「Dot1q-tunnel」から指定します。
	・「Translate」- マッチしたパケットの出力 VID と交換する VID を指定します。
	・「Dot1q-tunnel」- マッチしたパケットに出力 VID を追加します。
New Outer VID	新しいアウター VLAN ID(1-4094)を指定します。
802.1P Priority	802.1p 優先値を指定します。0-7 の範囲で指定できます。値が高い方が優先度が高くなります。
New Inner VID	「Dot1q-tunnel」を選択後、新しいインナー VLAN ID(1-4094)を指定します。「Dot1q-tunnel」を選択時のみ指定可能です。
	と並のページに互います

「Back」をクリックすると前のページに戻ります。 「Apply」をクリックし、設定内容を適用します。

## Add VLAN Mapping Rule(IP)(VLAN マッピングルールの追加 /IP)

「VLAN Mapping Profile」の Type で「IP」を選択、Add Rule をクリックし、新しいルールを追加します。



図 8-45 Add VLAN Mapping Rule (IP) 画面

### 画面に表示される項目:

項目	説明
Rule ID	VLAN マッピングルール ID を入力します。指定されていない場合、ルール ID は 10 から始まり新しいルールごとに 10 ず
	つ増えていきます。1 から 10000 の間で指定可能です。
Src-IP Address	送信元 IP アドレスとサブネットマスクを指定します。
(IP/Mask)	
Dst-IP Address	宛先 IP アドレスとサブネットマスクを指定します。
(IP/Mask)	
DSCP	DSCP 値を指定します。0-63 の範囲で指定できます。
Source / Destination	送信元 / 宛先 TCP/UDP ポート(1 - 65535)を指定します。
Port	
IP Protocol	L3 IP プロトコル値(0-255)を指定します。
Action	実行する動作を指定します。「Translate」「Dot1q-tunnel」から指定します。
	・「Translate」- マッチしたパケットの出力 VID と交換する VID を指定します。
	・「Dot1q-tunnel」- マッチしたパケットに出力 VID を追加します。
New Outer VID	新しいアウター VLAN ID(1-4094)を指定します。
802.1P Priority	802.1p 優先値を指定します。0-7 の範囲で指定できます。値が高い方が優先度が高くなります。
New Inner VID	「Dot1q-tunnel」を選択後、新しいインナー VLAN ID(1-4094)を指定します。「Dot1q-tunnel」を選択時のみ指定可能です。
「Back」をクリックするよ	と前のページに戻ります。

「Apply」をクリックし、設定内容を適用します。

## Add VLAN Mapping Rule(IPv6)(VLAN マッピングルールの追加 /IPv6)

「VLAN Mapping Profile」の Type で「IPv6」を選択、Add Rule をクリックし、新しいルールを追加します。

Add VLAN Mapping Ru	le		
VLAN Mapping Rule			
Profile ID	3		
Туре	IPv6		
Rule ID (1-10000)	2		
Src-IPv6 Address	2013::1/16		
Dst-IPv6 Address	3333::1/8		
Action	Dot1q-Tunnel 🔽	(1-4094)	
802.1P Priority	None 🗸		
New Inner VID (1-4094)			Back Apply

図 8-46 Add VLAN Mapping Rule (IPv6) 画面

## 画面に表示される項目:

項目	説明
Rule ID	VLAN マッピングルール ID を入力します。指定されていない場合、ルール ID は 10 から始まり新しいルールごとに 10 ず
	つ増えていきます。1 から 10000 の間で指定可能です。
Src-IPv6 Address	送信元 IPv6 アドレスとプリフィクス長を指定します。
Dst-IPv6 Address	宛先 IPv6 アドレスとプリフィクス長を指定します。
Action	実行する動作を指定します。「Translate」「Dot1q-tunnel」から指定します。
	・「Translate」- マッチしたパケットの出力 VID と交換する VID を指定します。
	・「Dot1q-tunnel」- マッチしたパケットに出力 VID を追加します。
New Outer VID	新しいアウター VLAN ID(1-4094)を指定します。
802.1P Priority	802.1p 優先値を指定します。0-7 の範囲で指定できます。値が高い方が優先度が高くなります。
New Inner VID	「Dot1q-tunnel」を選択後、新しいインナー VLAN ID(1-4094)を指定します。「Dot1q-tunnel」を選択時のみ指定可能です。
「Back」をクリックすると	≤前のページに戻ります。

「Apply」をクリックし、設定内容を適用します。

# Add VLAN Mapping Rule(Ethernet-IP)(VLAN マッピングルールの追加 /Ethernet-IP)

「VLAN Mapping Profile」の Type で「Ethernet-IP」を選択、Add Rule をクリックし、新しいルールを追加します。

Add VLAN Mapping R	Rule
VLAN Mapping Rule	
Profile ID	4
Туре	Ethernet-IP
Rule ID (1-10000)	2
Src-MAC Address	00-84-57-00-00
Dst-MAC Address	00-84-57-00-00
Priority	None
Inner VID (1-4094)	
Ethernet Type (0x0-0xffff)	0x 0800
Src-IP Address (IP/Mask)	
Dst-IP Address (IP/Mask)	
DSCP (0-63)	21
Source Port (1-65535)	65535
Destination Port (1-65535)	65535
IP Protocol (0-255)	1
Action	Dot1q-Tunnel 🔽 (1-4094)
802.1P Priority	None
New Inner VID (1-4094)	Back Apply

図 8-47 Add VLAN Mapping Rule (Ethernet-IP) 画面

画面に表示される項目:

項目	説明
Rule ID	VLAN マッピングルール ID を入力します。指定されていない場合、ルール ID は 10 から始まり新しいルールごとに 10 ず つ増えていきます。1 から 10000 の間で指定可能です。
Src-MAC Address	送信元 MAC アドレスを指定します。
Dst-MAC Address	宛先 MAC アドレスを指定します。
Priority	802.1p 優先値を指定します。0-7 の範囲で指定できます。値が高い方が優先度が高くなります。
Inner VID	インナー VLAN ID(1-4094)を指定します。
Ethernet Type	イーサネットタイプを指定します。「0x0」から「0xFFFF」の間で指定可能です。
Src-IP Address	送信元IPアドレスとサブネットマスクを指定します。
Dst-IP Address	宛先 IP アドレスとサブネットマスクを指定します。
DSCP	DSCP 値を指定します。0-63 の範囲で指定できます。
Source / Destination Port	送信元 / 宛先 TCP/UDP ポート(1 - 65535)を指定します。
IP Protocol	L3 IP プロトコル値(0-255)を指定します。
Action	実行する動作を指定します。「Translate」「Dot1q-tunnel」から指定します。 ・「Translate」- マッチしたパケットの出力 VID と交換する VID を指定します。 ・「Dot1q-tunnel」- マッチしたパケットに出力 VID を追加します。
New Outer VID	新しいアウター VLAN ID(1-4094)を指定します。
802.1P Priority	802.1p 優先値を指定します。0-7 の範囲で指定できます。値が高い方が優先度が高くなります。
New Inner VID	「Dot1q-tunnel」を選択後、新しいインナー VLAN ID(1-4094)を指定します。「Dot1q-tunnel」を選択時のみ指定可能です。

「Back」をクリックすると前のページに戻ります。

「Apply」をクリックし、設定内容を適用します。

# STP(スパニングツリー設定)

#### L2 Features > STP

本スイッチは 3 つのバージョンのスパニングツリープロトコル (IEEE 802.1D-1998 STP、IEEE 802.1D-2004 Rapid STP、および IEEE 802.1Q-2005 MSTP) をサポートしています。ネットワーク管理者の間では IEEE 802.1D-1998 STP が最も一般的なプロトコルとして認識されていますが、D-Link のマネジ メントスイッチには IEEE 802.1D-2004 RSTP と IEEE 802.1Q-2005 MSTP も導入されています。これらの技術について、以下に概要を紹介します。また、 802.1D-1998 STP、802.1D-2004 RSTP および 802.1Q-2005 MSTP の設定方法についても説明します。

## 802.1Q-2005 MSTP

MSTP (Multiple STP Protocol)は IEEE 委員会により定義された標準規格で、複数の VLAN を1つのスパニングツリーインスタンスにマッピングし、ネットワーク上に複数の経路を提供します。ロードバランシングが可能となるため、1つのインスタンスに障害が発生した場合でも、広い範囲に影響を与えないようにすることができます。障害発生時には、障害が発生したインスタンスに代わって新しいトポロジが素早く収束されます。

VLAN が指定されたフレームは、これらの3つのスパニングツリープロトコル(STP、RSTP、MSTP)のいずれかを使用し、相互接続されたブリッジ を介して素早く適切に処理されます。

MSTI ID(MST インスタンス ID)は、これらのインスタンスをクラス分けする ID です。MSTP では、複数のスパニングツリーを CIST(Common and Internal STP)で接続します。CIST は自動的に各 MSTP リージョンとその最大範囲を判定し、1 つのスパニングツリーを構成する 1 つの仮想ブリッジ のように見せかけます。そのため、VLAN が割り当てられた各フレームは、定義 VLAN の誤りや対応するスパニングツリーに関係なくシンプルで完全なフレーム処理が保持されたまま、ネットワーク上で管理用に設定されたリージョン内において異なるデータ経路を通ることができます。

ネットワーク上で MSTP を使用しているスイッチは、以下の3つの属性を持つ1つの MSTP で構成されています。

- 1. 32 文字までの半角英数字で定義された「Configuration 名」(「MST Configuration Identification」画面の「Configuration Name」で設定)。
- 2. 「Configuration Revision 番号」(「MST Configuration Identification」画面の「Revision Level」で設定)。
- 3. 4094 エレメントテーブル(「MST Configuration Identification」画面の「VID List」で設定)。スイッチがサポートする 4094 件までの VLAN とイ ンスタンスとの関連付けです。

スイッチ上で MSTP 機能を利用するためには、以下の手順を実行してください。

- 1. スイッチに MSTP 設定を行います。(「STP Bridge Global Settings」画面の「STP Version」で設定)
- 2. MSTP インスタンスに適切なスパニングツリープライオリティを設定します。(「STP Instance Settings」画面の「Priority」で設定)
- 3. 共有する VLAN を MSTP Instance ID に追加します。(「MST Configuration Identification」画面の「VID List」で設定)

### 802.1D-2004 Rapid STP

本スイッチは、IEEE 802.1Q-2005 に定義される MSTP (Multiple STP Protocol)、IEEE 802.1D-2004 に定義される RSTP (Rapid STP Protocol)、および 802.1D-1998 で定義される STP (STP Protocol)の3つのプロトコルを実装しています。RSTP は IEEE 802.1D-1998 をサポートするレガシー機器との 併用が可能ですが、その場合 RSTP を使用する利点は失われます。

RSTPは802.1D-1998 STP標準の改良型プロトコルであり、STPを使用する上での制限を克服する目的で開発されました。制限とは、特に今日イーサネットスイッチに取り入れられているレイヤ3の諸機能を妨げるものを指しています。RSTPの基本的な機能や用語の多くは STPと同じです。STP用の 設定項目の多くも RSTPで同じように使用されます。本項では、スパニングツリーの新しいコンセプトと、これらのプロトコル間の主な違いについ て説明します。

## ポートの状態遷移

3 つのプロトコル間の根本的な相違点は、ポートがどのように Forwarding 状態に遷移するかという点と、この状態遷移がトポロジ内でのポートの 役割(Forwarding/Not Forwarding)にどのように対応するかという点にあります。802.1D-1998規格で使用されていた3つの状態「Disabled」「Blocking」 「Listening」が、MSTP 及び RSTP では「Discarding」という1つの状態に統合されました。いずれの場合も、ポートはパケットの送信を行わない状態です。 STP の「Disabled」「Blocking」「Listening」であっても、RSTP/MSTP の「Discarding」であっても、ネットワークトポロジ内では「非アクティブ状態」 であり、機能の差はありません。以下の表では、3つのプロトコルにおけるポートの状態遷移の違いを示しています。

トポロジの計算については、3 つのすべてのプロトコルにおいて同様に行われます。各セグメントにはルートブリッジへのパスが1つ存在し、すべてのブリッジで BPDU パケットをリッスンします。RSTP/MSTP では、ルートブリッジから BPDU を受信しなくても BPDU パケットが Hello パケット 送信毎に送信されます。ブリッジ間の各リンクはリンクの状態を素早く検知することができるため、リンク断絶時の素早い検出とトポロジの調整が可能となります。802.1D-1998 規格では、隣接するブリッジ間においてこのような素早い状態検知が行われません。

#### ポート状態の比較

802.1Q-2005 MSTP	802.1D-2004 RSTP	802.1D-1998 STP	Forwarding	Learning
Disabled	Disabled	Disabled	不可能	不可能
Discarding	Discarding	Blocking	不可能	不可能
Discarding	Discarding	Listening	不可能	不可能
Learning	Learning	Learning	不可能	可能
Forwarding	Forwarding	Forwarding	可能	可能

RSTPでは、タイマ設定への依存がなくなり、Forwarding状態への高速な遷移が可能になりました。RSTP準拠のブリッジは、他のRSTPに準拠するブリッジリンクのフィードバックを素早く検知します。ポートはトポロジの安定を待たずに Forwarding 状態へ遷移することができます。こうした高速な状態遷移を実現するために、RSTP プロトコルでは以下の2つの新しい変数(Edge Port と P2P Port)が使用されています。

#### Edge Port

エッジポートは、ループが発生しないセグメントに直接接続しているポートに対して設定することができます。例えば、1台のワークステーション に接続しているポートがこれに該当します。エッジポートとして指定されたポートは、Listening 及び Learning の段階を経ずに、直接 Forwarding 状態に遷移します。エッジポートは BPDU パケットを受け取った時点でそのステータスを失い、通常のスパニングツリーポートに変わります。

#### P2P Port

P2P ポートにおいても高速な状態遷移が可能です。P2P ポートは他のブリッジとの接続に使用されます。RSTP と MSTP では、手動で設定の変更が行われていない限り、全二重モードで動作しているすべてのポートは P2P ポートと見なされます。

#### 802.1D-1998/802.1D-2004/802.1Q-2005の互換性

RSTP や MSTP はレガシー機器と相互運用が可能で、必要に応じて BPDU パケットを 802.1D-1998 形式に自動的に変換することができます。ただし、 802.1D-1998 STP を使用しているセグメントでは、MSTP や RSTP の利点である高速な状態遷移やトポロジ変更の検出を享受することはできません。 また、これらのプロトコルでは、セグメント上でレガシー機器の更新により RSTP や MSTP を使用する場合に必要となる変数が用意されており、マ イグレーションの際に使用されます。

### 2つのレベルで動作するスパニングツリープロトコル

- 1. スイッチレベルでは、設定はグローバルに実行されます。
- 2. ポートレベルでは、設定はポートベースのユーザ定義のグループに対して実行されます。

# STP Global Settings(STP グローバル設定)

STP をグローバルに設定します。

L2 Features > Spanning Tree > STP Global Settings の順にメニューをクリックし、以下に示す画面を表示します。

STP Global Settings		_		_		
STP State						
STP State	Disabled O Enable	led				Apply
STP Traps						
STP New Root Trap	Disabled OEnabl	led				
STP Topology Change Trap	Disabled O Enable	led				Apply
STP Mode						
STP Mode	RSTP	l				Apply
STP Priority						
Priority (0-61440)	32768	l				Apply
TP Configuration						
Bridge Max Age (6-40)	20	sec	Bridge Hello Time (1-2)	2	sec	
Bridge Forward Time (4-30)	15	sec	TX Hold Count (1-10)	6	times	
Max Hops (1-40)	20	times	NNI BPDU Address	Dot1d	~	Apply

図 8-48 STP Global Settings 画面

画面に表示される項目:

項目	説明
	STP State
STP State	STP をグローバルに「Enabled」(有効)/「Disabled」(無効)にします。
	STP Trap
STP New Root Trap	新しいルートトラップ送信の「Enabled」(有効)/「Disabled」(無効)を設定します。
STP Topology Change Trap	トポロジ変更トラップ送信の「Enabled」(有効)/「Disabled」(無効)を設定します。
	STP Mode
STP Mode	スイッチで使用する STP のバージョンをプルダウンメニューから選択します。 • STP - スイッチ上で STP がグローバルに使用されます。 • RSTP - スイッチ上で RSTP がグローバルに使用されます。
	・ MSIP - スイッテエで MSIP かクローハルに使用されます。 STD Drivity
Priority	STEPTIONLY STD 原生値を指定します。0 から 61/40 までで指定可能です。初期値は 32768 です。低い方が原生値は言いです。
	STP Configuration
Bridge Max Age (6-40)	本項目は、古い情報がネットワーク内の冗長パスをずっと循環し、新しい有効な情報の伝播を妨げるのを防ぐために 設定します。ルートブリッジによりセットされるこの値は、スイッチと他の Bridged LAN(ブリッジで相互接続され た LAN)内のデバイスが持っているスパニングツリー設定値が矛盾していないかを確認するための値です。本値が経 過した時にルートブリッジからの BPDU パケットが受信されていなければ、スイッチは自分で BPDU パケットを送信 し、ルートブリッジになる許可を得ようとします。この時点でスイッチのブリッジ識別番号が一番小さければ、スイッ チはルートブリッジになります。6-40(秒)の範囲から値を指定します。初期値では 20(秒)が指定されています。
Bridge Hello Time (1-2)	ルートブリッジは、他のスイッチに自分がルートブリッジであることを示すために BPDU パケットを送信します。本 値は、BPDU パケット送信間隔です。STP または RSTP が「STP Version」で選択された場合だけ本項目は表示されます。 MSTP に対して、Hello Time はポートごとに設定される必要があります。詳しくは「STP ポート設定」セクションを 参照してください。1-2 秒で指定します。初期値は2(秒)です。
Bridge Forward Time (4-30)	スイッチ上のすべてのポートは、Blocking 状態から Forwarding 状態に移行する間に本値で指定した時間 Listening 状 態を保ちます。4-30(秒)の範囲から指定します。初期値は 15(秒)です。
Tx Hold Count (1-10)	Hello パケットの最大送信回数を指定します。1-10 の範囲から指定します。初期値は6です。
Max Hops (1-40)	スイッチが送信した BPDU パケットが破棄される前のスパニングツリー範囲内のデバイス間のホップ数を設定します。 値が 0 に到達するまで、各スイッチは 1 つずつホップカウントを減らしていきます。スイッチは、その後 BPDU パケッ トを破棄し、ポートに保持していた情報を解放します。ホップカウントは 1-40 で指定します。初期値は 20 です。
NNI BPDU Address	NNI BPDU アドレスを指定します。「Dot1d」「Dot1ad」から指定可能です。初期値では「Dot1d」このパラメータはサービスプロバイダネットワークの STP の BPDU プロトコルアドレスの決定に使用されます。「802.1d STP アドレス」と「802.1ad サービスプロバイダ STP アドレス」が使用されます。

「Apply」ボタンをクリックし、設定を適用します。

# STP Port Settings(STP ポートの設定)

STP をポートごとに設定します。

L2 Features > STP > STP Port Settings の順にクリックし、以下の画面を表示します。

P Port Set	lings								
nit		1	~	From Port	th1/0/1 🔽	To Port	eth1/0/1		
ost (1-2000	00000, 0=Auto	o)		State E	nabled 🔽	Guard Root	Disabled 🗸		
nk Type		Auto	~	Port Fast	letwork 🔽	TCN Filter	Disabled 🗸		
PDU Forwa	ird	Disable	d 🗸	Priority 1	28 💌	Hello Time (1-2)		sec	
oop Guard		Disable	d 🗸					[	Apply
nit 1 Settin	gs								
nit 1 Settin Port	gs State	Cost	Guard Root	t Link Tyj	e Port Fast	TCN Filte	r BPDU Forward	Priority	Loop Guard
nit 1 Settin Port eth1/0/1	gs State Enabled	Cost 0/200000	Guard Root Disabled	t Link Typ Auto/P2	P Edge/Non-Edg	TCN Filte	r BPDU Forward Disabled	Priority 128	Loop Guard Disabled
nit 1 Settin Port eth1/0/1 eth1/0/2	gs State Enabled Enabled	Cost 0/200000 0/200000	Guard Root Disabled Disabled	Link Tyr Auto/P2 Auto/P2	P Edge/Non-Edg	ge Disabled	r BPDU Forward Disabled Disabled	Priority 128 128	Loop Guard Disabled Disabled
eth1/0/1 eth1/0/2 eth1/0/3	gs State Enabled Enabled Enabled	Cost 0/200000 0/200000 0/200000	Guard Root Disabled Disabled Disabled	Link Typ Auto/P2 Auto/P2 Auto/P2	Port Fast PEdge/Non-Edg PEdge/Non-Edg PEdge/Non-Edg	TCN Filte ge Disabled ge Disabled ge Disabled	r BPDU Forward Disabled Disabled Disabled	Priority 128 128 128 128	Loop Guard Disabled Disabled Disabled
nit 1 Settin Port eth1/0/1 eth1/0/2 eth1/0/3 eth1/0/4	State Enabled Enabled Enabled Enabled Enabled	Cost 0/200000 0/200000 0/200000 0/200000	Guard Root Disabled Disabled Disabled Disabled	t Link Typ Auto/P2 Auto/P2 Auto/P2 Auto/P2	P Edge/Non-Edg P Edge/Non-Edg P Edge/Non-Edg P Edge/Non-Edg P Edge/Non-Edg	TCN Filte ge Disabled ge Disabled ge Disabled ge Disabled	r BPDU Forward Disabled Disabled Disabled Disabled Disabled	Priority 128 128 128 128 128 128 128	Loop Guard Disabled Disabled Disabled Disabled
nit 1 Settin Port eth1/0/1 eth1/0/2 eth1/0/3 eth1/0/4 eth1/0/5	gs State Enabled Enabled Enabled Enabled Enabled	Cost 0/200000 0/200000 0/200000 0/200000 0/200000	Guard Root Disabled Disabled Disabled Disabled Disabled	Link Typ Auto/P2 Auto/P2 Auto/P2 Auto/P2 Auto/P2 Auto/P2	P Edge/Non-Edg P Edge/Non-Edg P Edge/Non-Edg P Edge/Non-Edg P Edge/Non-Edg P Edge/Non-Edg	TCN Filte ge Disabled ge Disabled ge Disabled ge Disabled ge Disabled	r BPDU Forward Disabled Disabled Disabled Disabled Disabled Disabled	Priority 128 128 128 128 128 128 128 128 128	Loop Guard Disabled Disabled Disabled Disabled Disabled
Port           eth1/0/1           eth1/0/2           eth1/0/3           eth1/0/4           eth1/0/5           eth1/0/6	State       Enabled       Enabled       Enabled       Enabled       Enabled       Enabled       Enabled	Cost 0/200000 0/200000 0/200000 0/200000 0/200000	Guard Root Disabled Disabled Disabled Disabled Disabled Disabled	L Link Tyr Auto/P2 Auto/P2 Auto/P2 Auto/P2 Auto/P2 Auto/P2 Auto/P2	P Edge/Non-Edg P Edge/Non-Edg P Edge/Non-Edg P Edge/Non-Edg P Edge/Non-Edg P Edge/Non-Edg P Edge/Non-Edg	TCN Filte ge Disabled ge Disabled ge Disabled ge Disabled ge Disabled ge Disabled	r BPDU Forward Disabled Disabled Disabled Disabled Disabled Disabled Disabled	Priority           128           128           128           128           128           128           128           128           128           128           128           128           128	Loop Guard Disabled Disabled Disabled Disabled Disabled Disabled

図 8-49 STP Port Settings 画面

参照

STP グループと VLAN グループを関連付けて定義することをお勧めします。

## 画面に表示される項目:

項目	説明
Unit	設定するユニットを選択します。
From Port	連続するポートグループの最初の番号を設定します。
To Port	連続するポートグループの最後の番号を設定します。
Cost	指定ポートへのパケット転送をするための適切なコストを表すメトリックを指定します。ポートのコストは自動か、メトリッ
(1-200000000,	クの値で設定します。初期値は0(Auto)です。
0=Auto)	• 0 (Auto)- 選択ポートに可能な最良のパケット転送速度を自動的に設定します。
	ポートコストの初期値 :100Mbps ポート = 200000、Gigabit ポート = 20000。
	<ul> <li>値 1-200000000 - 外部転送のコストとして 1 から 200000000 までの値を設定します。数字が低いほどパケット転送は 頻繁に行われるようになります。</li> </ul>
State	ポートグループでの STP の「Enabled」(有効)/「Disabled」(無効)を設定します。初期値は「Enabled」です。
Guard Root	Guard Root の「Enabled」(有効)/「Disabled」(無効)を設定します。
Link Type	リンクの種類を設定します。初期値は「Auto」です。
	・ P2P - P2P ポートとしてリンクを共有します。P2P ポートは全二重でなくてはならないという制限があります。
	・ Shared - 半二重ポートとして認識されます。
	・ Auto - 可能であれば常に P2P となるように設定します。ポートが、例えば強制的に半二重になるなど状態を維持できな
	した。 い場合には、Shared と同様の状態になります。
Port Fast	ポートファストオプションを指定します。
	Network」! Disabled」! Edge」から選択します。! Network」モデム内だとボートは3秒だけ非ボートファスト状態に残ります。ボー
	トは BPDU か受信されず、転送状態に変更されるとホートノアスト状態に変更します。のちに BPDU を受信すると非ホートノア
	人下へ戻りより。  Disable」モートではホートは常に非ホートノア人ト状態です。常に転送状態への変化のために   forward-time
	delay」を行らより。「Edge」モートではホートは   forward-time delay」を行たりに直接 SIP 転达状態に変化しより。インダノエー フボ「DDDU」を受信するとまピートファフトの移行します。初期値では「Network」にたけます。
	ヘル「DPDU」を文旨すると非ホートノアヘト、物目します。初期値では「NetWOIK」になります。
ICN Fliter	ICN(Topology Change Notification)ノイルダを「Enabled」(有効)/「Disabled」(無効)に設定します。   ポートの TCN フィルクリングをちかにする ト 域中のスドレスフラッシングを発生させる シットロークのつス域への効 部ゴリッ
	「ホードのTCN フィルダウンクを有効にすると、政内のケドレスノフタンフタを先生させるホットフークのコノ或への外部フラック
	トが TCN フィルタモードに設定されると、ポートは無視されることにより TC イベントは受信されます。初期値は無効です。
BPDU Forward	BPDU パケットの転送を「Enabled」(有効)または「Disabled」(無効)にします。
	有効にすると受信した STP BPDU はすべての VLAN メンバポートにタグなしフォームで転送されます。初期値は無効です。
Priority	優先値を指定します。0 から 240 で指定可能です。初期値は 128 です。少ない方が優先値は高くなります。
Hello Time	ハロータイムの値を指定します。1から2(秒)の間で指定可能です。
	この設定は指定ポートによる各設定メッセージの定期的な送信の間隔となります。

項目	説明
Loop Guard	指定ポートでのループガードを「Enabled」(有効)/「Disabled」(無効)に指定します。STP ループガードは L2 フォワーディ
	ングループ(STP ループ)に対する追加の防御機能です。STP ループはリダンダントトポロジ内の STP ブロックポートが、フォ
	ワーディングステートへ移行する際に発生するエラーにより生成されます。これは通常、物理リダンダントトポロジのポート
	の一つ(STP ブロックポートである必要なし)が、STP BPDU を受信しなくなることにより発生します。これにより、STP は継
	続した BPDU の受信や送信をポートにあてがわれた役割に依存することになります。宛先ポートは BPDU を送信し、非宛先ポー
	トは BPDU を受信することになります。
	物理リダンダントトポロジのポートの一つが BPDU を受信しなくなると、STP がトポロジをループ解除状態と認識します。最
	終的にブロック/バックアップだった幾つかのポートが宛先、そしてフォワーディングステートになり、ループを生成します。

「Apply」ボタンをクリックし、設定を有効にします。

注意 BPDU の送出をポートベースで有効とする場合は、はじめに以下の設定を行ってください。

- (1) STP をグローバルに無効とする。
- (2) BPDUの送出をグローバルに有効とする。

これらの設定は、前述の「STP Bridge Global Settings」メニューで行います。

### MST Configuration Identification (MST の設定)

スイッチ上で MST インスタンスの設定を行います。本設定は MSTI(マルチプルスパニングツリーインスタンス)を識別するためのものです。スイッチは 初期状態で 1 つの CIST(Common Internal STP)を持ちます。ユーザはその項目を変更できますが、MSTI ID の変更や削除は行うことができません。

L2 Features > STP > MST Configuration Identification の順にメニューをクリックし、以下の画面を表示します。

MST Configuration Ide	ntification	
MST Configuration Identifica	tion	
Configuration Name Revision Level (0-65535) Digest	F0:7D:68:34:00:10 0 AC36177F50283CD4B83821D8AB26DE62	Apply
Private VLAN Synchronize		
Private VLAN Synchronize		Apply
Instance ID Settings		
Instance ID (1-64)		
Action	Add VID	
VID List	1 or 3-5	Apply
Total Entries: 1		
Instance ID	VID List	
CIST	1-4094	Edit Delete
		1/1 < < 1 > > Go

図 8-50 MST Configuration Identification 画面

#### 画面に表示される項目:

項目	説明
Configuration Name	各 MSTI(Multiple Spanning Tree Instance)を識別するためにスイッチに名前を設定します。
	名前が設定されていない場合、MSTP が動作しているデバイスの MAC アドレスが表示されます。
Revision Level (0-65535)	スイッチ上に設定された MST リージョンの値を設定します。Configuration Name に同期しています。初期値は 0 です。
Instance ID	1-46 の番号を入力し、スイッチに Instance ID を設定します。
Action	MSTI に行う変更を選択します。
	・ Add VID - VID List 項目に指定された VID を MSTI ID に追加します。
	・ Remove VID - VID List 項目に指定された VID を MSTI ID から削除します。
VID List	VLAN の VID の範囲を指定します。

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

「Edit」をクリックして、指定エントリの編集を行います。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

# STP Instance (STP インタンス設定)

STP インスタンスの設定を行います。

#### L2 Features > STP > STP Instance をクリックし、以下の画面を表示します。

otal Entries: 1			
Instance	Instance State	Instance Priority	
CIST	Disabled	32768(32768 sysid 0)	Edit
		1/1	
nstance CIST		CIST Global Inf	o[Mode RSTP]
	Bridge Address	F0-7D-68	34-00-10
De	signated Root Address / Priority	00-00-00-0	0-00-00 / 0

図 8-51 STP Instance 画面

画面に表示される項目	:
------------	---

項目	説明
Edit	「Edit」をクリックし、指定エントリの編集を行います。
Instance Priority	「Edit」をクリック後、指定したインスタンスのためのプライオリティ(0-61440)を設定します。

「Apply」をクリックし、設定内容を適用します。

「Edit」をクリックして、指定エントリの編集を行います。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

## MSTP Port Information (MSTP ポート情報)

本画面では現在の MSTP ポート情報が表示され、MSTI ID 単位でポート構成の更新を行います。ループが発生した場合に MSTP 機能はポートプライ オリティを使用して、Forwarding 状態に遷移させるインタフェースを選択します。最初に選択したいインタフェースには高いプライオリティ(小 さい数値)を与え、最後に選択したいインタフェースには低いプライオリティ(大きい数値)を与えます。インタフェースに同じプライオリティ値 が与えられている場合、MSTP は MAC アドレスの値が最小のインタフェースを Forwarding 状態にし、他のインタフェースをブロックします。低い プライオリティ値ほど転送パケットに対して高いプライオリティを意味することにご注意ください。

各ポートに MSTP の設定を行うには、L2 Features > STP > MSTP Port Information の順にメニューをクリックし、以下の画面を表示します。



図 8-52 MSTP Port Information 画面

#### 画面に表示される項目:

項目	説明
Unit	設定を行うユニットを指定します。
Port	適用するポートを選択します。
Internal Path Cost (1-200000000)	インタフェースを STP インスタンスで選択する場合、指定ポートにパケットを転送する相対的なコストを設定します。 「Edit」をクリックして、指定インスタンスの編集を行います。 ・ 0 (Auto) - インタフェースに自動的で最適な最速のルートを設定します。(初期値) ・ 値 1-20000000 - ループが発生した場合、この範囲で指定した値を使用した最短のルートを設定します。コストが小 さいほど高速で伝送されます。
Priority	ポートインタフェースのプライオリティ (0-240) までの値を指定します。高いプライオリティほど、パケットの転送は 優先されます。値が低いほどプライオリティは高くなります。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。 「Clear Detected Protocol」ボタンをクリックし、選択したポートの検出したプロトコル設定をクリアします。 特定ポートの MSTP 設定を参照するためには、プルダウンメニューでポート番号を選択し、「Find」ボタンをクリックします。 設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

# ERPS (G.8032) (イーサネットリングプロテクション設定)

ERPS (Ethernet Ring Protection Switching) はイーサネットリング保護スイッチングの業界標準 (ITU-T G.8032) です。これは、イーサネットリングネットワークに対して十分に考慮されたイーサネット操作、管理、およびメンテナンス機能と簡単な APS (automatic protection switching) プロトコル を統合することによって実行されます。ERPS はリングトポロジ内のイーサネットトラフィックに sub-50ms 保護を提供します。これはイーサネット レイヤにループが全く形成されないことを保証します。

リング内の1つのリンクが、ループを回避するためにブロックされます(RPL:Ring Protection Link)。障害が発生すると、保護スイッチングは障害のあるリンクをブロックして RPLのブロックを解除します。障害が解決すると、保護スイッチングは再度 RPL をブロックして、障害が解決したリンクのブロックを解除します。

## ERPS

本項目では「Ethernet Ring Protection Switching」(ERPS)の表示、設定を行います。STP とループバック検知 (LBD) は ERPS の有効化の前にリングポートで無効になる必要があります。ERPS は「R-APS VLAN」リングポート、RPL ポート、RPL オーナが設定されていない状態では、有効にできません。

注意 ERPS バージョンを変更するとプロトコルが再起動します。

L2 Features >	ERPS (G.8032) >	- ERPS の順にメニュ	ーをクリックし、	以下の画面を表示し	、ます。
---------------	-----------------	---------------	----------	-----------	------

ERPS Status		ERPS Brief					
RPS Version Settings							
RPS Version	G.8032v2	~					Apply
hernet Ring G.8032							
Ring Name	32 chars						Apply
otal Entries: 1							
Ethernet Ring	Admin Port0	Admin Port1	Ring Type	Ring ID	Instance		
		10 SSA	Major ring	4		Edit Ping Show Detail	Delete

画面に表示される項目:

項目	説明			
	ERPS Version Settings			
ERPS Version	<ul> <li>ERPS バージョンを選択します。「G.8032v1」「G.8032v2」から選択可能です。</li> <li>「G.8032v2」では以下の事が可能です。: <ul> <li>物理リング内のマルチインスタンス</li> <li>「manual」「force」「clear」などの操作コマンド。</li> <li>物理リングのリング ID を持つ「R-APS PDU 宛先アドレス」の送信設定</li> </ul> </li> <li>「G.8032v2」が実行中の機器に対し「G.8032v1」を設定する前に、「G.8032v1」がサポートしない全ての ERPS 設定を 削除する必要があります。そうでない場合バージョンの変更は行えません。ERPS バージョンの変更は実行中のプロト コルの再起動を促します。</li> <li>「G.8032v2」から「G.8032v1」へ変更する前に、次の設定であることをチェックする必要があります。: <ul> <li>手動(Manual) または強制(force) スイッチコマンドの消去</li> <li>内部接続のメジャーリングインスタンスとサブリングインスタンス機器が違う「R-APS VLAN ID」を保持している。</li> <li>物理リング内で一つのみのインスタンスがサポートされている。</li> </ul> </li> </ul>			
	<ul> <li>イーサネットリング機器がイーサネットリングで「ITU-T G.8032v1」と「ITU-T G.8032v2」を同時に存在させている場合、「G.8032v2」機器において次の設定を行う必要があります。:</li> <li>全ての物理リング ID は初期値の 1 であること。</li> <li>内部接続のメジャーリングインスタンスとサブリングインスタンス機器が、それぞれ違う「R-APS VLAN ID」の保持</li> <li>手動(Manual)または強制(force)スイッチコマンドの消去</li> <li>物理リング内で一つのみのインスタンスをサポート</li> </ul>			
	Ethernet Ring G.8032			
Ring Name	ERP インスタンス名を入力します。(最大 32 文字)			

「Apply」をクリックして「ITU-T G.8032 ERP リング」を作成します。

図 8-53 ERPS 画面

# 第8章 L2 Features (L2機能の設定)

「Edit Ring」をクリックして ERP リングを編集します。 「Show Detail」をクリックして「ITU-T G.8032 ERP リング」の情報について表示します。 「Delete」をクリックして指定の「ITU-T G.8032 ERP リング」を削除します。 設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

## ■ Ring の編集

「Edit Ring」ボタンをクリックすると、以下の設定画面が表示されます。

nemet Ring Settings —		
thernet Ring Name	ring	
nstance ID (1-32)	None  Specify	
Sub Ring Name	32 chars ONone OSpecify	
Port0	1 eth1/0/1 None Specify	
Port1	1 None None Specify	
Ring ID	None Specify	
Ring Type	Major ring 🔽 🗆	
		Back Apply

図 8-54 ERPS 画面 - Edit

## 画面に表示される項目:

項目	説明
Instance ID	チェックを入れ「ERP インスタンス」の番号を指定します。32 まで指定可能です。
	「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
Sub Ring Name	チェックを入れ「サブリング名」を指定します。32文字まで指定可能です。「Specify」にチェックを入れパラメータを指
	定します。「None」にチェックを入れるとパラメータの値は初期値になります。
Port0	チェックを入れユニット ID と初期リングになるポート番号を指定します。ドロップダウンメニューから「None」を選
	択すると内部接続されたノードはオープンリングのエンドポイントのローカルノードとして指定されます。「Specify」に
	チェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
Port1	チェックを入れユニット ID と 2 番目のリングになるポート番号を指定します。ドロップダウンメニューから「None」を
	選択すると内部接続されたノードはオープンリングのエンドポイントのローカルノードとして指定されます。「Specify」
	にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
Ring ID	チェックを入れリング ID を指定します。1-239 まで指定可能です。
	「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
Ring Type	チェックを入れリングタイプを指定します。「Major Ring」「Sub Ring」から指定します。

「Back」をクリックすると設定は破棄され前画面に戻ります。 「Apply」をクリックして設定を適用します。

## 「ERPS Brief」タブの表示

「ERPS Brief」タブをクリックすると、以下の画面が表示されます。

ERPS	_	_		
ERPS Status	ERPS Brief			
Total Entries: 1				
Ethernet Ring	Instance ID	Status	Port State	
Disa		Departmented	P0:eth1/0/10,Forwarding	
Rang	1	Deactivated	P1:eth1/0/12,Forwarding	Edit Instance
			1/1	K < 1 > > Go

図 8-55 ERPS (ERPS Brief タブ) 画面

「Edit Instance」をクリックすると、ERP インスタンスを設定します。 設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

## ■ Instance の編集(Edit Instance)

「Edit Instance」ボタンをクリックすると、以下の設定画面が表示されます。

Ethernet Instance Settings					
Ethernet Ring Name	Ring				
Instance ID	1				
Description	64 chars	None  Specify			
R-APS Channel VLAN (1-4094)		None  Specify			
Inclusion VLAN List	1,3-5	None  Specify			
MEL (0-7)	1	None  Specify			
Profile Name	32 chars	ONone  Specify			
RPL Port	Port0	$\checkmark$			
RPL Role	Owner	None  Specify			
Activate	Disabled				
Sub Ring Instance (1-32)		None  Specify			
Force Ring Port Block	Port0				
Manual Ring Port Block	Port0				
			Back	Apply	Clear

図 8-56 ERPS 画面 - Instance

画面に表示される項目:

項目	説明
Description	チェックを入れ「ERP インスタンス」の概要を指定します。64 文字まで指定可能です。
	「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
R-APS Channel VLAN	チェックを入れ「ERP インスタンス」の「R-APS Channel VLAN ID」を指定します。サブインスタンスの「APS channel
	VLAN」はサブリングの仮想チャネルでもあります。1 から 4094 までの間で指定可能です。
	「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
Inclusion VLAN List	チェックを入れインスタンスに含まれる VLAN リストを指定します。
	「-」を使用すると範囲として指定され、「,」を使用すると個別に複数の VLAN を指定します(例;「VLAN1 から 5」は「1-5」、
	「VLAN1 と 3 と 5」は「1,3,5」)。指定された VLAN は ERP のメカニズムで保護されます。
	「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
MEL	チェックを入れ ERP インスタンスの「MEL」を指定します。0 から 7 までの間で指定可能です。
	同じ ERP インスタンスの全てのリングノードの MEL 値は同一です。
	「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
Profile Name	チェックを入れ ERP インスタンスに関連する「G.8032」のプロファイルを指定します。複数の ERP インスタンスが同じ
	G.8032 プロファイルに含まれることも可能です。同じプロファイルに含まれるインスタンスは同じセットの VLAN やー
	つのインスタンスに保護される VLAN、他のインスタンスに保護される LAN のサブセットを保護します。32 文字まで指
	Specify」にチェックを入れパラメータを指定します。 None」にチェックを入れるとパラメータの値は初期値になります。
RPL Port	チェックを入れ RPL ポートオプションを選択します。オプションは「Port0」「Port1」から指定します。
	選択されたオプションは RPL ポートとして設定されます。
RPL Role	チェックを入れノードが RPL オーナかネイバかを選択します。「Enable/Disable」から選択し、「Enable」の場合、RPL は「オー
	ナ」として設定されます。
Activate	チェックを入れ ERP インスタンスをアクティブにするか選択します。「Enable/Disable」から選択し、「Enable」の場合、
	ERP インスタンスはアクティブになります。
Sub Ring Instance	チェックを入れ ERP インスタンスに関連する識別子を指定します。物理リングインスタンスのサブリングインスタンス
	を指定に使用されます。1-32 字まで指定可能です。
	「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
Force Ring Port Block	チェックを入れブロックされる ERP インスタンスポートを選択します。リンク不具合などの発生有無にかかわらず、こ
	の強制インスタンスポートブロックは、設定後すぐに有効になります。
	オプションは「Port0」「Port1」から指定します。
Manual Ring Port Block	チェックを入れブロックされる ERP インスタンスポートを選択します。MS が設定されており、リンク不具合の発生や FS
	状態が空白である場合、この強制インスタンスポートブロックは、設定後すぐに有効になります。
	オプションは「Port0」「Port1」から指定します。

「Back」をクリックすると設定は破棄され前画面に戻ります。

「Apply」をクリックして設定を適用します。

「Clear All」をクリックすると入力したエントリを全てクリアします。

# ERPS Profile (ERPS プロファイル)

ERPS プロファイル設定を行います。

## L2 Features > ERPS (G.8032) > ERPS Profile の順にメニューをクリックし、以下の画面を表示します。

ERPS Profile				
Ethernet Ring G.8032 Profile				
Profile Name	32 chars			Apply
Total Entries: 1				
Profile	Guard Timer (ms)	Hold-Off Timer (ms)	WTR Timer (min)	
profile	500	0	5	Edit Delete
			1/1	< 1 > > Go

図 8-57 ERPS Profile 画面

#### 画面に表示される項目:

項目	説明
Profile Name	「G.8032」のプロファイル名を指定します。32 文字まで指定可能です。複数の ERP インスタンスが同じ「G.8032」プロファ
	イルとして指定できます。同じプロファイルに含まれるインスタンスは同じセットの VLAN や一つのインスタンスに保護
	される VLAN、他のインスタンスに保護される LAN のサブセットを保護します。

「Apply」をクリックして「G.8032」プロファイルと ERP インスタンスを作成します。 「Delete」をクリックして指定の「G.8032」プロファイルと ERP インスタンスを削除します。 「Edit」をクリックして「G.8032」プロファイルを編集します。

## ■「G.8032」プロファイルの編集

「Edit」ボタンをクリックすると、以下の設定画面が表示されます。

Profile Name	profile	
CN Propagation	Disabled 🔽	
Revertive	Enabled	
Buard Timer (10-2000)	500 ms 🗌	
lold-Off Timer (0-10)	0 s 🗌	
VTR Timer (1-12)	5 min	

図 8-58 「G.8032」プロファイル画面 - Edit

## 画面に表示される項目:

項目	説明
TCN Propagation	チェックを入れ「TCN Propagation」の設定を行います。「Enable/Disable」から選択します。 本機能はサブ ERP インスタンスからメジャーインスタンスへのトポロジ変更の通知の伝播を有効にします。
Revertive	チェックを入れ「Revertive」の設定を行います。「Enable/Disable」から選択します。本機能は送信エンティティへの復帰 に使用します。例えば RPL がブロックされた場合などです。
Guard Timer	チェックを入れ Guard Timer の設定を行います。10 から 2000 (ミリ秒)の間で指定可能です。初期値は 500 (ミリ秒)です。
Hold-Off Timer	チェックを入れ Hold-Off Timer の設定を行います。0 から 10(秒)の間で指定可能です。初期値は 0(秒)です。
WTR Timer	チェックを入れ WTR Timer の設定を行います。1 から 12(分)の間で指定可能です。初期値は 5(分)です。

「Back」をクリックすると設定は破棄され前画面に戻ります。

# Loopback Detection (ループバック検知設定)

ループバック検知(LBD)機能は、特定のポートに生成されるループを検出するために使用されます。本機能は、CTP(Configuration Testing Protocol) パケットがスイッチにループバックすると、スイッチのポートを一時的にシャットダウンします。スイッチが CTP パケットをポートまた は VLAN から受信したことを検知すると、ネットワークにループバックが発生していると認識します。スイッチは、自動的にポートまたは VLAN を ブロックして管理者にアラートを送信します。「Loopback Detection Recover Time」がタイムアウトになると、ループバック検知ポートは再起動 (Normal 状態へ遷移)を行います。ループバック検知機能はポート範囲に実行されます。

L2 Features > Loopback Detection の順にメニューをクリックし、以下の画面を表示します。

Loopback Detection				
Loopback Detection Global Set	tings			
Loopback Detection State	Disabled	Mode	Port-based	V
Enabled VLAN ID List	1-4094	Interval (1-32767)	10	sec
Trap State	Disabled 🗸	Action Mode	Shutdown	
Address Type	Multicast 🗸	Function Version	v4.07	Apply
	From Port eth1/0/1	To Port	eth1/0/1	State Disabled V Apply
Port	Loopback Det	ection State	Result	Time Left (sec)
eth1/0/1	Disab	led	Normal	-
eth1/0/2	Disab	led	Normal	-
eth1/0/3	Disab	led	Normal	2
eth1/0/4	Disab	led	Normal	
eth1/0/5	Disab	led	Normal	-
eth1/0/6	Disab	led	Normal	-
eth1/0/7	Disab	led	Normal	-
eth 1/0/8	Disab	led	Normal	

図 8-59 Loopback Detection 画面

## 画面に表示される項目:

項目	説明
	Loopback Detection Global Settings
Loopback Detection State	ループバック検知機能を「Enabled」(有効)または「Disabled」(無効)にします。初期値は「Disabled」です。
Mode	プルダウンメニューで「Port Based」または「VLAN Based」を選択します。
Enable VLAN ID List	「Mode」で「VLAN ID」を選択した場合 VLAN ID のリストを入力します。
Interval (1-32767)	ループ検知間隔を設定します。(1-32767 秒)
Traps State	トラップを「Enabled」(有効)/「Disabled」(無効)に設定します。
Action Mode	動作モードを指定します。 • Shutdown - ループ検出時にポートベースモードのポートをシャットダウン、または VLAN ベースモードの指定 VLAN のトラフィックをブロックします。 • None - ループ検出時でもポートベースモードのポートをシャットダウン、または VLAN ベースモードの指定 VLAN のトラフィックをブロックしません。
Address Type	アドレスタイプを「Multicast」「Broadcast」から指定します。
	Loopback Detection Port Settings
Unit	設定するユニットを指定します。
From Port	プルダウンメニューで開始ポートを選択します。
To Port	プルダウンメニューで終了ポートを選択します。
State	「Enabled」(有効)または「Disabled」(無効)を指定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

注意

「Untag(タグなし)」時でも「VID 0」は CTP に「Tag Field」を付与されます。規定上「VID 0」は「Untag(タグなし)」として扱われますが、 古い一部のハードウェア製品(chipset 等)では破棄する場合があるのでご注意ください。

# Link Aggregation (リンクアグリゲーション)

# ポートトランクグループについて

ポートトランクグループは、複数のポートを結合して1つの広帯域のデータパイプラインとして利用する機能です。 トランクグループは最大32個まで作成可能であり、各グループには1~8個までの物理ポートを割り当てることができます。



図 8-60 ポートトランクグループの例

トランクグループ内のすべてのポートは1つのポートと見なされます。あるホスト(宛先アドレス)へデータ転送が行われる際には、常にトランク グループ内の特定のポートが使用されるため、データは送信された順で宛先ホスト側に到着します。

リンクアグリゲーション機能により複数のポートが1つのグループとして束ねられ、1つのリンクとして動作します。この時、1つのリンクの帯域 は束ねられたポート分拡張されます。

リンクアグリゲーションは、サーバなどの広帯域を必要とするネットワークデバイスをバックボーンネットワークに接続する際に広く利用されています。

本スイッチでは、1~8個のリンク(ポート)から構成される最大 32個のリンクアグリゲーショングループの構築が可能です。各ポートは1つの リンクアグリゲーショングループにのみ所属することができます。

同じグループに含まれるポートはすべて同じ VLAN に属し、スパニングツリープロトコル(STP)ステータス、スタティックマルチキャスト、ストームコントロール、トラフィックセグメンテーション、および 802.1p デフォルトプライオリティの設定についても同じ構成となっている必要があります。また、ポートセキュリティ、ポートミラーリング、および 802.1X は無効にする必要があります。さらに、集約するリンクはすべて同じ速度で、 全二重モードで設定されている必要があります。

リンクアグリゲーショングループではマスタポートを1つ指定します。マスタポートに設定された、VLAN 設定を含む全ての構成オプションがグループ全体に適用されます。

グループ内のポート間では自動的にロードバランスが行われ、グループ内でのリンク断が発生した場合、ネットワークトラフィックはグループ内の 他のリンクに振り分けられます。

スパニングツリープロトコル(STP)は、スイッチレベルにおいて、リンクアグリゲーショングループを1つのリンクとして扱います。ポートレベ ルでは、STP はマスタポートのパラメータを使用してポートコストを計算し、リンクアグリゲーショングループの状態を決定します。スイッチに冗 長化された2つのリンクアグリゲーショングループが設定されている場合、STPにおいて片方のグループはブロックされます(冗長リンクを持つポー トがブロックされるケースと同様)。

# 第8章 L2 Features (L2機能の設定)

注意

トランクグループ内のいずれかのポートが接続不可になると、そのポートが処理するパケットはリンクアグリゲーション(集約)グループ 内の他のポート間でロードシェアされます。

注意 10/100/1000BASE-T ポートと SFP+ スロットでのリンクアグリゲーション、または SFP スロット /SFP コンボスロットと SFP+ スロットで のリンクアグリゲーションは利用できません。

L2 Features > Link Aggregation の順にクリックし、以下の画面を表示します。

System Priority (1-655: Load Balance Algorithr System ID	35) 3 n 5 3.	2768 Source Destination 2768,80-26-89-8D-A	MAC enhanced MF 7-00	PLS label			Apply
hannel Group Inform	ation						
Unit From 1  eth1 Note: Each Channel G	Port /0/1 🔽 roup supports (	to Port eth1/0/1	Group ID (1-32	) Mode On	~	Add	Delete Member Por
Unit From eth1 Note: Each Channel G Total Entries: 1	Port	To Port eth1/0/1	Group ID (1-32	) Mode On	~	bbA	Delete Member Po
Unit From I V eth1 Note: Each Channel G Total Entries: 1 Channel Group	Port /0/1  roup supports t Protocol	To Port eth1/0/1 v up to 12 member por Max Ports	Group ID (1-32 ts.	) Mode On Member Port	<b>×</b>	Add	Delete Member Po

図 8-61 Link Aggregation 画面

画面に表示される項目:

項目	説明
System Priority	システム優先値を指定します。1から65535の間で指定できます。初期値は32768です。システム優先値はどのポートがポー トチャネルに属するか、そしてポートがスタンドアロンモードに入るかを決定します。低い値の方が高い優先値を示します。 二つ以上のポートで同じ優先値を与えられた場合、ポート番号で優先値が決まります。
Load Balance Algorithm	ポートトランクグループを構成するポートのロードバランスに使用するアルゴリズムを選択します。「Source MAC」、 「Destination MAC」、「Source Destination MAC」、「Source IP」、「Destination IP」、「Source Destination IP」「Source L4 Port」 「Destination L4 Port」「Source Destination L4 Port」から指定してください。 初期値は「Source Destination MAC」です。
Unit	設定するユニットを指定します。
From Port / To Port	設定するポートの範囲を設定します。
Group ID (1-32)	グループの ID 番号(1-32)を設定します。
Mode	<ul> <li>モードを指定します。「On」「Active」「Passive」から指定できます。</li> <li>On - チャネルグループタイプは固定です。</li> <li>Active - Active ポートは LACP 制御フレームの処理と送信を行います。これにより LACP 準拠のデバイス同士はネゴシエーションとリンクの集約を行い、グループは必要に応じて動的に変更されます。グループへのポート追加、または削除などのグループの変更を行うためには、少なくともどちらかのデバイスで LACP ポートを Active に設定する必要があります。</li> <li>Passive - Passive ポートは自分から LACP 制御フレームの送信を行いません。リンクするポートグループがネゴシエーションを行い、動的にグループの変更を行うためには、コネクションのどちらか一端が Active な LACP ポートである必要があります。(初期値)</li> </ul>

指定のエントリを削除するためには、削除するグループの「Delete Channel」ボタンをクリックします。 指定のメンバポートを削除するためには、削除するグループの「Delete Member Port」ボタンをクリックします。

## ■ ポートトランキンググループの設定

各項目を入力後、「Add」ボタンをクリックし、ポートトランキンググループを設定します。

注意

レイヤ 3/ レイヤ 4 のアルゴリズムを利用している場合でも、「FDB にエントリがない、またはフラッディング対象」の場合は、MAC アル ゴリズムが利用されます。

注意

リンクトラップを有効にした場合、同時にリンクアグリゲーションのリンクトラップも有効になります。

### ■ ポートトランクグループの編集

チャネルについてのより詳細な情報の確認には「Show Detail」をクリックします。

escription	1						
rescription	64 chore						Apply
	04 chars						мрріу
Port	Status	Administra	itive		Description		
Port-channel1	down	enabled	1			De	lete Description
ort Channel Informat	ion						
ort Channel	1						
rotocol	Static						
ort Channel Detail Inf	ormation						
Port	LACP Timeout	Working Mo	de	LACP State	Port Priority	Port Number	
eth1/0/18	None	None		down	None	None	Edit
eth1/0/19	None	None		down	None	None	Edit
ort Channel Neighbo	r Information						
Port Part	ner System ID	Partner PortNo	Partne	er LACP Timeout	Partner Working	Mode Partr	ner Port Priority
eth1/0/18	None	None		None	None		None
eth1/0/19	None	None		None	None		None
lote:							Back
ACP State:							
ndl: Port is attached t	o an aggregator and	bundled with other port	ts.				
	an and ant state/act h	undled but able to switz	ch data tra	offic)			

図 8-62 Port Channel 画面

「Description」にポートチャネルの概要を指定します。64 字まで指定可能です。 「Delete Description」でポートチャネルの概要を指定します。 編集するエントリの「Edit」ボタンをクリックします。 「Back」ボタンをクリックし前の画面に戻ります。

# MLAG (マルチシャーシリンクアグリゲーション)

MLAG(マルチシャーシリンクアグリゲーション /Multi-Chassis Link Aggregation Group)ではポートブロックや不要なリンクスピードの低下、スイッチ / ケーブル接続の不具合を発生させるイベントなどに対処するため、ネットワークスイッチの帯域の増加を行います。「MLAG ピア」となったスイッチは同じ MLAG ドメインにある他の「MLAG ピア」スイッチと「Peer-Link(ピアリンク)」を通じて接続します。

MLAG ピアスイッチと接続した MLAG パートナースイッチは、ネットワーク内で単一の「MLAG スイッチ」として認識されます。その2台の MLAG ピアスイッチは MLAG 機能を除き、それぞれスタンドアロンのスイッチとして別々な操作が可能です。MLAG を使用すると物理的に拡張したトポロジ間でデータトラフィックの送受信が可能になります。

MLAGピア接続を構築するには同じファームウェアをインストールした同じ機種のスイッチである必要があります。MLAGピア接続を構築するスイッチは設定後の不安定化を避けるために「Link Aggregation」「MLAG Portchannel」「Interface」「VLAN settings」の項目において、設定内容を全く同じにする必要があります。

MLAG ピアスイッチはスタンドアロンで使用し、物理スタッキングが無効化されている必要があります。

注意 VRRP を含む L3 機能との併用はできません。

## MLAG Settings (MLAG 設定)

MLAG 設定ついて表示します。MLAG の設定は必ずもう一方の MLAG ピアスイッチと接続する前に行います。設定内容はスイッチが再起動した後に 有効になります。グループ内の全てのスイッチは必ず同じ MLAG バージョンで動作している必要があります。

L2 Features > MLAG > MLAG Settings の順にクリックし、以下の画面を表示します。

MLAG Settings		
MLAG State		
MLAG State	<ul> <li>Enabled          <ul> <li>Disabled</li> </ul> </li> </ul>	Apply
図 8-63 MLAG Set	ttings (Disabled) 画面	

「MLAG State」で MLAG を有効 / 無効(初期値)にします。有効にし、スイッチの再起動を行うと次の画面になり各設定項目が表示されます。

MLAG State			
MLAG State	Enabled      Disabled		Apply
MLAG Configuration			
Domain (1-255)	1 Default		
Device ID (1-2)	1 Default		
Hello Interval (1-10)	3 sec 🗌 Default	t,	Apply
MLAG Peer Link Settings -			
Port	PeerLink1/0/25 Peer Link	k	Apply
MLAG Information			
MLAG Version	1.0		
MLAG Hello Interval	3s		
MLAG Domain	1		
		MLAG Information	
ML	AG Status	Active	
MA	C Address	80-26-89-8D-A7-00	
MLAG	3 Device ID	1	
MLA	G Peer-link	25	
	M	ILAG Neighbor Information	
Neigi	hbor Status	Active	
MA	C Address	F0-7D-68-30-36-00	

MLAG Settings( 有効時 )

図 8-64 MLAG Settings (Enabled) 画面

画面に表示される項目:

項目	説明
MLAG State	MLAG を「Enabled」(有効)/「Disabled」(無効)(初期値)にします。有効の状態でのみ MLAG の設定が可能です。
Domain	MLAG ドメイン ID(1-255)を指定します。「Default」にチェックを入れると初期値(1)が適用されます。
Device ID	MLAG デバイス ID(1-2)を指定します。「Default」にチェックを入れると初期値(1)が適用されます。
Hello Interval	MLAG ハローインターバル ID(1-10 秒)を指定します。MLAG ハローメッセージの送信間隔(秒)になります。
	「Default」にチェックを入れると初期値(3 秒)が適用されます。
Port	Peer-Link(ピアリンク)に使用する物理ポートを指定します。
Peer Link	指定したポートを Peer-Link(ピアリンク)ポートとして指定します。MLAG ピアスイッチとの接続に使用します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

## MLAG Group (MLAG グループ)

MLAG グループについて表示します。

**L2 Features > MLAG > MLAG Group** の順にクリックし、以下の画面を表示します。

LAG Group				
LAG Group				
Flag:				
S - Port is requesting Slo	w LACPDUs F - Port is reg	uesting fast LACPDU		
A - Port is in active mode	P - Port is in passive mode	)		
LACP state:				
bndl: Port is attached to	an aggregator and bundled w	ith other ports.		
hot-sby: Port is in a hot-s	standby state.			
down: Port is down				
MLAG Group ID (1-32)				Find
Total Entries: 1				
Group ID	Algorithm	Group Status	Actor System	ID Partner System ID
10	src-dst-mac	Up	00-0F-36-31-AE	-01 00-20-00-16-99-00
				1/1 < < 1 > > Go
Group 10 Information				
D	evice ID	Port	Flags	LACP State
	1	1	FA	bndl
	1	2	FA	bndl
	2	1	FA	bndl
	2	2	FA	bndl
				1/1 < 1 > > Go

図 8-65 MLAG Group 画面

凹凹にな小で10次日・	画面に表示される項目	:
-------------	------------	---

項目	説明	
MLAG Group ID	MLAG Group ID(1-32)を指定します。	]

「Find」をクリックし指定 ID のエントリを表示します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

# Flex Links(フレックスリンクス)

本項目ではフレックスリンクス機能の表示、設定について説明します。フレックスリンクスはL2インタフェースのペアのうち、一つがもう片方のバックアップとして動作する機能です。フレックスリンクスにより、STPやLBD等のリンクレベルでの冗長性が提供されます。

L2 Features > Frex Links の順にメニューをクリックし、以下の画面を表示します。

Flex Links				
Flex Links Unit Primary Port 1 v eth1/0/1 Total Entries: 1	Unit Backup	) Port 1/1 🔽		Apply
Group	Primary Port	Backup Port	Status(Primary/Backup)	
1	eth1/0/10	eth1/0/11	Inactive/Inactive	Delete

図 8-66 Flex Links 画面

画面に表示される項目:

項目	説明
Unit	プライマリポートの存在するユニットを指定します。
Primary Port	プライマリポートを指定します。
Unit	セカンダリポートの存在するユニットを指定します。
Backup Port	セカンダリポートを指定します。

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

注意 フレックスリンクスは、STP、ERPS、LBD 機能と相互排他になります。

# L2 Protocol Tunnel (レイヤ 2 プロトコルトンネル)

レイヤ2プロトコルトンネリングポートを設定します。

L2 Features > L2 Protocol Tunnel の順にメニューをクリックし、以下の画面を表示します。

2 Protocol Tunn	el Global Settings L2 Proto	col Tunnel Port Setting	s			
CoS for Encapsu Drop Threshold (	lated Packets 5 100-20000) 0		] Default ] Default			Apply
Action Add 🔽	Tunneled Protocol	Protocol MAC 01-00-0C-CC-C	CC-CC	MAC Address	]	Apply
	Protocol		Drop Counter		Tunneling Address	_
GVRP			0		01-05-5D-00-00-21	
STP			0	0 01-05-5D-00-00		
01-00-0C-CC-CC			0		01-05-5D-00-00-10	
01-00-0C-CC-CD			0		01-05-5D-00-00-11	

図 8-67 Layer 2 Protocol Tunneling(L2 Protocol Tunnel Global Settings)画面

画面に表示される項目:	
項目	説明
CoS for Encapsulated Packets	カプセル化されたパケットの CoS 値(0-7)を指定します。「Default」を指定すると初期値を指定します。
Drop Threshold	破棄しきい値を指定します。100-20000 で指定可能です。初期値は「0」です。L2 プロトコルパケットのトンネ リングはパケットのカプセル化、非カプセル化、フォワーディングに CPU 処理容量を消費します。本オプション を使用することにより、システムにより処理される全L2 プロトコルパケットの数にしきい値を設け、消費され る CPU プロセス帯域を制限します。パケットの最大値がしきい値を超えた場合、超えた分のパケットは破棄され ます。「Default」を指定すると初期値を使用します。
Action	実行する動作を指定します。「Add」「Delete」から指定できます。指定のプロトコルへ / からの L2PT トンネリン グマルチキャストアドレスを追加 / 削除します。
Tunneled Protocol	<ul> <li>トンネルプロトコルを選択します。このプルダウンメニューでは以下のオプションを表示します。</li> <li>STP - 設定のアドレスに STP パケットをトンネルします。</li> <li>GVRP - 設定のアドレスに GVRP パケットをトンネルします。</li> <li>MAC - 指定の宛先アドレス付きのプロトコルパケットを設定のアドレスにトンネルします。</li> <li>All - 設定のアドレスに全パケットをトンネルします。</li> </ul>
Protocol MAC	トンネルプロトコルに MAC 選択時に トンネルする L2 プロトコルパケットの送信先 MAC アドレスを指定します。 現時点では、MAC アドレスは、01-00-0C-CC-CC-CC または 01-00-0C-CC-CD です。
MAC Address	指定のプロトコルをトンネルする MAC アドレスを入力します。この MAC アドレスはリザーブされたものや、他のプロトコルで使用のものは指定できません。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

## L2 Protocol Tunnel Port Setting タブをクリックし、次の画面を表示します。

rotocol T	Funnel Globa	Settings L2 Protocol T	unnel Port Settings	1				
t F	From Port	To Port	Action	Туре	Tunneled Protocol	Protocol MAC	Threshold	
~	eth1/0/1	✓ eth1/0/1	✓ Add ✓	None 🗸	GVRP 🗸	01-00-0C-CC-CC-		Apply
t 1 Settin	ngs							Clear Al
Port	Protocol	Shutdown Threshold	Drop Threshold	Encapsul	ation Counter	Decapsulation Counter	Drop Counter	
410100	avro				0	0	0	Class

図 8-68 Layer 2 Protocol Tunneling (L2 Protocol Tunnel Port Settings) 画面

画面に表示される項目	:
------------	---

項目	説明
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。
Action	実行する動作を指定します。「Add」「Delete」から指定できます。
Туре	ポートタイプを指定します。「None」「Shutdown」および「Drop」が選択可能です。
Tunneled Protocol	<ul> <li>トンネルプロトコルを選択します。このプルダウンメニューでは以下のオプションを表示します。</li> <li>STP - 設定のアドレスに STP パケットをトンネルします。</li> <li>GVRP - 設定のアドレスに GVRP パケットをトンネルします。</li> <li>MAC - 指定の宛先アドレス付きのプロトコルパケットを設定のアドレスにトンネルします。</li> <li>All - 設定のアドレスに全パケットをトンネルします。</li> </ul>
Protocol MAC	トンネルプロトコルに Protocol MAC 選択時に トンネルする L2 プロトコルパケットの送信先 MAC アドレスを指定します。現時点では、MAC アドレスは、01-00-0C-CC-CC てまたは 01-00-0C-CC-CD です。
Threshold	「Type」で「Shutdown」「Drop」を指定した場合、しきい値(1-4096)を入力します。

「Apply」ボタンをクリックして各セクションで行った変更を適用します

「Clear」をクリックすると入力したエントリをクリアします。

「Clear All」をクリックすると入力したエントリを全てクリアします。

# L2 Multicast Control (L2 マルチキャストコントロール)

IGMP (Internet Group Management Protocol) Snooping 機能を始めとした L2 Multicast Control (L2 マルチキャストコントロール)の設定を行います。

## IGMP Snooping (IGMP Snooping の設定)

IGMP(Internet Group Management Protocol)Snooping 機能を利用すると、スイッチはネットワークステーションまたはデバイスと IGMP ホスト 間で送信される IGMP クエリと IGMP レポートを認識するようになります。また、スイッチを通過する IGMP メッセージの情報に基づいて、指定し たデバイスに接続するポートをオープン / クローズできるようになります。

### IGMP Snooping Settings (IGMP Snooping 設定)

IGMP Snooping 設定をグローバルに有効または無効にします。

IGMP Snooping 機能を利用するためには、まず、画面上にある「IGMP Snooping Global Settings」でスイッチ全体を有効にする必要があります。その後、 対応する「Edit」ボタンをクリックして、各 VLAN に詳細な設定を行います。

IGMP Snooping を有効にすると、スイッチはデバイスと IGMP ホスト間で送信される IGMP メッセージに基づいて、特定のマルチキャストグループ メンバに接続するポートをオープンまたはクローズできるようになります。スイッチは IGMP メッセージをモニタして、マルチキャストパケットを 要求しているホストがもう存在していないと判断すれば、マルチキャストパケットの送信を停止します。

L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Settings の順にクリックし、以下の画面を表示します。

IGMP Snooping Settings			
Global Settings			
Global State	OEnabled  OEnabled		Apply
VLAN Status Settings			
VID (1-4094)	OEnabled  OEnabled		Apply
IGMP Snooping Table			
VID (1-4094)			Find Show All
Total Entries: 1			
VID	VLAN Name	Status	
1	default	Enabled	Show Detail Edit
			1/1 < < 1 > > Go

図 8-69 IGMP Snooping Settings 画面

画面に表示される項目:

項目	説明			
	Global Setting			
Global State	IGMP Snooping の有効 / 無効を設定します。			
	・ Enabled - デバイスで IGMP Snooping を有効にします。			
	• Disabled - デバイスで IGMP Snooping を無効に設定します。(初期値)			
	VLAN Status Settings			
VID	VLAN 上の IGMP Snooping を有効 / 無効にし、VLAN を識別する VLAN ID を指定します。			
・ Enabled - VLAN を有効にします。				
	<ul> <li>Disabled - VLAN を無効に設定します。(初期値)</li> </ul>			
IGMP Snooping Table				
VID	IGMP Snooping Table 上の VLAN を表示させるための VLAN ID を指定します。			
	・ Find - 指定の VLAN ID を入力して指定のエントリを表示します。			
	・ Show All - IGMP Snooping Table 上のすべてのエントリを表示します。			

「Find」をクリックして指定の VLAN ID を入力して指定のエントリを表示します。

「Show All」をクリックして IGMP Snooping Table 上のすべてのエントリを表示します。

### ■ IGMP Snooping VLAN の詳細情報表示

関連する VLAN エントリの「Show Detail」ボタンをクリックし、指定 VLAN の詳細情報を表示します。

IGMP Snooping VLAN Para	neters
ICMD Secondary VII AN Deservations	
- IGMP Shooping VLAN Parameters -	
VID	1
Status	Enabled
Minimum Version	v1
Fast Leave	Disabled (host-based)
Report Suppression	Disabled
Suppression Time	10 seconds
Querier State	Disabled
Query Version	v3
Query Interval	125 seconds
Max Response Time	10 seconds
Robustness Value	2
Last Member Query Interval	1 seconds
Proxy Reporting	Disabled Source Address (0.0.0.)
Rate Limit	0
Ignore Topology Change	Disabled
	Modify

図 8-70 IGMP Snooping VLAN Parameters 画面

本画面の「Modify」をクリックすると「IGMP Snooping VLAN Settings」画面へ移動し、IGMP Snooping の VLAN 設定を行うことができます。

#### ■ IGMP Snooping 機能の詳細設定

「IGMP Snooping Settings」で関連する VLAN エントリの「Edit」ボタンをクリックし、以下の画面を表示して各 VLAN に対して詳細な設定を行います。

IGMP Snooping VLAN Setting	S
IGMP Snooping VLAN Settings	
VID (1-4094)	1
Status	Enabled      Disabled
Minimum Version	
Fast Leave	CEnabled  Disabled
Report Suppression	OEnabled ODisabled
Suppression Time (1-300)	10
Querier State	OEnabled ODisabled
Query Version	3
Query Interval (1-31744)	125 sec
Max Response Time (1-25)	10 sec
Robustness Value (1-7)	2
Last Member Query Interval (1-25)	1 sec
Proxy Reporting	OEnabled ODisabled Source Address
Rate Limit (1-1000)	No Limit
Ignore Topology Change	OEnabled ODisabled
	Apply

図 8-71 IGMP Snooping VLAN Settings 画面

項目	説明
VID	IGMP Snooping 設定を変更する VLAN を識別する VLAN ID を表示します。
Status	指定した VLAN への IGMP Snooping 機能を「Enabled」(有効)/「Disabled」(無効)にします。初期値は無効です。
Minimum Version	VLAN に許可された IGMP ホストの最小バージョンを選択します。
Fast Leave	「Enabled」(有効)にすると、Fast Leave 機能が有効になります。この機能が有効になると、システムが最新メンバから IGMP done メッセージを受信すると、メンバシップはただちに失効します。Fast Leave が有効な場合、指定のキューは生成されません。
Report Suppression	特定の VLAN への IGMP スヌーピングレポートの抑制を「Enabled」(有効)/「Disabled」(無効)にします。 レポートサスペンション機能は「IGMPv1」「IGMPv2」トラフィックでのみ機能します。 有効になるとホストによるレポートの送信は抑制されます。抑制は抑制時間(Suppression Time)を過ぎるまで続きます。
Suppression Time	スヌーピングレポートの抑制時間を設定します。1 から 300(秒)で設定可能です。

## 画面に表示される項目:

項目	説明	
Querier State	「Enabled」(有効)にすると IGMP Query パケットを送信可能になります。初期値は「Disabled」(無効)です。	
Query Version	IGMP スヌーピングクエリアに送信されるクエリパケットのバージョンを選択します。「1」「2」「3」から選択可能です。	
Query Interval	IGMP query 送信間隔(秒)。1-31744 の範囲から指定します。初期値は 125 です。	
Max Response Time (1-25)	IGMP response report を送信するまでの最大時間(秒)。1-25 の範囲から指定します。初期値:10(秒)	
Robustness Value (1-7)	サブネットで発生が予想されるパケットロスに対する耐性を1~7の数値から設定します。 初期値:2	
Last Member Query Interval	Leave Group メッセージを受け取った時に送信する Group-Specific Membership Query の Max Response Time 欄に設	
(1-25)	定する値(Last Member Query Interval)。また、同 Query の送信間隔でもあります。初期値は 1 です。	
Proxy Reporting	プルダウンメニューを使用して、本機能を「Enabled」(有効)/「Disabled」(無効)にします。	
Source Address	プロキシレポーティングの送信元 IP アドレスを指定します。	
Rate Limit	レートリミット(1-1000)を指定します。「No Limit」を指定すると本プロファイルでのレートリミットをなくします。	
Ignore Topology Change	「Ignore Topology Change」を「Enabled」(有効)/「Disabled」(無効)にします。 有効にするとトポロジの変更は無視されます。	

設定を変更する際は、必ず「Apply」ボタンをクリックし設定内容を適用してください。

注意 Fast-Leave を設定したポート配下に複数の端末を配置しないでください。

注意 IGMP Snooping について、fast-leave は IGMPv2 のみサポートしています。

## IGMP Snooping AAA Settings(IGMP Snooping AAA 設定)

IGMP Snooping AAA 設定を指定、表示します。

L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping AAA Settings の順にクリックし、以下の画面を表示します。



図 8-72 IGMP Snooping AAA Settings 画面

画面に表示される項目	:
------------	---

項目	説明	
	IGMP Snooping AAA Settings	
Unit	設定を行うユニットを指定します。	
From Port / To Port	設定するポートの始点 / 終点を設定します。	
Authentication	認証を「Enabled」(有効)/「Disabled」(無効)にします。 「IGMP join メッセージ」認証機能の有効 / 無効において使用します。有効時にクライアントがグループへの参 加を希望する場合、システムにより認証が実行されます。	
Accounting	アカウンティングを「Enabled」(有効)/「Disabled」(無効)にします。 リスナーによる IGMP グループへの参加時にアカウンティングの有効 / 無効を指定します。有効時にクライア ントがグループへの参加する場合、アカウンティングメッセージが RADIUS に送信されます。	
IGMP Snooping AAA Table		
Unit	設定を行うユニットを指定します。	
Port	設定を行うポートを指定します。	

「Find」をクリックして指定の VLAN ID を入力して指定のエントリを表示します。

「Show All」をクリックして IGMP Snooping Table 上のすべてのエントリを表示します。

## IGMP Snooping Groups Settings (IGMP Snooping グループ設定)

「IGMP Snooping Group Table」を表示します。IGMP Snooping 機能では、スイッチを通過する IGMP パケットからマルチキャストグループ IP アドレスと対応する MAC アドレスを読み取ることができます。

L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Group Settings をクリックして表示します。

IGMP Snooping Gro	ups Settings		
IGMP Snooping Static Gr	oups Settings		
VID (1-4094)	Group Address Unit	From Port         To Port           eth1/0/1         eth1/0/1	Apply     Delete
VID (1-4094)	Group Address		Find Show All
Total Entries: 1			
VID	Grou	p Address	Ports
1	22	4.0.1.0	1/0/10
			1/1  < < 1 > >  Go
IGMP Snooping Groups T	able		
VID (1-4094)	Group Address		
۲	0 · · ·	Detail	Find Show All
Total Entries: 0			
VID	Gr	oup Address	Ports

図 8-73 IGMP Snooping Groups Settings 画面

以下の項目を使用して、設定します。

### IGMP Snooping Static Groups Settings (IGMP スヌーピングスタティックグループ設定)

項目	説明
	IGMP Snooping Static Groups Settings
VID	登録または削除するマルチキャストグループの VLAN ID(1-4094)を入力します。
Group Address	登録または削除するマルチキャストグループの IP アドレスを入力します。
Unit	設定するユニットを選択します。
From Port / To Port	設定するポートの範囲を設定します。
VID	チェックを入れ、検索するマルチキャストグループの VLAN ID(1-4094)を入力します。
Group Address	チェックを入れ、検索するマルチキャストグループの IP アドレスを入力します。

設定を変更する際は、必ず「Apply」ボタンをクリックし設定内容を適用します。

「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。「Show All」ボタンをクリックして、すべての定義済みエントリを表示します。

#### IGMP Snooping Groups Table (IGMP スヌーピンググループテーブル)

項目	説明
	IGMP Snooping Groups Table
VID	チェックを入れ、検索するマルチキャストグループの VLAN ID を入力します。
Group Address	チェックを入れ、検索するマルチキャストグループの IP アドレスを入力します。
Detail	IGMP グループの詳細情報を表示します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

「Show All」ボタンをクリックして、すべての定義済みエントリを表示します。

「Show Detail」指定のエントリの詳細情報を表示します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

## IGMP Snooping Filter Settings(IGMP Snooping フィルタ 設定)

IGMP Snooping フィルタの設定を行います。

L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Filter Settings をクリックして表示します。

IGMP Snoop	ing Filter Set	ttings		_		
IGMP Snooping	Rate Limit Settir	ngs				
Unit		From Port	To Port		Limit Number (1-1000)	
1	~	eth1/0/1	✓ eth1/0/1	~	No	Limit
Action		VID (1-4094)				
Port	~					Apply
IGMP Snooping	Limit Settings					
Unit		From Port	To Port		Limit Number (1-8192)	
1	~	eth1/0/1	<ul> <li>eth1/0/1</li> </ul>	~		
Exceed Action		Except ACL Name			VID (1-4094)	
Default	~	32 chars	Please Select			Apply
Unit		From Port	To Port		VID (1-4094)	
1	~	eth1/0/1	✓ eth1/0/1	~		Delete
Access Group	Settings					
Unit		From Port	To Port		Action	
1	~	eth1/0/1	✓ eth1/0/1	~	Add	
ACL Name			VID (1-40	94)		
32 chars	Pleas	e Select				Apply
IGMP Snooping	Filter Table					
Unit		From Port	To Port			
1	~	eth1/0/1	v eth1/0/1	~		Find Show All
Total Entries:	1					
	Po	ort		R	ate Limit	

図 8-74 IGMP Snooping Filter Settings 画面

#### 以下の項目を使用して、設定します。

## IGMP Snooping Rate Limit Settings (IGMP スヌーピングレートリミット設定)

項目	説明		
Unit	設定するユニットを選択します。		
From Port / To Port	設定するポートの範囲を設定します。		
Limit Number	制限する数を指定します。指定のインタフェースでスイッチがプロセス可能な IGMP コントロールパケットのレートを指定します。1-1000(パケット / 秒)で指定可能です。「No Limit」で制限を設定しません。		
Action	実行するインタフェースを指定します。「Port」「VLAN」から指定可能です。		
VID	「Action」で「VLAN」を選択すると表示されます。トランクポートの VLAN に受信するパケットに対して、 フィルタします。VLAN を 1-4094 から指定します。		

設定を変更する際は、必ず「Apply」ボタンをクリックし設定内容を適用します。

### IGMP Snooping Limit Settings (IGMP スヌーピングリミット設定)

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	設定するポートの範囲を設定します。
Limit Number	制限する数を指定します。生成される IGMP キャッシュエントリ数の制限をします。1-8192 で指定可能です。
Exceed Action	しきい値を超過した場合の動作について指定します。本パラメータでは制限が超過した場合の、新規学習 グループの取り扱いに対しての動作を指定します。 • Default - 初期動作を指定します。 • Drop - 新規グループは破棄されます。 • Replace - 新規グループは古いグループと代替されます。
Except ACL Name	通常のIPアクセスリストを指定します。本アクセスリストに許可されたグループ(*,G)は制限から外れます。 グループ(*,G)の許可にはアクセスリストエントリの送信元アドレスに「any」、宛先アドレスに「G」を指 定します。32字以内で指定可能です。「Please Select」をクリックすることにより、既に存在するアクセス リストから今回の設定に有効なアクセスリストを見つけることができます。
VID	トランクポートの VLAN に受信するパケットに対して、フィルタします。VLAN を 1-4094 から指定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

#### Access Group Settings(アクセスグループ設定)

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	設定するポートの範囲を設定します。
Action	入力した情報に基づき新しいエントリの追加「Add」または、既存エントリの削除「Delete」を行います。
ACL Name	通常の IP アクセスリストを指定します。グループ (*,G) の許可にはアクセスリストエントリの送信元アドレスに「any」、宛先アドレスに「G」を指定します。32 字以内で指定可能です。「Please Select」をクリックすることにより、既に存在するアクセスリストから今回の設定に有効なアクセスリストを見つけることができます。
VID	設定する VLAN を指定します。VLAN を 1-4094 から指定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし設定内容を適用します。

#### IGMP Snooping Filter Table (IGMP スヌーピングフィルタ設定)

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	設定するポートの範囲を設定します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

「Show All」ボタンをクリックして、すべての定義済みエントリを表示します。

「Show Detail」指定のエントリの詳細情報を表示します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

#### Please Select をクリックすると次の画面が表示されます。

	ID	ACL Name	ACL Type
0	1	SI-ACL	Standard IP ACL
			1/1 < < 1 > >

図 8-75 Please Select 画面

ACLを選択し「**OK**」をクリックします。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

Show Detail をクリックすると次の画面が表示されます。

P Snooping Detail F	ilter Table	
al Entries: 1		
	Port	: eth1/0/10
VID	Access Group	Groups/Channel Limit
	Not Configured	Not Configured

図 8-76 Show Detail 画面

「Back」をクリックすると前のページに戻ります。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

## IGMP Snooping Mrouter Settings(IGMP Snooping マルチキャストルータ設定)

指定インタフェースをマルチキャストルータポートへの移行、もしくはマルチキャストルータポートへの移行禁止に設定します。

L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Mrouter Settings をクリックして表示します。

IGMP Snooping	Mrouter Setting	S	_	_	_	_	_	_	_	_	-
IGMP Snooping Mrou	iter Settings										
VID (1-4094)	Configuration		Unit		From Port		To Port				
	Port	~	1	~	eth1/0/1	~	eth1/0/1	~	Apply	Dele	te
Total Entries: 1									Tild	3110W	
VID						ŀ	Ports				
1						1/0/1	3 (Static)				
								1	1/1 < < 1	> >	Go

図 8-77 IGMP Snooping Mrouter Settings 画面

画面には以下の項目があります。

### IGMP Snooping Mrouter Settings (IGMP スヌーピングマルチキャストルータ設定)

項目	説明			
IGMP Snooping Mrouter Settings				
VID	VLAN ID を入力します。			
Configuration	<ul> <li>ポートの設定を行います。「Port」「Forbidden Port」から選択します。</li> <li>Port - マルチキャストが有効なルータと接続するポート範囲を設定します。プロトコルに関係なくマルチキャスト有効ルータに全てのパケットが届くことを確実にします。</li> <li>Forbidden Router Port - マルチキャストが有効なルータと接続しないポート範囲を設定します。禁止されたルータポートはルーティングパケットを送信しません。</li> </ul>			
Unit	設定するユニットを選択します。			
From Port / To Port	設定するポートの範囲を設定します。			
コーウィーホーティーのローシー				

設定を変更する際は、必ず「Apply」ボタンをクリックし設定内容を適用します。

「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。

### IGMP Snooping Mrouter Table (IGMP スヌーピングマルチキャストルータテーブル)

坦日					
IGMP Snooping Mrouter Table					
VID	VLAN ID を入力します。				

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。「Show All」ボタンをクリックして、すべての定義済みエント リを表示します。
## IGMP Snooping Statistics Settings(IGMP Snooping 統計設定)

現在の IGMP Snooping の統計情報を表示します。

#### L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Statistics Settings の順にメニューをクリックし、以下の画面を表示します。



図 8-78 IGMP Snooping Statistics Settings 画面

以下の項目が表示されます。

#### IGMP Snooping Statistics Settings (IGMP スヌーピング統計設定)

項目	説明
Statistics	インタフェースを選択します。「All」「VLAN」「Port」から選択します。
VID	VLAN ID1 から 4094 の間で指定します。「Statistics」で「VLAN」を選択すると設定可能になります。
Unit	設定するユニットを選択します。「Statistics」で「Port」を選択すると設定可能になります。
From Port / To Port	設定するポートの範囲を設定します。「Statistics」で「Port」を選択すると設定可能になります。

「Clear」をクリックすると表示された統計情報がクリアされます。

## IGMP Snooping Statistics Table (IGMP スヌーピング統計テーブル)

項目	説明
Find Type	インタフェースを選択します。「VLAN」「Port」から選択します。
VID	VLAN ID1 から 4094 の間で指定します。「Find Type」で「VLAN」を選択すると設定可能になります。
Unit	設定するユニットを選択します。「Find Type」で「Port」を選択すると設定可能になります。
From Port / To Port	設定するポートの範囲を設定します。「Find Type」で「Port」を選択すると設定可能になります。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。「Show All」ボタンをクリックして、すべての定義済みエントリを表示します。

## MLD Snooping (MLD スヌーピング)

Multicast Listener Discovery(MLD)Snooping は、IPv4の IGMP Snooping と同じ機能を持つ、IPv6 用のマルチキャストトラフィック制御機能です。 VLAN 上でマルチキャストデータを要求するポートを検出するために使用されます。MLD Snooping では、所定の VLAN 上のすべてのポートにマル チキャストトラフィックを流すのではなく、要求元ポートとマルチキャストの送信元によって生成される MLD クエリと MLD レポートを使用して、 データを受信したいポートに対してのみ、マルチキャストデータを転送します。

MLD Snooping は、エンドノードと MLD ルータとの間で交換される MLD 制御パケットのレイヤ3部分を調べることでパケットを処理します。スイッ チは、ルートがマルチキャストトラフィックをリクエストしていることを検出すると、そのルートに直接接続されているポートを IPv6 マルチキャ ストテーブルに追加し、そのポートにマルチキャストトラフィックを転送する処理を開始します。マルチキャストルーティングテーブル内のエント リには、該当ポートや VLAN ID、関連する IPv6 マルチキャストグループアドレスが記録され、このポートはアクティブな Listening ポートと見なさ れます。アクティブな Listening ポートのみがマルチキャストグループデータを受信します。

#### MLD コントロールメッセージ

MLD Snooping を使用するデバイス間で以下の MLD コントロールメッセージが交換されます。これらのメッセージは、130、131、132 および 143 でラベル付けされた 4 つの ICMPv6 パケットヘッダによって定義されています。

- Multicast Listener Query IPv4の IGMPv2 Host Membership Query (HMQ) に相当するメッセージです。ルータは ICMPv6 パケットヘッダ内 に 130 とラベル付けされた本メッセージを送信し、マルチキャストデータをリクエストしているリンクがあるかどうか問い合わせます。ルー タが送信する MLD クエリメッセージには 2 つのタイプがあります。General Query はリンク上のすべての Listening ポートに対し送信され、 Multicast Specific Query は、特定のマルチキャストアドレスに対して送信されます。この 2 種類のメッセージは、IPv6 ヘッダ内のマルチキャス ト宛先アドレス及び Multicast Listener クエリメッセージ内のマルチキャストアドレスによって区別されます。
- Multicast Listener Report IGMPv2 の Host Membership Report (HMR) に相当するメッセージです。Listening ポートは、Multicast Listener ク エリメッセージへの応答として、ICMPv6 パケットヘッダ内に 131 とラベル付けされた本メッセージを送信し、マルチキャストアドレスからマ ルチキャストデータを受信する希望があることを伝えます。
- 3. Multicast Listener Done IGMPv2の Leave Group Message に相当するメッセージです。マルチキャスト Listening ポートは、ICMPv6 パケット ヘッダ内に 132 とラベル付けされた本メッセージを送信し、特定のマルチキャストグループアドレスからのマルチキャストデータの受信を停止 すること、つまり、このアドレスからのマルチキャストデータが "done"(完了)となった旨を伝えます。スイッチが本メッセージを受信すると、 この Listening ホストには特定のマルチキャストグループアドレスからのマルチキャストトラフィックを送信しなくなります。
- 4. Multicast Listener Report Version2 IGMPv3 の Host Membership Report (HMR) に相当するメッセージです。Listening ポートは、Multicast Listener クエリメッセージへの応答として、ICMPv6 パケットヘッダ内に 143 とラベル付けされた本メッセージを送信し、マルチキャストアドレスからマルチキャストデータを受信する希望があることを伝えます。

## MLD Snooping Settings (MLD スヌーピング設定)

MLD Snooping 設定を有効または無効にします。

## L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Settings の順にクリックし、以下の画面を表示します。

MLD Snooping Settings			
Global Settings			
Global State	OEnabled  OEnabled		Apply
VLAN Status Settings			
VID (1-4094)	OEnabled  OEnabled		Apply
MLD Snooping Table			
VID (1-4094)			Find Show All
Total Entries: 1			
VID	VLAN Name	Status	
1	default	Enabled	Show Detail Edit
			1/1 K < 1 > > Go

図 8-79 MLD Snooping Settings 画面

#### 画面に表示される項目:

項目	説明				
	Global Setting				
Global State	<ul> <li>MLD Snooping の有効 / 無効を設定します。</li> <li>Enabled - デバイスで MLD Snooping を有効にします。</li> <li>Disabled - デバイスで MLD Snooping を無効に設定します。(初期値)</li> </ul>				
	VLAN Status Settings				
VID	<ul> <li>VLAN 上の MLD Snooping を有効 / 無効にし、VLAN を識別する VLAN ID を指定します。</li> <li>Enabled - VLAN を有効にします。</li> <li>Disabled - VLAN を無効に設定します。(初期値)</li> </ul>				
MLD Snooping Table					
VID	<ul> <li>MLD Snooping Table 上の VLAN を表示させるための VLAN ID を指定します。</li> <li>Find - 指定の VLAN ID を入力して指定のエントリを表示します。</li> <li>Show All - MLD Snooping Table 上のすべてのエントリを表示します。</li> </ul>				

「Find」をクリックして指定の VLAN ID を入力して指定のエントリを表示します。 「Show All」をクリックして MLD Snooping Table 上のすべてのエントリを表示します。

## MLD Snooping VLAN の詳細情報表示

関連する VLAN エントリの「Show Detail」ボタンをクリックし、指定 VLAN の詳細情報を表示します。

MLD Snooping VLAN Pa	rameters
MLD Snooping VLAN Parameter	\$ —
VID	1
Status	Enabled
Minimum Version	v1
Fast Leave	Disabled (host-based)
Report Suppression	Disabled
Suppression Time	10 seconds
Proxy Reporting	Disabled Source Address (::)
Mrouter Port Learning	Enabled
Querier State	Disabled
Query Version	v2
Query Interval	125 seconds
Max Response Time	10 seconds
Robustness Value	2
Last Listener Query Interval	1 seconds
Rate Limit	0
Ignore Topology Change	Disabled
	Modify

本画面の「Modify」をクリックすると「MLD Snooping VLAN Settings」画面へ移動し、MLD Snooping の VLAN 設定を行うことができます。 MLD Snooping 機能の詳細設定

「MLD Snooping Settings」で関連する VLAN エントリの「Edit」ボタンをクリックし、以下の画面を表示して各 VLAN に対して詳細な設定を行います。

MLD Snooping VLAN Settin	gs	
MLD Snooping VLAN Settings		
VID (1-4094)	1	
Status	Enabled Disabled	
Minimum Version		
Fast Leave	CEnabled ODisabled	
Report Suppression	OEnabled  OEnabled	
Suppression Time (1-300)	10	
Proxy Reporting	OEnabled ODisabled Source Address	
Mrouter Port Learning	Enabled Obisabled	
Querier State	OEnabled  OEnabled	
Query Version	2	
Query Interval (1-31744)	125 sec	
Max Response Time (1-25)	10 sec	
Robustness Value (1-7)	2	
Last Listener Query Interval (1-25)	1 sec	
Rate Limit (1-1000)	✓ No Limit	
Ignore Topology Change	OEnabled  OEnabled	
	Apply	

図 8-81 MLD Snooping VLAN Settings 画面

画面に表示される項目:
-------------

項目	説明
VID	MLD Snooping 設定を変更する VLAN を識別する VLAN ID を表示します。
State	指定した VLAN への MLD Snooping 機能を「Enabled」(有効)/「Disabled」(無効)にします。初期値は無効です。
Minimum Version	VLAN に許可された MLD ホストの最小バージョンを選択します。1-2 で選択します。
Fast Leave	「Enabled」(有効)にすると、Fast Leave 機能が有効になります。この機能が有効になると、スイッチが MLD Leave Report パケットを受信する時、マルチキャストグループのメンバは(Last Member Query Time の失効を待たずに) 直ちにグループから脱退します。初期値は「Disabled」(無効)です。
Report Suppression	特定の VLAN への MLD スヌーピングレポートの抑制を「Enabled」(有効)/「Disabled」(無効)にします。 レポートサスペンション機能は「MLDv1」「MLDv2」トラフィックでのみ機能します。 有効になるとホストによるレポートの送信は抑制されます。抑制は抑制時間 (Suppression Time)を過ぎるまで続きます。
Suppression Time	スヌーピングレポートの抑制時間を設定します。1 から 300(秒)で設定可能です。
Proxy Reporting	プルダウンメニューを使用して、本機能を「Enabled」(有効)/「Disabled」(無効)にします。
Source Address	プロキシレポーティングの送信元 IP アドレスを指定します。
Mrouter Port Learning	マルチキャストルータポートラーニングを「Enabled」(有効)/「Disabled」(無効)にします。
Querier State	「Enabled」(有効)にすると MLD Query パケットを送信可能になります。初期値は「Disabled」(無効)です。
Query Version	MLD スヌーピングクエリアに送信されるクエリパケットのバージョンを選択します。「1」「2」から選択可能です。
Query Interval	MLD query 送信間隔(秒)。1-31744 の範囲から指定します。初期値は 125 です。
Max Response Time (1-25)	MLD response report を送信するまでの最大時間(秒)。1-25 の範囲から指定します。初期値は 10(秒)です。
Robustness Value (1-7)	サブネットで発生が予想されるパケットロスに対する耐性を1~7の数値から設定します。 初期値:2
Last Listener Query Interval	Leave Group メッセージを受け取った時に送信する Group-Specific Membership Query の Max Response Time 欄に設 定する値(Last Listener Query Interval)。また、同 Query の送信間隔でもあります。初期値は 1 です。
Rate Limit	レートリミット(1-1000)を指定します。「No Limit」を指定すると本プロファイルでのレートリミットをなくします。
Ignore Topology Change	「Ignore Topology Change」を「Enabled」(有効)/「Disabled」(無効)にします。 有効にするとトポロジの変更は無視されます。

設定を変更する際は、必ず「Apply」ボタンをクリックし設定内容を適用してください。

## MLD Snooping Groups Settings(MLD Snooping グループ設定)

「MLD Snooping Group Table」を表示します。MLD Snooping 機能では、スイッチを通過する MLD パケットからマルチキャストグループ IP アドレスと対応する MAC アドレスを読み取ることができます。

L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Groups Settings をクリックして表示します。

MLD Snooping Gro	ups Settings	_			_		
MLD Snooping Static Gro	oups Settings						
VID (1-4094)	Group Address	Unit	~	From Port eth1/0/1	To Port eth1/0/1	~	Apply Delete
VID (1-4094)	Grou	p Address F11::11					Find Show All
Total Entries: 1							
VID			Group	Address			Ports
1			FF1	1::11			1/0/10
							1/1  < < 1 > >  Go
MLD Snooping Groups T	able						
VID (1-4094)	Group	o Address F11::11		Detail			Find Show All
Total Entries: 0							
VID			Gro	up Address			Ports

図 8-82 MLD Snooping Groups Settings 画面

以下の項目を使用して、設定します。

#### ■ MLD Snooping Static Group Settings (MLD スヌーピングスタティックグループ設定)

項目	説明			
	MLD Snooping Static Groups Settings			
VID	登録または削除する IPv6 マルチキャストグループの VLAN ID(1-4094)を入力します。			
Group Address	登録または削除する IPv6 マルチキャストグループの IPv6 アドレスを入力します。			
Unit	設定するユニットを選択します。			
From Port / To Port	設定するポートの範囲を設定します。			
VID	チェックを入れ、検索するマルチキャストグループの VLAN ID を入力します。			
Group Address	チェックを入れ、検索するマルチキャストグループの IPv6 アドレスを入力します。			

設定を変更する際は、必ず「Apply」ボタンをクリックし設定内容を適用します。

「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。「Show All」ボタンをクリックして、すべての定義済みエントリを表示します。

#### ■ MLD Snooping Groups Table (MLD スヌーピンググループテーブル)

項目	説明			
MLD Snooping Groups Table				
VID	チェックを入れ、検索するマルチキャストグループの VLAN ID(1-4094)を入力します。			
Group Address	チェックを入れ、検索するマルチキャストグループの IPv6 アドレスを入力します。			
Detail	MLD グループの詳細について表示します。			

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。「Show All」ボタンをクリックして、すべての定義済みエントリを表示します。

## MLD Snooping Filter Settings (MLD Snooping フィルタ Settings)

MLD Snooping フィルタの設定を行います。

L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Filter Settings をクリックして表示します。

MLD Snooping Filter	Settings			
MLD Snooping Rate Limit	Settings			,
Unit	From Port	To Port	Limit Number (1-1000)	
1 V	eth1/0/1	eth1/0/1	No Limit	
Port V	VID (1-4054)			Apply
MLD Snooping Limit Settin	igs			
Unit	From Port	To Port	Limit Number (1-4096)	
1 🗸	eth1/0/1	eth1/0/1		
Exceed Action	Except ACL Name		VID (1-4094)	
Default 🗸	32 chars Pl	ease Select		Apply
Unit	From Port	To Port	VID (1-4094)	
1	eth1/0/1	eth1/0/1		Delete
Access Group Settings				
Linit	From Port	To Port	Action	
	eth1/0/1	eth1/0/1	Add	
ACL Name		VID (1-4094)		
32 chars	Please Select			Apply
MLD Snooping Filter Table				
Unit	From Port	To Port		
1 🗸	eth1/0/1	eth1/0/1		Find Show All
Total Entries: 1				
	Port	R	ate Limit	
	eth1/0/1	, , , , , , , , , , , , , , , , , , ,	500pps	Show Detail
				Show Octain

図 8-83 MLD Snooping Filter Settings 画面

#### 以下の項目を使用して、設定します。

#### ■ MLD Snooping Rate Limit Settings (MLD スヌーピングレートリミット設定)

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	設定するポートの範囲を設定します。
Limit Number	制限する数を指定します。指定のインタフェースでスイッチがプロセス可能な MLD コントロールパケットのレートを指定します。1-1000(パケット / 秒)で指定可能です。「No Limit」で制限を設定しません。
Action	実行するインタフェースを指定します。「Port」「VLAN」から指定可能です。
VID	「Action」で「VLAN」を選択すると表示されます。トランクポートの VLAN に受信するパケットに対して、 フィルタします。VLAN を 1-4094 から指定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし設定内容を適用します。

## ■ MLD Snooping Limit Settings (MLD スヌーピングリミット設定)

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	設定するポートの範囲を設定します。
Limit Number	制限する数を指定します。生成される MLD キャッシュエントリ数の制限をします。1-4096 で指定可能です。
Exceed Action	しきい値を超過した場合の動作について指定します。本パラメータでは制限が超過した場合の、新規学習 グループの取り扱いに対しての動作を指定します。 • Default - 初期動作を指定します。 • Drop - 新規グループは破棄されます。 • Replace - 新規グループは古いグループと代替されます。
Except ACL Name	通常のIPアクセスリストを指定します。本アクセスリストに許可されたグループ(*,G)は制限から外れます。 グループ(*,G)の許可にはアクセスリストエントリの送信元アドレスに「any」、宛先アドレスに「G」を指 定します。32字以内で指定可能です。「Please Select」をクリックすることにより、既に存在するアクセス リストから今回の設定に有効なアクセスリストを見つけることができます。
VID	トランクポートの VLAN に受信するパケットに対して、フィルタします。VLAN を 1-4094 から指定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

## ■ Access Group Settings(アクセスグループ設定)

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	設定するポートの範囲を設定します。
Action	入力した情報に基づき新しいエントリの追加「Add」または、既存エントリの削除「Delete」を行います。
ACL Name	通常の IP アクセスリストを指定します。グループ (*,G) の許可にはアクセスリストエントリの送信元アドレスに「any」、宛先アドレスに「G」を指定します。32 字以内で指定可能です。「Please Select」をクリックすることにより、既に存在するアクセスリストから今回の設定に有効なアクセスリストを見つけることができます。
VID	設定する VLAN を指定します。VLAN を 1-4094 から指定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし設定内容を適用します。

#### ■ MLD Snooping Filter Table (MLD スヌーピングフィルタ設定)

項目	説明					
Unit	設定するユニットを選択します。					
From Port / To Port	設定するポートの範囲を設定します。					

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

「Show All」ボタンをクリックして、すべての定義済みエントリを表示します。

「Show Detail」指定のエントリの詳細情報を表示します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

# Please Select をクリックすると次の画面が表示されます。

	ID	ACL Name	ACL Type
0	11000	SI6-ACL	Standard IPv6 ACL
0	13000	EI6-ACL	Extended IPv6 ACL
			1/1 🔀 < 1 > >

図 8-84 Please Select 画面

ACLを選択し「**OK**」をクリックします。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

Show Detail をクリックすると次の画面が表示されます。

MLD Snooping Det	ail Filter Table	
MLD Snooping Detail Fi	Iter Table	
Total Entries: 1		
	Port	: eth1/0/10
VID	Access Group	Groups/Channel Limit
	Not Configured	Not Configured
		1/1 K < 1 > > Go Back

図 8-85 Show Detail 画面

「Back」をクリックすると前のページに戻ります。 設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

## MLD Snooping Mrouter Settings(MLD Snooping マルチキャストルータ設定)

指定インタフェースをマルチキャストルータポートへの移行、もしくはマルチキャストルータポートへの移行禁止に設定します。

L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Mrouter Settings をクリックして表示します。

MLD Snooping Mrouter Settings								
MLD Snooping Mrouter Settings								
VID (1-4094)     Configuration     Unit     From Port     To Port       Port     1     eth1/0/1     eth1/0/1     Apply								
MLD Snooping Mrouter Table VID (1-4094) Find Show All								
Total Entries: 1								
VID			Ports					
1			1/0/11 (Static)					
				1/1 K < 1 > > Go				

図 8-86 MLD Snooping Mrouter Settings 画面

画面には以下の項目があります。

## MLD Snooping Mrouter Settings (MLD スヌーピングマルチキャストルータ設定)

項目	説明						
	MLD Snooping Mrouter Settings						
VID	VLAN ID を入力します。						
Configuration	<ul> <li>ポートの設定を行います。「Port」「Forbidden Port」「Learn pimv6」から選択します。</li> <li>Port - マルチキャストが有効なルータと接続するポート範囲を設定します。プロトコルに関係なくマルチキャスト有効ルータに全てのパケットが届くことを確実にします。</li> <li>Forbidden Router Port - マルチキャストが有効なルータと接続しないポート範囲を設定します。禁止されたルータポートはルーティングパケットを送信しません。</li> <li>Learn pimv6 - マルチキャストルータポートの自動取得を有効にします。</li> </ul>						
Unit	設定するユニットを選択します。						
From Port / To Port	設定するポートの範囲を設定します。						

設定を変更する際は、必ず「Apply」ボタンをクリックし設定内容を適用します。

「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。

## MLD Snooping Mrouter Table (MLD スヌーピングマルチキャストルータテーブル)

項目	項目 説明						
MLD Snooping Mrouter Table							
VID	VLAN ID(1-4094)を入力します。						

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。「Show All」ボタンをクリックして、すべての定義済みエント リを表示します。

## MLD Snooping Statistics Settings(MLD Snooping 統計設定)

現在の MLD Snooping の統計情報を表示します。

#### L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Statistics Settings の順にメニューをクリックし、以下の画面を表示します。



図 8-87 MLD Snooping Statistics Settings 画面

#### 以下の項目が表示されます。

#### MLD Snooping Statistics Settings (MLD スヌーピング統計設定)

項目	説明				
Statistics	インタフェースを選択します。「All」「VLAN」「Port」から選択します。				
VID	VLAN ID1 から 4094 の間で指定します。「Statistics」で「VLAN」を選択すると設定可能になります。				
Unit	設定するユニットを選択します。「Statistics」で「Port」を選択すると設定可能になります。				
From Port / To Port	設定するポートの範囲を設定します。「Statistics」で「Port」を選択すると設定可能になります。				

「Clear」をクリックすると表示された統計情報がクリアされます。

#### MLD Snooping Statistics Table (MLD スヌーピング統計テーブル)

項目	説明
Find Type	インタフェースを選択します。「VLAN」「Port」から選択します。
VID	VLAN ID1 から 4094 の間で指定します。「Find Type」で「VLAN」を選択すると設定可能になります。
Unit	設定するユニットを選択します。「Find Type」で「Port」を選択すると設定可能になります。
From Port / To Port	設定するポートの範囲を設定します。「Find Type」で「Port」を選択すると設定可能になります。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。「Show All」ボタンをクリックして、すべての定義済みエントリを表示します。

## Multicast VLAN (マルチキャスト VLAN)

L2 Features > L2 Multicast Control > Multicast VLAN

## Multicast VLAN Settings(マルチキャスト VLAN 設定)

マルチキャスト VLAN の設定を行います。

L2 Features > L2 Multicast Control > Multicast VLAN > Multicast VLAN Settings をクリックして表示します。

Multicast VL	AN Settings					_					
Multicast VLAN	Global Settings										
Multicast VLAM	IPv4 State	OEnabled (	Disabled	Forwa	ard Unmatched		Enabled	Oisal	oled		
Multicast VLAM	IPv6 State	OEnabled (	Disabled	Ignor	e VLAN		Enabled	<ul> <li>Disal</li> </ul>	bled		Apply
,											
VID (2-4094)			VLAN Name	32 cł	nars					Delete	Add
Member Port S	ettings										
VID (2-4094)	Action		Role		Туре		Unit		From Port		To Port
	Add	~	Receiver	~	Tagged	~	1	~	eth1/0/1	~	eth1/0/1
											Apply
Replace Priorit	v Settings										
	,		10 7		Delevite						
VID (2-4094)	Actio	n .	IP Type		Priority		a .				
	Add		IPV4	•	] [0	-					Apply
Replace Source	e IP Settings										
VID (2-4094)	Actio	n	Address Type		IP Address		From				
	Add	~	IPv4	~	]		Receiver		~		Apply
				_							
Multicast VLAN	Table										
VID (2-4094)									1	Find	Show All
1									200	2	
Total Entries:	1					_		_			
VID VLA	N Name U	ntagged Receive	r Tagged Receive	ſ	Untagged Source	Ti	agged Source		Replace S	Source IP	Replace Priority
2 M	IVLAN		1/0/9				1/0/17	10.9	90.90.12 (fro	m receiver)/No	ot 0 (IPv4)/Not replace
									repla	ace	(IPv6)
									1/1		1 > > Go

図 8-88 Multicast VLAN Settings 画面

画面に表示される項目:

項目	説明		
	Multicast VLAN Global Settings		
Multicast VLAN IPv4 State	マルチキャスト VLAN の IPv4 IGMP コントロールパケットを有効または無効にします。		
Forward Unmatched	「Forward Unmatched」を有効または無効にします。		
	「タグなし」「どのプロファイルともマッチしない」「マルチキャスト VLAN が関連する初期 VLAN」「マ		
	ルチキャスト VLAN にタグ付けも、どのプロファイルともマッチしない」などの条件の IGMP/MLD コ		
	ントロールパケットを受信した場合、本設定で破棄(Drop)か転送(Forward)を指定します。初期		
	値ではパケットは破棄されます。		
Multicast VLAN IPv6 State	マルチキャスト VLAN の IPv6 MLD コントロールパケットを有効または無効にします。		
Ignore VLAN	「Ignore VLAN」を「Enabled」(有効)/「Disabled」(無効)に指定します。本設定ではタグ付き IGMP/		
	MLD コントロールパケットの設定を行います。有効にするとパケットの VLAN は無視され、プロファ		
	イルにマッチするマルチキャスト VLAN を検出します。スイッチは受信する IGMP、または MLD コン		
	トロールパケットを無視し、マッチするプロファイルを照合します。		
VID (2-4094)	作成 / 削除する VLAN の VID(2-4094)を指定します。		
VLAN Name	作成 / 削除する VLAN 名を指定します。		
Member Port Settings			
VID (2-4094)	設定する VLAN の VID(2-4094)を指定します。		
Action	実行する動作を指定します。「Add」「Delete」から指定できます。		
Role	メンバポートの役割を指定します。「Receiver」「Source」から指定可能です。		
	・「Receiver」- マルチキャスト VLAN のマルチキャストデータのみを受信するサブスクライバポート		
	として設定します。		
	・「Source」- マルチキャスト VLAN のマルチキャストデータのみを送信するアップリンクポートとし		
	て設定します。		

項目	説明
Туре	メンバポートの種類を指定します。「Tagged」「Untagged」から指定可能です。
	• Tagged - ポートがタグ付きメンバに指定されると、当該ポートからのパケットはマルチキャスト
	VLAN ID をタグ付けされます。
	• Untagged - ポートがタグなしメンバに指定されると、パケットはタグ無しフォームで転送されます。
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。
	Replace Priority Settings
VID (2-4094)	設定する VLAN の VID(2-4094)を指定します。
Action	実行する動作を指定します。「Add」「Delete」から指定できます。
IP Туре	メンバポートの種類を指定します。「IPv4」「IPv6」から指定可能です。
	• IPv4 - マルチキャスト VLAN に転送される IPv4 マルチキャストパケットの優先値を再マップします。
	・ IPv6 - マルチキャスト VLAN に転送される IPv6 マルチキャストパケットの優先値を再マップします。
Priority	優先値を指定します。0-7 の範囲で指定できます。値が低い方が優先度が高くなります。
	Replace Source IP Settings
VID (2-4094)	設定する VLAN の VID(2-4094)を指定します。
Action	実行する動作を指定します。「Add」「Delete」から指定できます。
Address Type	アドレスの種類を指定します。「IPv4」「IPv6」から指定可能です。
	・ IPv4 - IGMP コントロールパケットの送信元 IPv4 アドレスを指定します。
	・ IPv6 - MLD コントロールパケットの送信元 IPv6 アドレスを指定します。
IP Address	IPv4/IPv6 アドレスを指定します。
From	送信元を指定します。
	• Receiver - マルチキャスト VLAN 受信ポートに受信した IGMP/MLD report/leave パケットの送信元
	IPv4/IPv6 アドレスを交代します。
	・ Source - マルチキャスト VLAN 送信元ポートに受信した IGMP/MLD report/leave パケットの送信元
	IPv4/IPv6 アドレスを交代します。
	• Both - マルチキャスト VLAN(送受信)ポートに受信した IGMP/MLD report/leave パケットの送信
	元 IPv4/IPv6 アドレスを交代します。
	Multicast VLAN Table
VID (2-4094)	設定する VLAN の VID(2-4094)を指定します。

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Show All」をクリックして、すべてのエントリを表示します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

## Multicast VLAN Group Settings(マルチキャスト VLAN グループ設定)

マルチキャスト VLAN グループの設定、表示を行います。

L2 Features > L2 Multicast Control > Multicast VLAN > Multicast VLAN Group Settings をクリックして表示します。

Multicast VLAN C	Group Settings		_	_			
Group Profile Setting	5						
Profile Name							
32 chars							Apply
Profile Name	Action		Address Type		From IP Address	To IP Address	
32 chars	Add	~	IPv4	~			Apply
Access Group Setting	IS						
VID (2-4094)	Profile Name		Action				
	32 chars		Add	~			Apply
Group Profile Table							
Profile Name 32 char	rs						Find Show All
Total Entrices 4							
Drofile Na	ma	_	_		Multicast Addresses	_	Delete All
profile	me	_	_	-	Mutucast Addresses		Delete
promo							
Access Group Table							
VID (2-4094)							Find Show All
Total Entries: 1		_		_			
VID					Multicast	Group Profiles	
2							
							Go

図 8-89 Multicast VLAN Group Settings 画面

画面に表示される項目:

項目	説明		
	Groups Profile Settings		
Profile Name	マルチキャスト VLAN のグループプロファイル名(32 字以内)を指定します。		
Action	実行する動作を指定します。「Add」「Delete」から指定できます。マルチプルの範囲をマルチキャスト		
	VLAN プロファイルに追加できます。単一のプロファイルに指定されている IP アドレス範囲は同じアドレ		
	スファミリである必要があります。		
Address Type	アドレスタイプを指定します。「IPv4」「IPv6」から指定します。		
	・ IPv4 - IPv4 マルチキャストアドレスを使用します。		
	・ IPv6 - IPv6 マルチキャストアドレスを使用します。		
From IP Address	送信元 IPv4/IPv6 アドレスを指定します。		
To IP Address	宛先 IPv4/IPv6 アドレスを指定します。		
	Access Group Settings		
VID	VLAN ID(2-4094)を指定します。		
Profile Name	マルチキャスト VLAN のグループプロファイル名(32 字以内)を指定します。		
Action	実行する動作を指定します。「Add」「Delete」から指定できます。		
	Group Profile Table		
Profile Name	マルチキャスト VLAN のグループプロファイル名(32 字以内)を指定します。		
	Access Group Table		
VID	VLAN ID(2-4094)を指定します。		

設定を変更する際は、必ず「Apply」ボタンをクリックし設定内容を適用します。

「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。

「Delete All」をクリックするとすべてのエントリを削除します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。「Show All」ボタンをクリックして、すべての定義済みエントリを表示します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

## PIM Snooping (PIM スヌーピング)

L2 Features > L2 Multicast Control > PIM Snooping

## PIM Snooping Global Settings(PIM スヌーピンググローバル設定)

Protocol Independent Multicast (PIM) をグローバルに設定します。

#### L2 Features > L2 Multicast Control > PIM Snooping > PIM Snooping Global Settings をクリックして表示します。

PIM Snooping Global Settings	_			
Global Settings				
Global State		O Enabled		Apply
VLAN Status Settings				
VID (1-4094)		O Enabled		Apply
PIM Snooping Table				
Number of user enabled VLANs	1			
User enabled VLANs	1			
VID (1-4094) 1				Find
VID Neighbor		Mroute	DR	Learned Neighbor On Ports
1 0		0		

図 8-90 PIM Snooping Global Settings 画面

画面に表示される項目:

項目	説明			
	Global Setting			
Global State	PIM Snooping の有効 / 無効を設定します。 • Enabled - デバイスで PIM Snooping を有効にします。 • Disabled - デバイスで PIM Snooping を無効に設定します。(初期値)			
VLAN Status Settings				
VID	<ul> <li>VLAN 上の PIM Snooping を有効 / 無効にし、VLAN を識別する VLAN ID(1-4094)を指定します。</li> <li>Enabled - VLAN を有効にします。</li> <li>Disabled - VLAN を無効に設定します。(初期値)</li> </ul>			
	PIM Snooping Table			
VID	PIM Snooping Table 上の VLAN を表示させるための VLAN ID(1-4094)を指定します。			

「Find」をクリックして指定の VLAN ID を入力して指定のエントリを表示します。

## PIM Snooping Neighbor Settings(PIM スヌーピングネイバ設定)

PIM スヌーピングネイバテーブルを表示します。

## L2 Features > L2 Multicast Control > PIM Snooping > PIM Snooping Neighbor Table をクリックして表示します。

Find
Find
Option Flags

図 8-91 PIM Snooping Neighbor Table 画面

画面に表示される項目:

項目	説明
VID	表示する VLAN を識別する VLAN ID(1-4094)を指定します。

「Find」をクリックして指定の VLAN ID を入力して指定のエントリを表示します。

## PIM Snooping Mroute Table(PIM Snooping マルチキャストルートテーブル)

PIM スヌーピングマルチキャストルートテーブルを表示します。

L2 Features > L2 Multicast Control > PIM Snooping > PIM Snooping Mroute Table をクリックして表示します。

IM Sno	oping Mroute	Table							
VID (1-4	4094)		Group Address						Find
Total E	ntries: 0								
VID	Address	Uptime/Expire	Downstream Ports	Outgoing Ports	Port	<b>JPState</b>	Exp	Upstream Neighbor	PPT/ET

図 8-92 PIM Snooping Mroute Table 画面

#### 画面に表示される項目:

項目 説明	
	PIM Snooping Mrouter Table
VID	VLAN ID(1-4094)を入力します。
Group Address	選択しグループアドレスを指定します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

## PIM Snooping Statistics Table (PIM Snooping 統計テーブル)

現在の PIM Snooping の統計情報を表示します。

L2 Features > L2 Multicast Control > PIM Snooping > PIM Snooping Statistics Table の順にメニューをクリックし、以下の画面を表示します。

PIM Snoopi	ing Statistics Table		_			
PIM Snooping	Statistics Table					
VID (1-4094)				Find	Clear Clear All	
Total Entries	:1					
VID	PIMv2 Hello	PIMv2 Join/Prune	PIM Error	PIM Error PIMv1 Messages PIMv2 Mess		
1	0	0	0	0	0	
				1/1	[< < 1 > >  Go	

図 8-93 PIM Snooping Statistics Table 画面

#### 画面に表示される項目:

項目	説明	
VID	VLAN ID(1-4094)を指定します。	
「Clear」をクリックすると表示された統計情報がクリアされます。		

「Clear All」をクリックすると入力したエントリを全てクリアします。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

## Multicast Filtering Mode(マルチキャストフィルタリングモード)

L2 マルチキャストフィルタリング設定を行います。

L2 Features > L2 Multicast Control > Multicast Filtering Mode をクリックし、以下の画面を表示します。

Multicast Filtering	Mode			
Multicast Filtering Mode				
VID List	3 or 1-5	Multicast Filtering Mode	Forward Unregistered	Apply
Total Entries: 1				
	VLAN		Multicast Filtering Mode	
	default		Forward Unregistered Group	)S
			1/1	< 1 > > Go

図 8-94 Multicast Filtering Mode 画面

#### 画面に表示される項目:

項目	説明
VID List	設定する VLAN の VLAN ID リストを入力します。
Multicast Filter Mode	<ul> <li>マルチキャストフィルタモードを選択します。</li> <li>「Forward Unregistered」「Forward All」「Filter Unregistered」から選択可能です。</li> <li>Forward Unregistered - 選択すると登録されたマルチキャストパケットはフォワーディングテーブルに基づいて 転送され、登録されていないマルチキャストパケットは VLAN ドメインに基づきフラッドします。</li> <li>Forward All - 選択するとすべてのマルチキャストパケットは VLAN ドメインに基づきフラッドします。</li> <li>Filter Unregistered - 選択すると登録されたマルチキャストパケットはフォワーディングテーブルに基づき転送さ れ、登録されていないマルチキャストパケットはフィルタされます。</li> </ul>

設定を変更する際は、必ず「Apply」ボタンをクリックし設定内容を適用します。 設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

## LLDP

## L2 Features > LLDP

LLDP(Link Layer Discovery Protocol)は、IEEE 802 ネットワークに接続しているステーションから同じ IEEE 802 ネットワークに接続している他のス テーションに通知を出します。本プロトコルによって送信される情報は、受信先によって標準の管理情報ベース(MIB)に格納されるので、SNMP (Simple Network Management Protocol) などの管理プロトコル使ったネットワーク管理システム(NMS)からその情報にアクセスできるようにな ります。

## LLDP Global Settings(LLDP グローバル設定)

L2 Features > LLDP > LLDP Global Settings の順にメニューをクリックし、以下の画面を表示します。

LLDP Global Settings		
LLDP Global Settings		
LL DR State		
LLDF State		
LLDF Hap State		0 h
LEDF-MED Trap State	Octioned Obisatied	Арріу
LLDP-MED Configuration		
Fast Start Repeat Count (1-10)	4 times	Apply
LLDP Configurations		
Message TX Interval (5-32768)	30 sec	
Message TX Hold Multiplier (2-10)	4 sec	
ReInit Delay (1-10)	2 sec	
TX Delay (1-8192)	2 sec	Apply
LLDP System Information		
Chassis ID Subtype	MAC Address	
Chassis ID	F0-7D-68-36-30-00	
System Name	Switch	
System Description	Gigabit Ethernet Switch	
System Capabilities Supported	Repeater, Bridge	
System Capabilities Enabled	Repeater, Bridge	
LLDP-MED System Information		
Device Class	Network Connectivity Device	
Hardware Revision	A1	
Firmware Revision	1.00.006	
Software Revision	1.00.015	
Serial Number	DGS3630102030	
Manufacturer Name	D-Link Corporation	
Model Name	DGS-3630-28TC Gigabit Ethernet S	
Asset ID		

図 8-95 LLDP Global Settings 画面

画面に表示される項目:

-= -	
月日 月日	記明
LLDP State	スイッチにおける LLDP 機能を「Enabled」(有効)または「Disabled」(無効)にします。
LLDP Forward State	同じ IEEE 802 ネットワークに割り当てられた他のステーションに通知するために LLDP 機能のメッセージ転送を
	「Enabled」(有効)または「Disabled」(無効)にします。
	「LLDP」が 無効で「LLDP Forward Sate」が有効の場合、受信した「LLDPDU」パケットは転送されます。
LLDP Trap State	LLDP Trap を「Enabled」(有効)/「Disabled」(無効)に指定します。
LLDP-MED Trap State	LLDP-MED Trap を「Enabled」(有効)/「Disabled」(無効)に指定します。
	LLDP-MED Settings
Fast Start Repeat Count	「LLDP-MED」ファストスタートリピートカウント値を指定します。1 から 10 の間で指定できます。
	LLDP Configurations
Message TX Interval	アクティブなポートが通知を再送する方法を制御します。パケット伝送間隔を変更するために、5-32768(秒)の範
(5-32768)	囲で値を入力します。
Message TX Hold Multiplier	LLDP スイッチに使用される乗数を変更することで LLDP Neighbor に LLDP 通知を作成して送信する有効期間(TTL:
(2-10)	Time-to-Live)を計算します。指定通知の TTL(Time-to-Live)の期限が来ると、通知データは Neighbor スイッチの
	MIB から削除されます。
Relnit Delay (1-10)	LLDP ポートが LLDP 無効にするコマンドを受け取った後、再初期化を行う前に待機する最小時間です。LLDP Reinit
	Delay を変更するために、1-10(秒)から値を入力します。
TX Delay (1-8192)	LLDP MIB のコンテンツ変更のために、LLDP ポートが連続した LLDP 通知の送信を遅らせる最短時間(遅延間隔)を
	変更します。LLDP TX Delay を変更するために、1-8192(秒)から値を入力します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

## LLDP Port Settings(LLDP ポート設定)

LLDP ポートパラメータを設定します。

L2 Features > LLDP > LLDP Port Settings の順にメニューをクリックし、以下の画面を表示します。

LDP Port Settings					
LLDP Port Settings Unit From Port 1 v eth1/0/1 v Note: The address should i	To Port Notification eth1/0/1 Disabled be the switch's address.	Subtype	Admin State IF	P Subtype Action Address	pply
Unit 1 Settings					
Port	Notification	Subtype	Admin State	IPv4/IPv6 Address	
eth1/0/1	Disabled	Local	TX and RX		
eth1/0/2	Disabled	Local	TX and RX		
eth1/0/3	Disabled	Local	TX and RX		
eth1/0/4	Disabled	Local	TX and RX		
eth1/0/5	Disabled	Local	TX and RX		
eth1/0/6	Disabled	Local	TX and RX		
eth1/0/7	Disabled	Local	TX and RX		
eth1/0/8	Disabled	Local	TX and RX		

図 8-96 LLDP Port Settings 画面

画面に表示される項目:

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	プルダウンメニューを使用して設定するポート範囲を指定します。
Subtype	プルダウンメニューを使用して LLDP TLV(s) のサブタイプを選択します。「MAC Address」「Local」から選択可能です。
Notification	プルダウンメニューを使用して LLDP 通知を「Enabled」(有効)または「Disabled」(無効)にします。
Admin State	プルダウンメニューを通知のステータスを選択します。:Tx(送信のみ)、Rx(受信のみ)、Tx And Rx(送受信)または 「Disabled」(無効)。 • TX - ローカル LLDP エージェントは LLDP フレーム送信のみします。 • RX - ローカル LLDP エージェントは LLDP フレーム受信のみします。 • TX and RX - ローカル LLDP エージェントは LLDP フレームの送受信をします。 • Disabled - ローカル LLDP エージェントは LLDP フレームの送受信をしません。 初期値は TX and RX です。
IP Subtype	プルダウンメニューを使用して送信する IP アドレスの種類を選択します。
Address	通知するエンティティの管理アドレスを入力します。
Action	ポートベースの管理アドレス機能を「Enabled」(有効)または「Disabled」(無効)にします。

「Apply」ボタンをクリックし、変更を有効にします。

注意 入力の IPv4/IPv6 アドレスは既存の LLDP 管理 IP アドレスである必要があります。

## LLDP Management Address List (LLDP 管理アドレスリスト)

L2 Features > LLDP > LLDP Management Address List の順にメニューをクリックし、以下の画面を表示します。

LLDP Manager	LLDP Management Address List						
				Find			
Subtype	Address	IF Type	OID	Advertising Ports			
IPv4	10.90.90.90 (default)	lfIndex	1.3.6.1.4.1.171.10.1				
IPv4	10.90.90.90	lfindex	1.3.6.1.4.1.171.10.1	-			

図 8-97 LLDP Management Address List 画面

画面に表示される項目:

項目	説明
Subtype	表示する LLDP 管理アドレスのサブタイプを「All」「IPv4」「IPv6」から選択します。
「Find」ボタンをクリックし、I	LLDP 管理情報を検索します。

LLDP Basic TLVs Settings(LLDP ベーシック TLV 設定)

TLV (Type-length-value) は、LLDP パケット内の TLV エレメントとして特定の送信情報を許可します。本スイッチにおけるベーシック TLV 設定を 有効にします。スイッチのアクティブな LLDP ポートは、通常その外向き通知にいつも必須データを含んでいます。外向き LLDP 通知からこれらの データタイプの 1 個以上を除外するために、個別のポートまたはポートグループに設定できる 4 つのオプションデータがあり、必須データタイプに は、4 つの基本的な情報タイプ (end f LLDPDU TLV、chassis ID TLV、port ID TLV および Time to Live TLV) があります。必須データタイプは無効に することができません。さらに、オプションで選択可能な 4 つのデータタイプ (Port Description、System Name、System Description および System Capability) があります。

本スイッチにおけるベーシック TLV 設定を有効にします。

L2 Features > LLDP > LLDP Basic TLVs Settings の順にメニューをクリックし、以下の画面を表示します。

LLDP Basic TLVs	Settings					
LLDP Basic TLVs Settin	ngs To Port ▼ eth1/0/1 ▼	Port Description Disabled	System Name Disabled 💌	System Description	System Capabilities Disabled 💌	Apply
Port	Port Description	System I	Name	System Descriptio	n	System Capabilities
eth1/0/1	Disabled	Disabl	led	Disabled		Disabled
eth1/0/2	Disabled	Disabl	led	Disabled		Disabled
eth1/0/3	Disabled	Disabl	led	Disabled		Disabled
eth1/0/4	Disabled	Disabl	led	Disabled		Disabled
eth1/0/5	Disabled	Disabl	led	Disabled		Disabled

図 8-98 LLDP Basic TLVs Settings 画面

```
プルダウンメニューを使用してベーシック TLV 設定を「Enabled」(有効)/「Disabled」(無効)にします。
```

#### 画面に表示される項目:

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	設定するポート範囲を指定します。
Port Description	ポート説明を「Enabled」(有効)/「Disabled」(無効)にします。
System Name	システム名を「Enabled」(有効)/「Disabled」(無効)にします。
System Description	システム説明を「Enabled」(有効)/「Disabled」(無効)にします。
System Capabilities	システム能力を「Enabled」(有効)/「Disabled」(無効)にします。

「Apply」ボタンをクリックし、変更を有効にします。

## LLDP Dot1 TLVs Settings(LLDP Dot1 TLV 設定)

LLDP Dot1 TLV は、IEEE 802.1 によって組織的に定義されている TLV で、送信する LLDP 通知から IEEE 802.1 規定のポート VLAN ID の TLV データタ イプを除外するようにポートやポートグループを設定する時に使用します。

L2 Features > LLDP > LLDP Dot1 TLVs Settings の順にメニューをクリックし、以下の画面を表示します。

LDP Dot1 T	LVs Settings			
LLDP Dot1 TLV	s Settings			
Unit From P	Port         To Port           D/1          eth1/0/1	Port VLAN     Protocol VLAN       V     Disabled V	VLAN Name Disabled	Protocol Identity Disabled V None V Apply
Unit 1 Settings				
Unit 1 Settings Port	Port VLAN ID	Enabled Port and Protocol VID	Enabled VLAN Name	Enabled Protocol Identity
Unit 1 Settings Port eth1/0/1	Port VLAN ID Disabled	Enabled Port and Protocol VID	Enabled VLAN Name	Enabled Protocol Identity
Unit 1 Settings Port eth1/0/1 eth1/0/2	Port VLAN ID Disabled Disabled	Enabled Port and Protocol VID	Enabled VLAN Name	Enabled Protocol Identity
Unit 1 Settings Port eth1/0/1 eth1/0/2 eth1/0/3	Port VLAN ID Disabled Disabled Disabled	Enabled Port and Protocol VID	Enabled VLAN Name	Enabled Protocol Identity
Unit 1 Settings Port eth1/0/1 eth1/0/2 eth1/0/3 eth1/0/4	Port VLAN ID Disabled Disabled Disabled Disabled	Enabled Port and Protocol VID	Enabled VLAN Name	Enabled Protocol Identity

図 8-99 LLDP Dot1 TLVs Settings 画面

画面に表示される項目:

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	設定するポート範囲を指定します。
Port VLAN	ポート VLAN ID TLV の通知を「Enabled」(有効)/「Disabled」(無効)にします。 「ポート VLAN ID TLV」は VLAN ブリッジポートにタグなし・タグ付きフレームの PVID の通知を許可するオプションのフィック ス長 TLV です。
Protocol VLAN	プロトコル VLAN ID の通知を「Enabled」(有効)/「Disabled」(無効)にします。 対象となるプロトコル VLAN を右の欄で VLAN ID で指定します。
VLAN Name	VLAN 名の通知を「Enabled」(有効)/「Disabled」(無効)にします。 対象となるプロトコル VLAN を右の欄で VLAN ID で指定します。
Protocol Identity	プロトコル識別子の通知を「Enabled」(有効)/「Disabled」(無効)にします。 次に対象とするプロトコルを None、EAPOL、LACP、GVRP、STP または All から選択します。

「Apply」ボタンをクリックし、変更を有効にします。

## LLDP Dot3 TLVs Settings(LLDP Dot3 TLV 設定)

個別のポートやポートグループが送信する LLDP 通知から IEEE 802.3 規定のポート VLAN ID TLV データタイプを除外するように設定します。

L2 Features > LLDP > LLDP Dot3 TLVs Settings の順にメニューをクリックし、以下の画面を表示します。

LLDP Dot3 TLVs Settings								
LLDP Dot3 TLVs Settings         Unit       From Port       To Port       MAC/PHY Configuration/Status       Link Aggregation       Maximum Frame Size       Energy-Efficient Ethernet       Power Via MDI         1       eth1/0/1       Disabled       Disabled       Disabled       Disabled       Apply								
Unit 1 Settin	igs							
Port	MAC/PHY Configurat	ion/Status	Link Aggregation	Maximum Frame	Size	Energy-Effi	cient Ethernet	Power Via MDI
eth1/0/1	Disabled		Disabled	Disabled		Dis	abled	Disabled
eth1/0/2	Disabled		Disabled	Disabled		Dis	abled	Disabled
eth1/0/3	/0/3 Disabled		Disabled	Disabled		Dis	abled	Disabled
eth1/0/4	Disabled		Disabled	Disabled		Dis	abled	Disabled
eth1/0/5	0/5 Disabled		Disabled	Disabled		Dis	abled	Disabled
eth1/0/6	Disabled		Disabled	Disabled		Dis	abled	Disabled
eth1/0/7	Disabled		Disabled	Disabled		Dis	abled	Disabled

図 8-100 LLDP Dot3 TLVs Settings 画面

画面に表示される項目:

項目	説明			
Unit	設定するユニットを指定します。			
From Port/To Port	設定するポート範囲を指定します。			
MAC/PHY Configuration/Status	スイッチの MAC または PHY 状態の通知を「Enabled」(有効)/「Disabled」(無効)にします。			
Link Aggregation	スイッチのリンクアグリゲーション状態の通知を「Enabled」(有効)/「Disabled」(無効)にします。			
Maximum Frame Size	最大フレームサイズの通知を「Enabled」(有効)/「Disabled」(無効)にします。			
Energy-Efficient Ethernet	「Energy-Efficient Ethernet TLV」送信を「Enabled」(有効)/「Disabled」(無効)に指定します。 「Energy-Efficient Ethernet TLV」はパケットが送信されていないリンクのエネルギー消費を削減する機能です。			
Power Via MDI	「MDI TLV」経由での電力送信を「Enabled」(有効)/「Disabled」(無効)にします。 IEEE802.3 PMD の実装により接続した電力供給のないシステムに対し電力を供給します。「Power Via MDI TLV」に より IEEE 802.3 LAN ステーションに MDI 電力サポート機能を提供するネットワーク管理を実現します。			

「Apply」ボタンをクリックし、変更を有効にします。

## LLDP-MED Port Settings(LLDP-MED ポート設定)

LLDP-MED TLV の送信を有効または無効にします。

```
L2 Features > LLDP > LLDP-MED Port Settings の順にメニューをクリックし、以下の画面を表示します。
```

LLDP-MED Port Settings						
LLDP-MED Port Settings	LLDP-MED Port Settings					
Unit From Port	To Port	Notification Capabilitie Disabled	s Inventory Disabled	Network Policy PSE Disabled Disabled	Apply	
Unit 1 Settings	Notification	Canabilities	Inventory	Network Dolicy	DSE	
eth1/0/1	Disabled	Disabled	Disabled	Disabled	Disabled	
eth1/0/2	Disabled	Disabled	Disabled	Disabled	Disabled	
eth1/0/3	Disabled	Disabled	Disabled	Disabled	Disabled	
eth1/0/4	Disabled	Disabled	Disabled	Disabled	Disabled	
eth1/0/5	Disabled	Disabled	Disabled	Disabled	Disabled	
eth1/0/6	Disabled	Disabled	Disabled	Disabled	Disabled	
eth1/0/7	Disabled	Disabled	Disabled	Disabled	Disabled	



以下の項目が使用できます。

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	設定するポート範囲を指定します。
Notification	「LLDP-MED notification TLV」の送信を「Enabled」(有効)/「Disabled」(無効)にします。
Capabilities	「LLDP-MED capabilities TLV」の送信を「Enabled」(有効)/「Disabled」(無効)にします。
Inventory	「LLDP-MED inventory TLV」の送信を「Enabled」(有効)/「Disabled」(無効)にします。
Network Policy	「LDP-MED network policy TLV」の送信を「Enabled」(有効)/「Disabled」(無効)にします。
PSE	「MDI TLV」経由での LLDP-MED 拡張電力送信を「Enabled」(有効) /「Disabled」(無効) にします。接続しているデバイスが「PSE」
	または「PD」である必要があります。

「Apply」ボタンをクリックして変更を適用します。

## LLDP-DCBX Port Settings(LLDP-DCBX ポート設定)

LLDP-DCBX (Data Center Bridging Exchange) TLV の送信を有効または無効にします。

L2 Features > LLDP > LLDP-DCBX Port Settings の順にメニューをクリックし、以下の画面を表示します。

LLDP-DCBX Port Settings						
LLDP-DCBX Port Settings						
Unit	From Port eth1/0/1	To Port eth1/0/1	Priority-based Flow Control Configuration TLV Disabled	Apply		
Unit 1 Settin	ngs					
	Port		Priority-based Flow Control			
	Poit		Configuration TLV			
	eth1/0/1		Disabled			
	eth1/0/2		Disabled			
	eth1/0/3		Disabled			
	eth1/0/4		Disabled			
	eth1/0/5		Disabled			
	eth1/0/6		Disabled			
	eth1/0/7		Disabled			
	eth1/0/8		Disabled			

図 8-102 LLDP-DCBX Port Settings 画面

画面に表示される項目:

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	設定するポート範囲を指定します。
Priority-based	「Priority-based Flow Control」 (PFC) Configuration TLV を「Enabled」(有効)/「Disabled」(無効)に指定します。
Flow Control	有効にすると「PFC Configuration TLV」が送信されます。「PFC TLV」はブリッジポートに現在の状況と PFC の今後の動作に
Configuration TLV	ついての通知を許可します。

「Apply」ボタンをクリックして変更を適用します。

## LLDP Statistics Information(LLDP 統計情報)

スイッチにおける LLDP 統計情報と各ポートの設定を参照できます。

L2 Features > LLDP > LLDP Statistics Information の順にメニューをクリックし、以下の画面を表示します。

LLDP Statis	stics Information						
LLDP Statistic	s Information						
Last Change	Time	0					Class Country
Tatal lasada	Time	0					Clear Counter
Total Inserts		U					
Total Deletes		0					
Total Drops		0					
Total Ageouts	÷	0					
Unit Unit 1 Setting	1 🗸	Port	eth1/0/1	~		Clear Counter	Clear All
Port	Total Transmits	Total Discards	Total Errors	Total Receives	Total TLV Discards	Total TLV Unknowns	Total Ageouts
eth1/0/1	0	0	0	0	0	0	0
eth1/0/2	0	0	0	0	0	0	0
eth1/0/3	0	0	0	0	0	0	0
eth1/0/4	0	0	0	0	0	0	0
	0	0	0	0	0	0	

図 8-103 LLDP Statistics Information 画面

以下の項目が使用できます。

項目	説明				
Unit	表示するユニットを選択します。				
Port	表示するポートを指定します。				
「Clear Counter」をク					

「Clear All」をクリックしてすべてのカウンタ数をクリアします。

## LLDP Local Port Information (LLDP ローカルポート情報)

以下のローカルポートの要約テーブルにポートベースの情報を表示します。

## L2 Features > LLDP > LLDP Local Port Information の順にメニューをクリックし、以下の画面を表示します。

LLDP Local Port Information						
LLDP Local Port Brief Table						
Unit T Port eth1/0/1 T Find Show Detail						
Port	Port ID Subtype	Port ID	Port Description			
eth1/0/1	Local	eth 1/0/1	D-Link Corporation DGS-1510-28			
eth1/0/2	Local	eth1/0/2	D-Link Corporation DGS-1510-28			
eth1/0/3	Local	eth 1/0/3	D-Link Corporation DGS-1510-28			

図 8-104 LLDP Local Port Information 画面

画面に表示される項目:

項目	説明
Unit	表示するユニットを選択します。
Port	表示するポートを指定します。

ポートを選択し、「Find」ボタンをクリックします。情報が画面下半分に表示されます。

## ■ 各パラメータの詳細の参照

「Show Detail」リンクをクリックし、以下の画面を表示します。

LLDP Local Port Information				
LIDDL and Information Table				
LEDP Local mornation rable				
Port	eth1/0/1			
Port ID Subtype	Local			
Port ID	eth1/0/1			
Port Description	D-Link Corporation DGS-3630-28TC HW A1 firmware 1.00.015 Port 1 on Unit 1			
Port PVID	1			
Management Address Count	2			
PPVID Entries	<u>0</u>			
VLAN Name Entries Count	1			
Protocol Identity Entries Count	<u>0</u>			
MAC/PHY Configuration/Status	Show Detail			
Link Aggregation	Show Detail			
Maximum Frame Size	1536			
Energy Efficient Ethernet	Show Detail			
LLDP-MED Capabilities	Show Detail			
LLDP-DCBX capabilities	Show Detail			
Network Policy	Show Detail			
	Back			

図 8-105 LLDP Local Port Information (Show Detail) 画面

## ■「MAC/PHY Configuration/Status」情報の参照

「Show Detail」リンクをクリックし、以下の画面を表示します。

LLDP Local Port Information		
LLDP Local Information Table		
Port	eth1/0/1	
Port ID Subtype	Local	
Port ID	eth1/0/1	
Port Description	D-Link Corporation DGS-3630-28TC HW A1 firmware 1.00.015 Port 1 on Unit 1	
Port PVID	1	
Management Address Count	2	
PPVID Entries	ō	
VLAN Name Entries Count	1	
Protocol Identity Entries Count	0	
MAC/PHY Configuration/Status	Show Detail	
Link Aggregation	Show Detail	
Maximum Frame Size	1536	
Energy Efficient Ethernet	Show Detail	
LLDP-MED Capabilities	Show Detail	
LLDP-DCBX capabilities	Show Detail	
Network Policy	Show Detail	
		Back
MAC/PHY Configuration/Status		
Auto-Negotiation Support	Supported	
Auto-Negotiation Enabled	Enabled	
Auto-Negotiation Advertised Capability	6c01(hex)	
Auto-Negotiation Operational MAU Type	001e(hex)	

図 8-106 LLDP Local Port Information - MAC/PHY Configuration/Status 画面

## LLDP Neighbor Port Information(LLDP ネイバポート情報)

Neighbor から学習したポート情報を表示します。

L2 Features > LLDP > LLDP Neighbor Port Information の順にメニューをクリックし、以下の画面を表示します。

DP Neighbo	or Port Brief Lable					
nit	1 🗸	Port eth1/0/1 🗸			Find	Clear
						Clear All
otal Entries	:1					
otal Entries Entity	: 1 Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	Port Description	

図 8-107 LLDP Neighbor Port Information 画面

画面に表示される項目	:
------------	---

項目	説明
Unit	表示するユニットを選択します。
Port	表示するポートを指定します。

ポートを選択し、「Find」ボタンをクリックします。情報が画面下半分に表示されます。 「Clear」をクリックしてポート情報をクリアします。

「Clear All」をクリックして全てのポート情報をクリアします。

「Show Detail」をクリックして指定ポート詳細情報を表示します。

DP Neighbor Information Table		
Entry ID	1	
Chassis ID Subtype	MAC Address	
Chassis ID	D0-AE-EC-D9-9E-5E	
ort ID Subtype	Local	
ort ID	1/16	
ort Description		
ystem Name		
system Description	Gigabit Ethernet Switch	
ystem Capabilities	Repeater, Bridge	
lanagement Address Entries	Show Detail	
ort PVID	0	
PVID Entries	Show Detail	
'LAN Name Entries	Show Detail	
rotocol Identity Entries	Show Detail	
IAC/PHY Configuration/Status	Show Detail	
ower Via MDI	Show Detail	
ink Aggregation	Show Detail	
laximum Frame Size	0	
nergy Efficient Ethernet	Show Detail	
Inknown TLVs	Show Detail	
LDP-MED Capabilities	Show Detail	
LDP-DCBX Capabilities	Show Detail	
letwork Policy	Show Detail	
xtended Power Via MDI	Show Detail	
nventory Management	Show Detail	Back

図 8-108 LLDP Neighbor Port Information (Show Detail) 画面

表示された項目の「Show Detail」をクリックすると、当該項目についての詳細情報を表示します。(例:MAC/PHY Configuration/Status)

LLDP Neighbor Information Table		
Entry ID	1	
Chassis ID Subtype	MAC Address	
Chassis ID	D0-AE-EC-D9-9E-5E	
Port ID Subtype	Local	
Port ID	1/16	
Port Description		
System Name		
System Description	Gigabit Ethernet Switch	
System Capabilities	Repeater, Bridge	
Management Address Entries	Show Detail	
Port PVID	0	
PPVID Entries	Show Detail	
VLAN Name Entries	Show Detail	
Protocol Identity Entries	Show Detail	
MAC/PHY Configuration/Status	Show Detail	
Power Via MDI	Show Detail	
Link Aggregation	Show Detail	
Maximum Frame Size	0	
Energy Efficient Ethernet	Show Detail	
Unknown TLVs	Show Detail	
LLDP-MED Capabilities	Show Detail	
LLDP-DCBX Capabilities	Show Detail	
Network Policy	Show Detail	
Extended Power Via MDI	Show Detail	
Inventory Management	Show Detail	Back
MAC/PHY Configuration/Status		
None		

図 8-109 LLDP Neighbor Port Information (Show Detail - MAC/PHY Configuration/Status) 画面

「Back」ボタンをクリックし前画面に戻ります。

# 第9章 L3 Features (レイヤ3機能の設定)

L3 Features メニューを使用し、本スイッチにレイヤ 3 機能を設定することができます。

以下は L3 Features サブメニューの説明です。必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明
ARP(ARP 設定)	ARP(Address Resolution Protocol)は、IP アドレスを物理的なアドレスに変換し、IP アドレスと MAC アドレスを対応させます。
Gratuitous ARP(Gratuitous ARP 設定)	Gratuitous ARP として知られている ARP 通知は、TAP と SPA が等しい場合、それを送信したホストに有効である SHA と SPA を含むパケット (通常 ARP リクエスト)です
IPv6 Neighbor (IPv6 ネイバ設定)	IPv6 ネイバ設定を行います。
Interface (インタフェース設定)	IP インタフェース設定を行います。
UDP Helper(UDP ヘルパー)	IP 転送プロトコルの設定を行います。本機能は指定の UDP サービスタイプのパケットの転 送を有効にします。また UDP ブロードキャストパケットを転送するターゲットアドレスを 指定します。
IPv4 Static/Default Route(IPv4 スタティック / デフォ ルトルート設定)	本スイッチは IPv4 アドレシングのためにスタティックルーティング機能をサポートしています。IPv4 には最大 512 個のスタティックルートエントリを作成することできます。
IPv4 Static Route BFD(IPv4 スタティックルート BFD)	IPv4 スタティックルート BFD(Bidirectional Forwarding Detection)の設定を行います。
IPv4 Route Table (IPv4 ルートテーブル)	IP ルーティングテーブルはスイッチに関するすべての外部経路情報を保存します。ここでは スイッチにおけるすべての外部経路情報を参照します。
IPv6 Static/Default Route(IPv6 スタティック / デフォ ルトルート設定)	IPv6 アドレスのスタティックエントリは IPv6 形式のアドレスで本スイッチのルーティング テーブルに入力します。
IPv6 Static Route BFD(IPv6 スタティックルート BFD)	IPv6 スタティックルート BFD(Bidirectional Forwarding Detection)の設定を行います。
IPv6 Route Table (IPv6 ルートテーブル)	IPv6 ルーティングテーブルを表示します。
Route Preference (ルート優先度設定)	ルート優先度を設定します。小さい優先度値を持つルートほど高いプライオリティを持ちます。
ECMP Settings(ECMP 設定)(EI/MI モードのみ)	ECMP OSPF 状態と ECMP ルートロードバランシングアルゴリズムを設定します。
IPv6 General Prefix(IPv6 汎用プリフィクス)	VLAN インタフェース IPv6 汎用プリフィクスの設定を行います。
IP Tunnel Settings(IP トンネル設定)	IP トンネルを設定します。
URPF Settings(URPF 設定)	「Unicast Reverse Path Forwarding」(URPF) の設定と表示を行います。
VRF(Virtual Routing and Forwarding)(EI/MI モードのみ)	「Virtual Routing and Forwarding」(VRF) の設定を行います。
RIP (Routing Information Protocol)	RIP(Routing Information Protocol)は、距離ベクトル型のルーティングプロトコルです。
RIPng(RIPng 設定)	RIPng(Routing Information Protocol next generation)をサポートしています。RIPng は、 ルートを計算するのに使用するルーティング情報を交換するルーティングプロトコルであ り、IPv6 ベースのネットワーク用です。
OSPF(OSPF 設定)(EI/MI モードのみ)	OSPF を設定します。
IP Multicast Routing Protocol (IP マルチキャストルー ティングプロトコル)	IP Multicast Routing Protocol (IP マルチキャストルーティングプロトコル)の設定を行います。
BGP(Border Gateway Protocol)(EI/MI モードのみ)	BGP(Border Gateway Protocol)をサポートしています。これは AS(自律システム)内のネッ トワーク到達性を指定する IP ネットワークまたはプレフィックスのテーブルを保持するレイ ヤ 3 ユニキャストルーティングプロトコルです。
BFD (Bidirectional Forwarding Detection)	Bidirectional Forwarding Detection (BFD) の設定を行います。
ISIS(Intermediate System to Intermediate System)(MI モードのみ)	Intermediate System to Intermediate System (ISIS) の設定を行います。
IP Route Filter(IP ルートフィルタ)	IP プレフィックスリスト、ルートマップの作成、またはルートマップへのシーケンスの追加、 およびシーケンスの削除を行います。
Policy Route(ポリシールート設定)	ポリシーベースルーティングの設定、表示を行います。
VRRP(VRRP 設定)	VRRP(Virtual Routing Redundancy Protocol)は、LAN 上の VRRP ルータの 1 つに仮想ルー タとしての役割を動的に割り当てる機能です。
VRRPv3 Settings(VRRPv3 設定)	VRRPv3 設定を行います。

## ARP (ARP 設定)

#### L3 Features > ARP

ARP(Address Resolution Protocol)は、IP アドレスを物理的なアドレスに変換し、IP アドレスと MAC アドレスを対応させます。特定のデバイスに 対する ARP 情報を参照、編集および削除することができます。

## ARP Elevation (ARP $\pm \nu \sqrt{-\nu} = \nu$ )

本項目では「Address Resolution Protocol」(ARP) エレベーションの表示、設定を行います。宛先がスイッチ自身の場合に、スイッチに ARP トラフィックを送信することが可能です。このトラフィックは他の ARP パケットよりも高い優先値にあります。

L3 Features > ARP > ARP Elevation の順にクリックし、以下の画面を表示します。

ARP Elevation			
ARP Elevation			
ARP Elevation State	O Enabled	Disabled	Apply
図 9-1 ARP Elevation 画	面		

画面に表示される項目:

項目	説明		
ARP Elevation State	ARP エレベーションを「Enabled」(有効)/「Disabled」(無効)に指定します。		

ARP エージングタイムの設定を行います。

L3 Features > ARP > ARP Aging Time の順にクリックし、以下の画面を表示します。

ARP Aging Time		
ARP Aging Time		
Total Entries: 1		
Interface Name	Timeout (min)	
vlan1	240	Edit
		1/1 K < 1 > > Go

図 9-2 ARP Aging Time 画面

画面に表示される項目:

項目	説明
Timeout	ARP テーブルエントリのリクエストから、エントリを保持する時間(分)設定します。
	この時間が経過すると、エントリはテーブルから削除されます。初期値は 20 分です。

## ■ ARP エージングタイムの編集

- 1. 編集するエントリの「Edit」ボタンをクリックします。
- 2. 「ARP Aging Time」を設定します。
- 3. 「Apply」ボタンをクリックします。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

## Static ARP(スタティック ARP 設定)

ARP(Address Resolution Protocol)は、IP アドレスを物理的なアドレスに変換する TCP/IP プロトコルです。ここでは特定のデバイスに対する ARP 情報を参照、編集および削除することができます。

スタティックエントリを ARP テーブルに定義します。スタティックエントリを定義する場合、継続的なエントリを入力し、IP アドレスを MAC アドレスに変換するために使用します。以下の手順で ARP 情報を定義します。

L3 Features > ARP > Static ARP の順にクリックし、以下の画面を表示します。

tatic ARP						
VRF Name	12 chars	IP Address	· · · Hardware A	Address 00-11	-22-33-44-AA	App
/RF Name	12 chars					Fin
otal Entries: 2						
VRF Name	Interface Name	IP Address	Hardware Address	Aging Time	Туре	
	vlan1	192.168.70.123	F0-7D-68-36-30-00	Forever		Edit Delete
	vlan1	192.168.70.222	00-11-22-33-44-55	Forever	Static	Edit Delete

図 9-3 Static ARP 画面

#### 画面に表示される項目:

項目	説明
VRF Name	VRF インスタンス名を 12 字以内で入力します。
ARP Aging Time (0-65535)	ARP エントリのエージングタイム(分)を設定します。この時間が経過すると、エントリはテーブルから削除されます。範囲は 0-65535(分)です。初期値は 20(分)です。
IP Address	MAC アドレスとスタティックに結びつける IP アドレスを設定します。
Hardware Address	ARP テーブルで IP アドレスとスタティックに結びつける MAC アドレスを設定します。
VRF Name	検索する VRF インスタンス名を 12 字以内で入力します。「Find」をクリックし VRF を検出します。

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

「Edit」をクリックして、指定エントリの編集を行います。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

## ARP Force Aging IP Address(ARP 強制エージアウト設定)

「ARP Force Aging IP Address」ではネクストホップルートエントリにアサインされている ARP エントリを VRF と IP アドレスで指定し、手動でエージアウトさせます。

L3 Features > ARP > ARP Force Aging IP Address の順にクリックし、以下の画面を表示します。

ARP Force Aging IP Address							
ARP Force Aging IP Address							
VRF Name 12 chars	VRF Name 12 chars IP Address Apply						
Total Entries: 1							
IP Address	VRF Name						
10.90.90.1	vrf	Delete					
	1/1	< < 1 > > Go					
IP Address 10.90.90.1	VRF Name vrf 1/1	Delete           <					

図 9-4 ARP Force Aging IP Address 画面

#### 画面に表示される項目:

項目	説明
VRF Name	VRF インスタンス名を 12 字以内で指定します。
IP Address	手動でエージアウトさせる ARP エントリの IP アドレスを指定します。
「Apply」をクリックし、設定	内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

## Proxy ARP (プロキシ ARP)

プロキシ ARP 機能に関する基本設定を参照および編集します。

プロキシ ARP 機能は、別の機器に対し IP/MAC アドレスを見せかけて送信される ARP リクエストに対して、スイッチが本来の ARP 回答元として返答します。従って、スタティックのルーティングやデフォルトゲートウェイを設定せずに、目的の宛先にパケットをルートすることが可能です。ホスト(通常レイヤ3スイッチ)は別の機器に送信されたパケットに応答します。例えばホスト A と B が異なる物理ネットワークに属している場合、B は A からの ARP ブロードキャストリクエストを受信も応答もしません。しかし、A の物理ネットワークがルータまたはレイヤ3スイッチを介して B に接続されると、ルータまたはレイヤ3スイッチは A からの ARP リクエストを参照することが可能です。ローカルプロキシ ARP 機能は送信元 IP アドレスと宛先 IP アドレスが同じ場合、スイッチがプロキシ ARP に応答することを許可します。

L3 Features > ARP > Proxy ARP の順にメニューをクリックし、以下の画面を表示します。

Proxy ARP			
Proxy ARP			
Total Entries: 1			
Interface Name	Proxy ARP State	Local Proxy ARP State	
vlan1	Disabled	Disabled	Edit
		1/1	K < 1 > X Go
		Landard	

#### 画面に表示される項目:

項目	説明
Proxy ARP State	プロキシ ARP を「Enabled」(有効)/「Disabled」(無効)にします。
Local Proxy ARP State	ローカルプロキシ ARP を「Enabled」(有効)/「Disabled」(無効)にします。 ローカルプロキシ ARP 機能は送信元 IP と宛先 IP が同じインタフェースの場合、スイッチがプロキシ ARP に返答します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

## ■ エントリの編集

- 1. 編集するエントリの「Edit」ボタンをクリックします。
- 2. 指定エントリを編集して、IP インタフェースのプロキシ ARP の状態を選択します。
- 3. Apply」ボタンをクリックします。

初期値では「Proxy ARP」「Local Proxy ARP State」の両方とも無効になります。

図 9-5 Proxy ARP 画面

## ARP Table (ARP テーブルの参照)

スイッチ上の現在の ARP エントリを表示します。

```
L3 Features > ARP > ARP Table メニューをクリックし、以下の画面を表示します。
```

Search					
F Name	12 chars				
Interface VLAN (1-4094)	0	P Address	Mask		
	00 44 00 00 44 55 55	All [37]			
Hardware Address	00-11-22-33-44-55-FF	All Y	) Mgmt		Find
Haroware Address	00-11-22-33-44-55-FF	ype All	) wgmt	[	Find
tal Entries: 3	00-11-22-33-44-55-FF	ype All 💟	() Mgmi	[	Find Clear All
Hardware Address tal Entries: 3 Interface Name	IP Address	Hardware Address	Aging Time (min)	Туре	Find Clear All
Hardware Address tal Entries: 3 Interface Name vlan1	IP Address 192.168.70.14	Hardware Address	Aging Time (min) 240	Туре	Find Clear All Clear
Haroware Address tal Entries: 3 Interface Name Vian1 Vian1	IP Address 192.168.70.14 192.168.70.123	Hardware Address 10-BF-48-D6-E2-E2 F0-7D-68-36-30-00	Aging Time (min) 240 Forever	Туре	Find Clear All Clear Clear

図 9-6 ARP Table 画面

## 画面に表示される項目:

項目	説明
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Interface VLAN	表示するインタフェースの VLAN ID を入力します。1 から 4094 で指定できます。
IP Address	表示する IP アドレスを入力します。
Mask	上記 IP アドレスのマスクを指定します。
Hardware Address	表示する MAC アドレスを入力します。
Туре	表示する ARP の種類を指定します。「All」「Dynamic」から指定できます。
Mgmt	管理ポートについての情報を表示します。

「Find」ボタンをクリックして入力した情報に基づく指定のエントリを検索します。 「Clear All」ボタンをクリックするとテーブル上のエントリが全て消去されます。

削除するエントリの「Delete」ボタンをクリックするとエントリが削除されます。

## Gratuitous ARP (Gratuitous ARP 設定)

Gratuitous ARP として知られている ARP 通知は、TAP と SPA が等しい場合、それを送信したホストに有効である SHA と SPA を含むパケット (通常 ARP リクエスト)です。このリクエストは、応答を求めることを意図されたものでなく、パケットを受信する他のホストの ARP キャッシュを更新しません。

本機能は、起動時に多くのオペレーティングシステムで一般的に行われています。これは、ネットワークカードの変更により、MAC アドレスに対する IP アドレスのマッピングが変更になっていても、他のホストがまだその ARP キャッシュに古いマップを持っているというような問題が発生した場合に、その問題を解決します。

Gratuitous ARP のグローバル設定を行います。

L3 Features > Gratuitous ARP の順にメニューをクリックし、以下の画面を表示します。

Gratuitous ARP	_	_		
Gratuitous ARP Global Settings				
IP Gratuitous ARP State	Enabled	Disabled		
Gratuitous ARP Trap State	O Enabled	Disabled		
IP Gratuitous ARP Dad-Reply State	O Enabled	Disabled		
Gratuitous ARP Learning State	Enabled	Obisabled		Apply
Gratuitous ARP Send Interval				
Total Entries: 1				
Interface Name			Interval Time (sec)	
vlan1			0	Edit
				1/1  < < 1 > >  Go

図 9-7 Gratuitous ARP 画面

#### 画面に表示される項目:

項目	説明
IP Gratuitous ARP State	ARP キャッシュテーブルの Gratuitous ARP パケットの習得を「Enabled」(有効)/「Disabled」(無効)にします。
Gratuitous ARP Trap State	Gratuitous ARP トラップを「Enabled」(有効)/「Disabled」(無効)にします。
IP Gratuitous ARP	IP Gratuitous ARP Dad-reply を「Enabled」(有効)/「Disabled」(無効)にします。
Dad-Reply State	
Gratuitous ARP Learning State	受信した Gratuitous ARP パケットに基づいて、ARP キャッシュの更新を有効または無効にします。スイッチが ARP テーブルに Gratuitous ARP パケットと送信元の IP アドレスを受信すると、ARP エントリを更新する必要が あります。初期値は「Disabled」です。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

「Edit」をクリックして指定エントリを再編集します。以下の項目を使用して設定します。

項目	説明				
	Gratuitous ARP Send Interval				
Interval Time(sec)	定期的に Gratuitous ARP を送信する間隔 (秒) を入力します。0 は Gratuitous ARP リクエストが定期的に送信されないことを意味します。 初期値は 0(秒) です				
	ことをやします。 初期値は 5(だ) にす。				

「Gratuitous ARP Global Settings」セクションにある「Apply」ボタンをクリックしてこのセクションで行った変更を適用します。

「Gratuitous ARP Send Interval」セクションにある「Apply」ボタンをクリックして行った変更を適用します。

## IPv6 Neighbor (IPv6 ネイバ設定)

スイッチの IPv6 ネイバ設定を行います。

L3 Features > IPv6 Neighbor の順にメニューをクリックし、以下の画面を表示します。

Pv6 Neighbor	_		_	_	_	_
IPv6 Neighbor Settings IPv6 Neighbor	or Force Aging Address	3				
Interface VLAN (1-4094)	IPv6 Address	2013::1	MAC Address	11-22-33-44-AA	FF	Apply
Interface VLAN (1-4094)	IPv6 Address	2013::1			Find	Clear
Total Entries: 1						Clear All
IPv6 Address	Link-Lay	er Address	Interface	Туре	State	
2018::1	00-11-22	2-33-44-56	vlan1	Static		Delete
				1/1	< <	1 > > Go

図 9-8 IPv6 Neighbor 画面

「IPv6 Neighbor Settings」タブには次の項目があります。

項目	説明
Interface VLAN	IPv6 Neighbor のインタフェース VLAN(1-4094)を指定します。
IPv6 Address	IPv6 Neighbor の IPv6 アドレスを入力します。
MAC Address	対応する IPv6 デバイスの MAC アドレスを指定します。

## ■ IPv6 Neighbor の新規登録

画面上段の「Interface VLAN」、「IPv6 Address」および「MAC Address」を入力し、「Apply」ボタンをクリックします。

## ■ エントリの検索

画面中央の「Interface VLAN」、「IPv6 Address」を入力し「Find」ボタンをクリックします。

## ■ 検索結果の削除

検索結果を削除するには、「Clear」、表示されているすべてのエントリを削除するには、「Clear All」ボタンをクリックします。

## ■ エントリの削除

該当エントリの「Delete」ボタンをクリックします。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「IPv6 Neighbor Force Aging Address」タブをクリックすると次の画面が表示されます。

IPv6 Neighbor				
IPv6 Neighbor Settings	IPv6 Neighbor Force Aging Add	ress		
Interface VLAN (1-4094)	IPv6 Address	2013::1		Apply
Total Entries: 1				
IPv6 Ad	dress	Interface		
2018	::2	vlan1		Delete
			1/1 < -	1 > > Go

図 9-9 IPv6 Neighbor Force Aging Address 画面

「IPv6 Neighbor Force Aging Address」タブには次の項目があります。

項目	説明
Interface VLAN	IPv6 Neighbor のインタフェース VLAN(1-4094)を指定します。
IPv6 Address	強制的にエージアウトする IPv6 Neighbor キャッシュエントリの IPv6 アドレスを入力します。

「Apply」ボタンをクリックし、設定内容を適用します。

「Delete」ボタンをクリックし、エントリを削除します。

## Interface (インタフェース設定)

スイッチの IP インタフェース設定を行います。

注意 Vlan Interface を経由して Mgmt 0 の IP アドレス宛に通信を行う事はできません。

注意 Mgmt Port の MAC Address は System MAC を使用し、Vlan 1 と重複するため、同じ スイッチに接続して Mgmt Port と Vlan 1 は使用でき ません。

## IPv4 Interface (IPv4 インタフェース)

スイッチの IP インタフェース設定を行います。

L3 Features > Interface > IPv4 Interface の順にメニューをクリックし、以下の画面を表示します。

nterrace						
face VLAN (1-4/	094)			]	Apply	Find
I Entries: 1					_	
Interface	State	IP Address	Secondary	Link Status		
Interface vlan1	State Enabled	IP Address 10.90.90.90/255.0.0.0 Manual	Secondary No	Up	Edit	Delete

図 9-10 IPv4 Interface 画面

スイッチの現在の IP インタフェース設定が表示されます。

項目	説明
Interface VLAN	設定、表示するインタフェースの VLAN ID を入力します。1 から 4094 までで入力可能です。
設定を変更する際は、必	ヘず「Apply」ボタンをクリックし、設定内容を適用してください。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

「Delete」ボタンをクリックして、指定エントリを削除します。

## ■ IPv4 インタフェースの編集(IPv4 Interface Settings)

指定エントリの「Edit」ボタンをクリックして以下の画面を表示します。

Pv4 Interface Configure				
IPv4 Interface Settings	DHCP Client			
Interface	vlan1			Back
Settings				
State	Enabled			
IP VRF Forwarding				
IP MTU (512-16383)	1500 bytes			
IP Directed Broadcast	Disabled			
Description	64 chars			Apply
IP Settings				
Get IP From	Static			
IP Address	14 14 14 14 1			
Mask	and the second sec			
Secondary			[	Apply Delete
Secondary IP Entry				
Total Entries: 1				
IP Address	Mask	Boot Mode	Secondary	
192.168.10.222	255.255.255.0	Manual	Yes	Delete
			1/1	<pre>1 &gt; &gt;1 Go</pre>

図 9-11 IPv4 Interface (Edit) 画面

画面に表示される項目:

項目	説明
State	該当エントリの IPv4 インタフェースをグローバルに「Enabled」(有効)/「Disabled」(無効)にします。
IP VRF Forwarding	転送される VRF インスタンス名を 12 字以内で入力します。
IP MTU	使用する IP レイヤの MTU 値を入力します。値は 512 to 16383(bytes)の範囲です。初期値は 1500 です。
IP Directed Broadcast	IP インタフェースの IP ダイレクトブロードキャストの状態を「Enabled」(有効)/「 Disabled」(無効)にします。
Description	エントリの概要について入力(64 字以内)します。
Get IP From	IPv4 アドレス、サブネットマスク、デフォルトゲートウェイに設定する「Static」「DHCP」プロトコルを選択します。

項目	説明
IP Address	IPv4 インタフェースに割り当てる IPv4 アドレスを入力します。
Mask	IPv4 インタフェースに割り当てるサブネットマスクを入力します。
Secondary	チェックを入れ IPv4 アドレスとマスクをセカンダリインタフェースとして設定します。

「Apply」ボタンをクリックし、設定を有効にします。

入力 / 指定した変更を破棄し前のページに戻る場合は「Back」をクリックします。

「Delete」ボタンをクリックして、指定エントリを削除します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

## ■ IPv4 インタフェースの編集(DHCP Client)

「IPv4 Interface Configure」の「DHCP Client」タブをクリックして以下の画面を表示します。

IPv4 Interface Configure			
IPv4 Interface Settings	DHCP Client		
DHCP Client Client-ID (1-4094)			
Class ID String	32 chars	Hex	
Host Name	64 chars		
Lease	Minutes	lays (0-10000) 00 V Hours 00 V	Apply

図 9-12 DHCP Client 画面

画面に表示される項目:

項目	説明
DHCP Client Client-ID	VLAN インタフェースを入力します。この 16 進数 MAC アドレスはディスカバメッセージを送信するクライアント ID と
	して使用されます。
Class ID String	最大 32 文字を使用してベンダクラス識別名を入力します。「Hex」にチェックを入れると 16 進数方式になります。
Host Name	ホスト名を入力します。最大64文字で入力可能です。ホスト名はアルファベットで始まり、アルファベットまたは数字
	で終わるようにします。
Lease	DHCP サーバから割り振られる IP アドレスのリース時間を指定します。
記点と本王とス際リーン。	

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

入力 / 指定した変更を破棄し前のページに戻る場合は「Back」をクリックします。

「Delete」ボタンをクリックして、指定エントリを削除します。

## IPv6 Interface (IPv6 インタフェース)

L3 Features > Interface > IPv6 Interface の順にメニューをクリックし、以下の画面を表示します。

v6 Optimistic DAD				
Pv6 Optimistic DAD State	O Enabled	Disabled		Apply
6 Interface				
nterface VLAN (1-4094)				Apply Find
Total Entries: 1				
		IPv6 State	Link Status	
interiace				

図 9-13 IPv6 Interface 画面

以下の項目が表示されます。(IPv6 Optimistic DAD)

項目	説明
IPv6 Optimistic DAD	IPv6 Optimistic DAD を「Enabled」(有効)/「Disabled」(無効)に指定します。
State	

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

以下の項目が表示されます。(IPv6 Interface)

項目	説明
Interface VLAN	設定、表示する IPv6 インタフェースの VLAN ID を入力します。1 から 4094 までで入力可能です。
。 設定を変更する際は、必	ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Find」ボタンをクリック	クして、入力した情報に基づく特定のエントリを検出します。
設定エントリページが複	数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

## IPv6 インタフェースの編集(IPv6 Interface Settings タブ)

指定エントリの「Show Detail」ボタンをクリックして以下の画面を表示します。

IPv6 Interface Settings	Interface IPv6 Address	Neighbor Discover	DHCP	v6 Client	
nterface	vlan1				
Pv6 MTU (1280-65534)	bytes				
Pv6 State	Disabled 🗸			Back	Apply
IPv6 Address Autoconfig					
State	Disabled 🔽	Default			Apply
Static IPv6 Address Settings					
Pv6 Address		EUI-64 Link Local			Apply
NS Interval Settings					
NS Interval (0-3600000)	0 ms				Apply
ND Settings					
Hop Limit (0-255)	0	Reachable Time (0-3600000)	0	ms	
Managed Config Flag	Off 🗸	Other Config Flag	Off	~	
RA Min Interval (3-1350)	0 sec	RA Max Interval (4-1800)	0	sec	
RA Lifetime (0-9000)	0 sec	RA Suppress	Disabled	~	Apply

図 9-14 IPv6 Interface (IPv6 Interface Settings) 画面

#### 画面に表示される項目:

項目	説明			
Interface				
IPv6 MTU	使用する IPv6 レイヤの MTU 値(Byte)を入力します。値は 1280 - 65534 の範囲です。初期値は 1500 です。RA メッ			
	セージ内での通知に使用されます。			
IPv6 State	該当エントリの IPv6 インタフェースをグローバルに「Enabled」(有効)/「Disabled」(無効)にします。			
	IPv6 Address Autoconfig			
State	自動設定(stateless auto-configuration)を「Enabled」(有効)/「Disabled」(無効)に指定します。			
	「Default」に指定すると、インタフェースの初期ルータが指定されます。初期ルータを使用すると初期ルートがイン			
	ストールされます。			
Static IPv6 Address Settings				
IPv6 Address	IPv6 インタフェースに割り当てる IPv6 アドレスを入力します。			
	「EUI-64」- EUI-64 インタフェース ID を使用してインタフェースの IPv6 アドレスを設定します。			
	「Link Local」- IPv6 インタフェースにリンクローカルアドレスを使用します。			
NS Interval Settings				
NS Interval	NS Interval を 0 から 3600000 ミリ秒で設定します。			
ND Settings				
Hop Limit (0-255)	この RA メッセージを受信するホストに送信されるパケットのために IPv6 ヘッダ内の「hop_limit」フィールドの初			
	期値を指定します。			
Reachable Time (0-3600000)	到達可能時間(0-3600000/ミリ秒)を指定します。「0」に指定すると、ルータはインタフェースで1200秒使い、RAメッ			
	セージでは0を通知します。到達可能時間はノードが隣接しているノードを到達可能と見なすまでの時間(ミリ秒)を			
	指定します。			
Managed Config Flag	• On - この RA を受信するホストは、ステートレスアドレス設定から取得したアドレスに加え、アドレス取得のため			
	にステートフルアドレス設定プロトコルを使用する必要があります。			
	• Off - アドレス取得のためにステートフルアドレス設定を使用した RA の受信を停止します。			
Other Config Flag	<ul> <li>On - この RA を受信するホストは、ステートレスアドレス設定から取得したアドレスに加え、アドレス取得のため</li> </ul>			
	にステートフルアドレス設定プロトコルを使用する必要があります。			
	• Off - アドレス取得のためにステートフルアドレス設定を使用した RA の受信を停止します。			
RA Min Interval	RA 通知が送信される最小時間 (3-1350 秒) を入力します。最大値の 3/4 より大きくしないでください。			
RA Max Interval	RA 通知が送信される最大時間 (4-1800 秒) を入力します。			
RA Lifetime	RA の生存時間(0-9000 秒)を指定します。			
RA Suppress	RA 通知の停止を「Enabled」(有効)/「Disabled」(無効)にします。			

「Apply」ボタンをクリックし、設定を有効にします。

## IPv6 インタフェースの編集(Interface IPv6 Settings タブ)

指定エントリの「Show Detail」ボタンをクリックして、「Interface IPv6 Address」タブを表示します。

v6 Interface				
IPv6 Interface Settings	Interface IPv6 Address	Neighbor Discover	DHCPv6 Client	
otal Entries: 0				
Address Type		IPv6 Address		

図 9-15 IPv6 Interface (Interface IPv6 Address) 画面

#### ■ エントリの削除

対象のエントリの「Delete」ボタンをクリックします。

## IPv6 インタフェースの編集( Neighbor Discover タブ)

指定エントリの「Show Detail」ボタンをクリックして、「Neighbor Discover」タブを表示します。

o interface					
IPv6 Interface Settings	Interface IPv6 Address	Neighbor Discover	C	HCPv6 Client	
Total Entries: 0					
IPv6 Prefix/Prefix Length	Preferred Life Time (sec)	Valid Life Time (sec)	Link Flag	Autoconfig Flag	
9-16 IPv6 Interface (Nei	abbor Discover) 画面				

## IPv6 インタフェースの編集(DHCPv6 Client タブ)

指定エントリの「Show Detail」ボタンをクリックして、「DHCPv6 Client」を表示します。

IPv6 Interface Settings	Interface IPv6 Address	Neighbor Discover	DHCPv6 Client	
HCPv6 Client				Restart
HCPv6 Client Settings				
Client State	Disabled  Ra	apid Commit		Apply
DHCPv6 Client PD Settings				
Client PD State	Disabled 🔽 🛛 Ra	apid Commit		
General Prefix Name	12 chars			Apply
Pv6 Dhcp Client PD Hint	2016::104/64			Apply

図 9-17 IPv6 Interface (DHCPv6 Client) 画面

#### 画面に表示される項目:

項目	説明	
DHCPv6 Client		
Restart	「Restart」をクリックすると、DHCPv6 クライアントサービスを再始動します。	
DHCPv6 Client Settings		
Client State	DHCPv6 クライアントを「Enabled」(有効)/「Disabled」(無効)に指定します。「Rapid Commit」にチェックを入れると、 プリフィクス委任のメッセージ交換を実行します。	
DHCPv6 Client PD Settings		
Client PD State	指定インタフェースに Prefix Delegation (PD) をリクエストする DHCPv6 クライアントプロセスを「Enabled」(有効) /「Disabled」(無効)に指定します。アドレス配布では通常 4 個のメッセージ交換を行いますが、「Rapid Commit」 にチェックを入れると、2 個のメッセージ交換を実行します。	
General Prefix Name	IPv6 の一般的なプリフィクス名(12 字以内)を指定します。	
IPv6 DHCP Client PD Hint	メッセージに含まれる IPv6 プリフィクスのヒントを指定します。	

「Apply」ボタンをクリックし、設定を有効にします。
## Loopback Interface (ループバックインタフェース設定)

ループバックインタフェースを設定します。ループバックインタフェースは、それを無効または削除するまで通常アクティブな論理 IP インタフェー スで、どんな物理インタフェースの状態からも独立しています。

L3 Features > Interface > Loopback Interface の順にメニューをクリックし、以下の画面を表示します。

lerface Loopback (1-8)				Apply	Find
tal Entrice: 1					
tai citulea. I					
Interface	State	Link Status	Description		

図 9-18 Loopback Interface 画面

画面に表示される項目:

項目	説明	
Interface Loopback	ループバックするインタフェース ID(1-8)を入力します。	
 Apply」をクリックし、設定内容を適用します。		
「Delete」をクリックすると指定のエントリを削除します。		
Interface Loopback 「Apply」をクリックし、設定 「Delete」をクリックすると	ループバックするインタフェース ID(1-8)を入力します。 E内容を適用します。 指定のエントリを削除します。	

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Edit」をクリックして、指定エントリの編集を行います。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

## ループバックインタフェースの編集(Edit)

「Edit」(編集)ボタンをクリックして、以下の画面を表示します。

IPv4 Interface Cont	figure		
Interface	loopback1		Back
Description	64 chars		Apply
IPv4			
IP Address	11 - 2 - 2 - 2	Mask 255 · 0 · 0 · 0	Apply
IPv6			
IPv6 Address		Link Local	Apply
Total Entries: 1			
	Address Type	IPv6 Address	
	Global Unicast Address	2015::15/64 Manual	Delete
		1/1	< < 1 > >  Go

図 9-19 Loopback Interface Settings - Edit 画面

#### 画面に表示される項目:

項目	説明
State	本ループバックインタフェースを「Enabled」(有効)/「Disabled」(無効)に指定します。
Description	本ループバックインタフェースの概要(64 字以内)を指定します。
IP Address	本ループバックインタフェースの IPv4 アドレスを入力します。
Mask	本ループバックインタフェースに割り当てるサブネットマスクを入力します。
IPv6 Address	本ループバックインタフェースの IPv6 アドレスを入力します。
Link Local	指定した IPv6 アドレスをリンクローカル IPv6 アドレスとして指定します。

該当項目を入力後、「Apply」ボタンをクリックし、設定内容を適用します。

「Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

### インタフェースの削除

「Delete」ボタンをクリックして、指定エントリを削除します。「Delete All」ボタンをクリックして、テーブルに表示されたすべてのエントリを削除 します。

注意 R1.xx 系と R2.xx 以降でインタフェース名が変更になっています。

- 1.xx 系:loopback 1

- 2.xx 系:Loopback1

## Null Interface (Null インタフェース)

Null インタフェースを設定します。

## L3 Features > Interface > Null Interface の順にメニューをクリックし、以下の画面を表示します。

terface Null (0-0)				Apply
tal Entries: 1				
otal Entries: 1 Interface	State	Link Status	Description	

図 9-20 Null Interface 画面

#### 画面に表示される項目:

項目	説明
Interface Null	Null インタフェース ID(0)を指定します。「0」のみ指定可能です。
Description	「Edit」をクリックし Null インタフェースの概要(64 字以内)を指定します。

「Apply」をクリックし、設定内容を適用します。

「Edit」をクリックして、指定エントリの編集を行います。

注意 Connected への NullO 経路は参照されません。

# UDP Helper (UDP ヘルパー)

### L3 Features > UDP Helper

IP 転送プロトコルの設定を行います。

## IP Forward Protocol (IP 転送プロトコル)

本項目では、IP 転送プロトコルの設定、表示を行います。本機能は指定の UDP サービスタイプのパケットの転送を有効にします。

#### L3 Features > UDP Helper > IP Forward Protocol の順にメニューをクリックし、以下の画面を表示します。

Forward Protocol		
Forward Protocol UDP Port (1-65535)		Арр
otal Entries: 7		1
UDP Port	Application	
37	Time Service	Delete
42	IEN-116 Name Service	Delete
49	TACACS	Delete
53	DNS	Delete
69	TFTP	Delete
137	NetBIOS-NS	Delete
138	NetBIOS-DS	Delete

図 9-21 IP Forward Protocol 画面

画面に表示される項目:

項目	説明
IP Forward Protocol UDP	転送する UDP サービスの宛先ポート(1-65535)を指定します。
Port	
E	

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

## IP Helper Address(IP ヘルパーアドレス)

本項目では UDP ブロードキャストパケットを転送するターゲットアドレスの追加 / 削除を指定します。本機能は IP アドレスがアサインされた受信 インタフェースのみ有効です。システムは以下の制限をクリアした場合のみパケットを転送します。

- 宛先 MAC アドレスがブロードキャストアドレスである。
- 宛先 IP アドレスがオールワンブロードキャストである。
- ・ パケットが IPv4 UDP パケットである。
- ・「IP TTL 値」が「2」以上である。

#### L3 Features > UDP Helper > IP Helper Address の順にメニューをクリックし、以下の画面を表示します。

IP Helper Address			
IP Helper Address			
Interface VLAN (1-4094)			
VRF State	True		
VRF Name	12 chars 🔽 Global		
Helper Address	20 (20 ) 20 (20 )		Apply
Total Entries: 1			
Interface VLAN	Helper Address	VRF Name	
VLAN1	192.168.10.3		Delete
			1/1 < < 1 > >  Go

図 9-22 IP Helper Address 画面

#### 画面に表示される項目:

項目	説明
Interface VLAN	VLAN インタフェース ID(1-4094)を指定します。
VRF State	VRF の状態を指定します。「True」「False」から指定可能です。
VRF Name	VRF インスタンス名を 12 字以内で入力します。「Global」を指定すると IP アドレスはグローバルアドレスとして指定されます。
Helper Address	UDP ブロードキャストパケットの転送のためのターゲット IPv4 アドレスを指定します。

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

# IPv4 Static/Default Route (IPv4 スタティック / デフォルトルート設定)

本スイッチは IPv4 アドレシングのためにスタティックルーティング機能をサポートしています。IPv4 には最大 512 個のスタティックルートエント リを作成することできます。

IPv4 スタティックルートのために、スタティックルートが一度設定されると、スイッチは設定されたネクストホップルータに ARP リクエストパケットを送信します。ARP の応答をネクストホップからスイッチが取得すると、ルートは有効になりますが、ARP エントリが既に存在している場合にはと、ARP 要求は送信されません。

また、スイッチはフローティングスタティックルートをサポートしています。これは、同じネットワークにある異なるネクストホップデバイスに代替のスタティックルートを作成できるものです。この2個目のネクストホップデバイスのルートは、プライマリスタティックルートがダウンした場合のバックアップ用スタティックルートであると見なされます。プライマリルートをなくした場合、バックアップルートがリンクアップし、アクティブな状態になります。本スイッチのフォワーディングテーブル内へのエントリはIPアドレスのサブネットマスクとゲートウェイの両方を使用して行います。

L3 Features > IPv4 Static/Default Route の順にメニューをクリックし、以下の画面を表示します。

IPv4 Static/Default Rou	ıte	_			_
IPv4 Static/Default Route					
VRF Name	12 chars				
IP Address		Mask	Default Route		
IP Tunnel (0-9999)		IP Tunnel			
Gateway	N 14 140				
Null Interface	Disabled	~			
Backup State	Please Select	~			Apply
VRF Name	12 chars				Find
Total Entries: 1					
IP Address	Mask	Gateway	Interface Name	VRF Name	
0.0.0	0.0.00	192.168.70.1	vlan1		Delete
				1/1 < < 1	> >  Go



#### 画面に表示される項目:

項目	説明
VRF Name	VRF インスタンス名を 12 字以内で入力します。
IP Address	スタティックルートに割り当てる IPv4 アドレスを入力します。「Default Route」をチェックすると、デフォルトルート
	に割り当てられます。
Mask	対応するサブネットマスクを入力します。
IP Tunnel	IP トンネル ID(0-9999)を指定します。
Gateway	対応するゲートウェイ IP アドレスを入力します。
Null Interface	ネクストホップとして Null インタフェースを有効または無効にします。Null インタフェースはトラフィックをフィルタ
	する別の方法を提供します。Null インタフェースに送信されるパケットはスイッチに破棄されます。
Backup State	Primary、Backup、または Weight から選択します。
	・ Primary - 宛先へのルートをプライマリルートとして指定します。
	・ Backup - 宛先へのルートをバックアップルートとして指定します。
	• Weight - 「0」以上の重みを指定しますが、最大パス数よりは小さくなります。本数値はルーティングテーブルの指
	定ルートパスの複製(複数の)に使用され、これによりパスはトラフィックルーティングに当たる確率が上がります。
	「Weight」選択後に表示される空欄に数値(1-64)を指定します。

「Apply」ボタンをクリックして行った変更を適用します。

### ■ エントリの削除

対象のエントリの行の「Delete」ボタンをクリックします。

## IPv4 Static Route BFD (IPv4 スタティックルート BFD)

本項目では IPv4 スタティックルート BFD(Bidirectional Forwarding Detection)の設定と表示を行います。

L3 Features > IPv4 Static Route BFD の順にメニューをクリックし、以下の画面を表示します。

v4 Static Route BFD				
nterface Name	12 chars	IP Address		Apply
otal Entries: 1				
and the second state of th				
1	nterface Name	IP Addres	s	

図 9-24 IPv4 Static Route BFD 画面

画面に表示される項目:

項目	説明
Interface Name	BFD セッションを作成するインタフェース名を 12 字以内で入力します。
IP Address	BFD ピアの IP アドレスを指定します。

「Apply」をクリックし、設定内容を適用します。 「Delete」をクリックすると指定のエントリを削除します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

## IPv4 Route Table (IPv4 ルートテーブル)

IP ルーティングテーブルはスイッチに関するすべての外部経路情報を保存します。ここではスイッチにおけるすべての外部経路情報を参照します。

L3 Features > IPv4 Route Table の順にメニューをクリックし、以下の画面を表示します。

v4 Route Tak	ole					
IP Address     Network A     RIP	ddress	· · · · · · · · · · · · · · · · · · ·	Summary	·		Find
IP Address	Mask	Gateway	Interface	Distance/Metric	Protocol	Candidate Default
in Franciss						

図 9-25 IPv4 Route Table 画面

画面には以下の項目が表示されます。一部項目は EI/MI モードのみに対応しています。

項目	説明
IP Address	表示するルートの宛先 IP アドレスを指定します。
Network Address	表示するルートの宛先ネットワークアドレスを指定します。1つ目の入力欄にネットワークプレフィックス、2つ目の入力欄
	にネットワークマスクを入力します。
RIP	本項目を選択すると、RIP ルートだけを表示します。
OSPF	本項目を選択すると、OSPF ルートだけを表示します。
BGP	本項目を選択すると、BGP ルートだけを表示します。
ISIS	本項目を選択すると、ISIS ルートエントリを表示します。
Connected	接続中のみ機器を表示します。
Hardware	チェックを入れるとチップに記録されたルートのみ表示されます。
Summary	アクティブなルーティングエントリのサマリを表示します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。

-「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。 複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

# IPv6 Static/Default Route (IPv6 スタティック / デフォルトルート設定)

IPv6 アドレスのスタティックエントリは IPv6 形式のアドレスで本スイッチのルーティングテーブルに入力します。

L3 Features > IPv6 Static/Default Route の順にメニューをクリックし、以下の画面を表示します。

IPv6 Static/Default Route					_	
IPv6 Static/Default Route						
IPv6 Address/Prefix Length	2013::1/64	Default Route				
IP Tunnel (0-9999)		IP Tunnel				
Interface Name	12 chars					
Next Hop IPv6 Address	3FE1::1					
Distance (1-254)						
Backup State	Please Select 🗸					Apply
Total Entries: 1						
IPv6 Address/Prefix Leng	th Next Hop	Interface Name	Distance/Metric	Protocol	Active	
::/0	3FE1::1		10/1	Static	No	Delete
				1/1	< 1 >	>  Go

図 9-26 IPv6 Static/Default Route 画面

#### 画面に表示される項目:

項目	説明
IPv6 Address/Prefix Length	ルートの宛先ネットワークを入力するか、「Default」をチェックしてデフォルトルートに割り当てます。
IP Tunnel	「IP Tunnel」をチェックして、使用する IP トンネル名を入力します。
Interface Name	スタティック IPv6 ルートが作成される IP インタフェース名を指定します。
Next Hop IPv6 Address	IPv6 形式におけるネクストホップゲートウェイアドレスに対応する IPv6 アドレスを指定します。
Distance	スタティックルートの管理ディスタンス(1-254)を指定します。低値がより良いルートを意味します。指定されない と初期値の「1」に設定されます。
Backup State	各 IPv6 アドレスは 1 つのプライマリルートを持っており、一方、他のルートはバックアップ状態に割り当てられる必要があります。プライマリルートに障害が発生すると、スイッチはバックアップルートを試します。IPv6 が設定されるバックアップ状態を示します。「Primary」または「Backup」を指定します。

「Apply」ボタンをクリックして行った変更を適用します。

#### ■ エントリの削除

テーブル内の削除するエントリの「Delete」ボタンをクリックします。すべてのエントリを削除するためには、「Delete All」ボタンをクリックします。

## IPv6 Static Route BFD (IPv6 スタティックルート BFD)

本項目では IPv6 スタティックルート BFD (Bidirectional Forwarding Detection)の設定と表示を行います。

#### L3 Features > IPv6 Static Route BFD の順にメニューをクリックし、以下の画面を表示します。

v6 Static Route BFD				
nterface Name	12 chars	IPv6 Address	2015::101	Apply
otal Entries: 1 In	iterface Name	IPv6 Addres	s	

図 9-27 IPv6 Static Route BFD 画面

画面に表示される項目:

項目	説明
Interface Name	BFD セッションを作成するインタフェース名を 12 字以内で入力します。
IPv6 Address	BFD ピアの IPv6 アドレスを指定します。
- [Δnnlv] をクロッ	/ クレー 設定内容を適用します

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

# IPv6 Route Table (IPv6 ルートテーブル)

現在の IPv6 ルーティングテーブルを表示します。

L3 Features > IPv6 Route Table の順にメニューをクリックし、以下の画面を表示します。

Pv6 Route Table			_	_	_	_
Pv6 Route Table						
Please Select	Database					
OHardware						
OSummary						
						Find
Total Entries: 0 entries, 0 routes						
IPv6 Address/Pro	efix Length	Next Hop	Interface	Distance/Metric	Protocol	Valid Route Selected Ro

図 9-28 IPv6 Route Table 画面

画面には以下の項目が表示されます。一部項目は EI(または MI)モードのみに対応しています。

項目	説明
IPv6 Address	プルダウンメニューから本項目を選択し、IPv6 アドレスを入力します。
IPv6 Address/Prefix Length	プルダウンメニューから本項目を選択し、ルートの IPv6 アドレスとプリフィクスを指定します。「Longer Prefixes」
	を指定するとプリフィクス長と同等、もしくはそれよりも長いプリフィクスの IPv6 ルートを表示します。
Interface Name	プルダウンメニューから本項目を選択し、表示するインタフェース名を指定します。
Connected	本項目を選択すると、接続中のみ機器を表示します。
RIPng	本項目を選択すると、RIPng ルートエントリを表示します。
OSPFv3	本項目を選択すると、OSPFv3 ルートエントリを表示します。
ISIS	本項目を選択すると、ISIS ルートエントリを表示します。
BGP	本項目を選択すると、BGP ルートだけを表示します。
Database	本項目を選択すると、ベストルートの代わりにルーティングデータベースの関連するすべてのエントリを表示します。
Hardware	本項目を選択すると、ハードウェアテーブルに記述されているルートだけを表示します。
Summary	本項目を選択すると、アクティブなルーティングエントリのサマリを表示します

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

# Route Preference (ルート優先度設定)

ルート優先度を設定します。小さい優先度値を持つルートほど高いプライオリティを持ちます。ルート信頼度レーティングを示唆するディスタンス を設定します。低いディスタンスがより高い優先値を意味します。ディスタンス 255 のルートは信頼度がないと見なされ、ルーティングパケットと してインストールされません。

L3 Features > Route Preference の順にメニューをクリックし、以下の画面を表示します。

Route Preference			
Route Preference			
VRF Name	12 chars	Please Select	
Distance Default (1-255)	1		
Distance Static (1-255)	60		Apply

図 9-29 Route Preference 画面

画面に表示される項目:

項目	説明
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Distance Default	デフォルトルートの管理優先度値(ディスタンス)を設定(1-255)します。初期値は 1 です。
Distance Static	Static 初期ルート優先度(ディスタンス)を指定(1-255)します。初期値は 60 です。
E	

「Apply」ボタンをクリックし、設定を有効にします。

「Please Select」をクリックすると次の画面が表示されます。

Route Preference			
Route Preference			
VRF Name	12 chars	Please Select	
Distance Default (1-255)	1		
Distance Static (1-255)	60		Apply

図 9-30 Route Preference (Please Select) 画面

VRF エントリを選択し、「OK」ボタンをクリックして、VRF エントリを選択します。 複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

## ECMP Settings (ECMP 設定) (EI/MI モードのみ)

このスイッチに ECMP OSPF 状態と ECMP ルートロードバランシングアルゴリズムを設定します。

L3 Features > ECMP Settings をクリックし、以下の画面を表示します。

ECMP Settings		
ECMP Load Balancing Settings		
Destination IP		
Source IP		
CRC 32 Lower		
CRC 32 Upper		
TCP/UDP Port		Apply
ECMP Advance Control Mode		
ECMP Advance Control Mode Setting	128	
ECMP Maximum Number of Path Running	32	Apply

図 9-31 ECMP Settings 画面

### 画面に表示される項目:

項目	説明
	ECMP Load Balancing Settings
Destination IP	ECMP ハッシュ鍵として宛先 IP を使用します。
Source IP	ECMP ハッシュアルゴリズムとして送信元 IP の下位ビットを使用します。
CRC 32 Lower	ECMP ハッシュアルゴリズムとして CRC-32 の下位ビットを使用します。
CRC 32 Upper	ECMP ハッシュアルゴリズムとして CRC-32 の上位ビットを使用します。
TCP/UDP Port	ECMP ハッシュ鍵として TCP または UDP ポート番号を使用します。
	ECMP Advance Control Mode
ECMP Advance	ECMP アドバンスコントロールモードの設定を行います。本設定では ECMP とマルチパスルートの数値と各 ECMP、または
Control Mode Setting	マルチパスルートのネクストホップ値を指定の値に変更、設定します。「64」「128」「256」「512」「1024」から指定します。
「Apply」ボタンをクリ	ックして行った変更を適用します。

## IPv6 General Prefix (IPv6 汎用プリフィクス)

本項目では、VLAN インタフェース IPv6 汎用プリフィクスの設定、表示を行います。

L3 Features >	IPv6 General	Prefix 7	をクリ	ックし、	以下の画面を表示しま	ミす。
					, , , , <u>, , , , , , , , , , , , , , , </u>	

IPv6 General Prefix				
IPv6 General Prefix				
Interface VI AN (1-4094)				
Drefy Name	12 abore			
Freix Name	12 chars			
IPv6 Address	2233::1/64			Apply
Prefix Name	12 chars			Find
Total Catalogs 4				
Total Entries: 1				
Prefix Name	Туре	Interface	IPv6 Address	
prefix	Acquired via Unassigned	vlan1	2233::1/64	Delete
			1/1 < <	1 > > Go

図 9-32 IPv6 General Prefix 画面

画面に表示される項目:

項目	説明
Interface VLAN	VLAN インタフェース ID(1-4094)を指定します。
Prefix Name	IPv6 汎用プリフィクスエントリ名(12 字以内)を指定します。
IPv6 Address	IPv6 アドレスとプリフィクス長を指定します。IPv6 アドレスのプリフィクス長は VLAN インタフェースのローカルサブネットでもあります。

「Apply」ボタンをクリックして行った変更を適用します。

「Delete」をクリックすると指定のエントリを削除します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

# IP Tunnel Settings (IP トンネル設定)

IP トンネルを設定します。

L3 Features > IP Tunnel Settings の順にメニューをクリックして以下の画面を表示します。

unnel Settings					
erface Tunnel ID (0-9999)				Apply	Find
tal Entries: 1					
			Description		
Interface	Status	Administrative	Description		
Interface tunnel1	Status	Enabled	Description	Edit	Delete

図 9-33 IP Tunnel Settings 画面

画面に表示される項目:

項目	説明
Interface Tunnel ID	IP トンネルのインタフェース ID(0-9999)を入力します。

### ■ エントリの登録

「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

#### ■ エントリの検索

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。「Show All」ボタンをクリックして、すべての定義済みエントリを表示します。

### ■ エントリの削除

テーブル内の削除するエントリの「Delete」ボタンをクリックします。すべてのエントリを削除するためには、「Delete All」ボタンをクリックします。

### ■ エントリの編集

編集するポートの「Edit」ボタンをクリックし、以下の画面を表示します。

IP Tunnel Configure		
IP Tunnel Configure		
Interface Tunnel ID	1	
Status	Up	
Description	64 chars	
Tunnel Mode	IPv6 IP	
Source IPv4 Address	the second second	
Source IPv6 Address	2015::1	
O Destination IPv4 Address	and the second second	
<ul> <li>Destination IPv6 Address</li> </ul>	2016::1	
Network Address		
IPv6 Address/Prefix Length	2013::1/64	Apply Back
Total Entries: 0		
Ad	ldress Type	IPv6 Address

図 9-34 IP tunnel Settings - Edit 画面

画面に表示される項目:	
項目	説明
Status	IP トンネルインタフェースの状態を「Up」「Down」から指定します。
Description	IP トンネルインタフェースの概要(64 字以内)を指定します。
Tunnel Mode	プルダウンメニューを使用してトンネルモードを選択します。「IPv6 IP」「6to4」「ISATAP」「GRE IP」「GRE IPv6」か ら選択します。 • IPv6 IP - IPv6 IP トンネルインタフェースとして指定します。 • 6to4 - 6to4 トンネルインタフェースとして指定します。 • ISATAP - ISATAP トンネルインタフェースとして指定します。 • GRE IP - GRE IP トンネルインタフェースとして指定します。到達プロトコルは IPv4 プロトコルです。 • GRE IPv6 - GRE IP トンネルインタフェースとして指定します。到達プロトコルは IPv6 プロトコルです。
Source IPv4/IPv6 Address	送信元 IPv4/IPv6 アドレスを指定します。
Destination IPv4/IPv6 Address	送信先 IPv4/IPv6 アドレスを指定します。
Network Address	アドレスネットワークアドレスを入力します。
IPv6 Address/Prefix Length	IPv6 アドレスネットワークアドレスとプリフィクス長を入力します。

項目を編集し、エントリの「Apply」ボタンをクリックします。

「Back」をボタンをクリックして前のページに戻ります。

## URPF Settings (URPF 設定)

本項目では「Unicast Reverse Path Forwarding」(URPF)の設定と表示を行います。ネットワークへの攻撃としてよくある手段に、IPv4/IPv6 送信元ア ドレススプーフィング発動があります。この方法として、ターゲットに知られた / 信頼された送信アドレスのネットワークにトラフィックを送信し ます。防御が設定されていない場合、ネットワーク組織は複数の種類の攻撃にオープンになり、トラッフィックを許可してしまいます。ユニキャス ト RPF はルータを通過する不正 / 偽造 IPv4/IPv6 アドレスによって生成された問題を軽減させることができます。

L3 Features > URPF Settings の順にメニューをクリックして以下の画面を表示します。

IRPF Settings					
JRPF Global Settings	) Enabled ) Disab	led			Apply
IRPF Port Default Settings					
Unit From Port	To Port eth1/0/1 💌	Reachable Via Allo	w Default IP Access Default Default	List Name IPv6 Acces	s List Name Apply
Unit From Port  Voit Settings Unit 1 Settings Unit 1 Settings	To Port eth1/0/1	Reachable Via Allo	w Default IP Access Ilse  32 chars	List Name IPv6 Acces 32 chars	s List Name Apply
Port	State	Reachable Via	Allow Default	IP Access List Name	IPv6 Access List Name
eth 1/0/1	Disabled	RX	False		
eth 1/0/2	Disabled	RX	False		
eth1/0/3	Disabled	RX	False		
eth 1/0/4	Disabled	RX	False		
eth 1/0/5	Disabled	RX	False		
eth 1/0/6	Disabled	RX	False		
eth 1/0/7	Disabled	RX	False		
eth1/0/8	Disabled	RX	False		

図 9-35 URPF Settings 画面

# 第9章 L3 Features (レイヤ3機能の設定)

画面に表示される項目:

項目	説明
	URPF Global Settings
URPF State	URPF を「Enabled」(有効)/「Disabled」(無効)に指定します。
	注意 有効になると、まずハードウェアルーティングテーブルの「Session Initiation Protocol」(SIP)を使った検出が必要になり、 その後「Dynamic Inspection Protocol」(DIP)を使用します。これによりテーブルは半分に分割され、IP ルーティングテー ブルは半分に削減されます。本設定はコンフィグを保存した上で、スイッチを再起動して初めて有効になります。
	URPF Port Default Settings
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。
Reachable Via	「RX」経由の到達可能な初期設定を使用します。
Allow Default	「default allow」の初期設定を使用します。「False」を意味します。
IP Access List Name	初期設定の IP アクセスリストを使用します。
IPv6 Access List	初期設定の IPv6 アクセスリストを使用します。
Name	
	URPF Port Default Settings
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。
Reachable Via	「Reachable Via」のオプションを選択します。
	• Any - 送信元アドレスがルーティングテーブルに存在しているか確かめます。(loose モードとして認識されます。)
	• RX - 送信元アドレスがルーティングテーブルに存在しているか、また送信元とマッチする内向きインタフェースがパ
	ケットが受信するインタフェースを通して到達可能がを確かめます。
Allow Default	Allow Default」のオプションを選択します。
	<ul> <li>Irue - ユニギャスト KPF 確認の初期ルートを使用します。</li> </ul>
	• False - ユニキヤスト KPF 確認の初期ルートを使用しません。
IP Access List Name	UKPF ナエツクに使用する IF アクセスリスト名(32 字以内)を指定します。
IPv6 Access List	URPF チェックに使用する IPv6 アクセスリスト名(32 字以内)を指定します。
Name	

「Apply」をクリックし、設定内容を適用します。

# VRF (Virtual Routing and Forwarding) (EI/MI モードのみ)

「Virtual Routing and Forwarding」(VRF)の設定を行います。

## VRF Settings (VRF 設定)

本項目では「Virtual Routing and Forwarding」(VRF)の設定、表示を行います。

## L3 Features > VRF > VRF Settings の順にメニューをクリックして以下の画面を表示します。

F Settings					
RF Name 12	chars		Apply	Find	Show All
otal Entries: 1					
VRF Name	RD	Interfaces			
vrf1	Not Set		Edit	Show Detail	Delete
			4/4		

図 9-36 VRF Settings 画面

画面に表示される項目:

項目	説明		
VRF Name	F インスタンス名を 12 字以内で入力します。		
「Apply」をクリックし、	 Apply」をクリックし、設定内容を適用します。		
¯Delete」をクリックすると指定のエントリを削除します。			
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。			
Show All」をクリックして、すべてのエントリを表示します。			
<sup>-</sup> Show Detail」をクリックして、指定エントリの詳細について表示します。			
「Edit」をクリックして	、指定エントリの編集を行います。		

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Edit」ボタンをクリックすると、以下の画面が表示されます。

VRF Settings		
VRF Name	vrf1	Back
Max Routes (1-16384)	Warning Threshold (1-100)	Apply
VRF Import Map Settings Import Map Name () 16 chars	○ None	Apply
Route Distinguisher Settings – Route Distinguisher ASN:NN or IP:NN		Apply
VPN Route Target Community S Route Target Extended Commu ASN:NN or IP:NN	Settings Nity Route Target Type Import	Apply

図 9-37 VRF Settings (Edit) 画面

以下の項日が表示されます	[Back]	をクリックす	スと前のペー	ジに豆りすす
以下の項目が衣小でれより。	Dack_	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	ると別のへ	ノに庆りより。

項目	説明
	VRF Max Routes Settings
Max Routes	VRF 内の最大ルート数(1-16384)を入力します。
Warning Threshold	警告しきい値を指定します。これ以上ハードウェアに記録できないルート数のしきい値に達すると通知メッセージが送信され ます。1-100 パーセントで指定します。「warning-only」を指定すると、しきい値を超えると通知が発生するものの、ハードウェ アへの記録は継続します。
None	制限を指定しません。
	VRF Import Map Settings
Import Map Name	VRF のインポートルートマップを指定します。
None	VRF のインポートルートマップを無効にします。
	Route Distinguisher Settings
Route Distinguisher	VRFのRoute Distinguisher (RD)を指定します。VPN-IPv4プリフィクスを作成する8バイトの値をIPv4プリフィクス指定します。
	VPN Route Target Community Settings
Route Target Extended Community	ルートターゲットを指定します。ルートターゲットは VPN のアプリケーションです。 VRF 一つにつき複数のルートターゲットがあります。
Route Target Type	<ul> <li>ルートターゲットの種類を指定します。</li> <li>Import - ターゲット VPN 拡張コミュニティからのインポートルーティング情報となるインポートルートを追加します。</li> <li>Export - ターゲット VPN 拡張コミュニティからのエクスポートルーティング情報となるエクスポートルートを追加します。</li> <li>Both - インポートルート / エクスポートルートどちらも追加します。</li> </ul>

「Apply」をクリックし、設定内容を適用します。

「Show Detail」をクリックすると、以下の画面が表示されます。

VRF Detail Information			
VRF Detail Information Table			
VRF Name	vrf1		
Default RD	Not Set		
Interfaces	Show Detail		
No Export VPN Route-target Community			
No Import VPN Route-target Community			
No Import Route-map			
			Back
Interfaces			
Total Entries: 1			
		Interface	
		loopback1	
			1/1 K < 1 > X Go

図 9-38 VRF Settings (Show Detail) 画面

「Back」をクリックすると前のページに戻ります。

## VRF Interface Settings (VRF インタフェース設定)

本項目では VRF インタフェースの設定、表示を行います。

L3 Features > VRF > VRF Interface Settings の順にメニューをクリックして以下の画面を表示します。

VRF Interface Settings			
VRF Interface Settings			
Interface VLAN (1-4094)	VRF Name		
	12 chars		Apply
VDF Loophask Interface Settings			
VRF Loopback Interface Settings			
Loopback Interface (1-8)	VRF Name		
1	12 chars		Apply
Find VRF Interface			
The VA menue			
VRF Name			
12 chars			Find
Total Entries: 1			
Interfaces	IP Address	VRF	
loopback1	0.0.0/0	vrf1	Delete
			1/1 < < 1 > > Go

図 9-39 VRF Interface Settings 画面

画面に表示される項目:

項目	説明		
VRF Interface Settings			
Interface VLAN	VLAN インタフェース ID(1-4094)を指定します。		
VRF Name	VRF インスタンス名を 12 字以内で入力します。		
	VRF Loopback Interface Settings		
Loopback Interface	ループバックインタフェース ID(1-8)を指定します。		
VRF Name	VRF インスタンス名を 12 字以内で入力します。		
Find VRF Interface			
VRF Name	VRF インスタンス名を 12 字以内で入力します。		

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

# **RIP** (Routing Information Protocol)

#### L3 Features > RIP

RIP (Routing Information Protocol) は、距離ベクトル型のルーティングプロトコルです。

## RIP Settings (RIP 設定)

IP インタフェースに RIP 設定を行います。

L3 Features > RIP > RIP Settingsの順にメニューをクリックし、以下の画面を表示します。RIPの設定を行ったインタフェースのリストが表示されます。

RIP Settings			_	
RIP Global Settings	Enabled ODisabled			Apply
VRF Address Family Table – VRF Name	12 chars			Apply
Total Entries: 2				
	VRF			
		Edit	Delete	
	vrf1	Edit	Delete	
			1/1  <	< 1 > > Go

図 9-40 RIP Settings 画面

### 画面に表示される項目:

項目	説明		
RIP Global Settings			
RIP State	State RIP の状態を有効または無効にします。初期値は無効です。		
	VRF Address Family Table		
VRF Name     RIP の状態を有効または無効にします。初期値は無効です。			

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

「Edit」をクリックして、指定エントリの編集を行います。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

#### エントリの編集

「Edit」ボタンをクリックすると、以下の画面が表示されます。

VRF Name	VRF	Back
Redistribution Configuration		
Redistribution	Disabled BGP metric (0-16) route-map (16 chars)	Apply
RIP Configuration		
Update Timer (1-65535)	30 sec 🗌 Default	
Invalid Timer (1-65535)	180 sec 🗌 Default	
Garbage Collection Timer (1-65535)	120 sec Default	
Default Metric (0-16)	0 Default	
Version	v1 Default	
Distance (1-255)	100 Default	
Send Version	v1	
Receive Version	any version	
Next Update	22	
Redistribution		
Maximum Path	1	
		Apply
Routing Information Sources		
Total Entries: 0		
Gate	Last Indate	

図 9-41 RIP Settings 画面 – Edit 画面

RIP インタフェース	への設定に使用する項目は以下の通りです。「Back」をクリックすると前のページに戻ります。
項目	説明
	Redistribution Configuration
Redistribution	<ul> <li>次の手順で指定します。</li> <li>1. RIP redistribution (RIP 再分配)機能を「Enabled」(有効) /「Disabled」(無効) に指定します。</li> <li>2. RIP に再分配されるルーティングプロトコル (ドメイン)を指定します。「BGP」「Connected」「OSPF」「Static」「ISIS」から指定します。「Static」は IP スタティックルートを再分配します。「Connected」はインタフェースの IP アドレス設定の際に自動的に構築するルートを意味します。</li> <li>3. 再分配ルートのメトリック値 (0-16)を指定します。</li> <li>4. 現在のルートプロトコルに再分配するルートのフィルタリングに使用するためのルートマップ名を指定します。指定されないと全てのルートが再分配されます。</li> </ul>
	RIP Configuration
Update Time	RIP アップデートメッセージを送信する間隔値 (1-65535 秒) を入力します。「Default」を指定すると初期値の「30」を指定します。
Invalid Time	無効にする値(1-65535 秒)を入力します。「Default」を指定すると初期値の「180」を指定します。
Garbage Collection Timer	フラッシュ値(1-65535 秒)を入力します。「Default」を指定すると初期値の「120」を指定します。
Default Metric	初期メトリック値(0-16 秒)を指定します。他のルーティングプロトコルからの再分配ルートで使用される初期メトリック値を 指定します。再分配されるルートは他のプロトコルに学習され、RIP との互換性がないメトリックになる場合があります。メトリッ クの指定により、メトリックが同期します。「Default」を指定すると初期メトリック値(0)を指定します。
Version	全インタフェースで使用される初期バージョンとしてのグローバル RIP バージョンを指定します。「v1(RIPv1)」「v2(RIPv2)」 から指定します。「Default」を指定すると初期値を使用します。初期値では v1/v2 どちらも受信しますが、v1 のみ送信します。
Distance	RIP の管理ディスタンス(1-255)を指定します。低い値ほど良いルートを意味します。「Default」を指定すると初期値である 100 を使用します。

「Apply」をクリックし、設定内容を適用します。

## RIP Distribute List (RIP ディストリビュートリスト)

RIP ディストリビュートリストの設定を行います。

L3 Features > RIP > RIP Distribute List の順にメニューをクリックし、以下の画面を表示します。

/RE Name	ACI Name	Interface Name		
2 chars	32 chars	12 chars		Apply
otal Entries: 2				
	VRF			
			Show Detail	

図 9-42 RIP Distribute List 画面

画面に表示される項目:

項目	説明
VRF Name	VRF インスタンス名を 12 字以内で入力します。
ACL Name	アクセスリスト名を 32 字以内で入力します。
Interface Name	インスタンス名を 12 字以内で入力します。
_	

「Apply」をクリックし、設定内容を適用します。

「Show Detail」をクリックして、指定エントリの詳細について表示します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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

RIP Distribute List			
VRF Name Distribute List	vrf1		Back
Total Entries: 0			
	Interface Name	Distribute List	

図 9-43 RIP Distribute List (Show Detail) 画面

## RIP Interface Settings (RIP インタフェース設定)

RIP インタフェースの設定を行います。

L3 Features > RIP > RIP Interface List の順にメニューをクリックし、以下の画面を表示します。

work		
		Apply Delete
sive Interface	BFD State	
abled 🔽 12 chars 🗌 Default	Disabled 🔽	Apply
	sive Interface abled 12 chars	sive Interface BFD State abled 12 chars Default Disabled

図 9-44 RIP Interface Settings 画面

画面に表示される項目:

項目	説明
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Network	RIP に使用される IPv4 ネットワークアドレスアドレスを指定します。本項目で指定するネットワークのサブネットを持つインタフェースの RIP が有効になります。
Passive Interface	パッシブインタフェースを「Enabled」(有効)/「Disabled」(無効)に指定します。インタフェースのルーティングアッ プデートの送信 / 受信を無効にします。しかし本インタフェースの他のルータから受信した RIP パケットは、継続して 処理されます。パッシブインタフェースの名前(12 字以内)を表示欄に入力します。「Default」を指定すると全イン タフェースに適用されます。
BFD State	指定インタフェースの BFD 機能を「Enabled」(有効) /「Disabled」(無効) に指定します。BFD がインタフェースで 有効な場合、ルータは現在のインタフェースの RIP ピアとともに BFD ピアを作成し、新しい RIP ピアが追加されると、 BFD ピアが作成されます。RIP ピアが RIP 無効により削除されると、関連する BFD ピアもまた削除されます。BFD セッ ションが落ちると、ピアにより学習された RIP セッションもまた削除されます。

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

## RIP Database (RIP データベース)

本項目では「Routing Information Protocol」(RIP) ルーティングデータベースの設定を行います。サマリアドレスは、子ルートがサマライズ(要約) されている場合、データベース内に表示されます。最後のサマリアドレスの子ルートが無効になると、サマリアドレスはルーティングテーブルから 削除されます。

L3 Features > RIP > RIP Database の順にメニューをクリックし、以下の画面を表示します。

RIP Database						
RIP Database Network Address	12 chars				Find	Show All
Total Entries: 0 Total Routes: 0						
Netw	ork	Next Hop	Metric	From	If	Time
Note: Codes: R - RIP, Rc - I	RIP connected, K - Kernel	, C – Connected, S – Static, O - OSP	F, B - BGP, I - IS-IS, A - /	Aggregate		
9-45 RIP Data	abase 画面					

画面に表示される項目:

項目	説明
Network Address	ネットワークのサブネットプリフィクスとプリフィクス長を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。

「Apply」をクリックし、設定内容を適用します。

「Show All」をクリックして、すべてのエントリを表示します。

# RIPng (RIPng 設定)

スイッチは、RIPng(Routing Information Protocol next generation)をサポートしています。RIPng は、ルートを計算するのに使用するルーティン グ情報を交換するルーティングプロトコルであり、IPv6 ベースのネットワーク用です。

## RIPng Settings (RIPng 設定)

本画面では、RIPng の設定を行います。

#### L3 Features > RIPng > RIPng Settings の順にメニューをクリックして以下の画面を表示します。

RIPng Settings		
RIPng Global Settings		
Global State	OEnabled  OEnabled	Apply
RIPng Settings		
Default Metric (1-16)	0 Default	
Distance (1-254)	120 Default	
Update Timer (5-65535)	30 sec 🗌 Default	
Invalid Timer (1-65535)	180 sec 🗌 Default	
Flush Timer (1-65535)	120 sec Default	
Poison Reverse	Disabled	
Split Horizon	Enabled	Apply
Redistribute Settings		
Protocol	Metric (0-16)	
Connected 🔽	Default	Apply Delete
Redistribute Table		
	Protocol	Metric
	connected	10

## 図 9-46 RIPng Settings 画面

#### 画面に表示される項目:

項目	説明
	RIPng Global Settings
Global State	RIPng の状態を有効または無効にします。初期値は無効です。
	RIPng Settings
Default Metric	初期メトリック値(1-16秒)を指定します。他のルーティングプロトコルからの再分配ルートで使用される初期メトリック値を指定します。再分配されるルートは他のプロトコルに学習され、RIPng との互換性がないメトリックになる場合があります。メトリックの指定により、メトリックが同期します。「Default」を指定すると初期メトリック値(0)を 指定します。
Distance	RIPng の管理ディスタンス(1-254)を指定します。低い値ほど良いルートを意味します。「Default」を指定すると初 期値である 120 を使用します。
Update Timer	RIP アップデートメッセージを送信する間隔値(5-65535 秒)を入力します。「Default」を指定すると初期値の「30」 を指定します。
Invalid Timer	無効にする値(1-65535 秒)を入力します。「Default」を指定すると初期値の「180」を指定します。
Flush Timer	フラッシュ値(1-65535 秒)を入力します。「Default」を指定すると初期値の「120」を指定します。
Poison Reverse	「Poison Reverse」を「Enabled」(有効)/「Disabled」(無効)に指定します。有効の場合、インタフェースから学習したルートは不達のメトリックとともに同じインタフェースに通知されます。
Split Horizon	「Split Horizon」を「Enabled」(有効)/「Disabled」(無効)に指定します。「Split Horizon」が有効の場合、インタフェー スから学習したルートは同じインタフェースに通知されません。
	Redistribute Settings
Protocol	RIPng に再分配されるルーティングプロトコル(ドメイン)を指定します。「BGP」「Connected」「OSPF」「Static」「ISIS」 から指定します。「Static」は IPv6 スタティックルートを再分配します。「Connected」は IPv6 インタフェースの IP ア ドレス設定の際に自動的に構築するルートを意味します。
Metric	再分配されるルートのメトリックとして使用される値(0-16)を指定します。「Default」は初期メトリック値を使用します。

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

## RIPng Interface Settings(RIPng インタフェース設定)

本画面では、RIPng インタフェースの設定を行います。

L3 Features > RIPng > RIPng Interface Settings の順にメニューをクリックして以下の画面を表示します。

Png Interface Settin	gs					_
Png Interface Settings						
nterface VLAN (1-4094)	All Interface	State Me	ric Offset (1-16)	BFD State Disabled	Passive Interface Disabled V	Apply
Png Interface Table						
Interface	State	Metric Offse	et BFD	State	Passive Inte	rface

図 9-47 RIPng Interface Settings 画面

画面に表示される項目:

項目	説明
Interface VLAN	RIPng 設定の VLAN インタフェース名(1-4094)を入力します。「All Interface」を選択すると全インタフェー
	スで適用します。
State	指定の VLAN インタフェースで IPv6 RIP 機能を「Enabled」(有効)/「Disabled」(無効)に指定します。
Metric Offset	指定インタフェースに受信する IPv6 RIP ルートのメトリックに本値(1-16)を追加します。メトリックはホッ プカウントを参照します。初期値では IPv6 RIP ルート受信時に、ルーティングテーブル挿入される前にメトリッ ク値「1」がルートに追加されます。複数のインタフェースに受信するルートのメトリックとルートへの干渉 に使用します。「Default」を指定すると初期値の「1」を指定します。
BFD State	IPv6 RIP インタフェースの BFD 機能を「Enabled」(有効)/「Disabled」(無効)に指定します。
Passive Interface	パッシブインタフェースを「Enabled」(有効)/「Disabled」(無効)に指定します。インタフェースのルーティ ングアップデートの送信/受信を無効にします。しかし本インタフェースの他のルータから受信した RIPng パ ケットは、継続して処理されます。パッシブインタフェースの名前(12字以内)を表示欄に入力します。「Default」 を指定すると全インタフェースに適用されます。

「Apply」をクリックし、設定内容を適用します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

## RIPng Database (RIPng データベース)

本画面では、RIPng データベースの設定を行います。

L3 Features > RIPng > RIPng Database の順にメニューをクリックして以下の画面を表示します。

RIPng Database			_	_
RIPng Database				
IPv6 Address/Prefix Length	2013::/64			Find
Total Entries: 0				
ESCOLOOPERAL ACT	IPv6 Address/Prefix Length	Metric	Nexthop	Expires

図 9-48 RIPng Database 画面

画面に表示される項目:

項目	説明
IPv6 Address/Prefix Length	IPv6 アドレスを入力します。

「Find」ボタンをクリックして、入力したエントリを検出します。

## OSPF (OSPF 設定) (EI/MI モードのみ)

#### L3 Features > OSPF

OSPF(Open Shortest Path First)ルーティングプロトコルは、Link-State アルゴリズムを使用して宛先ネットワークまでのルートを決定します。「リ ンク」はルータ上のインタフェースを指し、「State」(状態)はそのインタフェースと隣接するルータ間の関係を指しています。「State」には、IP ア ドレス、サブネットマスク、インタフェースに接続しているネットワークタイプ、そのネットワークに接続する他のルータなどの情報があります。 「Link-State」情報は、Link-State データベースに集められ、OSPF が動作するルータによって維持されます。

OSPF では、ルータがどのように通信を行い、Link-State データベースを維持するかについて規定し、また OSPF を使用するネットワークトポロジに ついての概念を定義しています。

ルータ間の Link-State アップデートのトラフィックを制限するために、OSPF ではエリアという概念が定義されています。1 つのエリア内にあるす べてのルータは、1 つの Link-State データベースを共有し、1 つのルータによってデータベースに変更が生じると、それをトリガーとして同一エ リア内にあるすべてのルータの Link-State データベースが更新されます。ルータのうち、複数のエリアに接続しているものを境界ルータ(Border Router)と呼びます。境界ルータはエリア間のルーティング情報を配信する役割を担います。

1つのエリアが、エリア0またはバックボーンとして定義されます。このエリアは、ネットワークの中心的なエリアで、他のすべてのエリアはこの バックボーンエリアに(ルータを経由して)接続します。バックボーンエリアにはルータのみが接続し、あるエリアでルーティング情報の変更が発 生するとバックボーンに伝えられ、そこから他のネットワークへ伝播されるような構造になっています。

OSPFを使用したネットワークを構築する際は、まずバックボーン(エリア 0)を構築し、そこからネットワークを広げるように構築することをお 勧めします。

## OSPFv2 (OSPFv2 設定)

#### L3 Features > OSPF > OSPFv2

#### OSPFv2 Process Settings (OSPF プロセス設定)

OSPFv2 プロセスを設定、表示にします。

L3 Features > OSPF > OSPFv2 > OSPFv2 Process Settings の順にメニューをクリックし、以下の画面を表示します。

PFV2 Pro	cess Setti	ngs	_	_	_	_	_	_	_	_	_	_
PF Process	Settings											
rocess ID (1-	65535)											
RF Name		12 chars		Select	VRF							
											[	Apply
											Clear	Clear All
											Find	Show All
PF Process	Table											
otal Entries:	1									_		
Process ID	VRF Name	OSPF State	Router ID	Default Metric	Distance	Settings	Defau	It Originate I	nfo	ECMP		
		Oldio			Туре	Distance	State	Orignate	Metric			
1		Enabled	10.90.90.90	20	Intra-area	80	Disabled	None	1	1	Edit	Show Detail
									1/	1 <	< 1	> > G

図 9-49 OSPFv2 Process Settings 画面

画面に表示される項目:

項目	説明
Process ID	OSPF プロセス ID(1-65535)を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。「Select VRF」をクリックすると設定済みの VRF インスタンスを使用します。
[Apply] たクロック	クレーションのなどの中国にする

「Apply」をクリックし、設定内容を適用します。

「Clear」をクリックし、指定プロセスをクリアします。

「Clear All」をクリックし、全ての指定プロセスをクリアします。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Show All」をクリックして、すべてのエントリを表示します。

「Show Detail」をクリックして、指定エントリの詳細について表示します。

「Edit」をクリックして、指定エントリの編集を行います。

「Edit」をクリックすると、以下の画面が表示されます。

PF PD	ocess Settings										
RF Na	ime	12 c	hars		Select VRF	]				Find	Show All
PF Pr	ocess Table										
otal Er	ntrips: 2										
otal El											
VRF		Deuter ID	Default	Distance	Settings	Def	ault Originate In	fo	FOND		
VRF Name	OSPF State	Router ID	Default Metric	Distance S	Settings Distance	Def State	ault Originate In Orignate	fo Metric	ECMP		
VRF Name	OSPF State	Router ID	Default Metric	Distance S Type Intra-Area	Settings Distance	Det State	ault Originate In Orignate Always 🔽	fo Metric	ECMP	Apply	Show Detail
VRF Name vrf1	OSPF State	Router ID	Default Metric 100	Distance S Type Intra-Area V Intra-area	Settings Distance 100	Def State Enabled V Enabled	autt Originate In Orignate Always 💌 Always	fo Metric 10	ECMP	Apply Edit	Show Detail

図 9-50 OSPFv2 Process Settings (Edit) 画面

画面に表示される項目:
-------------

項目	説明
OSPF State	指定 VRF インスタンスの OSPFv2 機能を「Enabled」(有効)/「Disabled」(無効)にします。
Router ID	IPv4アドレスフォーマットのルータIDを指定します。ルータIDはOSPFプロトコルを実行する各ルータにアサインされる32ビッ
	トの数です。AS内のルータを固有に識別します。各ルータは固有のルータ IDを持ちます。ルータが既に起動中で設定が済んで
	いる場合、新しいルータ ID はすぐに割り振られません。OSPF の再装填や再起動時に適用されます。
Default Metric	初期メトリック値(1-16777214)を指定します。
Туре	ディスタンス設定種類を指定します。「Intra-Area」「Inter-Area」「External-1」「External-2」から指定します。
	・ Inter-Area - OSPF インターエリアルートのディスタンスを指定します。
	・ Intra-Area - OSPF イントラエリアルートのディスタンスを指定します。
	・ External-1 - OSPF 「external type-5」と「type-1」メトリック付き「type-7」ルートのディスタンスを指定します。
	・ External-2 - OSPF「external type-5」と「type-2」メトリック付き「type-7」ルートのディスタンスを指定します。
Distance	管理ディスタンス値(1-255)を指定します。
State	初期「Originate」情報を「Enabled」(有効)/「Disabled」(無効)に指定します。AS に向かう初期外部ルート (type-5 LSA) ネッ
	トワーク「0.0.0.0」の生成に使用されます。
Originate	「Originate」のオプションを指定します。「Always」「None」から指定します。「Always」を指定すると、再分配されたルート内
	にデフォルトルートが存在していても、常にデフォルトルートを生成し続けます。
Metric	生成されたデフォルトルートにかかるコスト(1-65535)を入力します。指定されないと初期メトリックは「1」になります。
ECMP	ECMP 値(1-64)を指定します。

「Apply」ボタンをクリックして行った変更を適用します。

「Show Detail」をクリックすると、以下の画面が表示されます。

SPF Global Settings Informaion				
compatible rfc3509	Disabled	~		Apply
		Detail Info	maion	
Process bound to VRF			vrf1	
OSPF State			Enabled	
Router ID			10.1.1.1	
Default Metric			100	
Default Originate Information State			Enabled	
Default Originate Information Always			Always	
Default Originate Information Metric			10	
ntra-Area Distance			100	
Inter-Area Distance			90	
External-1 Distance			110	
External-2 Distance			115	
Conforms to RFC2328, and RFC1583 Com	patibility flag is disabled			
Process Uptime (sec)			0Day 00:01:47	
This Router is ABR			No	
This Router is ASBR			Yes	
SPF Schedule Hold Time Between Two SPI	Fs (sec)		3	
Number of External LSA			1	
External LSA Checksum			55267	
Number of LSA Originated			1	
Number of LSA Received			0	
Number of Current LSA			1	
LSDB Database Overflow Limit			49152	
Number of Areas Attached to This Router			1.	
Equal Cost Multi-Path (ECMP)			12	

図 9-51 OSPFv2 Process Settings (Show Detail) 画面

以下の項目があります。

項目	説明
Compatible RFC3509	Area Border Router (ABR) の実行を「Enabled」(有効)/「Disabled」(無効)に指定します。「RFC 3509」で定義されています。

「Apply」をクリックし、設定内容を適用します。 「OK」をクリックし、設定内容を適用します。

## OSPFv2 Distribute List(OSPFv2 ディストリビュートリスト)

OSPFv2 ディストリビュートリストの設定、表示を行います。

#### L3 Features > OSPF > OSPFv2 > OSPFv2 Distribute List の順にメニューをクリックし、以下の画面を表示します。

OSPFv2 Distribute List			
OSPFv2 Distribute List			
Process ID (1-65535) ACL Name 32 cha Interface Name 12 cha	rs		Apply
Total Entries: 1			
Process ID	ACL Name	Interface Name	
1	ACL	vlan1	Delete

図 9-52 OSPFv2 Distribute List 画面

画面に表示される項目:

項目	説明
Process ID	プロセス ID(1-65535)を指定します。
ACL Name	アクセスリスト名を 32 字以内で入力します。
Interface Name	インタフェース名を 12 字以内で入力します。

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

## OSPFv2 GR Helper Settings(OSPFv2 GR ヘルパー設定)

OSPFv2 グレースフルリスタート(GR)ヘルパーの設定、表示を行います。

L3 Features > OSPF > OSPFv2 > OSPFv2 GR Helper Settings の順にメニューをクリックし、以下の画面を表示します。

OSPFv2 GR Helper Settings		
OSPFv2 GR Helper Settings		
Process ID (1-65535) Graceful Restart Helper Unspec Max Grace Period (1-1800)	Sec Sec	Apply
Total Entries: 1		
Process ID	Graceful Restart Helper	Max Grace Period (sec)
1	Unspec	0
		1/1 K < 1 > > Go

図 9-53 OSPFv2 GR Helper Settings 画面

画面に表示される項目:

プロセス ID(1-65535)を指定します。
グレースフルリスタートヘルパーモードを指定します。 ・ Unspec - OSPF グレースフルリスタートヘルパーモードが設定されません。 ・ Never - OSPF グレースフルリスタートヘルパーモードを許可しません。 ・ Only Reload - OSPF グレースフルリスタートヘルパーモードをリロード時のみ許可します。 ・ Only Upgrade - OSPF グレースフルリスタートヘルパーモードをアップグレード時のみ許可します。
最大グレース期間(1-1800 秒)を指定します。

「Apply」をクリックし、設定内容を適用します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

### OSPFv2 Passive Interface Settings(OSPF パッシブインタフェース設定)

OSPFv2 パッシブインタフェースの設定、表示を行います。

#### L3 Features > OSPF > OSPFv2 > OSPFv2 Passive Interface Settings の順にメニューをクリックし、以下の画面を表示します。

OSPFv2 Passive Interface Settings		_		
OSPF Passive Interface Settings				
Process ID (1-65535) Interface Name I2 chars Default		Apply	Delete	Find
Total Entries: 1	Daseius Intorfaco	_		
Processio	Passive interface	_		
1	vian1		Dele	ete
		1/1	< < 1 >	Go

図 9-54 OSPFv2 Passive Interface Settings 画面

画面に表示される項目:

項目	説明
Process ID	プロセス ID(1-65535)を指定します。
Interface Name	使用するインタフェース名(12字以内)を指定します。「Default」を選択すると全ての有効なインタフェースを指定します。

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

## OSPFv2 Area Settings(OSPFv2 エリア設定)

本項目では OSPFv2 エリア設定を行います。

## L3 Features > OSPF > OSPFv2 > OSPFv2 Area Settings の順にメニューをクリックし、以下の画面を表示します。

OSPFv2 Area Setti	ngs	_	_		_	_	_
OSPF Area Settings							
Process ID (1-65535)			1				
Area ID	•			0-4294967295			
Range	O N	SSA	0:	Stub			
Area Range IP			Are	a Range Mask			
Advertise	A	dvertise		No-Advertise		Delete	Apply
OSPF Area Table							
Process ID (1-65535)							Find
Total Entries: 2							
Process ID	Area ID	Area Type	Metric	Area Range	Summary	Advertise	10.00 X 200
1	0.0.0.0	Normal	-	-	NO	-	Delete
1	0.0.0.1	Normal		-	NO	-	Delete
						1/1 < < 1	> >  Go

図 9-55 OSPFv2 Area Settings 画面

### 画面に表示される項目:

項目	説明
	OSPFv2 Area Settings
Process ID	プロセス ID(1-65535)を指定します。
Area ID	OSPFv2 ドメイン内の OSPF エリアを識別する 32 ビットの番号 (IP アドレスと同じ xxx.xxx.xxx.xxx 形式 ) または、10 進数(0-
	4294967295)を指定します。このエリアはインタフェースに設定されたサブネットが指定のネットワーク範囲で落ちた場合に、
	当該のインタフェースで作成されます。
Range	Area Border Router (ABR) の OSPF ルートをサマライズします。
NSSA	Not-So-Stubby Area (NSSA) として OSPF エリアをアサインします。
Stub	Stub エリアとして OSPF エリアを設定します。
Area Range IP	OSPF エリアに対応するネットワークを識別する IP アドレス範囲を入力します。
Area Range Mask	OSPF エリアに対応するネットワークを識別するネットマスク範囲を入力します。
Advertise	通知(Advertise)を有効または無効にします。
	<ul> <li>Advertise - 指定範囲のアドレスの「Type-3 summary Link-State Advertisement (LSA)」を通知します。</li> </ul>
	・ No-Advertise - 「Type-3 summary LSA」の通知を抑制します。コンポネントのルートが背後に存在しています。
Default Cost	「NSSA」または「Stub」選択時に有効です。初期コスト値(0-65535)を指定します。「stub」エリアと「no-so-stubby」エリ
	アに挿入される「Type-3」初期ルートに関連するコストです。
	・ Default - 初期コスト値を指定します。
	・ No-Summary - 本エリアにサマリルートを挿入しない場合、指定します。
	OSPF Area Table
Process ID	プロセス ID(1-65535)を指定します。

「Apply」ボタンをクリックして行った変更を適用します。

「Delete」をクリックすると指定のエントリを削除します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

### 「Process ID」のリンクをクリックすると、以下の画面が表示されます。

OSPF Area Settings		
OSPF Area Detail Information		
Process ID	1	
Area ID	0.0.0.0	
Area Type	Normal	
Summary	-	
Number of Interfaces in This Area	0	
Number of Active Interfaces in This Area	0	
Number of Fully Adjacent Neighbors in This Area	0	
Number of Fully Adjacent Virtual Neighbors Through This Area	0	
SPF Algorithm Executed Times	1	
Number of LSA	0	
Checksum	0×0	
Advertise Cost	0	1907 - O
		OK
Total Entries: 0		
Network Address Network Mask	Type	Advertise
	type	Autoliac

図 9-56 OSPFv2 Area Settings (Process ID) 画面

エントリを指定し「OK」をクリック、設定内容を適用します。 設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

## OSPFv2 Interface Settings(OSPFv2 インタフェース設定)

このスイッチの OSPFv2 インタフェースを設定します。

L3 Features > OSPF > OSPFv2 > OSPFv2 Interface Settings の順にメニューをクリックし、以下の画面を表示します。

OSPFv2 Interfac	e Settings						
OSPF Interface Setti	ngs						
Process ID (1-65535	5)						
Area ID	۲	)	0-429496	7295			
Network IP Address							
Network Mask							Apply
OSPF Interface Table Process ID (1-65535 Interface Name	e ;)	12 chars	]				Find
Total Entries: 1	Interface	Area ID	Notwork ID	Notwork Mack	Link Statue	Coet	
1	vian1	AleanD 0.0.0.1	10.90.90.90	255.0.0.0		1	Show Detail Delete
	Hall	0.0.0.1	10.30.30.30	233.0.0.0	op	1/1	

図 9-57 OSPFv2 Interface Settings 画面

画面に表示される項目:

項目	説明
	OSPF Interface Settings
Process ID	プロセス ID(1-65535)を指定します。
Area ID	OSPFv2 ドメイン内の OSPF エリアを識別する 32 ビットの番号 (IP アドレスと同じ xxx.xxx.xxx 形式 ) または、10 進数 (0-4294967295) を指定します。このエリアはインタフェースに設定されたサブネットが指定のネットワーク範囲で落ちた 場合に、当該のインタフェースで作成されます。
Network IP Address	IPv4 アドレスを指定します。
Network Mask	IPv4 サブネットマスクを指定します。
	OSPF Interface Table
Process ID	プロセス ID(1-65535)を指定します。
Interface Name	インタフェース名を指定します。

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Find」ボタンをクリックして、入力したインタフェースを検出します。

「Show Detail」をクリックして、指定エントリの詳細について表示します。

編集するポートの「Show Detail」ボタンをクリックし、以下の画面を表示します。

SPF Interface Settings			
Interface	vlan1		
Cost (1-65535)		Default	
Hello Interval (1-65535)	sec	Default	
Dead Interval (1-65535)	sec	Default	
Priority (0-255)		Default	
Network Type	Broadcost		
Authentication	None		
SPF Interface Information			Apply
SPF Interface Information		vlan1	Apply
SPF Interface Information		vlan1 Up	Apply
SPF Interface Information Interface Link Status Network IP Address		vlan1 Up 10.90.90	Apply
SPF Interface Information Interface Link Status Network IP Address Network Mask		vian1 Up 10.90.90 255.0.0	Apply
SPF Interface Information Interface Link Status Network IP Address Network Mask Area ID		vian1 Up 10.90.90.90 255.0.0.0 10.10.10.10	
SPF Interface Information Interface Link Status Network IP Address Network Mask Area ID Router ID		vian1 Up 10.90.90.90 255.0.00 10.10.10.10 10.90.90.90	Apply
SPF Interface Information Interface Link Status Network IP Address Network Mask Area ID Router ID Network Type		vian1 Up 10.90.90.90 255.0.0.0 10.10.10.10 10.90.90.90 Broadcast	
SPF Interface Information Interface Link Status Network IP Address Network Mask Area ID Router ID Network Type Cost		vlan1 Up 10.90.90.90 255.0.0.0 10.10.10.10 10.90.90.90 Broadcast 1	
SPF Interface Information Interface Link Status Network IP Address Network Mask Area ID Router ID Network Type Cost Transmit Delay (sec)		vlan1 Up 10.90.90.90 255.0.0.0 10.10.10.10 10.90.90 Broadcast 1 1	

図 9-58 OSPFv2 Interface Settings (Show Detail) 画面

### 画面に表示される項目:

項目	説明
Cost	コストの値(1-65535)を指定します。インタフェースのコストはインタフェース内のパケット送信に反映されます。コ
	ストはルータリンク通知の中でリンクコストとして通知されます。コストはインタフェースのスピードに比例します。コ
	ストは手動または自動でアサインすることが可能です。初期値ではインタフェースのコストは帯域情報に基づき計算され
	ます。コストは参照した帯域情報に対応して「1」になります。「Default」を指定すると初期期の「1」を採用します。
Hello Interval (1-65535)	OSPF Hello パケットの送出間隔(秒)を指定します。
Dead Interval (1-65535)	隣接ルータが Hello パケットを最後に受信してから、送信側のルータがダウンしたと判断するまでの時間(秒)。本値には
	Hello Interval の倍数を指定します。
Priority	代表ルータ選出のプライオリティ(0-255)を指定します。ルータプライオリティ0が指定されると、スイッチはそのネッ
	トワークの代表ルータとして選出されなくなります。
Network Type	ネットワークタイプを次から指定します。
	・ Broadcast - ネットワークタイプをブロードキャストとして指定します。
	・ Point-to-Point - ネットワークタイプを「point-to-point」として指定します。
	ブロードキャストネットワークでは「DR」と「BDR」のみが他の全てのルータのネイバになることが可能です。「point-
	to-point」ネットワークでは、通信できる 2 ルータのみが隣接者になることが可能です。
Authentication	OSPF ルーティングドメインでの OSPF パケットの送受信時における認証方法を設定します。
	・ None - 認証を行いません。
	• Simple Password - パケットが認証済みルータからのものであるかを判断するためにシンプルパスワードを使用しま
	す。本モードを選択した場合、「Password」に8文字までのパスワードを指定します。
	・ MD5 - 「MD5 Key Table Configuration」メニューで登録された暗号キーを使用します。本モードを選択した場合、「Key
	ID」欄に、登録済みのキーの中から1つを入力します。
Password	「Authentication」で「Simple Password」を選択した場合、シンプルテキストのパスワード(8 字以内)を入力します。
MD5 Key ID	MD5 暗号キー ID(1-255) を入力します。
MD5	MD5 キー(16 字)を指定します。シンタックスはスペースなしのアルファベット文字列です。
	MD5 モードでは OSPF メッセージ送信者は送信メッセージのメッセージダイジェストキーを元にメッセージのダイジェス
	トを解析します。メッセージダイジェストとキーIDはパケット内でエンコードされます。パケットの受信者は、同じキー
	ID に関連する、ローカル定義されたメッセージダイジェストキーを元に解析されたダイジェストに対するメッセージを確
	認します。
	ネイバルータの同じキー ID は同じ文字列で定義されます。インタフェースのすべての隣接するルータは、それぞれ OSPF
	パケットを交換するために同じキーを使用する必要があります。

「Apply」ボタンをクリックして行った変更を適用します。

## OSPFv2 BFD Settings(OSPFv2 BFD 設定)

このスイッチの OSPFv2 インタフェースを設定します。

L3 Features > OSPF > OSPFv2 > OSPF BFD Settings の順にメニューをクリックし、以下の画面を表示します。

OSPFv2 BFD Settings		
OSPFv2 BFD Settings		
Total Entries: 1		
Interface Name	BFD State	
vlan1	Disabled	Edit
		1/1 K < 1 > M Go

図 9-59 OSPFv2 BFD Settings 画面

#### 画面に表示される項目:

項目	説明
BFD State	指定インタフェースの BFD 機能を「Enabled」(有効)/「Disabled」(無効)に指定します。BFD がインタフェースで有効 な場合、ルータは現在のインタフェースの OSPF ネイバとともに BFD セッションを作成します。BFD セッションが落ちると、 学習された OSPF セッションもまた削除されます。

「Apply」ボタンをクリックして行った変更を適用します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

#### OSPFv2 Redistribute Settings (OSPFv2 再分配設定)

本項目では OSPFv2 再分配(redistribution)について、設定、表示します。外部ルートは ASBR により「Type-5」外部ルートとしてノーマルエリアに、 または「Type-7」外部ルートとして NSSA スタブエリアに再分配されます。

再分配外部ルートが「Type-1」の場合、メトリックはインターナルメトリックを意味します。再分配外部ルートが「Type-2」の場合、メトリックは 外部メトリックを意味します。内部メトリックは自身から宛先に到達するまでの通知コスト追加した、ルータ再分配のルートコストを認識します。 外部メトリックは宛先に到達するまでの通知メトリックのみを認識します。メトリックが初期メトリックとして設定されていない場合、他のプロト コルから再分配されたルートがメトリック値 20 を取得します。

L3 Features > OSPF > OSPFv2 > OSPFv2 Redistribute Settings の順にメニューをクリックし、以下の画面を表示します。

OSPFv2 Redistribut	e Settings		_		
OSPF Redistribute Setting	gs				
Process ID (1-65535)					
Protocol	Connected	~			
Metric Type	External Typ	e-1 🗸			
Metric (1-16777214)					
Router Map Name	16 chars				
					Apply
Process ID (1-65535)					Find
Total Entries: 1					
Process ID	Protocol	Metric Type	Metric	Route Map Name	
1	Connected	External Type-1	10	RouterMap	Delete

図 9-60 OSPFv2 Redistribute Settings 画面

以下の項目があります。

項目	説明
Process ID	プロセス ID(1-65535)を指定します。
Protocol	再分配される送信元プロトコルを指定します。「Connected」「Static」「RIP」「BGP」「ISIS」から指定します。OSPF のよう なルーティングプロトコルの場合、自立したシステムに外部として再分配されます。
Metric Type	メトリックの種類を指定します。「External Type-1」「External Type-2」から指定します。OSPF ルーティングドメインに再 分配されるルートの外部リンクタイプを指定します。メトリックタイプが指定されていないと、スイッチは「Type-2」外 部ルートを採用します。
Metric	再分配ルートのメトリック(1-16777214)を指定します。
Router Map Name	送信元ルーティングプロトコルからインポートされたルートをフィルタするルートマップ名を指定します。 指定されないと全ルートが再分配されます。

「Apply」ボタンをクリックして行った変更を適用します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Delete」をクリックすると指定のエントリを削除します。

### OSPFv2 Virtual Link Settings (OSPFv2 仮想リンク設定)

本項目では OSPFv2 仮想リンク設定を行います。「non-zero」エリアが物理的にゼロエリアと接続していない場合、仮想リンクを通じて必ず接続さ れる必要があります。仮想リンクは「point-to-point」リンクです、ルータは OSPF メッセージをユニキャスト IP パケットとしてネイバルータに送 信します。

L3 Features > OSPF > OSPFv2 > OSPFv2 Virtual Link Settings の順にメニューをクリックし、以下の画面を表示します。

OSPFv2 Virtual Link S	ettings	_	_	_		_	_
OSPF Virtual Link							
Process ID (1-65535)							
Area ID	• •	. 0 0-4	294967295				
Router ID							
Hello Interval (1-65535)		sec 🗌 Defa	ault				
Dead Interval (1-65535)		sec Defa	ault				
Authentication	None	<b>~</b>					
							Apply
OSPF Virtual Link Table							
Process ID (1-65535)							Find
Total Entries: 1							
Process ID	Area ID	Router ID	Hello	Dead	Authentication	LinkStatus	
1	0.0.0.1	192.168.70.1	10	40	None	Down	Delete
					1/1	< 1	> >  Go

図 9-61 OSPF Virtual Link Settings 画面

#### 画面に表示される項目:

項目	説明				
	OSPF Virtual Link				
Process ID	プロセス ID(1-65535)を指定します。				
Area ID	OSPFv2 ドメイン内の OSPF エリアを識別する 32 ビットの番号 (IP アドレスと同じ xxx.xxx.xxx 形式)または、10 進数(0-4294967295)を指定します。このエリアはインタフェースに設定されたサブネットが指定のネットワーク範囲で 落ちた場合に、当該のインタフェースで作成されます。				
Router ID	リモートエリアの OSPFv2 ルータ ID。リモートエリアの Area Border Router(エリア境界ルータ)を識別する 32 ビットの番号 (IP アドレスと同じ xxx.xxx.xxx 形式)を表示します。これは Neighbor ルータのルータ ID です。				
Hello Interval (1-65535)	OSPF Hello パケットの送出間隔(秒)を指定します。同一ネットワークのルータには同じ「Hello Interval」、「Dead Interval」、「Authorization Type」、「Authorization Key」が設定される必要があります。				
Dead Interval (1-65535)	隣接ルータが Hello パケットを最後に受信してから、選択エリアがダウンしたと判断するまでの時間(秒)を入力します。 1から 65535(秒)で指定します。本値には Hello Interval の倍数を指定します。				
Authentication	使用する認証を選択します。「None」、「Simple Password」または「MD5」を選択します。「Simple Password」認証を 選択するとパスワードの入力が必要です。「MD5」認証を選択すると KEY ID の入力が必要です。				
Password	「Authentication」で「Simple Password」を選択した場合、シンプルテキストのパスワードを入力します。				
MD5 Key ID	MD5 暗号キー ID(1-255) を入力します。				
MD5	MD5 キー(16 字)を指定します。シンタックスはスペースなしのアルファベット文字列です。				
	OSPF Virtual Link Table				
Process ID	プロセス ID(1-65535)を指定します。				

「Delete」をクリックすると指定のエントリを削除します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動しま エントリを指定し「OK」をクリック、設定内容を適用します。

### 「Process ID」のリンクをダブルクリックすると次の画面が表示されます。

OSPF Virtual Link Detail Information		
OSPF Virtual Link Information		
Process ID	1	
Neighbor Router ID	192.168.70.1	
Link Status	Linkdown	
Real Interface Name		
Adjacency State	Down	
Transit Area	0.0.0.1	
Local Address	0.0.0.0	
Remote Address	0.0.0.0	
Transmit Delay	1	
Hello Interval Configured (sec)	10	
Dead Interval Configured (sec)	40	
Retransmit Interval Configured (sec)	5	
Authentication Type	None	
Authentication Key	-	
		ОК

図 9-62 OSPFv2 Virtual Link Settings (Double Click) 画面

## OSPFv2 LSDB Table (OSPFv2 LSDB テーブル)

OSPFv2 Link State Database(LSDB) を表示します。

#### L3 Features > OSPF > OSPF 2 > OSPF LSDB Table Settings の順にメニューをクリックし、以下の画面を表示します。

OSPFv2 LSDE	B Table	_	_			_	_	_
OSPF LSDB Table	9							
Process ID (1-65	535)							
I SDB Type	,	All						
Link State		All					r	e' - 1
Link State		All					l	Find
OSPF LSDB Table	e							
Total Entries: 1								
Process ID	Link ID	ADV Router	Age	Sequence Number	Checksum	Count	LSDB Type	
1	10.90.90.90	10.90.90.90	277	0x80000003	0x39d8	1	Router	Show Detail
						1/1	< 1 >	Go

図 9-63 OSPFv2 LSDB Table Settings 画面

画面に表示される項目:	
項目	説明
Process ID	プロセス ID(1-65535)を指定します。
LSDB Type	表示する LSDB タイプを指定します。「All」「Router」「Network」「Summary」「ASBR Summary」「External」「Stub」「NSSA External」から選択します。
Link State	<ul> <li>表示されるリンクステート情報を選択します。「All」「Link State ID」「Self Originate」「Adv Router」から選択します。</li> <li>「All」-全ての「OSPFv2」リンクステート情報を表示します。</li> <li>「Link State ID」-指定するリンクステート ID に関する情報を表示します。表示される欄にリンクステート ID を指定します。</li> <li>「Self Originate」-ローカルルータによって起動している LSA を表示します。通知ルータ ID を空欄に入力します。</li> </ul>

「Find」ボタンをクリックして、指定したエントリを検索します。

「Show Detail」をクリックして、指定エントリの詳細について表示します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

エントリを指定し「OK」をクリック、設定内容を適用します。

### ■ OSPFv2 LSDB の詳細表示

「<u>Show Detail</u>」リンクをクリックすると、以下の画面が表示されます。

OSPF LSDB Detail Information	
OSDE   SDB Detail Information	
Process ID	1
Area ID	0.0.0.1
LS Age	332
Options	0x2 (* - - - - E -)
Flags	0x2
This Router is ABR	No
This Router is ASBR	Yes
This Router is Virtual Link Endpoint	No
LS Type	Router-LSA
Link State ID	10.90.90.90
Advertising Router	10.90.90.90
LS Seq Number	0x80000003
Checksum	0x39d8
Length	36
	Back
Detail Information	
Number of Links	1
Link Connected to Stub Network	
(Link ID) Network/Subnet Number	10.0.0.0
(Link Data) Network Mask	255.0.0.0
Number of TOS Metrics	0
TOS 0 Metric	1

図 9-64 OSPFv2 LSDB Table 画面(Show Detail)

「Back」をボタンをクリックして前のページに戻ります。

## OSPFv2 Neighbor Table (OSPF Neighbor テーブル)

インタフェースごとに OSPF-Neighbor 情報を表示します。

## L3 Features > OSPF > OSPFv2 > OSPF Neighbor Table の順にメニューをクリックし、以下の画面を表示します。

OSPFv2 Neighbor	r Table	_	_	_	_	
OSPF Neighbor Table						
Process ID (1-65535)						
Interface Name	12.0	hare				
intendee Hume	14. 0	andro				
Neighbor						Find
Total Entries: 6						
Process ID	Neighbor ID	Priority	State	Address	Interface	
65535	1.1.1.1	200	Full/DR	20.0.0.1	vlan20	Show Detail
65535	1.1.1.1	50	Full/DR	30.0.0.1	vlan30	Show Detail
65535	3.3.3.3	1	Full/DR	60.0.0.1	vlan60	Show Detail
65535	7.7.7.7	1	Full/DR	110.110.110.2	vlan110	Show Detail
65535	1.1.1.1	0	Full/-	20.0.0.1	-	Show Detail
65535	1.1.1.1	0	Full/-	30.0.0.1	-	Show Detail
						1/1 < < 1 > > Go

図 9-65 OSPFv2 Neighbor Table 画面

以下の項目を使用します。

項目	説明
Process ID	プロセス ID(1-65535)を指定します。
Interface Name	使用されるインタフェースを指定します。
Neighbor	Neighbor ルータの ID を入力します。

## ■ エントリの参照

「Find」ボタンをクリックして、指定したエントリを検索します。 「Show All」ボタンをクリックして、すべてのエントリを表示します。

「Show Detail」リンクをクリックすると、以下の画面が表示されます。

OSPF Neighbor Detail Information		
Neighbor Router ID	30.90.90	
Area	0.0.0.11	
Interface Name	vlan11	
IP Address	11.0.0.1	
Priority	1	
State	Full	
State Changes	5	
DR	11.0.0.3	
BDR	11.0.0.1	
Option	0×2 (* - - - - E -)	
		Back

図 9-66 OSPFv2 Neighbor Table 画面 (Show Detail)

「Back」をボタンをクリックして前のページに戻ります。

## OSPFv2 Host Route Settings(OSPFv2 ホストルート設定)

OSPFv2 ホストルート設定を行います。 L3 Features > OSPF > OSPFv2 > OSPFv2 Host Route Settings の順にメニューをクリックし、以下の画面を表示します。

OSPFv2 Host Route Settin	gs			
OSPFv2 Host Route Settings				
Process ID (1-65535)				
Area ID	• • • •	0-4294967295		
Host IP	· · · ·			
Cost (1-65535)		Default		Apply
OSPF Host Route Table				
Process ID /1.65525)				et al
11006331D (1-035335)				Find
Total Entries: 1				
Process ID	Area ID	Host IP	Cost	
1	0.0.0.1	192.168.70.14	1	Delete
			1/1 < <	1 > > Go

図 9-67 OSPFv2 Host Route Settings 画面

## 画面に表示される項目:

項目	説明				
	OSPFv2 Host Route Settings				
Process ID	プロセス ID(1-65535)を指定します。				
Area ID	OSPFv2 ドメイン内の OSPF エリアを識別する 32 ビットの番号 (IP アドレスと同じ xxx.xxx.xxx 形式) または、10 進数(0- 4294967295)を指定します。このエリアはインタフェースに設定されたサブネットが指定のネットワーク範囲で落ちた場合に、 当該のインタフェースで作成されます。				
Host IP	使用するホストの IP アドレスを指定します。				
Cost	スタブエントリのコスト (1-65535) を指定します。「Default」を指定すると初期値(1)を使用します。				
	OSPF Host Route Table				
Process ID	プロセス ID(1-65535)を指定します。				

「Apply」ボタンをクリックして行った変更を適用します。

「Find」ボタンをクリックして、指定したエントリを検索します。

「Delete」をクリックすると指定のエントリを削除します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

エントリを指定し「OK」をクリック、設定内容を適用します。

## OSPFv3

## OSPFv3 Process Settings (OSPFv3 プロセス設定)

スイッチに OSPFv3 プロセス設定を行います。

L3 Features > OSPF > OSPFv3 > OSPFv3 Process Settings の順にメニューをクリックして以下の画面を表示します。

PFv3 Process Se	ettings						
ocess ID (1-6553	5)						Apply
					[	Clear	Clear All
					[	Find	Show All
						Ting	SHOW AI
PFv3 Process Ta tal Entries: 1	Router ID	Default Matric	Distance	Settings	Auto Bandwidth		SHOW AI
PFv3 Process Ta otal Entries: 1 Process ID	Router ID	Default Metric	Distance Type	Settings Distance	Auto Bandwidth		SHOW AI
PFv3 Process Ta otal Entries: 1 Process ID 1	Router ID	Default Metric 20	Distance Type Intra-area	Settings Distance 110	L Auto Bandwidth 100	Edit	Delete

図 9-68 OSPFv3 Process Settings 画面

画面に表示される項目:

項目	説明	
Process ID	OSPFv3 のプロセス ID(1-65535)を指定します。	
「Apply」をクリック	し、設定内容を適用します。	
「Delete」をクリック	すると指定のエントリを削除します。	
「Find」をクリックし	て、入力した情報に基づく特定のエントリを検出します。	
「Show All」をクリッ	クして、すべてのエントリを表示します。	
「Edit」をクリックし	て、指定エントリの編集を行います。	
「Process ID」のリン	クをクリックすると指定の OSPFv3 プロセスのへのアクセス、設定を行います。	
「Clear」をクリックで	オスと入力   たエントリをクリア   すす	

「Clear All」をクリックすると入力したエントリを全てクリアします。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Edit」をクリックすると、以下の画面が表示されます。

PEv3 Process	Settings						
11101100000	ocumps						
rocess ID (1-65	535)						Apply
					[	Clear	Clear All
						Find	Show All
DEv3 Drocore	Table						
Prvj Plocess							
otal Entries: 1							
otal Entries: 1	Parter ID	Dofault Makie	Dist	ance Settings			-
otal Entries: 1 Process ID	Router ID	Default Metric	Dist	ance Settings Distance	Auto Bandwidth		
otal Entries: 1 Process ID 1	Router ID	Default Metric	Dist Type	ance Settings Distance 110	Auto Bandwidth	Apply	Delete

図 9-69 OSPFv3 Process Settings (Edit) 画面

画面に表示される項目:

項目	説明
Router ID	OSPF プロセスのためのルータ ID を入力します。
Default Metric	初期メトリック値(1-16777214)を指定します。初期値は20です。全ての再分配ルートに同じメトリックを使用する、現在のルー ティングプロトコルを有効にする OSPFv3 再分配機能と共同で使用されます。初期メトリックは不適合なメトリックの再分配 ルートの問題を解決します。メトリックが直接コンバートされなくても、初期メトリックを使用して、適当な代替策を提供し、 再分配を実行します。
Туре	ディスタンス設定種類を指定します。「Intra-Area」「Inter-Area」「External」から指定します。 ・ Inter-Area - OSPF インターエリアルートのディスタンスを指定します。 ・ Intra-Area - OSPF イントラエリアルートのディスタンスを指定します。 ・ External - OSPF エクスターナルルートのディスタンスを指定します。
Distance	管理ディスタンス値(1-254)を指定します。初期値は 110 で全ての OSPF ルートの値です。
Auto Bandwidth	自動帯域の値(1-4294967)を指定します。インタフェースのメトリックの計算時に IPv6 OSPF が使用する参照値をコントロー ルする機能です。

「Apply」ボタンをクリックして行った変更を適用します。

「Delete」をクリックすると指定のエントリを削除します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

#### 「Process ID」のリンクを指定すると次の画面が表示されます。

Process ID	1
OSPF State	Enabled
Router ID	192.168.10.90
Default Metric	20
ntra-Area Distance	110
Inter-Area Distance	110
External Distance	110
Auto Cost Reference Bandwidth	100
Process Uptime (sec)	0Day 00:00:02
This Router is ABR	No
This Router is ASBR	No
SPF Schedule Hold Time Between Two SPFs (sec)	10
SPF Schedule Delay (sec)	5
Number of External LSA	0
Number of LSA Originated	0
Number of LSA Received	0
Number of Areas Attached to This Router	0

図 9-70 OSPFv3 Process Settings (Process ID) 画面

「OK」をクリックして画面を終了し前画面に戻ります。

## OSPFv3 Passive Interface Settings(OSPFv3 パッシブインタフェース設定)

スイッチに OSPFv3 パッシブインタフェース設定を行います。インタフェースがパッシブ(受動態)の場合、OSPF ルーティングアップデートパケットは指定のインタフェースを通じての送受信がされなくなります。

L3 Features > OSPF > OSPFv3 > OSPFv3 Passive Interface Settings の順にメニューをクリックして以下の画面を表示します。

SPFv3 Passive Interface S	ettings				
Process ID (1-65535)					
Interface Name	12 chars	Default	Annly	Delete	Find

図 9-71 OSPFv3 Passive Interface Settings 画面

## 以下の項目を使用します。

項目	説明
Process ID	OSPFv3 のプロセス ID(1-65535)を指定します。
Interface Name	パッシブインタフェース名 (12 字以内) を指定します。「Default」を選択すると全てのインタフェースをパッシブインタフェー スとして指定します。
	スとして指定します。

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

## OSPFv3 Area Settings(OSPFv3 エリア設定)

スイッチに OSPFv3 エリア設定を行います。

L3 Features > OSPF > OSPFv3 > OSPFv3 Area Settings の順にメニューをクリックして以下の画面を表示します。

OSPFv3 Area Settings					
OSPFv3 Area Settings					
Process ID (1-65535)		OSPF Area ID			
Range	O Stub				
Area Range IPv6 Prefix	2013::1/64				
Advertise	Advertise	No-Advertise			
					Apply
OSPFv3 Area Table					
Process ID (1-65535)					Find
Total Entries: 2					
Process ID	Area ID	Area Type	Metric	Summary	
1	10.10.10.10	Stub	1	Yes	Delete
1	10.11.11.11	Normal	1	-	Delete
				1/1 < < 1	> >  Go

図 9-72 OSPFv3 Area Settings 画面

画面に表示される項目:

項目	説明
	OSPFv3 Area Settings
Process ID	OSPF のプロセス ID(1-65535)を指定します。
OSPF Area ID	OSPFv3 エリアの ID を指定します。IPv4 アドレス形式で入力します。
Range	Area Border Router (ABR) の OSPF ルートをサマライズします。
Stub	指定エリアをスタブエリアとして定義します。
Area Range IPv6 Prefix	「Range」を指定後、OSPF エリア範囲 IPv6 プリフィクスとプリフィクス長を指定します。
Advertise	通知(Advertise)を有効または無効にします。 ・Advertise - 指定範囲のアドレスの「inter-area prefix Link-State Advertisement (LSA)」を通知します。 ・No-Advertise - 「inter-area prefix LSA」の通知を抑制します。コンポネントのルートが背後に存在しています。
Metric (0-65535)	OSPFv3 スタブエリアの初期コストを指定します。「Default Metric」を選択するとエリアの初期メトリック値(1)を使用します。 「No-Summary」を選択するとスタブエリアの inter-area prefix LSA からの ABR を阻止します。
	OSPFv3 Area Table
Process ID	OSPF のプロセス ID(1-65535)を指定します。

# 第9章 L3 Features (レイヤ3機能の設定)

「Apply」をクリックし、設定内容を適用します。 「Delete」をクリックすると指定のエントリを削除します。 「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。 「Process ID」のリンクをクリックすると指定の OSPFv3 プロセスのへのアクセス、設定を行います。 設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Stub」エリアの「Process ID」をクリックすると、以下の画面が表示されます。

SPFv3 Area Detail Information		
Process ID	1	
Area ID	10.10.10	
Area Type	Stub	
Summary	Yes	
Number of Interfaces in This Area	0	
Number of Active Interfaces in This Area	0	
Number of Fully Adjacent Virtual Neighbors Through This Area	0	
SPF Algorithm Executed Times	0	
Number of LSA	0	
LSA Checksum	0x0	
Number of Unknown LSA	0	
		ОК
Total Entries: 0		
IPv6 Range Address	Advertise	

図 9-73 OSPFv3 Area Settings 画面 - Stub

「OK」をクリックして画面を終了し前画面に戻ります。

「Normal」エリアの「Process ID」をクリックすると、以下の画面が表示されます。

OSPFv3 Area Settings		
OSPFv3 Area Detail Information		
Process ID	1	
Area ID	10.11.11.11	
Area Type	Normal	
Summary		
Number of Interfaces in This Area	0	
Number of Active Interfaces in This Area	0	
Number of Fully Adjacent Virtual Neighbors Through This Area	0	
SPF Algorithm Executed Times	0	
Number of LSA	0	
LSA Checksum	0x0	
Number of Unknown LSA	0	
		ОК
Total Entries: 1		
IPv6 Range Address	Advertise	
2015::/64	Adverties	Delete
	1/1 < <	1 > > Go

図 9-74 OSPFv3 Area Settings 画面 - Normal

「OK」をクリックして画面を終了し前画面に戻ります。
# OSPFv3 Interface Settings (OSPFv3 インタフェース設定)

OSPFv3 設定または OSPFv3 インタフェース情報を表示します。

L3 Features > OSPF > OSPFv3 > OSPFv3 Interface Settings の順にメニューをクリックして以下の画面を表示します。

OSPFv3 Interfa	ace Settings	_	_	_	_	_	
OSPFv3 Interface	Settings						
Process ID (1-655	(35)	1					
Instance ID (0-	255)						
Area ID							
Interface Name		12	chars				Apply
OSPFv3 Interface Process ID (1-655	Table						
Interface Name		12	chars				Find
Total Entries: 1							
Process ID	Interface	Area ID	Router ID	Link Status	Cost	Instance ID	
1	vlan1	10.10.10.10	192.168.10.90	up	10	0	Delete
						1/1  <	< 1 > > Go

図 9-75 OSPFv3 Interface Settings 画面

画面に表示される項目:

項目	説明					
	OSPFv3 Interface Settings					
Process ID	IPv6 OSPF ルーティングのプロセス ID(1-65535)を指定します。					
Instance ID	インスタンス ID(0-255)を指定します。初期値は「0」					
Area ID	エリアの識別子として IPv4 アドレスを指定します。					
Interface Name	VLAN インタフェース名(12 字以内)を入力します。					
OSPFv3 Interface Table						
Process ID	IPv6 OSPF ルーティングのプロセス ID(1-65535)を指定します。					
Interface Name	インタフェース名を入力します。					

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Process ID」のリンクをクリックすると指定の OSPFv3 プロセスのへのアクセス、設定を行います。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Process ID」をクリックすると、以下の画面が表示されます。

Interface	vlan1		
Cost (1-65535)		Default	
Hello Interval (1-65535)	sec	Default	
Dead Interval (1-65535)	sec	Default	
Priority (0-255)		Default	
Transmit Delay (1-65535)	sec	Default	
Retransmit Interval (1-65535)	sec	Default	Apply
10000010			
Area ID		10 10 10 10	
Area ID		10.10.10	
Area ID Instance ID MTU		10.10.10.10 0 1500	
Area ID Instance ID MTU Interface Name		10.10.10.10 0 1500 vian1	
Area ID Instance ID MTU Interface Name Link State		10.10.10.10 0 1500 vlan1 up	
Area ID Instance ID MTU Interface Name Link State Line Protocol State		10.10.10.10 0 1500 vlan1 up up	
Area ID Instance ID MTU Interface Name Link State Line Protocol State Link Local Address		10.10.10.10 0 1500 vlan1 up up FE80::F27D:68FF:FE34:10/128	
Area ID Instance ID MTU Interface Name Link State Line Protocol State Link Local Address Interface ID		10.10.10.10 0 1500 vlan1 up up FE80::F27D:68FF:FE34:10/128 1	
Area ID Instance ID Interface ID Interface Name Link State Line Protocol State Link Local Address Interface ID Router ID		10.10.10.10 0 1500 vlan1 up up FE80::F27D:68FF:FE34:10/128 1 192.168.10.90	

図 9-76 OSPFv3 Interface Settings 画面 - Process ID

「OK」をクリックして画面を終了し前画面に戻ります。

	画面に表示される項目	:	
--	------------	---	--

項目	説明
Cost	指定した OSPFv3 インタフェースに到達する際の OSPFv3 コスト (1-65535) を指定します。「Default」を指定すると初期
	値を使用します。
Hello Interval (1-65535)	OSPF Hello パケットの送出間隔 (秒) を指定します。同じリンクの全ルータには同じ「Hello Interval」と「Dead Interval」
	が設定される必要があります。「Default」を指定すると初期値を使用します。初期値は 10 です。
Dead Interval (1-65535)	隣接ルータが Hello パケットを最後に受信してから、選択エリアがルータがダウンしたと判断するまでの時間(秒)を入
	力します。本値には Hello Interval の倍数を指定します。「Default」を指定すると初期値を使用します。初期値は 40 です。
Priority (0-255)	代表ルータ (DR : Designated Router) の選出に使用するプライオリティ (0-255) を入力します。「Default」を指定すると初
	期値を使用します。初期値は1です。ネットワークのOSPF Designated Router (DR)の優先値決定に使用します。二つのルー
	タが DR になろうとした場合、より高い優先値のルータが(DR)になります。二つのルータの優先値が同じ場合、より
	高いルータ ID を持つ方が高い優先性を持ちます。「non-zero」ルータ優先値を持つルータのみが宛先、またはバックアッ
	プ宛先ルータになりえます。複数アクセスネットワーク(非 point-to-point)のルータ優先値のみ指定します。
Transmit Delay	「Transmit Delay」値(1-65533)を指定します。「Default」を指定すると初期値(1)を使用します。
Retransmit Interval	「Retransmit Interval」(再送信間隔)の値(1-65533 秒)を指定します。LSA をネイバに送信後、ルータは LSA を受信の
	通知まで保持します。指定の間隔、ルータが受信の通知を受け取らなかった場合、LSA を再送信します。余計な再送信を
	減らすため、再送信間隔は控えめに指定することを推奨します。間隔値は予想されるルータ間の往復の遅れよりも大きい
	値である必要があります。「Default」を指定すると初期値(5)を使用します。

「Apply」ボタンをクリックして行った変更を適用します。

# OSPFv3 Redistribute Settings (OSPFv3 リディストリビュート設定)

OSPFv3 リディストリビュート(再分配)について設定、表示を行います。

L3 Features > OSPF > OSPFv3 > OSPFv3 Redistribute Settings の順にメニューをクリックし、以下の画面を表示します。

OSPFv3 Redistribute Setti	ngs			
OSPFv3 Redistribute Settings				
Process ID (1-65535)				
Protocol	Connected 🗸			
Metric Type	External Type-1 🗸			
Metric (0-16777214)				
				Apply
Process ID (1-65535)				Find
Total Entries: 1				
Process ID	Protocol	Metric Type	Metric	
1	Connected	External Type-1	100	Delete

図 9-77 OSPFv3 Redistribute Settings 画面

# 画面に表示される項目:

項目	説明
Process ID	IPv6 OSPF ルーティングのプロセス ID(1-65535)を指定します。
Protocol	再分配される送信元プロトコルを指定します。「Connected」「Static」「RIP」「BGP」「ISIS」から指定します。OSPF のよう
	なルーティングプロトコルの場合、自立したシステムに外部として再分配されます。
Metric Type	メトリックの種類を指定します。「External Type-1」「External Type-2」から指定します。OSPF ルーティングドメインに再 分配されるルートの外部リンクタイプを指定します。メトリックタイプが指定されていないと、スイッチは「Type-2」外 部ルートを採用します。
Metric	再分配ルートのメトリック(1-16777214)を指定します。
$[Apply]$ $\exists a > b > b = 1$	クレア行った亦再を適用します

「Apply」ボタンをクリックして行った変更を適用します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Delete」をクリックすると指定のエントリを削除します。

# OSPFv3 Virtual Link Settings(OSPFv3 仮想リンク設定)

OSPFv3 仮想リンク設定を行います。

L3 Features > OSPF > OSPFv3 > OSPFv3 Virtual Link Settings の順にメニューをクリックして以下の画面を表示します。

OSPFv3 Virtual	Link Setting	S		_	_	_			
OSPFv3 Virtual Link									
Process ID (1-6553)	5)								
Instance ID (0-25	55)								
Area ID									
Router ID				14					
Hello Interval (1-655	(35)		1	s	ec		Default		
Dead Interval (1-655	535)			s	ec		Default		
Transmit Delay (1-6	5535)			s	ec		Default		
Retransmit Interval	(1-65535)			s	ec		Default		
									Apply
OSPFv3 Virtual Link	Table								
Process ID (1-6553)	5)								Find
1100000 10 (1-0000).	<i></i>								ring
Total Entries: 1									
Process ID	Area ID	Router ID	Instance ID	Hello	Dead	Transmit	Retransmit	LinkStatus	
1	10.3.3.3	192.168.9.1	0	10	40	1	5	Down	Delete
								1/1 < <	1 > > Go

図 9-78 OSPFv3 Virtual Link Settings 画面

# 第9章 L3 Features (レイヤ3機能の設定)

### 画面に表示される項目:

項目	説明
Process ID	IPv6 OSPF ルーティングのプロセス ID(1-65535)を指定します。
Instance ID (0-255)	インタフェースのインスタンス ID(0-255)を入力します。初期値は 0 です。
Area ID	OSPFv3 ドメイン内の OSPFv3 エリアをユニークに識別する 32 ビットの番号を IPv4 アドレス形式で入力します。
Router ID	リモートエリアの OSPFv3 ルータ ID。
Hello Interval (1-65535)	OSPF Hello パケットの送出間隔 (秒) を指定します。同じリンクの全ルータには同じ「Hello Interval」と「Dead Interval」 が設定される必要があります。初期値は 10 (秒) です。
Dead Interval (1-65535)	隣接ルータが Hello パケットを最後に受信してから、選択エリアがルータがダウンしたと判断するまでの時間(秒)を入力します。
Transmit Delay	「Transmit Delay」値(1-65533)を指定します。「Default」を指定すると初期値(1)を使用します。
Retransmit Interval	「Retransmit Interval」(再送信間隔)の値(1-65533 秒)を指定します。「Default」を指定すると初期値(5)を使用します。

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Process ID」のリンクをクリックすると指定の OSPFv3 プロセスのへのアクセス、設定を行います。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

# 「Process ID」をクリックすると、以下の画面が表示されます。

OSPPVS Virtual Link Detail Information		
OSPFv3 Virtual Link Information		
Process ID	1	
Neighbor Router ID	192.168.9.1	
Link Status	Down	
Transit Area	10.3.3.3	
Interface Name		
Instance ID	0	
Local Peer Address	::/128	
Remote Peer Address	::/128	
Transmit Delay (sec)	1	
State	Down	
Hello Interval Configured (sec)	10	
Dead Interval Configured (sec)	40	
Retransmit Interval Configured (sec)	5	
Adjacency State	Down	
		ОК

図 9-79 OSPFv3 Virtual Interface Settings - Edit 画面

# OSPFv3 LSDB Table (OSPFv3 LSDB テーブル)

OSPFv3 Link State Database(LSDB)を表示します。

# L3 Features > OSPF > OSPFv3 > OSPFv3 LSDB Table の順にメニューをクリックして以下の画面を表示します。

OSPFv3 LSDB 1	Table	_	_		_	_	
OSPFv3 LSDB Table	8						
Process ID (1-6553	5)						
LSDB Type		All					
Area ID		All	▼				
Link State		All	✓				Find
Total Entries: 2							
Process ID	Area ID	ADV Router	Age	Sequence Number	Check Sum	LSDB Type	
1	0.0.0.0	192.168.10.90	317	0x80000001	0xb419	Link	Show Detail
1	10.10.10.10	192.168.10.90	141	0x80000003	0xadb6	Router	Show Detail
						1/1 < <	1 > >  Go

図 9-80 OSPFv3 LSDB Table 画面

画面に表示される項目:

項目	説明					
Process ID	IPv6 OSPF ルーティングプロセスの ID(1-65535)を指定します。ローカルにアサインされルータの各 IPv6 OSPF ルーティ					
	ングプロセス固有である必要があります。					
LSDB Type	表示する LSDB タイプを指定します。「All」「Router」「Network」「Prefix」「Link」「Inter-Area Prefix」「Inter-Area Router」「External」					
	から選択します。					
	<ul> <li>All - LSDB 情報の全種類を表示します。</li> </ul>					
	・ Router - ルータ LSA の情報のみ表示します。					
	・ Network - ネットワーク LSA の情報のみ表示します。					
	• Prefix - 「intra-area-prefix LSA」の情報を表示します。					
	・ Link - リンク LSA の情報を表示します。					
	<ul> <li>Inter-Area Prefix - 「inter-area prefix LSA」に基づいた LSA の情報のみ表示します。</li> </ul>					
	・ Inter-Area Router - 「inter-area router LSA」に基づいた LSA の情報のみ表示します。					
	・ External - 「external LSA」の情報のみ表示します。					
Area ID	エリア ID オプションを指定します。「All」「Area ID」から指定可能です。 すべての LSA を指定のエリアから表示するには、「Area					
	ID」を指定し、OSPF エリア ID を空欄に入力します。IPv4 アドレスの形式で指定します。					
Link State	表示されるリンクステート情報を選択します。「All」「Self Originate」「Adv Router」から選択します。					
	・ All - 全てのリンクステート情報を表示します。					
	・ Self Originate - ローカルルータによって起動している LSA を表示します。					
	・ Adv Router - 通知ルータによって起動済みの全ての LSA を表示します。通知ルータ ID を空欄に入力します。					

「Find」ボタンをクリックして、指定したエントリを検索します。

# ■ エントリの詳細表示

例えば「Router LSA」の下の「Show Detail」リンクをクリックすると、以下の画面が表示されます。

OSPFv3 LSDB Information		
OSPFv3 LSDB Information		
Process ID	1	
Advertising Router ID	192.168.10.90	
Area ID	0.0.0.0	
LS Age	367	
LS Type	LINK	
Link State ID	0.0.0.1	
LS Seq Number	0x80000001	
Checksum	0xb419	
Length	44	
		Back
Detail Information		
Priority	1	
Options	0x11 (- R - - V6)	
Link-Local Address	FE80::F27D:68FF:FE34:10	
Number of Prefixes	0	

図 9-81 OSPFv3 LSDB Router LSA Table 画面

# OSPFv3 Neighbor Table(OSPFv3 Neighbor テーブル)

OSPFv3 Neighbor 情報を表示します。

L3 Features > OSPF > OSPFv3 > OSPFv3 Neighbor Table の順にメニューをクリックして以下の画面を表示します。

SPEV3 Neighbo	r Table	_	_		_		
SPFv3 Neighbor Tat	ble						
Process ID (1-65535) Interface VLAN (1-409	94)						Find
rveighbol							1110
Total Entries: 2							
Total Entries: 2 Process ID	Neighbor ID	Priority	State	Link Local Address	Interface	Instance ID	1110
Total Entries: 2 Process ID 1	Neighbor ID 30.90.90.90	Priority 1	State Full/DR	Link Local Address FE80::206:28FF:FED8:FE94	Interface vlan11	Instance ID 11	Show Detail
Total Entries: 2 Process ID 1 1	Neighbor ID 30.90.90.90 30.90.90.90	Priority 1 0	State Full/DR Full/-	Link Local Address FE80::206:28FF:FED8:FE94	Interface vlan11	Instance ID 11 0	Show Detail

図 9-82 OSPFv3 Neighbor Table 画面

画面に表示される項目	:
------------	---

項目	説明		
Process ID	IPv6 OSPFv3 プロセスの ID(1-65535)を指定します。		
Interface Name	Neighbor が組み込まれている IP インタフェースを指定します。		
Neighbor	Neighbor のルータ ID を入力します。IPv4 アドレスで指定します。		

「Find」ボタンをクリックして、指定したエントリを検索します。

### エントリの詳細表示

例えば「Router LSA」の下の「Show Detail」リンクをクリックすると、以下の画面が表示されます。

OSPFv3 Neighbor Detail Info	ormation	
OSPFv3 Neighbor Detail Information		
Process ID	1	
Neighbor Router ID	30.90.90	
Area	0.0.0.11	
Interface Name	vlan11	
Link Local Address	FE80::206:28FF:FED8:FE94	
Priority	1	
State	Full	
State Changes	5	
DR	30.90.90.90	
BDR	107.100.0.1	
Option	0x000013 (- R - - E V6)	
		Back

図 9-83 OSPFv3 Neighbor Table (Show Detail) 画面

「Back」をボタンをクリックして前のページに戻ります。

# OSPFv3 Border Router Table (OSPFv3 ボーダールーターテーブル)

OSPFv3 ボーダールーターについての情報を表示します。

L3 Features > OSPF > OSPFv3 > OSPFv3 Border Router Table の順にメニューをクリックして以下の画面を表示します。

OSPFv3 Border Router Table	_					
OSPFv3 Border Router Table						
Process ID (1-65535)						Find
Total Entries: 0						
Process ID Route Type	Router ID	Metric	Nexthop	Interface	Router State	Area ID

図 9-84 OSPFv3 Border Router Table 画面

画面に表示される項目:

項目	説明
Process ID	IPv6 OSPF ルーティングプロセスの ID(1-65535)を指定します。
「Find」ボタンをクリッ	クして、指定したエントリを検索します。

# IP Multicast Routing Protocol (IP マルチキャストルーティングプロトコル)

### L3 Features > IP Multicast Routing Protocol

IP Multicast Routing Protocol (IP マルチキャストルーティングプロトコル)の設定を行います。

# IGMP(IGMP 設定)(EI/MI モードのみ)

# L3 Features > IP Multicast Routing Protocol > IGMP

# IGMP Interface Settings (IGMP インタフェース設定)

IGMP(Internet Group Management Protocol)は、IP インタフェースごとを基本にスイッチに設定されます。スイッチに設定した各 IP インタフェースは、以下の「IGMP Interface Settings」画面に表示されます。

L3 Features > IP Multicast Routing Protocol > IGMP > IGMP Interface Settings の順にメニューをクリックして、以下の画面を表示します。



図 9-85 IGMP Interface Settings 画面

画面に表示される項目:

項目	説明
Interface VLAN	本設定に使用する IP インタフェース VLAN を指定します。
- 「Find」ボタンをクリックして、入ナ	した情報に基づく特定のエントリを検出します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

#### ■ エントリの編集

「Edit」ボタンをクリックして、以下の画面を表示します。

http://dciess vian1   P Address 10.90.90/8   buerier 0.0.0   resion 3< < default   tate Disabled < default   buery Interval (1-31744) 125 sec   buery Max Response Time (1-25) 10 sec   tobustness Variable (1-7) 2   ast Member Query Interval (1-25) 1 sec   kubscriber Source IP Check Enabled < default	MP Interface Settings				
P Address 10.90.90/8   Duerier 0.0.0   Version 3   State Disabled   Duery Interval (1-31744) 125 sec   Duery Max Response Time (1-25) 10 sec   Robustness Variable (1-7) 2   Last Member Query Interval (1-25) 1 sec   Subscriber Source IP Check Enabled	nterface	vlan1			
Duerier 0.0.0   Version 3   State Disabled   Duery Interval (1-31744) 125   sec default   Duery Max Response Time (1-25) 10   sec default   Robustness Variable (1-7) 2   2 default   sec default   Subscriber Source IP Check Enabled	P Address	10.90.90.90/8			
version 3   State Disabled   Duery Interval (1-31744) 125   sec default   Duery Max Response Time (1-25) 10   sec default   Robustness Variable (1-7) 2   2 default   Last Member Query Interval (1-25) 1   Subscriber Source IP Check Enabled	Querier	0.0.0.0			
State Disabled   Query Interval (1-31744) 125   sec default   Query Max Response Time (1-25) 10   sec default   Robustness Variable (1-7) 2   2 default   Last Member Query Interval (1-25) 1   sec default   Subscriber Source IP Check Enabled	Version	3 🗸	default		
Query Interval (1-31744)       125         Sec       default         Query Max Response Time (1-25)       10         sec       default         Robustness Variable (1-7)       2         Last Member Query Interval (1-25)       1         sec       default         Subscriber Source IP Check       Enabled	State	Disabled 🗸			
Query Max Response Time (1-25)       10	Query Interval (1-31744)	125 sec	default		
Robustness Variable (1-7)     2	Query Max Response Time (1-25)	10 sec	default		
Last Member Query Interval (1-25)       1	Robustness Variable (1-7)	2	🗌 default		
Subscriber Source IP Check Enabled	Last Member Query Interval (1-25)	1 sec	🗌 default		
	Subscriber Source IP Check	Enabled 🔽			

図 9-86 IGMP Interface Settings - Edit 画面

#### 以下の項目を使用します。

説明
インタフェースにおける IGMP クエリを解釈するのに使用する IGMP のバージョンを選択します。
「Default」を指定すると初期値を使用します。
プルダウンメニューを使用して、IP インタフェースの IGMP を「Enabled」(有効) / 「Disabled」(無効) にします。
初期値は Disabled です。
IGMP クエリを送信する間隔 (1-31744) を指定します。初期値は 125 (秒) です。「Default」を指定すると初期
値を使用します。
IGMP response report を送信するまでの最大時間 (1-25 秒) を入力します。初期値は 10 (秒) です。「Default」
を指定すると初期値を使用します。
大量のパケットの喪失が予想されるサブネットワークで許可される調整変数。1-7 の範囲で入力します。大量
のパケットの喪失が予想されるサブネットワークでは大きい数値を使用します。初期値は 2 です。「Default」
を指定すると初期値を使用します。
Leave Group メッセージをへの応答で送信するものも含め。Group-Specific Query メッセージの送信間隔(1-25)
を入力します。初期値は1(秒)です。「Default」を指定すると初期値を使用します。
「subscriber source IP check」 を「Enabled」(有効) / 「Disabled」(無効) に指定します。 初期値では、インタフェー
スとして、同じネットワーク内にの送信元 IP を指定するインタフェースに受信する IGMP リポートまたはリー
ブメッセージです。同じネットワークにない場合、メッセージ情報は IGMP プロトコルに学習されません。

項目を編集後「Apply」ボタンをクリックします。

「Back」をボタンをクリックして前のページに戻ります。

注意 IGMP Snooping において Querier Emulation をご利用の環境で、Specific Query の間隔が設定値より短くなります。

# IGMP Static Group Settings(IGMP スタティックグループ設定)

スイッチスタックにおける IGMP スタティックグループを設定します。

L3 Features > IP Multicast Routing Protocol > IGMP > IGMP Static Group Table の順にメニューをクリックして以下の画面を表示します。

IGMP Static Group Settings	_		
IGMP Static Group Table			
Interface VLAN (1-4094)			
Group			Apply
Interface VLAN (1-4094)	⊖ Group		Find Show All
Total Entries: 0			
Interface		Group Address	

図 9-87 IGMP Static Group Settings 画面

画面に表示される項目:

項目	説明
Interface VLAN	本設定に使用する IP インタフェース VLAN(1-4094)を指定します。
Group	マルチキャストグループ IP アドレスを指定します。

「Apply」をクリックし、設定内容を適用します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

「Show All」ボタンをクリックして、本スイッチに定義済みの全インタフェースを表示します。

# IGMP Dynamic Group Table(IGMP ダイナミックグループテーブル)

本項目では、IGMP ダイナミックグループ情報の表示、設定を行います。IGMP バッファは同じサブネット内のホストであるダイナミックマルチキャ ストグループを含むリストを保有しています。

L3 Features > IP Multicast Routing Protocol > IGMP > IGMP Dynamic Group Table の順にメニューをクリックして以下の画面を表示します。

IGMP Static Group Settings			
IGMP Static Group Table			
Interface VLAN (1-4094)			
Group			
			Apply
Interface VLAN (1-4094)	() Group		Find Show All
Total Entries: 0			
Interface	Group Ad	dress	

図 9-88 IGMP Dynamic Group Table 画面

画面に表示される項目:

項目	説明
Interface VLAN	本設定に使用する IP インタフェース VLAN(1-4094)を指定します。
Group	マルチキャストグループ IP アドレスを指定します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

「Clear」をクリックすると入力したエントリをクリアします。

「Clear All」をクリックすると入力したエントリを全てクリアします。

「Show All」ボタンをクリックして、本スイッチに定義済みの全インタフェースを表示します。

# IGMP SSM Mapping Settings (IGMP SSM マッピング設定)

本項目では、IGMP SSM マッピングの設定、表示を行います。「Source Specific Multicast」(SSM)の開発により、ネットワークサービスプロバイダは IP マルチキャストアドレスの管理を簡易に行うことが可能です。

SSM が有効な場合、「last hop」 のルータは付属の IGMPv3 ホストから、SSM 範囲から破棄された INCLUDE リクエスト (S,G) を受信したチャネル (S,G) のソースベースツリーを構築します。

これらのケースは付属のホストが、(\*, G) リクエストのみを提供する IGMPv1 または IGMPv2 ホストである場合です。SSM マッピングでは、リクエ ストされたマルチキャストグループが SSM 範囲内で落ちる場合、ルータは、ここで定義された送信元アドレスマッピングのグループアドレスに基 づく、(\*, G) から (S, G) へのリクエスト wp マップできるようになります。そしてルータはソースベースツリーをマップします (S, G)。もし複数のア ソシエーションが存在する場合、ルータは (S, G) ソースベースツリーを各 S に構築します。

IGMP SSM Mapping Settings	_		
IGMP SSM Mapping Settings			
SSM Mapping State Disabled 💌			Apply
Add Static SSM Mapping			
Source Address	ACL Name	32 chars Please Select	Apply
Total Entries: 1			
Access List		Source Address	
ACL		10.90.90.91	Delete
		[	1/1  < < 1 > >  Go
IGMP SSM Mapping Table			
Group Address 224 · 0 · 0 · 0			Find
Group Address		Source Address	
224.0.0.0	10.90.90.91		

図 9-89 IGMP SSM Mapping Settings 画面

L3 Features > IP Multicast Routing Protocol > IGMP > IGMP SSM Mapping Settings の順にメニューをクリックして以下の画面を表示します。

### 画面に表示される項目:

-

項目	説明
	IGMP SSM Mapping Settings
SSM Mapping State	IGMPv1/IGMPv2 ホストのための SSM マッピング機能を「Enabled」(有効)/「Disabled」(無効)に指定します。
	Add Static SSM Mapping
Source Address	アクセスリストで定義されたグループの送信元アドレスを指定します。
ACL Name	マップされるマルチキャストグループを含む IP アクセスリスト名を指定します。グループを許可するには、送 信元アドレスの項目に「any」を指定し、アクセスアドレスエントリの宛先アドレス項目にグループアドレス を指定します。「Please Select」を指定すると既存のアクセスリストを選択することも可能です。
	IGMP SSM Mapping Table
Group Address	IGMP マルチキャストグループアドレスを指定します。

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

### 「Please Select」をクリックすると、次の画面を表示します。

al Entries:	1		
	ID	ACL Name	ACL Type
0	1	SI-ACL	Standard IP ACL

図 9-90 IGMP SSM Mapping Settings (Select) 画面

設定するエントリを選択し「OK」をクリックします。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

# MLD(MLD 設定)(EI/MI モードのみ)

Multicast Listener Discovery(MLD) は、IGMP が IPv4 ルータで使用されたように、IPv6 ルータによって使用され、直接接続するリンク上のマルチキャ ストリスナ (マルチキャストパケットの受信を希望するノード)の存在の検出し、どのマルチキャストアドレスが Neighbor ノードに関連するかを特 に検出します。プロトコルは別々のプロトコルを使用する代わりに ICMPv6 に埋め込まれています。MLDv1 は IGMPv2,MLDv2 は IGMPv3 に似ています。

# MLD Interface Settings(MLD インタフェース設定)

MLD インタフェース設定を行います。

### L3 Features > IP Multicast Routing Protocol > MLD > MLD Interface Settings の順にメニューをクリックして以下の画面を表示します。



図 9-91 MLD Interface Settings 画面

以下の項目を使用します。

項目		
Interface VLAN 本設定に使用するインタフェース VLAN (1-4094)を指定します。		
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。		
Show All」をクリックして、すべてのエントリを表示します。		

「Edit」をクリックして、指定エントリの編集を行います。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

# ■ エントリの編集

「Edit」ボタンをクリックして、以下の画面を表示します。

an1 E80::F27D:68FF:FE34:1	0/128
an1 E80::F27D:68FF:FE34:1	0/128 default
E80::F27D:68FF:FE34:1	0/128
	default
2	default
Disabled 🔽	
25 s	sec 🔲 default
0 s	ec 🗌 default
9	default
	default
s	ec 🗌 default
2	isabled

図 9-92 MLD Interface Settings - Edit 画面

#### 以下の項目を使用します。

項目	説明
Version	送信するインタフェースおよび処理するパケットバージョンを決定する MLD バージョンを選択します。 1-2 から選択可能です。「Default」を指定すると初期値(MLDv2)を使用します。
MLD State	プルダウンメニューを使用して、IP インタフェースの MLD を「Enabled」(有効)/「Disabled」(無効)にします。 初期値は「Disabled」です。
Query Interval (1-31744)	MLD クエリの送出間隔 (1-31744) を指定します。初期値は 125 (秒) です。「Default」を指定すると初期値を使用します。
Query Max Response Time	MLD response report を送信するまでの最大時間 (1-25 秒) を入力します。初期値は 10 (秒) です。「Default」を指定 すると初期値を使用します。
Robustness Variable (1-7)	大量のパケットの喪失が予想されるサブネットワークで許可される調整変数。2-7の範囲で入力します。大量のパケットの喪失が予想されるサブネットワークでは大きい数値を使用します。初期値は2です。「Default」を指定すると初期値を使用します。
Last Listener Query Count	ラストメンバクエリカウント値(1-7)を指定します。ルータがグループ内にローカルメンバがいないと認識する前に、 「group-specific」または「group-source specific」クエリ送信の設定を行います。ルータがタイムアウトまでにホス トからレポートを受領しない場合、ルータはインタフェースのマルチキャストグループトラフィックの送信を中止 します。「Default」を指定すると初期値(2)を使用します。
Last Member Query Interval (1-25)	Leave Group メッセージをへの応答で送信するものも含め、Group-Specific Query メッセージの送信間隔 (1-25) を入 力します。初期値は 1 (秒) です。「Default」を指定すると初期値を使用します。

「Apply」ボタンをクリックして行った変更を適用します。

「Back」をボタンをクリックして前のページに戻ります。

# MLD Static Group Settings(MLD スタティックグループ設定)

MLDスタティックグループ設定を行います。付属のホストが MLD プロトコルをサポートしていない場合に MLD スタティックグループを作成します。 設定すると、グループメンバエントリが MLD キャッシュに追加されます。

L3 Features > IP Multicast Routing Protocol > MLD > MLD Static Group Settings の順にメニューをクリックして以下の画面を表示します。

MLD Static Group Settings		
MLD Static Group Table		
Interface VLAN (1-4094) Group FF80::C		Apply
Interface VLAN (1-4094)	O Group FF80::C	Find Show All
Total Entries: 1		
Interface	Multicast Group	
vlan1	FF80::C	Delete
		1/1 < 1 > > Go

図 9-93 MLD Static Group Settings 画面

画面に表示される項目:

項目	説明
Interface VLAN	本設定に使用するインタフェース VLAN(1-4094)を指定します。
Group	IPv6 マルチキャストグループアドレスを指定します。

「Apply」をクリックし、設定内容を適用します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Show All」をクリックして、すべてのエントリを表示します。

「Delete」をクリックすると指定のエントリを削除します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

# MLD Group Table(MLD グループテーブル)

スイッチにおける MLD スタティックグループを表示します。

L3 Features > IP Multicast Routing Protocol > MLD > MLD Group Table の順にメニューをクリックして以下の画面を表示します。

LD Group Table				_
MLD Group Table				
Interface VLAN (1-4094)	OGroup	FF80::C	Find	Show All
Total Entries: 0				
Interface	Group Address	Up Time	Expire Time	

図 9-94 MLD Group Table 画面

#### 画面に表示される項目:

項目	説明	
Interface VLAN	本設定に使用するインタフェース VLAN(1-4094)を指定します。	
Group	IPv6 グループアドレスを入力します。	
· Find」ボタンをクリックして、入力したインタフェースを検出します。		

「Show All」ボタンをクリックして、本スイッチに定義済みの全インタフェースを表示します。

# MLD SSM Mapping Settings (MLD SSM マッピング設定)

本項目では、MLD SSM マッピングの設定、表示を行います。

L3 Features > IP Multicast Routing Protocol > MLD > MLD SSM Mapping Settings の順にメニューをクリックして以下の画面を表示します。

MLD SSM Mapping	Settings			
MLD SSM Mapping Settin	igs			
SSM Mapping State	Disabled 🔽			Apply
Add Static SSM Mapping				
Source Address	28FE::1	ACL Name	32 chars Please Select	Apply
Total Entries: 1				
	Access List		Source Address	
	IPv6		28FE::1	Delete
				1/1  < < 1 > >  Go
MLD SSM Mapping Table	i s			
Group Address				Find
Grou	p Address		Source Address	

図 9-95 MLD SSM Mapping Settings 画面

画面に表示される項目:

項目	説明		
MLD SSM Mapping Settings			
SSM Mapping State	MLD SSM マッピング機能を「Enabled」(有効)/「Disabled」(無効)に指定します。		
	Add Static SSM Mapping		
Source Address	アクセスリストで定義されたグループの送信元アドレスを指定します。		
ACL Name	マップされるマルチキャストグループを含む IPv6 アクセスリスト名(32 字以内)を指定します。「Please		
	Select」を指定すると既存のアクセスリストを選択することも可能です。		
MLD SSM Mapping Table			
Group Address	IPv6 マルチキャストグループアドレスを指定します。		

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Please Select」をクリックすると、次の画面を表示します。



図 9-96 MLD SSM Mapping Settings (Select) 画面

設定するエントリを選択し「OK」をクリックします。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

# IGMP Proxy(IGMP プロキシ)(EI/MI モードのみ)

IGMP プロキシは、IGMP フォワーディングに基づいてアップストリームでは IGMP のホスト部分を、ダウンストリームでは IGMP のルータ部分を実行して、エッジボックスなどのデバイスに VLAN を横切るマルチキャストトラフィックを複製します。これによりコアネットワークに送信される IGMP コントロールパケット数を削減します。

# IGMP Proxy Settings(IGMP プロキシ設定)

IGMP プロキシの状態と IGMP プロキシのアップストリームインタフェースを設定します。

L3 Features > IP Multicast Routing Protocol > IGMP Proxy > IGMP Proxy Settings の順にメニューをクリックし、以下の画面を表示します。

GMP Proxy Settings		
IGMP Proxy Global Settings		
Global State	OEnabled  OEnabled	Apply
IGMP Proxy Upstream Settings		
Interface VLAN (1-4094)	Upstream Disabled	Apply
GMP Proxy Downstream Settings		
Interface VLAN (1-4094)	Downstream Disabled	Apply
GMP Proxy Designated Forwarding	ettings	
Interface VLAN (1-4094)	Designated Forwarding Disabled	Apply
GMP Proxy Table		
Upst	ream Interface	Downstream Interface
late: DE: The devinetreem interface is	optiqueed as designated forwarder	

Note: DF: The downstream interface is configured as designated forw

図 9-97 IGMP Proxy Settings 画面

#### 画面に表示される項目:

項目	説明
	IGMP Proxy Global Settings
Global State	ラジオボタンを使用して IGMP プロキシのグローバル状態を「Enabled」(有効)/「Disabled」(無効)にします。
	IGMP Proxy Upstream Settings
Interface VLAN	本設定に使用するインタフェース VLAN(1-4094)を指定します。
Upstream	アップストリーム IGMP プロキシとしてのインタフェースを「Enabled」(有効)/「Disabled」(無効)に指定します。
	IGMP Proxy Downstream Settings
Interface VLAN	本設定に使用するインタフェース VLAN(1-4094)を指定します。
Downstream	ダウンストリーム IGMP プロキシとしてのインタフェースを「Enabled」(有効)/「Disabled」(無効)に指定します。
	IGMP Proxy Designated Forwarding Settings
Interface VLAN	本設定に使用するインタフェース VLAN(1-4094)を指定します。
Designated Forwarding	ノンクエリア IGMP プロキシダウンストリームインタフェースでの指定転送について「Enabled」(有効)/「Disabled」 (無効)に指定します。複数の IGMP ベース転送者によるダウンストリームリンクの、ローカルループとリダンダント(冗 長)トラフィックを避けるために、IGMP プロキシは LAN の単一の転送者を選出するために、IGMP クエリアエレクショ ンを使用します。このオプションによりノンクエリアデバイスが転送者になります。本機能はインタフェースがダウ ンストリームインタフェースでない場合、またはアップストリームインタフェースの場合には有効にはなりません。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

# IGMP Proxy Group Table(IGMP プロキシグループテーブル)

IGMP プロキシグループ設定を参照します。

L2 Features > L2 Multicast Control > IGMP Proxy > IGMP Proxy Group Table の順にメニューをクリックし、以下の画面を表示します。

IGMP Proxy Group Table		
IGMP Proxy Group Table		
Group Address		Find Show All
Total Entries: 0		
Group Address	Filter Mode	Source List

図 9-98 IGMP Proxy Group 画面

以下の項目を使用して、設定および表示を行います。

項目	説明		
Group Address	IPv4 グループマルチキャストアドレスを入力します。		
- 「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。			

「Show All」をクリックして、すべてのエントリを表示します。

# IGMP Proxy Forwarding Table (IGMP フォワーディングテーブル)

IGMP プロキシのフォワーディング情報を検索、表示します。

L3 Features > IP Multicast Routing Protocol > IGMP Proxy > IGMP Proxy Forwarding Table の順にメニューをクリックし、以下の画面を表示します。

IP Proxy Forwarding Table			
roup Address			Find Show All
otal Entries: 0			
One of Address	Source Address	Incoming Interface	Outgoing Interface

図 9-99 IGMP Proxy Forwarding Table 画面

画面に表示される項目:

項目	説明		
Group Address	IPv4 グループマルチキャストアドレスを入力します。		
Find」をクリックして、入力した情報に基づく特定のエントリを検出します。			

「Show All」をクリックして、すべてのエントリを表示します。

# MLD Proxy(MLD プロキシ)(EI/MI モードのみ)

MLD プロキシはアップストリームインタフェースでホストの役割を果たします。MLD Report パケットはルータポートに送信されます。MLD プロキシは ダウンストリームインタフェースでルータの役割を果たします。これによりコアネットワークに送信される MLD コントロールパケット数を削減します。

# MLD Proxy Settings(MLD プロキシ設定)

MLD プロキシの状態と MLD プロキシのアップストリームインタフェースを設定します。

L3 Features > IP Multicast Routing Protocol > MLD Proxy > MLD Proxy Settings の順にメニューをクリックし、以下の画面を表示します。

MLD Proxy Settings			
MLD Proxy Global Settings			
Global State	CEnabled  OEnabled		Apply
MLD Proxy Upstream Settings			
Interface VLAN (1-4094)	Upstream  Disabled		Apply
MLD Proxy Downstream Settings			
Interface VLAN (1-4094)	Downstream Disabled		Apply
MLD Proxy Designated Forwarding Setting	]5		
Interface VLAN (1-4094)	Designated Forwarding Disabled		Apply
MLD Proxy Table			
Upstrear	m Interface	Downstream Interface	
Note: DF: The downstream interface is config	ured as designated forwarder.		

図 9-100 MLD Proxy Settings 画面

# 画面に表示される項目:

項目	説明
	MLD Proxy Global Settings
Global State	ラジオボタンを使用して MLD プロキシのグローバル状態を「Enabled」(有効)/「Disabled」(無効)にします。
	MLD Proxy Upstream Settings
Interface VLAN	本設定に使用するインタフェース VLAN(1-4094)を指定します。
Upstream	アップストリーム MLD プロキシとしてのインタフェースを「Enabled」(有効)/「Disabled」(無効)に指定します。
	MLD Proxy Downstream Settings
Interface VLAN	本設定に使用するインタフェース VLAN(1-4094)を指定します。
Downstream	ダウンストリーム MLD プロキシとしてのインタフェースを「Enabled」(有効)/「Disabled」(無効)に指定します。
	MLD Proxy Designated Forwarding Settings
Interface VLAN	本設定に使用するインタフェース VLAN(1-4094)を指定します。
Designated Forwarding	ノンクエリア MLD プロキシダウンストリームインタフェースでの指定転送について「Enabled」(有効) /「Disabled」 (無効)に指定します。複数の MLD ベース転送者によるダウンストリームリンクの、ローカルループとリダンダント(冗 長) トラフィックを避けるために、MLD プロキシは LAN の単一の転送者を選出するために、MLD クエリアエレクショ ンを使用します。このオプションによりノンクエリアデバイスが転送者になります。本機能はインタフェースがダウ ンストリームインタフェースでない場合、またはアップストリームインタフェースの場合には有効にはなりません。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

# MLD Proxy Group Table(MLD プロキシグループテーブル)

MLD プロキシグループテーブルを参照します。

L3 Features > IP Multicast Routing Protocol > MLD Proxy > MLD Proxy Group Table の順にメニューをクリックし、以下の画面を表示します。

ILD Proxy Group Table				
Group Address FF01::1			Find	Show All
Total Entries: 0				
Group Address	Filter Mode	Source List		

図 9-101 MLD Proxy Group Table 画面

#### 画面に表示される項目:

項目	説明		
Group Address	IPv6 グループマルチキャストアドレスを入力します。		
Find」をクリックして、入力した情報に基づく特定のエントリを検出します。			

「Show All」をクリックして、すべてのエントリを表示します。

# MLD Proxy Forwarding Table (MLD フォワーディングテーブル)

MLD プロキシのダウンストリームインタフェースを設定します。MLD プロキシのダウンストリームインタフェースは MLD Snooping が有効な VLAN である必要があります。

L3 Features > IP Multicast Routing Protocol > MLD Proxy > MLD Proxy Forwarding Table の順にメニューをクリックし、以下の画面を表示します。

MLD Proxy Forwarding Table			
MLD Proxy Forwarding Table			
Group Address FF01::1			Find Show All
Total Entries: 0			
Group Address	Source Address	Incoming Interface	Outgoing Interface

図 9-102 MLD Proxy Forwarding Table 画面

#### 画面に表示される項目:

項目	説明
Group Address	IPv6 グループマルチキャストアドレスを入力します。
	っした情報に基づく特定のエントリを検出します。

「Show All」をクリックして、すべてのエントリを表示します。

# DVMRP(EI/MI モードのみ)

L3 Features > IP Multicast Routing Protocol > DVMRP

# DVMRP Interface Settings(DVMRP インタフェース設定)

DVMRP インタフェース設定を行います。

L3 Features > IP Multicast Routing Protocol > DVMRP > DVMRP Interface Settings の順にメニューをクリックして以下の画面を表示します。

MRP Interface Settings	5						
nterface Name	vlan1					Find	Show All
otal Entries: 1							
Interface	Address	Neighbor Timeout	Probe	Metric	Generation ID	State	
	10 00 00 00	25	10	1	0	Disabled	Edit

図 9-103 DVMRP Interface Settings 画面

画面に表示される項目:

項目	説明					
Interface Name	DVMRP のインタフェース名を入力します。					

「Find」ボタンをクリックして、入力したインタフェースを検出します。

「Show All」ボタンをクリックして、本スイッチに定義済みの全インタフェースを表示します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

# ■ エントリの編集

編集するエントリの「Edit」ボタンをクリックして以下の画面を表示します。

	vlan1				Find	Show All
Address	Neighbor Timeout	Probe	Metric	Generation ID	State	
10.90.90.90	35	10	1	0	Disabled 💌	Apply
	Address 10.90.90.90	Vian1 Address Neighbor Timeout 10.90.90.90 35	Vian1           Address         Neighbor Timeout         Probe           10.90.90.90         35         10	Vian1           Address         Neighbor Timeout         Probe         Metric           10.90.90.90         35         10         1	Vlan1           Address         Neighbor Timeout         Probe         Metric         Generation ID           10.90.90.90         35         10         1         0	Vlan1     Find       Address     Neighbor Timeout     Probe     Metric     Generation ID     State       10.90.90.90     35     10     1     0     Disabled     V

図 9-104 DVMRP Interface Settings 画面 - Edit

画面に表示される項目	:
------------	---

項目	説明
Neighbor Timeout	ネイバライフタイム値(1-65535 秒)を指定します。ルータがネイバからのプルーブメッセージをネイバタイムアウ
	トまで受領しない場合、ネイバはダウンします。初期値は 35 です。
Probe	DVMRP プルーブインターバル(1-65535 秒)を指定します。初期値は 10 です。
Metric	メトリック値(1-32)を指定します。「32」は不達を意味します。各ソースネットワークにレポートされるのは、レ ポートされたルートのルートメトリックになります。メトリックはルータ起源のレポートとソースネットワーク間 のインタフェースメトリックの総量になります。DVMRPではメトリック「32」は不達を意味します。これにより全 DVMRPネットワーク間の広がりを制限し、プロトコルの収束時間の上限値として必要な値です。
State	指定インタフェースでの DVMRP 機能を「Enabled」(有効)/「Disabled」(無効)に指定します。

項目を編集後「Apply」ボタンをクリックします。

# DVMRP Routing Table(DVMRP ルーティングテーブル)

スイッチにおける DVMRP ルーティングテーブルを表示します。

L3 Features > IP Multicast Routing Protocol > DVMRP > DVMRP Routing Table の順にメニューをクリックして以下の画面を表示します。

DVMRP Routing Table			_	_	_	
DVMRP Routing Table						
Source Network	20.0.1.0/8				Find	Show All
Total Entries: 0						
Source Network	Upstream Neighbor	Metric	Learned	Interface	State	ExpTime
Note: State :H = Hold-down						

図 9-105 DVMRP Routing Table 画面

#### 画面に表示される項目:

項目	説明
Source Network	送信先の IPv4 ネットワークアドレスとネットマスクを入力します。
「Find」ボタンをクリックして	、入力した情報に基づく特定のエントリを検出します。

「Show All」ボタンをクリックして、本スイッチに定義済みの全インタフェースを表示します。

# DVMRP Neighbor Table (DVMRP Neighbor テーブル)

スイッチにおける DVMRP Neighbor テーブルを表示します。

### L3 Features > IP Multicast Routing Protocol > DVMRP > DVMRP Neighbor Table の順にメニューをクリックして以下の画面を表示します。

DVMRP Neighbor Table				
Interface Name	vlan1	O Neighbor IP Address		Find Show All
Total Entries: 0				
Interface	Neigh	bor Address	Generation ID	ExpTime

図 9-106 DVMRP Neighbor Table 画面

画面に表示される項目:

項目	説明
Interface Name	インタフェース名を入力します。
Neighbor IP Address	ネイバの IP アドレスを入力します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

「Show All」ボタンをクリックして、本スイッチに定義済みの全インタフェースを表示します。

# PIM(PIM 設定)(EI/MI モードのみ)

### L3 Features > IP Multicast Routing Protocol > PIM

PIM (Protocol Independent Multicast) は、LAN、WAN またはインターネット上にデータの 1 対多および多対多の配布を提供する IP (Internet Protocol) ネットワーク用のマルチキャストルーティングプロトコルのファミリです。PIM は、自身のトポロジ検出メカニズムを含まないため、プロトコルに依存しませんが、RIP または OSPF など他の従来型ルーティングプロトコルが提供するルーティング情報を使用します。本スイッチは PIM, Dense Mode (PIM-DM)、Sparse Mode (PIM-SM)、PIM Source Specific multicast (PIM-SSM)、および Sparse-Dense Mode (PIM-DM-SM) の 4 つの PIM タイプをサポートしています。

### • PIM-SM (Protocol Independent Multicast-Sparse Mode)

Sparse Mode (PIM-SM) は、基本的なユニキャストルーティング情報または個別のマルチキャストが可能なルーティング情報をベースに使用できるマルチキャストルーティングプロトコルです。これは、グループごとの RP(Rendezvous Point)を元に単方向の共有ツリーを構築し、オプションで送信元ごとに最短パスツリーを作成します。

PIM-SM は、ネットワークをマルチキャストパケットでフラッドさせる多くのマルチキャストルーティングプロトコルと異なり、Rendezvous Point(RP)を使用して、トラフィックを明示的にマルチキャストグループの一部であるルータに対し転送します。この RP は PIM-SM が有効であるルー タからすべてのリクエストを取得し、その情報を分析してネットワーク内でリクエストしているルータに対して送信元から受信したマルチキャスト 情報を返します。この方法を通じ、配信ツリーは、ルートとしての RP とともに作成されます。この配信ツリーは、すべての PIM-SM が有効である全ルー タを保持しています。RP はこれらのルータから収集した情報をここに保存しています。

多くのルータがマルチアクセスネットワークの一部である場合に、代表ルータ (DR) が選出されます。DR の第一の機能は RP に Join/Prune メッセージを送信することです。LAN 上で最も高いプライオリティを持つルータが DR として選出されます。最も高いプライオリティへの接続がある場合、より高い IP アドレスを持つルータが選出されます。

PIM-SM 設定で作成される 3 番目のルータタイプは、Boot Strap Router(BSR)です。BSR の目的は、RP 情報を収集し、LAN 上の PIM-SM が有効であるルー タにリレーすることです。RP はスタティックに設定されますが、BSR メカニズムが RP を決定することもできます。複数の Candidate BSR(C-BSR) がネッ トワーク上に設定されますが、1 つの BSR だけが、RP 情報を処理するために選出されます。どの C-BSR が、BSR になるかが明白でない場合、すべ ての C-BSR は、PIM-SM が有効であるネットワークに Boot Strap Messages(BSM) を放出し、より高いプライオリティを持つ C-BSR が BSR として選出 されます。一度決定されると、BSR は、PIM-SM ネットワークで Candidate RP から送信される RP データを収集し、それを編集し、周期的な BSM を 使用して LAN 上に送信します。すべての PIM-SM ルータは Boot Strap メカニズムから RP 情報を取得し、データベースに保持します。

# ● マルチキャストグループの検出(Discovery)と接続(Join)

Helloパケットは PIM-SM ルータを検出しますが、これらのルータは DR と RP 間で交換される Join/Prune メッセージを使用することでマルチキャス トグループからの接合または「Pruned」を行います。Join/Prune メッセージは、マルチキャストデータを受信するためにどのインタフェースがあ るのか、またはないのかを効果的に記述しているルータ間で中継されるパケットです。これらのメッセージは、頻繁に設定されネットワーク上に送 信され、Helloパケットがはじめに受信される場合にだけルータに有効となります。Helloパケットは、ルータが存在し、RP の配信ツリーの一部に なる準備中であることを簡単に記述しています。ルータが IGMP グループのメンバを受け入れて、PIM-SM が有効である場合、興味があるルータは 明確な Join/Prune メッセージを RP に送信します。それは、送信元から興味があるルータにマルチキャストデータを順番に送信し、グループのため の一定方向の配布ツリーを作成します。マルチキャストパケットは、その後これらのツリー上の全ノードに送信されます。一度 Prune メッセージが RP の送信ツリーのメンバであるルータに受信されると、ルータはその配信ツリーからそのインタフェースを削除します。

# ● 配信ツリー

2つのタイプの配信ツリーが PIM-SM プロトコル、Rendezvous-Point Tree(RPT) および最短経路ツリー (Shortest Path Tree:SPT) に存在します。RP は、 マルチキャストデータを受信することが可能なすべての外向きインタフェースに、送信元から受信した特定のマルチキャストデータを送信します。 しかし、一度ルータが送信元の位置を決定すると、SPT は、RP などの送信元と送信先の間のホップを除去して作成されます。これは、マルチキャス トデータ転送速度のしきい値を設定することで設定されます。しきい値を越えると、データの経路は SPT に切り換えます。従って、より近いリンク が送信元と宛先の間で作成され、以前に使われたホップを取り除き、マルチキャストパケットが送信元から最終到達先に送信される時間を短縮しま す。

#### ● Register と Register Suppression メッセージ

マルチキャストソースは、いつも意図する受信グループに接合するわけではありません。最初のホップルータ (DR) は、グループのメンバでなくても、 または明示された送信元も持たなくてもマルチキャストデータを送信することができます。それは本質的に、この情報を RP 配信ツリーに中継する 方法についての情報を持っていないと言うことを意味しています。この問題は、Register と Register-Stop メッセージを通じて緩和されます。DR が 受信したはじめのマルチキャストパケットがカプセル化され、RP に送信されます。RP は逆にカプセル化を解いて RP 配信ツリーの下に向かってパ ケットを送信します。ルートが確立すると、SPT が作成され、ルータを直接ソースに接続するか、マルチキャストトラフィックフローを開始して、 DR から RP への通信を行います。後者の場合、カプセル化されているタイプとカプセル化されていないタイプで同じパケットが 2 回送信される可能 性があります。RP はこの不備を検出し、カプセル化されたパケットの送信を停止するようにリクエストをしている DR に Register-stop メッセージ を戻します。

# ● Assert メッセージ

PIM-SM が使用可能なネットワークにおいて、時々パラレルパスが送信元から受信先に対して作成されます。これは複数の受信先が2回同じマルチ キャストパケットを受信することを意味しています。この状況を改善するために、Assert メッセージが受信デバイスから両方のマルチキャストソー スに送信され、どのルータが受信者に必要なマルチキャストデータを送信するかを決定します。最短メトリック(ホップカウント)を持つ送信元が プライマリマルチキャストソースとして選出されます。このメトリックは Assert メッセージ内に含まれています。

#### • PIM-SSM

SSM (Source Specific Multicast)機能は、IP マルチキャストの拡張機能です。ここではデータトラフィックは受信者が明確に参加しているというマ ルチキャスト送信元だけから受信者に送信されます。SSM 範囲のマルチキャストグループにおいて、送信元を指定したマルチキャスト配信ツリー(共 有ツリーはない)だけが作成されます。

IANA(Internet Assigned Numbers Authority)は SSM アプリケーションとプロトコルのために 232.0.0.0 ~ 232.255.255.255 のアドレス範囲を予約しています。スイッチは IP マルチキャストアドレス範囲 224.0.0.0 ~ 239.255.255.255 の任意のサブセットに SSM を設定できます。

#### • PIM-DM

PIM-DM(Protocol Independent Multicast-Dense Mode) プロトコルは、オーバヘッド削減の目的ではなく、マルチキャストパケットの配送を保証するために利用されるため、低遅延で高帯域のネットワークに適したプロトコルです。

PIM-DM マルチキャストルーティングプロトコルは、下流のルータがマルチキャストメッセージの受信を希望していると仮定し、下流のルータからのプルーンメッセージ(削除メッセージ)を受けて、マルチキャスト配信ツリーから、マルチキャストグループメンバの存在しない枝葉を Pruned します(削除します)。

PIM-DM には明示的な "Join" メッセージは存在しません。その代わりに、すべてのインタフェースマルチキャストメッセージの定期的なフラッディ ングに依存し、タイマの期限切れ (Join/Prune インターバル) を待つか、または下流のルータが明示的な "Prune" メッセージを送信して、その枝に はマルチキャストメンバが存在しない旨を示すのを待ちます。PIM-DM はその後マルチキャスト配信ツリーからこれらの枝を削除します。

マルチキャスト配信ツリーから刈り込まれた枝も、マルチキャスト配信グループへの参加を ( 将来的に ) 希望している可能性があります。そのため、 プロトコルは定期的にデータベースから "Prune( 削除 )" 情報を削除し、その枝のすべてのインタフェース宛てにマルチキャストメッセージのフラッ ディングを行います。この、"Prune" 情報の削除を行う間隔が Join/Prune インターバルです。

#### • PIM-SM-DM

PIM-SM では、RP は送信側の最初のホップルータです。最初のホップは、送信側がいつデータを送信するか RP を持っていないと、パケットを破棄し、 何も実行しません。Sparse-Dense モードはこの条件で有益です。Sparse-Dense モードで、パケットがすべての外向きのインタフェースでフラッドし、 pruning/joining(prune/graft) が RP が検出されない場合にと外向きのインタフェースを制御することが可能です。つまり、PIM Sparse-Dense モードは、 マルチキャストグループがどのモードで操作するかによって操作の Sparse モードまたは Dense モードのどちらかで扱われます。インタフェースが マルチキャストトラフィックを受信する場合、グループに既知の RP があれば、インタフェースの現在の操作モードは Sparse モードになり、そうで ない場合、インタフェースの現在の操作モードは Dense モードになります。

# ■ PIM for IPv4(IPv4 用 PIM の設定)

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4

### PIM Interface (PIM インタフェース設定)

PIM インタフェースの設定を行います。

### L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM Interface の順にメニューをクリックして以下の画面を表示します:

PIM Interface	_	_	_	_	_	_	_	_
PIM Interface Search								
Interface Name vlan	n1	OMo	de Dense M	Node 🔽			Find	Show All
PIM Interface Table								
Total Entries: 1								
Interface Address	Interface Name	Mode	Passive	Neighbor Count	DR Priority	Designated Router	Generation ID	
10.90.90.90	vlan1	Dense	Disabled	0	1	0.0.0	0	Edit
							1/1 < < 1	> >  Go

図 9-107 PIM Interface Settings 画面

画面に表示される項目:

項目	説明	
Interface Name	インタフェース名を指定します。	
Mode	使用する PIM プロトコルのタイプ (Sparse Mode(SM)、Dense Mode(DM)、または Spare-Dense Mode(SM-DM)) を選 択します。初期値は「DM」です。	
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。		

「Show All」をクリックして、すべてのエントリを表示します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

# エントリの編集

「Edit」ボタンをクリックして、以下の画面を表示します。

PIM Interface Detail	
PIM Interface Detail	
Interface Name	vlan1
Interface Address	10.90.90
Neighbor Count	0
Generation ID	0
PIM State	Disabled
Mode	Sparse-Dense Mc
PIM Passive	Disabled
Query Interval (1-18724)	30 sec Default
Designated Router	
DR Priority (0-4294967295)	
Join Prune Interval (1-18000)	sec Default
BSR Domain Border	Disabled
	Apply Back

図 9-108 PIM Interface Settings - Edit 画面

画面に表示される項目:			
項目	説明		
PIM State	PIM を「Enabled」(有効)/「Disabled」(無効)にします。初期値は Disabled です。		
Mode	<ul> <li>使用する PIM プロトコルのタイプ (Sparse Mode(SM)、Dense Mode(DM)、または Spare-Dense Mode(SM-DM))を選択します。初期値は「DM」です。</li> <li>Dense Mode - 「PIM-DM」送信元が送信を開始した時、すべてのダウンストリームルータはマルチキャストデータストリームの受信を希望します。基本的にはマルチキャストデータストリームルータやグループメンバがない場合、ループメンバのインタフェースでフラッドします。ダウンストリームルータやグループメンバがない場合、ルータはマルチキャストデータが必要とされていないことを示すプルーンメッセージを送信します。</li> <li>Sparse Mode - マルチキャストトラフィックが「Sparse Mode」のインタフェースに受信すると、最初のホップルータは登録メッセージをカプセル化し、RP へ送信します。ルータがファーストホップでない場合、mroute エントリを元にトラフィックは転送されます。「sparse」モードインタフェースは mroute メンバインタフェースのように混雑した状態となり、ダウンストリームルータから、または sprse モードインタフェースのグループメンバからのジョインメッセージを受信します。PIM ジョインプロセスはシェアツリーまたはソースツリーの作成を開始します。</li> <li>Sparse-Dense Mode - インタフェースが「PIM Sparse-Dense」モードでも操作が可能になります。インタフェースがマルチキャストトラフィックを受信すると、グループの RP を学習済みの場合、グループは「sparse」モードで動作します。</li> </ul>		
PIM Passive	PIM パッシブ機能を「Enabled」(有効)/「Disabled」(無効)に指定します。パッシブモードが有効の場合、インタフェースは PIM の送信も、PIM メッセージの受信も行いません。ルータはネットワークで唯一の PIM ルータとして動作します。本機能は LAN に PIM ルータが一つのみある場合、使用します。		
Query Interval (1-18724)	この IP インタフェースから 1 ホップ隣の隣接ルータに Hello パケットを送信する間隔を設定します。これらの Hello パケットは他の PIM が有効なルータを検出し、PIM が有効なネットワーク上の DR としてプライオリティを指定する ために使用されます。1-18724(秒) で指定します。初期値は 30(秒) です。		
DR Priority (0-4294967295)	IP インタフェースのマルチアクセスネットワークで DR になるためのプライオリティを入力します。0-4294967295 で入力します。初期値は 1 です。		
Join Prune Interval (1-18000)	どのマルチキャストグループが PIM の有効なネットワークに接合し、そのグループから削除または「Pruned」を設定する Join/Prune パケットを送信する間隔を設定します。1-18000(秒)で指定します。初期値は 60(秒)です。		
BSR Domain Border	「Bootstrap Router」(BSR) ドメインボーダー機能を「Enabled」(有効)/「Disabled」(無効)に指定します。PIM は 有効なインタフェースでのみ有効です。インタフェースでこの機能を使用すると、ドメイン間の BSR メッセージを 交換を回避するために、他のドメインを隣接させます。		

項目を編集後「Apply」ボタンをクリックします。

「Back」をボタンをクリックして前のページに戻ります。

# PIM BSR Candidate (PIM BSR Candidate 設定)

PIM が有効なネットワークで Boot Strap Router(BSR) になるために、Candidate Boot Strap Router(C-BSR) 設定と指定 IP インタフェースのプライオリ ティを設定します。Boot Strap Router はネットワーク上のどのルータがマルチキャストグループに対して RP として選出され、他の PIM-SM が有効 なルータに RP 情報を収集して、配布するのかを決定する情報を保持しています。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM BSR Candidate の順にメニューをクリックして以下の画面を表示します。

PIM BSR Candidate				
BSR Candidate Settings				
Interface Name	vlan1			
Hash Mask Length(0-32)	30	Default		
Priority(0-255)	64	Default		
Interval(1-255)	60	sec 🖌 Default		
	de la constanción de			Add Delete
Bootstrap Information				
BSR Address				
BSR Priority				
BSR Hash Mask Length				
Next Bootstrap Message in				
Next Candidate RP Advertisement in				
Group Mapping Table				
Total Entries: 0				
	RP Candidate		Gro	up Access List

図 9-109 PIM BSR Candidate 画面

画面に表示される項目:

項目	説明
Interface name	インタフェース名を入力します。
Hash Mask Length	ハッシュマスク長を入力します。これは Candidate RP の IP アドレスとマルチキャストグループアドレスと共に使用 されます。ルータに使用されるハッシュアルゴリズムが PIM-SM の有効なネットワークでどの C-RP が RP になるか を決定するために計算します。0-32 で指定します。初期値は 30 です。
Priority	「Candidate Bootstrap Router」(CBSR) プライオリティ値(0-255)を指定します。最優先値での設定が望まれます。 優先値が同じ場合、最高値の IP アドレスを持つルータが優先的になります。「Default」を指定すると初期値(64) を使用します。
Interval	スイッチが PIM の有効なネットワークに Boot Strap Messages(BSM) を送信する間隔を 1-255 で入力します。初期値は 60(秒) です。

「Apply」ボタンをクリックして行った変更を適用します。

「Delete」をクリックすると指定のエントリを削除します。

#### ■ PIM RP Address (PIM RP アドレス設定)

本画面では RP マッピングを行うスタティックマルチキャストグループの設定、表示を行います。マルチキャストドメインでは RP マッピングのスタ ティックマルチキャストグループは BSR とともに使用されます。すべてのドメイン内のルータは RP マッピングに矛盾のないマルチキャストグルー プを保持する必要があります。レジスタメッセージを起動する最初のホップルータは、指定グループに向けられた PIM レジスタメッセージを送信す るための RP を決定するマッピングエントリを使用します。ジョインメッセージを起動する最後のホップルータは、指定グループに向けられたジョ イン / プルーンメッセージを送信するための RP を決定するマッピングエントリを使用します。ルータがジョインメッセージを受信すると、メッセー ジ転送のためにマッピングエントリをチェックします。RP がレジスタメッセージを受信する時、ルータがマルチキャストグループへの正しい RP で ない場合、レジスタ停止メッセージが送信されます。複数の RP が単一のアクセスリストとともに定義されます。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM RP Address の順にメニューをクリックして以下の画面を表示します。

PIM RP Address				_
RP Address Settings -				
RP Address	14 - 14 - 14 - 14 - 14 - 14 - 14 - 14 -	Group Access List Name	All Groups	Show List
			Add	Delete
RP Address Table				
	RP Address		Group Access List	
	10.10.10.10		224.0.0.0/4	
			1/1 < < 1	> >  Go

図 9-110 PIM RP Address 画面

#### 画面に表示される項目:

項目	説明
RP Address	RP IPv4 アドレスを入力します。
Group Access List Name	使用する通常のアクセスリストを指定します。「Show List」をクリックするとスイッチに既存作成されている ACL リストを検出、選択することができます。「All Groups」を指定すると「RP」を全マルチキャストグループにマップ します。

「Apply」ボタンをクリックして行った変更を適用します。

# エントリの登録

「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

#### エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。 「Show List」をクリックすると、以下の画面が表示されます。

Access Control Lis	st		
ACL Type	IP ACL		Find Show All
Total Entries: 1			
	ACL Name		Туре
۲	ACL		Standard IP ACL
			1/1  < < 1 > >  Go
ACL Rule			
Action		Rule	
Permit	any any		
			Apply

図 9-111 PIM RP Address (Show List) 画面

#### 以下の項目を使用します。

項目	説明
ACL Type	テーブル内の既存の表示する ACL タイプを指定します。
	「IP ACL」「Expert IP ACL」「IPv6 ACL」「Expert IPv6 ACL」「MAC ACL」「Expert ACL」から選択します。
ACL List	使用するアクセスリストを指定します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Show All」をクリックして、すべてのエントリを表示します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。 「Apply」をクリックし、設定内容を適用します。

# ■ PIM RP Candidate (PIM RP Candidate 設定)

本画面では PIM RP Candidate の設定、表示を行います。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM RP Candidate の順にメニューをクリックして以下の画面を表示します。

PIM RP Candidate		
RP Candidate Global Settings		
Priority(0-255)	192 Default	
Interval(1-16383)	60 sec 🗌 Default	
Wildcard Prefix Count(0 or 1)	0 Default	
		Арріу
RP Candidate Settings		
Interface Name vlan1	Group Access List Name	All Groups Show List
		Add Delete
RP Candidate Table		
Total Entries: 1		
l l	Interface Name	Group Access List
	vlan1	224.0.0.0/4
		1/1 < < 1 > > Go

図 9-112 PIM RP Candidate 画面

画面に表示される項目:

項目	説明	
	RP Candidate Global Settings	
Priority	「candidate RP」プライオリティ値(0-255)を指定します。「Default」を指定すると初期値(192)を使用します。	
Interval	「candidate RP」を送信する間隔を 1-16383 で入力します。Default」を指定すると初期値(60 秒)を使用します。	
Wildcard Prefix Count	C-RP メッセージのマルチキャストグループアドレスワイルドカード (224.0.0.0/4) プリフィクスカウント値(0-1)を 指定します。「Default」を指定すると初期値(0)を使用します。	
	RP Candidate Settings	
Interface name	インタフェース名を入力します。	
Group Access List Name	使用する通常のアクセスリストを指定します。「Show List」をクリックするとスイッチに既存作成されている ACL リストを検出、選択することができます。「All Groups」を指定すると「RP」を全マルチキャストグループにマップ します。	

「Apply」ボタンをクリックして行った変更を適用します。

#### エントリの登録

「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

#### エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Show List」をクリックすると、以下の画面が表示されます。

Access Control L	ist	
ACL Type	IP ACL	Find Show All
Total Entries: 1		
	ACL Name	Туре
۲	ACL	Standard IP ACL
		1/1 < < 1 > > Go
ACL Rule		
Action	Rule	
Permit	any any	
		Apply

図 9-113 PIM RP Candidate (Show List) 画面

画面に表示される項目:

項目	説明	
ACL Type	テーブル内の既存の表示する ACL タイプを指定します。	
	「IP ACL」「Expert IP ACL」「IPv6 ACL」「Expert IPv6 ACL」「MAC ACL」「Expert ACL」から選択します。	
ACL List	使用するアクセスリストを指定します。	

「Show All」をクリックして、すべてのエントリを表示します。 設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Apply」をクリックし、設定内容を適用します。

# ■ PIM RP Table (PIM RP テーブル)

本画面では PIM RP 情報の検索、表示を行います。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM RP Table の順にメニューをクリックして以下の画面を表示します。

PIM RP Table					
RP Mapping Table					
RP Hash .					Find Show All
Total Estate a					
Total Entries: 0					
Group(s)	RP Address	Info Source	RP Priority	Uptime	Expires
					· · · · · · · · · · · · · · · · · · ·

図 9-114 PIM RP Table 画面

#### 以下の項目を使用します。

項目	説明	
RP Hash	IPv4 マルチキャストグループアドレスを指定します。	

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。 「Show All」をクリックして、すべてのエントリを表示します。

# ■ PIM Register Settings (PIM レジスタ設定)

本画面では PIM レジスタの設定、表示を行います。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM Register Settings の順にメニューをクリックして以下の画面を表示します。

Plini Register Settings		
Register Checksum Wholepkt		
RP Address Access List Name		Add Delete
Register Probe Time		
Register Probe(1-127)	5 sec 🗌 Default	Apply
Register Suppression Time		
Register Suppression(3-65535)	60 sec 🗌 Default	Apply
Register Keepalive Time		
Register Keepalive(1-65525)	185 sec 🗌 Default	Apply

図 9-115 PIM Register Settings 画面

画面に表示される項目:

項目	説明	
	Register Checksum Wholepkt	
RP Address Access List Name	使用する通常のアクセスリストを指定します。「Show List」をクリックして既存のアクセスリストを指定することも可能です。	
Register Probe Time		
Register Probe	Register-Stop メッセージの再送を起こすように DR が Null-Register を RP に送信する場合に Register-Stop Timer (RS が期限切れになるまでの時間を入力します。「Default」を選択すると初期値(5 秒)を指定します。	
	Register Suppression Time	
Register Suppression レジスタ抑止タイムアウト値(3-65535)を入力します。DR がレジスタ停止メッセージを受領すると、抑止タイ が指導します。抑止の間、DR は RP へのレジスタメッセージを停止します。最初のホップルータで本機能を使用 ます。レジスタプローブタイムはレジスタ停止タイマのネガティブ値を防ぐためにも、レジスタ抑止タイムの半 以下である必要があります。最少タイマ値は「3」です。「Default」を選択すると初期値(60秒)を指定します		
Register Keepalive Time		
Register Keepalive	キープアライブ間隔(1-65525 秒)を入力します。「Default」を選択すると初期値(185 秒)を指定します。	

「Apply」ボタンをクリックして行った変更を適用します。

### エントリの登録

「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

# エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

「Show List」をクリックすると、以下の画面が表示されます。

Access Control L	ist		
ACL Type	IP ACL		Find Show All
Total Entries: 1			
	ACL Name		Туре
۲	ACL		Standard IP ACL
		1/1	< < 1 > >  Go
ACL Rule			
Action		tule	
Permit	any any		
			Apply

図 9-116 Show List 画面

# 画面に表示される項目:

説明	
テーブル内の既存の表示する ACL タイプを指定します。	
「IP ACL」「Expert IP ACL」「IPv6 ACL」「Expert IPv6 ACL」「MAC ACL」「Expert ACL」から選択します。	
使用するアクセスリストを指定します。	

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Show All」をクリックして、すべてのエントリを表示します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Apply」をクリックし、設定内容を適用します。

#### ■ PIM SPT Threshold Settings (PIM SPT しきい値設定)

本画面では PIM SPT しきい値を表示、設定します。最後のホップルータで使用します。PIM-SM モードだと、送信元からのマルチキャストトラフィックは「RPT シェアツリー」を通じて受信者へフローされます。最初のパケット最後のホップルータに受信されると、トラフィックの各グループは、次の二つのモードのどちらかで操作可能です。「Infinity」モードだとトラフィックはシェアツリーのフォローし、「0」モードの場合、ソースツリーが構築され、トラフィックスイッチオーバがソースツリーに向かいます。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM SPT Threshold Settingsの順にメニューをクリックして以下の画面を表示します。

PIM SPT Threshold Settings		
PIM SPT Threshold		
SPT Threshold	Infinity Default	Apply

図 9-117 PIM SPT Threshold Settings 画面

#### 画面に表示される項目:

項目	説明
SPT Threshold	SPT しきい値を指定します。 ・ 0 - 最初のパケットの到着でソースツリーを構築します。 ・ Infinity - シェアツリーに依存します。 「Default」を選択すると初期値(Infinity)を指定します。

「Apply」をクリックし、設定内容を適用します。

#### ■ PIM SSM Settings (PIM SSM 設定)

本画面では PIM SSM の設定、表示を行います。最後のホップルータでのみ使用可能です。SSM が有効な場合、最後のホップルータは、添付のホストから SSM 範囲内で破棄される (S,G) リクエストを含む IGMPv3 を受信するチャンネル (S,G) のソースベースツリーの構築を開始します。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM SSM Settings の順にメニューをクリックして以下の画面を表示します。

P	IM SSM Settings		_	
E F	PIM SSM Settings			
	Multicast Group Address Name	Default SSM Group(232.0.0.0/8)		Show List
			Add	Delete

#### 図 9-118 PIM SSM Settings 画面

#### 画面に表示される項目:

項目	説明
Multicast Group Address	ユーザ指定 SSM グループアドレスを定義する通常の IP アクセスリストを指定します。グループアドレスはルールエ
Name	ントリの宛先 IP アドレス項目で定義されます。「Show List」から既存のアクセスリストを指定することも可能です。
	「Default SSM Group」(232.0.0.0/8) オプションを指定すると、初期値の SSM グループアドレス(232/8)を指定します。

#### エントリの登録

「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

# エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

「Show List」をクリックすると、以下の画面が表示されます。

Access Control Lis			
ACL Type	IP ACL		Find Show All
Total Entries: 1			
	ACL Name		Туре
۲	ACL		Standard IP ACL
			1/1  < < 1 > >  Go
ACL Rule			
Action		Rule	
Permit	any any		
			Apply

図 9-119 Show List 画面

画面に表示される項目:

項目	説明
ACL Type	テーブル内の既存の表示する ACL タイプを指定します。
	「IP ACL」「Expert IP ACL」「IPv6 ACL」「Expert IPv6 ACL」「MAC ACL」「Expert ACL」から選択します。
ACL List	使用するアクセスリストを指定します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Show All」をクリックして、すべてのエントリを表示します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Apply」をクリックし、設定内容を適用します。

# ■ PIM Neighbor Table (PIM ネイバテーブル)

本画面では PIM ネイバ 情報の検索、表示を行います。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM Neighbor Table の順にメニューをクリックして以下の画面を表示します。

PIM Neighbor Table				_	_	_
Neighbor Information Ta	Neighbor Information Table					
Interface Name	Interface Name Vian1 Find Show All					
Total Entries: 0						
Neighbor	Interface Name	Uptime	Expires	Version	DR Priority	Mode
Note: DR - Designated I	Router. N - Default DR Priority.	G – Generation ID				

図 9-120 PIM Neighbor Table 画面

以下の項目を使用します。

項目	説明		
Interface Name	PIM-SM ネイバ情報を表示する VLAN インタフェースを指定します。		

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Show All」をクリックして、すべてのエントリを表示します。

# PIM for IPv6(IPv6 用 PIM の設定)

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv6

#### ■ PIM for IPv6 Interface (PIM IPv6 インタフェース設定)

PIM IPv6 インタフェースの設定を行います。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv6 > PIM for IPv6 Interface の順にメニューをクリックして以下の画面を表示します:

PIM for IPv	6 Interface		_	_		_	_	_	_	_
PIM for IPv6 I	nterface Search									
Interface N	Name 12 chars	ON	Node Spa	arse Mode 🖌	]			Find		Show All
PIM for IPv6 I	nterface Table									
Total Entries	:: 1									
Interface Name	Interface Link-Local Address	Interface Global Address	Mode	Neighbor Count	Designated Router	DR Priority	Helio Interval	Join Prune Interval	Border	
vlan1	:	:	None	0	not elected	1	30	60	disabled	Edit
							1/1	< <	1 >	>  Go

図 9-121 PIM for IPv6 Interface 画面

画面に表示される項目:

項目	説明
Interface Name	VLAN インタフェース名を指定します。
Mode	フィルタ検索における IPv6 PIM エントリの操作モードを「Sparse Mode」「Dense Mode」から指定します。
「Find」をクリックして、入力	した情報に基づく特定のエントリを検出します。

「Show All」をクリックして、すべてのエントリを表示します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

### エントリの編集

「Edit」ボタンをクリックして、以下の画面を表示します。

PIM for IPv6 Interface Detail	
PIM for IPv6 Interface Detail	
Interface Name	vian1
Interface Link-Local Address	FE80::F27D:68FF:FE34:10
Interface Global Address	:: · · · · · · · · · · · · · · · · · ·
Mode	None
Designated Router	not elected
Designated Router Priority(0-4294967295)	1 Default
Designated Router Priority Enabled	True
Generation ID	0
Hello Interval(1-18000)	30 sec 🗌 Default
Triggered Hello Interval	5 sec
Hello Holdtime	105 sec
Join Prune Interval(1-18000)	60 sec 🗌 Default
Join Prune Holdtime	210 sec
LAN Delay Enabled	True
Propagation Delay	1 sec
Override Interval	3 sec
Effective Propagation Delay	1 sec
Effective Override Interval	3 sec
Join Suppression Enabled	False
Bidirectional Capable	False
BSR Domain Border	Disabled 🔽
PIM Passive Mode	Disabled 🗸
	Apply Back

図 9-122 PIM for IPv6 Interface Detail 画面

画面に表示される項目:

項目	説明
Mode	使用する IPv6 PIM プロトコルのタイプ(「None」「Sparse Mode(SM)」「Dense Mode」)を選択します。
Designated Router Priority (0-4294967295)	本インタフェースに送信される IPv6 の PIM Hello メッセージの DR Priority(DR 優先度)オプションに挿入される Designated Router Priority(代表ルータ優先度)値を入力します。この値が高いほど高い優先度を示します。
Hello Interval (1-18000)	この IP インタフェースから 1 ホップ隣の隣接ルータに Hello パケットを送信する間隔を設定します。これらの Hello パケットは他の PIM が有効なルータを検出し、PIM が有効なネットワーク上の SM としてプライオリティを指定する ために使用されます。1-18000(秒) で指定します。初期値は 30(秒) です。
Join Prune Interval (0-18000)	本ルータが IPv6 インタフェースのこの PIM に IPv6 の PIM Join/Prune メッセージを送信する頻度を入力します。0 の 値は「無限」の間隔を示しており、定期的な IPv6 の PIM Join/Prune メッセージがこのインタフェースに送信される べきではないことを示します。
BSR Domain Border	プルダウンメニューを使用して、IPv6 PIM ドメインの境界のとなるインタフェースを「Enabled」(有効)/「Disabled」(無効) にします。このインタフェースが境界を設定すると、Bootstrap(BSR) ルータメッセージがそこを経由して送信 または受信されることを防止します。
PIM Passive Mode	PIM パッシブ機能を「Enabled」(有効)/「Disabled」(無効)に指定します。パッシブモードが有効の場合、インタフェースは PIM の送信も、PIM メッセージの受信も行いません。ルータはネットワークで唯一の PIM ルータとして動作します。本機能は LAN に PIM ルータが一つのみある場合、使用します。

項目を編集後「Apply」ボタンをクリックします。

「Back」をボタンをクリックして前のページに戻ります。

### ■ PIM for IPv6 BSR Candidate Settings (PIM for IPv6 BSR Candidate 設定)

本項目では「IPv6 PIM BSR candidate」設定を行います。「PIM-SM」の動作にのみ影響を与えます。これによりルータは全ての PIM ネイバに BSR アドレスとしての宛先インタフェースのアドレスとともに、「bootstrap」メッセージを送信するようになります。「PIM-SM」ドメインは RP 情報の通知 と収集に責任のある固有の「BSR」(Bootstrap Router) を含んでいる必要があります。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv6 > PIM for IPv6 BSR Candidate Settings の順にメニューをクリックして以下の画面 を表示します。

PIM for IPv6 BSR Candidate S	ettings	
BSR Candidate Settings		
Interface Name	vlan1	
Hash Mask Length(0-128)	Default	
Priority(0-255)	Default	
		Add Delete
Candidate BSR Information		
Candidate BSR Address		
Candidate BSR Priority		
Candidate BSR Hash Mask Length		
BSR Election Information		
BSR Address		
BSR Priority		
Hash Mask Length		
Uptime		
BSTIME		

図 9-123 PIM for IPv6 BSR Candidate Settings 画面

画面に表示される項目:

項目	説明
Interface name	インタフェース VLAN 名を入力します。
Hash Mask Length	ハッシュマスク長を入力します。これは Candidate RP の IP アドレスとマルチキャストグループアドレスと共に使用され ます。ルータに使用されるハッシュアルゴリズムが PIM-SM の有効なネットワークでどの C-RP が RP になるかを決定す るために計算します。0-128 で指定します。初期値は 126 です。
Priority	「Candidate Bootstrap Router」(CBSR) プライオリティ値(0-255)を指定します。最優先値での設定が望まれます。優先 値が同じ場合、最高値の IP アドレスを持つルータが優先的になります。「Default」を指定すると初期値 (64) を使用します。

「Add」をクリックし、入力した情報に基づくエントリを追加します。

「Delete」をクリックすると指定のエントリを削除します。

#### ■ PIM for IPv6 BSR Table (PIM for IPv6 BSR テーブル)

本項目は「IPv6 PIM BSR」情報を表示します。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv6 > PIM for IPv6 BSR Table の順にメニューをクリックして以下の画面を表示します。

PIM for IPv6 BSR Table		_		
BSR Candidate RP Cache				
Total Entries: 0				
Group(s)	RP Address	RP Priority	Uptime	Expires
BSR Candidate RP Information				
Total Entries: 0				
Candidate RP	Priority	Holdtime	Advertisement Interval	Next Advertisement

図 9-124 PIM for IPv6 BSR Table 画面

### ■ PIM for IPv6 RP Address (PIM for IPv6 RP アドレス)

本画面では IPv6 PIM RP アドレスの設定、表示を行います。「PIM-SM」の動作にのみ影響を与えます。

「sparse」モードで動作するマルチキャストグループの RP アドレスを手動で定義します。一つ以上のグループに単一の RP を使用します。アクセス リストによって設定された条件により、どのグループが RP を使用するのかを決定します。複数の RP が定義可能で、それぞれ単一のアクセスリスト を保持します。新しい設定内容は古いものを上書きします。

ドメインの全てのルータは RP マッピングに有効なマルチキャストグループを保持している必要があります。レジスタメッセージを起動する最初の ホップルータは、指定グループへの PM レジスタメッセージを送信する RP を決定するマッピングエントリを使用します。ジョインメッセージを起 動する最後のホップルータは、指定グループへのジョイン / プルーンメッセージを送信する RP を決定するマッピングエントリを使用します。ルー タがジョインメッセージを受信すると、メッセージの転送にマッピングエントリをチェックします。RP がレジスタメッセージを受信する時、マル チキャストグループにとってルータが正しい RP でない場合、レジスタ停止メッセージが送信されます。

PIM ドメインが埋め込まれた RP を使用する場合、RP は手動で「埋め込み RP 範囲」の RP として設定されます。他のルータが IPv6 グループアドレ スからの RP アドレスを発見します。それらのルータがスタティック RP を埋め込み RP の代わりとして選択する場合、指定の埋め込み RP グループ 範囲はスタティック RP のアクセスリスト内で設定されます。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM for IPv6 RP Address の順にメニューをクリックして以下の画面を表示します。

PIM for IPv6 RP Address	
RP Address Settings	
RP Address Group Access List Name	All Groups Override Show List
RP Address Table	
Total Entries: 1	
RP Address	Group Access List
2015::1	FF00::/8
	1/1 K < 1 > > Go

図 9-125 PIM for IPv6 RP Address 画面

#### 以下の項目を使用します。

項目	説明
RP Address	RP IPv6 アドレスを入力します。
Group Access List Name	使用する通常の IPv6 アクセスリストを指定します。「Show List」をクリックするとスイッチに既存作成されている ACL リストを検出、選択することができます。「All Groups」を指定すると「RP」を全マルチキャストグループにマッ プします。
Override	自動的に学習した RP をスタティック RP が上書きします。

「Add」をクリックし、入力した情報に基づくエントリを追加します。

### エントリの登録

「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

# エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

「Show List」をクリックすると、以下の画面が表示されます。

ACL Type IP ACL			Find Show All
Total Entricou 4			
Total Entries: 1			
	ACL Name		Туре
۲	ACL		Standard IP ACL
			1/1  < < 1 > >  Go
ACL Rule			
Action		Rule	
Permit any any			
			Apply

図 9-126 Show List 画面

#### 画面に表示される項目:

項目	説明
ACL Type	テーブル内の既存の表示する ACL タイプを指定します。 「IP ACL」「Expert IP ACL」「IPv6 ACL」「Expert IPv6 ACL」「MAC ACL」「Expert ACL」から選択します。
ACL List	使用するアクセスリストを指定します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Show All」をクリックして、すべてのエントリを表示します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Apply」をクリックし、設定内容を適用します。

# ■ PIM for IPv6 RP Candidate(PIM for IPv6 RP Candidate 設定)

スイッチの IPv6 PIM RP(Rendezvous Point)candidate に関連する項目を設定します。各インタフェースに一つずつのアクセスリストのみ指定可能 です。最新の設定を行うと古い設定は上書きされます。異なるインタフェースに対してそれぞれ設定することが可能です。「PIM-SM」の動作にのみ 影響を与えます。これによりルータは BSR に candidate RP として「PIMv2」メッセージを送信するようになります。

### L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv6 > PIM for IPv6 RP Candidate の順にメニューをクリックして以下の画面を表示します。

PIM for IPv6 RP Candidate				
RP Candidate Settings				
Interface Name				
Group Access List Name	All Groups			Show List
Priority(0-255)	Default			
Interval(1-16383)	sec 🗌 Default			
				Add
RP Candidate Table				
I otal Entries: 1				
Interface Name	Group Access List	Interval	Priority	
vlan1	FF00::/8	60	192	Edit Delete
			1/1	< < 1 > >  Go

図 9-127 PIM for IPv6 RP Candidate 画面

画面に表示される項目:

項目	説明
Interface Name	Candidate RP として機能するインタフェースを入力します。
Group Access List Name	使用する通常のアクセスリストを指定します。「Show List」をクリックするとスイッチに既存作成されている ACL リス
	トを検出、選択することができます。「All Groups」を指定すると「RP」を全マルチキャストグループにマップします。
Priority (0-255)	選出処理に使用される RP 優先度値を入力します。「Default」を指定すると初期値(192)を使用します。
Interval (1-16383)	Candidate RP 通知間隔(秒)を入力します。「Default」を指定すると初期値(60)を使用します。

「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

「Edit」をクリックして、指定エントリの編集を行います。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

# エントリの削除

削除するエントリの「Delete」ボタンをクリックします。

「Show List」をクリックすると、以下の画面が表示されます。

Access Control Li	st		
ACL Type	IP ACL		Find Show All
Total Entries: 1			
	ACL Name		Туре
۲	ACL		Standard IP ACL
			1/1  < < 1 > >  Go
ACL Rule			
Action		Rule	
Permit	any any		
			Apply

# 図 9-128 Show List 画面

画面に表示される項目:

項目	説明
ACL Type	テーブル内の既存の表示する ACL タイプを指定します。
	「IP ACL」「Expert IP ACL」「IPv6 ACL」「Expert IPv6 ACL」「MAC ACL」「Expert ACL」から選択します。
ACL List	使用するアクセスリストを指定します。
「Find」をクリックして、入力	

「Show All」をクリックして、すべてのエントリを表示します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Apply」をクリックし、設定内容を適用します。

「Edit」をクリックすると、以下の画面が表示されます。

PIM for IPv6 RP Candidate				
RP Candidate Settings				
Interface Name				
Group Access List Name	All Groups			Show List
Priority(0-255)	Default			
Interval(1-16383)	sec 🗌 Default			
				Add
RP Candidate Table				
Total Entries: 1				
Interface Name	Group Access List	Interval	Priority	
vlan1	FF00::/8	60	192	Apply Delete
			1/1	< < 1 > >  Go

図 9-129 PIM for IPv6 RP Candidate (Edit) 画面

画面に表示される項目:

項目	説明
Interval	「RP candidate」通知間隔値(1-16383 秒)を指定します。
Priority	RP 優先値(0-255)を指定します。

「Apply」をクリックし、設定内容を適用します。

# ■ PIM for IPv6 RP Embedded Settings (PIM for IPv6 RP 埋め込み設定)

本項目では、IPv6 PIM embedded の設定と、表示を行います。「Embedded RP」は IPv6 マルチキャストグループアドレスにエンコードされた RP のアドレスを定義するアドレス割当ポリシーです。これによりイントラドメインマルチキャスト同様に、スケーラブルなインタードメインマルチキャストの配置を簡略化します。RP 情報とともに埋め込まれた IPv6 マルチキャストグループアドレスは RP 埋め込みを意味するフラッグ値「7」の「ff70::/12」から開始します。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv6 > PIM for IPv6 RP Embedded Settings の順にメニューをクリックして以下の画面を 表示します。

bled	Apply
sa	sabled

図 9-130 PIM for IPv6 RP Embedded Settings 画面

### 画面に表示される項目:

項目	説明
Embedded	RP 埋め込みを「Enabled」(有効)/「Disabled」(無効)に指定します。
「Apply」をクリックし、言	設定内容を適用します。

# ■ PIM for IPv6 RP Table (PIM for IPv6 RP テーブル)

本項目では、IPv6 PIM RP 情報を表示します。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv6 > PIM for IPv6 RP Table の順にメニューをクリックして以下の画面を表示します。

PIM for IPv6 RP Table			
RP Mapping Table			
Group Address/Prefix Length	FF00::/8		
<ul> <li>Source</li> </ul>	Bootstrap 🗸		
		Γ	Find Show All
Total Entries: 1			
Group(s)		RP Address	Info Source
FF00::/8		2015::1	static
		1/1	< < 1 > >  Go

図 9-131 PIM for IPv6 RP Table 画面

―
---

項目	説明
Group Address/Prefix Length	マルチキャストグループ IPv6 アドレスとプレフィクス長を指定します。
Source	<ul> <li>ソースを指定します。「Bootstrap」「Embedded RP」「Static」から指定します。</li> <li>Bootstrap - BSR を通じて学習した範囲を表示します。</li> <li>Embedded RP - 埋め込み RP を通じて学習したグループ範囲を表示します。</li> <li>Static - 手動設定でして指定した範囲を表示します。</li> </ul>

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Show All」をクリックして、すべてのエントリを表示します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。
### ■ PIM for IPv6 Register Settings (PIM for IPv6 レジスタ設定)

本画面では IPv6 PIM レジスタの設定、表示を行います。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM for IPv6 Register Settings の順にメニューをクリックして以下の画面を表示します。

PIM for IPv6 Register Settings			
Register Checksum Wholepkt			
Register Checksum Wholepkt	O Enabled	Disabled	Apply
Register Probe Time			
Register Probe(1-127)	5	sec 🗌 Default	Apply
Register Suppression Time			
Register Suppression(3-65535)	60	sec 🗌 Default	Apply

図 9-132 PIM for IPv6 Register Settings 画面

### 画面に表示される項目:

項目	説明				
	Register Checksum Wholepkt				
Register Checksum Wholepkt	全パケットのレジスタチェックサムを「Enabled」(有効)/「Disabled」(無効)に指定します。有効にすると、ルー タはデータポーションを含めた全 PIM メッセージのレジスタメッセージのチェックサムを計算します。初期値はレ ジスタチェックサム方法は PIM RFC コンプライアントでレジスタメッセージ内のデータポーションは除かれます。				
Register Probe Time					
Register Probe	Register-Stop メッセージの再送を起こすように DR が Null-Register を RP に送信する場合に Register-Stop Timer (RST) が期限切れになるまでの時間(1-127 秒)を入力します。「Default」を選択すると初期値(5 秒)を指定します。				
	Register Suppression Time				
Register Suppression	レジスタ抑止タイムアウト値(3-65535)を入力します。DR がレジスタ停止メッセージを受領すると、抑止タイマ が指導します。抑止の間、DR は RP へのレジスタメッセージを停止します。最初のホップルータで本機能を使用し ます。レジスタプローブタイムはレジスタ停止タイマのネガティブ値を防ぐためにも、レジスタ抑止タイムの半分 以下である必要があります。最少タイマ値は「3」です。「Default」を選択すると初期値(60秒)を指定します。				

「Apply」ボタンをクリックして行った変更を適用します。

### ■ PIM for IPv6 SPT Threshold Settings (PIM for IPv6 SPT しきい値設定)

本画面では PIM for IPv6 SPT しきい値を表示、設定します

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM for IPv6 SPT Threshold Settings の順にメニューをクリックして以下の画面を表示します。

PIM for IPv6 SPT T	hreshold Settings	
SPT Threshold Settings		
SPT Threshold	Infinity Default	Apply

図 9-133 PIM for IPv6 SPT Threshold Settings 画面

### 画面に表示される項目:

項目	説明
SPT Threshold	SPT しきい値を指定します。 • 0 - 最初のパケットの到着でソースツリーを構築します。 • Infinity - シェアツリーに依存します。 「Default」を選択すると初期値(Infinity)を指定します。

「Apply」をクリックし、設定内容を適用します。

### ■ PIM for IPv6 SSM Settings(PIM for IPv6 SSM 設定)

本画面では IPv6 PIM SSM の設定、表示を行います。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM for IPv6 SSM Settingsの順にメニューをクリックして以下の画面を表示します。

SSM Settings		
Multicast Group Address Name		Show List
	Add	Delete

#### 画面に表示される項目:

項目	説明
Multicast Group Address	ユーザ指定 SSM グループアドレスを定義する通常の IP アクセスリストを指定します。グループアドレスはルールエ
Name	ントリの宛先 IP アドレス項目で定義されます。「Show List」から既存のアクセスリストを指定することも可能です。
	「Default SSM Group」 オプションを指定すると、初期値の SSM グループアドレス(FF3x::/32)を指定します。

### エントリの登録

「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

### エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

「Show List」をクリックすると、以下の画面が表示されます。

Access Control L	ist		
ACL Type	IP ACL		Find Show All
Total Entries: 1			
	ACL Name		Туре
۲	ACL		Standard IP ACL
			1/1  < < 1 > >  Go
ACL Rule			
Action		Rule	
Permit	any any		
			Apply

図 9-135 Show List 画面

#### 画面に表示される項目:

項目	説明
ACL Type	テーブル内の既存の表示する ACL タイプを指定します。
	「IP ACL」「Expert IP ACL」「IPv6 ACL」「Expert IPv6 ACL」「MAC ACL」「Expert ACL」から選択します。
ACL List	使用するアクセスリストを指定します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Show All」をクリックして、すべてのエントリを表示します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Apply」をクリックし、設定内容を適用します。

### ■ PIM for IPv6 (S,G) Keepalive Time (PIM for IPv6 (S,G) キープアライブ時間)

本項目では「IPv6 PIM (S,G)」キープアライブ時間の設定、表示を行います。明示的な (S, G) ローカルメンバシップや (S, G) ジョインメッセージの受 信がない間、PIM ルータが (S, G) ステートを維持するキープアライブタイマを指定します。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM for IPv6 (S,G) Keepalive Time の順にメニューをクリックして以下の画面を表示します。

(S,G) Keepalive Time	
	_
(S,G) Keepalive Time (120-65535) 210 Sec Default Apply	

図 9-136 PIM for IPv6 (S,G) Keepalive Time 画面

### 画面に表示される項目:

項目	説明
(S,G) Keepalive Time	有効な値は 120-65535 です。明示的な (S, G) ローカルメンバシップや (S, G) Join メッセージの受信がない間、PIM ルー タが (S, G) ステートを維持する (S,G) キープアライブタイマを指定します。「Default」を選択すると初期値(120 秒) を指定します。

「Apply」をクリックし、設定内容を適用します。

### ■ PIM for IPv6 Mroute Table (PIM for IPv6 マルチキャストルーティングテーブル)

IPv6 マルチキャストルーティングテーブルの全エントリを表示します。スイッチスターグループ (\*,G) エントリからソースグループ (S,G) エントリ を作成することにより、マルチキャストルーティングテーブルを設定します。スター (\*) は全ソースアドレスを意味し、"S" は単一ソースアドレス、 "G" は宛先マルチキャストグループアドレスを意味します。(S,G) エントリの作成には、ソフトウェア は「Reverse Path Forwarding」(RPF) を通じてユ ニキャストルーティングテーブル内の宛先グループへの最良のパスを使用します。

### L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM for IPv6 Mroute Table の順にメニューをクリックして以下の画面を表示します。

tal Entries: 159								
Source Address	Group Address	RPT	Uptime	Flags	RP Address	RPF Neighbor Address	Join/Prune State	
×	FF5E:5:1::1	-	00Day 02:33:09	S	3004::109		Joined	Show De
3101::1	FF5E:5:1::1	-	00Day 02:33:22	ST	-	FE80::200:FF:FE26:6667	Joined	Show De
3101::1	FF5E:5:1::1	rpt	00Day 02:33:22	S	3004::109		Pruned	Show De
*	FF5E:5:1::2	-	00Day 02:33:09	S	3004::109		Joined	Show De
3101::1	FF5E:5:1::2	-	00Day 02:33:21	ST	-	FE80::200:FF:FE26:6667	Joined	Show De
3101::1	FF5E:5:1::2	rpt	00Day 02:33:21	S	3004::109		Pruned	Show De
*	FF5E:5:1::3	-	00Day 02:33:09	S	3004::109	::	Joined	Show De
3101::1	FF5E:5:1::3	-	00Day 02:33:21	ST	-	FE80::200:FF:FE26:6667	Joined	Show De
3101::1	FF5E:5:1::3	rpt	00Day 02:33:21	S	3004::109		Pruned	Show De
×	FF5E:5:1::4	-	00Day 02:33:09	S	3004::109		Joined	Show De
						1/16 < 1	2 3 >	>

図 9-137 PIM for IPv6 Mroute Table 画面

「Show Detail」をクリックすると次の画面が表示されます。

PIM for IPv6 Mroute	Detail Table			_	_	_	_	_
Mroute Information								
Source Address	*							
Group Address	FF5E:5:1::	1						
RPT	-							
Uptime	00Day 02:	33:55						
Flags	S							
RP Address	3004::109							
RPF Neighbor Address								
Note: Flags: S - Sparse,	T - SPT-bit set, s - SS	SM Group						
Mroute Upstream Interfac	e							
Upstream Interface	-							
Join/Prune State	Joined							
Join Timer	0 sec							
Keepalive Timer	-							
Override Timer	-							
Mroute Downstream Inter	face List							
Total Entries: 3								
Deversite and later face			Deves Desides Times (see)			A	A distantion	Desferrers
Downstream Interface	Join/Prune State	Expiry Timer (sec)	Prune Pending Timer (sec)	Assert State	Assert Timer (sec)	Assert Winner	Metric	Preterence
vlan3	Join	195	-	No Info	-		0	0
vlan4	Join	157	-	No Info	-		0	0
vlan108	No Info	-	-	No Info	-	::	0	0
					[	1/1  < < 1	> >	Go

図 9-138 PIM for IPv6 Mroute DetailTable (Show Detail) 画面

「Back」をクリックすると前のページに戻ります。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

### ■ PIM for IPv6 Neighbor Table (IPv6 PIM Neighbor テーブル)

現在の IPv6 PIM Neighbor ルータテーブルを表示します。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv6 > PIM for IPv6 Neighbor Table の順にメニューをクリックして以下の画面を表示します。

Interface Name	12 char		OMode Searce M	ada X			Sind	Chaus All
Jinteriace Name	12 citata	,	O mode Sparse Mi	ode			Find	Show All
eighbor Information Table	,							
ignoor mornadon rabi								
Total Entries: 1								
Neighbor Addres	s	Interface Name	Uptime	Expires	Version	DR Priority	Mode	
	7:72B	vlan2017	00Day 00:22:10	00Day 00:01:35	v2	N	RG	Show Deta
FE80::200:20FF:FE1								

図 9-139 PIM for IPv6 Neighbor Table 画面

क क	- ± =	++	て石口	٠
回回(	に衣小	C1L	る項目	•

項目	説明
Interface Name	現在の IPv6 PIM Neighbor ルーティングテーブルを表示する IP インタフェース名を指定します。
Mode	フィルタ検索における IPv6 PIM エントリの操作モードを「Sparse Mode」「Dense Mode」から指定します。
「Find」ボタンをクリック	して、入力したインタフェースを検出します。

「Show All」ボタンをクリックして、本スイッチに定義済みの全インタフェースを表示します。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

「Show Detail」をクリックして、指定エントリの詳細について表示します。

「Show Detail」をクリックすると、以下の画面が表示されます。

nterface Name	vlan2	
Neighbor Address	FE80::233:38FF:FE10:1700	
Jptime	01Day 00:40:25	
Expires	00Day 00:01:22	
DR Priority	1	
Seneration ID	0x32c7	
Bidirectional Capable	Not support	
Propagation Delay	1000 millisecond	
Override Interval	3000 millisecond	
		Back

「Back」をクリックすると前のページに戻ります。

### MSDP (MSDP 設定)

#### L3 Features > IP Multicast Routing Protocol > PIM > MSDP

### ■ MSDP Global Settings(MSDP グローバル設定)

Multicast Source Discovery Protocol (MSDP)の表示、グローバル設定を行います。

L3 Features > IP Multicast Routing Protocol > PIM > MSDP > MSDP Global Settings の順にメニューをクリックして以下の画面を表示します。

MSDP Global Settings		
MSDP Global Settings		
Global State	OEnabled ODisabled	
Connect Retry Interval (1-65535)	30 sec 🗌 Default	
SA Cache Expiry Time (65-65535)	145 sec 🗌 Default	
SA Originating Filter	32 chars Configured Apply	

図 9-141 MSDP Global Settings 画面

### 以下の項目を使用します。

項目	説明
Global State	MSDP をグローバルに「Enabled」(有効)/「Disabled」(無効)に指定します。
Connect Retry Interval	接続再試行間隔(1-65535 秒)を指定します。MSDP ピアがピアリングセッションがリセットされ再接続を試みるまでの 時間間隔を指定します。間隔を大きく開けると接続までに時間を要するようになります。「1-60 秒」以内での設定を推奨 します。「Default」を選択すると初期値(30)を指定します。
SA Cache Expiry Time	「Source-Active」(SA) キャッシュの期限値 (65-65535 秒) を設定します。SA キャッシュエントリの期限設定に使用します。 SA の間隔は元々 60 秒で修正はできません。したがって、SA キャッシュ期限により、ネットワーク上の想定されるパケッ トロスに対して非明示的に調整を行います。「Default」を選択すると初期値を指定します。
SA Originating Filter	「Configured」を指定し、SA オリジナルフィルタの文字列を指定します。文字列は 32 字以内で指定します。RP によって MSDP の実行が設定されていて、該当の RP をレジスタする全ローカルソースへの SA メッセージを作成します。リスト のフィルタ設定により、RP は、通常 IP アクセスリストでマッチする指定グループに送信する、ローカルソースへの SA メッ セージを開始します。「Configured」オプションを選択しフィルタ文字列を指定しないことにより、全ローカルソースの オリジナル SA メッセージからの RP は防ぐことができます。

「Apply」をクリックし、設定内容を適用します。

### ■ MSDP Peer Settings (MSDP ピア設定)

Multicast Source Discovery Protocol (MSDP)の表示、ピア設定を行います。

L3 Features > IP Multicast Routing Protocol > PIM > MSDP > MSDP Peer Settings の順にメニューをクリックして以下の画面を表示します。

MSDP Peer Settings	_						_
MSDP Peer Settings							
IP MSDP Peer		Connect	Interface	12 chars			Apply
IP MSDP Peer				Find	Clear All	Clear Statistics Clear /	All Statistics
Configured		Shu	ıtdown	Down	Connect	Listen	Up
1			0	1	0	0	0
Total Entries: 1							
Peer's Address	State	SA Count	Up/Down Tim	e			
10.10.10.10	Down	0	-		Edit Show Deta	ail Delete	

図 9-142 MSDP Peer Settings 画面

画面に表示される項目:

項目	説明
IP MSDP Peer	MSDP ピア IP アドレスを指定します。
Connect Interface	接続インタフェース(12 字以内)を指定します。ソース IP アドレスに TCP 接続を使用するローカルインタフェースを指
	定します。
 「Apply」をクリックし、言	<b>没定内容を適用します。</b>

「Apply」をクリックし、改足内谷を適用しより。

「Delete」をクリックすると指定のエントリを削除します。

「Clear」をクリックすると入力したエントリをクリアします。

「Clear All」をクリックすると入力したエントリを全てクリアします。 「Clear Statistics」をクリックすると入力したエントリの統計情報をクリアします。

「Clear All Statistics」をクリックすると入力したエントリの統計情報を全てクリアします。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Show Detail」をクリックして、指定エントリの詳細について表示します。

「Edit」をクリックして、指定エントリの編集を行います。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Edit」をクリックすると、以下の画面が表示されます。

ISDP Peer	10.10.10.10	
Description	80 chars	
Shutdown	Disabled	
assword		
(eep-Alive (1-21845)	60 sec 🗌 Infinity 🗌 Default	
lold Time (3-65535)	75 sec 🗌 Infinity 🗌 Default	
SA Filter In	32 chars Configured	
SA Filter Out	32 chars Configured	
SA Filter Request	32 chars Configured	
Vinimum TTL (0-255)	0 Default	
SA Cache Maximum (0-8192)	▼ None	Back Apply

図 9-143 MSDP Peer Detail Settings 画面

以下の項目を使用します。

項目	説明
Description	MSDP ピアの概要(80 字以内)を指定します。
Shutdown	シャットダウンを「Enabled」(有効)/「Disabled」(無効)に指定します。シャットダウンは既存の MSDP ピアで必ず 設定する必要があります。MSDP ピアがシャットダウン状態にある場合、ピア間の TCP 接続は構築されません。MSDP ピアはシャットダウン状態でなくなる場合、ピア間の TCP 接続は再構築を試みます。
Password	ピア間のTCP接続用MD5パスワードを指定します。MD5認証はMSDPピアで同じパスワードを設定する必要があります。
Keep-Alive	キープアライブ値(1-21845 秒)を指定します。キープアライブ間隔はリモートサイドの MSDP TCP 接続で設定のホール ド時間よりも短い必要があります。そうしないと MSDP キープアライブメッセージを受信前にリモートサイドの MSDP TCP 接続は切断されてしまいます。「Infinity」を指定すると MSDP ピアはキープアライブメッセージを送信しません。 「Default」を選択すると初期値(60)を指定します。
Hold Time	ホールド時間(3-65535 秒)を指定します。ホールド時間間隔はリモートサイドの MSDP TCP 接続で設定のキープアライ ブ間隔よりも長い必要があります。そうしないと MSDP キープアライブメッセージを受信前にリモートサイドの MSDP TCP 接続は切断されてしまいます。「Infinity」を指定すると MSDP ピアは切断されません。「Default」を選択すると初期 値を指定します。
SA Filter In	「Configured」を指定して、「SA filter-in」文字列(32 字以内)を指定します。ルータは指定ピアからの全 SA メッセージ を受信します。本項目を指定しないと、ルータは指定ピアからの全 SA メッセージを無視します。設定することにより、ルー タはスタンダード IP アクセスリストで定義され、マッチした指定ピア (S, G) からの SA メッセージのみを受信します。
SA Filter Out	「Configured」を指定して、「SA filter-out」文字列(32 字以内)を指定します。ルータは全 SA メッセージを MSDP ピア に転送します。本項目を指定しないと、ルータは指定ピアへの全 SA メッセージ転送を無視します。設定することにより、 ルータはスタンダード IP アクセスリストで定義され、マッチした指定ピア (S, G) への SA メッセージのみを転送します。
SA Filter Request	「Configured」を指定して、「SA filter Request」文字列(32 字以内)を指定します。ルータは指定ピアからの全 SA リク エストメッセージを処理します。本項目を指定しないと、ルータは指定ピアからの全 SA リクエストメッセージを無視し ます。設定することにより、ルータはスタンダード IP アクセスリストで定義され、マッチした指定ピア (S, G) からの SA リクエストメッセージのみを処理します。
Minimum TTL	最小 TTL 値 (0-225)を指定します。SA メッセージが MSDP ピアから送信された時、SA メッセージ内のマルチキャストデー タパケットの「Time-To-Live」(TTL) 値が減少し、減少した TTL 値が SA メッセージが送信された MSDP ピアで設定の最小 TTL 値よりも小さい場合、SA は送信されません。「Default」を選択すると初期値(0)を指定します。
SA Cache Maximum	最大 SA キャッシュ値(0-8192)を指定します。SA キャッシュの最大値が0に設定されると、スイッチはピアからの SA キャッシュエントリを学習しません。SA キャッシュの最大値が既存の SA キャッシュエントリよりも小さい場合、古い 既存の SA キャッシュエントリは最大 SA キャッシュ値と SA キャッシュエントリ数が同じになるまで、削除されます。 「None」を指定すると SA キャッシュエントリの制限がなくなります。

「Apply」をクリックし、設定内容を適用します。

「Back」をクリックすると前のページに戻ります。

「Show Detail」をクリックすると、以下の画面が表示されます。

MSDP Peer Detail	
MSDP Peer	10.10.10
Description	
Mesh Group	
Static RPF	Not configured
State	Down
Password	
Up/Down Time	-
Connection Interface	vlan1 (10.90.90.90)
Keep-Alive/Hold-Time Interval	60/75
Remote/Local Port	0/0
The Total Number of Times This Peer Transfer into Up State	0
Incoming Filter	Not configured
Outgoing Filter	Not configured
Request Filter	Not configured
Minimum TTL for Data-Encapsulated SA Message	0
The Number of SAs Learned from This Peer	0
The Maximum Number of SAs Can Be Learned from This Peer	none
Count of RPF Check Failure	0
Incoming/Outgoing Control Messages	0/0
Incoming/Outgoing SA Messages	0/0
Incoming/Outgoing SA Requests	0/0
Incoming/Outgoing SA Responses	0/0
Incoming/Outgoing Data Packets	0/0

図 9-144 MSDP Peer Detail 画面

「Back」をクリックすると前のページに戻ります。

### ■ MSDP SA Cache (MSDP SA キャッシュ)

Multicast Source Discovery Protocol (MSDP)SA のキャッシュ設定を行います。

L3 Features > IP Multicast Routing Protocol > PIM > MSDP > MSDP SA Cache の順にメニューをクリックして以下の画面を表示します。

MSDP SA Cache				
MSDP SA Cache				
Group	Source	RP Address		Find Clear
Total Entries: 0				
Group Address	Source Address	RP Address	Learned Peer	Up/Expire Time

図 9-145 MSDP SA Cache 画面

画面に表示される項目:

項目	説明
Group	グループアドレスを指定します。
Source	ソースアドレスを指定します。
RP Address	RP アドレスを指定します。

「Clear」をクリックすると入力したエントリをクリアします。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

### ■ MSDP Static RPF Settings(MSDP スタティック RPF 設定)

本項目では、MSDP スタティック RPF 設定を行います。スタティック RPF ピアを設定する前に、MSDP ピアを追加する必要があります。RP プリフィ クスリストが設定されると、ピアはプリフィクスリストの RP のみのスタティック RPF になります。複数のスタティック RPF ピアが RP プリフィク スリスト抜きで設定されると、一番小さい接続ピアのみが有効なスタティック RPF ピアになります。MSDP ピアがスタティック RPF ピアに複数回設 定されていると、最新の設定が有効になります。MSDP ピアが一つしかない場合、該当の MSDP ピアはスタティック RPF ピアとなります。

L3 Features > IP Multicast Routing Protocol > PIM > MSDP > MSDP Static RPF Settings の順にメニューをクリックして以下の画面を表示します。

MSDP Static RPF Settings				_
MSDP Static RPF Settings				
Peer Address	RP List	32 chars		Apply
Peer Address				Find
Total Entries: 0				
	Peer's Address		RP List	

図 9-146 MSDP Static RPF Settings 画面

以下の項目を使用します。

項目	説明
Peer Address	MSDP ピアアドレスを指定します。
RP List	RP プリフィクスリストを定義するスタンダード IP リスト(32 字以内)を指定します。
RP Address	RP アドレスを指定します。

「Apply」をクリックし、設定内容を適用します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

### ■ MSDP Mesh Group Settings (MSDP メッシュグループ設定)

本項目では、MSDP メッシュグループの設定を行います。MSDP ピアを追加するメッシュグループに追加する前に、MSDP ピアを追加する必要があります。MSDP ピアが複数のメッシュグループに追加されている場合、最新の設定内容が有効になります。

L3 Features > IP Multicast Routing Protocol > PIM > MSDP > MSDP Mesh Group Settings の順にメニューをクリックして以下の画面を表示します。

MSDP Mesh Group Settings		
MSDP Mesh Group Settings		
Peer Address	Mesh Name 64 chars	Apply
Peer Address		Find
Total Entries: 1		
Peer's Address	Group Name	
10.10.10	mesh	Delete
		1/1 K < 1 > > Go

図 9-147 MSDP Mesh Group Settings 画面

以下の項目を使用します。

項目	説明
Peer Address	MSDP ピアアドレスを指定します。
Mesh Name	メッシュグループ名(64 字以内)を指定します。

「Apply」をクリックし、設定内容を適用します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Delete」をクリックすると指定のエントリを削除します。

# IPMC(IP マルチキャスト設定)

### L3 Features > IP Multicast Routing Protocol > IPMC

### IP Multicast Global Settings(IP マルチキャストグローバル設定)

IP Multicast Global Settings (IP マルチキャストグローバル設定)の表示、グローバル設定を行います。

L3 Features > IP Multicast Routing Protocol > IPMC > IP Multicast Global Settings の順にメニューをクリックして以下の画面を表示します。

IP Multicast Global Setting	js	_		_	_	_
IP Multicast Routing Global State						
Global State	O Enabled	Disabled				Apply
IP Multicast Table Lookup Mode -						
Table Lookup Mode	• IP	O MAC				Apply
IP Multicast boundary						
VID	ACL Name		Filter Mode	Action		
1-4094	32 chars	Please Select	Both	Add	~	Apply
IP Multicast Interface Table						
Interface Name	vlan1				Find	Show All
Total Entries: 1						
Interface Name	Interfac	e Address	Multicast Routing		Multicast Bou	indary
vlan1	10.90	90.90/8	disabled		not set	
					1/1 < < 1	> >  Go

図 9-148 IP Multicast Global Settings 画面

画面に表示される項目:

項目	説明
	IP Multicast Routing Global State
Global State	IP マルチキャストルーティングを「Enabled」(有効)/「Disabled」(無効)に指定します。IP マルチキャストルーティ ングが無効の場合、マルチキャストルーティングプロトコルが有効でも、システムはルーティングマルチキャストパケッ トを停止します。
	IP Multicast Table Lookup Mode
Table Lookup Mode	IP マルチキャストフォワーディングルックアップモードを指定します。 ・ IP - マルチキャストフォワーディングルックアップを IP アドレス基準で行います。 ・ MAC - マルチキャストフォワーディングルックアップを MAC アドレス基準で行います。
	IP Multicast Boundary
VID	VLAN ID(1-4094)を指定します。
ACL Name	指定する IP アクセスリスト名(32 字以内)を指定します。 「Please Select」を指定すると既存のアクセスリストを選択することも可能です。
Filter Mode	<ul> <li>フィルタモードを指定します。</li> <li>Both - インカミング / アウトゴーイングどちらのトラフィックもフィルタします。</li> <li>Out - インタフェースに到着する PIM ジョインメッセージ、または IGMP ジョインメッセージをフィルタします。このフィルタリングにより、インタフェースが拒否エントリ (G) (5,G) の外向きインタフェースになることを防止します。</li> <li>In - インタフェースに到着するマルチキャストユーザトラフィックを指定のアクセスリストに基づきフィルタします。このフィルタリングにより、指定ソースからの指定グループや指定グループのマルチキャストトラフィックなどをフィルタします。</li> </ul>
Action	動作を「Add」「Delete」から指定します。
	IP Multicast Interface Table
Interface Name	表示するインタフェース名を指定します。

「Apply」をクリックし、設定内容を適用します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Show All」をクリックして、すべてのエントリを表示します。

「Please Select」をクリックすると、次の画面を表示します。

al Entries:	1		
	ID	ACL Name	ACL Type
0	1	SI-ACL	Standard IP ACL
			1/1 < 1 > > 6
			OK

図 9-149 ACL Access List 画面

設定するエントリを選択し「OK」をクリックします。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

### IP Multicast Route Settings(IP マルチキャストルート設定)

IP Multicast Route Settings (IP マルチキャストルート設定)の表示、設定を行います。

### L3 Features > IP Multicast Routing Protocol > IPMC > IP Multicast Route Settings の順にメニューをクリックして以下の画面を表示します。

IP Multicast Route Set	tings			_	_	
Static Multicast Route Setting	gs					
Source Address	· · ·	Mask				
RPF Address	· · · . DNULL					Apply
IP Multicast Route Table						
Summary						
Static						
Multicast Protocol	PIM-DM					
Group Address	· · · · · · · ·	Source Address	· · · ·		Find	Show All
Total Entries: 0						
Source Address	Group Address	Incomi	ng Interface	Uptime	Expires	Protocol

図 9-150 IP Multicast Route Settings 画面

画面に表示される項目:

項目	説明		
	Static Multicast Route Settings		
Source Address	マルチキャストソースとなるネットワークアドレスを指定します。		
Mask	マルチキャストソースとなるサブネットマスクを指定します。		
RPF Address	RPF ネイバ IP アドレスを入力します。「NULL」オプションを選択すると、ソースネットワークから送信されたマルチキャス		
	トトラフィックの RPF チェックは必ず失敗します。		
	IP Multicast Route Table		
Summary	IP マルチキャストルーティングテーブルのサマリについて表示します。		
Static	マルチキャストスタティックルートを表示します。		
Multicast Protocol	表示するマルチキャストプロトコルを選択します。「PIM-DM」「PIM-SM」「DVMRP」から選択可能です。		
Group Address	マルチキャストグループ IP アドレスを指定します。		
Source Address	マルチキャストソース IP アドレスを指定します。		

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。 「Show All」をクリックして、すべてのエントリを表示します。

### IP Multicast RPF Table (IP マルチキャスト RPF テーブル)

IP Multicast RPF Table (IP マルチキャスト RPF テーブル)の表示、設定を行います。

L3 Features > IP Multicast Routing Protocol > IPMC > IP Multicast RPF Table の順にメニューをクリックして以下の画面を表示します。

P Multicast RPF Table				
IP Address Find				
Total Entries: 1				
Source Address	RPF Neighbor	RPF Interface	RPF Type	Metric
10.90.90.1	-	NULL	static	-

図 9-151 IP Multicast RPF Table 画面

#### 画面に表示される項目:

項目	説明
IP Address	ユニキャスト IPv4 アドレスを指定します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

### IP Multicast Forwarding Cache (IP マルチキャストフォワーディングキャッシュ)

IP Multicast Forwarding Cache (IP マルチキャストフォワーディングキャッシュ)の表示、設定を行います。

L3 Features > IP Multicast Routing Protocol > IPMC > IP Multicast Forwarding Cache の順にメニューをクリックして以下の画面を表示します。

IP Multicast Forwarding Ca	P Multicast Forwarding Cache						
IP Multicast Forwarding Table							
Group Address Source Address Find Show All							
Total Entries: 0							
Source Address	Group Address	Incoming Interface	Outgoing Interface				

図 9-152 IP Multicast Forwarding Cache 画面

画面に表示される項目:

項目	説明
Group Address	マルチキャストグループ IP アドレスを指定します。
Source Address	マルチキャストソース IP アドレスを指定します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。 「Show All」をクリックして、すべてのエントリを表示します。

### IP Multicast Protocol Statistics (IP マルチキャストプロトコル統計)

IP Multicast Protocol Statistics (IP マルチキャストプロトコル統計)の表示、設定を行います。

### L3 Features > IP Multicast Routing Protocol > IPMC > IP Multicast Protocol Statistics の順にメニューをクリックして以下の画面を表示します。

IP Multicast	IP Multicast Protocol Statistics											
Clear Multicas	Clear Multicast Protocol Packet Statistics											
Multicast Prot	Multicast Protocol IGMP PIM DVMRP All											
Multicast Prote	Multicast Protocol Packet Statistics Table											
Interface 1	Interface Name IGMP PIM DVMRP Find Show All								Show All			
	IGMP Packets Counter											
	Query v1/v2/v3				Repor	t v1/v2/v3		IGM	P Leave	Unknown IGMP		
Receive	d		0/0/0		0/0/0			0		0		
Sent			0/0/0		0	)/0/0		0			0	
					PIM Pac	kets Count	er					
	Hello	Register	Register-Stop	Join/Prune	Bootstrap	Assert	Graft	Graft-Ack	C-RP-Adv	State Refresh	Unknown PIM	
Received	0	0	0	0	0	0	0	0	0	0	0	
Sent	0	0	0	0	0	0	0	0	0	0	0	
					DVMRP Pa	ackets Cou	nter					
	F	robe	Report	P	rune	Graft	:	Graft	-Ack	Unknow	n DVMRP	
Received		0	0		0	0		0			0	
Sent		0	0		0	0		0	1		0	

図 9-153 IP Multicast Protocol Statistics 画面

### 画面に表示される項目:

項目	説明							
	Clear Multicast Protocol Packet Statistics							
Multicast Protocol	クリアするマルチキャストプロトコルを選択します。「IGMP」「PIM」「DVMRP」「AII」から選択可能です。							
	Multicast Protocol Packet Statistics Table							
Interface Name	本設定に使用するインタフェース名を指定します。							
Multicast Protocol	.ulticast Protocol 表示するマルチキャストプロトコルを選択します。「IGMP」「PIM」「DVMRP」から選択可能です。							

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Show All」をクリックして、すべてのエントリを表示します。

### Control Packet CPU Filtering(IP マルチキャストプロトコル統計 )

IP Multicast Protocol Statistics (IP マルチキャストプロトコル統計)の表示、設定を行います。

L3 Features > IP Multicast Routing Protocol > IPMC > Control Packet CPU Filtering の順にメニューをクリックして以下の画面を表示します。



図 9-154 Control Packet CPU Filtering 画面

画面に表示される項目:

項目	説明
	Control Packet CPU Filtering Settings
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。
Packet Type	<ul> <li>パケットの種類を指定します。</li> <li>DVMRP - CPU に対して送信された「DVMRP L3 コントロールパケット」を破棄します。</li> <li>PIM - CPU に対して送信された「PIM L3 コントロールパケット」を破棄します。</li> <li>IGMP Query - CPU に対して送信された「IGMP Query L3 コントロールパケット」を破棄します。</li> <li>OSPF - CPU に対して送信された「OSPF L3 コントロールパケット」を破棄します。</li> <li>RIP - CPU に対して送信された「RIP L3 コントロールパケット」を破棄します。</li> <li>VRRP - CPU に対して送信された「VRRP L3 コントロールパケット」を破棄します。</li> </ul>
Action	動作を「Add」「Delete」から指定します。
	Control Packet CPU Filtering Table
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Show All」をクリックして、すべてのエントリを表示します。

### IPv6MC(IPv6 マルチキャスト設定)

### L3 Features > IP Multicast Routing Protocol > IPv6MC

### IPv6 Multicast Global Settings (IPv6 マルチキャストグローバル設定)

IPv6 Multicast Global Settings (IPv6 マルチキャストグローバル設定)の表示、グローバル設定を行います。

### L3 Features > IPv6 Multicast Routing Protocol > IPv6MC > IPv6 Multicast Global Settings の順にメニューをクリックして以下の画面を表示します。

IPv6 Multicast Global Settings				
IPv6 Multicast Routing				
IPv6 Multicast Routing Global State	O Enabled	Disabled		Apply
IPv6 Multicast Interface Table				
Interface Name	vlan1			Find Show All
Total Entries: 0				
Interface Nam	ne		Owner Module	

図 9-155 IPv6 Multicast Global Settings 画面

画面に表示される項目:

項目	説明							
	IPv6 Multicast Routing							
IPv6 Multicast Routing Global State	IPv6 マルチキャストルーティングを「Enabled」(有効)/「Disabled」(無効)に指定します。IPv6 マルチキャストルーティングが無効の場合、マルチキャストルーティンプロトコルが有効でも、システムはルーティングマルチキャストパケットを停止します。							
	IPv6 Multicast Interface Table							
Interface Name	本設定に使用するインタフェース VLAN を指定します。							

「Apply」をクリックし、設定内容を適用します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Show All」をクリックして、すべてのエントリを表示します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

#### IPv6 Static Multicast Route Settings(IPv6 スタティックマルチキャストルート設定)

本項目ではIPv6スタティックマルチキャストルート設定を行います。PIM コントロールは自身のルーティングテーブルがなく、ユニキャストルーティ ングテーブルを使用して、ネットワークに届くリバースパスフォワーディングインタフェースを決定します。ネットワークの RPF アドレスを使用す るスタティックマルチキャストルートを設定します。

# L3 Features > IPv6 Multicast Routing Protocol > IPv6MC > IPv6 Static Multicast Route Settings の順にメニューをクリックして以下の画面を表示します。

IPv6 Static Multicast Route S	ettings			
IPv6 Static Multicast Route Settings				
IPv6 Address/Prefix Length Interface VLAN (1-4094) RPF Neighbor Address	2013::1/64 3FE1::1	] ☑ NULL		Apply
Total Entries: 1				Clear All
IPv6 Address/Pr	efix Length	RPF Neighbor Address	Interface Name	
2016:://	54		Null	Delete
			1/1 < 1	> >  Go

図 9-156 IPv6 Static Multicast Route Settings 画面

### 以下の項目を使用します。

項目	説明
IPv6 Address/Prefix	マルチキャストソースの IPv6 ネットワークアドレスとプリフィクス長を指定します。
Length	
Interface VLAN	本設定に使用するインタフェース VLAN(1-4094)を指定します。
RPF Neighbor	RPF ネイバ IPv6 アドレスを入力します。「NULL」オプションを選択すると、ソースネットワークから送信されたマルチキャ
Address	ストトラフィックの RPF チェックは必ず失敗します。

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

「Clear All」をクリックすると入力したエントリを全てクリアします。

### IPv6 Multicast Routing Table(IPv6 マルチキャストルーティングテーブル )

IPv6 Multicast Route Table (IPv6 マルチキャストルートテーブル)の表示、設定を行います。

L3 Features > IPv6 Multicast Routing Protocol > IPv6MC > IPv6 Multicast Routing Table の順にメニューをクリックして以下の画面を表示します。

IPv6 Multicast Routir	ng Table	_	_				
IPv6 Multicast Routing Tab	ole						
Group IPv6 Address     FF5E:3::1       Source IPv6 Address     2000:60:1:1::10       Dense     Sparse       Summary     Find							
Total Entries: 0	Total Entries: 0						
Source Address	Group Address	Uptime/Expires	Flags	Incoming Interface	RPF Neighbor Address	Outgoing Interface List	
Note: Flags: S - Sparse, D - Dense, s - SSM Group							

図 9-157 IPv6 Multicast Routing Table 画面

#### 画面に表示される項目:

項目	説明
Group IPv6 Address	マルチキャストグループ IPv6 アドレスを指定します。
Source IPv6 Address	マルチキャストソース IPv6 アドレスを指定します。 ・ Dense - PIM-DM ルートのみ表示します。 ・ Sparse - PIM-SM ルートのみ表示します。 ・ Summary - IPv6 マルチキャストルーティングテーブルにおける 1 行の要約されたサマリを表示します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Show All」をクリックして、すべてのエントリを表示します。

### IPv6 Multicast Forwarding Cache Table (IPv6 マルチキャストフォワーディングキャッシュテーブル)

IPv6 Multicast Forwarding Cache Table (IPv6 マルチキャストフォワーディングキャッシュテーブル)の表示、設定を行います。 L3 Features > IPv6 Multicast Routing Protocol > IPv6MC > IPv6 Multicast Forwarding Cache Table の順にメニューをクリックして以下の画面を表示 します。

Pv6 Multicast Routing Forwarding Cache Table						
IPv6 Multicast Routing Forwarding Cac	he Table					
Group IPv6 Address Source IPv6 Address	FF5E:3::1 2000:60:1:1::10		Find Show All			
Total Entries: 0						
Source Address	Group Address	Interface Name	Outgoing Interface List			

図 9-158 IPv6 Multicast Forwarding Cache Table 画面

#### 画面に表示される項目:

項目		説明
Group IPv6 Address	マルチキャストグループ IPv6 アドレスを指定します。	
Source IPv6 Address	マルチキャストソース IPv6 アドレスを指定します。	
「Find」をクリックし	て、入力した情報に基づく特定のエントリを検出します。	

「Show All」をクリックして、すべてのエントリを表示します。

### IPv6 RPF Table (IPv6 RPF テーブル)

IPv6 RPF Table (IPv6 RPF テーブル)の表示、設定を行います。

L3 Features > IPv6 Multicast Routing Protocol > IPv6MC > IPv6 RPF Table の順にメニューをクリックして以下の画面を表示します。

IPv6 RPF Table					_
IPv6 RPF Table					
IPv6 Source Address	2013::1	l		F	ind
IPv6 Source Address	RPF Interface	RPF Neighbor Address	RPF Route/Mask	RPF Type	Metric

図 9-159 IPv6 RPF Table 画面

画面に表示される項目:

項目	説明	
IPv6 Source Address	ユニキャストホスト IPv6 アドレスを指定します。	
		_

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

# BGP (Border Gateway Protocol) (EI/MI モードのみ)

### L3 Features > BGP

スイッチは BGP(Border Gateway Protocol)をサポートしています。これは、AS(自律システム)内のネットワーク到達性を指定する IP ネットワー クまたはプレフィックスのテーブルを保持するレイヤ 3 ユニキャストルーティングプロトコルです。BGP はパス、ネットワークポリシー、そして / または、ルールセットに基づいて経路の決定をします。

### BGP Global Settings(BGP グローバル設定)

スイッチに BGP のグローバル設定を行います。

### L3 Features > BGP > BGP Global Settings の順にメニューをクリックして以下の画面を表示します。

BGP Global Settings				
BGP AS Number				
BGP AS Number (1-4294967295)			E	Apply Delete
BGP Parameters				
BGP Global State		Version		
BGP Router Identifier	· · · · ·	Synchronization	Disabled 🗸	
Enforce First AS	Disabled 🗸	Scan Time (5-60)		sec
Keep-Alive Interval (0-65535)	sec	Hold Time (0-65535)		sec
Always Compare MED	Disabled 🗸	Deterministic MED	Disabled 🗸	
Default Local Preference (0-4294967295)		MED Confed	Disabled 🗸	
AS Path Ignore	Disabled 🗸	Compare Router ID	Disabled 🗸	
MED Missing as Worst	Disabled 🗸	Compare Confederation Path	Disabled 🗸	
Fast External Failover	Disabled 🗸	Aggregate Next Hop Check	Disabled 🗸	
Default IPv4 Unicast	Disabled 🗸	Graceful Restart State	Disabled 🗸	
Restart Time (1-3600)		Stalepath Time (1-3600)		
				Apply
BGP Trap Settings				
Peer Established Trap State	Disabled			
Peer Backward-Trans Trap State	Disabled 🔽			Apply

図 9-160 BGP Global Settings 画面

画面に表示される項目:

項目	説明
	BGP AS Number
BGP AS Number	1-4294967295 の範囲の BGP AS 番号を入力します。
(1-4294967295)	
	BGP AS Number
BGP Router Identifier	BGP ルータIDを設定します。BGP ルータを識別するID。Oに設定されると、ルータIDは自動的に決定されます。ネットワー
	ク内で固有のルータ ID を指定する必要があります。
Synchronization	通常、そのルートがローカルであるか、または IGP に存在していない場合、BGP スピーカは外部の Neighbor にルートを
	通知しません。初期値では、BGPとIGP間の同期はオフであり、BGPはIGPからのルート確認を待たないでネットワークルー
	トを通知することができます。本機能により、BGP が他の AS( 目律 ) システムに利用可能にする前に AS 内のルータとア
Fufaura First AC	クセ人サーハはルートを持つことかでさます。   AC リストロの思知の AC レーズ Neichber の AC た中にします。記白たた時にまても、別 奴 Neichber から形にまて声が。
Enforce First AS	AS リスト内の取初の AS として Neignborの AS を実行しより。設定を有効に りると、外部 Neignbor から受信 9 る史新 のうた母信した再新中の AS DATH の早知に Neighbor の自律システム (AS) を持たたい再新け振不されて、 Neighbor は
	のフラ文目した史利内のAS_FAILの取材に Neigilibol の日律ノステム (AS) を持たない史利は拒占されて、 Neigilibol は クローズされます。大機能を右効にすると 許可されていたいシステムからのトラフィックを許可したいてとで BCP ネッ
	「クロースされより。本機能を行効にすると、計引されていないシステムからのドラフィックを計引しないことで、DOF ネテートワークのセキュリティの1つに追加されます。
Scan Time	アークのビーエックイットアル追加されなり。   BGP スキャンタイマ値を 5-60(秒)で設定します。または「Default」をチェックします。初期値は 60(秒)です。
Keepalive Interval	有効な値は 0-65535 です。keepalive メッセージがピアに送信される間隔を指定します。値が 0 に設定されると、
(0-65535)	keepalive メッセージは送信されません。初期値は 60( 秒 ) です。BGP 接続を実装する 2 つのルータが、異なる keepalive
	タイマを持つ場合、より小さい keepalive タイマが使用されます。タイマを特定の Neighbor に指定すると、Neighbor の
	指定タイマが適用されます。
Hold Time (0-65535)	有効な値は 0-65535 です。keepalive メッセージが holdtime を超えて受信されると、システムはピアを Dead として判断
	します。初期値は180(秒)です。holdtimeが0に設定されると、無期限となります。BGP 接続を実装する2つのルータが、
	異なる保持時間を持つ場合、より小さい保持時間が使用されます。タイマを特定の Neighbor に指定すると、Neighbor
	の指定タイマが適用されます。保持時間は、keepalive 時間の少なくとも 3 倍である必要があります。
Always compare MED	異なる AS 内の Neighbor からの受信したバスに対する MED の比較を有効または無効にします。初期値では無効です。
Deterministic MED	同じ AS 内の Neighbor からの受信したバスに対する MED の決定的な比較を有効または無効にします。初期値では、本設定は無効です。
Default Local Preference	0-4294967295 の範囲でデフォルトローカル優先度を指定します。初期値は 100 です。
(0-4294967295)	
Med Confed	選択すると、BGP プロセスは、コンフェデレーションピアから受信するルートの MED を比較します。パスに外部 AS を 持つルートには、比較は行われません。
AS Path Ignore	選択すると、BGP プロセスは経路選定プロセスで AS パスを無視します。
Compare Router ID	選択すると、BGP プロセスは経路選定プロセスでルータ ID を含めます。同様のルートは比較され、最も低いルータ ID
	を持つルートが選択されます。
MED Missing As Worst	選択すると、BGP プロセスは MED 属性が欠けているルートに infinity(無限)の値を割り当てます。無効にすると、BGP
	プロセスは、MED属性が欠けているルートに本ルートがベストパスとして選択されるように0の値を割り当てます。
Compare Confederation	選択すると、BGP プロセスは、受信するルートのコンフェデレーション AS のバス長を比較します。コンフェデレーショ
Path	2  AS  0 / 人長が短いはと、よいルートとなります。
Fast External Fallover	Tast external fallover 機能を有効または無効にします。これは、外部の BGP ビアセッショフを、これらのビアに到産する
	のた使用されているサンフがダウンすると、直ちにサビサドするように border Galeway Flotocol(bGF) ルーナインサフ
Aggregate Next Hop	ロビハを改定します。初州値は行がしす。 aggregate nevt hon check 機能を有効すたけ無効にします。BGP アグリゲートルートのネクストホップチェックを設定
Check	Lます。同じネクストホップ属性を持つルートだけが、BGP アグリゲートネクストホップチェックが有効な場合に集約
	されます。初期値は無効です。
Default IPv4 Unicast	デフォルトでの IPv4 ユニキャスト機能を有効にします。IPv4 ユニキャスト情報の交換に使用します。
Graceful Restart State	BGP ネイバの BGP グレースフルリスタートステートを有効または無効にします。
Restart Time	グレースフルリスタート時間(1-3600 秒)を指定します。ネイバリスタートの最大時間を指定します。
Stalepath Time	「Stalepath」時間(1-3600 秒)を指定します。「stalepath」待ちからネイバリスタートまでの最大時間値を指定します。
	BGP Trap Settings
Peer Established Trap	BGP ピア構築トラップを「Enabled」(有効)/「Disabled」(無効)に指定します。
State	
Peer Backward-Trans	ピアアイドルトラップを「Enabled」(有効)/「Disabled」(無効)に指定します。
Trap State	

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

### BGP Aggregate Address Settings (BGP アグリゲートアドレス設定)

Border Gateway Protocol(BGP) データベースにアグリゲートエントリを作成します。

ルートアグリゲーションはルーティングエントリの減少に使われるメカニズムです。アグリゲートされたルートは、ルーティングテーブルで作成されます。アグリゲートされたルートはローカル AS から送信されます。アグリゲーションフラグはアグリゲートされたエントリから失われる可能性のある指定ルート情報の AS パス情報を示すために設定されます。

L3 Features > BGP > BGP Aggregate Address Settings の順にメニューをクリックして以下の画面を表示します。

BGP Aggregate Address Settings	
BGP Aggregate Address Settings	
Address Family           IPv6 Unicast          Please Select	
Network Address Summary Only AS Set	Apply Find
Total Entries: 1	
Network Address	Options
2016::/64	- Delete
	1/1 < 1 > > Go

図 9-161 BGP Aggregate Address Settings 画面

#### 画面に表示される項目:

項目	説明
Address Family	アドレスファミリーを選択します。
	・ IPv4 Unicast - IPv4 ユニキャストアドレスファミリーを指定します。
	・ IPv4 VRF - VRF インスタンス(12 字以内)を指定します。VRF インスタンス名を入力するか、「Please Select」で
	既存の VRF インスタンスを選択します。
	・ IPv4 Multicast - IPv4 マルチキャストアドレスファミリーを指定します。
	・ IPv6 Unicast - IPv6 ユニキャストアドレスファミリーを指定します。
Network Address	集約される IPv4/IPv6 アドレスとネットマスクを入力します。
Summary Only	チェックして、指定ルートの通知を停止します。初期値はチェックなしです。
AS Set	AS 設定パス情報を生成します。初期値はチェックなしです。

「Apply」ボタンをクリックして変更を適用します。

### エントリの検索

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。 「Show All」ボタンをクリックして、すべての定義済みエントリを表示します。

#### エントリの削除

削除するエントリの「Delete」ボタンをクリックします。「Delete All」ボタンをクリックして、表示されたすべてのエントリを削除します。

「Please Select」をクリックすると、次の画面が表示されます。

VRF List		
Total Entries: 1		
	VRF Name	RD
0	VRF1	192.168.70.1:24
		1/1 K < 1 > > Go
		OK

図 9-162 VRF List 画面

使用する VRF エントリを選択し、「OK」をクリックします。 設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

# BGP Network Settings (BGP ネットワーク設定)

Border Gateway Protocol(BGP) が通知するネットワークを指定します。

L3 Features > BGP > BGP Network Settings の順にメニューをクリックして以下の画面を表示します。

BGP Network Settings BGP Network Settings			
Address Family	Please Select		
Network Address	Route Map Name		Apply Find
Total Entries: 1	iteres	Davida Mara Marra	
2016/	34	Route-Map	Edit Delete
2010		i toute map	

図 9-163 BGP Network Settings 画面

画面に表示される項目:	
-------------	--

項目	説明
Address Family	アドレスファミリーを選択します。
	・ IPv4 Unicast - IPv4 ユニキャストアドレスファミリーを指定します。
	・ IPv4 VRF - VRF インスタンス(12 字以内)を指定します。VRF インスタンス名を入力するか、「Please Select」で既存の
	VRF インスタンスを選択します。
	・ IPv4 Multicast - IPv4 マルチキャストアドレスファミリーを指定します。
	・ IPv6 Unicast - IPv6 ユニキャストアドレスファミリーを指定します。
Network Address	集約される IPv4/IPv6 アドレスとネットマスクを入力します。
Route Map Name	通知されるネットワークに適用するルートマップを指定します。指定しない場合、すべてのネットワークを通知します。

「Apply」をクリックし、設定内容を適用します。

### エントリの検索

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

### エントリの削除

削除するエントリの「Delete」ボタンをクリックします。「Delete All」ボタンをクリックして、表示されたすべてのエントリを削除します。

「Please Select」をクリックすると、次の画面が表示されます。

al Entries: 1		
	VRF Name	RD
0	VRF1	192.168.70.1.24
		1/1 🔀 🖌 🔰

図 9-164 VRF List 画面

使用する VRF エントリを選択し、「OK」をクリックします。

### BGP Route Redistribution Settings (BGP ルート再分配設定)

BGP Route Redistribution Settings(BGP ルート再分配設定)の設定を行います。ルーティングドメインから BGP へのルート再分配に使用します。

L3 Features > BGP > BGP Route Redistribution Settings の順にメニューをクリックして以下の画面を表示します。

BGP Route Redis	tribution Settings	_	_		
BGP Route Redistribut	ion Settings				
Address Family					
IPv6 Unicast		Please Select			
Source Protocol	Destination Protocol	Туре	Metric (0-429496729	5) Route Map Name	
Connected 🗸	BGP 🗸	All [	⊻	16 chars	Apply
Total Entries: 1					
Source Protocol	Destination Protocol	Туре	Metric	Route Map Name	
Connected	BGP	N/A	100	Route-Map	Edit Delete
					1/1 < < 1 > > Go

図 9-165 BGP Route Redistribution Settings 画面

### 画面に表示される項目:

項目	説明
Address Family	アドレスファミリーを選択します。
	・ IPv4 Unicast - IPv4 ユニキャストアドレスファミリーを指定します。
	・ IPv4 VRF - VRF インスタンス(12 字以内)を指定します。VRF インスタンス名を入力するか、「Please Select」で既存の
	VRF インスタンスを選択します。
	・ IPv4 Multicast - IPv4 マルチキャストアドレスファミリーを指定します。
	・ IPv6 Unicast - IPv6 ユニキャストアドレスファミリーを指定します。
Source Protocol	プルダウンメニューを使用して送信元のプロトコルを選択します。
	・ Connected - BGP への接続ルートに再分配します。
	・ Static - BGP へのスタティックルートに再分配します。
	・ RIP - BGP への RIP ルートに再分配します。
	・ OSPF - BGP への OSPF ルートに再分配します。
	・ ISIS - BGP への ISIS ルートに再分配します。
Destination Protocol	送信先のプロトコルは BGP です。
Туре	「Source Protocol」で「OSPF」を選択した場合、これは設定可能となります。
	・ All - OSPF AS-internal と OSPF AS-external の両方のルートを RIP または BGP に再配布します。
	・ Internal - OSPF AS-internal ルートだけに再配布します。
	・ External - Ext Type1 と Ext Type2 ルートを含む OSPF AS-external ルートだけに再配布します。
	・ External Type1 - OSPF AS-external type-1 ルートだけを再配布します。
	・ External Type2 - OSPF AS-external type-2 ルートだけを再配布します。
	・ Internal-E1 - OSPF AS-external type-1 と OSPF AS-internal ルートだけを再配布します。
	・ Internal-E2 - OSPF AS-external type-2 と OSPF AS-internal ルートだけを再配布します。
Metric (0-4294967295)	再配布ルートに RIP メトリックを指定します。
Route Map Name	特定のルートを再配布するかどうか決定する基準として使用されるルートマップを指定します。

「Apply」をクリックし、設定内容を適用します。

#### エントリの検索

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

#### エントリの削除

削除するエントリの「Delete」ボタンをクリックします。「Delete All」ボタンをクリックして、表示されたすべてのエントリを削除します。

「Please Select」をクリックすると、次の画面が表示されます。

otal Entries: 1		
	VRF Name	RD
0	VRF1	192.168.70.1.24
		1/1 K < 1 > > G
		ОК

#### 図 9-166 VRF List 画面

# BGP Route Preference Settings (BGP ルート優先設定)

BGP Route Preference Settings (BGP ルート優先設定)の設定、表示を行います。

L3 Features > BGP > BGP Route Preference Settings の順にメニューをクリックして以下の画面を表示します。

GP Route Preference Settings -		
Address Family	IPv4 VRF V Please Se	elect
Distance EBGP (1-255)	70	
Distance IBGP (1-255)	130	Apply

図 9-167 BGP Route Preference Settings 画面

画面に表示される項目:
-------------

項目	説明
Address Family	アドレスファミリーを選択します。
	・ IPv4 Unicast - IPv4 ユニキャストアドレスファミリーを指定します。
	・ IPv4 VRF - VRF インスタンス(12 字以内)を指定します。VRF インスタンス名を入力するか、「Please Select」で既存の
	VRF インスタンスを選択します。
	・ IPv4 Multicast - IPv4 マルチキャストアドレスファミリーを指定します。
	・ IPv6 Unicast - IPv6 ユニキャストアドレスファミリーを指定します。
Distance EGBP	ディスタンスeBGPルート優先値(1-255: IPv4/VRFアドレスファミリー)(1-254: IPv6/VRFアドレスファミリー)を指定します。
Distance IBGP	ディスタンス iBGP ルート優先値(1-255: IPv4/VRF アドレスファミリー) (1-254: IPv6/VRF アドレスファミリー)を指定します。

「Apply」をクリックし、設定内容を適用します。

「Please Select」をクリックすると、次の画面が表示されます。

al Entries: 1		
	VRF Name	RD
0	VRF1	192.168.70.1.24
		OK

図 9-168 VRF List 画面

使用する VRF エントリを選択し、「OK」をクリックします。 設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

### BGP Dampening Settings (BGP ダンプニング設定)

Border Gateway Protocol(BGP) 処理のダンプニング設定を行います。本コマンドの目的は、ルートのダンプニングを排除して、フラッピングルート によりネットワークが不安定になることを避けることにあります。

L3 Features > BGP > BGP Dampening Settings の順にメニューをクリックして以下の画面を表示します。

BGP Dampening Settings		
BGP Dampening		
Address Family	IPv4 VRF Please Select	
BGP Dampening State		
Dampening State	Disabled	Apply
BGP Dampening Route Map		
BGP Dampening Route Map	16 chars	Apply
BGP Dampening Settings		
Half Life Time (1-45)	0 min	
Reuse Value (1-20000)	0	
Suppress Value (1-20000)	0	
Max Suppress Time (1-255)	0 min	
Unreachable Route's Half Life (1-45)	0 min	Apply

図 9-169 BGP Dampening Settings 画面

画面に表示される項目:

項目	説明	
	BGP Dampening	
Address Family	アドレスファミリーを選択します。	
	・ IPv4 Unicast - IPv4 ユニキャストアドレスファミリーを指定します。	
	・ IPv4 VRF - VRF インスタンス(12 字以内)を指定します。VRF インスタンス名を入力するか、「Please Select」で既存	
	の VRF インスタンスを選択します。	
	・ IPv4 Multicast - IPv4 マルチキャストアドレスファミリーを指定します。	
	・ IPv6 Unicast - IPv6 ユニキャストアドレスファミリーを指定します。	
	BGP Dampening	
Dampening State	プルダウンメニューを使用して、BGP ダンプニング機能の状態を「Enabled」(有効)/「Disabled」(無効)にします。	
BGP Dampening Route Map		
BGP Dampening Route BGP ダンプニングルートマップ名(16 字以内)を入力します。		
Мар		
	BGP Dampening Settings	
Half Life Time (1-45)	到達経路のペナルティが半分にダウンする時間(分)を指定します。 初期値は 15(分)です。	
Reuse Value (1-20000)	再利用値を入力します。フラッピングルートへのペナルティが本値以下にダウンすると、ルートは抑制されません。初期	
	値は 750 です。	
Suppress Value	抑制値を入力します。ペナルティがこの制限を超過すると、ルートは抑制されます。初期値は 2000 です。	
(1-20000)		
Max Suppress Time	ルートが抑制される最大時間(分)を入力します。初期値は60(分)です。	
(1-255)		
Un Reachability	未到達経路のペナルティが半分にダウンする時間(分)を指定します。初期値は15(分)です。	
Half Life (1-45)		

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

「Please Select」をクリックすると、次の画面が表示されます。

F List		
otal Entries: 1		
	VRF Name	RD
0	VRF1	192.168.70.1.24
		1/1 🔀 🕹 🗎 🕹
		ОК

図 9-170 VRF List 画面

# BGP Dampening Dampened Paths Table (BGP ダンプニングダンプドパステーブル)

BGP Dampening Dampened Paths Table (BGP ダンプニングダンプドパステーブル)の表示、クリアをしてします。

L3 Features > BGP > BGP Dampening Dampened Paths Table の順にメニューをクリックして以下の画面を表示します。

BGP Dampening Dampened Paths Table				
BGP Dampening Dampened Paths Table				
Address Family IPv6 Unicast	Please Select			
Type All 💌			Clear	
BGP Dampening Dampened Paths Information				
Total Entries: 0 Network From Reuse Path				

図 9-171 BGP Dampening Dampened Paths Table 画面

画面に表示される項目:

項目	説明
Address Family	アドレスファミリーを選択します。
	・ IPv4 Unicast - IPv4 ユニキャストアドレスファミリーを指定します。
	・ IPv4 VRF - VRF インスタンス(12 字以内)を指定します。VRF インスタンス名を入力するか、「Please Select」で
	既存の VRF インスタンスを選択します。
	・ IPv4 Multicast - IPv4 マルチキャストアドレスファミリーを指定します。
	・ IPv6 Unicast - IPv6 ユニキャストアドレスファミリーを指定します。
Туре	ダンプニングダンプドパスの「Type」を指定します。
	・ All - 全ての BGP ダンプニングダンプドパスを表示、クリアします。
	・ IP Address - 入力した IPv4 アドレスに基づく BGP ダンプニングダンプドパスを表示、クリアします。
	・ Network Address - 入力した IPv4 ネットワークアドレスに基づく BGP ダンプニングダンプドパスを表示、クリア
	します。
	・ IPv6 Address - 入力した IPv6 アドレスに基づく BGP ダンプニングダンプドパスを表示、クリアします。
	・ IPv6 Network Address - 入力した IPv6 ネットワークアドレスに基づく BGP ダンプニングダンプドパスを表示、ク
	リアします。

「Clear」をクリックすると入力したエントリをクリアします。

「Please Select」をクリックすると、次の画面が表示されます。

tal Entries: 1		
	VRF Name	RD
0	VRF1	192.168.70.1.24
		OK

使用する VRF エントリを選択し、「OK」をクリックします。

図 9-172 VRF List 画面

### BGP Dampening Flap Statistics Table (BGP ダンプニングフラップ統計テーブル)

BGP Dampening Flap Statistics Table (BGP ダンプニングフラップ統計テーブル)の表示、クリアをしてします。

L3 Features > BGP > BGP Dampening Flap Statistics Table の順にメニューをクリックして以下の画面を表示します。

BGP Dampening Flap Statistics Table							
BGP Dampening Flap Statistics Table							
Address Family IPv6 Unicast V Please Select Type All V Clear							
BGP Dampening Flap Statistics Information							
Total Entries: 0							
Network	From	Flaps	Duration	Reuse	Path		

図 9-173 BGP Dampening Flap Statistics Table 画面

画面に表示される項目:
-------------

項目	説明
Address Family	アドレスファミリーを選択します。
	・ IPv4 Unicast - IPv4 ユニキャストアドレスファミリーを指定します。
	・ IPv4 VRF - VRF インスタンス(12 字以内)を指定します。VRF インスタンス名を入力するか、「Please Select」で
	既存の VRF インスタンスを選択します。
	・ IPv4 Multicast - IPv4 マルチキャストアドレスファミリーを指定します。
	・ IPv6 Unicast - IPv6 ユニキャストアドレスファミリーを指定します。
Туре	「Type」を指定します。
	・ All - 全ての BGP ダンプニングフラップ統計を表示、クリアします。
	・ IP Address - 入力した IPv4 アドレスに基づく BGP ダンプニングフラップ統計を表示、クリアします。
	・ Network Address - 入力した IPv4 ネットワークアドレスに基づく BGP ダンプニングフラップ統計を表示、クリアしま
	す。
	・ IPv6 Address - 入力した IPv6 アドレスに基づく BGP ダンプニングフラップ統計を表示、クリアします。
	・ IPv6 Network Address - 入力した IPv6 ネットワークアドレスに基づく BGP ダンプニングフラップ統計を表示、クリアしま
	す。

「Clear」をクリックすると入力したエントリをクリアします。

### 「Please Select」をクリックすると、次の画面が表示されます。

VRF1 192.168.70.1:24				
		VRF1	0	
1/1   < < 1				

VRF List

使用する VRF エントリを選択し、「OK」をクリックします。

図 9-174 VRF List 画面

# BGP Reflector Settings(BGP リフレクタ設定)

BGP リフレクタの設定、表示を行います。

L3 Features > BGP > BGP Reflector Settings の順にメニューをクリックして以下の画面を表示します。

BGP Reflector Settings		
BGP Reflector Settings		
Route Reflector Cluster ID	10 - 10 - 10 - 10	
Client to Client Reflection	Enabled	Apply
Route Reflector Client		
Address Family	IPv4 Unicast	
Neighbor	IPv4 Address 🔽	
State	Disabled	Apply
Total Entries: 0		
	Route Reflector Client	

図 9-175 BGP Reflector Settings 画面

画面に表示される項目:

項目	説明					
BGP Reflector Settings						
Route Reflector Cluster ID	クラスタ ID の IP アドレスを指定します。					
Client to Client Reflection	クライアントからクライアントへのリフレクションを有効または無効にします。					
	BGP Reflector Client					
Address Family	<ul> <li>アドレスファミリーを選択します。</li> <li>IPv4 Unicast - IPv4 ユニキャストアドレスファミリーを指定します。</li> <li>IPv4 VRF - VRF インスタンス(12 字以内)を指定します。VRF インスタンス名を入力するか、「Please Select」で 既存の VRF インスタンスを選択します。</li> <li>IPv4 Multicast - IPv4 マルチキャストアドレスファミリーを指定します。</li> <li>IPv6 Unicast - IPv6 ユニキャストアドレスファミリーを指定します。</li> </ul>					
Neighbor	クライアントとなる「Neighbor」を指定します。 ・ IPv4 Address - ネイバリングルータの IPv4 アドレスを指定します。 ・ Peer Group - ルートリフレクタクライアントとなるピアグループ名を指定します。 ・ IPv6 Address - ネイバリングルータの IPv6 アドレスを指定します。					
State	状態を有効または無効にします。有効にすると、指定した Neighbor は、BGP リフレクタクライアントになります。					

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

### BGP Confederation Settings (BGP コンフェデレーション設定)

BGP のコンフェデレーション設定を行います。

L3 Features > BGP > BGP Confederation Settings の順にメニューをクリックして以下の画面を表示します。

Apply
Remote AS Number

図 9-176 BGP Confederation Settings 画面

以下の項目を使用して設定を行います。

項目	説明					
Confederation Identifier	BGP コンフェデレーションを指定するのに使用する AS 番号を入力します。					
(0-4294967295)						
Confederation Peer	プルダウンメニューを使用して「Add」(追加)または「Delete」(削除)を選択し、BGP コンフェデレーションピア					
	ID(1-4294967295)を指定します。					
 Apply」ボタンをクリックして行った変更を適用します。						

### BGP AS Path Access List Settings(BGP AS パスアクセスリストリスト設定)

AS パスアクセスリストを設定します。

L3 Features > BGP > BGP AS Path Access Settings の順にメニューをクリックして以下の画面を表示します。

BGP AS Path Acces	ss List Settings	_	_		
BGP AS Path Access Lis	t Settings				
List Name Mode	16 chars None		Regular Expression	80 chars	Apply
List Name	16 chars				Find Show All
Total Entries: 1					
		Li	st Name		
	List			Delete	
					1/1 < < 1 > > Go
List Name: List					
Mod	e			Regular Expression	
Perm	lit			Expression	
					1/1  < < 1 > >  Go

図 9-177 BGP AS Path Access List Settings 画面

#### 画面に表示される項目:

項目	説明
List Name	ASパスアクセスリスト名を入力します。
Mode	プルダウンメニューを使用して、条件の一致に基づいて通知について「Permit」(許可)、「Deny」(拒否)または「None」
	(何もしない)を指定します。
Regular Expression	as_path フィルタを定義する正規表現(80 字以内)を入力します。
<b>F</b>	

「Apply」ボタンをクリックして行った変更を適用します。

### エントリの参照

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。 「Show All」ボタンをクリックして、すべての定義済みエントリを表示します。

### エントリの削除

削除するエントリの「Delete」ボタンをクリックします。「Delete All」ボタンをクリックして、表示されたすべてのエントリを削除します。

# BGP Community List Settings(BGP コミュニティリスト設定)

BGP コミュニティリストに照合ルールを設定します。

L3 Features > BGP > BGP Community List Settings の順にメニューをクリックして以下の画面を表示します。

BGP Community List Sett	ings	_	_		_	
BGP Community List Settings						
List Name	16 chars					
Туре	Standard	~				
Mode	None	~				
Community Number (1-65535) ASN:NN						
Regular Option	Internet	Local AS	No Advertise	No Export		
Regular Expression	80 chars					Apply
List Name	16 chars					Find Show All
Total Entries: 1						
List	List Name			Туре	3	
U	st		Expanded		Delete	
						1/1 < < 1 > > Go
List Name: List						
Mode				Regular Ex	pression	
Permit				Expres	ssion	
						1/1 < < 1 > > Go

図 9-178 BGP Community List Settings 画面

画面に表示される項目	:
------------	---

項目	説明
List Name	コミュニティリスト名(16字以内)を入力します。
Туре	プルダウンメニューを使用して Standard または Expanded を選択します。Standard は標準的なコミュニティリストを設定し、
	Expanded は拡大コミュニティリストを設定します。
Mode	プルダウンメニューを使用して、ルールが一致した場合のルートのアクション「Permit」(許可)、「Deny」(拒否) または「None」
	(何もしない)を指定します。
Community	コミュニティ番号を指定します。「AA:NN」の形式のユーザ定義の番号で、「AA」は AS 番号、「NN」はユーザが定義する番号
Number	を指定します。スペースによって区切られた複数のコミュニティ番号も指定可能です。
Regular Option	標準的なオプションを選択します。
	・ Internet - このコミュニティを持つルートをすべてのピア (内部または外部) に送信します。
	・ Local AS - このコミュニティを持つルートは同じ AS のピアに送信されますが、同じコンフェデレーション内の別のサブ
	AS にあるピアと外部のピアには送信されません。
	• No Advertise - このコミュニティを持つルートはどんなピア (内部または外部)にも通知されません。
	・ No Export - このコミュニティを持つルートはコンフェデレーション内の同じ AS か別のサブ AS にあるピアに送信されま
	すが、外部の BGP(eBGP) ピアには送信されません。
Regular Expression	コミュニティセットの値を入力します。80文字以内で指定します。

「Apply」ボタンをクリックして行った変更を適用します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

「Show All」ボタンをクリックして、すべての定義済みエントリを表示します。

削除するエントリの「Delete」ボタンをクリックします。

# BGP Extended Community List Settings(BGP 拡張コミュニティリスト設定)

BGP 拡張コミュニティリストを設定します。

L3 Features > BGP > BGP Extended Community List Settings の順にメニューをクリックして以下の画面を表示します。

BGP Extended Commu	inity List Settings		
BGP Extended Community Li	st Settings		
List Name	16 chars		
Туре	Standard 🗸		
Mode	None 🗸		
Extended Community	RT 🔽 ASN:	NN or IP:NN	
Regular Expression	80 chars		Apply
List Name	16 chars		Find Show All
Total Entries: 1			
L	ist Name	Туре	
	List	Expanded	Delete
			1/1 K < 1 > > Go
List Name: List			
Mode		Regular Expression	
Permit		Expression	
			1/1 K < 1 > > Go

図 9-179 BGP Extended Community List Settings 画面

### 画面に表示される項目:

項目	説明
List Name	拡張コミュニティリスト名(16 字以内)を入力します。
Туре	プルダウンメニューを使用して Standard または Expanded を選択します。Standard は標準的な拡張コミュニティリストを設
	定し、Expanded は拡大拡張コミュニティリストを設定します。
Mode	プルダウンメニューを使用して、ルールが一致した場合のルートのアクション「Permit」(許可)、「Deny」(拒否) または「None」
	(何もしない)を指定します。
Extended	拡張コミュニティを指定します。
Community	・ RT - 「Route Target」(RT) を使用します。
	・ SoO - 「Site-of-Origin」(SoO) を使用します。
	表示される欄に拡張コミュニティ文字列を入力します。
Regular Expression	コミュニティセットの値を入力します。80 文字以内で指定します。

「Apply」ボタンをクリックして行った変更を適用します。

# BGP Clear Settings(BGP クリア設定)

ハードまたはソフト再構成を使用して Border Gateway Protocol(BGP) をリセットします。

L3 Features > BGP > BGP Clear Settings	の順にメニューをクリックして以下の画面を表示します
--	---------------------------

BGP Clear Settings		
BGP Clear Settings		
Address Family	IPv4 Unicast V Please Select	
Туре	All	
AS Number (1-4294967295)		
Peer Group	16 chars	
Neighbor Address	IPv4	
Mode Option	Soft In Prefix Filter Out	]

図 9-180 BGP Clear Settings 画面

画面に表示される項目:

項目	説明
Address Family	アドレスファミリーを選択します。
	・ IPv4 Unicast - IPv4 ユニキャストアドレスファミリーを指定します。
	・ IPv4 VRF - VRF インスタンス(12 字以内)を指定します。VRF インスタンス名を入力するか、「Please Select」で
	既存の VRF インスタンスを選択します。
	・ IPv4 Multicast - IPv4 マルチキャストアドレスファミリーを指定します。
	・ L2VPN VPLS - L2VPN VPLS アドレスファミリーを指定します。
	・ VPNv4 - VPNv4 アドレスファミリーを指定します。
	・ IPv6 Unicast - IPv6 ユニキャストアドレスファミリーを指定します。
Туре	BGP タイプを指定します。
	・ All - 指定アドレスの全ての BGP ピアセッションをクリアします。
	・ AS Number - 指定した AS の BGP ピアセッションをクリアします。
	・ Peer Group - ピアグループの BGP ピアセッションをクリアします。
	・ Neighbor Address - ネイバアドレスの BGP ピアセッションをクリアします。
	・ External - ハード / ソフト再設定を使用した BGP ピアセッションをクリアします。
AS Number (1-4294967295)	「Type」メニューで「AS」を選択した場合、AS 番号を入力します。
Peer Group	「Type」メニューで「Peer Group」を選択した場合、ピアグループ名を入力します。
Mode Option	希望のモードをチェックします。
	• Soft - ソフトリセットを開始します。セッションを切断しません。
	・ In - 内向き再構成を開始します。
	・ Prefix Filter - 既存の Outbound Route Filter (ORF) プリフィクスリストをクリアすることで、ピアルータからの
	ORF プリフィクスリストを更新し、新しいルートの更新を行います。
	・ Out - 外向きの再構成を開始します。
	「In」も「Out」キーワードも指定されないと、内向きと外向きのセッションの両方がリセットされます。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

# BGP Summary Table (BGP サマリテーブル)

BGP サマリ情報を表示します。

L3 Features > BGP > BGP Summary Table の順にメニューをクリックして以下の画面を表示します。

BGP Summary Table		_				
BGP Summary Table						
Address Family IPv4	Unicast 🔽					Find
BGP Summary Information						
Total Entries: 0						
Neighbor	Version	AS	Message Received	Message Sent	Up/Down	State/Prefix Received

図 9-181 BGP Summary Table 画面

項目	説明
Address Family	アドレスファミリーを選択します。
	・ IPv4 Unicast - IPv4 ユニキャストアドレスファミリーを指定します。
	・ IPv4 Multicast - IPv4 マルチキャストアドレスファミリーを指定します。
	・ IPv6 Unicast - IPv6 ユニキャストアドレスファミリーを指定します。
	・ IPv6 Multicast - IPv6 マルチキャストアアドレスファミリーを指定します。
	・ VPNv4 All - 全 VPNv4 アドレスファミリーを指定します。
	・ VPNv4 RD - Route Distinguisher (RD) VPNv4 アドレスファミリーを指定します。
	・ VPNv4 VRF - VRF インスタンス(12 字以内)を指定します。VRF インスタンス名を入力するか、「Please Select」
	で既存の VRF インスタンスを選択します。
	・ L2VPN VPLS - L2VPN VPLS アドレスファミリーを指定します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

### 「Please Select」をクリックすると、次の画面が表示されます。

VRF List		
Total Entries: 1		
	VRF Name	RD
0	VRF1	192.168.70.1.24
		1/1 K < 1 > > Go
		ОК

図 9-182 Please Select (VRF) 画面

使用する VRF エントリを選択し、「OK」をクリックします。 設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

# BGP Routing Table(BGP ルーティングテーブル)

BGP ルーティングを表示します。

L3 Features > BGP > BGP Routing Table の順にメニューをクリックして以下の画面を表示します。

BGP Routing Table		_		_	_
BGP Routing Table					
Address Family	IPv4 Unicast				
Туре	Please Select				Find
BGP Routing Information	1				
Total Entries: 0					
Network	Next Hop	Metric	Local Preference	Weight	Path

図 9-183 BGP Routing Table 画面

画面に表示される項目:

項目	説明
Address Family	アドレスファミリーを選択します。
	・ IPv4 Unicast - IPv4 ユニキャストアドレスファミリーを指定します。
	・ IPv4 Multicast - IPv4 マルチキャストアドレスファミリーを指定します。
	・ IPv6 Unicast - IPv6 ユニキャストアドレスファミリーを指定します。
	・ VPNv4 All - 全 VPNv4 アドレスファミリーを指定します。
	・ VPNv4 RD - Route Distinguisher (RD) VPNv4 アドレスファミリーを指定します。
	・ VPNv4 VRF - VRF インスタンス(12 字以内)を指定します。VRF インスタンス名を入力するか、「Please Select」
	で既存の VRF インスタンスを選択します。
	・ L2VPN VPLS All - L2VPN VPLS アドレスファミリーの全情報を指定します。
	・ L2VPN VPLS RD - L2VPN VPLS アドレスファミリーの Route Distinguisher (RD) 情報を指定します。
	・ L2VPN VPLS VFI - L2VPN VPLS アドレスファミリーの VFI インスタンス(12 字以内)を指定します。
Туре	プルダウンメニューを使用して、「Type」を指定します。選択タイプに基づいて以下のパラメータを変更します。
	・ IP Address - 特定の IPv4 アドレス /IPv6 アドレスを指定します。
	・ Netowork - 特定の IPv4/IPv6 ネットワークアドレスを指定します。「Longer Prefixes」をチェックして、指定ルー
	トの通知を停止します。
	・ Route Map - ルートマップを指定します。「Route Map Name」ルートマップ名(16 字以内)/「L2VPN Prefix」に
	一致するルートを表示します。
	・ CIDR Only - CIDR(Classless Inter-Domain Routing)を指定します。
	• Community - BGP コミュニティを指定します。「Community Set」コミュニティセットを入力します。「Local AS」
	- ローカル AS の外側には送信しません。( 既知のコミュニティ )。「No Advertise」- どんなピアにも通知しません。
	(既知のコミュニティ )。「No Export」- ネクスト AS にエクスポートしません。( 既知のコミュニティ )。「Internet」
	- インターネットに送信します ( 既知のコミュニティ )。「Exact Match」- 指定されると、コミュニティは正確に一
	致する必要があります。「L2VPN Prefix」 - L2VPN プリフィクスを入力します。
	• Community List - コミュニティリストを入力します。「Exact Match」が指定されると、コミュニティは正確に一致
	する必要があります。「L2VPN Prefix」- L2VPN プリフィクスを入力します。
	• Filter List - 「Filter List Name」フィルタリスト名を入力します。「L2VPN Prefix」 - L2VPN プリフィクスを入力します。
	<ul> <li>Inconsistent AS - 同じプレフィックスと異なる AS パスオリジンを持つ場合にルートを表示します。「L2VPN Prefix」</li> </ul>
	- L2VPN プリフィクスを入力します。
	・ Quote Regexp - 「Regexp」 - 「Regular Expression」にマッチするルートを指定します。「L2VPN Prefix」 - L2VPN プリ
	フィクスを入力します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

「Please Select」をクリックすると、次の画面が表示されます。

		RD
0	VRF1	192.168.70.1:24

図 9-184 Please Select(VRF)画面

使用する VRF エントリを選択し、「OK」をクリックします。

### BGP Labels Table (BGP ラベルテーブル)

BGP ラベルテーブルを表示します。

L3 Features > BGP > BGP Labels Table の順にメニューをクリックして以下の画面を表示します。

GP Labels Table			
GP Labels Table			
Address Family VPNv4			Find
BGP Labels Information			
Total Entries: 0			
Neb	vork	From	In Label/Out Label

図 9-185 BGP Labels Table 画面

#### 画面に表示される項目:

項目	説明
Address Family	アドレスファミリーを選択します。
	・ VPNv4 All - 全 VPNv4 アドレスファミリーを指定します。
	・ VPNv4 RD - Route Distinguisher (RD) VPNv4 アドレスファミリーを指定します。
	・ VPNv4 VRF - VRF インスタンス(12 字以内)を指定します。VRF インスタンス名を入力するか、「Please Select」
	で既存の VRF インスタンスを選択します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

「Please Select」をクリックすると、次の画面が表示されます。

tal Entries: 1		
	VRF Name	RD
0	VRF1	192.168.70.1:24

使用する VRF エントリを選択し、「OK」をクリックします。 設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

### BGP Neighbor (BGP ネイバ設定)

### Neighbor(ネイバ設定)

BGP ネイバを設定、表示します。

L3 Features > BGP > BGP Neighbor > Neighbor の順にメニューをクリックして以下の画面を表示します。

Neighbor				
Neighbor Settings				
IP Address	VRF Name	Remote AS Number (1-4294967295)	Action	
IPv4 · · ·	Please Select		Add	Apply
Neighbor Table				
Address Family				
IPv4 Unicast				
Neighbor Address	Туре			
IPv4 · · ·	None			Find
Total Entries: 1				
Neighbor /	Address	VI	RF Name	
192.168	3.60.1			Delete
			1/1 < 1	> >  Go
	Neighbor Detail Informati	ion		

図 9-187 Neighbor (BGP) 画面

図 9-186 VRF List 画面

画面に表示される項目:

項目	説明 説明		
	Neighbor Settings		
IP Address	ネイバルータの IPv4/IPv6 アドレスを指定します。		
VRF Name	VRF インスタンス名を 12 字以内で入力します。		
	「Please Select」で事前に設定済みの VRF を選択することが可能です。		
Remote AS Number	リモート AS 番号を入力します。範囲は 1-4294967295 です。		
(1-4294967295)			
Action	実行する動作を指定します。「Add」(追加)「Delete」(削除)から指定します。		
	Neighbor Table		
Address Family	アドレスファミリーを選択します。		
	・ IPv4 Unicast - IPv4 ユニキャストアドレスファミリーを指定します。		
	・ IPv4 Multicast - IPv4 マルチキャストアドレスファミリーを指定します。		
	・ IPv6 Unicast - IPv6 ユニキャストアドレスファミリーを指定します。		
	・ VPNv4 All - 全 VPNv4 アドレスファミリーを指定します。		
	・ VPNv4 RD - Route Distinguisher (RD) VPNv4 アドレスファミリーを指定します。		
	・ VPNv4 VRF - VRF インスタンス(12 字以内)を指定します。VRF インスタンス名を入力するか、「Please Select」		
	で既存の VRF インスタンスを選択します。		
	・ L2VPN VPLS - L2VPN VPLS アドレスファミリーの全情報を指定します。		
Neighbor Address	ネイバルータの IPv4/IPv6 アドレスを指定します。		
Туре	プルダウンメニューを使用して各種タイプを選択します。		
	・ None - 表示するタイプを指定しません。		
	<ul> <li>Advertised Routes - BGP Neighbor に通知されるルートを表示します。</li> </ul>		
	・ Received Routes - この Neighbor から受信したルートを表示します。		
	・ Routes - Neighbor から学習したルーティングテーブル内のルートを表示します。		
	・ Received Prefix Filter - BGP Neighbor から受信したプレフィックスフィルタ情報を表示します。		
「Find」ボタンをクリックして	て、入力した情報に基づく特定のエントリを検出します。		

「Delete」をクリックすると指定のエントリを削除します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Please Select」をクリックすると、次の画面が表示されます。

RF List		
tal Entries: 1		
	VRF Name	RD
0	VRF1	192.168.70.1:24
		1/1   < 1 > >   c
		ОК

図 9-188 VRF List 画面

使用する VRF エントリを選択し、「OK」をクリックします。 設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

### Peer Group (Peer グループ設定)

Border Gateway Protocol (BGP) ネイバ Peer グループを設定します。

### L3 Features > BGP > BGP Neighbor > Peer Group の順にメニューをクリックして以下の画面を表示します。

Peer Group			
Peer Group Group Name VRF Name 16 chars	Please Select	Remote AS Number (1-4294967295) Action Add	Apply
Peer Group Member IP Address IPv4 Peer Group Table	Group Name	Action Add	Apply
Address Family IPv4 Unicast	Group Name 16 chars		Find
Peer Group Group	p	VRF Name	Delete
		1/	1 K < 1 > > Go
	Peer Group	Detail Information	
Peer Group	Group	Remote AS	1
Configured Hold Time	180	Configured Keepalive Interval	60
BGP Version	4	Default Advertisement Interval	5 sec
AS Origination Interval	15 sec	Address Family Information	Show Detail

図 9-189 Peer Group 画面

#### 画面に表示される項目:

項目	説明
	Peer Group
Group Name	BGP ピアグループ名(16 字以内)を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。 「Please Select」で事前に設定済みの VRF を選択することが可能です。
Remote AS Number (1-4294967295)	リモート AS 番号を入力します。範囲は 1-4294967295 です。
Action	実行する動作を指定します。「Add」(追加)/「Delete」(削除)から指定します。
	Peer Group Member
IP Address	ピアグループメンバの IPv4/IPv6 アドレスを指定します。
Group Name	BGP ピアグループ名(16 字以内)を指定します。
Action	実行する動作を指定します。「Add」(追加)/「Delete」(削除)から指定します。
	Peer Group Table
Address Family	<ul> <li>アドレスファミリーを選択します。</li> <li>IPv4 Unicast - IPv4 ユニキャストアドレスファミリーを指定します。</li> <li>VPNv4 All - 全 VPNv4 アドレスファミリーを指定します。</li> <li>VPNv4 RD - Route Distinguisher (RD) VPNv4 アドレスファミリーを指定します。</li> <li>VPNv4 VRF - VRF インスタンス(12 字以内)を指定します。VRF インスタンス名を入力するか、「Please Select」 で既存の VRF インスタンスを選択します。</li> </ul>
Group Name	BGP ピアグループ名(16 字以内)を指定します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

「Delete」をクリックすると指定のエントリを削除します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Show Detail」をクリックして、指定エントリの詳細について表示します。

「Please Select」をクリックすると、次の画面が表示されます。

al Entries: 1		
	VRF Name	RD
0	VRF1	192.168.70.1:24

図 9-190 VRF List 画面

使用する VRF エントリを選択し、「OK」をクリックします。 設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

#### 「Show Detail」をクリックすると、次の画面が表示されます。

For Address Family: IPv4 Unicast				
BGP Neighbor	Group, no member	Index	0	
Offset	0	Mask	0x0	
Maximum Limit	16384	Warning Only	Disabled	
Warning Threshold	75%			

図 9-191 rAddress Family Information 画面

「Back」をクリックすると前のページに戻ります。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

### Neighbor Activate(ネイバ有効化)

Border Gateway Protocol (BGP) ネイバを有効化します。

L3 Features > BGP > BGP Neighbor > Neighbor Activate の順にメニューをクリックして以下の画面を表示します。

Neighbor Activate		
Neighbor Activate		
Address Family	Neighbor	Action
IPv4 Unicast	IPv4 Address	Activate Apply

図 9-192 Neighbor Activate 画面

画面に表示される項目:

項目	説明
Address Family	アドレスファミリーを選択します。
	・ IPv4 Unicast - IPv4 ユニキャストアドレスファミリーを指定します。
	・ IPv4 VRF - VRF インスタンス(12 字以内)を指定します。VRF インスタンス名を入力するか、「Please Select」で
	既存の VRF インスタンスを選択します。
	・ IPv4 Multicast - IPv4 マルチキャストアドレスファミリーを指定します。
	・ L2VPN VPLS - L2VPN VPLS アドレスファミリーを指定します。
	・ VPNv4 - VPNv4 アドレスファミリーを指定します。
	・ IPv6 Unicast - IPv6 ユニキャストアドレスファミリーを指定します。
Neighbor	ネイバを選択、指定します。
	・ IPv4 Address - ネイバの IPv4 アドレスを指定します。
	・ Peer Group - ネイバとなるピアグループ名を指定します。
	・ IPv6 Address - ネイバの IPv6 アドレスを指定します。
Action	実行する動作を指定します。「Activate」(有効化)/「No Activate」(無効化)から指定します。

「Apply」をクリックし、設定内容を適用します。
「Please Select」をクリックすると、次の画面が表示されます。

fotal Entries: 1		
	VRF Name	RD
0	VRF1	192.168.70.1.24
		1/1 K < 1 > > G
		OK

図 9-193 VRF List 画面

使用する VRF エントリを選択し、「OK」をクリックします。 設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

#### Neighbor Shutdown(ネイバシャットダウン)

Border Gateway Protocol (BGP) ネイバをシャットダウンします。

L3 Features > BGP > BGP Neighbor > Neighbor Shutdown の順にメニューをクリックして以下の画面を表示します。

Neighbor Shutdown				
■ Neighbor Shutdown				
Neighbor	VRF Name		Action	
IPv4 Address 🗸		Please Select	Shutdown 🗸	Apply
IPv4 Address 🔽		Please Select	Shutdown	Apply

図 9-194 Neighbor Shutdown 画面

#### 画面に表示される項目:

項目	説明
Neighbor	ネイバを選択、指定します。
	・ IPv4 Address - ネイバの IPv4 アドレスを指定します。
	• Peer Group - ネイバのピアグループ名を指定します。
	・ IPv6 Address - ネイバの IPv6 アドレスを指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。 「Please Select」で事前に設定済みの VRF を選択することが可能です。
Action	実行する動作を指定します。「Shutdown」「No Shutdown」から指定します。

「Apply」をクリックし、設定内容を適用します。

「Please Select」をクリックすると、次の画面が表示されます。

VRF List		
tal Entries: 1	VRF Name	RD
0	VRF1	192.168.70.1:24
		ок

図 9-195 VRF List 画面

使用する VRF エントリを選択し、「OK」をクリックします。 設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

# Neighbor Map Settings(ネイバマップ設定)

Border Gateway Protocol (BGP) ネイバマップを設定、表示します。

L3 Features > BGP > BGP Neighbor > Neighbor Map Settings の順にメニューをクリックして以下の画面を表示します。

Neighbor Map Settings		
Neighbor Map Settings		
Address Family	IPv4 Unicast V Please Select	
Neighbor	IPv4 Address 🔽	
Unsuppress Map Action	Add	
Unsuppress Map Name	16 chars	
Route Map Type	In 🔽	
Route Map Action	Add	
Route Map Name	16 chars	
	Apply	

図 9-196 Neighbor Map Settings 画面

#### 画面に表示される項目:

項目	説明
Address Family	アドレスファミリーを選択します。
	・ IPv4 Unicast - IPv4 ユニキャストアドレスファミリーを指定します。
	・ IPv4 VRF - VRF インスタンス(12 字以内)を指定します。VRF インスタンス名を入力するか、「Please Select」で
	既存の VRF インスタンスを選択します。
	・ IPv4 Multicast - IPv4 マルチキャストアドレスファミリーを指定します。
	・ L2VPN VPLS - L2VPN VPLS アドレスファミリーを指定します。
	・ VPNv4 - VPNv4 アドレスファミリーを指定します。
	・ IPv6 Unicast - IPv6 ユニキャストアドレスファミリーを指定します。
Neighbor	ネイバを選択、指定します。
	・ IPv4 Address - ネイバの IPv4 アドレスを指定します。
	• Peer Group - ネイバとなるピアグループ名を指定します。
	・ IPv6 Address - ネイバの IPv6 アドレスを指定します。
Unsuppress Map Action	「Unsuppress Map Action」の設定を行います。アドレスアグリゲートにより抑制されている通知ルートを選択的に使
	用するルータマップ名を「Add」(追加)/「Delete」(削除)します。
Unsuppress Map Name	アドレスアグリゲートにより抑制されている通知ルートを選択的に使用するルートマップ名 (16 字以内)を指定します。
Route Map Type	プルダウンメニューを使用して In または Out を選択します。In は Neighbor からの内向きルートで、Out はピアに送
	信する外向きルートを示します。
Route Map Action	ルートマップの動作を追加または削除から指定します。
Route Map Name	内向きまたは外向きルートに適用するルートマップ名(16 字以内)を指定します。
E	

「Apply」をクリックし、設定内容を適用します。

VRF List		
otal Entries: 1		
	VRF Name	RD
0	VRF1	192.168.70.1:24
		ОК

図 9-197 VRF List 画面

使用する VRF エントリを選択し、「OK」をクリックします。 設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

<sup>「</sup>Please Select」をクリックすると、次の画面が表示されます。

## Neighbor Filter Settings(ネイバフィルタ設定)

Border Gateway Protocol (BGP) ネイバフィルタを設定、表示します。

L3 Features > BGP > BGP Neighbor > Neighbor Filter Settings の順にメニューをクリックして以下の画面を表示します。

Neighbor Filter Settings	
Neighbor Filter Settings	
Address Family	IPv4 Unicast V Please Select
Neighbor	IPv4 Address 🔽
Filter List Type	In V
Filter List Action	Add
Filter List Name	16 chars
Prefix List Type	In V
Prefix List Action	Add 🔽
Prefix List Name	32 chars
Capability ORF Prefix List Action	Please Select
Capability ORF Prefix List Type	Receive
	Apply

図 9-198 Neighbor Filter Settings 画面

画面に表示される項目:	
項目	説明
Address Family	アドレスファミリーを選択します。
	・ IPv4 Unicast - IPv4 ユニキャストアドレスファミリーを指定します。
	• IPv4 VRF - VRF インスタンス(12 字以内)を指定します。VRF インスタンス名を入力するか、「Please Select」で
	既存の VRF インスタンスを選択します。
	・ IPv4 Multicast - IPv4 マルチキャストアドレスファミリーを指定します。
	・ L2VPN VPLS - L2VPN VPLS アドレスファミリーを指定します。
	・ VPNv4 - VPNv4 アドレスファミリーを指定します。
	・ IPv6 Unicast - IPv6 ユニキャストアドレスファミリーを指定します。
Neighbor	ネイバを選択、指定します。
	・ IPv4 Address - ネイバの IPv4 アドレスを指定します。
	• Peer Group - ネイバとなるピアグループ名を指定します。
	・ IPv6 Address - ネイバの IPv6 アドレスを指定します。
Filter List Type	フィルタするルートの内向きまたは外向きを「In」または「Out」で指定します。
Filter List Action	フィルタリストの追加または削除を使用します。「Add」「Delete」で指定します。
Filter List Name	フィルタリスト名(16 字以内)を指定します。
Prefix List Type	フィルタするネイバ「から / へ」の通知を、内向きまたは外向き、「In」または「Out」で指定します。
Prefix List Action	プリフィクスリストの追加または削除を使用します。「Add」「Delete」で指定します。
Prefix List Name	プリフィクスリスト名(32 字以内)を指定します。
Capability ORF Prefix List	ORF プリフィクスリスト機能を「Enabled」(有効)/「Disabled」(無効)に指定します。BGP ORF 機能はピアのプリフィ
Action	クス交換の数の減少に使用します。通常、ローカル / リモートルータのペアで指定します。単方向 / 双方向でも指定
	可能です。
Capability ORF Prefix List	外向きルートフィルタプレフィックスリスト機能を設定します。
Туре	以下の値と共に送信することができます。
	• Receive - ORF プレフィックスリスト機能を受信方向に有効にします。ローカルルータはリモートルータによって
	通知されるプレフィックスフィルタリストをインストールします。
	・ Send - ORF プレフィックスリスト機能を送信方向に有効にします。ローカルルータは ORF プレフィックスリスト
	機能のためにリモートルータに通知します。
	• Both - ORF プレフィックスリスト機能を送受信両方向で有効にします。

「Apply」をクリックし、設定内容を適用します。

「Please Select」をクリックすると、次の画面が表示されます。

# VRF List Total Entries: 1 VRF Name ND VRF1 192.168.70.1:24 K OK K

# Neighbor Maximum Prefix Settings(ネイバ最大プレフィクス設定)

Border Gateway Protocol (BGP) ネイバ最大プレフィクスを設定、表示します。BGP ネイバから受け入れることのできる最大プレフィクス数を指定します。

L3 Features > BGP > BGP Neighbor > Neighbor Maximum Prefix Settings の順にメニューをクリックして以下の画面を表示します。

Neighbor Maximum Prefix	Settings
Neighbor Maximum Prefix Setting	S
Address Family	IPv4 Unicast V Please Select
Neighbor	IPv4 Address 🔽
Prefix Action	Disabled
Prefix Max Count (1-16384)	
Prefix Warning Threshold (1-100)	
Prefix Warning Only	Disabled
	Appiy

図 9-200 Neighbor Maximum Prefix Settings 画面

#### 画面に表示される項目:

項目	説明
Address Family	アドレスファミリーを選択します。
	・ IPv4 Unicast - IPv4 ユニキャストアドレスファミリーを指定します。
	・ IPv4 VRF - VRF インスタンス(12 字以内)を指定します。VRF インスタンス名を入力するか、「Please Select」で
	既存の VRF インスタンスを選択します。
	・ IPv4 Multicast - IPv4 マルチキャストアドレスファミリーを指定します。
	・ L2VPN VPLS - L2VPN VPLS アドレスファミリーを指定します。
	・ VPNv4 - VPNv4 アドレスファミリーを指定します。
	・ IPv6 Unicast - IPv6 ユニキャストアドレスファミリーを指定します。
Neighbor	ネイバを選択、指定します。
	・ IPv4 Address - ネイバの IPv4 アドレスを指定します。
	・ Peer Group - ネイバとなるピアグループ名を指定します。
	・ IPv6 Address - ネイバの IPv6 アドレスを指定します。
Prefix Action	プレフィクス動作を「Enabled」(有効)/「Disabled」(無効)から指定します。
Prefix Max Count (1-16384)	指定したネイバから許可されるプレフィックスの最大数を入力します。
Prefix Warning Threshold (1-	ルータにおける最大のプレフィックス制限が警告メッセージの生成を開始するパーセントを指定する整数を入力しま
100)	す。範囲は 1-100 です。
Prefix Warning Only	プルダウンメニューを使用して、プレフィックスの警告のみ「Enabled」(有効)/「Disabled」(無効)にします。ピ
	アリングセッションを終了する代わりに最大のプレフィックス制限を超過する際にルータがログメッセージを生成す
	ることを許可します。

「Apply」をクリックし、設定内容を適用します。

	VRF Name	RD
0	VRF1	192.168.70.1:24
		1/1 < 1 > >

図 9-201 Please Select (VRF) 画面

使用する VRF エントリを選択し、「OK」をクリックします。 設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

<sup>「</sup>Please Select」をクリックすると、次の画面が表示されます。

# Neighbor General Settings(ネイバー般設定)

Border Gateway Protocol (BGP) ネイバの一般設定を行います。

L3 Features > BGP > BGP Neighbor > Neighbor General Settings の順にメニューをクリックして以下の画面を表示します。

Neighbor General Settin	gs	_	_	
Neighbor General Settings				
Address Family	IPv/ Unicast			Diase Salact
Noighbor	IPv4 Addross			
Advantisement later val. (4. 000)	IFV4 Address		Defeult	
Advertisement Interval (1-600)			Default	
AS Origination Interval (1-600)			Default	
Limers	Default			
Keep-Alive (0-05535)				
Hold Time (U-65535)				
Next Hop Self	Please Select	~		
Send Community	Please Select	✓ Sta	andard 🗸	
Soft Reconfiguration Inbound	Please Select	~		
Remove Private AS	Please Select	~		
Capability Graceful Restart	Please Select	~		
Description	80 chars		Clear	
EBGP Multihop (1-255)			Default	
Password	25 chars		Clear	
TCP Reconnect (1-65535)			Default	
Update Source	Default			
●VID (1-4094)				
OLoopback ID (1-8)				
Weight (0-65535)			Default	
Allow AS in	Please Select	~		
Allow AS in Value (1-10)				
Default Originate	Please Select	~		
Route Map Name	16 chars			
				Apply

図 9-202 Neighbor General Settings 画面

#### 画面に表示される項目:

月月 項目 日本	。」「1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.
Address Family	アドレスファミリーを選択します。
	・ IPv4 Unicast - IPv4 ユニキャストアドレスファミリーを指定します。
	• IPv4 VRF - VRF インスタンス(12 字以内)を指定します。VRF インスタンス名を入力するか、「Please Select」で
	既存の VRF インスタンスを選択します。
	・ IPv4 Multicast - IPv4 マルチキャストアドレスファミリーを指定します。
	・ L2VPN VPLS - L2VPN VPLS アドレスファミリーを指定します。
	・ VPNv4 - VPNv4 アドレスファミリーを指定します。
	・ IPv6 Unicast - IPv6 ユニキャストアドレスファミリーを指定します。
Neighbor	ネイバを選択、指定します。
	• IPv4 Address - ネイバの IPv4 アドレスを指定します。
	• Peer Group - ネイバとなるピアグループ名を指定します。
	・ IPv6 Address - ネイバの IPv6 アドレスを指定します。
Advertisement Interval	BGP プロセスがピアに更新メッセージを送信する間隔 (1-600) を指定します。
(1-600)	「Default」を選択すると初期値を指定します。
AS Origination Interval	AS の生成するルーティング更新を送信する最小間隔を入力します。範囲は 1-600 です。
(1-600)	「Default」を選択すると初期値を指定します。
Timers	タイマーを指定します。
	・ Keepalive (0-65535) - keepalive メッセージがピアに送信される間隔を指定します。BGP 接続を実装する 2 つのルー
	タが、異なる keepalive タイマを持つ場合、小さい方の keepalive タイマは設定されません。範囲は 0-65535 です。
	keepalive 値が 0 に設定されると、keepalive メッセージは送信されません。ネイバ指定の keepalive 設定をクリア
	します。
	・ Hold Time (0-65535) - keepalive メッセージが本値を超えても受信されないと、システムはピアを Dead として判
	断します。BGP 接続を実装する 2 つのルータが、異なる保持時間を持つ場合、小さい保持時間が使用されます。
	範囲は 0-65535 です。
Next Hop Self	ネクストホップセルフ属性を有効または無効にします。

項目	説明
Send community	「Standard」「Extended」「Both」を選択します。これは BGP Neighbor に送信される(されない)コミュニティ属性を
	指定します。
	・ Standard - 標準コミュニティだけが送信されます(されません)。
	• Extended - 拡張コミュニティだけが送信されます(されません)。
	• Both - 標準 / 拡張、どちらのコミュニティも送信されます(されません)。
Soft Reconfiguration	内向きソフト再構成機能を有効または無効にします。
Inbound	
Remove Private AS	本設定が有効になると、BGP 更新パケットにおける AS パス属性内のプライベートの AS 番号は破棄されます。
Capability Graceful Restart	グレースフルリスタート機能を「Enabled」(有効)/「Disabled」(無効)に指定します。
	ネイバにグレースフルリスタート機能の「Enabled」(有効)/「Disabled」(無効)を通知します。
Description	BGP ネイバの概要(80 字以内)を指定します。「Clear」を選択すると概要を消去します。
EBGP Multihop (1-255)	ネイバに送信される eBGP マルチホップ TTL(1-255)を指定します。これによりルータはローカルピアと直接接続し
	ていない eBGP ピアとの BGP セッションを構築します。「Default」を選択すると初期値を指定します。
Password	BGP ピア間で使用するパスワード(25 字以内)を指定します。「Clear」を選択すると消去します。
TCP Reconnect	TCP 再接続ポート値(1-65535)を指定します。TCP 接続が失敗した後、BGP が TCP 接続リクエストをピアに送信す
	る際の最小間隔値を指定します。「Default」を選択すると初期値(120 秒)を指定します。
Update Source	TCP 接続の BGP セッションによって使用されるインタフェースを指定します。「Default」を選択すると初期値を指定
	します。
	• VID - VLAN ID(1-4094)を指定します。
	・ Loopback - ループバックインタフェースの ID(1-8)を指定します。
Weight	BGP ウェイト値(0-65535)を指定します。 指定ネイバからの受信したルートにアサインするウェイトを指定します。
	「Default」を選択すると初期値を指定します。
Allow AS in	「Allow AS In」を「Enabled」(有効)/「Disabled」(無効)に指定します。これによりルータは受信 BGP パケット内
	に自身の AS 番号を表示させることができます。
Allow AS in Value (1-10)	「Allow AS In」値(1-10)を指定します。
	ローカル AS の最大数を指定し、アップデートパケットの AS パス属性に表示させます。
Default Originate	デフォルトオリジネート機能を有効または無効にします。これによりネイバへのデフォルトルートの起動を有効にし
	ます。
Route Map Name	ルートマップ名(1-16)を指定します。

「Apply」をクリックし、設定内容を適用します。

## 「Please Select」をクリックすると、次の画面が表示されます。

al Entries: 1		
	VRF Name	RD
0	VRF1	192.168.70.1:24
		1/1  < < 1 > >
		OK

図 9-203 VRF List 画面

使用する VRF エントリを選択し、「OK」をクリックします。 設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

# **BFD** (Bidirectional Forwarding Detection)

#### L3 Features > BFD

# BFD Settings(BFD 設定)

Bidirectional Forwarding Detection (BFD)の設定、表示を行います。

#### L3 Features > BFD > BFD Settings の順にメニューをクリックして以下の画面を表示します。

BFD Settings			_	_	_
BFD State					
BFD State	<ul> <li>Enabled</li> <li>Disal</li> </ul>	bled			Apply
BFD Interface Settings					
Interface VLAN (1-4094)					Find
Total Entries: 1					
Interface Name	MinTxInt (ms)	MinRxInt (ms)	Multiplier	Slow Time (ms)	
vlan1	500	500	3	2000	Edit
Note: MinTxInt : Desired Minimum TX	Interval, MinRxInt : Required Minir	mum RX Interval	1	1/1  < < 1	> >  Go

図 9-204 BFD Settings 画面

画面に表示される項目:

項目	説明				
BFD State					
BFD State	BFD を「Enabled」(有効)/「Disabled」(無効)に指定します。				
BFD Interface Settings					
Interface VLAN	本設定に使用するインタフェース VLAN(1-4094)を指定します。				

「Apply」をクリックし、設定内容を適用します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Edit」をクリックして、指定エントリの編集を行います。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

対象エントリで「Edit」をクリックすると次の画面が表示します。

Interface Name	MinTxInt (ms)	MinRxInt (ms)	Multiplier	Slow Time (ms)	
vlan1	500	500	3	2000	Apply
Note: MinTxInt : Desired	Minimum TX Interval, MinRxInt : Requi	red Minimum RX Interval		1/1 < < 1 >	>  Go

図 9-205 BFD Settings (Edit) 画面

# 画面に表示される項目:

項目	説明
MinTxInt	BFD パケットを送信する最小間隔値(50-1000 ミリ秒)を指定します。
MinRxInt	システムがサポートする BFD パケットを受信する最小間隔値(50-1000 ミリ秒)を指定します。
Multiplier	BFD 検出時間乗算値(3-99)を指定します。
Slow Time	BFD スロータイム値(1000-3000 ミリ秒)を指定します。

「Apply」をクリックし、設定内容を適用します。

# BFD Neighbor Table (BFD ネイバテーブル)

Bidirectional Forwarding Detection (BFD) ネイバテーブルの表示を行います。

注意 実際の動作速度は設定内容やトラフィックの状況で変わります。実環境に BFD を設定する前にテストを実施することをお勧めします。

L3 Features > BFD > BFD Neighbor Table の順にメニューをクリックして以下の画面を表示します。

Neighbor Table						
al Entries: 2						
Neighbor Address	Interface Name	Local Discriminator	Remote Discriminator	Detect Time (ms)	Status	
11.0.0.1	vlan11	2	0	0	Down	Show Detai
11.0.0.2	vlan11	1	1	1500	Uó	Show Detai

図 9-206 BFD Neighbor Table 画面

「Show Detail」をクリックして、指定エントリの詳細について表示します。 設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Show Detail」をクリックすると、以下の画面が表示されます。

BFD Neighbor Detail		
BFD Neighbor Detail		
Local Diagnostic	No Diagnostic	
Poll Bit	Not Set	
Remote Minimum RX Interval	50 ms	
Remote Minimum TX Interval	500 ms	
Remote Multiplier	3	
Register Protocol	OSPF VRRP SRT	
		Back

図 9-207 BFD Neighbor Detail 画面

「Back」をクリックすると前のページに戻ります。

# ISIS (Intermediate System to Intermediate System) (MI モードのみ)

#### L3 Features > ISIS

Intermediate System to Intermediate System (ISIS) の設定を行います。

# ISIS Global Settings(ISIS グローバル設定)

Intermediate System to Intermediate System (ISIS)の設定、表示を行います。

#### L3 Features > ISIS > ISIS Global Settings の順にメニューをクリックして以下の画面を表示します。

s Global Setti	ngs			_	_		_
S Global Settings							
rea Tag	16 chars					Apply	Find
otal Entries: 1		_		_	_		_
Alea lau							
Area			Edit	NET List	Delete		

図 9-208 ISIS Global Settings 画面

#### 画面に表示される項目:

項目	説明		
Area Tag	ISIS エリアタグ(16 字以内)を指定します。		
 Apply」をクリックし、設定内容を適用します。			
「Find」をクリックして、入力	)した情報に基づく特定のエントリを検出します。		

「NET List」をクリックして、すべてのエントリを表示します。

「Edit」をクリックして、指定エントリの編集を行います。

「Delete」をクリックすると指定のエントリを削除します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

#### 「Edit」をクリックすると、以下の画面が表示されます。

ISIS Router Global Settings						
ISIS Router Global Settings						
Area Tag	Area					
Area Password		Validate 🗸	Authenticate SNP [	Default		
Domain Password		Validate 🗸	Authenticate SNP [	Default		
Hostname Dynamic	Enabled 🗸					
Ignore LSP Errors	Enabled 🗸					
IS Type	Level-1-2					
LSP Generation Interval Level-1(1-120)	5 s	sec 🔄 Default				
LSP Generation Interval Level-2(1-120)	5 s	sec 📃 Default				
LSP Refresh Interval (1-65535)	900 s	sec 📃 Default				
Max Area Addresses (3-254)	3	Default				
Max LSP Lifetime (1-65535)	1200 s	sec 📃 Default				
Metric Style	Narrow 🗸	Level-1-2				
Set Overload Bit	Disabled 🗸					
On Startup (5-86400)	S	sec				
Suppress	None 🗸					
SPF Interval Level-1 (1-120)	10 s	sec 📃 Default				
SPF Interval Level-2 (1-120)	10 s	sec 🔄 Default				
VRF Name		Please Select No V	/RF		Apply	Back

図 9-209 ISIS Global Settings (Edit) 画面

画面に表示される項目:

項目	説明
Area Password	ISIS エリア認証パスワードを指定します。エリアの全スイッチに、非認証のスイッチによるリンクステートデータベー
	スへの不正ルーティング情報の挿入を防止します。パスワードはプレーンテキストに変換され、現時点で唯一の認証
	方法になります。「Authenticate SNP」を指定するとパスワードを「sequence number PDU」(SNP) に挿入します。
	・ Validate - SNP へのパスワード挿入と SNP によるパスワード受信を指定します。
	・ Send Only - SNP へのパスワード挿入のみを指定します。
	「Default」を選択すると初期値を指定します。
Domain Password	ISIS ドメイン認証パスワードを指定します。「Authenticate SNP」を指定するとパスワードを「sequence number
	PDU」(SNP) に挿入します。
	・ Validate - SNP へのパスワード挿入と SNP によるパスワード受信を指定します。
	・ Send Only - SNP へのパスワード挿入のみを指定します。
	、 「Default」を選択すると初期値を指定します。
Hostname Dynamic	ーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーー
-	ングを有効に指定します。
	ダイナミックホスト名メカニズムはネットワーク間の「router-name-to-system-ID」マッピング情報を分配する「Link-
	State Protocol」(LSP) フラッディングを使用します。ネットワークの各ルータはシステム ID ルータ名マッピング情報
	のルーティングテーブルへのインストールを試みます。ルータが既に通知を急に停止したネットワークのダイナミッ
	クネーム Type, Length, Value (TLV) を通知している場合、最後に受信したマッピング情報は最大一時間、ダイナミッ
	クホストテーブルに残り、ネットワーク管理者にネットワークに問題が発生している間、マッピングエントリテーブ
	ルのエントリを表示します。
Ignore LSP Errors	「Ignore LSP Errors」(LSP エラー無視)を「Enabled」(有効)/「Disabled」(無効)に指定します。バッドチェックサ
	ムのリンクステートパケットの無視 (LSPs) に使用されます。ISIS プロトコル定義は受信者から除かれる不正のデータ
	リンクチェックサムの受信 LSP を必要とし、パケットの再起動を実行を引き起こします。しかしネットワークがデー
	タ衝突を起こすリンクの保持や、同時に正しいデータリンクチェックサムの LSP の通達などを実行する場合、大量パ
	ケットの排除や再起動などが繰り返し発生する場合があります。このような状況はネットワークの不動作のレンダリ
	ングを発生させるため、パケットの除外よりも LSP を無視するコマンドを使用します。
IS Type	「IS type」を指定します。ISIS ルーティングプロセスのインスタンスのルーティングレベルの設定に使用されます。
	・ Level1 - レベル 1 ルーティングのみ実行します。スイッチはエリア内の宛先のみ学習します。レベル 2 ルーティン
	グはレベル 1-2 の両ルータで実行されます。
	・ Level-1-2 - レベル 1-2 ルーティングを実行します。
	・ Level-2 - レベル 2 ルーティングのみを実行します。
LSP Generation Interval	LSP 生成間隔レベル1(1-120 秒)を指定します。レベル1エリアのみのリンクステートパケット生成間隔の設定に使
Level-1	用します。ネットワークの不安定期間に、LSP 生成レートの減少に使用します。ルータの CPU 起動と ISIS ネイバへの
	LSP 送信の減少に使用されます。「Default」を選択すると初期値を指定します。
LSP Generation Interval	LSP 生成間隔レベル2(1-120秒)を指定します。レベル2エリアのみのリンクステートパケット生成間隔の設定に使
Level-2	用します。ネットワークの不安定期間に、LSP 生成レートの減少に使用します。ルータの CPU 起動と ISIS ネイバへの
	LSP 送信の減少に使用されます。「Default」を選択すると初期値を指定します。
LSP Refresh Interval	LSP 更新間隔値(1-65535)を指定します。リンクステートパケット再生成の設定を行います。
	ライフタイムが切れる前に LSP は一定期間で更新される必要があります。本項目で設定された値は「Max LSP
	Lifetime」で設定されたパラメータの値よりも少ない必要があります。そうでない場合、LSP は史新前にタイムパワト
	します。LSP ライフタイムの設定ミスは LSP 更新間隔よりも小さい設定値を設定することで、LSP のタイムパワトを防
	ぐ LSP 更新間隔の減少をもたらします。更新間隔を短くすると、リンク使用率は上昇しますかリンクステートテータ
	ベース破損が検出されない時間を減らすことかぐきます。更新間隔を長くすると、更新ハケットのノフッティノクに
	よるリンク使用率を減らすことかできます。  Default」を選択すると初期値を指定します。
Max Area Addresses	最大エリアアドレ人値(3-254)を指定します。追加マニュアルアドレ人の設定により、ISIS エリアサイ人の取天化を
A A L CD L ifatime a	行います。「Default」を選択すると初期値を指定します。   BLICD = ノフタノノは(ACCOD)ませらします。UNAフニートパケットの見まうノフタノノ体を指定します。
Max LSP Lifetime	最大 LSP フイノダイム 個(1-05535)を指定しより。リノソ人ナートハケットの取入フィノダイム 胆を拍走しより。
Matria Chida	Default」を迭折りるこ初期他で拍走します。
Metric Style	アトリツクスダイルを拍走します。IDIDフロで入土成とアトリックスダイル文明で改走します。
	<ul> <li>NdITOW - ロスダイルクトリック TLV を土成します。</li> <li>Mida</li></ul>
	<ul> <li>Wild - 初へダイルクドワワワーLV で土成します。</li> <li>Narrow Transition - 旧フタイルメトロックTIV を生成し、新旧市フタイルメトロックTIV を受け入れます。</li> </ul>
	• Nation Infinition - 新スタイルメトリックTIVを生成し、新旧両スタイルメトリックTIVを受け入れます。
	・ Wide Hallslub AIT スタイルメトリックTIVを生成します。タメトリックスタイルは選択したレベルにたります。
	- Lavel-1-レベル1ルーティングのみ右効に指定します。
	- Level - レ ベル 1/2 ルーティングを有効に指定します。
	- Level - 2 レベル フルーティングのみ右効に指定します。
Set Overload Bit	「Set Overload Bit Iの[Enabled I (有効)/[Disabled I (毎効) に指定します。[non-nseudo I / ード I SP におけるオーバロー
	「ジビットの設定」SISプロセスを強制」ます。通営オーバロードビットの設定はルータに問題が発生した場合に許可さ
	ービットの設定しまう」ロビスを運動します。 通常オーバロート ビットの設定なが デルに向感が先生した場合によりで
	「キャッシュアン」」、「「「「「「「」」」」、「「」」」、「「」」」、「「」」、「」」、「」」
	111711週日本間本が完全します。こうのカインロードビットの設定して、他のカレージが、問題がり日度するようにもす

項目	説明
On Startup	オーバロードビット設定の開始時間(5-86400秒)を指定します。システムスタート時のオーバロードビットの設定
	を行います。オーバロードビットは指定の時間残ります。
Suppress	抑制オプションを指定します。サブシークエントキーワード/キーワードによって識別される、抑制されるプリフィ
	クスタイプを指定します。
	• None - 他の ISIS レベルから、そして通知された他のプロトコルから学習した、如何なる IP プリフィクスを防止し
	ません。
	・ Interlevel - 通知された他の ISIS レベルから学習した IP プリフィクスを防止します。
	• External - 通知された他のプロトコルから学習した IP プリフィクスを防止します。
	・ Both - 他の ISIS レベルから、そして通知された他のプロトコルから学習した、全ての IP プリフィクスを防止します。
SPF Interval Level-1	SPF 間隔レベル 1 値 (1-120 秒) を指定します。レベル 1 エリアでのみの SPF 計算の ISIS スロットルをカスタムします。
	「Default」を選択すると初期値を指定します。
SPF Interval Level-2	SPF 間隔レベル 2 値 (1-120 秒)を指定します。レベル 2 エリアでのみの SPF 計算の ISIS スロットルをカスタムします。
	「Default」を選択すると初期値を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
	「Please Select」で事前に設定済みの VRF を選択することが可能です。「No VRF」で VRF インスタンスを指定しません。

「Apply」をクリックし、設定内容を適用します。

「Back」をクリックすると前のページに戻ります。

「Please Select」をクリックすると、次の画面が表示されます。

al Entries: 1		
	VRF Name	RD
0	VRF1	192.168.70.1.24
		OK

図 9-210 Please Select (VRF) 画面

使用する VRF エントリを選択し、「OK」をクリックします。 設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「NET List」をクリックすると、次の画面が表示されます。

ea Tag: Area	
VET 49.0001.0001.0001.0001.00	Apply Back
Total Entrine: 4	
NET	
49.0001.0001.0001.0001.00	Delete

図 9-211 ISIS Global Settings (NET List) 画面

画面に表示される項目:

項目	説明
NET	NET Network Services Access Point (NSAP) アドレスを指定します。
	「Intermediate System」(IS) は NSAP として知られるアドレスによって識別されます。NSAP は「ISO10589」によって
	指定された 3 つのパートに分割されます。「NET」は最後のバイトが常に「n-selector」そして「zero」となる NSAP です。
	「NET」は 8 から 20 バイト長です。「Multiple NET」はエリアの分割、統合が可能です。 IP ルーティングでのみ実行され、
	「NET」は必ずシステム ID とエリア ID を定義されている必要があります。

「Apply」をクリックし、設定内容を適用します。

「Back」をクリックすると前のページに戻ります。

「Delete」をクリックすると指定のエントリを削除します。

# ISIS Router Settings(ISIS ルータ設定)

Intermediate System to Intermediate System (ISIS) ルータの設定、表示を行います。

L3 Features > ISIS > ISIS Router Settings の順にメニューをクリックして以下の画面を表示します。

ISIS Router Settings					
ISIS Router Settings					
Protocol	IPv4	$\checkmark$			
Area Tag	16 chars				
Adjacency Check	Enabled	$\checkmark$			
Default Information Originate	Disabled	$\checkmark$			
Distance (1-255)		Default			
					Apply
Protocol IPv4	~	Area Tag	16 chars	]	Find
Total Entries: 1					
Area Tag Adjacer	ncy Check	Default Informat	ion Originate	Distance	
Area En	abled	Disabl	ed	150	Summary Address List
					1/1  < < 1 > >  Go

図 9-212 ISIS Router Settings (IPv4) 画面

ISIS Router Settin	ngs				
ISIS Router Settings					
Protocol	IPv6				
Area Tag	16 chars				
Adjacency Check	Enabled	~			
Default Information O	riginate Disabled	$\checkmark$			
Distance (1-254)		Default			
					Apply
Protocol	/6	Area Tag	16 chars		Find
Total Entries: 2					
Area Tag	Adjacency Check	Default Info	rmation Originate	Distance	
1	Enabled	D	isabled	116	Summary Prefix List
2	Enabled	D	isabled	120	Summary Prefix List
					1/1  < < 1 > >  Go

図 9-213 ISIS Router Settings (IPv6) 画面

#### 画面に表示される項目:

項目	説明
Protocol	プロトコル(IPv4/IPv6)を指定します。
Area Tag	ISIS エリアタグ (16 字以内)を指定します。 有効な lp インタフェースにおいてルーティングプロセスタグを指定します。
Adjacency Check	「Adjacency Check」を「Enabled」(有効)/「Disabled」(無効)に指定します。ISIS はハローパケットでの整合性チェッ クの実行と同じプロトコルをサポートするネイバリングルータとの隣接を形成します。本項目はその「Enabled」(有効) /「Disabled」(無効)を確認します。
Default Information	「Default Information Originate」を「Enabled」(有効)/「Disabled」(無効)に指定します。有効にすると、ISIS が
Originate	Level-2 Link-State Packets (LSP) のデフォルトルートの通知を実行します。
Distance	「Distance」を指定します。ISIS ルートの管理ディスタンス(1-255/IPv4、1-254/IPv6)です。

「Apply」をクリックし、設定内容を適用します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Summary Address List」をクリックして、サマリアドレスリストを指定します。

「Summary Prefix List」をクリックして、サマリプリフィクスリストを指定します。

「Summary Address List」をクリックすると、次の画面が表示されます。

Summary Address	Level-2	6 8 1	]	Apply	Back
ODDE ENTRES: 1					
otal Entries: 1	Summary Address	Mask	Level		

図 9-214 ISIS Router Settings (Summary Address List) 画面

#### 画面に表示される項目:

項目	
Summary Address	サマリアドレスとレベルを指定します。ISIS のアドレスアグリゲートを行います。
	複数のサマリ化可能アドレスグループにはレベルを付与することができます。ルートは同様にレベルを付与される他
	のルーティングプロトコルから学習します。サマリを通知するメトリックは指定の全ルートのメトリックで最小です。
	本コマンドではルーティングテーブルのサイズを減少させることができます。本コマンドはまた、リンクステートパ
	ケットとリンクステートデータベースのサイズを減少させることも可能です。サマリ通知は多くのルートに依存して
	いるためネットワークの安定性にも有効です。単一のルートフラップはほとんどの場合、フラップのサマリ通知にな
	りません。サマリアドレスの欠点は、他のルートの場合の方が、より少ない情報で各宛先へ最適なルーティングテー
	ブルを計算できます。
	<ul> <li>Level-1 - レベル1で再配分される唯一のルートを指定のIPアドレスとマスク値でサマリ化します。</li> </ul>
	・ Level-1-2 - エリア内のレベル 1 ルートがレベル 2ISIS に到達可能なステータスを通知され、レベル 1 と 2 ISIS で再
	配分されるルートをサマリ化します。
	・ Level-2 - レベル1ルーティングによって学習するルートがレベル2がIPアドレスとマスク値を設定されたバック
	ボーンとともにサマリ化されます。

「Apply」をクリックし、設定内容を適用します。

「Back」をクリックすると前のページに戻ります。

「Delete」をクリックすると指定のエントリを削除します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

#### 「Summary Prefix List」をクリックすると、次の画面が表示されます。

Summary Prefix	List		
Area Tag: 1			
Summary Prefix	Level-2 1000:1::/64		Apply Back
Total Entries: 1			
	Summary Prefix	Level	
	2015::/64	level-2	Delete
			1/1 K < 1 > X Go

図 9-215 ISIS Router Settings (Summary Prefix List) 画面

## 画面に表示される項目:

項目	説明
Summary Prefix	レベルを選択しサマリプリフィクスを入力します。
	<ul> <li>Level-1 - レベル1で再配分される唯一のルートを指定のIPアドレスとマスク値でサマリ化します。</li> </ul>
	・ Level-1-2 - エリア内のレベル 1 ルートがレベル 2ISIS に到達可能なステータスを通知され、レベル 1 と 2 ISIS で再
	配分されるルートをサマリ化します。
	・ Level-2 - レベル1ルーティングによって学習するルートがレベル2が IP アドレスとマスク値を設定されたバック
	ボーンとともにサマリ化されます。

「Apply」をクリックし、設定内容を適用します。

「Back」をクリックすると前のページに戻ります。

「Delete」をクリックすると指定のエントリを削除します。

# ISIS Interface Settings(ISIS インタフェース設定)

Intermediate System to Intermediate System (ISIS) インタフェースの設定、表示を行います。

L3 Features > ISIS > ISIS Interface Settings の順にメニューをクリックして以下の画面を表示します。

ISIS Interface Se	ettings			
- ISIS Interface Setting	gs			
Interface VLAN (1-4	094)	● IPv4 ◯ IPv	r6 Area Tag	16 chars Apply
Interface VLAN (1-4	094)			Find
Total Entries: 1				
Interface	Link Status	Line Protocol	Routing Protocol	
vlan1	Up	Up	IS-IS (Area)	Edit Delete
				1/1 < < 1 > > Go

図 9-216 ISIS Interface Settings 画面

画面に表示される項目	:

項目	説明
Interface VLAN	本設定に使用するインタフェース VLAN(1-4094)を指定します。
IPv4	インタフェースにおいて IPv4 の ISIS ルーティングプロトコル有効に指定します。
IPv6	インタフェースにおいて IPv6 の ISIS ルーティングプロトコル有効に指定します。
Area Tag	ISIS エリアタグ(16 字以内)を指定します。
- · · · · · · · · · · · · · · · · · · ·	

「Apply」をクリックし、設定内容を適用します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Edit」をクリックして、指定エントリの編集を行います。

「Delete」をクリックすると指定のエントリを削除します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

#### 「Edit」をクリックすると、以下の画面が表示されます。

Interface Name	vlan1		Link Status	Up	
Line protocol	Up		Routing Protocol	IS-IS (1)	
Network Type	Broadcast		Local Circuit ID	0x1	
Extended Local circuit ID	0x1		Local SNPA	f07d.6836.3000	
IP Interface Address	10.90.90.90		Circuit Type	Level-1-2	
Hello Padding	Enabled 🔽	]	Mesh Group		Block Default
Retransmit Interval (1-65535)	5	sec 🗌 Default	Network Point-to-Point	Disabled 🔽	]
CSNP Interval Level-1 (1-65535)	10	sec 🗌 Default	CSNP Interval Level-2 (1-65535)	10	sec 🗌 Default
Hello Interval Level-1 (1-65535)	10	sec 🗌 Default	Hello Interval Level-2 (1-65535)	10	sec 🗌 Default
Hello Multiplier Level-1 (2-100)	3	Default	Hello Multiplier Level-2 (2-100)	3	Default
Metric Level-1 (1-63)	10	Default	Metric Level-2 (1-63)	10	Default
Password Level-1		Default	Password Level-2		Default
Priority Level-1 (0-127)	64	Default	Priority Level-2 (0-127)	64	Default
Vide Metric Level-1 (1-16777214)	10	Default	Wide Metric Level-2 (1-16777214)	10	Default
Level-1 Circuit ID	0000.0000.0000.00		Level-2 Circuit ID	0000.0000.0000.00	
Number of Active Level-1 Adjacencies	0		Number of Active Level-2 Adjacencies	0	
Next IS-IS LAN Level-1 Hello	0 millisecond		Next IS-IS LAN Level-2 Hello	0 millisecond	

図 9-217 ISIS Interface Settings (Edit) 画面

画面に表示される項目:	
項目	説明
Circuit Type	サーキットタイプを指定します。
	<ul> <li>Level-1 - レベル1隣接のみ指定します。</li> </ul>
	・ Level-1-2 - レベル 1/2 隣接を指定します。
	・ Level-2 - レベル 2 隣接を指定します。
Hello Padding	「Hello Padding」を「Enabled」(有効)/「Disabled」(無効)に指定します。ISIS ハローパケットは「maximum
	transmission unit」(MTU) サイズまで大きくされます。フル MTU までの ISIS ハローパケットの巨大化は大きいフレー
	ムの送信問題などを発生させるエラーの早期検出や、隣接インタフェースでの MTU のミスマッチなどを発生させるエ
	ラーも検出などに有効です。両インタフェースの MTU が同じである場合において、ネットワーク帯域の消費を避ける
	ために本機能を無効化します。
Mesh Group	
	point-to-point ネットワーク間の「Link-State Packet」(LSP) フラッディングの最適化に使用します。
	「Block」でインタフェースでのLSPフラッディングの発生はありません。「Default」を選択すると初期値を指定します。
Retransmit Interval	「Retransmit Interval」(再送信問隔)の値(1-65533 秒)を指定します。全計な再送信を減らすため、再送信問隔は控
	これにおいていたいない。「そこに同帰」のに(105555)」を目足しなり。示いな号之にを減りすため、号之に同帰るエースめにお完することを堆将します。問隠値は予想されるルーク問の往復の遅れよりも大きい値である必要があります
Notwork Point to Point	へのに指定することで推奨します。間隔値はすぶとれてのハーチ間の圧後の遅れますの人とい値しのる必要がのサます。
	「Network Point-to-Point」を「Linabled」(有効)/「Disabled」(無効)に指定しより。 秋日 ISIS ルーナインツノロド コルた体田」 スプロードキャストリンクの伴わりに「ポイントトゥポイント」のとうにプロードキャストメディスを
	コルを使用してフロードキャストリングの代わりに「ホイントトリホイント」のようにフロードキャストメナイナを
	使用する2 200イットワーク機器を成形させます。
CSINP INTERVAL LEVEL- I	「RVPFICSNP」の送信间隔(I-05055 秒)の指定をします。
	例先ルータにのみ有効です。「Default」を迭折すると初期値を指定します。
CSINP Interval Level-2	「level-2 CSNP」の送信間隔(I-65535 秒)の指定をします。
	例先ルータにのみ有効です。「Default」を迭折すると初期値を指定します。
Hello Interval Level- I	「IEVEFT ハローハケット」の送信間隔(I-65535 秒)の指定をします。
	例先ルータにのみ有効です。「Default」を迭折すると初期値を指定します。
Hello Interval Level-2	「level-2 ハローハケット」の达信间隔(l-65535 秒)の指定をします。
	死先ルーダにのみ有効ぐす。「Default」を選択すると初期値を指定します。
Hello Multiplier Level- I	Hello Multiplier」の値(2-100)を入力します。ハローマルナフライヤ時間は ISIS ハローハケットのハローインター
	ハルホールドダイムと同じぐす。小さいハローマルナノフイヤは早い収束を取得します。ルーテインクとしては不安
	定です。ネットリークの安定性か必要な場合は、ハローマルチフライヤ時間は長い万か埋想です。  Default」を選択 
Hello Multiplier Level-2	Hello Multiplier」の値(2-100)を入力します。   Default」を選択すると初期値を指定します。
Metric Level-1	ISIS メトリック値を指定します。他の宛先へのリンクネットリークや他の宛先のネットリーク内の各リンクのコスト
	計算に使用されより。メトリックは SPF レベル I ルーティングの唯一の SPF 計算です。
	Default」を選択すると初期値を指定します。
Metric Level-2	ISISメトリック値を指定します。他の宛先へのリンクネットワークや他の宛先のネットワーク内の各リンクのコスト
	計算に使用されます。メトリックは SPF レベル 2 ルーティングの唯一の SPF 計算です。
	Default」を選択すると初期値を指定します。
Password Level-1	レベル1ルーティンク使用時の ISIS バスワード (16 字以内) を指定します。本ルータと形成する隣接からの非認証ルー
	タの防止を有効にし、ネットワークを侵入者から守ります。バスワードはプレーンテキストとして交換されるため、
	セキュリティに制限があります。「Default」を選択すると初期値を指定します。
Password Level-2	レベル2ルーティンク使用時の ISIS バスワード (16 字以内)を指定します。本ルータと形成する隣接からの非認証ルー
	タの防止を有効にし、ネットリークを侵入者から守ります。バスリードはフレーンテキストとして父換されるため、
	セギュリティに制限があります。「Default」を選択すると初期値を指定します。
Priority Level-1	レベル 1 ルーティンク使用時の優先値 (0-127) を指定します。優先値は LAN のどのルータが DIS になるかを決めます。
	優先値はハローバケットで通知されます。最高の優先値を持つデバイスが DIS になります。ISIS では宛先ルータのバッ
	クアッフはありません。0 に近い値の優先値設定はシステムか DIS になるチャンスは低いですか、完全に防げるわけ
	ではありません。システムか高い優先値を持つていると現在の DIS からその座を引き継ぎます。優先値か同値の場合、
	MACアドレスの値の大きさで、決まります。「Default」を選択すると初期値を指定します。
Priority Level-2	レベル 2 ルーティンク使用時の優先値 (0-127) を指定します。優先値は LAN のどのルータが DIS になるかを決めます。
	優先値はハローバケットで通知されます。最高の優先値を持つデバイスが DIS になります。ISIS では宛先ルータのバッ
	クアッフはありません。0 に近い値の優先値設定はシステムか DIS になるチャンスは低いですか、完全に防げるわけ
	(ではめりません。ン人テムか局い優先値を狩つていると現在の DIS からその座を引き継ぎます。優先値が同値の場合、
	MACアドレスの値の大ささぐ、決まります。「Detault」を選択すると初期値を指定します。
Wide Metric Level-1	リンクにアサインする広いメトリック値(1-16777214)を指定し、レベル1ルーティングの他の宛先へのネットワー
	ク内のリンク経田の他のルータからのコストを計算します。
	Delduit」を迭折9 ると初期他を指定しよ9。
Wide Metric Level-2	リンクにアサインする広いメトリック値(1-16777214)を指定し、レベル 2 ルーティングの他の宛先へのネットワー
	ク内のリンク経田の他のルータからのコストを計算します。
	Derault」を選択すると初期値を指定します。

「Apply」をクリックし、設定内容を適用します。

「Back」をクリックすると前のページに戻ります。

# ISIS Redistribute Settings(ISIS 再配分設定)

Intermediate System to Intermediate System (ISIS) 再分配の設定、表示を行います。

L3 Features > ISIS > ISIS Redistribute Settings の順にメニューをクリックして以下の画面を表示します。

ISIS Redistribute Settin	ngs	_			
ISIS Redistribute Settings					
Protocol	IPv4	]			
Area Tag	16 chars	]			
Redistribute Type	Connected 🗸	]			
Metric (1-63)		]			
Metric Type	None 🗸	]			
Route Map	32 chars	]			
Level	Level-2 Only			Apply	Delete
Protocol IPv4	<b>v</b>	Area Tag	16 chars		Find
Total Entries: 1					
Area Tag	Protocol	Metric	Metric Type	Route Map	Level
Area	connected	10	internal	Route-Map	level-2
				1/1 < 1	> >  Go

図 9-218 ISIS Redistribute Settings 画面

#### 画面に表示される項目:

項目	説明
Protocol	プロトコル(IPv4/IPv6)を指定します。
Area Tag	ISIS エリアタグ(16 字以内)を指定します。
Redistribute Type	プルダウンメニューを使用して再分配のタイプを選択します。
	・ Connected - ISIS への接続ルートに再分配します。
	・ Static - ISIS へのスタティックルートに再分配します。
	・ RIP - ISIS への RIP ルートに再分配します。
	・ OSPF - ISIS への OSPF ルートに再分配します。
	・ ISIS - ISIS への ISIS ルートに再分配します。
Metric	再分配ルートのメトリック(1-63)を指定します。
Metric Type	メトリックの種類を指定します。「None」「Internal」「External」から指定します。
Route Map	ルートマップを(32 字以内)指定します。
Level	ルーティングレベルを指定します。「Level-1」「Level-1-2」「Level-2 Only」から指定します。

「Apply」をクリックし、設定内容を適用します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Delete」をクリックすると指定のエントリを削除します。

# ISIS Redistribute ISIS Settings(ISIS 再配分 ISIS 設定)

Intermediate System to Intermediate System (ISIS) 再分配 ISIS 設定、表示を行います。レベル1から2(レベル2から1)の ISIS ルート再配分に使用します。

L3 Features > ISIS > ISIS Redistribute ISIS Settings の順にメニューをクリックして以下の画面を表示します。

ISIS Redistribute ISIS Setting	5	_		
ISIS Redistribute ISIS Settings				
Protocol	IPv4			
Area Tag	16 chars			
From	Level-1			
Into	Level-2			
Distribute List	32 chars			Apply
Protocol IPv4	•	Area Tag	16 chars	Find
Total Entries: 1				
Area Tag	From	Into	Distribute List	
Area	Level-1	Level-2	Distribute	Delete
				1/1 < < 1 > > Go

図 9-219 ISIS Redistribute ISIS Settings 画面

#### 画面に表示される項目:

項目	説明
Protocol	プロトコル(IPv4/IPv6)を指定します。
Area Tag	ISIS エリアタグ(16 字以内)を指定します。
From	再配分を行う元のレベルを指定します。「Level-1」「Level-2」から指定します。
Into	再配分を行う先のレベルを指定します。「Level-1」「Level-2」から指定します。
Distribute List	分配リスト(32 字以内)を指定します。

「Apply」をクリックし、設定内容を適用します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Delete」をクリックすると指定のエントリを削除します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

# ISIS Route Table(ISIS ルートテーブル)

Intermediate System to Intermediate System (ISIS) ルートテーブル ISIS を表示します。

L3 Features > ISIS > ISIS Route Table の順にメニューをクリックして以下の画面を表示します。

ISIS Route Table	_				
ISIS Route Table					
Protocol IPv4	~	Area Tag 16	chars		Find
Total Entries: 1					
Area Tag	Туре	Destination	Metric	Next-Hop	Interface
Area					
				1/1 <	< 1 > >  Go
Note: Codes: C - connected, E -	external, L1 - IS-I	S level-1, L2 - IS-IS level-2, ia - IS-IS inte	er area, D - discard, e -	external metric	

図 9-220 ISIS Route Table 画面

画面に表示される項目:
-------------

項目	説明
Protocol	プロトコル(IPv4/IPv6)を指定します。
Area Tag	ISIS エリアタグ(16 字以内)を指定します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

# ISIS Database(ISIS データベース)

Intermediate System to Intermediate System (ISIS) データベースを表示します。

L3 Features > ISIS > ISIS Database の順にメニューをクリックして以下の画面を表示します。

Database -							
a Tag 1	6 chars		Level Level-1	LSP ID	0001.0001.0001.00-00	D	Find
tal Entries: 2	2		5.0 				
Area Tag	Level	LSP ID	LSP Seq Num	LSP Checksum	LSP Holdtime	ATT/P/OL	
(2010)	level-1	Switch.00-00	* 0x0000009	0xF844	1152	0/0/0	Show Detail
(null)	level-2	Switch 00-00	* 0x000000D	0x4165	521	0/0/0	Show Detail

図 9-221 ISIS Database 画面

画面に表示される項目:

項目	説明
Area Tag	ISIS エリアタグ(16 字以内)を指定します。
Level	ルーティングレベルを指定します。「Level-1」「Level-2」から指定します。
LSP ID	表示する LSP ID を指定します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。 設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。 「Show Detail」をクリックして、指定エントリの詳細について表示します。

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

ISIS Database Detail		
Auth	Length: 8	
Area Address	49.0001	
NLPID	0xCC 0x8E	
Hostname	Switch	
IP Address	107.100.0.1	
IPv6 Address	2107:100:A::1	
Metric	10 IP 107.100.0.0 255.255.0.0	
Metric	10 IPv6 2107:100:A::/64	
Metric	10 IPv6 1234::/64	

図 9-222 ISIS Database (Show Detail) 画面

「Back」をクリックすると前のページに戻ります。

# ISIS Topology(ISIS トポロジ)

Intermediate System への ISIS パスを表示します。

L3 Features > ISIS > ISIS Topology の順にメニューをクリックして以下の画面を表示します。



図 9-223 ISIS Topology 画面

画面に表示される項目:

項目	説明
Protocol	プロトコル(IPv4/IPv6)を指定します。
Area Tag	ISIS エリアタグ(16 字以内)を指定します。
Level	ルーティングレベルを指定します。「Level-1」「Level-2」から指定します。
$\begin{bmatrix} Find \mid & f \neq f \\ & f \neq f \neq f \\ & f \neq f$	コーた情報に基づく特定のエントリを検出します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

## ISIS Hostname (ISIS ホスト名)

ISISの「ルータ名 - システム ID」マッピングテーブルエントリを表示します。

L3 Features > ISIS > ISIS Hostname の順にメニューをクリックして以下の画面を表示します。

ostname			
Entries: 0			
Lovel	System ID	Dynamic Hostname	Area Tag

図 9-224 ISIS Hostname 画面

# ISIS Neighbors(ISIS ネイバ)

Intermediate System to Intermediate System (ISIS) ネイバ情報を表示します。 L3 Features > ISIS > ISIS Neighbors の順にメニューをクリックして以下の画面を表示します。

eighbors							
Entries: 2							
Area Tag	System ID	Interface	State	Туре	Priority	Circuit ID	
0000600	DXS3600	vlan11	Up	L1	64	DXS3600.01	Show Detail
DGS3630	DXS3600	vlan11	Up	L2	64	DXS3600.01	Show Detail

図 9-225 ISIS Neighbors 画面

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。 「Show Detail」をクリックして、指定エントリの詳細について表示します。

「Show Detail」をクリックすると、以下の画面が表示されます。

SIS Neighbors Detail	
Area Tag	DGS3630
Uptime	0D:18H:5M:5S
Level 1 Protocol Supported	IPv4, IPv6
Level 2 Protocol Supported	IPv4, IPv6
Area Address(es)	49.0001
IP Address(es)	11.0.0.2
IPv6 Address(es)	FE80::206:28FF:FED8:FEAC

図 9-226 ISIS Neighbors (Show Detail) 画面

# IP Route Filter (IP ルートフィルタ)

IP プレフィックスリスト、ルートマップの作成を行います。

# IP Prefix List (IP プレフィックスリスト設定) (EI/MI モードのみ)

IP プレフィックスリストを作成します。

# L3 Features > IP Route Filter > IP Prefix List の順にメニューをクリックして以下の画面を表示します。

IP Prefix List List Name 32 chars Direction Permit ▼ Sequence ID (1-65535)   IP Network Address 2015:2/64 GE (1-32) LE (1-32) LIST Name 32 chars Clear Find
List Name       32 chars         Direction       Permit         Sequence ID (1-65535)         ● IP Network Address         ● IP Network IP Network         ● IP Network IP Network         ● IP Network IP Network         ● IP Network         ● IP Network         ● IP Network
Direction     Permit       Sequence ID (1-65535)          ● IP Network Address           ● IP Network           ● IP Network           ■ IP Network           ■ IP Network           ■ IP Network           ■
Sequence ID (1-65535)
IP Network Address
O         IPv6 Network Address         2015::2/64           GE (1-32)
GE (1-32) LE (1-32) LE (1-32) List Name 32 chars Clear Find
LE (1-32) Apply List Name 32 chars Clear Find
List Name 32 chars Clear Find
Total Entries: 1 Clear IP All Clear IPv6 All
List Name Count Direction Sequence ID Network Address GE LE Hit Count Description
List 1 Permit 5 192.168.64.0/21 0 Edit Clear Delete Clear
1/1 < 1 > > Go

図 9-227 IP Prefix List 画面

#### 画面に表示される項目:

項目	説明
List Name	プレフィックスリスト(32 字以内)を識別する名称を入力します。
Direction	プルダウンメニューを使用して、指定ネットワークを「Permit」(許可)または「Deny」(拒否) します。
Sequence ID (1-65535)	ルールエントリのシーケンス番号を指定します。
IP Network Address	IPv4 ネットワークアドレスを入力します。
IPv6 Network Address	IPv6 ネットワークアドレスを入力します。
GE (1-32/IPv4_1-128/IPv6)	一致する最小プレフィックス長を入力します。
LE (1-32/IPv4_1-128/IPv6)	一致する最大プレフィックス長を入力します。

「Apply」をクリックし、設定内容を適用します。

「Clear」をクリックすると入力したエントリをクリアします。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

「Delete」ボタンをクリックして、指定エントリを削除します。

「Edit」をクリックして、指定エントリの編集を行います。

「Clear IP All」をクリックすると入力した IP エントリを全てクリアします。

「Clear IPv6 All」をクリックすると入力した IPv6 エントリを全てクリアします。

# Route Map (ルートマップ設定)

ルートマップの作成、またはルートマップへのシーケンスの追加、およびシーケンスの削除を行います。

L3 Features > IP Route Filter > Route Map の順にメニューをクリックして以下の画面を表示します。

loute Map					
Route Map					
Route Map Name	16 chars				
Direction	Permit 🗸				
Sequence ID (1-65535)					Apply
Route Map Name	16 chars				Find
Total Entries: 1					
Route Map Name	Direction	Sequence ID	Match Clauses	Set Clauses	
Route-Map	Permit	1	Edit	Edit	Delete
			he da Sha d	1/1 < <	1 > >  Go

図 9-228 Route Map 画面

以下の項目を使用して設定を行います。

項目	説明
Route Map Name	ルートマップ名を入力します。
Direction	プルダウンメニューを使用して、一致するルールを「Permit」(許可)または「Deny」(拒否)します。
Sequence ID (1-65535)	ルールエントリのシーケンス番号を指定します。

「Apply」をクリックし、設定内容を適用します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

「Delete」ボタンをクリックして、指定エントリを削除します。

「Edit」をクリックして、指定エントリの編集を行います。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

#### 「Match Clause」の編集

「Match Clauses」下の「Edit」ボタンをクリックすると、以下の画面が表示されます。

Action	Add 💙			
Interface Name				
IP Address Prefix List	32 chars	O IP Address ACL	32 chars	
IPv6 Address Prefix List	32 chars	O IPv6 Address ACL	32 chars	
IP Next Hop Prefix List	32 chars	O IP Next Hop ACL	32 chars	
IPv6 Next Hop Prefix List	32 chars	O IPv6 Next Hop ACL	32 chars	
AS Path	16 chars			
Community	16 chars			
) Extcommunity	16 chars			
Route Source	32 chars			
Metric (0-4294967294)				
Route Type	Internal 🗸			Apply
	_	Route Map Detail Informa	tion	_
route-type	intern	al		

図 9-229 Route Map Settings - Match Clauses 画面

画面に表示される項目:

項目	説明
Action	プルダウンメニューを使用して、シーケンスエントリを「Add」(追加)または「Delete」(削除)します。
Interface Name	インタフェース名を指定します。外部インタフェースにマッチするルートの条件を定義します。
IP Address Prefix List	IP プレフィックスリスト(32 字以内)を指定します。本リストにマッチするルートの条件を定義します。
IP Address ACL	IP ACL リスト(32 字以内)を指定します。本リストにマッチするルートの条件を定義します。
IPv6 Address Prefix List	IPv6 プレフィックスリスト(32 字以内)を指定します。本リストにマッチするルートの条件を定義します。
IPv6 Address ACL	IPv6 ACL リスト(32 字以内)を指定します。本リストにマッチするルートの条件を定義します。

項目	説明		
IP Next Hop Prefix List	IP ネクストホッププレフィクスリスト(32 字以内)を指定します。本リストにマッチするルートの条件を定義します。		
IP Next Hop ACL	<sup>,</sup> ネクストホップ ACL リスト(32 字以内)を指定します。本リストにマッチするルートの条件を定義します。		
IPv6 Next Hop Prefix List			
IPv6 Next Hop ACL	IPv6 ネクストホップ ACL リスト(32 字以内)を指定します。本リストにマッチするルートの条件を定義します。		
AS Path	IP/IPv6 アクセスリスト名(16 字以内)を指定します。本リストにマッチするルートの条件を定義します。		
Community	スタンダード / エクステンデッド IPv4/IPv6 アクセスリスト名(16 字以内)を指定します。本リストにマッチするルー		
	トのコミュニティ条件を定義します。		
Extcommunity	スタンダード / エクステンデッド IPv4/IPv6 アクセスリスト名(16 字以内)を指定します。本リストにマッチするルー		
	トのエクステンデッドコミュニティ条件を定義します。		
Route Source	スタンダード / エクステンデッド IPv4/IPv6 アクセスリスト名(32 字以内)を指定します。本リストにマッチするルー		
	トソースの条件を定義します。		
Metric	ルートのメトリック値(0-4294967294)を指定します。		
Route Type	ルートタイプを指定します。		
	・ Internal - OSPF AS-internal ルートを指定します。		
	・ External - Ext Type1 と Ext Type2 ルートを含む OSPF AS-external ルートを指定します。		
	・ External Type1 - OSPF AS-external type-1 ルートを指定します。		
	・ External Type2 - OSPF AS-external type-2 ルートを指定します。		

「Apply」ボタンをクリックして行った変更を適用します。

「Back」をボタンをクリックして前のページに戻ります。

## 「Set Clauses」の編集

「Set Clauses」の下の「Edit」ボタンをクリックすると、以下の画面が表示されます。

Route Map					
Route Map: route, Permit, Sequence	ce 1 Set Clauses				
Action IP Default Next Hop IP Next Hop IPv6 Default Next Hop IPv6 Next Hop	Add IP Address 2011::1 IPv6 Address	2015::1			
O Community	Community String	ASN:NN			
IPv6 Precedence IPv6 Precedence	Routine (0)	Additive	O Dampening Half Life Time (1-45)		min
O Metric (0-4294967294)			Reuse Value (1-20000)		
O Metric Type	Type 1 💙		Suppress Value (1-20000)		
Origin	EGP 💌		Max Suppress Time (1-255)		min
O Weight (0-65535)			Unreachable Route's Half Life (1-45)		min
O AS Path	e.g.: 100, 200, 300				Apply
	_	Pouto Map Dr	stail Information	_	_
metric-type	tv	ne-1			
meancrype	ty	PO-1			Back

図 9-230 Route Map Settings - Set Clauses 画面

画面に表示される項目	:
------------	---

項目	説明
Action	プルダウンメニューを使用して、シーケンスエントリを「Add」(追加)または「Delete」(削除)します。
IP Default Next Hop	パケットのルートに使用するデフォルトのネクストホップ IP アドレスを指定します。本機能は複数のデフォルトネク
	ストホップルータの設定に使用されます。デフォルトネクストホップが既に設定済みの場合、後から設定したデフォ
	ルトネクストホップはデフォルトネクストホップリストに追加されます。最初のデフォルトネクストホップルータが
	ダウンすると、次のデフォルトネクストホップルータがパケットのルートを開始します。最大 16 までのデフォルトネ
	クストホップ IP アドレスが入力できます。
IP Next Hop	ネクストホップ属性を設定します。プルダウンメニューを使用して「IP Address」「Peer Address」および「Recursive」
	を選択します。
	・ IP Address - 設定する IP アドレス。
	• Peer Address - これはイングレスとイーグレス両方に有効です。イングレス方向では、ネクストホップが
	Neighbor ピアアドレスに設定されます。イーグレス方向では、パケットのルートに関連するネクストホップがロー
	カルルータ ID アドレスになります。
	<ul> <li>Recursive - ネクストホップルータとして繰り返し使用する IP アドレスを指定します。</li> </ul>

項目	説明
IPv6 Default Next Hop	パケットのルートに使用するデフォルトのネクストホップ IPv6 アドレスを指定します。本機能は複数のデフォルトネ
	クストホップルータの設定に使用されます。デフォルトネクストホップが既に設定済みの場合、後から設定したデフォ
	ルトネクストホップはデフォルトネクストホップリストに追加されます。最初のデフォルトネクストホップルータが
	ダウンすると、次のデフォルトネクストホップルータがパケットのルートを開始します。最大 16 つまでのデフォルト
	ネクストホップ IPv6 アドレスが入力できます。
IPv6 Next Hop	IPv6 ネクストホップ属性を設定します。ルートマップシーケンスの条件の照合にパスするパケットをルートするネク
	ストホップルータを指定します。
	・ IP Address - パケットをルートするネクストホップ IPv6 アドレスを指定します。
	<ul> <li>Recursive - ネクストホップルータとして繰り返し使用する IPv6 アドレスを指定します。</li> </ul>
Community	使用するコミュニティ、またはルートのオリジナルのコミュニティに追加されるコミュニティを指定します。
,	・ Community String - コミュニティは 4 バイト長 (AS 番号用に 2 バイト、ネットワーク番号用に 2 バイト ) です。
	この値は「:   (コロン)によって区切られた2バイトの番号2つによって設定されています。両方の番号の範囲は
	1-65535です。コミュニティ設定は、「」(カンマ)で区切ることによって複数のコミュニティで形成されます。コミュ
	ニティストリングの例は 200:1024, 300:1025, 400:1026 です。
	<ul> <li>Internet - このコミュニティを持つルートをすべてのピア(内部または外部)に送信します。</li> </ul>
	・ No Export - このコミュニティを持つルートはコンフェデレーション内の同じ AS か別のサブ AS にあるピアに送信
	されますが、外部の BGP(eBGP) ピアには送信されません。
	<ul> <li>No Advertise - このコミュニティを持つルートはどんなピア(内部または外部)にも通知されません。</li> </ul>
	・ Local AS - このコミュニティを持つルートは同じ AS のピアに送信されますが、同じコンフェデレーション内の別
	のサブASにあるピアと外部のピアには送信されません。
	<ul> <li>Additive - このキーワードを指定すると、指定したコミュニティストリングをオリジナルのコミュニティストリン</li> </ul>
	グに追加します。指定しないと、指定したコミュニティストリングはオリジナルのコミュニティストリングを置
	き換えます。
IP Precedence	P 優先オプションを指定します。「Routine」「Priority」「Immediate」「Flash」「Flash Override」「Critical」「Internet」
	「Network」から指定します。IP ヘッダの優先値を設定します。ポリシールーティングが IPv4 パケットを含む場合有
	効になる機能です。
IPv6 Precedence	Pv6 優先オプションを指定します。「Routine」「Priority」「Immediate」「Flash」「Flash Override」「Critical」「Internet」
	「Network」から指定します。IPv6 ヘッダの優先値を設定します。ポリシールーティングが IPv6 パケットを含む場合
	有効になる機能です。
Metric (0-4294967294)	
	ルートに関連するメトリックを送信しません。BGP ルートがメトリックを持つルートを受信すると、このメトリック
	はベストパス選択に使用されます。これは、ルートのイングレス設定であるメトリックによって上書きされます。受
	信ルートがメトリックが設定したメトリック属性またはメトリックイングレスのいずれかを持っていると、デフォル
	トメトリック「0」がベストパス選択のためにルートに関連付けられます。med-missing-as-worst がルータに有効に
	「たると、「infinite」(無限)の値がルートに関連付けられます。これはイングレスとイーグレス両方に有効です。
Metric Type	編集に使用するメトリックタイプを指定します。
	• Type-1 - OSPF エクスターナルタイプ1メトリックを指定します。
	・ Type-2 - OSPF エクスターナルタイプ 2 メトリックを指定します。
Origin	レートの開始失を入力します。それは以下の 3 つの値 (EGP   IGP または incomplete) の 1 つです。
	・ IGP - [Interior Gateway Protocol」 (IGP) をプレフィクスの由来とする設定です
	・ FGP - [Exterior Gateway Protocol」 (FGP) をプレフィクスの由来とする設定です。
	・ Incomplete - 不明たソースをプレフィクスの由来とする設定です。
Weight (0-65535)	→ medinplete 「「別な」、スピノレノイノスの出来とする認定とす。
	「
	したって設定されたいと 別の BGP ピアを通して学習されたルートは デフォルトの重み付けのを持ちます ローカル
	ルートの重み付けは通堂 32768 です。これはイングレスにだけ有効です。
AS Path	AS リストを最初に付加するのに使用される AS パスリストを指定します。
Dampening	ダンプニングの値を指定します。5つのアイテムを指定可能です。
Dampening	<ul> <li>Half Life Time - ペナルティとして到達可能ルートが半分に減らされるハーフライフ時間値 (1-45/分) を指定します。</li> </ul>
	· Reuse Value - Edentia (0-20000) $k$
	<ul> <li>Suppress Value - 圧縮値 (0-20000) を指定します。本値とりルートのペナルティ値が高い提合 ルートけに続けれています。</li> </ul>
	<ul> <li>Suppress value 圧相値 (0 20000) を目在します。本値の ワル 「ひアマアルアイ 値が同い 物ロマル 「下は圧相 されより。</li> <li>Mavimum Suppress Time - 圧縮されるルートの是十圧線時間値 (1_255) たビデト ます</li> </ul>
	Inreachable Route's Half Life - ペナルティント ア不達ルートが半分に演にたわスハーフライフ時間値(1 45/公)
	- Officaciable Noules Hall Life ヽフ /レ / 4 として小庄/レートが十万に成りされるハーノノ4 ノ吋间値(I-43/ 刀) たと史」ます
L	2.1日だしより。

「Apply」ボタンをクリックして行った変更を適用します。

「Back」をボタンをクリックして前のページに戻ります。

# Policy Route(ポリシールート設定)

ポリシーベースルーティングの設定、表示を行います。

L3 Features > Policy Route の順にメニューをクリックし、以下の画面を表示します。

Policy Route				
Type IP Policy V				
Total Entries: 1				
Interface Name Route Map				
vlan1 Edit				
111 K < 1 > X Go				

図 9-231 Policy Route 画面

画面に表示される項目:

項目	説明
Туре	ポリシールートタイプを指定します。「IP Policy」「IPv6 Policy」から指定します。

「Edit」をクリックして、指定エントリの編集を行います。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

#### エントリの編集

ポリシールートの編集をするためには、「Edit」ボタンをクリックして以下の画面を表示します。

Policy Route		
Policy Route Type IP Policy		
Total Entries: 1		
Interface Name	Route Map	
vlan1		Apply
		1/1 < < 1 > > Go

図 9-232 Policy Route Settings (Edit) 画面

画面に表示される項目:

項目	説明
Route Map	ポリシールートマップ名を入力します。

項目を編集し、エントリの「Apply」ボタンをクリックします。

# VRRP (VRRP 設定)

VRRP(Virtual Routing Redundancy Protocol)は、LAN上のVRRPルータの1つに仮想ルータとしての役割を動的に割り当てる機能です。VRRPルータのうち、仮想ルータと対向するIPアドレスの制御を行うものをマスタルータと呼び、このルータが本IPアドレス向けのパケットを送出します。また、エンドホストはLAN上の仮想ルータのIPアドレスをデフォルトのファーストホップとして使用できます。VRRP機能を使用して、管理者はすべてのエンドホストにダイナミックルーティングやルート検出プロトコルの設定を行わなくても、デフォルトパスコストを取得することができます。

LAN 上に静的に設定されたデフォルトルートは、障害発生箇所となる傾向があります。VRRP 機能はこの障害を回避するために、選出プロトコルを 使用して LAN 上の VRRP ルータの1つに仮想ルータとしての役割を割り当てるよう設計されています。仮想ルータがダウンすると、選出プロトコル が優先度の最も高い仮想ルータを選び、LAN 上のマスタルータに任命します。これによりダウンした箇所に関係なく、リンクとコネクションはその 状態を保つことができます。

VRRP では、1 台の物理的ルータの代わりに、物理的ルータのグループから構成される仮想ルータを導入します。仮想ルータは2 台以上の物理ルー タから構成され、その中で実際に稼動するのは1 台のみです。その仮想ルータの中で実際に稼動しているルータが停止した場合、自動的に別のルー タに切り替わり稼動を開始します。実際に稼動している物理ルータをマスタルータと呼び、マスタルータ異常時に備えて待機している物理ルータを バックアップルータと呼びます。

スイッチに仮想ルータ用の VRRP 機能を設定するためには、IP インタフェースが存在し、その IP アドレスが VLAN に所属している必要があります。 VRRP 用 IP インタフェースはスイッチの VLAN(IP インタフェース)ごとに設定します。VRRP 機能が正しく動作するために、同じ VRRP グループ内 の VRRP ルータは、同じ設定内容を持つ必要があります。

L3 Features > VRRP Settings の順にメニューをクリックし、以下の画面を表示します。

VRRP Settings				
VRRP Settings				
SNMP Server Traps VRRP New Mas	ter O Enabled	Disabled		
SNMP Server Traps VRRP Auth Fail	⊖ Enabled	Disabled		Apply
Non-owner-ping Response	O Enabled	Disabled		Apply
Virtual Router Settings				
VLAN(1-4094)				
VRID (1-255)				
Virtual IP Address				
VRRP Authentication				Apply
Interface Name	12 chars			Find
Total Entries: 1				
Interface VRID Priority	Owner Preemption	State Master IP	Virtual Router IP	
vlan1 1 100	Y	Init 10.90.90.90	192.168.70.254	Edit Delete
				1/1 K < 1 > > Go

図 9-233 VRRP Settings 画面

#### 画面に表示される項目:

項目	説明				
VRRP Settings					
SNMP Server Traps VRRP	新しい VRRP マスタの SNMP サーバトラップ機能を「Enabled」(有効)/「Disabled」(無効)に指定します。				
New Master	有効にするとデバイスがマスタ状態になった時トラップが送信されます。				
SNMP Server Traps VRRP	認証失敗時の SNMP サーバトラップ機能を「Enabled」(有効)/「Disabled」(無効)に指定します。有効にすると認				
Auth Fail	証鍵 / 認証タイプが衝突、または一致しないルータからパケットを受領した時にトラップが送信されます。				
Non-owner-ping Response	「Non-owner-ping Response」(非オーナ Ping 応答)機能を「Enabled」(有効)/「Disabled」(無効)に指定します。				
	マスタ状態の仮想ルータによる、本仮想ルータと関連のある「ICMP エコーリクエスト」への応答を有効にします。				
	Virtual Router Settings				
VLAN	VLAN ID(1-4094)を指定します。				
VRID (1-255)	仮想ルータの ID を指定します。この値は VRRP グループの仮想ルータを識別するために使用します。				
Virtual IP Address	仮想ルータグループの IPv4 アドレスを指定します。				
VRRP Authentication	VRRP 認証を有効に指定し、インタフェースの VRRP 認証パスワード(8 字以内)をプレーンテキストで指定します。				
	認証はインタフェースの全ての仮想ルータに適用されます。同じ VRRP グループのデバイスは同じ認証パスワードを				
	保持している必要があります。				
Interface Name	インタフェース名(12 字以内)を指定します。				

「Apply」ボタンをクリックし、設定を有効にします。

「Delete」をクリックすると指定のエントリを削除します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。 「Edit」をクリックして、指定エントリの編集を行います。 設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

#### 「Edit」をクリックすると、以下の画面が表示されます。

lan1 - Group 1		
State	Init	
Virtual IP Address	192.168.70.254	
Virtual MAC Address	00-00-5E-00-01-01	
Advertisement Interval (1-255)	1 sec	
Preemption	Enabled	
Priority (1-254)	100	
BFD Remote IP	1	
Master Router	10.90.90.90	
Critical IP Address		
Authentication		
Shutdown	Disabled	Back Apply

図 9-234 VRRP Virtual Router Settings 画面

#### 画面に表示される項目:

項目	説明
Advertisement Interval	通知間隔(1-255)を指定します。マスタルータによる VRRP 通知の間隔値です。初期値は「1」です。
Preemption	「Preemption」(優先置き換え)機能を「Enabled」(有効)/「Disabled」(無効)に指定します。 より高いプライオリティを持つバックアップルータがより低いプライオリティを持つマスタルータと置き替わるかどうか を設定します。
Priority (1-254)	仮想ルータのマスタ選出のプロセスで使用する優先値を指定します。
BFD Remote IP	「Bidirectional Forwarding Detection」(BFD) リモート IP アドレスを指定します。本 IP アドレスは同じ VRRP 仮想グループ の実存デバイスの実存 IP アドレスである必要があります。BFD セッションはこの VRRP ルータとピア間で生成されます。 セッションが落ちると VRRP はバックアップステートになり、マスタと交換します。
Critical IP Address	インターネットへの最も直接的な経路、またはこの仮想ルータからの他のクリティカルなネットワーク接続を提供する物 理デバイスの IP アドレスを入力します。これはネットワークにある本物のデバイスの IP アドレスです。仮想ルータから この IP アドレスへの接続に失敗すると、仮想ルータは自動的に無効になります。新しいマスタは VRRP グループに所属す るバックアップルータから選出されます。異なる Critical IP Address が VRRP グループに所属する異なるルータに割り当て られ、インターネットまたは他のクリティカルネットワーク接続に複数の経路を定義します。
Shutdown	シャットダウンを「Enabled」(有効)/「Disabled」(無効)に指定します。インタフェースの仮想ルータを無効にします。 他のオーナルータをシャットダウンする前に、指定 IP アドレスのルータをシャットダウンするミスを回避する目的です。

「Apply」をクリックし、設定内容を適用します。

「Back」をクリックすると前のページに戻ります。

# VRRPv3 Settings (VRRPv3 設定)

VRRPv3 設定を行います。

L3 Features > VRRPv3 Settings の順にメニューをクリックし、以下の画面を表示します。

/RRPv3 Se	ttings		_	_	_	_	_	_	_		_	
VRRPv3 Setti	ngs											
VLAN(1-4094	I)			-								
VRID (1-255)				1								
Address Fam	ily		IPv4	า							Apply	
Interface Nar	ne		12 chars								Find	
Total Entries	: 2											
Interface	VRID	Version	Address Family	Priority	Owner	Preemption	State	Virtual Router IP				
vlan1	2	3	IPv4	100		Y	Init	0.0.0.0		Edit	Delete	
vlan1	3	3	IPv6	100		Y	Init			Edit	Delete	
									1/1			

図 9-235 VRRPv3 Settings 画面

画面に表示される項目:

項目	説明
VLAN	VLAN ID(1-4094)を指定します。
VRID (1-255)	仮想ルータの ID を指定します。この値は VRRP グループの仮想ルータを識別するために使用します。
Address Family	アドレスファミリーを指定します。
	・ IPv4 - IPv4 仮想ルータを指定します。
	・ IPv6 - IPv6 仮想ルータを指定します。
Interface Name	インタフェース名(12 字以内)を指定します。

「Apply」ボタンをクリックし、設定を有効にします。

「Delete」をクリックすると指定のエントリを削除します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Edit」をクリックして、指定エントリの編集を行います。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「IPv4 Address Family」エントリの「Edit」をクリックすると、以下の画面が表示されます。

VRRPv3 Virtual Router Settings				
vlan1 - Group 2 - Version 3 - Add	ess Family IPv4			
State	Init			
Virtual IP Address	0 · 0 · 0 · 0			
Virtual MAC Address	00-00-5E-00-01-02			
Advertisement Interval (1-255)	1 sec			
Preemption	Enabled			
Priority (1-254)	100			
Critical IP Address				
Non-owner-ping	Disabled			
Shutdown	Disabled			
Master Router	0.0.0 Back Apply			

図 9-236 VRRPv3 Virtual Router Settings (Edit/IPv4 Address Family) 画面

両面目にま	ミデナ・	hΖ	百口	٠
凹凹に乙	ミノヽご/	110	火日	٠

項目	説明
Virtual IP Address	仮想 IPv4 アドレスを指定します。同じ VRRP グループの全てのルータは同じルータ ID と仮想アドレスで設定されている
	必要があります。仮想ルータの IP アドレスは不使用のアドレス、またはルータの実存のアドレスである必要があります。
	仮想アドレスがインタフェースの実存するアドレスと同等の場合、仮想ルータは IP アドレスのオーナとなります。
Advertisement Interval	通知間隔(1-255)を指定します。マスタルータによる VRRP 通知の間隔値です。マスタルータはコンスタントに VRRP 通
	知を送信します。VRRP グループ内の全仮想ルータは同じ間隔値である必要があります。
Preemption	「Preemption」(優先置き換え)機能を「Enabled」(有効)/「Disabled」(無効)に指定します。より高いプライオリティ
	を持つバックアップルータがより低いプライオリティを持つマスタルータと置き替わるかどうかを設定します。

項目	説明
Priority (1-254)	仮想ルータの優先値(1-254)を指定します。VRRP グループのマスタ選出のプロセスで使用する優先値になります。最優先値の仮想ルータがマスタとなり、他のルータは VRRP グループのバックアップとなります。最優先値のルータが複数存在する場合は、より大きい IPv4 アドレス値のルータがマスタとなります。VRRP グループの IPv4 アドレスオーナのルータは常に VRRP グループのマスタになり、最高値(255)となります。
Critical IP Address	インターネットへの最も直接的な経路、またはこの仮想ルータからの他のクリティカルなネットワーク接続を提供する物 理デバイスのIPアドレスを入力します。これはネットワークにある本物のデバイスのIPアドレスです。仮想ルータから このIPアドレスへの接続に失敗するとが、仮想ルータは自動的に無効になります。新しいマスタは VRRP グループに所属 するバックアップルータから選出されます。異なる Critical IP Address が VRRP グループに所属する異なるルータに割り当 てられ、インターネットまたは他のクリティカルネットワーク接続に複数の経路を定義します。
Non-owner ping	「Non-owner ping」(非オーナ Ping)機能を「Enabled」(有効)/「Disabled」(無効)に指定します。 マスタステートの非 IP アドレスオーナ仮想ルータによる IPv4 アドレスの ICMP エコーリクエスト、または IPv6 アドレス の ND リクエストへの応答を有効にします。
Shutdown	シャットダウンを「Enabled」(有効)/「Disabled」(無効)に指定します。インタフェースの仮想ルータを無効にします。 他のオーナルータをシャットダウンする前に、指定 IP アドレスのルータをシャットダウンするミスを回避する目的です。

「Apply」をクリックし、設定内容を適用します。 「Back」をクリックすると前のページに戻ります。

## 「IPv6 Address Family」エントリの「Edit」をクリックすると、以下の画面が表示されます。

VRRPv3 Virtual Router Se	ttings	
vlan1 - Group 3 - Version 3 - Addr	ress Family IPv6	
State	Init	
Virtual IPv6 Address		
Virtual MAC Address	00-00-5E-00-02-03	
Advertisement Interval (1-255)	1 sec	
Preemption	Enabled	
Priority (1-254)	100	
Critical IPv6 Address		
Name	12 chars	
Non-owner-ping	Disabled	
Shutdown	Disabled	
Master Router		Back Apply

図 9-237 VRRPv3 Virtual Router Settings (Edit/IPv6 Address Family) 画面

項目	説明
Virtual IPv6 Address	仮想 IPv6 アドレスを指定します。同じ VRRP グループの全てのルータは同じルータ ID と仮想アドレスで設定されている
	必要があります。仮想ルータの IP アドレスは不使用のアドレス、またはルータの実存のアドレスである必要があります。
	仮想アドレスがインタフェースの実存するアドレスと同等の場合、仮想ルータは IP アドレスのオーナとなります。
Advertisement Interval	通知間隔(1-255)を指定します。マスタルータによる VRRP 通知の間隔値です。マスタルータはコンスタントに VRRP 通
	知を送信します。VRRP グループ内の全仮想ルータは同じ間隔値である必要があります。
Preemption	「Preemption」(優先置き換え)機能を「Enabled」(有効)/「Disabled」(無効)に指定します。より高いプライオリティ
	を持つバックアップルータがより低いプライオリティを持つマスタルータと置き替わるかどうかを設定します。
Priority (1-254)	仮想ルータの優先値(1-254)を指定します。VRRP グループのマスタ選出のプロセスで使用する優先値になります。最優
	先値の仮想ルータがマスタとなり、他のルータは VRRP グループのバックアップとなります。最優先値のルータが複数存
	在する場合は、より大きい IPv4 アドレス値のルータがマスタとなります。VRRP グループの IPv4 アドレスオーナのルータ
	は常に VRRP グループのマスタになり、最高値(255)となります。
Critical IPv6 Address	インターネットへの最も直接的な経路、またはこの仮想ルータからの他のクリティカルなネットワーク接続を提供する物
	理デバイスの IPv6 アドレスを入力します。これはネットワークにある本物のデバイスの IPv6 アドレスです。仮想ルータ
	からこの IPv6 アドレスへの接続に失敗するとが、仮想ルータは自動的に無効になります。新しいマスタは VRRP グループ
	に所属するバックアップルータから選出されます。異なる Critical IPv6 Address が VRRP グループに所属する異なるルータ
	に割り当てられ、インターネットまたは他のクリティカルネットワーク接続に複数の経路を定義します。
Non-owner ping	「Non-owner ping」(非オーナ Ping)機能を「Enabled」(有効)/「Disabled」(無効)に指定します。マスタステートの非
	IP アドレスオーナ仮想ルータによる IPv4 アドレスの ICMP エコーリクエスト、または IPv6 アドレスの ND リクエストへの
	回答を有効にします。
Shutdown	シャットダウンを「Enabled」(有効)/「Disabled」(無効)に指定します。インタフェースの仮想ルータを無効にします。
	┃他のオーナルータをシャットダウンする前に、指定 IPv6 アドレスのルータをシャットダウンするミスを回避する目的です。
「Apply」をクリックし、	設定内容を適用します。

「Back」をクリックすると前のページに戻ります。

## 画面に表示される項目:

# 第 10 章 QoS (QoS 機能の設定)

本スイッチは、802.1p プライオリティキューイングの QoS(Quality of Service)機能をサポートしています。次のセクションでは、QoS(Quality of Service)の実装と、802.1p プライオリティキューイングを使用する利点について説明します。

サブメニュー	説明
Basic Settings(基本設定)	QoS の Basic Settings(基本設定)を行います。
Advanced Settings(アドバンス設定)	QoS の Advanced Settings(アドバンス設定)を行います。
QoS PFC	ネットワーク「Quality of Service」(QoS) プライオリティベースフローコントロール (PFC) クラスマップの
	設定を行います。
WRED(WRED 設定)	WRED(WRED 設定)の設定を行います。
iSCSI (アイスカジー)	iSCSIの設定を行います。

以下は QoS サブメニューの説明です。必要に応じて、設定 / 変更 / 修正を行ってください。

## QoS の長所

QoS は IEEE 802.1p 標準で規定される技術であり、VoIP(Voice-over Internet Protocol)、Web 閲覧用アプリケーション、ファイルサーバアプリケーション、ビデオ会議など、広帯域を必要としたり高い優先順位を持つ重要なサービスのために、帯域を確保することができます。ネットワーク帯域を拡張するだけでなく、重要度の低いトラフィックに対して制限を行うことで、ネットワークが必要以上の帯域を使用しないようにします。スイッチの各物理ポートには個別のハードウェアキューがあり、様々なアプリケーションからのパケットがマッピングされ、優先順位が付けられます。以下の図に、802.1p プライオリティキューイングがどのように本スイッチに実装されているかを示します。



図 10-1 スイッチ上での QoS マッピングの例

上の図は本スイッチのプライオリティの初期設定です。クラス7はスイッチにおける7つのプライオリティクラスの中で、最も高い優先度を持って います。QoSを実行するためには、パケットのヘッダを調べて適切な識別タグがあるかどうかを確認するようにスイッチに指示する必要があります。 そして、ユーザはそれらのタグ付きパケットをスイッチ上の指定されたキューに送り、優先順序に従って送出するようにします。

例えば、遠隔地に設置した2台のコンピュータ間でビデオ会議を行うとします。管理者はAccess Profile コマンドを使用して、送信するビデオパケットにプライオリティタグを追加することができます。そして、受信側ではそのタグを検査するように設定し、受信したタグ付きパケットをスイッチのクラスキューに関連付けるようにします。また、管理者はこのキューに優先順位を与え、他のパケットよりも先に送信されるように設定を行います。この結果、このサービス用のパケットはできる限り早く送信されます。キューが優先されることにより、パケットは中断せずに送信されるため、このビデオ会議用に帯域を最適化することが可能になります。

## QoS について

本スイッチは、802.1p プライオリティキューをサポートしており、8 個のプライオリティキューがあります。プライオリティキューには、最高レベルの7番キュー(クラス7)から最低レベルの0番キュー(クラス0)までがあります。IEEE 802.1p (p0 から p7)に規定される8つのプライオリティ タグは、以下のようにスイッチのプライオリティキューにマッピングされます。

- ・ プライオリティ0は、スイッチのQ2キューに割り当てられます。
- プライオリティ1は、スイッチのQ0キューに割り当てられます。
- プライオリティ2は、スイッチのQ1キューに割り当てられます。
- プライオリティ3は、スイッチのQ3キューに割り当てられます。
- ・ プライオリティ4は、スイッチのQ4キューに割り当てられます。
- ・ プライオリティ5は、スイッチのQ5キューに割り当てられます。
- ・ プライオリティ6は、スイッチのQ6キューに割り当てられます。
- プライオリティ7は、スイッチのQ7キューに割り当てられます。

Strict(絶対優先)のプライオリティベースのスケジューリングでは、優先度の高いキューに属するパケットから送信されます。Strict 方式のキュー が複数ある場合、プライオリティタグに従って順番に送信されます。優先度の高いキューが空になると、次の優先度を持つパケットが送信されます。

重み付けラウンドロビンキューイングでは、各プライオリティキューから送信されるパケットの数は、指定された重み付けによって決定されます。 8 つの CoS (Class of Service)キュー、A ~ H に 8 から 1 までの重み付けを設定したとすると、パケットは以下の順に送信されます。 A1, B1, C1, D1, E1, F1, G1, H1, A2, B2, C2, D2, E2, F2, G2, A3, B3, C3, D3, E3, F3, A4, B4, C4, D4, E4, A5, B5, C5, D5, A6, B6, C6, A7, B7, A8, A1, B1, C1, D1, E1, F1, G1, H1

重み付けラウンドロビンキューイングにおいて各 CoS キューが同じ重み付けを持つ場合、ラウンドロビンキューイングのように、各 CoS キューの パケットは同じ割合で送信されます。また、ある CoS キューの重み付けとして 0 を設定すると、そのキューから送信するパケットがなくなるまでパ ケットを処理します。0 以外の値を持つ他のキューでは、重み付けラウンドロビンの規則により、重みに従って送信を行います。

神足 本スイッチは、スイッチ上の各ポートに8つのプライオリティキューを持っています。これらのクラスの1つはスイッチにおける内部利用のために予約されており、設定することができません。次のセクションで参照されるサービスクラスは、管理者によって設定・管理可能な7つのクラスのみを示しています。

# Basic Settings(基本設定)

QoS の Basic Settings (基本設定)を行います。

# Port Default CoS(ポートデフォルト CoS 設定)

各ポートにデフォルト CoS の設定を行います。

## **QoS > Basic Settings > Port Default CoS**の順にメニューをクリックし、以下の画面を表示します。

Port Default CoS		
Port Default CoS		
Unit From Port           1	Port         Default CoS           h1/0/1         Image: Compared to the second se	Apply
Unit 1 Settings		
Port	Default CoS	Override
eth1/0/1	0	No
eth1/0/2	0	No
eth1/0/3	0	No
eth1/0/4	0	No
eth1/0/5	0	No
eth1/0/6	0	No

図 10-1 Port Default CoS 画面

#### 画面に表示される項目:

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	設定するポート範囲を指定します。
Default CoS	ポートに初期 CoS を指定します。0から7の間で指定可能です。「Override」にチェックを入れるとポートに受信したすべてのパケット(タグありなし関わらず)にポートの CoS が適用されます。「None」を選択すると、初期設定を有効にします。 プライオリティを割り当てるクラス(キュー)を設定します。「Class-0」(クラス0)は最も低い優先度のキューで、「Class-7」 (クラス7)が最も高くなります。
記点ナ亦市ナフト	ンボ「Anacha」ボタンナクリックト 記中中京大海田トマイジャン

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

# Port Scheduler Method(ポートスケジューラーメソッド設定)

ポートスケジューラーメソッドを設定します。

**QoS > Basic Settings > Port Scheduler Method** の順にクリックし、以下の画面を表示します。

Port Scheduler Method					
Port Scheduler Method					
Unit     From Port     To Port     Scheduler Method       1     eth1/0/1     eth1/0/1     WRR     Apply					
Port	Scheduler Method				
eth1/0/1 WRR					
eth1/0/2	WRR				

図 10-2 Port Scheduler Method 画面

画面に表示される項目:

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	設定するポート / ポート範囲を入力します。
Scheduler Method	指定ポートに対するスケジューリングの方法を設定します。 「Strict Priority」(SP)、「Round-Robin」(RR)、「Weighted Round-Robin」(WRR)、「Weighted Deficit Round-Robin」(WDRR) から指 定できます。初期値ではアウトプットキュースケジューリングアルゴリズムは「WRR」です。「WDRR」は送信キューに蓄積 したバックログクレジットのセットを供給することで作動します。 はじめに各キューはクレジットカウンタを量の値として設定します。CoS キューからのパケットが送信される度に、パケッ トのサイズはクレジットカウンタから差し引かれ、サービスの権利は次の低い CoS キューに移行されます。 クレジットカウンタが 0 以下になると、クレジットが補完されるまでキューは停止します。すべての CoS キューが 0 に到達 するとクレジットカウンタは補完されます。すべてのパケットはクレジットカウンタが 0 かそれ以下の場合、実行され最後 のパケットも全て送信されます。こうなった場合、クレジットは補完されます。クレジットが補完されるといくつかのクレ ジットは各 QoS キュークレジットカウンタに追加されます。各 CoS キューの集合体はユーザ定義に基づいてそれぞれ同じで はありません。SP モードでの CoS キューの設定はより優先値の高い CoS キューがストリクトプライオリティーモードで設定 されている必要があります。優先値の高い CoS キューの手合(Weight)が1差し引か れ、次の低い CoS キューがのパケットが実行されます。CoS キューの重量(Weight)がゼロになると、補完されるまでキュー は実行されません。すべての CoS キューの重量(Weight)が 0 に到達すると同時にその重量(Weight)は補完されます。
設定を変更する際は、	必ず「Apply」ボタンをクリックし、設定内容を適用してください。

# Queue Settings(QoS 設定)

キューを設定、表示します。

## **QoS > Basic Settings > Queue Settings** の順にクリックし、以下の画面を表示します。

Queue Settings						
Queue Settings						
Unit From Port     IV   eth1/0/1	To Port Queue ID eth1/0/1 V 0 V	WRR Weight (0-127) WDR	R Quantum (0-127)			
Unit 1 Settings						
Port	Queue ID	WRR Weight	WDRR Quantum			
	0	1	1			
	1	1	1			
	2	1	1			
eth1/0/1	3	1	1			
	4	1	1			
	5	1	1			
	6	1	1			
	7	0	1			
	0	1	1			
	1	1	1			
	2	1	1			
eth1/0/2	3	1	1			
Garrioz	4	1	1			
	5	1	1			
	6	1	1			

図 10-3 Queue Settings 画面

## 画面に表示される項目:

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	設定するポート / ポート範囲を入力します。
Queue ID	キュー ID を指定します。0 から 7 の間で指定可能です。
WRR Weight	WRR の値を入力します。0 から 127 の間で指定可能です。「Expedited Forwarding」(EF) の要件を満たすには最高のキュー は常に「Per-hop Behavior」(PHB) により選択されキューのスケジュールモードはストリクトプライオリティである必要があ ります。そのため最後のキューの重さは「Differentiate Service」がサポートされている間は 0 に設定する必要があります。
WDRR Quantum	「WDRR Quantum」の値を入力します。0 から 127 の間で指定できます。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

# CoS to Queue Mapping (CoS キューマッピング設定)

CoS-to-Queue マッピングの表示、設定を行います。

#### **QoS > Basic Settings > CoS to Queue Mapping**の順にクリックし、以下の画面を表示します。

# CoS to Queue Mapping

CoS	Queue ID
0	2 🗸
1	0 🗸
2	1
3	3 🗸
4	4
5	5 🗸
6	6 🗸
7	7 🗸
	Apply

図 10-4 CoS to Queue Mapping 画面

画面に表示される項目:

項目	説明
Queue ID	プライオリティを割り当てるクラス(キュー)を設定します。「0」(クラス 0)は最も低い優先度のキューで、「7」(クラス 7)が最 も高くなります。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

# Port Rate Limiting(ポートレート制限設定)

ポートレート制限の設定を行います。

**QoS > Basic Settings > Port Rate Limiting**の順にメニューをクリックし、以下の画面を表示します。

t Rate Limiting							
Jnit From Port	To Port eth1/0/1	Direction	Rate Limit                Bandwidth (8-10000000)             [             Percent (1-100)             [             None	Kbps Burst Size (0- % Burst Size (0-	128000) Kbyte 128000) Apply		
Jnit 1 Settings							
Dect		Input		Outp	ut		
Port	Rate		Burst	Rate	Burst		
eth1/0/1	No Limit		No Limit	No Limit	No Limit		
eth1/0/2	No Limit		No Limit	No Limit	No Limit		
eth1/0/3	No Limit		No Limit	No Limit	No Limit		
eth1/0/4	No Limit		No Limit	No Limit	No Limit		
eth1/0/5	No Limit		No Limit	No Limit	No Limit		
eth1/0/6	No Limit		No Limit	No Limit	No Limit		

図 10-5 Port Rate Limiting 画面

## 画面に表示される項目:

項目	説明
Unit	設定するユニット名を選択します。
From Port / To Port	設定するポート / ポート範囲を入力します。
Direction	レート制限の対象を Input(イングレス)、Output(イーグレス)から選択します。
Rate Limit	<ul> <li>レート制限の値を指定します。</li> <li>Bandwidth - 「Bandwidth」を選択し、受信/送信の帯域値を入力欄に入力します。この値は 8 から 10000000 Kbps で指定できます。また「Burst Size」の値も 0 から 128000Kbyte で指定可能です。</li> <li>Percent - 「Percent」を選択し、受信/送信の帯域パーセントを入力欄に入力します。この値は 1 から 100%で指定できます。また「Burst Size」の値も 0 から 128000 Kbytes で指定可能です。</li> <li>None - 「None」を選択すると指定ポートのレート制限を削除します。指定の制限はインタフェースの最大スピードを超えません。イングレスは受信したトラフィックが制限を超えた場合、PAUSE フレームまたはフローコントロールフレームを送信します。</li> </ul>

「Apply」ボタンをクリックして行った変更を適用します。

# Queue Rate Limiting(キューレート制限設定)

キューレートの制限設定をします。

**QoS > Basic Settings > Queue Rate Limiting** の順にメニューをクリックし、以下の画面を表示します。

Queue l	Rate Lim	iting														
Queue Ra	ate Limiting															
Unit From Port To Port				(	Queue ID	Rate Limit										
1 🗸	eth1/0/1 [	✓ [	eth1/0/1	<b>~</b>	0 🗸	Min Bandwidth (8-10000000)     Kbps Max Bandwidth (8-10000000)						0000)	Kbps			
						O Min Pe	rcent (1-10	0)		%	Max	Percent (	1-100)			%
						None									Aj	oply
Unit 4 C	attinga															
Unit 1 S		000	Oue	1	Oue	2010	Oue	2003	Oue	uo4	Oue	1105	Our	8006	Oue	107
Dort		llow			- Ceuc	Nex		New		Nov	- CQUC	New	- Ceur	New		How
Ροπ	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	мах	Min	Max	Min	Max
	Rate	Rate	Rate	Rate	Rate	Rate	Rate	Rate	Rate	Rate	Rate	Rate	Rate	Rate	Rate	Rate
eth1/0/1	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li
eth1/0/2	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li
eth1/0/3	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li
eth1/0/4	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li
eth1/0/5	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li
eth1/0/6	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li	No Li

図 10-6 Queue Rate Limiting 画面

画面に表示される項目:

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	この設定に使用するポート範囲を選択します。
Queue ID	キュー ID を指定します。「0」(クラス 0)は最も低い優先度のキューで、「7」(クラス 7)が最も高くなります。
Rate Limit	キューレート制限の設定を行います。 「Min Bandwidth」を選択し、最小限の帯域値を入力欄に入力します。この値は 8 から 10000000 Kbps で指定できます。 また「Max Bandwidth」で最大限の帯域値も入力可能です。この値は 8 から 10000000 Kbps で指定できます。最小帯域 が指定されるとこのキューから送信されるパケットは保障されます。最大値の帯域値が指定されると、その帯域が有効 であっても、このキューからの送信パケットは最大の帯域幅を超えることができません。 最小の帯域を設定する時、設定する最小帯域の集合体はインタフェース帯域の 75 パーセント以下に設定する必要があ ります。 最高に厳しい優先キューの最小保証帯域は必ずしも必要という訳ではありません。これはすべてのキューの最小帯域が 条件を満たしていれば、キューのトラフィックは実行されるからです。 このコマンドの設定は物理ポートにのみ設定可能でポートチャネルには不可能です。それは一つの CoS の最小保証帯 域は物理ポート間では使用不可能だからです。 「Min Percent」では最小帯域パーセントを入力欄に入力します。この値は 1 から 100%で指定できます。最大値(Max Percent) も 1 から 100%で指定できます。

「Apply」ボタンをクリックして行った変更を適用します。

注意 キュー帯域幅制御の最小グラニュラリティは 64Kbps です。システムは自動的に 64 倍の数に調整します。

# Queue Statistics Table(キュー統計テーブル)

キュー統計テーブルを表示します。

# QoS > Basic Settings > Queue Statistics Table の順にメニューをクリックし、以下の画面を表示します。

Queue St	atistics Tab	le	_	_	_	_	_	_	
Queue Stati	stics Table								
		-							
Unit	1 🗸	Port eth1/0/	1 🗸					Find	Show All
Unit 1 Sett	ings								
Port	Queue ID	Min Bandwidth	Max Bandwidth	Packets/sec	Total Packets	Drop Packets	Bytes/sec	Total Bytes	Drop Bytes
	0	0	100000	0	0	0	0	0	0
	1	0	100000	0	0	0	0	0	0
	2	0	100000	0	378	0	0	44539	0
ath 1/0/1	3	0	100000	0	0	0	0	0	0
ett 1/0/1	4	0	100000	0	0	0	0	0	0
	5	0	100000	0	0	0	0	0	0
	6	0	100000	0	0	0	0	0	0
	7	0	100000	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0
	1	0	0	0	0	0	0	0	0
	2	0	0	0	0	0	0	0	0

図 10-7 Queue Statistics Table 画面

画面に表示される項目:

項目	説明
Unit	ユニットを選択します。
Port	ポートを選択します。

ポートを選択し「Find」ボタンをクリックして、指定のポートについて表示します。 「Show All」ボタンをクリックして全ポートについて表示します。

# Advanced Settings (アドバンス設定)

QoS の Advanced Settings (アドバンス設定)を行います。

## DSCP Mutation Map (DSCP 変更マップ設定)

本項目では「Differentiated Services Code Point」(DSCP) 変更マップ設定を行います。インタフェースでパケットを受信すると DSCP 変更マップに 基づき受信 DSCP は QoS 動作の前に他の DSCP に変化します。DSCP 変更は違う DSCP タスクの統合にとても有効です。DSCP-CoS マップと DSCPcolor マップはパケット本来の DSCP に基づいて動作します。すべての後続の動作は変更 DSCP に基づいています。

**QoS > Advanced Settings > DSCP Mutation Map**の順にクリックし、以下の画面を表示します。

CP Mutation Map												
utation Name Inpu	t DSCP List (0-63)	Output DSCP	(0-63)									
? chars 1,3,	60-63											Apply
tal Entries: 1												
							Digit	in ones				
Mutation Name	Digit in tens	0	1	2	3	4	5	6	7	8	9	
	00	0	10	2	3	4	5	6	7	8	9	
	10	10	11	12	13	14	15	16	17	18	19	
	20	20	21	22	23	24	25	26	27	28	29	
mutation	30	30	31	32	33	34	35	36	37	38	39	Delete
	40	40	41	42	43	44	45	46	47	48	49	
	50	50	51	52	53	54	55	56	57	58	59	
	60	60	61	62	63							

図 10-8 DSCP Mutation Map 画面

画面に表示される項目:

項目	説明
Mutation Name	DSCP 変更マップ名を指定します。32 文字以内で指定可能です。
Input DSCP List	インプットされる DSCP リスト値を入力します。0 から 63 で指定可能です。
Output DSCP	アウトプットされる DSCP 値を入力します。0 から 63 で指定可能です。
<b>F</b>	

「Apply」ボタンをクリックし、各項目の変更を適用します。

「Delete」をクリックすると指定のエントリを削除します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

# Port Trust State and Mutation Binding (ポートトラスト設定)

本スイッチにおけるポートトラスト設定と表示を行います。

#### **QoS > Advanced Settings > Port Trust State and Mutation Binding**の順にメニューをクリックし、以下の画面を表示します。

Port Trust State and Mutation E	Binding		
Port Trust State and Mutation Binding -			
Unit From Port	To Port Trus eth1/0/1 🔽 Cos	t State DSCP Mutation Map S S 32 chars O	None Apply
Port	Trust State	DSCP Mutation Map	
eth1/0/1	Trust CoS		
eth1/0/2	Trust CoS		
eth1/0/3	Trust CoS		

図 10-9 Port Trust State and Mutation Binding 画面

画面に表示される項目:

項目	説明
Unit	設定するユニット名を選択します。
From Port / To Port	設定するポート / ポート範囲を入力します。
Trust State	ポートトラストの設定をします。「CoS」「DSCP」から選択可能です。
DSCP Mutation	DSCP 変更マップ名を入力します。32 文字以内で設定可能です。
Мар	「None」を選択するとどのポートに DSCP 変更マップを指定しません。

「Apply」ボタンをクリックして行った変更を適用します。
## DSCP CoS Mapping (DSCP CoS マップ設定)

本スイッチにおける DSCP CoS マップの設定と表示を行います。

#### **QoS > Advanced Settings > DSCP CoS Mapping** の順にメニューをクリックし、以下の画面を表示します。

DSCP CoS Mapping		_		
DSCP CoS Mapping				
Unit From Po	ort         To Port           1	CoS I	DSCP List (0-63)	Apply
Unit 1 Settings				
Port	CoS		DSCP List	
	0		0-7	
	1		8-15	
	2		16-23	
ath 1/0/1	3		24-31	
eth 1/0/1	4		32-39	
	5		40-47	
	6		48-55	

図 10-10 DSCP CoS Mapping 画面

#### 画面に表示される項目:

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	設定の対象となるポートを指定します。
CoS	CoSの値を指定します。0から7の間で指定可能です。
DSCP List (0-63)	DSCP リストの値を入力します。0 から 63 の範囲で設定します。

## CoS Color Mapping(CoS カラーマップ設定)

本スイッチにおける CoS カラーマップの設定と表示を行います。

#### **QoS > Advanced Settings > CoS Color Mapping**の順にメニューをクリックし、以下の画面を表示します。

CoS Color Mapping		
CoS Color Mapping		
Unit From Po	ort         To Port           /1          eth1/0/1	CoS List (0-7) Color Green V Apply
Unit 1 Settings		
Port	Color	CoS List
	Green	0-7
eth1/0/1	Yellow	
	Red	
	Green	0-7
eth1/0/2	Yellow	
	Red	
	Green	0-7
eth1/0/3	Yellow	
	Red	
	Green	0-7
eth1/0/4	Yellow	
	Red	

図 10-11 CoS Color Mapping 画面

## 画面に表示される項目:

説明
設定するユニットを指定します。
設定の対象となるポートを指定します。
カラーマップされる CoS の値を指定します。0 から 7 の間で指定可能です。
マップされるカラーを指定します。「Green」「Yellow」「Red」から指定可能です。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

## DSCP Color Mapping (DSCP カラーマップ設定)

本スイッチにおける DSCP カラーマップの設定と表示を行います。

**QoS > Advanced Settings > DSCP Color Mapping**の順にメニューをクリックし、以下の画面を表示します。

DSCP Color Mappin	9			
DSCP Color Mapping				
Unit From Po	ort To Port 1 V eth1/0/1 V	DSCP List (0-63) Color Gree	r en 🗸	Apply
Unit 1 Settings				
Port	Color		DSCP List	
	Green		0-63	
eth1/0/1	Yellow			
	Red			
	Green		0-63	
eth1/0/2	Yellow			
	Red			

図 10-12 DSCP Color Mapping 画面

画面に表示される項目	:
------------	---

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	設定の対象となるポートを指定します。
DSCP List	カラーマップされる DSCP の値を指定します。0 から 63 の間で指定可能です。
Color	マップされるカラーを指定します。「Green」「Yellow」「Red」から指定可能です。
設定を変更する際は、	、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

# Class Map(クラスマップ設定)

本スイッチにおけるクラスマップの設定と表示を行います。

#### **QoS > Advanced Settings > Class Map**の順にメニューをクリックし、以下の画面を表示します。

Class Map			
Class Map Name	32 chars	Multiple Match Criteria Match Any	Apply
Total Entries: 2			
Class	s Map Name	Multiple Match Criteria	
	class	Match Any	Match Delete
	ee-dofault	Match Any	Match Delete
cia	55-deladir	matori / ury	Match

図 10-13 Class Map 画面

#### 画面に表示される項目:

項目	説明
Class Map Name	クラスマップ名を指定します。32文字まで指定可能です。
Multiple Match Criteria	複数のマッチクライテリアを指定します。「Match All」「Match Any」から選択可能です。
設定を変更する際は	必ず「Annly」ボタンをクリック」。 設定内容を適用してください。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。 「Match」ボタンをクリックし、指定のエントリを設定します。 「Delete」ボタンをクリックし、指定のエントリを削除します。 「Match」ボタンをクリックすると下記の画面が表示されます。

Match Rule		
Class Map Name	class	
Match:		
ONone		
<ul> <li>Specify</li> </ul>		
<ul> <li>ACL Name</li> </ul>	32 chars	
O CoS List (0-7)	0,5-7	
O DSCP List (0-63)	1,2,61-63	
<ul> <li>Precedence List (0-7)</li> </ul>	0,5-7	
O Protocol Name	None	
<ul> <li>VID List (1-4094)</li> </ul>	1,3-5	
		Back Apply
図 10-14 Match Rule 画面		

画面に表示される項目:

項目	説明
None	このクラスマップと何もマッチさせない場合選択します。
Specify	このクラスマップと下記のオプションのどれかをマッチさせる場合に選択します。
ACL Name	クラスマップとマッチさせるアクセスリスト名を指定します。32 文字まで指定できます。
CoS List	クラスマップとマッチさせる CoS リスト名を指定します。0 から 7 まで指定できます。 「Inner」をチェックした場合、インナー CoS とマッチさせます。
DSCP List	クラスマップとマッチさせる DSCP リスト名を指定します。0 から 63 まで指定できます。 「IPv4 only」にチェックを入れると IPv4 パケットのみとマッチします。チェックを入れないと IPv4/v6 どちらのパケットともマッ チします。
Precedence List	クラスマップとマッチさせる優先リスト名を指定します。0から7まで指定できます。 「IPv4 only」にチェックを入れるとIPv4パケットのみとマッチします。チェックを入れないとIPv4/v6どちらのパケットともマッ チします。IPv6パケットの場合、IPv6 ヘッダのトラフィッククラスにある3つの重要なビットになります。
Protocol Name	クラスマップとマッチさせるプロトコル名を以下から指定します。 「None」「ARP」「BGP」「DHCP」「DNS」「EGP」「FTP」「IPv4」「IPv6」「NetBIOS」「NFS」「NTP」「OSPF」「PPPOE」「RIP」「RTSP」 「SSH」「Telnet」「TFTP」
VID List	クラスマップとマッチさせる VLAN リストを指定します。1 から 4094 まで指定できます。 「Inner」をチェックした場合、インナー VLAN ID とマッチさせます。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

「Back」をクリックすると前のページに戻ります。

## Aggregate Policer(アグリゲートポリサー設定)

本スイッチにおけるアグリゲートポリサーの設定と表示を行います。

**QoS > Advanced Settings > Aggregate Policer** の順にメニューをクリックし、以下の画面を表示します。

Aggregate Policer	_	_	_	_	_	
Single Rate Settings	Two R	ate Settings				
Aggregate Policer Name *			Avera (0-10	ge Rate * 000000)		Kbps
Normal Burst Size (0-16384)		Kbyte	Maxir (0-16	num Burst Size 384)		Kbyte
Conform Action	Transmit	✓ DSCP 1P	Excee	ed Action	Transmit	✓ DSCP 1P
Violate Action	None	✓ DSCP 1P	Color	Aware	Disabled	$\checkmark$
* Mandatory Field						Apply
Total Entries: 1						
Name Average Rate	Normal Burst Size	Max. Burst Size	Conform Action	Exceed Action	Violate Action	Color Aware

図 10-15 Aggregate Policer 画面

画面に表示される項目:

項目	説明
Aggregate Policer Name	アグリゲートポリサー名を入力します。
Average Rate	平均レート値を入力します。0 から 10000000 kbps まで指定可能です。
Normal Burst Size	ノーマルバーストサイズを入力します。0 から 16384 Kbytes まで指定可能です。
Maximum Burst Size	最大バーストサイズを入力します。0 から 16384 Kbytes まで指定可能です。
Confirm Action	<ul> <li>ここでは緑色パケットに行う操作を指定します。</li> <li>アクションをここで指定しない場合、初期アクションは「Transmit」になります。</li> <li>オプションは「Drop」「Set-DSCP-Transmit」「Set-1P-Transmit」「Transmit」「Set-DSCP-1P」から選択します。</li> <li>・「Drop」-パケットを破棄します。</li> <li>・「Set-DSCP-Transmit」- IP differentiated services code points (DSCP) を設定して、新しい DSCP 値設定でパケットを送信します。</li> <li>・「Set-1P-Transmit」-パケット CoS 値を設定して、新しい CoS 値で送信します。</li> <li>・「Set-DSCP-1p」- IP DSCP と 1P transmit の値を入力します。</li> <li>・「Transmit」-パケットはそのまま送信されます。</li> </ul>
Exceed Action	<ul> <li>レート制限を超えたパケットに行う操作を指定します。</li> <li>アクションをここで指定しない場合、初期アクションは「Transmit」になります。</li> <li>オプションは「Drop」「Set-DSCP-Transmit」「Set-1P-Transmit」「Transmit」「Set-DSCP-1P」から選択します。</li> <li>・「Drop」-パケットを破棄します。</li> <li>・「Set-DSCP-Transmit」- IP differentiated services code points (DSCP)を設定して、新しい DSCP 値設定でパケットを送信します。</li> <li>・「Set-1P-Transmit」-パケット CoS 値を設定して、新しい CoS 値で送信します。</li> <li>・「Set-DSCP-1p」- IP DSCP と 1P transmit の値を入力します。</li> <li>・「Transmit」-パケットはそのまま送信されます。</li> </ul>
Violate Action	<ul> <li>ノーマル、そしてシングルレートの最大バーストサイズを超えたパケットに行う操作を指定します。</li> <li>「CIR」や「PIR」を順守しないパケットの動作を指定します。シングルレートのポリサーの場合、本項目で指定がされないと、</li> <li>シングルレート2色ポリサーを作成します。2レートポリサーの場合、本項目で指定されないと初期設定は Exceed Action と</li> <li>同等になります。オプションは「Drop」「Set-DSCP-Transmit」「Set-1P-Transmit」「Transmit」「Set-DSCP-1P」から選択します。</li> <li>・「Drop」-パケットを破棄します。</li> <li>・「Set-DSCP-Transmit」- IP differentiated services code points (DSCP)を設定して、新しい DSCP 値設定でパケットを送信します。</li> <li>・「Set-1P-Transmit」-パケット CoS 値を設定して、新しい CoS 値で送信します。</li> <li>・「Set-DSCP-1p」- IP DSCP と 1P transmit の値を入力します。</li> <li>・「Transmit」-パケットはそのまま送信されます。</li> </ul>
Color Aware	「Color Aware」を有効 / 無効に指定します。「Color Aware」が指定されないとポリサーはブラインドモードで動作します。有 効の場合はポリサーは Color Aware モードで動作します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

「Delete」をクリックすると指定のエントリを削除します。

「Two Rate Setting」タブをクリックすると次のページが表示されます。

Aggregate Policer	-			_	_	_
Single Rate Settings	Two	Rate Settings				
Aggregate Policer Name *						
CIR * (0-1000000)		Kbps	Confirm Burst (0-16384	)	Kbyt	е
PIR * (0-10000000)		Kbps	Peak Burst (0-16384)		Kbyt	e
Conform Action	Transmit	DSCP 1P	Exceed Action	Drop		P 1P
Violate Action	Drop	DSCP 1P	Color Aware	Disabled		
* Mandatory Field						Арр
Name CIR Confirm B	urst PIR Pea	k Burst Conform Actio	on Exceed Action	Violate Action	Color Aware	
APN-2 100 100	100	120 Transmit	Drop	Drop	Disabled	Delete

図 10-16 Two Rate Setting 画面

画面に表示される項目:	
-------------	--

項目	説明
Aggregate Policer Name	アグリゲートポリサー名を入力します。
CIR	CIR 値を入力します。0 から 10000000 kbps まで指定可能です。 コミットされたパケットは 2 レートメータリングにおける最初のトークンバケットになります。
Confirm Burst	バーストサイズを入力します。0 から 16384 Kbytes まで指定可能です。 Confirm Burst は kbps における最初のトークンバケットのバーストサイズになります。
PIR	PIR 値を入力します。0 から 10000000 kbps まで指定可能です。 PIR は 2 レートメータリングにおける二つ目のトークンバケットになります。
Peak Burst	ピークバーストサイズを入力します。0 から 16384 Kbytes まで指定可能です。 ピークバーストサイズは kbps における二つ目のトークンバケットのバーストサイズになります。
Confirm Action	<ul> <li>ここでは緑色パケットに行う操作を指定します。</li> <li>アクションをここで指定しない場合、初期アクションは「Transmit」になります。</li> <li>オプションは「Drop」「Set-DSCP-Transmit」「Set-1P-Transmit」「Transmit」「Set-DSCP-1P」から選択します。</li> <li>「Drop」-パケットを破棄します。</li> <li>「Set-DSCP-Transmit」- IP differentiated services code points (DSCP)を設定して、新しい DSCP 値設定でパケットを送信します。</li> <li>「Set-1P-Transmit」-パケット CoS 値を設定して、新しい CoS 値で送信します。</li> <li>「Set-DSCP-1p」 - IP DSCP と 1P transmit の値を入力します。</li> <li>「Transmit」-パケットはそのまま送信されます。</li> </ul>
Exceed Action	<ul> <li>レート制限を超えたパケットに行う操作を指定します。</li> <li>アクションをここで指定しない場合、初期アクションは「Transmit」になります。</li> <li>オプションは「Drop」「Set-DSCP-Transmit」「Set-1P-Transmit」「Transmit」「Set-DSCP-1P」から選択します。</li> <li>・「Drop」-パケットを破棄します。</li> <li>・「Set-DSCP-Transmit」- IP differentiated services code points (DSCP)を設定して、新しい DSCP 値設定でパケットを送信します。</li> <li>・「Set-1P-Transmit」-パケット CoS 値を設定して、新しい CoS 値で送信します。</li> <li>・「Set-DSCP-1p」- IP DSCP と 1P transmit の値を入力します。</li> <li>・「Transmit」-パケットはそのまま送信されます。</li> </ul>
Violate Action	<ul> <li>ノーマル、そしてシングルレートの最大バーストサイズを超えたパケットに行う操作を指定します。</li> <li>「CIR」や「PIR」を順守しないパケットの動作を指定します。シングルレートのポリサーの場合、本項目で指定がされないと、</li> <li>シングルレート2色ポリサーを作成します。2レートポリサーの場合、本項目で指定されないと初期設定は Exceed Action と</li> <li>同等になります。オプションは「Drop」「Set-DSCP-Transmit」「Set-1P-Transmit」「Transmit」「Set-DSCP-1P」から選択します。</li> <li>「Drop」-パケットを破棄します。</li> <li>「Set-DSCP-Transmit」- IP differentiated services code points (DSCP)を設定して、新しい DSCP 値設定でパケットを送信します。</li> <li>「Set-1P-Transmit」-パケット CoS 値を設定して、新しい CoS 値で送信します。</li> <li>「Set-DSCP-1p」 - IP DSCP と 1P transmit の値を入力します。</li> <li>「Transmit」-パケットはそのまま送信されます。</li> </ul>
Color Aware	「Color Aware」を有効 / 無効に指定します。「Color Aware」が指定されないとポリサーはブラインドモードで動作します。有効の場合はポリサーは Color Aware モードで動作します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

## Policy Map (ポリシーマップ設定)

本スイッチにおけるポリシーマップの設定と表示を行います。

**QoS > Advanced Settings > Policy Map** の順にメニューをクリックし、以下の画面を表示します。

Policy Map	
Create/Delete Policy Map	
Policy Map Name 32 chars	Apply
Traffic Policy	
Policy Map Name 32 chars Class Map Name 32 chars	Apply
Total Entries: 1	
Policy Map Name	
Policy-Map-1	Delete
	1/1 K < 1 > 2 Go
Class Rules	
Class Map Name	

図 10-17 Policy Map 画面

本画面の「Create/Delete Policy Map」には以下の項目があります。

項目	説明
Policy Map Name	ポリシーマップ名を指定します。32 文字まで指定可能です。
設定を変更する際は、	、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

本画面の「Traffic Policy」には以下の項目があります。

項目	説明
Policy Map Name	ポリシーマップ名を指定します。32 文字まで指定可能です。
Class Map Name	クラスマップ名を指定します。32 文字まで指定可能です。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。 「Policer」ボタンをクリックし、指定のポリシーマップのポリサーアクション設定をします。 「Delete」ボタンをクリックし、指定のエントリを削除します。

「Set Action」ボタンをクリックし、指定のポリシーマップの設定をします。以下の画面が表示されます。

Policy Map Name	policy	
Class Map Name	class	
et Action		
None		
<ul> <li>Specify</li> </ul>		
New Precedence (0-7)	None IPv4 only	
ONew DSCP (0-63)	None V IPv4 only	
ONew CoS (0-7)	None	
New CoS Queue (0-7)	None	

図 10-18 Set Action 画面

画面に表示される項目	:
------------	---

項目	説明
None	このマップと何もマッチさせない場合選択します。
Specify	このマップとオプションのどれかをマッチさせる場合に選択します。
New Precedence	パケットの優先値を指定します。0 から 7 まで指定できます。 「IPv4 only」にチェックを入れると IPv4 パケット優先になります。CoS キュー選択には影響ありません。
New DSCP	パケットの新しい DSCP 名を指定します。0 から 63 まで指定できます。 「IPv4 only」にチェックを入れると IPv4 パケット優先になります。CoS キュー選択には影響ありません。
New CoS	パケットの新しい CoS 値を指定します。0 から 7 まで指定できます。 「IPv4 only」にチェックを入れると IPv4 パケット優先になります。CoS キュー選択には影響ありません。
New CoS Queue	パケットの新しい CoS キューを指定します。0 から 7 まで指定できます。 「IPv4 only」にチェックを入れると IPv4 パケット優先になります。CoS キュー上書きします。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

「Back」をクリックすると前のページに戻ります。

「Policer」ボタンをクリックすると以下の画面が表示されます。

Police Action	
Policy Map Name	policy
Class Map Name	class
Police Action	
O None	
Specify	Police
Average Rate * (0-10000000)	Kbps
Normal Burst Size (0-16384)	Kbyte
Maximum Burst Size (0-16384)	Kbyte
Conform Action	Transmit DSCP 1P
Exceed Action	Transmit DSCP 1P
Violate Action	None V DSCP 1P
Color Aware	Disabled
* Mandatory Field	
	Back Apply
Normal Burst Size (0-16384) Maximum Burst Size (0-16384) Conform Action Exceed Action Violate Action Color Aware * Mandatory Field	Kbyte Kbyte Transmit V DSCP 1P Transmit V DSCP 1P None V DSCP 1P Disabled V Back Apply

図 10-19 Policer 画面

#### 画面に表示される項目:

項目	説明
None	このマップと何もマッチさせない場合選択します。
Specify	このマップとオプションのどれかをマッチさせる場合に選択します。
Average Rate	アベレージレート値(0-1000000/Kbps)を入力します。
Normal Burst Size	ノーマルバーストサイズ(0-16384/Kbyte)を入力します。
Maximum Burst	最大バーストサイズ(0-16384/Kbyte)を入力します。
Size	
Confirm Action	ここでは緑色パケットに行う操作を指定します。
	アクションをここで指定しない場合、初期アクションは「Transmit」になります。
	オプションは「Drop」「Set-DSCP-Transmit」「Set-1P-Transmit」「Transmit」「Set-DSCP-1P」から選択します。
Exceed Action	ここでは黄色パケットに行う操作を指定します。
	アクションをここで指定しない場合、初期アクションは「Transmit」になります。
	オプションは「Drop」「Set-DSCP-Transmit」「Set-1P-Transmit」「Transmit」「Set-DSCP-1P」から選択します。
Violate Action	ここでは赤色パケットに行う操作を指定します。
	「CIR」や「PIR」を順守しないパケットの動作を指定します。シングルレートのポリサーの場合、本項目で指定がされないと、
	シングルレート 2 色ポリサーを作成します。 2 レートポリサーの場合、本項目で指定されないと初期設定は Exceed Action と
	同等になります。オプションは「Drop」「Set-DSCP-Transmit」「Set-1P-Transmit」「Transmit」「Set-DSCP-1P」から選択します。
Color Aware	「Color Aware」を有効 / 無効に指定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

# Policy Binding(ポリシーバインディング設定)

ポリシーバインディング設定を行います。

**QoS > Advanced Settings > Policy Binding**の順にメニューをクリックし、以下の画面を表示します。

Policy Binding						
Policy Binding Set	tting					
Unit	From Port eth1/0/1	To Port eth1/0/1	Direction	Policy Map Name <ul> <li>32 chars</li> </ul>	⊖ None	Apply
Unit 1 Settings						
	Port		Direction		Policy Map Name	
	eth1/0/1					
	eth1/0/2					
	eth1/0/3					
	eth1/0/4					
	eth1/0/5					
	eth1/0/6					

図 10-20 Policy Binding 画面

画面に表示される項目:

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	設定の対象となるポートを指定します。
Direction	方向を指定します。「Input」「Output」が選択可能です。 「Input」は指定のイングレストラフィックのことです。「Output」は指定のイーグレストラフィックのことです。
Policy Map Name	ポリシーマップ名を指定します。32 文字まで指定可能です。 「None」を選択すると本エントリにポリシーマップは関連付けられません。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

# QoS PFC

ネットワーク「Quality of Service」(QoS) プライオリティベースフローコントロール (PFC) クラスマップの設定を行います。

## Network QoS Class Map(ネットワーク QoS クラスマップ)

本項目ではネットワーク「Quality of Service」(QoS) プライオリティベースフローコントロール (PFC) クラスマップの設定、表示を行います。 ポリシーバインディング設定を行います。

#### **QoS > QoS PFC > Network QoS Class Map**の順にメニューをクリックし、以下の画面を表示します。

Network QoS Class Map	
Network QoS Class Map Settings	
Network QoS Class Map Name 32 chars Total Entries: 1	Apply
Network QoS Class Map Name	
classmap	Match Delete
	1/1  < < 1 > >  Go

図 10-21 Network QoS Class Map 画面

#### 画面に表示される項目:

項目	説明
Network QoS Class Map Name	トラフィックポリシーのネットワーク QoS クラスマップ名(32 字以内)を指定します。
	ず「Apply」ボタンをクリック」 設定内容を適用してください

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください 「Delete」をクリックすると指定のエントリを削除します。

「Match」をクリックすると指定のエントリのマッチルール設定を設定します。

「Watch」をフリフノダると相座のエントラのマフリルール政定を改定します。 記字エントリュ。ごぶ複数で、ジキス担合」で、ジヂ早も地学して「Co」もカリックオストル法ので、

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

#### 「Match」をクリックすると、以下の画面が表示されます。

Match Rule		
Network QoS Class Map Name	classmap	
Match C05	• • • • • • • • • • • • • • • • • • •	Rack Apply

図 10-22 Network QoS Class Map (Match) 画面

画面に表示される項目:

項目	説明
Match CoS	マッチする IEEE 802.1Q Class of Service (CoS) 値(0-7)を指定します。パケットを受信するとパケットはインターナル
	CoS に配布されます。インターナル CoS は CoS に基づいたキューマップへの送信キューを選択するのに使用されます。
	高い値の CoS キューは高い優先値を保持します。「None」を選択すると該当の CoS 値でのマッチングを無効にします。

「Back」をクリックすると前のページに戻ります。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください

## Network QoS Policy Map(ネットワーク QoS ポリシーマップ)

本項目ではネットワーク「Quality of Service」(QoS) ポリシーマップの設定、表示を行います。 QoS > QoS PFC > Network QoS Policy Map の順にメニューをクリックし、以下の画面を表示します。

Network QoS Policy Map		
Create/Delete Network QoS Policy Map Network QoS Policy Map Name 32 chars		Apply
Traffic Policy       Network QoS Policy Map Name       32 chars       32 chars		Apply
Total Entries: 1		
Network QoS Policy Map Name		
qospolicy		Delete
		1/1 < < 1 > >  Go
qospolicy Rules		
Network QoS Class Map Name	Pause	
qosclass	Disabled	Edit Delete

図 10-23 Network QoS Policy Map 画面

画面に表示される項目:

項目	説明
	Create/Delete Network QoS Policy Map
Network QoS Policy Map Name	トラフィックポリシーのネットワーク QoS ポリシーマップ名(32 字以内)を指定します。
	Traffic Policy
Network QoS Policy Map Name	トラフィックポリシーのネットワーク QoS ポリシーマップ名(32 字以内)を指定します。
Network QoS Class Map Name	トラフィックポリシーのネットワーク QoS クラスマップ名(32 字以内)を指定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください

「Delete」をクリックすると指定のエントリを削除します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Edit」をクリックし、以下の画面で指定エントリの編集を行います。

Network QoS Policy Map			
Create/Delete Network QoS Policy Map Network QoS Policy Map Name 32 chars			Apply
Traffic Policy Network QoS Policy Map Name 32 chars	Network QoS Class Map Name 32 chars		Apply
Total Entries: 1			
	Network QoS Policy Map Name		
	qospolicy		Delete
			1/1  < < 1 > >  Go
qospolicy Rules			
Network QoS (	Class Map Name	Pause	
qos	class	Disabled	Apply         Delete           1/1         <

図 10-24 Network QoS Policy Map (Edit) 画面

画面に表示される項目:

項目	説明
Pause	「Pause」機能を有効 / 無効に指定します。タイプネットワーク QoS ポリシーマップ内参照クラスの PFC を有効にします。
設定を変更する際は、必	ず「Apply」ボタンをクリックし、設定内容を適用してください

# Network QoS Policy Binding(ネットワーク QoS ポリシーバインディング)

本項目ではネットワーク「Quality of Service」(QoS) ポリシーバインディングの設定、表示を行います。

**QoS > QoS PFC > Network QoS Policy Binding**の順にメニューをクリックし、以下の画面を表示します。

Network QoS Policy Bind	ing			
Network QoS Policy Binding Sett	ing			
Unit From Port	To Port Direction	on Network QoS Policy Map Name		
1 V eth1/0/1 V	eth1/0/1 V Input	32 chars	○ None	Apply
Unit 1 Settings				
Port	Direction	Network C	QoS Policy Map Name	
eth1/0/1				
eth1/0/2				
eth1/0/3				
eth1/0/4				
eth1/0/5				
eth1/0/6				
eth1/0/7				
eth1/0/8				

図 10-25 Network QoS Policy Binding 画面

画面に表示される項目:

項目	説明
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。
Direction	「Input」を指定します。インタフェースでポリシーマップはイングレスフローとなります。
Network QoS Policy Map Name	トラフィックポリシーのネットワーク QoS ポリシーマップ名(32 字以内)を指定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください

# PFC Port Settings(PFC ポート設定)

本項目では Priority-based Flow Control (PFC) の設定、表示を行います。

注意 Priority-based Flow Control (PFC) は 10G ポートでのみ有効です。

QoS > QoS PFC > PFC Port Settings の順にメニューをクリックし、以下の画面を表示します。

FC Port S	ettings				_	_
FC Port Set	tings					
Unit	From Port	To Port	Willing			
1 🗸	eth1/0/1 🔽	eth1/0/1 🔽	Disabled 🗸			Apply
ear PFC Co	ounters					
Jnit	From Port	To Port	Frame Type			
1 🔽	eth1/0/1 🔽	eth1/0/1 🔽 🖌 All	Both 🛩			Clear
Init 1 Settin	gs					
Port	PFC Capability	Admin PFC On Prioriti	es Oper PFC On Priorities	Willing	Rx PFC Frame(s)	Tx PFC Frame(s
eth1/0/1	8			Off	0	0
eth1/0/2	8			Off	0	0
eth1/0/3	8			Off	0	0
eth1/0/4	8			Off	0	0
eth1/0/5	8			Off	0	0
	0			0#	0	0

図 10-26 PFC Port Settings 画面

画面に表示される項目:

	· · · · · · · · · · · · · · · · · · ·		
項目	説明		
	PFC Port Settings		
Unit	設定を行うユニットを指定します。		
From Port / To Port	設定するポートの始点 / 終点を設定します。		
Willing	「Willing」機能を有効 / 無効に指定します。「Data Center Bridging Exchange Protocol」(DCBX) PFC willing 機能は指定ポートでリモートシステムからの PFC 設定を受け入れる機能です。		
	Clear PFC Counters		
Unit	設定を行うユニットを指定します。		
From Port / To Port	設定するポートの始点 / 終点を設定します。		
Frame Type	クリアするフレームタイプを指定します。 • RX - 受信 PFC フレームカウンタをクリアします。 • TX - 送信 PFC フレームカウンタをクリアします。 • Both - 送受信 PFC フレームカウンタをクリアします。		

「Apply」をクリックし、設定内容を適用します。

「Clear」をクリックすると入力したエントリをクリアします。

# WRED (WRED 設定)

WRED のプロファイルやキュー、ドロップカウンタの設定を行います。

## WRED Profile (WRED プロファイル設定)

WRED プロファイル設定を行います。

#### QoS > WRED > WRED Profile の順にメニューをクリックし、以下の画面を表示します。

RED Profile	_	_		_	_	_
RED Profile						
rofile (1-128)	Packet Type TCP	Packet Colour Green	Min Thresho 20	old (0-100) Ma 80	ax Threshold (0-100)	Max Drop Rate (0-14) 0 Apply
ofile (1-128)						Find
otal Entries: 128	<b>0</b> . 1 . <b>2</b>			the Theorem 1		
WRED Profile	TOP OPERN	Mir	Threshold	Max Threshold	Max Drop Rate	
	TCP-VELLOW	1	20	80	0	
	TCP-RED		20	80	0	
1	NON-TCP-GRE	EN	20	80	0	Reset Configuration
	NON-TCP-YELL	ow	20	80	0	
	NON-TCP-REI	D	20	80	0	
	TCP-GREEN		20	80	0	
2	TCP-YELLOW	t	20	80	0	
	TCP-RED		20	80	0	Death Configuration
	NON-TCP-GRE	EN	20	80	0	Reset Configuration
	NON-TCP-YELL	OW	20	80	0	
	NON-TCP-REI	D	20	80	0	

図 10-27 WRED Profile Settings 画面

画面に表示される項目:

項目	説明
Profile (1-128)	WRED プロファイル ID を入力します。
Packet Type	パケットタイプ(TCP または Non-TCP)を選択します。
Packet Colour	破棄するパケットカラー(Green、Yellow または Red)を選択します。
Min Threshold (0-100)	使用するしきい値(最小)を入力します。キューサイズがこの値より高いと、カラー「Yellow」が割り当てられます。キューサイズがこの値より低いと、カラー「Green」が割り当てられ、破棄されないことを保証されます。「Yellow」パケットの動作は、このカラーのプロファイル設定に依存します。
Max Threshold (0-100)	使用するしきい値(最大)を入力します。キューサイズがこの値より低いと、カラー「Yellow」が割り当てられます。キューサイズがこの値より高いと、カラー「Red」が割り当てられ、破棄されます。「Yellow」パケットの動作は、このカラーのプロファイル設定に依存します。
Max Drop Rate (0-14)	

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

「Reset Configuration」をクリックして指定エントリの再設定を行います。

## WRED Queue (WRED キュー設定)

WRED のキュー設定を行います。

WRED は指定のしきい値を超えた平均キューサイズのパケットを破棄します。「Explicit Congestion Notification」(ECN) は指定しきい値を超えた平均 キューサイズのパケットを破棄する代わりの、ECN パケット内の WRED の拡張機能です。WRED ECN 機能の設定時にルータとエンドホストはネッ トワークの密集と送信遅延状態を示す「しるし」として使用します。

QoS > WRED >	> WRED Queue	の順にメニュ	ーをクリックし	、以下の画面を表示し	ます。
--------------	--------------	--------	---------	------------	-----

ED Queue	_				
it From Port	To Port eth1/0	CoS WRED	State Profile (1-128)	Weight (0-15) 9	ECN State Disabled Apply
it 1 Settings Port	CoS	WRED State	Exp-weight-constant	Profile	ECN State
	0	Disabled	9	1	Disabled
	1	Disabled	9	1	Disabled
	2	Disabled	9	1	Disabled
alb 1/0/1	3	Disabled	9	1	Disabled
etrillori	4	Disabled	9	1	Disabled
	5	Disabled	9	1	Disabled
	6	Disabled	9	1	Disabled
	7	Disabled	9	1	Disabled
	0	Disabled	9	1	Disabled
	1	Disabled	9	1	Disabled
	2	Disabled	9	1	Disabled
eth1/0/2	3	Disabled	9	1	Disabled
00111012	4	Disabled	9	1	Disabled
	5	Disabled	9	1	Disabled
	6	Disabled	9	1	Disabled
	7	Disabled	9	1	Disabled

図 10-28 WRED Queue 画面

画面に表示される項目:

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	この設定に使用するポート範囲を選択します。
CoS	CoS 値(0-7)を指定します。
WRED State	指定ポートの WRED 状態を有効または無効にします。
Profile	WERD ポートとキューに使用するプロファイル ID を指定します。
Weight (0-15)	通常のキューサイズ計算における重み付け(0-15)を指定します。
ECN State	指定ポートの ECN 機能を有効 / 無効に指定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

## WRED Drop Counter(WRED ドロップカウンタ設定)

WRED のドロップカウンタの設定、表示を行います。

**QoS > WRED > WRED Drop Counter** の順にメニューをクリックし、以下の画面を表示します。

ED Drop Counter			
RED Drop Counter	1 V To Port eth1/0/1 V		Clear Clear All
nit 1 Settings			
Port	Green	Yellow	Red
eth1/0/1	0	0	0
eth1/0/2	0	0	0
eth1/0/3	0	0	0
eth 1/0/4	0	0	0
eth1/0/5	0	0	0
eth1/0/6	0	0	0
eth1/0/7	0	0	0
eth1/0/8	0	0	0

図 10-29 WRED Drop Counter 画面

画面に表示される項目:

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	この設定に使用するポート範囲を選択します。

「Clear」をクリックすると入力したエントリをクリアします。

「Clear All」をクリックすると入力したエントリを全てクリアします。

# iSCSI (アイスカジー)

#### QoS > iSCSI

iSCSI アウェアネスアプリケーションは iSCSI のフローの自動 QoS 優先対応で使用され、次の動作カテゴリに分類されます。:

- ・ iSCSI セッションの構築と終了の検出と iSCSI プロトコルを使用したスヌーピングパケットによる接続
- ・ 進行中の iSCSI セッションデータベースとストアデータ用接続の維持。これにより目的の QoS 対応セッションのデータパケット提供のルールを 分類することができます。
- ・ iSCSI セッショントラフィックに必要なルール群分類の導入と削除。
- ・ セッション終了パケット未受信時のセッションエントリのエージアウトを許可する iSCSI セッションの動作確認。

# iSCSI Settings(アイスカジー設定)

iSCSI の設定、表示を行います。

QoS > iSCSI > iSCSI Settings の順にメニューをクリックし、以下の画面を表示します。

iSCSI Settings			
iSCSI State	OEnabled  OEnabled		
ISCSI CoS	VPT 💙 7	Remark	
Session Aging Time (1-43200)	5 mi	n 🗌 Default	
Maximum Number of Sessions	256		Apply
ISCSI Targets and TCP Ports			
ISCSI Target Port (1-65535)	IP Address	Target Name	
		255 chars	Apply
Total Entries: 1			
TCP Target Port	IP Address	Name	
1	10.90.90.91	target	Delete

図 10-30 iSCSI Settings 画面

#### 画面に表示される項目:

項目	説明
iSCSI State	iSCSI アウェアネス機能を有効/無効に指定します。
iSCSI CoS	設定する iSCSI CoS を指定します。 ・ VPT - iSCSI セッションパケットをアサインする「VLAN Priority Tag」(VPT) を指定します。VPT 値を指定します。 ・ DSCP - iSCSI セッションパケットをアサインする「DSCP」を指定します。DSCP 値を指定します。 ・ Default - 初期値を使用します。初期値では VPT が「7」で使用されます。 イーグレス時に VPT または DSCP の iSCSI フレームをマークする「Remark」を指定します。
Session Aging Time	セッションエージング時間(1-43200/分)を指定します。iSCSI セッションのエージング時間に使用します。現在の設定よりもエージング時間を長くする場合、現在のセッションはタイムアウトされ、新しいエージング時間が採用されます。現在の設定よりもエージング時間を短くする場合、新しいエージング時間よりも長い現セッションは削除され、新しいエージング時間よりも短い、または同じ現セッションは続行され、新しいエージング時間が採用されます。「Default」を指定すると初期値(5分)を使用します。

「Apply」をクリックし、設定内容を適用します。

#### 「iSCSI Targets and TCP Ports」には以下の項目があります。

項目	説明
iSCSI Target Port	iSCSI ターゲットポート番号(1-65535)を指定します。
IP Address	iSCSI ターゲットの IP アドレスを指定します。
Target Name	iSCSI ターゲット名を指定します。文字列は 255 字まで指定可能す。手動での設定の他に、「iSNS」または「sendTargets」 の応答から取得可能です。イニシエータは「iSCSI Initiator Name」と「iSCSI ターゲット名」を最初のセッション / 接続時に ログインリクエストとして表示します。

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

## iSCSI Sessions(アイスカジーセッション)

iSCSIのセッションを表示します。

QoS > iSCSI > iSCSI Sessions の順にメニューをクリックし、以下の画面を表示します。

iSCSI Sessions			
iSCSI Sessions Table			
Total Entries: 0			
Target	Session	Initiator	

図 10-31 iSCSI Sessions 画面

# 第 11 章 ACL (ACL 機能の設定)

ACL メニューを使用し、本スイッチにアクセスプロファイルおよびルールの設定を行うことができます。

サブメニュー	説明
ACL Configuration Wizard(ACL 設定ウィザード)	ACL 設定ウィザードは、アクセスプロファイルと ACL ルールの新規作成を行います。
ACL Access List(ACL アクセスリスト)	ACL アクセスリストの設定を行います。
ACL Interface Access Group(ACL インタフェースアクセ	ACL インタフェースアクセスグループの設定を行います。
スグループ)	
ACL VLAN Access Map(ACL VLAN アクセスマップ)	ACL VLAN アクセスマップの設定を行います。
ACL VLAN Filter(ACL VLAN フィルタ設定)	ACL VLAN フィルタの設定を行います。
CPU ACL(CPU ACL 設定)	CPU インタフェースフィルタリング機能の設定を行います。

# ACL Configuration Wizard (ACL 設定ウィザード)

ウィザードを使用してアクセスプロファイルとルールを作成・更新します。

## ACL Configuration Wizard (ACL 設定ウィザードの開始)

ACL 設定ウィザードは、アクセスプロファイルと ACL ルールの新規作成を行います。

## ACL > ACL Configuration Wizard の順にメニューをクリックし、以下の画面を表示します。

ACL Configuration Wizard		
Access-List Assignment >> Select Packet Type >>	Add Rule >> Apply Port	
Do you want to create a new ACL access-list or upo	late an existing access-list?	
Create		
ACL Name 32 chars		
○ Update		
		Next
Note: The first character of ACL name must be a letter		
11.1 ACL Configuration Minorel (Co		
11-1 ACL Configuration Wizard (Cre	eate) 画面	
ACL Configuration Wizard		
ACL Configuration Wizard		
ACE comparation means		
Access-List Assignment >> Select Packet Type >> /	Add Rule >> Apply Port	
Do you want to create a new ACL access-list or upo	late an existing access-list?	
O Create		
ACL Name 32 chars		
• Update		
Note: The first character of ACL name must be a latter		Next
Note. The first character of ACE name must be a letter		
Total Entries: 6		
ACL Name	ACL Type	Total Rules
O S-IP-ACL	Standard IP ACL	0
O E-IP-ACL	Extended IP ACL	0
O E-MAC-ACL	Extended MAC ACL	0
O E-E-ACL	Extended Expert ACL	0
O S-IPv6-ACL	Standard IPv6 ACL	0
O E-IPv6-ACL	Extended IPv6 ACL	0
		1/1  < < 1 > >  Go

図 11-2 ACL Configuration Wizard (Update) 画面

### 画面に表示される項目:

項目	説明
Create	新しいアクセスルールを作成する場合は、「Create」を選択します。
ACL Name	ACL 名(32 字以内)を指定します。
Update	既存の ACL アクセスリストを表示し、エントリを再設定する場合に選択します。

「Next」をクリックし、パケットタイプの選択を行います。

## パケットタイプ選択(ACL 設定ウィザード)

「ACL Configuration Wizard」にて設定する ACL エントリを指定した後、パケットタイプを指定します。

ACL Configuration Wizard	
ACL Configuration Wizard	
Access-List Assignment >> <u>Select Packet Type</u> >> Add Rule >> Apply Port	
Which type of packet do you want to monitor?	
MAC	
⊙ IPv4	
© IPv6	
	Back Next

図 11-3 ACL Configuration Wizard ((Select Packet Type) 画面

#### 画面に表示される項目:

項目	説明
MAC	MAC アドレスから送信されたパケットを対象に ACL を適用します。
IPv4	IPv4 アドレスから送信されたパケットを対象に ACL を適用します。
IPv6	IPv6 アドレスから送信されたパケットを対象に ACL を適用します。

「Next」をクリックします。選択したパケットの種類により次に表示される画面が違います。プロファイルの種類に合わせた設定方法に従い設定を行います。

## ルール追加(ACL 設定ウィザード)

「ACL Configuration Wizard」にて ACL のパケットタイプを指定した後、各パケットの ACL エントリにおける ACL ルールの追加設定を行います。

## MAC ACL Rule の設定

MAC ACL Rule を設定します。「MAC」を選択し「Next」をクリックし、表示された以下の画面の設定を行います。

ess-List Assignment >>	Select Packet Type >> A	<u>dd Rule</u> >> A	pply Port				
ise assign a sequence n	umber to create a new r	ıle.					
equence No. (1-65535)			OAut	o Assign			
sign rule criteria							
MAC Address	Ethernet Type	802.10	VLAN	]			
				1			
MAC Address							
Any			Any		_		
OHost	11-DF-36-4B-A7-CC	Destination	OHost	11-DF-36-4B-A7-CC			
OMAC	11-DF-36-4B-A7-CC		OMAC	11-DF-36-4B-A7-CC			
Wildcard	11-DF-36-4B-A7-CC		Wildca	d 11-DF-36-4B-A7-CC			
Ethernet Type							
Specify Ethernet Type	Please Se	lect 🗸					
Ethernet Type (0x600-0)	(FFFF)						
Ethernet Type Mask (0x	0-0xFFFF)						
802.1Q VLAN							
CoS Pleas	e Select V Mask (0x0-0	x7)		Inner CoS Plea	se Select V Mas	k (0x0-0x7)	
VID(1-4094)	Mask (0x0-0	xFFF)				· · _	
O VLAN Range	~			Inner VID (1-4094)	Masl	(0x0-0xFFF)	
Time Range	32 chars						
Action	Permit O Den	y O Deny C	PU				
Action							

図 11-4 ACL Configuration Wizard 画面

画面に表示される項目:

項目	説明
	Assign sequence number(シーケンス番号の指定)
Sequence No. (1-65535)	シーケンス番号を指定します。「1」から「65535」の間で指定できます。
Auto Assign	新規ルール用のシーケンス番号を自動でアサインします。
	Assign Rule Criteria (MAC アドレスの設定)
Source	送信元の MAC アドレスを指定します。「Any」「Host」「MAC」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの MAC アドレスを入力します。 「MAC」を選択すると「Wildcard」オプションが選択可能になり送信元 MAC アドレスとワイルドカードを入力する ことができます。
Destination	宛先の MAC アドレスを指定します。「Any」「Host」「MAC」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択すると宛先ホストの MAC アドレスを入力します。 「MAC」を選択すると「Wildcard」オプションが選択可能になり宛先 MAC アドレスとワイルドカードを入力するこ とができます。
Specify Ethernet Type	イーサネットタイプを選択します。「aarp」「appletalk」「decent-iv」「etype-6000」「etype-8042」「lat」「lavc-sca」 「mop-console」「mop-dump」「vines-echo」「vines-ip」「xns-idp」「arp」から選択します。
Ethernet Type	イーサネットタイプの 16 進数値を指定します。0x0 から 0xFFFF の間で指定できます。「Specify Ethernet Type」で 指定したイーサネットタイプに基づき適切な値が入力されます。
Ethernet Type Mask	イーサネットタイプマスクの 16 進数値を指定します。0x0 から 0xFFFF の間で指定できます。「Specify Ethernet Type」で指定したイーサネットタイプに基づき適切な値が入力されます。
CoS	CoSの値を入力します。0から7の間で入力できます。「Mask」にマスクを入力します。
Inner CoS	inner CoS の値を入力します。0 から 7 の間で入力できます。「Mask」にマスクを入力します。
VID	ACL ルールに関連する VLAN ID を入力します。1 から 4094 の間で入力可能です。「Mask」にマスクを入力します。
Inner VID	ACLルールに関連する inner VLAN IDを入力します。1から4094の間で入力可能です。「Mask」にマスクを入力します。
VLAN Range	ACL ルールに関連する VLAN 範囲を入力します。1 から 4094 の間で入力可能です。
Time Range	ACL ルールに関するタイムレンジ名を指定します。
Action	ルールド動作に関する設定を行います。「Permit」または「Deny」「Deny CPU」から指定できます。

「Next」をクリックします。

「Back」をクリックすると前のページに戻ります。

## IPv4 ACL Rule の設定

IPv4 ACL Rule を設定します。「IPv4」を選択し「Next」をクリックし、表示された以下の画面の設定を行います。

cess-List Assignment >> S	elect Packet Type >> <u>A</u>	dd Rule >> Apply Port				
Sequence No. (1-65535)			ian			
otocol Type	TCP		(0-255) Mask (0x0-0xFF)		Fragments	
ssign rule criteria						
IPv4 Address	Port	IPv4 DSCP	TCP Flag			
IPv4 Address		Anv				
OHost		OHost				
Source OIP		Destination OIP				
Wildcard		Wildca	rd v v v			
Dert						
Source Port Please 9	Select V					
Please		(0-65535) Place	e Select	(0-65535)		
Destination Port Please		(0 00000) [11000		(0.00000)		
Please		(0-65535) Pleas	e Select	(0-65535)		
10400				(0 00000)		
IPV4 DSCP	Select Value (0	.7)	Mask (0v0.0v7)			
ToS     Please	Select Value (0	-15)	Mask (0x0-0x7)			
ODSCP (0-63) Please	Select Value (0	-63)	Mask (0x0-0x3F)			
Top 51-						
	lpsh 🗌 rst 🗌 syn 🗍 i	Ira				
		~ 9				
Time Deserve	0.0					

図 11-5 ACL Configuration Wizard -IPv4 画面

画面に表示される項目	:	
------------	---	--

項目	説明		
	Assign sequence number:(シーケンス番号の指定)		
Sequence No. (1-65535)	シーケンス番号を指定します。「1」から「65535」の間で指定できます。		
Auto Assign	新規ルール用のシーケンス番号を自動でアサインします。		
Protocol Type	<ul> <li>プロトコルの種類を選択します。「TCP」「UDP」「ICMP」「EIGRP」「ESP」「GRE」「IGMP」「OSPF」「PIM」「VRRP」「IP-in-IP」</li> <li>「PCP」「Protocol ID」「None」から選択します。</li> <li>Value - 選択したプロトコルの種類によってはプロトコルに関連する数値(ID等)を右の欄に入力する必要があり ます。その際、欄の右にある制限値(0-255等)に注意して入力してください。</li> <li>Mask - 「Protocol ID」選択後、プロトコルマスク(0x0-0xFF)を入力します。</li> <li>Fragments - パケットフラグメントフィルタを含む場合に指定します。</li> </ul>		

選択したプロトコルにより表示される項目が異なります。以下の表示項目を参照してください。

#### すべてのプロトコル選択時に表示される項目(IPv4 ACL Rule)

項目	説明
Source	送信元のアドレスを指定します。「Any」「Host」「IP」から指定します。
	「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。
	「Host」を選択するとホストの IP アドレスを入力します。
	「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い送信元 IP アド
	レス群を入力します。ビットは1の値が無視され、0が認識されます。
Destination	宛先のアドレスを指定します。「Any」「Host」「IP」から指定します。
	「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。
	「Host」を選択するとホストの IP アドレスを入力します。
	「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い宛先 IP アドレ
	ス群を入力します。ビットは1の値が無視され、0が認識されます。
IP Precedence	IP 優先値を指定します。「0 (routine)」「1 (priority)」「2, (immediate)」「3 (flash)」「4 (flash-override)」「5 (critical)」「6
	(internet)」「7 (network)」から指定できます。「Mask」にマスクを入力します。
ToS	IP 優先値を選択後、使用する「Type-of-Service」(ToS) の値を指定します。「0 (normal)」「1 (min-monetary-cost)」「2
	(max-reliability)」「3, 4(max-throughput)」「5, 6, 7, 8 (min-delay)」「9」「10」「11」「12」「13」「14」「15」から指定
	できます。「Mask」にマスクを入力します。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。「Mask」にマスクを入力します。
Time Range	ACL ルールに関するタイムレンジ名を指定します。
Action	ルールド動作に関する設定を行います。「Permit」または「Deny」「Deny CPU」から指定できます。

#### 「TCP」選択時に表示される項目(IPv4 ACL Rule)

項目	説明
Source Port	送信元ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。
Destination Port	宛先ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択 した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると 選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが 使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウン リストに選択するポート番号がない場合は項目欄に手動で指定できます。
TCP Flag	TCP フラグを本ルールに含める場合、該当のフラグにチェックを入れます。「ack」「fin」「psh」「rst」「syn」「urg」 から指定できます。

## 「UDP」選択時に表示される項目(IPv4 ACL Rule)

項目	説明
Source Port	送信元ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選 択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択する と選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポート が使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウ ンリストに選択するポート番号がない場合は項目欄に手動で指定できます。
Destination Port	宛先ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択 した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると 選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが 使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウン リストに選択するポート番号がない場合は項目欄に手動で指定できます。

#### 「ICMP」選択時に表示される項目(IPv4 ACL Rule)

項目	説明
Specify ICMP Message Type	使用する ICMP メッセージの種類を指定します。自動的に ICMP メッセージ種類の数値とメッセージコードは指定 されます。
ICMP Message Type	ICMP メッセージを指定しない場合、手動で ICMP メッセージ種類の数値を指定します。
Message Code	ICMP メッセージを指定しない場合、手動でメッセージコードを指定します。

## 「EIGRP」「ESP」「GRE」「IGMP」「OSPF」「PIM」「VRRP」「IP-in-IP」「PCP」「Protocol ID」「None」選択時に表示される項目(IPv4 ACL Rule)

項目	説明
Fragments	パケットフラグメントフィルタリングを使用する場合、選択します。

「Next」をクリックします。

## IPv6 ACL Rule の設定

IPv6 ACL Rule を設定します。「IPv6」を選択し「Next」をクリックし、表示された以下の画面の設定を行います。

Sequence No. (1-65535) tocol Type TCP ♥ (0-255) Mask (0x0-0xFF) Fragments ssign rule criteria IPv6 Address Port IPv6 DSCP TCP Flag Flow Label IPv6 Address ● Any ● Host 2012::1 PHost 2012::1 Prefix Length Prefix Length Port Source Port Please Select ♥ Please Select ♥	
tocol Type TCP ♥ (0-255) Mask (0x0-0xFF) Fragments ssign rule criteria IPv6 Address Port IPv6 DSCP TCP Flag Flow Label IPv6 Address ● Any ● Host 2012::1 ● Host 2012::1 ● Host 2012::1 ● Host 2012::1 ● Prefix Length Prefix Length Port Source Port Please Select ♥ ● Ple	
IPv6 Address     Port     IPv6 DSCP     TCP Flag     Flow Label       IPv6 Address <ul> <li>Any</li> <li>Host</li> <li>2012::1</li> <li>Destination</li> <li>IPv6</li> <li>2012::1</li> <li>Prefix Length</li> <li>Prefix Length</li> <li>Prefix Length</li> <li>Please Select ♥</li> <li>(0-65535) Please Select ♥</li></ul>	
IPv6 Address     Port     IPv6 DSCP     TCP Flag     Flow Label       IPv6 Address <ul> <li>Any</li> <li>Host</li> <li>2012::1</li> <li>Destination</li> <li>IPv6</li> <li>2012::1</li> <li>Destination</li> <li>IPv6</li> <li>2012::1</li> <li>Prefix Length</li> <li>Prefix Length</li> <li>Prefix Length</li> <li>Prefix Length</li> <li>Please Select ♥</li> <li>(0-65535) Please Select ♥</li> <li>(0-65535)</li></ul>	
IPv6 Address         ● Any       ● Host       2012::1       ● Host       2012::1         Source       ● IPv6       2012::1       ● IPv6       2012::1         ● Prefix Length       ● Prefix Length       ● Prefix Length         Port       ●       ●       ●         Source Port       ● Iease Select ♥       ●       ●         ● Destination       ● Iease Select ♥       ●       ●         ● Iease Select ♥       ●       ●       ●	
IPv6 Address	
OHINY     OHINY       Host     2012::1       OHOSt     2012::1       OHOSt     2012::1       OHOSt     2012::1       Prefix Length     Prefix Length   Port Source Port Please Select Please Select O(0-65535) Please Select	
Source OIPv6 2012::1 Destination OIPv6 2012::1 Prefix Length Prefix Length Port Source Port Please Select  (0-65535) Please Se	
Prefix Length     Prefix Length       Port     Source Port       Please Select     (0-65535)       Destination Port     Please Select       Please Select     (0-65535)       Please Select     (0-65535)	
Port Source Port Please Select (0-65535) P	
Port         Source Port         Please Select         Please Select         Destination Port         Please Select	
Source Port       Please Select         Please Select       (0-65535)         Destination Port       Please Select         Please Select       (0-65535)         Please Select       (0-65535)         Please Select       (0-65535)	
Please Select       (U-65535)         Destination Pot       Please Select         Please Select       (U-65535)         Please Select       (U-65535)	
Please Select     Image: Constraint of the select     Image: Conselect     Image: Constraint of the select	
Please Select V (U-65535) Please Select V (U-65535)	
IPv6 DSCP	
DSCP (0-63) Please Select Mask (0x0-0x3F)	
O Traffic Class (0-255) Mask (0x0-0xFF)	
TCP Flag	
TCP Flag ack fin psh rst syn urg	
Flow Label	
Flow Label (0-1048575) Mask (0x0-0xFFFF)	
Time Range 32 chars	

図 11-6 ACL Configuration Wizard -IPv6 画面

画面に表示される項目	:
------------	---

項目	説明
	Assign sequence number:(シーケンス番号の指定)
Sequence No. (1-65535)	シーケンス番号を指定します。「1」から「65535」の間で指定できます。
Auto Assign	新規ルール用のシーケンス番号を自動でアサインします。
Protocol Type	プロトコルの種類を選択します。「TCP」「UDP」「ICMP」「ESP」「PCP」「Protocol ID」「SCTP」「None」から選択します。 選択したプロトコルの種類によってはプロトコルに関連する数値(ID等)を右の欄に入力する必要があります。その際、 欄の右にある制限値(0-255等)に注意して入力してください。 ・ Value - 選択したプロトコルの種類によってはプロトコルに関連する数値(ID等)を右の欄に入力する必要があり ます。その際、欄の右にある制限値(0-255等)に注意して入力してください。 ・ Mask - 「Protocol ID」選択後、プロトコルマスク(0x0-0xFF)を入力します。 ・ Fragments - パケットフラグメントフィルタを含む場合指定します。

選択したプロトコルにより表示される項目が異なります。以下の表示項目を参照してください。

#### すべてのプロトコル選択時に表示される項目(IPv6 ACL Rule)

項目	説明
Source	送信元のアドレスを指定します。「Any」「Host」「IPv6」から指定します。
	「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。
	「Host」を選択するとホストの IPv6 アドレスを入力します。
	「IPv6」を選択すると「Prefix Length」が指定可能になり、送信元 IPv6 アドレスと Prefix Length を入力します。
Destination	宛先のアドレスを指定します。「Any」「Host」「IPv6」から指定します。
	「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。
	「Host」を選択するとホストの IPv6 アドレスを入力します。
	「IPv6」を選択すると「Prefix Length」が指定可能になり、宛先 IPv6 アドレスと Prefix Length を入力します。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。「Mask」には適用するマスクを入力します。
Flow Label	フローラベルの値を入力します。0 から 1048575 まで指定可能です。「Mask」には適用するマスクを入力します。
Time Range	ACL ルールに関するタイムレンジ名を指定します。
Action	ルールド動作に関する設定を行います。「Permit」または「Deny」「Deny CPU」から指定できます。

## 「TCP」選択時に表示される項目(IPv6 ACL Rule)

項目	説明
Source Port	送信元ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選 択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択する と選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポート が使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウ ンリストに選択するポート番号がない場合は項目欄に手動で指定できます。「Mask」には適用するマスクを入力し ます。
Destination Port	宛先ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択 した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると 選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが 使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウン リストに選択するポート番号がない場合は項目欄に手動で指定できます。「Mask」には適用するマスクを入力します。
TCP Flag	TCP フラグを本ルールに含める場合、該当のフラグにチェックを入れます。「ack」「fin」「psh」「rst」「syn」「urg」 から指定できます。

## 「UDP」選択時に表示される項目(IPv6 ACL Rule)

項目	説明
Source Port	送信元ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選 択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択する と選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポート が使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウ ンリストに選択するポート番号がない場合は項目欄に手動で指定できます。「Mask」には適用するマスクを入力し ます。
Destination Port	宛先ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択 した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると 選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが 使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウン リストに選択するポート番号がない場合は項目欄に手動で指定できます。「Mask」には適用するマスクを入力します。

## 「ICMP」選択時に表示される項目(IPv6 ACL Rule)

項目	説明
Specify ICMP Message Type	使用する ICMP メッセージの種類を指定します。自動的に ICMP メッセージ種類の数値とメッセージコードは指定
	されます。
ICMP Message Type	ICMP メッセージを指定しない場合、手動で ICMP メッセージ種類の数値を指定します。
Message Code	ICMP メッセージを指定しない場合、手動でメッセージコードを指定します。

#### 「ESP」「PCP」「Protocol ID」「SCTP」「None」選択時に表示される項目(IPv6 ACL Rule)

項目	説明
Fragments	パケットフラグメントフィルタリングを使用する場合、選択します。
- 「Next」をクリックします。	

パケットタイプ、プロトコルの設定後、「Next」をクリックすると以下の画面が表示されます。

# ポート設定(ACL 設定ウィザード)

「ACL Configuration Wizard」にて適用するポートの設定を行います。

ACL Config	juration	Wizard	_	_	_	_	_	_	_		_
ACL Configur	ration Wiza	rd									
Access-List Which port(s	Assignmer s) do you wa	nt >> Select Pack ant to apply the A	et Type > ccess-Li	> Add Rule >> <u>Ap</u> st?	ply Port						
Unit		From Port		To Port		Direction					
1	•	eth1/0/1	•	eth1/0/1	•	In	•				
										Back	Apply

図 11-7 ACL Configuration Wizard (Apply Port) 画面

#### 画面に表示される項目:

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	設定の対象となるポート範囲を指定します。
Direction	方向を指定します。「In」「Out」が選択可能です。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。 「Back」をクリックすると前のページに戻ります。

# ACL Access List (ACL アクセスリスト)

ACL アクセスリストの設定、表示を行います。

ACL > ACL Access List の順にメニューをクリックし、以下の画面を表示します。

L Access	List							
CL Type	All	ID (1-14999)			Name 32 chars			Find
otal Entrie	s: 6							Add ACL
ID	ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark		
1	S-IP-ACL	Standard IP ACL	10	10	Enabled		Edit	Delete
2000	E-IP-ACL	Extended IP ACL	10	10	Disabled		Edit	Delete
6000	E-MAC-ACL	Extended MAC ACL	10	10	Disabled		Edit	Delete
8000	E-E-ACL	Extended Expert ACL	10	10	Disabled		Edit	Delete
11000	S-IPv6-ACL	Standard IPv6 ACL	10	10	Disabled		Edit	Delete
13000	E-IPv6-ACL	Extended IPv6 ACL	10	10	Disabled		Edit	Delete
						1/1 <	< 1 :	> >  G
-IP-ACL (IE	): 1) Rule				Clear	All Counter C	lear Counter	Add Rule
Sequence	No. Action	Rule	Time R	ange	Co	unter		
10	Permit	any any			(Ing: 0 pad	ckets Egr: 0		Delete
						1/1	< 1	> >  G

図 11-8 ACL Access List 画面

#### 画面に表示される項目:

項目	説明
ACL Type	ACL プロファイルの種類を選択します。「AII」「IP ACL」「IPv6 ACL」「MAC ACL」「Expert ACL」から選択します。
ID	ACL ID を入力します。1 から 14999 の範囲で入力できます。
ACL Name	ACL 名を入力します。32 文字まで指定できます。
「Find」ボタンをクリック	クし、入力した情報を元に特定のエントリを指定します。

「Clear All Counter」ボタンをクリックし、表示されたすべてのカウンタ情報を消去します。

「Clear Counter」ボタンをクリックし、表示された指定ルールのカウンタ情報を消去します。

「Add Rule」ボタンをクリックし、ACL ルールを作成します。

「Add ACL」ボタンをクリックし、新しい ACL プロファイルを作成します。

「Edit」をクリックして、指定エントリの編集を行います。

「Delete」をクリックすると指定のエントリを削除します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

## Standard IP ACL(通常 IP ACL)

#### Standard IP ACL の作成(Add ACL)

「Add ACL」をクリックし新しい ACL プロファイルを作成します。以下の画面が表示されます。

CL Type	Standard IP ACL	
) (1-1999)		
CL Name	32 chars	
		Apply
ote: The first ch	aracter of ACL name must be a letter.	

#### 画面に表示される項目:

項目	説明
ACL Type	ACL プロファイルの種類を選択します。「Standard IP ACL」「Extended IP ACL」「Standard IPv6 ACL」「Extended IPv6 ACL」
	「Extended MAC ACL」「Extended Expert ACL」から選択します。
ID	ACL ID を入力します。1 から 1999 の範囲で入力できます。
ACL Name	ACL 名を入力します。32 文字まで指定できます。

「Apply」ボタンをクリックして、設定を適用します。

ACL プロファイルを作成すると、「ACL Profile Table」に新しく作成した ACL プロファイルが以下の様に表示されます。

CL Type	All	•	ID (1-14999)			ACL Name 32 ch	ars	Find
otal Entries	:1							Add ACL
ID AC	L Name	AC	L Type	Start Sequence No.	Step	Counter State	Remark	
1 Sta	indardIP	Standa	ard IP ACL	10	10	Disabled		Edit Delete
							1/1	< < 1 > > <
						le la		Class Country Add Dula

図 11-10 Standard IP ACL (Main) 画面

「Edit」をクリックし、指定 ACL プロファイルの編集を行います。 「Delete」ボタンをクリックし、指定 ACL プロファイルの削除を行います。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

ACL プロファイルにルールを追加する場合、ACL プロファイルを選択後「Add Rule」ボタンをクリックします。

## ACL ルールの追加 (Add Rule) (Standard IP ACL)

「Add Rule」をクリックし新しい ACL ルールを追加します。

ACL プロファイルを選択後「Add Rule」ボタンをクリックすると、以下の画面が表示され新しい ACL ルールを設定できます。

Id ACL Rule		
D	1	
ACL Name	SIPACL	
ACL Type	Standard IP ACL	
Sequence No. (1-65535)	ti)	it isn't specified, the system automatically assigns.)
Action	Permit O Deny O D	Deny CPU
Match IP Address		
Any		(● Any
⊖ Host	4 - 4 - 4	O Host
Source OIP	Destination	
Wildcard	· · · ·	Wildcard · · ·
ime Ranne	32 chars	

図 11-11 Standard IP ACL (Add Rule) 画面

画面に表示される項目:

項目	説明
Sequence No. (1-65535)	シーケンス番号を指定します。「1」から「65535」の間で指定できます。値を指定しない場合は自動的に番号が割
	り振られます。
Action	ルール動作に関する設定を行います。「Permit」または「Deny」「Deny CPU」から指定できます。
Source	送信元のアドレスを指定します。「Any」「Host」「IP」から指定します。
	「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。
	「Host」を選択するとホストの IP アドレスを入力します。
	「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い送信元 IP アド
	レス群を入力します。ビットは1の値が無視され、0が認識されます。
Destination	宛先のアドレスを指定します。「Any」「Host」「IP」から指定します。
	「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。
	「Host」を選択するとホストのIPアドレスを入力します。
	「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い宛先 IP アドレ
	ス群を入力します。ビットは1の値が無視され、0が認識されます。
Time Range	ACL ルールに関するタイムレンジ名を指定します。

「Back」ボタンをクリックして、変更を破棄し前の画面に戻ります。 「Apply」ボタンをクリックして、設定を適用します。

## ACL ルールの編集(Edit)(Standard IP ACL)

「Counter State」オプションの有効化やプロファイルへの「Remark」の入力など ACL ルールの編集を行う場合、「ACL Profile Table」で該当するプロ ファイル横の「Edit」ボタンをクリックします。以下の画面が表示されます。

CL Access Lis	st	_	_	_	_	
ACL Access List						
ACL Type	All 🔻	ID (1-14999)		O ACL	Name 32 chars	Find
Total Entries: 1						Add ACL
ID ACL Name	ACL Type	Start Sequence No.	Step	Counter St	ate Remark	
1 StandardIP	Standard IP ACL	10	10	Disabled	-	Apply Delete
						1/1  < < 1 > >   Go
StandardIP (ID: 1) I	Rule				Clear All Co	ounter Clear Counter Add Rule
Sequence No.	Action	Rule		Time Range	Counter	
10	Permit	any any				Delete
						1/1  < < 1 > > Go

図 11-12 Standard IP ACL (Edit ACL) 画面

画面に表示される項目:

項目	説明
Start Sequence No.	シーケンス番号の開始番号を指定します。
Step	シーケンス番号の増加番号を指定します。
Counter State	カウンタ機能の「Enabled」(有効)/「Disabled」(無効)を指定します。
Remark	指定プロファイルと関連するリマークを入力します。
<b>F</b> ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) (	

「Apply」ボタンをクリックして、設定を適用します。

「Delete」ボタンをクリックして、指定エントリを削除します。

特定の ACL プロファイルに関連する ACL ルール表示するには「ACL Profile Table」で該当の ACL プロファイルを選択します。ACL ルールが表示されます。

CL ACCESS LI	st			_		_	_	_	
CL Type	All	<ul> <li>ID (1-14999)</li> </ul>			ACL Name	32 chars			Find
otal Entries: 1									Add ACL
ID ACL Na	ne	ACL Type	Start Sequence No	o. Step	Counter S	State	Remark		
1 Standar	dIP	Standard IP ACL	10	10	Enable	ed		Edit	Delete
							1/1	< < 1	> >  G
tandardIP (ID: 1)	Rule					Clear	All Counter	Clear Counter	Add Rule
Sequence No.	Action	Rule		Time Ran	ge	Co	unter		
10	Permit	any any				(Ing: 0	packets)		Delete
							1/1	< < 1	> >  G

図 11-13 Standard IP ACL (Rule Display) 画面

「Delete」ボタンをクリックして、指定ルールを削除します。 複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

## Extended IP ACL(拡張 IP ACL)

## Extended IP ACL の作成(Add ACL)

「Add ACL」をクリックし新しい ACL プロファイルを作成します。以下の画面が表示されます。

	S LIST	
Add ACL Access Lis	st	
ACL Type	Extended IP ACL T	
ID (2000-3999)		
ACL Name	32 chars	
		Apply
Note: The first chara	acter of ACL name must be a letter.	

図 11-14 Extended IP ACL (Add ACL Access List) 画面

画面に表示される項目:

項目	説明
ACL Type	ACL プロファイルの種類を選択します。「Standard IP ACL」「Extended IP ACL」「Standard IPv6 ACL」「Extended IPv6 ACL」
	「Extended MAC ACL」「Extended Expert ACL」から選択します。
ID	ACL ID を入力します。2000 から 3999 の範囲で入力できます。
ACL Name	ACL 名を入力します。32 文字まで指定できます。

「Apply」ボタンをクリックして、設定を適用します。

ACL プロファイルを作成すると、「ACL Profile Table」に新しく作成した ACL プロファイルが以下の様に表示されます。

ICL Access	All	<ul> <li>ID (1-14999)</li> </ul>			ACL Name 32 chars		Find
otal Entries	s: 2						Add ACL
ID	ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark	
1	StandardIP	Standard IP ACL	10	10	Enabled		Edit Delete
2000	ExtendIP	Extended IP ACL	10	10	Disabled		Edit Delete
						1/1	< 1 > > (
					Clea	ar All Counter	lear Counter Add Rule
Sequence	No. Action	Rule	Ті	me Range		Counter	

図 11-15 Extended IP ACL (Main) 画面

「Edit」をクリックし、指定 ACL プロファイルの編集を行います。 「Delete」ボタンをクリックし、指定 ACL プロファイルの削除を行います。 複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

ACL プロファイルにルールを追加する場合、ACL プロファイルを選択後「Add Rule」ボタンをクリックします。

## ACL ルールの追加 (Add Rule)(Extended IP ACL)

「Add Rule」をクリックし新しい ACL ルールを追加します。

ACL プロファイルを選択後「Add Rule」ボタンをクリックすると、以下の画面が表示され新しい ACL ルールを設定できます。

dd ACL Rule	
D ACL Name ACL Type Sequence No. (1-85535) Action Protocol Type	2000         EIPACL           Extended IP ACL         (If it isn't specified, the system automatically assigns.)                • Permit Openy Openy CPU          Deny CPU            TCP         (0-255) Mask (0x0-0xFF)         Fragments
Match IP Address	
Any  Host  IP  Wildcard  Match Port	· · ·     Destination       · ·     · · ·       · ·     · · ·       · · ·     · · ·       · · ·     · · · ·       · · ·     · · · ·       · · ·     · · · ·       · · ·     · · · ·
Source Port Disase Salas	
Destination Port Please Selec Please Selec Please Selec Please Selec	t V (0-65535) Please Select V (0-65535) t V (0-65535) Please Select V (0-65535))
Destination Port Please Selec Please Selec Please Selec Please Selec	t v (0-65535) Please Select v (0-65535) t v (0-65535) Please Select v (0-65535)) ack fin psh rst syn urg
Control Point Please Select Please Select Please Select Please Select Please Select Please Select CP Flag IP Precedence Please Select ToS Please Select ODSCP (0-63) Please Select Time Range	t v (0-65535) Please Select v (0-65535) t v (0-65535) Please Select v (0-65535)) ack fin psh rst syn urg ct v Value (0-7) Mask (0x0-0x7) ct v Value (0-15) Mask (0x0-0xF) ct v Value (0-63) Mask (0x0-0x3F) 32 chars

図 11-16 Extended IP ACL (Add Rule) 画面

#### 画面に表示される項目:

項目	説明
Sequence No. (1-65535)	シーケンス番号を指定します。「1」から「65535」の間で指定できます。値を指定しない場合は自動的に番号が割り振ら れます。
Action	ルール動作に関する設定を行います。「Permit」または「Deny」「Deny CPU」から指定できます。
Protocol Type	プロトコルの種類を選択します。「TCP」「UDP」「ICMP」「EIGRP (88)」「ESP (50)」「GRE (47)」「IGMP (2)」「OSPF (89)」 「PIM (103)」「VRRP (112)」「IP-in-IP (94)」「PCP (108)」「Protocol ID」「None」から選択します。 選択したプロトコルの種類によってはプロトコルに関連する数値(ID 等)を右の欄に入力する必要があります。そ の際、欄の右にある制限値(0-255 等)に注意して入力してください。

選択したプロトコルにより表示される項目が異なります。以下の表示項目を参照してください。

#### すべてのプロトコルタイプに表示される項目(Extended IP ACL)

「Protocol Type」でどの項目を選択しても表示される項目です。(以下の画面は TCP 選択時のものです。)

Add ACL Rule	
Add ACL Rule	
ID	2000
ACL Name	ExtendIP
ACL Type	Extended IP ACL
Sequence No. (1-65535)	(If it isn't specified, the system automatically assigns.)
Action	ermit O Deny
Protocol Type	TCP (0-255) Fragments
Match IP Address	
<ul> <li>Any</li> </ul>	Any
Host	⊘ Host
Source	Destination O IP
Wildcard	Wildcard
Match Port	
Source Port Please Select	
Please Select	▼ (0-65535) Please Select ▼ (0-65535)
Destination Port Please Select	
Please Select	▼ (0-65535) Please Select ▼ (0-65535)
TCP Flag	ack fin psh rst syn urg
IP Precedence Diseas Cale	
Precedence Please Sele	
DSCP (0-03) Please Sele	
Time Range	32 chars
	Back Apply

図 11-17 Extended IP ACL (Add Rule) TCP 画面

#### すべてのプロトコル選択時に表示される項目(Extended IP ACL)

項目	説明
Source	送信元のアドレスを指定します。「Any」「Host」「IP」から指定します。
	「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。
	「Host」を選択するとホストのIPアドレスを入力します。
	「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い送信元 IP アド
	レス群を入力します。ビットは1の値が無視され、0が認識されます。
Destination	宛先のアドレスを指定します。「Any」「Host」「IP」から指定します。
	「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。
	「Host」を選択するとホストの IP アドレスを入力します。
	「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い宛先 IP アドレ
	ス群を入力します。ビットは1の値が無視され、0が認識されます。
IP Precedence	IP 優先値を指定します。「0 (routine)」「1 (priority)」「2, (immediate)」「3 (flash)」「4 (flash-override)」「5 (critical)」「6
	(internet)」「7 (network)」から指定できます。「Mask」には適用するマスクを入力します。
ToS	IP 優先値を選択後、使用する「Type-of-Service」(ToS) の値を指定します。「0 (normal)」「1 (min-monetary-cost)」「2
	(max-reliability)」「3, 4(max-throughput)」「5, 6, 7, 8 (min-delay)」「9」「10」「11」「12」「13」「14」「15」から指定
	できます。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。「Mask」には適用するマスクを入力します。
Time Range	ACL ルールに関するタイムレンジ名を指定します。

## 「TCP」選択時に表示される項目(Extended IP ACL)

項目	説明
Source Port	送信元ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択する と選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポート が使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウ ンリストに選択するポート番号がない場合は項目欄に手動で指定できます。「Mask」には適用するマスクを入力し ます。
Destination Port	宛先ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択 した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると 選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが 使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウン リストに選択するポート番号がない場合は項目欄に手動で指定できます。「Mask」には適用するマスクを入力します。
TCP Flag	TCP フラグを本ルールに含める場合、該当のフラグにチェックを入れます。「ack」「fin」「psh」「rst」「syn」「urg」 から指定できます。

## 「UDP」選択時に表示される項目(Extended IP ACL)

項目	説明
Source Port	送信元ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選 択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択する と選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポート が使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウ ンリストに選択するポート番号がない場合は項目欄に手動で指定できます。「Mask」には適用するマスクを入力し ます。
Destination Port	宛先ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択 した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると 選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが 使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウン リストに選択するポート番号がない場合は項目欄に手動で指定できます。「Mask」には適用するマスクを入力します。

### 「ICMP」選択時に表示される項目(Extended IP ACL)

項目	説明
Specify ICMP Message Type	使用する ICMP メッセージの種類を指定します。自動的に ICMP メッセージ種類の数値とメッセージコードは指定
	されます。
ICMP Message Type	ICMP メッセージを指定しない場合、手動で ICMP メッセージ種類の数値を指定します。
Message Code	ICMP メッセージを指定しない場合、手動でメッセージコードを指定します。

#### 「EIGRP」「ESP」「GRE」「IGMP」「OSPF」「PIM」「VRRP」「IP-in-IP」「PCP」「Protocol ID」「None」選択時に表示される項目(Extended IP ACL)

項目	説明
Fragments	パケットフラグメントフィルタリングを使用する場合、選択します。
- 「Back」ボタンをクリックして、	変更を破棄し前の画面に戻ります。

「Apply」ボタンをクリックして、設定を適用します。

## ACL ルールの編集(Edit)(Extended IP ACL)

「Counter State」オプションの有効化やプロファイルへの「Remark」の入力など ACL ルールの編集を行う場合、「ACL Profile Table」で該当するプロ ファイル横の「Edit」ボタンをクリックします。以下の画面が表示されます。

ACL Ad	cess List	_		_	_	-			_
ACL Ac	cess List								
ACL Ty	pe All	•	ID (1-14999)		O ACL	Name	32 chars	Find	
Total E	ntries: 2							Add ACL	
ID	ACL Name	ACL Type	Start Sequence No.	Step	Counter	State	Remark		
1	StandardIP	StandardIP Standard IP ACL 10		10	Enabled			Edit Delete	
2000	ExtendIP	Extended IP ACL	10	10	Disabled	-		Apply Delete	
							1/1		Go
Extend	IP (ID: 2000) Ru	le					Clear All Counter	Clear Counter Add Rule	
Sequ	ence No.	Action	Rule	T	ime Range		Counter		
	10	Permit	any any					Delete	
							1/1		Go

図 11-18 Extended IP ACL (Edit ACL) 画面

#### 画面に表示される項目:

項目	説明
Start Sequence No.	シーケンス番号の開始番号を指定します。
Step	シーケンス番号の増加番号を指定します。
Counter State	カウンタ機能の「Enabled」(有効)/「Disabled」(無効)を指定します。
Remark	指定プロファイルと関連するリマークを入力します。
E	

「Apply」ボタンをクリックして、設定を適用します。

「Delete」ボタンをクリックして、指定エントリを削除します。

特定の ACL プロファイルに関連する ACL ルール表示するには「ACL Profile Table」で該当の ACL プロファイルを選択します。ACL ルールが表示されます。

CL Access	List							
CL Type	All	ID (1-14999)			ACL Name 32 chars			Find
otal Entries	s: 2							Add ACL
ID	ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark		
1	StandardIP	Standard IP ACL	10	10	Enabled		Edit	Delete
2000	ExtendIP	Extended IP ACL	10	10	Enabled		Edit	Delete
						1/1	< < 1	> >  G
ktendiP (ID	: 2000) Rule				Clea	r All Counter	lear Counter	Add Rule
Sequence No. Action Rule		Ti	Time Range		Counter			
10 Permit any any					(Ing	0 packets)		Delete

図 11-19 Extended IP ACL (Rule Display) 画面

「Delete」ボタンをクリックして、指定ルールを削除します。 複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

## Standard IPv6 ACL(通常 IPv6 ACL)

#### Add ACL(Standard IPv6 ACL の作成)

「Add ACL」をクリックし新しい ACL プロファイルを作成します。以下の画面が表示されます。

Add ACL Acces	s List t	
ACL Type	Standard IPv6 ACL V	
ID (11000-12999)		
ACL Name	32 chars	
		Apply
Note: The first chara	cter of ACL name must be a letter.	

図 11-20 Standard IPv6 ACL (Add ACL Access List) 画面

画面に表示される項目:

項目	説明
ACL Type	ACL プロファイルの種類を選択します。「Standard IP ACL」「Extended IP ACL」「Standard IPv6 ACL」「Extended IPv6 ACL」
	「Extended MAC ACL」「Extended Expert ACL」から選択します。
ID	ACL ID を入力します。11000 から 12999 の範囲で入力できます。
ACL Name	ACL 名を入力します。32 文字まで指定できます。

「Apply」ボタンをクリックして、設定を適用します。

ACL プロファイルを作成すると、「ACL Profile Table」に新しく作成した ACL プロファイルが以下の様に表示されます。

CL Access	All •	ID (1-14999)			ACL Name 32 chars			Find
otal Entries	:3							Add ACL
ID	ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark		
1	StandardIP	Standard IP ACL	10	10	Enabled		Edit	Delete
2000	ExtendIP	Extended IP ACL	10	10	Enabled		Edit	Delete
11000	Standardv6	Standard IPv6 ACL	10	10	Disabled		Edit	Delete
						1/1	< 1 2	- >I
					Clear	All Counter	ear Counter	Add Rule
Sequence	No. Action	Rule	Time	Range	С	ounter		

図 11-21 Standard IPv6 ACL (Main) 画面

「Edit」をクリックし、指定 ACL プロファイルの編集を行います。 「Delete」ボタンをクリックし、指定 ACL プロファイルの削除を行います。 複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

ACL プロファイルにルールを追加する場合、ACL プロファイルを選択後「Add Rule」ボタンをクリックします。
### ACL ルールの追加 (Add Rule) (Standard IPv6 ACL)

「Add Rule」をクリックし新しい ACL ルールを追加します。

ACL プロファイルを選択後「Add Rule」ボタンをクリックすると、以下の画面が表示され新しい ACL ルールを設定できます。

D		11000				
ACL Name		SIP6ACL				
CL Type		Standard IPv6 A	CL			
equence	No. (1-65535)		(If it isn'	specified, the sys	tem automatically assigns.)	
ction		Permit	Deny O Deny C	PU		
Match IP	v6 Address					
	<ul> <li>Any</li> </ul>			<ul> <li>Any</li> </ul>		
Source	OHost	2012::1		OHost	2012::1	
	O IPv6	2012::1	Destination	O IPv6	2012::1	
	Prefix Leng	pth		Prefix Length		
		an allow				

図 11-22 Standard IPv6 ACL (Add Rule) 画面

#### 画面に表示される項目:

項目	説明
Sequence No. (1-65535)	シーケンス番号を指定します。「1」から「65535」の間で指定できます。
	1世を指定しない場合は目期的に备亏が割り振られます。
Action	ルール動作に関する設定を行います。「Permit」「Deny」「Deny CPU」から指定できます。
Source	送信元のアドレスを以下から指定します。
	• Any - どの送信元トラフィックでも本ルールに従って評価されます。
	・ Host - ホストの IPv6 アドレスを入力します。
	・ IPv6 -「Prefix Length」オプションが選択可能になり、送信元 IPv6 アドレスと Prefix Length を入力します。
Destination	宛先のアドレスを以下から指定します。
	・ Any - どの宛先トラフィックでも本ルールに従って評価されます。
	・ Host - ホストの IPv6 アドレスを入力します。
	・ IPv6 -「Prefix Length」オプションが選択可能になり、宛先 IPv6 アドレスと Prefix Length を入力します。
Time Range	ACL ルールに関するタイムレンジ名を指定します。

「Back」ボタンをクリックして、変更を破棄し前の画面に戻ります。 「Apply」ボタンをクリックして、設定を適用します。

### ACL ルールの編集 (Edit) (Standard IPv6 ACL)

「Counter State」オプションの有効化やプロファイルへの「Remark」の入力など ACL ルールの編集を行う場合、「ACL Profile Table」で該当するプロ ファイル横の「Edit」ボタンをクリックします。以下の画面が表示されます。

CL ACC	ess List e All	• •	ID (1-14999)		ACL Name	32 chars	Find
otal Ent	ries: 3						Add ACL
ID	ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark	
1	StandardIP	Standard IP ACL	10	10	Enabled		Edit Delete
2000	ExtendIP	Extended IP ACL	10	10	Enabled		Edit Delete
1000	Standardv6	Standard IPv6 ACL	10	10	Disabled *		Apply Delete
						1/1	< 1 > > G
andard	iv6 (ID: 11000)	Rule				Clear All Counter	Clear Counter Add Rule
Sequer	ice No. A	ction	Rule	Time	Range	Counter	
1	0 F	ermit	any any				Delete

図 11-23 Standard IPv6 ACL (Edit ACL) 画面

画面に表示される項目:	:
-------------	---

項目	説明
Start Sequence No.	シーケンス番号の開始番号を指定します。
Step	シーケンス番号の増加番号を指定します。
Counter State	カウンタ機能の「Enabled」(有効)/「Disabled」(無効)を指定します。
Remark	指定プロファイルと関連するリマークを入力します。
<b>E</b>	

「Apply」ボタンをクリックして、設定を適用します。

「Delete」ボタンをクリックして、指定エントリを削除します。

特定の ACL プロファイルに関連する ACL ルール表示するには「ACL Profile Table」で該当の ACL プロファイルを選択します。ACL ルールが表示されます。

CL Access	List							
CL Type	All 🔹	ID (1-14999)		) A(	CL Name 32 chars			Find
otal Entries	: 3							Add ACL
ID	ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark		
1	StandardIP	Standard IP ACL	10	10	Enabled		Edit	Delete
2000	ExtendIP	Extended IP ACL	10	10	Enabled		Edit	Delete
11000	Standardv6	Standard IPv6 ACL	10	10	Enabled		Edit	Delete
						1/1	: < 1 :	> >  G
tandardv6 (	ID: 11000) Rule				Clear	All Counter	lear Counter	Add Rule
Sequence I	No. Action	Rule	Time	Range	c	ounter		
10	Permit	any any			(Ing:	0 packets)		Delete
10	Permit	any any			(Ing:	0 packets)		Delete

図 11-24 Standard IPv6 ACL (Rule Display) 画面

「Delete」ボタンをクリックして、指定ルールを削除します。 複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

### Extended IPv6 ACL(拡張 IPv6 ACL)

#### Extended IPv6 ACL の作成(Add ACL)

「Add ACL」をクリックし新しい ACL プロファイルを作成します。以下の画面が表示されます。

Add ACL Access List       ACL Type     Extended IPv6 ACL ▼       ID (13000-14999)	
ACL TypeExtended IPv6 ACL ▼ID (13000-14999)	
ID (13000-14999) ACL Name 32 chars	
ACL Name 32 chars	
	Apply
Note: The first character of ACL name must be a letter.	

図 11-25 Extended IPv6 ACL (Add ACL Access List) 画面

#### 画面に表示される項目:

項目	説明
ACL Type	ACL プロファイルの種類を以下から選択します。 「Standard IP ACL」「Extended IP ACL」「Standard IPv6 ACL」「Extended IPv6 ACL」「Extended MAC ACL」「Extended Expert ACL」
ID	ACL ID を入力します。13000 から 14999 の範囲で入力できます。
ACL Name	ACL 名を入力します。32 文字まで指定できます。

「Apply」ボタンをクリックして、設定を適用します。

ACL プロファイルを作成すると、「ACL Profile Table」に新しく作成した ACL プロファイルが以下の様に表示されます。

CL Type	All 🝷	ID (1-14999)		0/	ACL Name 32 chars		(	Find
tal Entries:	4						ſ	Add ACL
ID	ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark		
1	StandardIP	Standard IP ACL	10	10	Enabled		Edit	Delete
2000	ExtendIP	Extended IP ACL	10	10	Enabled		Edit	Delete
11000	Standardv6	Standard IPv6 ACL	10	10	Enabled		Edit	Delete
13000	Extendv6	Extended IPv6 ACL	10	10	Disabled		Edit	Delete
						1/1	< 1 >	

図 11-26 Extended IPv6 ACL (Main) 画面

「Edit」をクリックし、指定 ACL プロファイルの編集を行います。

「Delete」ボタンをクリックし、指定 ACL プロファイルの削除を行います。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

ACL プロファイルにルールを追加する場合、ACL プロファイルを選択後「Add Rule」ボタンをクリックします。

### ACL ルールの追加 (Add Rule) (Extended IPv6 ACL)

「Add Rule」をクリックし新しい ACL ルールを追加します。

ACL プロファイルを選択後「Add Rule」ボタンをクリックすると、以下の画面が表示され新しい ACL ルールを設定できます。

Add ACL Rule	
Add ACL Rule	
ID ACL Name ACL Type Sequence No. (1-65535) Action Protocol Type	13000 EIP6ACL Extended IPv6 ACL (If it isn't specified, the system automatically assigns.) Permit O Deny ODeny CPU TCP (0-255) Mask (0x0-0xFF) Fragments
Match IPV6 Address    Any  Host  Dive  Dive Dive	Image: Constraint of the st         2012:::1           Image: Constraint of the st         2012:::1           Image: Constraint of the st         2012:::1           Image: Constraint of the st         Prefix Length
Match Port Source Port Please Select Please Select	✓ (0-65535) Please Select ▼ (0-65535)
Destination Port Please Select Please Select	<ul> <li>✓</li> <li>(0-65535) Please Select ✓</li> <li>(0-65535))</li> </ul>
TCP Flag          • DSCP (0-63)           • Traffic Class (0-255)	ack         fin         psh         rst         syn         urg           e Select         Value (0-63)         Mask (0x0-0x3F)         Mask (0x0-0x7F)
Flow Label (0-1048575) Time Range	Mask (0x0-0xFFFF) 32 chars Back Apply

図 11-27 Extended IPv6 ACL (Add Rule) 画面

#### 画面に表示される項目:

項目	説明
Sequence No. (1-65535)	シーケンス番号を指定します。「1」から「65535」の間で指定できます。 値を指定しない場合は自動的に番号が割り振られます。
Action	ルール動作に関する設定を行います。「Permit」「Deny」「Deny CPU」から指定できます。
Protocol Type	プロトコルの種類を以下から選択します。 「TCP」「UDP」「ICMP」「ESP」「PCP」「Protocol ID」「SCTP」「None」 選択したプロトコルの種類によってはプロトコルに関連する数値(ID 等)を右の欄に入力する必要があります。そ
	の際、欄の右にある制限値(0-255 等)に注意して入力してください。

選択したプロトコルにより表示される項目が異なります。以下の表示項目を参照してください。

#### すべてのプロトコルタイプに表示される項目(Extended IPv6 ACL)

「Protocol Type」でどの項目を選択しても表示される項目です。(以下の画面は TCP 選択時のものです。)

Add ACL Rule
Add ACL Rule
ID     13000       ACL Name     EIP6ACL       ACL Type     Extended IPv6 ACL       Sequence No. (1-65535)     (If it isn't specified, the system automatically assigns.)       Action     Permit     Denv
Protocol Type TCP (0-255) Mask (0x0-0xFF) Fragments
Match IPv6 Address         Image: Any         Image: Any           Image: Any         Image: A
Match Port Source Port Please Select Please Select O Destination Port Please Select O Destination Port Please Select O Destination O Destination O Destination O Destination D D D D D D D D D D D D D D D D D D D
TCP Flag ack fin psh rst syn urg
DSCP (0-63)     Please Select     Value (0-63)     Mask (0x0-0x3F)     Mask (0x0-0x7F)

図 11-28 Extended IPv6 ACL (Add Rule) TCP 画面

#### すべてのプロトコル選択時に表示される項目(Extended IPv6 ACL)

項目	説明
Source	送信元のアドレスを以下から指定します。
	・ Any - どの送信元トラフィックでも本ルールに従って評価されます。
	・ Host - ホストの IPv6 アドレスを入力します。
	・ IPv6 - Prefix Length」が指定可能になり、送信元 IPv6 アドレスと Prefix Length を入力します。
Destination	宛先のアドレスを以下から指定します。
	・ Any - どの宛先トラフィックでも本ルールに従って評価されます。
	・ Host - ホストの IPv6 アドレスを入力します。
	・ IPv6 - 「Prefix Length」が指定可能になり、宛先 IPv6 アドレスと Prefix Length を入力します。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。「Mask」には適用するマスクを入力します。
Flow Label	フローラベルの値を入力します。0 から 1048575 まで指定可能です。「Mask」には適用するマスクを入力します。
Time Range	ACL ルールに関するタイムレンジ名を指定します。

### 「TCP」選択時に表示される項目(Extended IPv6 ACL)

項目	説明
Source Port	送信元ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選 択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択する と選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポート が使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウ ンリストに選択するポート番号がない場合は項目欄に手動で指定できます。「Mask」には適用するマスクを入力し ます。
Destination Port	宛先ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択 した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると 選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが 使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウン リストに選択するポート番号がない場合は項目欄に手動で指定できます。「Mask」には適用するマスクを入力します。
TCP Flag	TCP フラグを本ルールに含める場合、該当のフラグにチェックを入れます。「ack」「fin」「psh」「rst」「syn」「urg」 から指定できます。

### 「UDP」選択時に表示される項目(Extended IPv6 ACL)

項目	説明
Source Port	送信元ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択する と選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポート が使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウ ンリストに選択するポート番号がない場合は項目欄に手動で指定できます。「Mask」には適用するマスクを入力し ます。
Destination Port	宛先ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択 した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると 選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが 使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウン リストに選択するポート番号がない場合は項目欄に手動で指定できます。「Mask」には適用するマスクを入力します。

#### 「ICMP」選択時に表示される項目(Extended IPv6 ACL)

項目	説明
Specify ICMP Message Type	使用する ICMP メッセージの種類を指定します。自動的に ICMP メッセージ種類の数値とメッセージコードは指定
	されます。
ICMP Message Type	ICMP メッセージを指定しない場合、手動で ICMP メッセージ種類の数値を指定します。
Message Code	ICMP メッセージを指定しない場合、手動でメッセージコードを指定します。

#### 「ESP」「PCP」「Protocol ID」「SCTP」「None」選択時に表示される項目(Extended IPv6 ACL)

項目	説明
Fragments	パケットフラグメントフィルタリングを使用する場合、選択します。
- 「Back」ボタンをクリックして、	変更を破棄し前の画面に戻ります。

「Apply」ボタンをクリックして、設定を適用します。

#### ACL ルールの編集 (Edit) (Extended IPv6 ACL)

「Counter State」オプションの有効化やプロファイルへの「Remark」の入力など ACL ルールの編集を行う場合、「ACL Profile Table」で該当するプロ ファイル横の「Edit」ボタンをクリックします。以下の画面が表示されます。

CL Type	e All	• 0	ID (1-14999)		🔿 ACL Name 📴	chars	Find
otal Ent	tries: 4						Add ACL
ID	ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark	
1	StandardIP	Standard IP ACL	10	10	Enabled		Edit Delete
2000	ExtendIP	Extended IP ACL	10	10	Enabled		Edit Delete
1000	Standardv6	Standard IPv6 ACL	10	10	Enabled		Edit Delete
3000	Extendv6	Extended IPv6 ACL	10	10	Disabled 🔻		Apply Delete
						1/1	
tendve	6 (ID: 13000) R	ule				Clear All Counter	Clear Counter Add Rule
Sequer	ice No.	Action	Rule	Time	e Range	Counter	
1	0 1	Permit	any any				Delete

図 11-29 Extended IPv6 ACL (Edit ACL) 画面

画面に表示される項目:

項目	説明
Start Sequence No.	シーケンス番号の開始番号を指定します。
Step	シーケンス番号の増加番号を指定します。
Counter State	カウンタ機能の「Enabled」(有効)/「Disabled」(無効)を指定します。
Remark	指定プロファイルと関連するリマークを入力します。

「Apply」ボタンをクリックして、設定を適用します。

「Delete」ボタンをクリックして、指定エントリを削除します。

特定の ACL プロファイルに関連する ACL ルール表示するには「ACL Profile Table」で該当の ACL プロファイルを選択します。ACL ルールが表示されます。

### Extended MAC ACL(拡張 MAC ACL)

#### Extended MAC ACL の作成(Add ACL)

「Add ACL」をクリックし新しい ACL プロファイルを作成します。以下の画面が表示されます。

Add ACL Acce	ss List	
Add ACL Access Li	st	
ACL Type	Extended MAC ACL 🔻	
ID (6000-7999)		
ACL Name	32 chars	
		Apply
Note: The first cha	racter of ACL name must be a letter.	

図 11-30 Extended MAC ACL (Add ACL Access List) 画面

#### 画面に表示される項目:

項目	説明
ACL Type	ACL プロファイルの種類を以下から選択します。 「Standard IP ACL」「Extended IP ACL」「Standard IPv6 ACL」「Extended IPv6 ACL」「Extended MAC ACL」「Extended Expert ACL」
ID	ACL ID を入力します。6000 から 7999 の範囲で入力できます。
ACL Name	ACL 名を入力します。32 文字まで指定できます。

「Apply」ボタンをクリックして、設定を適用します。

#### ACL プロファイルを作成すると、「ACL Profile Table」に新しく作成した ACL プロファイルが以下の様に表示されます。

L Type	All	ID (1-14999)		0 A	CL Name 32 chars			Find
tal Entries	:: 5							Add ACL
ID	ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark		
1	StandardIP	Standard IP ACL	10	10	Enabled		Edit	Delete
2000	ExtendIP	Extended IP ACL	10	10	Enabled		Edit	Delete
6000	ExtendMAC	Extended MAC ACL	10	10	Disabled		Edit	Delete
11000	Standardv6	Standard IPv6 ACL	10	10	Enabled		Edit	Delete
13000	Extendv6	Extended IPv6 ACL	10	10	Enabled		Edit	Delete
						1/1	< 1	> >

図 11-31 Extended MAC ACL (Main) 画面

「Edit」をクリックし、指定 ACL プロファイルの編集を行います。 「Delete」ボタンをクリックし、指定 ACL プロファイルの削除を行います。 複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

ACL プロファイルにルールを追加する場合、ACL プロファイルを選択後「Add Rule」ボタンをクリックします。

### ACL ルールの追加(Add Rule)(Extended MAC ACL)

「Add Rule」をクリックし新しい ACL ルールを追加します。

ACL プロファイルを選択後「Add Rule」ボタンをクリックすると、以下の画面が表示され新しい ACL ルールを設定できます。

D		6000						
ACL Name		EMACL						
ACL Type		Extended MAC ACL						
Sequence No. (1-	65535)		(If it isn't specifie	d, the system automation	cally assigns.)			
Action		Permit O Deny	O Deny CPU					
Match MAC Add	iress							
() A	ny		() Any					
OH	ost 11-DF-36-	4B-A7-CC	OHost	11-DF-36-4B-A7-CC				
Source	AC 11-DE-26	AR-AZ-CC Desti	nation	11-DE-26-4B-47-00	=			
U.M.	AC THDE-SO	4B-A/-CC	OWAG	11-DF-30-4B-A7-00				
W	/ildcard 11-DF-36-	-4B-A7-CC	Wildcard	11-DF-36-4B-A7-CC				
Match Ethernet	Type							
Specify Ethernet	Type	Please Select						
opecity Ethernel	r type	riedse Gelect						
Ethernet Type (0	0x600-0xFFFF)							
Ethernet Type M	lask (0x0-0xFFFF)							
							-	
CoS	Please Select	Mask (0x0-0x7)		Inner CoS	Please Select	Mask (0x0-0x7)		
VID(1-4094)		Mask (0x0-0xFFF)						
VLAN Range		~		Inner VID (1-4094)		Mask (0x0-0xFFF)		
O								

図 11-32 Extended MAC ACL (Add Rule) 画面

―
---

項目	説明
Sequence No. (1-65535)	シーケンス番号を指定します。「1」から「65535」の間で指定できます。
Action	ルール動作に関する設定を行います。「Permit」または「Deny」「Deny CPU」から指定できます。
Source	送信元の MAC アドレスを以下から指定します。
	・ Any - どの送信元トラフィックでも本ルールに従って評価されます。
	・ Host - ホストの MAC アドレスを入力します。
	・ MAC - 「Wildcard」オプションが選択可能になり送信元 MAC アドレスとワイルドカードを入力できます。
Destination	宛先の MAC アドレスを以下から指定します。
	・ Any - どの宛先トラフィックでも本ルールに従って評価されます。
	・ Host - 宛先ホストの MAC アドレスを入力します。
	・ MAC - 「Wildcard」オプションが選択可能になり宛先 MAC アドレスとワイルドカードを入力できます。
Specify Ethernet Type	イーサネットタイプを以下から選択します。
	[aarp][appletalk][decent-iv][etype-6000][etype-8042][lat][lavc-sca][mop-console][mop-dump][vines-echo]
	「vines-ip」「xns-idp」「arp」
Ethernet Type	イーサネットタイプの 16 進数値を指定します。0x600 から 0xFFFF の間で指定できます。「Specify Ethernet Type」
	で指定したイーサネットタイプに基づき適切な値が入力されます。
Ethernet Type Mask	イーサネットタイプマスクの 16 進数値を指定します。0x0 から 0xFFFF の間で指定できます。「Specify Ethernet
	Type」で指定したイーサネットタイプに基づき適切な値が入力されます。
CoS	CoSの値を入力します。0から7の間で入力できます。「Mask」には適用するマスクを入力します。
Inner CoS	Inner CoS の値を入力します。0 から 7 の間で入力できます。「Mask」には適用するマスクを入力します。
VID	ACL ルールに関連する VLAN ID を入力します。1 から 4094 の間で入力可能です。
	「Mask」には適用するマスクを入力します。
Inner VID	ACL ルールに関連する Inner VID を入力します。1 から 4094 の間で入力可能です。
	「Mask」には適用するマスクを入力します。
VLAN Range	ACL ルールに関連す VLAN 範囲を入力します。1 から 4094 の間で入力可能です。
Time Range	ACL ルールに関するタイムレンジ名を指定します。

「Back」ボタンをクリックして、変更を破棄し前の画面に戻ります。

「Apply」ボタンをクリックして、設定を適用します。

### ACL ルールの編集(Edit)(Extended MAC ACL)

「Counter State」オプションの有効化やプロファイルへの「Remark」の入力など ACL ルールの編集を行う場合、「ACL Profile Table」で該当するプロ ファイル横の「Edit」ボタンをクリックします。以下の画面が表示されます。

CL Acc	ess List						
CL Typ	e All	• 0	ID (1-14999)		O ACL Name	2 chars	Find
otal Ent	tries: 5						Add ACL
ID	ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark	
1	StandardIP	Standard IP ACL	10	10	Enabled		Edit Delete
2000	ExtendIP	Extended IP ACL	10	10	Enabled		Edit Delete
6000	ExtendMAC	Extended MAC ACL	10	10	Disabled -		Apply Delete
11000	Standardv6	Standard IPv6 ACL	10	10	Enabled		Edit Delete
13000	Extendv6	Extended IPv6 ACL	10	10	Enabled		Edit Delete
						1/1	< 1 > > G
xtendM	IAC (ID: 6000) F	Rule				Clear All Counter	Clear Counter Add Rule
Seque	nce No. 🛛	Action	Rule	Time	Range	Counter	
1	0 8	Permit	any any				Delete

図 11-33 Extended MAC ACL (Edit ACL) 画面

#### 画面に表示される項目:

項目	説明
Start Sequence No.	シーケンス番号の開始番号を指定します。
Step	シーケンス番号の増加番号を指定します。
Counter State	カウンタ機能の「Enabled」(有効)/「Disabled」(無効)を指定します。
Remark	指定プロファイルと関連するリマークを入力します。

「Apply」ボタンをクリックして、設定を適用します。

「Delete」ボタンをクリックして、指定エントリを削除します。

特定の ACL プロファイルに関連する ACL ルール表示するには「ACL Profile Table」で該当の ACL プロファイルを選択します。ACL ルールが表示されます。

CL Access	List							
CL Type	All 🔻	ID (1-14999)		⊙ A(	CL Name 32 chars			Find
otal Entries	: 5							Add ACL
ID	ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark		
1	StandardIP	Standard IP ACL	10	10	Enabled		Edit	Delete
2000	ExtendIP	Extended IP ACL	10	10	Enabled		Edit	Delete
6000	ExtendMAC	Extended MAC ACL	10	10	Enabled		Edit	Delete
11000	Standardv6	Standard IPv6 ACL	10	10	Enabled		Edit	Delete
13000	Extendv6	Extended IPv6 ACL	10	10	Enabled		Edit	Delete
						1/1	: < 1 :	> >  Ga
xtendMAC	(ID: 6000) Rule				Clear	All Counter	lear Counter	Add Rule
Sequence	No. Action	Rule	Time	Range	C	ounter		
10	Permit	any any			(Ing: (	0 packets)		Delete

図 11-34 Extended MAC ACL (Rule Display) 画面

「Delete」ボタンをクリックして、指定ルールを削除します。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

### Extended Expert ACL(拡張詳細 ACL)

### Extended Expert ACL の作成(Add ACL)

「Add ACL」をクリックし新しい ACL プロファイルを作成します。以下の画面が表示されます。

Add ACL Acces	s List	
Add ACL Access Lis	L	
ACL Type	Extended Expert A(	
ID (8000-9999)		
ACL Name	32 chars	
		Apply
Note: The first chara	cter of ACL name must be a letter.	

図 11-35 Extended Expert ACL (Add ACL Access List) 画面

画面に表示される項目:

項目	説明
ACL Type	ACL プロファイルの種類を選択します。「Standard IP ACL」「Extended IP ACL」「Standard IPv6 ACL」「Extended IPv6 ACL」
	「Extended MAC ACL」「Extended Expert ACL」から選択します。
ID	ACL ID を入力します。8000 から 9999 の範囲で入力できます。
ACL Name	ACL 名を入力します。32 文字まで指定できます。
<b>E</b>	

「Apply」ボタンをクリックして、設定を適用します。

ACL プロファイルを作成すると、「ACL Profile Table」に新しく作成した ACL プロファイルが以下の様に表示されます。

CL Type	All 👻	ID (1-14999)		O AC	L Name 32 chars			Find
tal Entries	:: 6							Add ACL
ID	ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark		
1	StandardIP	Standard IP ACL	10	10	Enabled		Edit	Delete
2000	ExtendIP	Extended IP ACL	10	10	Enabled		Edit	Delete
6000	ExtendMAC	Extended MAC ACL	10	10	Enabled		Edit	Delete
8000	ExtendExpe	Extended Expert ACL	10	10	Disabled		Edit	Delete
11000	Standardv6	Standard IPv6 ACL	10	10	Enabled		Edit	Delete
13000	Extendv6	Extended IPv6 ACL	10	10	Enabled		Edit	Delete
						1/1	< 1	> >

図 11-36 Extended Expert ACL (Main) 画面

「Edit」をクリックし、指定 ACL プロファイルの編集を行います。 「Delete」ボタンをクリックし、指定 ACL プロファイルの削除を行います。 複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

ACL プロファイルにルールを追加する場合、ACL プロファイルを選択後「Add Rule」ボタンをクリックします。

### ACL ルールの追加 (Add Rule) (Extended Expert ACL)

「Add Rule」をクリックし新しい ACL ルールを追加します。

ACL プロファイルを選択後「Add Rule」ボタンをクリックすると、以下の画面が表示され新しい ACL ルールを設定できます。

Add ACL Rule           ID         8000           ACL Name         EEACL           ACL Type         Extended Expert ACL	
Sequence No. (1-65535) (If it isn't specified, the system automatically assigns.)	
Action   Permit  Deny  Deny  CPU	
Protocol Type TCP (0-255) Mask (0x0-0xFF) Fragments	
r Match IP Address	
Source     Image: Constraint of the second sec	
Match MAC Address	
Image: Source         Image: Any control of the state of the sta	
Match Port Source Port Please Select O(0-65535)	
IP Precedence         Please Select         Value (0-7)         Mask (0x0-0x7)           ToS         Please Select         Value (0-15)         Mask (0x0-0xF)	
ODSCP (0-63) Please Select Value (0-63) Mask (0x0-0x3F)	
VID(1-4094)     Mask (0x0-0xFFF)     Inner VID (1-4094)     Mask (0x0-0xFFF)     OVIAN Range	
CoS Please Select V Mask (0x0-0x7) Inner CoS Please Select V Mask (0x0-0x7)	
Time Range 32 chars Back Apply	

図 11-37 Extended Expert ACL (Add Rule) 画面

#### 画面に表示される項目:

項目	説明
Sequence No. (1-65535)	シーケンス番号を指定します。「1」から「65535」の間で指定できます。 値を指定しない場合は自動的に番号が割り振られます。
Action	ルール動作に関する設定を行います。「Permit」「Deny」「Deny CPU」から指定できます。
Protocol Type	プロトコルの種類を以下から選択します。 「TCP」「UDP」「ICMP」「EIGRP」「ESP」「GRE」「IGMP」「OSPF」「PIM」「VRRP」「IP-in-IP」「PCP」「Protocol ID」「None」
	選択したフロトコルの種類によってはフロトコルに関連する数値(ID 等)を右の欄に人力する必要があります。そ の際、欄の右にある制限値(0-255 等)に注意して入力してください。

選択したプロトコルにより表示される項目が異なります。以下の表示項目を参照してください。

### すべてのプロトコルタイプに表示される項目(Extended Expert ACL)

「Protocol Type」でどの項目を選択しても表示される項目です。(以下の画面は TCP 選択時のものです。)

Add ACL Rule		
Add ACL Rule		
ID ACL Name ACL Type Sequence No. (1-65535) Action Protocol Type Match IP Address	8000         EEACL         Extended Expert ACL         (If it isn't specified, the system automatically assigns.)            • Permit O Deny O Deny CPU          TCP          • (0-255) Mask (0x0-0xFF)	
Olp Wildcard	OHost     O	
Match MAC Address		
OAny     OHost 11-DF-36     MAC 11-DF-36     Wildcard 11-DF-36	AB-A7-CC         Destination         11-DF-36-4B-A7-CC           AB-A7-CC         MAC         11-DF-36-4B-A7-CC           Wildcard         11-DF-36-4B-A7-CC	
Match Port		
Source Port Please Select Please Select Destination Port Please Select Please Select	✓       (0-65535)       Please Select       ✓       (0-65535)         ✓       (0-65535)       Please Select       ✓       (0-65535)	
IP Precedence Please Select	Value (0-7) Mask (0x0-0x7)	
ToS     Please Select	Value (0-15) Mask (0x0-0xF)	
ODSCP (0-63) Please Select	Value (0-63) Mask (0x0-0x3F)	
TCP Flag	ack fin psh rst syn urg	
VID(1-4094)     VLAN Range	Mask (0x0-0xFFF) Inner VID (1-4094) Mask (0x0-0xFFF)	
CoS Please Select	Mask (0x0-0x7) Inner CoS Please Select Mask (0x0-0x7)	
Time Range	32 chars	
		Back Apply
	L	

図 11-38 Extended Expert ACL (Add Rule) TCP 画面

#### すべてのプロトコル選択時に表示される項目(Extended Expert ACL)

項目	説明
Source IP Address	送信元のアドレスを以下から指定します。
	・ Any - どの送信元トラフィックでも本ルールに従って評価されます。
	・ Host - ホストの IP アドレスを入力します。
	• IP - 「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い送信元 IP アドレス群を入力
	します。ビットは1の値が無視され、0が認識されます。
Destination IP Address	宛先のアドレスを以下から指定します。
	・ Any - どの宛先トラフィックでも本ルールに従って評価されます。
	・ Host - ホストの IP アドレスを入力します。
	• IP -「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い宛先 IP アドレス群を入力し
	ます。ビットは1の値が無視され、0が認識されます。
Source MAC Address	送信元の MAC アドレスを以下から指定します。
	・ Any - どの送信元トラフィックでも本ルールに従って評価されます。
	・ Host - ホストの MAC アドレスを入力します。
	・ MAC - 「Wildcard」オプションが選択可能になり送信元 MAC アドレスとワイルドカードを入力することができ
	ます。
Destination MAC Address	宛先の MAC アドレスを以下から指定します。
	・ Any - どの宛先トラフィックでも本ルールに従って評価されます。
	・ Host - 宛先ホストの MAC アドレスを入力します。
	・ MAC - 「Wildcard」オプションが選択可能になり宛先 MAC アドレスとワイルドカードを入力することができます。
IP Precedence	IP 優先値を指定します。「0 (routine)」「1 (priority)」「2, (immediate)」「3 (flash)」「4 (flash-override)」「5 (critical)」「6
	(internet)」「7 (network)」から指定できます。「Mask」には適用するマスクを入力します。
ToS	IP 優先値を選択後、使用する「Type-of-Service」(ToS) の値を指定します。「0 (normal)」「1 (min-monetary-cost)」「2
	(max-reliability)」「3, 4(max-throughput)」「5, 6, 7, 8 (min-delay)」「9」「10」「11」「12」「13」「14」「15」から指定
	できます。「Mask」には適用するマスクを入力します。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。「Mask」には適用するマスクを入力します。
CoS	CoS の値を入力します。0 から 7 の間で入力できます。「Mask」には適用するマスクを入力します。
Inner CoS	Inner CoS の値を入力します。0 から 7 の間で入力できます。「Mask」には適用するマスクを入力します。

項目	説明
VID	ACL ルールに関連する VLAN ID を入力します。1 から 4094 の間で入力可能です。
	「Mask」には適用するマスクを入力します。
Inner VID	ACL ルールに関連する Inner VID を入力します。1 から 4094 の間で入力可能です。
	「Mask」には適用するマスクを入力します。
Time Range	ACL ルールに関するタイムレンジ名を指定します。

#### 「TCP」選択時に表示される項目(Extended Expert ACL)

項目	説明
Source Port	送信元ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選 択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択する と選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポート が使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウ ンリストに選択するポート番号がない場合は項目欄に手動で指定できます。
Destination Port	宛先ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択 した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると 選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが 使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウン リストに選択するポート番号がない場合は項目欄に手動で指定できます。
TCP Flag	TCP フラグを本ルールに含める場合、該当のフラグにチェックを入れます。「ack」「fin」「psh」「rst」「syn」「urg」 から指定できます。

#### 「UDP」選択時に表示される項目(Extended Expert ACL)

項目	説明
Source Port	送信元ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選 択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択する と選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポート が使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウ ンリストに選択するポート番号がない場合は項目欄に手動で指定できます。
Destination Port	宛先ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択 した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると 選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが 使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウン リストに選択するポート番号がない場合は項目欄に手動で指定できます。

#### 「ICMP」選択時に表示される項目(Extended Expert ACL)

項目	説明
Specify ICMP Message Type	使用する ICMP メッセージの種類を指定します。自動的に ICMP メッセージ種類の数値とメッセージコードは指定 されます。
ICMP Message Type	ICMP メッセージを指定しない場合、手動で ICMP メッセージ種類の数値を指定します。
Message Code	ICMP メッセージを指定しない場合、手動でメッセージコードを指定します。

#### 「EIGRP」「ESP」「GRE」「IGMP」「OSPF」「PIM」「VRRP」「IP-in-IP」「PCP」「Protocol ID」「None」選択時に表示される項目(Extended Expert ACL)

項目	説明
Fragments	パケットフラグメントフィルタリングを使用する場合、選択します。

「Back」ボタンをクリックして、変更を破棄し前の画面に戻ります。 「Apply」ボタンをクリックして、設定を適用します。

### ACL ルールの編集 (Edit) (Extended Expert ACL)

「Counter State」オプションの有効化やプロファイルへの「Remark」の入力など ACL ルールの編集を行う場合、「ACL Profile Table」で該当するプロ ファイル横の「Edit」ボタンをクリックします。以下の画面が表示されます。

ACL Acc	ess List	• • D (	(1-14999)		O ACL Name	2 chars	Find
otal En	tries: 6						Add ACL
ID	ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark	
1	StandardIP	Standard IP ACL	10	10	Enabled		Edit Delete
2000	ExtendIP	Extended IP ACL	10	10	Enabled		Edit Delete
6000	ExtendMAC	Extended MAC ACL	10	10	Enabled		Edit Delete
8000	ExtendExpe	Extended Expert ACL	10	10	Disabled 🔻		Apply Delete
11000	Standardv6	Standard IPv6 ACL	10	10	Enabled		Edit Delete
13000	Extendv6	Extended IPv6 ACL	10	10	Enabled		Edit Delete
						1/1	< < 1 > >  G
xtendE	xpert (ID: 8000) F	Rule				Clear All Counter	Clear Counter Add Rule
Seque	nce No. Ac	tion	Rule	Time R	tange	Counter	
1	0 Pe	ermit an	iy any any any				Delete
						1/1	

図 11-39 Extended Expert ACL (Edit ACL) 画面

画面に表示される項目:

項目	説明
Start Sequence No.	シーケンス番号の開始番号を指定します。
Step	シーケンス番号の増加番号を指定します。
Counter State	カウンタ機能の「Enabled」(有効)/「Disabled」(無効)を指定します。
Remark	指定プロファイルと関連するリマークを入力します。

「Apply」ボタンをクリックして、設定を適用します。

「Delete」ボタンをクリックして、指定エントリを削除します。

特定の ACL プロファイルに関連する ACL ルール表示するには「ACL Profile Table」で該当の ACL プロファイルを選択します。ACL ルールが表示されます。

#### ACL Access List ACL Access List ACL Type All ID (1-14999) ACL Name 32 chars Find Total Entries: 6 Add ACL Start Sequence No. Step ID ACL Name ACL Type Counter State StandardIP Standard IP ACL 10 10 Enabled Delete 1 Edit Extended IP ACL 10 2000 ExtendIP 10 Enabled Edit Delete ExtendMAC Extended MAC ACL 10 10 Enabled 6000 Edit Delete 8000 ExtendExpe... Extended Expert ACL 10 10 Enabled Delete Edit Standard IPv6 ACL 10 10 11000 Standardv6 Enabled Delete Edit 13000 Extendv6 Extended IPv6 ACL 10 10 Enabled Edit Delete 1/1 |< < 1 > >| Go ExtendExpert (ID: 8000) Rule Clear All Counter Clear Counter Add Rule ence No. Action Counter Seau (Ing: 0 packets) Delete 10 Permit any any any any 1/1 |< < 1 > >| Go

図 11-40 Extended Expert ACL (Rule Display) 画面

「Delete」ボタンをクリックして、指定ルールを削除します。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

# ACL Interface Access Group (ACL インタフェースアクセスグループ)

ACL インタフェースアクセスグループの設定、表示を行います。

ACL > ACL Interface Access Group の順にメニューをクリックし、以下の画面を表示します。

ACL Interface Acces	ss Group Port To D/1 V e	o Port Dir th1/0/1 ♥ In	rection Actio	on Type d V IP ACL	ACL Na	me Please	Select	Apply
Dent			In			o	ut	
Роп	IP ACL	IPv6 ACL	MAC ACL	Expert ACL	IP ACL	IPv6 ACL	MAC ACL	Expert ACL
eth1/0/1								
eth1/0/2								
oth1/0/3								

図 11-41 ACL Interface Access Group 画面

画面に表示される項目:

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	設定の対象となるポートを指定します。
Direction	方向を指定します。「In」が選択可能です。
Action	ACL インタフェースアクセスグループの「Add」(追加)/「Delete」(削除)をします。
Туре	ACL の種類を以下から選択します。
	「IP ACL」「IPv6 ACL」「MAC ACL」「Expert ACL」
ACL Name	ACL 名を入力します。32 文字以内で入力できます。

「Please Select」ボタンをクリックし、作成した ACL プロファイルを選択します。 「Apply」ボタンをクリックして、設定を適用します。

「Please Select」ボタンをクリックすると次の画面が表示されます。

	ID	ACL Name	ACL Type
0	1	S-IP-ACL	Standard IP ACL
•	2000	E-IP-ACL	Extended IP ACL

図 11-42 Please Select 画面

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。 設定するエントリを選択し「OK」をクリックします。

# ACL VLAN Access Map (ACL VLAN アクセスマップ)

ACL VLAN アクセスマップの設定、表示を行います。

ACL > ACL VLAN Access Map の順にメニューをクリックし、以下の画面を表示します。

CL VLAN Access N	lap	_	_	_	_	_	_	_
ACL VLAN Access Map —								
Access Map Name	32 chars							
Sub Map Number (1-6553	5)							
Action	Forward	~						Apply
Access Map Name	32 chars		Counter State	Disabled	~			Apply
Access Map Name	32 chars				[	Clear All Counter	Clear Counter	Find
Total Entries: 1								
Access Map Name	Sub Map Number	Action	Match	Access-List		Counter State		
map	1	Forward				Disabled	Binding	Delete
						1/1	K < 1	Go

図 11-43 ACL VLAN Access Map 画面

画面に表示される項目:

項目	説明
Access Map Name	アクセスマップ名を入力します。32 文字以内で入力できます。
Sub Map Number	サイトマップ番号を入力します。1 から 65535 までで指定できます。
Action	本項目の動作を「Forward」「Drop」「Redirect」から指定します。
	「Redirect」を選択した場合、ドロップダウンリストからリダイレクトされるインタフェースを選択できます。
Counter State	カウンターの「Enabled」(有効)/「Disabled」(無効)を指定します。

「Apply」ボタンをクリックして、設定を適用します。

「Clear All Counter」ボタンをクリックし、表示されたすべてのカウンタ情報を消去します。

「Clear Counter」ボタンをクリックし、表示された指定ルールのカウンタ情報を消去します。

「Find」ボタンをクリックし、入力した情報を元に特定のエントリを指定します。

「Binding」ボタンをクリックし、新しく合致したアクセスリストを指定します。

「Delete」ボタンをクリックし、指定エントリを削除します。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

### Match Access-List(合致するアクセスリスト設定)

「Binding」ボタンをクリックすると以下の画面が表示されます。

ccess Man Name	map	
ub Map Number	1	
Match IP Access-List		
Please Se	elect	Apply Delete
Match IPv6 Access-List		
Please Se	elect	Apply Delete
Please Se	elect	Apply Delete
Match MAC Access-List	elect	Apply Delete

図 11-44 Match Access-List 画面

画面に表示される項目:

項目	説明
Match IP Access-List	「Standard」(通常) または「Extended」(拡張)の IP ACL を選択します。
Match IPv6 Access-List	「Standard」(通常) または「Extended」(拡張)の IPv6 ACL を選択します。
Match MAC Access-	「Standard」(通常) または「Extended」(拡張)の MAC ACL を選択します。
List	

「Please Select」ボタンをクリックし、作成した ACL プロファイルを選択します。 「Apply」ボタンをクリックして、設定を適用します。 「Delete」ボタンをクリックし、指定エントリを削除します。

「Please Select」ボタンをクリックすると次の画面が表示されます。

	ID	ACL Name	ACL Type
0	1	S-IP-ACL	Standard IP ACL
•	2000	E-IP-ACL	Extended IP ACL
	2000	E-IP-ACL	Extended IP ACL

図 11-45 ACL Access List 画面

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。 設定するエントリを選択し「OK」をクリックします。

# ACL VLAN Filter (ACL VLAN フィルタ設定)

ACL VLAN フィルタの設定、表示を行います。

ACL > ACL VLAN Filter の順にメニューをクリックし、以下の画面を表示します。

ACL VLAN Filter	_	_		
ACL VLAN Filter				
Access Map Name	32 chars			
Action	Add	~		
VID List	1,3-5			Apply
Total Entries: 1				
Access M	ap Name		VID List	
ma	map		1	Delete
				1/1  < < 1 > >  Go

図 11-46 ACL VLAN Filter 画面

画面に表示される項目:

項目	説明
Access Map Name	アクセスマップ名を入力します。32 文字以内で入力できます。
Action	ACL VLAN フィルタの「Add」(追加)/「Delete」(削除)をします。
VID List	使用する VLAN ID リストを入力します。「All VLAN」を選択するとスイッチに設定されているすべての VLAN が対象となり
	ます。

「Apply」ボタンをクリックして、設定を適用します。

「Delete」ボタンをクリックし、指定エントリを削除します。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

# CPU ACL (CPU ACL 設定)

本スイッチは、CPU インタフェースフィルタリング機能の設定を行います。

```
ACL > CPU ACL の順にメニューをクリックし、以下の画面を表示します。
```

UACL							
Iter Map Name	32 ch	ars				Apply	Find
otal Entries: 1		Mat	ch Access-list	_			_
Filter Map Name	IP ACL	IPv6 ACL	MAC ACL	Expert ACL	<ul> <li>Match Ingress Interface</li> </ul>		
121 52/25/27						Binding	Delete

図 11-47 CPU ACL 画面

画面に表示される項目:

項目	説明
Filter Map Name	CPU ACL フィルタマップ名(32 字以内)を指定します。

「Apply」をクリックし、設定内容を適用します。

「Binding」ボタンをクリックし、新しく合致したアクセスリストを指定します。

「Delete」ボタンをクリックし、指定エントリを削除します。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

「Binding」ボタンをクリックすると以下の画面が表示されます。

Match Access-List			
CPU ACL Configure			
Filter Map Name	map		
Match IP Access List			
Sequence No. (1-65535)	ACL Name	Please Select	Apply Delete
Match IPv6 Access List			
Sequence No. (1-65535)	ACL Name	Please Select	Apply Delete
Match MAC Access List			
Sequence No. (1-65535)	ACL Name	Please Select	Apply Delete
Match Expert Access List			
Sequence No. (1-65535)	ACL Name	Please Select	Apply Delete
Match Ingress Interface			
Unit	From Port	To Port	
1 🗸	eth1/0/1	eth1/0/1	Apply Delete

図 11-48 Match Access-List 画面

画面に表示される項目:

項目	説明				
	Match IP Access List				
Sequence No. (1-65535)	シーケンス番号を指定します。「1」から「65535」の間で指定できます。「1」が最優先値となります。				
ACL Name	マッチする「standard」または「extended」IP アクセスリスト名(32 字以内)を指定します。 「Please Select」をクリックし、既存の ACL から選択することも可能です。				
	Match IPv6 Access List				
Sequence No. (1-65535)	シーケンス番号を指定します。「1」から「65535」の間で指定できます。「1」が最優先値となります。				
ACL Name	マッチする「standard」または「extended」アクセスリスト名(32 字以内)を指定します。 「Please Select」をクリックし、既存の ACL から選択することも可能です。				
	Match MAC Access List				
Sequence No. (1-65535)	シーケンス番号を指定します。「1」から「65535」の間で指定できます。「1」が最優先値となります。				
ACL Name	マッチする「standard」または「extended」アクセスリスト名(32 字以内)を指定します。 「Please Select」をクリックし、既存の ACL から選択することも可能です。				
	Match Expert Access List				
Sequence No. (1-65535)	シーケンス番号を指定します。「1」から「65535」の間で指定できます。「1」が最優先値となります。				
ACL Name	マッチする「standard」または「extended」アクセスリスト名(32 字以内)を指定します。 「Please Select」をクリックし、既存の ACL から選択することも可能です。				
	Match Expert Access List				
Unit	設定を行うユニットを指定します。				
From Port / To Port	設定するポートの始点 / 終点を設定します。				

「Apply」ボタンをクリックして、設定を適用します。

「Delete」ボタンをクリックし、指定エントリを削除します。

「Please Select」ボタンをクリックすると次の画面が表示されます。

	ID	ACL Name	ACL Type
0	1	S-IP-ACL	Standard IP ACL
0	2000	E-IP-ACL	Extended IP ACL
	2000	L'II TICL	

図 11-49 ACL Access List 画面

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。 設定するエントリを選択し「OK」をクリックします

# 第 12 章 Security (セキュリティ機能の設定)

本セクションではユーザアカウントを含むデバイスのセキュリティの設定について解説します。

以下は Security サブメニューの説明です。必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明		
Port Security(ポートセキュリティ)	ポートセキュリティは、ポートのロックを行う前にスイッチが(ソース MAC アドレスを)認識してい ない不正なコンピュータが、ロックしたポートに接続してネットワークへのアクセスを行わないように するための機能です。		
802.1X(802.1X 設定)	IEEE 802.1X 標準規格は、クライアント・サーバベースのアクセスコントロールモデルの使用により、 特定の LAN 上の様々な有線 / 無線デバイスへのアクセスを行う場合にユーザ認証を行うセキュリティ 方式です。		
AAA(AAA 設定)	AAA(Authentication、Authorization、Accounting)の設定を行います。		
RADIUS(RADIUS 設定)	RADIUSの設定を行います。		
TACACS+(TACACS+ 設定)	TACACS+ の設定を行います。		
IMPB (IP-MAC-Port Binding / IP-MAC- ポー トバインディング)	IP-MAC バインディングにより、スイッチにアクセスするユーザ数を制限します。		
DHCP Server Screening (DHCP サーバス クリーニング設定)	DHCP サーバスクリーニングは不正な DHCP サーバへのアクセスを拒否する機能です。		
ARP Spoofing Prevention (ARP スプーフィ ング防止設定)	ARP スプーフィング防止機能は、設定したゲートウェイ IP アドレスとマッチしなかった IP アドレスの ARP パケットをバイパスします。		
BPDU Attack Protection(BPDU アタック 防止設定)	スイッチのポートに BPDU 防止機能を設定します。		
NetBIOS Filtering(NetBIOS フィルタリン グ設定)	NetBIOS フィルタリングの設定を行います。		
MAC Authentication(MAC 認証)	MAC 認証機能は、MAC アドレスにてネットワークの認証を設定する方法です。		
Web-based Access Control (Web 認証)	Web ベース認証はスイッチを経由でインターネットにアクセスする場合、ユーザを認証する機能です。		
Japanese Web-based Access Control (JWAC 設定)	JWAC の有効化および設定をします。 本機能は CLI でのみサポートされています。Web GUI では未サポートです。		
Network Access Authentication(ネット ワークアクセス認証)	Network Access Authentication(ネットワークアクセス認証)の設定を行います。		
Safeguard Engine(セーフガードエンジン)	セーフガードエンジンは、攻撃中にスイッチの稼働を最小化して、スイッチ全体の操作性を保ち、限ら れたリソース内で必要不可欠なパケットの送受信を可能にします。		
Trusted Host(トラストホスト)	トラストホストの設定を行います。		
Traffic Segmentation (トラフィックセグメンテーション)	トラフィックセグメンテーション機能はポート間のトラフィックの流れを制限を行います。		
Storm Control Settings(ストームコント ロール設定)	ストームコントロールの設定を行います。		
DoS Attack Prevention Settings(DoS 攻 擊防止設定)	各 DoS 攻撃に対して防御設定を行います。		
Zone Defense Settings(ゾーンディフェ ンス設定)	「ゾーンディフェンス(Zone Defense)」機能の設定と表示を行います。		
SSH (Secure Shell)	SSH(Secure Shell)は、安全性の低いネットワーク上で、安全なリモートログインと安全なネットワー クサービスを実現するためのプログラムです。		
SSL (Secure Socket Layer)	Secure Sockets Layer(SSL)とは、認証、デジタル署名および暗号化を使用して、ホストとクライアン ト間に安全な通信パスを提供するセキュリティ機能です。		
SFTP Server Settings(SFTP サーバ設定)	「Secure File Transfer Protocol」(SFTP) サーバの設定、表示を行います。		
SFTP Client Settings (SFTP クライアント設定)	「Secure File Transfer Protocol」(SFTP) クライアントの設定、表示を行います。		
Network Protocol Port Protect Settings(ネット ワークプロトコルポートプロテクト設定)	ネットワークプロトコルポートプロテクションの設定、表示を行います。		

# Port Security (ポートセキュリティ)

ポートセキュリティは、ポートのロックを行う前にスイッチが(ソース MAC アドレスを)認識していない不正なコンピュータが、ロックしたポートに接続してネットワークへのアクセスを行わないようにするための機能です。

### Port Security Global Settings(ポートセキュリティグローバル設定)

ポートセキュリティは、ポートのロックを行う前にスイッチが(ソース MAC アドレスを)認識していない不正なコンピュータが、ロックしたポートに接続してネットワークへのアクセスを行わないようにするための機能です。

#### Security > Port Security > Port Security Global Settings の順にクリックし、以下の画面を表示します。

Port Security Global Settings		
Port Security Trap Settings		
Trap State	O Enabled	Apply
Port Security Trap Rate Settings		
Trap Rate (0-1000)	31	Apply
Port Security System Settings		
System Maximum Address (1-12288)	No Limit	Apply
Port Security VLAN Settings		
VID List	1, 4-6	
VLAN Max Learning Address (1-12288)	No Limit	Apply
Find VLAN		
VID (1-4094)	1	Find
VID	Max Learning Address	Current No.
1	No Limit	0

図 12-1 Port Security Global Settings 画面

#### 画面に表示される項目:

項目	説明
Trap State	ポートセキュリティトラップ設定を「Enabled」(有効)または「Disabled」(無効)にします。
Trap Rate	毎秒のトラップ数を指定します。0 から 1000 までの間で指定できます。初期値の 31 は SNMP トラップがあらゆるセキュリティ違反に対して動作することを意味します。
System Maximum Address	システムの最大 MAC アドレス数を入力します。1 から 12288 まで指定可能です。指定しない場合、または「No Limit」にチェックを入れた場合、初期値の「No Limit」となり、スイッチに MAC アドレス最大数が適用されます。
VID List	VLAN ID(s)を指定します。
VLAN Max Learning Address	指定の VLAN が学習可能な MAC アドレスの最大値(1-12288)を指定します。「No Limit」を選択すると無制限に MAC アドレスを学習します。
VID	VLAN ID を指定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

# Port Security Port Settings(ポートセキュリティポート設定)

ポートセキュリティのポート設定と設定内容の表示をお行います。

Security > Port Security > Port Security Port Settings の順にメニューをクリックし、以下の画面を表示します。

Port Secur	ity Port S	ettings		_		_	_	_	_
Port Security	Port Setting	\$							
Unit From	n Port To	o Port St th1/0/1 ✔ D	ate Visabled	Maximum (0-12288)	Violation Action	Security Mode Delete-on-Timeo	Aging Time (0-1440)	) Aging Ty Absolu	rpe te 🗸
Unit 1 Settin									Apply
Port	Maximum	Current No.	Violation Action	Violation Count	Security Mode	Admin State	Current State	Aging Time	Aging Type
eth1/0/1	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
eth1/0/2	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
eth1/0/3	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
eth1/0/4	32	0	Protect		Delete-on-Timeout	Disabled	-	0	Absolute
eth1/0/5	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
eth1/0/6	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
eth1/0/7	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
eth1/0/8	32	0	Protect	-	Delete-on-Timeout	Disabled		0	Absolute

図 12-2 Port Security Port Settings 画面

画面に表示される項目:

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	設定の対象となるポートを指定します。
State	指定ポートへのポートセキュリティ機能を「Enabled」(有効)/「Disabled」(無効)にします。
Maximum	指定ポートで許可される安全な MAC アドレスの最大数を指定します。0 から 12288 まで指定可能で初期値は 32 です。
Violation Action	違反に対する動作を以下から指定します。
	• Protect - ポートセキュリティレベルで不正ホストからのパケットをすべて破棄しますが、セキュリティ違反カウントとし
	ては数えられません。
	• Restrict - ポートセキュリティレベルで不正ホストからのパケットをすべて破棄し、セキュリティ違反としてカウントされ
	システムログに記録されます。
	• Shutdown - セキュリティ違反があるとポートをシャットダウンし、システムログに記録されます。
Security Mode	セキィリティモードを以下から選択します。
	• Permanent - すべての学習した MAC アドレスは手動でエントリを削除しない限り削除されません。
	• Delete-on-Timeout - すべての学習した MAC アドレスはタイムアウトにより自動的に削除されるか、手動でエントリを削
	除します。
Aging Time	指定ポートの自動取得アドレスに使用するエージングタイムです。0から1440分の間で指定可能です。
Aging Type	エージングの種類を以下から指定します。
	• Absolute - ポート上のすべてのアドレスは指定された時間を過ぎるとアドレスリストから削除されます。(初期値)
	・ Inactivity - 指定の期間安全なアドレスからのトラフィックがない場合、エージアウトします。

-設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

### Port Security Address Entries (ポートセキュリティアドレスエントリ設定)

ポートセキュリティアドレスエントリの設定、表示を行います。

Security > Port Security > Port Security Address Entries の順にメニューをクリックし、以下の画面を表示します。

ort Security Add	ress Entries			
Unit	Port eth1/0/1	MAC Address 00-84-57-00-00-00	VID (1-4094) anent Add Delete	Clear by Port Clear by MAC
Doct	1/0	MAC Address	Address Tyrpe	Remaining Time (minc)
POIL	VID	MAC Aduless	Aduress Type	Remaining Time (mins)
	1	00-84-57-00-00-00	Permanent	

図 12-3 Port Security Address Entries 画面

画面に表示される項目:

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	設定の対象となるポートを指定します。
MAC Address	MAC アドレスを入力します。
VID	VLAN ID を指定します。1 から 4094 の間で指定できます。

「Add」ボタンをクリックして、入力した情報に基づく新しいエントリを追加します。 「Delete」ボタンをクリックし、入力した情報に基づく新しいエントリを削除します。

「Delete」小ダノをクリックし、八月した順報に奉フへ利しいエノドリを削除します

「Clear by Port」ボタンをクリックし、選択したポートに基づく情報を消去します。

「Clear by MAC」ボタンをクリックし、選択した MAC アドレスに基づく情報を消去します。

「Clear All」ボタンをクリックし、テーブル上のすべての情報を消去します。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

# 802.1X(802.1X 設定)

#### 802.1X(ポートベースおよびホストベースのアクセスコントロール)

IEEE 802.1X は、ユーザ認証を行うセキュリティの規格です。

クライアント/サーバベースのアクセスコントロールモデルを使用し、特定のローカルエリアネットワーク上の有線/無線デバイスへのアクセスを 許可および認証するために使用します。この認証方法は、ネットワークへアクセスするユーザの認証に RADIUS サーバを使用し、EAPOL(Extensible Authentication Protocol over LAN)と呼ばれるパケットをクライアント/サーバ間でリレーして実現します。

以下の図は、基本的な EAPOL パケットの構成です。



EAPOL パケット

図 12-1 EAPOL パケット

IEEE 802.1X を使用すると、未認証のデバイスが接続ポート経由で LAN に接続することを制限できます。 EAPOL パケットは、承認完了前でも指定ポート経由で送受信できる唯一のトラフィックです。

802.1X アクセスコントロールには認証サーバ、オーセンティケータ、クライアントの3つの役割があります。 それぞれがアクセスコントロールセキュリティの作成、状態の維持、動作のために重要です。



図 12-2 802.1X の 3 つの役割

以降の項目では、認証サーバ、オーセンティケータ、クライアントのそれぞれの役割について説明します。

### 認証サーバ

認証サーバは、クライアントやオーセンティケータと同じネットワークに接続されるリモートデバイスです。

認証サーバ上で RADIUS サーバプログラムが実行され、認証サーバのデータがオーセンティケータ(スイッチ)に正しく登録されている必要があり ます。スイッチポートに接続しているクライアントは、LAN 上のスイッチが提供するサービスを使用する前に、認証サーバ(RADIUS)によって認 証される必要があります。

認証サーバの役割は、ネットワークにアクセスするクライアントの身元を証明することです。認証サーバ(RADIUS)とクライアントの間で EAPOL パケットによるセキュアな情報交換を行い、クライアントが「LAN やスイッチのサービスに対するアクセス許可があるか」をスイッチに通知します。



図 12-3 認証サーバ

#### オーセンティケータ

2つ目の役割:

オーセンティケータ(スイッチ)は、認証サーバとクライアントの間を仲介します。

802.1Xを使用する場合、オーセンティケータには2つの役割があります。

- 1つ目の役割:
   クライアントに EAPOL パケットを通して認証情報を提出するよう要求することです。
   EAPOL パケットはクライアントにアクセスが許可される前にオーセンティケータを通過することのできる唯一の情報です。
  - クライアントから収集した情報を認証サーバに確認してもらい、その結果をクライアントに伝達することです。

スイッチをオーセンティケータとして設定するには、以下の手順を実行します。

- 1. スイッチの 802.1X 機能を有効にします。(Security > 802.1X > 802.1X Global Settings)
- 2. 対象ポートに 802.1X の設定を行います。(Security > 802.1X > 802.1X Port Settings)
- 3. スイッチに RADIUS サーバの設定を行います。(Security > RADIUS > RADIUS Server Settings)



図 12-4 オーセンティケータ

### クライアント

クライアントとは、LAN やスイッチが提供するサービスへアクセスしようとする端末です。

クライアントとなる端末では、802.1X プロトコルに準拠したソフトウェアが起動している必要があります。一部の Windows OS のように、OS 内に 既にそのソフトウェアが組み込まれている場合がありますが、それ以外の OS をお使いの場合は、802.1X クライアントソフトウェアを別途用意する 必要があります。

クライアントは EAPOL パケットを使用して LAN へのアクセスを要求し、スイッチからの要求に応答します。



#### 認証プロセスについて

前述の「認証サーバ」「オーセンティケータ」「クライアント」により、802.1X プロトコルはネットワークへアクセスするユーザの認証を安定的かつ 安全に行います。

認証完了前には EAPOL トラフィックのみが特定のポートの通過を許可されます。このポートは、有効なユーザ名とパスワード(802.1Xの設定によっては MAC アドレスも)を持つクライアントがアクセス権を取得してポートのロックが解除されるまで、ロック状態を保ちます。ロックが解除されると、通常のトラフィックがポートを通過できるようになります。

本製品の 802.1X では、以下の 2 種類のアクセスコントロールが選択できます。



図 12-6 802.1X 認証プロセス

本製品の 802.1X 機能では、以下の 2 つのタイプのアクセスコントロールから選択することができます。

#### 1. ポートベースのアクセスコントロール

本方式では、リモート RADIUS サーバが、ポートごとに1人のユーザのみを認証することで、同じポート上の残りのユーザがネットワークにアクセスできるようにします。

#### 2. ホストベースのアクセスコントロール

本方式では、スイッチはポートで最大 448 件までの MAC アドレスを自動的に学習してリストに追加します。 スイッチはリモート RADIUS サーバを使用して、ネットワークへのアクセスを許可する前に MAC アドレスごと (ユーザごと)の認証を行います。

#### 802.X ポートベース / ホストベースのネットワークアクセスコントロールについて

802.1X は、元々は LAN 上で Point to Point プロトコルの特長を活用するために開発されました。

単一のLAN セグメントが2台より多くのデバイスを持たない場合、デバイスのどちらかがブリッジポートとなります。 ブリッジポートは、「リンクのリモートエンドにアクティブなデバイスが接続された」「アクティブなデバイスが非アクティブ状態になった」などのイベン トを検知します。これらのイベントをポートの認証状態の制御に利用し、ポートの許可がされていない接続デバイスの認証プロセスを開始します。これをポー トベースのアクセスコントロールと呼びます。

### ポートベースネットワークアクセスコントロール

接続デバイスが認証に成功すると、ポートは「Authorized」(認証済み)の状態になります。ポートが未認証になるようなイベントが発生するまで、ポート上のすべてのトラフィックはアクセスコントロール制限の対象になりません。

そのため、ポートが複数のデバイスが所属する共有LAN セグメントに接続される場合、接続デバイスの1つが認証に成功すると共有セグメント上のすべてのLAN に対してアクセスを許可することになります。このような場合、ポートベースネットワークアクセスコントロールは脆弱であるといえます。



図 12-7 ポートベースアクセスコントロールのネットワーク構成例

### ホストベースネットワークアクセスコントロール

共有 LAN セグメント内で 802.1X を活用するには、LAN へのアクセスを希望する各デバイスに論理ポートを定義する必要があります。

スイッチは、共有 LAN セグメントに接続する1つの物理ポートを異なる論理ポートの集まりであると認識し、それら論理ポートを EAPOL パケット交換と認証状態に基づいて別々に制御します。スイッチは接続する各デバイスの MAC アドレスを学習し、それらのデバイスがスイッチ経由で LAN と通信するための論理ポートを確立します。



図 12-8 ホストベースアクセスコントロールのネットワーク構成例

## 802.1X Global Settings (802.1X グローバル設定)

本画面では 802.1X グローバル設定を行います。

802.1X 認証設定をするには、Security > 802.1X > 802.1X Global Settings の順にメニューをクリックします。

802.1X Global Settin	ngs		
802.1X Global Settings			
802.1X State	Disabled 💌		
802.1X Trap State	Disabled 💌		
			Apply

図 12-9 802.1X Global Settings 画面

画面に表示される項目:

項目	説明
802.1X State	802.1X 認証を「Enabled」(有効)/「Disabled」(無効)に設定します。
802.1X Trap State	802.1X トラップを「Enabled」(有効)/「Disabled」(無効)に設定します。
設定を変更する際は、必ず「	Apply」ボタンをクリックし、設定内容を適用してください。

### 802.1X Port Settings (802.1X ポート設定)

802.1X 認証ポートを設定します。

Security > 802.1X > 802.1X Port Settings の順にメニューをクリックします。

802.1X Port \$	Settings	_	_	_		_	_	_
802.1X Port Sett	ings							
Linit		From Port		To Port		Direction		
1	-	eth1/0/1	•	eth1/0/	/1 🔽	Both		
Port Control		Forward PD	U	MaxReq	(1-10)	PAE Authenticator		
Auto	•	Disabled		2	times	Disabled 💌		
ServerTimeout	(1-65535)	SuppTimeo	ut (1-65535)	TX Perio	od (1-65535)			
30	sec	30	sec	30	sec		(	Apply
Unit 1 Settings	e e e e e e e e e e e e e e e e e e e							
Port	Direction	Port Control	Forward PDU	MaxReq	PAE Authenticator	ServerTimeout	SuppTimeout	TX Period
eth1/0/1	Both	Auto	Disabled	2	None	30	30	30
eth1/0/2	Both	Auto	Disabled	2	None	30	30	30

図 12-10 802.1X Settings 画面

画面に表示される項目	:
------------	---

項目	説明
Unit	設定するユニットを表示します。
From Port/To Port	設定対象のポート範囲を指定します。
Direction	制御するトラフィックの方向を指定します。初期値は「both」です。 ・ in - 指定したポートへの入力トラフィックのみ制御対象となります。 ・ Both - ポートが受信送信する両方向のトラフィックについて処理します。
Port Control	<ul> <li>ポートの認証状態を指定します。</li> <li>ForceAuthorized - 802.1X を無効にします。この場合、ポートが認証状態になるのに、どのような認証の交換も必要ありません。つまり、ポートは 802.1X ベースの認証無しのトラフィックを送受信します。</li> <li>ForceUnauthorized - ポートは常に認証されていない状態になり、クライアントからの認証要求を無視します。スイッチはクライアントに対して認証サービスを提供しません。</li> <li>Auto - 802.1X を有効にし、ポートはまず、認証されていない EAPOL フレームだけを送受信できる状態になります。リンク状態が接続、切断と変化したり、EAPOL-start フレームを受け取ると認証プロセスが始まります。スイッチはクライアントの識別を要求し、クライアントと認証サーバ間の認証メッセージの中継を開始します。(初期値)</li> </ul>
Forward PDU	PDU 要求の再送を「Enabled」(有効)/「Disabled」(無効)にします。
MaxReq (1-10)	認証セッションがタイムアウトになるまでに EAP リクエストをクライアントに送信する最大の回数を指定します。1 から 10 までの間で指定可能です。初期値は 2 です。
PAE Authenticator	PAE Authenticator を「Enabled」(有効)/「Disabled」(無効)に指定します。 本項目では特定ポートを IEEE 802.1X Port Access Entity(PAE)認証として指定します。
ServerTimeout (1-65535)	Authenticator と認証サーバの通信が切れてタイムアウト状態となる時間を指定します。初期値は 30(秒)です。
SuppTimeout (1-65535)	Authenticator とクライアントの通信が切れてタイムアウト状態となる時間を指定します。初期値は 30(秒)です。
TxPeriod (1-65535)	PAE を管理する Authenticator の TxPeriod の値を指定します。EAP Request/Identity パケットがクライアントに送信され る間隔を決定します。初期値は 30(秒)です。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

### Authentication Session Information (オーセンティケーションセッションの状態)

オーセンティケーションセッションの状態を表示します。

Security > 802.1X > Authentication Session Information の順にメニューをクリックし、以下の画面を表示します。

Authenticatio	on Sessions Informati	DN	
Authentication S	essions Information		
Unit	From Port eth1/0/1	To Port eth1/0/1	Init by Port ReAuth by Port
Total Entries: 1	Port	MAC Address	
	eth1/0/1	10-BF-48-D6-E2-E2	Init by MAC ReAuth by MAC
			1/1 < 1 > > Go

図 12-11 Authentication Session Information 画面

画面に表示される項目:

項目	説明
Unit	設定するユニットを表示します。
From Port/To Port	設定対象のポート範囲を指定します。
「Init by Port」ボタン	をクリックして、入力した情報に基づくセッション情報を起動します。
「ReAuth by Port」 ポ	タンをクリックして λカーた情報に基づく再認証(Re-Authenticate)を行います。

「ReAuth by Port」示ダフをクリックして、入力した情報に基づく中認証(Re-Authenticate)を行います。 「Init by MAC」ボタンをクリックして、入力した情報に基づくセッション情報を起動します。

「ReAuth by MAC」ボタンをクリックして、入力した情報に基づく再認証(Re-Authenticate)を行います。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

### Authenticator Statistics(オーセンティケータ統計情報)

オーセンティケータの統計情報を表示します。

Security > 802.1X > Authenticator Statistics の順にメニューをクリックし、以下の画面を表示します。

uthontica	tor Statistics											
umentica	tor statistics -											
Unit	1 💌	]	F	Port	eth1/0/1 [	-					Find	Clear Counter
												Clear All
Init 4 Cot	tinge											
Jnit 1 Set	tings											
Jnit 1 Set Total Entr	tings ties: 0											
Jnit 1 Set Fotal Entr	tings ties: 0 Frames	Frames	Start	Regid	LogOff	Req	Respid	Resp	Invalid	Еггог	I ast Version	Last Source

図 12-12 Authenticator Statics 画面

画面に表示される項目:

項目	説明
Unit	表示するユニットを選択します。
Port	プルダウンメニューを使用して表示するポート範囲を指定します。

-「Find」ボタンをクリックし、入力した情報に基づくエントリを検出します。

「Clear Counters」ボタンをクリックし、選択に基づく情報を消去します。

「Clear All」ボタンをクリックし、テーブル上のすべての情報を消去します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

### Authenticator Session Statistics(オーセンティケータセッション統計情報)

オーセンティケータセッションの統計情報を表示します。

Security > 802.1X > Authenticator Session Statistics の順にメニューをクリックし、以下の画面を表示します。

uthenticator Session Sta	tistics							
Unit 1	Port	eth1/0/1					Find	Clear Counter Clear All
Jnit 1 Settings								
Total Entries: 0								
Dort Octote BY	Octote TY	Eramos DY	Eramoe TY	ID	AuthenticMethod	Time	TerminateCause	Liser Name

図 12-13 Authenticator Session Statistics 画面

画面に 表示される 項目	:

項目	説明
Unit	表示するユニットを選択します。
Port	プルダウンメニューを使用して表示するポート範囲を指定します。
「Find」ボタンをクリ	リックし、入力した情報に基づくエントリを検出します。

「Clear Counters」ボタンをクリックし、選択に基づく情報を消去します。 「Clear All」ボタンをクリックし、テーブル上のすべての情報を消去します。

### Authenticator Diagnostics(オーセンティケータ診断)

オーセンティケータ診断情報を表示します。

Security > 802.1X > Authenticator Diagnostics の順にメニューをクリックし、以下の画面を表示します。

uthenticator Diagnostics			
Authenticator Diagnostics			
Unit 1 V Port	eth1/0/1 🔽		Find Clear Counters Clear All
Unit 1 Settings			
Total Entries: 1			
Port		eth1/0/1	
EntersConnecting		3	
EAP-LogoffsWhileConnecting		0	
EntersAuthenticating		0	
SuccessesWhileAuthenticating		0	
TimeoutsWhileAuthenticating		0	
FailsWhileAuthenticating		0	
ReauthsWhileAuthenticating		0	
EAP-StartsWhileAuthenticating		0	
EAP-LogoffsWhileAuthenticating		0	
ReauthsWhileAuthenticated		0	
EAP-StartsWhileAuthenticated		0	
EAP-LogoffsWhileAuthenticated		0	
BackendResponses		0	
BackendAccessChallenges		0	
BackendOtherRequestsToSupplicant		0	
BackendNonNakResponsesFromSupplicant		0	
BackendAuthSuccesses		0	
BackendAuthFails		0	
		1/1	< < 1 > >  Go

図 12-14 Authenticator Diagnostics 画面

画面に表示される項目:

項目	説明
Unit	表示するユニットを選択します。
Port	プルダウンメニューを使用して表示するポート範囲を指定します。
「Find」ボタンをクリ	

「Clear Counters」ボタンをクリックし、選択に基づく情報を消去します。 「Clear All」ボタンをクリックし、テーブル上のすべての情報を消去します。 設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

# AAA (AAA 設定)

#### Security > AAA

本項目では AAA (Authentication、Authorization、Accounting)の「Enabled」(有効) /「Disabled」(無効)を行います。

### AAA Global Settings (AAA グローバル設定)

本項目では AAA をグローバルに「Enabled」(有効)/「Disabled」(無効)に設定します。

Security > AAA > AAA Global Settings の順にメニューをクリックし、以下の画面を表示します。

AAA Global Sett	ings		
AAA State Settings			
AAA State	<ul> <li>Disabled</li> </ul>	CEnabled	Apply

図 12-15 AAA Global Settings 画面

「AAA State」をグローバルに「有効」(Eneable)/「無効」(Disable)をグローバルに指定します。

### Application Authentication Settings(アプリケーションの認証設定)

ログインする際に使用するスイッチの設定用アプリケーション(コンソール、Telnet、SSH、HTTP)を設定します。

Security > Access Authentication Control > Application Authentication Settings の順にクリックし、以下の画面を表示します。

Application Authentication Settin	gs	
Application Authentication Settings		
Application	Login Method List	
Console	default	Edit
Telnet	default	Edit
SSH	default	Edit
HTTP	default	Edit

図 12-16 Application Authentication Settings 画面

指定エントリの「Edit」ボタンをクリックし編集を行います。

「Edit」をクリックすると、以下の画面が表示されます。

Application Authentication Settin	gs	
Application Authentication Settings		
Application	Login Method List	
Console	default	Apply
Telnet	default	Edit
SSH	default	Edit
HTTP	default	Edit

図 12-17 Application Authentication Settings (Edit) 画面

画面に表示される項目:

項目	説明
Login Method List	指定エントリの「Edit」ボタンをクリックし編集を行います。使用するログインメソッドリスト名を入力します。
設定を変更する際は	必ず「Annly」ボタンをクリック」。 設定内容を適用してください

### Application Accounting Settings(アプリケーションアカウント設定)

アプリケーションアカウントを設定します。

**Security > AAA > Application Accounting Settings**の順にクリックし、以下の画面を表示します。

Application	E	xec Method List	
Console			Edit
Teinet			Edit
SSH			Edit
Court.			
HTTP	hod List		Edit
HTTP plication Accounting Commands Me pplication Console otal Entries: 1 Application	thod List Level 1 Commands	Method List 32 Chars	Edit

図 12-18 Application Accounting Settings 画面

「Edit」をクリックし、以下の画面で指定エントリの設定を行います。

Application Accounting Settings	_		
Application Accounting Exec Method List			
Application		Exec Method List	
Console			Apply
Telnet			Edit
SSH			Edit
HTTP			Edit
Application Accounting Commands Method List			
Application Console  Level	1 🗸	Commands Method List 32 chars	Apply
Total Entries: 1			
Application	Level	Commands Method List	
Console	1	method	Delete
			1/1  < < 1 > >  Go

図 12-19 Application Accounting Settings (Edit) 画面

画面に表示される項目:	長示される項目:
-------------	----------

項目	説明
Exec Method List	指定エントリの「Edit」ボタンをクリックし編集を行います。使用する EXEC メソッドリスト名を入力します。
Application	使用するアプリケーションを選択します。「Console」「Telnet」「SSH」から選択します。
Level	権限レベルを指定します。1 から 15 の間で指定できます。
Commands Method List	使用するコマンドメソッドリストを入力します。

「Delete」をクリックして指定エントリを削除します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

### Authentication Settings(認証設定)

AAA ネットワークと EXEC 認証設定を行います。

Security > AAA > Authentication Settings の順にメニューをクリックし、以下の画面を表示します。

AAA Authe	entication Network	AAA Authentication Exec			
AAA Authen	tication 802.1X				
Status	Disabled	~			
Method 1	Please Select	$\checkmark$	Method 2	Please Select	
Method 3	Please Select	$\checkmark$	Method 4	Please Select	Apply
AAA Authon	tication MAC Auth				
Status	Disabled	~			
Method 1	Please Select	~	Method 2	Please Select	
Method 3	Please Select	$\checkmark$	Method 4	Please Select	Apply
AAA Authen	tication WEB-Auth				
Status	Disabled	~			
Method 1	Please Select	~	Method 2	Please Select	
Method 3	Please Select	V	Method 4	Please Select	Apply
AAA Authen	tication IGMP-Auth Del	fault Group Radius			
Status	Disabled				Apply

図 12-20 Authentication Settings - AAA Authentication Settings タブ画面

#### 「AAA Authentication Network」タブ

「AAA Authentication Network」タブ内の設定を行います。

「AAA Authentication 802.1X」「AAA Authentication MAC-Auth」「AAA Authentication WEB-Auth」「AAA Authentication IGMP-Auth Default Group Radius」それぞれの項目において設定を行います。

項目	説明
Status	各項目の認証設定の「有効」(Eneable)/「無効」(Disable)を設定します。
Method 1 to 4	本設定項目のメソッドリストを選択します。「none」「local」「group」「radius」から選択します。
設定を変更する際は	

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

### 「AAA Authentication Exec」タブ

「AAA Authentication Exec」タブをクリックして、タブ内の設定を行います。

uthentica	tion Settings		_		_	_
AAA Authe	entication Network	AAA Authentication Exec				
AAA Authen	tication Enable					
Status	Disabled	<ul> <li></li> </ul>				
Method 1	Please Select		Method 2	Please Select		
Method 3	Please Select		Method 4	Please Select		Apply
AAA Authen List Name	tication Login 32 chars					
Method 1	none	~	Method 2	Please Select 🔽		
Method 3	Please Select		Method 4	Please Select		Apply
fotal Entries	:1					
N	lame	Method 1	Method 2	Method 3	Method 4	
	list	radius	tacacs+	local		Delete

図 12-21 Authentication Settings - AAA Authentication Exec タブ画面

画面に表示される項目:

項目	説明
	AAA Authentication Enable(AAA 認証有効)
Status	AAA 認証設定の「有効」(Eneable)/「無効」(Disable)を設定します。
Method 1 to 4	本設定項目のメソッドリストを選択します。「none」「enable」「group」「radius」「tacacs+」から選択します。
	AAA Authentication Login(AAA 認証ログイン)
List Name	AAA 認証ログインオプションを使用するメソッドリスト名を入力します。
Status	AAA 認証設定の「有効」(Eneable)/「無効」(Disable)を設定します。
Method 1 to 4	使用するメソッドリストを選択します。「none」「enable」「group」「radius」「tacacs+」から選択します。
シーンであるものです。	

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

「Delete」をクリックして指定エントリを削除します。

# Accounting Settings(アカウンティング設定)

アカウンティングの設定を行います。

Security > AAA > Accounting Settings の順にメニューをクリックし、以下の画面を表示します。

Accounting	Settings		_	_		_	
AAA Accou	unting Network	AAA Accounting System	AAA	Accounting Exec	AAA Accounting Commands		
Default	Disabled						
Method 1	Please Select		Method 2	Please Select	•		
Method 3	Please Select	-	Method 4	Please Select	<b>T</b>		Apply

図 12-22 Accounting Settings 画面

「AAA Accounting Network」「AAA Accounting System」「AAA Accounting Exec」「AAA Accounting Commands」それぞれのタブにおいて設定を行います。

項目	説明
	「AAA Accounting Network」タブ
Default	メソッドリストの「Enabled」(有効)/「Disabled」(無効)を指定します。
Method 1 to 4	使用するメソッドリストを選択します。「none」「group」「radius」「tacacs+」から選択します。
	「AAA Accounting System」タブ
Default	メソッドリストの「Enabled」(有効)/「Disabled」(無効)を指定します。
Method 1 to 4	使用するメソッドリストを選択します。「none」「group」「radius」「tacacs+」から選択します。
	「AAA Accounting Exec」タブ
List Name	使用する AAA アカウンティング EXE オプションのメソッドリストを入力します。
Method 1 to 4	使用するメソッドリストを選択します。「none」「group」「radius」「tacacs+」から選択します。
	「AAA Accounting Commands」タブ
Level	権限レベルを指定します。1 から 15 までで指定可能です。
List Name	使用する AAA アカウンティングコマンドオプションのメソッドリストを入力します。
Method 1 to 4	使用するメソッドリストを選択します。「none」「group」「tacacs+」から選択します。

「Delete」をクリックして指定エントリを削除します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

# RADIUS (RADIUS 設定)

RADIUS サーバの設定を行います。

### RADIUS Global Settings (RADIUS グローバル設定)

RADIUS をグローバルに「Enabled」(有効)/「Disabled」(無効)にします。

#### Security > RADIUS > RADIUS Global Settings の順にメニューをクリックし、以下の画面を表示します。

RADIUS Global Settings		
RADIUS Global Settings		
Dead Time (0-1440)	0 min	Apply
RADIUS Global IPv4 Source Interface		
IPv4 RADIUS Source Interface Name		Apply
RADIUS Global IPv6 Source Interface		
IPv6 RADIUS Source Interface Name		Apply
RADIUS Server Attribute Settings		
RADIUS Server Attribute NAS-IP-Address		Apply

図 12-23 RADIUS Global Settings 画面

画面に表示される項目:

項目	説明
DeadTime	デッドタイムの設定を行います。1 から 1440 (分)の間で指定できます。初期値は「0」です。0 に設定されている場合、応答
(0-1440)	しないサーバは「Dead」として認識されることはありません。この設定により、応答しないサーバホストエントリをスキップ
	する「デッドタイム」が設定され認証プロセスは改善されます。システムが認証サーバと連携して動作する場合、一度に一つ
	のサーバと連携します。もし連携しようとしたサーバが応答しない場合、システムは次のサーバとの連携を模索します。シス
	テムにより応答しないサーバが見つけられると、該当のサーバは「down」として認識され、「デッドタイム」タイマーが開始
	され、それ以後のリクエスト認証はデッドタイム時間が過ぎるまでスキップされます。
IPv4 RADIUS	IPv4 RADIUS アドレスソースインタフェース名を入力します。
Source Interface	
Name	
IPv6 RADIUS	IPv6 RADIUS アドレスソースインタフェース名を入力します。
Source Interface	
Name	
RADIUS Server	RADIUS サーバ属性 NAS-IP アドレスを指定します。
Attribute NAS-IP-	
Address	

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

### RADIUS Server Settings(RADIUS サーバの設定)

RADIUS サーバによって集約したユーザ管理や Sniffing やハッカーからの保護が可能になります。

Security > RADIUS > RADIUS Server Settings をクリックし、以下の画面を表示します。

RADIUS Server Settings						
RADIUS Server Settings						
IP Address		O IPv6 Add	ess	2013::1		
Authentication Port (0-65535)	1812	Accounting F	Port (0-65535)	1813		
Retransmit (0-20)	2	times Timeout (1-2	55)	5	sec	
Кеу Туре	Plain Text 🗸	Key		254 chars		Apply
Total Entries: 1						
IPv4/IPv6 Address	Authentication Port	Accounting Port	Timeout	Retransmit	Key	
10.90.90.1	1812	1813	5	2	*****	Delete

図 12-24 RADIUS Server Settings 画面

画面に表示される項目:

項目	説明
IP Address	RADIUS サーバの IPv4 アドレスを入力します。
IPv6 Address	RADIUS サーバの IPv6 アドレスを入力します。
Authentication Port (0-65535)	RADIUS 認証サーバの UDP ポートを 0-65535 の範囲で入力します。(初期値:1812) 認証しない場合は、0 を入力します。
Accounting Port (0-65535)	RADIUS アカウントサーバのポートを 0-65535 の範囲で入力します。(初期値:1813) 認証しない場合は、0 を入力します。
Retransmit (0-20)	RADIUS サーバの再転送間隔(秒)を設定します。初期値は 3(秒)です。
Timeout (1-255)	RADIUS サーバのタイムアウト時間(秒)を設定します。初期値は 5(秒)です。
Кеу Туре	RADIUS サーバに設定する鍵の種類を以下から選択します。 「Plain Text」「Encrypted」
Кеу	RADIUS サーバに設定したものと同一の鍵を指定します。254 文字以内で指定します。
設定を変更する際は、必ず「App	

「Delete」をクリックして指定エントリを削除します。

### RADIUS Group Server Settings(RADIUS グループサーバの設定)

RADIUS グループサーバの表示、設定を行います。

Security > RADIUS > RADIUS Group Server Settings をクリックし、以下の画面を表示します。

RADIUS Group Server Settings									
RADIUS Group Server Settings									
Group Server Name IP Address IPv6 Address	32 chars	· ·							Add
Total Entries: 2									
Group Server Name	IPv4/IPv6 Address								
group	10.1.1.1		-	-	-	-	-	-	Show Detail Delete
radius	10.90.90.9	-	-	-	-	-	-	-	

図 12-25 RADIUS Group Server Settings 画面

画面に表示される項目:

項目	説明
Group Server Name	RADIUS グループサーバ名を入力します。15 文字までで指定可能です。
IP Address	RADIUS サーバの IPv4 アドレスを入力します。
IPv6 Address	RADIUS サーバの IPv6 アドレスを入力します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

「Delete」をクリックして指定エントリを削除します。

「Show Detail」をクリックして、指定エントリの詳細について表示します。
「Show Detail」をクリックすると、以下の画面が表示されます。

12 chars			Apply
12 chars			Apply
			Apply
s			
		Delete	
			Back
	5	5	S Delete

図 12-26 RADIUS Group Server Settings (Detail) 画面

#### 画面に表示される項目:

項目	説明		
VRF Name	VRF インスタンス名を 12 字以内で入力します。		
IPv4 RADIUS Source Interface Name	IPv4 RADIUS アドレスソースインタフェース名を入力します。		
IPv6 RADIUS Source Interface Name	IPv6 RADIUS アドレスソースインタフェース名を入力します。		
。 役定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。			

「Delete」をクリックして指定エントリを削除します。 「Back」をクリックして以前の画面に戻ります。

#### RADIUS Statistic (RADIUS 統計情報)

RADIUS 統計情報の表示、設定を行います。

Security > RADIUS > RADIUS Statistic をクリックし、以下の画面を表示します。

ADIUS Statistic			
ADIUS Statistic			
Group Server Name Please Select 💌			Clear Clear All
Total Entries: 1			
RADIUS Server Address	Authentication Port	Accounting Port	State
10.90.90.254	1812	1813	Up
		1/1	
RADIUS Server Address: 10.90.90.254			Clear
Parameter	Authentication Port		Accounting Port
Round Trip Time	0		0
Access Requests	0		NA
Access Accepts	0		NA
Access Rejects	0		NA
Access Challenges	0		NA
Acct Request	NA		0
Acct Response	NA		0
Retransmissions	0		0
Malformed Responses	0		0
Bad Authenticators	0		0
Pending Requests	0		0
Timeouts	0		0
Unknown Types	0		0
Packets Dropped	0		0

#### 図 12-27 RADIUS Statistic 画面

画面に表示される項目:

項目	説明			
Group Server Name	表示する RADIUS グループサーバ名を選択します。			
	ページ番号を入力後 「Go」ボタンをクリックトアー性定のページへ移動します			

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

「Clear」ボタンをクリックし、選択に基づいて表示した情報を消去します。

「Clear All」ボタンをクリックし、テーブル上のすべての情報を消去します。

## TACACS+(TACACS+設定)

TACACS+ サーバの設定を行います。

### TACACS+ Global Settings (TACACS+ サーバグローバル設定)

TACACS+ サーバをグローバルに「Enabled」(有効)/「Disabled」(無効)に指定します。

#### Security > TACACS+ > TACACS+ Global Settings をクリックし、以下の画面を表示します。

TACACS+ Global Settings	
TACACS+ Global IPv4 Source Interface	
IPv4 TACACS+ Source Interface Name	Apply
TACACS+ Global IPv6 Source Interface	
IPv6 TACACS+ Source Interface Name	Apply

図 12-28 TACACS+ Global Settings 画面

画面に表示される項目:	
項目	説明
IPv4 TACACS+	IPv4 TACACS+ ソースインタフェース名を入力します。
Source Interface	
Name	
IPv6 TACACS+	IPv6 TACACS+ アドレスソースインタフェース名を入力します。
Source Interface	
Name	

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

#### TACACS+ Server Settings (TACACS+ サーバの設定)

TACACS+ サーバの表示、設定を行います。

#### Security > TACACS+ > TACACS+ Server Settings をクリックし、以下の画面を表示します。

ACACS+ Server Settings					
IP Address         •		○ IPv6 Address Timeout (1-255) Key	○ IPv6 Address         2013∷1           Timeout (1-255)         5           Key         254 chars		Apply
Fotal Entries: 1					
IPv4/IPv6 Address	: Pi	ort Tin	neout	Key	
10.90.90.1	4	9	5	*****	Delete

図 12-29 TACACS+ Server Settings 画面

#### 画面に表示される項目:

項目	説明
IP Address	TACACS+ サーバの IPv4 アドレスを入力します。
IPv6 Address	TACACS+ サーバの IPv6 アドレスを入力します。
Port (1-65535)	TACACS+ サーバのポートです。初期値は 49 です。
Timeout (1-255)	TACACS+ サーバのタイムアウト時間(秒)を設定します。初期値は 5(秒)です。
Кеу Туре	TACACS+ サーバに設定する鍵の種類を以下から選択します。
	[Plain Text] [Encrypted]
Кеу	TACACS+サーバに設定したものと同一の鍵を指定します。254文字以内で指定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

「Delete」をクリックして指定エントリを削除します。

## TACACS+ Group Server Settings(TACACS+ グループサーバの設定)

TACACS+ グループサーバの表示、設定を行います。

Security > TACACS+ :	> TACACS+ Grou	o Server Settings	<b>。</b> をクリックし、	以下の画面を表示します。
----------------------	----------------	-------------------	------------------	--------------

TACACS+ Group Ser	ver Setting	S	_	_	_	_	_	_	
TACACS+ Group Server Se	ettings								
Group Server Name IPv4 Address IPv6 Address		32 char	s 						Add
Total Entries: 2									
Group Server Name				IPv4/IPv6	6 Address				
Group	10.90.90	-	-	-	-	-	-	-	Show Detail Delete
tacacs+	10.90.90	-		-	-	-		-	

図 12-30 TACACS+ Group Server Settings 画面

画面に表示される項目:

項目	説明
Group Server Name	TACACS+ グループサーバ名を入力します。32 文字までで指定可能です。
IPv4 Address	TACACS+ グループサーバの IPv4 アドレスを入力します。
IPv6 Address	TACACS+ グループサーバの IPv6 アドレスを入力します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

「Delete」をクリックして指定エントリを削除します。

「Show Detail」をクリックすると TACACS+ グループサーバの詳細情報について表示されます。

#### TACACS+ Group Server Settings - Show Detail(TACACS+ グループサーバ詳細設定)

TACACS+ Group Server Settings	
Group Server Name: Group	
VRF Name 12 chars	Apply
Group Server Name: Group	
IPv4 TACACS+ Source Interface Name	
IPv6 TACACS+ Source Interface Name	Apply
Group Server Name: Group	
IPv4/IPv6 Address	
10.90.90.14	Delete
	Back

図 12-31 TACACS+ Group Server Settings - Show Detail 画面

画面に表示される項目:

項目	説明		
VRF Name	VRF インスタンス名を 12 字以内で入力します。		
IPv4 TACACS+	IPv4 TACACS+ ソースインタフェース名を入力します。		
Source Interface			
Name			
IPv6 TACACS+	IPv6 TACACS+ ソースインタフェース名を入力します。		
Source Interface			
Name			

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。 「Delete」をクリックして指定エントリを削除します。 「Back」をクリックして以前の画面に戻ります。

## TACACS+ Statistic(TACACS+ 統計情報)

TACACS+ 統計情報の表示、設定を行います。

Security > TACACS+ > TACACS+ Statistic をクリックし、以下の画面を表示します。

TACACS+ Statistic		_	_					
TACACS+ Statistic								
Group Server Name Please Select 💙						Clear	Clear All	
Total Entries: 1	Total Entries: 1							
TACACS+ Server Address	State	Socket Opens	Socket Closes	Total Packets Sent	Total Packets Recv	Reference Count		
10.90.90.1/49	Up	0	0	0	0	0	Clear	

図 12-32 TACACS+ Statistic 画面

画面に表示される項目:

項目	説明			
Group Server Name	表示する TACACS+ グループサーバ名を選択します。			

「Clear」ボタンをクリックし、選択に基づいて表示した情報を消去します。

「Clear by Group」ボタンをクリックし、選択したグループのすべての情報を消去します。

「Clear All」ボタンをクリックし、テーブル上のすべての情報を消去します。

## IMPB (IP-MAC-Port Binding / IP-MAC- ポートバインディング)

IP ネットワークレイヤ(IP レベル)では4バイトのアドレスを使用し、イーサネットリンクレイヤ(データリンクレベル)では6バイトの MAC ア ドレスを使用します。これらの2つのアドレスタイプを結合させることにより、レイヤ間のデータ転送を可能にします。IP-MAC バインディングの 第一の目的は、スイッチにアクセスするユーザ数を制限することです。IP アドレスと MAC アドレスのペアを、事前に設定したデータベースと比較 を行い、認証クライアントのみがスイッチのポートアクセスできるようにします。もしくは DHCP スヌーピングが有効な場合において、スイッチが スヌーピング DHCP パケットから自動的に IP/MAC ペアを学習し、IMPB ホワイトリストに保存することで、認証クライアントのポートアクセスが 可能になります。未認証ユーザが IP-MAC バインディングが有効なポートにアクセスしようとすると、システムはアクセスをブロックして、パケッ トを廃棄します。本機能はポートベースであるため、ポートごとに本機能を「Enabled」(有効)/「Disabled」(無効)にすることができます。

#### IPv4

#### DHCPv4 Snooping (DHCPv4 スヌーピング)

■ DHCP Snooping Global Settings (DHCP スヌーピンググローバル設定)

DHCP スヌーピングについてグローバルに表示、設定します。

Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Global Settings の順にクリックして、以下の画面を表示します。

DHCP Snooping Global Sett	tings		
DHCP Snooping Global Settings			
DHCP Snooping	Enabled	Disabled	
Information Option Allow Untrusted	OEnabled	Disabled	
Source MAC Verification	Enabled	ODisabled	
Station Move Deny	OEnabled	Disabled	Apply

図 12-33 DHCP Snooping Global Settings 画面

#### 画面に表示される項目:

項目	説明
DHCP Snooping	DHCP スヌーピングをグローバルに「Enabled」(有効)または「Disabled」(無効)にします。
Information Option	不明インタフェースのリレーオプション 82 付き DHCP パケットをグローバルに「Enabled」(有効)または「Disabled」(無効)
Allow Untrusted	にします。
Source MAC	クライアントのハードウェアアドレスと DHCP パケットの送信元 MAC アドレスの合致確認を「Enabled」(有効)または
Verification	「Disabled」(無効)にします。
Station Move Deny	DHCP スヌーピングステーションムーブを「Enabled」(有効)/「Disabled」(無効)にします。
	有効の場合、指定ポートにある同じ VLAN ID と MAC アドレスを持つダイナミック DHCP バインディングエントリは、新しい
	DHCP プロセスが同じ VLAN ID と MAC アドレスに属している事を検出した場合、他のポートへ移動することが可能です。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

#### ■ DHCP Snooping Port Settings (DHCP スヌーピングポート設定)

DHCP スヌーピングポートの表示、設定を行います。

Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Port Settings の順にクリックして、以下の画面を表示します。

DHCP Snooping Port Settings			
DHCP Snooping Port Settings			
Unit	1		
From Port	eth1/0/1		
To Port	eth1/0/1		
Entry Limit (0-1024)	V No Limit		
Rate Limit (1-300)	No Limit		
Trusted	No		Apply
Port	Trusted	Rate Limit	Entry Limit
eth1/0/1	No	No Limit	No Limit
eth1/0/2	No	No Limit	No Limit
eth1/0/3	No	No Limit	No Limit
eth1/0/4	No	No Limit	No Limit
eth1/0/5	No	No Limit	No Limit
eth1/0/6	No	No Limit	No Limit
eth1/0/7	No	No Limit	No Limit
eth 1/0/8	No	No Limit	No Limit
eth 1/0/9	No	No Limit	No Limit
eth1/0/10	No	No Limit	No Limit
eth1/0/11	No	No Limit	No Limit
eth1/0/12	No	No Limit	No Limit
eth1/0/13	No	No Limit	No Limit
eth1/0/14	No	No Limit	No Limit
eth1/0/15	No	No Limit	No Limit

図 12-34 DHCP Snooping Port Settings 画面

画面に表示される項目:

項目	説明
Unit	設定するユニットを表示します。
From Port/To Port	設定対象のポート範囲を指定します。
Entry Limit	エントリリミットの値を入力します。0 から 1024 の間で入力可能です。「No Limit」にチェックをすると、本機能は無効 になります。
Rate Limit	レートリミットの値を入力します。1から300の間で入力可能です。「No Limit」にチェックをすると、本機能は無効になります。
Trusted	トラストのオプションを選択します。「No」または「Yes」から選択します。DHCP サーバや他のスイッチなどに接続して いるポートはトラストインタフェースとして設定される必要があります。DHCP クライアントに接続しているポートはア ントラストとして設定します。DHCP スヌーピングは DHCP サーバとアントラストインタフェースの間でファイアウォー ルとして動作します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

#### DHCP Snooping VLAN Settings(DHCP スヌーピング VLAN 設定)

DHCP スヌーピング VLAN の設定、表示を行います。

Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping VLAN Settings の順にクリックして、以下の画面を表示します。

DHCP Snooping VLAN Settings						
DHCP Snooping VLAN Settings						
VID List 1, 4-6	State Enabled	Apply				
DHCP Snooping Enabled VID : 1						

図 12-35 DHCP Snooping VLAN Settings 画面

画面に表示される項目:

項目	説明
VID List	設定する VLAN ID リストを入力します。
State	DHCP スヌーピング VLAN を「Enabled」(有効)/「Disabled」(無効)に指定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

#### ■ DHCP Snooping Database (DHCP スヌーピングデータベース)

DHCP スヌーピングデータベースの表示、設定を行います。

#### Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Database の順にクリックして、以下の画面を表示します。

DHCP Snooping Data	base			
DHCP Snooping Database				
DHCP Snooping Database				Reset
Write Delay (60- 86400)	300	sec		Apply
Store DHCP Snooping Datab	base			
URL	TFTP I// A URL beginnin	g with this prefix //location/filename		Apply
Load DHCP Snooping Datab	ase			
URL	TFTP  // A URL beginnin	g with this prefix //location/filename		Apply
IP DHCP Snooping Database	e Information			
Write Delay URL	300 seconds			
Last ignored Bindings counter	rs			
Binding Collisions	0	Expired Lease	0	
Invalid Interfaces	0	Unsupported VLAN	0	
Parse Failures	0	Checksum Errors	0	Clear

図 12-36 DHCP Snooping Database 画面

画面に表示される項目:

項目	説明				
	DHCP Snooping Database				
Write Delay	書き込み遅延の値を入力します。60から86400(秒)の間で指定できます。初期値は300秒です。				
	「Apply」ボタンをクリックし、設定内容を適用してください。				
	Store DHCP Snooping Database				
URL	JRL ロケーションをドロップダウンメニューから選択し、ストアされる DHCP スヌーピングデータベースの URL を入力します。 選択できるロケーションは「TFTP」「FTP」「Flash」です。				
Load DHCP Snooping Database					
URL	ロケーションをドロップダウンメニューから選択し、ロードされる DHCP スヌーピングデータベースの URL を入力します。				
	選択できるロケーションは「TFTP」「FTP」「Flash」です。				

「Apply」ボタンをクリックし、設定内容を適用してください。 「Clear」ボタンをクリックするとカウンタ情報が消去されます。 「Reset」ボタンをクリックすると入力した情報がリセットされます。

#### ■ DHCP Snooping Binding Entry (DHCP スヌーピングバインディングエントリ設定)

DHCP スヌーピングバインディングエントリの表示、設定を行います。

#### Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Binding Entry の順にクリックして画面を表示します。

DHCP Snooping Binding E	intry					
DHCP Snooping Manual Binding						
MAC Address	00-84-57-00-00-	00				
VID (1-4094)						
IP Address		4				
Unit	1					
Port	eth1/0/1					
Expiry (60-4294967295)		sec				
						Add
Total Entries: 1						
MAC Address	VID	IP Address	Port	Expiry	Туре	
00-84-57-00-00-00	1	10.90.90.254	eth1/0/1	3600	dhcp-snooping	Delete
					1	/1  < < 1 > >  Go

図 12-37 DHCP Snooping Binding Entry 画面

# 第12章 Security(セキュリティ機能の設定)

#### 本画面には以下の項目があります。

項目	説明
MAC Address	DHCP スヌーピングバインディングエントリの MAC アドレスを入力します。
VID	DHCP スヌーピングバインディングエントリの VLAN ID を入力します。1 から 4094 の間で入力可能です。
IP Address	DHCP スヌーピングバインディングエントリの IP アドレスを入力します。
Unit	設定するユニットを指定します。
Port	設定するポートを指定します。
Expiry	有効期限を入力します。60 から 4294967295(秒)で指定可能です。

「Add」をクリックして入力した情報を元に新しいエントリを追加します。

「Delete」をクリックして指定エントリを削除します。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

#### Dynamic ARP Inspection(ダイナミック ARP インスペクション)

■ ARP Access List (ARP アクセスリスト)

ARP アクセスリストの設定、表示を行います。

Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Access List の順にクリックして、以下の画面を表示します。

ARP Access List		
ARP Access List		
ARP Access List Name	32 chars	Add
Total Entries: 1		
	ARP Access List Name	
	ARP-Access-List	Edit Delete

図 12-38 ARP Access List 画面

#### 画面に表示される項目:

項目	説明
ARP Access List	ARP アクセスリスト名を入力します。32 文字まで入力可能です。
Name	

「Add」をクリックして入力した情報を元に新しいエントリを追加します。 「Delete」をクリックして指定エントリを削除します。

#### エントリの編集

「Edit」ボタンをクリックして指定のエントリを編集します。以下の画面が表示されます。

Action Permit	~							
P Any		Sender IP		2 2	Sender IP M	ask .		
MAC Any	~	Sender M	AC		Sender MAC	Mask		
						E	Back /	Apply
RP Access List Nam	e: ARP						Back /	Apply
RP Access List Nam Total Entries: 1	e: ARP						Back	Apply
RP Access List Nam Total Entries: 1 Action	e: ARP IP Type	Sender IP	Sender IP Mask	MAC Type	Sender MAC	Sender MAC Mask	Back	Apply

図 12-39 ARP Access List - Edit 画面

画面に表示される項目:

項目	説明
Action	動作について指定します。「Permit」「Deny」から選択します。
IP	使用する送信者の IP アドレスの種類を指定します。「Any」「Host」「IP with Mask」から指定します。
Sender IP	送信者の IP アドレスを「Host」「IP with Mask」から選択した後、使用する送信者の IP アドレスを入力します。
Sender IP Mask	「IP with Mask」を選択した場合、使用する送信者の IP マスクを入力します。
MAC	送信者の MAC アドレスの種類を指定します。「Any」「Host」「MAC with Mask」から指定します。
Sender MAC	送信者の MAC アドレスを「Host」「MAC with Mask」から選択した後、使用する送信者の MAC アドレスを入力します。
Sender MAC Mask	「MAC with Mask」を選択した場合、使用する送信者の MAC マスクを入力します。

「Back」をクリックして前のページに戻ります。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

「Delete」をクリックして指定エントリを削除します。

#### ■ ARP Inspection Settings(ARP インスペクション設定)

ARP インスペクションの設定、表示を行います。

Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Settings の順にクリックして、以下の画面を表示します。

ARP Inspect	tion Settings		
ARP Inspection	Validation		
Src-MAC	Enabled	Oisabled	
Dst-MAC	CEnabled	Disabled	
IP	CEnabled	Disabled	Apply
ARP Inspection	VLAN Logging		
Total Entries:	0		
VID		ACL Logging	DHCP Logging
ARP Inspection	n Filter		
ARP Access L	ist Name	32 chars	
VID List		1, 4-6	
Static ACL		No	Add Delete
Total Entries:	1		
VID		ARP Access List Name	Static ACL
1		ARP-Access-List	No
			1/1  < < 1 > >  Go

図 12-40 ARP Inspection Settings 画面

#### 画面に表示される項目:

項目	説明
Src-MAC	送信元 MAC のオプションについて「Enabled」(有効)/「Disabled」(無効)に設定します。本オプションを有効にすると ARP 本体内の送信者 MAC アドレスに対する送信元 MAC アドレスのイーサネットヘッダの一貫性や ARP リクエスト、応対パケットな どをチェックします。
Dst-MAC	宛先 MAC のオプションについて「Enabled」(有効)/「Disabled」(無効)に設定します。本オプションを有効にすると ARP 本 体内の宛先 MAC アドレスに対する宛先 MAC アドレスのイーサネットヘッダの一貫性や ARP リクエスト、応対パケットなどを チェックします。
IP	IP のオプションについて「Enabled」(有効) /「Disabled」(無効) に設定します。本オプションを有効にすると不正や予期せぬ IP アドレスの ARP 本体をチェックします。本オプションはまた ARP ペイロードにおける IP アドレスの妥当性もチェックします。 ARP リクエストとレスポンスの両方の送信元 IP および ARP レスポンスのターゲット IP の妥当性を確認します。IP アドレス「0.0.0.」 「255.255.255」に向かうパケットとすべての IP マルチキャストは破棄されます。送信者 IP アドレスはすべての ARP リクエス トとレスポンスでチェックされ、宛先 IP アドレスは ARP レスポンス内のみでチェックされます。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

本画面の「ARP Inspection Filter」には以下の項目があります。

項目	説明
ARP Access List	ARP アクセスリスト名を入力します。32 文字まで入力可能です。
Name	
VID List	使用する VLAN ID リストを指定します。
Static ACL	スタティック ACL を使用するか否かを選択します。

「Add」をクリックして入力した情報を元に新しいエントリを追加します。

「Delete」をクリックして指定エントリを削除します。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

#### ■ ARP Inspection Port Settings (ARP インスペクションポート設定)

ポートでの ARP インスペクションの設定、表示を行います。

#### Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Port Settings の順にクリックして、以下の画面を表示します。

ARP Inspection Port	Settings			
Unit	1	From Port	eth1/0/1	To Port eth1/0/1
Rate Limit (1-150)	pps	Burst Interval (1-15)	Von	e
Trust State	Disabled			Apply Set to Default
Port	Trust State		Rate Limit (pps)	Burst Interval
eth1/0/1	Untrusted		15	1
eth1/0/2	Untrusted		15	1
eth1/0/3	Untrusted		15	1
eth1/0/4	Untrusted		15	1
eth1/0/5	Untrusted		15	1
eth1/0/6	Untrusted		15	1
eth1/0/7	Untrusted		15	1
eth1/0/8	Untrusted		15	1
eth1/0/9	Untrusted		15	1
eth1/0/10	Untrusted		15	1
eth1/0/11	Untrusted		15	1
eth1/0/12	Untrusted		15	1

図 12-41 ARP Inspection Port Settings 画面

画面に表示される項目:

項目	説明
Unit	設定するユニットを指定します。
From Port/	ポートの範囲を指定します。
To Port	
Rate Limit	レート制限の値を入力します。1 から 150(パケット / 秒)の間で設定します。
Burst Interval	バーストインターバルの値を入力します。1から15の間で設定します。「None」にチェックをするとオプションは無効になります。
Trust State	トラスト状態について「Enabled」(有効)/「Disabled」(無効)にします。

「Apply」ボタンをクリックし、設定内容を適用してください。

## 「Set to Default」ボタンをクリックすると、設定内容は初期値に変更します。

#### ■ ARP Inspection VLAN(ARP インスペクション VLAN 設定)

VLAN での ARP インスペクションの設定、表示を行います。

#### Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection VLAN の順にクリックして、以下の画面を表示します。

	ARP Inspection VLAN			
(	VID List	4-6	State Enabled	Apply
	ARP Inspection Enabled VID :	1		

図 12-42 ARP Inspection VLAN 画面

画面に表示される項目:

項目	
VID List	設定する VLAN ID リストを入力します。
State	指定 VLAN の ARP インスペクションについて「Enabled」(有効)/「Disabled」(無効)に設定します。

「Apply」ボタンをクリックし、設定内容を適用してください。

#### ■ ARP Inspection Statistics (ARP インスペクション統計)

ARP インスペクションの統計情報の表示、消去を行います。

Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Statistics の順にクリックして、以下の画面を表示します。

/ID List		1, 4-6		]				Clear b	y VLAN Clear All
otal Er	ntries: 1								
VIAN	Forwarded	Dropped	DHCP Drops	ACL Drops	DHCP Permits	ACL Permits	Source MAC Failures	Dest MAC Failure	IP Validation Failure
V Louis								La contra de la co	

図 12-43 ARP Inspection Statistics 画面

#### 画面に表示される項目:

項目	説明
VID List	設定する VLAN ID リストを入力します。

「Clear by VLAN」ボタンをクリックし、入力した VLAN ID についての情報を消去します。

「Clear All」ボタンをクリックし、テーブルのすべての情報を消去します。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

#### ARP Inspection Log (ARP インスペクションログ)

ARP インスペクションログ情報の表示、消去、設定を行います。

Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Log の順にクリックして、以下の画面を表示します。

ARP Inspection Log				
ARP Inspection Log				
Log Buffer (1-1024)	32			Apply Clear Log
Total Entries: 0				
Port	VLAN	Sender IP	Sender MAC	Occurrence

図 12-44 ARP Inspection Log 画面

画面に表示される項目:

項目	説明
Log Buffer	使用するログバッファの値を入力します。1 から 1024 の間で指定可能です。初期値は 32 です。
「Apply」ボタンを	

「Clear Log」ボタンをクリックし、ログを消去します。

### IP Source Guard(IP ソースガード)

IP ソースガードを使用する場合は、必ず、有効にするポートに所属しているすべての VLAN が"DHCP Snooping VLAN Settings"のページ で有効に設定している必要があります。

### IP Source Guard Port Settings (IP ソースガードポート設定)

IP ソースガード(IPSG)の表示、設定を行います。

Security > IMPB > IPv4 > IP Source Guard > IP Source Guard Port Settings の順にクリックして、以下の画面を表示します。

IP Source Guard Port Settings			
Unit 1  From Port eth1/0/1 State Enabled	To Port Validation	eth1/0/1	Арріу
Port		Validation Type	
eth1/0/10		ip	

図 12-45 IP Source Guard Port Settings 画面

#### 画面に表示される項目:

項目	説明
Unit	設定するユニットを指定します。
From Port/	ポートの範囲を指定します。
To Port	
State	指定ポートの IP ソースガードを「Enabled」(有効)/「Disabled」(無効)に設定します。
Validation	検証方法について選択します。「IP」「IP-MAC」から選択します。「IP」を選択すると受信パケットの IP アドレスがチェックされます。
	「IP-MAC」を選択すると受信パケットの IP アドレスと MAC アドレスがチェックされます。

「Apply」ボタンをクリックし、設定内容を適用してください。

#### ■ IP Source Guard VLAN Settings(IP ソースガード VLAN 設定)

IP ソースガード VLAN (IPSG VLAN)の表示、設定を行います。

Security > IMPB > IPv4 > IP Source Guard > IP Source Guard VLAN Settings の順にクリックして、以下の画面を表示します。

IP Source Guard VLAN S	iettings
VID List	1, 4-6
State	Enabled
Validation	IP Y Apply
Total Entries: 1	
VID	Validation Type
2	ip
	1/1  < < 1 > >  Go

図 12-46 IP Source Guard VLAN Settings 画面

#### 画面に表示される項目:

項目	
VID List	VLAN ID を指定します。
State	指定ポートの IP ソースガードを「Enabled」(有効)/「Disabled」(無効)に設定します。
Validation	検証方法について選択します。「IP」「IP-MAC」から選択します。「IP」を選択すると受信パケットの IP アドレスがチェックされます。 「IP-MAC」を選択すると受信パケットの IP アドレスと MAC アドレスがチェックされます。

「Apply」ボタンをクリックし、設定内容を適用してください。

注意

#### ■ IP Source Guard Binding (IP ソースガードバインディング)

IP ソースガードバインディングの表示、設定を行います。

Security > IMPB > IPv4 > IP Source Guard > IP Source Guard Binding の順にクリックして、以下の画面を表示します。

IP Source Guard	Binding			_	_		
IP Source Binding Se	ttings						
MAC Address VID (1-4094) IP Address Unit Erom Port	00-84-57-00-00		To Port	ath 1/0/1			Apply
FIGHTOIL	euritori		TOPOR	eurion	<b></b>		Арріу
- IP Source Binding En	try						
Unit	1	$\checkmark$					
From Port	eth1/0/1	$\checkmark$		To Port	eth1/0	)/1 🔽	
IP Address	1			MAC Address	00-84-5	57-00-00-00	
VID (1-4094)				Туре	All	~	Find
Total Entries: 1							
MAC A	ddress	IP Address	Lease (sec)	Туре	VLAN	Port	
00-11-22-	33-44-55	10.90.90.233	infinite	Static	1	eth1/0/10	Delete
						1/1  <	< 1 > > Go

図 12-47 IP Source Guard Binding 画面

画面に表示される項目:

項目	説明
	IP Source Binding Settings
MAC Address	バインディングエントリの MAC アドレスを入力します。
VID	バインディングエントリの VLAN ID を入力します。
IP Address	バインディングエントリの IP アドレスを入力します。
Unit	設定するユニットを指定します。
From Port/	ポートの範囲を指定します。
To Port	

「Apply」ボタンをクリックし、設定内容を適用してください。

	IP Source Binding Entry
Unit	このクエリで設定するユニットを指定します。
From Port/	このクエリでポートの範囲を指定します。
To Port	
IP Address	バインディングエントリの IP アドレスを入力します。
MAC Address	バインディングエントリの MAC アドレスを入力します。
VID	バインディングエントリの VLAN ID を入力します。
Туре	バインディングエントリの種類を選択します。「All」「DHCP Snooping」「Static」から選択します。「All」を選択するとすべての DHCP バインディングエントリが表示されます。「DHCP Snooping」を選択すると、DHCP バインディングスヌーピングに習得さ れた IP ソースガードバインディングが表示されます。「Static」を選択すると手動で設定した IP ソースガードバインディングが表示されます。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

「Delete」をクリックして指定エントリを削除します。

「Find」をクリックして入力した情報を元に指定のエントリを表示します。

#### IP Source Guard HW Entry (IP ソースガードハードウェアエントリ)

IP ソースガードハードウェアエントリの表示を行います。

Security > IMPB > IPv4 > IP Source Guard > IP Source Guard HW Entry の順にクリックして、以下の画面を表示します。

it 1	From Port	eth1/0/1 💌	To Port eth1/0/1		Find
otal Entries: 1					
and a standard and a standard a st					
Port	Filter-type	Filter-mode	IP Address	MAC Address	VLAN
Port eth1/0/10	Filter-type ip	Filter-mode Active	IP Address 10.90.90.254	MAC Address	VLAN 1

図 12-48 IP Source Guard HW Entry 画面

#### 画面に表示される項目:

項目	説明
Unit	このクエリで使用するユニットを指定します。
From Port/	このクエリでポートの範囲を指定します。
To Port	

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。 「Find」をクリックして入力した情報を元に指定のエントリを表示します。

#### Advanced Settings (アドバンス設定)

IP-MAC-Port Binding Settings (IP-MAC ポートバインディング設定) IP-MAC ポートバインディングの設定、表示を行います。

Security > IMPB > IPv4 > Advanced Settings > IP-MAC-Port Binding Settings の順にクリックして、以下の画面を表示します。

IP-MAC-Port Binding Settin	ngs			
IP-MAC-Port Binding Trap Setting				
Trap State	Enabled	Oisabled		Apply
IP-MAC-Port Binding Port Settings	0			
Unit 1 From Port etb1/0/1		To Port eth1/0/1		
Mode Disabled		Currort		<u> </u>
				Apply
	Port	_	Mode	Apply
	Port eth1/0/1	_	Mode Disabled	Apply
	Port eth1/0/1 eth1/0/2	_	Mode Disabled Disabled	Apply
	Port eth1/0/1 eth1/0/2 eth1/0/3	_	Mode Disabled Disabled Disabled	Apply
	Port eth1/0/1 eth1/0/2 eth1/0/3 eth1/0/4	_	Mode Disabled Disabled Disabled Disabled	Apply
	Port eth1/0/1 eth1/0/2 eth1/0/3 eth1/0/4 eth1/0/5		Mode Disabled Disabled Disabled Disabled Disabled	



画面に表示される項目:

項目	説明		
IP-MAC-Port Binding Trap Settings			
Trap State	IP-MAC ポートバインディングのトラップ設定を「Enabled」(有効)/「Disabled」(無効)に指定します。		
「Apply」ボタンをクリックし、設定内容を適用してください。			
IP-MAC-Port Binding Port Settings			
Unit	設定するユニットを指定します。		
From Port/	ポートの範囲を指定します。		

To Port アクセスコントロールのモードを選択します。「Disabled」「Strict」「Loose」から選択します。ポートが「IMPB strict-mode」の アクセスコントロールを有効にしている時は、ホストは ARP/IP パケット送信後にそれらの ARP/IP パケットがバインディング チェックを通過した後のみ、ポートヘアクセスできます。バインディングチェックを通過するには、送信元 IP アドレス、送信 元 MAC アドレス、VLAN ID、そして受領ポート番号が、IP ソースガードスタティックバインディングエントリ、または DHCP ス ヌーピングを習得したダイナミックバインディングエントリに定義されたエントリにマッチする必要があります。ポートが「IMPB loose-mode」のアクセスコントロールを有効にしている場合、ホストは ARP/IP パケット送信後にそれらの ARP/IP パケットがバ インディングチェックを通過せず、ポートへのアクセスを拒否されます。バインディングチェックを通過するには、送信元 IP ア ドレス、送信元 MAC アドレス、VLAN ID、そして受領ポート番号が、IP ソースガードスタティックバインディングエントリ、ま たは DHCP スヌーピングを習得したダイナミックバインディングエントリに定義されたエントリにマッチする必要があります。

設定後、「Apply」ボタンをクリックして設定を有効にします。

Mode

#### ■ IP-MAC-Port Binding Blocked Entry (IP-MAC ポートバインディングブロックエントリ)

IP-MAC ポートバインディングブロックエントリの表示、消去を行います。

Security > IMPB > IPv4 > Advanced Settings > IP-MAC-Port Binding Blocked Entry の順にクリックして、以下の画面を表示します。

MAC-Port Binding Blo	cked Entry		
lear  by Port Unit  F	rom Port eth 1/0/1	To Port eth 1/0/1 💟 🔿 by MAC	Clear All Apply
otal Entries: 0			

図 12-50 IP-MAC-Port Binding Blocked Entry 画面

#### 画面に表示される項目:

項目	説明
Clear by Port	選択ポートに基づいたエントリテーブルをクリアにします。
Unit	設定するユニットを指定します。
From Port/	ポートの範囲を指定します。
To Port	
Clear by MAC	MAC アドレスを含むエントリを消去します。項目欄にクリアされる MAC アドレスを入力します。
Clear All	MAC アドレスを含むすべてのエントリを消去します。
	ギカンをカリッカーで記字をちかにします

設定後、「Apply」ボタンをクリックして設定を有効にします。

## IPv6

#### IPv6 Snooping (IPv6 スヌーピング)

IPv6 スヌーピングについて表示、設定します。

Security > IMPB > IPv6 > IPv6 Snooping の順にクリックして、以下の画面を表示します。

#### ■ IPv6 Snooping Policy Settings タブ

IPv6 Snooping				
IPv6 Snooping Policy Settings Station Move Setting	IPv6 Snooping DHCP Entry Settings	IPv6 Snooping NDP Entry Settings	IPv6 Snooping DHCP-PD Entry Settings	
Station Move Permit v	]			Apply
IPv6 Snooping Policy Settings				
Policy Name Limit Address Count (0-1024) Protocol Data Glean	32 chars	No Limit CP-PD DHCP-PD-EXT		
VID List	1, 4-6			Apply
Total Entries: 0	rotocol Data Glean	Limit Address Count	Target VI AN	
Snooping Policy P	rotocol Data Glean	Limit Address Count	Target VLAN	

図 12-51 IPv6 Snooping - IPv6 Snooping Policy Settings タブ画面

画面に表示される項目:

項目	説明
	Station Move Setting
Station Move	ステーション動作について設定します。「Permit」「Deny」から指定します。
	をクリックト 設定内容を適用してください

「Apply」ボタンをクリックし、設定内容を適用してください。

	IPv6 Snooping Policy Settings
Policy Name	IPv6 スヌーピングポリシー名を入力します。32 文字内で指定可能です。
Limit Address	アドレスカウント制限の値を指定します。0 から 1024 まで指定可能です。
Count	「No Limit」を指定するとアドレスカウント制限は無効になります。

項目	説明
Protocol	本ポリシーに対応するプロトコルを以下から選択します。 「DHCP」「NDP」「DHCP-PD」「DHCP-PD-EXT」
	DHCPv6 スヌーピングはアドレス割り当ての段階での DHCPv6 クライアントとサーバ間の DHCPv6 パケットを傍受します。 DHCPv6 クライアントが有効な IPv6 アドレスを取得すると、DHCPv6 スヌーピングはバインディングデータベースを作成します。 ND スヌーピングはステートレスな自動設定 IPv6 アドレスと手動設定 IPv6 アドレスのための機能です。IPv6 アドレスをアサイン する前に、ホストは「Duplicate Address Detection」(DAD) を実行する必要があります。ND スヌーピングは DAD メッセージ (DAD NS と DAD NA) を受信しバインディングデータベースを構築します。NDP パケット (NS と NA) もまたホストが到達可能かを判 断しバインディングを削除するかどうかを決定するために使用されます。
Data Glean	Data-Glean 機能を「Enabled」(有効)/「Disabled」(無効)にします。 ある状況下(DAD-NS パケットの喪失やスイッチの再起動)においては有効な IPv6 アドレスがバインディングテーブルで検出で きず、それらのデバイス向け / からのトラフィックが IPv6 ソースガードで拒否されます。Data-Glean 機能により IPv6 Duplicate Address Detection (DAD) を使用して紛失した IPv6 アドレスを回復する手段を提供します。
VID List	使用する VLAN ID リストを入力します。

設定後、「Apply」ボタンをクリックして設定を有効にします。 「Delete」をクリックして指定エントリを削除します。 「Edit」をクリックして指定エントリを編集します。

#### ■ IPv6 Snooping DHCP Entry Settings タブ

IPv6 Snooping					
IPv6 Snooping Policy Settings IPv6 Snooping DHCP Entry Settings IPv6 Snooping NDP Entry Settings IPv6 Snooping DHCP-PD Entry Settings					
Unit From Port To 1 V eth1/0/1 V e	o Port Binding Max Entries (0-1	024) ☑ No Limit	Apply		
Port	Protocol	Max Entries			
eth1/0/1	DHCP	1024	Clear		
eth1/0/2	DHCP	1024	Clear		

図 12-52 IPv6 Snooping - IPv6 Snooping DHCP Entry Settings タブ画面

#### 画面に表示される項目:

項目	説明
Unit	ユニットを選択します。
From Port/	ポートの範囲を指定します。
To Port	
Binding Max	ここで許可される IPv6 スヌーピングバインディングエントリの最大数を入力します。
Entries	設定可能範囲:0-1024
	ゴムンをクリックトブ設定を方効にします

設定後、「Apply」ボタンをクリックして設定を有効にします。 「Clear」をクリックすると、ポートの DHCP スヌーピングエントリがクリアされます。

#### ■ IPv6 Snooping NDP Entry Settings タブ

IPv6 Snooping					
IPv6 Snooping Policy Settings IPv6 Snooping DHCP Entry Settings IPv6 Snooping NDP Entry Settings IPv6 Snooping DHCP-PD Entry Settings					
Unit         From Port         To Port         Binding Max Entries (0-1024)           1         eth1/0/1         eth1/0/1         Image: Weight of the second			Apply		
Port	Protocol	Max Entries			
eth1/0/1	NDP	1024	Clear		
eth1/0/2	NDP	1024	Clear		

図 12-53 IPv6 Snooping - IPv6 Snooping NDP Entry Settings タブ画面

#### 画面に表示される項目:

項目	説明
Unit	ユニットを選択します。
From Port/	ポートの範囲を指定します。
To Port	
Binding Max	ここで許可される IPv6 スヌーピングバインディングエントリの最大数を入力します。
Entries	設定可能範囲:0-1024

設定後、「Apply」ボタンをクリックして設定を有効にします。

「Clear」をクリックすると、ポートのNDスヌーピングエントリがクリアされます。

#### ■ IPv6 Snooping DHCP-PD Entry Settings タブ

IPv6 Snooping							
IPv6 Snooping Policy Settings IPv6 Snoop	ping DHCP Entry Settings IPv6 Snooping NE	P Entry Settings IPv6 Snooping DHCP-PD En	try Settings				
Unit From Port T	o Port Binding Max Entries (0-	1024)					
1 V eth1/0/1 V	eth1/0/1 🔽	No Limit	Apply				
Port	Protocol	Max Entries					
eth1/0/1	DHCP-PD	1024	Clear				
eth1/0/2	DHCP-PD	1024	Clear				
eth1/0/3	DHCP-PD	1024	Clear				

図 12-54 IPv6 Snooping - IPv6 Snooping DHCP-PD Entry Settings タブ画面

#### 画面に表示される項目:

項目	説明
Unit	ユニットを選択します。
From Port/	ポートの範囲を指定します。
To Port	
Binding Max	ここで許可される IPv6 スヌーピングバインディングエントリの最大数を入力します。
Entries	設定可能範囲:0-1024
。 設定後、「Apply」	ボタンをクリックして設定を有効にします。

「Clear」をクリックすると、ポートの DHCP PD スヌーピングエントリがクリアされます。

#### IPv6 ND Inspection (IPv6 ND インスペクション)

IPv6 ND インスペクションについて表示、設定します。

## Security > IMPB > IPv6 > IPv6 ND Inspection の順にクリックして、以下の画面を表示します。

IPv6 ND Inspection				
IPv6 ND Inspection				
Policy Name	32 chars			
Device Role	Host 🗸			
Mode	Precise 🗸			
Validate Source-MAC	Disabled 🔽			
Target Port	From Port eth1/0/1 💟	To Port	eth1/0/1 🔽	Apply
Total Entries: 0				
Policy Name	Device Role	Mode	Validate Source-MAC	Target Port

図 12-55 IPv6 ND Inspection 画面

#### 画面に表示される項目:

項目	説明
Policy Name	ポリシー名を入力します。32 文字内で指定可能です。
Device Role	デバイスロールを「Host」「Router」から選択します。
	・ Host - NS、NA メッセージのインスペクションは動作します。(初期値)
	・ Router - NS、NA のインスペクションは動作しません。NS/NA インスペクションを動作させるときは、DHCP もしくは ND プ
	ロトコルから学習したダイナミックバインディングテーブルに対しての妥当性の確認が必要です。
Mode	モードを以下から選択します。
	• Precise - NDインスペクションは、ターゲットアドレスがDANA/NA パケットのソースアドレスと同一であるかどうかをチェッ
	クします。
	・ Fuzzy - ND インスペクションは、ターゲットアドレスとソースアドレスの両方がバインディングテーブルに存在するかどう
	かをチェックします。
Validate Source-	送信 MAC アドレスオプションの妥当性確認を「Enabled」(有効)/「Disabled」(無効)にします。
MAC	リンクレイヤアドレスを含む ND メッセージを受信した時に、リンクレイヤアドレスに対する送信元 MAC アドレスを確認します。
	リンクレイヤアドレスと MAC アドレスが違う場合、パケットは破棄されます。
Target Port	チェックを入れターゲットポートを指定します。
Unit	設定するユニットを指定します。
From Port/	ポートの範囲を指定します。
To Port	
	ギタンをクリックレブジウをちかにします

設定後、「Apply」ボタンをクリックして設定を有効にします。

「Delete」をクリックして指定エントリを削除します。

「Edit」をクリックして指定エントリを編集します。

## IPv6 RA Guard (IPv6 RA ガード)

IPv6 RA ガードについて表示、設定します。

Security > IMPB > IPv6 > IPv6 RA Guard の順にクリックして、以下の画面を表示します。

v6 RA Guard	_				
Pv6 RA Guard					
Policy Name		32 chars			
Device Role		Host			
Match IPv6 Access List		Please Select			
Target Port	Unit	I          From Port         eth1/0/1	To Port	eth1/0/1 💟	Apply
otal Entries: 1					
Policy Name	Device Role	Match IPv6 Access List	Target Port		
policy	Host	S-IPv6-ACL	eth1/0/12	Edit	Delete

図 12-56 IPv6 RA Guard 画面

国面に表示される項目:					
説明					
ポリシー名を入力します。32 文字内で指定可能です。					
デバイスロールを「Host」「Router」から選択します。					
・ Host - RA パケットはすべてブロックされます。(初期値)					
・ Router - を選択した場合、RA パケットはポート宛ての ACL に従い転送されます。					
マッチさせる IPv6 アクセスリストを入力、選択します。					
チェックを入れターゲットポートを指定します。					
設定するユニットを指定します。					
ポートの範囲を指定します。					

設定後、「Apply」ボタンをクリックして設定を有効にします。 「Delete」をクリックして指定エントリを削除します。 「Edit」をクリックして指定エントリを編集します。

「Please Select」をクリックすると次の画面が表示されます。

	ID	ACL Name	ACL Type
0	11000	S-IPv6-ACL	Standard IPv6 ACL
•	13000	E-IPv6-ACL	Extended IPv6 ACL

図 12-57 IPv6 RA Guard (Please Select) 画面

設定するエントリを選択し「OK」をクリックします。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

#### IPv6 DHCP Guard (IPv6 DHCP ガード)

IPv6 DHCP ガードについて表示、設定します。

#### Security > IMPB > IPv6 > IPv6 DHCP Guard の順にクリックして、以下の画面を表示します。

Pv6 DHCP Guard	_		_	_	_
IPv6 DHCP Guard					
Policy Name Device Role Match IPv6 Access List Target Port	32 Cli Unit 1	chars ient Please Select From Port eth1/0/1	To Port	eth1/0/1 🔽	Apply
Total Entries: 1					
Policy Name	Device Role	Match IPv6 Access List	Target Port		
policy	Client	S-IPv6-ACL	eth1/0/14	Edit	Delete

図 12-58 IPv6 DHCP Guard 画面

画面に表示される項目:

<i>、</i> ます。
-

設定後、「Apply」ボタンをクリックして設定を有効にします。

「Delete」をクリックして指定エントリを削除します。 「Edit」をクリックして指定エントリを編集します。

and Market Managements

「Please Select」をクリックすると次の画面が表示されます。

	ID	ACL Name	ACL Type
0	11000	S-IPv6-ACL	Standard IPv6 ACL
•	13000	E-IPv6-ACL	Extended IPv6 ACL
			1/1 < 1 > >

図 12-59 IPv6 Guard (Please Select) 画面

設定するエントリを選択し「OK」をクリックします。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

## IPv6 Source Guard (IPv6 ソースガード)

#### ■ IPv6 Source Guard Settings(IPv6 ソースガード設定)

IPv6 ソースガードの表示、設定を行います。

Security > IMPB > IPv6 > IPv6 Source Guard > IPv6 Source Guard Settings の順にクリックして、以下の画面を表示します。

IPv6 Source Gu	ard Settings					
- IPv6 Source Guard	Policy Settings					
Policy Name	32 chars	Global Auto-Confi	gure Address Pern	nit 🔽		
Validate Address	Enabled 🔽	Validate Prefix	Disa	bled 🔽		
Link Local Traffic	Deny 💙					Apply
Total Entries: 1						
Policy Name	Global Auto-Configure Address	Link Local Traffic	Validate Address	Validate Prefix	Target Port VID	
Policy	Permit	Deny	Enabled	Disabled	eth1/0/10 1	Edit Delete
IPv6 Source Guard Policy Name	Attach Policy Settings 32 chars					
VID List	1, 4-6					
Target Port	Unit 1	From Port	eth1/0/1 🔽	To Port	eth1/0/1 🔽	Apply
						Detele All
Policy Name	e		Target Port			
Policy			eth1/0/10			Delete
Total Entries: 1						Detele All
Policy Name	e		VID			
Policy			1			Delete
					1/1 < <	1 > > Go

図 12-60 IPv6 Source Guard Settings 画面

#### 画面に表示される項目:

項目	説明
	IPv6 Source Guard Policy Settings
Policy Name	ポリシー名を入力します。32 文字内で指定可能です。
Global Auto- Configure Address	自動設定グローバルアドレスからのデータトラフィックの許可 / 拒否を選択します。リンクのすべてのグローバルアドレスが DHCP と送信トラフィックから設定アドレスのホストをブロックしたい管理者よってアサインされている場合、有効です。
Validate Address	Validate(認証)アドレス機能を「Enabled」(有効)/「Disabled」(無効)に指定します。 IPv6 ソースガードで認証アドレス機能を有効にします。
Validate Prefix	「validate(認証)」プリフィクス機能を「Enabled」(有効)/「Disabled」(無効)に指定します。 IPv6 ソースガードで IPv6 認証プリフィクス機能を有効に指定します。
Link Local Traffic	リンクローカルアドレスによって送信されたデータトラフィックの許可 / 拒否を選択します。
	IPv6 Source Guard Attach Policy Settings
Policy Name	ポリシー名(32 文字まで)を指定します。
VID List	ターゲット VLAN の VLAN ID を指定します。
Target Port	ターゲットポートを指定します。
Unit	設定するユニットを指定します。
From Port/ To Port	ポートの範囲を指定します。

「Apply」ボタンをクリックし、設定内容を適用してください。

「Edit」をクリックして、指定エントリの編集を行います。

「Delete」をクリックすると指定のエントリを削除します。

#### ■ IPv6 Neighbor Binding (IPv6 ネイババインディング)

IPv6 ネイババインディングの表示、設定を行います。

Security > IMPB > IPv6 > IPv6 Source Guard > IPv6 Neighbor Binding の順にクリックして、以下の画面を表示します。

IPv6 Neighbor Bin	ding		_		
IPv6 Neighbor Binding	Settings				
MAC Address VID (1-4094)	00-84-57-00-00-00				
IPv6 Address	2233::1				
Unit	1				
From Port	eth1/0/1 💌	To Port	eth1/0/1 🔽		Apply
IPv6 Neighbor Binding I	Entry				
Unit	1				
From Port	None 💌	To Port	None 🗸		
IPv6 Address	2233::1	MAC Address	00-84-57-00-00-	-00	
VID (1-4094)					Find
Total Entries: 1					
IPv6 Address	MAC Address	Port	VLAN 0	Owner Time left	
2015::1	00-11-22-33-44-55	eth1/0/15	1 5	Static N/A	Delete
				1/1	< < 1 > >  Go

図 12-61 IPv6 Neighbor Binding 画面

#### 画面に表示される項目:

VID

項目	説明
	IPv6 Neighbor Binding Settings
MAC Address	バインディングエントリの MAC アドレスを入力します。
VID	バインディングエントリの VLAN ID を入力します。1 から 4094 の間で指定します。
IPv6 Address	バインディングエントリの IPv6 アドレスを入力します。
Unit	設定するユニットを指定します。
From Port/	ポートの範囲を指定します。
To Port	
「Apply」ボタンを	をクリックし、設定内容を適用してください。
	IPv6 Neighbor Binding Entry
Unit	このクエリで設定するユニットを指定します。
From Port/	このクエリでポートの範囲を指定します。
To Port	
IPv6 Address	バインディングエントリの IPv6 アドレスを入力します。

「Delete」をクリックして指定エントリを削除します。

「Find」をクリックして入力した情報を元に指定のエントリを表示します。

表示する VLAN ID を入力します。

MAC Address バインディングエントリの MAC アドレスを入力します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

# DHCP Server Screening (DHCP サーバスクリーニング設定)

DHCP サーバスクリーニングは不正な DHCP サーバへのアクセスを拒否する機能です。この DHCP サーバフィルタ機能が有効になると指定ポートからのすべての DHCP サーバパケットはフィルタされます。

## DHCP Server Screening Global Settings (DHCP サーバスクリーニンググローバル設定)

DHCP サーバスクリーニンググローバル設定の表示、設定をします。

#### Security > DHCP Server Screening > DHCP Server Screening Global Settings の順にメニューをクリックして画面を表示します。

DHCP Server Screening	Global Settings			
Trap Settings				
Trap State	Disabled			Apply
Profile Settings				
Profile Name	32 chars			Create
Total Entries: 1				
Profile Name	Client MAC	Bind Client MAC		
Policy		Binding	Delete	Delete Profile
Log Information				
Log Buffer Entries (10-1024)	32			Apply Clear Log
Total Entries: 0				
VLAN	Server	P	Client MAC	Occurrence

図 12-62 DHCP Server Screening Global Settings 画面

画面に表示される項目:

項目	説明
	Trap Settings
Trap State	DHCP サーバスクリーニングトラップ機能を「Enabled」(有効)/「Disabled」(無効)にします。
「Apply」ボタンをクリックし	、設定内容を適用してください。
	Profile Settings
Profile Name	プロファイル名を入力します。32 文字内で指定可能です。
「Create」ボタンをクリックし	、設定内容にて作成します。
「Delete」をクリックして指定	ミエントリを削除します。
「Delete Profile」をクリックし	て指定プロファイルを削除します。
	Log Information
Log Buffer Entries	ログバッファエントリ数を入力します。10から 1024 までで指定します。初期値は 32 です。
設定後、「Apply」ボタンをクリ	ノックして設定を有効にします。

「Clear Log」ボタンをクリックしてログを消去します。

「Binding」ボタンをクリックすると以下の画面が表示されます。

Bind Client MAC		
Profile Name Client MAC	Policy 00-84-57-00-00-00	Apply

図 12-63 DHCP Server Screening Global Settings (Binding Client) 画面

画面に表示される項目:

項目	説明
Client MAC	使用する MAC アドレスを指定します。
- 翌定後 「Apply」ボタンをクレ	

設定後、「Apply」ボタンをクリックして設定を有効にします。

## DHCP Server Screening Port Settings (DHCP サーバスクリーニングポート設定)

DHCP サーバスクリーニングポートの表示、設定を行います。

Security > DHCP Server Screening > DHCP Server Screening Port Settings の順にクリックし、画面を表示します。

DHCP Serve	r Screening Por	rt Settings			
DHCP Server Serv	creening Port Setting	]5			
From Port	To Port	State	Server IP	Profile Name	
eth1/0/1 🔽	eth1/0/1	Disabled 🗸		32 chars	Apply
Port	State	Server IP		Profile Name	
eth1/0/1	Disabled	-		-	Delete
eth1/0/2	Disabled	-		-	Delete
eth1/0/3	Disabled	-		-	Delete
eth1/0/4	Disabled	-		-	Delete
eth1/0/5	Disabled	-		-	Delete
eth1/0/6	Disabled	-		-	Delete
eth1/0/7	Disabled	-		-	Delete
eth1/0/8	Disabled	-		-	Delete
eth1/0/9	Disabled	-		-	Delete
eth1/0/10	Disabled	-		-	Delete
eth1/0/11	Disabled	-		-	Delete
eth1/0/12	Disabled	-		-	Delete
eth1/0/13	Disabled	-		-	Delete
eth1/0/14	Disabled	-		-	Delete
eth1/0/15	Disabled	-		-	Delete
eth1/0/16	Disabled	-		-	Delete
eth1/0/17	Disabled	-		-	Delete

図 12-64 DHCP Server Screening Port Settings 画面

#### 画面に表示される項目:

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	ポートの範囲を指定します。
State	指定ポートでの DHCP サーバスクリーニング機能を「Enabled」(有効)/「Disabled」(無効)にします。
Server IP	DHCP サーバの IP アドレスを入力します。
Profile Name	ポートに設定する DHCP サーバスクリーニングプロファイル名を入力します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。 「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。

## ARP Spoofing Prevention (ARP スプーフィング防止設定)

ユーザは保護されたゲートウェイに対し、MACのスプーフィングを防ぐためにスプーフィング防止を設定することができます。エントリーが作成 された場合に、送信先 ARP パケットはエントリのゲートウェイ IP にマッチしているが、送信先 MAC フィールドもしくは送信元 MAC フィールドの どちらかがエントリのゲートウェイ MAC と合致しない場合はシステムにより破棄されます。

ARP スプーフィング防止機能は、設定したゲートウェイ IP アドレスとマッチしなかった IP アドレスの ARP パケットをバイパスします。もし ARP アドレスが設定したゲートウェイの IP アドレス、MAC アドレスそしてポートリストなどとマッチする場合、受信ポートが ARP トラストかどうかは関係なく Dynamic ARP Inspection (DAI) チェックをバイパスします。

Security > ARP Spoofing Prevention の順にメニューをクリックし、以下の画面を表示します。

ARP Spoofing Prevention				
ARP Spoofing Prevention Logging St ARP Spoofing Prevention Logging Sta	tate OEnabled	Disabled		Apply
ARP Spoofing Prevention Unit From Port Gateway IP	<ul><li>✓</li><li>✓</li><li>✓</li></ul>	To Port Gateway MAC	eth1/0/1	Apply
Total Entries: 1				
Gateway IP	Gateway	MAC	Port	
10.90.90.1	00-11-22-33	-44-55	eth1/0/10	Delete

図 12-65 ARP Spoofing Prevention 画面

画面に表示される項目:

項目	説明
	ARP Spoofing Prevention Logging State
ARP Spoofing Prevention Logging State	ARP スプーフィング防止ロギング状態を「Enabled」(有効)/「Disabled」(無効)に指定します。
	ARP Spoofing Prevention
Unit	設定するユニットを指定します。
From Port / To Port	ポートの範囲を指定します。
Gateway IP	ゲートウェイの IP アドレスを入力します。
Gateway MAC	ゲートウェイの MAC アドレスを入力します。

\_\_\_\_\_\_ 「Apply」ボタンをクリックし、変更を有効にします。

「Delete」ボタンをクリックして、指定エントリを削除します。

## BPDU Attack Protection (BPDU アタック防止設定)

スイッチのポートに BPDU 防止機能を設定します。通常、BPDU 防止機能には 2 つの状態があります。1 つは正常な状態で、もう1 つはアタック状態です。 アタック状態には、3 つのモード(破棄、ブロックおよびシャットダウン)があります。BPDU 防止が有効なポートは、STP BPDU パケットを受信す るとアタック状態に入ります。そして、設定に基づいてアクションを行います。このように、BPDU 防止は STP が無効なポートにだけ有効にするこ とができます。BPDU 防止では、「STP Port Settings」 画面の「Forward BPDU」に設定したものより高い優先度を持っています。つまり、ポートが「STP Port Settings」 画面の「Forward BPDU」に設定されており、BPDU 防止が有効であると、ポートは STP BPDU を転送しません。

BPDU 防止では、BPDU の処理を決定するために設定した BPDU トンネルポートより高い優先度を持っています。つまり、ポートが「Tunnel STP Port(s)」で BPDU トンネルポートとして設定されていると、ポートは STP BPDU を転送します。しかし、ポートで BPDU 防止が有効であると、ポートは STP BPDU を転送しません。

Security > BPDU Attack Protection の順にメニューをクリックし、以下の画面を表示します。

BPDU Attack Protection	_				
BPDU Attack Protection Global Setting	js				
BPDU Attack Protection State BPDU Attack Protection Trap State	<ul> <li>Enabled</li> <li>Enabled</li> </ul>	<ul><li>Disabled</li><li>Disabled</li></ul>			Apply
BPDU Attack Protection Port Settings					
Unit From Por	t	To Port	State	Mode	
1 eth1/0/		eth1/0/1	Enabled	Shutdown	Apply
Unit 1 Settings		eth1/0/1	Enabled	Shutdown	Apply
1 eth1/0/ Unit 1 Settings Port eth1/0/1		eth1/0/1 State	Enabled [	Shutdown	Status Normal
1 eth1/0/ Unit 1 Settings Port eth1/0/1 eth1/0/2		eth1/0/1 State Disabled Disabled	Enabled [	Aode utdown utdown	Status Normal Normal
1 vit 1 Settings Port eth1/0/1 eth1/0/2 eth1/0/3		eth1/0/1 State Disabled Disabled Disabled	Enabled Sh Sh Sh Sh	Aode utdown utdown utdown utdown	Status Normal Normal Normal
1 vit 1 Settings Port eth1/0/1 eth1/0/2 eth1/0/3 eth1/0/4		eth1/0/1 State Disabled Disabled Disabled Disabled Disabled	Enabled Sh Sh Sh Sh Sh Sh	Aode utdown utdown utdown utdown utdown utdown utdown	Status Normal Normal Normal Normal Normal
1 vit 1 Settings Port eth1/0/1 eth1/0/2 eth1/0/3 eth1/0/4 eth1/0/5		eth1/0/1 State Disabled Disabled Disabled Disabled Disabled Disabled Disabled	Enabled Sh Sh Sh Sh Sh Sh Sh	Aode utdown utdo	Apply     Apply     Status     Normal     Normal     Normal     Normal     Normal     Normal     Normal

図 12-66 BPDU Attack Protection 画面

#### 画面に表示される項目:

項目	説明		
BPDU Attack Protection State	BPDU アタック防止機能を有効または無効にします。初期値は無効です。		
BPDU Attack Protection Trap	トラップの状態を「Enabled」(有効)/「Disabled」(無効)にします。		
State			
Unit	設定するユニットを選択します。		
From Port / To Port	設定を使用するポート範囲を選択します。		
State	指定ポートに対してモードを有効または無効にします。		
Mode	BPDU防止モードを指定します。		
	・ Drop - ポートがアタック状態に入るとすべての受信 BPDU パケットを破棄します。		
	・ Block - ポートがアタック状態に入るとすべてのパケット(BPDU と正常なパケットを含む)を破棄します。		
	・ Shutdown - ポートがアタック状態に入るとポートをシャットダウンします。		

「Apply」ボタンをクリックし、変更を有効にします。

# NetBIOS Filtering (NetBIOS フィルタリング設定)

本項目では NetBIOS フィルタリングの設定、表示を行います。

Security > NetBIOS Filtering の順にメニューをクリックし、以下の画面を表示します。

NetBIOS Filtering		
NetBIOS Filtering		
Unit	From Port To Port	NetBIOS Filtering State Extensive NetBIOS Filtering State
1 🗸	eth1/0/1 🗸 eth1/0/1	Disabled         Disabled         Apply
Port	NetBIOS Filtering Stat	e Extensive NetBIOS Filtering State
eth1/0/1	Disabled	Disabled
eth1/0/2	Disabled	Disabled
eth1/0/3	Disabled	Disabled
eth1/0/4	Disabled	Disabled
eth1/0/5	Disabled	Disabled
eth1/0/6	Disabled	Disabled
eth1/0/7	Disabled	Disabled
eth1/0/8	Disabled	Disabled

図 12-67 NetBIOS Filtering 画面

画面に表示される項目:

項目	説明
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。
NetBIOS Filtering State	指定ポートでの NetBIOS フィルタリングを「Enabled」(有効)/「Disabled」(無効)に指定します。 これにより物理ポートでの NetBIOS パケットが許可 / 拒否されます。
Extensive NetBIOS Filtering	指定ポートでの Extensive NetBIOS フィルタリングを「Enabled」(有効)/「Disabled」(無効)に指定します。
State	これにより物理ポートでの NetBIOS パケット over 802.3 フレームが許可 / 拒否されます。
「Apply」ボタンをクリック」。	変更を有効にします。

Apply」ホタンをクリックし、変更を有効にします。

## MAC Authentication (MAC 認証)

MAC 認証機能は、MAC アドレスにてネットワークの認証を設定する方法です。

スイッチはローカル認証方式、RADIUS サーバ認証方式のどちらもサポートされています。MAC アドレス認証では MAC アドレス情報がローカルまたは RADIUS サーバに認証権限用にデータベース化されます。

Security > MAC Authentication の順にメニューをクリックし、以下の画面を表示します。

MAC Authentication				
MAC Authentication Global Settin	igs			
MAC Authentication State	<ul> <li>Enabled</li> <li>Enabled</li> </ul>	Disabled		
MAC Authentication Trap State	<ul> <li>Enabled</li> <li>Enabled</li> </ul>	Disabled		Apply
MAC Authentication User Name a	nd Password Settings			
User Name 16 chars	Default	Password 16 chars	Encrypt 🗹 Default	Apply
MAC Authentication Port Settings	3			
Unit	From Port	To Port	State	
1 💌	eth1/0/1	eth1/0/1	Disabled	Apply
	Port		State	
	eth1/0/1		Disabled	
	eth1/0/2		Disabled	
	eth1/0/3		Disabled	
eth1/0/4			Disabled	
eth1/0/5			Disabled	
eth1/0/6				

図 12-68 MAC Authentication 画面

画面に表示される項目:

項目	説明			
	MAC Authentication Global Settings			
MAC Authentication State	「Enabled」(有効)または「Disabled」(無効)を選択し、スイッチの MAC 認証をグローバルに設定します。] 初期値 :「Disabled」			
MAC Authentication Trap	MAC 認証のトラップのステータスを「Enabled」(有効)/「Disabled」(無効)にします。			
State				
「Apply」ボタンをクリック	「Apply」ボタンをクリックし、設定内容を適用してください。			
MAC Authentication User Name and Password Settings				
User Name	MAC 認証のユーザ名を入力します。16 文字まで入力可能です。			
	「Default」にチェックを入れるとクライアントの MAC アドレスがユーザ名として指定されます。			
Password	MAC 認証のパスワードを入力します。「Encrypt」にチェックを入れると、パスワードを暗号化します。			
	「Default」にチェックを入れると、クライアントの MAC アドレスをパスワードとして指定します。			
「Apply」ボタンをクリック	「Apply」ボタンをクリックし、設定内容を適用してください。			

MAC Authentication Port Settings		
Unit	設定するユニットを指定します。	
From Port / To Port	ポートの範囲を指定します。	
State	MAC 認証のポート指定を「Enabled」(有効)/「Disabled」(無効)にします。	

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

注意 Guest VLAN 使用時に認証された MAC アドレスは、Guest VLAN で Log に記録されます。

## Web-based Access Control (Web 認証)

Web ベース認証のログインは、スイッチを経由してインターネットにアクセスを試みる場合に、ユーザを認証するように設計された機能で、認証 処理には HTTP/HTTPS プロトコルを使用します。Web ブラウザ経由で Web ページ (例:http://www.dlink.com)の閲覧を行う場合に、スイッチは認 証段階に進みます。スイッチは、HTTP/HTTPS パケットを検出し、このポートが未認証である場合に、ユーザ名とパスワードの画面を表示して、ユー ザに問い合わせます。認証処理を通過するまで、ユーザはインターネットにアクセスすることはできません。

スイッチは、認証サーバとなってローカルデータベースに基づく認証を行うか、または RADIUS クライアントとなってリモート RADIUS サーバと共に RADIUS プロトコルを介する認証処理を実行します。Web へのアクセスを試みることによって、クライアントユーザは WAC の認証処理を開始します。

D-LinkのWACの実行には、WAC機能が排他的に使用し、スイッチの他のモジュールに知られていない仮想 IP を使用します。実際は、スイッチの他の機能への影響を避ける場合にだけ、WAC は仮想 IP アドレスを使用してホストとの通信を行います。そのため、すべての認証要求を仮想 IP アドレスに送信し、スイッチの物理インタフェースの IP アドレスには送信しないようにする必要があります。

ホスト PC が仮想 IP 経由で WAC スイッチと通信する場合、仮想 IP は、スイッチの物理的な IPIF(IP インタフェース) アドレスに変換されて通信を可 能にします。ホスト PC と他のサーバの IP 構成は WAC の仮想 IP に依存しません。仮想 IP は、ICMP パケットまたは ARP リクエストに応答しません。 つまり、仮想 IP は、スイッチの IPIF(IP インタフェース) と同じサブネット、またはホスト PC のサブネットと同じサブネットには設定することはで きません。

仮想 IP が他のサーバや PC と同じ場合、WAC が有効なポートに接続するホストは、IP アドレスを実際に所有しているサーバまたは PC とは通信ができません。ホストがサーバまたは PC にアクセスする必要がある場合、仮想 IP をサーバまたは PC の1つと同じにすることはできません。ホスト PC がプロキシを使用して Web にアクセスする場合、PC のユーザは、認証を適切に実行するために、プロキシ設定の例外として仮想 IP を加える必要があります。

スイッチの WAC の実行は、ユーザ定義のポート番号により HTTP または HTTPS プロトコルのいずれかに対して TCP ポートを設定できることを特徴 としています。HTTP か HTTPS に対するこの TCP ポートは、認証処理のために CPU にトラップされる HTTP か HTTPS パケットを識別するためやロ グインページにアクセスするために使用されます。指定しない場合、HTTP に対するポート番号の初期値は 80、HTTPS に対するポート番号の初期値 は 443 となります。プロトコルも指定されないと、プロトコルの初期値は HTTP になります。

次の図は、Web ベースのアクセスコントロールを実現させるために、認証に関わる各ノードで行われる基本の6つのステップを例示しています。



#### 条件および制限

- 1. クライアントが IP アドレス取得のために DHCP を使用している場合、認証 VLAN はクライアントが IP アドレス取得を行えるように、DHCP サー バまたは DHCP リレー機能を持つ必要があります。
- 2. アクセスプロファイル機能のように、スイッチ上に存在する機能の中には HTTP パケットをフィルタしてしまうものがあります。ターゲット VLAN にフィルタ機能の設定を行う際には、HTTP パケットがスイッチにより拒否されないように、十分に注意してください。
- 3. 認証に RADIUS サーバを使用する場合、Web 認証を有効にする前に、ターゲット VLAN を含む必要な項目を入力して RADIUS サーバの設定を行っ てください。

注意 WAC/JWAC 認証では、VLAN インタフェースが Up している必要があります。

注意 HTTPS をサポートしません。

## Web Authentication(Web 認証設定)

スイッチの Web 認証設定をに行います。

画面に表示される項目:

Security > Web-based Access Control > Web Authentication をクリックして、以下の画面から設定します。

Web Authentication				
Web Authentication				
Web Authebtication State	Enabled  Disabled			Apply
Trap State	Enabled  Disabled			
Virtual IPv4		Virtual IPv6	2013::1	
Virtual URL	128 chars	Redirection Path	128 chars	Apply

図 12-69 Web Authentication 画面

項目	説明
Web Authentication	Web 認証機能を「Enable」(有効)/「Disable」(無効)にします。
State	
Trap State	Web 認証のトラップの状態を「Enabled」(有効)/「Disabled」(無効)にします。
Virtual IPv4	仮想 IP アドレスを入力します。このアドレスは WAC にだけ使用され、スイッチの他のモジュールには知られません。 すべての Web 認証のプロセスはこの IPv4 アドレスとの連携で行われますが、しかし仮想 IP はどの ICMP パケットや ARP リクエストにも応答しません。そのため仮想 IP はスイッチやホスト PC のインタフェースと同じサブネットに設定 することはできません。でなければ Web 認証は正しく動作しません。設定した URL は仮想 IP アドレスが設定された後、 有効になります。仮想 IP アドレス取得のために DNS サーバにストアされた FQDN URL をユーザは取得します。取得し た IP アドレスは本コマンドで指定した仮想 IP アドレスと一致する必要があります。もし仮想 IPv4 アドレスが設定され ない場合、IPv4 は Web 認証を開始することができません。
Virtual IPv6	仮想 IPv6 アドレスを入力します。もし仮想 IPv6 アドレスが設定されない場合、IPv6 は Web 認証を開始することができません。
Virtual URL	仮想 URL を指定します。128 文字以内で指定できます。
Redirection Path	認証に成功し、ターゲット VLAN に割り当てられたユーザを導く Web サイトの URL を入力します。128 文字以内で指定 できます。

「Apply」ボタンをクリックし、設定を有効にします。

注意 仮想 IP アドレスを「0.0.0.」もしくはスイッチの IPIF (IP インターフェイス) と同一のサブネットに設定した場合、WAC 機能は正常に動作しません。

## WAC Port Settings(Web 認証ポート設定)

Web 認証用のユーザアカウントを登録するには、Security > Web-based Access Control > WAC Port Settings をクリックし、以下の設定用画面を表示します。

WAC Port Setting	JS				
WAC Port Settings					
Unit	From Port eth1/0/1	To Port eth1/0/1	State  Disabled		Apply
	Port			State	
eth1/0/1		Disabled			
eth1/0/2			Disabled		
eth1/0/3		Disabled			
eth1/0/4		Disabled			
eth1/0/5			Disabled		

図 12-70 WAC Port Settings 画面

画面に表示される項目:

項目	説明	
Unit	設定するユニットを選択します。	
From Port / To Port	ポート範囲を設定します。	
State		
。 設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。		

WAC Customize Page(WAC カスタマイズページ設定)

認証ページの項目をカスタマイズします。

Security > Web-based Access Control > WAC Customize Page の順にメニューをクリックし、以下の画面を表示します。

WAC Customize Page				
2.	Note: Note: Name should be las	is than 128 charáctars		
	Current Status:Un-	Authenticated		
	Authentication Login			
	User Name			
	Password			
		Enter	Clear	
	Logout From The Network			
			Logout	
	la se			
	Notification			
	J			
				Set to Default Apply

図 12-71 WAC Customize Page 画面

画面に表示される項目:

項目	説明	
Page Title	カスタムページタイトルとなるメッセージを入力します。128文字まで入力可能です。	
Login window Title	カスタムログインウィンドウタイトルを入力します。64 文字まで入力可能です。	
User Name Title	カスタムユーザ名タイトルを入力します。32 文字まで入力可能です。	
Password Title	カスタムパスワードタイトルを入力します。32 文字まで入力可能です。	
Logout window Title	カスタムログアウトウィンドウタイトルを入力します。64 文字まで入力可能です。	
Notification	通知エリアに表示させる情報を入力します。各ライン 128 文字以内で入力可能です。5 ライン入力できます。	
MAC ページの設定を行うためにけての両面の WAC 認証情報をすべて 3 カーズ「Apply」ボタンをクリック」で行った亦再た適用します		

WAC ページの設定を行うためにはこの画面の WAC 認証情報をすべて入力して「Apply」ボタンをクリックして行った変更を適用します。 「Set to Default」ボタンをクリックして、全項目を初期設定に復元します。

# Japanese Web-based Access Control (JWAC 設定)

注意 本機能は CLI でのみサポートされています。Web GUI では未サポートです。

## JWAC Global Settings (JWAC グローバル設定)

スイッチにおける JWAC(Japanese Web-based Access Control)の有効化および設定をします

Security > Japanese Web-based Access Control (JWAC) > JWAC Global Settings の順にメニューをクリックし、以下の画面を表示します。

JWAC Global Settings				
JWAC Global Settings				
JWAC State	$\bigcirc$ Enabled $\odot$ Disabled			Apply
JWAC Settings				
UDP Filtering	Enabled 🗸	Authentication Method	PAP 🔽	
Virtual IP	IPv4	IPv4 Address		
Forcible Logout	Enabled 🔽	Redirect State	Enabled 🗸	
Redirect Destination	JWAC Login Pag	Redirect Delay Time (0-10)	1se	Apply Apply
Quarantine Server Settings Timeout (5-300) 30	sec Monitor D	isabled 🗸 URL	IPv4 V	Apply
Update Server Settings				
IPv4 Network Prefix/Prefix I	Length 20.0.1.0/8	O IPv6 Network Prefix/Prefix	Length 8FFE::/64	
Port (1-65535)	•	TCP O UDP		Add
Total Entries: 0				
	Update Server IP	TCP Por	rt	UDP Port

図 12-72 JWAC Global Settings 画面

画面に表示される項目:

項目	説明			
	JWAC Global Settings			
JWAC State	JWAC 機能を「Enabled」(有効)/「Disabled」(無効)にします。			
JWAC Settings				
UDP Filtering	JWAC UDP フィルタリングを「Enabled」(有効)/「Disabled」(無効)にします。			
Authentication Method	JWAC に使用される認証方法を以下から選択します。 「MD5」「PAP」「CHAP」「MS-CHAP」「MS-CHAP-v2」			
Virtual IP	使用する仮想 IP の種類を選択します。「IPv4」「IPv6」「URL」から選択可能です。			
IPv4 Address	「IPv4」を「Virtual IP」で選択した後、項目が表示されます。仮想 IP アドレスを入力します。 Web 認証の仮想 IP は WAC にだけ使用され、スイッチの他のモジュールでは使用されません。すべての Web 認証のプロ セスはこの IPv4 アドレスとの連携で行われますが、しかし仮想 IP はどの ICMP パケットや ARP リクエストにも応答しま せん。そのため仮想 IP はスイッチのインタフェースやホスト PC と同じサブネットに設定することはできません。同じサ ブネットに設定した場合、Web 認証は正しく動作しません。設定した URL は仮想 IP アドレスが設定されている場合のみ 有効です。DNS サーバに格納されている FQDN URL を取得して仮想 IP アドレスを取得します。取得した IP アドレスは本 コマンドで指定した仮想 IP アドレスと一致する必要があります。もし仮想 IPv4 アドレスが設定されない場合、IPv4 アク セスは Web 認証を開始することができません。			
IPv6 Address	未認証ホストからの認証リクエストを受け入れるために使用する JWAC 仮想 IPv6 アドレスを入力します。 もし仮想 IPv6 アドレスが設定されない場合、IPv6 アクセスは JWAC 認証を開始することができません。			
Virtual URL	「URL」を「Virtual IP」で選択した後、使用する仮想 URL を入力します。			
Forcible Logout	JWAC Forcible Logout を「Enabled」(有効) /「Disabled」(無効) にします。「Enabled」の場合、認証ホストから JWAC スイッチに TTL=1 を持つ ping パケットはログアウトリクエストと見なされ、ホストは未認証状態に戻ります。			
Redirect State	JWAC リダイレクト機能を「Enabled」(有効)/「Disabled」(無効)にします。リダイレクトが「Enabled」な場合、すべ ての Web アクセスは検疫サーバや、スイッチの JWAC Login Page にリダイレクトされます。			

項目	説明				
Redirect Destination	リダイレクト先を「Quarantine Server」(検疫サーバ)または「JWAC Login Page」に指定します。				
	リダイレクト先に検疫サーバを指定した場合、ランダムな URL にアクセスしようとする未認証ホストは検疫サーバにリダ				
	イレクトされます。「JWAC Login Page」を選択した場合、未認証ホストはスイッチの「JWAC Login Page」にリダイレク				
	トされ認証を完了します。検疫サーバをリダイレクト先に指定する場合、JWAC 機能をグローバルに有効にする前に検疫				
	サーバの設定を完了してください。リダイレクトを無効にすると、すべての Web アクセスは JWAC ログインページや検				
	疫サーバなどを除き拒否されます。				
Redirect Delay Time (0-	未認証ホストが Quarantine Server (検疫サーバ) または JWAC Login Page にリダイレクトされる場合の遅延時間を 0-10(秒)				
10)	の間で指定します。0はリダイレクトの遅延がないことを示します。				
	Quarantine Server Settings				
Timeout (5-300)	Quarantine Server のエラータイムアウトを設定します。				
	<ul> <li>・設定可能範囲:5-300(秒)</li> </ul>				
	<ul> <li>初期値:30(秒)</li> </ul>				
Monitor	JWAC Quarantine Server モニタを「Enabled」(有効)/「Disabled」(無効)にします。				
	Quarantine Server モニタが有効な場合、JWAC スイッチは、定期的に検疫サーバが正常かどうかをチェックします。検疫サー				
	バを検出できない場合、リダイレクトオプションが有効で、リダイレクト先が検疫サーバに設定されている場合、未認証				
	のすべての HTTP アクセスが JWAC ログインページにリダイレクトされます				
URL	検疫サーバの URL(IPv4/IPv6)を指定します。				
	Update Server Settings				
IPv4 Network Prefix/	更新用サーバの IPv4 アドレス / プリフィクス長を指定します。				
Prefix Length	認証が必要なあらゆるサーバはその IP アドレスもしくはネットワークアドレスを追加する必要があります。				
	ネットワークアドレスを追加する事により、エントリは同じネットワークの複数のアップデートサーバにデータを供給す				
	ることが可能になります。複数のアップデートサーバもしくはネットワークアドレスを設定することが可能です。				
IPv6 Network Prefix/	更新用サーバの IPv6 アドレス / プリフィクス長を指定します。				
Prefix Length					
Port-(1-65535)	更新サーバが使用するポート番号を以下から選択します。				
	・ TCP - TCP ポートを使う場合に選択します。				
	・ UDP - UDP ポートを使う場合に選択します。				
設定を変更する際は、必	ず「Apply」ボタンをクリックし、設定内容を適用してください。				

「Delete」ボタンをクリックして、指定エントリを削除します。

「Add」ボタンをクリックして、入力した情報に基づいたエントリを追加します。

## JWAC Port Settings (JWAC ポート設定)

スイッチに JWAC ポート設定を行います。

Security > Japanese Web-based Access Control (JWAC) > JWAC Port Settings の順にメニューをクリックし、以下の画面を表示します。

JWAC Port Settings				
JWAC Port Settings				
From Port To I eth1/0/1 eth	Port State	Max Authenticating User (1-100) bled 100 Apply		
Port	State	Max Authenticating User		
eth1/0/1	Disabled	100		
eth1/0/2	Disabled	100		

図 12-73 JWAC Port Settings 画面

#### 画面に表示される項目:

項目	説明			
JWAC Port Settings				
From Port/To Port	JWAC ポートとして有効になるポート範囲を選択します。			
State	プルダウンメニューを使用して JWAC ポートとして設定するポートを有効にします。			
Max Authenticating	同時に各ポートに許可される認証処理を試みるユーザの最大数を指定します。			
User (0-100)	設定可能範囲:1-100			

「Apply」ボタンをクリックし、設定を有効にします。

## JWAC Customize Page Language (JWAC カスタマイズ画面言語設定)

JWAC カスタムページの言語設定を行います。

Security > Japanese Web-based Access Control (JWAC) > JWAC Customize Page Language の順にメニューをクリックし、以下の画面を表示します。

JWAC Customize Page Language	
JWAC Customize Page Language	
Customize Page Language   English  Japanese	Apply

図 12-74 JWAC Customize Page Language 画面

#### 以下の項目を使用して設定を行います。

項目	説明	
	JWAC Customize Page Language	
Customize Page	JWAC カスタマイズ画面の言語を「English」「Japanese」から選択します。	
Language		
Apply」ボタンをクリック」 設定を右効にします		

「Apply」ボタンをクリックし、設定を有効にします。

## JWAC Customized Page (JWAC 画面のカスタマイズ)

JWAC 画面の設定を行います。

Security > Japanese Web-based Access Control (JWAC) > JWAC Customize Page の順にメニューをクリックし、以下の画面を表示します。

Cun	rent Status:Un-Aut	henticated			
Authentication Login				1	
User Name					
Password					
		Enter	Clear		
Logout From The Network					
			Logout		
Notification					
Notification					
Notification				_	
Notification				-	
Notification					
Notification					

図 12-75 JWAC Customize Page 画面(English)

JWAC Customize Page Language 画面で日本語を選択した場合は以下の画面が表示されます。

JWAC Customize Page	
認識的	態:未認証
社内LAN認証ログイン	
ユーザID	
パスワード	
	Enter Clear
社内LAN認証ログアウト	
	Logout
Notification	
L	
	Set to Default Apply

図 12-76 JWAC Customize Page 画面(Japanese)

JWAC 認証情報を入力して、JWAC 画面の設定を行います。最初の欄に認証名を入力し、「Apply」ボタンをクリックします。次にユーザ名とパスワードを入力し、「Enter」ボタンをクリックします。

画面に表示される項目:

項目	説明
Page Title	カスタムページタイトルとなるメッセージを入力します。128文字まで入力可能です。
Login window Title	カスタムログインウィンドウタイトルを入力します。64 文字まで入力可能です。
User Name Title	カスタムユーザ名タイトルを入力します。32 文字まで入力可能です。
Password Title	カスタムパスワードタイトルを入力します。32 文字まで入力可能です。
Logout window Title	カスタムログアウトウィンドウタイトルを入力します。64 文字まで入力可能です。
Notification	通知エリアに表示させる情報を入力します。各ライン 128 文字以内で入力可能です。5 ライン入力できます。

WAC ページの設定を行うためにはこの画面の WAC 認証情報をすべて入力して「Apply」ボタンをクリックして行った変更を適用します。 「Set to Default」ボタンをクリックして、全項目を初期設定に復元します。

# Network Access Authentication (ネットワークアクセス認証)

Network Access Authentication(ネットワークアクセス認証)の設定を行います。

## Guest VLAN(ゲスト VLAN 設定)

ネットワークアクセス認証のゲスト VLAN の表示、設定を行います。

Security > Network Access Authentication > Guest VLAN の順にメニューをクリックし、以下の画面を表示します。

Guest VLAN		_		
Guest VLAN				
Unit	From Port eth1/0/1	To Port eth1/0/1	VID (1-4094)	Apply
Total Entries: 1				
	Port		VID	
	eth1/0/10		1	Delete
				1/1  < < 1 > >  Go

図 12-77 Guest VLAN 画面

#### 画面に表示される項目:

項目	説明	
Unit	設定するユニットを選択します。	
From Port / To Port	設定するポート範囲を指定します。	
VID	設定する VLAN ID を入力します。1 から 4094 まで指定できます。	
ーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーー		

「Delete」ボタンをクリックして、指定エントリを削除します。

#### Network Access Authentication Global Settings(ネットワークアクセス認証グローバル設定)

ネットワークアクセス認証のグローバルに設定します。

Security > Network Access Authentication > Network Access Authentication Global Settings の順にメニューをクリックし、以下の画面を表示します。

Network Access Authentication Global Settings				
Network Access Authentication MAC Format Settings				
Case	Uppercase 🗸			
Delimiter	Dot 🗸			
Delimiter Number	2			Apply
General Settings				
Max Users (1-4096)	4096			
Deny MAC-Move	Disabled			
Authorization State	Enabled			Apply
User Information				
User Name	32 chars	VID (1-4094)		
Password Type	Plain Text	Password	32 chars	Apply
Total Entries: 1				
User Name	Password	Password Type	VID	
user	*****	Plaintext	1	Delete

図 12-78 Network Access Authentication Global Settings 画面
画面に表示される項目:	
-------------	--

項目	説明
	Network Access Authentication MAC Format Settings
Case	ネットワークアクセス認証に使用する MAC アドレスの形式を「Uppercase」(大文字)または「Lowercase」(小文字)から選択します
Delimiter	MACアドレスを入力する際の区切り「Hyphen」(ハイフン) 「Colon」(コロン) またけ「Dot」(ドット)を選択します
	区切り文字を持たない場合には「None」を選択します。
Delimiter Number	MAC アドレスにおける区切り数を選択します。「1」「2」「5」から指定します。
	General Settings
Max Users	最大ユーザ数を指定します。1 から 1000 の間で指定できます。初期値は 1000 です。
Deny MAC-Move	「MAC-move」機能の拒否を「Enabled」(有効)/「Disabled」(無効)を指定します。
	本オプションは認証ホストが複数スイッチポートのローミングする場合、指定ポートのみ認証される状態からポートを複
	数認証モードにして、ホストの認証ポートの移動を可能にする機能です。ホストによる認証ポート間の移動には二つの状
	況が考えられます。再認証が必要になるか次のルールに従い再認証なしで新しいポートへ直接移動します。もし新しいポー
	トが元々のポートと同じ認証設定であれば、再認証は不要です。ホストは新しいポートに同じ認証属性を引き継ぎます。
	認証ホストはポート1からポート2へローミングができ、再認証なしで認証属性を引き継ぎます。もし新しいポートが元々
	のポートと違う認証設定の場合、再認証の必要があります。ポート1の認証ホストはポート2へ移動して再認証を受けます。
	もし新しいポートが認証方式を有効にしていない場合、ステーションは直接新しいポートへ移動させられます。そして元々
	のポートとのセッションは削除されます。ポート1の認証ホストはポート2へ移動可能です。
	本機能が無効の場合、認証ホストは他のポートへ移動可能ですが違反エラーとして認識されます。
Authorization State	認証について「Enabled」(有効)/「Disabled」(無効)に指定します。本オプションについては権限設定の受容の「Enabled」
	(有効)/「Disabled」(無効)に使用されます。権限への認証が有効になると、RADIUS サーバにより付与される権限属性(VLAN,
	802.1p default priority, bandwidth,ACL など)が、権限が有効になると許容されます。「Bandwidth」「ACL」はポートベー
	スでアサインされます。マルチ認証モードの場合「VLAN」と「802.1p」は各ホストベースでアサインされます。しかし
	「Bandwidth」「ACL」は各ポートベースでアサインされます。
	User Information
User Name	ユーザ名を入力します。32 文字まで入力可能です。
VID	VLAN ID を入力します。
Password Type	パスワード種類を選択します。「Plain Text」「Encrypted」から選択可能です。
Password	パスワードを入力します。
設定を変更する際は、必	いず「Apply」ボタンをクリックし、設定内容を適用してください。

設定を変更する際は、必ず「Applif」ホタンをクリックし、設定内容を適用して「 「Delete」ボタンをクリックして、指定エントリを削除します。

# Network Access Authentication Port Settings(ネットワークアクセス認証ポート設定)

ネットワークアクセス認証のポート設定を行います。

Security > Network Access Authentication > Network Access Authentication Port Settings の順にメニューをクリックし、以下の画面を表示します。

			ungs					
Network Access	Authentication Po	rt Settings						
Unit	F T T	From Port	To	Port				
Host Mode		/ID List Action	VII	D List		CompAuth Mod	e	
Multi Auth Max Users (1-40	96) F	None 🔽	1, Re	6-9 Auth Timer (1-65535)		Any Note Inactivity State		
4096		Disabled 🔽	36	i00 s	sec	Disabled	•	
Inactivity Timer (	120-65535) F	Restart (1-65535)	sec					Apply
Inactivity Timer (	120-65535) F	Restart (1-65535) 60	sec					Apply
Unit 1 Settings Port	120-65535) F sec ( Host Mode	Restart (1-65535) 50 VID List	sec	Max Users	Periodic	ReAuth	Inactivity Timer	Apply Restart
Unit 1 Settings Port eth1/0/1	120-65535) F sec ( Host Mode Multi Auth	Restart (1-65535) 50 VID List	sec CompAuth Mode Any	Max Users 4096	Periodic Disabled	ReAuth 3600	Inactivity Timer Disabled	Apply Restart 60
Inactivity Timer ( Unit 1 Settings Port eth1/0/1 eth1/0/2	120-65535) F sec 6 Host Mode Multi Auth Multi Auth	Restart (1-65535) 50 VID List	sec CompAuth Mode Any Any	Max Users 4096 4096	Periodic Disabled Disabled	ReAuth 3600 3600	Inactivity Timer Disabled Disabled	Apply Restart 60 60
Inactivity Timer ( Unit 1 Settings Port eth1/0/1 eth1/0/2 eth1/0/3	120-65535) F sec ( Mutti Auth Mutti Auth Mutti Auth	Restart (1-65535) 50 VID List	sec CompAuth Mode Any Any Any	Max Users 4096 4096 4096	Periodic Disabled Disabled Disabled	ReAuth 3600 3600 3600	Inactivity Timer Disabled Disabled Disabled	Apply Restart 60 60 60
Inactivity Timer ( Unit 1 Settings Port eth1/0/1 eth1/0/2 eth1/0/3 eth1/0/4	120-65535) F sec d Multi Auth Multi Auth Multi Auth Multi Auth Multi Auth	VID List	Sec CompAuth Mode Any Any Any Any	Max Users           4096           4096           4096           4096           4096	Periodic Disabled Disabled Disabled Disabled	ReAuth           3600           3600           3600           3600           3600	Inactivity Timer Disabled Disabled Disabled Disabled	Apply Restart 60 60 60 60 60
Inactivity Timer ( Unit 1 Settings Port eth1/0/1 eth1/0/2 eth1/0/3 eth1/0/4 eth1/0/5	Host Mode Host Mode Multi Auth Multi Auth Multi Auth Multi Auth Multi Auth	VID List	Sec CompAuth Mode Any Any Any Any Any Any	Max Users           4096           4096           4096           4096           4096           4096           4096	Periodic Disabled Disabled Disabled Disabled Disabled	ReAuth 3600 3600 3600 3600 3600	Inactivity Timer Disabled Disabled Disabled Disabled Disabled	Apply Restart 60 60 60 60 60 60

図 12-79 Network Access Authentication Port Settings 画面

# 第12章 Security(セキュリティ機能の設定)

#### 画面に表示される項目:

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	設定するポート範囲を指定します。
Host Mode	選択ポートと関連するホストモードを選択します。「Multi Host」「Multi Auth」から選択します。ポートがマルチホスト モードで動作していて一つのホストが認証されている場合、すべての他のホストはポートへのアクセスを許可されます。 802.1X 認証に従い、再認証失敗や認証ユーザーのログオフなどの場合、ポートはしばらくの間ブロックされます。一定期 間終了後 EAPOL パケットのプロセスにてポートはリストアします。ポートがマルチ認証モードで動作しており、各ホスト がポートへのアクセスに認証が必要な場合、ホストは MAC アドレスとして認識され、認証されたホストのみポートへの アクセスが可能になります。
VID List	ホストモードでマルチ認証オプションを選択した後、次のパラメータが有効になります。使用する VLAN ID を入力します。 これは複数の認証要件があるスイッチの複数 VLAN に有効です。クライアントが認証されたのちに、クライアントは他の VLAN に受信をしても再認証されません。これは各 VLAN の認証コントロールを行うトランクポートにとって有効です。ポー トの認証モードがマルチホストに変更された場合、ポートにある以前の認証 VLAN はクリアされます。
CompAuth Mode	コンパウンド認証モードのオプションを選択します。「Any」「MAC-WAC」から選択します。「Any」を選択すると、あら ゆる認証方式 (802.1X, MAC-based Access Control, WAC) でのアクセスを指定します。「MAC-WAC」を選択すると MAC ベー スの認証を最初に検証します。クライアントがパスをすると、WAC が次に検証され、最終的には両方の認証をパスする必 要があります。
Max Users	最大ユーザ数を指定します。1 から 1000 の間で指定できます。
Periodic	選択ポートの定期再認証を「Enabled」(有効)/「Disabled」(無効)にします。802.1X プロトコルにのみ影響します。
ReAuth Timer	再認証時間を指定します。1 から 65535(秒)で指定します。初期値では 3600 秒です。
Inactivity State	「Inactivity」(休止)を「Enabled」(有効)/「Disabled」(無効)に指定します。
Inactivity Timer	「Inactivity」(休止)を有効にした場合、休止時間の値を入力します。120 から 65535(秒)です。このパラメータは WAC と JWAC の認証プロトコルにのみ影響します。
Restart	リスタート時間を入力します。1 から 65535(秒)の間で指定可能です。
「Apply」ボタンをクリッ	クレ、設定を有効にします。

「Delete」ボタンをクリックして、指定エントリを削除します。

## Network Access Authentication Sessions Information(ネットワークアクセス認証セッション情報)

ネットワークアクセス認証セッションの情報表示、クリアを行います。

Security > Network Access Authentication > Network Access Authentication Sessions Information の順にメニューをクリックし、以下の画面を表示 します。

Network Access Authentication Sess	ions Information		
Port	1 V eth1/0/1 V	Clear by Port	Find
MAC Address	00-84-57-00-00	Clear by MAC	Find
Protocol	MAC	Clear by Protocol	Find
		Clear All	Show All
Authentication Sessions Total	0		
Total Authenticated Hosts	0		
Total Blocked Hosts	0		
Authentication Sessions Information			
Total Entries: 0			

図 12-80 Network Access Authentication Sessions Information 画面

画面に表示される項目:

項目	説明
Port	表示するポートとユニットを指定します。
MAC Address	表示する MAC アドレスを指定します。
Protocol	プロトコルオプションを選択します。「MAC」「WAC」「JWAC」「DOT1X」から選択します。

「Apply」ボタンをクリックし、設定を有効にします。

「Clear by Port」ボタンをクリックし、選択したポートに基づく情報を消去します。

「Clear by MAC」ボタンをクリックし、選択した MAC アドレスに基づく情報を消去します。

「Clear by Protocol」ボタンをクリックし、選択したプロトコルに基づく情報を消去します。

「Clear All」ボタンをクリックし、テーブル上のすべての情報を消去します。

「Find」ボタンをクリックし、入力した情報を元に指定のエントリを検出します。

```
「View All」ボタンをクリックし、すべてのエントリを表示します。
```

# Safeguard Engine (セーフガードエンジン)

ネットワーク上の悪意のあるホストがスイッチに対して、パケットフラッディング(ARPストーム)などを利用して、周期的に攻撃してくることが あります。これらの攻撃によりスイッチのCPUはその対応量を超えて増加してしまう可能性があります。このような問題を軽減するために、本スイッ チのソフトウェアにセーフガードエンジン機能を付加しました。

セーフガードエンジンは、攻撃が行われている間、スイッチの稼働を最小化して、スイッチ全体の操作性を保ち、限られたリソース内で必要不可欠なパケットの送受信を可能にします。省パワーモード(exhausted mode)の場合、スイッチは ARP と IP パケットのための帯域を制限します。もし CPU の稼働がしきい値以下に下がった場合、セーフガードエンジンは動作を停止しスイッチは省パワーモードを脱却し通常モードへ移行します。

CPU に宛てられるパケットは3つのグループに分類されます。サブインタフェースとしても知られるこれらのグループはCPU が特定の種類のトラフィックを認識するうえで使用する論理的なインタフェースです。この3つのグループは「Protocol」「Manage」「Route」があります。通常、「Protocol」 グループは、スイッチのCPU プロセスがパケットを受信した時に、最高のプライオリティ受信し、そして「Route」グループは、スイッチのCPU が入り込むルーティングパケットのプロセスの中で、グループの最低の優先値を受信します。「Protocol」グループでのパケットはルータによって識別されたプロトコルコントロールパケットです。管理(Manage)グループ内で、パケットはTelentやSSHと同様に、インタラクティブアクセスプロトコルの内容でルータやシステムネットワークマネジメントインタフェースへ向かいます。「Route」グループではパケットは通常ルータCPUトラバース(行ったり来たり)するルートパケットとして認識されます。

以下の表ではプロトコルと対応するサブインタフェースを表示します。

プロトコル名	サブインタフェース(グループ)	概要
802.1X	Protocol	Port-based Network Access Control(ポートベースアクセスコントロール)
ARP	Protocol	Address resolution Protocol (ARP)
BGP	Protocol	Border Gateway Protocol
DHCP	Protocol	Dynamic Host Configuration Protocol (DHCP)
DNS	Protocol	Domain Name System (DNS)
DVMRP	Protocol	Distance Vector Multicast Routing Protocol
GVRP	Protocol	GARP VLAN Registration Protocol (GVRP)
ICMPv4	Protocol	Internet Control Message Protocol (ICMP)
ICMPv6-Neighbor	Protocol	IPv6 Internet Control Message Protocol Neighbor Discovery Protocol (NS/NA/RS/RA) (ICMPv6-Neighbor)
ICMPv6-Other	Protocol	IPv6 Internet Control Message Protocol except Neighbor Discovery Protocol (NS/NA/RS/RA) (ICMPv6-Other)
IGMP	Protocol	Internet Group Management Protocol (IGMP)
LACP	Protocol	Link Aggregation Control Protocol (LACP)
NTP	Protocol	Network Time Protocol
OSPF	Protocol	Open Shortest Path First
PIM	Protocol	Protocol Independent Multicast
PPPoE	Protocol	Point-to-point protocol over Ethernet
RIP	Protocol	Routing Information Protocol
SNMP	Manage	Simple Network Management Protocol (SNMP)
SSH	Manage	Secure Shell (SSH)
STP	Protocol	Spanning Tree Protocol (STP)
Telnet	Manage	Telnet
TFTP	Manage	Trivial File Transfer Protocol (TFTP)
VRRP	Protocol	Virtual Router Redundancy Protocol
Web	Manage	Hypertext Transfer Protocol (HTTP) Hypertext Transfer Protocol Secure (HTTPS)

カスタマイズされたレートリミット(パケット/毎秒)、をセーフガードエンジンのサブインタフェースに対してまとめてアサイン、または管理インタフェースで指定した個々のプロトコルに対してアサインすることが可能です。個々のプロトコルのレートリミットをカスタマイズする場合に注意しなければいけないのは、本機能を使用して不適切なレートリミットを設定すると、スイッチのパケットプロセスに異常をきたす場合があります。

注意

エンジンガードが有効になっている場合、CPU使用率とトラフィック制限を制御するために、スイッチはFFP(高速フィルタプロセッサ)メー タリングテーブルを使用して、さまざまなトラフィックフロー(ARP、IP)に帯域幅を割り当てます。これはネットワークを介してトラフィッ クをルーティングするスピードが制限される場合があります。

## Safeguard Engine Settings(セーフガードエンジン設定)

スイッチにセーフガードエンジンの設定を行うためには、Security > Safeguard Engine > Safeguard Engine Settings の順にクリックし、以下の画面 を表示します。

Safeguard Engine Settings		
Safeguard Engine Settings		
Safeguard Engine State Trap State Safeguard Engine Current Status	Disabled Disabled Normal	
CPU Utilization Settings		
Rising Threshold (20% ~ 100%)	30 %	
Falling Threshold (20% ~ 100%)	20 %	Apply

図 12-81 Safeguard Engine Settings 画面

画面に表示される項目	;
------------	---

項目	説明
	Safeguard Engine Settings
Safeguard Engine State	セーフガードエンジン機能を「Enabled」(有効)/「Disabled」(無効)にします。
Trap State	セーフガードエンジントラップを「Enabled」(有効)/「Disabled」(無効)にします。
Safeguard Engine Current Status	現在のセーフガードエンジンの状態を表示します。
	CPU Utilization Settings
Rising Threshold	Safeguard Engine を有効にする前に許容可能な CPU 使用率のレベルを設定します。CPU 使用率がこのしきい値
(20% ~ 100%)	に到達すると、ここで設定した項目に基づいて、Exhausted モードに入ります。
Falling Threshold	許容可能な CPU 使用率のレベルを設定します。スイッチは CPU 使用率がこのしきい値に到達すると Safeguard
(20% ~ 100%)	Engine 状態から Normal モードに戻ります。
設定を変更する際は、必ず「Apply	」ボタンをクリックし、設定内容を適用してください。

## CPU Protect Counters (CPU プロテクトカウンタ)

CPU プロテクションのカウンタ情報を表示、消去します。

Security > Safeguard Engine > CPU Protect Counters の順にクリックし、以下の画面を表示します。

CPU Protect Counters		
Clear CPU Protect Counters		
<ul> <li>Sub Interface</li> </ul>	Manage	
Protocol Name	dhcp Clear	Clear All

図 12-82 CPU Protect Counters 画面

#### 画面に表示される項目:

項目	説明
Sub Interface	サブインタフェースのオプションを選択します。「Manage」「Protocol」「Route」「All」から選択します。 CPU プロテクトに関連したサブインタフェースのカウンタの消去を指定します。
Protocol Name	プロトコル名のオプションを選択します。

「Clear」ボタンをクリックし、設定に基づいた情報を消去します。 「Clear All」ボタンをクリックし、すべての情報を消去します。

## CPU Protect Sub-Interface (CPU プロテクトサブインタフェース)

CPU プロテクションのサブインタフェースを設定、表示します。

Security > Safeguard Engine > CPU Protect Sub-Interface の順にクリックし、以下の画面を表示します。

CPU Protect Sub	CPU Protect Sub-Interface					
CPU Protect Sub-Inte	erface					
Sub-Interface	Manage	~	Rate Limit (0-1024)		pps 🗌 No Limit	Apply
Sub-Interface Information	ation					
Sub-Interface	Manage	~				Find
Rate Limit	100 pps					
	Unit		Total			Drop
	1		23			0

図 12-83 CPU Protect Sub-Interface 画面

画面に表示される項目:

項目	説明						
	CPU Protect Sub-Interface(CPU プロテクトサブインタフェース)						
Sub Interface	サブインタフェースのオプションを選択します。「Manage」「Protocol」「Route」から選択します。						
Rate Limit	レートリミットの値を入力します。0 から 1024 パケット / 毎秒の間で指定できます。						
	「No Limit」を指定するとレートリミットを無効にします。						
設定を変更する際は、必ず「Apply	」ボタンをクリックし、設定内容を適用してください。						
項目							
Sub-Interface Information(サブインタフェース情報)							
Sub Interface	サブインタフェースのオプションを選択します。「Manage」「Protocol」「Route」から選択します。						
	した桂却を二にやウェントリを検山します						

「Find」ボタンをクリックし、入力した情報を元に指定エントリを検出します。

## CPU Protect Type(CPU プロテクトタイプ)

CPU プロテクションの種類の設定、表示します。

Security > Safeguard Engine > CPU Protect Type の順にクリックし、以下の画面を表示します。

CPU Protect Type		
CPU Protect Type		
Protocol Name dhcp 🔽	Rate Limit (0-1024)	pps No Limit Apply
Protect Type Information		
Type dhcp 🗸	Rate Limit 100 pps	Find
Unit	Total	Drop
1	0	0

図 12-84 CPU Protect Type 画面

画面に表示される項目:

項目	説明						
	CPU Protect Type(CPU プロテクトタイプ)						
Protocol Name	プロトコル名のオプションを選択します。						
Rate Limit	レートリミットの値を入力します。0 から 1024 パケット / 毎秒の間で指定できます。						
	「No Limit」を指定するとレートリミットを無効にします。						
設定を変更する際は必ず「Apply」ボタンをクリックし、設定内容を適用してください。							
項目	説明						
	Protect Type Information(プロテクトタイプ情報)						
Type プロトコルタイプを選択します。選択するとアサインするレートリミットの値が表示されます。							
	「unit」を選択した場合、物理スタックのユニット ID を選択します。						
設定を変更する際は必ず「Apply」 項目 Type	「No Limit」を指定するとレートリミットを無効にします。         ボタンをクリックし、設定内容を適用してください。         説明         Protect Type Information(プロテクトタイプ情報)         プロトコルタイプを選択します。選択するとアサインするレートリミットの値が表示されます。         「unit」を選択した場合、物理スタックのユニット ID を選択します。						

「Find」ボタンをクリックし、入力した情報を元に指定エントリを検出します。

# Trusted Host (トラストホスト)

トラストホストの設定、表示を行います。

Security > Trusted Host の順にクリックし、以下の画面を表示します。

	_		
32 chars	Туре	Telnet	Apply
ter of ACL name must be a	a letter.		
e		ACL Name	
iet		Standard-IP-ACL	Delete
	32 chars	32 chars Type cter of ACL name must be a letter.	32 chars     Type     Telnet       cter of ACL name must be a letter.       De     ACL Name       het     Standard-IP-ACL

図 12-85 Trusted Host 画面

#### 画面に表示される項目:

項目	説明			
ACL Name	使用する ACL 名を入力します。32 文字までで指定可能です。			
Туре	トラストホストの種類を指定します。「Telnet」「SSH」「Ping」「HTTP」「HTTPS」から指定します。			

「Delete」をクリックして指定のエントリを削除します。

# Traffic Segmentation (トラフィックセグメンテーション)

トラフィックセグメンテーション機能は、(単一/複数)ポート間のトラフィックの流れを制限するために使用します。「トラフィックフローの分割」という方法は、「VLAN によるトラフィック制限」に似ていますが、さらに制限的です。本機能によりマスタスイッチ CPU のオーバヘッドを増加させないようにトラフィックを操作することが可能です。

Security > Traffic Segmentation Settings の順にメニューをクリックし、以下の画面を表示します。

Traffic Se	gmentation Settings						_
Traffic Segr	nentation Settings						
Unit 1	From Port eth1/0/1	To Port eth1/0/1	Forward Unit	From Forward Port eth1/0/1	To Forward Port eth1/0/1	Add	Delete
Unit 1 Sett	ings						
	Port			Forwarding Dom	ain		
eth1/0/10				eth1/0/11			

図 12-86 Traffic Segmentation 画面

画面に表示される項目:

項目	説明
Unit	設定する受信スイッチユニットを選択します。
From Port /	設定する受信ポート範囲を指定します。
To Port	
Forward Unit	設定する転送スイッチユニットを指定します。
From Forward Port	設定する転送ポート範囲を指定します。
/ To Forward Port	

「Add」ボタンをクリックすると、入力した情報を元に新しいエントリを追加します。 「Delete」ボタンをクリックすると、入力した情報を元にエントリを削除します。

# Storm Control Settings (ストームコントロール設定)

ストームコントロールの設定、表示を行います。Security > Storm Control Settings の順にクリックします。

Storm Control Settings		_					
Storm Control Trap Settings –							
Trap State Nor	Trap State None 🗸						
Storm Control Polling Settings							
Polling Interval (5-600) 5	sec Shu	utdown Retries (0-360)	3 times	] Infinite	Apply		
Storm Control Dort Sottings							
storm control Port Settings -							
Unit From Port	To Port T	ype Act	ion Level Type	PPS Rise (1-2147483647)	PPS Low (1-2147483647)		
1 v eth1/0/1	✓ eth1/0/1 ✓ E	Broadcast 🔽 No	one 💙 PPS 🔽	pps	pps		
					Apply		
Total Entries: 78							
Port	Storm	Action	Threshold	Current	State		
	Broadcast		-	-	Inactive		
eth1/0/1	Multicast	Drop	-	-	Inactive		
	Unicast		÷		Inactive		
	Broadcast		-	-	Inactive		
eth1/0/2	Multicast	Drop	-	-	Inactive		
	Unicast		-	-	Inactive		

図 12-87 Storm Control Settings 画面

画面に表示される項目:

項目	説明
	Storm Control Trap Settings
Trap State	ストームコントロールトラップのオプションを「None」「Storm Occur」「Storm Clear」「Both」から指定します。 「None」が選択されるとトラップは送信されません。「Storm Occur」が選択されると、ストームの発生を検出した 時点でトラップは通知されます。「Storm Clear」が選択されるとストームが解消された時点でトラップは通知され ます。
設定を変更する際は、必ず「App	oly」ボタンをクリックし、設定内容を適用してください。
項目	説明
	Storm Control Polling Settings
Polling Interval	インターバルの値を指定します。5から600(秒)で指定できます。初期値は5秒です。
Shutdown Retries	再試行の値を入力します。0 から 360 で指定できます。初期値は 3 です。「Infinite」にチェックを入れると本機能 は無効になります。
設定を変更する際は、必ず「App	oly」ボタンをクリックし、設定内容を適用してください。
項目	説明
	Storm Control Port Settings
Unit	設定するユニットを選択します。
From Port / To Port	設定するポート範囲を指定します。
Туре	コントロールするストームの種類を「Broadcast」「Multicast」「Unicast」から選択します。 シャットダウンモードで選択すると、ユニキャストは「Known」「Unknown」両方が設定してある場合、どちらに も対応しポートはシャットダウンします。そうでない場合は「Unknown」にのみ対応します。
Action	動作について指定します。「None」「Shutdown」「Drop」から指定します。 「None」を指定するとストームパケットをフィルタしません。「Shutdown」は選択すると、指定したしきい値に 達するとポートはシャットダウンされます。「Drop」を選択すると指定したしきい値に達するとパケットを破棄し ます。
Level Type	レベルタイプを指定します。「PPS」「Kbps」「Level」から選択します。
PPS Rise	毎秒のパケット増加の上限値について指定します。毎秒増加するパケットの量について上限しきい値を指定しま す。0から 2147483647 パケット毎秒で指定できます。「Low PPS」の値が指定されていない場合、初期値は増加し たパケット毎秒の 80%に指定されます。
PPS Low	毎秒のパケット減少の下限値について指定します。毎秒減少するパケットの量について下限しきい値を指定します。0から 2147483647 パケット毎秒で指定できます。「Low PPS」の値が指定されていない場合、初期値は増加したパケット毎秒の 80%に指定されます。

# 第12章 Security(セキュリティ機能の設定)

「Level Type」で「Kbps」を選択すると、以下の画面が表示されます。

Storm Cont	trol Port	Settings						
Unit		From Port	To Port	Туре	Action	Level Type	KBPS Rise (0-2147483647)	KBPS Low (0-2147483647)
1	~	eth1/0/1 💌	eth1/0/1 🔽	Broadcast 🗸	None 🔽	Kbps 🗸	Kbps	Kbps
								Apply

図 12-88 Storm Control (Kbps) 画面

画面に表示される項目:

項目	説明
KBPS Rise	上限 KBPS の値を指定します。ポートに受信するトラフィックの上限しきい値をキロビット / 毎秒で指定します。 0 から 2147483647 Kbps の間で指定できます。
KBPS Low	下限 KBPS の値を指定します。ポートに受信するトラフィックの下限しきい値をキロビット / 毎秒で指定します。 0 から 2147483647 Kbps の間で指定できます。「Low PPS」の値が指定されていない場合、初期値は増加したパケッ ト毎秒の 80%に指定されます。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

「Level Type」で「Level」を選択すると、以下の画面が表示されます。

Storm Control Po	t Settings						
Unit	From Port	To Port	Туре	Action	Level Type	Level Rise (0-100)	Level Low (0-100)
1 🗸	eth1/0/1	eth1/0/1 💙	Broadcast 🗸	None 🔽	Level 🗸	%	%
							Apply

図 12-89 Storm Control (Level) 画面

画面に表示される項目:

項目	説明
Level Rise	下限レベルについて入力します。本オプションはポートに受信するトラフィックの総帯域のパーセンテージを上限
	のしきい値として指定します。0 から 100%で指定可能です。
Level Low	下限レベルについて入力します。本オプションはポートに受信するトラフィックの総帯域のパーセンテージを下限
	のしきい値として指定します。0 から 100%で指定可能です。「Level Low」の値が指定されていない場合、初期値
	は増加したパケット毎秒の 80%に指定されます。

注意 Level に 0 を指定した場合、H/W Entry が作成されるまでの間、スイッチは対象の通信を許可します。

注意 Multicast を指定した場合、予約 MAC Address(VRRP、OSPF、IGMP、MLD など) に対する制限は適用されません。

注意 % および kbps を指定した場合は、受信 Frame Size を 64 Octet 固定長とし、Packet per second に基づいて表示するため、状態を正しく 反映しません。

# DoS Attack Prevention Settings(DoS 攻撃防止設定)

各 DoS 攻撃に対して防御設定を行います。

Security > DoS Attack Prevention Settings の順にメニューをクリックし、以下の画面を表示します。

DoS Attack Prev	vention Setting	S		
SNMP Server Enable	e Traps DoS Setting	S		
Trap State	Disabled	~		Apply
DoS Attack Preventi	ion Settings			
DoS Type Selection	n			
Land Attack		Blat Attack	TCP Null	TCP Xmas
TCP SYN-FIN		TCP SYN SrcPort Less 1024	Ping of Death Attack	TCP Tiny Fragment Attack
All Types				
DoS Settings				
State	Action			
Disabled V	Drop 🗸			Apply
	DoS Type		State	Action
	Land Attack		Disabled	Drop
	Blat Attack		Disabled	Drop
	TCP Null		Disabled	Drop
	TCP Xmas		Disabled	Drop
	TCP SYN-FIN		Disabled	Drop
TCP	SYN SrcPort Less 10	024	Disabled	Drop
1	Ping of Death Attack		Disabled	Drop

図 12-90 DoS Attack Prevention Settings 画面

#### 画面に表示される項目:

項目	説明				
	SNMP Server Enable Traps DoS Settings				
Trap State	本オプションは、DoS 攻撃防止トラップ状態を有効または無効にします。				
	DoS Attack Prevention Settings				
DoS Type Selection	<ul> <li>適切な DoS 攻撃防御のタイプを選択します。</li> <li>Land Attack - DoS 攻撃防止タイプに LAND 攻撃を指定します。</li> <li>Blat Attack - DoS 攻撃防止タイプに BLAT 攻撃を指定します。</li> <li>TCP Null - DoS 攻撃防止タイプに TCP Null Scan 攻撃を指定します。</li> <li>TCP Xmas - DoS 攻撃防止タイプに TCP Xmascan 攻撃を指定します。</li> <li>TCP SYN-FIN - DoS 攻撃防止タイプに TCP SYNFIN 攻撃を指定します。</li> <li>TCP SYN-FIN - DoS 攻撃防止タイプに TCP SYNFIN 攻撃を指定します。</li> <li>TCP SYN SrcPort Less 1024 - DoS 攻撃防止タイプに TCP SYN Source Port Less 1024 攻撃を指定します。</li> <li>Ping Death Attack - DoS 攻撃防止タイプに Ping Death Attack 攻撃を指定します。</li> <li>TCP Tiny Fragment Attack - DoS 攻撃防止タイプに TCP Tiny Frag 攻撃を指定します。</li> <li>All Types - DoS 攻撃防止タイプにすべての攻撃を指定します。</li> </ul>				
State	DoS 攻撃防止の状態を指定します。• Enabled - DoS 攻撃防止の状態を有効にします。• Disabled - DoS 攻撃防止の状態を無効にします。				
Action	DoS 攻撃を検出したときに実行されるアクションを指定します。 ・ Drop - 一致する DoS 攻撃パケットをすべて破棄します。				

# Zone Defense Settings (ゾーンディフェンス設定)

「ゾーンディフェンス(Zone Defense)」機能の設定と表示を行います。ゾーンディフェンスが有効な場合、ACL リソースがゾーンディフェンスのた めに使用されます。十分な ACL リソースがない場合は、本機能を有効にすることはできません。ゾーンディフェンスはネットワークトラフィックの 異常がファイアウォールに設定したしきい値に到達すると実行されます。この場合、ファイアウォールは即座にスイッチにコンタクトし、コマンド を実行します。その結果、疑いのあるホストからのあらゆるトラフィックをブロックします。

Security > Zone Defense Settings の順にメニューをクリックし、以下の画面を表示します。

Zone Def	Zone Defense Settings		
Zone Defer	nse Settings		
State	O Enabled		Apply
⊠ 12-91	Zone Defense Settings 画面		

項目	説明		
State	本機能を「Enabled」(有効)/「Disabled」(無効)にします。		

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

# SSH (Secure Shell)

画面に表示される項目:

SSH (Secure Shell) は、安全性の低いネットワーク上で、安全なリモートログインと安全なネットワークサービスを実現するためのプログラムです。 SSH は、リモートのホストコンピュータへの安全なログインや、リモートのエンドノードでの安全なコマンド実行メソッドを可能にし、信頼関係を 結んでいないホスト間に暗号化と認証を利用した安全な通信を提供します。高度なセキュリティ機能を備えた SSH は、今日のネットワーク環境に必 要不可欠なツールです。ネットワーク通信を脅かす数々のセキュリティハザードに対して、強力な監視者としての役割を担います。

リモート PC(SSH クライアント)とスイッチ(SSH サーバ)間でセキュアな通信を行うための SSH プロトコルの設定は、以下の手順で行います。

- 1. 「User Accounts Settings」で管理者レベルのアクセス権を持つアカウントを作成します。本手順はスイッチに管理者レベルのユーザアカウント を作成する方法と同じで、パスワードの設定を含みます。本パスワードは、SSH プロトコルを使用した安全な通信経路が確立された後、スイッ チにログインする際に使用します。
- 2. 「SSH User Settings」画面を使用して、ユーザアカウントを設定します。この時スイッチが SSH 接続の確立を許可する際のユーザの認証方法を 指定します。この認証方法には、「Host Based」、「Password」、「Public Key」の3つがあります。
- 3. 「Host Key」画面を使用して、SSH クライアントとサーバ間で送受信するメッセージの暗号化、復号化に用いる暗号化アルゴリズムを設定します。
- 4. 最後に「SSH Global Settings」画面で、SSH を有効にします。

これらの手順が完了後、安全な帯域内の接続でスイッチの管理を行うために、リモート PC 上の SSH クライアントの設定を行います。

## SSH Global Settings(SSH グローバル設定)

SSH グローバル設定および設定内容の確認に使用します。

Security > SSH > SSH Global Settings の順にメニューをクリックします。

Disabled	
22	
V2	
120 sec	
3 times	Apply
	Disabled 22 V2 120 sec 3 times

図 12-92 SSH Global Settings 画面

設定および表示する項目は以下の通りです。

項目	説明
IP SSH Server State	グローバルに SSH 機能を「Enabled」(有効)/「Disabled」(無効)にします。
	初期值:「Disabled」
IP SSH Service Port	SSH サービスポート番号を設定します。
(1-65535)	初期値:22
Authentication	認証のタイムアウト時間を指定します。30 から 600(秒)が指定できます。
Timeout(30-600)	初期值:120(秒)
Authentication Retries	ユーザが SSH サーバに対して認証を試みることができる回数を指定します。指定した回数を超えるとスイッチは接続を切
Attempts (1-32)	り、ユーザは再度スイッチに接続する必要があります。1 から 32 が指定できます。
	初期值:3

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

# Host Key(Host Key 設定)

SSHホスト鍵の設定(有効化)および設定内容の確認に使用します。

Security > SSH > Host Key の順にメニューをクリックし、以下の画面を表示します。

lost Key Management		
Crypto Key Type	RSA	
Key Modulus	768 <b>v</b> bit	Generate Delete
lost Key		
Crypto Key Type	RSA	
Key pair was generated at	02:45:17, 2000-01-01	
Key Size	768	
Key Data	AAAAB3NzaC1vc2EAAAADAQABAAAAYQDa5HxonYoT	

図 12-93 Host Key 画面

#### 画面に表示される項目:

項目	説明				
	Host Key Management				
Crypto Key	暗号鍵の種類を選択します。「Rivest Shamir Adleman (RSA)」または「Digital Signature Algorithm (DSA)」から選択します。				
Туре					
Key Modulus	鍵係数の値を入力します。「360」「512」「768」「1024」「2048」ビットから選択します。				
Host Key					
Crypto Key	暗号鍵の種類を選択します。「Rivest Shamir Adleman (RSA)」または「Digital Signature Algorithm (DSA)」から選択します。				
Туре					

「Generate」ボタンをクリックし、指定したホスト鍵を有効にします。 「Delete」ボタンをクリックし、指定したホスト鍵を削除します。

注意 スタック構成において、設定済みで「Key」の無い「Stack slave」を組み込んだ場合は同期されません。

「Generate」ボタンをクリックすると次の画面が表示されます。

Host Key Mai	nagement	
Result	Generating	

図 12-94 Host Key (Generating) 画面

「Generate」が終了すると次の画面が表示されます。

Host Key M	lanagement	
Host Key Ma	nagement	
Result	Success.	

図 12-95 Host Key (Generating, Success) 画面

## SSH Server Connection (SSH サーバ接続)

SSH サーバ接続テーブルの内容を確認します。

Security > SSH > SSH Server Connection の順にメニューをクリックし、以下の画面を表示します。

able				
tal Entries: 0				
SID	Version	Cipher	User ID	Client IP Address

図 12-96 SSH Server Connection 画面

表示されるエントリの内容を確認します。

### SSH User Settings (SSH ユーザ設定)

SSH ユーザの設定を行います。

Security > SSH > SSH User Settings の順にメニューをクリックし、以下の画面を表示します。

SSH User Settings				
SSH User Settings				
User Name	32 chars	Authentication Method	Password 🗸	
Key File	779 chars	Host Name	255 chars	
IPv4 Address		IPv6 Address	2013::1	Apply
Total Entries: 1				
User Name	Authentication Method	Key File	Host Name	Host IP
user	Password			
			1/1	< 1 > >  Go

図 12-97 SSH User Settings 画面

#### 画面に表示される項目:

項目	説明
User Name	SSH ユーザを識別するユーザ名を 32 文字までの半角英数字で指定します。
Authentication	スイッチにアクセスを試みるユーザの認証モードを以下から指定します。
Method	• Host-based - 認証用にリモート SSH サーバを使用する場合に選択します。本項目を選択すると、SSH ユーザ識別のために以下の情報を入力することが必要になります。
	• Password - 管理者定義のパスワードを使用して認証を行う場合に選択します。本項目を選択すると、スイッチは管理者にパスワードの入力(確認のため2回)を促します。
	• Public Key - SSH サーバ上の公開鍵を使用して認証を行う場合に選択します。
Key File	「Public Key」または「Host-based」を選択した場合ここで公開鍵(Public Key)を入力します。
Host Name	リモート SSH ユーザを識別する 31 文字までの半角英数字を入力します。
	本項目は「Authentication Method」で「Host-based」を選択した場合のみ入力が必要です。
IPv4 Address	SSH ユーザの IPv4 アドレスを入力します。
	本項目は「Authentication Method」で「Host-based」を選択した場合のみ入力が必要です。
IPv6 Address	SSH ユーザの IPv6 アドレスを入力します。
	本項目は「Authentication Method」で「Host-based」を選択した場合のみ入力が必要です。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。 複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

# SSH Client Settings(SSH クライアント設定)

SSH クライアントの設定を行います。

Security > SSH > SSH Client Settings の順にメニューをクリックし、以下の画面を表示します。

SSH Client Settings				
SSH Client Settings				
Authentication Method	Password			
Public Key File Path	/c:/ldentity.pub			
Private Key File Path	/c:/Identity Apply			

図 12-98 SSH Client Settings 画面

#### 画面に表示される項目:

項目	説明
Authentication	認証方法を以下から選択します。
Method	・ Password - ユーザアカウントに対してパスワード認証を行います。(初期値)
	・ Public Key - ユーザアカウントに対してパブリックキー認証を行います。
Public Key File Path	パブリックキーとして使用するローカルファイルのパスとファイル名を入力します。
Private Key File Path	プライベートキーとして使用するローカルファイルのパスとファイル名を入力します。

## SSL (Secure Socket Layer)

Secure Sockets Layer (SSL) とは、認証、デジタル署名および暗号化を使用して、ホストとクライアント間に安全な通信パスを提供するセキュリティ 機能です。このセキュリティ機能は、暗号スイートを使用して実現されます。暗号スイートは、認証セッションに使用される特定の暗号化アルゴリ ズムおよびキー長を決定するセキュリティ文字列であり、以下の3つの段階で構成されます。

1. 鍵交換(Key Exchange)

暗号スイート文字列の最初の部分では、使用する公開鍵アルゴリズムを規定しています。本スイッチは、RSA(Rivest Shamir Adleman)公開鍵 アルゴリズムとデジタル署名アルゴリズム(DSA、ここでは DHE:DHE DSS Diffie-Hellman 公開鍵アルゴリズムとして指定)を使用します。こ れはクライアントとホスト間の最初の認証プロセスであり、「鍵交換」を行って一致した場合、認証が受諾され、以下のレベルで暗号化のネゴシ エーションが行われます。

2. 暗号化(Encryption)

暗号スイートの次の部分は、クライアントとホスト間で送受信するメッセージの暗号化を含む暗号化方式です。本スイッチは2種類の暗号化ア ルゴリズムをサポートしています。

- ストリーム暗号 (Stream Ciphers) スイッチは 2 種類のストリーム暗号 (40 ビット鍵での RC4 と、128 ビット鍵での RC4) に対応しています。 これらの鍵はメッセージの暗号化に使用され、最適に利用するためにはクライアントとホスト間で一致させる必要があります。
- CBC ブロック暗号 CBC (Cipher Block Chaining:暗号ブロック連鎖)とは、1 つ前の暗号化テキストのブロックを使用して、現在のブロッ クの暗号化を行う方法です。本スイッチは、DES (Data Encryption Standard)で定義される 3 DES EDE 暗号化コードと高度な暗号化規格 (AES) をサポートし、暗号化されたテキストを生成します。
- 3. ハッシュアルゴリズム (Hash Algorithm)

暗号スイートの最後の段階では、メッセージ認証コードを決定するメッセージダイジェスト機能を規定します。このメッセージ認証コードは送 信されたメッセージと共に暗号化され、整合性を提供し、リプレイアタックを防止します。本スイッチは、MD5 (Message Digest 5) と SHA (Secure Hash Algorithm)、SHA-256 の 3 つのハッシュアルゴリズムをサポートします。

これら3つのパラメータは、スイッチ上での11個の選択肢として独自に組み合わされ、サーバとクライアント間で安全な通信を行うための3層の 暗号化コードを生成します。暗号スイートの中から1つ、または複数を組み合わせて実行することができますが、選択する暗号スイートによりセキュ リティレベルや安全な接続時のパフォーマンスは変化します。暗号スイートに含まれる情報はスイッチには存在していないため、証明書と呼ばれる ファイルを第三者機関からダウンロードする必要があります。この証明書ファイルがないと本機能をスイッチ上で実行することができません。証明 書ファイルは、TFTPサーバを使用してスイッチにダウンロードできます。また、本スイッチは、TLSv1.0/1.1/1.2をサポートしています。それ以外のバー ジョンは本スイッチとは互換性がない恐れがあり、クライアントからホストへの認証やメッセージ送信時に問題が発生する可能性があります。

「SSL Configuration Settings」画面では、スイッチで SSL を有効にして各種暗号スイートのステータスを設定することができます。暗号スイートは、 認証セッションに使用される正確な暗号のパラメータ、特定の暗号化アルゴリズム、および鍵のサイズを決定するセキュリティ文字列です。スイッ チには 11 個の暗号スイート設定が用意されています。特定の暗号スイートのみ有効にして、他のものを無効にすることも可能です。

SSL機能が有効化されると、通常の HTTP 接続はできなくなります。SSL 機能を使用した Web ベースの管理を行うには、SSL 暗号化がサポートされた Web ブラウザにおいて、https:// で始まる URL を使用する必要があります(例: https://10.90.90.90)。これらの条件を満たさない場合、エラーが発生し、Web ベースの管理機能への接続認証が行われません。

SSL 機能で使用する証明書ファイルは TFTP サーバからスイッチへダウンロードすることができます。証明書ファイルは、ネットワーク上のデバイ スを認証するために使われるデータであり、所有者や認証のための鍵、デジタル署名などの情報が格納されています。SSL 機能を最大限に活用する ためには、サーバ側とクライアント側で整合性のある証明書ファイルを保持している必要があります。スイッチは、拡張子 ".der"を持つ証明書の みをサポートします。スイッチには初期状態で証明書がインストールされていますが、ユーザ環境に応じて追加のダウンロードが必要になる場合が あるかもしれません。

## SSL Global Settings(SSL グローバル設定)

SSL グローバル設定を行います。

Security > SSL > SSL Global Settings の順にメニューをクリックし、以下の画面を表示します。

SSL Global Settings		
SSL Global Settings		
SSL Status	C Enabled      Disabled	
Service Policy	32 chars	Apply
Import File		
File Select	Certificate      Private Key     Browse     (The file name range is 1-32 chars.)	
Destination File Name	32 chars	Apply
Note: You can access the File	System page to manage these imported files.	

図 12-99 SSL Global Settings 画面

### 画面に表示される項目:

項目	説明			
	SSL Global Settings			
SSL Status	SSL をグローバルに「Enabled」(有効)、「Disabled」(無効)に設定します。初期値は「Disabled」です。			
Service Policy	SSL ポリシー名を入力します。32 文字まで指定できます。			
項目	説明			
	Import File			
File Select	ロードされるファイル種類を指定します。「Certificate」「Private Key」から指定可能です。ファイル種類を選択した後、			
「Browse/参照」ボタンをクリックして、適切なファイルを選択しローカルコンピュータにロードします。				
Destination File Name 宛先ファイル名を指定します。32 文字まで指定可能です。				
設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。				

## Crypto PKI Trustpoint(暗号 PKI トラストポイント)

暗号 PKI トラストポイントの表示、設定を行います。

#### Security > SSL > Crypto PKI Trustpoint の順にメニューをクリックし、以下の画面を表示します。

Crypto PKI Trustpoint					
Crypto PKI Trustpoint					
Trustpoint	32 chars	]		Apply	Find
Trustpoint	32 chars	]			
File System Path	e.g.:c:/cacert	Password	64 chars	]	
O TFTP Server Path	e.g.:ip/name	Туре	Local		Apply
Total Entries: 1					
Primary Trustpoin	nt Name	CA	Local Certificate	Local Private Key	er
trust;	point				Delete

図 12-100 Crypto PKI Trustpoint 画面

画面に表示される項目:

項目	説明
Trustpoint	インポートした証明書と鍵ペアに対応するトラストポイント名を入力します。32文字まで指定できます。
File System Path	証明書と鍵ペアのファイルシステムパスを入力します。
Password	インポートしたプライベート鍵の暗号を解除する暗号パスフレーズを入力します。パスフレーズは 64 文字まで指定可能 です。パスフレーズが指定されないと「NULL」文字列が使用されます。
TFTP Server Path	TFTP サーバのパスを指定します。
Туре	インポートされる証明書の種類を指定します。「Both」「CA」「Local」。「Both」を選択すると「CA 証明書」「ローカル証明書 の鍵ペア」をインポートします。「CA」を選択すると「CA 証明書」のみインポートします。「Local」を選択すると「ローカ ル証明書の鍵ペア」のみインポートします。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。 「Find」ボタンをクリックして、入力した情報に基づいて指定エントリを検出します。 「Delete」ボタンをクリックして、指定エントリを削除します。

# SSL Service Policy(SSL サービスポリシー)

SSL サービスポリシーの表示、設定を行います。

Security > SSL > SSL Service Policy の順にメニューをクリックし、以下の画面を表示します。

SSL Service Policy				
SSL Service Policy				
Policy Name	32 chars			Apply Find
Policy Name	32 chars			
Version	TLS 1.0 TLS 1.1			
Session Cache Timeout (60-86400)	600 sec			
Secure Trustpoint	32 chars			
Cipher Suites	DHE_DSS_WITH_3DES_EDE RSA_WITH_3DES_EDE_CE RSA_WITH_RC4_128_SHA RSA_EXPORT_WITH_RC4 RSA_WITH_RC4_128_MD5 RSA_WITH_AES_128_CBC RSA_WITH_AES_128_CBC RSA_WITH_AES_256_CBC RSA_WITH_AES_256 CBHE_DSS_WITH_AES_256 DHE_DSS_WITH_AES_256 CBHE_RSA_WITH_AES_256CBHE_RSA_WITH_AES_256 CBHE_RSA_WITH_AES_256CBHE_RSA_WITH_AES_256 CBHE_RSA_WITH_AES_256CBHE_RSA_WITH_AES_256CBHE_RSA_WITH_AES_256CBHE_RSA_WITH_AES_256CBHE_RSA_WITH_AES_256CBHE_RSA_WITH_AES_256CBHE_RSA_WITH_AES_256CBHE_RSA_WITH_AES_256CBHE_RSA_WITH_AES_256CBHE_RSA_WITH_AES_256CBHE_RSA_WITH_AES_256CBHE_RSA_WITH_AES_256CBHE_RSA_WITH_AES_256 CBHE_RSA_WITH_AES_256CBHE_RSA_WITH_AES_256 CBHE_RSA_WITH_AES_256C CBHE_RSA_WITH_AES_256C CBHE_RSA_WITH_AES_256C CBHE_RSA_WITH_AES_256C CBHE_RSA_WITH_AES_256C CBHE_RSA_WITH_AES_256C CBHE_RSA_WITH_AES_256C CBHE_RS	DE_CBC_SHA IC_SHA _40_MD5 _SHA _SHA _SHA256 _SHA256 _SHA256 _CBC_SHA _CBC_SHA		Apply
Total Entries: 1				
Policy Name Version	Cipher Suites	Session Cache Timeout (sec)	Secure Trustpoint	
Policy TLS 1.0,TLS 1.1	DHE_DSS_WITH_3DES_ED	600		Edit Delete

図 12-101 SSL Service Policy 画面

画面に表示される項目:

項目	説明
Policy Name	SSL サービスポリシー名を入力します。32 文字まで指定可能です。
Version	「Transport Layer Security」(TLS) バージョンを指定します。「TLS 1.0」「TLS 1.1」「TLS 1.2」から指定します。
Session Cache Timeout	セッションキャッシュタイムアウトの時間を指定します。初期値は 600(秒)です。
Secure Trustpoint	セキュアなトラストポイントの名前を入力します。32 文字まで指定可能です。
Cipher Suites	本プロファイルの暗号スイートを選択します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

「Find」ボタンをクリックして、入力した情報に基づいて指定エントリを検出します。

「Edit」ボタンをクリックして、指定エントリを編集します。

「Delete」ボタンをクリックして、指定エントリを削除します。

## SFTP Server Settings (SFTP サーバ設定)

本項目では「Secure File Transfer Protocol」(SFTP) サーバの設定、表示を行います。SFTP は信頼できるデータストリームにおけるリモートでセキュ アなファイルトランスファープロトコルです。SFTP はそれ自身で認証や、セキュリティを提供しないため、SFTP サーバを SSH サーバのサブシステ ムとして構築させる必要があります。

注意 IPv4 SFTP サーバのみサポートされています。

Security > SFTP Server Settings の順にメニューをクリックし、以下の画面を表示します。

SFTP Server Settings		
SFTP Server Settings		
SFTP Server	Enabled     Oisabled	
Idle Timeout (30-600)	120 sec	
Protocol Version	3	Apply

図 12-102 SFTP Server Settings 画面

画面に表示される項目:

項目	説明
SFTP Server	SFTP サーバ「Enabled」(有効)/「Disabled」(無効)に指定します。
Idle Timeout	<ul> <li>アイドルタイムアウトの時間を設定します。SFTP サーバが指定値の時間 SFTP セッションの活動が行われていないことを検出すると、SFTP セッションは閉じられます。</li> <li>・設定可能範囲: 30-600(秒)</li> <li>・初期値: 120(秒)</li> </ul>

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

# SFTP Client Settings(SFTP クライアント設定)

本項目では「Secure File Transfer Protocol」(SFTP) クライアントの設定、表示を行います。

#### Security > SFTP Client Settings の順にメニューをクリックし、以下の画面を表示します。

SFTP Client Settings		
SFTP Client Settings		
Authentication Method	'assword	
Public Key File Path	://dentity.pub	
Private Key File Path	/Identity A	pply

図 12-103 SFTP Client Settings 画面

#### 画面に表示される項目:

項目	説明
Authentication Method	SFTP クライアントの認証方法を指定します。 ・ Password - ユーザ名 / パスワードで認証します。 ・ Public key - パブリックキー(公開鍵)で認証します。
Public Key File Path	SFTP クライアントのパブリックキーファイル名 / パスを指定します。
Private Key File Path	SFTP クライアントのプライベートキーファイル名 / パスを指定します。

# Network Protocol Port Protect Settings (ネットワークプロトコルポートプロテクト設定)

本項目ではネットワークプロトコルポートプロテクションの設定、表示を行います。

Security > Network Protocol Port Protect Settings の順にメニューをクリックし、以下の画面を表示します。

Network Protocol Port Protect Settings		
Network Protocol Port Protect Settings		
TCP Port Protect State	Enabled O Disabled	
UDP Port Protect State	nabled Obisabled	
		Apply

図 12-104 Network Protocol Port Protect Settings 画面

画面に表示される項目:

項目	説明
TCP Port Protect State	TCP ポートネットワークプロトコルプロテクション機能を「Enabled」(有効)/「Disabled」(無効)にします。
UDP Port Protect State	UDP ポートネットワークプロトコルプロテクション機能を「Enabled」(有効)/「Disabled」(無効)にします。
	Apply」ボタンをクリックし、設定内容を適用してください。

# 第13章 OAM (Operations, Administration, Maintenance:運用・管理・保守)

以下は OAM サブメニューの説明です。

必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明
CFM(Connectivity Fault Management : 接続性障害管理)	CFM 機能を設定します。
Cable Diagnostics(ケーブル診断機能)	スイッチの特定のポートに接続する UTP ケーブルの詳細について表示します。
Ethernet OAM(イーサネット OAM)	ポートにイーサネット OAM モード、イベント、ログを設定します。
DDM(DDM 設定)	Digital Diagnostic Monitoring(DDM)機能を実行します。スイッチに挿入した SFP モジュールの DDM 状態の参照、各種設定(アラーム設定、警告設定、温度しきい値設定、電圧しきい値設定、バイアス電流 しきい値設定、Tx(送信)電力しきい値設定、および Rx(受信)電力しきい値設定)を行うことができ ます。

# CFM(Connectivity Fault Management:接続性障害管理)

CFM は IEEE 802.1ag に定義されており、ネットワークにおける接続性故障の検出、隔離、およびレポートを行う標準規格です。CFM は サービスインスタンスごとの End-to-End の OAM(Operations : 操作、Administration : 管理、および Maintenance : メンテナンス)のための機能です。802.1ag によって定義されるように、CFM 機能にはパスの発見、障害検出、故障検証、分離、および故障通知があります。

イーサネット CFM フレームには、特別なイーサネットタイプ(0x8902)があります。すべての CFM メッセージは VLAN ベースごとにメンテナンス ドメインに制限されます。CFM フレームペイロードの固有のユニークな OpCode によって識別される様々なメッセージタイプがあります。

CFM メッセージタイプには Continuity Check Message (CCM: 連続性チェックメッセージ)、Loopback Message と Response (LBM: ループバックメッ セージ、LBR: ループバックレスポンス)、および Link Trace Message と Response (LTM: リンクトレースメッセージ、LTR: リンクトレースレスポンス) が含まれます。

### CFM Settings(CFM 設定)

CFM 機能を設定します。

#### OAM > CFM > CFM Settings の順にメニューをクリックし、以下の画面を表示します。

CFM Settings	_	_			_
CFM Global Settings					
CFM State	OEnabled  OEnabled				
AIS Trap State	OEnabled  OEnabled				
LCK Trap State	OEnabled				Apply
All MPs Reply LTRs	OEnabled				Apply
CFM Domain Name Settings					
Domain Name	22 chars	Dom	ain Level 0	<b>~</b>	Apply
Total Entries: 1					
Domain Name	Domain Level	MIP Creation	SenderID TLV		
domain	0	None	None	Edit Del	ete Add MA

図 13-1 CFM Settings 画面

画面に表示される項目	:
------------	---

項目	説明
	CFM Global Settings
CFM State	CFM 機能を有効または無効にします。
AIS Trap State	「Alarm Indication Signal」(AIS) トラップ機能を有効 / 無効に指定します。有効にすると「ETH-AIS」イベント発生 / 解消時に トラップが送信されます。
LCK Trap State	「Locked Signal」(LCK)トラップ機能を有効 / 無効に指定します。有効にすると「ETH-LCK」イベント発生 / 解消時にトラッ プが送信されます。
All MPs Reply LTRs	Link Trace Reply (LTR) メッセージに応答するために、すべての MP (メンテナンスポイント) を有効または無効にします。
	CFM Domain Name Settings
Domain Name	メンテナンスドメインの名称を入力します。22 文字内で指定します。
Domain Level	メンテナンスドメインのレベルを選択します。レベルは、0-7の範囲で設定します。0 が最も低く、7 が最も高いレベルです。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

#### エントリの編集

編集するエントリの「Edit」ボタンをクリックして、以下の画面を表示します。

CFM Settings				
CFM Global Settings				
CFM State	OEnabled ODisabled			
AIS Trap State	OEnabled ODisabled			
LCK Trap State	OEnabled  OEnabled			Apply
All MPs Reply LTRs	OEnabled  OEnabled			Apply
CFM Domain Name Settings				
Domain Name	22 chars	Domain Level	0 🔽	Apply
Total Entries: 1				
Domain Name	Domain Level	MIP Creation Sende	erID TLV	
domain	0	None V None		Apply Delete Add MA

図 13-2 CFM Settings 画面 - Edit

画面に表示される項目:

項目	説明
MIP Creation	<ul> <li>MIP の作成を制御します。</li> <li>None - MIP を作成しません。(初期値)</li> <li>Auto - ポートがこの MD の MEP で設定されないと、MIP は常にこの MD のどのポートにも作成されます。MA の中間スイッ チでは、この設定は、MIP がこのデバイスで作成されるために「Auto」である必要があります。</li> <li>Explicit - 次に存在する低いレベルのポートに設定済みの MEP がなく、ポートがこの MD の MEP に設定されないと、MIP がこの MD のどのポートにも作成されません。</li> </ul>
Sender ID TLV	SenderID TLV の転送を制御します。 ・ None - SenderID TLV を転送しません。(初期値) ・ Chassis - シャーシ ID 情報を持つ SenderID TLV を転送します。 ・ Manage - 管理アドレス情報を持つ SenderID TLV を転送します。 ・ Chassis_Manage - シャーシ ID 情報と管理アドレス情報を持つ SenderID TLV を転送します。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

#### エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

注意 グループ名は 22 文字未満とします。

### Add MA 設定(CFM Settings)

メンテナンスアソシエーションを設定します。

OAM > CFM > CFM Settings 画面で「Add MA」ボタンをクリックし、以下の画面を表示します。

	dom	nain						
	22 (	chars						
							Apply	Back
A VID M/	A Mode	MIP Creation	CCM Interval	SenderID TLV	MEPID List		1.015 S.	
1 Se	oftware	Defer	10sec	Defer		Edit	Delete	Add MEP
	VID M. 1 S	don 22 d VID MA Mode 1 Software	domain 22 chars VID MA Mode MIP Creation 1 Software Defer	domain       22 chars       22 chars       VID     MA Mode       MIP Creation     CCM Interval       1     Software       Defer     10sec	domain       22 chars       22 chars       VID     MA Mode     MIP Creation     CCM Interval     SenderID TLV       1     Software     Defer     10sec     Defer	domain       22 chars       22 chars       VID     MA Mode     MIP Creation     CCM Interval     SenderID TLV     MEPID List       1     Software     Defer     10sec     Defer	domain         22 chars         22 chars         VID       MA Mode       MIP Creation       CCM Interval       SenderID TLV       MEPID List         1       Software       Defer       10sec       Defer       Edit	domain         22 chars       Apply         VID       MA Mode       MIP Creation       CCM Interval       SenderID TLV       MEPID List         1       Software       Defer       10sec       Defer       Edit       Delete



画面に表示される項目:

項目	説明			
MA Name	メンテナンスアソシエーションの名称(22 字以内)を入力します。			
MA VID (1-4094)	VLAN 識別子(1-4094)。異なる MA は異なる VLAN に関連付ける必要があります。			

|Apply」をクリックし、設定内容を適用します。

「Back」をボタンをクリックし、変更を破棄して前のページに戻ります。 「Add MEP」ボタンをクリックして、MEP(Maintenance End Point)エントリを追加します。

## エントリの削除

テーブルからエントリを削除するためには、削除対象のエントリの列の「Delete」ボタンをクリックします。

#### エントリの編集

エントリ横の「Edit」ボタンをクリックして以下の画面を表示します。

CFM MA Sett	ings	_	_	_	_	_	_	_	_
CFM MA Setting	5								
Domain Name		doma	iin						
MA Name		22 ch	nars						
MA VID (1-4094	0							Apply	Back
Total Entries: 1									
MA Name	MA VID	MA Mode	MIP Creation	CCM Interval	SenderID TLV	MEPID List			
ma	1	Software 🔽	Defer 🖌	10sec 🗸	Defer 🗸		Apply	Delete A	dd MEP

図 13-4 CFM MA Settings 画面 - Edit

画面に表示される項目:

項目	説明
MA Mode	プルダウンメニューを使用して、MAの動作モード(CFM ソフトウェアまたはハードウェアモード)を選択します。
	↓ ・ Software - MA は CFM ソフトウェアモードで動作します。(初期値)
	・ Hardware - MA は CFM ハードウェアモードで動作します。
MIP Creation	MIP の作成を制御します。
	<ul> <li>None - MIP を作成しません。(ハードウェアモード:初期値)</li> <li>Defer - この MA が関連するメンテナンスドメインの設定を継承します。(ソフトウェアモード:初期値)</li> <li>Auto - ポートがこの MD の MEP で設定されないと、MIP は常にこの MD のどのポートにも作成されます。MA の中間スイッチでは、この設定は、MIP がこのデバイスで作成されるために「Auto」である必要があります。</li> <li>Explicit - 次に存在する低いレベルのポートに設定済みの MEP がなく、ポートがこの MD の MEP に設定されない と、MIP がこの MD のどのポートにも作成されません。</li> </ul>
	注意 CFM ハードウェアモードでは初期値は「None」です。
CCM Interval	これは CCM 送信間隔です。
	<ul> <li>3.3ms - 3.3 (ミリ秒)。これは CFM ハードウェアモードでのみ動作します。</li> <li>10ms - 10 (ミリ秒)。これは CFM ハードウェアモードでのみ動作します。</li> </ul>
	• 100ms - 100 (ミリ秒)。推奨されません。テストの目的のために使用します。
	• 1sec - 1 (秒)。
	• IUSEC - IU(秒)(初明10)。
	• 10min - 10 (分)。
SenderID TLV	これは、SenderID TLV の転送を制御します。
	 ・ None - SenderID TLV を転送しません。
	・ Chassis - シャーシ ID 情報を持つ SenderID TLV を転送します。
	・ Manage - 管理アドレス情報を持つ SenderID TLV を転送します。
	・ Chassis_Manage - シャーシ ID 情報と管理アドレス情報を持つ SenderID TLV を転送します。
	• Defer - この MA が関連するメンテナンスドメインの設定を継承します。(初期値)
MEPID List	メンテナンスアソシエーションに含まれる MEP ID を指定します。
	初期値ぐは、初めく作成されたメンテナンスアソシエーションには MEP ID はありません。MEP ID の範囲は、   1-8191 です。
1	

項目設定後、「Apply」ボタンをクリックします。

## Add MEP 設定(CFM Settings)

MEP を追加します。

**OAM > CFM > CFM Settings** 画面で「Add MEP」ボタンをクリックし、以下の画面を表示します。

CFM MEP Settings					
CFM MEP Settings Domain Name MEPID (1-8191) Direction	domain	<b>v</b>	MA Name Port	ma 1 v eth1/0/1	Apply Back
Total Entries: 1					
MEPID	Port	Direction			
1 е	eth1/0/11	Up	Show Detail Remote MEP	Edit LCK Edit DM	Edit LM Delete

図 13-5 CFM MEP Settings 画面

画面に表示される項目:

項目	説明
MEP ID (1-8191)	MA の MEP ID リストに設定される MEP ID を入力します。
Port	プルダウンメニューを使用してポートを指定します。本ポートは MA の関連付けられている VLAN メンバである必要があり ます。CFM ハードウェアモードでは、本ポートは MA の関連付けられている VLAN のメンバである必要があります。
Direction	<ul> <li>MEP の方向を指定します。</li> <li>Up - 内向き (アップ) MEP。内向きの MEP は、内側から受信する同じかそれ以下のレベルにあるすべての CFM フレームを破棄します。そして、フレームの送信元が内向きまたは外向きにかかわらず、より高いレベルにあるすべての CFM フレームを転送します。</li> <li>Down - 外向き (ダウン) MEP。外向きのポートは、ブリッジリレー機能側から受信する同じかそれ以下のレベルにあるす べての CFM フレームを破棄します。それは、そのレベルにあるすべての CFM フレームを処理して、ブリッジポートから から受信する低いレベルの CFM フレームすべてを破棄します。外向きポートは、フレームの送信先の方向にかかわらず、より高いレベルにあるすべての CFM フレームを転送します。</li> </ul>

項目設定後、「Add」ボタンをクリックします。

「Apply」ボタンをクリックして行った変更を適用します。

「Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

## 詳細情報の参照(Show Detail)

「Show Detail」ボタンをクリックし、以下の画面を表示します。

Domain Name	domain			
MA Name	ma			
MEPID	1			
Mode	Software			
Port	eth1/0/11			
Direction	Up			
CFM Port Status	Disabled			
MAC Address	F0-7D-68-34-01-1A			
MEP State	Disabled			
DCM State	Disabled			
PDU Priority	7			
Fault Alarm	None			
Alarm Time	250 centisecond((1/100)s)			
Alarm Reset Time	1000 centisecond((1/100)s)			
Highest Fault	None			
AIS State	Disabled			
AIS Period	1 Second			
AIS Client Level	Invalid			
AIS Status	Not Detected			
LCK State	Disabled			
LCK Period	1 Second			
LCK Client Level	Invalid			
LCK Status	Not Detected			
CK Action	Stop			
Out-of-Sequence CCMs Received	0			
Cross-connect CCMs	0			
Error CCMs Received	0	Normal CCMs Received	0	
Port Status CCMs Received	0	If Status CCMs Received	0	
CCMs transmitted	0	In-order LBRs Received	0	
Out-of-order LBRs Received	0	Next LTM Trans ID	0	
Unexpected LTRs Received	0	LBMs Transmitted	0	
AIS PDUs Received	0	AIS PDUs Transmitted	0	
LCK PDUs Received	0	LCK PDUs Transmitted	0	

図 13-6 Show Detail Information 画面

#### MEP の編集

「Edit」ボタンをクリックし、以下の画面を表示します。

Domain Name	domain				
/A Name	ma				
MEPID	1				
Node	Software				
Port	eth1/0/11				
Direction	Up				
FM Port Status	Disabled				
AC Address	F0-7D-68-34-01-1A				
IEP State	Disabled 🗸	-			
CM State	Disabled 🗸				
DU Priority	7 🗸	•			
ault Alarm	None	-			
Jarm Time	250	centisecond((1/100)s)			
Narm Reset Time	1000	centisecond((1/100)s)			
lighest Fault	None				
US State	Disabled 🗸				
US Period	1 Second V				
US Client Level	0 ~				
US Status	Not Detected				
CK State	Disabled 🗸				
CK Period	1 Second 🗸				
CK Client Level	0 🗸				
CK Status	Not Detected				
CK Action	Stop				
Out-of-Sequence CCMs Received	0				
Cross-connect CCMs	0				
Error CCMs Received	0		Normal CCMs Received	0	
Port Status CCMs Received	0		If Status CCMs Received	0	
CCMs transmitted	0		In-order LBRs Received	0	
Out-of-order LBRs Received	0		Next LTM Trans ID	0	
Unexpected LTRs Received	0		LBMs Transmitted	0	
AIS PDUs Received	0		AIS PDUs Transmitted	0	
CK PDUs Received	0		LCK PDUs Transmitted	0	

図 13-7 CFM MEP Information 画面 - Edit

#### 画面に表示される項目:

項目	説明
MEP State	MEP 管理状態を「Enabled」(有効)/「Disabled」(無効)にします。初期値は「Disabled」です。
CCM State	CCM 送信状態を「Enabled」(有効)/「Disabled」(無効)にします。初期値は「Disabled」です。
PDU Priority	802.1p 優先度は MEP によって送信された CCM および LTM メッセージに設定されます。初期値は 7 です。
Fault Alarm	これは、MEP によって送信される障害アラームの制御タイプです。
	<ul> <li>All - すべての障害アラームのタイプが送信されます。</li> <li>MAC-Status - 優先度が「Some Remote MEP MAC Status Error」(リモート MEP の MAC ステータスエラー)以上である 障害アラームだけが送信されます。</li> <li>Remote-CCM - 優先度が「Some Remote MEP Down」(リモート MEP のダウン)以上である障害アラームだけが送信さ れます。</li> <li>Error-CCM - 優先度が「Error CCM Received」(エラー CCM の受信)以上である障害アラームだけが送信されます。</li> <li>Xcon-CCM - 優先度が「Cross-connect CCM Received」(クロスコネクト CCM の受信)以上である障害アラームだけが送 信されます。</li> <li>None 障害アラームは送信されません (初期値)</li> </ul>
Alarm Time (250-1000)	これは、障害検出後に障害アラームが送信されるまでの経過時間です。範囲は 250-1000(センチ秒)です。初期値は 250(センチ秒)です。
Alarm Reset Time (250-1000)	これは、障害による再度アラーム送信前の検知が始動されるまでの待機時間です。範囲は 250-1000(センチ秒)です。初期 値は 1000( センチ秒 ) です。
AIS State	チェックし、プルダウンメニューを使用して、AIS 機能を「Enabled」(有効)/「Disabled」(無効)にします。
AIS Period	チェックし、プルダウンメニューを使用して、AIS PDU 送信間隔を選択します。
AIS Client Level	チェックし、プルダウンメニューを使用して、MEP が AIS PDU を送信するクライアントレベル ID を選択します。クライア ント MD レベルの初期値は最も近いクライアントレイヤの MIP と MEP が存在する MD レベルです。オプションを 0-7 から を選択します。
LCK State	↓   チェックし、プルダウンメニューを使用して、LCK 機能を「Enabled」( 有効 )/「Disabled」( 無効 ) にします。

項目	説明
LCK Period	チェックし、プルダウンメニューを使用して、LCK PDU 送信間隔を選択します。
LCK Client Level	チェックし、プルダウンメニューを使用して、MEP が LCK PDU を送信するクライアントレベル ID を選択します。クライア ント MD レベルの初期値は最も近いクライアントレイヤの MIP と MEP が存在する MD レベルです。オプションを 0-7 から を選択します。

### Remote MEP (CFM Settings)

Remote MEP を参照します。

**OAM > CFM > CFM Settings** 画面で「Remote MEP」ボタンをクリックします。

CFM Remote MEP	
CFM Remote MEP Table	
	Back
Long Long and the second se	
Total Entries: 0	

図 13-8 Remote MEP 画面

「Back」をクリックすると前のページに戻ります。

#### Edit LCK (CFM Settings)

LCK を編集します。

**OAM > CFM > CFM Settings** 画面で「Edit LCK」ボタンをクリックします。

CFM LCK Setting	js	
CFM LCK Settings		
Domain Name	domain	
MA Name	ma	
MEPID	1	
Olata	Stop	Apply Back

図 13-9 Edit LCK 画面

ロック動作を「Start」「Stop」から指定します。これにより MEP においてクライアントレベル MEP に LCK PDU を送信します。

「Apply」をクリックし、設定内容を適用します。 「Back」をクリックすると前のページに戻ります。

## Edit DM (CFM Settings)

DM を編集します。

## **OAM > CFM > CFM Settings** 画面で「Edit DM」ボタンをクリックします。

CFM DM Settings			_			_	_	
CFM DM Settings								
Domain Name	domain		MA Name		ma			
MEPID	1		State		Disable	d 🔽		Apply
CFM DM Test								
Domain Name	domain		MA Name		ma			
MEPID	1		MAC Address		00-84-57	-00-00-00		
Period Interval	1sec-10	sec 🔽	Percentile		75			
PDU Priority	None	~						Apply
Clear CFM DM								
Domain Name	domain		MA Name		ma			
MEPID	1		Туре		Result	~		Clear Back
								Clear All
State	Enabled							
DMM Transmitted	10							
DMR Received	0							
DMM Received	0							
DMR Transmitted	0							
ID MAC Addre	SS	Status	Period:Interval	РСТ	Priority	FD nanosec	FDV nanosec	Start Time
1 00-11-22-33-4	4-55	Running	1s:10s	75	0	0	0	2015-12-01 10:20:38

図 13-10 Edit DM 画面

#### 画面に表示される項目:

項目	説明
	CFM DM Settings
State	「ITU Y.1731」フレーム「Delay Measurement」(DM) 機能を有効 / 無効に指定します。有効にすると MEP はタイムスタンプを 実行し、DMM メッセージ受信時に、DMR メッセージを返信できるようになります。
	CFM DM Test
MAC Address	MAC アドレスを指定します。
Period Interval	<ul> <li>DMM メッセージと診断の送信間隔を指定します。</li> <li>100ms-1sec - 送信間隔は 100 ミリ秒、診断間隔は 1 秒です。</li> <li>1sec-10sec - 送信間隔は 1 秒、診断間隔は 10 秒です。(初期値)</li> <li>10sec-1min - 送信間隔は 10 秒、診断間隔は 1 分です。</li> </ul>
Percentile	パーセンタイル値を指定します。「Frame Delay」(FD) と「Frame Delay Variation」(FDV) のパーセンタイル(0-100)を指定し ます。初期値は 75 です。
PDU Priority	PDU 優先値(0-7)を選択します。MEP に送信される DMM メッセージの 802.1p 優先値を指定します。
	Clear CFM DM
Туре	消去する情報の種類について指定します。 Result - DM 情報について消去します。 Statistics - 「ETH-DM」フレーム (DMM と DMR) の統計について消去します。

「Clear」をクリックすると入力したエントリをクリアします。 「Clear All」をクリックすると入力したエントリを全てクリアします。 「Back」をクリックすると前のページに戻ります。

## Edit LM (CFM Settings)

LM を編集します。

**OAM > CFM > CFM Settings** 画面で「Edit LM」ボタンをクリックします。

CFM LM Settings	_	_	_	_	_	_	
CFM LM Settings							
Domain Name	domain		MA Name	ma			
MEPID	1		State	Disa	abled 🗸		Apply
CFM LM Test							
Domain Name	domain		MA Name	ma			
MEPID	1		MAC Address	00-8	4-57-00-00-00	]	
Period	1sec	~	PDU Priority	Nor	e 🗸		Apply
Clear CFM LM							
Domain Name	domain		MA Name	ma			
MEPID	1		Туре	Res	ult 💌		Clear Back Clear All
State	Enabled						
LMM Transmitted	3						
LMR Received	0						
LMM Received	0						
LMR Transmitted	0						
ID MAC A	ddress	Status	Period	Priority	Far-End	Near-End	Start Time
1 00-11-22	-33-44-55	Running	1sec	0	0	0	2015-12-01 10:23:18

図 13-11 Edit LM 画面

画面に表示される項目:

項目	説明
	CFM LM Settings
State	「ITU Y.1731」フレーム「Loss Measurement」(LM) 機能を有効 / 無効に指定します。有効にすると MEP フレームロス計測の カウンタを維持し、LMM メッセージ受信時に、LMR メッセージを返信できるようになります。
	CFM LM Test
MAC Address	MAC アドレスを指定します。
Period	LM PDU の送信間隔を指定します。 • 100ms - 送信間隔は 100 ミリ秒です。 • 1sec - 送信間隔は 1 秒です。 • 10sec - 送信間隔は 10 秒です。
Percentile	パーセンタイル値を指定します。「Frame Delay」(FD) と「Frame Delay Variation」(FDV) のパーセンタイル(0-100)を指定し ます。初期値は 75 です。
PDU Priority	PDU 優先値(0-7)を選択します。MEP に送信される LMM メッセージの 802.1p 優先値を指定します。
	Clear CFM LM
Туре	消去する情報の種類について指定します。 Result - LM 情報について消去します。 Statistics -「ETH-LM」フレーム (LMM と LMR) の統計について消去します。
「Clear」をクリックす	ると入力したエントリをクリアします。

「Clear」をクリックすると入力したエントリをクリアします。 「Clear All」をクリックすると入力したエントリを全てクリアします。 「Back」をクリックすると前のページに戻ります。

## CFM Port Settings(CFM ポート設定)

CFM ポート状態を有効または無効にします。

**OAM > CFM > CFM Port Settings** の順にメニューをクリックし、以下の画面を表示します。

CFM Port S	ettings			
CFM Port Sett	ings			
Unit	From Port	To Port	State	
1~	eth1/0/1 🔽	eth1/0/1 🔽	Disabled	Apply
Unit 1 Setting	15			
	Port	State	MAC Address	
	eth1/0/1	Enabled	F0-7D-68-34-01-10	Show Detail
	eth1/0/2	Enabled	F0-7D-68-34-01-11	Show Detail
	eth1/0/3	Enabled	F0-7D-68-34-01-12	Show Detail
	eth1/0/4	Enabled	F0-7D-68-34-01-13	Show Detail
	eth1/0/5	Enabled	F0-7D-68-34-01-14	Show Detail
	eth1/0/6	Enabled	F0-7D-68-34-01-15	Show Detail
	eth1/0/7	Enabled	F0-7D-68-34-01-16	Show Detail
	eth1/0/8	Enabled	F0-7D-68-34-01-17	Show Detail

図 13-12 CFM Port Settings 画面

画面に表示される項目:

項目	説明
Unit	設定を行うユニットを指定します。
From Port/To Port	本設定に使用されるポート範囲を選択します。
State	特定ポートの CFM 設定を有効または無効にします。初期値は無効です。

「Apply」ボタンをクリックし、変更を有効にします。

「Show Detail」ボタンをクリックし、以下の画面を表示します。

FM Port Detail				_	_	_
CFM Port Detail						
Port	eth1/0/11					Back
State	Enabled					
1110 1 1 1 1 1 1 1	F0-7D-68-34-01-1A					
MAC Address						
MAC Address	omain Name	Level	MA Name	VID	MEPID	Direction

図 13-13 CFM Port Settings - Show Detail 画面

「Back」をクリックすると前のページに戻ります。

# CFM Loopback Test(CFM ループバックテスト)

CFM ループバックを設定します。

OAM > CFM > CFM Loopback Test の順にメニューをクリックし、以下の画面を表示します。

CFN	Loopback Test		l
CFM	Loopback Test		
۲	MAC Address	00-84-57-00-00	
0	Reomte MEPID (1-8191)		
	MEPID (1-8191)		
	MA Name	22 chars	
	Domain Name	22 chars	
	LBMs Number (1-65535)	4	
۲	LBM Payload Length (0-1500)	0	
0	LBM Payload Pattern	1500 chars	
	PDU Priority	None Apply	

図 13-14 CFM Loopback Settings 画面

画面に表示される項目:

項目	説明
MAC Address	宛先 MAC アドレスを入力します。
Remote MEPID (1-8191)	Remote MEP ID を入力します。
MEP ID (1-8191)	MEP ID を入力します。
MA Name	使用するメンテナンスアソシエーション名を指定します。
Domain Name	使用するメンテナンスドメイン名を指定します。
LBMs Number (1-65535)	送信する LBM 数を指定します。初期値は 4 です。1 ~ 65525 の範囲で指定します。
LBM Payload Length (0-1500)	送信される LBM のペイロード長を指定します。初期値は 0 です。
LBM Payload Pattern (Max: 1500 characters)	LBM のペイロードパターンを指定します。Data TLV が含まれるかどうかの指定と、Data TLV に含まれることになる任意の数のデータとなります。1500 字以内で指定し、スペースは許可されません。
PDU Priority	送信される LBM に設定される 802.1p 優先度(0-7)を指定します。指定しない場合、MA が送信した CCM と LTM と同じ優先度を使用します。初期値は「None」(なし)です。

「Apply」ボタンをクリックし、変更を有効にします。

## CFM Linktrace Settings (CFM リンクトレース設定)

CFM リンクトレースを設定します。

#### **OAM > CFM > CFM Linktrace Settings** の順にメニューをクリックし、以下の画面を表示します。

CFM Linktrace S	ettings	_			_	_
CFM Linktrace Settin	gs					
MAC Address	00-84-57-0	00-00-00	MEPID (1-8191)			
MA Name	22 chars		Domain Name	22 chars		
TTL (2-255)	64		PDU Priority	None		Apply
Find and Clear CFM L	Linktrace					
MEPID (1-8191)			MA Name	22 chars		
Domain Name	22 chars				Find	Clear
						Clear All
Transacti	on ID	MEPID	MAC Address	Start Time		
0		1	00-11-22-33-44-55	2015-12-01 10:53	41	Show Detail

図 13-15 CFM Linktrace Settings 画面

#### 画面に表示される項目:

項目	説明
	CFM Linktrace Settings
MAC Address	送信先 MAC アドレスを入力します。
MEP ID (1-8191)	使用するエンドポイント ID を指定します。
MA Name	使用するメンテナンスアソシエーション名を指定します。
Domain Name	使用するメンテナンスドメイン名を指定します。
TTL (2-255)	リンクトレースメッセージの TTL 値。初期値は 64 です。範囲は 2-255 です。
PDU Priority	送信される LTM に設定される 802.1p 優先度(0-7)。指定しない場合、MEP が送信した CCM と同じ優先度を使用します。
	Find and Clear CFM Linktrace
MEP ID (1-8191)	使用するエンドポイント ID を指定します。
MA Name	使用するメンテナンスアソシエーション名を指定します。
Domain Name	使用するメンテナンスドメイン名を指定します。

「Apply」ボタンをクリックし、変更を有効にします。 「Clear」をクリックすると入力したエントリをクリアします。

「Clear All」をクリックすると入力したエントリを全てクリアします。

#### エントリの参照

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

検出後、「Show Detail」リンクをクリックすると、CFM リンクトレースの詳細情報が表示されます。

CFM Linktrace S	ettings			
CFM Linktrace Settin	gs			
Transaction ID	0			Back
From MEPID	1			
То	00-11-22-33-44-55			
Start Time	2015-12-01 10:53:42			
Hop MEPID	Ingress MAC Address	Egress MAC Address	Forwarded	Relay Action

図 13-16 CFM Linktrace Settings 画面

「Back」をクリックすると前のページに戻ります。

## CFM Packet Counter (CFM パケットカウンタ)

OSPF パケットカウンタ情報を表示します。CFM ハードウェアモードにおける MEP の CCM パケット統計情報はカウントしません。

**OAM > CFM > CFM Packet Counter** の順にメニューをクリックし、以下の画面を表示します。

M Packe	t Counter		_	_	_	_	_	_	_	_	_	_	_	
M Packet C	ounter Table													
Init	1 🔽	] F	Port	eth1/0/1	✓ ту	pe	All 🔽	1				Find		lear
								<sup>1</sup>				Show All	Cle	ar All
Init 1 Setting	js													
Deat		6. (		CFM RX	Statistics						CFM TX	Statistics		
Роп	AllPkt	ССМ	LBR	LBM	LTR	LTM	VidDrop	OpcoDrop	AllPkt	ССМ	LBR	LBM	LTR	LTM
eth1/0/1	0	0	0	0	0	0	0	0	72	0	0	0	0	0
eth1/0/2	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth1/0/3	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth1/0/4	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth1/0/5	0	0	0	0	0	0	0	0	72	0	0	0	0	0
eth1/0/6	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth1/0/7	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth1/0/8	0	0	0	0	0	0	0	0	0	0	0	0	0	0

図 13-17 CFM Packet Counter 画面

画面に表示される項目:

項目	説明
Unit	設定を行うユニットを指定します。
Port	参照するポートを選択します。
Туре	<ul> <li>RX - 受信したすべての CFM パケットを表示します。</li> <li>TX - 送信したすべての CFM パケットを表示します。</li> <li>All - 送受信したすべての CFM パケットを表示します。</li> </ul>

参照するポート番号を入力し、「Find」ボタンをクリックします。 「Clear」ボタンをクリックして、本欄に入力したすべてのエントリをクリアします。 「Clear All」をクリックすると入力したエントリを全てクリアします。 「Show All」をクリックして、すべてのエントリを表示します。

## CFM Counter CCM(CFM カウンタ CCM)

CFM カウンタ CCM 情報を表示します。

OAM > CFM > CFM Counter CCM の順にメニューをクリックし、以下の画面を表示します。

M Counter CCM T	able						
							Clear
otal Entries: 1							
MCDID	VID	Level	Direction	Port	XCON	Error	Normal
MEPID							
MEPID 1	1	0	Up	eth1/0/11	0	0	0
1	1	0	Up	eth1/0/11 Total	0	0	0

図 13-18 CFM Counter CCM 画面

「Clear」をクリックすると入力したエントリをクリアします。 設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

## CFM MIP CCM Table (CFM MIPCCM テーブル)

CFM MIPCCM 情報を表示します。

OAM > CFM > CFM MIP CCM Table の順にメニューをクリックし、以下の画面を表示します。

CFM MIPCCN	/I Table			O Safeguard
Total Entries: 0				
MA	VID	MAC Address	Port	

図 13-19 CFM MIP CCM Table 画面

## CFM MEP Fault Table (CFM MEP 障害テーブル)

CFM MEP 障害テーブルを表示します。

OAM > CFM > CFM MEP Fault Table の順にメニューをクリックし、以下の画面を表示します。

CFM MEP Fault Table		_	_		
CFM MEP Fault Table					
Total Entries: 0					
Domain Name	MA Name	MEPID	Status	AIS Status	LCK Status

図 13-20 CFM MEP Fault Table 画面

# Cable Diagnostics (ケーブル診断機能)

スイッチの特定のポートに接続する UTP ケーブルの詳細について表示します。ケーブルにエラーがある場合、エラーのタイプと発生箇所を判断します。ケーブル診断機能は UTP ケーブルを簡易的に確認するために設計されています。ケーブルの品質やエラーの種類を診断します。

注意 ケーブル診断機能は簡易機能であり、参考としてご利用ください。正確な検査やテストのためには専用のテスタを使用して行ってください。

OAM > Cable Diagnostics の順にメニューをクリックし、以下の画面を表示します。

ble Diagnostics					
ble Diagnostics					
nit	From Port		To Port		
~	eth1/0/1	$\checkmark$	eth1/0/1		Test
nit 1 Settings					Clear All
Port	Туре	Link Status	Test Result	Cable Length (M)	
			Pair 1 Open at 0M		
	1000405 T	Link Up	Pair 2 Ok at 5M		chara
eth1/0/1	10GBASE-1		Pair 3 Ok at 6M		Clear
			Pair 4 Open at 0M		
eth1/0/2	10GBASE-T	Link Down	-	-	Clear
eth1/0/3	10GBASE-T	Link Down		•	Clear
eth1/0/4	10GBASE-T	Link Down	-	•	Clear
eth1/0/5	10GBASE-T	Link Up	-	•	Clear

図 13-21 Cable Diagnostics 画面

特定のポートに対するケーブル診断を表示するためには、プルダウンメニューを使用して設定するユニットとポートを選択し、「Test」ボタンをクリックします。情報が画面に表示されます。

「Clear」ボタンをクリックし、指定ポートの情報を消去します。

「Clear All」ボタンをクリックし、テーブル上のすべての情報を消去します。

注意 ケーブル診断を実行すると、対象のポートにおいてリンクダウンを伴います。

#### ケーブル診断機能の制限;

- ・ GE ポートのみサポート
- ・ 最大対応ケーブル長 120 メートル
- ケーブル長の誤差±5メートル

# Ethernet OAM(イーサネット OAM)

ポートに対するイーサネット OAM モード、イベントの設定や、ログの参照を行います。

## Ethernet OAM Settings(イーサネット OAM 設定)

ポートにイーサネット OAM モードを設定します。

#### OAM > Ethernet OAM > Ethernet OAM Settings の順にメニューをクリックし、以下の画面を表示します。

thernet OAM Setting	js		
Ethernet OAM Settings			
Unit	From Port	To Port	
1 🗸	eth1/0/1 🗸	eth1/0/1	
State	Mode	1.1.	
Disabled 🗸	Active		Apply
Received Remote Loopback	Remote Loopback		(A-16)
Ignore 🗸	Start		Apply
Unit F	rom Port To Port eth1/0/1 🔽 eth1/0/1	V	Find Show All
		Ethernet1/0/1	
		Local Client	
	Admin State		Disabled
	Mode		Active
	Max OAMPDU size		1518 bytes
	Remote loopback		Supported

図 13-22 Ethernet OAM Settings 画面

#### 画面に表示される項目:

項目	説明
	Ethernet OAM Settings
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。
State	OAM 機能を有効または無効にします。初期値は無効です。
	本機能を有効化すると、インタフェースでOAMディスカバリが開始されます。OAMモードが Active 状態の場合、ディ
	スカバリが開始され、それ以外の場合、ビアから受信したディスカバリに反応します。
Mode	動作するモード(「Active」または「Passive」)を指定します。初期モードは「Active」です。
	Active モードでは、次の 2 つのアクションが許可されます。Passive モードでは許可されません。
	(1)OAM discovery の開始
	(2)リモートループバックの開始 / 停止
Received Remote Loopback	クライアントが受信したイーサネット OAM リモートループバックコマンドの処理を指定します。
	• Process - 受信したイーサネット OAM リモートループバックコマンドを処理します。
	<ul> <li>Ignore - 受信したイーサネット OAM リモートループバックコマンドを無視します。(初期値)</li> </ul>
	リモートループバックモードでは、全てのユーザトラフィックが処理されます。受信したリモートループバック機
	能を無視すると、ポートがリモートループバックモードに移行することが回避されます。
Remote Loopback	<ul> <li>Start - リモートループバックモードに変更するようにピアに要求します。</li> </ul>
	• Stop - 通常の操作モードに変更するようにピアに要求します。
	リモートピアがリモートループバック要求を無視するように設定されている場合、要求を受信してもリモートルー
	プバックモードへの移行や離脱を行いません。リモートピアがリモートループバックモードへ移行するには、ロー
	カルクライアントが Active モードかつ OAM 接続が確立されている必要があります。ローカルクライアントが既に
	リモートループバックモードの場合、本機能は適用されません。
	Ethernet OAM Table
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。

「Apply」ボタンをクリックし、変更を有効にします。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Show All」をクリックして、すべてのエントリを表示します。

## Ethernet OAM Configuration Settings(イーサネット OAM コンフィグレーション設定)

ポートにイーサネット OAM のイベントを設定します。

**OAM > Ethernet OAM > Ethernet OAM Configuration Settings**の順にメニューをクリックし、以下の画面を表示します。

thernet OAM Cor	figuration Settings				
Ethernet OAM Configur	ation Settings				
Linit	From Port	To Port	Dving Gash	Critical Event	
1	ath1/0/1	oth1/0/1	Disabled	Disabled	
1				Disabled	
Link Monitor	Notity State	Inresnold (0-4294967295)	Window (10-600)		
Error Symbol	Enabled	1	10	Deciseconds Apply	
Ethernet OAM Configur	ation Table				
Unit	From Port	To Port			
1	eth1/0/1	✓ eth1/0/1		Find Show All	
		Ethernet1/	0/1		
	Ethernet oam state			Disabled	
	Mode		Active		
	Dying gasp			Enabled	
	Critical event			Enabled	
	Remote loopback OAMPDU		Not Processed		
		Error symbol per	iod event		
	Notify state			Enabled	
Threshold			1 Error Symbol		
	Window			10 deciseconds	
		Error frame e	event		
	Notify state			Enabled	
	Threshold			1 Error Frame	

図 13-23 Ethernet OAM Configuration Settings 画面

#### 画面に表示される項目:

項目	説明
	Ethernet OAM Configuration Settings
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポート範囲を指定します。
Dying Gasp	「Dying Gasp」を有効 / 無効に指定します。リモートデバイスの電源障害など回復不可能なイベントの発生の検出を指定します。
Critical Event	イーサネット OAM のクリティカルなリンクイベント機能を有効 / 無効に指定します。イベント機能が無効になると、ポートは対応するクリティカルなリンクイベントを送信しません。
Link Monitor	ポートにイーサネット OAM リンクモニタリング (Error Symbol) を設定します。リンクモニタリング機能は、さまざまな条件のもとでリンク障害を検出して示すメカニズムを提供します。OAM はコード化されたシンボルのエラー数と共にフレーム エラー数により統計情報をモニタリングします。シンボルエラー数が、期間内に定義したしきい値以上になる場合およびイ ベント通知状態 (Notify) が有効になる場合、リモート OAM ピアに通知するエラーシンボル期間のイベントを生成します。使 用可能オプションは、Error Symbol、Error Frame、Error Frame Period、および Error Frame Second です。
Notify State	イベント通知を有効または無効にします。初期値は有効です。
Threshold (0-4294967295)	イベント生成のためには、期間内に要求以上のにシンボルエラー数を指定します。しきい値は 0 - 4294967295 の範囲です。 初期値は 1 です。
Window (1000-6000)	エラーフレームまたはシンボルのサマリイベントの期間(デシ秒)を入力します。
	Ethernet OAM Configuration Table
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポート範囲を指定します。

「Apply」ボタンをクリックし、設定を有効にします。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Show All」をクリックして、すべてのエントリを表示します。

## Ethernet OAM Event Log Table(イーサネット OAM イベントログテーブル)

ポートのイーサネット OAM イベントログ情報を表示します。

**OAM > Ethernet OAM > Ethernet OAM Event Log Table** の順にメニューをクリックし、以下の画面を表示します。

		Port		Action					
	~	eth1/0/1	~	Find	~				Find
					Ethernet	I/0/1 Records Stat	istics		
		Lin	ik Fault		0			Link Fault	0
Local Faults Dying		ng Gasp		0	Remo	Remote Faults	Dying Gasp	0	
	Critical Event			0			Critical Event	0	
Errored Symb		d Symbol		0			Errored Symbol	0	
		Error	ed Frame		0	Demote	Description of the second	Errored Frame	0
Local even	tLogs	Errored F	Frame Peri	od	0	Remote event Logs		Errored Frame Period	0
	Errored Frame Second		ond	0	0		Errored Frame Second	0	
otal Entries: (	)								
					Etherne	1/0/1 Event Log T	able		
Index	Loc	ation	Гуре	Time	Stamp	Value	Window	Threshold	Accumulated Errors

図 13-24 Ethernet OAM Event Log Table 画面

画面に表示される項目:

項目	説明
Unit	参照するユニットを指定します。
Port	参照するポート番号を選択します。

参照するポート番号またはポートリストを指定し、「Action」で「Find」を指定します。

エントリを削除するためには、適切な情報を入力して、「Action」で「Clear」ボタンをクリックします。

## Ethernet OAM Statistics Table(イーサネット OAM 統計情報テーブル)

スイッチの各ポートに関するイーサネット OAM 統計情報を表示します。

OAM > Ethernet OAM > E	Ethernet OAM Statistics	Table の順にメニ	ューをクリックし、	以下の画面を表示します。
------------------------	-------------------------	-------------	-----------	--------------

thernet OAM Statistics Table			
Ethernet OAM Statistics Table			
Unit From Port 1 V eth1/0/1 V	To Port Acti eth1/0/1 Fin	on d	Find Show All
	Eti	hernet1/0/1	
Information OAMPDU TX	0	Information OAMPDU RX	0
Unique event notification OAMPDU TX	0	Unique event notification OAMPDU RX	0
Duplicate event notification OAMPDU TX	0	Duplicate event notification OAMPDU RX	0
Loopback control OAMPDU TX	0	Loopback control OAMPDU RX	0
Variable request OAMPDU TX	0	Variable request OAMPDU RX	0
Variable response OAMPDU TX	0	Variable response OAMPDU RX	0
Organization specific OAMPDU TX	0	Organization specific OAMPDU RX	0
Unsupported OAMPDU TX	0	Unsupported OAMPDU RX	0
Frame lost due to OAM	0		
	Eti	hernet1/0/2	25
Information OAMPDU TX	0	Information OAMPDU RX	0
Unique event notification OAMPDU TX	0	Unique event notification OAMPDU RX	0

図 13-25 Ethernet OAM Statistics Table 画面

画面に表示される項目:

項目	説明
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。

参照するポート番号またはポートリストを指定し、「Action」で「Find」を指定します。 エントリを削除するためには、適切な情報を入力して、「Action」で「Clear」ボタンをクリックします。
### Ethernet OAM DULD Settings(イーサネット OAM DULD 設定)

本項目では Ethernet OAM「D-Link Unidirectional Link Detection」(DULD)の設定、表示を行います。DULD は「802.3ah」イーサネット OAM の拡張 機能です。PHY サポート外の単方向「ポイント to ポイント」イーサネットリンクの検出を行います。OAM ベンダの仕様メッセージが検出に使用さ れます。検出のプロセスは OAM ディスカバリの開始後、設定のディスカバリ時間内でのネゴシエーションを完了していない状態で開始します。

OAM > Ethernet OAM > Ethernet OAM DULD Settings の順にメニューをクリックし、以下の画面を表示します。

hernet OAM DULD Se	ttings				
Recovery Time (0,60-10	00000) 60	sec			Apply
Jnit	From Port	To Port	Admin State	Action	Discovery Time (5-65535)
1 🗸	eth1/0/1	eth1/0/1	Disabled 🗸	Normal	5 sec Apply
Port	Admin State	Oper Status	Action	Link Statu	s Discovery Time(Sec)
Ethernet1/0/1	Disabled	Disabled	Normal	Unknown	5
Ethernet1/0/2	Disabled	Disabled	Normal	Unknown	5
	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Disabled	Normal	Unknown	5
Ethernet1/0/3	Disabled	Discorda			
Ethernet1/0/3 Ethernet1/0/4	Disabled	Disabled	Normal	Unknown	5
Ethernet1/0/3 Ethernet1/0/4 Ethernet1/0/5	Disabled Disabled Disabled	Disabled Disabled	Normal	Unknown Unknown	5

図 13-26 Ethernet OAM DULD Settings 画面

#### 画面に表示される項目:

項目	説明
	Ethernet OAM DULD Settings
Recovery Time	DULD によって無効化されたポートの回復にかかる時間間隔を指定します。設定時間が過ぎると DULD による無効ポートは自動的に回復します。「0」は本機能の無効を意味します。「0」または「60」から「1000000」(秒)で設定します。
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。
Admin State	プルダウンメニューか選択ポートの単方向リンク検出状態を「Enabled」(有効)または「Disabled」(無効)に設定します。
Action	プルダウンメニューを使用してモード(「Shutdown」および「Normal」)を選択します。 ・ Shutdown - 単方向のリンクが検出されると、ポートを無効にしてイベントをログに出力します。 ・ Normal - 単方向のリンクが検出した場合にイベントを単にログに出力します。
Discovery Time (5-65535)	これらのポートの Neighbor 検出時間を入力します。検出がタイムアウトになると、単方向リンク検出が開始します。
	Ethernet OAM DULD Table
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。

「Apply」をクリックし、設定内容を適用します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Show All」をクリックして、すべてのエントリを表示します。

### DDM(DDM 設定)

本フォルダにはスイッチに Digital Diagnostic Monitoring(DDM)機能を実行する画面があります。これらの画面により、スイッチに挿入した SFP モジュールの DDM 状態の参照、各種設定(アラーム設定、警告設定、温度しきい値設定、電圧しきい値設定、バイアス電流しきい値設定、Tx(送信) 電力しきい値設定、および Rx(受信)電力しきい値設定)を行うことができます。

### DDM Settings(DDM 設定)

超過しているアラームしきい値または警告しきい値を超過するイベントが発生した場合に、指定ポートに行う動作を設定します。

OAM > DDM > DDM Settings の順にメニューをクリックし、以下の画面を表示します。

DDM Settings				
DDM Global Settings Transceiver Monitoring Traps Alarm Transceiver Monitoring Traps Warning	Disabled      Enabled     Disabled      Enabled			Apply
DDM Shutdown Settings Unit From Port	To Port eth1/0/1	State Disabled V	Shutdown	Apply
Port		State	Shutdo	- mu
eth1/0/21		Disabled	None	
eth1/0/22		Disabled	None	3
eth1/0/23	1	Disabled	None	9
eth1/0/24	1	Disabled	None	•
eth1/0/25		Disabled	None	9
eth1/0/26		Disabled	None	e

図 13-27 DDM Settings 画面

画面に表示される項目:

項目	説明
Transceiver Monitoring Traps	アラームしきい値を超過した際にトラップを送信するか否かを指定します。
Alarm	
Transceiver Monitoring Traps	警告しきい値を超過した際にトラップを送信するか否かを指定します。
Warning	
Unit	設定するユニットを選択します。
From Port / To Port	設定するポート範囲を指定します。
State	DDM の状態を有効または無効にします。
Shutdown	操作パラメータが Alarm または Warning しきい値を超過した際に、ポートをシャットダウンするか否か指定し
	ます。「None」を選択するとしきい値の超過に関わらずシャットダウンは実行されません。初期値になります。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

### DDM Temperature Threshold Settings (DDM 温度しきい値設定)

スイッチの特定ポートに DDM 温度しきい値設定を行います。

**OAM > DDM > DDM Temperature Threshold Settings**の順にメニューをクリックし、以下の画面を表示します。

nit vit 1 Settings	eth1/0/1	Action Type Add V Low Alar	Value (-128-127.)	996) Celsius	Apply
Port	Current	High Alarm (Celsius)	High Warning (Celsius)	Low Warning (Celsius)	Low Alarm (Celsius)

図 13-28 DDM Temperature Threshold Settings 画面

画面に表示される項目	:
------------	---

項目	説明
Unit	設定するユニット番号を指定します。
Port	適用するポートを指定します。
Action	作動する動作について指定します。「Add」「Delete」から指定できます。
Туре	温度しきい値の種類について指定します。「High Alarm」「Low Alarm」「High Warning」「Low Warning」から指定 できます。
Value	温度しきい値の値について指定します。「-128」から「127.996」(℃)までの間で指定可能です。
設定を変更する際は、必ず「App	

### DDM Voltage Threshold Settings (DDM 電圧しきい値設定)

スイッチの特定ポートに電圧しきい値を設定します。

#### **OAM > DDM > DDM Voltage Threshold Settings** の順にメニューをクリックし、以下の画面を表示します。

nit vit 1 Settings	Port eth1/0/1	Action Type Add V Low Alarn	Value (U-6.55)	V	Apply
Port	Current	High Alarm (V)	High Warning (V)	Low Warning (V)	Low Alarm (V)

図 13-29 DDM Voltage Threshold Settings 画面

画面に表示される項目:

項目	説明
Unit	設定するユニット番号を指定します。
Port	適用するポートを指定します。
Action	作動する動作について指定します。「Add」「Delete」から指定できます。
Туре	電圧しきい値の種類について指定します。「High Alarm」「Low Alarm」「High Warning」「Low Warning」から指定できます。
Value	電圧しきい値の値について指定します。「0」から「6.55」(V)までの間で指定可能です。
Value	

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

### DDM Bias Current Threshold Settings (DDM バイアス電流しきい値設定)

スイッチの特定ポートにバイアス電流しきい値を設定します。

**OAM > DDM > DDM Bias Current Threshold Settings**の順にメニューをクリックし、以下の画面を表示します。

Jnit 1 🔽	Port eth1/0/1	Action Type Add V Low	y Alarm	0-131) mA	Apply
Port	Current	High Alarm (mA)	High Warning (	mA) Low Warning (mA)	Low Alarm (mA)

図 13-30 DDM Bias Current Threshold Settings 画面

画面に表示される項目:	
項目	説明
Unit	設定するユニット番号を指定します。
Port	適用するポートを指定します。
Action	作動する動作について指定します。「Add」「Delete」から指定できます。
Туре	電流しきい値の種類について指定します。「High Alarm」「Low Alarm」「High Warning」「Low Warning」から指定できます。
Value	電流しきい値の値について指定します。「0」から「131」(mA)までの間で指定可能です。
設定を変更する際は、必ず	、 「Apply」ボタンをクリックし、設定内容を適用してください。

### DDM TX Power Threshold Settings (DDM 送信電力しきい値設定)

スイッチの特定ポートに送信電力しきい値を設定します。

#### **OAM > DDM > DDM TX Power Threshold Settings** の順にメニューをクリックし、以下の画面を表示します。

it 🔽	Port eth1/0	1 🗸	Action Add	Type Low Al	arm 💌	Power Unit	Va	alue (0-6.5535)	mW	Apply
t i Settings	Cı	irrent	High	Alarm	High	Warning	Low	Varning	Low	Alarm
D					and the second se	and a second sec	(common and	000000000000000000000000000000000000000		1 Contraction
Port	mW	dBm	mW	dBm	mW	dBm	mW	dBm	mW	dBm

図 13-31 DDM TX Power Threshold Settings 画面

#### 画面に表示される項目:

項目	説明
Unit	設定するユニット番号を指定します。
Port	適用するポートを指定します。
Action	作動する動作について指定します。「Add」「Delete」から指定できます。
Туре	送信電力しきい値の種類について指定します。「High Alarm」「Low Alarm」「High Warning」「Low Warning」から指定できます。
Power Unit	送信電力単位について指定します。「mW」「dBm」から指定できます。
Value	送信電力しきい値の値について指定します。 「Power Unit」で「mW」を選択した場合、「0」から「6.5535」の間で指定します。「dBm」を選択した場合、「-40」か ら「8.1647」までの間で指定可能です。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

### DDM RX Power Threshold Settings(DDM 受信電力しきい値設定)

スイッチの特定ポートに受信電力しきい値を設定します。

**OAM > DDM > DDM RX Power Threshold Settings** の順にメニューをクリックし、以下の画面を表示します。

it	Port	Action	Туре		Power Unit		Value (0-6.55	35)		
~	eth1/0/1	Add 🗸	Low Alarm	~	mW 🕓	-		mW		Apply
A Cattings										
t 1 Settings										
	Cu	rrent	High #	Alarm	High V	Warning	Low	Warning	Low	v Alarm
Port	Cu mW	rrent dBm	High A mW	Alarm dBm	High V mW	Varning dBm	Low mW	Warning dBm	Lov mW	r Alarm dBm

図 13-32 DDM RX Power Threshold Settings 画面

#### 画面に表示される項目:

項目	説明
Unit	設定するユニット番号を指定します。
Port	適用するポートを指定します。
Action	作動する動作について指定します。「Add」「Delete」から指定できます。
Туре	受信電力しきい値の種類について指定します。「High Alarm」「Low Alarm」「High Warning」「Low Warning」から指定できます。
Power Unit	受信電力単位について指定します。「mW」「dBm」から指定できます。
Value	受信電力しきい値の値について指定します。「Power Unit」で「mW」を選択した場合、「0」から「6.5535」の間で指
	定します。「dBm」を選択した場合、「-40」から「8.1647」までの間で指定可能です。
シーンボーンボー	

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

### DDM Status Table (DDM ステータステーブル)

指定ポートで現在操作中の DDM パラメータと SFP モジュールの値を表示します。

#### **OAM > DDM > DDM Status Table** の順にメニューをクリックし、以下の画面を表示します。

A Status I	able						
otal Entries	s: 1						
Deat Townships (Outstan)	Temperature (Coleine)		Diae Current (m&)	TX Power	Power	RX Power	
POIL	remperature (Cersius)	voltage (v)	Dias Current (IIIA)	mW	dBm	mW	dBm
eth1/0/21	25.496	3.315	0.225	0.034	-14.681	0.000	-

図 13-33図 13-8 DDM Status Table 画面

#### 画面に表示される項目:

項目	説明
Port	ポート番号を表示します。
Temperature	ポートの現在の温度を表示します。
Voltage	ポートの現在の電圧を表示します。
Bias Current	ポートの現在のバイアス電流を表示します。
TX Power	ポートの現在の送信電力を表示します。
RX Power	ポートの現在の受信電力を表示します。

# 第 14 章 MPLS (MI モードのみ)

以下は MPLS サブメニューの説明です。必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明
MPLS LDP Information Settings(MPLS LDP 情報設定)	「Multiprotocol Label Switching」(MPLS) の「Label Distribution Protocol」(LDP) 情報の設定を行います。
MPLS LSP Trigger Information(MPLS LSP トリガ情報)	「Multiprotocol Label Switching」(MPLS) の「Label-Switched Label-Switched Path」(LSP) トリガ情報の設定 を行います。
MPLS Forwarding Settings(MPLS フォ ワーディング設定)	MPLS フォワーディングの設定を行います。
MPLS LDP Neighbor Password Settings (MPLS LDP ネイバパスワード設定)	MPLS LDP ネイバパスワードの設定を行います。
MPLS LDP Neighbor Targeted Settings (MPLS LDP ネイバターゲット設定)	MPLS LDP ネイバターゲットの設定を行います。
MPLS LDP Neighbor Information (MPLS LDP ネイバ情報)	MPLS LDP Neighbor Information(MPLS LDP ネイバ情報)の表示をします。
MPLS Global Settings(MPLS グローバ ル設定)	MPLS Global Settings(MPLS グローバル設定)の設定を行います。
MPLS LDP Interface Settings(MPLS LDP インタフェース設定)	MPLS LDP Interface Settings(MPLS LDP インタフェース設定)の設定をします。
MPLS LDP Session Information(MPLS LDP セッション情報)	MPLS LDP Session Information(MPLS LDP セッション情報)の検出、表示をします。
MPLS LDP Statistic (MPLS LDP スタティ スティック)	MPLS LDP Statistic(MPLS LDP スタティスティック)の表示をします。
MPLS LDP Binding Table(MPLS LDP バインディングテーブル)	MPLS LDP Binding Table(MPLS LDP バインディングテーブル)の表示をします。
MPLS LDP Discovery Information (MPLS LDP ディスカバリ情報)	MPLS LDP Discovery Information(MPLS LDP ディスカバリ情報)の表示をします。
MPLS QoS Settings(MPLS QoS 設定)	MPLS QoS Settings(MPLS QoS 設定)の設定、表示をします。
Ping MPLS	指定 FEC の LSP の接続状態を確認します。
Traceroute MPLS IPv4(トレースルー ト MPLS IPv4)	指定 FEC の LSP パストレースのような「hop-by-hop fault localization」を指定します。

注意 MPLS については MI モードのみとなっています。

# MPLS LDP Information Settings(MPLS LDP 情報設定)

本項目では、「Multiprotocol Label Switching」(MPLS)「Label Distribution Protocol」(LDP) 情報の設定、表示を行います。

MPLS > MPLS LDP Information Settings の順にメニューをクリックし、以下の画面を表示します。

MPLS LDP Information Set	tings				
MPLS LDP Information Settings					
LSR ID	10 - 90 - 90 - 90	Default	LDP Version	1.0	
LDP State	Disabled 🗸		TCP Port	646	
UDP Port	646		Max PDU Length	1500	
Initial Backoff (15-65535)	15 sec	Default	Max Backoff (120-65535)	600 sec	Default
Transport Address	10 - 90 - 90 - 90	Default Interface	Keep-Alive Time (15-65535)	40 sec	Default
Link Hello Interval (1-65535)	5 sec	Default	Link Hello Hold Time (5-65535)	15 sec	Default
Hello Source Address Type	Interface 🗸		Hello Source Address		
Distribution Method	DU 🗸	Default	LSP Control Mode	Independent 🗸	Default
Label Retention Mode	Liberal 🗸	Default	Loop Detection	Disabled 🗸	
Path Vector Limit (1-255)	254	Default	Hop Count Limit (1-255)	254	Default
Authentication	Disabled 🗸		PHP	Implicit Null	
Trap Status	Disabled 🗸		Graceful Restart	Disabled 🗸	
Neighbor Liveness Time (5-300)	120 sec	Default	Recovery Time (12-600)	300 sec	Default
					Apply

図 14-1 MPLS LDP Information Settings 画面

#### 画面に表示される項目:

項目	説明
LSR ID	LSR ID を指定します。LSR ID はインタフェースの IPv4 アドレスであり、MPLS ネットワークで LSR を特定するのに
	使用されます。「Default」を指定すると初期設定を使用します。
LDP Version	LDP バージョンが表示されます。
LDP State	LDP を「Enabled」(有効)/「Disabled」(無効)に指定します。
TCP Port	LDP TCP ポートが表示されます。
UDP Port	LDP UDP ポートが表示されます。
Max PDU Length	最大 LDP PDU 長が表示されます。
Initial Backoff	初期バックオフ時間を入力します。LDP バックオフメカニズムは、互換性なく設定された 2 つの LSR が、セッショ
	ン確立失敗という無限のシーケンスに陥ることを防ぎます。セッション確立の試みが非互換性のために失敗するな
	ら、アクティブな LSR は次の試みを遅らせて、セッション確立を再試行します。この値は 15-65535(秒)である必
	要があります。「Default」を選択すると初期値(15 秒)を指定します。
Max Backoff	最大のバックオフ時間を入力します。この値は 120-65535(秒)である必要があります。「Default」を選択すると初
	期値(600 秒)を指定します。
Transport Address	トランスポート IPv4 アドレスを選択します。トランスポートアドレスは、LDP TCP 接続を確立するのに使用されます。
	「Interface」をトランスポートアドレスとして設定すると、各インタフェースの IP アドレスがトランスポートアドレ
	スとして使用されます。「Default」を選択すると初期値を指定します。
Keep-Alive Time	キープアライブ時間を入力します。LDP は各ピアセッションのためにキープアライブタイマを保持します。キープ
	アライブタイマがピアからの LDP PDU の受信なしで期限が切れると、LDP はピアが失敗したと結論づけて、LDP セッ
	ションを終えます。各 LSR は、セッションをアクティブに保つために一定の間隔を置いて LDP ピアにキープアライ
	ブメッセージを送信します。この値は 15-65535 (秒) である必要があります。「Default」を選択すると初期値(40)
	を指定します。
Link Hello Interval	Hello メッセージを送信する間隔を入力します。この値は 1-65535( 秒 ) である必要があります。「Default」を選択す
	ると初期値(5)を指定します。
Link Hello Hold Time	Helloの保持時間を入力します。この値は 5-65535(秒)である必要があります。「Default」を選択すると初期値(15)
	を指定します。
Hello Source Address Type	Helloパケットの送信元アドレスタイプを指定します。
	・ Interface - 各インタフェースの IP アドレスを指定します。
	・ Router ID - LSR ID ( ルータ ID) を指定します。
	・ IP Address - 手動で入力した IP アドレスを指定します。
Hello Source Address	Hello パケットの送信元アドレスとなる IP アドレスを指定します。

項目	説明
Distribution Method	配布方式を選択します。「Default」を選択すると初期値(DU)を指定します。
	・ DU - 配布モードを「Downstream-Unsolicited」に設定します。
	・ DoD - 配布モードを「Downstream-on-Demand」に設定します。
	「Downstream-on-Demand」に設定されると、ダウンストリーム LSR はアップストリームの接続が行き過ぎたリク
	エストをした場合、ラベルマッピングを通知します。「Downstream-Unsolicited」に設定されると、ダウンストリー
	ム LSR はルーティングテーブルでラベルが学習されるとラベルマッピングを通知します。
LSP Control Mode	LSP 制御モードを選択します。「Default」を選択すると初期値(Independent)を指定します。
	・ Independent LSP Control (独立 LSP 制御) - 各 LSR は独自にラベルを FEC に割り当てて、ラベル配布ピアにその
	割り当てを配布します。
	・ Ordered LSP Control (順次 LSP 制御) - その FEC のためのイーグレス LSR である場合、またはその FEC のネクス
	トホップから FEC へのラベル割り当てを既に受信している場合にだけ、LSR はラベルを FEC に割り当てます。
Label Retention Mode	LDP ラベル保持モードを選択します。「Default」を選択すると初期値(Liberal)を指定します。
	・ Conservative - ラベル配布方式が Downstream-Unsolicited(DU)で、ラベル保持モードが「Conservative」であ
	る場合、LSR が、(その FEC のネクストホップでない)LSR からラベル割り当てを一度受信すると、割り当てを
	破棄します。
	・ Liberal - ラベル保持モードが「Liberal」であると、その割り当てを維持します。これは、ネクストホップに変更
	があった場合に LSP の迅速なセットアップを補助します。
Loop Detection	LDP ループ検知モードを有効または無効にします。LDP ループ検知メカニズムは、ループする LSP を検知するため
	にラベル要求とラベルマッピングメッセージによって運ばれた Path Vector および Hop Count TLV を利用します。
Path Vector Limit	使用するパスベクトルの制限値を入力します。この値は 1-255 である必要があります。
	「Default」を選択すると初期値(254)を指定します。
Hop Count Limit	使用するホップカウントの制限値を入力します。この値は 1-255 である必要があります。
	「Default」を選択すると初期値(254)を指定します。
Authentication	LDP 認証オプションを有効または無効にします。認証が有効であると、LSR は MD5 アルゴリズムを適用して、ピア
	に送信される TCP セグメントのために MD5 ダイジェストを計算します。この計算は TCP セグメントと同様にピア
	パスワードを利用します。LSR が MD5 ダイジェストと共に TCP セグメントを受信すると、MD5 ダイジェストを算
	出し、自身の記録を使用して、ダイジェストを受信したダイジェストと比較することで、セグメントを有効にします。
	比較でエラーとなると、セグメントは送信側に応答せずに破棄されます。LSR はパスワードが設定されていない LSR
	からの LDP Hello メッセージをすべて無視します。
PHP	PHP(Penultimate Hop Popping)の動作を選択します。LSR を「egress」に、PHP を「Implicit NULL」(暗黙 NULL)
	に設定する場合、Implicit NULL ラベルを上流(Penultimate Hop: 最後から 2 番目のホップ)に配布します。その後、
	上流は PHP を行います。Penultimate Hop に配布されたラベルを「Explicit NULL」に設定すると、Penultimate Hop
	はそれをポップ(ラベル削除)しません。
Trap Status	LDP トラップの状態を有効または無効にします。
Graceful Restart	「Graceful Restart」を「Enabled」(有効)/「Disabled」(無効)に指定します。「LDP Graceful Restart」は Label
	Switching Router's (LSR) 制御の再起動時に、MPLS トラッフィクへの悪影響を最小限にとどめるメカニズムです。こ
	れにより LDP は LDP セッションリカバリの間、MPLS フォワーディングステートを保持し、データに影響を与えま
	せん。「Graceful Restart」はローカル / ピアの両方が有効な場合において、LDP セッションで使用されます。
Neighbor Liveness Time	「Neighbor Liveness Time」値を入力します。機器がダウンしたネイバとの LDP セッションを検出した場合、再接続
	時間において LDP コミュニケーションの再構築を試みます。再接続時間(Reconnection Time)はネイバによって通
	知された FT 再接続タイムアウト値よりも少ない値と、ローカル生存時間に基づいて、設定されます。LDP セッショ
	ンが再接続時間内で構築されなかった場合、すべての関連するラベルフォワーディングエントリは削除されます。
	「LDP Graceful Restart」が有効な場合、通知された FT 再接続タイムアウトはネイバ生存タイム値に基づいて設定さ
	れます。5-300 秒の間で指定可能です。「Default」を選択すると初期値を指定します。
Recovery Time	リカバリタイムを指定します。「LDP Graceful Restart」が有効時で、LDP セッションが再構築された場合、デバイス
	はリカバリタイムの間、ネイバのラベルマッピング情報交換を完了します。リカバリタイムが過ぎると、デバイス
	は全てのラベルフォワーディングエントリを削除します。「12-600」秒で指定可能です。「Default」を選択すると
	初期値を指定します。

「Apply」をクリックし、設定内容を適用します。

# MPLS LSP Trigger Information (MPLS LSP トリガ情報)

本項目では、「Multiprotocol Label Switching」(MPLS)「Label-Switched Label-Switched Path」(LSP) トリガ情報の設定、表示を行います。LSP トリガフィ ルタルールは LSP 構築のトリガとなる IP ルート制御に使われる IP アクセスリストルールです。

MPLS > MPLS LSP Trigger Information の順にメニューをクリックし、以下の画面を表示します。

MPLS LSP Trig	gger Information		
MPLS LSP Trigger	Information		
SN (1-10000)		Action	Permit 🔽
IP Address	· · · ·	Mask	Any
			Apply
SN (1-10000)			Find Clear All
Total Entries: 1			
SN	Prefix FEC	Action	
1	Any	Permit	Delete
			1/1 K < 1 > > Go

図 14-2 MPLS LSP Trigger Information 画面

画面に表示される項目:

項目	説明
SN	LSP トリガフィルタルールのシーケンス番号 (1-10000) を指定します。新しくルールを作成する場合に指定されていないと、
	SN は 10 から始まり 10 ずつ増加していきます。
Action	動作を指定します。
	・ Permit - LSP 構築における LDP による IP prefix FEC フォローを許可します。
	・ Deny - LSP 構築における LDP による IP prefix FEC フォローを許可しません。
IP Address	ルールが適用される IPv4 アドレス FEC を指定します。
Mask	ルールが適用されるサブネットマスク FEC を指定します。「Any」を選択するとどの IP プリフィクス FEC でも適用さ
	れます。

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

「Clear All」をクリックすると入力したエントリを全てクリアします。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

# MPLS Forwarding Settings (MPLS フォワーディング設定)

本項目では、MPLS フォワーディングの設定、表示を行います。

「Static FTN Settings」セクションではスタティック「FEC-To-NHLFE」マップ (FTN) エントリの追加 / 削除を行います。FEC は「Forwarding Equivalence Class」を意味し、NHLFE は「Next Hop Label Forwarding Entry」を意味します。イングレス「Label Edge Router」(LER) では、「Forwarding Equivalence Class」(FEC) に分類された内向きパケットは MPLS ラベルとともにプッシュされ、「FEC-to-NHLFE」(FTN) に従い、ネクストホップに転送されます。

「Static ILM Settings」セクションではスタティック「Incoming Label Map」(ILM) エントリの追加 / 削除を行います。LSR では内向きラベルにマッチ した内向き MPLS パケット ILM の設定に基づき処理されます。ラベル操作は内向きトップラベルから設定した外向きラベルへ変換され、パケットは ネクストホップに転送されます。

MPLS > MPLS Forwarding Settings の順にメニューをクリックし、以下の画面を表示します。

MPLS Forwarding Se	ettings			
Static FTN Settings				
FEC	· · ·	Mask	. Out Label (0-999)	
Next Hop			Apply	Delete by IP Delete All
Static ILM Settings				
In Lable (0-999)		Forward Action Swap Label	Swap Label (0-999)	
Next Hop		FEC · ·	. Mask	
			Apply	Delete by In Label Delete All
Find FTN				
IP Address	· · Ma	sk · · ·	]	Find
Total Entries: 0				
LSP FEC	In Label	Out Label	Out Interface	Next Hop

図 14-3 MPLS Forwarding Settings 画面

画面に表示される項目:	
-------------	--

項目	説明			
	Static FTN Settings			
FEC	スタティック FTN の FEC IPv4 アドレスを指定します。			
Mask	スタティック FTN の FEC サブネットマスクを指定します。			
Out Label	FEC のアウトラベル値(0-999)を指定します。			
Next Hop	FEC のネクストホップ IPv4 アドレスを指定します。			
	Static ILM Settings			
In Label	ILM の内向きラベル(0-999)を指定します。			
Forward Action	転送動作について指定します。「Swap Label」「Pop」から指定します。			
Swap Label	「Swap Label」を選択後、「Swap Label」(0-999)を指定します。			
Next Hop	「Swap Label」を選択後、FEC のネクストホップ IPv4 アドレスを指定します。			
FEC	「ILM」に関連する、FEC IPv4 アドレスを指定します。			
Mask	「ILM」に関連する、FECサブネットマスクを指定します。			
	Find FTN			
IP Address	FTN の FEC IPv4 アドレスを指定します。			
Mask	FTN の FEC サブネットマスクを指定します。			

「Apply」をクリックし、設定内容を適用します。

「Delete by IP」をクリックすると指定のエントリを IP アドレスに基づき削除します。

「Delete by In Label」をクリックすると指定のエントリを「In Label」に基づき削除します。

「Delete All」をクリックするとすべてのエントリを削除します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。



MPLS が無効な「Connected 経路」は、MPLS テーブルに載せることはできません。

### MPLS LDP Neighbor Password Settings (MPLS LDP ネイバパスワード設定)

本項目では、MPLS LDP ネイバパスワードの設定、表示を行います。MD5 認証が有効な場合、同じパスワードを交換して、LSR はピアとのみセッションを構築します。パスワードの設定はリンクネイバかターゲットネイバとの交渉で適用されます。

MPLS > MPLS LDP Neighbor Password Settings の順にメニューをクリックし、以下の画面を表示します。

IPLS LDP Neighbor Password Settings		
Neighbor IP	] Password	Default
Neighbor IF	Þ	Password
10.1.1.1		*****

図 14-4 MPLS LDP Neighbor Password Settings 画面

画面に表示される項目:

項目	説明
Neighbor IP	ネイバ IPv4 アドレスを指定します。ネイバ(ピア)の LSR ID でもあります。
Password	LDP ピアパスワードを指定します。「Default」を指定すると初期値(空欄)を使用します。

「Apply」をクリックし、設定内容を適用します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

# MPLS LDP Neighbor Targeted Settings (MPLS LDP ネイバターゲット設定)

本項目では、MPLS LDP ネイバターゲットの設定、表示を行います。LDP はネイバ検出のためにターゲットハローメッセージを指定の期間で送信します。検 出されたネイバは、LDP はタイマを一時停止します。ネイバはネイバからのハローメッセージを一定期間内に受信しない場合、タイマは期限切れになります。

MPLS > MPLS LDP Neighbor Targeted Settings の順にメニューをクリックし、以下の画面を表示します。

MPLS LDP Neight	oor Targeted Settings			
MPLS LDP Neighbor Ta	argeted Settings			
Neighbor Targeted Targeted Hello Interval Targeted Hello Hold Tir Targeted Hello Source	(5-65535)	sec Default		
Targeted Hello Source	Address			
				Apply
Total Entries: 1				
Targeted Peer	Targeted Hello Interval (sec)	Targeted Hold Time (sec)	Targeted Hello Source Address	
10.1.1.1	15	45	Interface	Delete
			1/1 < 1	> >  Go

図 14-5 MPLS LDP Neighbor Targeted Settings 画面

#### 画面に表示される項目:

項目	説明
Neighbor Targeted	使用するターゲットピアの IP アドレスを入力します。ターゲットとするピアの LSR ID とします。
Targeted Hello Interval	Target Hello メッセージを送信する間隔を入力します。この値は 5-65535( 秒 ) である必要があります。 「Default」を指定すると初期値を使用します。
Targeted Hello Hold Time	Target Hello の保持時間を入力します。この値は 15-65535( 秒 ) である必要があります。 「Default」を指定すると初期値を使用します。
Targeted Hello Source	Target Hello の送信元アドレスタイプを指定します。
Address Type	・ Interface - 各インタフェースの IP アドレスを指定します。
	・ Router ID - LSR ID ( ルータ ID) を指定します。
	・ IP Address - 手動で入力した IP アドレスを指定します。
Targeted Hello Source Address	Target Hello の送信元アドレスとなる IP アドレスを指定します。

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

## MPLS LDP Neighbor Information (MPLS LDP ネイバ情報)

本項目では、MPLS LDP Neighbor Information (MPLS LDP ネイバ情報)の表示とクリアをします。

MPLS > MPLS LDP Neighbor Information の順にメニューをクリックし、以下の画面を表示します。

MPLS LDP Neig	nbor Informa	tion	_	_	_	_	_	_	_
MPLS LDP Neighbor	Information								
Peer							Find	Clear by Peer	Clear All
Total Entries: 0									
Protocol	Transport	Keep-Alive Time	Distribution	Loop	Path Vector	Max PDU	Graceful	Reconnection Time	Recovery Time
Version	Address	(sec)	Method	Detect	Limit	Length	Restart	(sec)	(sec)

図 14-6 MPLS LDP Neighbor Information 画面

画面に表示される項目:

項目	説明
Peer	ピア LSR ID(IP アドレス)を入力します。
「Clear by Peer」をクリックす	ると入力したピア情報をクリアします。
「Clear All」をクリックするとフ	<b>\力したエントリを全てクリアします。</b>

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

# MPLS Global Settings (MPLS グローバル設定)

本項目では、MPLS Global Settings(MPLS グローバル設定)の設定、表示をします。

MPLS > MPLS Global Settings の順にメニューをクリックし、以下の画面を表示します。

MPLS Global Settings				_
MPLS Global Settings				
MPLS Global State	Disabled 🗸			
LSP Trap State	Disabled 🗸			
				Apply
MPLS Interface Settings				
Interface VID (1-4094)		MPLS State	Disabled	
				Apply
Interface VID (1-4094)				Find
Total Entries: 1				
Interface		IP Address	Oper Status	
vlan1		10.90.90/8	Down	
			1/1 < 1	> >  Go

図 14-7 MPLS Global Settings 画面

画面に表示される項目:

項目	説明
	MPLS Global Settings
MPLS Global State	MPLS 機能を「Enabled」(有効)/「Disabled」(無効)に指定します。
LSP Trap State	MPLS LSP トラップを「Enabled」(有効)/「Disabled」(無効)に指定します。
	MPLS Interface Settings
Interface VID	インタフェース VLAN ID(1-4094)を指定します。
MPLS State	MPLS 機能を「Enabled」(有効)/「Disabled」(無効)に指定します。

「Apply」をクリックし、設定内容を適用します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

# MPLS LDP Interface Settings (MPLS LDP インタフェース設定)

本項目では、MPLS LDP Interface Settings(MPLS LDP インタフェース設定)の設定、表示をします。

MPLS > MPLS LDP Interface Settings の順にメニューをクリックし、以下の画面を表示します。

MPLS LDP Interface Settings				
MPLS LDP Interface Settings				
Interface VID (1-4094)				
LDP State	Disabled 🗸			
Discovery Accept	Disabled 🗸			
Distribution Mode	DU			
Discovery Hello Interval (1-65535)	sec [	Default		
Discovery Hello Hold Time (5-65535)	sec [	Default		
				Apply
Interface VID (1-4094)				Find
Total Entries: 1				
Interface Admin State Oper State	Targeted Hello Accept	Hello Interval (sec)	Hello Hold Time (sec)	Distribution Method
vlan1 Disabled Disabled	Acceptable	5	15	DU
			1/1  <	< 1 > >  Go

図 14-8 MPLS LDP Interface Settings 画面

#### 画面に表示される項目:

項目	説明
Interface VID	インタフェース VLAN ID(1-4094)を指定します。
LDP State	LDP 機能をインタフェースで「Enabled」(有効)/「Disabled」(無効)に指定します。
Discovery Accept	「Discovery Accept」を「Enabled」(有効)/「Disabled」(無効)に指定します。「targeted hello message」の受信が 無効の場合、そして受信「targeted hello」が設定されたローカルのターゲットピアから来たものではない場合、メッ セージは無視されます。「targeted hello message」受信が有効の場合、LSR は全てのネイバから受信した「targeted hello messages」を評価します。
Distribution Mode	配布方式を選択します。「Default」を選択すると初期値(DU)を指定します。 ・ DU - 配布モードを「Downstream-Unsolicited」に設定します。 ・ DoD - 配布モードを「Downstream-on-Demand」に設定します。
Discovery Hello Interval	Discovery Hello メッセージを送信する間隔を入力します。この値は 1-65535( 秒 ) である必要があります。 「Default」を指定すると初期値を使用します。
Discovery Hello Hold Time	Discovery Hello の保持時間を入力します。この値は 5-65535( 秒 ) である必要があります。 「Default」を指定すると初期値を使用します。

「Apply」をクリックし、設定内容を適用します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

### MPLS LDP Session Information (MPLS LDP セッション情報)

本項目では、MPLS LDP Session Information (MPLS LDP セッション情報)の検出、表示をします。

MPLS > MPLS LDP Session Information の順にメニューをクリックし、以下の画面を表示します。

MPLS LDP S	MPLS LDP Session Information									
MPLS LDP Sess	sion Information									
Peer Total Entries: 2	Peer Find									
Peer	Peer Status Role Keep-Alive (sec) Distribution Method									
1.2.3.4:0	OPERATIONAL	Active	40	DU	Show Detail Show Statistic					
3.4.5.6:0	OPERATIONAL	Passive	40	DU	Show Detail Show Statistic					
					1/1  < < 1 > >  Go					

図 14-9 MPLS LDP Session Information 画面

画面に表示される項目:

項目	説明
Peer	LSR ID としての IP アドレスを指定します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Show Statistics」をクリックして、統計情報を表示します。

「Show Detail」をクリックして、指定エントリの詳細について表示します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Show Detail」をクリックすると、以下の画面が表示されます。

MPLS LDP Session Detail	
MDLS LDD Session Datail	
MPL3 LDF 36351011 Detail	
Peer	1.2.3.4:0
Status	OPERATIONAL
Role	Active
Keep-Alive (sec)	40
Remain Time (sec)	28
Create Time	2000-6-9 19:33:41
Distribution Method	DU
Loop Detection	Enabled
Max PDU Length	1500
Graceful Restart	Disabled
Reconnection Time (sec)	0
Recovery Time (sec)	0
Address List	101.1.1.1, 192.168.102.1, 152.1.1.1, 1.2.3.4, 60.1.1.4, 103.1.1.1
	Back

図 14-10 MPLS LDP Session Information (Show Detail) 画面

「Back」をクリックすると前のページに戻ります。

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

		Back Refre
	ТХ	RX
Notification Message	1	2
Initialization Message	t	1
Keep-Alive Message	119	119
Address Message	1	2
Address Withdraw Message	0	1
Label Mapping Message	30	40
Label Request Message	3	6
Label Withdraw Message	4	5
Label Release Message	25	17
Label Abort Message	0	1

図 14-11 MPLS LDP Session Information (Show Statistics) 画面

「Back」をクリックすると前のページに戻ります。

### MPLS LDP Statistic (MPLS LDP スタティスティック)

本項目では、MPLS LDP Statistic (MPLS LDP スタティスティック)の表示をします。

MPLS > MPLS LDP Statistic の順にメニューをクリックし、以下の画面を表示します。

MPLS LDP Statistic		
MPLS I DP Statistic		
III ES EDF Statistic		
SessionAttempts	0	
SessionRejectedNoHelloErrors	0	
SessionRejectedAdErrors	0	
SessionRejectedMaxPduErrors	0	
SessionRejectedLRErrors	0	
BadLdpldentifierErrors	0	
BadPduLengthErrors	0	
BadMessageLengthErrors	0	
BadTlvLengthErrors	0	
MalformedTlvValueErrors	0	
KeepAliveTimerExpErrors	0	
ShutdownReceivedNotifications	0	
ShutdownSentNotifications	0	

図 14-12 MPLS LDP Statistic 画面

# MPLS LDP Binding Table (MPLS LDP バインディングテーブル)

本項目では、MPLS LDP Binding Table (MPLS LDP バインディングテーブル)の表示をします。

MPLS > MPLS LDP Binding Table の順にメニューをクリックし、以下の画面を表示します。

LDP Bind	ing Table				
Entries: 0	0				
FEC	State	In Label	Upstream	Out Label	Downstream

図 14-13 MPLS LDP Binding Table 画面

# MPLS LDP Discovery Information (MPLS LDP ディスカバリ情報)

本項目では、MPLS LDP Discovery Information (MPLS LDP ディスカバリ情報)の表示をします。

MPLS > MPLS LDP Discovery Information の順にメニューをクリックし、以下の画面を表示します。

MPLS LDP Discovery Informati	on				
MPLS LDP Discovery Information	MPLS LDP Discovery Information				
Local LDP Identifier	10.90.90.90:0				
Interfaces	Show Detail				
Targeted Hellos	Show Detail				

図 14-14 MPLS LDP Discovery Information 画面

「Interfaces」横の「Show Detail」をクリックすると、以下の画面が表示されます。

MPLS LDP Discovery Information		
MPLS LDP Discovery Information		
Local LDP Identifier	10.90.90.90:0	
Interfaces	Show Detail	
Targeted Hellos	Show Detail	
I-to-fe		
Interfaces		
Total Entries: 0		
Interface	Hello Messages Sent/Hello Messages Received	LDP ID

図 14-15 MPLS LDP Discovery Information (Show Detail) 画面

「Targeted Hellos」横の「Show Detail」をクリックすると、以下の画面が表示されます。

MPLS LDP Discovery Information	
MPLS LDP Discovery Information	
Local LDP Identifier	10.90.90:00
Interfaces	Show Detail
Targeted Hellos	Show Detail
Targeted Hellos Total Entries: 1	
LSR ID	Action Target Hello Sent/Target Hello Received LDP ID
10.90.90.90 ->10.1.1.1 (LDP)	active
	1/1 i< < 1 > >i c

図 14-16 MPLS LDP Discovery Information (Show Detail - Targeted Hellos) 画面

### MPLS QoS Settings (MPLS QoS 設定)

本項目では、MPLS QoS Settings (MPLS QoS 設定)の設定、表示をします。

MPLS > MPLS QoS Settings の順にメニューをクリックし、以下の画面を表示します。

MPLS	QoS Settings	5			
MPLS	QoS Settings				
Policy	y Name 32 cha	ars	Trust EXP	Disabled 🔽	Apply
۲	Policy Name	32 chars			
0	IP		Mask		
0	VC		VC ID		Find Delete All
Total	Entries: 1				
	Policy	Trust EXP			
	Policy	Disabled			Edit Delete

図 14-17 MPLS QoS Settings 画面

画面に表示される項目:

項目	説明
Policy Name	「MPLS QoS」ポリシー名(32 字以内)を指定します。「MPLS QoS」ポリシーは「MPLS FEC」に適用可能です。
Trust EXP	トラスト EXP 機能を「Enabled」(有効)/「Disabled」(無効)に指定します。
	EXP がトラストされると、マッチしたパケットは EXP に従い MPLS QoS ポリシーのプライオリティマッピングにス
	ケジュールされます。 そうでない場合、パケットは「802.1p」プライオリティに従いスケジュールされます。
IP	QoS ポリシーに関連する FEC IP アドレスを指定します。
Mask	QoS ポリシーに関連する FEC サブネットマスクを指定します。
VC	QoS ポリシーに関連する FEC VC アドレスを指定します。
VCID	QoS ポリシーに関連する FEC VC ID アドレスを指定します。

「Apply」をクリックし、設定内容を適用します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Delete」をクリックすると指定のエントリを削除します。

「Delete All」をクリックするとすべてのエントリを削除します。

「Edit」をクリックして、指定エントリの編集を行います。

設定エントリページが複数ページある場合、ページ番号を指定し「Go」をクリックすると当該のページへ移動します。

「Edit」をクリックすると、以下の画面が表示されます。

MPLS QoS Detail Settings			_	_	_
Policy: Policy					
Inbound EXP to CoS Settings	Outbound CoS to EXP Settings	Binding FECs Settings			
Inbound EXP to CoS					
EXP CoS					
			Add	Delete	Apply
					Back

図 14-18 MPLS QoS Settings (Edit) 画面

「Apply」をクリックし、設定内容を適用します。 「Back」をクリックすると前のページに戻ります。 「Delete」をクリックすると指定のエントリを削除します。 「Add」をクリックするとエントリを追加します。 「Add」をクリックすると、以下の画面が表示されます。

MPLS QoS Detail Settings						_
Policy: Policy						
Inbound EXP to CoS Settings	Outbound CoS to EXP Setting	s Binding FECs Settings				
Inbound EXP to CoS						
EXP			CoS			
0		2	~	Default		
1		0	~	Default		
2		1	$\checkmark$	Default		
3		3	$\checkmark$	Default		
4		4	$\checkmark$	Default		
5		5	~	Default		
6		6	~	Default		
7		7	$\checkmark$	Default		
			/	Add	Delete	Apply
						Back

図 14-19 MPLS QoS Settings (Edit, Add) 画面

#### 画面に表示される項目:

項目	説明
CoS	EXP 値にマップする CoS 値のリスト (0-7) を選択します。「Class of Service」(CoS) を「Experimental bits」(EXP) へのマッ
	とフクホリシーの設定を行います。「Delduit」を指定するこ初期値を使用します。

「Apply」をクリックし、設定内容を適用します。 「Back」をクリックすると前のページに戻ります。

「Outbound CoS to EXP Settings」タブをクリックすると、以下の画面が表示されます。

MPLS QoS Detail Settings		
Policy: Policy		
Inbound EXP to CoS Settings Outbound CoS to EXP Settings	Binding FECs Settings	
Outbound CoS to EXP		
CoS		ЕХР
		Add Delete Apply
		Back

図 14-20 MPLS QoS Settings (Edit, Outbound CoS to EXP Settings) 画面

「Apply」をクリックし、設定内容を適用します。

「Back」をクリックすると前のページに戻ります。

「Delete」をクリックすると指定のエントリを削除します。

「Add」をクリックするとエントリを追加します。

「Add」をクリックすると、以下の画面が表示されます。

nbound EXP to CoS Settings Outbound CoS to	EXP Settings	Binding FECs Settings				
tbound CoS to EXP						
CoS			EXP			
0		0	~	Default		
1		0	~	Default		
2		0	~	Default		
3		0	~	Default		
4		0	~	🗌 Default		
5		0	~	🗌 Default		
6		0	~	🗌 Default		
7		0	~	Default		
			,	Add	Delete	Apply

図 14-21 MPLS QoS Settings (Edit, Outbound CoS to EXP Settings, Add) 画面

以下の項目を設定できます。

項目	説明		
EXP	CoS 値にマップする EXP 値(0-7)を選択します。「Default」を指定すると初期値を使用します。		
ーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーー			

「Back」をクリックすると前のページに戻ります。

「Binding FECs Settings」タブをクリックすると、以下の画面が表示されます。

MPLS QoS Detail Settings			
Policy: Policy			
Inbound EXP to CoS Settings	Outbound CoS to EXP Settings	Binding FECs Settings	
• IP · · ·		Mask .	· ·
0 VC		VC ID	
			Apply Delete Delete All
Total Entries: 1			
		Binding FECs	
		VC 1/10.1.1.1	
			1/1  < < 1 > >  Go
			Back

図 14-22 MPLS QoS Settings (Edit, Binding FECs Settings) 画面

画面に表示される項目:

項目	説明
IP	MPLS QoS ポリシーに関連する FEC IP アドレスを指定します。
Mask	FEC サブネットマスクを指定します。
VC	FEC VC アドレスを指定します。
VC ID	FEC VC ID を指定します。

「Apply」をクリックし、設定内容を適用します。

「Back」をクリックすると前のページに戻ります。

「Delete」をクリックすると指定のエントリを削除します。

「Delete All」をクリックするとすべてのエントリを削除します。

# Ping MPLS

本項目では、指定 FEC の LSP の接続状態を確認します。FEC に LSP がない場合、"Destination unreachable" メッセージが表示されます。そうでな い場合は、「MPLS echo」リクエストメッセージが指定の FEC の LSP とともに送信されます。イーグレス LSR リクエストメッセージを受信した場合、 「MPLS echo」返信メッセージをリクエストメッセージの送信者に返信します。送信者がタイムアウト前にメッセージを受信できない場合、"Request timed out" メッセージが表示されます。

MPLS > Ping MPLS の順にメニューをクリックし、以下の画面を表示します。

	Ping I	MPLS		
Γ	Ping N	APLS		
	۲	IPv4 Address		
		Mask	· · · ·	
	$\bigcirc$	VC		
		VC ID		
		Ping Times (1-255)		
		Timeout (1-99)	sec	
				Start

図 14-23 Ping MPLS 画面

画面に表示される項目:

項目	説明
IPv4 Address	接続性をチェックされる LSP の FEC IPv4 アドレスを指定します。
Mask	FEC サブネットマスクを指定します。
VC	FEC VC IP アドレスを指定します。
VC ID	FEC VC ID を指定します。
Ping Times	Ping の回数(1-255)を指定します。送信される Ping パケットの回数です。
Timeout	タイムアウト値(1-99 秒)を指定します。

「Start」をクリックし、MPLS Ping を開始します。

Ping MPLS	
IPv4 Ping Result	
<ol> <li>Destination unreachable</li> <li>Destination unreachable</li> <li>Destination unreachable</li> <li>Destination unreachable</li> <li>Destination unreachable</li> </ol>	^
<pre>Ping Statistics for FEC: 10.90.90.15/8 Packets: Sent =4, Received =0, Lost =4</pre>	~
Stop Back	

図 14-24 Ping MPLS (Start) 画面

「Stop」をクリックして MPLS Ping を停止します。 「Back」をクリックすると前のページに戻ります。

### Traceroute MPLS IPv4 (トレースルート MPLS IPv4)

本項目では、指定 FEC の LSP パストレースのような「hop-by-hop fault localization」を指定します。

FEC に LSP がない場合、"Destination unreachable" メッセージが表示されます。そうでない場合は、「MPLS echo」リクエストメッセージが指定の FEC の LSP とともに送信されます。 MPLS エコーリクエスト最遠ラベル内の TTL は 1、2、3 といった具合に設定されます。各 LSR においてエコー リクエストは期限が強制的に切れます。LSR は MPLS エコーリプライに戻ります。送信者がタイムアウト前に返信を受信できない場合、トレースルー トは停止します。

MPLS > Traceroute MPLS IPv4 の順にメニューをクリックし、以下の画面を表示します。

Traceroute MPLS IP	v4	
Traceroute MPLS IPv4		
IPv4 Address		
Mask	· · · ·	
Timeout (1-99)	sec	
		Start

図 14-25 Traceroute MPLS IPv4 画面

画面に表示される項目:

項目 説明	
IPv4 Address	接続性をチェックされる LSP の FEC IPv4 アドレスを指定します。
Mask	FEC サブネットマスクを指定します。
Timeout	タイムアウト値(1-99 秒)を指定します。

「Start」をクリックし、MPLSトレースルートを開始します。

Traceroute MPLS IPv4						
IPv4 Traceroute Result						
[1] Destination unreachable Trace complete.	^					
	,					
Stop Back						

図 14-26 Traceroute MPLS IPv4 (Start) 画面

「Stop」をクリックして MPLS Ping を停止します。 「Back」をクリックすると前のページに戻ります。

# 第 15 章 MPLS L2VPN(MI モードのみ)

以下は MPLS L2VPN サブメニューの説明です。

必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明
VPWS Settings(VPWS 設定)	「Virtual Private Wire Service」(VPWS) を設定を行います。
L2VC Interface Description (L2VC $\checkmark$	L2VC Interface Description(L2VC インタフェース概要)を設定を行います。
タフェース概要)	
VPLS Settings(VPLS 設定)	「Virtual Private LAN Service」(VPLS) を設定を行います。
VPLS MAC Address Table (VPLS MAC	「VPLS MAC Address Table」(VPLS MAC アドレステーブル)を表示を行います。
アドレステーブル)	

注意 MPLS L2VPN については MI モードのみとなっています。

### VPWS Settings (VPWS 設定)

本項目では、「Virtual Private Wire Service」(VPWS)を表示、設定を行います。

MPLS L2VPN > VPWS Settings の順にメニューをクリックし、以下の画面を表示します。

VPWS Set	tings		_		_	_	_	
VPWS Settin	igs							
Unit Port	t 11/0/1 🔽	SVID (1-4094)	Peer	VC ID (1-	4294967295)	Type None	MTU (0-	65535) Apply
FIND VPWS								
VC ID (1-42	94967295)						Find	Show All
Total Entrie	es: 1							
VC ID	Peer	Local AC	MTU	Туре	Oper Status			
1	10.90.90.15	Eth1/0/1	1500	Tagged	Down	Edit	Show Detail	Delete
						1/1	< < 1	> >  Go

図 15-1 VPWS Settings 画面

画面に表示される項目:

項目	説明				
	VPWS Settings				
Unit	設定を行うユニットを指定します。				
Port	設定するポートを指定します。				
SVID	カプセル化された VLAN ID(1-4094)を指定します。				
Peer	PE のピア IP アドレスを入力します。ピア IP アドレスはその LSR ID とします。				
VC ID	Pseudo-Wire (PW) サービスインスタンス ID を入力します。この値は 1-4294967295 である必要があります。				
Туре	タイプを「None」「Manual」「Raw」「Tagged」「Manual Raw」「Manual Tagged」から指定します。 Raw モードで動作している場合、S- タグは PW には送信されません。Tagged モードで動作している場合、S- タグは PW に送 信されます。初期値では PW タイプは Ethernet タグモードにあります。				
MTU	リモートピアに通知されるローカルな CE PE リンクの MTU 値を入力します。MTU に 0 を指定すると、LDP はローカルな MTU に通知されません。MTU はローカルとリモートの両方で同じである必要があり、違う場合、PW は成功しません。指定 しないと、MTU の初期値を使用します。MTU 値の初期値は 1500 です。この値は 0-65535 である必要があります。				
	Find VPWS				
VC ID	Pseudo-Wire (PW) サービスインスタンス ID を入力します。この値は 1-4294967295 である必要があります。				
E					

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Show All」をクリックして、すべてのエントリを表示します。

「Show Detail」をクリックして、指定エントリの詳細について表示します。

「Edit」をクリックして、指定エントリの編集を行います。

「Edit」をクリックすると、以下の画面が表示されます。

VPWS Settings			
VC ID 1			Back
PW Name 64 chars			Apply
PW Redundancy Settings			
Peer	VC ID (1-4294967295)	Delay (0-180) sec  Never	Apply
Dot1q Tunneling Ethertype Settings			
Dot1q Tunneling Ethertype (0x1-0xFFFF)     ① x 8100	○ None		Apply
VLAN Mode Settings			
Nochange	⊖ None		Apply
Egress VLAN Mode Settings			
Egress VLAN Mode	○ None		Apply

図 15-2 VPWS Settings (Edit) 画面

「Back」をクリックすると前のページに戻ります。

画面に表示される項目:

項目	説明					
PW Settings						
PW Name	Pseudo-Wire (PW) 名(64 字以内)を入力します。「None」を指定すると初期値を使用します。					
	PW Redundancy Settings					
Peer	PE のピア IP アドレスを入力します。ピア IP アドレスはその LSR ID とします。					
VC ID	Pseudo-Wire (PW) サービスインスタンス ID を入力します。この値は 1-4294967295 である必要があります。					
Delay	遅延時間の値(0-180 秒)を指定します。指定の遅延時間の後にプライマリ PW に戻ります。					
	「Never」を指定するとプライマリ PW へ戻る事はありません(初期値)。					
	Dot1q Tunneling Ethertype Settings					
Dot1q Tunneling	サービス VLAN タグのアウタ TPID を指定します。					
Ethertype	16 進数形式の「0x1-0xFFFF」で指定します。「None」を指定すると無効になります。					
	VLAN Mode Settings					
VLAN Mode	<ul> <li>PW の VLAN モードを指定します。</li> <li>No Change - イングレスパケットの VLAN タグを変更しません。イーサネット VLAN ベース AC 時のみ有効です。</li> <li>Add VLAN - イングレスパケットの VLAN タグを追加します。ポートベース AC の初期動作は VLAN ID 0 の追加になります。 イーサネット / イーサネット VLAN ベース AC 時のみ有効です。</li> <li>Change VLAN - イングレスパケットの VLAN タグを指定の VLAN ID に変更します。イーサネット VLAN ベース AC 時のみ 有効です。</li> <li>「None」を指定すると初期値を使用します。</li> </ul>					
	Egress VLAN Mode Settings					
Egress VLAN Mode	<ul> <li>PW のイーグレス VLAN モードを指定します。</li> <li>Strip - AC でイーグレスする前にパケットの「outer-tag」を分離します。</li> <li>Change VLAN - AC でイーグレスする前にパケットの「outer-tag」を AC の VLAN ID に変更します。イーサネット VLAN ベース AC 時のみ有効です。</li> <li>「None」を指定すると初期値を使用します。</li> </ul>					
Annly  をクリック	設定内容を適用  ます。					

「Apply」をクリックし、設定内容を適用します。

「Show Detail」をクリックすると、以下の画面が表示されます。

VPWS Detail Information		
VPWS Detail Information Table		
VC ID	1	
Peer IP Address	10.90.90.15	
Operate Status	Down	
Name	VC1/10.90.90.15	
Description		
Local AC	Eth1/0/1	
Status	Down	
VLAN Mode	Default	
802.1q Tunneling Ethernet Type	0x8100	
Egress VLAN Mode	Strip VLAN	
Remote AC Status	N/A	
MPLS VC Labels	Local N/A, Remote N/A	
Outbound Tunnel label	N/A	
MTU	Local 1500, Remote 0	
Group ID	Local 0, Remote 0	
Signaling Protocol	LDP	
Local VCCV Capabilities:		
CC:	Type 2, Type 3	
CV:	LSP ping	
Remote VCCV Capabilities:		
CC:	N/A	
CV:	N/A	
VC Statistics:		
RX Bytes: 0, RX Packets: 0		
TX Bytes: 0, TX Packets: 0	Back	

図 15-3 VPWS Settings (Show Detail) 画面

## L2VC Interface Description (L2VC インタフェース概要)

本項目では、L2VC Interface Description(L2VC インタフェース概要)を表示、設定を行います。

MPLS L2VPN > L2VC Interface Description の順にメニューをクリックし、以下の画面を表示します。

L2VC Interface Description	_			
Create L2VC Interface Description				
L2VC Interface Name Descri 64 chars 64 cha	ption Irs			Apply
Find L2VC Interface Description L2VC Interface Name 64 chars				Find Show All
Total Entries: 1				
Interface	Status	Administrative	Description	
L2VC VC1/10.90.90.15	down	enabled		Delete Description
				1/1  < < 1 > >  Go

図 15-4 L2VC Interface Description 画面

画面に表示される項目:

項目	説明					
	Create L2VC Interface Description					
L2VC Interface	L2VC インタフェース名(64 字以内)を指定します。					
Name						
Description	L2VC インタフェース概要(64 字以内)を指定します。					
	Find L2VC Interface Description					
L2VC Interface	L2VC インタフェース名(64 字以内)を指定します。					
Name						

「Apply」をクリックし、設定内容を適用します。

「Delete Description」をクリックすると指定のエントリの概要を削除します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Show All」をクリックして、すべてのエントリを表示します。

# VPLS Settings(VPLS 設定)

本項目では、「Virtual Private LAN Service」(VPLS)を表示、設定を行います。

MPLS L2VPN > VPLS Settings の順にメニューをクリックし、以下の画面を表示します。

VPLS Settings				
VPLS Settings				
VPLS Name	VPLS Type			
32 chars	Manual			Apply Find Show All
VDI S AC Sottings				
VPL3 AC Settings				
Unit From Port	To Port	SVID	VPLS Name	
1 🕶 eth1/0/1 💌	eth1/0/1 🔽	3 or 2-5	32 chars	
				Apply
Total Entries: 1				
VPLS Name	VPLS ID	Peers/ACs	Oper Status	
VPLS	0	0/0	Down	Edit Show Detail Delete
				1/1  < < 1 > >  Go

図 15-5 VPLS Settings 画面

画面に表示される項目:

項目	説明					
	VPLS Settings					
VPLS Name	VPLS 名(32 字以内)を指定します。					
VPLS Type	VPLS タイプを指定します。					
	・ Manual - ネイバを手動で指定し、通達に LDP を使用します。					
	・ Autodiscovery - ネイバを自動検出し、通達に BGP を使用します。					
	VPLS AC Settings					
Unit	設定を行うユニットを指定します。					
From Port / To Port	設定するポートの始点 / 終点を設定します。					
SVID	SVID(1-4094)を指定します。					
VPLS Name	VPLS 名(32 字以内)を指定します。					

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Show All」をクリックして、すべてのエントリを表示します。

「Show Detail」をクリックして、指定エントリの詳細について表示します。

「Edit」をクリックして、指定エントリの編集を行います。

「Edit」をクリックすると、以下の画面が表示されます。

VPLS Settings		
VPLS Settings		
VPLS Name	VPLS	Back
VPLS ID (1-4294967295)	0	
PW Type	Tagged	
MTU (0-65535)	1500	
MAC Limit (0-1000000)	0	
		Apply
Neighbor Settings		
Remote Peer VC ID	(1-4294967295) Type no-split-horizon	
· · ·	Standalone 🔽	Apply
Dotta Tunneling Ethertype Settings		
		Apply
VLAN Mode Settings		
VLAN Mode		
Nochange	○ None	Apply
Egress VLAN Mode Settings		
Egress VLAN Mode		
<ul> <li>Strip</li> </ul>	○ None	Apply

図 15-6 VPLS Settings (Edit) 画面 「Back」をクリックすると前のページに戻ります。

ーDack」をクリックすると前のペークに戻りま 画面に表示される項目:

- 20510	1.50	~ -
百日		

項目	説明
	VPLS Settings
VPLS ID	VPLS インスタンス ID を入力します。この値は「1-4294967295」である必要があります。
PW Type	<ul> <li>PW タイプを「Raw」「Tagged」「Manual Raw」から指定します。</li> <li>Raw - イーサネット Raw モードでの動作を意味します。VPLS のすべての PW のカプセル化はイーサネット Raw モード で行われます。</li> </ul>
	<ul> <li>Tagged - イーサネット Tagged モードでの動作を意味します。VPLS のすべての PW のカプセル化はイーサネット Tagged モードで行われます。</li> </ul>
MTU	リモートピアに通知される VPLS のローカルな AC リンクの MTU 値を入力します。MTU はローカルとリモートの両方で同じ である必要があり、違う場合、PW は成功しません。MTU に 0 を指定すると、ローカルな MTU は VPLS のリモートピアに通 知されません。指定しないと、MTU 値の初期値は 1500 です。この値は 0-65535 である必要があります。
MAC Limit	MAC リミットを指定します。VPLS の MAC アドレスエントリ学習制限値を指定します。「non-zero」MAC アドレス学習制 限が指定、または MAC アドレス学習制限値を超えると、VPLS の未学習送信元 MAC アドレスのパケットは破棄されます。 0-1000000 の間で指定可能です。
	Neighbor Settings
Remote Peer	PE がどのピアに属しているのかを識別する LSR ID を指定します。
VC ID	PW VC ID を入力します。この値は 1-4294967295 である必要があります。 VPLS のピアを固有に識別する IP アドレスに指定します。指定されないと「PW ID」は VPLS の VPN ID により指定されます。
Туре	タイプを指定します。「Backup」「Standalone」から指定可能です。「Backup」オプションでは H-VPLS の PW 冗長のためにバッ クアップピアを作成します。
No-Split-Horizon	スポーク PW としてピアを使用します。 VPLS の他の PW からのパケットはこの PW に転送され、この PW からのパケットは VPLS のまた別の PW に転送されます。本 オプションが指定されていない場合、ピアはネットワーク PW として使用されます。VPLS の他のネットワーク PW からのパケッ トこの PW には転送されません。そしてこの PW からのパケットは VPLS の他のネットワーク PW に転送されません。
	Dot1q Tunneling Ethertype Settings
Dot1q Tunneling Ethertype	サービス VLAN タグのアウタ TPID を指定します。 16 進数形式の「0x1-0xFFFF」で指定します。
	VLAN Mode Settings
VLAN Mode	<ul> <li>PW の VLAN モードを指定します。</li> <li>No Change - イングレスパケットの VLAN タグを変更しません。イーサネット VLAN ベース AC 時のみ有効です。</li> <li>Add VLAN - イングレスパケットの VLAN タグを追加します。ポートベース AC の初期動作は VLAN ID 0 の追加になります。 イーサネット / イーサネット VLAN ベース AC 時のみ有効です。</li> <li>Change VLAN - イングレスパケットの VLAN タグを指定の VLAN ID に変更します。イーサネット VLAN ベース AC 時のみ 有効です。</li> <li>「None」を指定すると初期値を使用します。</li> </ul>

項目	説明
	Egress VLAN Mode Settings
Egress VLAN Mode	<ul> <li>PW のイーグレス VLAN モードを指定します。</li> <li>Strip - AC でイーグレスする前にパケットの「outer-tag」を分離します。</li> <li>Change VLAN - AC でイーグレスする前にパケットの「outer-tag」を AC の VLAN ID に変更します。 イーサネット VLAN ベース AC 時のみ有効です。</li> <li>「None」を指定すると初期値を使用します。</li> </ul>

<sup>「</sup>Apply」をクリックし、設定内容を適用します。

「Show Detail」をクリックすると、以下の画面が表示されます。

VPLS Detail Information		
VPLS Detail Information Table		
VPLS Name	VPLS	
Operate Status	Down	
Туре	Manual	
VPLS ID	0	
Service Type	Tagged	
MTU	1500	
MAC Limit	0	
VLAN mode	Default	
802.1q tunneling Ethernet Type	0x8100	
Egress VLAN Mode	Default	
Peers Via Pseudowires	Show Detail	
Local ACs	Show Detail	Back

図 15-7 VPLS Settings (Show Detail) 画面

「Back」をクリックすると前のページに戻ります。

「Peers Via Pseudowires」の「Show Detail」をクリックすると、以下の画面が表示されます。

VPLS Detail Information		
VPLS Detail Information Table		
VPLS Name	VPLS	
Operate Status	Down	
Туре	Manual	
VPLS ID	0	
Service Type	Tagged	
MTU	1500	
MAC Limit	0	
VLAN mode	Default	
802.1q tunneling Ethernet Type	0x8100	
Egress VLAN Mode	Default	
Peers Via Pseudowires	Show Detail	
Local ACs	Show Detail	Back

図 15-8 VPLS Settings (Show Detail) 画面

「Back」をクリックすると前のページに戻ります。

# VPLS MAC Address Table (VPLS MAC アドレステーブル)

本項目では、VPLS MAC Address Table (VPLS MAC アドレステーブル)を表示、クリアを行います。

MPLS L2VPN > VPLS MAC Address Table の順にメニューをクリックし、以下の画面を表示します。

VPLS MAC /	Address Table	_	_	_	_	_	_
VPLS MAC Add	dress Table						
VPLS Name	32 chars	IP Address		VC ID (1-4294967295	)		Clear By PW
VPLS Name	32 chars	Interface	1 🗸 eth1/0/1 🗸	VLAN (1-4094)			Clear By AC
VPLS Name	32 chars	MAC Address	00-84-57-00-00-00				Clear By MAC
VPLS Name	32 chars						Clear By VPLS
VPLS Name	Туре	MAC Addre	ess				
32 chars	None 🗸	00-84-57-0	00-00-00				Find
Total Entries:	0					Clear All	Show All
	VPLS Name		MAC Ad	dress	Pe	er (VC ID/IP) or AC	

図 15-9 VPLS MAC Address Table 画面

画面に表示される項目:

項目	説明		
VPLS Name	VPLS インスタンス名(32 字以内)を指定します。		
IP Address	ピアが属する PE を識別する LSR ID を指定します。		
VC ID	PW VC ID(1-4294967295)を指定します。		
Interface	設定を行うユニット / ポートを指定します。		
VLAN	VLAN ID(1-4094)を指定します。		
MAC Address	MAC アドレスを指定します。		
Туре	サーチクエリでの情報を指定します。「None」「Peer」「AC」から指定します。		
「Find」をクリックし			

「Show All」をクリックして、すべてのエントリを表示します。

「Clear All」をクリックすると入力したエントリを全てクリアします。

「Clear By PW」をクリックして指定した「PW」に関連する情報をクリアします。

「Clear By AC」をクリックして指定した「AC」に関連する情報をクリアします。

「Clear By MAC」をクリックして指定した「MAC」に関連する情報をクリアします。

「Clear By VPLS」をクリックして指定した「VPLS」に関連する情報をクリアします。

# 第 16 章 Monitoring(スイッチのモニタリング)

Monitoring メニューを使用し、本スイッチのポート使用率、パケットエラーおよびパケットサイズ等の情報を提供することができます。

以下は Monitoring サブメニューの	の説明です。	必要に応じて、	設定/変更/	′修正を行って	ください。
------------------------	--------	---------	--------	---------	-------

サブメニュー	説明
VLAN Counter(VLAN カウンタ)	VLAN カウンタの設定を行います。L2 VLAN インタフェースにおけるトラフィック統計のコントロー ルエントリを指定します。
Utilization(利用分析)	スイッチの Utilization(利用分析)を表示します。
Statistics(統計情報)	スイッチの Statistics(統計情報)を表示します。
Mirror Settings(ミラー設定)	ミラーリング機能の設定を行います。本スイッチは対象ポートで送受信するフレームをコピーし、 フレームの出力先を他のポートに変更する機能(ポートミラーリング)があります。
sFlow (sFlow 設定)	sFlow は(RFC3176)、スイッチやルータを経由するネットワークトラフィックをモニタする機能です。sFlow によるモニタリングは「sFlow エージェント」(スイッチやルータ内に内蔵)と「セント ラル sFlow コレクタ」によって構成されています。
Device Environment(機器環境確認)	Device Environment(機器環境確認)ではスイッチの内部の温度状態を表示します。
External Alarm Settings(外部アラーム設定)	外部アラーム設定はアラーム起動時のアラームメッセージについて設定します。

# VLAN Counter (VLAN カウンタ)

本画面では、VLAN カウンタの設定、表示を行います。指定の L2 VLAN インタフェースにおけるトラフィック統計のコントロールエントリを指定します。

Monitoring > VLAN Counter の順にメニューをクリックし、以下の画面を表示します。

VLAN Counter			
VLAN Counter Settings			
Interface VLAN (1-4094)	Unit From Port To Port	Frame Type Traffic Direction	
	1 eth1/0/1 v eth1/0/1 v	MAII Any Both	Apply Delete
VLAN Counter Table			
Interface VLAN (1-4094)	Traffic Direction		
	All Both 🗸		Find
Total Entries: 2			
VLAN	Frame Type	Ports	
1	RX Any	1/0/10	
1	TX Any	1/0/10	
			1/1  < < 1 > >  Go

図 16-1 VLAN Counter 画面

#### 画面に表示される項目:

項目	説明
	VLAN Counter Settings
Interface VLAN	インタフェース VLAN(1-4094)を指定します。
Unit	設定するユニットを選択します。
From Port / To	設定するポートの始点 / 終点を設定します。「All」を指定すると全ポートを指定します。
Port	
Frame Type	フレームタイプを指定します。
	・ Broadcast - ブロードキャストフレームのみをカウントします。
	・ Multicast - マルチキャストフレームのみをカウントします。
	・ Unicast - ユニキャストフレームのみをカウントします。
	・ Any - フレームタイプに関係なく全てのフレームをカウントします。
	・ All - 上記全てのフレームをカウントします。
Traffic Direction	トラフィックの向きを指定します。
	・ RX - イングレストラフィックを指定します。
	・ TX - イーグレストラフィックを指定します。
	・ Both - 両方のトラフィックをカウントします。
	VLAN Counter Table
Interface VLAN	インタフェース VLAN(1-4094)を指定します。「All」を指定すると全 VLAN を指定します。
Traffic Direction	トラフィックの向きを指定します。
	・ RX - イングレストラフィックを指定します。
	・ TX - イーグレストラフィックを指定します。
	・ Both - 両方のトラフィックをカウントします。

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

「Find」ボタンをクリックし、入力した情報を元に指定のエントリを検出します。

「Detele」ボタンをクリックし、指定したエントリを削除します。

# Utilization (利用分析)

CPU 使用率、ポートの帯域使用率などを表示します。

### Port Utilization (ポート使用率)

本画面では、ポートの帯域使用率を表示します。

#### Monitoring > Utilization > Port Utilization の順にメニューをクリックし、以下の画面を表示します。

Port Utilization			
Port Utilization			
Unit 1 🗸	From Port eth1/0/1 V To Port e	eth1/0/1 🔽	nd Refresh
Port	TX (packets/sec)	RX (packets/sec)	Utilization
eth1/0/1	0	0	0
eth1/0/2	0	0	0
eth1/0/3	0	0	0
eth1/0/4	0	0	0
eth1/0/5	0	0	0
eth1/0/6	0	0	0
eth1/0/7	0	0	0
eth1/0/8	0	0	0
eth1/0/9	0	0	0
eth1/0/10	0	0	0
eth1/0/11	0	0	0
eth1/0/12	0	0	0
eth1/0/13	0	0	0
eth1/0/14	n	0	Π

図 16-2 Port Utilization 画面

画面に表示される項目:

項目	説明
Unit	表示するユニットを指定します。
Port	プルダウンメニューで統計情報を表示するポート番号を選択します。

「Find」ボタンをクリックし、入力した情報を元に指定のエントリを検出します。 「Refresh」ボタンをクリックし、テーブルを再起動します。

## History Utilization(使用履歴)

本項目ではメモリ、CPU およびポートの使用履歴について表示します。

#### Monitoring > Utilization > History Utilization の順にメニューをクリックし、以下の画面を表示します。

History Utilization								
History Utilization								
Type Unit T Memory 1	me Based Slot Index		Find					
Туре	Start Time	End Time	Utilization					
Memory	13 Mar 2018 11:25:32	13 Mar 2018 11:10:32	39%					
Memory	13 Mar 2018 11:10:32	13 Mar 2018 10:55:32	39%					
Memory	13 Mar 2018 10:55:32	13 Mar 2018 10:40:32	39%					
Memory Memory	13 Mar 2018 10:55:32 13 Mar 2018 10:40:32	13 Mar 2018 10:40:32 13 Mar 2018 10:25:32	39% 39%					

図 16-3 History Utilization (Memory) 画面

History Utilization			
History Utilization			
Type Time Based	Slot Index		
CPU V 15 Minutes V	All		Find
Туре	Start Time	End Time	Utilization
CPU	13 Mar 2018 11:26:21	13 Mar 2018 11:11:21	14%
CPU	13 Mar 2018 11:11:21	13 Mar 2018 10:56:21	14%
CPU	13 Mar 2018 10:56:21	13 Mar 2018 10:41:21	14%
0011			
CPU	13 Mar 2018 10:41:21	13 Mar 2018 10:26:21	14%

図 16-4 History Utilization (CPU) 画面

History Utilization			
History Utilization			
Type Unit Fro	m Port To Port	Time Based Slot Index	
Port v 1v et	h1/0/1 🗸 eth1/0/1 🗸	15 Minutes V All V	Find
Port	Start Time	End Time	Utilization
eth1/0/1	13 Mar 2018 11:26:43	13 Mar 2018 11:11:43	0%
eth1/0/1	13 Mar 2018 11:11:43	13 Mar 2018 10:56:43	0%
eth1/0/1	13 Mar 2018 10:56:43	13 Mar 2018 10:41:43	0%
eth1/0/1	13 Mar 2018 10:41:43	13 Mar 2018 10:26:43	0%
eth1/0/1	13 Mar 2018 10:26:43	13 Mar 2018 10:11:43	0%

図 16-5 History Utilization (Port) 画面

#### 画面に表示される項目:

項目	説明
Туре	表示する使用項目を指定します。
	・ Memory - メモリの使用履歴を表示します。
	<ul> <li>CPU - CPU の使用履歴を表示します。</li> </ul>
	• Port - ポートの使用履歴を表示します。
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。
Time Based	表示する統計情報の期間を指定します。
	<ul> <li>15 Minutes - 15 分間の使用情報を表示します。</li> </ul>
	<ul> <li>1 Day - 1 日の使用情報を表示します。</li> </ul>
	「15 Minutes」を選択すると「Slot1」は 15 分前から現在までの情報を表示し、「Slot2」は 30 分前から 15 分前までの情報を
	表示します。「1day」を選択すると「Slot1」は 24 時間前から現在までの情報を表示し、「Slot2」は 48 時間前から 24 時間前
	までの情報を表示します。
Slot Index	スロットのインデックスを指定します。「All」、「1-5」(15 Minutes 選択時)、「1-2(1 Day 選択時)」で指定可能です。
-	

「Find」ボタンをクリックし、入力した情報を元に指定のエントリを検出します。

# Statistics (統計情報)

スイッチの統計情報を表示します。

### Port (ポート統計情報)

ポートのパケット情報を表示します。

**Monitoring > Statistics > Port**の順にメニューをクリックし、以下の画面を表示します。

Port									
Port									
						_			
Unit 1	✓ Fro	m Port eth1/0/1	<b>~</b>	To Port	eth1/0/1 🗸			Find	Refresh
-		RX	_	_		ТХ	_		_
Port		Rate	То	tal	Rate		Total		
	bits/sec	packets/sec	bytes	packets	bits/sec	packets/sec	bytes	packets	
eth1/0/1	0	0	190169	2319	0	0	1122976	11029	Show Detail
eth1/0/2	0	0	0	0	0	0	0	0	Show Detail
eth1/0/3	0	0	2986503	23855	0	0	4205950	9374	Show Detail
eth1/0/4	0	0	0	0	0	0	0	0	Show Detail
eth1/0/5	0	0	0	0	0	0	0	0	Show Detail
eth1/0/6	0	0	0	0	0	0	0	0	Show Detail
eth1/0/7	0	0	0	0	0	0	0	0	Show Detail
eth1/0/8	0	0	0	0	0	0	0	0	Show Detail

図 16-6 Port Statistics 画面

画面に表示される項目:

項目	説明
Unit	表示するユニットを選択します。
From Port /	表示するポート範囲を指定します。
To Port	

「Find」ボタンをクリックし、入力した情報を元に指定のエントリを検出します。

「Refresh」ボタンをクリックし、テーブルを再起動します。

「Show Detail」ボタンをクリックし、指定ポートの詳細情報について表示します。

「Show Detail」ボタンをクリックすると以下の画面が表示されます。

Port Detail	
Port Detail	
	Davis Default
	Back Refresh
eth1/0/1	
RX rate	0 bits/sec
TX rate	0 bits/sec
RX rate	0 packets/sec
TX rate	0 packets/sec
RX bytes	190169
TX bytes	1122976
RX packets	2319
TX packets	11029
RX multicast	207
RX broadcast	4607
RX CRC error	0
RX undersize	0
RX oversize	0
RX fragment	0
RX jabber	0
RX dropped Pkts	257
RX MTU exceeded	0
TX CRC error	0
TX excessive deferral	0
TX single collision	0
TX excessive collision	0
TX late collision	0
TX collision	0

図 16-7 Port Statistics - Show Detail 画面

「Refresh」ボタンをクリックし、テーブルを再起動します。 「Back」ボタンをクリックし、前の画面に戻ります。

# CPU Port(CPU ポート)

CPU の統計情報について表示します。

Monitoring > Statistics > CPU Port の順にメニューをクリックし、以下の画面を表示します。

CPU Port			
CPU Port			
Туре			
All		Fir	nd Refresh Clear All
Туре	PPS	Total	Drop
802.1X	0	0	0
ARP	0	128	0
BGP	0	0	0
CFM	0	0	0
CTP	0	0	0
DHCP	0	0	0
DHCPv6	0	0	0
DNS	0	0	0
DVMRP	0	0	0
ERPS	0	0	0

図 16-8 CPU Port 画面

#### 画面に表示される項目:

項目	説明				
Туре	表示するタイプを指定します。「All」「L2」「L3」「Protocol」から指定可能です。				
「Find」ボタンをク	リックし、入力した情報を元に指定のエントリを検出します。				
Refresh」ボタンをクリックし、テーブルを再起動します。					
「Clear All」ボタンを	Clear All」ボタンをクリックし、テーブル上のすべての情報を消去します。				

### Interface Counters(インタフェースカウンタ)

インタフェースカウンタ情報について表示します。

#### **Monitoring > Statistics > Interface Counters** の順にメニューをクリックし、以下の画面を表示します。

Interface Cou	unters	_	_	_	_	_	_		_
- Interface Counter	ers								
Type	Unit	From Po	urt	To Port					
Port V	1	eth1/0/	1 🔽	eth1/0/1	~			Find	Refresh
Unit 4 Sottings									
Port	InOctets	InUcastPkts	InMcastPkts	InBcastPkts	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts	
eth1/0/1	190169	1151	207	961	1122976	755	4607	5667	Show Errors
eth1/0/2	0	0	0	0	0	0	0	0	Show Errors
eth1/0/3	3032288	10927	5991	7263	4278175	9217	127	175	Show Errors
eth1/0/4	0	0	0	0	0	0	0	0	Show Errors
eth1/0/5	0	0	0	0	0	0	0	0	Show Errors
eth1/0/6	0	0	0	0	0	0	0	0	Show Errors
eth1/0/7	0	0	0	0	0	0	0	0	Show Errors
eth1/0/8	0	0	0	0	0	0	0	0	Show Errors

図 16-9 Interface Counters 画面

画面に表示される項目:

項目	説明
Туре	表示するタイプを指定します。「Port」「VLAN」から指定可能です。
Unit	設定を行うユニットを指定します。
From Port / To	設定するポートの始点 / 終点を設定します。
Port	

「Find」ボタンをクリックし、入力した情報を元に指定のエントリを検出します。 「Refresh」ボタンをクリックし、テーブルを再起動します。 「Show Errors」ボタンをクリックすると、指定ポートのエラー情報について表示します。

#### 「Show Errors」ボタンをクリックすると、次の画面が表示されます。

Counters Errors	
Counters Errors	
	Back Refresh
eth1/0/1 Counters Errors	
Align-Err	0
Fcs-Err	0
Rcv-Err	0
Undersize	0
Xmit-Err	0
OutDiscard	0
Single-Col	0
Multi-Col	0
Late-Col	0
Excess-Col	0
Carri-Sen	0
Runts	0
Giants	0
Symbol-Err	0
SQETest-Err	0
DeferredTx	0
IntMacTx	0
IntMacRx	0

図 16-10 Interface Counters (Show Errors) 画面

「Back」をクリックすると前のページに戻ります。 「Refresh」ボタンをクリックし、テーブルを再起動します。
「Type」で「VLAN」を選択すると、次の画面が表示されます。

Interface Counters					_		_	_
Interface Counters								
Туре І	Interface VLA	AN (1-4094)						
VLAN							Find	Refresh
Total Entries: 0								
VLAN	InOctets	InUcastPkts	InMcastPkts	InBcastPkts	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts

図 16-11 Interface Counters (VLAN) 画面

画面に表示される項目:

項目	説明	
Туре	表示するタイプを指定します。「Port」「VLAN」から指定可能です。	
Interface VLAN	表示する VLAN ID を指定します。	
	リックし、入力した情報を元に指定のエントリを検出します。	

「Refresh」ボタンをクリックし、テーブルを再起動します。

## Interface History Counters(インタフェースカウント履歴)

本項目ではインタフェースにおけるカウンタの履歴を表示します。

Monitoring > Statistics > Interface History Counters の順にメニューをクリックし、以下の画面を表示します。

Interface Histor	y Counters	_	_	_		_
Interface History Co	ounters					
Type Port 🗸	Unit	Port eth1/0/1	Time Based	Slot Index		Find
		eth1/0/1, 15-Minute Slo	t 1, Starttime: 3 Aug 2017 '	14:33:45, Endtime : 3	Aug 2017 14:18:45	
		Frame Size/Typ	æ		Frame Count	
		rxHCTotalPkts	Ê.		2281	
		rxHCTotalPkts	i		1225	
		rxHCUnicastPk	ts		1581	
		txHCUnicastPk	ts		1215	
		rxHCMulticastPl	ds		258	
		txHCMulticastPl	ts		6	
		rxHCBroadcastP	kts		442	

図 16-12 Interface History Counters 画面

画面に表示される項目:

項目	説明
Туре	表示する情報のタイプを指定します。
Unit	表示するユニットを選択します。
Port	表示するポートを指定します。
Time Based	<ul> <li>表示する統計情報の期間を指定します。</li> <li>15 Minutes - 15 分間の使用情報を表示します。</li> <li>1 Day - 1 日の使用情報を表示します。</li> <li>「15 Minutes」を選択すると「Slot1」は 15 分前から現在までの情報を表示し、「Slot2」は 30 分前から 15 分前までの情報を表示します。「1 day」を選択すると「Slot1」は 24 時間前から現在までの情報を表示し、「Slot2」は 48 時間前から 24 時間前までの情報を表示します。</li> </ul>
Slot Index	スロットのインデックスを指定します。「All」、「1-5」(15 Minutes 選択時)、「1-2(1 Day 選択時)」で指定可能です。

「Find」ボタンをクリックし、入力した情報を元に指定のエントリを検出します。

# Counters (カウンタ)

すべてのポートのカウンタ情報を表示、消去します。

**Monitoring > Statistics > Counters** の順にメニューをクリックし、以下の画面を表示します。

Counters					
Counters					
Туре	Unit	From Port	To Port		
Port 🗸	1 🗸	eth1/0/1 🗸	eth1/0/1 🔽	Find	Refresh
				Clear	Clear All
Unit 1 Settings					
Port			linkChange		
eth1/0/1			2		Show Detail
eth1/0/2			0		Show Detail
			5 Y Y		

図 16-13 Counters 画面

画面に表示される項目:

項目	説明
Туре	表示するタイプを指定します。「Port」「VLAN」から指定可能です。
Unit	表示するユニットを選択します。
From Port /	表示するポート範囲を指定します。
To Port	

「Find」ボタンをクリックし、入力した情報を元に指定のエントリを検出します。 「Refresh」ボタンをクリックし、テーブルを再起動します。 「Clear」ボタンをクリックし、指定ポートの情報を消去します。 「Clear All」ボタンをクリックし、テーブル上のすべての情報を消去します。 「Show Detail」ボタンをクリックし、指定ポートの詳細情報について表示します。

「Show Detail」ボタンをクリックすると以下の画面が表示されます。

Port Counters Detail		_	_
Port Counters Detail			
		Back	Refresh
		Duck	Kurtan
eth1/0/1 Counters			
rxHCTotalPkts	0		
txHCTotalPkts	0		
rxHCUnicastPkts	0		
txHCUnicastPkts	0		
rxHCMulticastPkts	0		
txHCMulticastPkts	0		
rxHCBroadcastPkts	0		
txHCBroadcastPkts	0		
rxHCOctets	0		
txHCOctets	0		
rxHCPkt64Octets	0		
rxHCPkt65to127Octets	0		
rxHCPkt128to255Octets	0		
rxHCPkt256to511Octets	0		
rxHCPkt512to1023Octets	0		
rxHCPkt1024to1518Octets	0		
rxHCPkt1519to1522Octets	0		
rxHCPkt1519to2047Octets	0		
rxHCPkt2048to4095Octets	0		

図 16-14 Port Counters Detail 画面 「Refresh」ボタンをクリックし、テーブルを再起動します。 「Back」ボタンをクリックし、前の画面に戻ります。 「Type」で「VLAN」を選択すると、次の画面が表示されます。

Interface Counters	_				_			
Interface Counters								
Туре	Interface VL	AN (1-4094)						
VLAN							Find	Refresh
Total Entries: 0								
VLAN	InOctets	InUcastPkts	InMcastPkts	InBcastPkts	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts

図 16-15 Interface Counters (VLAN) 画面

画面に表示される項目:

項目	説明
Туре	表示するタイプを指定します。「Port」「VLAN」から指定可能です。
Interface VLAN	表示する VLAN ID を指定します。
「Find」ボタンをク	リックし、入力した情報を元に指定のエントリを検出します。

「Refresh」ボタンをクリックし、テーブルを再起動します。 「Clear」ボタンをクリックし、指定ポートの情報を消去します。 「Clear All」ボタンをクリックし、テーブル上のすべての情報を消去します。

# Mirror Settings (ミラー設定)

ミラーリング機能についての設定、表示を行います。本スイッチは対象ポートで送受信するフレームをコピーして、そのコピーしたフレームの出力 先を他のポートに変更する機能(ポートミラーリング)を持っています。ミラーリングポートに監視機器(スニファや RMON probe など)を接続し、 最初のポートを通したパケットの詳細を確認することができます。トラブルシューティングやネットワーク監視の目的において適しています。

#### Monitoring > Mirror Settings をクリックします。

ID List (1-4094) rror Settings	3 or 2-5					Add	Delete
ession Number	1 💌						
		Unit	Port				
estination	Port	✓ 1	✓ eth1/0/1	$\mathbf{\mathbf{x}}$			
		Unit	From Port	To Port		Frame Type	
ource	Port	✓ 1	✓ eth1/0/1	eth1/0/1	$\mathbf{\vee}$	Both	$\sim$
		CPU RX					
						Add	Delete
ror Session Table	9						
Session							Find

図 16-16 Mirror Settings 画面

画面に表示される項目:

項目	説明
	RSPAN VLAN Settings
VID List	VLAN ID のリストを指定します。
	Mirror Settings
Session Number	該当エントリのセッション番号を指定します。1から4までで指定可能です。
Destination	<ul> <li>チェックボックスにチェックを入れポートミラーエントリの宛先について設定します。</li> <li>宛先タイプオプションとして「Port」「Remote VLAN」「Replace」を選択します。</li> <li>「Port」を選択した後に、宛先ユニットやポート番号を指定します。</li> <li>「Remote VLAN」を選択した後に、宛先ユニットやポート番号を指定し、「VID」(2-4094)も指定します。</li> <li>「Replace」を選択した後に、ACL 名と、「VID」(2-4094) も指定します。</li> </ul>
Source	<ul> <li>チェックボックスにチェックを入れポートミラーエントリの送信元について設定します。</li> <li>送信元タイプオプションとして「Port」「ACL」「VLAN」「Remote VLAN」から選択します。「Port」を選択した後に、「From Port」と「To Port」の番号を指定します。最後に「Frame Type」オプションを指定します。「Frame Type」で指定可能なオプションは「Both」「RX」「TX」「TX Forwarding」です。「Both」を選択すると送受信どちらのトラフィックもミラーされます。「RX」の場合、受信トラフィックのみミラーされ、「TX」は送信トラフィックのみミラーされます。「TX Forwarding」はポートが「STG Forwarding」状態の場合、送信トラフィックのみミラーされます。「ACL」オプションを選択した場合は ACL プロファイル名を表示される項目欄に入力します。</li> <li>・「VLAN」を選択した後に、「VID List」を指定し、Frame Type を選択します。</li> <li>・「Remote VLAN」を選択した後に「VID」(2-4094)を指定します。</li> </ul>
	Mirror Session Table
Mirror Session Type	表示する情報のミラーセッションを選択します。「All Session」「Session Number」「Remote Session」「Local Session」から選択します。 「Session Number」を選択すると表示されるドロップダウンメニューからセッション番号を選択します。1から4の間で選択可能です。

「Add」ボタンをクリックして、入力した情報に基づいた新規のミラーエントリを追加します。 「Delete」ボタンをクリックして、入力した情報に基づいた既存のミラーエントリを削除します。 「Find」ボタンをクリックして、入力した情報に基づいたエントリを検出します。

注意 ミラー機能において、TX を設定している場合、Source Port が STP、ERPS などにより、Block の状態のために実際には送信していない場合でも、 宛先ポートにモニタします。

注意 LACP/STP/ERPS/802.1X/MBA の機能によりパケットの送信が制限されている場合でも、TX のミラーリングは行われます。

「Show Detail」リンクをクリックし、以下の画面を表示します。

Session Number	1
Session Type	Local Session
Both Port	eth1/0/4
RX Port	
TX Port	
TX Forwarding Port	
Flow Based Source	
Destination Port	Ethernet1/0/1

図 16-17 Mirror Settings - Show Detail 画面

## sFlow (sFlow 設定)

sFlowは(RFC3176)、スイッチやルータを経由するネットワークトラフィックをモニタする機能です。sFlowによるモニタリングは「sFlow エージェント」(スイッチやルータ内に内蔵)と「セントラル sFlow コレクタ」によって構成されています。sFlow モニタリングシステムのアーキテクチャとサンプル技術は、サイトレベル、または企業レベルでの高速スイッチ / ルータネットワークにおける継続的なトラフィックモニタリングを提供します。



sFlow の機能において、「Agent Address」は「Vlan 1」に設定された IP アドレスを使用し、これを変更する事はできません。「Vlan 1」の IP アドレスが設定されていない場合、または「Interface vlan 1」が存在しない場合は「Agent Address」は「0.0.0.0」となります。

## sFlow Agent Information (sFlow エージェント情報)

sFlow エージェント情報を表示します。

Monitoring > sFlow > sFlow Global Settings の順にメニューをクリックし、以下の画面を表示します。

apporation Inc. 100
k C 90

図 16-18 sFlow Agent Information 画面

#### 画面に表示される項目:

項目	説明
sFlow Agent Version	現在の sFlow エージェントバージョンを表示します。
sFlow Agent Address	sFlow エージェント IP アドレスを表示します。
sFlow Agent IPv6 Address	sFlow エージェント IPv6 アドレスを表示します。
「Apply」 ボカンをクリック」 て 割	

「Apply」ボタンをクリックして、設定を有効にします。

## sFlow Receiver Settings(sFlow レシーバ設定)

sFlow エージェントのレシーバ設定と設定表示を行います。レシーバは sFlow エージェントから消去や追加することはできません。

#### Monitoring > sFlow > sFlow Receiver Settings の順にメニューをクリックし、以下の画面を表示します。

I IOW INC	eceiver Setti	ngs			_	_	_		_
sFlow Rece	eiver Settings								
Receiver I	index (1-4)			Owner	Name			32 chars	
Expire Tim	ne (1-2000000)		sec 🗌 I	nfinite Max Da	atagram Size (7	700-1400)		1400	bytes
Collector A	Address	1.1.	1.1 or 2013::1	UDP P	ort (1-65535)			6343	
VRF Name	e	12 c	hars						Apply
Total Entr	ries: 4								
Total Entr	ries: 4 Owner	Expire Time	Current Countdown Time	Max Datagram Size	Address	VRF Name	Port	Datagram Version	_
Total Entr Index 1	ries: 4 Owner	Expire Time	Current Countdown Time 0	Max Datagram Size	Address	VRF Name	Port 6343	Datagram Version 5	Reset
Total Entr Index 1 2	ries: 4 Owner	Expire Time 0	Current Countdown Time 0 0	Max Datagram Size 1400 1400	Address 0.0.0.0 0.0.0.0	VRF Name	Port 6343 6343	Datagram Version 5 5	Reset Reset
Total Entr Index 1 2 3	ries: 4 Owner	Expire Time 0 0	Current Countdown Time 0 0 0	Max Datagram Size 1400 1400 1400	Address 0.0.0.0 0.0.0.0 0.0.0.0	VRF Name	Port 6343 6343 6343	Datagram Version 5 5 5 5	Reset Reset Reset

図 16-19 sFlow Receiver Settings 画面

#### 画面に表示される項目:

項目	説明
Receiver Index	追加する sFlow レシーバの識別子(1-4)を指定します。最大 4 個のエントリを追加できます。
Owner Name	sFlow レシーバオーナ名を指定します 32 文字まで指定できます。
Expire Time	タイムアウト時間を指定します。期限になるとエントリはリセットされます。1-2000000(秒)の範囲から指定します。 「Infinite」を設定するとサーバはタイムアウトしません。
Max Datagram Size (700-1400)	1 つの sFlow データにパッケージ化する最大データバイト数を指定します。 700 から 1400 で設定できます。初期値:1400(バイト)
Collector Address	リモート sFlow コレクタの IP(v4/v6)アドレスを指定します。
UDP Port (1-65535)	リモート sFlow コレクタの UDP ポートを指定します。初期値:6343
VRF Name	VRF インスタンス名を 12 字以内で入力します。

「Apply」ボタンをクリックして、設定を有効にします。「Reset」ボタンをクリックして、指定エントリの設定を初期値に戻します。

## sFlow Sampler Settings (sFlow サンプラ設定)

ネットワークからサンプルパケットを取得するための設定をします。これには、サンプリングのレートや抽出されるパケットヘッダの量も含まれます。

Monitoring > sFlow > sFlow Sampler Settings の順にメニューをクリックし、以下の画面を表示します。

w Sampler Se	ttings						
it From	Port 1	To Port	Instance (1-655	35) Receiver (1-4	) Mode	Sampling Rate (0-6553)	6) Max Header Size (18-256)
ath1	0/4	ath 1/0/1					429 h
• eur	/0/1 💌	eurivovi		][	Inbound		Apply
tal Entries: 1			Hoto	Admin Data	Activo Data	Mar Header Size	Apply
tal Entries: 1 Port	Instance	Receiver	Mode	Admin Rate	Active Rate	Max Header Size	Apply

図 16-20 sFlow Sampler Settings 画面

四囲に衣小で1〜頃日・
-------------

項目	説明				
Unit	設定するユニットを指定します。				
From Port / To Port	パケットサンプリングの設定を行うポートおよびポート範囲を指定します。				
Instance	複数のサンプラを一つのインスタンスで使用する場合、インスタンスの識別番号を指定します。				
Receiver (1-4)	レシーバの識別番号を指定します。何も指定しない場合、値は「0」になります。1 から 4 までの間で指定可能です。				
Mode	モードを指定します。「Inbound」または「Outbound」から指定します。「Inbound」を選択するとサンプルのイング レスパケットを指定します(初期値)。「Outbound」を選択するとサンプルのイーグレスパケットを指定します。				
Sampling Rate	パケットサンプリングのレートを設定します。0-65536 の値を指定します。エントリ「0」は、パケットのサンプリン グを無効にします。0 が初期値であるため、指定しないと本機能は動作しません。				
MAX Header Size (18-256)	本項目はサンプリングされるパケットヘッダのバイト数を設定します。このサンプルサンプリングされるヘッダは、アナ ライザサーバに送信されるデータと共にカプセル化されます。18-256バイトの値を設定します。初期値は128バイトです。				

## sFlow Poller Settings(sFlow ポーラ設定)

スイッチのポーラの設定を行います。

**Configuration > sFlow > sFlow Poller Settings** の順にメニューをクリックし、以下の画面を表示します。



図 16-21 sFlow Poller Settings 画面

画面に表示される項目	:
------------	---

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	ポーリングの設定を行うポートおよびポート範囲を指定します。
Instance	複数のサンプラを一つのインスタンスで使用する場合、インスタンスの識別番号を指定します。
Receiver (1-4)	レシーバの識別番号を指定します。何も指定しない場合、値は「0」になります。1 から 4 までの間で指定可能です。
Interval (0-120)	ポーリングサンプリングの間隔を設定します。0から120(秒)で指定可能です。「0」を入力すると機能は無効になります。
	初期値:「0」

「Apply」ボタンをクリックして、設定を有効にします。

「Delete」ボタンをクリックして、指定エントリを削除します。

## Device Environment (機器環境確認)

本画面ではスイッチの内部温度状態を表示します。

Monitoring > Device Environment をクリックして次の画面を表示します。

wice Environment				
etail Temperature Status				
Unit	Temperature Descri/D Current/Threshold Range			
1	Central Temperature /1	25C/0~45C		
Status code: * temperature	is out of threshold range			
etail Fan Status				
	Items	Status		
	Unit	1		
R	light Fan 1	(OK)		
R	light Fan 2	(OK)		
etail Power Status				
Unit	Power Module	Power Status		
	Power 1	In-operation		
1.10	Power 2	Empty		

図 16-22 Device Environment 画面

# External Alarm Settings (外部アラーム設定)

外部アラーム設定はアラームが起動した時のアラームメッセージについて設定します。 Monitoring > External Alarm Settings の順にメニューをクリックし、以下の画面を表示します。

External #	Alarm Settings	_	_		
External Ala	arm Trap Settings				
External Ala	arm Trap State	O Enabled	<ul> <li>Disable</li> </ul>	d	Apply
External Ala	arm Settings				
Unit 1	Channel	1	Message	128 chars	Apply
Total Entri	es: 2				
Unit	Channel		Status	Message	
1	1		Normal	External Alarm 1	Default
1 A A	2		Normal	External Alarm 2	Default
					1/1  < < 1 > >  Go

図 16-23 External Alarm Settings 画面

画面に表示される項目:

項目	説明				
External Alarm Trap Settings					
External Alarm Trap State	外部アラームトラップを有効 / 無効に指定します。				
	External Alarm Settings				
Unit	設定を行うユニットを指定します。				
Channel	設定するチャネル(1-2)を指定します。				
Message	チャネルに紐づくアラームメッセージ(128 字以内)を指定します。				

「Apply」ボタンをクリックして、設定を有効にします。

「Default」ボタンをクリックして、初期値に戻ります。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

# 第17章 Green(省電力機能)

以下は Green サブメニューの説明です。必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明
Power Saving(省電力)	スイッチの省電力機能を設定、表示します。
EEE(Energy Efficient Ethernet/ 省電力イーサネット)	「Energy Efficient Ethernet」(EEE/ 省電力イーサネット ) は「IEEE 802.3az」によって定義され ており、パケットの送受信がリンクに発生していない場合の電力消費を抑える目的で設計さ れています。

# Power Saving(省電力)

スイッチの省電力機能を設定、表示します。

**Green > Power Saving** メニューをクリックし、以下の画面を表示します。

## Power Saving Global Settings タブ

Power Saving				
Power Saving Global Settings	Power Saving Shutdown Setting	ıgs		
Function Version	3.00			
Link Detection Power Saving	<ul> <li>Enabled</li> </ul>	Disabled		
Length Detection Power Saving	<ul> <li>Enabled</li> </ul>	Disabled		
Scheduled Port-shutdown Power Sav	ing 🔿 Enabled 💿	Disabled		
Scheduled Dim-LED Power Saving	O Enabled	Disabled		Apply
Administrative Dim-LED	<ul> <li>Enabled</li> </ul>	Disabled		Apply
Time Range Settings				
Type Dim-LED	) V Time Range	32 chars	Apply	Delete
Timo Papao				

図 17-1 Power Saving - Power Saving Global Settings タブ画面

#### 画面に表示される項目:

項目	説明
Link Detection Power Saving	「リンク検出」を有効 / 無効に指定します。有効にするとリンクダウンしているポートへの電力供給は止めら
	れ、スイッチの消費電力を抑えます。これによりリンクアップしているポートへの影響はありません。
Length Detection Power Saving	「ケーブル長検出」を有効/無効に指定します。有効にするとケーブルの長さに応じて必要な電力消費を調整
	します。
Scheduled Port-shutdown Power	スケジュールによるポートシャットダウン機能の有効 / 無効を指定します。
Saving	
Scheduled Dim-LED Power Saving	スケジュールによりスイッチの LED 照明を消すことで、消費電力を抑えます。
Administrative Dim-LED	ポート LED 機能の有効 / 無効を指定します。
Туре	省電力モードの種類を指定します。「Dim-LED」「Hibernation」から指定できます。
Time Range	上記省電力機能に対応するスケジュールを指定します。

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。画面は自動的に更新されます。 「Delete」ボタンをクリックし指定のエントリを削除します。

注意 「Hibernation」(休止)機能を有効にする場合、物理スタック機能は無効である必要があります。

## Power Saving Shutdown Settings タブ

ower saving				_	_
Power Saving Global Settings	Power Saving Shutdown Settings				
Unit	From Port	To Port	Time Range		
1 🗸	eth1/0/1 🗸	eth1/0/1 🗸	32 chars		Apply
Unit 1 Settings					
Port	n	me Range			
eth1/0/1				Delete	
eth1/0/2				Delete	
eth1/0/3				Delete	
eth1/0/4				Delete	
eth1/0/5				Delete	
all 4/0/2				Delete	

図 17-2 Power Saving - Power Saving Shutdown Settings タブ画面

画面に表示される項目:

項目	説明
Unit	設定するユニットを選択します。
From Port /	設定するポート範囲を指定します。
To Port	
Time Range	ポートに対応するスケジュール名を指定します。

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。画面は自動的に更新されます。 「Delete」ボタンをクリックし指定のエントリを削除します。

# EEE (Energy Efficient Ethernet/ 省電力イーサネット)

「Energy Efficient Ethernet」(EEE/ 省電力イーサネット ) は「IEEE 802.3az」によって定義されています。パケットの送受信がリンクに発生していない 場合の電力消費を抑える目的で設計されています。

## Green > EEE メニューをクリックし、以下の画面を表示します。

EEE			_		
FFF Settings					
LLL octango					
Unit	From Port	To Port		State	
1	eth1/0/1	eth1/0/1	-	Disabled 💌	Apply
Unit 1 Settings					
	Port			State	
	eth1/0/1			Disabled	
	eth1/0/2			Disabled	
	eth1/0/3			Disabled	
	eth1/0/4			Disabled	
	eth1/0/5			Disabled	
	eth1/0/6			Disabled	
	eth1/0/7			Disabled	

図 17-3 EEE 画面

画面に表示される項目:

項目	説明
Unit	設定するユニットを選択します。
From Port /	設定するポート範囲を指定します。
To Port	
State	本機能を有効 / 無効に指定します。

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。画面は自動的に更新されます。

注意 本機能を使用するには、接続する対向の機器も EEE に対応している必要があります。

# 第18章 OpenFlow

以下は Openflow サブメニューの説明です。必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明
Openflow Settings(OpenFlow 設定)	OpenFlow の設定を行います。

注意 OpenFlow V1.3 のみサポートされています。OpenFlow コントローラ側のプロトコルバージョンが同じであることをご確認下さい。

# **OpenFlow Settings**(**OpenFlow** 設定)

**OpenFlow > OpenFlow Settings** メニューでは、OpenFlow の設定を行います。

注意 現在のバージョンでは Web GUI による OpenFlow の設定はサポートされていません。CLI をご利用ください。

## OpenFlow Global Settings タブ

**OpenFlow > OpenFlow Settings > OpenFlow Global Settings** タブをクリックし、以下の画面を表示します。

OpenFlow Settings		
OpenFlow Global Settings	OpenFlow Port	OpenFlow Controller
Global State	⊖ Enabled	Disabled
Mode	Pure	⊖ Hybrid
Fail-Mode	<ul> <li>Secure</li> </ul>	○ Standalone
Clear Statistics Cookie ID (64 bits)	0xa37c1f	
Table-Miss Action	Default	

図 18-1 OpenFlow Settings - OpenFlow Global Settings タブ画面

#### 画面に表示される項目:

項目	説明		
Global State	OpenFlow をグローバルで有効 / 無効に設定します。		
Mode	)penFlow のモードを「Pure」または「Hybrid」に設定します。		
Fail-Mode	Fail モードを「Secure」または「Standalone」に設定します。		
Clear Statistics Cookie ID (64 bits)	クッキー ID を指定して「Clear」ボタンをクリックすると、Flow テーブル内の指定したエントリの統計情報 が削除されます。		
Table-Miss Action	<ul> <li>Table-miss フローエントリに対するアクションを指定します。</li> <li>Default - Table-Miss エントリが設定されていません。</li> <li>Drop - Clear-Actions インストラクションを実行します。不明なパケットは破棄されます。</li> <li>Controller - Apply-Actions インストラクションを実行します。不明なパケットはコントローラに送信されます。</li> </ul>		

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。 「Clear」ボタンをクリックし指定のエントリを削除します。

#### OpenFlow Port タブ

**OpenFlow > OpenFlow Settings > OpenFlow Port** タブをクリックし、以下の画面を表示します。

OpenFlow Global Se	ettings	OpenFlow Port	OpenFlow Controller	
From Port eth1/0/1 🔹	To Port eth1/0/1	OpenFlow Sta Disabled	ate 🔻	Apply
_	Port	_	s	tate
-	Port eth1/0/1	_	S Dis	tate sabled
_	Port eth1/0/1 eth1/0/2	_	S Dis Dis	tate sabled sabled

図 18-1 OpenFlow Settings - OpenFlow Port タブ画面

画面に表示される項目:

項目	説明
From Port/To Port	ポートを選択します。
OpenFlow State	OpenFlow を「Enabled」(有効)/「Disabled」(無効)に設定します。

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

## OpenFlow Controller タブ

**OpenFlow > OpenFlow Settings > OpenFlow Controller** タブをクリックし、以下の画面を表示します。

OpenFlow Settings					
OpenFlow Global Settin	ngs Openl	low Port	OpenFlow Controller		
IP Address	ess Service Port (1-65535) Connection 6653 TCP		V	E	Apply
Total Entries: 0					
IP Address	Port	Connection	Role	Status	

図 18-2 OpenFlow Settings - OpenFlow Controller タブ画面

#### 画面に表示される項目:

項目	説明
IP Address	OpenFlow コントローラの IP アドレスを入力します。
Service Port (1-65535)	OpenFlow コントローラのポート番号を入力します。
Connection	接続方法を「TCP」「TLS」から選択します。

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

「Delete」ボタンをクリックし指定のエントリを削除します。

# 第19章 Save and Tools (Save メニュー /Tools メニュー)

メンテナンス用のメニューを使用し、本スイッチのリセットおよび再起動等を行うことができます。

サブメニュー	説明	
Save (Save メニュー)		
Save Configuration (コンフィグレーションの保存)	コンフィグレーションをスイッチに保存します。	
	Tools メニュー	
Firmware Upgrade & Backup(ファームウェアアップグレード&バックアップ)	様々なプロトコルを使用してファームウェアアップグレード/バックアップを実行します。	
Configuration Restore & Backup(コンフィグレーションリ ストア&バックアップ)	様々なプロトコルを使用してコンフィグレーションリストア/バックアップを実行します。	
Certificate & Key Restore & Backup(証明書 / 鍵リス トア&バックアップ)	様々なプロトコルを使用して証明書と鍵のリストア/バックアップを実行します。	
Log Backup(ログファイルのバックアップ)	様々なプロトコルを使用してログファイルのバックアップを実行します。	
Ping	「Ping」は指定した IP アドレスに ICMP Echo パケットを送信するプログラムです。	
Trace Route (トレースルート)	パケットの経路をスイッチに到着する前に遡ってトレースすることができます。	
Reset (リセット)	スイッチの設定内容を工場出荷時状態に戻します。	
Reboot System(システム再起動)	スイッチの再起動を行います。	
DLMS Settings(DLMS 設定)	「D-Link License Management System」(DLMS) の設定、表示を行います。	

## Save (Save メニュー)

現在のコンフィグレーションを保存します。

### Save Configuration (コンフィグレーションの保存)

Save > Save Configuration をクリックし、以下の画面を表示します。

#### コンフィグレーションの保存

「Save Configuration」では現在のコンフィグレーションをスイッチに保存します。「Type」プルダウンメニューの「Configuration」を選択し、スイッチのファイルシステムにおけるパス名を「File Path」に入力して「Apply」ボタンをクリックします。

Save Cor	nfiguration			
Unit	1 V Fi	ile Path	C:/config.cfg	Apply
19-1	Save - Config	uration	画面	

## Tools (Tools メニュー)

ファームウェアアップグレード&バックアップ、コンフィグレーションリストア&バックアップ、ログファイルのバックアップ、Ping、トレースルート、リセット、システム再起動、DLMS 設定を行います。

## Firmware Upgrade & Backup (ファームウェアアップグレード&バックアップ)

注意

A1 を含む全てのハードウェアバージョンの製品について、R2.00.xxx 以上のファームウェアを使用しているもしくは一度 R2.00.xxx 以上の ファームウェアにアップグレードしたデバイスを、R1.00.060 を含むすべての R1.00.xxx バージョンへダウングレードしてお使いになること はできません。

また、Bootloader バージョンが 2.00.002 以上のものをお使いの場合にも、すべての R1.00.xxx にダウングレードすることはできませんので 十分にご注意ください。(お使いのファームウェアバージョン、Bootloader バージョンは、「show version」コマンドでご確認いただけます) 必ず 2.10.B022 以上のファームウェアのままお使いください。ダウングレードした場合、正常に起動・動作することができなくなります。

## Firmware Upgrade from HTTP(HTTP を使用したファームウェアアップグレード)

HTTP を使用してローカル PC からファームウェアアップグレードを実行します。

Tools > Firmware Upgrade & Backup > Firmware Upgrade from HTTP をクリックし、設定画面を表示します。

Firmware Upgrade from HTTP			
Unit	All		
Source File	Browse		
Destination File	64 chars		
	Upgrade		

図 19-2 Firmware Upgrade from HTTP 画面

画面に表示される項目:

項目	説明
Unit	設定するユニットを選択します。
Source File	ローカル PC にあるファームウェアのパスとファームウェアファイル名を入力します。64 文字まで指定します。「Browse/参
	照」ボタンをクリックしてローカル PC 上のファームウェアファイルの場所を指定できます。
Destination File	ファームウェアがストアされるスイッチの場所を指定します。64文字までで指定できます。

「Upgrade」ボタンをクリックしてアップグレードを開始します。

## Firmware Upgrade from TFTP(TFTP を使用したファームウェアアップグレード)

TFTP を使用してファームウェアアップグレードを実行します。

**Tools > Firmware Upgrade & Backup > Firmware Upgrade from TFTP** をクリックし、設定画面を表示します。

Firmware Upgrad	de from TFTP	
Unit	All	
TFTP Server IP	• IPv4	
	◯ IPv6	
VRF Name	12 chars	
Source File	64 chars	
Destination File	64 chars	
		Upgrade

図 19-3 Firmware Upgrade from TFTP 画面

画面に表示される項目:	
-------------	--

項目	説明
Unit	設定するユニットを選択します。
TFTP Server IP	TFTP サーバの IP アドレスを入力します。「IPv4」オプションを選択した場合、TFTP サーバの IPv4 アドレスを入力します。「IPv6」 オプションを選択した場合、TFTP サーバの IPv6 アドレスを入力します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Source File	ローカル PC にあるファームウェアのパスとファームウェアファイル名を入力します。64 文字まで指定します。「Browse/参照」ボタンをクリックしてローカル PC 上のファームウェアファイルの場所を指定できます。
Destination File	ファームウェアがストアされるスイッチの場所を指定します。64 文字までで指定できます。

「Upgrade」ボタンをクリックしてアップグレードを開始します。

## Firmware Upgrade from FTP(FTP を使用したファームウェアアップグレード)

FTP を使用してファームウェアアップグレードを実行します。

Tools > Firmware Upgrade & Backup > Firmware Upgrade from FTP をクリックし、設定画面を表示します。

irmware Upgrad	e from FTP
Unit	All
FTP Server IP	• IPv4
	O IPv6
TCP Port (1-65535)	
User Name	32 chars
Password	15 chars
VRF Name	12 chars
Source File	64 chars
Destination File	64 chars

図 19-4 Firmware Upgrade from FTP 画面

#### 画面に表示される項目:

項目	説明
Unit	設定するユニットを選択します。
FTP Server IP	FTP サーバの IP アドレスを入力します。「IPv4」オプションを選択した場合、FTP サーバの IPv4 アドレスを入力します。「IPv6」
	オプションを選択した場合、FTP サーバの IPv6 アドレスを入力します。
TCP Port	TCP ポート番号(1-65535)を指定します。
User Name	FTP 接続のユーザ名(32 字以内)を指定します。
Password	FTP 接続のパスワード(15 字以内)を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Source File	ローカル PC にあるファームウェアのパスとファームウェアファイル名を入力します。64 文字まで指定します。「Browse/参
	照」ボタンをクリックしてローカル PC 上のファームウェアファイルの場所を指定できます。
Destination File	ファームウェアがストアされるスイッチの場所を指定します。64 文字までで指定できます。

「Upgrade」ボタンをクリックしてアップグレードを開始します。

## Firmware Upgrade from RCP(RCP を使用したファームウェアアップグレード)

RCP を使用してファームウェアアップグレードを実行します。

**Tools > Firmware Upgrade & Backup > Firmware Upgrade from RCP** をクリックし、設定画面を表示します。

Firmware Upgra	Firmware Upgrade from RCP	
Unit	All	
RCP Server IP		
User Name	32 chars	
VRF Name	12 chars	
Source File	64 chars	
Destination File	64 chars	
		Upgrade

図 19-5 Firmware Upgrade from RCP 画面

## 画面に表示される項目:

項目	説明
Unit	設定するユニットを選択します。
RCP Server IP	RCP サーバの IP アドレスを入力します。
User Name	RCP 接続のユーザ名(32 字以内)を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Source File	ローカル PC にあるファームウェアのパスとファームウェアファイル名を入力します。64 文字まで指定します。「Browse/参照」ボタンをクリックしてローカル PC 上のファームウェアファイルの場所を指定できます。
Destination File	ファームウェアがストアされるスイッチの場所を指定します。64文字までで指定できます。

「Upgrade」ボタンをクリックしてアップグレードを開始します。

## Firmware Upgrade from SFTP(SFTP を使用したファームウェアアップグレード)

```
SFTP を使用してファームウェアアップグレードを実行します。
```

Tools > Firmware Upgrade & Backup > Firmware Upgrade from SFTP をクリックし、設定画面を表示します。

Firmware Upgrade from SFTP		
Unit	All	
SFTP Server IP		
Authentication Method	Password	
User Name	32 chars	
Password	15 chars	
VRF Name	12 chars	
Source File	64 chars	
Destination File	64 chars	
	Upgrade	

図 19-6 Firmware Upgrade from SFTP 画面

#### 画面に表示される項目:

項目	説明
Unit	設定するユニットを選択します。
SFTP Server IP	SFTP サーバの IP アドレスを入力します。
Authentication Method	認証方法が表示されます。
User Name	SFTP 接続のユーザ名(32 字以内)を指定します。
Password	SFTP 接続のパスワード(15 字以内)を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Source File	ローカル PC にあるファームウェアのパスとファームウェアファイル名を入力します。64 文字まで指定します。 「Browse/ 参照」ボタンをクリックしてローカル PC 上のファームウェアファイルの場所を指定できます。
Destination File	ファームウェアがストアされるスイッチの場所を指定します。64 文字までで指定できます。

「Upgrade」ボタンをクリックしてアップグレードを開始します。

## Firmware Backup to HTTP(HTTP を使用したファームウェアバックアップ)

HTTP サーバにファームウェアバックアップを行います。

Tools > Firmware Upgrade & Backup > Firmware Backup to HTTP をクリックし、設定画面を表示します。

Firmware Bac	Firmware Backup to HTTP		
Unit Source File	1 64 chars	Backup	

図 19-7 Firmware Backup to HTTP 画面

画面に表示される項目:

項目	説明
Unit	設定するユニットを選択します。
Source File	スイッチにあるパスとファイル名を入力します。64文字まで指定します。

「Backup」ボタンをクリックしてバックアップを開始します。

## Firmware Backup to TFTP(TFTP を使用したファームウェアバックアップ)

TFTP サーバにファームウェアバックアップを行います。

Tools > Firmware Upgrade & Backup > Firmware Backup to TFTP をクリックし、設定画面を表示します。

Firmware Backup to TFTP		
Unit		
TFTP Server IP	● IPv4	
	○ IPv6	
VRF Name	12 chars	
Source File	64 chars	
Destination File	64 chars	
	Backup	

図 19-8 Firmware Backup to TFTP 画面

画面に表示される項目:

項目	説明
Unit	設定するユニットを選択します。
TFTP Server IP	TFTP サーバの IP アドレスを入力します。「IPv4」オプションを選択した場合、TFTP サーバの IPv4 アドレスを入力します。「IPv6」 オプションを選択した場合、TFTP サーバの IPv6 アドレスを入力します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Source File	スイッチにあるパスとファイル名を入力します。64文字まで指定します。
Destination File	ファームウェアファイルがバックアップされる TFTP サーバの場所(パス / ファイル名)を指定します。64 文字までで指定 できます。

## Firmware Backup to FTP(FTP を使用したファームウェアバックアップ)

FTP を使用してファームウェアバックアップを実行します。

Tools > Firmware Backup & Backup > firmware Backup to FTP をクリックし、設定画面を表示します。

Firmware Backup	to FTP		_	_	_
Unit	1 🗵				
FTP Server IP					
	◯ IPv6				
TCP Port (1-65535)					
User Name	32 chars				
Password	15 chars				
VRF Name	12 chars				
Source File	64 chars				
Destination File	64 chars				
		Backup			

図 19-9 Firmware Backup to FTP 画面

#### 画面に表示される項目:

項目	説明
Unit	設定するユニットを選択します。
FTP Server IP	FTP サーバの IP アドレスを入力します。「IPv4」オプションを選択した場合、FTP サーバの IPv4 アドレスを入力します。「IPv6」 オプションを選択した場合、FTP サーバの IPv6 アドレスを入力します。
TCP Port	TCP ポート番号(1-65535)を指定します。
User Name	FTP 接続のユーザ名(32 字以内)を指定します。
Password	FTP 接続のパスワード(15 字以内)を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Source File	スイッチにあるファームウェアのパスとファームウェアファイル名を入力します。64文字まで指定します。
Destination File	ファームウェアがストアされる FTP サーバの場所を指定します。64 文字までで指定できます。
	リックトアバックフップを明始します

「Backup」ボタンをクリックしてバックアップを開始します。

#### Firmware Backup to RCP (RCP を使用したファームウェアバックアップ)

RCP を使用してファームウェアバックアップを実行します。 Tools > Firmware Backup & Backup > firmware Backup to RCP をクリックし、設定画面を表示します。

Firmware Backu	to RCP
Unit	
RCP Server IP	
User Name	32 chars
VRF Name	12 chars
Source File	64 chars
Destination File	64 chars
	Backup

図 19-10 Firmware Backup to RCP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定するユニットを選択します。
RCP Server IP	RCP サーバの IP アドレスを入力します。
User Name	RCP 接続のユーザ名(32 字以内)を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Source File	スイッチにあるファームウェアのパスとファームウェアファイル名を入力します。64文字まで指定します。
Destination File	ファームウェアがストアされる RCP サーバの場所を指定します。64 文字までで指定できます。

## Firmware Backup to SFTP(SFTP を使用したファームウェアバックアップ)

SFTP を使用してファームウェアバックアップを実行します。

Tools > Firmware Backup & Backup > firmware Backup to SFTP をクリックし、設定画面を表示します。

Firmware Backup to SFTP		
Unit		
SFTP Server IP		
Authentication Method	Password	
User Name	32 chars	
Password	15 chars	
VRF Name	12 chars	
Source File	64 chars	
Destination File	64 chars	
	Backup	

図 19-11 Firmware Backup to SFTP 画面

画面に表示される項目	:
------------	---

項目	説明
Unit	設定するユニットを選択します。
SFTP Server IP	SFTP サーバの IP アドレスを入力します。
Authentication Method	認証方法が表示されます。
User Name	SFTP 接続のユーザ名(32 字以内)を指定します。
Password	SFTP 接続のパスワード(15 字以内)を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Source File	ローカル PC にあるファームウェアのパスとファームウェアファイル名を入力します。64 文字まで指定します。 「Browse/ 参照」ボタンをクリックしてローカル PC 上のファームウェアファイルの場所を指定できます。
Destination File	ファームウェアがストアされるスイッチの場所を指定します。64 文字までで指定できます。

## Configuration Restore & Backup (コンフィグレーションリストア&バックアップ)

## Configuration Restore from HTTP(HTTP サーバからコンフィグレーションのリストア)

HTTP サーバを使用してローカル PC からコンフィグレーションをリストアします。

注意 R1.xx の機器に R2.xx の機器からバックアップした設定をリストアしないでください。

Tools > Configuration Restore & Backup > Configuration Restore from HTTP をクリックし、設定画面を表示します。

Configuration Re	store from HTTP	
Unit	All	
Source File	Browse	
Destination File	64 chars	running-config 🔲 startup-config
Replace		
		Restore

図 19-12 Configuration Restore from HTTP 画面

#### 画面に表示される項目:

項目	説明
Unit	設定するユニットを選択します。
Source File	ローカル PC にあるコンフィグレーションのパスとコンフィグレーションファイル名を入力します。64 文字まで指定します。 「Browse/ 参照」ボタンをクリックしてローカル PC 上のコンフィグレーションファイルの場所を指定できます。
Destination File	コンフィグレーションファイルがストアされるスイッチの場所を指定します。64 文字までで指定できます。 「running-config」オプションを選択するとリストアと同時に実行中のコンフィグレーションファイルは上書きされます。 「startup-config」オプションを選択すると起動時にコンフィグレーションファイルはリストア&上書きされます。
Replace	現在実行中のコンフィグレーションを置き換えます。

「Restore」ボタンをクリックしてコンフィグレーションのリストアを開始します。

## Configuration Restore from TFTP(TFTP サーバからコンフィグレーションのリストア)

TFTP サーバを使用してローカル PC からコンフィグレーションをリストアします。

## Tools > Configuration Restore & Backup > Configuration Restore from TFTP をクリックし、設定画面を表示します。

Configuration R	estore from TFTP	
Unit	All	
TFTP Server IP		
	O IPv6	
VRF Name	12 chars	
Source File	64 chars	
Destination File	64 chars	running-config startup-config
Replace		
		Restore

図 19-13 Configuration Restore from TFTP 画面

## 画面に表示される項目:

項目	説明
Unit	設定するユニットを選択します。
TFTP Server IP	TFTPサーバのIPアドレスを入力します。「IPv4」オプションを選択した場合、TFTPサーバのIPv4アドレスを入力します。「IPv6」
	オプションを選択した場合、TFTP サーバの IPv6 アドレスを入力します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Source File	TFTP サーバにあるコンフィグレーションのパスとコンフィグレーションファイル名を入力します。64 文字まで指定します。
Destination File	コンフィグレーションファイルがストアされるスイッチの場所を指定します。64文字までで指定できます。
	「running-config」オプションを選択するとリストアと同時に実行中のコンフィグレーションファイルは上書きされます。
	「startup-config」オプションを選択すると起動時にコンフィグレーションファイルはリストア&上書きされます。
Replace	現在実行中のコンフィグレーションを置き換えます。

「Restore」ボタンをクリックしてコンフィグレーションのリストアを開始します。

## Configuration Restore from FTP(FTP サーバからコンフィグレーションのリストア)

FTP サーバを使用してローカル PC からコンフィグレーションをリストアします。

**Tools > Configuration Restore & Backup > Configuration Restore from FTP** をクリックし、設定画面を表示します。

Configuration Res	tore from FTP		
Unit FTP Server IP		<ul> <li>IPv4</li> <li>IPv6</li> </ul>	
TCP Port (1-65535)			
User Name	32 chars		
Password	15 chars		
VRF Name	12 chars		
Source File	64 chars		
Destination File	64 chars		running-config startup-config
Replace			
			Restore

図 19-14 Configuration Restore from FTP 画面

#### 画面に表示される項目:

項目	説明		
Unit	設定するユニットを選択します。		
FTP Server IP	FTP サーバの IP アドレスを入力します。「IPv4」オプションを選択した場合、FTP サーバの IPv4 アドレスを入力します。「IPv6」 オプションを選択した場合、FTP サーバの IPv6 アドレスを入力します。		
TCP Port	TCP ポート番号(1-65535)を指定します。		
User Name	FTP 接続のユーザ名(32 字以内)を指定します。		
Password	FTP 接続のパスワード(15 字以内)を指定します。		
VRF Name	VRF インスタンス名を 12 字以内で入力します。		
Source File	FTP サーバにあるコンフィグレーションのパスとコンフィグレーションファイル名を入力します。64 文字まで指定します。		
Destination File	コンフィグレーションファイルがストアされるスイッチの場所を指定します。64 文字までで指定できます。 「running-config」オプションを選択するとリストアと同時に実行中のコンフィグレーションファイルは上書きされます。 「startup-config」オプションを選択すると起動時にコンフィグレーションファイルはリストア&上書きされます。		
Replace	現在実行中のコンフィグレーションを置き換えます。		

「Restore」ボタンをクリックしてコンフィグレーションのリストアを開始します。

#### Configuration Restore from RCP(RCP サーバからコンフィグレーションのリストア)

RCP サーバを使用してローカル PC からコンフィグレーションをリストアします。

#### **Tools > Configuration Restore & Backup > Configuration Restore from RCP** をクリックし、設定画面を表示します。

Configuration R	estore from RCP	
Unit	All	
RCP Server IP	14 - 14 - 14 T	
User Name	32 chars	
VRF Name	12 chars	
Source File	64 chars	
Destination File	64 chars	running-config startup-config
Replace		
		Restore

図 19-15 Configuration Restore from RCP 画面

画面に表示される項目:

項目	説明
Unit	設定するユニットを選択します。
RCP Server IP	RCP サーバの IP アドレスを入力します。「IPv4」オプションを選択した場合、RCP サーバの IPv4 アドレスを入力します。「IPv6」 オプションを選択した場合、RCP サーバの IPv6 アドレスを入力します。
User Name	RCP 接続のユーザ名(32 字以内)を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Source File	RCP サーバにあるコンフィグレーションのパスとコンフィグレーションファイル名を入力します。64 文字まで指定します。
Destination File	コンフィグレーションファイルがストアされるスイッチの場所を指定します。64 文字までで指定できます。 「running-config」オプションを選択するとリストアと同時に実行中のコンフィグレーションファイルは上書きされます。 「startup-config」オプションを選択すると起動時にコンフィグレーションファイルはリストア&上書きされます。
Replace	現在実行中のコンフィグレーションを置き換えます。

「Restore」ボタンをクリックしてコンフィグレーションのリストアを開始します。

## Configuration Restore from SFTP(SFTP サーバからコンフィグレーションのリストア)

SFTP サーバを使用してローカル PC からコンフィグレーションをリストアします。

**Tools > Configuration Restore & Backup > Configuration Restore from SFTP** をクリックし、設定画面を表示します。

Configuration Rest	ore from SFTP	
Unit	All	
SFTP Server IP		
Authentication Method	Password	
User Name	32 chars	]
Password	15 chars	]
VRF Name	12 chars	]
Source File	64 chars	]
Destination File	64 chars	running-config startup-config
Replace		
		Restore

図 19-16 Configuration Restore from SFTP 画面

画面に表示される項目	
------------	--

項目	説明
Unit	設定するユニットを選択します。
SFTP Server IP	SFTPサーバのIPアドレスを入力します。「IPv4」オプションを選択した場合、SFTPサーバのIPv4アドレスを入力します。「IPv6」
	オブションを選択した場合、SFTP サーバの IPv6 アドレスを入力します。
User Name	SFTP 接続のユーザ名(32 字以内)を指定します。
Password	SFTP 接続のパスワード(15 字以内)を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Source File	SFTP サーバにあるコンフィグレーションのパスとコンフィグレーションファイル名を入力します。64 文字まで指定します。
Destination File	コンフィグレーションファイルがストアされるスイッチの場所を指定します。64 文字までで指定できます。
	「running-config」オプションを選択するとリストアと同時に実行中のコンフィグレーションファイルは上書きされます。
	「startup-config」オプションを選択すると起動時にコンフィグレーションファイルはリストア&上書きされます。
Replace	現在実行中のコンフィグレーションを置き換えます。

「Restore」ボタンをクリックしてコンフィグレーションのリストアを開始します。

## Configuration Backup to HTTP(HTTP を使用したコンフィグレーションバックアップ)

HTTP サーバを使用してローカル PC にコンフィグレーションバックアップを行います。

#### **Tools > Configuration Restore & Backup > Configuration Backup to HTTP** をクリックし、設定画面を表示します。

Configuration Backup to HTTP			
Unit	1		
Source File	64 chars	running-config startup-config	
		Backup	

図 19-17 Configuration Backup to HTTP 画面

画面に表示される項目:

項目	説明
Unit	設定するユニットを選択します。
Source File	スイッチにあるパスとファイル名を入力します。64 文字まで指定します。 「running-config」オプションを選択すると実行中のコンフィグレーションファイルがバックアップされます。「startup- config」オプションを選択すると起動時のコンフィグレーションファイルがバックアップされます。
「Backup」ボタンをク	リックしてバックアップを開始します。

## Configuration Backup to TFTP (TFTP を使用したコンフィグレーションバックアップ)

TFTP サーバにコンフィグレーションバックアップを行います。

## **Tools > Configuration Restore & Backup > Configuration Backup to TFTP** をクリックし、設定画面を表示します。

Configuration Ba	ickup to TFTP	
Unit	1	
TFTP Server IP	• • IPv4	
	O IPv6	
VRF Name	12 chars	
Source File	64 chars	running-config startup-config
Destination File	64 chars	
		Backup

図 19-18 Configuration Backup to TFTP 画面

画面に表示される項目	:
項目	説明
Unit	設定するユニットを選択します。
TFTP Server IP	TFTP サーバのIP アドレスを入力します。「IPv4」オプションを選択した場合、TFTP サーバのIPv4 アドレスを入力します。「IPv6」 オプションを選択した場合、TFTP サーバの IPv6 アドレスを入力します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Source File	スイッチにあるパスとファイル名を入力します。64 文字まで指定します。 「running-config」オプションを選択すると実行中のコンフィグレーションファイルがバックアップされます。「startup- config」オプションを選択すると起動時のコンフィグレーションファイルがバックアップされます。
Destination File	コンフィグレーションファイルがストアされる TFTP サーバの場所を指定します。64 文字までで指定できます。

## Configuration Backup to FTP (FTP を使用したコンフィグレーションバックアップ)

FTP サーバにコンフィグレーションバックアップを行います。

#### **Tools > Configuration Restore & Backup > Configuration Backup to FTP** をクリックし、設定画面を表示します。

Configuration Bac	kup to FTP	
Unit	1	
FTP Server IP	• • • • • • • • • • • • • • • • • • •	
	◯ IPv6	
TCP Port (1-65535)		]
User Name	32 chars	]
Password	15 chars	]
VRF Name	12 chars	]
Source File	64 chars	running-config startup-config
Destination File	64 chars	]
		Backup

図 19-19 Configuration Backup to FTP 画面

#### 画面に表示される項目:

項目	説明
Unit	設定するユニットを選択します。
FTP Server IP	FTP サーバの IP アドレスを入力します。「IPv4」オプションを選択した場合、FTP サーバの IPv4 アドレスを入力します。「IPv6」
	オプションを選択した場合、FTP サーバの IPv6 アドレスを入力します。
TCP Port	TCP ポート番号(1-65535)を指定します。
User Name	FTP 接続のユーザ名(32 字以内)を指定します。
Password	FTP 接続のパスワード(15 字以内)を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Source File	スイッチにあるパスとファイル名を入力します。64 文字まで指定します。
	「running-config」オプションを選択すると実行中のコンフィグレーションファイルがバックアップされます。「startup-
	config」オプションを選択すると起動時のコンフィグレーションファイルがバックアップされます。
Destination File	コンフィグレーションファイルがストアされる FTP サーバの場所を指定します。64 文字までで指定できます。

「Backup」ボタンをクリックしてバックアップを開始します。

## Configuration Backup to RCP (RCP を使用したコンフィグレーションバックアップ)

RCP サーバにコンフィグレーションバックアップを行います。

#### Tools > Configuration Restore & Backup > Configuration Backup to RCP をクリックし、設定画面を表示します。

Configuration Ba	ckup to RCP	
Unit	1 💌	
RCP Server IP	· · ·	
User Name	32 chars	
VRF Name	12 chars	
Source File	64 chars	running-config startup-config
Destination File	64 chars	
		Backup

図 19-20 Configuration Backup to RCP 画面

#### 画面に表示される項目:

項目	説明
Unit	設定するユニットを選択します。
RCP Server IP	RCP サーバの IP アドレスを入力します。
User Name	RCP 接続のユーザ名(32 字以内)を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Source File	スイッチにあるパスとファイル名を入力します。64 文字まで指定します。 「running-config」オプションを選択すると実行中のコンフィグレーションファイルがバックアップされます。「startup- config」オプションを選択すると起動時のコンフィグレーションファイルがバックアップされます。
Destination File	コンフィグレーションファイルがストアされる RCP サーバの場所を指定します。64 文字までで指定できます。

## Configuration Backup to SFTP(SFTP を使用したコンフィグレーションバックアップ)

SFTP サーバにコンフィグレーションバックアップを行います。

Tools > Configuration Restore & Backup > Configuration Backup to SFTP をクリックし、設定画面を表示します。

Configuration Back	Configuration Backup to SFTP				
Unit	1 🗸				
SFTP Server IP					
Authentication Method	Password				
User Name	32 chars				
Password	15 chars				
VRF Name	12 chars	]			
Source File	64 chars	running-config startup-config			
Destination File	64 chars				
		Backup			

図 19-21 Configuration Backup to SFTP 画面

	画面に表示される項目	:
--	------------	---

項目	説明	
Unit	設定するユニットを選択します。	
SFTP Server IP		
User Name	SFTP 接続のユーザ名(32 字以内)を指定します。	
Password	SFTP 接続のパスワード(15 字以内)を指定します。	
VRF Name	VRF インスタンス名を 12 字以内で入力します。	
Source File	スイッチにあるパスとファイル名を入力します。64文字まで指定します。	
「running-config」オプションを選択すると実行中のコンフィグレーションファイルがバックアップされます。「		
	config」オプションを選択すると起動時のコンフィグレーションファイルがバックアップされます。	
Destination File	コンフィグレーションファイルがストアされる SFTP サーバの場所を指定します。64 文字までで指定できます。	

# Certificate & Key Restore & Backup (証明書 / 鍵リストア&バックアップ)

## Certificate & Key Restore from HTTP(HTTP を使用した証明書 / 鍵リストア)

HTTP を使用してローカル PC から証明書 / 鍵リストアを実行します。

#### Tools > Certificate & Key Restore & Backup > Certificate & Key Restore from HTTP をクリックし、設定画面を表示します。

ertificate & Key	Restore from HTTP	_		
Unit	All			
Source File		参照		
Destination File	64 chars			
			Restore	

図 19-22 Certificate & Key Restore from HTTP 画面

#### 画面に表示される項目:

説明	
設定するユニットを選択します。	
ローカル PC にある証明書 / 鍵のパスと証明書 / 鍵ファイル名を入力します。64 文字まで指定します。「Browse/参照」ボタ	
ノをクリックしてローカルドビエの証明者が遅ノアイルの物所を相応できより。	
証明書 / 鍵がストアされるスイッチの場所を指定します。64 文字までで指定できます。	

「Restore」ボタンをクリックしてリストアを開始します。

## Certificate & Key Restore from TFTP (TFTP を使用した証明書 / 鍵リストア)

TFTP を使用して証明書 / 鍵リストアを実行します。

Tools > Certificate & Key Restore & Backup > Certificate & Key Restore from TFTP をクリックし、設定画面を表示します。

Certificate & Key	Restore from TFTP
Unit	
TFTP Server IP	· · · • • • • • • • • • • • • • • • • •
	O IPv6
VRF Name	12 chars
Source File	64 chars
Destination File	64 chars
	Restore

図 19-23 Certificate & Key Restore from TFTP 画面

## 画面に表示される項目:

項目	説明	
Unit	設定するユニットを選択します。	
TFTP Server IP	TFTPサーバのIPアドレスを入力します。「IPv4」オプションを選択した場合、TFTPサーバのIPv4アドレスを入力します。「IPv6」	
	オプションを選択した場合、TFTP サーバの IPv6 アドレスを入力します。	
VRF Name	VRF インスタンス名を 12 字以内で入力します。	
Source File	ローカル PC にある証明書 / 鍵のパスと証明書 / 鍵ファイル名を入力します。64 文字まで指定します。「Browse/ 参照」ボタ ンをクリックしてローカル PC 上の証明書 / 鍵ファイルの場所を指定できます。	
Destination File	証明書 / 鍵がストアされるスイッチの場所を指定します。64 文字までで指定できます。	

「Restore」ボタンをクリックしてリストアを開始します。

## Certificate & Key Restore from FTP(FTP を使用した証明書 / 鍵リストア)

FTP を使用して証明書 / 鍵リストアを実行します。

Tools > Certificate & Key Restore & Backup > Certificate & Key Restore from FTP をクリックし、設定画面を表示します。

Certificate & Key	Restore from FTP
11-3	
Unit	
FTP Server IP	• • • • • • • • • • • • • • • • • • •
	O IPv6
TCP Port (1-65535)	
User Name	32 chars
Password	15 chars
VRF Name	12 chars
Source File	64 chars
Destination File	64 chars
	Restore
	Record

図 19-24 Certificate & Key Restore from FTP 画面

画面に表示される項目	:		
項目	説明		
Unit	設定するユニットを選択します。		
FTP Server IP	FTP サーバの IP アドレスを入力します。「IPv4」オプションを選択した場合、FTP サーバの IPv4 アドレスを入力します。「IPv6」 オプションを選択した場合、FTP サーバの IPv6 アドレスを入力します。		
TCP Port	TCP ポート番号(1-65535)を指定します。		
User Name			
Password	FTP 接続のパスワード(15 字以内)を指定します。		
VRF Name	VRF インスタンス名を 12 字以内で入力します。		
Source File	ローカル PC にある証明書 / 鍵のパスと証明書 / 鍵ファイル名を入力します。64 文字まで指定します。「Browse/ 参照」ボタンをクリックしてローカル PC 上の証明書 / 鍵ファイルの場所を指定できます。		
Destination File	証明書 / 鍵がストアされるスイッチの場所を指定します。64 文字までで指定できます。		

「Restore」ボタンをクリックしてリストアを開始します。

#### Certificate & Key Restore from RCP (RCP を使用した証明書 / 鍵リストア)

RCP を使用して証明書 / 鍵リストアを実行します。

Tools > Certificate & Key Restore & Backup > Certificate & Key Restore from RCP をクリックし、設定画面を表示します。

Certificate & Key	/ Restore from RCP
Unit	All V
RCP Server IP	
User Name	32 chars
VRF Name	12 chars
Source File	64 chars
Destination File	64 chars
	Restore

図 19-25 Certificate & Key Restore from RCP 画面

画面に表示される項目:		
項目	説明	
Unit	設定するユニットを選択します。	
RCP Server IP	RCP サーバの IP アドレスを入力します。	
User Name	RCP 接続のユーザ名(32 字以内)を指定します。	
VRF Name	VRF インスタンス名を 12 字以内で入力します。	
Source File	ローカル PC にある証明書 / 鍵のパスと証明書 / 鍵ファイル名を入力します。64 文字まで指定します。「Browse/ 参照」ボタンをクリックしてローカル PC 上の証明書 / 鍵ファイルの場所を指定できます。	
Destination File	証明書 / 鍵がストアされるスイッチの場所を指定します。64 文字までで指定できます。	

「Restore」ボタンをクリックしてリストアを開始します。

## Certificate & Key Restore from SFTP(SFTP を使用した証明書 / 鍵リストア)

SFTP を使用して証明書 / 鍵リストアを実行します。

Tools > Certificate & Key Restore & Backup > Certificate & Key Restore from SFTP をクリックし、設定画面を表示します。

Certificate & Key Restore from SFTP		
Unit		
SFTP Server IP		
Authentication Method	Password	
User Name	32 chars	
Password	15 chars	
VRF Name	12 chars	
Source File	64 chars	
Destination File	64 chars	
	Restore	

図 19-26 Certificate & Key Restore from SFTP 画面

#### 画面に表示される項目:

項目	説明	
Unit	設定するユニットを選択します。	
SFTP Server IP	SFTP サーバの IP アドレスを入力します。	
User Name		
Password	SFTP 接続のパスワード(15 字以内)を指定します。	
VRF Name	VRF インスタンス名を 12 字以内で入力します。	
Source File	ローカル PC にある証明書 / 鍵のパスと証明書 / 鍵ファイル名を入力します。64 文字まで指定します。「Browse/参照」 ボタンをクリックしてローカル PC 上の証明書 / 鍵ファイルの場所を指定できます。	
Destination File	証明書 / 鍵がストアされるスイッチの場所を指定します。64 文字までで指定できます。	

「Restore」ボタンをクリックしてリストアを開始します。

## Certificate & Key Backup to HTTP (HTTP を使用した証明書 / 鍵バックアップ)

HTTP サーバに証明書 / 鍵バックアップを行います。

Tools > Certificate & Key Upgrade & Backup > Certificate & Key Backup to HTTP をクリックし、設定画面を表示します。

Certificate & Key Backup to HTTP			
Unit Source File	1 64 chars	Backup	

図 19-27 Certificate & Key Backup to HTTP 画面

#### 画面に表示される項目:

項目	説明	
Unit	設定するユニットを選択します。	
Source File	スイッチにあるパスとファイル名を入力します。64 文字まで指定します。	

## Certificate & Key Backup to TFTP(TFTP を使用した証明書 / 鍵バックアップ)

TFTP サーバに証明書 / 鍵バックアップを行います。

Tools > Certificate & Key Upgrade & Backup > Certificate & Key Backup to TFTP をクリックし、設定画面を表示します。

Firmware Backu	Firmware Backup to TFTP		
Unit	1		
TFTP Server IP	• • IPv4		
	○ IPv6		
VRF Name	12 chars		
Source File	64 chars		
Destination File	64 chars		
		Backup	

図 19-28 Certificate & Key Backup to TFTP 画面

#### 画面に表示される項目:

項目	説明	
Unit	設定するユニットを選択します。	
TFTP Server IP	TFTPサーバのIPアドレスを入力します。「IPv4」オプションを選択した場合、TFTPサーバのIPv4アドレスを入力します。「IPv6」	
	オプションを選択した場合、TFTP サーバの IPv6 アドレスを入力します。	
VRF Name	VRF インスタンス名を 12 字以内で入力します。	
Source File	スイッチにあるパスとファイル名を入力します。64文字まで指定します。	
Destination File	証明書/鍵ファイルがバックアップされる TFTP サーバの場所(パス/ファイル名)を指定します。64 文字までで指定できます。	

「Backup」ボタンをクリックしてバックアップを開始します。

## Certificate & Key Backup to FTP (FTP を使用した証明書 / 鍵バックアップ)

#### FTP を使用して証明書 / 鍵バックアップを実行します。

Tools > Certificate & Key Backup & Backup > Certificate & Key Backup to FTP をクリックし、設定画面を表示します。

Firmware Backup to FTP		
Unit	1	
FTP Server IP	• • IPv4	
	◯ IPv6	
TCP Port (1-65535)		
User Name	32 chars	
Password	15 chars	
VRF Name	12 chars	
Source File	64 chars	
Destination File	64 chars	
		Backup

図 19-29 Certificate & Key Backup to FTP 画面

## 画面に表示される項目:

項目	説明
Unit	設定するユニットを選択します。
FTP Server IP	FTP サーバの IP アドレスを入力します。「IPv4」オプションを選択した場合、FTP サーバの IPv4 アドレスを入力します。「IPv6」 オプションを選択した場合、FTP サーバの IPv6 アドレスを入力します。
TCP Port	TCP ポート番号(1-65535)を指定します。
User Name	FTP 接続のユーザ名(32 字以内)を指定します。
Password	FTP 接続のパスワード(15 字以内)を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Source File	スイッチにある証明書 / 鍵のパスと証明書 / 鍵ファイル名を入力します。64 文字まで指定します。
Destination File	証明書 / 鍵がストアされる FTP サーバの場所を指定します。64 文字までで指定できます。

## Certificate & Key Backup to RCP(RCP を使用した証明書 / 鍵バックアップ)

RCP を使用して証明書 / 鍵バックアップを実行します。

Tools > Certificate & Key Backup & Backup > Certificate & Key Backup to RCP をクリックし、設定画面を表示します。

Firmware Backu	Firmware Backup to RCP		
Unit	1		
RCP Server IP			
User Name	32 chars		
VRF Name	12 chars		
Source File	64 chars		
Destination File	64 chars		
	Backup		

図 19-30 Certificate & Key Backup to RCP 画面

## 画面に表示される項目:

項目	説明	
Unit	設定するユニットを選択します。	
RCP Server IP	RCP サーバの IP アドレスを入力します。	
User Name	RCP 接続のユーザ名(32 字以内)を指定します。	
VRF Name	VRF インスタンス名を 12 字以内で入力します。	
Source File	スイッチにある証明書 / 鍵のパスと証明書 / 鍵ファイル名を入力します。64 文字まで指定します。	
Destination File	証明書 / 鍵がストアされる RCP サーバの場所を指定します。64 文字までで指定できます。	

「Backup」ボタンをクリックしてバックアップを開始します。

#### Certificate & Key Backup to SFTP (SFTP を使用した証明書 / 鍵バックアップ)

## SFTP を使用して証明書 / 鍵バックアップを実行します。

Tools > Certificate & Key Backup & Backup > Certificate & Key Backup to SFTP をクリックし、設定画面を表示します。

Firmware Backup to SFTP		
Unit		
SFTP Server IP		
Authentication Method	Password	
User Name	32 chars	
Password	15 chars	
VRF Name	12 chars	
Source File	64 chars	
Destination File	64 chars	
	Backup	

図 19-31 Certificate & Key Backup to SFTP 画面

#### 画面に表示される項目:

項目	説明
Unit	設定するユニットを選択します。
SFTP Server IP	SFTP サーバの IP アドレスを入力します。
Authentication Method	認証方法が表示されます。
User Name	SFTP 接続のユーザ名(32 字以内)を指定します。
Password	SFTP 接続のパスワード(15 字以内)を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Source File	ローカル PC にある証明書 / 鍵のパスと証明書 / 鍵ファイル名を入力します。64 文字まで指定します。「Browse/ 参照」 ボタンをクリックしてローカル PC 上の証明書 / 鍵ファイルの場所を指定できます。
Destination File	証明書 / 鍵がストアされるスイッチの場所を指定します。64 文字までで指定できます。

# Log Backup(ログファイルのバックアップ)

## Log Backup to HTTP(HTTP サーバを使用したログファイルのバックアップ)

HTTP サーバを使用してローカル PC へのシステムログのバックアップを行います。

## **Tools > Log Backup > Log Backup to HTTP** をクリックし、設定画面を表示します。

Log Backup to HTTP		
Log Type	ick Log Backup	
図 19-32 Log Backup to HTTP 画面		

#### 画面に表示される項目:

項目	説明
Log Type	HTTP を使用してローカル PC にバックアップするログの種類を選択します。「System Log」オプションを選択するとシステ
	ムログエントリをバックアップします。「Attack Log」オプションを選択すると攻撃関連のログをバックアップします。
 「Backup」ボタンをクリックしてバックアップを開始します。	

# Log Backup to TFTP(TFTP サーバを使用したログファイルのバックアップ)

#### **Tools > Log Backup > Log Backup to TFTP** をクリックし、設定画面を表示します。

Log Backup to TFTP		
TFTP Server IP	• IPv4	
	○ IPv6	
VRF Name	12 chars	]
Destination File	64 chars	]
Log Type	System Log O Attack Log	
		Backup

図 19-33 Log Backup to TFTP 画面

#### 画面に表示される項目:

項目	説明
TFTP Server IP	TFTP サーバの IP アドレスを入力します。「IPv4」オプションを選択した場合、TFTP サーバの IPv4 アドレスを入力します。「IPv6」 オプションを選択した場合、TFTP サーバの IPv6 アドレスを入力します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Destination File	ログファイルがストアされる TFTP サーバの場所を指定します。64 文字までで指定できます。
Log Type	バックアップするログの種類を選択します。「System Log」オプションを選択するとシステムログエントリをバックアップ します。「Attack Log」オプションを選択すると攻撃関連のログをバックアップします。

## Log Backup to RCP(RCP サーバを使用したログファイルのバックアップ)

RCP サーバへのシステムログのバックアップを行います。

#### **Tools > Log Backup > Log Backup to RCP** をクリックし、設定画面を表示します。

CP Server IP	· · ·		
User Name	32 chars		
VRF Name	12 chars		
Destination File	64 chars		
Log Type	System Log      Attack Log		
		Backup	

図 19-34 Log Backup to RCP 画面

## 画面に表示される項目:

項目	説明	
RCP Server IP	RCP サーバの IP アドレスを入力します。「IPv4」オプションを選択した場合、RCP サーバの IPv4 アドレスを入力します。「IPv6」 オプションを選択した場合、RCP サーバの IPv6 アドレスを入力します。	
User Name RCP 接続のユーザ名(32 字以内)を指定します。		
VRF NameVRF インスタンス名を 12 字以内で入力します。		
Destination File	ログファイルがストアされる RCP サーバの場所を指定します。64 文字までで指定できます。	
Log Type	バックアップするログの種類を選択します。「System Log」オプションを選択するとシステムログエントリをバックアップ します。「Attack Log」オプションを選択すると攻撃関連のログをバックアップします。	

「Backup」ボタンをクリックしてバックアップを開始します。

## Log Backup to SFTP(SFTP サーバを使用したログファイルのバックアップ)

SFTP サーバへのシステムログのバックアップを行います。

#### **Tools > Log Backup > Log Backup to SFTP** をクリックし、設定画面を表示します。

Log Backup to SFTP				
SFTP Server IP	and the second sec			
Authentication Method	Password			
User Name	32 chars			
Password	15 chars			
VRF Name	12 chars			
Destination File	64 chars			
Log Type	System Log O Attack Log			
		Backup		

図 19-35 Log Backup to SFTP 画面

## 画面に表示される項目:

項目	説明		
SFTP Server IP	SFTP サーバの IP アドレスを入力します。「IPv4」オプションを選択した場合、SFTP サーバの IPv4 アドレスを入力します。「IPv6」		
	オプションを選択した場合、SFTP サーバの IPv6 アドレスを入力します。		
User Name SFTP 接続のユーザ名(32 字以内)を指定します。			
PasswordSFTP 接続のパスワード(15 字以内)を指定します。			
VRF Name VRF インスタンス名を 12 字以内で入力します。			
Destination File	ログファイルがストアされる SFTP サーバの場所を指定します。64 文字までで指定できます。		
Log Type	バックアップするログの種類を選択します。「System Log」オプションを選択するとシステムログエントリをバックアップ		
	します。「Attack Log」オプションを選択すると攻撃関連のログをバックアップします。		

# Ping

「Ping」は指定した IP アドレスに ICMP Echo パケットを送信するプログラムです。宛先の機器はスイッチから送信された "echoes" に応答します。これはネットワーク上のスイッチと機器の接続状況を確認するうえで非常に有効です。

Tools > Ping をクリックし、設定画面を表示します。

Ping	Ping				
Ping	Ping Access Class				
AC	L Name Please Select	Action Add 🔽		Apply	
			Added Access Class		
			ACL		
- IPv4	Ping				
	VRF Name	12 chars	1		
۲	Target IPv4 Address	1 (1) (1	]		
0	Domain Name	255 chars	]		
	Ping Times (1-255)		☑ Infinite		
	Timeout (1-99)	1	sec		
	Frequency (0-86400)	0	sec		
	Length (1-1420)	56	bytes		
	ToS (0-255)	0	]		
	Stop Time (0-99)	0	]		
	Source IPv4 Address		]		
				Start	
IPv6	Ping				
	Target IPv6 Address	22221	7		
	Domain Name	255 chars			
	Ping Times (1-255)	200 011010			
	Timeout (1-99)	1	sec		
	Frequency (0-86400)	0	sec		
	Length (1-1420)	56	bytes		
	Stop Time (0-99)	0			
	Source IPv6 Address				
			_	Start	

図 19-36 Ping 画面

## 画面に表示される項目:

項目	説明		
	Ping Access Class		
ACL Name	ACL 名(32 字以内)を指定します。「Please Select」で既存の ACL を選択することができます。		
Action	実行する動作を「Add」「Clear」から指定します。		
	IPv4 Ping		
VRF Name   VRF インスタンス名を 12 字以内で入力します。			
Target IPv4 Address Ping する IPv4 アドレスを入力します。			
Domain Name 検出するシステムのドメイン名を入力します。			
Ping Times繰り返し行う Ping の回数を入力します。1 から 255 の間で指定できます。「Infinite」にチェックを入れるとプログラ止するまで「ICMP Echo」パケットを送信します。			
Timeout         Ping メッセージが到達するまでのタイムアウトの時間を指定します。1 から 99 (秒) までの間で指定できます。指定時           にパケットが IP アドレスを検出できない場合、Ping パケットは破棄されます。			
Frequency     Ping 頻度 (0-86400)を指定します。			
Length         Ping 長(1-1420/バイト)を指定します。送信データバイトの数になります。初期値は 56 で、ICMP ヘッダ           トと結合した時に、64 の ICMP データバイトになります。あらゆる「VLAN」「IEEE 802.1Q タグ長」は含まれ			
ToS	ToS 値(0-255)を指定します。ICMP データグラムの QoS を指定します。		
Stop Time	停止時間(0-99)を指定します。本項目で指定の回数を過ぎると Ping を停止します。「0」に指定すると自動的には止まらず、 「Stop」をクリックするまで続きます。		
Source IPv4 Address	送信元 IPv4 アドレスを入力します。もし現在のスイッチが一つ以上の IP アドレスを保持している場合、そのうちのどれか を入力することが可能です。入力した IPv4 アドレスはリモートホストに送信されるパケットの送信元 IP アドレスやプライ マリ IP アドレスになります。		

項目	説明			
	IPv6 Ping			
Target IPv6 Address	s Ping する IPv6 アドレスを入力します。			
Domain Name	 Jomain Name 検出するシステムのドメイン名を入力します。			
Ping Times	繰り返し行う Ping の回数を入力します。1 から 255 の間で指定できます。 「Infinite」にチェックを入れるとプログラムが停止するまで「ICMP Echo」パケットを送信します。			
Timeout	eout Ping メッセージが到達するまでのタイムアウトの時間を指定します。1 から 99 (秒) までの間で指定できます。指定時 にパケットが IP アドレスを検出できない場合、Ping パケットは破棄されます。			
Frequency	Ping 頻度(0-86400)を指定します。			
Length	Ping 長(1-1420/バイト)を指定します。送信データバイトの数になります。初期値は 56 で、ICMP ヘッダデータの 8 パトと結合した時に、64 の ICMP データバイトになります。あらゆる「VLAN」「IEEE 802.1Q タグ長」は含まれません。			
Stop Time 停止時間(0-99)を指定します。本項目で指定の回数を過ぎると Ping を停止します。「0」に指定すると自動的 「Stop」をクリックするまで続きます。				
Source IPv6 Address	送信元 IPv6 アドレスを入力します。もし現在のスイッチが一つ以上の IP アドレスを保持している場合、そのうちのどれかを入力することが可能です。入力した IPv6 アドレスはリモートホストに送信されるパケットの送信元 IP アドレスやプライマリ IP アドレスになります。			

「Start」ボタンをクリックして、各個別セクションでの Ping テストを実行します。

「Please Select」をクリックすると、以下の画面が表示されます。



図 19-37 Ping (Please Select) 画面

```
設定するエントリを選択し「OK」をクリックします。
```

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「IPv4 Ping」セクションで「Start」をクリックすると以下の「IPv4 Ping Result」画面が表示されます。

1] Reply from 10.90.90.90, time<10ms	
2] Reply from 10.90.90.90, time<10ms	A
3] Reply from 10.90.90.90, time<10ms	
4] Reply from 10.90.90.90, time<10ms	
Ping Statistics for 10.90.90	
Packets: Sent = 4, Received = 4, Lost = $0$	

図 19-38 IPv4 Ping Result 画面

「Stop」ボタンをクリックして、Ping テストを停止します。 「Back」ボタンをクリックして、前の画面に戻ります。

# Trace Route (FV-XIV-F)

ネットワークとホスト間のルートをトレースします。

Tools > Trace Route の順にメニューをクリックし、以下の画面を表示します。

Trac	e Route		
IPv4	Trace Route		
	VRF Name	12 chars	]
۲	IPv4 Address	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
0	Domain Name	255 chars	
	Initial TTL (1-255)	1	
	Max TTL (1-255)	30	
	Port (1-65535)	33434	
	Timeout (1-65535)	5	sec
	Length (1-1420)	40	bytes
	ToS (0-255)	0	
	Frequency (0-86400)	0	sec
	Source IPv4 Address		]
	Probe Number (1-1000)	1	Start
IPv6	Trace Route		
۲	IPv6 Address	2233::1	
0	Domain Name	255 chars	
	Initial TTL (1-255)	1	
	Max TTL (1-255)	30	
	Port (1-65535)	33434	
	Timeout (1-65535)	5	sec
	Length (1-1420)	40	bytes
	Frequency (0-86400)	0	sec
	Source IPv6 Address	2233::2	
	Probe Number (1-1000)	1	Start
		-	

図 19-39 Trace Route 画面

|--|

説明
IPv4 Trace Route
VRF インスタンス名を 12 字以内で入力します。
宛先 IPv4 アドレスを入力します。
宛先のドメイン名を入力します。
初期トレースルートリクエストの有効期間です。
トレースルートリクエストの有効期間。2つのデバイス間のネットワークパスを検索する場合に traceroute コマンド
が通過するルータの最大数です。
ポート数。ポート番号 1-65535 で指定します。
リモートデバイスからのレスポンスを待つ場合のタイムアウトの時間を定義します。1-65535(秒)で指定します。
Ping 長(1-1420/ バイト)を指定します。送信データバイトの数になります。
ToS 値(0-255)を指定します。外部データグラムの IP ヘッダを指定します。
Ping 頻度(0-86400)を指定します。
送信元 IPv4 アドレスを入力します。もし現在のスイッチが一つ以上の IP アドレスを保持している場合、そのうちの
どれかを入力することが可能です。
予定された traceroute パス上の次のホップに probe パケットをスイッチが送信する回数を指定します。 初期値は1です。

「Start」ボタンをクリックし、Traceroute プログラムを開始します。
項目	説明		
IPv6 Trace Route			
IPv6 Address	宛先ステーションの IPv6 アドレスを入力します。		
Domain Name	宛先のドメイン名を入力します。		
Initial TTL(1-255)	初期トレースルートリクエストの有効期間です。		
Max TTL(1-255)	トレースルートリクエストの有効期間。2つのデバイス間のネットワークパスを検索する場合に traceroute コマンド が通過するルータの最大数です。		
Port (1-65535)	ポート番号を 1-65535 で指定します。		
Timeout (1-65535)	リモートデバイスからのレスポンスを待つ場合のタイムアウトの時間を定義します。1-65535(秒)で指定します。		
Length	Ping 長(1-1420/ バイト)を指定します。送信データバイトの数になります。		
Frequency	Ping 頻度(0-86400)を指定します。		
Source IPv6 Address	送信元 IPv6 アドレスを入力します。もし現在のスイッチが一つ以上の IP アドレスを保持している場合、そのうちの どれかを入力することが可能です。		
Probe Number(1-1000)	予定された traceroute パス上の次のホップに probe パケットをスイッチが送信する回数を指定します。 初期値:1		

「Start」ボタンをクリックし、Traceroute プログラムを開始します。

#### 以下の結果画面が表示されます。

[1] <10 ms Frace complete	[10.90.90.90]	^
		~

図 19-40 Trace Route Result (IPv4) 画面

「Back」ボタンをクリックして、前の画面に戻ります。

#### Reset (リセット)

スイッチの設定内容を工場出荷時状態に戻します。

Tools > Reset をクリックし、次の設定画面を表示します。

Reset	
Reset	
The Switch will reset to its factory default settings and then reboot.	
The Switch will reset to its factory default settings and then reboot. This option excludes the IP address.	
O The Switch will reset to its factory default settings and not reboot. This option excludes the stacking information.	Apply
	CKM1

図 19-41 Reset System 画面

画面に表示される項目:

項目	説明		
The Switch will reset to its factory default settings	スイッチを工場出荷時設定にリセットして、保存、再起動を実行します。		
and then repoot.	(ドアトレス、スタック情報を含む)		
The Switch will reset to its factory default settings and then reboot. This option excludes the IP address.	スイッチを工場出荷時の設定に戻し、保存、再起動を実行します。 (IP アドレスは除く)		
The Switch will reset to its factory default settings and not reboot. This option excludes the stacking information.	スイッチを工場出荷時設定にリセットしますが、再起動は行いません。 (スタック情報は除く)		

「Apply」ボタンをクリックして、リセット操作を開始します。

#### Reboot System(システム再起動)

スイッチの再起動を行います。

Tools > Reboot をクリックし、以下の設定画面を表示します。

Reboot System	
Reboot System	
Do you want to save the settings ?  Yes No If you do not save the settings, all changes made in this session will be lost.	Reboot

図 19-42 Reboot System 画面

画面に表示される項目:

項目	説明
Yes	スイッチは再起動する前に現在の設定を保存します。
No	スイッチは再起動する前に現在の設定を保存しません。すべての設定情報は破棄され、最後に保存した時の設定が使われます。
Reboot	スイッチは再起動します。

#### 「Reboot」をクリックして再起動を開始します。

Rebo	ot System	
	Saving and rebooting system, please wait	
	10%	
⊠ 19-43	System Rebooting 画面	

#### DLMS Settings(DLMS 設定)

本項目では「D-Link License Management System」(DLMS)の設定、表示を行います。

ライセンスは特定の機能を有効にする場合において指定します。「License keys」は購入する必要があります。物理的なパッケージとして印刷されているか、メールやポータルなどで画面に表示される場合もあります。ユーザは「Global Registration Portal」(GRP)にてライセンスキーを登録し、アクティベーションコードを取得する必要があります。様々な機能の有効化/ロック解除において、適切にアクティベーションコードを取得してインストールする必要があります。アクティベーションコードのインストールに成功すると、スイッチは再起動しライセンスのアクティベートを行います。

Tools > DLMS Settings をクリックし、次の設定画面を表示します。

DLMS Settings			
DLMS Settings			
Unit	1 💌		
DLMS Activation Code	25 chars		Apply
Device Default License :	MI		
Current Active License :	MI		
Unit 1 Settings			
License Model		Activation Code	Time Remaining

#### 図 19-44 DLMS Settings 画面 画面に表示される項目:

回面に仅小される項目・			
項目	説明		
Unit	設定を行うユニットを指定します。		
DLMS Activation Code	DLMS アクティベーションコード(25 字以内)を指定します。		

「Apply」ボタンをクリックして、リセット操作を開始します。

#### 付録 A パスワードリカバリ手順

弊社スイッチのパスワードのリセットについて記述します。ネットワークにアクセスを試みるすべてのユーザに認証は必要で重要です。 権限のあるユーザを受け入れるために使用する基本的な認証方法は、ローカルログイン時にユーザ名とパスワードを利用することです。ネットワー ク管理者は、パスワードが忘れられたり、壊れた場合に、これらのパスワードをリセットする必要があります。このパスワードリカバリ機能は、そ のような場合にネットワーク管理者を助けるものです。以下にパスワードを容易に回復するパスワードリカバリ機能の使用方法を説明します。

以下の手順を終了するとパスワードはリセットされます。

- セキュリティの理由のため、パスワードリカバリ機能は物理的にデバイスにアクセスすることが必要です。そのため、デバイスのコンソールポートへの直接接続を行っている場合だけ、本機能を適用することができます。ユーザは端末エミュレーションソフトを使用して、スイッチのコンソールポートに端末または PC を接続する必要があります。
- **2.** 電源をオンにします。「Password Recovery Mode」に入るためには、「UART init」が 100% までロードされた後 2 秒以内に、ホットキー「^」 を押します。「Password Recovery Mode」に一度入ると、スイッチのすべてのポートが無効になります。

```
Password Recovery Mode
Switch(reset-config)#
```

3. 「Password Recovery Mode」では、以下のコマンドのみ使用できます。

コマンド	説明
no enable password	全アカウントレベルのパスワードを削除します。
no login password	ローカルログイン方法をクリアします。
no username	全ローカルユーザアカウントを削除します。
password-recovery	パスワードリカバリ手順を開始します。
reload	スイッチを再起動します。
reload clear	起動中の設定を工場出荷値に戻し、保存、スイッチを再起動します。
running-config	
show running-config	起動中の設定を表示します。
show username	ローカルユーザアカウント情報を表示します。

### 付録 B システムログエントリ

スイッチのシステムログに表示される可能性のあるログイベントとそれらの意味を以下に示します。

Critical (重大)、Warning (警告)、Informational (報告)、Notice (通知)

ログの内容	緊急度	イベントの説明
802.1X		
802.1X authentication fail [due to <reason>] from (Username: <username>.</username></reason>	Critical	802.1X 認証に失敗しました。
<interface-id>, MAC: <mac-address>)</mac-address></interface-id>		
パラメータ説明:		
・ username:認証されているユーザ名		
<ul> <li>interface-id:スイッチインタフェース番号</li> </ul>		
・ mac-addres:認証されたナバイスの MAC アドレス		
802.1X authentication success (Username: <username>, <interface-id>, MAC: <mac- address&gt;)</mac- </interface-id></username>	Informational	802.1X 認証に成切しました。
・ UseIndine · 応証されたユーリム · interface_id · インタフェースタ		
・ mac-addres: 認証されたデバイスの MAC アドレス		
AAA	1	
AAA is <status></status>	Informational	AAA グローバルステートが有効または
パーイーク説明:		無効です。
NJアーン記号・ status:AAA が有効または無効		
Successful login through $<$ exec-type> [from $<$ client-ip>] authenticated by	Informational	ログインに成功しました。
AAA <aaa-method> <server-ip> (Username: <username>)</username></server-ip></aaa-method>		
パラメータ説明:		
・ exec-type::EXEC タイプ。		
(例:Console、Telnet、SSH、Web、Web(SSL))		
・ client-ip:IP フロトコルを通し有効なクライアントの IP アドレス		
• aaa-metnod · 認証/J I/。		
(例: Horle、local、server) ・ server-in:認証方式がリモートサーバの場合の AAA サーバ IP アドレス		
<ul> <li>username:認証されるユーザ名</li> </ul>		
Login failed through <exec-type> [from <client-ip>] authenticated by AAA</client-ip></exec-type>	Warning	ログインに失敗しました。
<aaa-method> <server-ip> (Username: <username>)</username></server-ip></aaa-method>		
パラメー々説明:		
・exec-type::EXEC タイプ。		
例:Console、Telnet、SSH、Web、Web(SSL)		
・ client-ip:IP プロトコルを通し有効なクライアントの IP アドレス		
• aaa-method:認証方式。		
(例:none、local、server)		
・ server-ip:認証方式がリモートサーバの場合の AAA サーバ IP アドレス		
・ username:認証されるユーザ名		
Login failed through <exec-type> [from <client-ip>] due to AAA server</client-ip></exec-type>	Warning	サーバタイムアウト、または不適切な
<server-ip> timeout (Username: <username>)</username></server-ip>		設定によるログイン失敗。
パラメータ説明:		
・ exec-type::EXEC タイプ。		
(例:Console、Telnet、SSH、Web、Web(SSL))		
・ client-ip:IP ブロトコルを通し有効なクライアントの IP アドレス		
・ server-Ip:AAA サーハ IF アドレ人		
・ username・脳証されるエーリム	1	

ログの内容	緊急度	イベントの説明
Successful enable privilege through <exec-type> [from <client-ip>]</client-ip></exec-type>	Informational	特権の有効化に成功しました。
authenticated by AAA <aaa-method> <server-ip> (Username: <username>)</username></server-ip></aaa-method>		
バラメータ説明:		
・ exec-type::EXEL タイノ。 (例::Console_Telest_CCL_Web_Web(CCL))		
(例)、Console、Telnet、SSH、Web、Web(SSL)/		
<ul> <li>Client-IP・IP ノロトコルを通し有効なグライアントのIP アトレス         <ul> <li>app. method:認証方式</li> </ul> </li> </ul>		
(例: none_local_server)		
・ server-in:認証方式がリモートサーバの場合の AAA サーバ IP アドレス		
<ul> <li>username:認証されるユーザ名</li> </ul>		
Enable privilege failed through <exec-type> [from <client-ip>] authenticated by</client-ip></exec-type>	Warning	特権の有効化に失敗しました。
AAA <aaa-method> <server-ip> (Username: <username>)</username></server-ip></aaa-method>		
パラメータ説明:		
・ exec-type:EXEC タイプ。		
(例:Console、Telnet、SSH、Web、Web(SSL))		
・ client-ip:IP プロトコルを通し有効なクライアントの IP アドレス		
• aaa-method:認証方式。		
(例:none、local、server)		
・ server-IP: 認証万式かリモートサーハの場合の AAA サーハ IP アドレス		
<ul> <li>username · 認証されるユーザ名</li> </ul>		
Enable privilege failed through <exec-type> [from <client-ip>] due to AAA</client-ip></exec-type>	warning	リモートサーハか有効なハスワート認
server < server-ip> timeout (osername: < username>)		証リクエストに心谷しません。
パラメー々説明・		
・exec-type・FXFC タイプ		
(例:Console、Telnet、SSH、Web、Web(SSL))		
・ client-ip:IP プロトコルを通し有効なクライアントの IP アドレス		
・ server-ip:AAA サーバIP アドレス		
・ username:認証されるユーザ名		
RADIUS server <server-ip> assigned VID: <vid> to port <interface-id> (Username:</interface-id></vid></server-ip>	Informational	RADIUS が有効な VLAN ID 属性を割り
<username>)</username>		当てました。
パラメータ説明:		
・ server-ip:RADIUS サーバの IP アドレス		
・ vid:KADIUS サーハから認証された VLAN ID 割り当く		
<ul> <li>Interface=Id: 認証されにクライアノトの小一下番号 </li> <li>username: 認証されるユーザタ</li> </ul>		
• Username : 認証されるユーリム	lofo montion ol	
RADIUS server <server-ip> assigned <direction> bandwidth: <threshold> to port &lt;</threshold></direction></server-ip>	Informational	RADIUS か有効な市域幅属性を割り当く ました
パラメータ説明:		
・server-ip:RADIUS サーバの IP アドレス		
<ul> <li>direction::帯域幅制御の方向。</li> </ul>		
(例:イングレスまたはイーグレス)		
• threshold: サーバから認証された帯域幅のしきい値割り当て		
• interface–id:認証されたクライアントのポート番号		
・ username:認証されるユーザ名		
RADIUS server < server-ip> assigned 802.1p default priortiy: < priority> to port <	Informational	RADIUS が有効な優先度属性を割り当て
interface -id> (Username: <username>)</username>		ました。
パラメータ説明:		
・ server-ip:RADIUS サーバの IP アドレス		
<ul> <li>priority: RADIUS サーバから認証された優先度割り当て</li> </ul>		
<ul> <li>INTERFACE-ID:認証されたクライアントのホート番号</li> <li>INTERFACE-ID:認証されたクライアントのホート番号</li> </ul>		
• username・認証されるユーサ名	1	1

ログの内容	緊急度	イベントの説明	
RADIUS server <server-ip> assigns <username> ACL failure at port &lt; interface -id&gt;</username></server-ip>	Warning	RADIUS が ACL スクリプトを割り当て	
( <acl-script>)</acl-script>		ましたが、不十分なリソースのためシ	
		ステムへの適用に失敗しました。	
パラメータ説明:			
・ server-ip:RADIUS サーバの IP アドレス			
・ username:認証されるユーザ名			
<ul> <li>interface-id:認証されたクライアントのポート番号</li> </ul>			
・ acl-script:RADIUS サーバから認証された ACL スクリプト			
ARP			
Conflict IP was detected with this device (IP: <ipaddr>, MAC: <macaddr>, Port</macaddr></ipaddr>	Warning	Gratuitous ARP は重複した IP を検出し	
<[unitID:]portNum>, Interface: <ipif_name>).</ipif_name>		ました。	
パラメータ説明:			
・ ipaddr:IP アドレス			
・ macaddr:MAC アドレス			
・ unitID:ユニット番号			
<ul> <li>portNum:ポート番号</li> </ul>			
<ul> <li>ipif_name: IP インタフェース名</li> </ul>			
ARP Spoofing Prevention			
Gateway <ipaddr> is under attack by <macaddr> from <intf-name></intf-name></macaddr></ipaddr>	Warning	偽の ARP パケットが ARP スプーフィン グ防止に検出されました。	
パラメータ説明:			
・ ipaddr:IP アドレス			
・ macaddr:MAC アドレス			
・ intf_name:インタフェース名			
Auto image			
The downloaded firmware was successfully executed by DHCP Auto image update	Informational	DHCP 自動イメージによるファーム	
(TFTP Server IP: <ipaddr>)</ipaddr>		ウェアダウンロードは成功しました。	
パラメータ説明:			
・ ipaddr:IP アドレス			
The downloaded firmware was not successfully executed by DHCP Autoimage	Informational	DHCP 自動イメージによるファーム	
update (TFTP Server IP: <ipaddr>)</ipaddr>		ウェアダウンロードは失敗しました。	
パラメータ説明:			
・ ipaddr:IP アドレス			
Auto Save			
CONFIG-6-DDPSAVECONFIG: [Unit <unitid>, ]Configuration automatically saved to</unitid>	Informational	DDP の設定情報が自動で保存されまし	
flash due to configuring from DDP(Username: <username>, IP: <ipaddr>)</ipaddr></username>		た。	
パラメータ説明:			
・ unitID:ボックス ID			
・ username:ユーザ名			
・ ipaddr:IP アドレス			

ログの内容	緊急度	イベントの説明
Auto Surveillance VLAN	·	
New surveillance device detected ( <interface-id>, MAC: <mac-address>)</mac-address></interface-id>	Informational	インタフェースで新しい監視デバイス が検出されました。
パラメータ説明:		
<ul> <li>interface-id:インタフェース名(ID)</li> <li>mac-address:MAC アドレス</li> </ul>		
<interface-id> add into surveillance VLAN <vid></vid></interface-id>	Informational	サーベイランス VLAN が有効のインタ フェースが自動的にサーベイランス
パラメータ説明:		VLAN に追加されました。
<ul> <li>interface-id:インタフェース名(ID)</li> <li>vid:VLAN ID</li> </ul>		
<interface-id> remove from surveillance VLAN <vid></vid></interface-id>	Informational	インタフェースがサーベイランス VLAN
		から離脱しました。同時に一定の期間
パラメータ説明:		内に当該のインタフェースに監視デバ
<ul> <li>interface-id:インタフェース名(ID)</li> <li>id: 1/(ANID)</li> </ul>		イスが検出されす、ロクメッセージが
VIG . VLAN ID		送信されました。
BGP 6 ESTABLISH: BGP connection is successfully established (Peer-sinaddra)	Informational	ピアとの BCD ESM の構築に成功しまし
bar-o-LorAblion, bar connection is successfully established (reel.ipadul>).	Innonnational	た。
• IPAUGI · IP / F V A	Informational	DCD 接続が通常通り用いました
BGP-0-NORWIALCLOSE: BGP connection is normally closed (Peer:<1paddr>).	Informational	BGP 接続が通吊通り闭しました。
パラメータ説明:		
・ ipaddr:IP アドレス		
BGP-4-ERRCLOSE: BGP connection is closed due to error (Code: <num> Subcode:<num> Field:<field> Peer:<ipaddr>).</ipaddr></field></num></num>	Warning	BGP 接続かエラーによって閉じまし た。(エラーコード、エラーサブコード、 RFC 参照のデータ項目)
パラメータ説明:		
・ num:エラーコード / サブコード		
<ul> <li>filed:エフー発生場所</li> <li>inoddr: ID スピース</li> </ul>		
・ IPaddi ・ IP アトレス PCD 4 PC// INIKOW/NEPP-PCD Notific upknown Error code/pum) Sub Error	Warning	
code(num), Peer: <ipaddr>.</ipaddr>	warning	RFC42/1 による未定我のエフーコート /エラーサブコード付きBGP 通知パケッ トの受信
パラメータ説明:		
<ul> <li>num:エラーコード/サブコード</li> <li>ipaddr: IP アドレス</li> </ul>		
BGP-4-BADNHOP: BGP Update Attr NHop: Erroneous NHop <ipaddr> Peer:<ipaddr>.</ipaddr></ipaddr>	Warning	 ネクストホップポイントがローカルイ
パニノーク発明・		ンタフェースの BGP アップデートパ
・ ipaddr:IP アドレス		
BGP-4-EVENTCLOSE: BGP connection is closed due to Event: <num> (Peer:<ipaddr>).</ipaddr></num>	Warning	イベント発生による BGP 接続の切断(イ ベントは PEC で完美)
パラメータ説明:		
<ul> <li>num: RFC4271 で定義されたイベント</li> <li>ipaddr: IP アドレス</li> </ul>		
BGP-4-NOTIFYCI OSE: BGP connection is closed due to Notify: Code <num> Subcode</num>	Warning	   通知パケットの受信による RGP 接続の
<num> (Peer:<ipaddr>).</ipaddr></num>		切断 (RFC 定義のエラーコード / エラー サブコード)
パラメータ説明:		
・ num:RFC4271 で定義されたエラーコード / エラーサブコード		
・ ipaddr:IP アドレス		

	网络萨	
	<u> </u>	
BGP-6-PEERPFXMAX: The number of prefix received reaches <num>, max <limit></limit></num>	Informational	BGP のフリフィクスが最大しきい値に
(Peer < ipaddr>).		到達しました。
パニメーカ部門・		
・ IIUIII:文信したフリフィンス Limit:丹信可能たプロファクスの値		
・ infine · CEPTEなノリンイノスの値 ・ inaddr · IPアドレフ		
PCD 6 TOTAL DEVMAY. The total number of prefy received reaches may prefy limit	Informational	一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一
BGP-0-TOTALPFXMAX: The total number of prefix received reaches max prefix limit.	Informational	文信 BGP ノリノイクスの総数かしさい 値を招えす」た
PCD 4 PCV/ ININECEAS4DATH: Paceined AS4 DATH attribute from power (4 bytes AS)	Warning	$E^{-2}$ 超えるじた。 新しい PCD ピア ( $A$ バイト AS) から
DGP-4-RCVONNECEAS4PATH. RECEIVED AS4-PATH allindule from new (4-bytes AS)	warning	
peer. (Peer < ipador >).		BGP が小安な「AS4-PAIH」 属性を受信
パラメーク説明:		
POD 4 DOULININGCAS 4ACCER: Descined AS4 ACCERCATOR attribute from now		
BGP-4-RCVUNNECEAS4AGGRE: RECEIVED AS4-AGGREGATOR allipule from new	warning	
(4-bytes AS) peer. (Peer < Ipador>).		BGP か不安な「AS4-AGGREGATOR」属       株式兵信しました
パラメーク説明・		
・ inaddr · IP アドレス		
	Marping	
BGP-4-RCVASCONFEDINAS4PATH: Received AS_CONFED_SEQUENCE of AS_	vvarning	BGP か「AS4-PATH」 属性の「AS_
CONFED_SET path segment type in AS4-PATH attribute. (Peer <ipaddr>).</ipaddr>		CONFED_SEQUENCE OF AS_CONFED_
		SEI」ハスセクメフトダイフを受信しま
		C/Z.
BGP-4-RCVBADAS4AGGKE: Received invalid AS4- AGGREGATOR attribute. Value :	Warning	BGP 無効な「AS4-AGGREGATOR」属性 キャー・
<pre><string> (Peer <ipaddr>).</ipaddr></string></pre>		を受信しました。
BGP-4-RCVBADAS4PATH: Received invalid AS4-PATH attribute. Value : <string> (Peer</string>	Warning	BGP 無効な「AS4-PAIH」属性を受信し
<li>(ipaddr&gt;).</li>		ました。
BPDU Potection(BPDU 攻撃防御)		
<interface-id> enter STP BPDU under protection state (mode: <mode>)</mode></interface-id>	Informational	BPDU アタックが発生しました。
パラメータ説明:		
・ interface-id:STP BPDU アタックが検出されたインタフェース		
・ mode: インタフェースの BPDU フロテクションモード。モードは、ドロップ、		
フロック、またはシャットタウンにすることかできます。 		
<pre><interface-id> recover from BPDU under protection state</interface-id></pre>	Informational	SIP BPDU 攻撃から回復しました。
Interface-Id:STP BPDU / タックか検出されたインタフェース	l	
CFM	1	
CFM cross-connect. VLAN: <vlanid>, Local(MD Level:<mdlevel>, Interface-</mdlevel></vlanid>	Critical	クロス接続が検出されました。
id>, Direction: <mepdirection>) Remote(MEPID:<mepid>, MAC:<macaddr>)</macaddr></mepid></mepdirection>		
バラメータ説明:		
・vlanid:MEPのVLAN ID		
・ mdlevel:MEPのMDレベル		
<ul> <li>Interface-id: MEPのインタフェース</li> </ul>		
<ul> <li>mepdirection:MEPの方向。</li> <li>(Function + 10.4 + 5)</li> </ul>		
(Inward」 または Ioutward」)		
<ul> <li>mepid: MEP の MEPID。 10」は不明な MEIPD を意味します。</li> </ul>		
・ macaddr: MEP の MAC アドレス。すべて「0」となっている場合は、不明な		
・ CFIMI ハートリェアセート (びは、リセート MEP 情報 (mepid/macaddr) は不明 マオ		
[		

ログの内容	緊急度	イベントの説明
CEM arror CCM MD Loval: Emdlovels VI AN: Evianids Local/Interface: Einterface.ids	Warning	エラー CEM CCM パケットが検出され
Direction: cmondirections.) Demote(MEDID: cmonids. MAC: cmocoddrs.)	warning	
• VIANIC MEP () VLAN ID		
・ mdlevel: MEP の MD レベル		
・ interface-id:MEP のインタフェース		
<ul> <li>mepdirection: MEP の方向。</li> </ul>		
(linward」または「outward」)		
<ul> <li>mepid:MEPのMEPID。「0」は不明なMEIPDを意味します。</li> </ul>		
・ macaddr:MEP の MAC アドレス。すべて「0」となっている場合は、不明な		
MAC アドレスです。		
・ CFM ハードウェアモードでは、リモート MEP 情報(mepid/macaddr)は不明		
です。		
CFM remote down. MD Level: <mdlevel>, VLAN:<vlanid>, Local(Interface:<interface-< td=""><td>Warning</td><td>MEP の CCM パケットを受信できませ</td></interface-<></vlanid></mdlevel>	Warning	MEP の CCM パケットを受信できませ
id>, Direction: <mepdirection>)</mepdirection>		$h_{0}$
パラメータ説明:		
vlanid · MEP ( VLANLID		
· mdlavel · MEP () MD L/ VI/		
· Indeversimer of Nid D. (1)		
・ Interface-id 、 MEP のインダフェース		
• mepid: MEP の MEPID。「0」は不明な MEIPD を意味します。		
・ macaddr:MEPのMACアドレス。		
CFM remote MAC error. MD Level: <mdlevel>, VLAN:<vlanid>,</vlanid></mdlevel>	Warning	リモートMEPのMACレポートがエラー
Local(Interface: <interface-id>, Direction:<mepdirection>)</mepdirection></interface-id>		状態です。
パラメータ説明:		
・vlanid:MEPのVLAN ID		
・ mdlevel:MEP の MD レベル		
・ interface-id:MEP のインタフェース		
・ mepdirection:MEP の方向。		
(「inward」または「outward」)		
<ul> <li>mepid: MEPの MEPID。「0」は不明な MEIPD を意味します。</li> </ul>		
・macaddr:MEPのMACアドレス。		
CEM remote detects a defect MD Level-cmdlevel> VI AN:-cvlanid>	Informational	レート MEP による CEM 不良の検出
L ocal/Interface.cida Direction: <mandirection>)</mandirection>	Informational	
Local(Interface-lu>, Direction.		
• VIANIG . MEP O VLAN ID		
• mdlevel : MEP () MD DAVD		
・ interface-id:MEPのインタフェース		
<ul> <li>mepdirection: MEPの方向。</li> </ul>		
(linward」または「outward」)		
<ul> <li>mepid:MEPのMEPID。「0」は不明なMEIPDを意味します。</li> </ul>		
・ macaddr:MEP の MAC アドレス。		
CFM Extension		
AIS condition detected. MD Level: <mdlevel>, VLAN:<vlanid>,</vlanid></mdlevel>	Notice	AIS コンディションの検出
Local(Interface: <interface-id>, Direction:<mepdirection>, MEPID:<mepid>)</mepid></mepdirection></interface-id>		
パラメータ説明:		
・ vlanid:MEP の VLAN ID		
・ mdlevel:MEP の MD レベル		
・ interface-id:MEP のインタフェース		
・mendirection:MEPの方向。		
$([inward] \pm tct [outward])$		
<ul> <li>menid: MFP の MFPID。「0」は不明な MFIPD を意味します。</li> </ul>		

ログの内容	緊急度	イベントの説明
AIS condition cleared. MD Level: <mdlevel>, VLAN:<vlanid>,</vlanid></mdlevel>	Notice	AIS コンディションの解消
Local(Interface: <interface-id>, Direction:<mepdirection>, MEPID:<mepid>)</mepid></mepdirection></interface-id>		
パラメータ説明:		
・ vlanid:MEP の VLAN ID		
・ mdlevel:MEP の MD レベル		
・ interface-id:MEP のインタフェース		
・ mepdirection:MEP の方向。		
(「inward」または「outward」)		
<ul> <li>mepid:MEPのMEPID。「0」は不明なMEIPDを意味します。</li> </ul>		
LCK condition detected. MD Level: <mdlevel>, VLAN:<vlanid>,</vlanid></mdlevel>	Notice	LCK コンディションの検出
Local(Interface: <interface-id>, Direction:<mepdirection>, MEPID:<mepid>)</mepid></mepdirection></interface-id>		
パラメータ説明:		
・vlanid:MEPのVLAN ID		
・ mdlevel:MEP の MD レベル		
・ interface-id:MEP のインタフェース		
・ mepdirection:MEP の方向。		
(linward」または「outward」)		
・ mepid:MEP の MEPID。「0」は不明な MEIPD を意味します。		
LCK condition cleared. MD Level: <mdlevel>, VLAN:<vlanid>,</vlanid></mdlevel>	Notice	LCK コンディションの解消
Local(Interface: <interface-id>, Direction:<mepdirection>, MEPID:<mepid>)</mepid></mepdirection></interface-id>		
パラメータ説明:		
・ vlanid:MEP の VLAN ID		
• mdlevel : MEP 0) MD LAN		
・ Interface-Id:MEPのインタノエース		
<ul> <li>mepdirection:MEPの万同。</li> <li>(Figure 1): またない「「「」」」</li> </ul>		
• Thepid: MEP の MEPID。 10」は不明な MEIPD を意味します。		
Configuration/Firmware	Informational	
[Unit <unitile], <session="" by="" jrinnwale="" upgraded=""> successiony (Username.</unitile],>	Informational	ファームウェアのアッククレードに成
<pre>cuseIname&gt;[, if. <ipaddi>, iviAC. <imacaddi>], Server if. <serverif>, file Name.</serverif></imacaddi></ipaddi></pre>		切しよした。
<pre><pre>cpatifrie&gt;)</pre></pre>		
パラメーク説明・		
• $\operatorname{cession}$ · $\operatorname{7-H}(\pi_{1})$		
・ username <sup>・</sup> 現在のログインコーザタ		
• inaddr: $2\pi$ $2\pi$ $2\pi$		
• macaddr • $\sqrt{2}$		
• server $P \cdot \# - x \cap P = F + x$		
・ nathEile・サーバのパスとファイル名		
[Unit <unit[d>] Firmware upgraded by <session> upsuccessfully (Lisename)</session></unit[d>	Warning	ファームウェアのアップグレードに生
[Unit Cumtos, ] minimule upgraded by Cossion's disdecession's (Oserhame.	Warning	
<pre>custifiers)</pre>		× 0 × 0/2°
│パラメータ説明:		
・ unitID:ユニット ID		
・ session:ユーザのセッション		
・ username:現在のログインユーザ名		
・ ipaddr:クライアントの IP アドレス		
・ macaddr:クライアントの MAC アドレス		
・ serverIP:サーバの IP アドレス		
・ pathFile:サーバのパスとファイル名		

「ログの内容	緊急度	イベントの説明
[Unit_cunitID> ]Eirmware unloaded by csession> successfully (Username:		ファートウェアのアップロードに成功
[Unit CumuD2, Ji innivate uploaded by Csession2 succession9 (Osemaine.	Informational	
<pre></pre>		
パラメー々説明・		
• session : $7 - \# D + \psi > 3 > 2$		
・ username <sup>・</sup> 現在のログインコーザタ		
• inaddr $\cdot \sqrt{2}$		
• macaddr: $2\pi/2$ $\lambda$ $\lambda$ $\lambda$		
• server IP : $\pm - \sqrt{0}$ IP $= 7 \times 123$		
・ nathEile・サーバのパスとファイルタ		
Ulpit supitIDs TEirmware upleaded by scossions upsuccossfully (Licorname)	Warping	ファームウェアのアップロードに生敗
[UTIL < UTILID>, JFITTIWATE UPIDAUED by < SESSIOT> UTSUCCESSIUTY (USETTIATTE:	warning	ノアームウェアのアップロードに天敗
<pre>cuseIname&gt;[, if. <ipadui>, MAC. <inacadui>], Server if. <serverif>, file Name. <pre>cpathEilos)</pre></serverif></inacadui></ipadui></pre>		
<pre><pre>cpatifie&gt;)</pre></pre>		
パニマーク苦明・		
• $\operatorname{unitio} \cdot \underline{\neg} = \forall \neg \operatorname{unitio}$		
<ul> <li>Session、ユーリのビダノヨノ</li> <li>usorpama・現在のログインスーザタ</li> </ul>		
・ username、現在のロッキンユーッカー 、 ipaddr・クライアントのID アドレフ		
• servenin $\cdot$ $- \pi \omega r \gamma - \tau \omega r$		
[Unit <unitid>, ]Configuration downloaded by <session> successfully. (Username:</session></unitid>	Informational	コンフィクレーションのタワンロード
<pre><username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverip>, File Name:</serverip></macaddr></ipaddr></username></pre>		に成切しました。
<pre><pre>cpathFile&gt;)</pre></pre>		
・ unitiD:ユニット ID		
<ul> <li>session: ユーサのセッション</li> <li>現在の中がくション</li> </ul>		
<ul> <li>username:現任のログインユーザ名 </li> </ul>		
<ul> <li>macaddr: クライアントの MAC アドレス</li> </ul>		
<ul> <li>pathFile、リーハのハスとファイル名</li> </ul>		
[Unit <unitid>, ]Configuration downloaded by <session> unsuccessfully. (Username:</session></unitid>	Warning	コンノイクレーションのタウンロード
<username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverip>, File Name:</serverip></macaddr></ipaddr></username>		に矢敗しました。
<pathfile>)</pathfile>		
・ unitiD:ユニット ID		
<ul> <li>session: ユーサのセッション</li> </ul>		
Username:現在のログインユーザ名     Lot ちち イマント の ID コパトコ		
<ul> <li>patnFile、リーハのハスとファイル名</li> </ul>		
[Unit <unitid>, ]Configuration uploaded by <session> successfully. (Username:</session></unitid>	Informational	コンフィグレーションのアップロード
<username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverip>, File Name:</serverip></macaddr></ipaddr></username>		に成功しました。
<pathfile>)</pathfile>		
・ session:ユーザのセッション		
<ul> <li>username: 現在のロクインユーザ名</li> <li>・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・</li></ul>		
<ul> <li>macaddr: クライアントの MAC アドレス</li> </ul>		
I • patnhle・サーハのハスとファイル名	1	1

	<b> </b>	イベントの説明	
[Unit_cunitID> ]Configuration unloaded by csessions unsuccessfully (Userpare)	Warning	コンフィグレーションのアップロード	
[Unit <unitib_, <session="" by="" jconingulation="" uploaded=""> unsuccession, (Username, elementarie, elementarie), (Username, eleme</unitib_,>	warning		
cuselliane>[, ir. <ipaudi>, MAC. <inacadui>], serverir. <serverir>, rile Name.</serverir></inacadui></ipaudi>			
<pre><pre>cpatifrie&gt;)</pre></pre>			
  パラメータ説明:			
・ unitID:ユニット ID			
・ session:ユーザのセッション			
<ul> <li>username:現在のログインユーザ名</li> </ul>			
・ ipaddr:クライアントのIP アドレス			
・ macaddr:クライアントの MAC アドレス			
・ serverIP:サーバの IP アドレス			
・ pathFile:サーバのパスとファイル名			
[Unit <unitid>. ]Downloaded by <session> unsuccessfully. (Username: <username>[. IP:</username></session></unitid>	Warning	未知のタイプのファイルのダウンロー	
<pre><ipaddr>, MAC: <macaddr>], Server IP: <serverip>, File Name: <pathfile>)</pathfile></serverip></macaddr></ipaddr></pre>		ドに失敗しました。	
│パラメータ説明:			
・ unitID:ユニット ID			
・ session:ユーザのセッション			
・ username:現在のログインユーザ名			
・ ipaddr:クライアントの IP アドレス			
・ macaddr:クライアントの MAC アドレス			
・ serverIP:サーバの IP アドレス			
・ pathFile:サーバのパスとファイル名			
DAD	•		
Duplicate address <ipv6address> on <interface-id> via receiving Neighbor</interface-id></ipv6address>	Warning	DAD の間に DUT が「Neighbor	
Solicitation Messages		Solicitation」(NS) メッセージを重複ア	
		ドレスとともに受信、ログに追加…	
パラメータ説明:			
・ ipv6address:NS メッセージの IPv6 アドレス			
・ interface-id:ポートインタフェース ID			
Duplicate address <ipv6address> on <interface-id> via receiving Neighbor</interface-id></ipv6address>	Warning	DAD の間に DUT が「Neighbor	
Advertisement Messages		Advertisement」(NA) メッセージを重	
		複アドレスとともに受信、ログに追加	
パラメータ説明:			
・ ipv6address:NA メッセージの IPv6 アドレス			
・ interface-id:ポートインタフェース ID			
DDM			
Optical transceiver <interface-id> <component> <high-low> warning threshold</high-low></component></interface-id>	Warning	SFP パラメータのどれかが警告しきい	
exceeded		値を超えました。	
パラメータ説明:			
・ interface-id:ポートインタフェース ID			
・ component:DDM のしきい値タイプ。しきい値タイプは以下のうちのどれか			
10.			
- temperature			
- supply voltage			
- bias current			
- IX power			
- KX power			
- high-low:高もしくは低しきい値			

ログの内容	緊急度	イベントの説明
Optical transceiver < interface-id> < component> < high-low> alarm threshold	Critical	SEP パラメータのどわかがアラームし
exceeded		きい値を超えました。
パラメータ説明:		
・ interface-id:ポートインタフェース ID		
• component:DDM のしきい値タイプ。しきい値タイプは以下のうちのどれか		
- temperature		
- supply voltage		
- bias current		
- TX power		
- RX power		
- high-low:高もしくは低しきい値		
Optical transceiver <interface-id> <component> back to normal</component></interface-id>	Warning	SFP パラメータのどれかが警告しきい
	_	値から回復しました。
パラメータ説明:		
・ interface-id:ポートインタフェース ID		
• component:DDM のしきい値タイプ。しきい値タイプは以下のうちのどれか		
10.		
- temperature		
- supply voltage		
- bias current		
- TX power		
- RX power		
- high-low:高もしくは低しきい値		
DHCPv6 Client		
DHCPv6 client on interface <ipif-name> changed state to [enabled   disabled]</ipif-name>	Informational	DHCPv6 クライアントインタフェース
		管理者ステートが変更されました。
パラメータ説明:		
・ <ipif-name>:DHCPv6 クライアントインタフェース名</ipif-name>		
DHCPv6 client obtains an ipv6 address < ipv6address > on interface <ipif-name></ipif-name>	Informational	DHCPv6 クライアントが DHCPv6 サー
		バから ipv6 アドレスを取得しました。
パラメータ説明:		
・ ipv6address:DHCPv6 サーバから取得された ipv6 アドレス		
・ ipif-name:DHCPv6 クライアントインタフェース名		
The IPv6 address < ipv6address > on interface <ipif-name> starts renewing</ipif-name>	Informational	DHCPv6 サーバから取得した IPv6 アド
		レスが更新を開始します。
パラメータ説明:		
・ ipv6address:DHCPv6 サーバから取得された ipv6 アドレス		
・ ipif-name:DHCPv6 クライアントインタフェース名		
The IPv6 address < ipv6address > on interface <ipif-name> renews success</ipif-name>	Informational	DHCPv6 サーバから取得された IPv6 ア
		ドレスの更新に成功しました。
パラメータ説明:		
・ ipv6address:DHCPv6 サーバから取得された ipv6 アドレス		
・ ipif-name:DHCPv6 クライアントインタフェース名		
The IPv6 address < ipv6address > on interface <ipif-name> starts rebinding</ipif-name>	Informational	DHCPv6 サーバから取得された IPv6 ア
		ドレスのリバインドを開始します。
パラメータ説明:		
・ ipv6address:DHCPv6 サーバから取得された ipv6 アドレス		
・ ipif-name:DHCPv6 クライアントインタフェース名		
Log Message: The IPv6 address < ipv6address > on interface <ipif-name> rebinds</ipif-name>	Informational	DHCPv6 サーバから取得された IPv6 ア
success		ドレスがリバインドに成功しました。
パラメータ説明:		
・ ipv6address:DHCPv6 サーバから取得された ipv6 アドレス		
• ipif-name:DHCPv6 クライアントインタフェース名		

ログの内容	緊急度	イベントの説明
The IPv6 address < ipv6address > on interface <ipif-name> was deleted</ipif-name>	Informational	DHCPv6 サーバからの IPv6 アドレスが
		削除されました。
パラメータ説明:		
<ul> <li>ipv6address: DHCPv6 サーバから取得された ipv6 アドレス         <ul> <li>if and ipv6 クドレス</li> </ul> </li> </ul>		
<ul> <li>Ipit-name: DHCPv6 クライアントインタフェース名</li> </ul>		
DHCPV6 client PD on interface <intt-name> changed state to <enabled disabled=""  =""></enabled></intt-name>	Informational	DHCPV6 クライ アント PD インダノエー フの管理者フラートが亦再されました
パラメータ説明:		への皆连有へり一下が多史されよした。
・ intf-name:DHCPv6 クライアント PD インタフェース名		
DHCPv6 client PD obtains an ipv6 prefix < ipv6networkaddr> on interface <intf-name></intf-name>	Informational	DHCPv6 クライアント PD が、デリゲ
		イションルータから IPv6 プレフィック
パラメータ説明:		スを取得しました。
<ul> <li>ipv6networkaddr:デリゲイションルータから取得した IPv6 プレフィックス</li> </ul>		
・ intf-name : DHCPv6 クライアント PD インタフェース名		
The IPv6 prefix < ipv6networkaddr > on interface <intf-name> starts renewing</intf-name>	Informational	デリゲイションルータから取得した
パーメーク説明・		IPV6 ノレノイックスは更新を開始しま す
・ inv6networkaddr・デリゲイションルータから取得した IPv6 プレフィックス		9 0
<ul> <li>intf-name: DHCPv6 クライアント PD インタフェース名</li> </ul>		
The IPv6 prefix < ipv6networkaddr > on interface <intf-name> renews success</intf-name>	Informational	デリゲイションルータから取得した
		IPv6 プレフィックスは更新に成功しま
パラメータ説明:		した。
・ ipv6networkaddr : デリゲイションルータから取得した IPv6 プレフィックス		
・ intf-name : DHCPv6 クライアント PD インタフェース名		
The IPv6 prefix < ipv6networkaddr > on interface <intf-name> starts rebinding</intf-name>	Informational	デリゲイションルータから取得した
		IPv6 ブレフィックスはリバインティン
		クを開始しより。
<ul> <li>IPV01etworkduur: フリケイフョンルーブルつび付したirv0フレフィンフハ</li> <li>intf-name・DHCPv6 クライアント PD インタフェース名</li> </ul>		
The IPv6 prefix < inv6petworkaddr > on interface < intf-name > rebinds success	Informational	↓ デリゲイションルータから取得した
		IPv6 プレフィックスはリバインドに成
パラメータ説明:		功しました。
・ ipv6networkaddr : デリゲイションルータから取得した IPv6 プレフィックス		
・ intf-name : DHCPv6 クライアント PD インタフェース名		
The IPv6 prefix < inv6petworkaddr > op interface < intf-name> was deleted	Informational	デリゲイションルータからの IPv6 プレ
The involution of the second		フィックスは削除されました。
パラメータ説明:		
・ ipv6networkaddr : デリゲイションルータから取得した IPv6 プレフィックス		
・ intf-name : DHCPv6 クライアント PD インタフェース名		
DHCPv6 Relay		
DHCPv6 relay on interface <ipif-name> changed state to [enabled   disabled]</ipif-name>	Informational	特定のインタフェースの管理者ステー
		トの DHCPv6 リレーが変更されました。
The address of the DHCPv6 Server pool spool-names is used up	Informational	DHCDv6 サーバプールのアドレスが柱
		るしました。
パラメータ説明:		
<ul> <li><pool-name>: DHCPv6 サーバプール名</pool-name></li> </ul>		
The number of allocated ipv6 addresses of the DHCPv6 Server pool is equal to 4096.	Informational	割り当てられた IPv6 アドレス数が
		4096 に達しました。
DLMS		
Illegal activation code (AC: <string25>).</string25>	Informational	入力したアクティベーションコードが
		違法のものです。
$\bullet$ <string25>, <math>f \mathcal{I} \mathcal{I} \mathcal{I} \mathcal{I} \mathcal{I} \mathcal{I} \mathcal{I} \mathcal{I}</math></string25>		

	1	1
ログの内容	緊急度	イベントの説明
License expired (license: <license-model>, AC: <string25>).</string25></license-model>	Critical	ライセンスが期限切れです。
Ĩ		
パラメータ説明:		
・ <string25>:アクティベーションコード</string25>		
License successfully installed (license models, AC), (string2Es)	Informational	ニノセンスのノンストールに成功した
License successiuily installed (license: <license-model>, AC: <string2>&gt;).</string2></license-model>	Informational	フィセンスのインストールに成功しま
		U/Eo
パラメータ説明:		
・ <li><li><li><li>icense-model&gt;:ライセンスモデル名</li></li></li></li>		
・ <string25>:アクティベーションコード</string25>		
Unbound Activation Code (AC: <string25>).</string25>	Critical	アクティベーションコードが紐づいて
		いません (Unbound)。
パラメータ説明:		
<ul> <li><string25>・アクティベーションコード</string25></li> </ul>		
Licence will evolve a 20 deve (licence readely AC, setvine 25)	Informational	ニノトンフの期間が 20 日以中に泣って
License will expire in 30 days. (license: <license-model>, AC: <string25>).</string25></license-model>	Informational	フイセンスの期限か30日以内に迫って
		いより。
ハフメータ説明:		
・ <license-model>:ライセンスモデル名</license-model>		
・ <string25>:アクティベーションコード</string25>		
DNS Resolver		
[DNS_RESOLVER(1):]Duplicate Domain name case name: <domain-name>_static IP-</domain-name>	Informational	重複するドメイン名キャッシュが追加
<pre>cinaddr&gt; dynamic IP-cinaddr&gt;</pre>		さわ ダイナミックドメインタキャッ
		これに、パープミングーン・ローイン
パニメ _ カ 部 明 ・		ノエが前家でれていてい
domainame · トメイノ名文字列		
・ ipaddr:IP アドレス		
DoS Prevention		
<pre><dos-type> is dropped from (IP: <ip-address> Port <interface-id>).</interface-id></ip-address></dos-type></pre>	Notice	DoS 攻撃を検出しました。
パラメータ説明:		
・ dos-type・DoS 攻撃タイプ		
in address: ID アドレフ		
· Ip-address. · IF / I VA		
・ Interface-io:・1 ノダフェース名		
DULD	<b>1</b>	
DULD <interface-id> is detected as unidirectional link.</interface-id>	Warning	DULD はインタフェースが単一方向性
		であることを検出しました。
パラメータ説明:		
・ INTERFACE-ID:インタフェース名		
Dynamic ARP Inspection (DA	AI)	
Illegal ARP <type> packets (IP: <in-address> MAC: <mac-address> VI AN <vlan-id></vlan-id></mac-address></in-address></type>	Warning	DAI が無効た ABP パケットを検出しま
on zinterface_id>)	l vvarning	
		0/20
type:ARP ハケットの種類。ARP ハケットか、「request」か「ARP response」     type:ARP ハケットの		
かを示します。		
・ ip-address:IP アドレス		
・ mac-address:MAC アドレス		
• vlan-id:VLAN ID		
・ interface-id:インタフェース ID		
Legal ARP <type> packets (IP: <ip-address>, MAC: <mac-address>. VI AN <vlan-id>.</vlan-id></mac-address></ip-address></type>	Informational	DAI が有効な ARP パケットを検出しま
on <interface-id>)</interface-id>		
パラメーク説明:		
<ul> <li>type・AKF ハワットの性親。AKP ハワットか、「request」か、AKP response」</li> <li>いたーレナナ</li> </ul>		
かを示します。		
・ ip-address:IP アドレス		
・ mac-address:MAC アドレス		
• vlan-id:VLAN ID		
・ interface-id:インタフェース ID		

	取刍卋	イベントの説明
	系忌反	イインドの説明
	1	
"Manual Switch is issued on node (MAC: <macaddr>, instance <instanceid>)"</instanceid></macaddr>	Warning	ノードにスイッナかイシューされまし +
パニマーク部門・		/ζ <sub>0</sub>
・ Inde-address · MAC アドレス		
• IllistalicelD • 1 > X × > X ID	10/	
Signal fail detected on node (MAC: <macaddr>, instance <instanceid>)</instanceid></macaddr>	Warning	ノートにシクナル矢敗が検出されまし
		Γ <sub>ο</sub>
・ mac-address 、 MAC アドレス		
InstanceID - 1 / X & / X ID		
"Signal fail cleared on node(MAC: <macaddr>, instance <instanceid>)"</instanceid></macaddr>	Warning	ノードのシクナル失敗がクリアされま
		L <i>T</i> E <sub>0</sub>
・ mac-address MAC アドレス		
InstanceID:インスタンスID		
"Force Switch is issued on node (MAC: <macaddr>, instance <instanceid>)"</instanceid></macaddr>	Warning	フォーススイッチがイシューされまし
		た。
パラメータ説明:		
・mac-address:MACアドレス		
InstanceID:インスタンス ID		
"Clear command is issued on node (MAC: <macaddr>, instance <instanceid>)"</instanceid></macaddr>	Warning	クリアコマンドがイシューされました。
パラメータ説明:		
・ mac-address:MAC アドレス		
・ InstanceID:インスタンス ID		
"RPL owner conflicted on the node (MAC: <macaddr>, instance <instanceid>)"</instanceid></macaddr>	Warning	RPL オーナーがノードでコンフリクト
		しています。
パラメータ説明:		
・ mac-address:MAC アドレス		
・ InstanceID:インスタンス ID		
Ethernet OAM		
OAM dying gasp event received (Port <interface-id>)</interface-id>	Warning	リモートで「Dying gasp」イベントが
		発生。
パラメータ説明:		
・ interface-id:インタフェース ID		
Device encountered an OAM dying gasp event	Warning	ローカルで「Dying gasp」イベントが
		発生。
OAM critical event received (Port< interface-id >)	Warning	リモートで危機的なイベントが発生。
	l	
パラメータ説明:		
・ interface-id:インタフェース ID		
Device $encountered an OAM critical event (Port< interface-id > < condition >)$	Warning	ローカルで危機的たイベントが発生。
	Warning	
パラメータ説明:		
・interface-id・インタフェース ID		
・ condition: 合機的た リンクイベントにより発生した状況について表示します。		
(例: OAM disable Port shutdown Port link down Packet overload たど)		
(1) for sumbal pariad a part received (Part c interface id 2)	Marning	リエートズェニーシンギル期間ノベン
Litor symbol period event received (Port < Interface-IQ >)	warning	「シェートでエノーシン小ル期间1 ハノ」 「トが発生」
パラメーク説明・		
· interface_id・インタフェーフ ID		
Finishing of the second of the	Mareire e	/ ノベンノレンマッチ
Error mame event received(Port < Interface-Id >)	warning	エラーフレーム1 ハノトか発生。
パーメーク説明・		
ハノクーダ研明・ interface id: インクフェーフ ID		
Error frame period event received(Port < interface-id >)	Warning	リモートでエラーフレーム期間イベン
		トの発生。
・ Interface-Id:インダノエー人 ID		

ログの内容	緊急度	イベントの説明
Error frame seconds summary event received (Port < interface-id >)	Warning	リモートでエラーフレーム秒サマリイ ベントが発生。
パラメータ説明:		
・ interface-id:インタフェース ID		
OAM Remote loopback started (Port < interface-id >)	Warning	リモートでループバックが発生。
	Warning	
パラメーク説明・		
interface id: (2/27-710		
OAM Remote loopback stopped (Port < interface-id >)	Warning	リモート ごルーノハックか停止。 
パラメータ説明:		
・ interface-id:インタフェース ID		
Device encountered an errored symbol period event (Port <interface-id>)</interface-id>	Warning	シンボル期間イベントでエラーが発生
パラメータ説明:		
· interface-id·インタフェース ID		
	14/2	
Device encountered an errored frame event (Port <interface-id>)</interface-id>	vvarning	ノレームイベントでエラーが発生して
		いより。
ハフメータ説明:		
・ interface-id:インタフェース ID		
Device encountered an errored frame period event (Port <interface-id>)</interface-id>	Warning	フレーム期間イベントでエラーが発生
		しています。
パラメータ説明:		
・ interface-id:インタフェース ID		
Device encountered an errored frame seconds summary event (Port <interface-id>)</interface-id>	Warning	フレーム秒サマリイベントでエラーが
パラメータ説明:		発生しています。
・ interface-id:インタフェース ID		
Interface	1	1
	Informational	キート おいい クマップレオレキ
Port <portivum> inik up, <iiiik state=""></iiiik></portivum>	Informational	ホードがリング ゲッノしました。
<ul> <li>portNum・ハート 金方。 登奴 値 ぐ (機 なの) 論理 ハート 金方</li> </ul>		
• IINK STATE - リンク状態(例,IOUMIDPS FULL duplex)		
Port <portnum> link down</portnum>	Informational	ポートがリンクダウンしました。
パラメータ説明:		
• portNum:ポート番号。整数値で機器の論理ポート番号		
IP Directed Broadcast		
IP Directed Broadcast packet rate is high on subnet. [(IP: %s)]	Informational	あるサブネットにおいて IP ダイレクト
		ブロードキャストレートが毎秒 50 パ
パラメータ説明:		ケットを超えました。
<ul> <li>・ IP:ブロードキャスト IP 宛先アドレス。</li> </ul>		
	Informational	
IP Directed Broadcast rate is high	Informational	
	l	バ毋ヤジ100 ハケットを超えました。
IP Source Guard (IPSG)	1	1
Failed to set IPSG entry due to no hardware rule resource. (IP: <ipaddr>, MAC:</ipaddr>	Warning	DHCP スヌーピングエントリを ISPG
<macaddr>, VID: <vlanid>, Interface <interface-id>)</interface-id></vlanid></macaddr>		テーブルにセットするに当たり、ハー
		ドウェアルールのリソースがない場合、
パラメータ説明:		シスログが記録されます。
・ ip-address:IP アドレス		
・ mac-address:MAC アドレス		
• vlan-id:VLAN ID		
・ interface-id:インタフェース ID		

	取刍由	イベントの説明
IDu6 Source Guard	糸芯反	
Failed to set IPv6SG entry due to no hardware rule resource. (IP: <ipaddr>, MAC: <macaddr>, VID: <vlanid>, Interface <interface-id>)</interface-id></vlanid></macaddr></ipaddr>	Warning	DHCP スヌーピングエントリを IPv6SG テーブルにセットするに当たり、ハー ドウェアルールのリソースがない場合、
<b>パラメータ説明:</b> ・ ip-address:IPv6 アドレス		シスログが記録されます。
<ul> <li>mac-address: MACアドレス</li> </ul>		
<ul> <li>vlanid: VLAN ID</li> <li>interface-id: インタフェース ID</li> </ul>		
	1	
Failed to glean (IP: <ipaddr>_MAC: <macaddr>_VID: <vlanid> Port <interface-< td=""><td>Notice</td><td>IPv6 Data Glean に失敗しました。</td></interface-<></vlanid></macaddr></ipaddr>	Notice	IPv6 Data Glean に失敗しました。
ID>)		
パラメータ説明:		
VIANIC / F / A		
<ul> <li>INTERFACE_ID:インタフェース ID</li> </ul>		
Glean to recover (IP: <ipaddr>, MAC: <macaddr>, VID: <vlanid>, Port <interface-id>)</interface-id></vlanid></macaddr></ipaddr>	Informational	IPv6 Data Glean に成功しました。
パラメータ説明:		
<ul> <li>IPADDR: IPv6アドレス</li> </ul>		
<ul> <li>MACADDR: MACアドレス</li> </ul>		
• vlanid : VLAN ID		
・ INTERFACE_ID:インタフェース ID		
LACP		
Link Aggregation Group <group_id> link up.</group_id>	Informational	リンクアグリゲーショングループがリ ンクアップします。
パラメータ説明:		
・ group-id:リンクアップアグリゲーショングループのグループ ID		
Link Aggregation Group <group_id> link down.</group_id>	Informational	リンクアグリゲーショングループがリ ンクダウンします。
バラメータ説明: ・ group-id:リンクアップアグリゲーショングループのグループⅠD		
<pre><igreating <group="" a="" aggregation="" group="" id="" link="" stack="" to="">.</igreating></pre>	Informational	 メンバポートがリンクアグリゲーショ
パラメータ説明:		ングループにアタッチします。
<ul> <li>Ifname:アグリゲーショングループにアタッチするポートのインタフェース名</li> <li>group-id:リンクアップアグリゲーショングループのグループID</li> </ul>		
<pre></pre>	Informational	メンバポートがリンクアグリゲーショ
パニ ノ _ ケ 弐 叩・		ングループにデタッチします。
<ul> <li>・ Ifname:アグリゲーショングループにアタッチするポートのインタフェース名。</li> </ul>		
・ group-id:リンクアップアグリゲーショングループのグループ ID		
LBD(ループバック検知)		
IfInfo LBD loop occurred.	Critical	ポートベースモードでループバックが 検出されました。
<b>パラメータ説明:</b> ・ IfInfo:インタフェース情報		
IfInfo LBD loop recovered.	Critical	ポートベースモードでループバックか
  パラメータ説明:		ら回復しました。
<ul> <li>IfInfo: インタフェース情報</li> </ul>		
lfInfo VID <vlanid> LBD loop occurred.</vlanid>	Critical	VLAN ベースモードでループバックが
   パラメータ説明:		検出されました。 
<ul> <li>IfInfo: インタフェース情報</li> </ul>		
vlanID:VLAN ID		

	1	
ログの内容	緊急度	イベントの説明
IfInfo VID <vlanid> LBD loop recovered.</vlanid>	Critical	VLAN ベースモードでループバックか
		らポートが回復しました。
パラメータ説明:		
・ IfInfo:インタフェース情報		
• vlanID : VLAN ID		
Loop VLAN number overflow.	Critical	ループバックが発生した VLAN の数が
		指定の数に達しました。
LLDP-MED		
LLDP-MED topology change detected (on port <portnum>. chassis id:</portnum>	Notice	LLDP-MED トポロジの変更が検出
<chassistype>, <chassisid>, port id: <porttype>, <portid>, device class:</portid></porttype></chassisid></chassistype>		されました。
<deviceclass>)</deviceclass>		
パラメータ説明:		
・ portNum:ポート番号		
・ chassisType:シャーシ ID サブタイプ		
値のリスト:		
1. chassisComponent(1)		
2. interfaceAlias(2)		
3. portComponent(3)		
4. macAddress(4)		
5. networkAddress(5)		
6. interfaceName(6)		
7. local(7)		
- chassic D : Stat - St ID		
• Chassis $D$ · $\mathcal{P}_{\mathcal{T}} = \mathcal{P}_{\mathcal{T}} D$		
・ portype・小 「 」 クラメイク 値のリスト・		
1 interfaceAlias(1)		
2 portComponent(2)		
3 macAddress(3)		
4 networkAddress(4)		
5 interfaceName(5)		
6. agentCircuitld(6)		
7. local(7)		
・ portID:ポート ID		
・ deviceClass:LLDP-MED デバイスタイプ		

ログの内容	緊急度	イベントの説明
Conflict LLDP-MED device type detected ( on port < portNum >, chassis id:	Notice	LLDP-MED デバイスタイプの重複
< chassisType>, <chassisid>, port id: &lt; portType&gt;, <portid>, device class:</portid></chassisid>		が検出されました。
<deviceclass>)</deviceclass>		
パラメータ説明:		
<ul> <li>portNum:ポート番号</li> </ul>		
・ chassisType:シャーシ ID サブタイプ		
値のリスト:		
1. chassisComponent(1)		
2. interfaceAlias(2)		
3. portComponent(3)		
4. macAddress(4)		
5. networkAddress(5)		
6. interfaceName(6)		
7. local(7)		
・ chassisiD シャーン ID		
<ul> <li>port lype · ホート ID サノダイノ</li> <li>(古のリスト)</li> </ul>		
1世のリスト: 1 interface Alice(1)		
1. InterfaceAllds(1)		
2. policomponent(2)		
5. HacAddress(5)		
4.  hetwork-duless(4) 5 interfaceName(5)		
6 agentCircuitId(6)		
7 local(7)		
・ portID:ポート ID		
・ deviceClass:LLDP-MED デバイスタイプ		
Incompatible LLDP-MED TLV set detected ( on port < portNum >, chassis id:	Informational	LLDP-MED TLV の非互換性が検出され
< chassisType>, <chassisid>, port id: &lt; portType&gt;, <portid>, device class:</portid></chassisid>		ました。
<deviceclass>)</deviceclass>		
パラメータ説明:		
<ul> <li>portNum:ポート番号</li> </ul>		
・ chassisType : シャーシ ID サブタイプ		
値のリスト:		
1. chassisComponent(1)		
2. interfaceAlias(2)		
3. portComponent(3)		
4. macAddress(4)		
5. HetworkAddress(5) 6. interfaceName(6)		
$7 \log(7)$		
・ chassisID:シャーシ ID		
<ul> <li>portType:ポートIDサブタイプ</li> </ul>		
1. interfaceAlias(1)		
2. portComponent(2)		
3. macAddress(3)		
4. networkAddress(4)		
5. interfaceName(5)		
6. agentCircuitld(6)		
7. local(7)		
・ portID:ポート ID		
・ deviceClass:LLDP-MED デバイスタイプ		

ログの内容	緊急度	イベントの説明
Login/Logout		
[Unit <unitid>, ]Successful login through Console (Username: <username>)</username></unitid>	Informational	コンソール経由のログインに成功しま
		した。
パラメータ説明:		
・ unitID:ユニット ID		
• username、ユーリ名		
[Unit <unitid>, ] Login failed through Console (Username: <username>)</username></unitid>	vvarning	コンソール経田のログインに失敗しま
パラメータ説明:		
・ unitID:ユニット ID		
・ username:ユーザ名		
[Unit <unitid>, ] Console session timed out (Username: <username>)</username></unitid>	Informational	コンソールのセッションはタイムアウ
		トしました。
パラメータ説明:		
・ unitlD:ユニット ID		
・ username:ユーザ名		
[Unit <unitid>, ] Logout through Console (Username: <username>)</username></unitid>	Informational	コンソール経由でログアウトしました。
・ unitiD · ユニット ID username : ユーザタ		
• UserHallie、ユーリ石 Successful Legin through Telpet (Username: Successme) ID: Sinaddr Lin (Gaddress)	Informational	
succession login through reiner (osemanie, <usemanie>, iP: <ipador ipvoaddress=""  ="">)</ipador></usemanie>	Informational	Tellet 程田のログインに成功しま
パラメータ説明:		
・ username:現在のログインユーザ		
・ ipaddr:クライアントの IP アドレス		
・ ipv6addr:クライアントの IPv6 アドレス		
Login failed through Telnet (Username: <username>, IP: <ipaddr ipv6address=""  ="">)</ipaddr></username>	Warning	Telnet 経由のログインに失敗しま
		した。
パラメータ説明:		
<ul> <li>username: 現在のログインユーザ</li> <li>・</li> </ul>		
Ipvoduul · 771 / 7 F 0/ IPvo / F D A	Informational	
reinet session timed out (Osername: <username>, iP: <ipaddr ipvoaddress=""  ="">)</ipaddr></username>	Informational	Tellet のセッションはダイムアウトし 車」た
パラメータ説明:		6 0720
<ul> <li>username:現在のログインユーザ</li> </ul>		
・ ipaddr:クライアントの IP アドレス		
・ ipv6addr:クライアントの IPv6 アドレス		
Logout through Telnet (Username: <username>, IP: <ipaddr ipv6address=""  ="">)</ipaddr></username>	Informational	Telnet 経由でログアウトしました。
パラメーク説明・		
<b>ハノア テルヴ・</b> ・ username <sup>・</sup> 現在のログインコーザ		
• ipaddr: $2 = 7 = 7$		
<ul> <li>ipv6addr: クライアントの IPv6 アドレス</li> </ul>		

ログの内容	緊急度	イベントの説明
Successful login through SSH (Username: <username>, IP: <ipaddr>)</ipaddr></username>	Informational	SSH 経由のログインに成功しま
		した。
パラメータ説明:		
<ul> <li>username:現在のログインユーザ</li> <li>・ トレ・ケニ・パフト・クロフェドレス</li> </ul>		
• Ipaddr: $7747750$ IP $750$ IP $750$		
Login failed through SSH (Username: <username>, IP: <ipaddr>)</ipaddr></username>	Critical	SSH 経由のログインに失敗しま
		した。
• ipaddr: $2\pi T \nabla D \nabla T \nabla T$		
<ul> <li>ipv6addr: クライアントの IPv6 アドレス</li> </ul>		
SSH session timed out (Username: <username>, IP: <ipaddr>)</ipaddr></username>	Informational	SSHのセッションはタイムアウトしま した。
パラメータ説明:		
・ username:現在のログインユーザ		
・ ipaddr:クライアントの IP アドレス		
・ ipv6addr:クライアントの IPv6 アドレス		
Logout through SSH (Username: <username>, IP: <ipaddr>)</ipaddr></username>	Informational	SSH 経由でログアウトしました。
パラメータ説明:		
・ username:現在のログインユーザ		
・ ipaddr:クライアントの IP アドレス		
・ ipv6addr:クライアントの IPv6 アドレス		
MAC(MAC 認証)	1	
MAC-based Access Control host login success (MAC: <mac-address>, <interface-id>, VID: <vlan-id></vlan-id></interface-id></mac-address>	Informational	ホストは MAC 認証をパスしました。
<ul> <li>パラメータ説明:</li> <li>mac-address:ホストの MAC アドレス</li> <li>interface-id:ホストが認証されたインタフェース</li> <li>vlan-id:ホストが存在する VLAN ID</li> </ul>		
MAC-based Access Control host aged out (MAC: <mac-address>, <interface-id>, VID: <vlan-id>).</vlan-id></interface-id></mac-address>	Informational	ホストはエージアウトしました。
<b>パラメータ説明:</b> • mac-address:ホストの MAC アドレス • interface-id:ホストが認証されたインタフェース • vlan-id:ホストが存在する VLAN ID		
MAC-based Access Control host login fail (MAC: <mac-address>, <interface-id>, VID: <vlan-id>).</vlan-id></interface-id></mac-address>	Critical	ホストは認証に失敗しました。
<ul> <li>パラメータ説明:</li> <li>mac-address:ホストの MAC アドレス</li> <li>interface-id:ホストが認証されたインタフェース</li> <li>vlan-id:ホストが存在する VLAN ID</li> </ul>		
MAC-based Access Control enters stop learning state	Warning	デバイス全体で認証されたユーザ数が ユーザの最大制限数に達しました。
MAC-based Access Control recovers from stop learning state	Warning	デバイス全体で認証されたユーザ数が 時間間隔内のの最大ユーザ制限数未満 になりました。
<interface-id> enters MAC-based Access Control stop learning state</interface-id>	Warning	インタフェースの認証されたユーザ数 が最大ユーザ制限数に達しました。
<b>パラメータ説明:</b> <ul> <li>interface-id:ホストが認証されたインタフェース</li> </ul>		
<pre><interface-id> recovers from MAC-based Access Control stop learning state</interface-id></pre>	Warning	インタフェースの認証されたユーザ数
		が時間間隔内の最大ユーザ制限数未満
<b>ハファーダ説明</b> : ・ interface-id:ホストが認証されたインタフェース		になりました。
	1	

ログの内容	緊急度	イベントの説明
MLAG		
Multi-Chassis Link Aggregation Group <group id=""> <link status=""/></group>	Informational	MLAG グループのリンクステータスが
パラメータ説明:		
・ group id:MLAGのグループ ID		
<ul> <li>Link status: リンクステータス</li> </ul>		
値のリスト:		
1. link up:グループの最初のメンバポートがリンクアップ状態です。		
2. link down:グループの最後のメンバポートがリンクダウン状態です。		
The MLAG logical switch is <status></status>	Informational	MLAG 論理スイッチのステータスが変 更されました。
パラメータ説明:		
・ status:論理スイッチのステータス		
値のリスト:		
1. built up:MLAG の論理スイッチが確立しています。		
2. destroy:MLAG の論理スイッチが削除されました。		
The MLAG state is conflict ( <conflict>)</conflict>	Informational	MLAG グループで競合が発生しています。
パラメータ説明:		
<ul> <li>conflict: 競合の原因</li> </ul>		
値のリスト:		
1. domain is different:ドメインがピアデバイスと異なります。		
2. device id is same:デバイス D がビアスイッチと同じです。		
3. hello interval is different: hello 間隔かビアスイッチと異なります。		
4. MLAG found third device: 3 つ目のテハイスか MLAG に接続されました。		
5. peer-link is not set ・ビアリングのインタフェースが設定されていません。 The MLAG group <group_id> is down (<causes>)</causes></group_id>	Informational	MLAG グループでピアと異なる設定が
		使用されています。
• group id . MLAG のグルーフ ID courses : 記字が思たっている 原田		
<ul> <li>Causes・設定が共なりている原因</li></ul>		
追りり入し、 1. aroun ID is not evisted · MLAG のグループ ID が左右しません。		
2. algorithm is different: リンクアグリゲーションのアルゴリズムが異なります。		
3. total member port is over maximum number:ローカルポート数とピアポー		
ト数がサポートされる数を超えています。		
MPLS		
I SP <lsp, id=""> is up</lsp,>	Informational	ISP がアップされました。
	linomational	
パラメータ説明:		
・ lsp-id:インスタンス ID		
LSP <lsp_id> is down</lsp_id>	Informational	LSP がダウンされました。
パーイーク説明・		
MSTD Dobug (MSTD デバッグ)		
Topology changed [( [Instance: < Instance D> ] nort: < nortNum>_MA(; <macaddrs)]< td=""><td>Notico</td><td>トポロジに亦再がちりました</td></macaddrs)]<>	Notico	トポロジに亦再がちりました
	Notice	
パラメータ説明:		
・ Instance-id:インスタンス ID		
<ul> <li>portNum:ボート番号</li> </ul>		
・ macaddr · MAC アトレス		
[CIST   CIST Regional   MSTI Regional] New Root bridge selected( [Instance: <instanceid> ]MAC: <macaddr> Priority :<value>)</value></macaddr></instanceid>	Informational	新しいルートブリッジが選定されました。
パラメータ説明:		
・ Instance-id:インスタンス ID		
<ul> <li>macaddr: MACアドレス</li> </ul>		
・ value:優先値		

ログの内容	緊急度	イベントの説明
Spanning Tree Protocol is enabled	Informational	スパニングツリープロトコル有効化
Spanning Tree Protocol is disabled	Informational	スパニングツリープロトコル無効化
New root port selected [( [Instance: <instanceid> ], <portnum>)]</portnum></instanceid>	Notice	新しいルートポートが選定されました。
パラメータ説明:		
・ Instance-id:インスタンス ID		
・ portNum:ボート番号		
Spanning Tree port status change [( [Instance: <instanceid> ], <portnum>)] <old_< td=""><td>Notice</td><td> スパニングツリーポートのステートが</td></old_<></portnum></instanceid>	Notice	スパニングツリーポートのステートが
status> -> <new_status></new_status>		② 史されました。
パラメーク説明:		
· Instance-id:インスタンス ID		
<ul> <li>portNum:ポート番号</li> </ul>		
・ old_status:旧ステータス		
・ new_status:新ステータス		
Spanning Tree port role change. [( [Instance: <instanceid> ], &lt;[ portNum&gt;)] <old_< td=""><td>Informational</td><td>スパニングツリーポートのロールが変</td></old_<></instanceid>	Informational	スパニングツリーポートのロールが変
role>-> <new_role></new_role>		更されました。
パラメータ説明:		
・ Instance-id:インスタンス ID		
<ul> <li>portNum:ボート番号</li> </ul>		
• Old_status:旧人ナーダ人		
New_status · 新人ナーダ人		
spanning Tree Instance created (Instance :< Instance-id >)	Informational	スハーノクツリー1ノスタノスか1F成 さわました
パラメーク説明・		
・ Instance-id:インスタンス ID		
Spanning Tree instance deleted (Instance -< Instance-id >)	Informational	スパニングツリーインスタンスが削除
		されました。
パラメータ説明:		
・ Instance-id:インスタンス ID		
Spanning Tree version change (new version :< new_version>)	Informational	スパニングツリーのバージョンが変更
		されました。
パラメータ説明:		
・ new_version:新しいスパニングツリーのバージョン		
Spanning Tree MST configuration ID name and revision level change (name: <name></name>	Informational	スパニングツリー MST コンフィグレー
revision level <revision_level>).</revision_level>		ションロ名とリビションレベルか変更
パラメーク説明:		
・ name:指定された MST リージョンの名前		
<ul> <li>revision level: リビジョンレベル</li> </ul>		
Spanning Tree MST configuration ID VLAN mapping table change (instance:	Informational	スパニングツリー MST インスタンスか
<pre></pre>		ら VLAN が削除されました。
パラメータ説明:		
・ Instance-id:インスタンス ID		
<ul> <li>startvlanid:削除する VLAN 範囲の開始 VID</li> </ul>		
endvlanid:削除する VLAN 範囲の終了 VID		
Spanning Tree MST configuration ID VLAN mapping table changed (instance:	Informational	
<pre>  <instanceiu> add vlan <startvlanid> [- <endvlanid>])</endvlanid></startvlanid></instanceiu></pre>		VLAN マッヒンクテーフルか追加され   ました
パラメーク説明・		a U/Lo
・ Instance-id:インスタンス ID		
・ startvlanid:削除する VLAN 範囲の開始 VID		
endvlanid:削除する VLAN 範囲の終了 VID		
	1	1

ログの内容	緊急度	イベントの説明
Spanning Tree port role change (Instance : <instanceid>, <portnum>) to alternate</portnum></instanceid>	Informational	ガードルートのためにスパニングツ
port due to the guard root.		リーポートロールが交代します。
パラメータ説明:		
・ Instance-id:インスタンス ID		
<ul> <li>portNum:ポート番号</li> </ul>	ļ	
Spanning Tree loop guard blocking(Instance : <instanceid>, <portnum>)</portnum></instanceid>	Informational	スパニングツリーループガードがブ ロックしています。
パラメータ説明:		
・ Instance-id:インスタンス ID		
・ portNum:ポート番号		
OSPFv2 Enhancement (OSPFv2 エンハ	ンスメント)	
OSPF interface <intf-name> changed state to [Up   Down]</intf-name>	Informational	OSPF インタフェースのリンクステート
		が変更されました。
パラメータ説明:		
・ intf-name:OSPF インタフェース	ļ	
OSPF protocol on interface <intf-name> changed state to [Enabled   Disabled]</intf-name>	Informational	OSPF インタフェースの管理者ステート が変更されました。
パラメータ説明:		
・ intf-name:OSPF インタフェース		
OSPF interface <intf-name> changed from area <area-id> to area <area-id></area-id></area-id></intf-name>	Informational	OSPF インタフェースがエリア変更され ました。
パラメータ説明:		
・ intf-name:OSPF インタフェース		
・ area-id:OSPF エリア ID		
OSPF nbr <nbr-id> on interface <intf-name> changed state from Loading to Full</intf-name></nbr-id>	Notice	OSPF ネイバステートが「Loading」か ら「Full」に変更されました。
パラメータ説明:		
・ intf-name:OSPF インタフェース		
・ nbr-id:ネイバルータ ID		
OSPF nbr <nbr-id> on interface <intf-name> changed state from Full to Down</intf-name></nbr-id>	Notice	OSPF ネイバステートが「Full」から 「Down」に変更されました。
パラメータ説明:		
・ intf-name:OSPF インタフェース		
・ nbr-id:ネイバルータ ID		
OSPF nbr <nbr-id> on interface <intf-name> dead timer expired</intf-name></nbr-id>	Notice	OSPF ネイバステートデッドタイマ期限 が切れました。
パラメータ説明:		
・ intf-name:OSPF インタフェース		
・ nbr-id:ネイバルータ ID		
OSPF nbr <nbr-id> on virtual link changed state from Loading to Full</nbr-id>	Notice	OSPF 仮想ネイバステートが「Loading」 から「Full」に変わりました。
パラメータ説明:		
・ nbr-id:ネイバルータ ID		
OSPF nbr <nbr-id> on virtual link changed state from Full to Down</nbr-id>	Notice	OSPF 仮想ネイバステートが「Full」か ら「Down」に変わりました
パラメータ説明:		5 - DOWING (C&1) 7 & C/Co
• nbr-id: $\overline{x}$		
OSPE router ID changed to <router-id></router-id>	Informational	OSPF ルータ ID が変更されました。
ハノスーテ記明・ ・ nhr-id:OSPF ルータ ID		
• Horid · Ostri / F F F		
Ferpiled (问2/2016)	Critical	ファンが回復しました
Unit <uriit-iu>, <idi-descr> ddCK to normal</idi-descr></uriit-iu>	Chucal	ノ / ノ / 凹復しよし/こ。
パラメータ説明:		
・ unitID:ユニット ID for deapy : フラン/即西		
・ <ld>・ <ld>・ <ld>・ <ld>・ / / ノ</ld></ld></ld></ld>	1	

ログの内容	緊急度	イベントの説明
Unit cunit-id> cfan-descr> failed	Critical	ファンの故陪
パラメー々説明・		
・ dimub·ユニアトロ ・ cfan docorx:ファン標画		
Unit <unit-id> <tnermai-sensor-descr> detects abnormal temperature <degree></degree></tnermai-sensor-descr></unit-id>	warning	温度センサかどフーム状態に入りまし
		/c <sub>o</sub>
・ thermal-sensor-descr ・ セノサ ID		
• degree . 温度		
Unit <unit-id> <thermal-sensor-descr> temperature back to normal</thermal-sensor-descr></unit-id>	Informational	温度が通常に戻りました。
パラメータ説明:		
・ unitID:ユニット ID		
・ thermal-sensor-descr:センサ ID		
• degree:温度		
Unit <unit-id> <power-descr> failed</power-descr></unit-id>	Critical	電源故障
パラメータ説明:		
・ unitID:ユニット ID		
・ power-descr:電源 ID		
Unit <unit-id> <power-descr> back to normal</power-descr></unit-id>	Critical	電源回復
パラメータ説明:		
・ unitID:ユニット ID		
• power-descr:電源 ID		
Unit <unit-id> External Alarm Channel <channelid> :<alarmmsg></alarmmsg></channelid></unit-id>	Critical	外部アラームステートが変更されまし
		tc.
パラメータ説明:		
・ unitID:ユニット ID		
・ channelID:チャネル ID		
・ alarmMsg:アラームメッセージ		
PoE		
Unit <unit-id> usage threshold <percentage> is exceeded</percentage></unit-id>	Warning	総電力の使用率がしきい値を超えまし
		te
パラメータ説明:		
・ unitID:ユニット ID		
<ul> <li>percentage:使用率しきい値</li> </ul>		
Unit cupit id> usage threshold concentage> is recovered	Warning	松電力の使用変がしきい値を下向りま
onit Cunicid > usage tineshold <percentage> is recovered</percentage>	VVarning	
パラメータ説明・		
・ unitio · ユニット io ・ porcentage · 佶田変」 きい値		
PD alive check failed. (Port: <portnum>, PD: <ipaddr>)</ipaddr></portnum>	Warning	PD か Ping リクエストに回答しません。
<ul> <li>portNum: ホート番号</li> <li>・ トレーロマード・マート</li> </ul>		
・ ipaddr:IP アドレス		
Port	1	
Port <port> link up, <nway></nway></port>	Informational	ポートリンクアップしました。
パラメータ説明:		
<ul> <li>port:論理ポート番号</li> </ul>		
• nway:リンクスピードと二重通信方式		
Port <port> link down</port>	Informational	ボートリンクダウンしました。
パラメータ説明:		
・ port:論理ポート番号		

		イベントの説明
	糸芯  攵	
POIL Security		ピートのマドレスが切り
MAC address <macaddr> causes port security violation on <interface-id></interface-id></macaddr>	vvarning	ホート上のアトレスが超過
パラメータ説明:		
・ macaddr : 違反 MAC アドレス		
・ interface-id:インタフェース名		
Limit on system entry number has been exceeded	Warning	システム上のアドレスが超過
Reboot Schedule		
Reboot scheduled in 5 minutes	Warning	5分以内に再起動します。
Reboot scheduled in 1 minute	Critical	1 分以内に再起動します。
System was restarted by schedule in an interval time	Informational	指定間隔での再起動
System was restarted by schedule at specific time	Informational	指定時間での再起動
Configuration was saved by schedule	Informational	スケジュールされた再起動の前にコン
		フィグを保存します。
Safequard	1	
Unit <unit-id> Safeguard Engine enters EXHAUSTED mode</unit-id>	Warning	CPU使用率がしきい値を超え、ス
onit varite lay, suregular Engine enters EXTROSTED mode	l	イッチは「 $exhausted$ 」 モードに移行、
パラメータ説明:		Svslog に記録されます。
・unit-id:ユニット ID		
Unit <unit-id>. Safequard Engine enters NORMAL mode</unit-id>	Informational	CPU 使用率がしきい値を下回り、スイッ
		チはノーマルモードに移行、Svslog に
パラメータ説明:		記録されます。
・ unit-id:ユニット ID		
SD Card Management	•	
Entry <entry-name> to execute configuration <filename> at time <time-range></time-range></filename></entry-name>	Warning	実行スケジュールの設定失敗
failure.		
パラメータ説明:		
・ entry-name:実行スケジュール設定エントリ		
・ filename:ファイル名		
・ time-range:時間範囲		
Entry <entry-name> to backup <type>:<filename> at time <time-range> failure.</time-range></filename></type></entry-name>	Warning	実行スケジュールの設定 / ログ失敗
パラメータ説明:		
・ entry-name:実行スケジュール設定エントリ		
<ul> <li>type:設定/ログ</li> </ul>		
<ul> <li>filename:ファイル名</li> </ul>		
• time-range:時間範囲		
Entry <entry-name> to execute configuration <filename> success at time <time-< td=""><td>Informational</td><td>実行スケジュールの設定成功</td></time-<></filename></entry-name>	Informational	実行スケジュールの設定成功
range>		
<b>ハフメーダ説明・</b>		
・ entry-name、天行人ケンユール改走エントリ 、 filonomo、ファイルタ		
・ Ille laille ・ ノアイル石 ・ time-range ・ 時間範囲		
Entry contry names to back up at years afternames success at time at ime ranges	Informational	
Entry centry-name> to backup < type>: <mename> success at time &lt; time-range&gt;</mename>	Informational	美1]スクシュールの設定7ロク成功
パラメー々説明・		
・ entry-name: 実行スケジュール設定エントリ		
<ul> <li>type:設定/ログ</li> </ul>		
・ filename:ファイル名		
• time-range:時間範囲		
SNMP		·
SNMP request received from <ipaddr> with invalid community string</ipaddr>	Informational	SNMP リクエストは無効なコミュニ
,		ティストリングを受信しました。
パラメータ説明:		
・ ipaddr:IP アドレス		

	取刍亩	イベントの説明
Unit <unitid> SRM mode is different with master</unitid>	Alert	スタック成功時にマスタにより違う SRM モードのスレーブが確認されまし
パラメータ説明: ・ unitID:フェット ID		tc.
SSH	]	
SSH server is enabled	Informational	SSH サーバは有効
SSH server is disabled	Informational	SSH サーバは無効
Stacking	International	
Unit: <unitid>, MAC: <macaddr> Hot insertion.</macaddr></unitid>	Informational	デバイスが挿入されました。
パラメータ説明: ・ unitID:フェット ID		
<ul> <li>macaddr: MAC アドレス ID</li> </ul>		
Unit: <unitid>, MAC: <macaddr> Hot removal.</macaddr></unitid>	Informational	デバイスが削除されました。
<b>パラメータ説明:</b> ・ unitID:ユニット ID		
・ macaddr:MAC アドレス ID		
Stacking topology is <stack_tp_type>. Master(Unit <unitid>, MAC:<macaddr>)</macaddr></unitid></stack_tp_type>	Critical	スタッキングトポロジ変更
<ul> <li>パラメータ説明:</li> <li>Stack_TP_TYPE:スタッキングトポロジタイプ</li> <li>1. Ring</li> </ul>		
2. Chain		
・ unitID:ボックス ID		
・ Macaddr:MAC アドレス		
Backup master changed to master. Master (Unit: <unitid>)</unitid>	Informational	バックアップマスタがマスタに変更
パーメーク説明・		
Slave changed to master (Linit: <unitid>)</unitid>	Informational	スレーブがマス々に変更
<b>パラメータ説明:</b> ・ unitID:ボックス ID		
Hot insert failed, box ID conflict: Unit <unitid> conflict (MAC: <macaddr> and MAC:</macaddr></unitid>	Critical	ボックス ID が重複
<macaddr>)</macaddr>		
パラメータ説明:		
・ unitID:ホックス ID Massaddr:MAC スドレス		
Stacking port <portiu> link up</portiu>	Critical	スタックホートかりフクアップ
<b>パラメータ説明:</b> <ul> <li>portID:スタックポート番号</li> </ul>		
Stacking port <portid> link down</portid>	Critical	スタックポートがリンクダウン
パラメータ説明:		
<ul> <li>portID:スタックポート番号</li> </ul>		
SIO interface Unit <unitid> <sioid> link up</sioid></unitid>	Critical	SIO インタフェースがリンクアップ
  パラメータ説明:		
・ unitID:SIO インタフェースがリンクアップしているボックス ID		
・ SIOID: SIO インタフェース番号。サポートされている SIO インタフェース番号		
は「SIO1」か「SIO2」です。		

ログの内容	緊急度	イベントの説明
SIO interface Unit <unitid> <sioid> link down</sioid></unitid>	Critical	SIO インタフェースがリンクダウン
<b>ハフメータ説明:</b> ・ unitID:SIO インタフェースがリンクアップレブレスボックス ID		
<ul> <li>・ UIIIIU - SIO インタフェース番号 サポートされている SIO インタフェース番号</li> </ul>		
は「SIO1」か「SIO2」です。		
Storm Control	1	1
<broadcast multicast="" unicast=""  =""> storm is occurring on <interface-id></interface-id></broadcast>	Warning	ストーム発生
· Broducast · Ju-F+7XF/V/ yF (DA=FF:FF:FF:FF:FF:FF) / CASXF-		
<ul> <li>Multicast:未知のL2マルチキャスト、既知のL2マルチキャスト、未知のIP</li> </ul>		
マルチキャストと既知の IP マルチキャストを含むマルチキャストパケットによ		
るストーム		
<ul> <li>Unicast: 既知と未知のユニキャストパケットを含むユニキャストパケットによ</li> </ul>		
$3\lambda - \lambda$		
・ Interface-id : ストーム光王のインタフェース ID		
	Informational	フトーケが観光されました
	IIIIOIIIIatioiiai	
パラメータ説明:		
・ Broadcast:ブロードキャストパケット (DA = FF:FF:FF:FF:FF:FF) によるストー		
<ul> <li>Multicast: 木知のL2 マルナキャスト、 成知のL2 マルナキャスト、 木知のIP フルチキャストと 野知のIP フルチキャストを 含むフルチキャスト 、 木知のIP</li> </ul>		
<ul> <li>Unicast: 既知と未知のユニキャストパケットを含むユニキャストパケットによ</li> </ul>		
るストーム		
・ interface-id:ストーム発生のインタフェース ID		
<interface-id> is currently shut down due to the <broadcast multicast="" unicast=""  =""></broadcast></interface-id>	Warning	パケットストームによりポートシャッ
storm		
パラメータ説明:		
・Broadcast:ブロードキャストパケット (DA = FF:FF:FF:FF:FF) によるストー		
Д		
・ Multicast:未知のL2 マルチキャスト、既知のL2 マルチキャスト、未知の IP		
マルチキャストと 助知の IP マルチキャストを含むマルチキャストバケットによ		
<ul> <li>る人下ーム</li> <li>Ilnicast: 既知と未知のコーキャストパケットを含むコーキャストパケットによ</li> </ul>		
・ interface-id:ストーム発生のインタフェース ID		
System		
[Unit <unitid>, ]System warm start</unitid>	Critical	システムがウォームスタートしました。
[Unit <unit]d>. ]System cold start</unit]d>	Critical	<u> </u>  システムがコールドスタートしました。
パラメータ説明:		
・ unitID:ユニット ID		
[Unit <unitid>, ]System started up.</unitid>	Critical	システムが起動しました。
パラメーク説明・		
・unitID:ユニットID		
Telnet	1	1

ログの内容	緊急度	イベントの説明
Successful login through Telnet (Username: <username>. IP: <ipaddr>)</ipaddr></username>	Informational	Telnet 経由のログインに成功しま
		した。
パラメータ説明:		
・ ipaddr:Telnet クライアントの IP アドレス		
・ username:Telnet サーバーにログインするユーザ名		
Login failed through Telnet (Username: <username>, IP: <ipaddr>)</ipaddr></username>	Warning	Telnet 経由のログインに失敗しま
		した。
パラメータ説明:		
・ ipaddr:Telnet クライアントの IP アドレス		
・ username:Telnet サーバーにログインするユーザ名	ļ	
Logout through Telnet (Username: <username>, IP: <ipaddr>)</ipaddr></username>	Informational	Telnet からログアウトしました。
パラメータ説明:		
<ul> <li>ipaddr: leinet クライアントのIP アドレス </li> </ul>		
username · Teinet サーハーにログインするユーザ名		
leinet session timed out (Username: <username>, IP: <ipaddr>)</ipaddr></username>	Informational	Telnet セッションのタイムアウト
パラメーク説明・		
・ inaddr · Telnet クライアントの IP アドレス		
・ username: Telnet サーバーにログインするユーザ名		
	1	1
cinterface id> Breadcast storm is occurring	Warning	ブロードキャストストールが発生
	Warning	
パラメータ説明:		
・ interface-id:インタフェース ID		
<interface-id> Broadcast storm is cleared</interface-id>	Informational	ブロードキャストストームが解消
パラメータ説明:		
・ interface-id:インタフェース ID		
<interface-id> Multicast storm is occurring</interface-id>	Warning	マルチキャストストームが発生
	5	
パラメータ説明:		
・ interface-id:インタフェース ID		
<interface-id> Multicast storm is cleared</interface-id>	Informational	マルチキャストストームが解消
パラメータ説明:		
・ interface-id:インタフェース ID		
<interface-id> Unicast storm is occurring</interface-id>	Warning	ユニキャストストームが発生
<pre></pre> interrace-id> Unicast storm is cleared	Informational	ユーキャストストームか解消
パラメーク説明・		
・interface-id:インタフェース ID		
<pre><interface-id> is currently shut down due to a packet storm</interface-id></pre>	Warning	パケットストームの登生に伴い ポー
		トシャットダウン
  パラメータ説明:		
・ interface-id:インタフェース ID		
Voice VLAN		·
New voice device detected ( <interface-id>, MAC: <mac-address>)</mac-address></interface-id>	Informational	インタフェースで音声機器が検出され
		ました。
パラメータ説明:		
・ interface-id:インタフェース ID		
・ mac-address:MAC アドレス		
<interface-id> add into voice VLAN <vid></vid></interface-id>	Informational	自動音声 VLAN モードのインタフェー
		スが音声 VLAN に追加されました。
パラメータ説明:		
• vid : VLAN ID		
・ interface-id:インタフェース ID		

ログの内容	<b> </b>	イベントの説明
zinterface ids remove from voice VI AN suids	Informational	
<pre>\IIICITACETU2 TETTUVE ITUTTI VUICE VLAIN &lt; VIU2</pre>		「ノブノエーへか自戸 VLAIN から離脱」
パラメーク説明・		
vid VIANID		グエージが送信されます
・interface-id・インタフェース ID		
VPLS		
V/PLS	Informational	VPIS がリンクアップ
パラメータ説明:		
<ul> <li>vpls_name: VPLS 名</li> </ul>		
VPLS <vpls_name> link down</vpls_name>	Informational	VPLS がリンクダウン
パラメータ説明:		
• vpls_name:VPLS 名		
VPWS	·	·
Pseudowire id <vc_id> peer ip <ipaddr> link down</ipaddr></vc_id>	Informational	Pseudowire がリンクダウン
パラメータ説明:		
<ul> <li>vc_id : pseudowire ID</li> </ul>		
・ ipaddr:IP アドレス		
Pseudowire id <vc_id> peer ip <ipaddr> link up</ipaddr></vc_id>	Informational	Pseudowire がリンクアップ
パラメータ説明:		
vc_id : pseudowire ID		
Pseudowire id <vc_id> peer ip <ipaddr>is deleted</ipaddr></vc_id>	Informational	Pseudowire か削除
パーメーク説明・		
・ ipaddr:IP アドレス		
Pseudowire id < vc. id> peer in <inaddr> link standhy</inaddr>	Informational	Pseudowire $U^{2}/2\pi^{3}$
パラメータ説明:		
<ul> <li>vc_id : pseudowire ID</li> </ul>		
・ ipaddr:IP アドレス		
VRRP Debug (VRRP デバック	``)	
VR <vr-id> at interface <intf-name> switch to Master</intf-name></vr-id>	Informational	ある仮想ルータがマスタに移行しまし
		た。
パラメータ説明:		
・ vr-id:VRRP 仮想ルータ ID		
・ intf-name:仮想ルータがベースにしているインタフェース名		
VR <vr-id> at interface <intf-name> switch to Backup</intf-name></vr-id>	Informational	ある仮想ルータがバックアップに移行
		しました。
<ul> <li>VI-IQ · VKKP 仮想ルータ ID </li> <li>intf name · 伝想ルークボベーフにしているインクフェーフタ</li> </ul>		
<ul> <li>Inti-name、仮想ルーダルベースにしているインダフェース名 </li> </ul>		
vr <vr-iu> at interface <intr-name> switch to init</intr-name></vr-iu>	Informational	のつ仮想ルーメか「INIT」に移行しまし た
パラメーク説明・		/ Lo
・ vr-id:VRRP 仮想ルータ ID		
・ intf-name:仮想ルータがベースにしているインタフェース名		
Authentication type mismatch on VR $<$ vr-id> at interface $<$ intf-name>	Warning	」 認証タイプが受信した VRRP アドバタ
		イズメッヤージと合致しません。
パラメータ説明:		
・ vr-id:VRRP 仮想ルータ ID		
• intf-name:仮想ルータがベースにしているインタフェース名		

Authentication fail on VR <vr-id> at interface <intf-name>. Auth type <auth-type> Warning 受信した.VRRP アドバタイズメッセージのチェックに失敗しました。 パラメータ説明: ・vr-id: VRRP 伝想ルータID ・intf-name : 仮想ルータがペースにしているインタフェース名 Received an ADV msg with incorrect checksum on VR <vr-id> at interface <intf-name> ジのチェックに失敗しました。 パラメータ説明: ・vr-id: VRRP 伝想ルータ ID ・intf-name : 仮想ルータがヘースにしているインタフェース名 Received ADV msg virtual router ID mismatch. VR <vr-id> at interface <intf-name> Warning 受信した.VRRP アドバタイズメッセージのチェックに失敗しました。 パラメータ説明: ・vr-id: VRRP 仮想ルータ ID ・intf-name : 仮想ルータがヘースにしているインタフェース名 Received ADV msg virtual router ID mismatch. VR <vr-id> at interface <intf-name> Warning 受信した.VRRP アドバタイズメッセージと仮想ルータ ID ・intf-name : 仮想ルータ ID ・intf-name : 仮想 MAC フドレス Added a virtual MAC <vrrp-mac-addr> into L2 table vrrp-mac-addr : VRRP 仮想 MAC フドレス Added a virtual IMAC <vrrp-mac-addr> IND L2 table Notice 仮想 MAC アドレスがスイッチの L2 テーブルに追加されました。 パラメーク説明 : ・vrp-mac-addr : VRRP 仮想 MAC フドレス Added a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> IND L2 table Notice 仮想 MAC アドレスがスイッチの L2 テーブルの時間除されました。 パラメーク説明 : ・vrp-mac-addr : VRRP 仮想 MAC フドレス Added a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> IND L2 table Notice 仮想 MAC アドレスがスイッチの L2 Fーブルレジの前除されました。</vrrp-mac-addr></vrrp-ip-addr></vrrp-mac-addr></vrrp-ip-addr></vrrp-mac-addr></vrrp-mac-addr></intf-name></vr-id></intf-name></vr-id></intf-name></vr-id></auth-type></intf-name></vr-id>
Notice Inductor landor for the lab of microlic California (Decadar type)       Notice       ジロデェックに失敗した。         NF3メータ説明:       ・ vr-id : VRRP 仮想ルータがペースにしているインタフェース名       Warning       受信した VRRP アドバタイズメッセージのチェックにエラーが発生しました。         NF3メータ説明:       ・ vr-id : VRRP 仮想ルータ ID       ・ vr-id : VRRP 仮想ルータ ID       ・ vr-id : VRRP 仮想ルータ ID         ・ intf-name:       仮想ルータがペースにしているインタフェース名       Warning       受信した VRRP アドバタイズメッセージのチェックにエラーが発生しました。         N75メータ説明:       ・ vr-id : VRRP 仮想ルータ ID       ・ vr-id : VRRP 仮想ルータ ID       ・ vr-id : VRRP 仮想ルータ ID         ・ intf-name:       仮想ルータ ID       ・ vr-id : VRRP 仮想ルータ ID       ・ vr-id : VRRP 仮想ルータ ID         ・ intf-name:       仮想ルータ ID       ・ vr-id : VRRP 仮想ルータ ID       ・ vr-id : VRRP 仮想ルータ ID         ・ intf-name:       仮想ルータ ID       ・ vr-id : VRRP 仮想ルータ ID       ・ vr-id : VRRP 仮想ルータ ID         ・ intf-name:       仮想ルータ ID       ・ vr-id : VRRP 仮想ルータ ID       ・ vr-id : VRRP 仮想ルータ ID         ・ intf-name:       仮想ルータ ID       ・ vr-id : VRRP 仮想ルータ ID       ・ vr-id : VRRP 仮想ルータ ID         ・ intf-name:       仮想ルータ ID       ・ vr-id : VRRP 仮想 MAC アドレス
パラメータ説明:       ・vr-id: VRRP 仮想ルータ ID         ・intf-name: 仮想ルータがベースにしているインタフェース名       Warning         Received an ADV msg with incorrect checksum on VR <vr-id> at interface <intf-name>       Warning         アメーク説明:       ・vr-id: VRRP 仮想ルータ ID         ・ vr-id: VRRP 仮想ルータ ID       ·intf-name: 仮想ルータがペースにしているインタフェース名         Received ADV msg virtual router ID mismatch. VR <vr-id> at interface <intf-name>       Warning         アメーク説明:       ·vr-id: VRRP 仮想ルータ ID         · vr-id: VRRP 仮想ルータ ID       ·intf-name: 仮想ルータがペースにしているインタフェース名         Received ADV msg virtual router ID mismatch. VR <vr-id> at interface <intf-name>       Warning         ジーク説明:       ·vr-id: VRRP 仮想ルータ ID         · vr-id: VRRP 仮想ルータ ID       ·intf-name: 仮想ルータがペースにしているインタフェース名         Received ADV msg adv interval mismatch. VR <vr-id> at interface <intf-name>       Warning         ジーク説明:       ·vr-id: VRRP 仮想 // ク ID         · vr-id: VRRP 仮想// ク ID       ·intf-name: 仮想// ク がペースにしているインタフェース名         Received ADV msg adv interval mismatch. VR <vr-id> at interface <intf-name>       Warning         ジーク説明:       ·vr-id: VRRP 仮想// ク ID       ·vr-id&gt;: VRRP 仮想// ク ID         · intf-name: 仮想// ク 原 // の // の // の // の // の // の //</intf-name></vr-id></intf-name></vr-id></intf-name></vr-id></intf-name></vr-id></intf-name></vr-id>
・ vr-id: VRRP 仮想ルータID       ・ <ul> <li>intf-name: 仮想ルータがペースにしているインタフェース名</li> <li>Auth-type: VRRP インタフェース認証タイブ</li> </ul> Warning         受信した VRRP アドバタイズメッセージのチェックにエラーが発生しました。           パラメータ説明:         ・             vr-id: VRRP 仮想ルータ ID         Warning         受信した VRRP アドバタイズメッセージのチェックにエラーが発生しました。           パラメータ説明:         ・             vr-id: VRRP 仮想ルータ ID         Warning         受信した VRRP アドバタイズメッセージと仮想ルータ ID           ・             intf-name: 仮想ルータがペースにしているインタフェース名         Warning         受信した VRRP アドバタイズメッセージと仮想ルータ ID がら含致しません。           パラメーク説明:         ・             vr-id: VRRP 仮想ルータ ID         Warning         受信した VRRP アドバタイズメッセージと仮想ルータ ID がら含致しません。           パラメーク説明:         ・             vr-id: VRP 仮想ルータ ID         Warning         受信した VRRP アドバタイズメッセージとアドバタイズメッセージとアドバタイズメッセージとアドバタイズメッセージとアドバタイズメッセージとアドバタイズメッセージとアドバタイズメッセージとアドバタイズメント間隔が合致しません。           パラメーク説明:         ・             vr-id: VRP 仮想ルータ ID              interface <intf-name>         Warning         受信した VRRP アドバタイズメッセージとアドバタイズメッセージとアドバタイズメッセージとアドバタイズメット間隔が合致しません。           パラメーク説明:         ・             vr-dix RP 仮想ルータ ID              interface <intf-name>         Warning         受信した VRRP アドレスがスイントロロン・ ジェアドバタイズメント間隔が合致し              retwardia WAC アドレスがスインチロン              retwardia WAC アドレスがスイッチレン              Pile 48              vretwardia WAC アドレスがス              retwardia WAC アドレス              State Aaget State State State State S</intf-name></intf-name>
・ intf-name : 仮想ルータがベースにしているインタフェース名WarningReceived an ADV msg with incorrect checksum on VR <vr-id> at interface <intf- </intf- name&gt;Warningパラメータ説明 : ・ vr-id : VRRP 仮想ルータ ID ・ intf-name : 仮想ルータがベースにしているインタフェース名WarningReceived ADV msg vitual router ID mismatch. VR <vr-id> at interface <intf-name>Warningパラメータ説明 : ・ vr-id : VRRP 仮想ルータ ID ・ intf-name : 仮想ルータ DWarningグラメータ説明 : ・ vr-id : VRRP 仮想ルータ ID ・ intf-name : 仮想ルータ IDWarningグラメータ説明 : ・ vr-id : VRRP 仮想ルータ ID ・ intf-name : 仮想ルータ DWarningグラメータ説明 : ・ vr-id : VRRP 仮想ルータ ID ・ intf-name : 仮想ルータ DWarningグロック (アラススンシャセージ) ジと (アメント間隔が合致し ません。ジェック(アメン・セージ) ジン (アメント間隔が合致し ません。パラメータ説明 : ・ vr-id : VRRP 仮想ルータ ID ・ intf-name : 仮想ルータ IDWarningグ目 - type 伝想ルータ ID ・ intf-name : 仮想ルータ IDWarningグロ - ケンロ - スにしているインタフェース名WarningKded a virtual MAC Warning : ・ vr-id : VRRP 仮想 MAC アドレスパラメータ説明 : ・ vrp-mac-addr : VRRP 仮想 MAC アドレスNoticeパラメーク説明 : ・ vrp-mac-addr : VRRP 仮想 MAC マドレスNoticeパラ - ク説明 : ・ vrp-mac-addr : VRRP 仮想 MAC マドレスNoticeパラ - ブルから削除されました。パラーブルから削除されました。パラ - ク説明 : ・ vrp-mac-addr : VRRP 仮想 MAC Notice・ vrp-mac-addr : VRRP 仮想 MAC アドレス・ vrp-mac-addr : VRRP 仮想 MAC アドレス・ vrp-mac-addr : VRRP 仮想 MAC アドレス</br></br></intf-name></vr-id></vr-id>
・ Auth-type : VRRP インタフェース認証タイプWarningReceived an ADV msg with incorrect checksum on VR <vr-id> at interface <intf- </intf- name&gt;Warning受信した VRRP アドバタイズメッセー ジのチェックにエラーが発生しました。バラメータ説明 : ・ vr-id : VRRP 仮想ルータ ID ・ intf-name : 仮想ルータがベースにしているインタフェース名WarningReceived ADV msg virtual router ID mismatch. VR <vr-id> at interface <intf-name>Warningパラメータ説明 : ・ vr-id : VRRP 仮想ルータ ID ・ intf-name : 仮想ルータがベースにしているインタフェース名WarningReceived ADV msg virtual router ID mismatch. VR <vr-id> at interface <intf-name>Warningビオタ説の中の ID ・ intf-name : 仮想ルータがベースにしているインタフェース名WarningReceived ADV msg adv interval mismatch. VR <vr-id> at interface <intf-name>Warningパラメーク説明 : ・ vr-id : VRRP 仮想ルータ ID ・ intf-name : 仮想ルータがベースにしているインタフェース名Warningパラメーク説明 : ・ vr-id : VRRP 仮想 MAC アドレスNotice仮想 MAC アドレスがスイッチの L2 テーブルに追加されました。パラメーク説明 : ・ vrrp-mac-addr : VRRP 仮想 MAC アドレスNotice仮想 MAC アドレスがスイッチの L2 テーブルいら削除されました。パラメーク説明 : ・ vrrp-mac-addr : VRRP 仮想 MAC アドレスNotice仮想 MAC アドレスがスイッチの L2 テーブルいら削除されました。パラメーク説明 : ・ vrrp-mac-addr : VRRP 仮想 MAC アドレスNotice仮想 MAC アドレスがスイッチの L2 テーブルいら削除されました。パラメーク説明 : ・ vrrp-mac-addr : VRRP 仮想 MAC アドレスNotice仮想 MAC アドレスがスイッチの L3 テーブルいら削除されました。パラメーク説明 : ・ vrrp-mac-addr : VRRP 仮想 MAC アドレスNotice仮想 MAC アドレスがスイッチの L3 テーブルいら削除されました。パラメーク説明 : ・ vrrp-mac-addr : VRRP 仮想 MAC マドレスNotice「切想 MAC アドレスがスイッチの L3 テーブルいら削除されました。</intf-name></vr-id></intf-name></vr-id></intf-name></vr-id></vr-id>
Received an ADV msg with incorrect checksum on VR <vr-id> at interface <intf- </intf- name&gt;Warning受信した VRRP アドバタイズメッセー ジのチェックにエラーが発生しました。パラメータ説明: ・ vr-id : VRRP 仮想ルータ ID ・ intf-name : 仮想ルータがペースにしているインタフェース名Warning受信した VRRP アドバタイズメッセー ジのチェックにエラーが発生しました。パラメータ説明: ・ vr-id : VRRP 仮想ルータ ID ・ intf-name : 仮想ルータ DD ・ intf-name : 仮想ルータ CD ・ intf-name : 仮想ルータ DD ・ intf-name : 仮想ルータ DD ・ intf-name : 仮想ルータ DD ・ intf-name : 仮想ルータ DD ・ intf-name : 仮想ルータ CD ・ intf-name : 仮想ルータ CD ・ intf-name : 仮想ルータ DD ・ intf-name : 仮想ルータ DD ・ intf-name : 仮想ルータ DD ・ intf-name : 仮想ルータ DD ・ intf-name : 仮想ルータ CD ・ intf-name : 仮想ルータ DD ・ intf-name : 仮想 MAC アドレスNotice仮想 MAC アドレスがスイッチの L2 アーブルに追加されました。パラメータ説明: ・ vrrp-mac-addr : VRRP 仮想 MAC アドレスNotice仮想 MAC アドレスがスイッチの L2 アーブルいら削除されました。デーブルに追加されました。パラメータ説明: ・ vrrp-mac-addr : VRRP 仮想 MAC アドレスNotice仮想 MAC アドレスがスイッチの L3 アーブルいら削除されました。パラムータは回: ・ vrrp-mac-addr : VRRP 仮想 MAC アドレスNotice仮想 MAC アドレスがスイッチの L3 アーブルに追加されました。</vr-id>
name>ジのチェックにエラーが発生しました。パラメータ説明: ・ vr-id : VRRP 仮想ルータ ID ・ intf-name : 仮想ルータがベースにしているインタフェース名Warning受信した VRRP アドバタイズメッセー ジと仮想ルータ ID が合致しません。パラメータ説明: ・ vr-id : VRRP 仮想ルータ ID ・ intf-name : 仮想ルータ D ・ vr-id : VRRP 仮想ルーク ID ・ intf-name : 仮想ルーク D ・ intf-name : 仮想ルーク D ・ intf-name : 仮想ルーク D ・ intf-name : 仮想ルーク D ・ intf-name : 仮想ルーク ID ・ intf-name : 仮想 MAC マドレス Added a virtual MAC ・ Vrrp-mac-addr > into L2 tableNotice仮想 MAC アドレスがスイッチの L2 テーブルに追加されました。パラメーク説明 : ・ vrrp-mac-addr : VRRP 仮想 MAC アドレスNotice仮想 MAC アドレスがスイッチの L2 テーブルに追加されました。パラメーク説明 : ・ vrrp-mac-addr : VRRP 仮想 MAC アドレスNotice仮想 MAC アドレスがスイッチの L3 テーブルに追加されました。パラメーク説明 : ・ vrrp-mac-addr : VRRP 仮想 MAC アドレスNotice仮想 MAC アドレスがスイッチの L3 テーブルに追加されました。
バラメータ説明: ・ vr-id : VRRP 仮想ルータ ID ・ intf-name : 仮想ルータがベースにしているインタフェース名Warning受信した VRRP アドバタイズメッセー ジと仮想ルータ ID が合致しません。Received ADV msg virtual router ID mismatch. VR <vr-id> at interface <intf-name> ・ vr-id : VRRP 仮想ルータ ID ・ intf-name : 仮想ルータがベースにしているインタフェース名Warning受信した VRRP アドバタイズメッセー ジと仮想ルータ ID が合致しません。パラメータ説明: ・ vr-id : VRRP 仮想ルータ ID ・ intf-name : 仮想ルータがベースにしているインタフェース名Warning受信した VRRP アドバタイズメッセー ジとアドバタイズメット間隔が合致し ません。パラメータ説明: ・ vr-id : VRRP 仮想.NL  ・ vrrig : VRRP 仮想.NL  ・ vrrig : VRRP 仮想.NL  ・ vrrp-mac-addr : VRRP 仮想.MAC アドレスNotice仮想.MAC アドレスがスイッチの L2 アーブルに追加されました。パラメータ説明: ・ vrrp-mac-addr : VRRP 仮想.MAC アドレスNotice仮想.MAC アドレスがスイッチの L2 アーブルのら削除されました。パラメータ説明 : ・ vrrp-mac-addr : VRRP 仮想.MAC アドレスNotice仮想.MAC アドレスがスイッチの L2 アーブルのら削除されました。パラメータ説明 : ・ vrrp-mac-addr : VRRP 仮想.MAC アドレスNotice仮想.MAC アドレスがスイッチの L3 アーブルのら削除されました。パラメータ説明 : ・ vrrp-mac-addr : VRRP 仮想.MAC アドレスNotice仮想.MAC アドレスがスイッチの L3 アーブルのら削除されました。パラスーク説明 : ・ vrrp-mac-addr : VRRP 仮想.MAC アドレスNotice仮想.MAC アドレスがスイッチの L3 アーブルのら削除されました。</intf-name></vr-id>
ハフネータ説明・       ・ vrid: VRRP 仮想ルータ ID         ・ intf-name: 仮想ルータがペースにしているインタフェース名       Warning         Received ADV msg virtual router ID mismatch. VR <vr-id> at interface <intf-name>       Warning         パラメータ説明:       ・ vr-id: VRRP 仮想ルータ ID         ・ vr-id: VRRP 仮想ルータがペースにしているインタフェース名       Warning         Received ADV msg adv interval mismatch. VR <vr-id> at interface <intf-name>       Warning         アドパタイズメッセージと仮想ルータ ID       ・ vr-id: VRRP 仮想ルータ ID         ・ vr-id: VRRP 仮想ルータ ID       ●         ・ vr-id: VRRP 仮想ルータ ID       ●         ・ intf-name: 仮想ルータがペースにしているインタフェース名       Warning         グ信した VRRP アドパタイズメッセージとアドパタイズメット間隔が合致しません。         パラメータ説明:       ●         ・ vr-id: VRRP 仮想ルータ ID       ●         ・ intf-name: 仮想ルータがペースにしているインタフェース名       Notice         Added a virtual MAC <vrrp-mac-addr> into L2 table       Notice         パラメータ説明:       ●         ・ vrrp-mac-addr: VRRP 仮想 MAC アドレス       Notice         Deleted a virtual MAC <vrrp-mac-addr> from L2 table       Notice         パラメータ説明:       ●         ・ vrrp-mac-addr: VRRP 仮想 MAC アドレス       R         Added a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr into="" l3="" table<="" td="">       Notice         グ想 MAC アドレスがスイッチの L3       ●         パラスークドレスがスイッチの L3       ●    <!--</td--></vrrp-mac-addr></vrrp-ip-addr></vrrp-mac-addr></vrrp-mac-addr></intf-name></vr-id></intf-name></vr-id>
<ul> <li>intf-name: 仮想ルータがペースにしているインタフェース名</li> <li>Received ADV msg virtual router ID mismatch. VR <vr-id> at interface <intf-name></intf-name></vr-id></li> <li>Warning</li> <li>受信した VRRP アドバタイズメッセージと仮想ルータ ID が合致しません。</li> <li>バラメータ説明:         <ul> <li>vr-id: VRRP 仮想ルータ ID</li> <li>intf-name: 仮想ルータがペースにしているインタフェース名</li> </ul> </li> <li>Received ADV msg adv interval mismatch. VR <vr-id> at interface <intf-name></intf-name></vr-id></li> <li>Warning</li> <li>受信した VRRP アドバタイズメッセージと仮想ルータ ID</li> <li>intf-name: 仮想ルータがペースにしているインタフェース名</li> <li>Warning</li> <li>ジェアドバタイズメント間隔が合致しません。</li> <li>パラメータ説明:         <ul> <li>vr-id: VRRP 仮想ルータ ID</li> <li>intf-name: 仮想ルータがペースにしているインタフェース名</li> </ul> </li> <li>Added a virtual MAC </li> <li>Vrrp-mac-addr: into L2 table</li> <li>Notice</li> <ul> <li>仮想 MAC アドレスがスイッチの L2</li> <li>アーブルのら削除されました。</li> </ul> <li>vrp-mac-addr: VRRP 仮想 MAC アドレス</li> </ul> <li>Notice</li> <li>K想 MAC アドレスがスイッチの L2</li> <li>アーブルのら削除されました。</li> <li>パラメータ説明:         <ul> <li>vrp-inac-addr: VRRP 仮想 MAC アドレス</li> </ul> </li> <li>Added a virtual IP <ul> <li>vrp-ip-addr&gt; MAC <ul> <li>WAC マドレスがスイッチの L3</li> <li>アーブルのら削除されました。</li> </ul> </li> </ul></li>
Received ADV msg virtual router ID mismatch. VR <vr-id> at interface <intf-name>       Warning       受信した VRRP アドバタイズメッセー ジと仮想ルータ ID が合致しません。         パラメータ説明: ・ vr-id : VRRP 仮想ルータ ID ・ intf-name : 仮想ルータがペースにしているインタフェース名       Warning       受信した VRRP アドバタイズメッセー ジとアドバタイズメッセー ジとアドバタイズメッセー         パラメータ説明: ・ vr-id : VRRP 仮想ルータ ID ・ intf-name : 仮想ルータ ID ・ intf-name : 仮想ルータ D       Warning       受信した VRRP アドバタイズメッセー ジとアドバタイズメント間隔が合致し ません。         パラメータ説明: ・ vr-id : VRRP 仮想ルータがペースにしているインタフェース名       Notice       仮想 MAC アドレスがスイッチの L2 テーブルに追加されました。         パラメータ説明: ・ vrrp-mac-addr : VRRP 仮想 MAC アドレス       Notice       仮想 MAC アドレスがスイッチの L2 テーブルから削除されました。         パラメータ説明: ・ vrrp-mac-addr : VRRP 仮想 MAC アドレス       Notice       仮想 MAC アドレスがスイッチの L2 テーブルから削除されました。         パラメータ説明: ・ vrrp-mac-addr : VRRP 仮想 MAC アドレス       Notice       仮想 MAC アドレスがスイッチの L2 テーブルから削除されました。         パラメータ説明: ・ vrrp-ina-caddr : VRRP 仮想 MAC アドレス       Notice       仮想 MAC アドレスがスイッチの L3 テーブルに追加されました。</intf-name></vr-id>
パラメータ説明: ・ vr-id : VRRP 仮想ルータ ID ・ intf-name : 仮想ルータ Dジと仮想ルータ ID が合致しません。パラメータ説明: ・ vr-id : VRRP 仮想ルータ ID ・ intf-name : 仮想ルータ IDWarning受信した VRRP アドバタイズメッセー ジとアドバタイズメント間隔が合致し ません。パラメータ説明: ・ vr-id : VRRP 仮想ルータ ID ・ intf-name : 仮想ルータがベースにしているインタフェース名Warning受信した VRRP アドバタイズメット間隔が合致し ません。Added a virtual MAC <vrrp-mac-addr> into L2 tableNotice仮想 MAC アドレスがスイッチの L2 アーブルに追加されました。パラメータ説明: ・ vrrp-mac-addr : VRRP 仮想 MAC アドレスNotice仮想 MAC アドレスがスイッチの L2 アーブルに追加されました。パラメータ説明: ・ vrrp-mac-addr : VRRP 仮想 MAC アドレスNotice仮想 MAC アドレスがスイッチの L2 アーブルに追加されました。パラメータ説明: ・ vrrp-mac-addr : VRRP 仮想 MAC アドレスNotice仮想 MAC アドレスがスイッチの L2 アーブルに追加されました。パラメータ説明: ・ vrrp-mac-addr : VRRP 仮想 MAC アドレスNotice仮想 MAC アドレスがスイッチの L2 アーブルから削除されました。パラメータ説明: ・ vrrp-mac-addr : VRRP 仮想 MAC アドレスNotice仮想 MAC アドレスがスイッチの L3 アーブルに追加されました。</vrrp-mac-addr>
パラメータ説明: ・ vr-id : VRRP 仮想ルータ ID ・ intf-name : 仮想ルータがベースにしているインタフェース名Warning受信した VRRP アドバタイズメッセー ジとアドバタイズメント間隔が合致し ません。Received ADV msg adv interval mismatch. VR <vr-id> at interface <intf-name>Warning受信した VRRP アドバタイズメント間隔が合致し ません。パラメータ説明: ・ vr-id : VRRP 仮想ルータ ID ・ intf-name : 仮想ルータがベースにしているインタフェース名Notice仮想 MAC アドレスがスイッチの L2 テーブルに追加されました。Added a virtual MAC <vrrp-mac-addr> into L2 tableNotice仮想 MAC アドレスがスイッチの L2 テーブルに追加されました。パラメータ説明: ・ vrrp-mac-addr : VRRP 仮想 MAC アドレスNotice仮想 MAC アドレスがスイッチの L2 テーブルから削除されました。パラメータ説明: ・ vrrp-mac-addr : VRRP 仮想 MAC アドレスNotice仮想 MAC アドレスがスイッチの L2 テーブルから削除されました。パラメータ説明: ・ vrrp-mac-addr : VRRP 仮想 MAC アドレスNotice仮想 MAC アドレスがスイッチの L2 テーブルから削除されました。パラメータ説明: ・ vrrp-mac-addr : VRRP 仮想 MAC アドレスNotice仮想 MAC アドレスがスイッチの L3 テーブルから削除されました。パラメータ説明: ・ vrrp-mac-addr : VRRP 仮想 MAC マドレスNotice仮想 MAC アドレスがスイッチの L3 テーブルから削除されました。</vrrp-mac-addr></intf-name></vr-id>
<ul> <li>vr-id: VRRP 仮想ルータ ID</li> <li>intf-name: 仮想ルータがベースにしているインタフェース名</li> <li>Received ADV msg adv interval mismatch. VR <vr-id> at interface <intf-name></intf-name></vr-id></li> <li>Warning</li> <li>受信した VRRP アドバタイズメッセージとアドバタイズメット間隔が合致しません。</li> <li>vr-id: VRRP 仮想ルータ ID</li> <li>intf-name: 仮想ルータがベースにしているインタフェース名</li> <li>Added a virtual MAC <vrrp-mac-addr> into L2 table</vrrp-mac-addr></li> <li>Notice</li> <li>仮想 MAC アドレスがスイッチのL2</li> <li>デーブルに追加されました。</li> <li>パラメータ説明:</li> <li>vrrp-mac-addr: VRRP 仮想 MAC アドレス</li> <li>Deleted a virtual MAC <vrrp-mac-addr> from L2 table</vrrp-mac-addr></li> <li>Notice</li> <li>仮想 MAC アドレスがスイッチのL2</li> <li>デーブルから削除されました。</li> <li>パラメータ説明:</li> <li>vrrp-mac-addr: VRRP 仮想 MAC アドレス</li> <li>Motice</li> <li>仮想 MAC アドレスがスイッチのL2</li> <li>デーブルから削除されました。</li> <li>パラメータ説明:</li> <li>vrrp-mac-addr: VRRP 仮想 MAC アドレス</li> </ul>
<ul> <li>intf-name : 仮想ルータがベースにしているインタフェース名</li> <li>Received ADV msg adv interval mismatch. VR <vr-id> at interface <intf-name></intf-name></vr-id></li> <li>Warning 受信した VRRP アドバタイズメット間隔が合致しません。</li> <li>vr-id : VRRP 仮想ルータ ID</li> <li>intf-name : 仮想ルータがベースにしているインタフェース名</li> <li>Added a virtual MAC <vrrp-mac-addr> into L2 table</vrrp-mac-addr></li> <li>Notice 仮想 MAC アドレスがスイッチの L2 テーブルに追加されました。</li> <li>パラメータ説明:</li> <li>vrrp-mac-addr : VRRP 仮想 MAC アドレス</li> <li>Deleted a virtual MAC <vrrp-mac-addr> from L2 table</vrrp-mac-addr></li> <li>パラメータ説明:</li> <li>vrrp-mac-addr : VRRP 仮想 MAC アドレス</li> <li>Motice 仮想 MAC アドレスがスイッチの L2 テーブルに追加されました。</li> <li>パラメータ説明:</li> <li>vrrp-mac-addr : VRRP 仮想 MAC アドレス</li> <li>Motice 仮想 MAC アドレスがスイッチの L2 テーブルに追加されました。</li> </ul>
Received ADV msg adv interval mismatch. VR <vr-id> at interface <intf-name>Warning受信した VRRP アドバタイズメッセー ジとアドバタイズメント間隔が合致し ません。パラメータ説明: • vr-id : VRRP 仮想ルータ ID • intf-name : 仮想ルータがベースにしているインタフェース名Notice仮想 MAC アドレスがスイッチのL2 テーブルに追加されました。Added a virtual MAC <vrrp-mac-addr> into L2 tableNotice仮想 MAC アドレスがスイッチのL2 テーブルに追加されました。パラメータ説明: • vrrp-mac-addr : VRRP 仮想 MAC アドレスNotice仮想 MAC アドレスがスイッチのL2 テーブルから削除されました。パラメータ説明: • vrrp-mac-addr : VRRP 仮想 MAC アドレスNotice仮想 MAC アドレスがスイッチのL2 テーブルから削除されました。パラメータ説明: • vrrp-mac-addr : VRRP 仮想 MAC アドレスNotice仮想 MAC アドレスがスイッチのL3 テーブルから削除されました。パラメータ説明: • vrrp-mac-addr : VRRP 仮想 MAC マドレスNotice仮想 MAC アドレスがスイッチのL3 テーブルに追加されました。</vrrp-mac-addr></intf-name></vr-id>
パラメータ説明: ・ vr-id : VRRP 仮想ルータ ID ・ intf-name : 仮想ルータがベースにしているインタフェース名Noticeジとアドバタイズメント間隔が合致し ません。Added a virtual MAC <vrrp-mac-addr> into L2 tableNotice仮想 MAC アドレスがスイッチの L2 テーブルに追加されました。パラメータ説明: ・ vrrp-mac-addr : VRRP 仮想 MAC アドレスNotice仮想 MAC アドレスがスイッチの L2 テーブルに追加されました。Deleted a virtual MAC <vrrp-mac-addr> from L2 tableNotice仮想 MAC アドレスがスイッチの L2 テーブルに追加されました。パラメータ説明: ・ vrrp-mac-addr : VRRP 仮想 MAC アドレスNotice仮想 MAC アドレスがスイッチの L2 テーブルから削除されました。パラメータ説明: ・ vrrp-mac-addr : VRRP 仮想 MAC アドレスNotice仮想 MAC アドレスがスイッチの L3 テーブルに追加されました。パラメータ説明: ・ vrrp-mac-addr : VRRP 仮想 MAC <vrrp-mac-addr> into L3 tableNotice仮想 MAC アドレスがスイッチの L3 テーブルに追加されました。</vrrp-mac-addr></vrrp-mac-addr></vrrp-mac-addr>
ハフメータ説明:       ません。         ・ vr-id: VRRP 仮想ルータ ID       intf-name: 仮想ルータがベースにしているインタフェース名         Added a virtual MAC <vrrp-mac-addr> into L2 table       Notice       仮想 MAC アドレスがスイッチの L2         パラメータ説明:       ・ vrrp-mac-addr : VRRP 仮想 MAC アドレス       アーブルに追加されました。         レeleted a virtual MAC <vrrp-mac-addr> from L2 table       Notice       仮想 MAC アドレスがスイッチの L2         レeleted a virtual MAC <vrrp-mac-addr> from L2 table       Notice       仮想 MAC アドレスがスイッチの L2         パラメータ説明:       ・ vrrp-mac-addr : VRRP 仮想 MAC アドレス       Notice       仮想 MAC アドレスがスイッチの L2         メータ説明:       ・ vrrp-mac-addr : VRRP 仮想 MAC アドレス       Notice       仮想 MAC アドレスがスイッチの L3         Added a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table       Notice       仮想 MAC アドレスがスイッチの L3         パラメーク説明:       ・       ・       アーブルに追加されました。</vrrp-mac-addr></vrrp-ip-addr></vrrp-mac-addr></vrrp-mac-addr></vrrp-mac-addr>
<ul> <li>・ VF-IG - VRRP 仮想ルータがベースにしているインタフェース名</li> <li>Added a virtual MAC <vrrp-mac-addr> into L2 table</vrrp-mac-addr></li> <li>Notice</li> <li>レクガンータ説明:         <ul> <li>・ vrrp-mac-addr : VRRP 仮想 MAC アドレス</li> </ul> </li> <li>Deleted a virtual MAC <vrrp-mac-addr> from L2 table</vrrp-mac-addr></li> <li>Notice</li> <li>レクガンータ説明:         <ul> <li>・ vrrp-mac-addr : VRRP 仮想 MAC アドレス</li> </ul> </li> <li>Deleted a virtual MAC </li> <li>vrrp-mac-addr : VRRP 仮想 MAC アドレス</li> <li>レクガンータ説明:             <ul> <li>・ vrrp-mac-addr : VRRP 仮想 MAC アドレス</li> <li>レクガンータ説明:             <ul> <li>・ vrrp-mac-addr : VRRP 仮想 MAC アドレス</li> <li>レクガンータ説明:             <ul> <li>・ vrrp-mac-addr : VRRP 仮想 MAC アドレス</li> <li>レクガントク (位想 MAC アドレスがスイッチの L2 テーブルから削除されました。</li> <li>レクガントク (位想 MAC アドレスがスイッチの L3 table</li> <li>Notice</li> <li>レクガントク (位想 MAC アドレスがスイッチの L3 table</li> <li>レクガントク (切割 MAC アドレスがスイッチの L3 table</li> <li>レクガントク (切割 MAC アドレスがスイッチの L3 table)</li> </ul> </li> </ul></li></ul></li></ul>
Added a virtual MAC <vrrp-mac-addr> into L2 table       Notice       仮想 MAC アドレスがスイッチのL2         パラメータ説明:       ・ vrrp-mac-addr : VRRP 仮想 MAC アドレス       Notice       仮想 MAC アドレスがスイッチのL2         Deleted a virtual MAC <vrrp-mac-addr> from L2 table       Notice       仮想 MAC アドレスがスイッチのL2         パラメータ説明:       ・ vrrp-mac-addr&gt; from L2 table       Notice       仮想 MAC アドレスがスイッチのL2         パラメータ説明:       ・ vrrp-mac-addr&gt; from L2 table       Notice       仮想 MAC アドレスがスイッチのL2         パラメータ説明:       ・ vrrp-mac-addr : VRRP 仮想 MAC アドレス       アーブルから削除されました。         パラメータ説明:       ・ vrrp-ip-addr&gt; MAC <vrrp-mac-addr> into L3 table       Notice       仮想 MAC アドレスがスイッチの L3         パラメータ説明:       ・ vrrp-ip-addr&gt; MAC <vrrp-mac-addr> into L3 table       Notice       仮想 MAC アドレスがスイッチの L3</vrrp-mac-addr></vrrp-mac-addr></vrrp-mac-addr></vrrp-mac-addr>
Added a virtual MAC      VRPP 仮想 MAC アドレス       パラメータ説明:     ・ vrrp-mac-addr : VRRP 仮想 MAC アドレス       Deleted a virtual MAC      vrrp-mac-addr > from L2 table       パラメータ説明:     ・ vrrp-mac-addr > from L2 table
パラメータ説明:       ・ vrrp-mac-addr : VRRP 仮想 MAC アドレス         Deleted a virtual MAC <vrrp-mac-addr> from L2 table       Notice       仮想 MAC アドレスがスイッチの L2         パラメータ説明:       ・ vrrp-mac-addr : VRRP 仮想 MAC アドレス       んdded a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table       Notice       仮想 MAC アドレスがスイッチの L3         パラメータ説明:       ・ vrrp-mac-addr : VRRP 仮想 MAC マドレス       ・ vrrp-mac-addr : VRRP 仮想 MAC マドレス       ・ vrrp-mac-addr : VRRP 仮想 MAC <vrrp-mac-addr> into L3 table       Notice       仮想 MAC アドレスがスイッチの L3         パラメータ説明:       ・ vrrp-ip-addr&gt; MAC <vrrp-mac-addr> into L3 table       Notice       仮想 MAC アドレスがスイッチの L3</vrrp-mac-addr></vrrp-mac-addr></vrrp-mac-addr></vrrp-ip-addr></vrrp-mac-addr>
<ul> <li>vrrp-mac-addr: VRRP 仮想 MAC アドレス</li> <li>Deleted a virtual MAC <vrrp-mac-addr> from L2 table</vrrp-mac-addr></li> <li>パラメータ説明:         <ul> <li>vrrp-mac-addr: VRRP 仮想 MAC アドレス</li> </ul> <ul> <li>Motice</li> <li>仮想 MAC アドレスがスイッチの L2</li> <li>テーブルから削除されました。</li> </ul> </li> <li>Added a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table</vrrp-mac-addr></vrrp-ip-addr></li> <li>Notice</li> <li>仮想 MAC アドレスがスイッチの L3</li> <li>テーブルに追加されました。</li> </ul>
Deleted a virtual MAC <vrrp-mac-addr> from L2 table     Notice     仮想 MAC アドレスがスイッチの L2       パラメータ説明:     ・ vrrp-mac-addr : VRRP 仮想 MAC アドレス     んdded a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table     Notice     仮想 MAC アドレスがスイッチの L3       パラメータ説明:     ・ vrrp-ip-addr&gt; MAC <vrrp-mac-addr> into L3 table     Notice     仮想 MAC アドレスがスイッチの L3</vrrp-mac-addr></vrrp-mac-addr></vrrp-ip-addr></vrrp-mac-addr>
Deleted a virtual MAC      virtp-mac-addr> from L2 table     Notice     仮想 MAC アドレスがスイッチのL2       パラメータ説明:     ・     ・     ・       ・     vrrp-mac-addr : VRRP 仮想 MAC アドレス     Notice     仮想 MAC アドレスがスイッチのL3       Added a virtual IP      vrrp-ip-addr> MAC      vrrp-mac-addr> into L3 table     Notice     仮想 MAC アドレスがスイッチのL3       パラメータ説明:     ・     ・     ・     ・
パラメータ説明:     ・ vrrp-mac-addr: VRRP 仮想 MAC アドレス       Added a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table     Notice       パラメータ説明:     ・ の想 MAC アドレスがスイッチの L3       アーブルに追加されました。     ・ アーブルに追加されました。</vrrp-mac-addr></vrrp-ip-addr>
<ul> <li>vrrp-mac-addr: VRRP 仮想 MAC アドレス</li> <li>Added a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table</vrrp-mac-addr></vrrp-ip-addr></li> <li>Notice</li> <li>仮想 MAC アドレスがスイッチの L3 テーブルに追加されました。</li> </ul>
Added a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table Notice 仮想 MAC アドレスがスイッチの L3 テーブルに追加されました。</vrrp-mac-addr></vrrp-ip-addr>
テーブルに追加されました。
パラメーク説明・
・ vrrp-ip-addr:VRRP IP アドレス
・ vrrp-mac-addr:VRRP 仮想 MAC アドレス
Deleted a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> from L3 table Notice 仮想 MAC アドレスがスイッチの L3</vrrp-mac-addr></vrrp-ip-addr>
「デーノルから削除されました。」 パーイーク説明・
ハファーメ武明・ ・ vrrp-ip-addr:VRRP IP アドレス
・ vrrp-mac-addr:VRRP 仮想 MAC アドレス
Failed to add virtual MAC <vrrp-mac-addr> into chip L2 table. Errcode <vrrp- error="" td="" スイッチチップl2="" テーブルへの仮想<=""></vrrp-></vrrp-mac-addr>
errcode> MAC の追加に失敗しました。
パラメータ説明:
・ vrrp-mac-addr:VRRP 仮想 MAC アドレス
・ vrrp-errcode ・ VKKY ノロトコル動作のノエフーコード
Failed to delete virtual MAC <vrrp-mac-addr> from chip L2 table. Errcode <vrrp-lp l2="" lp="" td="" テーブルの仮想<=""></vrrp-lp></vrrp-mac-addr>
encode> MAC の削除に失敗しました。
パラメータ説明:
・ vrrp-mac-addr:VRRP 仮想 MAC アドレス
・ vrrp-errcode:VRRP プロトコル動作のエラーコード
Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. L3 table Error スイッチL3 テーブルへの仮想 MAC の</vrrp-mac-addr></vrrp-ip-addr>
is full 追加に失敗しました。L3 テーブルは満
杯です。

ログの内容	緊急度	イベントの説明
Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Port</vrrp-mac-addr></vrrp-ip-addr>	Error	スイッチ L3 テーブルへの仮想 MAC の
<mac-port> is invalid</mac-port>		追加に失敗しました。MAC を学習した
		ポートが無効です。
パラメータ説明:		
・ vrrp-ip-addr:VRRP IP アドレス		
・ vrrp-mac-addr:VRRP 仮想 MAC アドレス		
・ mac-port:VRRP 仮想 MAC のボート番号		
Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Interface</vrrp-mac-addr></vrrp-ip-addr>	Error	スイッチL3 テーブルへの仮想 MAC の
<mac-intt> is invalid</mac-intt>		道加に矢敗しました。MAC を字習した
パニマーク説明・		$1 \mathcal{I} \mathcal{I} \mathcal{I} \mathcal{I} \mathcal{I} \mathcal{I} \mathcal{I} \mathcal{I}$
ハノアーン読号・ vrrn-in-addr:VBRPIP アドレス		
・ vrrp-mac-addr:VRRP 仮相 MAC アドレス		
<ul> <li>mac-intf: VRRP 仮想 MAC アドレスを基にしたインタフェース</li> </ul>		
Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into I 3 table Box id</vrrp-mac-addr></vrrp-ip-addr>	Frror	   スイッチ 3 テーブルへの仮相 MAC の
<pre><mac-box> is invalid</mac-box></pre>		追加に失敗しました。MAC を学習した
		ボックスが無効です。
パラメータ説明:		
・ vrrp-ip-addr:VRRP IP アドレス		
・ vrrp-mac-addr:VRRP 仮想 MAC アドレス		
・ mac-box:VRRP 仮想 MAC アドレスを基にしたインタフェース		
Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into chip L3 table.</vrrp-mac-addr></vrrp-ip-addr>	Error	スイッチチップのL3 テーブルへの仮想
Errcode <vrrp-errcode></vrrp-errcode>		MAC の追加に失敗しました。
パラメータ説明:		
・ vrrp-ip-addr:VRRP IP アドレス		
・ vrrp-mac-addr:VRRP 仮想 MAC アドレス		
・ vrrp-errcode:VRRP フロトコル動作のエラーコード		
Failed to delete virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> from chip L3 table.</vrrp-mac-addr></vrrp-ip-addr>	Error	スイッチチップのL3 テーブルへの仮想
Errcode <vrrp-errcode></vrrp-errcode>		MAC の削除に矢敗しました。 
パニマーク説明・		
ハノアーン読号・ vrrn-in-addr:VBRPIP アドレス		
・ vrrp-mac-addr · VRRP 仮相 MAC アドレス		
・ vrrp-errcode:VRRP プロトコル動作のエラーコード		
WAC	<u> </u>	1
Web-Authentication host login fail (User Name: <string>, IP: <ipaddr ipy6address="" l="">,</ipaddr></string>	Warning	クライアントホストが認証に失敗しま
MAC: <macaddr>, Port: &lt;[unitID:]portNum&gt;, VID: <vlan-id>)</vlan-id></macaddr>	l	
- · · · · · · · · · · · · · · · · · · ·		
パラメータ説明:		
・ string:ユーザ名		
・ ipaddr:IP アドレス		
・ ipv6address:IPv6 アドレス		
・ macaddr:MAC アドレス		
・ unitID:ユニット ID		
・ portNum:ポート番号		
• vlan-id:VLAN ID		

ログの内容	緊急度	イベントの説明
Web-Authentication enters stop learning state	Warning	デバイス全体において認証ユーザ数が 最大値に達した時、本ログが生成され ます。
Web-Authentication recovered from stop learning state	Warning	タイムインターバルのデバイス全体に おいて認証ユーザ数が最大値を割り込 んだ時、本ログが生成されます。
Web-Authentication host login success (Username: <string>, IP: <ipaddr  <br="">ipv6address&gt;, MAC: <macaddr>, Port: &lt;[unitID:] portNum&gt;, VID: <vlan-id>)</vlan-id></macaddr></ipaddr></string>	Informational	クライアントホストが認証に成功しま した。
<ul> <li>パラメータ説明:</li> <li>string:ユーザ名</li> <li>ipaddr: IP アドレス</li> <li>ipv6address: IPv6 アドレス</li> <li>macaddr: MAC アドレス</li> <li>unitID:ユニット ID</li> <li>portNum:ポート番号</li> </ul>		
• Vian-Id • VLAN ID		
Successful login through Web (Username: <username>, IP: <ipaddr>).</ipaddr></username>	Informational	Web 経由でのログインに成功しまし
<b>パラメータ説明:</b> ・ username:ユーザ名 ・ ipaddr:IP アドレス		
Login failed through Web (Username: <username>, IP: <ipaddr>).</ipaddr></username>	Warning	Web 経由でのログインに失敗しました。
<b>パラメータ説明:</b> ・ username:ユーザ名 ・ ipaddr:IP アドレス		
Web session timed out (Username: <username>, IP: <ipaddr>).</ipaddr></username>	Informational	Web セッションがタイムアウトしました。
<b>パラメータ説明:</b> ・ username:ユーザ名 ・ ipaddr:IP アドレス		
Logout through Web (Username: <username>, IP: <ipaddr>).</ipaddr></username>	Informational	Web 経由でのログアウトしました。
<b>パラメータ説明:</b> ・ username:ユーザ名 ・ ipaddr:IP アドレス		
Successful login through Web (SSL) (Username: <username>, IP: <ipaddr>)</ipaddr></username>	Informational	Web 経由でのログイン成功(SSL)
<b>パラメータ説明:</b> • username:ユーザ名 • ipaddr:IP アドレス		
Login failed through Web (SSL) (Username: <username>, IP: <ipaddr>).</ipaddr></username>	Warning	Web 経由でのログイン失敗(SSL)
<ul> <li>パラメータ説明:</li> <li>username:ユーザ名</li> <li>ipaddr: IP アドレス</li> </ul>		
Web (SSL) session timed out (Username: <username>, IP: <ipaddr>).</ipaddr></username>	Informational	Web セッションがタイムアウトしました。(SSL)
<ul> <li>パラメータ説明:</li> <li>username:ユーザ名</li> <li>ipaddr:IPアドレス</li> </ul>		

ログの内容	緊急度	イベントの説明
Logout through Web (SSL) (Username: <username>, IP: <ipaddr>).</ipaddr></username>	Informational	Web 経由でのログアウト成功(SSL)
パラメータ説明:		
・ username:ユーザ名		
・ ipaddr:IP アドレス		
Zone Defense		
Zone defense function has been enabled by <session> (Username: <username>, IP:</username></session>	Warning	ゾーンディフェンスが有効化されまし
<ipaddr>)</ipaddr>		た。
パラメータ説明:		
・ session:ユーザセッション(Console, SNMP, WEB, Telnet)		
・ username:ユーザ名		
・ ipaddr:IP アドレス		
Zone defense function has been disabled by <session> (Username: <username>, IP:</username></session>	Warning	ゾーンディフェンスが無効化されまし
<ipaddr>)</ipaddr>		た。
パラメータ説明:		
・ session:ユーザセッション(Console, SNMP, WEB, Telnet)		
・ username:ユーザ名		
・ ipaddr:IP アドレス		

# 付録C トラップログエントリ

カテゴリ	トラップ名	説明	OID
802.1X	dDot1xExtLoggedSuccess	ホストがログインに成功したときに送信されます。	1.3.6.1.4.1.17
		(802.1X 認証にパス)	1.14.30.0.1
		関連オブジェクト:	
		(1) ifIndex	
		(2) dnaSessionClientMacAddress	
		(3) dnaSessionAuthVlan	
		(4) dnaSessionAuthUserName	
	dDot1xExtLoggedFail	ホストが 802.1X 認証に失敗したときに送信されます。	1.3.6.1.4.1.17
		(ログインに失敗)	1.14.30.0.2
		関連オブジェクト:	
		(1) ifIndex	
		(2) dnaSessionClientMacAddress	
		(3) dnaSessionAuthVlan	
		(4) dnaSessionAuthUserName	
		(5) dDot1xExtNotifyFailReason	
902 2ab 04M	dat20amThrashaldEvant	「キい店も招ラスローカルノリエートノベントが検出されま」	126121
OUZ.Jan UAM		してい 値を超えるローカルアウモードイバンドが快山されよし	1.5.0.1.2.1.
			150.0.1
		関連オブジェクト:	
		(1) dot3OamEventLogTimestamp	
		(2) dot3OamEventLogOui	
		(3) dot3OamEventLogType	
		(4) dot3OamEventLogLocation	
		(5) dot3OamEventLogWindowHi	
		(6) dot3OamEventLogWindowLo	
		(7) dot3OamEventLogThresholdHi	
		(8) dot3OamEventLog1hresholdLo	
		(9) dot3OamEventLogValue	
		(10) dot3OamEventLogRunningTotal	
	dat30amNanThrashaldEvant	(11) dot Solan Event Log Event Total	1361
		した。	21158
			0.2
		Binding objects:	
		(1) dot3OamEventLogTimestamp	
		(2) dot3OamEventLogOui	
		(3) dot3OamEventLogType	
		(4) dot3OamEventLogLocation	
		(5) dot3OamEventLogEventTotal	
Authentication	authenticationFailure	authenticationFailure トラップは、SNMPv2 エンティティが、	1.3.6.1.6.3.1.
Fail		エージェントロールで動作し、正しく認証されないプロトコル	1.5.5
(認証失敗)		メッセージを受信したことを表します。SNMPv2のすべての実	
		装は、このトラップを生成することができる必要がある一方、	
		snmpEnableAuthenTraps オブジェクトは、このトラップが生	
		成されるか否かを示します。	

スイッチにおいて現れる可能性のあるトラップログエントリとそれらの意味を以下に示します。
カテゴリ	トラップ名	説明	OID
BGP	bgpEstablishedNotification	BGP FSM が完成状態になった時に、 「bgpEstablishedNotification」イベントが起動します。	1.3.6.1.2.1.15.0.1
		関連オブジェクト : (1) bgpPeerRemoteAddr (2) bgpPeerLastError (3) bgpPeerState	
	bgpBackwardTransNotification	BGP FSM が高い値から低い値への移行時に、 「bgpBackwardTransNotification」イベントが起動します。	1.3.6.1.2.1.15.0.2
		関連オブジェクト : (1) bgpPeerRemoteAddr (2) bgpPeerLastError (3) bgpPeerState	
BPDU Protection	dBpduProtectionAttackOccur	インタフェースで BPDU アタックが発生したときに送信されます。 問題ませブジェクト・	1.3.6.1.4.1.17 1.14.47.0.1
		国連オフジェクト: (1) ifIndex (2) dBpduProtectionIfCfgMode	
	dBpduProtectionAttackRecover	インタフェースで BPDU アタックが回復したときに送信されます。	1.3.6.1.4.1.17 1.14.47.0.2
		剣連オフジェクト : (1) ifIndex	
CFM	dot1agCfmFaultAlarm	接続に不具合が生じた場合、生成されます。 関連オブジェクト: (1) dot1ag(fmMapHigbortPrDofact	1.3.111.2.802. 1.1.8.0.1
CFM Extension	dCfmAisOccurred	<ul> <li>(i) dottageninkepingiteat ibeteet</li> <li>ローカル MEP が AIS ステータスになった場合、生成されます。</li> <li>関連オブジェクト: <ul> <li>(1) dCfmEventMdIndex</li> <li>(2) dCfmEventMaIndex</li> <li>(3) dCfmEventMepIdentifier</li> </ul> </li> </ul>	1.3.6.1.4.1.171. 14.86.0.1
	dCfmAisCleared	ローカル MEP が AIS ステータスから解除された場合、生成さ れます。	1.3.6.1.4.1.171. 14.86.0.2
		関連オブジェクト : (1) dCfmEventMdIndex (2) dCfmEventMaIndex (3) dCfmEventMepIdentifier	
	dCfmLockOccurred	ローカル MEP が鍵ステータスになった場合、生成されます。 関連オブジェクト: (1) dCfmEventMdIndex (2) dCfmEventMaIndex (3) dCfmEventMepIdentifier	1.3.6.1.4.1.171. 14.86.0.3
	dCfmLockCleared	ローカル MEP の鍵ステータスが解除された場合、生成されます。 関連オブジェクト: (1) dCfmEventMdIndex (2) dCfmEventMaIndex (3) dCfmEventMepIdentifier	1.3.6.1.4.1.171. 14.86.0.4

カテゴリ	トラップ名	説明	OID
DDM	dDdmAlarmTrap	異常なアラームが発生、または正常な状態に回復した際に通 知されます。現在の値 > low warning または現在の値 < high warning にときにのみリカバトラップを送信します。	1.3.6.1.4.1.17 1.14.72.0.1
		関連オブジェクト: (1) dDdmNotifyInfolfIndex, (2) dDdmNotifyInfoComponent (3) dDdmNotifyInfoAbnormalLevel (4) dDdmNotifyInfoThresholdExceedOrRecover	
	dDdmWarningTrap	異常な警告が発生、または正常な状態に回復した際に通知され ます。	1.3.6.1.4.1.17 1.14.72.0.2
		関連オブジェクト: (1) dDdmNotifyInfolfIndex, (2) dDdmNotifyInfoComponent (3) dDdmNotifyInfoAbnormalLevel (4) dDdmNotifyInfoThresholdExceedOrRecover	
DHCP サーバ スクリーン	dDhcpFilterAttackDetected	DHCP サーバスクリーンが有効なとき、スイッチが偽造 DHCP サーバパケットを受信すると、攻撃パケットを受信したイベン トをトラップ送信します。	1.3.6.1.4.1.17 1.14.133.0.1
防止		関連オブジェクト: (1) dDhcpFilterLogBufServerlpAddr (2) dDhcpFilterLogBufClientMacAddr (3) dDhcpFilterLogBufferVlanId (4) dDhcpFilterLogBufferOccurTime	
DoS 防止	dDosPreveAttackDetectedPacket	DoS アタックを検出したとき送信されます。 関連オブジェクト: (1) dDoSPrevCtrlAttackType (2) dDosPrevNotiInfoDropIpAddr (3) dDosPrevNotiInfoDropPortNumber	1.3.6.1.4.1.17 1.14.59.0.2
ERPS	dErpsFailuredetectedNotif	「dErpsNotificationEnabled」が 'true' でシグナル不具合が検出 されると「dErpsFailureNotification」が送信されます。	1.3.6.1.4.1.171. 14.78.0.1
	dErpsFailureClearedNotif	「dErpsNotificationEnabled」が 'true' でシグナル不具合が解消 されると「dErpsFailureClearedNotif」が送信されます。	1.3.6.1.4.1.171. 14.78.0.2
	dErpsRPLOwnerConflictNotif	「dErpsNotificationEnabled」が 'true' で RPL オーナコンフリク トが検出されると「dErpsOwnerConflictNotif」が送信されます。	1.3.6.1.4.1.171. 14.78.0.3
ErrDisable	dErrDisNotifyPortDisabledAssert	ポートがエラー無効状態になった時に送信されます。 関連オブジェクト: (1) dErrDisNotifyInfoPortIfIndex (2) dErrDisNotifyInfoReasonID	1.3.6.1.4.1.171. 14.45.0.1
	dErrDisNotifyPortDisabledClear	指定間隔の後、ポートループ再始動時に送信されます。 関連オブジェクト: (1) dErrDisNotifyInfoPortIfIndex (2) dErrDisNotifyInfoReasonID	1.3.6.1.4.1.171. 14.45.0.2
External Alarm	dExternalAlarmStatusChg	<ul> <li>外部警告ステートが変更されると、コマンダスイッチは本通知 を送信します。</li> <li>関連オブジェクト: <ul> <li>(1) dExternalAlarmUnitID</li> <li>(2) dExternalAlarmChannel</li> <li>(3) dExternalAlarmStatus</li> </ul> </li> </ul>	1.3.6.1.4.1.171. 14.32.0.1
Gratuitous ARP 機能	agentGratuitousARPTrap	<ul> <li>IP アドレスが重複していた場合に送信されます。</li> <li>関連オブジェクト: <ul> <li>(1) ipaddr</li> <li>(2) macaddr</li> <li>(3) portNumber</li> <li>(4) agentGratuitousARPInterfaceName</li> </ul> </li> </ul>	1.3.6.1.4.1.17 1.14.75.0.1

カテゴリ	トラップ名	説明	OID
IP-MAC-Port Binding	dImpbViolationTrap	アドレス違反通知は IP-MAC ポートバインディングアドレス違反が検出された際に生成されます。	1.3.6.1.4.1.17 1.14.22.0.1
(IMPB)		関連オブジェクト: (1) ifIndex (2) dImpbViolationIpAddrType (3) dImpbViolationIpAddress (4) dImpbViolationMacAddress (5) dImpbViolationVlan	
LACP	linkUp	「linkUp」トラップはエージェント役の SNMP エンティティに よって、コミュニケーションリンクの一つが「notPresent」ス テート以外の他のステートからダウンステートに移行しよう としている「ifOperStatus」オブジェクトの検出を意味します。 他のステートは「ifOperStatus」に含まれる値によって識別さ れます。	1.3.6.1.6.3.1.1.5.4
		関連オブジェクト: (1) ifIndex, (2) if AdminStatus (3) ifOperStatu	
	linkDown	「linkDown」トラップはエージェント役の SNMP エンティティ によって、コミュニケーションリンクの一つがダウンステート に残り、「notPresent」ステート以外の他のステートに移行す る「ifOperStatus」オブジェクトの検出を意味します。他のステー トは「ifOperStatus」に含まれる値によって識別されます。	1.3.6.1.6.3.1.1.5.3
		関連オブジェクト: (1) ifIndex, (2) if AdminStatus (3) ifOperStatu	
LBD	swPortLoopOccurred	インタフェースにループが発生したときに送信されます。 関連オブジェクト: (1) dLbdNotifyInfolfIndex	1.3.6.1.4.1.17 1.14.46.0.1
	swPortLoopRestart	間隔時間後、インタフェースのループが再スタートしたときに 送信されます。	1.3.6.1.4.1.17 1.14.46.0.2
		関連オフジェクト: (1) dLbdNotifyInfolfIndex	
	swVlanLoopOccurred	インタフェースに VID ループが発生したときに送信されます。 関連オブジェクト : (1) dLbdNotifyInfolfIndex (2) dLbdNotifyInfoVIanId	1.3.6.1.4.1.17 1.14.46.0.3
	swVlanLoopRestart	間隔時間後、VIDのインタフェースループが再スタートしたと きに送信されます。 関連オブジェクト: (1) dl bdNatifidafalfaday	1.3.6.1.4.1.17 1.14.46.0.4
		(2) dLbdNotifyInfoVlanId	
LDP	mplsLdpInitSessionThresholdExceeded	「backoff」有効時、セッション初期化メッセージ数が「mplsLdp EntityInitSessionThreshold」のしきい値を超えると送信されます。	1.3.6.1.2.1.10. 166.4.0.1
	mplsLdpPathVectorLimitMismatch	「mplsLdpEntityPathVectorLimit」が指定のエントリで 「mplsLdpPeerPathVectorLimit」の値と合致しない場合、送信 されます。	1.3.6.1.2.1.10. 166.4.0.2
	mplsLdpSessionUp	「mplsLdpSessionState」ステートが「operational(5)」ステート になると送信されます。	1.3.6.1.2.1.10. 166.4.0.3
	mplsLdpSessionDown	「mplsLdpSessionState」ステートが「operational(5)」ステート になると送信されます。	1.3.6.1.2.1.10. 166.4.0.4

カテゴリ	トラップ名	説明	OID
LLDP-MED	lldpRemTablesChange	「IldpRemTablesChange」通知は「IldpStatsRemTableLastChang eTime」変更時に送信されます。	1.0.8802. 1.1.2.0.0.1
		関連オブジェクト: (1) lldpStatsRemTablesInserts (2) lldpStatsRemTablesDeletes (3) lldpStatsRemTablesDrops (4) lldpStatsRemTablesAgeouts	
	lldpXMedTopologyChangeDetected	ローカルポートに新しいリモートデバイスがアタッチされた、 またはリモートデバイスがポートから切断 / 移動した場合のト ポロジの変更を感知するローカルデバイスによって送信されま す。	1.0.8808. 1.1.2.1.5.4795.0.1
		関連オブジェクト: (1) IldpRemChassisIdSubtype (2) IldpRemChassisId (3) IldpXMedRemDeviceClass	
MAC-based アクセス	dMacAuthLoggedSuccess	MAC ベースのアクセスコントロールホストがログインに成功 したときに送信されます。	1.3.6.1.4.1.17 1.14.153.0.1
コントロール		関連オブジェクト : (1) ifIndex, (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan	
	dMacAuthLoggedFail	MAC ベースのアクセスコントロールホストがログインに失敗 したときに送信されます。	1.3.6.1.4.1.17 1.14.153.0.2
		関連オブジェクト: (1) ifIndex, (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan	
	dMacAuthLoggedAgesOut	MAC ベースのアクセスコントロールホストがエージングアウトしたときに送信されます。	1.3.6.1.4.1.17 1.14.153.0.3
		関連オブジェクト: (1) ifIndex, (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan	
MAC Notification	dL2FdbMacNotification	本トラップはアドレステーブルの MAC アドレスに変更が生じたことを意味します。	1.3.6.1.4.1.17 1.14.3.0.1
		関連オブジェクト : (1) dL2FdbMac ChangeNotifyInfo	
	dL2FdbMacNotificationWithVID	本トラップはアドレステーブルの MAC アドレス(VLAN ID)に 変更が生じたことを意味します。	1.3.6.1.4.1.17 1.14.3.0.2
		関連オブジェクト : (1) dL2FdbMacChangeNotifyInfoWithVID	
MPLS	mplsXCUp	「mplsXCOperStatus」オブジェクトが「mplsXCTable」におい て近接するエントリが他のステートから「Up」ステートになっ た際、送信されます。	1.3.6.1.2.1.10. 166.2.0.1
	mplsXCDown	「mplsXCOperStatus」オブジェクトが「mplsXCTable」におい て近接するエントリが他のステートから「Down」ステートに なった際、送信されます。	1.3.6.1.2.1.10. 166.2.0.2

カテゴリ	トラップ名	説明	OID
MSTP	newRoot	newRoot トラップは、送信側のエージェントがスパニングツ	1.3.6.1.2.1.17
		リーの新しいルートになったことを示します。トラップは、新	.0.1
		しいルートとして選出された後にすぐにブリッジによって送信	
		され、その選出に続いてすぐに Topology Change Timer のアク	
		ションの起動などを行います。	
		本トラップの実行はオプションです。	
	topologyChange	topologyChange トラップは、構成するいずれかのポートが	1.3.6.1.2.1.17
		Learning 状態から Forwarding 状態に、Forwarding 状態から	.0.2
		Blocking 状態に遷移する場合にブリッジによって送信されま	
		す。本トラップは、newRoot トラップが同様の変更に対して送	
		信される場合には送信されません。	
		本トラップの実行はオプションです	
Peripheral	dEntityExtFanStatusChg	ファン状態の変更通知	1.3.6.1.2.1.17
(周辺機器)		(ファンの不具合 (dEntityExtEnvFanStatus is 'fault') または回復	1.14.5.0.1
		(dEntityExtEnvFanStatus is 'ok'))	
		関連オブジェクト・	
		(1) dEntitvExtEnvEanUnitId	
		(2) dEntityExtEnvFanIndex	
		(3) dEntityExtEnvFanStatus	
	dEntityExtThermalStatusChg		1.3.6.1.2.1.17
		(温度警告 (dEntityExtEnvTempStatus is 'abnormal') または回復	1.14.5.0.2
		(dEntityExtEnvTempStatus is 'ok'))	
		目海オブジェクト・	
		(1) dEntityExtEnvTempUnitId	
		(2) dEntityExtEnvTempIndex	
		(3) dEntityExtEnvTempStatus	
	dEntityExtPowerStatusChg	電力状態の変更通知(電源モジュールの不具合、または不具合	1.3.6.1.2.1 17
		からの回復)	1.14.5.0.3
		(1) GENTITYEXTENVPOWERUNITIG	
		(2) dentityextenvPowerIndex	
		(3) dEntityExtEnvPowerStatus	

カテゴリ	トラップ名	説明	OID
PIM6-SM	pimNeighborLoss	「pimNeighborLoss」通知はネイバとの近隣性の消失時を 意味します。本通知はネイバタイマが期限切れになり、同 じIPバージョン、より低い IP アドレスの同じインタフェー スにネイバがいない場合に起動します。本通知はカウンタ 「pimNeighborLossCount」が増加し、「pimNieghborLossNotif icationsPeriod」によってレートリミットが指定されている場合 も起動します。	1.3.6.1.2.1. 157.0.1
		(1)pimNeighborUpTime	
	pimInvalidRegister	「pimInvalidRegister」通知はデバイスによって不正な PIM Register メッセージが受信された場合に起動します。 本通知はカウンタ「pimInvalidRegisterMsgsRcvd」が増加し、 「pimInvalidRegisterNotificationPeriod」によってレートリミッ トが指定されている場合も起動します。	1.3.6.1.2.1. 157.0.2
		関連オブジェクト: (1) pimGroupMappingPimMode (2) pimInvalidRegisterAddressType (3) pimInvalidRegisterOrigin (4) pimInvalidRegisterGroup (5) pimInvalidRegisterRp	
	pimInvalidJoinPrune	「pimInvalidJoinPrune」通知はデバイスによって不正な PIM Join/Prune メッセージが受信された場合に起動します。 本通知はカウンタ「pimInvalidJoinPruneMsgsRcvd」が増加し、 「pimInvalidJoinPruneNotificationPeriod」によってレートリミッ トが指定されている場合も起動します。	1.3.6.1.2.1. 157.0.3
		関連オブジェクト: (1) pimGroupMappingPimMode (2) pimInvalidJoinPruneAddressType (3) pimInvalidJoinPruneOrigin (4) pimInvalidJoinPruneGroup (5) pimInvalidJoinPruneRp (6) pimNeighborUpTime	
	pimRPMappingChage	「pimRPMappingChange」通知はデバイスによって不正な PIM Join/Prune メッセージが受信された場合に起動します。 本通知はカウンタ「pimRPMappingChangeCount」が増加し、 「pimRPMappingChangeNotificationPeriod」によってレートリ ミットが指定されている場合も起動します。	1.3.6.1.2.1. 157.0.4
		関連オブジェクト : (1) pimGroupMappingPimMode (2) pimGroupMappingPrecedence	
	pimInterfaceElection	「pimInterfaceElection」通知はデバイスによって不正な PIM Join/Prune メッセージが受信された場合に起動します。 本通知はカウンタ「pimInterfaceElectionWinCount」が増加し、 「pimInterfaceElectionNotificationPeriod」によってレートリ ミットが指定されている場合も起動します。	1.3.6.1.2.1. 157.0.5
		関連オブジェクト: (1) pimInterfaceAddressType (2) pimInterfaceAddress	

カテゴリ	トラップ名	説明	OID
PoE	pethMainPowerUsageOnNotification	使用率が PSE しきい値に到達した事を示唆しています。同じ	1.3.6.1.2.1.105
		オブジェクトインスタンスによって通知が放出されるまで最低	.0.2
		500 ミリ秒が経過する必要があります。	
		関連オブジェクト:	
		(1) pethMainPseConsumptionPower	
	pethMainPowerUsageOffNotification	使用率が PSE しきい値を下回った事を示唆しています。同じ	1.3.6.1.2.1.105
		オノンエクトイノスタノスによつく通知が放出されるまで最低	.0.3
		500 ミリ杉が柱廻する必要がめります。 関連オブジェクト・	
		(1) pethMainPseConsumptionPower	
	dPoelfPowerDeniedNotification	PSE 状況ダイアグラムが POWER_DENIED になった事を示唆す	136141171
		る通知です。同じオブジェクトインスタンスによって通知が放	.14.24.0.1
		出されるまで最低 500 ミリ秒が経過する必要があります。	
		関連オブジェクト:	
		(1) pethPsePortPowerDeniedCounter	
	dPoelfPowerOverLoadNotification	PSE 状況ダイアグラムが ERROR_DELAY_OVER になった事を示	1.3.6.1.4.1.171
		唆するトラップです。同じオブジェクトインスタンスによって	.14.24.0.2
		通知が放出されるまで最低 500 ミリ秒が経過する必要がありま	
		浅理オフンエクト:	
	dDoolfDowerShortCircuitNotification		1 2 6 1 / 1 171
	appenpowershortcircultinotification	$PSE 状 ( ボダイアク ノム ) ERROR_DELAT_SHORT になりた事を 示唆するトラップです。同じオブジェクトインスタンスによっ$	1.3.0.1.4.1.171
		て通知が放出されるまで最低 500 ミリ秒が経過する必要があり	.17.27.0.3
		関連オブジェクト:	
		(1) pethPsePortShortCounter	
	dPoelfPdAliveFailOccurNotification	PD が動作を中止、回答不能になった事を示唆するトラップで	1.3.6.1.4.1.171
		す。同じオブジェクトインスタンスによって通知が放出される	.14.24.0.4
		まで最低 500 ミリ秒が経過する必要があります。	
Port Security	dPortSecMacAddrViolation	ポートセキュリティトラップが有効な場合、事前定義された	1.3.6.1.4.1.17
		ボートセキュリティ設定に違反する新しい MAC アドレスが送	1.14.8.0.1
セキュリティ)		出するトリカトラツノメツセーンです。 関連オゴジェクト・	
		実更オブジェット・   (1) ifIndex	
		(2) dPortSeclfCurrentStatus	
		(3) dPortSecIfViolationMacAddress	
Port	linkUp	ポートがリンクアップしたときに生成されます。	1.3.6.1.6.3.1
(ポート)		間連オブジェクト・	1.5.4
		(1) ifIndex	
		(2) if AdminStatus	
		(3) ifOperStatu	
	linkDown	ポートがリンクダウンしたときに生成されます。	1.3.6.1.6.3.1
		周浦ナブジェクト・	1.5.3
		(1) ifIndex	
		(2) if AdminStatus	
		(3) ifOperStatu	
Reboot	agent Reboot In 5 Min	再起動のカウントダウンが5分になった時点で送信されます。	1.3.6.1.4.1.171.
Schedule			14.170.0.1
	agentRebootIn1Min	再起動のカウントダウンが1分になった時点で送信されます。	1.3.6.1.4.1.171.
			14.170.0.2

カテゴリ	トラップ名	説明	OID
RMON	risingAlarm	SNMP トラップは、アラームエントリが上昇しきい値超える時	1.3.6.1.2.1.16
		に生成され、SNMP トラップの送信に設定されたイベントを生	.0.1
		成します。	
		関連オブジェクト:	
		(1)alarmIndex	
		(2)alarmVariable	
		(3)alarmSampleType	
		(4) alarmValue	
		(5) alarmRisingThreshold	
	fallingAlarm	SNMP トラップは、アラームエントリが下降しきい値を下回る	1.3.6.1.2.1.16
		ときに生成され、NSMP トラップの送信に設定されたイベント	.0.2
		を生成します。	
		関連オブジェクト:	
		(1)alarmIndex	
		(2) alarmVariable	
		(3)alarmSampleType	
		(4)alarmValue	
		(5) alarmFallingThreshold	
Safeguard	dSafeguardChgToExhausted	システムが操作モードをノーマルから exhausted に変更したこ	1.3.6.1.4.1.17
(セーフガード)		とを示します。	1.14.19.1.1.0.
		関連オブジェクト:	1
		(1) dSafeguardEngineCurrentMode	
	dSafeguardChgToNormal	システムが操作モードを exhausted からノーマルに変更したこ	1.3.6.1.4.1.17
		とを示します。	1.14.19.1.1.0.
		  関連オブジェクト:	2
		(1) dSafeguardEngineCurrentMode	

カテゴリ	トラップ名	説明	OID
SIM	swSingleIPMSColdStart	コマンダースイッチはメンバが cold start 通知を生成するとき にこの通知を送信します。	1.3.6.1.4.1.17 1.12.8.6.0.11
		関連オブジェクト : (1) swSingleIPMSID (2) swSingleIPMSMacAddr	
	swSingleIPMSWarmStart	コマンダースイッチはメンバが warm start 通知を生成するとき にこの通知を送信します。	1.3.6.1.4.1.17 1.12.8.6.0.12
		関連オブジェクト : (1) swSingleIPMSID (2) swSingleIPMSMacAddr	
	swSingleIPMSLinkDown	コマンダースイッチはメンバがリンクダウン通知を生成すると きにこの通知を送信します。	1.3.6.1.4.1.17 1.12.8.6.0.13
		関連オブジェクト: (1) swSingleIPMSID (2) swSingleIPMSMacAddr (3) ifIndex	
	swSingleIPMSLinkUp	コマンダースイッチはメンバがリンクアップ通知を生成すると きにこの通知を送信します。	1.3.6.1.4.1.17 1.12.8.6.0.14
		関連オブジェクト: (1) swSingleIPMSID (2) swSingleIPMSMacAddr (3) ifIndex	
	swSingleIPMSAuthFail	コマンダースイッチはメンバが認証失敗の通知を生成するとき にこの通知を送信します。	1.3.6.1.4.1.17 1.12.8.6.0.15
		関連オブジェクト : (1) swSingleIPMSID (2) swSingleIPMSMacAddr	
	swSingleIPMSnewRoot	コマンダースイッチはメンバが新しいルートの通知を生成する ときにこの通知を送信します。	1.3.6.1.4.1.17 1.12.8.6.0.16
		関連オブジェクト : (1) swSingleIPMSID (2) swSingleIPMSMacAddr	
	swSingleIPMSTopologyChange	コマンダースイッチはメンバがトポロジ変更の通知を生成する ときにこの通知を送信します。	1.3.6.1.4.1.17 1.12.8.6.0.17
		関連オブジェクト: (1) swSingleIPMSID (2) swSingleIPMSMacAddr	

カテゴリ	トラップ名	説明	OID
Stacking	dStackInsertNotification	ユニットホットインサート(活線挿入)の通知です。	1.3.6.1.4.1.171.
_		問連オブジェクト・	14.9.0.1
		(1) dStackNotifyInfoBoxId	
		(1) dStackhofn Meddadd	
	dStackBemoveNotification	ユニットホットリムーブ(活線抜出)の通知です。	1.3.6.1.4.1.171.
			14.9.0.2
		(1) dStackInotligiTioboxid (2) dStackInfoMacAddr	
	dStackEailureNotification	コニットスタック生敗の通知です	1361/1171
			14903
		関連オブジェクト:	1 1151015
		(1) dStackNotifyInfoBoxId	
	dStackTPChangeNotification	スタックトボロジ変更の通知です。	1.3.6.1.4.1.171.
		関連オブジェクト:	14.9.0.4
		(1) dStackNotifyInfoTopologyType	
		(2) dStackNotifyInfoBoxId	
		(3) dStackInfoMacAddr	
	dStackRoleChangeNotification	スタックユニットロール変更の通知です。	1.3.6.1.4.1.171.
		関連オブジェクト:	14.9.0.5
		(1) dStackNotifyInfoRoleChangeType	
		(2) dStackNotifyInfoBoxId	
Start	coldStart	coldStart トラップは、SNMPv2 エンティティが、エージェント	1.3.6.1.6.3.1.
(スタート)		ロールで動作し、自身を再起動し、設定か変更されたかもしれ	1.5.1
		ないことを衣しまり。	
	warmStart	warmStart トラップは、SNMPv2 エンティティが、エージェン	1.3.6.1.6.3.1.
		トロールで動作し、設定が変更されないような再起動を表しま	1.5.2
Storm Control	dStormCtrlOccurred	dStormCtrlNotifyEnable」か "stormOccurred" または "both" ぐ、	1.3.6.1.4.1.17
		ストームが検古されたことをに送信されます。	1.14.25.0.1
		関連オブジェクト:	
		(1) ifIndex,	
		(2) astormetrinotity frame type	12614117
	astormctristormcleared	「dstormLtriNotliyEnable」か stormLleared または both で、	1.3.0.1.4.1.17
			1.14.23.0.2
		関連オブジェクト:	
		(1) ifIndex,	
Custom File	defi inte adima e a		12614117
System File	lasiopioadimage	イメーシノアイルのアップロートに成功したとさに送信されま	1.3.0.1.4.1.17
(シス)ム ファイル)	dsfDownloadImage	/ メージファイルのダウンロードに成功したときに洋信されま	1361/117
	asibownioadinnage	す。	1.14.14.0.2
	dsfUploadCfg	コンフィグレーションファイルのアップロードに成功したとき	1.3.6.1.4.1.17
		に送信されます。	1.14.14.0.3
	dsfDownloadCfg	コンフィグレーションファイルのダウンロードに成功したとき	1.3.6.1.4.1.17
		に送信されます。	1.14.14.0.4
	dsfSaveCfg	コンフィグレーションファイルの保存に成功したときに送信さ	1.3.6.1.4.1.17
		れます。	1.14.14.0.5

カテゴリ	トラップ名	説明	OID
Upload/ Download	agentFirmwareUpgrade	SNMP 経由でのファームウェアアップグレードが終了した際、 送信されます。	1.3.6.1.4.1.17
		関連オブジェクト: (1) swMultilmageVersion	
	agentCfgOperCompleteTrap	コンフィグレーションが保存、アップロード、ダウンロードさ れた場合、送信されます。	1.3.6.1.4.1.17 1.12.1.7.2.0.9
		関連オブジェクト : (1) unitlD (2) agentCfgOperate (3) agentLoginUserName	
VPWS	pwDown	「pwTable」において「pwOperStatus」オブジェクトの近 接するエントリが他のステートから「down (2) 」または 「lowerLayerDown (6)」ステートになった際、送信されます。 (「notPresent (5)」からの移行時は除く)	1.3.6.1.2.1. 10.246.0.1
	pwUp	「pwTable」において「pwOperStatus」オブジェクトの近接す るエントリが他のステートから「up (1)」ステートになった際、 送信されます。(「notPresent (5)」からの移行時は除く)	1.3.6.1.2.1. 10.246.0.2
	pwDeleted	PW が削除された時に送信されます。(例;「pwRowStatus」が 「destroy (6)」にセットされる、または「non-MIB」アプリケーショ ンか「auto-discovery」のプロセス上、PW が削除された場合)	1.3.6.1.2.1. 10.246.0.3
VRRP	vrrpTrapNewMaster	送信エージェントが「Master」に変換された場合、送信されます。 関連オブジェクト: (1) vrrpOperMasterlpAddr	1.3.6.1.2.1.68 0.1
	vrrpTrapAuthFailure	<ul> <li>ルータからの受信したパケットの認証鍵、または認証タイプが ルータの認証鍵、または認証タイプと一致しない事を意味しま す。本トラップの適用はオプションです。</li> <li>関連オブジェクト:         <ol> <li>(1) vrrpTrapPacketSrc</li> <li>(2) vrrpTrapAuthErrorType</li> </ol> </li> </ul>	1.3.6.1.2.1.68 0.2
WAC (Web 認証)	swWACLoggedSuccess	<ul> <li>クライアントが Web 認証をパスしてログインに成功したとき に送信されます。</li> <li>関連オブジェクト:</li> <li>(1) swWACAuthStatePort</li> <li>(2) swWACAuthStateOriginalVid</li> <li>(3) swWACAuthStateMACAddr</li> <li>(4) swWACAuthUserName</li> <li>(5) swWACClientAddrType</li> <li>(6) swWACClientAddress</li> </ul>	1.3.6.1.4.1.17 1.14.154.0.1
	swWACLoggedFail	<ul> <li>クライアントが Web 認証に失敗してログインに失敗したとき に送信されます。</li> <li>関連オブジェクト:</li> <li>(1) swWACAuthStatePort</li> <li>(2) swWACAuthStateOriginalVid</li> <li>(3) swWACAuthStateMACAddr</li> <li>(4) swWACAuthUserName</li> <li>(5) swWACClientAddrType</li> <li>(6) swWACClientAddress</li> </ul>	1.3.6.1.4.1.17 1.14.154.0.2

# 付録

# 付録 D OpenFlow オブジェクト

アプリケーション開発者は、OpenFlow プロトコル V1.3 を使用してオブジェクトのプログラムを行うことができます。ここでは、プログラム可能な オブジェクト(Flow Table、Group Table エントリ、Meter Table エントリのオブジェクト)について説明します。

# Flow Table (フローテーブル)

### Flow Table Number Assignments

Flow Table 名	Flow Table ID	Default Table Miss Action
Policy ACL Flow Table	0	Drop

#### **Flow Table Counters**

フィールド	説明
Reference Count (Active Entries)	テーブル内のアクティブエントリ数の参照カウント
Packet Lookups	サポートされていません。
Packet Matches	サポートされていません。

# **Policy ACL Flow Table**

### Policy ACL Flow Table Match Fields

フィールド	説明	
IN_PORT	スイッチの入力ポートです。	
IN_PHY_PORT	スイッチの物理入力ポートです。	
ETH_DST	イーサネット宛先アドレスです。	
	注意 IPv6 Flow(ETH_TYPE=0x86DD)はサポートされていません。	
ETH_SRC	イーサネット送信元アドレスです。	
	注意 IPv6 Flow (ETH_TYPE=0x86DD) はサポートされていません。	
ETH_TYPE	イーサネットフレームタイプです。	
	注意 Policy ACL Flow Table は、2 つの相互排他論理サブテーブルに構成されます。IPv6 論理テーブ ルの Flow エントリは、IPv6 パケット(ETH_TYPE=0x86DD)のみに一致します。非 IPv6 論理 テーブルは非 ipv6 パケットに一致します。(ETH_TYPE ≠ 0x86DD、または ETH_TYPE の指定 なしの場合)	
VLAN_VID	VLAN ID です。	
	注意 0x1000(OFPVID_PRESENT)でプログラムされる必要があります。	
VLAN_PCP	VLAN の優先度です。	
IP_DSCP	IP DSCP(ToS フィールド内の6ビット)です。	
IP_PROTO	IP プロトコルです。	
IPV4_SRC	送信元 IPv4 アドレスです。	
IPV4_DST	宛先 IPv4 アドレスです。	
TCP_SRC	送信元 TCP ポートです。	
TCP_DST	宛先 TCP ポートです。	
UDP_SRC	送信元 UDP ポートです。	
UDP_DST	宛先 UDP ポートです。	
SCTP_SRC	送信元 SCTP ポートです。	
SCTP_DST	宛先 SCTP ポートです。	
ARP_SPA	ARP 送信元 IPv4 アドレスです。	
IPV6_SRC	送信元 IPv6 アドレスです。	
IPV6_DST	宛先 IPv6 アドレスです。	

#### Policy ACL Flow Table Instructions

フィールド	説明
Write-Actions	Policy ACL Flow Table Action Set テーブルのアクションのみ指定可能です。
Apply-Actions	Policy ACL Flow Table Action List Actions テーブルのアクションのみ指定可能です。
Clear-Actions	アクションセットを削除します。
Goto-Table	サポートされていません。
Write-Metadata	サポートされていません。
Meter	指定されたメーターを適用します。メーターエントリはフローの設定前に存在してい る必要があります。

#### Policy ACL Flow Table Action List Actions

フィールド	説明
Output	出力ポートを設定します。物理ポート及び予約済みのコントローラポートがサポート されています。
Set-Field	VLAN_PCP、IP_ECN、IP_DSCP フィールドがサポートされています。

#### Policy ACL Flow Table Action Set

フィールド	説明
Group	このテーブルの後のパケットを処理するために出力グループエントリを設定します。
	ルール及びパケットの種類と一致するグループが存在する必要があります。以下のい
	ずれかになります。
	・ レイヤ2インタフェースグループエントリ
	・ レイヤ2リライトグループエントリ
	・ レイヤ2マルチキャストグループエントリ
	・ レイヤ3ユニキャストグループエントリ
	・ レイヤ 3 ECMP グループエントリ

#### Policy ACL Flow Table Counters

フィールド	説明
Received Packets	このフローエントリによって受信されるパケット数です。
Received Bytes	このフローエントリによって受信されるパケット byte 数です。
Duration (Seconds)	フローエントリがセットされてから経過した時間(秒)です。

#### 制限事項

Policy ACL Flow Table は 2 つの排他論理サブテーブルに構成されます。1 つは IPv6 Flow に一致し、もう 1 つは非 IPv6 Flow に一致します。これら 2 つのテーブルは単一のテーブルとみなされる必要があります。以下の制限があります。

- IPv6 パケットは、Policy ACL Flow テーブルの2つのルールに一致する可能性があります。本問題を回避するため、非 IPv6 論理テーブルに、ETH\_ TYPE または他の Match Field を追加することを推奨します。
- ・ 異なるサブテーブルの2つのルールに対し、同じメーターを適用することはできません。異なるルールに対しては、それぞれ別のメーターを適用 することを推奨します。

# Group Table(グループテーブル)

# L2 Interface Group Entry Type

フィールド	説明
Group Identifier	32 ビットの符号なし整数で、OpenFlow のグループを一意に識別します。命名規則は
	L2 Interface Group Entry Naming Conversion テーブルの通りです。
Group Type	グループのタイプは Indirect です。
Counters	グループ毎のエントリカウンタを指定します。
Action Buckets	単一のアクションバケットがサポートされます。

### L2 Interface Group Entry Naming Conversion

フィールド	Bits	説明
Interface ID	0-15	インタフェース ID を指定します。
Chain ID	16-27	他のグループタイプエントリと紐づく ID を 1-4094 の範囲で指定します。
Kind	28-31	0(L2インタフェース)

### L2 Interface Group Entry Bucket Actions

フィールド	説明
Output	物理ポートのみでサポートされています。

### L2 Interface Group Entry Counters

フィールド	説明
Reference Count (Flow Entries)	現在このグループエントリを参照しているフローエントリまたはグループエントリの 数です。
Duration (Seconds)	グループエントリがセットされてから経過した時間(秒)です。

# L2 Rewrite Group Entry Type

フィールド	説明
Group Identifier	32 ビットの符号なし整数で、OpenFlow のグループを一意に識別します。命名規則は
	L2 Rewrite Group Entry Naming Conversion テーブルの通りです。
Group Type	グループのタイプは Indirect です。
Counters	グループ毎のエントリカウンタを指定します。
Action Buckets	単一のアクションバケットがサポートされます。

#### L2 Rewrite Group Entry Naming Conversion

フィールド	Bits	説明
ID	0-27	本タイプのグループエントリを区別するためのインデックス値です。
Kind	28-31	1 (L2 Rewrite)

### L2 Rewrite Group Entry Bucket Actions

フィールド	説明
Group	このフィールドはレイヤ2インタフェースグループエントリに紐づく必要があります。
Set-Field	ETH_DST、ETH_SRC、VLAN_VID フィールドを設定します(オプション)。

### L2 Rewrite Group Entry Counters

フィールド	説明
Reference Count (Flow Entries)	現在このグループエントリを参照しているフローエントリまたはグループエントリの 数です。
Duration (Seconds)	グループエントリがセットされてから経過した時間(秒)です。

# L2 Multicast Group Entry Type

フィールド	説明
Group Identifier	32 ビットの符号なし整数で、OpenFlow のグループを一意に識別します。命名規則は
	L2 Multicast Group Entry Naming Conversion テーブルの通りです。
Group Type	グループのタイプは All です。
Counters	グループ毎のエントリカウンタを指定します。
Action Buckets	単一のアクションバケットがサポートされます。

#### L2 Multicast Group Entry Naming Conversion

. , , ,		
フィールド	Bits	説明
Index	0-15	これらの種類のグループのインデックスです。
Chain ID	16-27	レイヤ2インタフェースグループエントリの参照に使用されます。1-4094の範囲で指 定します。
Kind	28-31	3(L2 マルチキャスト)

### L2 Multicast Group Entry Bucket Actions

フィールド	説明
Group	このフィールドはレイヤ2インタフェースグループエントリに紐づきます。該当エン
	トリの Chain ID 名コンポーネントは、本グループエントリ名の Chain ID コンポーネン
	トに一致します。

### L2 Multicast Group Entry Counters

フィールド	説明
Reference Count (Flow Entries)	現在このグループエントリを参照しているフローエントリまたはグループエントリの 数です。
Duration (Seconds)	グループエントリがセットされてから経過した時間(秒)です。

# L3 Unicast Group Entry Type

フィールド	説明
Group Identifier	32 ビットの符号なし整数で、OpenFlow のグループを一意に識別します。命名規則は
	L3 Unicast Group Entry Naming Conversion テーブルの通りです。
Group Type	グループのタイプは Indirect です。
Counters	グループ毎のエントリカウンタを指定します。
Action Buckets	単一のアクションバケットがサポートされます。

### L3 Unicast Group Entry Naming Conversion

フィールド	Bits	説明
ID	0-27	本タイプのグループエントリを区別するためのインデックス値です。
Kind	28-31	2 (L3 ユニキャスト)

### L3 Unicast Group Entry Bucket Actions

フィールド	説明
Group	このフィールドはレイヤ2インタフェースグループエントリに紐づく必要があります。
Decremented TTL	デクリメント TTL です。
	注意 不正な TTL の検証はサポートされていません。
Set-Field	ETH_DST、ETH_SRC、VLAN_VID フィールドを設定します(オプション)。

### L3 Unicast Group Entry Counters

フィールド	説明
Reference Count (Flow Entries)	現在このグループエントリを参照しているフローエントリまたはグループエントリの 数です。
Duration (Seconds)	グループエントリがセットされてから経過した時間(秒)です。

# 付録

# L3 ECMP Group Entry Type

フィールド	説明
Group Identifier	32 ビットの符号なし整数で、OpenFlow のグループを一意に識別します。命名規則は L3 ECMP Group Entry Naming Conversion テーブルの通りです。
Group Type	グループのタイプは Select です。
Counters	グループ毎のエントリカウンタを指定します。
Action Buckets	単一のアクションバケットがサポートされます。

# L3 ECMP Group Entry Naming Conversion

フィールド	Bits	説明
ID	0-27	レイヤ 3 ECMP グループエントリを区別するために使用されます。
Kind	28-31	7 (L3 ECMP)

#### L3 ECMP Group Entry Bucket Actions

フィールド	説明
Group	レイヤ3ユニキャストグループエントリに紐付きます。

### L3 ECMP Group Entry Counters

フィールド	説明
Reference Count (Flow Entries)	現在このグループエントリを参照しているフローエントリまたはグループエントリの 数です。
Duration (Seconds)	グループエントリがセットされてから経過した時間(秒)です。

### Meter Table Entry Parameters

フィールド	説明
Meter Identifier	メーターインスタンスです。
Flags	ビット位置です。 ・ 0:Kbps(Kbps」と「Packets」は同時に使用できません) ・ 1:Packets(Kbps」と「Packets」は同時に使用できません) ・ 2:Burst(必須) ・ 3:Stats(サポートされていません)
Meter Bands	1つのメーター帯域のみサポートされています。
Counters	メーター毎のエントリカウンタを指定します。

### **Meter Entry Counters**

フィールド	説明
Flow Count	現在このメーターテーブルエントリを参照しているフローエントリ数です。
Input Packet Count	サポートされていません。
Input Byte Count	サポートされていません。
Duration (Seconds)	メーターテーブルエントリがセットされてから経過した時間(秒)です。

### Meter Band Configuration Parameters

フィールド	説明	
Band Type	帯域のタイプは Drop のみサポートされています。	
Rate	メーター帯域が選択される際に使用されます。帯域に適用される最小値のレートを定 義します。	
Burst	メーター帯域の粒度を定義します。	
Counters	サポートされていません。	

# 付録 E RADIUS 属性割り当て

本スイッチの RADIUS 属性割り当てが次のモジュールに使用されます。 「コンソール」「Telnet」「SSH」「Web」「802.1X」「MAC ベースアクセスコントロール」「WAC」

RADIUS 属性タイプ:

- 特権レベル
- イングレス/イーグレス帯域幅
- 802.1p 初期値優先度
- VLAN
- ACL

RADIUS サーバで特権レベルを割り当てるには、適切なパラメータが RADIUS サーバで設定されている必要があります。以下は帯域幅のパラメータを表しています。

#### ベンダ指定属性パラメータ

ベンダ指定属性	説明	値	使用法
Vendor-ID	ベンダ定義	171 (DLINK)	必須
Vendor-Type	属性定義	1	必須
Attribute-Specific Field	スイッチを操作するユーザの特権レベルの 割り当てに使用します。	範囲(1-15)	必須

ユーザが RADIUS サーバの特権レベル属性(例えば、レベル 15)を設定し、コンソール、Telnet、SSH、Web 認証が成功した場合、デバイスは、 このアクセスユーザに特権レベル(RADIUS サーバによる)を割り当てます。しかしながら、ユーザが特権レベル属性を設定せず、認証に成功 した場合、デバイスはアクセスユーザにいかなる特権レベルも割り当てません。特権レベルは、最小サポート値よりも小さく、最大サポート値 よりも大きい場合、特権レベルは無視されます。

RADIUS サーバにより Ingress/Egress 帯域を割り当てるには、正しいパラメータが RADIUS サーバに設定されている必要があります。以下に、帯 域のパラメータを示します。

#### ベンダ指定属性パラメータ

ベンダ指定属性	説明	値	使用法
Vendor-ID	ベンダ定義	171 (DLINK)	必須
Vendor-Type	属性定義	2(イングレス帯域幅) 3(イーグレス帯域幅)	必須
Attribute-Specific Field	ポートの帯域幅の割り当に使用します。	ユニット (Kbits)	必須

ユーザが RADIUS サーバの帯域属性(例えば、イングレス帯域 1000Kbps)を設定し、802.1X、MAC ベースアクセスコントロール、WAC 認証に 成功した場合、デバイスはポートへ帯域(RADIUS サーバによる)を割り当てます。しかしながら、ユーザが帯域属性を設定せず、認証に成功 した場合、デバイスは、ポートにいかなる帯域も割り当てません。帯域属性が RADIUS サーバ上で "0"の値で設定されている場合、実効的な帯域は、 "no\_limited" に設定され、帯域が "0" より小さいもしくは最大サポート値よりも大きい場合、帯域は無視されます。

RADIUS サーバにより802.1p デフォルトプライオリティを割り当てるには、正しいパラメータがRADIUS サーバに設定されている必要があります。 以下に、802.1p デフォルトプライオリティのパラメータを示します。

#### ベンダ指定属性パラメータ

ベンダ指定属性	説明	値	使用法
Vendor-ID	ベンダ定義	171 (DLINK)	必須
Vendor-Type	属性定義	4	必須
Attribute-Specific Field	802.1p 初期値優先度の割り当に使用します。	0-7	必須

ユーザは、RADIUS サーバの 802.1p 優先度属性(例えば、優先度 7)を設定し、802.1X、MAC ベースアクセスコントロール、WAC 認証に成功した場合、 デバイスはポートに 802.1p デフォルト優先度(RADIUS サーバによる)を割り当てます。しかしながら、ユーザが優先度属性を設定せず、認証 が成功した場合、デバイスは、このポートにプライオリティを割り当てません。RADIUS サーバで設定された優先度属性が、範囲外の値(>7) である場合、デバイスに設定しません。

RADIUS サーバにより VLAN を割り当てるには、正しいパラメータが RADIUS サーバに設定されている必要があります。 VLAN 割り当てを使うため、 RFC3580 は RADIUS パケット内の以下のトンネル属性を定義しています。

#### VLAN のパラメータ

RADIUS トンネル属性	説明	値	使用法
Tunnel-Type	この属性は、使用される(トンネルイニシ エータの場合)トンネリングプロトコルもし くは、使用中の(トンネルターミネータの場 合)トンネリングプロトコルを示します。	13 (VLAN)	必須
Tunnel-Medium-Type	使用されるトランスポートミディアムタイ プ	6 (802)	必須
Tunnel-Private-Group-ID	特定のトンネルセッションのグループ ID	Aストリング(VID)	必須

### トンネルプライベートグループ ID 属性形式の概要

0		1	2	3
01234	45678	9 0 1 2 3 4 5	6 7 8 9 0 1 2 3 4	15678901
+-				
T	ype	Length	Tag	String
+-+-+-	+-+-+-+-	-+-+-+-+-+-+-+-	-+-+-+-+-+-+-+-+	+-+-+-+-+-+-+

#### タグフィールドの定義(異なる RFC 2868 の)

タグフィールド値	文字列のフィールド形式
0x01	VLAN 名(ASCII)
0x02	VLAN ID (ASCII)
他 (0x00, 0x03 ~ 0x1F, >0x1F)	スイッチが VLAN の設定文字列を受信するとき、まずはじめに VLAN ID と考えます。つまり、スイッチは すべての存在している VLAN ID を確認し、一致するものがあるかどうかを確認します。一致するものを検 出できた場合はその VLAN に移動し、検出できなかった場合は VLAN 設定文字列を VLAN 名だと考え、一致 する VLAN 名を検出できたことを確認します。

注意 0x1Fより大きなタグフィールドは次に続くフィールドの初めのオクテットとして判断されます。

ユーザが設定された RADIUS サーバの VLAN 属性(VID3 など)を持ち、802.1X、MAC ベースアクセスコントロール、または WAC 認証に成功した場合、ポートは VLAN3 が割り当てられます。しかしながら、ユーザが VLAN 属性を設定していない場合、ポートはゲスト VLAN メンバではないときは、現在の認証 VLAN にとどまり、ポートがゲスト VLAN メンバであるときは、元々の VLAN に割り当てられます。

RADIUS サーバで ACL を割り当てるには、適切なパラメータが RADIUS サーバで設定されている必要があります。以下は ACL のパラメータを表します。

#### ベンダ指定属性パラメータ

ベンダ指定属性	説明	値	使用法
Vendor-ID	ベンダ定義	171 (DLINK)	必須
Vendor-Type	属性定義	14 (ACL スクリプト )	必須
Attribute-Specific Field	ACL スクリプトの割り当てに使用します。 形式は Access Control List (ACL) コマンドに 基づきます。	ACL スクリプト 例: ip access-list a1;permit host 10.90.90.100;exit; mac access-list extended m1;permit host 00-00- 00-01-90-10 any; exit;	必須

ユーザは RADIUS サーバの ACL 属性を設定(ACL スクリプト: ip access-list a1;permit host 10.90.90.100;exit; mac access-list extended m1;permit host 00-00-01-90-10 any; exit; など)し、802.1X、MAC ベースアクセスコントロール、または WAC に成功した場合、デバイスは RADIUS サーバーによる ACL スクリプトを割り当てます。アクセスコンフィグモードに移行したり、出たりすることは対である必要があります。そうでなければ、ACP スクリプトは拒否されます。

# 付録 F IETF RADIUS 属性サポート

リモート認証ダイヤルインユーザサービス(RADIUS)属性は、特定の認証、承認、情報、リクエストとリプライに対する設定詳細を実行します。 本付録は現在スイッチによりサポートされる RADIUS 属性一覧です。

RADIUS 属性は、IETF 規格やベンダ特定属性(VSA)によりサポートされます。VSA は、ベンダが、追加で自身の RADIUS 属性を作成することを許可 します。D-Link VSA についてのより詳しい情報は、下記を参照してください。IETF 規格 RADIUS 属性は、RFC2865 リモート認証ダイヤルインユーザ サービス(RADIUS)、RFC2866 RADIUS アカウンティング、トンネルプロトコルサポートに対する RFC2868 RADIUS 属性、RFC2869 RADIUS 拡張で定 義されています。以下のリストは、D-LInk スイッチでサポートされた IETF RADIUS 属性です。

#### RADIUS 認証属性

ナンバー	IETF 属性
1	User-Name
2	User-Password
3	CHAP-Password
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
7	Framed-Protocol
8	Framed-IP-Address
12	Framed-MTU
18	Reply-Message
24	State
26	Vendor-Specific
27	Session-Timeout
29	Termination-Action
30	Called-Station-ID
31	Calling-Station-ID
32	NAS-Identifier
60	CHAP-Challenge
61	NAS-Port-Type
64	Tunnel-Type
65	Tunnel-Medium-Type
77	Connect-Info
79	EAP-Message
80	Message-Authenticator
81	Tunnel-Private-Group-ID
85	Acct-Interim-Interval
87	NAS-Port-ID
95	NAS-IPv6-Address

### RADIUS アカウンティング属性

ナンバー	IETF 属性
1	User-Name
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
8	Framed-IP-Address
31	Calling-Station-ID
32	NAS-Identifier
40	Acct-Status-Type
41	Acct-Delay-Time
42	Acct-Input-Octets
43	Acct-Output-Octets
44	Acct-Session-ID
45	Acct-Authentic
46	Acct-Session-Time
47	Acct-Input-Packets
48	Acct-Output-Packets
49	Acct-Terminate-Cause
52	Acct-Input-Gigawords
53	Acct-Output-Gigawords
61	NAS-Port-Type
95	NAS-IPv6-Address

# 付録 G 機能設定例

本項では、一般によく使う機能についての設定例を記載します。実際に設定を行う際の参考にしてください。

- Traffic Segmentation (トラフィックセグメンテーション)
- VLAN
- Link Aggregation (リンクアグリゲーション)
- Access List (アクセスリスト)
- Loopback Detection (LBD) (ループ検知)

# 対象機器について

本コンフィグレーションサンプルは以下の製品に対して有効な設定となります。

• DGS-3630

# Traffic Segmentation (トラフィックセグメンテーション)



図 20-1 Traffic Segmentation (DGS-3630-28TC)

#### 概要

ポート 1 ~ 16 に対し、トラフィックセグメンテーションを設定します。1 ~ 16 のポート間ではお互いに通信ができないようにし、ポート 1 ~ 16 は、 アップリンクポートとして使用するポート 23 とのみ通信ができるようにします。

### 設定手順

1. ポート(1-16)のセキュリティ設定をします。

```
Switch#configure terminal
Switch(config)#interface range ethernet 1/0/1-16
Switch(config-if-range)#traffic-segmentation forward interface ethernet 1/0/23
Switch(config-if-range)#end
```

2. 情報確認

Switch#show traffic-segmentation forward

注意 本機能を利用する場合、送信先 MAC アドレスが不明な Unknown ユニキャストについて、スイッチの全ポートにフラッドされます。

**3.** 設定を保存します。

Switch#copy running-config startup-config

VLAN



#### 概要

VLAN を設定します。ポート1~8に VLAN10を「Untagged」で割り当て、ポート9~16に VLAN20を「Untagged」で割り当て、ポート24において、VLAN10と VLAN20を「Tagged」で割り当てます。

#### 設定手順

1. VLAN10、VLAN20を作成します。

```
Switch#configure terminal
Switch(config)#vlan 10,20
Switch(config-vlan)#exit
```

2. ポート 1-8 に VLAN10、ポート 9-16 に VLAN20 を 割り当てます。

```
Switch#configure terminal
Switch(config)#interface range ethernet 1/0/1-8
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit
Switch(config)#interface range ethernet 1/0/9-16
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#end
```

3. 上位のネットワークへ接続されているポート 24 に VLAN10、20 の通信を転送することができるように、VLAN を設定します。

■設定方法①(hybrid mode を設定する場合)

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/24
Switch(config-if)#switchport mode hybrid
Switch(config-if)#switchport hybrid allowed vlan add tagged 10,20
Switch(config-if)#end
```

■設定方法②(hybrid mode を使用せず、trunk にて同様の設定を行う場合)

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/24
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan add 10,20
Switch(config-if)#end
```

**4.** 設定を保存します。

Switch#copy running-config startup-config

#### 5. 情報確認

Switch#show vlan

(作成した VLAN と各ポートに割り当てられている VLAN が表示されます。)

Switch#show vlan int ethernet 1/0/xx

(ポートに紐づいている VLAN 情報が表示されます。)

# Link Aggregation (リンクアグリゲーション)



#### 図 20-3 Link Aggregation (DGS-3630-28TC)

#### 概要

VLAN10 と 20 の Tagged VLAN を設定したポートにリンクアグリゲーションを設定します。ポート 22 と 24 に VLAN10 と VLAN20 を「Tagged」で 割り当て、ポート 22 と 24 をグループ 1 として LACP によるリンクアグリゲーションに設定します。

#### 設定手順(Switch1、Switch2 共通)

1. VLAN10、VLAN20を作成します。

Switc'	h#configure terminal
Switc	h(config)#vlan 10,20
Switc	h(config-vlan)#exit

2. Link Aggregation (LACP) のグループを作成します。

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/22
Switch(config-if)#channel-group 1 mode active
Switch(config-if)#exit
Switch(config)#interface ethernet 1/0/24
Switch(config-if)#channel-group 1 mode active
Switch(config-if)#exit
```

3. Link Aggregation のポートを設定します。

Switch(config)#interface port-channel 1

- 4. 作成した port-channel に VLAN を設定します。
  - LAG ポートに設定する VLAN は、各物理インターフェイス上では設定せず、Port-channel インターフェイス上で VLAN の設定を行います。

```
Switch(config)#interface port-channel 1
Switch(config if)#switchport mode trunk
Switch(config if)#switchport trunk native vlan 1
Switch(config if)#switchport trunk allowed vlan 1,10,20
Switch(config if)#exit
Switch(config)#exit
```

5. 設定を保存します。

Switch#copy running-config startup-config

- 6. 情報確認
  - Port-channel に設定されている VLAN 情報を表示します。

Switch#show vlan interface port-channel 1

- グループ番号とグループで使用されている Protocol を表示します。

Switch#show channel-group

- 各グループに所属している Port 番号と、リンクアグリゲーションの状態を表示します。

Switch#show channel-group channel 1 detail

# Access List(アクセスリスト)



図 20-4 Access List (DGS-3630-28TC)

#### 概要

ポート1~16に対し、アクセスリストを設定します。ポート1~16に接続される端末のIPの中から、「192.168.2.50」の端末から社内サーバ(192.168.2.200) へのアクセスは許可し、それ以外の端末から社内サーバへのアクセスは禁止するように設定します。

#### 設定手順

アクセスリストに名前 (extended ACL) を付けて定義します。
 「192.168.2.50 ⇔ 192.168.2.200」間の通信を許可するルールを追加します。
 「192.168.2.200」へのすべての通信を拒否するルールを追加します。

```
Switch#configure terminal
Switch(config)#ip access-list extended ACL
Switch(config-ip-ext-acl)#permit 192.168.2.50 0.0.0.0 192.168.2.200 0.0.0.0
Switch(config-ip-ext-acl)#deny any 192.168.2.200 0.0.0.0
Switch(config-ip-ext-acl)#end
```

2. アクセスリストのルールを、適用対象ポート1~16へ設定します。

```
Switch#configure terminal
Switch(config)#interface range ethernet 1/0/1-16
Switch(config-if-range)#ip access-group ACL in
Switch(config-if-range)#end
```

3. 設定を保存します。

Switch#copy running-config startup-config

4. 情報確認

```
Switch#show access-list
Switch#show access-list ip
Switch#show access-group
```

# Loopback Detection (LBD) (ループ検知)



(ポート1-8)

図 20-5 Loopback Detection (DGS-3630-28TC)

#### 概要

ポート 1~8 に対しループバック検知を設定します。ポート 1~8 でループを検知した際、ポートをシャットダウンするように設定します。

#### 設定手順

1. ポートベースでループ検知機能を動作させ、ループ検知後はポートをシャットダウンする設定をします。

```
Switch#enable
Switch#configure terminal
Switch(config)#loopback-detection
Switch(config)#loopback-detection mode port-based
```

2. ループ発生を確認する間隔を 20 秒に設定します。

Switch(config)#loopback-detection interval 20

3. (必要に応じて)ループ発生後のループ解消確認間隔を 20 秒に設定し、ループ解消確認後、自動で Port 開放するように設定します。

Switch(config)#errdisable recovery cause loopback-detect interval 20

- 注意 この設定をしない場合、永続的にポートが「shutdown」状態となります。ポートを開放する場合、該当のポートに対し、インターフェイスモードにて「no shutdown」コマンドを投入する必要があります。
- 4. ポート 1-8 でループバック検知機能を有効にします。

Switch(config)#interface range ethernet 1/0/1-8 Switch(config-if-range)#spanning-tree state disable Switch(config-if-range)#loopback-detection Switch(config-if-range)#end



「spanning-tree」が「enable」になっている場合、ループ検知機能を設定できないため、設定するインターフェイスの「spanning-tree」の 設定をまず「disable」にします。

注意 「spanning-tree」はデフォルトでグローバルでは「disable」に設定されていますが、各インターフェイス「enable」となっています。各イ ンターフェイスにて「disable」設定が必要となります。

5. show コマンドで「Spanning Tree」が無効になっているかを確認します。

Switch#show spanning-tree configuration interface ethernet 1/0/1-8

6. 「Spanning Tree」がポート単位で「disable」に設定されている場合、ステータスが Disabled と表示されます。

Spanning tree state : Disabled

7. 設定を保存します。

Switch#copy running-config startup-config

#### **8.** 情報確認

Switch#show loopback-detection

(ループ検知の有効/無効、設定しているモード、対象の VLAN、各ポートのループ状態等を表示します。)

Switch#show errdisable recovery

(ループ解消後の自動ポート解放設定 有効 / 無効、確認間隔を表示します。)